

SUSE Manager '5.0'

Installation and Upgrade Guide

April 29 2024



Table of Contents

Deployment and Upgrade Guide Overview	1
1. Requirements	2
2. Deployment	3
3. Upgrade and Migration	4
4. Public Cloud	5
5. Requirements	6
5.1. General Requirements	6
5.1.1. SUSE Customer Center Account and Credentials	6
5.1.2. Supported Browsers for SUSE Manager Web UI	6
5.1.3. SSL Certificates	7
5.2. Hardware Requirements	7
5.2.1. Server Requirements	7
5.2.2. Proxy Requirements	9
5.2.3. Database Requirement	10
5.2.4. Persistent Storage and Permissions	10
5.3. Network Requirements	12
5.3.1. Fully Qualified Domain Name (FQDN)	12
5.3.2. Hostname and IP Address	13
5.3.3. Offline Deployment	13
5.3.4. Ports	13
5.4. Public Cloud Requirements	18
5.4.1. Network Requirements	18
5.4.2. Prepare Storage Volumes	19
6. Deployment	21
6.1. Server	21
6.1.1. Deploy	21
6.1.2. Setup	26
6.1.3. Manage	46
6.1.4. Public Cloud	50
6.2. Proxy	51
6.2.1. Deploy	51
7. Upgrade	62
7.1. Upgrade the Server	63
7.1.1. Migrating the SUSE Manager server to a containerized environment	64
7.2. Upgrade the Clients	65
8. GNU Free Documentation License	66

Deployment and Upgrade Guide

Overview

Updated: 2024-04-29

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

Chapter 1. Requirements

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

Chapter 2. Deployment

Describes tasks for deploying SUSE Manager as a container and initial setup.

Chapter 3. Upgrade and Migration

Describes upgrade and migration of SUSE Manager

Chapter 4. Public Cloud

You can also deploy SUSE Manager to a public cloud instance.

For more information on using SUSE Manager on a public cloud, see [Specialized-guides › Public-cloud-guide](#).

Chapter 5. Requirements

5.1. General Requirements

Before you begin installation, ensure that you have:

1. A SUSE Customer Center account. This account gives you access to organization credentials and registration keys for SLE Micro 5.5 and SUSE Manager Server and Proxy
2. Supported Browsers for SUSE Manager Web UI
3. SSL certificates for your environment. By default SUSE Manager '5.0' uses a self-signed certificate.

The following section contains more information on these requirements.

5.1.1. SUSE Customer Center Account and Credentials

Create an account with SUSE Customer Center prior to deployment of SUSE Manager '5.0'.

Procedure: Obtain Your Organization Credentials

1. Navigate to <https://scc.suse.com/login> in your Web browser.
2. Log in to your SCC account, or follow the prompts to create a new account.
3. If you have not yet done so, click **[Connect to an Organization]** and type or search for your organization.
4. Click **[Manage my Organizations]** and select your organization from the list by clicking on the organization name.
5. Click the **[Organization]** tab, and then select the **[Organization Credentials]** tab.
6. Record your login information for use during SUSE Manager setup.

Depending on your organization's setup, you might also need to activate your subscription, using the **[Activate Subscriptions]** menu.

For more information about using SCC, see <https://scc.suse.com/docs/help>.

5.1.2. Supported Browsers for SUSE Manager Web UI

In order to use the Web UI to manage your SUSE Manager environment, you will need to ensure

you are running an up-to-date web browser.

SUSE Manager is supported on:

- Latest Firefox browser shipped with SUSE Linux Enterprise Server
- Latest Chrome browser on all operating systems
- Latest Edge browser shipped with Windows

Windows Internet Explorer is not supported. The SUSE Manager Web UI will not render correctly under Windows Internet Explorer.

5.1.3. SSL Certificates

SUSE Manager uses SSL certificates to ensure that clients are registered to the correct server. By default, SUSE Manager uses a self-signed certificate. If you have certificates signed by a third-party CA, you can import them to your SUSE Manager installation.

- For more on self-signed certificates, see [Administration › Ssl-certs-selfsigned](#).
- For more on imported certificates, see [Administration › Ssl-certs-imported](#).

5.2. Hardware Requirements

This table outlines hardware and software requirements for the SUSE Manager Server and Proxy, on x86-64, ARM and s390x architecture.

For SUSE Manager for Retail hardware requirements, see [Retail › Retail-requirements](#).

5.2.1. Server Requirements

By default the SUSE Manager Server container stores packages in the `/var/lib/containers/storage/volumes/var-spacewalk/` directory. Repository synchronization fails if this directory runs out of disk space. Estimate how much space the `/var/lib/containers/storage/volumes/var-spacewalk/` directory requires based on the clients and repositories you plan to mirror.

Table 1. Server Hardware Requirements

Hardware	Details	Recommendation
CPU	x86-64, ARM, s390x	Minimum 4 dedicated 64-bit CPU cores
RAM	Minimum	16 GB
	Recommended	32 GB
Disk Space	/ (root directory)	Minimum 40 GB
	<code>/var/lib/containers/storage/volumes/var-pgsql</code>	Minimum 50 GB
	<code>/var/lib/containers/storage/volumes/var-spacewalk</code>	<p>Minimum storage required: 100 GB (this will be verified by the implemented check)</p> <p>* 50 GB for each SUSE product and Package Hub</p> <p>* 360 GB for each Red Hat product</p>
	<code>/var/lib/containers/storage/volumes/var-cache</code>	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

SUSE Manager performance depends on hardware resources, network bandwidth, latency between clients and server, etc.



