SUSE Manager 5.0

Installation and Upgrade Guide

Preface

Installation, Deployment and Upgrade
SUSE Manager 5.0

This guide provides comprehensive, step-by-step instructions for deploying, upgrading, and managing SUSE Manager Server and Proxy.

It is organized into the following sections:

- **Requirements:** Outlines the essential hardware, software, and networking prerequisites to ensure a smooth setup.
- **Deployment and Installation:** Guides you through deploying SUSE Manager as a container and completing the initial configuration.
- **Upgrade and Migration:** Details the process for upgrading and migrating SUSE Manager while minimizing downtime.
- **Basic Server Management:** Covers fundamental server operations, helping you get started with SUSE Manager efficiently.

Publication Date: 2025-12-12

Copyright © 2011–2025 SUSE LLC and contributors. All rights reserved. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or (at your option) version 1.3; with the Invariant Section being this copyright notice and license. A copy of the license version 1.2 is included in the section entitled **Legal › License**.

For SUSE trademarks, see https://www.suse.com/company/legal/ . All third-party trademarks are the property of their respective owners. Trademark symbols (®, ™ etc.) denote trademarks of SUSE and its affiliates. Asterisks (*) denote third-party trademarks. All information found in this book has been compiled with utmost attention to detail. However, this does not guarantee complete accuracy. Neither SUSE LLC, its affiliates, the authors nor the translators shall be held liable for possible errors or the consequences thereof.

Contents

Preface 1

1. Requirements 4

1.1. General Requirements 4

SUSE Customer Center Account and Credentials 4

Supported Browsers for SUSE Manager Web UI 4

SSL Certificates 5

1.2. Hardware Requirements 5

Server Requirements 5

Proxy Requirements 7

Database Requirement 8

Persistent Storage and Permissions 8

Logical Volume Management (LVM) 9

1.3. Network Requirements 9

Fully Qualified Domain Name (FQDN) 9

Hostname and IP Address 10

Reenable router advertisements 10

Deployment behind HTTP or HTTPS OSI level 7 proxy 10

Air-gapped Deployment 11

Required Network Ports 11

1.4. Public Cloud Requirements 18

Network Requirements 19

Prepare Storage Volumes 19

2. Installation and Deployment 21

2.1. Server 21

SUSE Manager 5.0 Server Deployment 21

SUSE Manager 5.0 Server Deployment as a Virtual Machine - KVM 27

SUSE Manager 5.0 Server Deployment as a Virtual Machine - VMware 33

SUSE Manager Server Air-gapped Deployment 36

Public Cloud Deployment 38

Connect PAYG instance 38

2.2. Install SUSE Manager Proxy 42

SUSE Manager 5.0 Proxy Deployment 42

SUSE Manager Proxy Deployment as a Virtual Machine - KVM 46

SUSE Manager Proxy Deployment as a Virtual Machine - VMware 52

SUSE Manager 5.0 Proxy Deployment on K3s 54

SUSE Manager Proxy Air-gapped Deployment 55

3. Upgrade and Migration 57

3.1. Server 57

SUSE Manager Server Migration to a Containerized Environment 57

Server Upgrade 60

3.2. Proxy 62

Proxy Migration 62

Proxy Upgrade 63

3.3. Clients 64

Upgrade the Clients 65

4. Basic Server and Proxy Management 66
4.1. Custom YAML Configuration and Deployment with mgradm 66
4.2. Starting and Stopping Containers 67
4.3. Containers used by SUSE Manager 67
4.4. List of persistent storage volumes 68
Server 68
Proxy 70
4.5. Understanding mgr-storage-server and mgr-storage-proxy 70
What these tools do 71
What these tools do **not** do 71
Post-installation storage management 72
When to use, or not use 72
Summary 72
5. GNU Free Documentation License 74

Chapter 1. Requirements

1.1. 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 SUSE Manager Server, Proxy and Retail Branch Server.
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.

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 the organization name.
5. Click the **[Users]** tab, and then select the **[Organization Credentials]** sub-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 from the left navigation bar.

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

Supported Browsers for SUSE Manager Web UI

To use the Web UI to manage your SUSE Manager environment, you must run 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.

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**.

1.2. Hardware Requirements

This table outlines hardware and software requirements for the SUSE Manager Server and Proxy, on x86-64, ARM, ppc64le and s390x architecture.

SUSE Manager installations based on ppc64le or s390x architecture cannot use secure boot for network booting clients. This limitation exists because the shim bootloader is not available for both these architectures.

For SUSE Manager for Retail hardware requirements, see **Retail › Retail-requirements**.

Server Requirements

One of SLE Micro 5.5 or SUSE Linux Enterprise Server 15 SP6 is the operating system of the container host. In the following, SUSE Linux Enterprise Server as the installed host operating system is explicitly mentioned only if it matters. Otherwise we either write SLE Micro or just host operating system.

The container host with SLE Micro as operating system requires as free disk space:

- Minimum for base installation 100 GB
- Plus a minimum of 130 GB for repository data

Depending on the amount of selected software, SUSE Linux Enterprise Server as operating system can require considerably more disk space.

By default the SUSE Manager Server container stores mirrored repository (packages or products), database, and other data in subdirectories of the /var/lib/containers/storage/volumes/ directory. Repository synchronization

fails if this directory runs out of disk space. Estimate how much space the /var/lib/containers/storage/volumes/ directory requires based on the number and kind of clients and repositories you plan to mirror.

