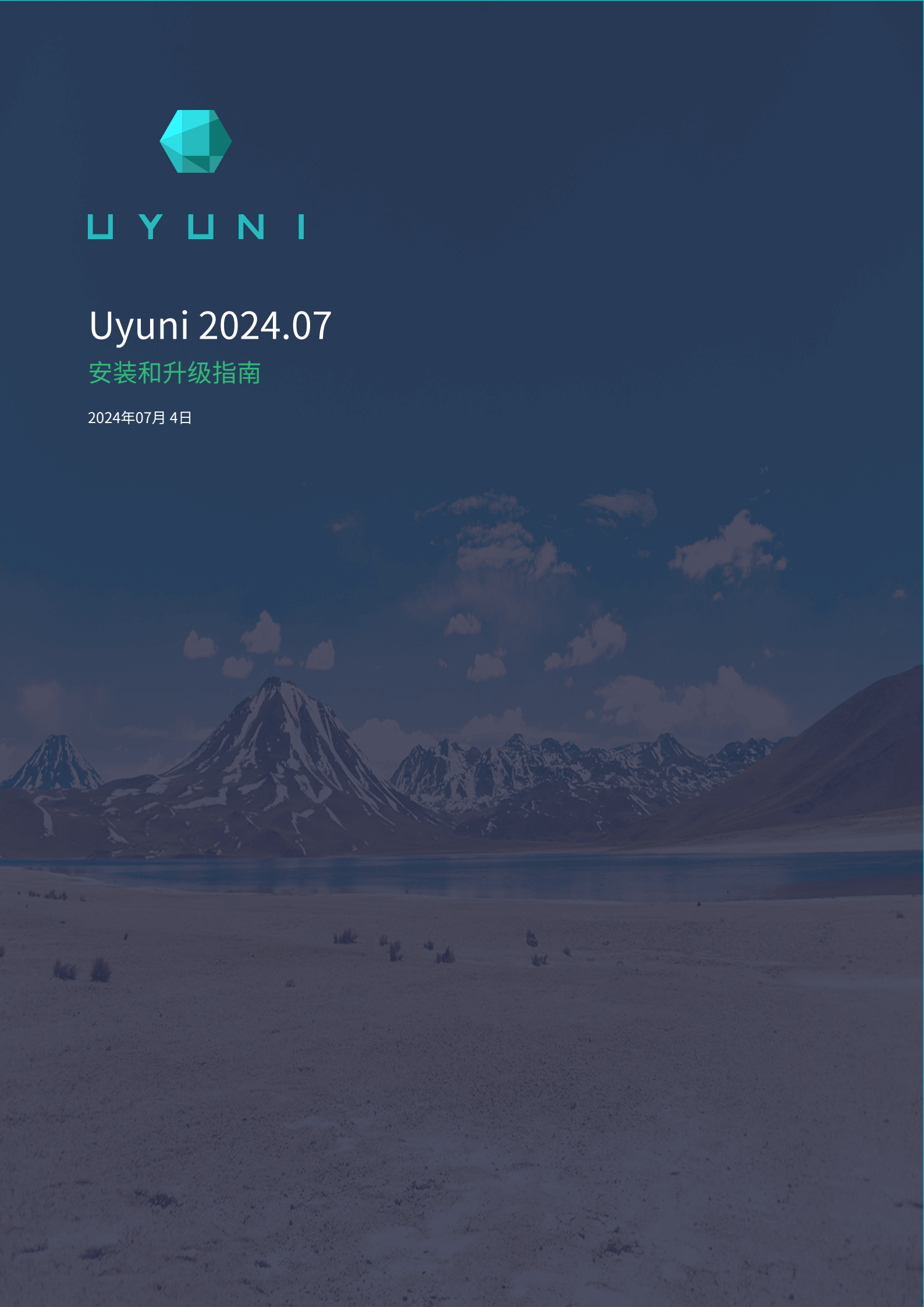


Uyuni 2024.07

安装和升级指南

2024年07月 4日

目录

Deployment and Upgrade Guide Overview

更新日期：2024-07-04

This book provides guidance on deploying and upgrading Uyuni Server and Proxy. It is split into the following sections:

要求

Describes hardware, software, and networking requirements before you begin.

Deployment

Describes tasks for deploying Uyuni as a container and initial setup.

Upgrade and Migration

Describes upgrade and migration of Uyuni

公有云

You can also deploy Uyuni to a public cloud instance.

For more information on using Uyuni on a public cloud, see **Specialized-guides › Public-cloud-guide**.

Chapter 1. 要求

1.1. 要求

下表指定了服务器和代理的最低要求。

1.1.1. 服务器要求

表格 1. x86-64 体系结构的服务器要求

软件和硬件	细节	建议
openSUSE Leap 15.5	干净安装，最新版本	openSUSE Leap 15.5
CPU		至少 4 个专用 64 位 CPU 核心 (x86-64)
RAM	测试或基础安装	至少 16 GB
	生产服务器	至少 32 GB
磁盘空间	/（根目录）	至少 40 GB
	`/var/lib/pgsql`	至少 50 GB
	`/var/spacewalk`	至少所需的存储空间：100 GB（实施的检查功能将会校验是否满足这一点） * 每个 SUSE 产品和软件包中心 50 GB 360 GB for each Red Hat product
	`/var/cache`	Minimum 10 GB. Add 100 MB per SUSE product, 1 GB per Red Hat or other product. Double the space if the server is an ISS Master.
	Swap space	3 GB

1.1.2. 代理要求

表格 2. 代理要求

Software and Hardware	Details	Recommendation
openSUSE Leap 15.5	Clean installation, up-to-date	openSUSE Leap 15.5
CPU		Minimum 2 dedicated 64-bit CPU cores
RAM	Test Server	Minimum 2 GB
	Production Server	Minimum 8 GB

Software and Hardware	Details	Recommendation
Disk Space	/ (root directory)	Minimum 40 GB
	/srv	Minimum 100 GB
	/var/cache (Squid)	Minimum 100 GB

Uyuni Proxy 将软件包缓存在 /var/cache/ 目录中。如果 /var/cache/ 中的可用空间不足，代理将去除旧的未使用软件包，并将其替换为较新的软件包。

鉴于这种行为：

- 代理上的 /var/cache/ 目录越大，代理与 Uyuni 服务器之间的流量就越少。
- 使代理上的 /var/cache/ 目录与 Uyuni 服务器上的 /var/spacewalk/ 保持相同的大小，可以避免在首次同步后出现大量的流量。
- Uyuni 服务器上的 /var/cache/ 目录相比代理上的目录可能较小。 有关大小估算的指导，请参见 [server-hardware-requirements] 一节。

1.2. 网络要求

本节详细说明 Uyuni 的网络和端口要求。

1.2.1. 完全限定的域名 (FQDN)

Uyuni 服务器必须正确解析其 FQDN。如果无法解析 FQDN，可能会导致许多不同的组件出现严重问题。

For more information about configuring the hostname and DNS, see https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-network.html#sec-network-yast-change-host.

1.2.2. 主机名和 IP 地址

为确保 Uyuni 域名可由其客户端解析，服务器和客户端计算机都必须连接到一台正常工作的 DNS 服务器。还需要确保正确配置反向查找。

For more information about setting up a DNS server, see https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-dns.html.

1.2.3. Air-gapped Deployment

If you are on an internal network and do not have access to SUSE Customer Center, you can use an **Installation-and-upgrade › Container-deployment**.

在生产环境中，Uyuni Server 和客户端始终应使用防火墙。有关所需端口的完整列表，请参见 **Installation-and-upgrade › Ports**。

1.2.4. Ports

本节提供了 Uyuni 中各种通讯使用的端口的综合列表。

您不需要打开所有这些端口。某些端口只有在您使用需要这些端口的服务时才需打开。

1.2.4.1. 外部入站服务器端口

必须打开外部入站端口，以在 Uyuni 服务器上配置防火墙用于防范未经授权访问服务器。

打开这些端口将允许外部网络流量访问 Uyuni 服务器。

表格 3. Uyuni Server 的外部端口要求

Port number	Protocol	Used By	Notes
22			Required for ssh-push and ssh-push-tunnel contact methods.
67	TCP/UDP	DHCP	Required only if clients are requesting IP addresses from the server.
69	TCP/UDP	TFTP	Required if server is used as a PXE server for automated client installation.
80	TCP	HTTP	Required temporarily for some bootstrap repositories and automated installations.
443	TCP	HTTPS	Serves the Web UI, client, and server and proxy (`tftpsync`) requests.
4505	TCP	salt	Required to accept communication requests from clients. The client initiates the connection, and it stays open to receive commands from the Salt master.
4506	TCP	salt	Required to accept communication requests from clients. The client initiates the connection, and it stays open to report results back to the Salt master.
25151	TCP	Cobbler	

1.2.4.2. 外部出站服务器端口

必须打开外部出站端口，以在 Uyuni 服务器上配置防火墙用于限制服务器可访问的内容。

打开这些端口将允许来自 Uyuni 服务器的网络流量与外部服务通讯。

表格 4. Uyuni Server 的外部端口要求

Port number	Protocol	Used By	Notes
80	TCP	HTTP	Required for SUSE Customer Center. Port 80 is not used to serve the Web UI.