Based on the experience and different deployments that are in use, the advice for optimal performance of SUSE Manager Server with an adequate number of proxies is to not exceed 10,000 clients per single server. It is highly recommended to move to the Hub setup and involve consultancy when you have more than 10,000 clients. Even with fine-tuning and an adequate number of proxies, such a large number of clients can lead to performance issues.

For more information about managing a large number of clients, see [Specialized-guides › Large-deployments](#).

5.2.2. Proxy Requirements

Table 2. Proxy Hardware Requirements

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

By default the SUSE Manager Proxy container caches packages in the `/var/lib/containers/storage/volumes/var-cache/` directory. If there is not enough space available in `/var/lib/containers/storage/volumes/var-cache/`, the proxy will remove old, unused packages and

replace them with newer packages.

As a result of this behavior:

- The larger `/var/lib/containers/storage/volumes/var-cache/` directory is on the proxy, the less traffic there will be between it and the SUSE Manager Server.
- By making the `/var/lib/containers/storage/volumes/var-cache/` directory on the proxy the same size as `/var/lib/containers/storage/volumes/var-spacewalk/` on the SUSE Manager Server, you avoid a large amount of traffic after the first synchronization.
- The `/var/lib/containers/storage/volumes/var-cache/` directory can be small on the SUSE Manager Server compared to the proxy. For a guide to size estimation, see the [Server Requirements](#) section.

5.2.3. Database Requirement

PostgreSQL is the only supported database. Using a remote PostgreSQL database or remote file systems (such as NFS) with the PostgreSQL database is not supported. In other words, PostgreSQL should be on the fastest available storage device for SUSE Manager.



Because of potential performance issues, running a PostgreSQL database remotely from SUSE Manager is discouraged. While such an environment is possible and even stable in many cases, there is always a risk of data loss if something goes wrong.

SUSE might not be able to provide assistance in such cases.

5.2.4. Persistent Storage and Permissions

Persistent volumes are created by default when deploying the container.

However, it is recommended that the repositories and the database for SUSE Manager are stored on separate storage devices. Such a setup helps avoid data loss in production environments.

Storage devices must be setup prior to deploying the container. For more details see: [Installation-and-upgrade › Container-management](#)

SUSE Manager requires three different volumes:

- Database volume: `/var/lib/containers/storage/volumes/var-pgsql`

- Channel volume: `/var/lib/containers/storage/volumes/var-spacewalk`
- Cache: `/var/lib/containers/storage/volumes/var-cache`

We recommend you use XFS as the filesystem type for all volumes. Additionally, for on-premise installations, consider using logical volume management (LVM) to manage the disks. The size of the disk for repositories storage is dependent on the number of distributions and channels you intend to manage with SUSE Manager. See the tables in this section for guides to estimate the size required.

On your SUSE Manager Server, use this command to find all available storage devices:

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

Use the `lsblk` command to see the name and size of each device.

Use the `suma-storage` command with the device names to set up the external disks as the locations for the database and repositories:

```
suma-storage <channel_devicename> [<database_devicename>]
```

The external storage volumes are set up as XFS partitions mounted at `/manager_storage` and `/pgsql_storage`.

It is possible to use the same storage device for both channel data and the database. This is not recommended, as growing channel repositories might fill up the storage, which poses a risk to database integrity. Using separate storage devices may also increase performance. If you want to use a single storage device, run `suma-storage` with a single device name parameter.

If you are installing a proxy, the `suma-storage` command only takes a single device name parameter and will set up the external storage location as the Squid cache.

When you create disk partitions for the SUSE Manager Server and Proxy, ensure you set the permissions correctly.

For `/var/lib/containers/storage/volumes/var-pgsql`:

- Owner: Read, Write, Execute
- Group: Read, Execute
- User: None

For `/var/lib/containers/storage/volumes/var-spacewalk`:

- Owner: Read, Write, Execute
- Group: Read, Write, Execute
- User: Read, Execute

Check the permissions with this command:

```
ls -l /var/lib/containers/storage/volumes/var-pgsql  
/var/lib/containers/storage/volumes/var-spacewalk
```

The output should look like this:

```
/var/lib/containers/storage/volumes/var-pgsql:  
total 0  
drwxr-x--- 1 10556 10556 48 Apr 19 14:33 _data  
  
/var/lib/containers/storage/volumes/var-spacewalk:  
total 0  
drwxr-xr-x 1 10552 root 30 Apr 19 14:34 _data
```

If required, change the permissions with these commands:

```
chmod 750 /var/lib/containers/storage/volumes/var-pgsql  
chmod 775 /var/lib/containers/storage/volumes/var-spacewalk
```

And owners with:

```
chown postgres:postgres /var/lib/containers/storage/volumes/var-pgsql  
chown wwwrun:www /var/lib/containers/storage/volumes/var-spacewalk
```

5.3. Network Requirements

This section details the networking and port requirements for SUSE Manager.

5.3.1. Fully Qualified Domain Name (FQDN)

The SUSE Manager 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>.

5.3.2. Hostname and IP Address

To ensure that the SUSE Manager 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>.