For more information about filesystem and partitioning details, see installation-and-upgrade:hardware-requirements.pdf and the detailed installation instructions in the Installation and Deployment sections of this guide.

Table 1. Server Hardware Requirements

Hardware	Details	Recommendation
CPU	x86-64, ARM, ppc64le, or s390x	Minimum 4 dedicated 64-bit CPU cores
RAM	Minimum	16 GB
	Recommended	32 GB
Disk Space	/ (root directory)	40 GB
	/var/lib/containers/storage/volumes	Minimum 150 GB (depending on the number of products)
	/var/lib/containers/storage/volumes/var-pgsql	Minimum 50 GB

The images by default have a 40 GB / partition. The cloud image of SLE Micro 5.5 has just a 5 GB / partition. Both work flawlessly with SUSE Manager. As long as external storage is mounted to /var/lib/containers/storage/volumes, SUSE Manager does not need or use storage on the / partition, but leaves that to the management of the container host itself.

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**.

Proxy Requirements

One of SLE Micro 5.5 or SUSE Linux Enterprise Server 15 SP6 is the operating system of the container host.

Minimum requirements are suitable for a quick test installation, such as a Proxy with one client. If you want to use a production environment start with recommended values.

Table 2. Proxy Hardware Requirements

Hardware	Details	Recommendation
CPU	x86-64, ARM	Minimum 2 dedicated 64-bit CPU cores
	Recommended	The same as minimum values
RAM	Minimum	2 GB
	Recommended	8 GB
Disk Space	/ (root directory)	Minimum 40 GB
	/var/lib/containers/storage/volumes	Minimum 100 GB

By default the SUSE Manager Proxy container caches packages in the /var/lib/containers/storage/volumes/uyuni-proxy-squid-cache/ directory. If there is not enough space available, 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/uyuni-proxy-squid-cache/ directory is on the proxy, the less traffic will be between the proxy and the SUSE Manager Server.
- By making the /var/lib/containers/storage/volumes/uyuni-proxy-squid-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/uyuni-proxy-squid-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.

In general, SUSE recommends to adjust the value for the cache directory to about 80 % of available free space. The cache_dir value is set when generating proxy configuration on the server. You cannot set the option directly in squid.conf.

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.

Persistent Storage and Permissions

Persistent volumes are created by default when deploying the container.

However, it is recommended that the volumes are stored on one or more separate storage devices. Such a setup helps avoid data loss in production environments. This can be done after container deployment.

Storage devices best should be set up after first deploying the container. For more details, see **Installation-and-upgrade › Container-management**.

We recommend you use XFS as the filesystem type for all volumes. 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.

Do not use NFS for Cobbler or PostgreSQL storage, neither NFS on SELinux environments. These scenarios are not supported.

On the 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 mgr-storage-server command with the device names to set up the external disks as the locations for the storage and, optionally on a disk of its own, for the database:

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

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 mgr-storage-server with a single device name parameter.

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

Logical Volume Management (LVM)

For all kind of virtual machines (VM), LVM is generally not needed and not recommended. The disk setup is virtual and separate disks for volumes are possible and recommended.

For other deployments, separate disks for volumes are also recommended.

On the container host of the SUSE Manager Server, the mgr-storage-server command moves the complete content of the /var/lib/containers/storage/volumes directory to a separate disk and remounts it to /var/lib/containers/storage/volumes. Optionally, if a second device name is specified, mgr-storage-server moves the content of the /var/lib/containers/storage/volumes/var-pgsql database directory to a second separate disk and remounts it to /var/lib/containers/storage/volumes/var-pgsql.

Similarly, on the container host of the SUSE Manager Proxy, the mgr-storage-proxy command moves the complete content of the /var/lib/containers/storage/volumes directory to a separate disk and remounts it to /var/lib/containers/storage/volumes.

1.3. Network Requirements

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

IP forwarding will be enabled by containerized installation. This means SUSE Manager Server and Proxies will behave as a router. This behavior is done by podman directly. Podman containers do not run if IP forwarding is disabled.

Consider achieving network isolation of the SUSE Manager environment according to your policies.

For more information, see https://www.suse.com/support/kb/doc/?id=000020166.

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.

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.

Reenable router advertisements

When the SUSE Manager is installed using mgradm install podman or mgrpxy install podman, it sets up Podman which enables IPv4 and IPv6 forwarding. This is needed for communication from the outside of the container.

However, if your system previously had /proc/sys/net/ipv6/conf/eth0/accept_ra set to 1, it will stop using router advertisements. As a result, the routes are no longer obtained via router advertisements and the default IPv6 route is missing.

To recover correct functioning of the IPv6 routing, follow the procedure:

Procedure: Reenabling router advertisements

1. Create a file in /etc/sysctl.d, for example 99-ipv6-ras.conf.
2. Add the following parameter and value to the file:

```
net.ipv6.conf.eth0.accept_ra = 2
```

3. Reboot.

Deployment behind HTTP or HTTPS OSI level 7 proxy

Some environments enforce internet access through a HTTP or HTTPS proxy. This could be a Squid server or similar. To allow the SUSE Manager Server internet access in such configuration, you need to configure the following.