Port number	Protocol	Used By	Notes
443	TCP	HTTPS	Required for SUSE Customer Center.
25151	TCP	Cobbler	

1.2.4.3. 内部服务器端口

内部端口由 Uyuni 服务器在内部使用。只能从 `localhost` 访问内部端口。

大多数情况下无需调整这些端口。

表格 5. Uyuni Server 的内部端口要求

端口号	备注
2828	Satellite-search API，由 Tomcat 和 Taskomatic 中的 RHN 应用程序使用。
2829	Taskomatic API，由 Tomcat 中的 RHN 应用程序使用。
8005	Tomcat 关机端口。
8009	Tomcat 到 Apache HTTPD (AJP)。
8080	Tomcat 到 Apache HTTPD (HTTP)。
9080	Salt-API，由 Tomcat 和 Taskomatic 中的 RHN 应用程序使用。
32000	与运行 Taskomatic 和 satellite-search 的 Java 虚拟机 (JVM) 建立 TCP 连接时使用的端口。

32768 和更高的端口用作临时端口。这些端口往往用于接收 TCP 连接。收到 TCP 连接请求后，发送方将选择其中一个临时端口号来与目标端口进行匹配。

可使用以下命令来确定哪些端口是临时端口：

```
cat /proc/sys/net/ipv4/ip_local_port_range
```

1.2.4.4. 外部入站代理端口

必须打开外部入站端口，以在 Uyuni Proxy 上配置防火墙用于防范未经授权访问代理。

打开这些端口将允许外部网络流量访问 Uyuni Proxy。

表格 6. Uyuni Proxy 的外部端口要求

Port number	Protocol	Used By	Notes
22			Required for ssh-push and ssh-push-tunnel contact methods. Clients connected to the proxy initiate check in on the server and hop through to clients.

Port number	Protocol	Used By	Notes
67	TCP/UDP	DHCP	Required only if clients are requesting IP addresses from the server.
69	TCP/UDP	TFTP	Required if the server is used as a PXE server for automated client installation.
443	TCP	HTTPS	Web UI, client, and server and proxy (`tftpsync`) requests.
4505	TCP	salt	Required to accept communication requests from clients. The client initiates the connection, and it stays open to receive commands from the Salt master.
4506	TCP	salt	Required to accept communication requests from clients. The client initiates the connection, and it stays open to report results back to the Salt master.

1.2.4.5. 外部出站代理端口

必须打开外部出站端口，以在 Uyuni Proxy 上配置防火墙用于限制代理可访问的内容。

打开这些端口将允许来自 Uyuni Proxy 的网络流量与外部服务通讯。

表格 7. Uyuni Proxy 的外部端口要求

Port number	Protocol	Used By	Notes
80			Used to reach the server.
443	TCP	HTTPS	Required for SUSE Customer Center.

1.2.4.6. 外部客户端端口

必须打开外部客户端端口，以在 Uyuni 服务器及其客户端之间配置防火墙。

大多数情况下无需调整这些端口。

表格 8. Uyuni 客户端的外部端口要求

Port number	Direction	Protocol	Notes
22	Inbound	SSH	Required for ssh-push and ssh-push-tunnel contact methods.
80	Outbound		Used to reach the server or proxy.
9090	Outbound	TCP	Required for Prometheus user interface.
9093	Outbound	TCP	Required for Prometheus alert manager.
9100	Outbound	TCP	Required for Prometheus node exporter.
9117	Outbound	TCP	Required for Prometheus Apache exporter.

Port number	Direction	Protocol	Notes
9187	Outbound	TCP	Required for Prometheus PostgreSQL.

1.2.4.7. 所需的 URL

Uyuni 必须能够访问某些 URL 才能注册客户端和执行更新。大多数情况下，允许访问以下 URL 便已足够：

- scc.suse.com
- updates.suse.com

如果您正在使用非 SUSE 客户端，则还可能需要允许访问为这些操作系统提供特定软件包的其他服务器。例如，如果您使用的是 Ubuntu 客户端，则需要能够访问 Ubuntu 服务器。

有关为非 SUSE 客户端排查防火墙访问权限问题的详细信息，请参见 **Administration › Troubleshooting**。

1.3. 公有云要求

本节介绍在公有云基础结构上安装 Uyuni 所要满足的要求。我们已在 Amazon EC2、Google Compute Engine 和 Microsoft Azure 上对这些指令进行过测试，不过它们进行一定修改后在其他提供商的云服务上也应能正常工作。

在开始之前，请注意以下一些事项：

- Uyuni 设置过程执行正向确认的反向 DNS 查找。此操作必须成功，设置过程才能完成，并且 Uyuni 才能按预期方式运行。请务必在设置 Uyuni 之前执行主机名和 IP 配置。
- Uyuni Server 和 Proxy 实例需在适当的网络配置中运行，该网络配置可让您控制 DNS 项，但无法通过因特网自由访问。
- 在此网络配置中必须提供 DNS 解析：`hostname -f` 必须返回完全限定的域名 (FQDN)。
- DNS 解析对于连接客户端也很重要。
- DNS 取决于所选的云框架。有关详细说明，请参见云提供商文档。
- 我们建议将软件储存库、服务器数据库和代理 squid 缓存存储在外部虚拟磁盘上。这可以防止在实例意外终止时丢失数据。本节包含有关设置外部虚拟磁盘的说明。

1.3.1. 网络要求

在公有云上使用 Uyuni 时，必须使用受限制的网络。我们建议使用带有适当防火墙设置的 VPN 专用子网。只能允许指定 IP 范围内的计算机访问该实例。

在公有云上运行 Uyuni 意味着需要实施强大的安全措施。限制、过滤、监控并审计对实例的访问至关重要。SUSE 强烈建议不要配置全球均可访问但缺少充足边界安全保护的 Uyuni 实例。

要访问 Uyuni Web UI，请在配置网络访问控制时允许 HTTPS。这将允许您访问 Uyuni Web UI。

在 EC2 和 Azure 中，创建一个新安全组，并添加 HTTPS 入站和出站规则。在 GCE 中，选中¬¬¬¬¬¬部分下的¬¬¬¬ HTTPS ¬¬¬¬复选框。

1.3.2. Prepare Storage Volumes

We recommend that the repositories and the database for Uyuni are stored on separate storage devices from the root volume. This will help to avoid data loss and possibly increase performance.

The Uyuni container utilizes default storage locations. These locations should be configured prior to deployment for custom storage. For more information see **Installation-and-upgrade › Container-management**

Do not use logical volume management (LVM) for public cloud installations.

用于存储储存库的磁盘大小取决于您要使用 Uyuni 管理的发行套件和通道数目。挂接虚拟磁盘时，它们将作为 Unix 设备节点显示在实例中。设备节点的名称因提供商及所选实例类型而异。

确保 Uyuni 服务器的根卷大小不少于 100 GB。如果可能，请另外添加一个 500 GB 或以上大小的存储磁盘，并选择 SSD 存储类型。当您的实例启动时，Uyuni 服务器的云映像会使用脚本来指派这个单独的卷。

启动实例后，您便可登录 Uyuni 服务器，并使用以下命令查找所有可用的存储设备：

```
hwinfo --disk | grep -E "Device File:"
```

如果您不确定应选择哪个设备，可使用 `lsblk` 命令查看每个设备的名称和大小。请选择与要寻找的虚拟磁盘大小匹配的名称。

You can set up the external disk with the `mgr-storage-server` command. This creates an XFS partition mounted at `/manager_storage` and uses it as the location for the database and repositories:

```
/usr/bin/mgr-storage-server <devicename>
```

Chapter 2. Deployment and Installation

2.1. Server

2.1.1. Deploy on openSUSE Leap Micro 5.5

2.1.1.1. Deployment preparations

In this section, you will gain expertise in setting up and deploying a Uyuni Server. The process encompasses the installation of `Podman`, `Uyuni container utilities`, deployment, and then initiating interaction with the container through `mgrctl`.

This section assumes you have already configured an openSUSE Leap Micro 5.5 host server, whether it is running on a physical machine or within a virtual environment.

2.1.1.2. Container Host general requirements

For general requirements, see **Installation-and-upgrade › General-requirements**.

An openSUSE Leap Micro 5.5 server should be installed from installation media. This procedure is described below.

2.1.1.3. 容器主机要求

For CPU, RAM, and storage requirements, see **Installation-and-upgrade › Hardware-requirements**.

To guarantee that clients can resolve the FQDN domain name, both the containerized server and the host machines must be linked to a functional DNS server. Additionally, it is essential to ensure correct configuration of reverse lookups.

2.1.1.4. Installing Uyuni tools for use with containers

Procedure: Installing Uyuni Tools on openSUSE Leap Micro 5.5

1. On your local host open a terminal window or start up a virtual machine running openSUSE Leap Micro 5.5.
2. Login.
3. Enter the `transactional-update shell`:

```
transactional-update shell
```

4. Add the following repository to your openSUSE Leap Micro 5.5 server:

```
zypper ar
https://download.opensuse.org/repositories/systemsmanagement:/Uyuni:
/Stable:/ContainerUtils/openSUSE_Leap_Micro_5.5/systemsmanagement:Uy
uni:Stable:ContainerUtils.repo
```

5. Refresh the repository list and accept the key:

```
zypper ref
```

6. Install the container tools:

```
zypper in mgradm mgrctl mgradm-bash-completion mgrctl-bash-
completion netavark
```

7. Exit the transactional shell:

```
transactional update # exit
```

8. Reboot the host.

For more information on the Uyuni Container Utilities, see Uyuni Container Utilities.