5.3.3. Offline Deployment

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

In a production environment, the SUSE Manager 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**.

5.3.4. Ports

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

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.

5.3.4.1. External Inbound Server Ports

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

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

Table 3. External Port Requirements for SUSE Manager 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.
80	TCP	HTTP	Required temporarily for some bootstrap repositories and automated installations.
443	TCP	HTTPS	Serves the Web UI, client, and server and proxy (<code>tftpsync</code>) requests.
4505	TCP	salt	Required to accept communication requests from clients. The client initiates the connection, and it stays open to receive commands from the Salt master.
4506	TCP	salt	Required to accept communication requests from clients. The client initiates the connection, and it stays open to report results back to the Salt master.
25151	TCP	Cobbler	

5.3.4.2. External Outbound Server Ports

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

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

Table 4. External Port Requirements for SUSE Manager 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.
25151	TCP	Cobbler	

5.3.4.3. Internal Server Ports

Internal ports are used internally by the SUSE Manager 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 SUSE Manager 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
```

5.3.4.4. External Inbound Proxy Ports

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

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

Table 6. External Port Requirements for SUSE Manager 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 (<code>tftpsync</code>) 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.

5.3.4.5. External Outbound Proxy Ports

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

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

Table 7. External Port Requirements for SUSE Manager Proxy

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

5.3.4.6. External Client Ports

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

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

Table 8. External Port Requirements for SUSE Manager Clients

Port number	Direction	Protocol	Notes
22	Inbound	SSH	Required for ssh-push and ssh-push-tunnel contact methods.
80	Outbound		Used to reach the server or proxy.
9090	Outbound	TCP	Required for Prometheus user interface.
9093	Outbound	TCP	Required for Prometheus alert manager.
9100	Outbound	TCP	Required for Prometheus node exporter.
9117	Outbound	TCP	Required for Prometheus Apache exporter.
9187	Outbound	TCP	Required for Prometheus PostgreSQL.

5.3.4.7. Required URLs

There are some URLs that SUSE Manager 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](#).

5.4. Public Cloud Requirements

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

5.4.1. Network Requirements

When you use SUSE Manager 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.



Running SUSE Manager on the public cloud means implementing robust security measures. It is essential to limit, filter, monitor, and audit access to the instance. SUSE strongly advises against a globally accessible SUSE Manager instance that lacks adequate perimeter security.

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

5.4.2. Prepare Storage Volumes

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

The SUSE Manager container utilizes default storage locations. These locations should be configured prior to deployment for custom storage. For more information see [Installation-and-upgrade › Container-management](#)



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

The size of the disk for repositories storage is dependent on the number of distributions and channels you intend to manage with SUSE Manager. 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 SUSE Manager 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 SUSE Manager 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 SUSE Manager 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>
```

For more information about setting up storage volumes and partitions, including recommended minimum sizes, see [Installation-and-upgrade › Hardware-requirements](#).

Chapter 6. Deployment

6.1. Server

6.1.1. Deploy

6.1.1.1. Deploy on SLE Micro 5.5

In this section, you will gain expertise in setting up and deploying a containerized SUSE Manager '5.0' Server. This process installs SLE Micro, and then interacts with the container through the container utilities `mgradm` and `mgrctl`.

6.1.1.1.1. Container Host General Requirements

For general requirements, see [Installation-and-upgrade › General-requirements](#).

A SLE Micro or SUSE Linux Enterprise Server server should be installed from installation media. This procedure is described in [installation-and-upgrade:container-deployment/suma/sle-micro-deployment.pdf](#).

6.1.1.1.2. Container Host Requirements

For CPU, RAM, and storage requirements, see [Installation-and-upgrade › Hardware-requirements](#).



To guarantee that clients can resolve the SUSE Manager '5.0' domain name, both the container server and host machines must be linked to a functional DNS server. Additionally, it is essential to ensure correct configuration of reverse lookups.

6.1.1.1.3. SLE Micro 5.5 Installation

Get a copy of the SLE Micro 5.5 installation media. You can begin the installation on either a virtual machine or on a physical server.

Procedure: SLE Micro 5.5 installation

1. Begin the installation from the installation media.

2. Adjust keyboard and language. Click the **checkbox** to accept the license agreement.
3. Click **[Next]** to continue.
4. Select your registration method. For this example, we will register the server with the SUSE Customer Center.
5. Enter your SUSE Customer Center e-mail address.
6. Enter your registration code for SLE Micro 5.5.



Base operating system for SUSE Manager '5.0' containerized Server

For SUSE Manager 5.0, the base operating system of the container is SUSE Linux Enterprise Server 15 SP6. You can find these keys in your SUSE Customer Center account.

7. If wanted activate online repositories.
8. Click **[Next]** to continue.
9. Select the SUSE Manager '5.0' Server extension **Checkbox**.
10. Click **Next** to continue.
11. Enter your SUSE Manager '5.0' Server extension registration code.



SUSE Manager as an extension

SUSE Manager '5.0' is installed as an extension. Therefore, in addition to acquiring SUSE Customer Center registration keys for the base Server, you will also need SUSE Customer Center registration codes for the following extensions:

- SUSE Manager '5.0' Server
- SUSE Manager '5.0' Proxy
- Retail Branch Server

12. Click **Next** to continue.
13. Enter or accept default **NTP Server**.
14. Click **Next** to continue.

15. Add the **root user** password twice to confirm.
16. Click **Next** to continue.
17. Adjust **Installation Settings** as required.
18. Click **Next** to continue.

