



U Y U N I

# Uyuni 2023.10

## Installation and Upgrade Guide

October 31 2023

# Table of Contents

Installation and Upgrade Guide Overview	1
1. Requirements	2
1.1. Server Requirements	2
1.2. Proxy Requirements	2
1.3. Network Requirements	3
1.3.1. Required Network Ports	4
1.4. Supported Client Systems	10
1.5. Public Cloud Requirements	12
1.5.1. Network requirements	13
1.5.2. Prepare storage volumes	13
2. Installation	15
2.1. Uyuni Server	15
2.1.1. Install Uyuni Server with openSUSE	15
2.1.2. Installation on Public Cloud	16
2.2. Uyuni Proxy	16
2.2.1. Install Uyuni Proxy with openSUSE Leap	16
2.2.2. Install containerized Uyuni Proxy	17
2.2.3. Install Containerized Uyuni Proxy on k3s	20
3. Setup	23
3.1. Uyuni Server	23
3.1.1. Uyuni Server Setup	23
3.1.2. Setup Wizard	27
3.1.3. Web Interface Setup	29
3.1.4. Public Cloud Setup	32
3.1.5. Connect PAYG instance	35
3.2. Uyuni Proxy	38
3.2.1. Uyuni Proxy Registration	38
3.2.2. Uyuni Proxy Setup	39
3.2.3. Containerized Uyuni Proxy Setup	44
3.2.4. Containerized proxy deployment using internal registry	46
4. Upgrade introduction	49
4.1. Upgrade the Server	49
4.1.1. Server - Minor Upgrade	49
4.1.2. Server - Major Upgrade	51
4.2. Upgrade the Proxy	52
4.2.1. Proxy - Major Upgrade	52
4.2.2. Proxy - Minor Upgrade	53
4.3. Upgrade the Database	54
4.3.1. Database Migration to Latest Version	55
4.4. Upgrade the Clients	57
5. GNU Free Documentation License	58

---

# Installation and Upgrade Guide Overview

**Updated:** 2023-10-31

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

- **Requirements:** Describes the hardware, software, and networking requirements that you require before you begin.
- **Installation:** Describes the process to install Uyuni components.
- **Setting Up:** Describes the initial steps you need to take after installation to make your Uyuni environment ready to use.
- **Upgrade:** Describes upgrading of the Uyuni components, including the underlying database.

It is possible to use a public cloud instance to install Uyuni. For more information on using Uyuni on a public cloud, see **Specialized-guides > Public-cloud-guide**. For more information on upgrading clients, see **Client-configuration > Client-upgrades**.

# Chapter 1. Requirements

The following tables specify the minimum server and proxy requirements.

## 1.1. Server Requirements

*Table 1. Server Requirements for x86-64 Architecture*

Software and Hardware	Details	Recommendation
openSUSE Leap 15.5	Clean installation, up-to-date	openSUSE Leap 15.5
CPU	-	Minimum 4 dedicated 64-bit CPU cores (x86-64)
RAM	Test or Base Installation	Minimum 16 GB
	Production Server	Minimum 32 GB
Disk Space	/ (root directory)	Minimum 40 GB
	/var/lib/pgsql	Minimum 50 GB
	/var/spacewalk	Minimum storage required: 100 GB (this will be verified by the implemented check)  * 50 GB for each SUSE product and Package Hub  * 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

## 1.2. Proxy Requirements

*Table 2. Proxy Requirements*

Software and Hardware	Details	Recommendation
openSUSE Leap 15.5	Clean installation, up-to-date	openSUSE Leap 15.5

Software and Hardware	Details	Recommendation
CPU		Minimum 2 dedicated 64-bit CPU cores
RAM	Test Server	Minimum 2 GB
	Production Server	Minimum 8 GB
Disk Space	/ (root directory)	Minimum 40 GB
	/srv	Minimum 100 GB
	/var/cache (Squid)	Minimum 100 GB

Uyuni Proxy caches packages in the `/var/cache/` directory. If there is not enough space available in `/var/cache/`, the proxy will remove old, unused packages and replace them with newer packages.

As a result of this behavior:

- The larger `/var/cache/` directory is on the proxy, the less traffic there will be between it and the Uyuni Server.
- By making the `/var/cache/` directory on the proxy the same size as `/var/spacwalk/` on the Uyuni Server, you avoid a large amount of traffic after the first synchronization.
- The `/var/cache/` directory can be small on the Uyuni Server compared to the proxy. For a guide to size estimation, see the [\[server-hardware-requirements\]](#) section.

## 1.3. Network Requirements

This section details the networking and port requirements for Uyuni.

### Fully Qualified Domain Name (FQDN)

The Uyuni server must resolve its FQDN correctly. If the FQDN cannot be resolved, it can cause serious problems in a number of different components.

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>.

### Hostname and IP Address

To ensure that the Uyuni domain name can be resolved by its clients, both server and client machines must be connected to a working DNS server. You also need to ensure that reverse lookups are correctly configured.

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

## Using a Proxy When Installing from SUSE Linux Enterprise Media

If you are on an internal network and do not have access to SUSE Customer Center, you can set up and use a proxy during installation.

For more information about configuring a proxy for access to SUSE Customer Center during a SUSE Linux Enterprise installation, see <https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-boot-parameters.html#sec-boot-parameters-advanced-proxy>.



The hostname of Uyuni must not contain uppercase letters as this may cause *jabberd* to fail. Choose the hostname of your Uyuni server carefully. Although changing the server name is possible and supported, it is important to plan for this change before going ahead with it. When you change the hostname of the server, all clients attached to the server must be made aware of the change.

In a production environment, the Uyuni Server and clients should always use a firewall. For a comprehensive list of the required ports, see **Installation-and-upgrade > Ports**.

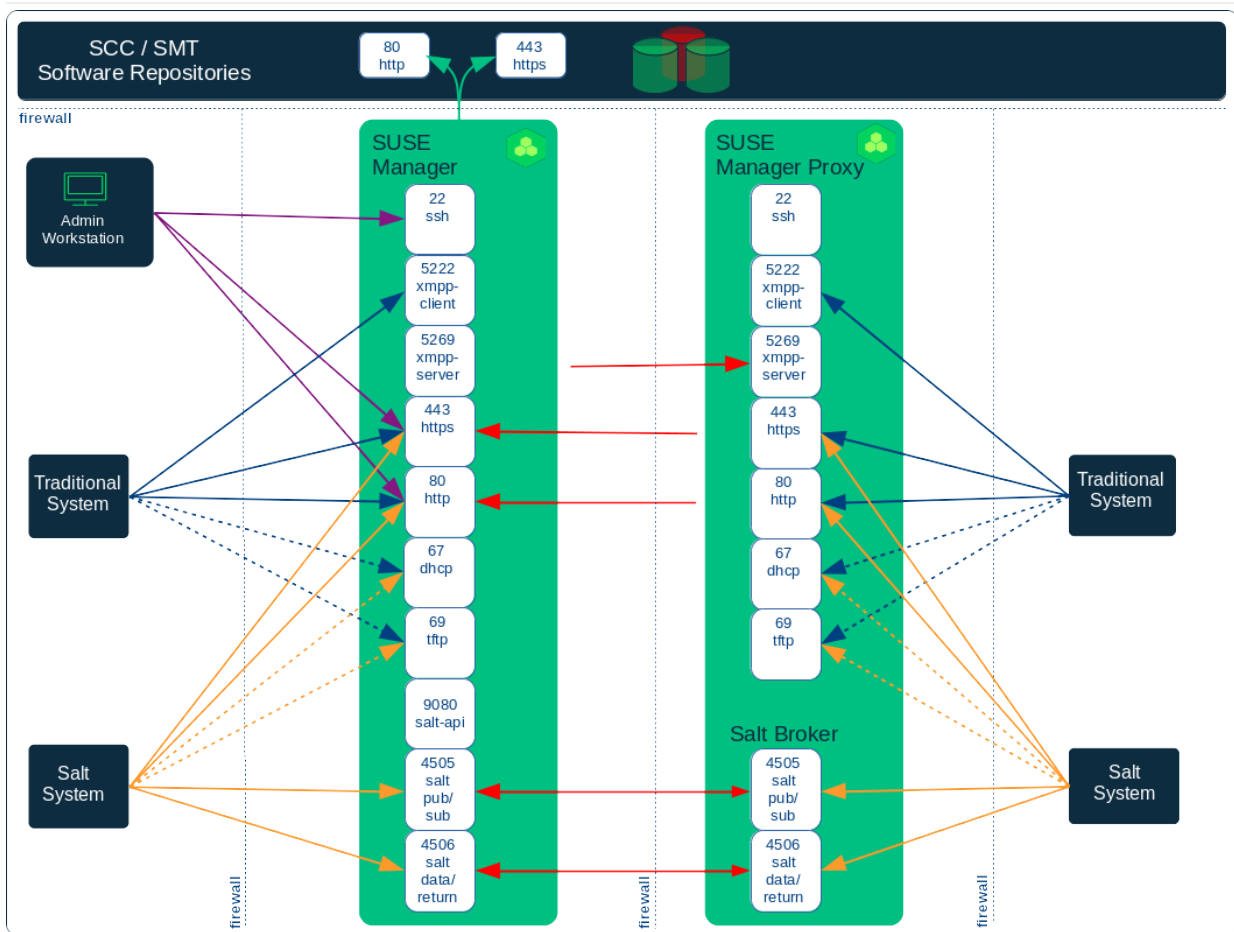
For more information on disconnected setup and port configuration, see **Administration > Disconnected-setup**.

### 1.3.1. Required Network Ports

This section contains a comprehensive list of ports that are used for various communications within Uyuni.

You will not need to open all of these ports. Some ports only need to be opened if you are using the service that requires them.

This image shows the main ports used in Uyuni:



#### 1.3.1.1. External Inbound Server Ports

External inbound ports must be opened to configure a firewall on the Uyuni Server to protect the server from unauthorized access.

Opening these ports allows external network traffic to access the Uyuni Server.

Table 3. External Port Requirements for Uyuni Server

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.



Port number	Protocol	Used By	Notes
80	TCP	HTTP	Required temporarily for some bootstrap repositories and automated installations. Port 80 is not used to serve the Web UI.
443	TCP	HTTPS	Web UI, client, and server and proxy (tfhttpsync) 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.
5222	TCP	osad	Required to push OSAD actions to clients.
5269	TCP	jabberd	Required to push actions to and from a proxy.
25151	TCP	Cobbler	

#### 1.3.1.2. External Outbound Server Ports

External outbound ports must be opened to configure a firewall on the Uyuni Server to restrict what the server can access.

Opening these ports allows network traffic from the Uyuni Server to communicate with external services.