2.1.1.5. Configure Custom Persistent Storage

This step is optional. However, if custom persistent storage is required for your infrastructure, use the `mgr-storage-server` tool.

For more information, see `mgr-storage-server --help`. This tool simplifies creating the container storage and database volumes.

Use the command in the following manner:

+

```
mgr-storage-server <storage-disk-device> [<database-disk-device>]
```

For example:

```
mgr-storage-server /dev/nvme1n1 /dev/nvme2n1
```

+

This command will create the persistent storage volumes at `/var/lib/containers/storage/volumes`.

For more information, see **Installation-and-upgrade › Container-management**.

2.1.1.6. Deploying an Uyuni container with Podman

2.1.1.6.1. mgradm overview

Uyuni is deployed as a container using the `mgradm` tool. There are two methods of deploying a Uyuni server as a container. In this section we will focus on basic container deployment.

For information on using a custom configuration file to deploy, see **Installation-and-upgrade › Container-management**.

For additional information, you can explore further by running `mgradm --help` from the command line.

Procedure: Deploying an Uyuni container with Podman

1. From the terminal run the following command as the sudo user or as root.

```
sudo mgradm install podman
```

You must deploy the container as sudo or root. The following error will be displayed at the terminal if you miss this step.

```
INF Setting up uyuni network
9:58AM INF Enabling system service
9:58AM FTL Failed to open
/etc/systemd/system/uyuni-server.service for
writing error="open /etc/systemd/system/uyuni-
server.service: permission denied"
```

2. Wait for deployment to complete.
3. Open a browser and proceed to your servers FQDN.

In this section you learned how to deploy an Uyuni Server container.

2.1.1.6.2. Persistent volumes

Many users will want to specify locations for their persistent volumes.

If you are just testing out Uyuni you do not need to specify these volumes. `mgradm` will setup the correct volumes by default.

Specifying volume locations will generally be used for larger production deployments.

By default `podman` stores its volumes in `/var/lib/containers/storage/volumes/`.

You can provide custom storage for the volumes by mounting disks on this path or the expected volume path inside it such as: `/var/lib/containers/storage/volumes/var-spacewalk`. This is especially important for the database and package mirrors.

For a list of all persistent volumes in the container, see **Installation-and-upgrade › Container-management**.

2.1.2. Uyuni Server Air-gapped Deployment

2.1.2.1. What is air-gapped deployment?

Air-gapped deployment refers to the setup and operation of any networked system that is physically isolated from insecure networks, especially the internet. This type of deployment is commonly used in high-security environments such as military installations, financial systems, critical infrastructure, and anywhere sensitive data is handled and must be protected from external threats.

You can easily deploy container images using `Podman`, `Docker`, or `Skopeo` on a machine with internet access.

Pull the desired image then, save the image as a tar archive. For example:

列表 1. Podman

```
podman pull registry.suse.com/suse/manager/5.0/x86_64/server:5.0.0-beta2
podman save --output server.tar
registry.suse.com/suse/manager/5.0/x86_64/server:5.0.0-beta2
```

列表 2. Docker

```
docker pull registry.suse.com/suse/manager/5.0/x86_64/server:5.0.0-beta2
docker save --output server.tar
registry.suse.com/suse/manager/5.0/x86_64/server:5.0.0-beta2
```

列表 3. Skopeo

```
skopeo copy
docker://registry.suse.com/suse/manager/5.0/x86_64/server:5.0.0-beta2
docker-
archive:server.tar:registry.suse.com/suse/manager/5.0/x86_64/server:5.0.0
-beta2
```

Transfer the resulting `server-image.tar` to the Server container host and load it using the following command:

列表 4. Load the Server Image

```
podman load -i server.tar
```

2.2. Install the Server (Legacy)

2.2.1. 安装使用 openSUSE 的 Uyuni Server

可以在 openSUSE 上安装 Uyuni Server。

有关要求，请参见 **Installation-and-upgrade › Uyuni-install-requirements**。

有关 openSUSE Leap 最新版本和更新的详细信息，请参见 https://doc.opensuse.org/release-notes/。

2.2.1.1. 在 openSUSE Leap 上安装 Uyuni

过程：安装包含 Uyuni 的 openSUSE Leap

1. 安装应用了所有可用服务包和软件包更新的 openSUSE Leap 作为基础系统。
2. 通过 **yast › 系统 › 网络设置 › 主机名/DNS** 配置一个可解析的完全限定域名 (FQDN)。
3. 以 `root` 身份设置用于创建储存库的变量：

```
repo=repositories/systemsmanagement:/
repo=${repo}Uyuni:/Stable/images/repo/Uyuni-Server-POOL-x86_64-
Media1/
```

4. 以 `root` 身份添加用于安装 Uyuni Server 软件的储存库：

```
zypper ar https://download.opensuse.org/$repo uyuni-server-stable
```

5. 以 root 身份刷新储存库中的元数据：

```
zypper ref
```

6. 以 root 身份安装 Uyuni Server 的软件集：

```
zypper in patterns-uyuni_server
```

7. 重引导。
    - 有关稳定版 Uyuni 的详细信息，请参见 https://www.uyuni-project.org/pages/stable-version.html。
    - 有关开发版 Uyuni 的详细信息，请参见 https://www.uyuni-project.org/pages/devel-version.html。

安装完成后，可以继续设置 Uyuni。有关详细信息，请参见 **Installation-and-upgrade › Uyuni-server-setup**。

2.3. Migration

2.3.1. Migrating the Uyuni server to a containerized environment

To migrate a regular Uyuni server to a container, a new machine is required.

It is not possible to perform an in-place migration.

The original server is referred to as the **source server,** while the newly set-up machine is designated as the **destination server.**

The migration procedure currently does not include any hostname renaming functionality. Consequently, the fully qualified domain name (FQDN) on the new server will remain identical to that on the source server. Therefore, following migration, it will be necessary to manually adjust the DNS records to point to the new server.

Procedure: Initial preparation

1. Stop the source server:

```
spacewalk-service stop
```

2. Stop the source services:

```
systemctl stop postgresql
```

Procedure: Preparing the SSH connection

1. The SSH configuration and agent should be ready on the host for a passwordless connection to the source server.

To establish a passwordless connection, the migration script relies on an SSH agent running on the server. If one isn't active yet, initiate it by running `eval $(ssh-agent)`. Then, add the SSH key to the running agent with `ssh-add /path/to/the/private/key`. You'll be prompted to enter the password for the private key during this process.

2. The migration script only uses the source server fully qualified domain name in the SSH command.
3. This means that every other configuration required to connect needs to be defined in the `~/.ssh/config` file.

2.3.1.1. Prepare for Kubernetes

Before executing the migration command with mgradm migrate, it's essential to predefine **Persistent Volumes**, especially considering that the migration job initiates the container from scratch. Please consult the installation section for comprehensive guidance on preparing these volumes.

See: **Installation-and-upgrade › Container-management**

2.3.1.2. Migrating

Execute the following command to install a new Uyuni server, replacing **<Uyuni.source.fqdn>** with the appropriate FQDN of the source server:

```
mgradm migrate podman <{productname}.source.fqdn>
```

或

```
mgradm migrate kubernetes <{productname}.source.fqdn>
```

After successfully running the `mgradm migrate` command, the Salt setup on all clients will still point to the old server (source server). To redirect them to the new server (destination server), it is required to rename the new server at the infrastructure level (DHCP and DNS) to use the same Fully Qualified Domain Name and IP address as old server (source server).

2.4. Proxy

2.4.1. 容器化 Uyuni Proxy 设置

为 Uyuni Proxy 容器准备好容器主机后，需要额外执行几步容器设置才能完成配置。

1. 生成 Uyuni Proxy 配置存档文件
2. 将配置存档传输到在安装步骤中准备的容器主机并解压缩
3. Start the proxy sevices with `mgrpxy`

2.4.1.1. Generate the Proxy Configuration

The configuration archive of the Uyuni Proxy is generated by the Uyuni Server. Each additional Proxy requires its own configuration archive.

2 GB represents the default proxy squid cache size. This will need to be adjusted for your environment.

For Podman deployment, the container host for the Uyuni Proxy must be registered as a client to the Uyuni Server prior to generating this proxy configuration.

If a proxy FQDN is used to generate a proxy container configuration that is not a registered client (as in the Kubernetes use case), a new system entry will appear in system list. This new entry will be shown under previously entered Proxy FQDN value and will be of `Foreign` system type.

2.4.1.1.1. Generate the Proxy Configuration with Web UI

Procedure: Generating a Proxy Container Configuration using Web UI

1. 在 Web UI 中，导航到**系统 › 代理配置**，然后填写所需数据：
2. 在¬¬¬¬ FQDN字段中，键入代理的完全限定域名。
3. 在¬¬ FQDN字段中，键入 Uyuni 服务器或另一个 Uyuni 代理的完全限定域名。
4. 在¬¬¬¬ SSH ¬¬¬¬字段中，键入 SSH 服务在 Uyuni 代理上监听的 SSH 端口。建议保留默认值 8022。
5. In the `Max Squid cache size [MB]` field type maximal allowed size for Squid cache. Recommended is to use at most 60% of available storage for the containers.