This concludes the installation of SLE Micro 5.5.

6.1.1.1.4. Update the Container Host

When the installation completes, update the container host system.

Procedure: Update the container host and install the container utilities

1. Log in at the prompt as **root**.
2. Run **transactional-update**:

```
transactional-update
```

3. Reboot the system.
4. Log in as **root**.
5. Install the container utilities:

```
transactional-update pkg install mgradm mgrctl mgradm-bash-completion mgrctl-bash-completion
```

6. Reboot the system.

6.1.1.1.5. Deploy as container on SLE Micro 5.5

Basic and Advanced Deployment with mgradm

Procedure: Basic deployment of a SUSE Manager '5.0' container with Podman

1. From the terminal of the container host, run the following command as the **root** user. Entering your server's FQDN is optional. Leave blank for a default setup.

```
mgradm install podman <FQDN>
```

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



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

2. Enter a database and certificate password when prompted. Press [**Enter**].
3. Enter a certificate and administrator account password when prompted.



The administrator account password must be at least 5 characters and less than 48 characters in length.

4. Press [**Enter**].
5. Wait for deployment to complete.
6. Open a browser and proceed to your server's FQDN, or IP address.

In this section you learned the basic method for deploying a SUSE Manager '5.0' Server container.

Procedure: Advanced deployment of a SUSE Manager '5.0' container using a custom configuration file

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

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

# Password for the CA certificate
ssl:
  password: MySuperSecretSSLPassword

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

# Organization name
organization: YourOrganization

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

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



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

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

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



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

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

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

In this section you learned how to deploy the SUSE Manager Server container.

Persistent Volumes



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

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

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

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

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

For a list of all persistent volumes in the container see, [Installation-and-upgrade › Container-management](#).

6.1.1.2. SUSE Manager Offline Deployment

6.1.2. Setup

6.1.2.1. Setup Wizard

When you have completed your SUSE Manager installation, you can use the setup wizard to complete the last few steps. Here you can configure your organization credentials, and SUSE products.

You can access the setup wizard directly by navigating to **Admin › Setup Wizard**.

6.1.2.1.1. 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).

6.1.2.1.2. 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 SUSE Manager 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 SUSE Manager 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](#).

6.1.2.2. Web Interface Setup

To use the SUSE Manager Web UI, navigate to your SUSE Manager URL in a browser. Sign in to the Web UI using your SUSE Manager 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 SUSE Manager 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.

6.1.2.2.1. Web Interface Navigation

The SUSE Manager 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.