*Table 4. External Port Requirements for Uyuni Server*



Port number	Protocol	Used By	Notes
80	TCP	HTTP	Required for SUSE Customer Center. Port 80 is not used to serve the Web UI.
443	TCP	HTTPS	Required for SUSE Customer Center.
5269	TCP	jabberd	Required to push actions to and from a proxy.
25151	TCP	Cobbler	

### 1.3.1.3. Internal Server Ports

Internal port are used internally by the Uyuni Server. Internal ports are only accessible from localhost.

In most cases, you will not need to adjust these ports.

*Table 5. Internal Port Requirements for Uyuni Server*

Port number	Notes
2828	Satellite-search API, used by the RHN application in Tomcat and Taskomatic.
2829	Taskomatic API, used by the RHN application in Tomcat.
8005	Tomcat shutdown port.
8009	Tomcat to Apache HTTPD (AJP).
8080	Tomcat to Apache HTTPD (HTTP).
9080	Salt-API, used by the RHN application in Tomcat and Taskomatic.
32000	Port for a TCP connection to the Java Virtual Machine (JVM) that runs Taskomatic and satellite-search.

Port 32768 and higher are used as ephemeral ports. These are most often used to receive TCP connections. When a TCP connection request is received, the sender will choose one of these ephemeral port numbers to match the destination port.

You can use this command to find out which ports are ephemeral ports:

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

#### 1.3.1.4. External Inbound Proxy Ports

External inbound ports must be opened to configure a firewall on the Uyuni Proxy to protect the proxy from unauthorized access.

Opening these ports allows external network traffic to access the Uyuni proxy.

*Table 6. External Port Requirements for Uyuni Proxy*

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.
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.

Port number	Protocol	Used By	Notes
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.
5222	TCP		Required to push OSAD actions to clients.
5269	TCP		Required to push actions to and from the server.

#### 1.3.1.5. External Outbound Proxy Ports

External outbound ports must be opened to configure a firewall on the Uyuni Proxy to restrict what the proxy can access.

Opening these ports allows network traffic from the Uyuni Proxy to communicate with external services.

*Table 7. External Port Requirements for Uyuni Proxy*

Port number	Protocol	Used By	Notes
80			Used to reach the server.
443	TCP	HTTPS	Required for SUSE Customer Center.
5269	TCP		Required to push actions to and from the server.

#### 1.3.1.6. External Client Ports

External client ports must be opened to configure a firewall between the Uyuni Server and its clients.

In most cases, you will not need to adjust these ports.

*Table 8. External Port Requirements for Uyuni Clients*

Port number	Direction	Protocol	Notes
22	Inbound	SSH	Required for ssh-push and ssh-push-tunnel contact methods.

Port number	Direction	Protocol	Notes
80	Outbound		Used to reach the server or proxy.
5222	Outbound	TCP	Required to push OSAD actions to 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.
9187	Outbound	TCP	Required for Prometheus PostgreSQL.

#### 1.3.1.7. Required URLs

There are some URLs that Uyuni must be able to access to register clients and perform updates. In most cases, allowing access to these URLs is sufficient:

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

If you are using non-SUSE clients you might also need to allow access to other servers that provide specific packages for those operating systems. For example, if you have Ubuntu clients, you will need to be able to access the Ubuntu server.

For more information about troubleshooting firewall access for non-SUSE clients, see **Administration > Troubleshooting**.

## 1.4. Supported Client Systems

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

In this table, ✓ indicates that clients running the operating system are supported by SUSE, and ✗ indicates that it is not supported. Fields marked as ? are under consideration, and may or may not be supported at a later date.



For SUSE operating systems, the version and SP level must be under general support (normal or LTSS) to be supported with Uyuni. For details on supported product versions, see:

<https://www.suse.com/lifecycle>

For non-SUSE operating systems, including Red Hat Enterprise Linux, CentOS, and Oracle Linux, only the latest available version is under general support.

*Table 9. Supported Client Systems*

Operating System	Architecture	Salt Clients
SUSE Linux Enterprise 15	x86-64, ppc64le, IBM Z, aarch64	✓
SUSE Linux Enterprise 12	x86-64, ppc64le, IBM Z, aarch64	✓
SUSE Linux Enterprise Server for SAP 15	x86-64, ppc64le	✓
SUSE Linux Enterprise Server for SAP 12	x86-64, ppc64le	✓
SLE Micro	x86-64, aarch64, s390x	✓
openSUSE Leap 15	x86-64, aarch64	✓
Alibaba Cloud Linux 2	x86-64, aarch64	✓
AlmaLinux 9	x86-64, aarch64	✓
AlmaLinux 8	x86-64, aarch64 ppc64le, s390x	✓
Amazon Linux 2	x86-64, aarch64	✓
CentOS 7	x86-64, ppc64le, aarch64	✓
Debian 12	x86-64	✓
Debian 11	x86-64	✓
Debian 10	x86-64	✓
Oracle Linux 9	x86-64, aarch64	✓
Oracle Linux 8	x86-64, aarch64	✓
Oracle Linux 7	x86-64, aarch64	✓
Red Hat Enterprise Linux 9	x86-64	✓
Red Hat Enterprise Linux 8	x86-64	✓
Red Hat Enterprise Linux 7	x86-64	✓

Operating System	Architecture	Salt Clients
Rocky Linux 9	x86-64, aarch64	✓
Rocky Linux 8	x86-64, aarch64, ppc64le, s390x	✓
Ubuntu 22.04	amd64	✓
Ubuntu 20.04	amd64	✓
Ubuntu 18.04	amd64	✓

When the distribution reaches end-of-life, it enters grace period of 3 months when the support is considered deprecated. After that period, the product is considered unsupported. Any support may only be available on the best-effort basis.

For more information about end-of-life dates, see <https://endoflife.software/operating-systems>.



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



Salt SSH 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 Salt SSH to reach a client.

When you are setting up your client hardware, you need to ensure you have enough for the operating system and for the workload you want to perform on the client, with these additions for Uyuni:

Table 10. Client Additional Hardware Requirements

Hardware	Additional Size Required
RAM	512 MB
Disk Space:	200 MB

## 1.5. Public Cloud Requirements

This section provides the requirements for installing Uyuni on public cloud infrastructure. We have tested these instructions on Amazon EC2, Google Compute Engine, and Microsoft Azure, but they should work on other providers as well, with some variation.

Before you begin, here are some considerations:

- The Uyuni setup procedure performs a forward-confirmed reverse DNS lookup. This must succeed in order for the setup procedure to complete and for Uyuni to operate as expected. It is important to perform hostname and IP configuration before you set up Uyuni.

- Uyuni Server and Proxy instances need to run in a network configuration that provides you control over DNS entries, but cannot be accessed from the internet at large.
- Within this network configuration DNS resolution must be provided: `hostname -f` must return the fully qualified domain name (FQDN).
- DNS resolution is also important for connecting clients.
- DNS is dependent on the cloud framework you choose. Refer to the cloud provider documentation for detailed instructions.
- We recommend that you locate software repositories, the server database, and the proxy squid cache on an external virtual disk. This prevents data loss if the instance is unexpectedly terminated. This section includes instructions for setting up an external virtual disk.



If you are attempting to bootstrap traditional clients, check that you can resolve the host name of the server while you are logged in to the client. You might need to add the FQDN of the server to `/etc/hosts` local resolution file on the client. Check using the `hostname -f` command with the local IP address of the server.

### 1.5.1. Network requirements

When you use Uyuni on a public cloud, you must use a restricted network. We recommend using a VPC private subnet with an appropriate firewall setting. Only machines in your specified IP ranges must be able to access the instance.



When you run Uyuni on public clouds, you must apply security measures to limit access to the instance. A world-accessible Uyuni instance violates the terms of the Uyuni EULA, and is not supported by SUSE.

To access the Uyuni Web UI, allow HTTPS when configuring the network access controls. This allows you to access the Uyuni Web UI.

In EC2 and Azure, create a new security group, and add inbound and outbound rules for HTTPS. In GCE, check the `Allow HTTPS traffic` box under the `Firewall` section.

### 1.5.2. Prepare storage volumes

We recommend that the repositories and the database for Uyuni are stored on separate storage devices to the root volume. This will help to avoid data loss. Do not use logical volume management (LVM) for public cloud installations.

You must set up the storage devices before you run the YaST Uyuni setup procedure.

The size of the disk for repositories storage is dependent on the number of distributions and channels you intend to manage with Uyuni. When you attach the virtual disks, they will appear in your instance as Unix device nodes. The names of the device nodes will vary depending on your provider, and the instance type selected.



Ensure the root volume of the Uyuni Server is 100 GB or larger. Add an additional storage disk of 500 GB or more, and choose SSD storage if you can. The cloud images for Uyuni Server use a script to assign this separate volume when your instance is launched.

When you launch your instance, you can log in to the Uyuni Server and use this command to find all available storage devices:

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

If you are not sure which device to choose, use the `lsblk` command to see the name and size of each device. Choose the name that matches with the size of the virtual disk you are looking for.

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

```
/usr/bin/suma-storage <devicename>
```

## Chapter 2. Installation

This section describes the process to install Uyuni components.

It is possible to use a public cloud instance to install Uyuni. For more information on using Uyuni on a public cloud, see **Specialized-guides > Public-cloud-guide**.

### 2.1. Uyuni Server

#### 2.1.1. Install Uyuni Server with openSUSE

Uyuni Server can be installed on openSUSE.

For requirements, see **Installation-and-upgrade > Uyuni-install-requirements**.



For more information about the latest version and updates of openSUSE Leap, see <https://doc.opensuse.org/release-notes/>.

##### 2.1.1.1. Install Uyuni on openSUSE Leap

*Procedure: Installing openSUSE Leap with Uyuni*

1. As the base system, install openSUSE Leap with all available service packs and package updates applied.
2. Configure a resolvable fully qualified domain name (FQDN) with **yast > System > Network Settings > Hostname/DNS**.
3. Set variables to use to create repository as root:

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

4. Add the repository for installing the Uyuni Server software as root:

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

5. Refresh metadata from the repositories as root:

```
zypper ref
```

6. Install the pattern for the Uyuni Server as root:

```
zypper in patterns-uyuni_server
```

## 7. Reboot.

- 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>.

When the installation is complete, you can continue with Uyuni setup. For more information, see **Installation-and-upgrade > Uyuni-server-setup**.

### 2.1.2. Installation on Public Cloud

Public clouds provide Uyuni under a Bring Your Own Subscription (BYOS) model. That means that they pre-install Uyuni, so you do not need to perform any installation steps.

However, you will need to perform some additional setup steps before you can use Uyuni. For public cloud setup instructions, see **Installation-and-upgrade > Pubcloud-setup**.