Procedure: Configuring HTTP or HTTPS OSI level 7 proxy

1. For operating system internet access, modify /etc/sysconfig/proxy according to your needs:

```
PROXY_ENABLED="no"
HTTP_PROXY=""
HTTPS_PROXY=""
NO_PROXY="localhost, 127.0.0.1"
```

2. For Podman container internet access, modify /etc/systemd/system/uyuni-server.service.d/custom.conf according to your needs. For example, set:

```
[Service]
Environment=TZ=Europe/Berlin
Environment="PODMAN_EXTRA_ARGS="
Environment="https_proxy=user:password@http://192.168.10.1:3128"
```

3. For Java application internet access, modify /etc/rhn/rhn.conf according to your needs. On the container host, execute mgrctl term to open a command line inside the server container:

    a. Modify /etc/rhn/rhn.conf according to your needs. For example, set:

```
# Use proxy FQDN, or FQDN:port
server.satellite.http_proxy =
server.satellite.http_proxy_username =
server.satellite.http_proxy_password =
# no_proxy is a comma seperated list
server.satellite.no_proxy =
```

4. On the container host, restart the server to enforce the new configuration:

```
systemctl restart uyuni-server.service
```

Air-gapped Deployment

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

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:network-requirements.pdf.

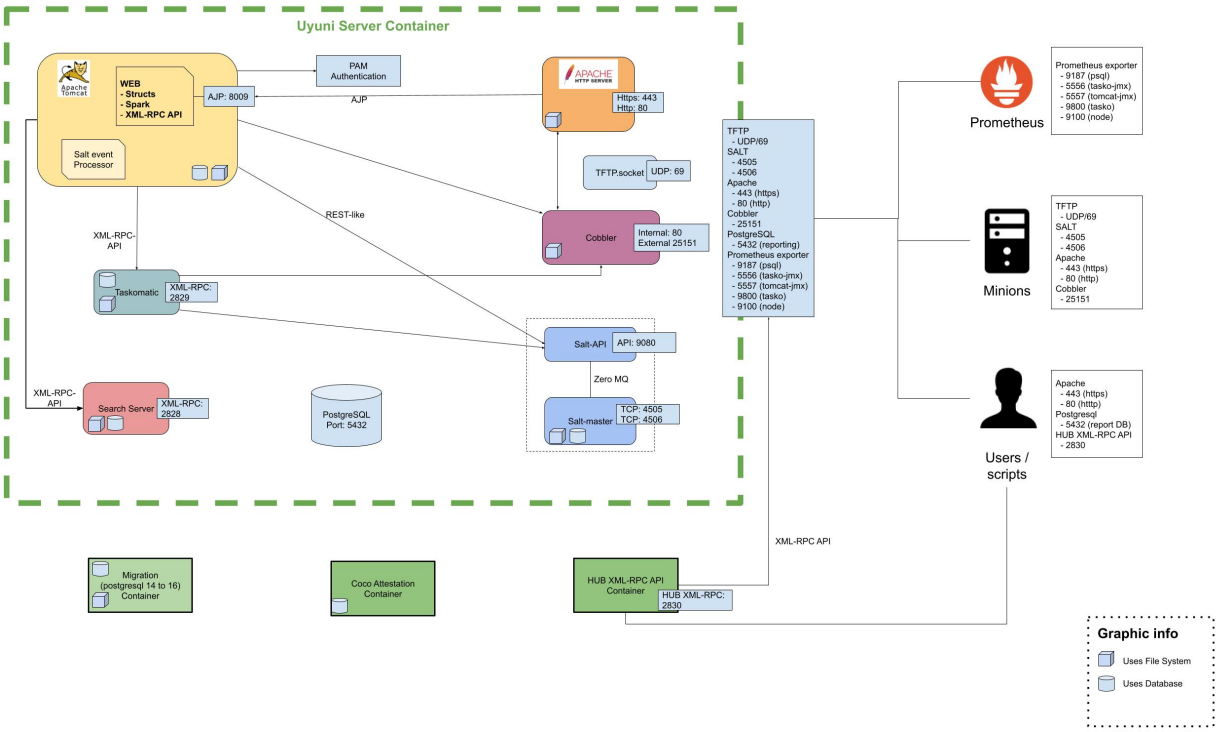
Required Network Ports

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