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 SUSE Manager 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
```

Left Navigation Bar

The left navigation bar is the main menu to the SUSE Manager 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 SUSE Manager Administrators can access these sections:

- Images
- Users
- Admin`

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.

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.

Interface Customization

By default, the SUSE Manager 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**.

Request Timeout Value

As you are using the Web UI, you are sending requests to the SUSE Manager 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.

6.1.2.3. Public Cloud Setup

SUSE Manager 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 SUSE Manager setup procedure. For more information, see [Installation-and-upgrade › Pubcloud-requirements](#).

Follow the cloud providers instructions to SSH into the instance.

6.1.2.3.1. Activate the Public Cloud Module

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

Procedure: Activating the Public Cloud Module

1. On the SUSE Manager 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/{sles-version}.{sp-version-number}/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 SUSE Manager 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

6.1.2.3.2. Complete Setup in the Web UI

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

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

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

Table 9. 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 SUSE Manager Server, see **Installation-and-upgrade › Server-setup**.

6.1.2.3.3. Adding Products and Starting Repositories Synchronization

Use the SUSE Manager 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 SUSE Manager 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](#).

6.1.2.4. 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 SUSE Manager server, and gives basic information about credentials collection from the instance. The goal of this connection is to extract authentication data so the SUSE Manager Server can connect to a cloud RMT host. Then the SUSE Manager 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
- SUSE Manager 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 SUSE Manager 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.

6.1.2.4.1. Connecting PAYG Instance

Procedure: Connecting new PAYG Instance

1. In the SUSE Manager 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 SUSE Manager.
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 [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 SUSE Manager 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 SUSE Manager 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.

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.

6.1.2.4.2. Instance Credential Collect Status

SUSE Manager 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 SUSE Manager 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 SUSE Manager 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`

6.1.2.4.3. 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](#).

6.1.2.4.4. 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.

6.1.2.5. SUSE Manager Server Setup

This section covers SUSE Manager Server setup, using these procedures:

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

- Set up SUSE Manager with external database



SUSE Manager is part of the SUSE Linux Enterprise product family and thus compatible with the software shipped with SUSE Linux Enterprise Server.

SUSE Manager is a complex system, and therefore installing third party software is not allowed. Installing monitoring software provided by a third party vendor is allowed only if you do not exchange basic libraries such as SSL, cryptographic software, and similar tools. As part of providing product support, SUSE reserves the right to ask to remove any third party software (and associated configuration changes) and then to reproduce the problem on a clean system.



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

6.1.2.5.1. Creating the Main Administration Account

This section guides you through creating your organization's main administration account for SUSE Manager.



The main administration account is the highest authority account within SUSE Manager and therefore account access information should be stored in a secure location.

For security it is recommended that the main administrator creates low level admin accounts designated for administration of organizations and individual groups.



Newer browser versions can block web access to the SUSE Manager Server FQDN in case the user enabled HSTS.

Installing the CA certificate from the **pub** directory via HTTP and importing it to the browser will then 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 the browser, enter the address provided after completing setup. With this address you open the SUSE Manager Web UI.
2. In 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.

Create Organization

Organization Details

Organization Name*:

Tip: Between 3 and 128 characters

Create SUSE Manager Administrator

Create the first SUSE Manager Administrator account. This account will have access to all resources on this SUSE Manager. This account will also be able to create new users and delegate permissions to them.

Desired Login*:

Tip: Between 5 and 64 characters

Desired Password*:

Confirm Password*:

Password Strength:

Email*:

First Name*:

Last Name*:

* - Required Field

Create Organization

You are now presented with the SUSE Manager **Home › Overview** page.

6.1.2.5.2. 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 may receive updates, and 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.

Before you can synchronize software repositories with SCC, you will need to enter organization credentials in SUSE Manager. In previous versions, so-called mirror credentials were used instead. 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 SUSE Manager Web UI:


Procedure: Entering Organization Credentials

1. In the SUSE Manager Web UI, select **Admin › Setup Wizard**.
2. From the **Setup Wizard** page select the **[Organization Credentials]** tab.
3. Click **[Add a new credential]**.
4. In the dialog, enter **Username** and **Password**, and confirm with **[Save]**.

When the credentials are confirmed with a check-mark icon, proceed with **Procedure: Synchronizing with SUSE Customer Center**.

Procedure: Synchronizing with SUSE Customer Center

1. In the Web UI, navigate to **Admin › Setup Wizard**.
2. From the **Setup Wizard** page select the **[SUSE Products]** tab. If you previously registered with SUSE Customer Center a list of products will populate the table. This operation could take up to a few minutes. You can monitor the progress of the operation in section on the right **Refresh the product catalog from SUSE Customer Center**. The table of products lists architecture, channels, and status information. For more information, see **Reference › Admin**.



























Setup Wizard 

HTTP Proxy Organization Credentials **SUSE Products**

Clear + Add products

Filter by product Description Filter by architecture 25 items per page


Items 1 - 25 of 94

Product Description	Arch	Channels
<input type="checkbox"/> Open Enterprise Server 2018	x86_64	
<input type="checkbox"/> RHEL Expanded Support 5	i386	
<input type="checkbox"/> RHEL Expanded Support 5	x86_64	
<input type="checkbox"/> > RHEL Expanded Support 6	i386	
<input type="checkbox"/> > RHEL Expanded Support 6	x86_64	
<input type="checkbox"/> > RHEL Expanded Support 7	x86_64	
<input type="checkbox"/> SUSE Container as a Service Platform 1.0	x86_64	
<input type="checkbox"/> SUSE Container as a Service Platform 2.0	x86_64	
<input type="checkbox"/> > SUSE Linux Enterprise Desktop 11 SP2	i586	
<input type="checkbox"/> > SUSE Linux Enterprise Desktop 11 SP2	x86_64	
<input type="checkbox"/> > SUSE Linux Enterprise Desktop 11 SP3	i586	
<input type="checkbox"/> > SUSE Linux Enterprise Desktop 11 SP3	x86_64	
<input type="checkbox"/> > SUSE Linux Enterprise Desktop 11 SP4	i586	
<input type="checkbox"/> > SUSE Linux Enterprise Desktop 11 SP4	x86_64	
<input type="checkbox"/> > SUSE Linux Enterprise Desktop 12	x86_64	
<input type="checkbox"/> > SUSE Linux Enterprise Desktop 12 SP1	x86_64	
<input type="checkbox"/> > SUSE Linux Enterprise Desktop 12 SP2	x86_64	
<input type="checkbox"/> > SUSE Linux Enterprise Desktop 12 SP3	x86_64	
<input checked="" type="checkbox"/> > SUSE Linux Enterprise Desktop 15	x86_64	 100% 
<input type="checkbox"/> > SUSE Linux Enterprise High Performance Computing 15	aarch64	 include recommended
<input type="checkbox"/> > SUSE Linux Enterprise High Performance Computing 15	x86_64	 include recommended
<input type="checkbox"/> > SUSE Linux Enterprise Server 10 SP3	i586	
<input type="checkbox"/> > SUSE Linux Enterprise Server 10 SP3	ia64	
<input type="checkbox"/> > SUSE Linux Enterprise Server 10 SP3	ppc	
<input type="checkbox"/> > SUSE Linux Enterprise Server 10 SP3	s390x	

Page 1 of 4 First Prev Next Last

Refresh the product catalog from SUSE Customer Center

☐ Channels
☐ Channel Families
☐ Products
☐ Product Channels
☐ Subscriptions

 Refresh

Why aren't all SUSE products displayed in the list?

The products displayed on this list are directly linked to your Organization credentials (Mirror credentials) as well as your SUSE subscriptions.

If you believe there are products missing, make sure you have added the correct Organization credentials in the previous wizard step.

← Prev 3 of 3

- Use **Filter by product description** and **Filter by architecture** to filter the list of displayed products. 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 SUSE Manager 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, SUSE Manager will schedule the channel to be synchronized. This can take a long time as SUSE Manager will copy channel software sources from the SUSE repositories located at SUSE Customer Center to local `/var/pacewalk/` directory of your server.



In some environments, Transparent Huge Pages provided by the kernel may slow down PostgreSQL workloads significantly.

To disable Transparent Huge Pages set the `transparent_hugepage` kernel parameter to `never`. This has to be changed in `/etc/default/grub` and added to 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](#).

6.1.2.5.3. Set up SUSE Manager with external database

In this example, we use RDS product from Amazon Web Service.



Currently, configuring an external database is not supported by `yast2` setup.

You can configure an external database using the `mgr-setup` command line tool.

This section guides you through SUSE Manager setup using `mgr-setup`.

Procedure : Configuring server with external database

1. Create `setup_env.sh` file in the `/root` directory.
2. Set the variables defining your certificate information and password. For more information about certificates, see [\[proc-quickstart-certificate-information-yast\]](#).