2 GB represents the default proxy squid cache size. This will need to be adjusted for your environment.

在 SSH ¬¬¬¬选择列表中，选择应为 Uyuni 代理生成新服务器证书还是使用现有证书。您可以考虑作为 Uyuni 内置（自我签名）证书生成的证书。

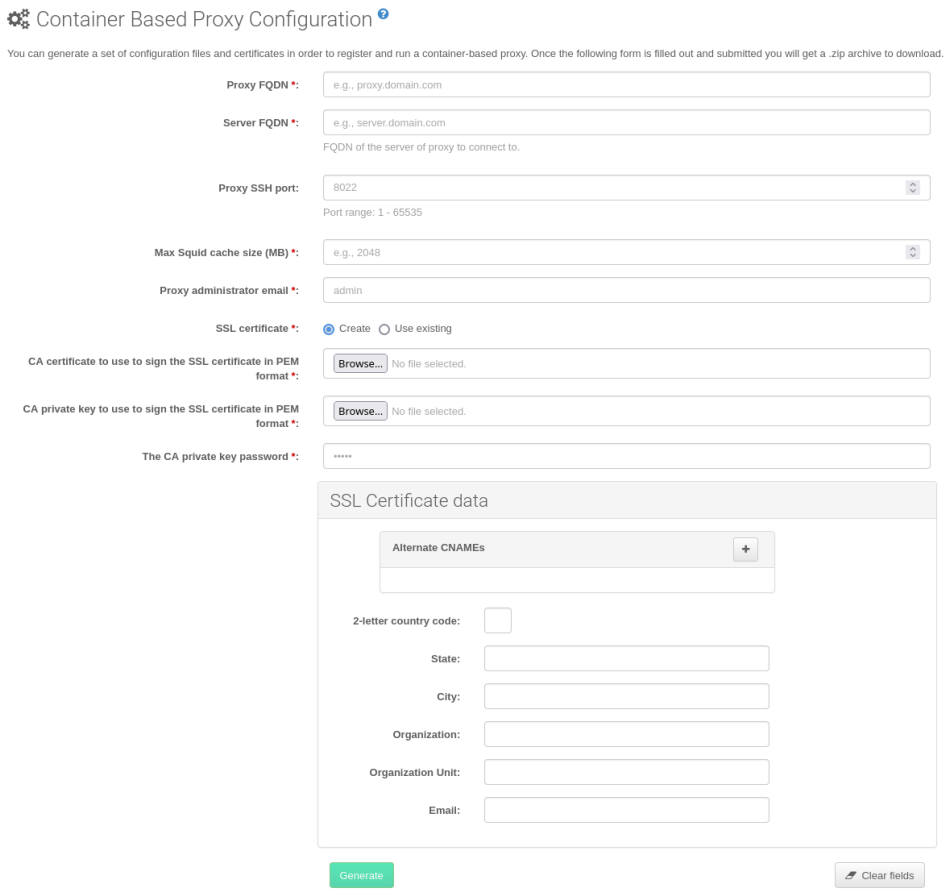
+ 然后根据所做的选择提供用于生成新证书的签名 CA 证书的路径，或者要用作代理证书的现有证书及其密钥的路径。

+ The CA certificates generated by the server are stored in the

`/var/lib/containers/storage/volumes/root/_data/ssl-build` directory.

+ 有关现有或自定义证书的详细信息以及企业和中间证书的概念，请参见 **Administration › Ssl-certs-imported**。

1. Click [Generate] to register a new proxy FQDN in the Uyuni Server and generate a configuration archive (`config.tar.gz`) containing details for the container host.
2. After a few moments you are presented with file to download. Save this file locally.



2.4.1.1.2. Generate the Proxy Configuration with spacecmd and Self-Signed Certificate

Procedure: Generating Proxy Configuration with spacecmd and Self-Signed Certificate

You can generate a Proxy configuration using spacecmd.

1. SSH into your container host.
2. Execute the following command replacing the Server and Proxy FQDN:

```
mgrctl exec -ti 'spacecmd proxy_container_config_generate_cert --
dev-pxy.example.com dev-srv.example.com 2048 email@example.com' -o
/tmp/config.tar.gz
```

3. Copy the generated configuration from the server container:

```
mgrctl cp server:/tmp/config.tar.gz .
```

2.4.1.1.3. Generate the Proxy Configuration with spacecmd and Custom Certificate

You can generate a Proxy configuration using spacecmd for a custom certificates rather than the default self-signed certificates.

Procedure: Generating Proxy Configuration with spacecmd and Custom Certificate

1. SSH into your Server container host.
2. Execute the following command replacing the Server and Proxy FQDN:

```
for f in ca.crt proxy.crt proxy.key; do
  mgrctl cp $f server:/tmp/$f
done
mgrctl exec -ti 'spacecmd proxy_container_config -- -p 8022
pxy.example.com srv.example.com 2048 email@example.com /tmp/ca.crt
/tmp/proxy.crt /tmp/proxy.key -o /tmp/config.tar.gz'
```

3. Copy the generated configuration from the server container:

```
mgrctl cp server:/tmp/config.tar.gz .
```

2.4.1.2. 传输 Uyuni Proxy 配置

Both spacecmd command and Web UI ways generate a configuration archive. This archive needs to be made available on container host.

Transfer this generated archive to the container host.

For installation instructions to use the archive to get the proxy containers, see **Installation-and-upgrade › Container-deployment**.

2.4.1.3. 启动 Uyuni Proxy 容器

Container can now be started with the `mgrpxy` command:

列表 5. 过程：启动 Uyuni Proxy 容器

```
mgrpxy start uyuni-proxy-pod
```

通过调用以下命令检查是否所有容器都已按预期启动

```
podman ps
```

应该会显示五个 Uyuni Proxy 容器：

- proxy-salt-broker
- proxy-httpd
- proxy-tftpd
- proxy-squid
- proxy-ssh

并且它们应该是 `proxy-pod` 容器 Pod 的一部分。

2.4.2. Deploy a Uyuni 2024.07 Proxy

This guide outlines the deployment process for the Uyuni 2024.07 Proxy. This guide presumes you have already successfully deployed a Uyuni 2024.07 Server. To successfully deploy, you will perform the following actions:

Checklist: Proxy Deployment

1. Review hardware requirements.
2. Synchronize the openSUSE Leap Micro 5.5 parent channel and the Proxy extension child channel on the server.
3. Install openSUSE Leap Micro 5.5 on a bare-metal machine.
4. During the installation, register openSUSE Leap Micro 5.5 along with the Uyuni 2024.07 Proxy extension.
5. Create a Salt activation key.
6. Bootstrap the Proxy as a Salt minion.
7. Generate a Proxy configuration.
8. Transfer the Proxy configuration from Server to Proxy
9. Use the Proxy configuration to register the Salt minion as a Proxy with Uyuni.

Supported operating system for the Proxy Container Host

The supported operating system for the container host is openSUSE Leap Micro 5.5.

Container host

A container host is a server equipped with a container engine like Podman, which lets it manage and deploy containers. These containers hold applications and their essential parts, such as libraries, but not a full operating system, making them lightweight. This setup ensures applications run the same way in different environments. The container host supplies the necessary resources such as CPU, memory, and storage for these containers.

2.4.2.1. Hardware Requirements for the Proxy

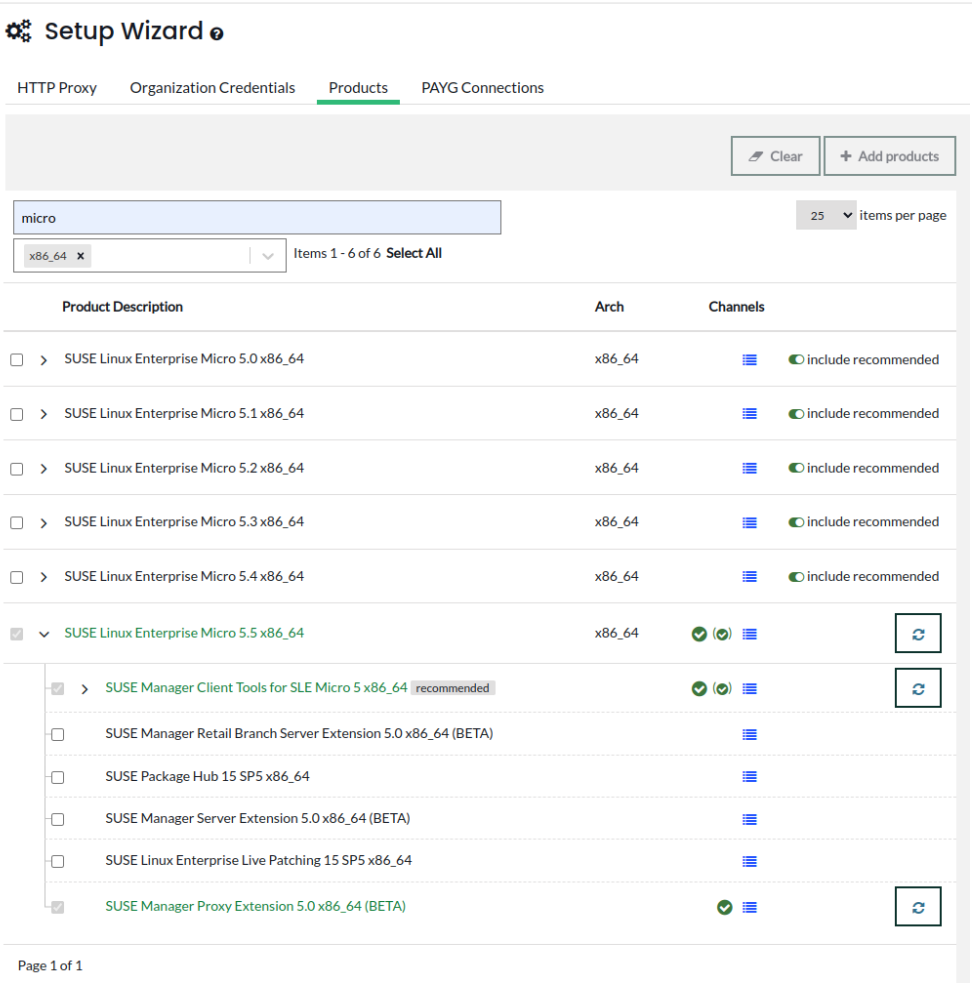
This table shows the hardware requirements for deploying Uyuni Proxy.