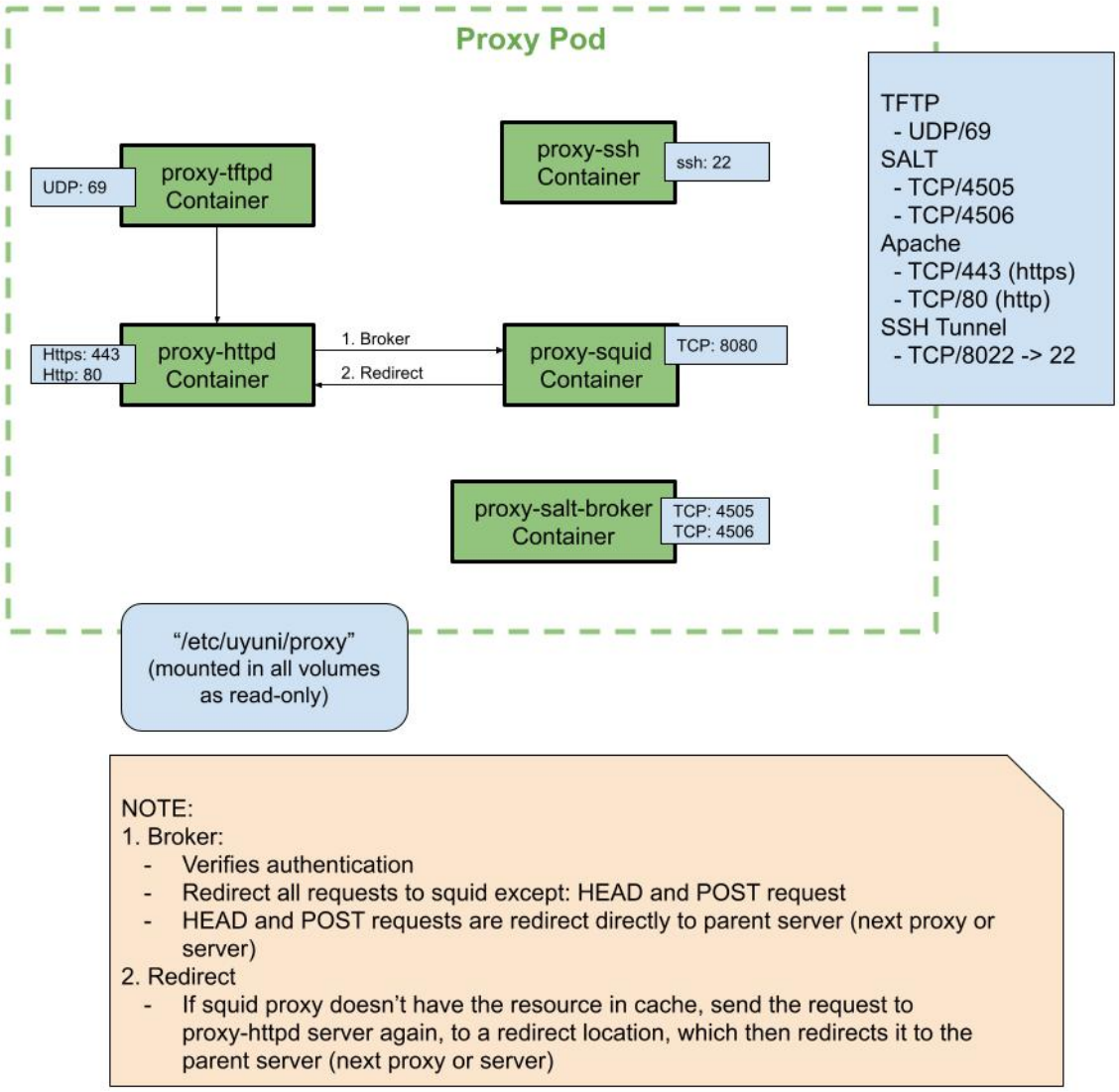
You will not need to open all of these ports. Some ports only need to be opened if you are using the service that requires them.

Overview

Server



Proxy



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
67	TCP/UDP	DHCP	Required only if clients are requesting IP addresses from the server.

Port number	Protocol	Used By	Notes
69	TCP/UDP	TFTP	Required if server is used as a PXE server for automated client installation.
80	TCP	HTTP	Required temporarily for some bootstrap repositories and automated installations.
443	TCP	HTTPS	Serves the Web UI, client, and server and proxy (tftpsync) requests.
4505	TCP	salt	Required to accept communication requests from clients. The client initiates the connection, and it stays open to receive commands from the Salt master.
4506	TCP	salt	Required to accept communication requests from clients. The client initiates the connection, and it stays open to report results back to the Salt master.
5556	TCP	Prometheus	Required for scraping Taskomatic JMX metrics.
5557	TCP	Prometheus	Required for scraping Tomcat JMX metrics.
9100	TCP	Prometheus	Required for scraping Node exporter metrics.
9187	TCP	Prometheus	Required for scraping PostgreSQL metrics.
9800	TCP	Prometheus	Required for scraping Taskomatic metrics.
25151	TCP	Cobbler	

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.