## 2.2. Uyuni Proxy

### 2.2.1. Install Uyuni Proxy with openSUSE Leap

Uyuni Proxy can be installed on openSUSE Leap 15.5.

*Procedure: Installing openSUSE Leap with Uyuni Proxy*

1. Install openSUSE Leap and apply all package updates available.
2. Configure a resolvable fully qualified domain name (FQDN) with **yast > System > Network Settings > Hostname/DNS**.
3. Add the repository with the Uyuni Proxy software. As root enter:

```
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. Refresh metadata from the repositories. As root enter:

```
zypper ref
```

5. Install the pattern for the Uyuni Proxy: As root enter:

```
zypper in patterns-uyuni_proxy
```

6. Reboot the 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>.

When the installation is complete, you can continue with Uyuni setup. For more information, see **Installation-and-upgrade > Uyuni-proxy-registration**.

### 2.2.2. Install containerized Uyuni Proxy



Only openSUSE Leap 15.3 and newer are supported to be used as container host for Uyuni Proxy containers.

The container host must be connected to Uyuni as a Salt client. Connecting container host as a traditional client will not work because required packages will not be available.

#### 2.2.2.1. Container host requirements

Table 11. Proxy Container host hardware requirements

Hardware	Details	Recommendation
CPU		Minimum 2 dedicated 64-bit CPU cores
RAM	Test Server	Minimum 2 GB
	Production Server	Minimum 8 GB
Disk Space		Minimum 100 GB

Table 12. Proxy Container host software requirements

Software	Details	Remark
Connection Method	Salt	Host must be configured as a Salt client



To ensure that domain name of the Uyuni Server can be resolved by the clients:

- \* Both container proxy and client machines must be connected to a DNS server
- \* Reverse lookup must work

#### 2.2.2.2. Install container services on the host system



Container host to be used as a base for Uyuni Proxy containers needs to be first registered as a Salt client to the Uyuni Server.

For more information about registering Salt client to the Uyuni Server, see **Client-configuration > Registration-overview**.



`Containers` Module is required to be available for container host.

Uyuni Proxy containers are using `podman` and `systemd` to run and manage all proxy containers.

First step is to install container control files provided by package `uyuni-proxy-systemd-services`.

#### *Procedure: Installation of container services for Uyuni Proxy*

1. Assign `Containers` Module software channel to the container host in the Uyuni. For more information about assigning software channels to the system, see **Administration > Channel-management**.
2. Log in as `root` on the container host.
3. Manually install Uyuni Proxy service package:

```
zypper install uyuni-proxy-systemd-services
```

#### 2.2.2.3. Customize Uyuni Proxy configuration

Uyuni Proxy containers require some volumes to be mounted for long term storage. Those volumes are automatically created by `podman` and can be listed using the `podman volume ls` command. By default, `podman` stores the files of the volumes in `/var/lib/containers/storage/volumes`. The volumes are named:

- `uyuni-proxy-squid-cache`
- `uyuni-proxy-rhn-cache`
- `uyuni-proxy-tftpboot`

To override default volume settings, create the volumes prior to the first start of the pod using the `podman volume create` command.

It is possible to add custom arguments passed to `podman container pod` to `/etc/sysconfig/uyuni-proxy-systemd-services.config`:

```
EXTRA_POD_ARGS=' '
```

In this file it is possible to modify `tag` to use for container images:

```
TAG=latest
```



Changing the `uyuni-proxy-systemd-services.config` file and especially the TAG setting is dangerous and can cause a non-functional system.

#### 2.2.2.3.1. Using a custom container image for a service

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. The `uyuni-proxy` CLI bundled with the package, runs `update image` with the following parameters:

- `-s` for the service name
- `-t` for the version tag
- `-r` for the registry path

For example, use it like this:

```
uyuni-proxy update image -s httpd -t 0.1.0 -r registry.opensuse.org/uyuni
```

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

To reset the values to defaults, run the `proxy reset` command, specifying the service with the `-s` parameter:

```
uyuni-proxy reset -s httpd
```

This command first resets the configuration of the `httpd` service to the global defaults and then reloads it.

For more information, see `uyuni-proxy --help`.

#### 2.2.2.4. Allow network access for provided services on container host firewall

Uyuni Proxy containers work as so called node-port service. This means proxy container pod shares container host network TCP and UDP port space. For this reason container host firewall must be configured to accept incoming traffic on ports used by Uyuni Proxy containers. Those ports are:

- 69/UDP - TFTP
- 80/TCP - HTTP
- 443/TCP - HTTPS
- 4505/TCP - Salt

- 4506/TCP - Salt
- 8022/TCP - SSH

Continue with setting up the installed Uyuni Proxy as a containers at [proxy-container-setup.pdf](#).

## 2.2.3. Install Containerized Uyuni Proxy on k3s

### 2.2.3.1. Installing k3s

On the container host machine, install k3s without the load balancer and traefik router (replace <K3S\_HOST\_FQDN> with the FQDN of your k3s host):

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

### 2.2.3.2. Configuring cluster access

helm needs a configuration file to connect to the target kubernetes cluster.

On the cluster server machine run the following command to create the kubeconfig-k3s.yaml configuration file. The kubeconfig-k3s.yaml file can be optionally transferred to a work machine:

```
kubectl config view --flatten=true | sed 's/127.0.0.1/<K3S_HOST_FQDN>/'
>kubeconfig-k3s.yaml
```

Before calling helm, run:

```
export KUBECONFIG=/path/to/kubeconfig-k3s.yaml
```

### 2.2.3.3. Installing helm



The Containers Module is required to install helm.

To install it run:

```
zypper in helm
```

### 2.2.3.4. Installing metalLB

metalLB is the load balancer that will expose the Uyuni proxy pod services to the outside world. To install it, run:



```
helm repo add metallb https://metallb.github.io/metallb
helm install --create-namespace -n metallb metallb metallb/metallb
```

MetallB still requires a configuration to know the virtual IP address range to be used. In this example, the virtual IP addresses will be from 192.168.122.240 to 192.168.122.250, but that range could be lowered to a single address if the host only exposes the Uyuni proxy. These addresses need to be a subset of the server network.

Create a metallb-config.yaml configuration file with the following settings and an IP address range that aligns with the deployed network:

```
apiVersion: metallb.io/v1beta1
kind: IPAddressPool
metadata:
  name: l2-pool
  namespace: metallb
spec:
  addresses:
  - 192.168.122.240-192.168.122.250
---
apiVersion: metallb.io/v1beta1
kind: L2Advertisement
metadata:
  name: l2
  namespace: metallb
spec:
  ipAddressPools:
  - l2-pool
```

Apply this configuration by running:

```
kubectl apply -f metallb-config.yaml
```

### 2.2.3.5. Deploying the Uyuni proxy helm chart

Create a configuration file forcing the IP address that MetallB will use for the Uyuni Proxy services. This IP address needs to be the one to which the proxy FQDN entered when creating the proxy configuration. It also needs to be resolvable from both the Uyuni Server and the client systems to connect to the proxy.

This example will use 192.168.122.241.

Create a custom-values.yaml file with the following content. If the MetallB IP address range only contains a single address, the last line can be removed.

```
services:
  annotations:
    metallb.universe.tf/allow-shared-ip: key-to-share-ip
    metallb.universe.tf/loadBalancerIPs: 192.168.122.241
```



The parameter `metallb.universe.tf/allow-shared-ip` does not need changing.

You need to adjust the parameter `metallb.universe.tf/loadBalancerIPs` to your network setup.

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 [proxy-container-setup.pdf](#). Copy and extract the configuration `tar.gz` file and then deploy the helm chart:

```
tar xf /path/to/config.tar.gz
helm install uyuni-proxy oci://registry.opensuse.org/uyuni/proxy -f
config.yaml -f httpd.yaml -f ssh.yaml -f custom-values.yaml
```

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

## Chapter 3. Setup

This section describes the initial steps you need to take after installation to make your Uyuni environment ready to use.

### 3.1. Uyuni Server

#### 3.1.1. Uyuni Server Setup

This section covers Uyuni Server setup, using these procedures:

- Start Uyuni setup with YaST
- Create the main administration account with the Uyuni Web UI
- Name your base organization and add login credentials
- Synchronize the SUSE Linux Enterprise product channel from SUSE Customer Center

##### 3.1.1.1. Set up Uyuni with YaST

This section will guide you through Uyuni setup procedures.

###### *Procedure: Uyuni Setup*

1. Log in to the Uyuni Server and start YaST.
2. In YaST, navigate to **Network Services > Uyuni Setup** to begin the setup.
3. From the introduction screen select **Uyuni Setup > Set up Uyuni from scratch** and click **[Next]** to continue.
4. Enter an email address to receive status notifications and click **[Next]** to continue. Uyuni can sometimes send a large volume of notification emails. You can disable email notifications in the Web UI after setup, if you need to.
5. Enter your certificate information and a password. Passwords must be at least seven characters in length, and must not contain spaces, single or double quotation marks ( ' or " ), exclamation marks ( ! ), or dollar signs ( \$ ). Always store your passwords in a secure location.



You must have the certificate password to set up the Uyuni Proxy.

6. Click **[Next]** to continue.
7. From the **Uyuni Setup > Database Settings** screen, enter a database user and password and click **[Next]** to continue. Passwords must be at least seven characters in length, and must not contain spaces, single or double quotation marks ( ' or " ), exclamation marks ( ! ), or dollar signs ( \$ ). Always store your passwords in a secure location.
8. Click **[Next]** to continue.
9. Click **[Yes]** to run setup when prompted.

10. When setup is complete, click **[Next]** to continue. You will see the address of the Uyuni Web UI.
11. Click **[Finish]** to complete Uyuni setup.

### 3.1.1.2. Create the Main Administration Account

This section covers how to create your organization's main administration account for Uyuni.



The main administration account has the highest authority within Uyuni. Ensure you keep access information for this account secure.

We recommend that you create lower level administration accounts for organizations and groups. Do not share the main administration access details.



Newer browser versions can block web access to the Uyuni Server FQDN because of HSTS.

Installing the CA certificate from the pub directory via HTTP and importing it to the browser will allow access to the server.

1. On the server, go to <http://<server>.example.com/pub/RHN-ORG-TRUSTED-SSL-CERT>.
2. Import the certificate file. In the browser settings (for Firefox), open **Privacy & Security > Certificates > View Certificates**, and import the file.

#### *Procedure: Setting Up the Main Administration Account*

1. In your web browser, enter the address for the Uyuni Web UI. This address was provided after you completed setup. For more information, see [uyuni-server-setup.pdf](#).
2. Log in to the Web UI, navigate to the **Create Organization > Organization Name** field, and enter your organization name.
3. In the **Create Organization > Desired Login** and **Create Organization > Desired Password** fields, enter your username and password.
4. Fill in the Account Information fields including an email for system notifications.
5. Click **[Create Organization]** to finish creating your administration account.

When you have completed the Uyuni Web UI setup, you are taken to the **Home > Overview** page.

### 3.1.1.3. Optional: Synchronizing Products from SUSE Customer Center

SUSE Customer Center (SCC) maintains a collection of repositories which contain packages, software and updates for all supported enterprise client systems. These repositories are organized into channels each of which provide software specific to a distribution, release, and architecture. After synchronizing with SCC, clients can receive updates, be organized into groups, and assigned to specific product software

channels.

This section covers synchronizing with SCC from the Web UI and adding your first client channel.



For Uyuni, synchronizing products from SUSE Customer Center is optional.

Before you can synchronize software repositories with SCC, you will need to enter organization credentials in Uyuni. The organization credentials give you access to the SUSE product downloads. You will find your organization credentials in <https://scc.suse.com/organizations>.

Enter your organization credentials in the Uyuni Web UI:

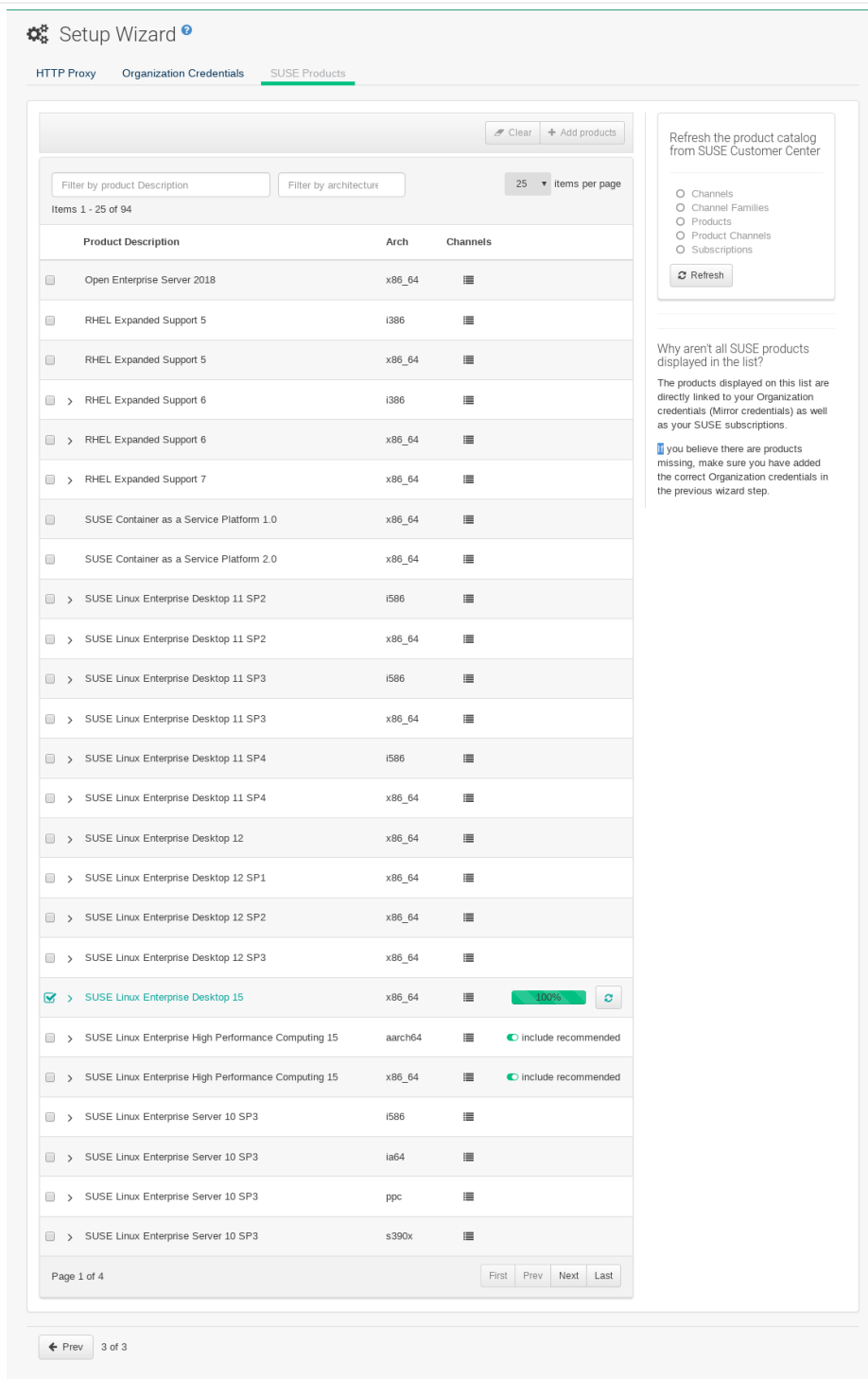
*Procedure: Entering Organization Credentials*

1. In the SUSE Manager Web UI, navigate to **Main Menu > Admin > Setup Wizard**.
2. In the Setup Wizard page, navigate to the **[Organization Credentials]** tab.
3. Click **[Add a new credential]**.
4. Enter a username and password, and click **[Save]**.

A check mark icon is shown when the credentials are confirmed. When you have successfully entered the new credentials, you can synchronize with SUSE Customer Center.

*Procedure: Synchronizing with SUSE Customer Center*

1. In the Uyuni Web UI, navigate to **Admin > Setup Wizard**.
2. From the Setup Wizard page select the **[SUSE Products]** tab. Wait a moment for the products list to populate. If you previously registered with SUSE Customer Center a list of products will populate the table. This table lists architecture, channels, and status information. For more information, see **Reference > Admin**.



3. If your SUSE Linux Enterprise client is based on x86\_64 architecture scroll down the page and select the check box for this channel now.

- Add channels to Uyuni by selecting the check box to the left of each channel. Click the arrow symbol to the left of the description to unfold a product and list available modules.
- Click **[Add Products]** to start product synchronization.

After adding the channel, Uyuni will schedule the channel to be synchronized. This can take a long time as Uyuni will copy channel software sources from the SUSE repositories located at SUSE Customer Center to local `/var/spacwalk/` directory of your server.



In some environments, transparent huge pages provided by the kernel can slow down PostgreSQL workloads significantly.

To disable transparent huge pages, set the `transparent_hugepage` kernel parameter to `never`. You will also need to open the `/etc/default/grub` file and add or edit the line `GRUB_CMDLINE_LINUX_DEFAULT`. For example:

```
GRUB_CMDLINE_LINUX_DEFAULT="resume=/dev/sda1
splash=silent quiet showopts elevator=none
transparent_hugepage=never"
```

To write the new configuration run `grub2-mkconfig -o /boot/grub2/grub.cfg`.

Monitor the channel synchronization process in real-time by viewing channel log files located in the directory `/var/log/rhn/reposync`:

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

When the channel synchronization process is complete, you can continue with client registration. For more instructions, see **Client-configuration > Registration-overview**.

### 3.1.2. Setup Wizard

When you have completed your Uyuni installation, you can use the setup wizard to complete the last few steps. The setup wizard allows you to configure the HTTP proxy, organization credentials, and SUSE products.

The setup wizard is displayed by default when you log in the Uyuni Web UI for the first time. You can access the setup wizard directly by navigating to **Admin > Setup Wizard**.

#### 3.1.2.1. Configure the HTTP Proxy

Uyuni can connect to the SUSE Customer Center (SCC) or other remote servers using a proxy. Navigate to the **HTTP Proxy** tab to configure the proxy.

You will need to provide the hostname of the proxy. Use the syntax `<hostname>:<port>`. For example: `<example.com>:8080`.

You can disable use of the proxy by clearing the fields.



When choosing a username or password for your Uyuni Proxy, ensure it does not contain an `@` or `:` character. These characters are reserved.



### 3.1.2.2. Configure Organization Credentials

Your SUSE Customer Center account is associated with the administration account of your organization. You can share your SUSE Customer Center access with other users within your organization. Navigate to the `Organization Credentials` tab to grant users within your organization access to your SUSE Customer Center account.

Click `[Add a new credential]`, enter the username and password of the user to grant access to, and click `[Save]`. A new credential card is shown for the user you have granted access to. Use these buttons on the card to edit or revoke access:

- Check credential validation status (green tick or red cross icon). To re-check the credential with SCC, click the icon.
- Set the primary credentials for inter-server synchronization (yellow star icon).
- List the subscriptions related to a certain credential (list icon).
- Edit the credential (pencil icon).
- Delete the credential (trash can icon).

### 3.1.2.3. Configure Products

Your SUSE subscription entitles you to access a range of products. Navigate to the `Products` tab to browse the products available to you and synchronize Uyuni with SUSE Customer Center.

Filters help you search for products by description or architecture.

The list is organized by product name showing products on top which have a subscription. Freely available products appear at the end of the list. For each product, you can see the architecture it can be used on. Click the arrow next to the product name to see associated channels and extensions. Click the `[Channels]` icon to see the complete list of channels associated with each product.

For products based on SUSE Linux Enterprise 15 and above, you can choose to only synchronize required packages, or to also include recommended products. Toggle the `[include recommended]` switch on to synchronize all products, and toggle the switch off to synchronize only required products.

You can further refine which products you want to synchronize by selecting or deselecting individual product.

When you have completed your selection, click `[Add products]`, and click `[Refresh]` to schedule the synchronization.

Synchronization progress for each product is shown in a progress bar next to the product name. Depending on the products you have chosen, synchronization can take up to several hours. New products will be available for you to use in Uyuni when synchronization is complete.

If your synchronization fails, it could be because of a third party GPG key or your company firewall blocking access to the download server. Please check the notification details for the error. For more information about troubleshooting product synchronization, see **Administration > Troubleshooting**.

### 3.1.3. Web Interface Setup

To use the Uyuni Web UI, navigate to your Uyuni URL in a browser. Sign in to the Web UI using your Uyuni Administration account.

While you are using the Web UI, click the  icon to access the documentation for that section.

The first time you sign in to the Web UI, complete the setup wizard to set your user preferences. You can access the setup wizard at any time by navigating to **Admin > Setup Wizard**.

After the initial setup is complete, signing in will take you the **Home > Overview** section. This section contains summary panes that provide important information about your systems.

The **Tasks** pane provides shortcuts to the most common Web UI tasks.

The **Inactive Systems** pane shows any clients that have stopped checking in to the Uyuni Server. You will need to check these clients.

The **Most Critical Systems** pane shows any clients that require software updates. Click the name of a client in the list to be taken to the **Systems > System Details** section for that client. From this page, you can apply any required updates.


The **Recently Scheduled Actions** pane shows all recent actions that have been run, and their status. Click the label of an action to see more detail.

The **Relevant Security Patches** pane shows all available security patches that need to be applied to your clients. It is critical that you apply security patches as soon as possible to keep your clients secure.

The **System Groups** pane shows any system groups you have created, and if the clients in those groups are fully updated.

The **Recently Registered Systems** pane shows all clients registered in the past thirty days. Click the name of a client in the list to be taken to the **Systems > System Details** section for that client.

#### 3.1.3.1. Web Interface Navigation

The Uyuni Web UI uses some standard elements to help you navigate. While you are using the Web UI, click the  icon to access the documentation for that section.

##### 3.1.3.1.1. Top Navigation Bar

The top navigation bar gives access to system-wide functions.

#### Notifications

The notification bell icon displays the number of unread notification messages in a circle. Click the notification icon to go to **Home > Notification Messages**.

## Search

Click the search magnifying glass icon to open the search box. You can search for systems (clients), packages, patches, or documentation. Click **[Search]** to go to the relevant Advanced Search page, and see your search results.

## Systems Selected

The systems selected icon displays the number of currently selected systems in a circle. Click the systems selected icon to go to **Systems > System Set Manager > Overview**. Click the eraser icon to unselect all systems. For more information about the system set manager, see **Client-configuration > System-set-manager**.

## User Account

The user account icon is displayed with the name of the currently signed-in user. Click the user account icon to go to **Home > User Account > My Account**.

## Organization

The organization icon is displayed with the name of the currently active organization. Click the organization icon to go to **Home > My Organization > Configuration**.

## Preferences

Click the cogs icon to go to **Home > My Preferences**.

## Sign Out

Click the exit icon to sign out the current user and return to the sign in screen.



If you add a distribution, newly synchronize channels, or register a system to the Uyuni Server, it can take several minutes for it to be indexed and appear in search results. If you need to force a rebuild of the search index, use this command at the command prompt:

```
rhns-search cleanindex
```

### 3.1.3.1.2. Left Navigation Bar

The left navigation bar is the main menu to the Uyuni Web UI.

## Expand

If you click the icon or the down-arrow of a menu entry, it expands this part of the menu tree without actually loading a page.

## Collapse

To collapse an open part of the menu system, click the up-arrow of a menu entry.

## Autoload

If you click the name of a menu entry, the first available page of that menu entry will get loaded and displayed automatically.

## Search

Enter a search string in the `Search` page field to find an entry of the menu tree. Available menu entries depend on the roles of the user.



Only Uyuni Administrators can access these sections:

- Images
- Users
- Admin`




### 3.1.3.1.3. Tables

Many sections present information in tables. You can navigate through most tables by clicking the back and next arrows above and below the right side of the table. Change the default number of items shown on each page by navigating to **Home > My Preferences**.

You can filter the content in most tables using the search bar at the top of the table. Sort table entries by clicking on the column header you want to sort by. Click the column header again to reverse the sort.

### 3.1.3.1.4. Patch Alert Icons

Patches are represented by three main icons, depending on the type of patch. Icons are coloured either green, yellow, or red, depending on the severity.

Icon	Description
	The shield icon is a security alert. A red shield is the highest priority security alert.
	The bug icon is a bug fix alert.
	The squares icon is an enhancement alert.

Some additional icons are used to give extra information:

Icon	Description
	The circling arrows icon indicates that applying a patch will require a reboot.
	The archive box icon indicates that a patch will have an effect on package management.

### 3.1.3.1.5. Interface Customization

By default, the Uyuni Web UI uses the theme appropriate to the product you have installed. You can change the theme to reflect the Uyuni or SUSE Manager colors. The SUSE Manager theme also has a dark option available. To change the theme using the Web UI, navigate to **Home > My Preferences** and locate the **Style Theme** section.

For information about changing the default theme, see **Administration > Users**.

### 3.1.3.1.6. Request Timeout Value

As you are using the Web UI, you are sending requests to the Uyuni Server. In some cases, these requests can take a long time, or fail completely. By default, requests will time out after 30 seconds, and a message is displayed in the Web UI with a link to try sending the request again.

You can configure the default timeout value in the `etc/rhn/rhn.conf` configuration file, by adjusting the `web.spa.timeout` parameter. Restart the `tomcat` service after you change this parameter. Changing this setting to a higher number could be useful if you have a slow internet connection, or regularly perform actions on many clients at once.

## 3.1.4. Public Cloud Setup

Uyuni Server needs to be registered with SUSE Customer Center to receive updates before you can sign in.



You must have set up the storage devices before you run the YaST Uyuni setup procedure. For more information, see **Installation-and-upgrade > Pubcloud-requirements**.

Follow the cloud providers instructions to SSH into the instance, and run this command to start set up:

```
yast2 susemanager_setup
```

Follow the prompts, and wait for the setup to finish.

For detailed instructions on setting up Uyuni with YaST, see **Installation-and-upgrade > Server-setup**.

### 3.1.4.1. Activate the public cloud module

To use Uyuni on a public cloud instance, you need to activate the public cloud module.

*Procedure: Activating the public cloud module*

1. On the Uyuni Server, open the YaST management tool, and navigate to **Software > Software Repositories**.
2. Click **[Add]** and select **Extensions and Modules** from **Registration Server**.

3. In the Available extensions field, select Public Cloud Module.

If you prefer to use the command line, you can add the module with this command:

```
SUSEConnect -p sle-module-public-cloud/15.5/x86_64
```

When the installation procedure has finished, you can check that you have all the required modules. At the command prompt, enter:

```
SUSEConnect --status-text
```

For Uyuni Server on a public cloud, the expected modules are:

- SUSE Linux Enterprise Server Basesystem Module
- Python 3 Module
- Server Applications Module
- Web and Scripting Module
- SUSE Manager Server Module
- Public Cloud Module

#### 3.1.4.2. Complete setup in the Web UI

Open the Uyuni Web UI with a web browser, using an address like this:

```
https://<public_IP>
```

Sign in to the Uyuni Web UI with the administrator account. The username and password varies depending on your provider.

*Table 13. Default Administrator Account Details*

Provider	Default Username	Default Password
Amazon EC2	admin	<instance-ID>
Google Compute Engine	admin	<instance-ID>
Microsoft Azure	admin	<instance-name>-suma

You can retrieve the instance name or ID from the public cloud instance web console, or from the command prompt:

Amazon EC2:

```
ec2metadata --instance-id
```

Google Compute Engine:

```
gcemetadata --query instance --id
```

Microsoft Azure:

```
azuremetadata --compute --name
```

When you sign in to the administrator account for the first time, you are given an automatically generated organization name. Change this by navigating to **Admin > Organizations**, and editing the organization name.



When you have signed in to the administrator account for the first time, change the default password to protect your account.

For more information about setting up your Uyuni Server, see **Installation-and-upgrade > Server-setup**.

#### 3.1.4.3. Adding Products and Starting Repositories Synchronization

Use the Uyuni Web UI to add the required software products, and schedule a repository synchronization. The best way to do this is to navigate to **Admin > Setup Wizard** and follow the prompts.

For more information about the setup wizard, see **Installation-and-upgrade > Setup-wizard**.

If you are intending to register Ubuntu or Red Hat Enterprise Linux clients, you need to set up custom repositories and channels. For more information, see the relevant section in **Client-configuration > Registration-overview**.

To synchronize your channels, navigate to **Software > Manage > Channels**. Click each channel you created, navigate to the **Repositories > Sync** tab, and click **[ Sync Now ]**. You can also schedule synchronization from this screen.



Before bootstrapping a client, make sure all the selected channels for that product are synchronized.

Synchronization can sometimes take several hours, in particular for openSUSE, SLES ES, and RHEL channels.

When you have your Uyuni Server set up, you are ready to start registering clients. For more information about registering clients on a public cloud, see **Client-configuration > Clients-pubcloud**.



### 3.1.5. Connect PAYG instance

In the three major public cloud providers (AWS, GCP and Azure), SUSE:

- provides customized PAYG product images for SLES, SLES for SAP, etc.
- operates per-region RMT Servers mirroring repositories for products available as PAYG

This document describes how to connect existing PAYG instance to Uyuni server, and gives basic information about credentials collection from the instance. The goal of this connection is to extract authentication data so the Uyuni Server can connect to a cloud RMT host. Then the Uyuni Server has access to products on the RMT host that are not already available with the SUSE Customer Center organization credentials.

Before using the PAYG feature ensure:

- The PAYG instance is launched from the correct SUSE product image (for example, SLES, SLES for SAP, or SLE HPC) to allow access to the desired repositories
- Uyuni Server has connectivity to the PAYG instance (ideally in the same region) either directly or via a bastion
- A basic SUSE Customer Center account is required. Enter your valid SUSE Customer Center credentials in **Admin > Setup Wizard > Organization Credentials**. This account is required for accessing the Uyuni client tools for bootstrapping regardless of PAYG instances.
- If you bootstrap the PAYG instance to SUSE Manager, SUSE Manager will disable its PAYG repositories then add repositories from where it mirrored the data from the RMT server. The final result will be PAYG instances acquiring the same repositories from the RMT servers but through the SUSE Manager server itself. Of course repositories can still be setup primarily from SCC.

#### 3.1.5.1. Connecting PAYG instance

*Procedure: Connecting new PAYG instance*

1. In the Uyuni Web UI, navigate to **Admin > Setup Wizard > PAYG**, and click **[Add PAYG]**.
2. Start with the page section `PAYG connection Description`.
3. In the `Description` field, add the description.
4. Move to the page section `Instance SSH connection data`.
5. In the `Host` field, enter the instance DNS or IP address to connect from Uyuni.
6. In the `SSH Port` field, enter the port number or use default value 22.
7. In the `User` field, enter the username as specified in the cloud.
8. In the `Password` field, enter the password.
9. In the `SSH Private Key` field, enter the instance key.
10. In the `SSH Private Key Passphrase` field, enter the key passphrase.



Authentication keys must always be in PEM format.

If you are not connecting directly to the instance, but via SSH bastion, proceed with [Procedure: Adding SSH bastion connection data](#).

Otherwise, continue with [Procedure: Finishing PAYG connecting](#).

*Procedure: Adding SSH bastion connection data*

1. Navigate to the page section `Bastion SSH connection data`.
2. In the `Host` field, enter the bastion hostname.
3. In the `SSH Port` field, enter the bastion port number.
4. In the `User` field, enter the bastion username.
5. In the `Password` field, enter the bastion password.
6. In the `SSH Private Key` field, enter the bastion key.
7. In the `SSH Private Key Passphrase` field, enter the bastion key passphrase.

Complete the setup process with with [Procedure: Finishing PAYG connecting](#).

*Procedure: Finishing PAYG connecting*

1. To complete adding new PAYG connection data, click **[Create]**.
2. Return to PAYG connection data `Details` page. The updated connection status is displayed on the top section named `Information`.
3. Connection status is shown in `Admin > Setup Wizard > Pay-as-you-go` screen too.
4. If the authentication data for the instance are correct, the column `Status` shows "Credentials successfully updated."



If the invalid data are entered at any point, the newly created instance is shown in `Admin > Setup Wizard > PAYG`, with column `Status` displaying error message.

As soon as the authentication data is available on the server, the list of available products is updated.

Available products are all versions of the same product family and architecture as the one installed in the PAYG instance. For example, if the instance has the SLES 15 SP1 product installed, SLES 15 SP2, SLES 15 SP3, SLES 15 SP4 and SLES 15 SP5 are automatically shown in `Admin > Setup Wizard > Products`.

Once the products are shown as available, the user can add a product to Uyuni by selecting the checkbox next to the product name and clicking **[Add product]**.

After the success message you can verify the newly added channels in the Web UI, by navigating to `Software > Channel List > All`.

To monitor the syncing progress of each channel, check the log files in the `/var/log/rhn/reposync` directory on the Uyuni Server.



If a product is provided by both the PAYG instance and one of the SUSE Customer Center subscriptions, it will appear only once in the products list.

When the channels belonging to that product are synced, the data might still come from the SCC subscription, and not from the Pay-As-You-Go instance.

#### 3.1.5.1.1. Deleting the instance connection data

The following procedure describes how to delete SSH connection data of the instance.

*Procedure: Deleting connection data to instance*

1. Open Admin > Setup Wizard > PAYG.
2. Find the instance on the list of existing instances.
3. Click on the instance details.
4. Select **[Delete]** and confirm your selection.
5. You are returned to the list of instances. The one that was just deleted is no longer shown.

#### 3.1.5.2. Instance credential collect status

Uyuni server uses credentails collected from the instance to connect to the RMT server and to download the packages using reposync. These credentials are refreshed every 10 minutes by taskomatic using the defined SSH connection data. Connection to RMT server always uses the last known authentication credentials collected from the PAYG instance.

The status of the PAYG instance credentials collect is shown in the column `Status` or on the instance details page. When the instance is unreachable, the credential update process will fail and the credentials will become invalid after the second failed refresh. Synchronization of channels will fail when the credentials are invalid. To avoid this keep the connected instances running.

PAYG instance remains connected to Uyuni server unless SSH connection data is explicitly deleted. To delete the SSH connection data to the instance, use [Procedure: Deleting connection data to instance](#).

PAYG instance may not be accessible from the Uyuni server at all times.

- If the instance exists, but is stopped, the last known credentials will be used to try to connect to the instance. How long the credentials remain valid depends on the cloud provider.
- If the instance no longer exists, but is still registered with SUMA, its credentials are no longer valid and the authentication will fail. The error message is shown in the column `Status`.



The error message only indicates that the instance is not available. Further diagnostics about the status of the instance needs to be done on the cloud provider.



Any of the following actions or changes in the PAYG instance will lead to credentials failing: \* removing zypper credentials files \* removing the imported certificates \* removing cloud-specific entries from `/etc/hosts`

### 3.1.5.3. Registering PAYG system as a client

You can register a PAYG instance from where you harvest the credentials as a Salt client. The instance needs to have a valid cloud connection registered, otherwise it will not have access to channels. If the user removes the cloud packages, the credentials harvesting may stop working.

First set up the PAYG instance to collect authentication data, so it can synchronize the channels.

The rest of the process is the same as for any non-public-cloud client and consists of synchronizing channels, automatic bootstrap script creation, activation key creation and starting the registration.

For more about registering clients, see **Client-configuration > Registration-overview**.

### 3.1.5.4. Troubleshooting

#### Checking the credentials

- If the script fails to collect the credentials, it should provide a proper error message in the logs and in the Web UI.
- If the credentials are not working, `reposync` should show the proper error.

#### Using `registercloudguest`

- Refreshing or changing the `registercloudguest` connection to the public cloud update infrastructure should not interfere with the credentials usage.
- Running ``registercloudguest --clean`` will cause problems if no new cloud connection is registered with the cloud guest command.

## 3.2. Uyuni Proxy

### 3.2.1. Uyuni Proxy Registration

Proxy systems are registered as Salt clients using bootstrap script or Web UI.

This procedure describes software channel setup and registering the installed proxy as the Uyuni client, using an activation key.

#### *Procedure: Registering the Proxy*

1. On the Uyuni Server, create openSUSE Leap and the Uyuni Proxy channels with the `spacewalk-common-channels` command. `spacewalk-common-channels` is part of the `spacewalk-utils` package:

```
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
```

Instead of `uyuni-proxy-stable-leap-155` you can also try `uyuni-proxy-devel-leap` which is the current development version.



Before you can select the correct child channels while creating the activation key, ensure you have properly synchronized the openSUSE Leap channel with all the needed child channels and the Uyuni Proxy channel.

2. Create an activation key with openSUSE Leap as a base channel and the other channels as child channels. For more information about activation keys, see **Client-configuration > Activation-keys**.
3. Create a bootstrap script for the proxy, and adjust it. Add the GPG key to the `ORG_GPG_KEY=` parameter.
4. Bootstrap the client using the script. For more information, see **Client-configuration > Registration-bootstrap**.
5. Navigate to **Salt > Keys** and accept the key. When the key is accepted, the new proxy will show in **Systems > Overview** in the Recently Registered Systems section.
6. Alternatively, in the Uyuni Web UI, navigate to **System > Bootstrapping**.
7. Navigate to **System Details > Software > Software Channels**, and check that the proxy channel is selected.

For setting up a registered Uyuni Proxy, see [uyuni-proxy-setup.pdf](#).

### 3.2.2. Uyuni Proxy Setup

Uyuni Proxy requires additional configuration.

#### 3.2.2.1. Install the `uyuni_proxy` pattern

Check that the Proxy pattern is installed correctly. This step is part of **Installation-and-upgrade > Install-proxy-uyuni**. To verify a successful installation, on the server select the `pattern_uyuni_proxy` package for installation.

The salt-broker service will be automatically started after installation is complete. This service forwards Salt interactions to the Uyuni Server.



### Proxy Chains

It is possible to arrange Salt proxies in a chain. In such a case, the upstream proxy is named `parent`.

Make sure the TCP ports 4505 and 4506 are open on the proxy. The proxy must be able to reach the Uyuni Server or a parent proxy on these ports.

#### 3.2.2.2. Copy Server Certificate and Key

The proxy will share some SSL information with the Uyuni Server. Copy the certificate and its key from the Uyuni Server or the parent proxy.

As root, enter the following commands on the proxy using your Uyuni Server or parent Proxy (named `PARENT`):

```
mkdir -m 700 /root/ssl-build
cd /root/ssl-build
scp root@PARENT:/root/ssl-build/RHN-ORG-PRIVATE-SSL-KEY .
scp root@PARENT:/root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT .
scp root@PARENT:/root/ssl-build/rhn-ca-openssl.cnf .
```



To keep the security chain intact, the Uyuni Proxy functionality requires the SSL certificate to be signed by the same CA as the Uyuni Server certificate. Using certificates signed by different CAs for proxies and server is not supported.

#### 3.2.2.3. Run `configure-proxy.sh`

The `configure-proxy.sh` script finalizes the setup of your Uyuni Proxy.

Execute the interactive `configure-proxy.sh` script. Pressing *Enter* without further input will make the script use the default values provided between brackets [ ]. Here is some information about the requested settings:

#### Uyuni Parent

The Uyuni parent can be either another proxy or the Uyuni Server.

#### HTTP Proxy

A HTTP proxy enables your Uyuni proxy to access the Web. This is needed if direct access to the Web is prohibited by a firewall.

#### Traceback Email

An email address where to report problems.

#### Use SSL

For safety reasons, press Y.

## Do You Want to Import Existing Certificates?

Answer N. This ensures using the new certificates that were copied previously from the Uyuni server.

## Organization

The next questions are about the characteristics to use for the SSL certificate of the proxy. The organization might be the same organization that was used on the server, unless of course your proxy is not in the same organization as your main server.

## Organization Unit

The default value here is the proxy's hostname.

## City

Further information attached to the proxy's certificate.

## State

Further information attached to the proxy's certificate.

## Country Code

In the `country code` field, enter the country code set during the Uyuni installation. For example, if your proxy is in the US and your Uyuni is in DE, enter DE for the proxy.



The country code must be two upper case letters. For a complete list of country codes, see <https://www.iso.org/obp/ui/#search>.

## Cname Aliases (Separated by Space)

Use this if your proxy can be accessed through various DNS CNAME aliases. Otherwise it can be left empty.

## CA Password

Enter the password that was used for the certificate of your Uyuni Server.

## Do You Want to Use an Existing SSH Key for Proxying SSH-Push Salt Minion?

Use this option if you want to reuse a SSH key that was used for SSH-Push Salt clients on the server.

If parts are missing, such as CA key and public certificate, the script prints commands that you must execute to integrate the needed files. When the mandatory files are copied, run `configure-proxy.sh` again. If you receive an HTTP error during script execution, run the script again.

`configure-proxy.sh` activates services required by Uyuni Proxy, such as `squid`, `apache2`, `salt-broker`, and `jabberd`.

To check the status of the proxy system and its clients, click the proxy system's details page on the Web UI (**Systems** > **Proxy**, then the system name). `Connection` and `Proxy` subtabs display various status information.

### 3.2.2.4. Enable PXE Boot

#### 3.2.2.4.1. Synchronize Profiles and System Information

To enable PXE boot through a proxy, additional software must be installed and configured on both the Uyuni Proxy and the Uyuni Server.

1. On the Uyuni Proxy, install the `susemanager-tftpsync-recv` package:

```
zypper in susemanager-tftpsync-recv
```

2. On the Uyuni Proxy, run the `configure-tftpsync.sh` setup script and enter the requested information:

```
configure-tftpsync.sh
```

You need to provide the hostname and IP address of the Uyuni Server and the proxy. You also need to enter the path to the tftpboot directory on the proxy.

3. On the Uyuni Server, install `susemanager-tftpsync`:

```
zypper in susemanager-tftpsync
```

4. On the Uyuni Server, run `configure-tftpsync.sh`. This creates the configuration, and uploads it to the Uyuni Proxy:

```
configure-tftpsync.sh FQDN_of_Proxy
```

5. Start an initial synchronization on the Uyuni Server:

```
cobbler sync
```

It can also be done after a change within Cobbler that needs to be synchronized immediately. Otherwise Cobbler synchronization will run automatically when needed. For more information about PXE booting, see **Client-configuration > Autoinst-pxeboot**.

#### 3.2.2.4.2. Configure DHCP for PXE through Proxy

Uyuni uses Cobbler for client provisioning. PXE (tftp) is installed and activated by default. Clients must be able to find the PXE boot on the Uyuni Proxy using DHCP. Use this DHCP configuration for the zone which contains the clients to be provisioned:



```
next-server: <IP_Address_of_Proxy>
filename: "pxelinux.0"
```

### 3.2.2.5. Replace the Uyuni Proxy

A proxy does not contain any information about the clients that are connected to it. Therefore, a proxy can be replaced by a new one at any time. The replacement proxy must have the same name and IP address as its predecessor.

Shut down the old proxy, and leave it installed while you prepare the replacement. Create a reactivation key for this system and then register the new proxy using the reactivation key. If you do not use the reactivation key, you will need to re-register all the clients against the new proxy.



The reactivation key is only needed if you do not want to lose the history of the machine. If you do not use a reactivation key, the replacement proxy will become a "new" one with a new ID.

#### *Procedure: Replacing a Proxy and Keeping the Clients Registered*

1. Before starting the actual migration procedure, save the data from the old proxy, if needed. Consider copying important or manually created data to a central place that can also be accessed by the new proxy.
2. Shut down the proxy.
3. Install a new Uyuni Proxy. For installation instructions, see [Proxy Installation](#).
4. In the Uyuni Web UI, select the newly installed Uyuni Proxy, and delete it from the systems list.
5. In the Web UI, create a reactivation key for the old proxy system: On the System Details tab of the old proxy click **Reactivation**. Click **Generate New Key**, and make a note of the new key, as you will need it later. For more information about reactivation keys, see **Reference > Systems**.
6. **OPTIONAL:** After the installation of the new proxy, you might also need to:
  - Copy the centrally saved data to the new proxy system
  - Install any other needed software
  - Set up TFTP synchronization if the proxy is used for autoinstallation



During the installation of the proxy, clients will not be able to reach the Uyuni Server. After you have deleted a proxy, the systems list can be temporarily incorrect. All clients that were previously connected to the proxy will show as being directly connected to the server instead. After the first successful operation on a client, such as execution of a remote command or installation of a package or patch, this information will automatically be corrected. This may take some hours.

### 3.2.3. Containerized Uyuni Proxy Setup

Once container host for Uyuni Proxy containers is prepared, setup of containers require few additional steps to finish configuration.

1. Generate Uyuni Proxy configuration archive file
2. Transfer configuration archive to the container host prepared in installation step and extract it
3. Start `systemd` proxy services

#### 3.2.3.1. Create and generate Uyuni Proxy configuration

Configuration of Uyuni Proxy is generated by Uyuni Server and this configuration generation is required to be done for each containerized proxy. There are two ways how to generate Uyuni configuration: use the Web UI or the `spacecmd` command.

*Procedure: Generating Of Container Services Configuration using Web UI*

1. In the Web UI, navigate to **Systems > Proxy Configuration** and fill the required data:
2. In the `Proxy FQDN` field type fully qualified domain name for the proxy.
3. In the `Parent FQDN` field type fully qualified domain name for the Uyuni Server or another Uyuni Proxy.
4. In the `Proxy SSH port` field type SSH port on which SSH service is listening on Uyuni Proxy. Recommended is to keep default 8022.
5. In the `Max Squid cache size [MB]` field type maximal allowed size for Squid cache. Typically this should be at most 60% of available storage for the containers.
6. In the `SSL certificate` selection list choose if new server certificate should be generated for Uyuni Proxy or an existing one should be used. You can consider generated certificates as Uyuni builtin (self signed) certificates.

Depending on the choice then provide either path to signing CA certificate to generate a new certificate or path to an existing certificate and its key to be used as proxy certificate.

The CA certificates generated on the server are stored in the `/root/ssl-build` directory.

For more information about existing or custom certificates and the concept of corporate and intermediate certificates, see **Administration > Ssl-certs-imported**.

7. Click **[Generate]** to register new proxy FQDN in Uyuni Server and generate configuration archive with details for container host.
8. After a few moments you are presented with file to download. Save this file locally.

### Container Based Proxy Configuration

You can generate a set of configuration files and certificates in order to register and run a container-based proxy. Once the following form is filled out and submitted you will get a .zip archive to download.

Proxy FQDN \*:

Server FQDN \*:   
FQDN of the server of proxy to connect to.

Proxy SSH port:   
Port range: 1 - 65535

Max Squid cache size (MB) \*:

Proxy administrator email \*:

SSL certificate \*: ☒ Create ☐ Use existing

CA certificate to use to sign the SSL certificate in PEM format \*:  No file selected.

CA private key to use to sign the SSL certificate in PEM format \*:  No file selected.

The CA private key password \*:

SSL Certificate data

Alternate CNAMES

2-letter country code:

State:

City:

Organization:

Organization Unit:

Email:

#### Procedure: Generating Of Container Services Configuration using spacecmd command

1. In the console run following command:

```
spacecmd proxy_container_config_generate_cert -- <proxy_fqdn>
<parent_fqdn> <squid_max_cache> <admin_email>
```

2. Answer questions presented by script, namely Uyuni credentials and CA password.

This will generate file `config.tar.gz` with configuration for the Uyuni Proxy containers.

For more information about `spacecmd` container proxy generation, see **Reference > Spacecmd**.

If a Proxy FQDN is used to generate Uyuni Proxy container configuration that is not a registered minion, 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.

#### 3.2.3.2. Transfer Uyuni Proxy configuration

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

Transfer this generated archive to the container host and extract it to configuration directory (by default `/etc/uyuni/proxy`).

### 3.2.3.3. Start Uyuni Proxy containers

Container can now be started by single `systemctl` command:

*Listing 1. Procedure: Start Uyuni Proxy containers*

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

*Listing 2. Procedure: Start Uyuni Proxy containers and make settings permanent*

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

Check if all containers started up as expected by calling

```
podman ps
```

Five Uyuni Proxy containers should be present:

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

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

## 3.2.4. Containerized proxy deployment using internal registry

It is possible to deploy containerized images in an environment without an internet connection. In such case, the images can be copied from SUSE registry to an internal registry, or saved to a tar file.

### 3.2.4.1. Image copying from SUSE registry to internal registry

This example illustrates deployment of Salt proxies only. Machines must have access to `registry.suse.com`.

*Procedure: Deploying Salt Proxy from an internal image registry*

1. On a machine with access to `registry.suse.com` install `skopeo`:

```
zypper in skopeo
```



This can be Uyuni Server.

## 2. Copy images between registries:

```
for image in httpd salt-broker squid ssh tftpd; do
    skopeo copy docker://registry.suse.com/suse/manager/4.3/proxy-
$image:latest
    docker://<your_server>/registry.suse.com/suse/manager/4.3/proxy-$image
done
skopeo copy docker://k8s.gcr.io/pause:latest
docker://<your_server>/k8s.gcr.io/pause:latest
```



For every skopeo command add `--dest-tls-verify=false` if the registry is not secured.

3. If the registry is unsecured, for example not configured with SSL, add the registry domain to the section `registries.insecure` on the containerized proxy virtual machine by editing:

```
/etc/containers/registries.conf
```

4. Before starting the pod, point the Podman where to get the pause image from on the internal registry:

```
echo -e '[engine]\ninfra_image =
"<your_server>/pause:latest"'>>/etc/containers/containers.conf
```

5. To start using the images from the internal registry please adapt the `NAMESPACE` value in file `/etc/sysconfig/uyuni-proxy-systemd-services.config`.



For the k3s deployment, add `--set repository=<your_server>` to the helm install command line.

### 3.2.4.2. Air-gapped solution for Podman

This example illustrates deployment of containerized image on a machine with no access to internet.

#### Procedure: Deploying air-gapped proxy

1. Before starting the pod, point the Podman where to get the pause image from on the internal registry:

```
echo -e '[engine]\ninfra_image =
"<your_server>/pause:latest"'>>/etc/containers/containers.conf
```



This command does not work on SLE 15 SP3 and earlier container hosts.

2. On a machine with internet access run:

```
for image in httpd salt-broker squid ssh tftpd; do
    podman pull registry.suse.com/suse/manager/4.3/proxy-$image
done
podman pull k8s.gcr.io/pause

podman save -m -o proxy-images.tar \
    k8s.gcr.io/pause \
    registry.suse.com/suse/manager/4.3/proxy-httpd \
    registry.suse.com/suse/manager/4.3/proxy-salt-broker \
    registry.suse.com/suse/manager/4.3/proxy-squid \
    registry.suse.com/suse/manager/4.3/proxy-ssh \
    registry.suse.com/suse/manager/4.3/proxy-tftpd
```



For the k3s deployment, add `--set repository=<your_server>` to the helm install command line.

3. Transfer the `proxy-images.tar` to the air-gapped proxy.
4. To make images available to be started when needed, run the command:

```
podman load -i proxy-images.tar
```

## Chapter 4. Upgrade introduction

**Updated:** 2023-10-31

Uyuni has three main components, all of which need regular updates. This guide covers updating the Uyuni Server, Proxy, and clients, as well as some underlying components, such as the database.

It is possible to automate some of the upgrades, but others need to be performed manually.



This guide is not intended to be read cover to cover. Instead, navigate to the component you want to upgrade, then identify the versions you are upgrading from and to.

Uyuni uses an YYYY.MM versioning schema suitable for rolling releases.

If you are upgrading the Uyuni Server, see **Installation-and-upgrade > Server-intro-uyuni**.

If you are upgrading the Uyuni Proxy, see **Installation-and-upgrade > Proxy-intro**.

If you are upgrading clients, see **Client-configuration > Client-upgrades**.

### 4.1. Upgrade the Server

Uyuni uses a rolling release versioning schema. Check the release notes for information about which upgrade strategy to use to upgrade to the next version:

#### Minor Upgrades

You can consider minor upgrades as regular upgrades. For more information, see **Installation-and-upgrade > Server-minor-upgrade-uyuni**.

#### Major Upgrades

You can consider major upgrades as special upgrades. In this case components such as the base operating system, Salt, or the PostgreSQL database will be upgraded. For more information, see **Installation-and-upgrade > Server-major-upgrade-uyuni**.

#### 4.1.1. Server - Minor Upgrade

Several times a year, the Uyuni team releases minor upgrades of the Uyuni Server. These updates address bug fixes and feature improvements, and sometimes include new features.



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>.

Performing a minor upgrade is similar to installing operating system package updates.

#### *Procedure: Updating Packages on the Uyuni Server*

By default, several update repositories are configured and enabled for the Uyuni Server. New and updated packages become available automatically.

It is recommended you make a backup of the server before upgrading. For more information about backing up Uyuni, see **Administration > Backup-restore**.

1. On the Uyuni Server, at the command prompt, as root, stop the spacewalk services:

```
spacewalk-service stop
```

2. Refresh software repositories:

```
zypper ref
```

3. Update new packages: (Repeat this if prompted by zypper)

```
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. Restart the spacewalk services:

```
spacewalk-service start
```



Reboot the server if a patch update recommends rebooting.