表格 9. 代理硬件要求

Hardware	Details	Recommendation
CPU	x86-64, ARM	Minimum 2 dedicated 64-bit CPU cores
RAM	Minimum	2 GB
	Recommended	8 GB
Disk Space	/ (root directory)	Minimum 40 GB
	`/var/lib/containers/storage/volumes/srv-www`	Minimum 100 GB, Storage requirements should be calculated for the number of ISO distribution images, containers, and bootstrap repositories you will use.
	`/var/lib/containers/storage/volumes/var-cache` (Squid)	Minimum 100 GB

2.4.2.2. Sync the Parent and Proxy Extension Child channels

Products are listed on the **Admin › Setup Wizard → Products** page. This channel must be fully synchronized on the server, with the child channel [systemitem]Proxy as an extension option selected.



图表 1. Uyuni 2024.07 Channel Sync for Proxy

Task: Sync the Proxy Parent Channel and Proxy Extension

1. In the Uyuni Web UI select **Admin › Products**.
2. From the products page enter SLE Micro in the filter field.
3. Next use the dropdown to select the required architecture. For this example x86-64.
4. In the `Product Description` field select the SLE Micro 5.5 checkbox then use the dropdown to select the `SUSE Manager Proxy Extension 5.0 x86_64 BETA` extension.
5. Click the **[+ Add products]** button.
6. Wait for the sync to complete.

2.4.2.3. SLE Micro 5.5 Installation

Task: Download the Installation Media

1. Locate the SLE Micro 5.5 installation media at https://www.suse.com/download/sle-micro/.
2. You will need an account with SUSE Customer Center and must be logged in to download the ISO.
3. Download the following file: `SLE-Micro-5.5-DVD-x86_64-GM-Media1.iso`
4. Prepare a USB fash disk or DVD for installation.

5. Insert a DVD or a bootable USB stick containing the installation image for SLE Micro 5.5.
6. Boot or reboot your system.

   For detailed documentation on preparing your machines OS (virtual or physical), see SLE Micro 5.5 Deployment Guide.

Task: SLE Micro 5.5 Installation

1. Use the arrow keys to select `Installation`.
2. Adjust Keyboard and language. Click the `checkbox` to accept the License Agreement.
3. Click `Next` to continue.
4. Select your registration method. For this example we will register the server with SUSE Customer Center.

Uyuni 2024.07 Proxy as an extension

The Uyuni 2024.07 Proxy is registered as an extension. Therefore, in addition to acquiring an SUSE Customer Center registration key for SLE Micro 5.5, you will also need an SUSE Customer Center registration code for the following extension:

- Uyuni 2024.07 Proxy

5. Enter your SUSE Customer Center Email address.
6. Enter your registration code for SLE Micro 5.5.
7. Click `Next` to continue.
8. On the `Extension and Module Selection` page uncheck the **Hide Development Versions** checkbox.
9. Select the Uyuni 2024.07 Proxy extension `Checkbox`.
10. Click `Next` to continue.
11. Enter your Uyuni 2024.07 Proxy extension registration code.
12. 单击 [下一步] 继续。
13. On the `NTP Configuration` page click [Next].
14. On the `Authentication for the System` page enter a password for the root user. Click [Next].
15. On the `Installation Settings` page click [Install].

This concludes installation of SLE Micro 5.5 and Uyuni 2024.07 Proxy as an extension.

2.4.2.3.1. Update the system

Task: Update the System

1. Login as **root**.

2. Run **transactional-update**:

```
transactional-update
```

3. Reboot the system.
4. Login as root.
5. Install the container utilities:

Alternatively you may install `mgrpxy-zsh-completion` or `mgrpxy-fish-completion`.

```
transactional-update pkg install mgrpxy mgrpxy-bash-completion
```

6. Reboot the system.

2.4.2.4. Configure Custom Persistent Storage

This step is optional. However, if custom persistent storage is required for your infrastructure, use the `mgr-storage-proxy` tool.

For more information, see `mgr-storage-proxy --help`. This tool simplifies creating the container storage and Squid cache volumes.

Use the command in the following manner:

+

```
mgr-storage-proxy <storage-disk-device>
```

For example:

```
mgr-storage-proxy /dev/nvme1n1
```

+

This command will create the persistent storage volumes at `/var/lib/containers/storage/volumes`.

For more information, see **Installation-and-upgrade › Container-management**.

2.4.2.5. Create an Activation Key for the Proxy

Task: Create an Activation Key

1. Select **Systems › Activation Keys** then click **[+ Create key]**.
2. Create an activation key for the proxy host with SLE Micro 5.5 as the parent channel. This key should include all recommended channels and the Proxy as an extension child channel.
3. Proceed to boostrapping the proxy host as a minion.

2.4.2.6. Bootstrap the Proxy Host as a Minion

Task: Bootstrap the Proxy Host

1. Select **Systems › Bootstrapping**.
2. Fill in the fields for your Proxy host.
3. Select the Activation key created in the previous step from the dropdown.
4. Click **[+ Bootstrap]**.
5. Wait for the Bootstrap process to complete successfully. Check the **Salt** menu and confirm the Salt minion key is listed and accepted.
6. Reboot the Proxy host.
7. Select the host from the **System** list and trigger a second reboot after all events are finished to conclude the onboarding.

Task: Update the Proxy Host

1. Select the host from the **Systems** list and apply all patches to update it.
2. Reboot the Proxy host.

2.4.2.7. Generate the Proxy Configuration

The configuration archive of the Uyuni Proxy is generated by the Uyuni Server. Each additional Proxy requires its own configuration archive.

The container host for the Uyuni Proxy must be registered as a salt minion to the Uyuni Server prior to generating this Proxy configuration.

You will perform the following tasks:

1. Generate a Proxy configuration file.
2. Transfer the configuration to the Proxy.
3. Start the Proxy with the `mgrpxy` command.

Task: Generating a Proxy Container Configuration using Web UI

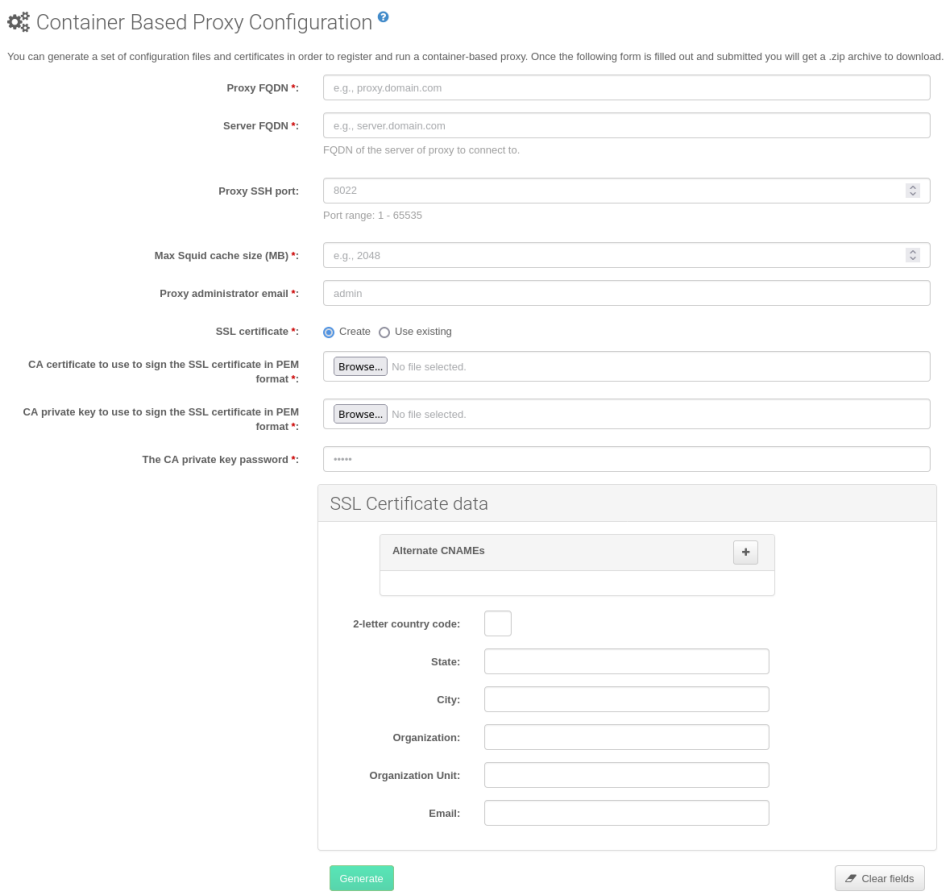
1. 在 Web UI 中，导航到**系统 › 代理配置**，然后填写所需数据：

2. 在¬¬¬¬ FQDN字段中，键入代理的完全限定域名。
3. 在¬¬ FQDN字段中，键入 Uyuni 服务器或另一个 Uyuni 代理的完全限定域名。
4. 在¬¬¬¬ SSH ¬¬¬¬字段中，键入 SSH 服务在 Uyuni 代理上监听的 SSH 端口。建议保留默认值 8022。
5. 在¬¬¬¬ Squid ¬¬¬¬¬¬¬¬ [MB]字段中，键入允许的最大 Squid 缓存大小。一般该值最多应为容器可用存储空间的 60 %。 在 SSH ¬¬¬¬选择列表中，选择应为 Uyuni 代理生成新服务器证书还是使用现有证书。您可以考虑作为 Uyuni 内置（自我签名）证书生成的证书。

   然后根据所做的选择提供用于生成新证书的签名 CA 证书的路径，或者要用作代理证书的现有证书及其密钥的路径。

   The CA certificates generated on the server are stored in the `/var/lib/containers/storage/volumes/root/ssl-build` directory.