Port number	Protocol	Used By	Notes
25151	TCP	Cobbler	

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.
25151	Cobbler's XMLRPC API
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
```

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			Only required if the user wants to manage the proxy host with Salt SSH.
67	TCP/UDP	DHCP	Required only if clients are requesting IP addresses from the server.
69	TCP/UDP	TFTP	Required if the server is used as a PXE server for automated client installation.
443	TCP	HTTPS	Web UI, client, and server and proxy (tftpsync) requests.
4505	TCP	salt	Required to accept communication requests from clients. The client initiates the connection, and it stays open to receive commands from the Salt master.
4506	TCP	salt	Required to accept communication requests from clients. The client initiates the connection, and it stays open to report results back to the Salt master.
8022			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.

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.
4505	TCP	Salt	Required to connect to Salt master either directly or via proxy.

Port number	Protocol	Used By	Notes
4506	TCP	Salt	Required to connect to Salt master either directly or via proxy.

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.
443	Outbound		Used to reach the server or proxy.
4505	Outbound	TCP	Required to connect to Salt master either directly or via proxy.
4506	Outbound	TCP	Required to connect to Salt master either directly or via 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.

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
- installer-updates.suse.com

- registry.suse.com
- registry-storage.suse.com
- opensuse.org

Additionally, you may need access to these URLs for non-SUSE products:

- download.nvidia.com
- public.dhe.ibm.com
- nu.novell.com

You can find additional details on whitelisting the specified URLs and their associated IP addresses in this article: Accessing SUSE Customer Center and SUSE registry behind a firewall and/or through a proxy.

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

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

1.4. 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.

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.

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 mgr-storage-server command. This creates an XFS partition mounted at /manager_storage and uses it as the location for the database and repositories:

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

For more information about setting up storage volumes and partitions, including recommended minimum sizes, see **Installation-and-upgrade › Hardware-requirements**.

Chapter 2. Installation and Deployment

2.1. Server

SUSE Manager 5.0 Server Deployment

This guide shows you how to install and configure a SUSE Manager 5.0 container on SLE Micro 5.5 or SUSE Linux Enterprise Server 15 SP6.

Hardware Requirements for SUSE Manager

This table shows the software and hardware requirements for deploying SUSE Manager Server on your bare metal machine. For the purposes of this guide your machine should have 16 GB of RAM, and at least 200 GB of disk space. For background information about disk space, see **Installation-and-upgrade › Hardware-requirements**.

Table 9. Software and Hardware Requirements

Software and Hardware	Recommended
Operating System	SLE Micro 5.5 or SUSE Linux Enterprise Server 15 SP6
Architecture	x86-64, ARM, s390x, ppc64le
Processor (CPU)	Minimum of four (4) 64-bit CPU cores
RAM	16 GB
Disk Space	200 GB
Channel Requirements	50 GB per SUSE or openSUSE product 360 GB per Red Hat product
Swap space:	3 GB

Supported operating system for the Server Container Host

The supported operating system for the container host is SLE Micro 5.5 or SUSE Linux Enterprise Server 15 SP6.

Container host

A container host is a server equipped with a container engine like Podman, which lets

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

Server deployment mandates the use of a fully qualified domain name (FQDN). In the absence of automatic DNS provision of an FQDN by your router or network, the deployment process will not proceed successfully. An FQDN typically follows the format <host>.<domain>.com.

For instance:

- suma.example.com
- suma.container.lab

For more information, see the section on network requirements in **Installation-and-upgrade › Network-requirements**.

Persistent Volumes

SUSE Manager 5.0 defines the required persistent storage volumes by default. These are created during installation by the mgradm tool if they do not already exist.

These volumes are created in /var/lib/containers/storage/volumes/, where Podman stores its volumes by default.

Recommendations

You can leverage the simplicity of storage by mounting an external storage device to this directory. Because it will store the PostgreSQL database, binary packages for repositories, caches, operating system images, autoinstallation distributions, and configuration files, we have three recommendations:

Fast Storage

This mount point should ideally be NVMe or SSD-class devices. Slower storage will adversely affect SUSE Manager performance.

Large Capacity

Recommended minimum size for this is at least 300 GB, and larger if there will be multiple Linux distributions or architectures to manage.

Recommended Filesystem

XFS (though any supported filesystem for SLE Micro 5.5 could work).

Optional

You can provide custom storage for the volumes by mounting disks on the expected volume path inside it such as /var/lib/containers/storage/volumes/var-spacewalk. This adds to the complexity of a SUSE Manager deployment, and may affect the resilience the default storage recommendation provides.

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

Prepare SUSE Manager Server Host

You can deploy SUSE Manager on SLE Micro 5.5 or SUSE Linux Enterprise Server 15 SP6. SLE Micro is a transactional system, while SUSE Linux Enterprise Server is a full server operating system.

Depending on your decision, either continue with installation-and-upgrade:container-deployment/suma/server-deployment-suma.pdf or with installation-and-upgrade:container-deployment/suma/server-deployment-suma.pdf and skip the not selected section.

Unresolved directive in modules/installation-and-upgrade/pages/container-deployment/suma/server-deployment-suma.adoc - include::../../partials/container-deployment/prepare-micro-host.adoc[leveloffset=+1]

To continue with deployment, see installation-and-upgrade:container-deployment/suma/server-deployment-suma.pdf.

Unresolved directive in modules/installation-and-upgrade/pages/container-deployment/suma/server-deployment-suma.adoc - include::../../partials/container-deployment/prepare-sles-host.adoc[leveloffset=+1]

To continue with deployment, see installation-and-upgrade:container-deployment/suma/server-deployment-suma.pdf.

Configure Custom Persistent Storage

Configuring persistent storage is optional, but it is the only way to avoid serious trouble with container full disk conditions. It is highly recommended to configure custom persistent storage with the mgr-storage-server tool.

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

  Use the command in the following manner:

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

For example:

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

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

For more information, see

- **Installation-and-upgrade › Container-management**
- **Administration › Troubleshooting**

Deploy SUSE Manager with mgradm

Procedure: Deploying SUSE Manager 5.0 Using mgradm

1. Log in as root.
2. Execute the following command, replacing <suma.example.com> with your fully qualified domain name:

```
mgradm install podman <suma.example.com>
```

If the above command fails ensure that you have registered SUSE Manager 5.0. If you skipped registration during installation and now need to register from the command line, follow the steps below to log in to the registry:

```
podman login -u <EMAIL> -p <REGISTRATION-CODE> registry.suse.com
```

Use the SUSE Manager 5.0 registration key when prompted.

3. Enter CA key (certificate authority) 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. Enter the email address of the administration account. Press **[Enter]**.
6. Wait for deployment to complete.
7. Open a browser and proceed to your servers FQDN.

8. Enter your username (default is admin) and the password you set during the deployment process.

In this guide you deployed SUSE Manager 5.0 Server as a container. Proceed to the next section to add your organization credentials for syncing with SUSE Customer Center.

Connect SUSE Manager 5.0 to SUSE Customer Center

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

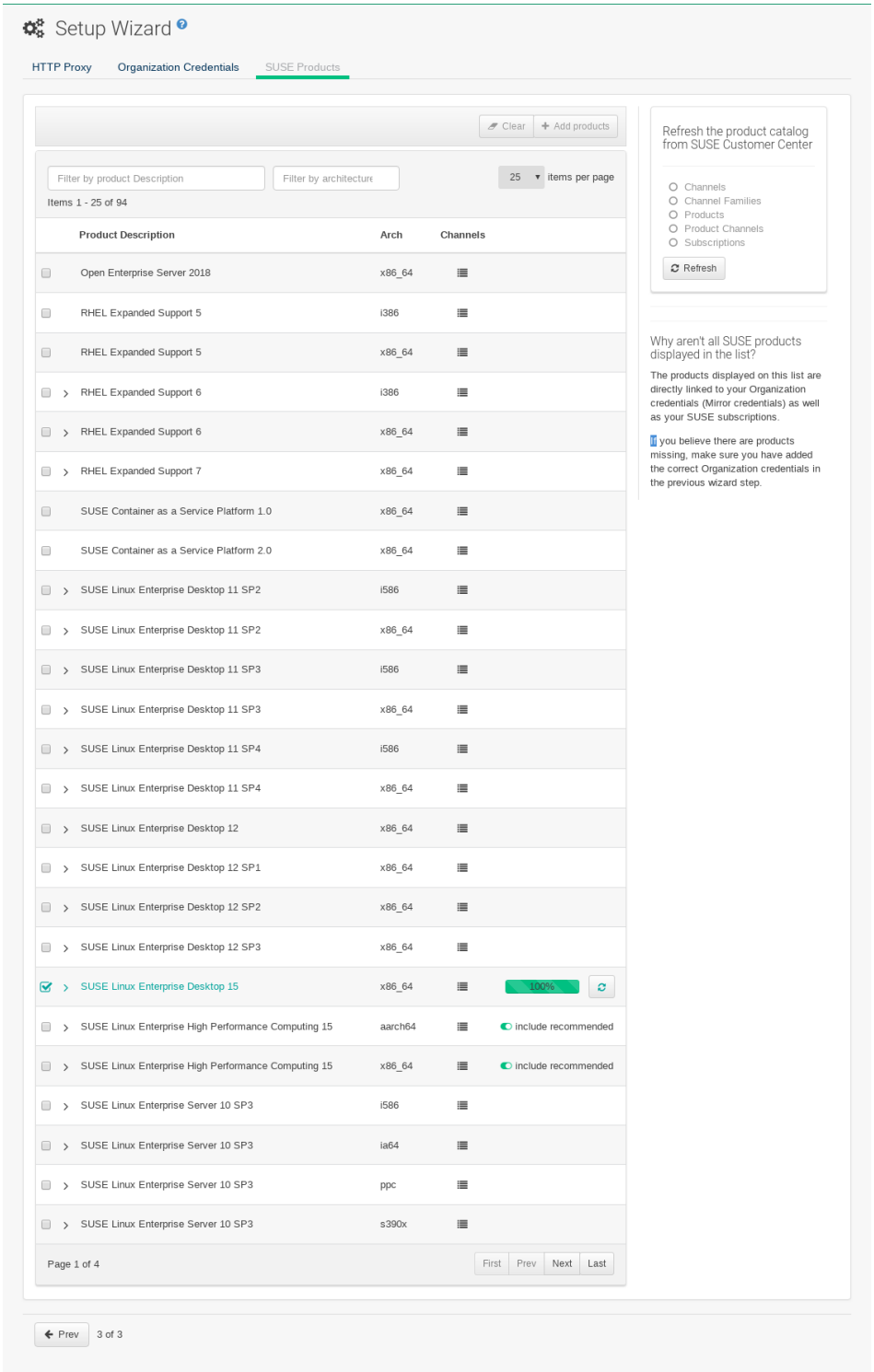
Procedure: Entering Organization Credentials

1. Open a browser and proceed to your servers FQDN.
2. Enter your username (default is admin) and the password you set during the deployment process.
3. In the SUSE Manager Web UI, select **Admin › Setup Wizard**.
4. From the Setup Wizard page select the **[Organization Credentials]** tab.
5. Click **[Add a new credential]**.
6. Point your browser to the SUSE Customer Center.
7. Select your organization from the left navigation.
8. Select the users tab from the top of the page then **[Organization Credentials]**.
9. Make a note of your **Mirroring credentials**.
10. Back in the SUSE Manager Web UI enter your Username and Password, and confirm with **[Save]**.

When the credentials are confirmed with a green 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 recently registered with SUSE Customer Center a list of products will begin populating 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**.



3. Use the Filter by product description and Filter by architecture to filter the list of displayed products. The channels listed on the **[Products]** page provide repositories for clients.
    - 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]** at the top of the page 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 the local /var/lib/containers/storage/volumes/var-spacewalk/ directory of your server.

When the channel is fully synchronized, a bootstrap repository for it will be automatically generated. This step is crucial for successfully bootstrapping clients, ensuring that the channel synchronization and distribution are operational on the client side. This completes the installation and configuration of SUSE Manager, along with preparing the channels necessary for bootstrapping clients.

When the channel synchronization process is complete, you can proceed with registering the SUSE Manager 5.0 Proxy or additional clients.

For more instructions, see **Client-configuration › Registration-overview**.

Entering the Container for Management

To get to a shell inside the container, run on the container host:

```
mgrctl term
```

SUSE Manager 5.0 Server Deployment as a Virtual Machine - KVM

This chapter provides the required Virtual Machine settings for deployment of SUSE Manager 5.0 as an image. KVM will be combined with Virtual Machine Manager (virt-manager) as a sandbox for this installation.

Available Images

The preferred method for deploying SUSE Manager 5.0 Server is to use one of the following available images. All tools are included in these images greatly simplifying deployment.

Images for SUSE Manager 5.0 are available at SUSE Manager 5.0 VM images.

Customized SUSE Manager 5.0 VM images are provided only for SLE Micro 5.5. To run the product on SUSE Linux Enterprise Server 15 SP6, use the standard SUSE Linux Enterprise Server 15 SP6 installation media available at https://www.suse.com/download/sles/ and enable the SUSE Manager 5.0 extensions on top of it.

For more information on preparing raw images, see:

- https://documentation.suse.com/en-us/sle-micro/5.5/single-html/SLE-Micro-deployment/#sec-raw-preparation

- https://documentation.suse.com/en-us/sle-micro/5.5/single-html/SLE-Micro-deployment/#cha-images-procedure

For additional information on the self install images, see:

- https://documentation.suse.com/en-us/sle-micro/5.5/single-html/SLE-Micro-deployment/#cha-selfinstal-procedure

Table 10. Available Server Images

Architecture	Image Format
aarch64	qcow2, vmdk