By default, zypper refreshes the repository every ten minutes (see `repo.refresh.delay` in `/etc/zypp/zypp.conf`). If `autorefresh` is disabled, run `zypper ref` to refresh all repositories.



Starting with Uyuni 2020.04 `spacewalk-schema-upgrade` is not needed anymore.

The schema upgrade is run automatically when the `spacewalk` service is started with `spacewalk-service start`.



Services affected by a package update are not automatically restarted after an update. You need to restart these services manually to avoid potential failures. Use `zypper ps` to check for applications that are using old code and require restarting.

### 4.1.2. Server - Major Upgrade

When Uyuni core components are upgraded to new major versions, you need to perform a major upgrade on the Uyuni Server. This is the case if a version upgrade of PostgreSQL, Salt, or openSUSE Leap is needed. openSUSE Leap is the underlying base operating system (OS).



Some additional manual steps might be required, and this information is only available in the release notes. For important extra information about your upgrade, see the release notes at:

<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.



Before the upgrade, ensure that storage requirements are met. For more information, see [uyuni-install-requirements.pdf](#). The migration procedure can fill the root partition if there is not enough space available due to the service pack migration and the download of new software packages. It is the same for the `/var/lib/pgsql` when upgrading PostgreSQL. It takes a copy of the old database, thus be sure to have at least enough space available to cope with a copy of the database.

The `server-migrator.sh` script migrates Uyuni Server to the latest version. It also upgrades the

underlying operating system to version 15.5. The script is part of the `susemanager` package.

#### *Procedure: Migrating the Uyuni Server*

1. Before running the `server-migrator.sh` script, check whether the most recent version of the `susemanager` package is installed:

```
zypper ref
zypper up susemanager
```

2. Run the `/usr/lib/susemanager/bin/server-migrator.sh` script to upgrade the base OS and Uyuni Server.



After the migration is complete, manually reboot the Uyuni Server:

## 4.2. Upgrade the Proxy

Uyuni Proxies are managed in the same way as clients.

Before you perform any proxy update, schedule a maintenance window. The clients registered to Uyuni through the proxy will not be able to connect to Uyuni while the update is in progress. For more information about maintenance windows, see **Administration > Maintenance-windows**.



The upgrade procedure to 2023.10 can either be a major or a minor upgrade. For more information, see the Uyuni 2023.10 release notes.

### Major Upgrade

See [proxy-uyuni.pdf](#).

### Minor Upgrade

See [proxy-minor-uyuni.pdf](#).

### 4.2.1. Proxy - Major Upgrade

Before you perform any proxy update, schedule a maintenance window. The clients registered to Uyuni through the proxy will not be able to connect to Uyuni while the update is in progress. For more information about maintenance windows, see **Administration > Maintenance-windows**.



Major proxy upgrades include a version upgrade of the operating system. For more information, see the Uyuni 2023.10 release notes.

#### 4.2.1.1. Preparation for the Upgrade

##### *Procedure: Adding openSUSE Leap 15.5 Software Channels at the Command Prompt*

1. At the command prompt on the Uyuni Server, as root, use the `spacewalk-common-`

channels command to add the appropriate channels:

```
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. Fully synchronize all channels with `spacewalk-repo-sync`.

#### 4.2.1.2. Upgrade the Proxy

To upgrade a proxy you first stop the proxy service, then you replace the software repositories and update the software, and finally you restart the proxy service.

##### *Procedure: Updating the Uyuni Proxy*

1. On the Uyuni Proxy, stop the proxy service:

```
spacewalk-proxy stop
```

2. In the Uyuni Server Web UI, navigate to **Systems > Proxy** and click the name of the proxy.
3. Click **Software > Software Channels**, and as the base channel select the openSUSE Leap 15.5 channel that is listed in the Customs Channels list.
4. In the Child Channels pane, select the 15.5 child channels.
5. Click **[Next]**, and Confirm Software Channel Change with **[Confirm]**.
6. Click **Details > Remote Command**, add `zypper --non-interactive dup --allow-vendor-change --replacefiles` to the script field, and click **[Schedule]**.
7. Wait until the remote command is executed.
8. On the Uyuni Proxy, start the proxy service:

```
spacewalk-proxy start
```

If you need to update many proxies, you can create an action chain of this command sequence on the Uyuni Server. You can use the action chain to perform updates on multiple proxies at the same time.

#### 4.2.2. Proxy - Minor Upgrade

Before you perform any proxy update, schedule a maintenance window. The clients registered to Uyuni through the proxy will not be able to connect to Uyuni while the update is in progress. For more information about maintenance windows, see **Administration > Maintenance-windows**.



Minor proxy upgrades do not include a version upgrade of the operating system. For more information, see the Uyuni 2023.10 release notes.

#### 4.2.2.1. Upgrade the Proxy

To update a proxy you first stop the proxy service, then update the software and finally restart the proxy service.

##### *Procedure: Updating the Uyuni Proxy*

1. On the Uyuni Proxy, stop the proxy service:

```
spacewalk-proxy stop
```

2. In the Uyuni Server Web UI, navigate to **Systems > Proxy** and click the name of the proxy.
3. Select all the packages to be updated on the proxy, and then apply the selection.
4. On the Uyuni Proxy, start the proxy service:

```
spacewalk-proxy start
```

If you need to update many proxies, you can create an action chain of this command sequence on the Uyuni Server. You can use the action chain to perform updates on multiple proxies at the same time.

## 4.3. Upgrade the Database

To successfully perform a major Uyuni update, you might need to upgrade the underlying database.

To upgrade to the latest PostgreSQL, see **Installation-and-upgrade > Db-migration-xy**.

This table shows the PostgreSQL version required for each version of Uyuni and openSUSE:

*Table 14. PostgreSQL Versions*

Uyuni version	Operating System version	PostgreSQL version
Uyuni >= 2020.07	openSUSE 15.2	PostgreSQL 12
Uyuni >= 2021.06	openSUSE 15.3	PostgreSQL 13
Uyuni >= 2022.06	openSUSE 15.4	PostgreSQL 14
Uyuni >= 2023.09	openSUSE 15.5	PostgreSQL 14

### 4.3.1. Database Migration to Latest Version

This section covers upgrading the PostgreSQL database to the latest version. If you are already using PostgreSQL 14, you do not need to perform this migration.

If you want to upgrade to the latest Uyuni version, you must be using PostgreSQL version 13, 14, or 15 depending on the underlying operating system:

- If you are running openSUSE Leap 15.3, use PostgreSQL 13.
- If you are running openSUSE Leap 15.4, use PostgreSQL 14.
- If you are running openSUSE Leap 15.5, use PostgreSQL 14.

#### 4.3.1.1. Prepare to Upgrade

Before you begin the upgrade, prepare your existing Uyuni Server and create a database backup.

PostgreSQL stores data at `/var/lib/pgsql/data/`.

*Procedure: Preparing to Upgrade*

1. Check the active PostgreSQL version:

```
psql --version
```

2. Check the active smdba version:

```
rpm -q smdba
```

PostgreSQL 14 requires smdba version 1.7.6 or later.

3. Perform a database backup. For more information on backing up, see **Administration > Backup-restore**.

#### 4.3.1.2. Upgrade PostgreSQL



Always create a database backup before performing a migration.

PostgreSQL upgrades can be performed in two ways: a regular upgrade, or a fast upgrade:

A regular upgrade creates a complete copy of the database, so you need double the existing database size of space available. Regular upgrades can take a considerable amount of time, depending on the size of the database and the speed of the storage system.

A fast upgrade only takes a few minutes, and uses almost no additional disk space. However, if a fast upgrade fails, you must restore the database from the backup. A fast upgrade reduces the risk of running out of disk space, but increases the risk of data loss when a backup does not exist or cannot be replayed.

A regular upgrade will copy the database files instead of creating hard links between the files.

PostgreSQL stores data at `/var/lib/pgsql/data/`.



Before running the DB upgrade make sure that the PostgreSQL user exists on the system. The `/etc/passwd` entry should look as follows:

```
postgres:x:26:26:PostgreSQL
Server:/var/lib/pgsql:/bin/bash
```

#### *Procedure: Performing a Regular Upgrade*

1. Perform a database backup. For more information on backing up, see **Administration > Backup-restore**.
2. Start the upgrade. Run the script:

```
/usr/lib/susemanager/bin/pg-migrate-x-to-y.sh
```

3. When the upgrade has successfully completed, you can safely delete the old database directory and reclaim lost disk space. The old directory is renamed to `/var/lib/pgsql/data-pg12` or `/var/lib/pgsql/data-pg10`, depending on the version you started from.

The `pg-migrate-x-to-y.sh` script performs these operations:

- Stop spacewalk services
- Shut down the running database
- Check if the latest PostgreSQL is installed and install it if necessary
- Switch from previous version of PostgreSQL to the latest as the new default
- Initiate the database migration
- Create a PostgreSQL configuration file tuned for use by Uyuni
- Start the database and spacewalk services



If the upgrade fails, the migration script will attempt to restore the database to its original state.

#### *Procedure: Performing a Fast PostgreSQL Upgrade*

1. Perform a database backup. Without a verified database backup, you must not initiate a fast upgrade. For more information on backing up, see **Administration > Backup-restore**.
2. Start the upgrade. Run the script.

```
/usr/lib/susemanager/bin/pg-migrate-x-to-y.sh -f
```

- 
3. When the upgrade has successfully completed, you can safely delete the old database directory and reclaim lost disk space. The old directory is renamed to `/var/lib/pgsql/data-pg12` or `/var/lib/pgsql/data-pg10`, depending on the version you started from.

## 4.4. Upgrade the Clients

Clients use the versioning system of their underlying operating system. For clients using SUSE operating systems, you can perform upgrades within the Uyuni Web UI.

For more information about upgrading clients, see **Client-configuration > Client-upgrades**.

---

## Chapter 5. 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. Secondly, 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".
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with...Texts.” line with this:

with the Invariant Sections being LIST THEIR TITLES, with the  
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.