   有关现有或自定义证书的详细信息以及企业和中间证书的概念，请参见 **Administration › Ssl-certs-imported**。
6. 单击 [生成] 以在 Uyuni 服务器中注册新代理 FQDN，并生成包含容器主机细节的配置存档。
7. 片刻之后，系统会显示文件可供下载。请将此文件保存在本地。



2.4.2.8. Transfer the Proxy Configuration

The Web UI generates a configuration archive. This archive needs to be made available on the Proxy

container host.

Task: Copy the Proxy configuration

1. Copy the files from the Server container to the Server host OS:

```
mgrctl cp server:/root/config.tar.gz .
```

2. Next copy the files from the Server host OS to the Proxy host:

```
scp config.tar.gz <proxy-FQDN>:/root
```

3. Install the Proxy with:

```
mgrpxy install podman config.tar.gz
```

2.4.2.9. Start the Uyuni 2024.07 Proxy

Container can now be started with the `mgrpxy` command:

Task: Start and Check Proxy Status

1. Start the Proxy by calling:

```
mgrpxy start
```

2. Check container status by calling:

```
mgrpxy status
```

应该会显示五个 Uyuni Proxy 容器：

- proxy-salt-broker
- proxy-httpd
- proxy-tftpd
- proxy-squid
- proxy-ssh

And should be part of the `proxy-pod` container pod.

2.4.2.9.1. 为服务使用自定义容器映像

By default, the Uyuni Proxy suite is set to use the same image version and registry path for each of its services. However, it is possible to override the default values for a specific service using the install parameters ending with `-tag` and `-image`.

例如，可以按如下方式使用此命令：

```
mgrpxy install podman --httpd-tag 0.1.0 --httpd-image
registry.opensuse.org/uyuni/proxy-httpd /path/to/config.tar.gz
```

It adjusts the configuration file for the httpd service, where `registry.opensuse.org/uyuni/proxy-httpds` is the image to use and `0.1.0` is the version tag, before restarting it.

To reset the values to defaults, run the install command again without those parameters:

```
mgrpxy install podman /path/to/config.tar.gz
```

This command first resets the configuration of all services to the global defaults and then reloads it.

2.4.3. 在 k3s 上安装容器化 Uyuni 代理

2.4.3.1. 安装 k3s

On the container host machine, install `k3s` (replace `<K3S_HOST_FQDN>` with the FQDN of your k3s host):

```
curl -sfL https://get.k3s.io | INSTALL_K3S_EXEC="--tls-
san=<K3S_HOST_FQDN>" sh -
```

2.4.3.2. Installing tools

The installation requires the `mgrpxy` and `helm` packages.

The `mgrpxy` package is available in the container utils repository: pick the one matching the distribution in: https://download.opensuse.org/repositories/systemsmanagement:/Uyuni:/Stable:/ContainerUtils/.

To install them run:

```
zypper in helm mgrpxy
```

2.4.3.3. 部署 Uyuni 代理 helm 图表

To configure the storage of the volumes to be used by the Uyuni Proxy pod, define persistent volumes for the following claims. If you do not customize the storage configuration, k3s will automatically create the storage volumes for you.

The persistent volume claims are named:

- `squid-cache-pv-claim`
- `/package-cache-pv-claim`
- `/tftp-boot-pv-claim`

Create the configuration for the Uyuni Proxy as documented in **Installation-and-upgrade › Container-deployment**. Copy the configuration `tar.gz` file and then install:

```
mgrpxy install kubernetes /path/to/config.tar.gz
```

For more information see https://kubernetes.io/docs/concepts/storage/persistent-volumes/ (kubernetes) or https://rancher.com/docs/k3s/latest/en/storage/ (k3s) documentation.

2.5. Install the Proxy

2.5.1. 在 openSUSE Leap 中安装 Uyuni Proxy

可以在 openSUSE Leap 15.5 上安装 Uyuni Proxy。

过程：安装包含 Uyuni Proxy 的 openSUSE Leap

1. 安装 openSUSE Leap 并应用所有可用的软件包更新。
2. 通过 **yast › 系统 › 网络设置 › 主机名/DNS** 配置一个可解析的完全限定域名 (FQDN)。
3. 添加包含 Uyuni Proxy 软件的储存库。 以 `root` 身份输入：

```
repo=repositories/systemsmanagement:/
repo=${repo}Uyuni:/Stable/images/repo/Uyuni-Proxy-POOL-x86_64-
Media1/
zypper ar https://download.opensuse.org/$repo uyuni-proxy-stable
```

4. 刷新储存库中的元数据。 以 `root` 身份输入：

```
zypper ref
```

5. 安装 Uyuni Proxy 的软件集： 以 `root` 身份输入：

```
zypper in patterns-uyuni_proxy
```

6. 重引导 Uyuni Proxy。
    - For more information about the stable version of Uyuni, see https://www.uyuni-project.org/pages/stable-version.html.
    - For more information about the development version of Uyuni, see https://www.uyuni-project.org/pages/devel-version.html.

安装完成后，可以继续设置 Uyuni。有关详细信息，请参见 **Installation-and-upgrade › Uyuni-proxy-registration**。

Chapter 3. Upgrade and Migration

3.1. Server

3.1.1. Migrating the Uyuni server to a containerized environment

To migrate a regular Uyuni server to a container, a new machine is required.

It is not possible to perform an in-place migration.

The original server is referred to as the **source server,** while the newly set-up machine is designated as the **destination server.**

The migration procedure currently does not include any hostname renaming functionality. Consequently, the fully qualified domain name (FQDN) on the new server will remain identical to that on the source server. Therefore, following migration, it will be necessary to manually adjust the DNS records to point to the new server.

Procedure: Initial preparation

1. Stop the source server:

```
spacewalk-service stop
```

2. Stop the source services:

```
systemctl stop postgresql
```

Procedure: Preparing the SSH connection

1. The SSH configuration and agent should be ready on the host for a passwordless connection to the source server.

To establish a passwordless connection, the migration script relies on an SSH agent running on the server. If one isn't active yet, initiate it by running `eval $(ssh-agent)`. Then, add the SSH key to the running agent with `ssh-add /path/to/the/private/key`. You'll be prompted to enter the password for the private key during this process.

2. The migration script only uses the source server fully qualified domain name in the SSH command.
3. This means that every other configuration required to connect needs to be defined in the `~/.ssh/config` file.

3.1.1.1. Prepare for Kubernetes

Before executing the migration command with mgradm migrate, it’ s essential to predefine **Persistent Volumes**, especially considering that the migration job initiates the container from scratch. Please consult the installation section for comprehensive guidance on preparing these volumes.

See: **Installation-and-upgrade › Container-management**

3.1.1.2. Migrating

Execute the following command to install a new Uyuni server, replacing **<Uyuni.source.fqdn>** with the appropriate FQDN of the source server:

```
mgradm migrate podman <{productname}.source.fqdn>
```

或

```
mgradm migrate kubernetes <{productname}.source.fqdn>
```

3.2. Proxy

3.2.1. Proxy Migration

In Uyuni 2024.04, the containerized proxy is managed by a set of systemd services.

In Uyuni 2024.07, management of the containerized proxy was re-designed and made simpler with the `mgrpxy` tool.

This section will help you migrate from the legacy `systemd` proxy using the new `mgrpxy` tool.

An in-place migration from Uyuni 2024.04 to 2024.06 will remain unsupported due to the HostOS change from SUSE Linux Enterprise Server 15 SP4 to openSUSE Leap Micro 5.5

The traditional contact protocol is no longer supported in Uyuni 2024.07 and later. Before migrating from Uyuni 2024.04 to 2024.07, any existing traditional clients including the traditional proxies must be migrated to Salt.