```
CERT_O="SUSE"
CERT_OU="SUSE"
CERT_CITY="N"
CERT_STATE="B"
CERT_COUNTRY="DE"
CERT_EMAIL="email@prov.com"
CERT_PASS="spacewalk"
USE_EXISTING_CERTS="N"
```

3. Define your database. The user and password are created during the setup. If you are using an external database, specify the hostname and port.

```
MANAGER_USER="spacewalk"
MANAGER_PASS="spacewalk"
MANAGER_ADMIN_EMAIL="email@prov.com"
MANAGER_DB_NAME="susemanager"
MANAGER_DB_HOST="db hostname"
MANAGER_DB_PORT="db port"
MANAGER_DB_PROTOCOL="TCP"
MANAGER_ENABLE_TFTP="Y"
```

4. Set up the variables defining the specific configuration for the external database. In this scenario, an RDS database has been deployed and is accessible by the server. To establish a connection, an AWS certificate is also required. `EXTERNALDB_ADMIN_USER` and `EXTERNALDB_ADMIN_PASS` are the credentials set during the RDS deployment:

```
EXTERNALDB_ADMIN_USER="postgres"
EXTERNALDB_ADMIN_PASS="spacewalk"
MANAGER_DB_CA_CERT="/path_to/aws.crt"
REPORT_DB_CA_CERT="/path_to/aws.crt"
EXTERNALDB_PROVIDER="aws"
```



The AWS certificate can be found at <https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html>.

5. To connect to the external database, configure the report database with the RDS hostname and port. `REPORT_DB_USER` and `REPORT_DB_PASS` will be created by the script:

```
REPORT_DB_HOST="db hostname"
REPORT_DB_PORT="db port"
REPORT_DB_NAME="reportdb"
REPORT_DB_USER="pythia_susemanager"
REPORT_DB_PASS="pythia_susemanager"
```



Do not use `MANAGER_USER` as the user when deploying RDS.

6.1.3. Manage

6.1.3.1. Custom YAML configuration and deployment with mgradm

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



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

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

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

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


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

# Password for the CA certificate
ssl:
  password: MySuperSecretSSLPassword

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

# Organization name
organization: YourOrganization

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

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

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

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



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

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

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

In this section you learned how to deploy an SUSE Manager '5.0' Server container using a custom YAML configuration.

6.1.3.2. Starting and Stopping Containers

The SUSE Manager '5.0' Server container can be restarted, started, and stopped using the following commands:

To **restart** the SUSE Manager '5.0' Server execute the following command:

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

To **start** the server execute the following command:

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

To **stop** the server execute the following command:

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

6.1.3.3. Update containers

The SUSE Manager '5.0' Server container can be updated using the following command:

```
mgradm update
```

This command will bring the status of the container up-to-date and restart the server.

6.1.3.4. List of persistent storage volumes

Modifications performed within containers are not retained. Any alterations made outside of persistent volumes will be discarded. Below is a list of persistent volumes for SUSE Manager '5.0'.

To customize the default volume locations, ensure you create the necessary volumes before

launching the pod for the first time, utilizing the `podman volume create` command.



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

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

Table 10. Persistent Volumes: Podman Default Storage

Volume Name	Volume Directory
Podman Storage	<code>/var/lib/containers/storage/volumes/</code>

Table 11. Persistent Volumes: root

Volume Name	Volume Directory
root	<code>/root</code>

Table 12. Persistent Volumes: var/

Volume Name	Volume Directory
var-cobbler	<code>/var/lib/cobbler</code>
var-salt	<code>/var/lib/salt</code>
var-pgsql	<code>/var/lib/pgsql</code>
var-cache	<code>/var/cache</code>
var-spacewalk	<code>/var/spacewalk</code>
var-log	<code>/var/log</code>

Table 13. Persistent Volumes: srv/

Volume Name	Volume Directory
srv-salt	<code>/srv/salt</code>
srv-www	<code>/srv/www/</code>
srv-tftpboot	<code>/srv/tftpboot</code>

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

Table 14. Persistent Volumes: etc/

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

6.1.4. Public Cloud

6.1.4.1. SUSE Manager Server and the Public Cloud

Public clouds provide SUSE Manager under a Bring-your-own-subscription (BYOS) or Pay-as-you-go (PAYG) models.

For more information on using SUSE Manager in the public cloud, see, [Specialized-guides › Public-cloud-guide](#).

6.2. Proxy

6.2.1. Deploy

6.2.1.1. SUSE Manager '5.0' Proxy Deployment

This quick start guide shows you how to prepare, configure and deploy a SUSE Manager '5.0' Proxy container on SLE Micro 5.5.

6.2.1.1.1. Hardware Requirements for the Proxy

This table shows the hardware requirements for deploying SUSE Manager Proxy.

Table 15. Proxy Hardware Requirements

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



Supported operating system for the Proxy Container Host

The supported operating system for the Proxy container host is SLE Micro 5.5.

6.2.1.1.2. SLE Micro 5.5 Installation

Procedure: Download the Installation Media

1. Locate the SLE Micro 5.5 installation media at <https://www.suse.com/download/sle-micro/>.
2. You will need an account with SUSE Customer Center and must be logged in to download the ISO.
3. Download the following file: `SLE-Micro-5.5-DVD-x86_64-GM-Media1.iso`
4. Prepare the installation media for use. For this guide a USB flash disk was used.
5. For detailed documentation covering installation on bare metal or in a virtual machine, see [SLE Micro 5.5 Deployment Guide](#).

Procedure: SLE Micro 5.5 Installation

1. Use the arrow keys to select **Installation**.
2. Adjust Keyboard and language. Click the **checkbox** to accept the License Agreement.
3. Click **Next** to continue.
4. Skip Registration.
5. On the **NTP Configuration** page click [**Next**].
6. On the **Authentication for the System** page enter a password for the root user. Click [**Next**].
7. On the **Installation Settings** page click [**Install**].

This concludes installation of SLE Micro 5.5.

Once the container host is prepared, the Proxy requires the following steps to complete configuration.

6.2.1.1.3. Register the Proxy Host as a Minion with the Server

Before proceeding with configuration of the proxy you need to sync the correct channels, create a Salt activation key and register the proxy host as a Salt minion with SUSE Manager '5.0' Server.



The container host for the SUSE Manager Proxy must be registered as a salt minion to the SUSE Manager Server.

For more information about registering a client to the SUSE Manager Server, see [Client-configuration › Registration-overview](#).



The following procedure assumes you have added your Organization Credentials to the [Admin › Setup Wizard → Organization Credentials](#) page on the SUSE Manager '5.0' Server.

Procedure: Prepare the Proxy and Required Channels

1. Log in to the SUSE Manager Web UI.
2. Select [Admin › Setup Wizard → Products](#).
3. Use the checkbox to select SLE Micro 5.5 then select the dropdown and check the Proxy Extension.
4. Select the [\[+ Add Products \]](#) button.
5. Wait for the sync to complete.
6. Select [Systems › Activation Keys](#) then click [\[+ Create key \]](#).
7. Create an activation key for the proxy host with SLE Micro 5.5 as the parent channel. This key should include all recommended channels and the proxy extension.
8. Proceed to bootstrapping the proxy host as a minion.

Procedure: Bootstrap the Proxy Host

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

Procedure: Update the Proxy Host

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

6.2.1.1.4. Proxy Container Configuration and Deployment

Create and generate the SUSE Manager Proxy Configuration Files

The configuration archive of the SUSE Manager Proxy is generated by the SUSE Manager Server. Each additional Proxy requires its own configuration archive. There are two paths for generating SUSE Manager Proxy configuration archives: use the Web UI or the `spacecmd` command.

The following tasks will be performed:

1. Generate SUSE Manager a Proxy configuration archive file
2. Transfer the configuration archive to the container host from the Server and extract it
3. Start the Proxy with `mgrpxy`

Procedure: Generating a Proxy Container 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 SUSE Manager Server or another SUSE Manager Proxy.
4. In the **Proxy SSH port** field type SSH port on which SSH service is listening on SUSE Manager 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 SUSE Manager Proxy or an existing one should be used. You can consider generated certificates as SUSE Manager 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 SUSE Manager 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:

6.2.1.1.5. Transfer the Proxy Configuration

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

Procedure: Copy the Proxy configuration generated with the `spacecmd` command

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

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

2. Next copy the files from the server host OS to the proxy host:

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

3. Install the Proxy with:

```
mgrpky install podman config.tar.gz
```

For installation instructions to use the archive to get the proxy containers, see [Installation-and-upgrade › Container-deployment](#).

6.2.1.1.6. Start SUSE Manager Proxy containers

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

Listing 1. Procedure: Start SUSE Manager Proxy containers

```
mgrpky start uyuni-proxy-pod
```

Check if all containers started up as expected by calling

```
podman ps
```

Five SUSE Manager 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.

6.2.1.2. Install containerized SUSE Manager Proxy



Only SUSE Linux Enterprise Server 15 SP5 or SLE Micro 5.5 and newer are supported to be used as container host for SUSE Manager Proxy containers.



To ensure that domain name of the SUSE Manager Server can be resolved by the clients: * Both container proxy and client machines must be connected to a DNS server * Reverse lookup must work

Procedure: Installation of container utility tool `mgrpxy` for SUSE Manager Proxy

1. Assign `Containers Module` software channel to the container host in the SUSE Manager. 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 `mgrpxy` package:

```
zypper install mgrpxy
```

6.2.1.2.1. Install SUSE Manager Proxy containers

SUSE Manager 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.

To install the systemd service starting the SUSE Manager proxy, run the `mgrpxy install podman /path/to/config.tar.gz` command.

It is possible to add custom arguments passed to podman container pod with the one or more `--podman-arg` parameters to the install command.

It is possible to modify the tag to use for container images with the `--tag=latest` parameter to the install command.



Changing the containers images and version parameters is dangerous and can cause a non-functional system.

6.2.1.3. 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.

6.2.1.3.1. Image Copying from SUSE Registry to Internal Registry

Machines must have access to **registry.suse.com**.

Procedure: Deploying Proxy from an Internal Image Registry

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

```
zypper in skopeo
```



This can be SUSE Manager 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.

6.2.1.3.2. 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
```

6.2.1.4. Install Containerized SUSE Manager Proxy on k3s

6.2.1.4.1. Installing k3s

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

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

6.2.1.4.2. Installing tools

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

The `mgrpxy` package is available in the SUSE Manager Proxy product repositories.



The Containers Module is required to install `helm`.

To install them run:

```
zypper in helm mgrpxy
```

6.2.1.4.3. Deploying the SUSE Manager proxy helm chart

To configure the storage of the volumes to be used by the SUSE Manager 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 SUSE Manager Proxy as documented in [Installation-and-upgrade › Container-deployment](#). Copy the configuration `tar.gz` file and then install:

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

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

Chapter 7. Upgrade

Updated: 2024-04-29

SUSE Manager has three main components, all of which need regular updates. This guide covers updating the SUSE Manager 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.

SUSE Manager uses an **X.Y.Z** versioning schema. To determine which upgrade procedure you need, look at which part of the version number is changing.



The version numbers below are just examples. Do not understand them as most recent available options. SUSE uses these numbers for illustrative purposes only.

Major Version Upgrade (X Upgrade)

Major upgrade is usually an upgrade from X.Y to X+1.0 or to X+1.1, where Y is the latest minor version of the X series. For example:

- From version 3.2 to 4.0 or to 4.1 (upgrading directly from 3.2 to 4.2 or later is not supported).

Minor Version Upgrade (Y Upgrade)

Minor upgrade refers to upgrading to the next minor version, from X.Y to X.Y+1. This is often referred to as a product migration, service pack migration, or SP migration. For example:

- From 4.2 to 4.3.



You always upgrade from and to the latest patch level of the minor version.

For example, from 4.2.12 to 4.3.8, or newer.

Patch Level Upgrade (Z Upgrade)

Upgrading within the same minor version. This is often referred to as a maintenance update or MU. For example:

- From 4.3.7 to 4.3.8.

If you are upgrading the SUSE Manager Server, see [Installation-and-upgrade › Server-intro](#).

If you are upgrading the SUSE Manager Proxy, see [Installation-and-upgrade › Proxy-intro](#).

If you are upgrading clients, see [Client-configuration › Client-upgrades](#).

In addition to upgrading the server, you need to upgrade other underlying technologies, including the database. For more information about upgrading the database, see [Installation-and-upgrade › Db-intro](#).

7.1. Upgrade the Server

SUSE Manager uses an **X.Y.Z** versioning schema. To determine which upgrade procedure you need, look at which part of the version number is changing.



The version numbers below are just examples. Do not understand them as most recent available options. SUSE uses these numbers for illustrative purposes only.

Major Version Upgrade (X Upgrade)

Major upgrade is usually an upgrade from X.Y to X+1.0 or to X+1.1, where Y is the latest minor version of the X series. For example:

- From version 3.2 to 4.0 or to 4.1 (upgrading directly from 3.2 to 4.2 or later is not supported).
- See [Installation-and-upgrade › Server-x](#).

Minor Version Upgrade (Y Upgrade)

Minor upgrade refers to upgrading to the next minor version, from X.Y to X.Y+1. This is often referred to as a product migration, service pack migration, or SP migration. For example:

- From 4.2 to 4.3.



You always upgrade from and to the latest patch level of the minor version.

For example, from 4.2.12 to 4.3.8, or later.

- See [Installation-and-upgrade › Server-y](#).

Patch Level Upgrade (Z Upgrade)

Upgrading within the same minor version. This is often referred to as a maintenance update or MU. For example:

- From 4.3.7 to 4.3.8.
- See [Installation-and-upgrade › Server-z](#).

7.1.1. Migrating the SUSE Manager server to a containerized environment

To migrate a SUSE Manager '5.0' Server to a container, a new machine is required.



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

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

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

7.1.1.1. Initial Preparation on the Source Server

Procedure: Initial preparation on the source server

1. Stop the SUSE Manager services:

```
spacewalk-service stop
```

2. Stop the PostgreSQL service:

```
systemctl stop postgresql
```

7.1.1.2. Prepare the SSH Connection

Procedure: Preparing the SSH connection

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



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

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

7.1.1.3. Perform the Migration

Procedure: Performing the Migration

1. Execute the following command to install a new SUSE Manager server, replacing `<source.fqdn>` with the appropriate FQDN of the source server:

```
mgradm migrate podman <source.fqdn>
```

7.2. 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 SUSE Manager Web UI.

For more information about upgrading clients, see [Client-configuration](#) › [Client-upgrades](#).

Chapter 8. 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".