For more information about migrating traditional Uyuni 2024.04 clients to Salt clients, see https://documentation.suse.com/suma/4.3/en/suse-manager/client-configuration/contact-methods-migrate-traditional.html

3.2.1.1. Migrate from Legacy to Containerized Proxy with Systemd

3.2.1.1.1. Generate the Proxy Configuration

Task: Generate the Proxy Configuration

1. Log in to the Uyuni Server Web UI.
2. Select **Systems › Proxy Configuration** from the left navigation.
3. Enter your Proxy FQDN. Use the same FQDN as the original proxy host.
4. Enter your Server FQDN.
5. Enter the Proxy port number. We recommend using the default port of 8022
6. Certificate and private key are located on the Server container host in `/var/lib/containers/storage/volumes/root/_data/ssl-build/`.
    - RHN-ORG-TRUSTED-SSL-CERT
    - RHN-ORG-PRIVATE-SSL-KEY
7. Copy the certificate and key to your machine with:

```
scp root@uyuni-server-example.com:/root/ssl-build/RHN-ORG-PRIVATE-
SSL-KEY .
scp root@uyuni-server-example.com:/root/ssl-build/RHN-ORG-TRUSTED-
SSL-CERT .
```

8. Select [Choose File] and browse your local machine for the certificate.
9. Select [Choose File] and brose your local machine for the private key.
10. Enter the CA password.
11. Click [Generate].

3.2.1.1.2. Transfer Proxy Configuration to New Host

Task: Transfer the Proxy Configuration

1. From the Server transfer the generated tar.gz file containing the proxy configuration to the new Proxy host:

```
scp config.tar.gz <uyuni-proxy-FQDN>:/root/
```

2. Disable the legacy proxy prior to executing the next step:

列表 6. Disable the Legacy Proxy

```
spacewalk-proxy stop
```

3. Deploy the new Proxy with:

```
systemctl start uyuni-proxy-pod
```

4. Enable the new Proxy with:

```
systemctl enable --now uyuni-proxy-pod
```

5. Run `podman ps` to verify all the containers are present and running:

```
proxy-salt-broker
proxy-httpd
proxy-tftpd
proxy-squid
proxy-ssh
```

3.2.1.2. Migrate Uyuni 2024.04 Proxy to Uyuni 2024.07 Containerized Proxy

Task: Migrate Uyuni 2024.04 Containerized Proxy to Uyuni 2024.07 New Containerized Proxy

1. Boot your new machine and begin installation of openSUSE Leap Micro 5.5.
2. Complete the installation.
3. Update the system:

```
transactional-update --continue
```

4. Install `mgrpxy` and optionally, `mgrpxy-bash-completion`:

```
transactional-update pkg install mgrpxy mgrpxy-bash-completion
```

5. 重引导。
6. Copy your tar.gz proxy configuration to the host.

3.2.1.3. Installing packages using the Web UI

The `mgrpxy` and `mgrpxy-bash-completion` packages can also be installed via the web UI after the minion has been bootstrapped and registered with the Server.

Task: Installing Packages using the Web UI

1. After installation, ensure that the SLE Micro 5.5 Parent channel and Proxy child channels are added and synced from the **Admin › Setup Wizard → Products** page.

2. In the Web UI, go to **Systems › Activation Keys** and create an activation key linked to the synced SLE Micro 5.5 channel.
3. Bootstrap your system as a minion using the **Systems › Bootstrapping** page.
4. Once the new machine is onboarded and displayed in the systems list, select the system and navigate to the **System Details › Install Package** page.
5. Install the packages `mgrpxy` and `mgrpxy-bash-completion`.
6. Reboot the system.

3.2.1.4. Generate Proxy Config with spacecmd and Self-Signed Certificate

Task: Generate Proxy Config with spacecmd and Self-Signed Certificate

You can generate a Proxy configuration using spacecmd.

1. SSH into your container host.
2. Execute the following command replacing the Server and Proxy FQDN:

```
mgrctl exec -ti 'spacecmd proxy_container_config_generate_cert --
dev-pxy.example.com dev-srv.example.com 2048 email@example.com' -o
/tmp/config.tar.gz
```

3. Copy the generated config to the Proxy:

```
mgrctl cp server:/tmp/config.tar.gz .
```

4. Deploy the Proxy with:

```
mgrpxy install podman config.tar.gz
```

3.2.1.5. Generate Proxy Config with spacecmd and Custom Certificate

You can generate a Proxy configuration using spacecmd for a custom certificates rather than the default self signed certificates.

2 GB represents the default proxy squid cache size. This will need to be adjusted for your environment.

Task: Generate Proxy Config with spacecmd and Custom Certificate

1. SSH into your Server container host.
2. Execute the following command replacing the Server and Proxy FQDN:

```
for f in ca.crt proxy.crt proxy.key; do
  mgrctl cp $f server:/tmp/$f
done
mgrctl exec -ti 'spacecmd proxy_container_config -- -p 8022
pxy.example.com srv.example.com 2048 email@example.com /tmp/ca.crt
/tmp/proxy.crt /tmp/proxy.key -o /tmp/config.tar.gz'
```

3. Copy the generated config to the Proxy:

```
mgrctl cp server:/tmp/config.tar.gz .
```

4. Deploy the Proxy with:

```
mgrpxy install podman config.tar.gz
```

3.3. Clients

3.3.1. 升级客户端

客户端采用底层操作系统的版本控制系统。对于运行 SUSE 操作系统的客户端，可在 Uyuni Web UI 中进行升级。

有关升级客户端的详细信息，请参见 **Client-configuration › Client-upgrades**。

Chapter 4. Upgrade and Migration

4.1. Server

4.1.1. Container

4.1.1.1. Migrating the Uyuni server to a containerized environment

To migrate a regular Uyuni server to a container, a new machine is required.

It is not possible to perform an in-place migration.

The original server is referred to as the **source server,** while the newly set-up machine is designated as the **destination server.**

The migration procedure currently does not include any hostname renaming functionality. Consequently, the fully qualified domain name (FQDN) on the new server will remain identical to that on the source server. Therefore, following migration, it will be necessary to manually adjust the DNS records to point to the new server.

Procedure: Initial preparation

1. Stop the source server:

```
spacewalk-service stop
```

2. Stop the source services:

```
systemctl stop postgresql
```

Procedure: Preparing the SSH connection

1. The SSH configuration and agent should be ready on the host for a passwordless connection to the source server.

To establish a passwordless connection, the migration script relies on an SSH agent running on the server. If one isn't active yet, initiate it by running `eval $(ssh-agent)`. Then, add the SSH key to the running agent with `ssh-add /path/to/the/private/key`. You'll be prompted to enter the password for the private key during this process.

2. The migration script only uses the source server fully qualified domain name in the SSH command.
3. This means that every other configuration required to connect needs to be defined in the `~/.ssh/config` file.

4.1.1.1.1. Prepare for Kubernetes

Before executing the migration command with mgradm migrate, it’ s essential to predefine **Persistent Volumes**, especially considering that the migration job initiates the container from scratch. Please consult the installation section for comprehensive guidance on preparing these volumes.

See: **Installation-and-upgrade › Container-management**

4.1.1.1.2. Migrating

Execute the following command to install a new Uyuni server, replacing **<Uyuni.source.fqdn>** with the appropriate FQDN of the source server:

```
mgradm migrate podman <{productname}.source.fqdn>
```

或

```
mgradm migrate kubernetes <{productname}.source.fqdn>
```

After successfully running the `mgradm migrate` command, the Salt setup on all clients will still point to the old server (source server). To redirect them to the new server (destination server), it is required to rename the new server at the infrastructure level (DHCP and DNS) to use the same Fully Qualified Domain Name and IP address as old server (source server).

4.1.2. Legacy

4.1.2.1. 服务器 - 次要升级

Uyuni 团队每年都会发布几次 Uyuni Server 的次要升级。这些更新旨在修复 Bug 并改进功能，有时也包含一些新功能。

Some additional manual steps might be required, and this information is only available in the release notes. For more information about such a major upgrade, see **Installation-and-upgrade › Server-major-upgrade-uyuni**.

For information about your upgrade, see the release notes at https://www.uyuni-project.org/pages/stable-version.html.

执行次要升级的过程与安装操作系统软件包更新类似。

过程：更新 Uyuni 服务器上的软件包

默认会为 Uyuni 服务器配置并启用多个更新储存库。新软件包和更新的软件包会自动变为可用状态。

It is recommended you make a backup of the server before upgrading. For more information about

backing up Uyuni, see **Administration › Backup-restore**.

1. 在 Uyuni 服务器上的命令提示符处，以 root 身份停止 spacewalk 服务：

```
spacewalk-service stop
```

2. 刷新软件储存库：

```
zypper ref
```

3. 更新新的软件包：（如果 zypper 显示提示，请重复此步骤）

```
zypper up
```

Uyuni is different from SUSE Manager in this step. SUSE Manager uses `zypper patch`, but Uyuni requires `zypper up`.

+

1. If zypper reports that the Uyuni package will not be upgraded, run the command manually:

```
zypper install Uyuni-Server-release
```

2. 重启动 spacewalk 服务：

```
spacewalk-service start
```

如果补丁更新建议重引导服务器，请将其重引导。

Zypper 默认每十分钟刷新一次储存库（请参见 `/etc/zypp/zypp.conf` 中的 `repo. refresh.delay`）。如果¬¬¬¬¬¬¬¬被禁用，请运行 `zypper ref` 以刷新所有储存库。

从 Uyuni 2020.04 开始，不再需要 `spacewalk-schema-upgrade`。

使用 `spacewalk-service start` 启动 spacewalk 服务时，会自动运行纲要升级。

更新后，受软件包更新影响的服务不会自动重启动。您需要手动重启动这些服务，以免发生潜在故障。运行 `zypper ps` 检查有无使用旧代码并需要重启动的应用程序。

4.1.2.2. 服务器 - 主要升级

当 Uyuni 核心组件升级到新的主要版本时，需在 Uyuni 服务器上执行主要升级。如果需要升级 PostgreSQL、Salt 或 openSUSE Leap 的版本，就需要进行主要升级。openSUSE Leap 为底层基础操作系统 (OS)。

您可能需要执行一些额外的手动步骤，这些信息仅在发行说明中提供。有关升级的额外重要信息，请参见发行说明，网址：

https://www.uyuni-project.org/pages/stable-version.html。

You will not be able to fix issues that arise during the migration. Ensure you have created a backup before you start the migration. For more information about backing up Uyuni, see **Administration › Backup-restore**. If you are running Uyuni Server on a virtual machine, we recommend that you create a snapshot before you start.

开始升级前，请确保满足存储要求。有关详细信息，请参见 uyuni-install-requirements.pdf。如果可用空间不足，在迁移过程中根分区可能会被填满，因为系统会迁移服务包并会下载新软件包。升级 PostgreSQL 时，`/var/lib/pgsql` 也会发生同样的情况。该目录会存放旧数据库副本，因此请确保可用空间至少足以容纳该数据库副本。

`server-migrator.sh` 脚本会将 Uyuni 服务器迁移到最新的版本， 还会将底层操作系统升级到版本 15.5。该脚本包含在 `susemanager` 软件包中。

过程：迁移 Uyuni 服务器

1. 在运行 `server-migrator.sh` 脚本前，需检查是否安装了 `susemanager` 软件包的最新版本：

```
zypper ref
zypper up susemanager
```

2. 运行 `/usr/lib/susemanager/bin/server-migrator.sh` 脚本以升级基础 OS 和 Uyuni 服务器。

完成迁移后，请手动重引导 Uyuni 服务器：

4.2. Proxy

4.2.1. 升级代理

Uyuni 代理的注册方式与客户端的管理方式相同。

升级到 2024.07 的过程可能是主要升级，也可能是次要升级。有关详细信息，请参见 Uyuni 2024.07 版本说明。

主要升级

请参见 **Installation-and-upgrade › Proxy-uyuni**。

次要升级

请参见 **Installation-and-upgrade › Proxy-minor-uyuni**。

4.2.2. 代理 - 主要升级

在执行任何代理更新前，请安排维护时段。进行更新时，通过代理注册到 Uyuni 的客户端将无法连接到 Uyuni。有关维护时段的详细信息，请参见 **Administration › Maintenance-windows**。

代理主要升级包括操作系统的版本升级。有关详细信息，请参见 Uyuni 2024.07 版本说明。

4.2.2.1. 升级的准备工作

过程：在命令提示符处添加 openSUSE Leap 15.5 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 opensuse_leap15_5 \
opensuse_leap15_5-non-oss \
opensuse_leap15_5-non-oss-updates \
opensuse_leap15_5-updates \
opensuse_leap15_5-backports-updates \
opensuse_leap15_5-sle-updates \
uyuni-proxy-stable-leap-155
```

2. 使用 `spacewalk-repo-sync` 完全同步所有通道。

4.2.2.2. 升级代理

要更新代理，首先需停止代理服务，然后替换软件储存库，更新软件，最后重启动代理服务。

过程：更新 Uyuni 代理

1. 在 Uyuni 代理上，停止代理服务：

```
spacewalk-proxy stop
```

2. 在 Uyuni 服务器 Web UI 中，导航到**系统 › 代理**，然后单击代理名称。
3. 单击**软件 › 软件通道**，选择¬¬¬¬¬¬¬¬¬¬列表中所列的 openSUSE Leap 15.5 通道作为基础通道。
4. 在¬¬¬¬¬¬窗格中，选择 15.5 子通道。
5. 单击 [下一步]，然后单击 [确认] 以¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬¬。
6. 单击**细节 › 远程命令**，将 `zypper --non-interactive dup --allow-vendor-change --replacefiles` 添加到脚本字段中，然后单击 [日程安排]
7. 等待远程命令执行。
8. 在 Uyuni 代理上，启动代理服务：

```
spacewalk-proxy start
```

如果需要更新许多代理，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代理执行更新。

4.2.3. 代理 - 次要升级

在执行任何代理更新前，请安排维护时段。进行更新时，通过代理注册到 Uyuni 的客户端将无法连接到 Uyuni。有关维护时段的详细信息，请参见 **Administration › Maintenance-windows**。

代理次要升级不包括操作系统的版本升级。有关详细信息，请参见 Uyuni 2024.07 版本说明。

4.2.3.1. 升级代理

要更新代理，首先需停止代理服务，然后更新软件，最后重启动代理服务。

过程：更新 Uyuni 代理

1. 在 Uyuni 代理上，停止代理服务：

```
spacewalk-proxy stop
```

2. 在 Uyuni 服务器 Web UI 中，导航到**系统 › 代理**，然后单击代理名称。
3. 选择代理上要更新的所有软件包，然后应用选择。
4. 在 Uyuni 代理上，启动代理服务：

```
spacewalk-proxy start
```

如果需要更新许多代理，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代理执行更新。

Chapter 5. Basic Server Management

5.1. Custom YAML Configuration and Deployment with mgradm

You have the option to create a custom `mgradm.yaml` file, which the `mgradm` tool can utilize during deployment.

`mgradm` will prompt for basic variables if they are not provided using command line parameters or the `mgradm.yaml` configuration file.

For security, **using command line parameters to specify passwords should be avoided**: use a configuration file with proper permissions instead.

Procedure: Deploying the Uyuni container with Podman using a custom configuration file

1. Prepare a configuration file named `mgradm.yaml` similar to the following example:

```
# Database password. Randomly generated by default
db:
  password: MySuperSecretDBPass

# Password for the CA certificate
ssl:
  password: MySuperSecretSSLPassword

# Your SUSE Customer Center credentials
scc:
  user: ccUsername
  password: ccPassword

# Organization name
organization: YourOrganization

# Email address sending the notifications
emailFrom: notifications@example.com

# Administrators account details
admin:
  password: MySuperSecretAdminPass
  login: LoginName
  firstName: Admin
  lastName: Admin
  email: email@example.com
```

2. From the terminal, as root, run the following command. Entering your server’s FQDN is optional.

```
mgradm -c mgradm.yaml install podman <FQDN>
```

You must deploy the container as sudo or root. The following error will be displayed on the terminal if you miss this step.

```
INF Setting up uyuni network
9:58AM INF Enabling system service
9:58AM FTL Failed to open
/etc/systemd/system/uyuni-server.service for
writing error="open /etc/systemd/system/uyuni-
server.service: permission denied"
```

3. Wait for deployment to complete.
4. Open a browser and proceed to your server’s FQDN or IP address.

In this section you learned how to deploy an Uyuni 2024.07 Server container using a custom YAML configuration.

5.2. Starting and Stopping Containers

The Uyuni 2024.07 Server container can be restarted, started, and stopped using the following commands:

To `restart` the Uyuni 2024.07 Server execute the following command:

```
# mgradm restart
5:23PM INF Welcome to mgradm
5:23PM INF Executing command: restart
```

To `start` the server execute the following command:

```
# mgradm start
5:21PM INF Welcome to mgradm
5:21PM INF Executing command: start
```

To `stop` the server execute the following command:

```
# mgradm stop
5:21PM INF Welcome to mgradm
5:21PM INF Executing command: stop
```

5.3. List of persistent storage volumes

Modifications performed within containers are not retained. Any alterations made outside of persistent volumes will be discarded. Below is a list of persistent volumes for Uyuni 2024.07.

To customize the default volume locations, ensure you create the necessary volumes before launching the pod for the first time, utilizing the `podman volume create` command.

Ensure that this table aligns precisely with the volumes mapping outlined in both the Helm chart and the systemctl services definitions.

The following volumes are stored under the **Podman** default storage location.

表格 10. Persistent Volumes: **Podman Default Storage**

Volume Name	Volume Directory
Podman Storage	`/var/lib/containers/storage/volumes/`

表格 11. Persistent Volumes: **root**

Volume Name	Volume Directory
root	`/root`

表格 12. Persistent Volumes: **var/**

Volume Name	Volume Directory
var-cobbler	`/var/lib/cobbler`
var-salt	`/var/lib/salt`
var-pgsql	`/var/lib/pgsql`
var-cache	`/var/cache`
var-spacewalk	`/var/spacewalk`
var-log	`/var/log`

表格 13. Persistent Volumes: **srv/**

Volume Name	Volume Directory
srv-salt	`/srv/salt`
srv-www	`/srv/www/`
srv-tftpboot	`/srv/tftpboot`

Volume Name	Volume Directory
srv-formulametadata	`/srv/formula_metadata`
srv-pillar	`/srv/pillar`
srv-susemanager	`/srv/susemanager`
srv-spacewalk	`/srv/spacewalk`

表格 14. Persistent Volumes: **etc/**

Volume Name	Volume Directory
etc-apache2	`/etc/apache2`
etc-rhn	`/etc/rhn`
etc-systemd-multi	`/etc/systemd/system/multi-user.target.wants`
etc-systemd-sockets	`/etc/systemd/system/sockets.target.wants`
etc-salt	`/etc/salt`
etc-tomcat	`/etc/tomcat`
etc-cobbler	`/etc/cobbler`
etc-sysconfig	`/etc/sysconfig`
etc-tls	`/etc/pki/tls`
etc-postfix	`/etc/postfix`
ca-cert	`/etc/pki/trust/anchors`

Chapter 6. GNU Free Documentation License

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".
```