x86_64	qcow2, vmdk, raw, Self Installer
ppc64le	raw, Self Installer
s390x *	qcow2, raw

* Two storage options are available for s390x: CDL DASD and FBA.

Virtual Machine Manager (virt-manager) Settings

Enter the following settings when creating a new virtual machine using **virt-manager**.

This table specifies the minimum requirements. These are suitable for a quick test installation, such as a server with one client. If you want to use a production environment and need background information about disk space, see **Installation-and-upgrade › Hardware-requirements**.

KVM Settings	
Installation Method	Import Existing Disk Image
OS:	Linux
Version:	SUSE Manager-Server.x86_64-5.0.0-Build16.10.qcow2
Memory:	Minimum *)
CPU's:	Minimum *)
Storage Format:	.qcow2 40 GB (Default) Root Partition
Name:	test-setup

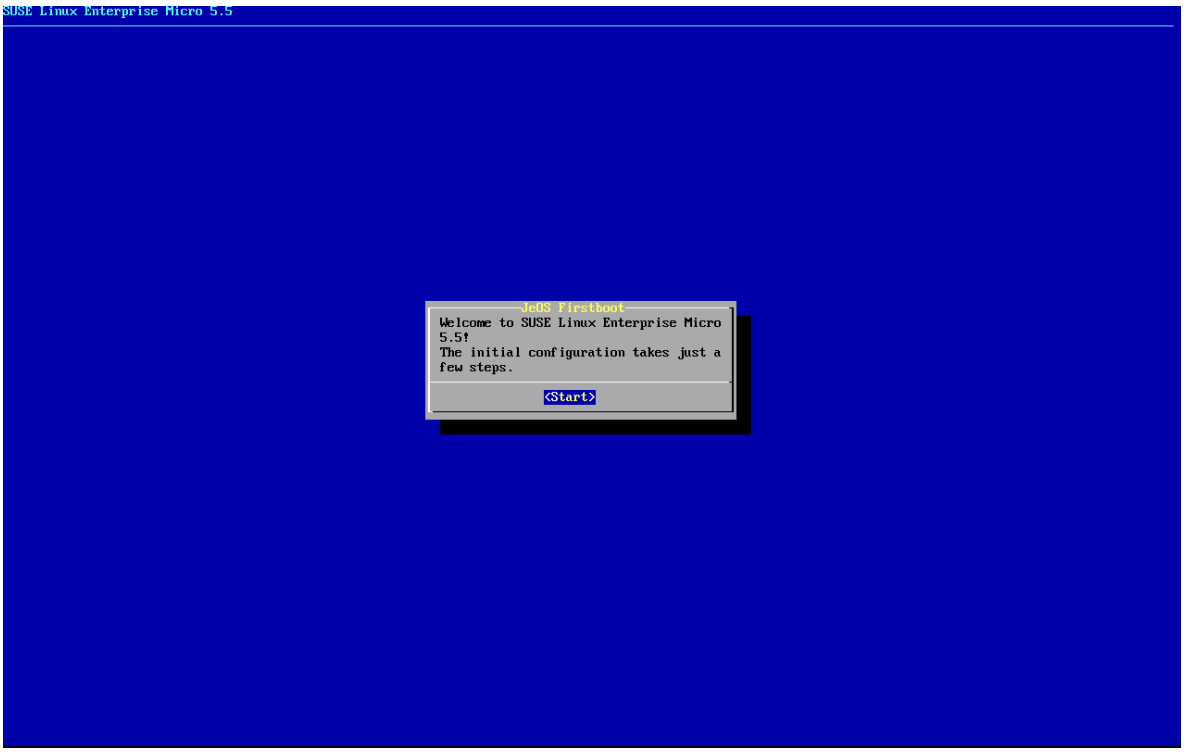
KVM Settings	
Network	Bridge br0

*) For minimum values, see installation-and-upgrade:hardware-requirements.pdf.

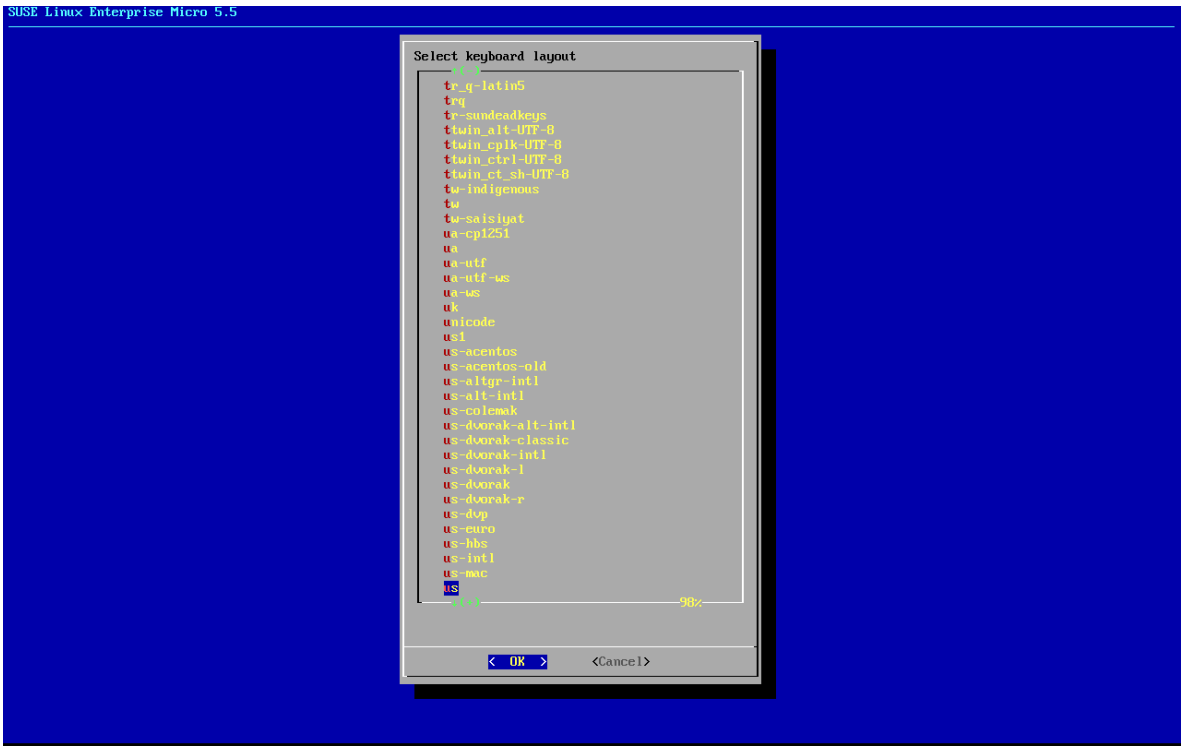
Initial KVM Setup

Procedure: Creating Initial Setup

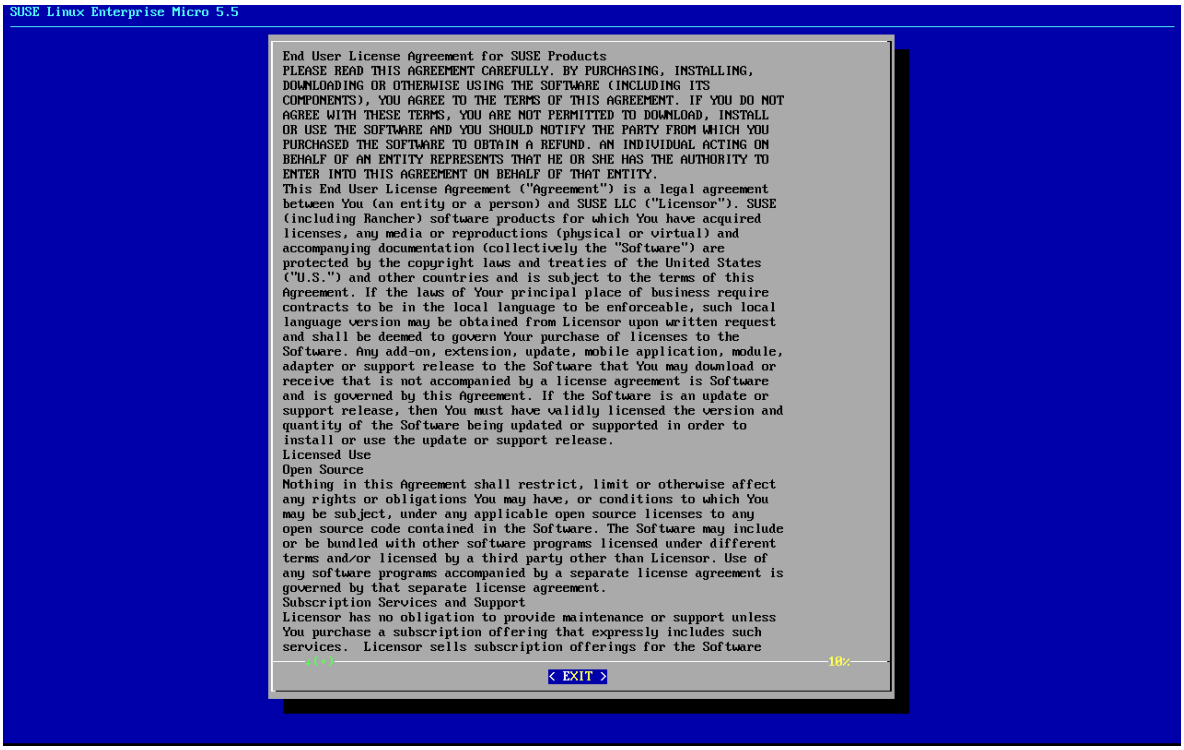
1. Create a new virtual machine using the downloaded Minimal KVM image and select Import existing disk image.
2. Configure RAM and number of CPUs with minimum values. *)
3. Name your KVM machine.
4. Click **[Begin Installation]** to boot from the image.
5. At the JeOS Firstboot screen select start to continue.



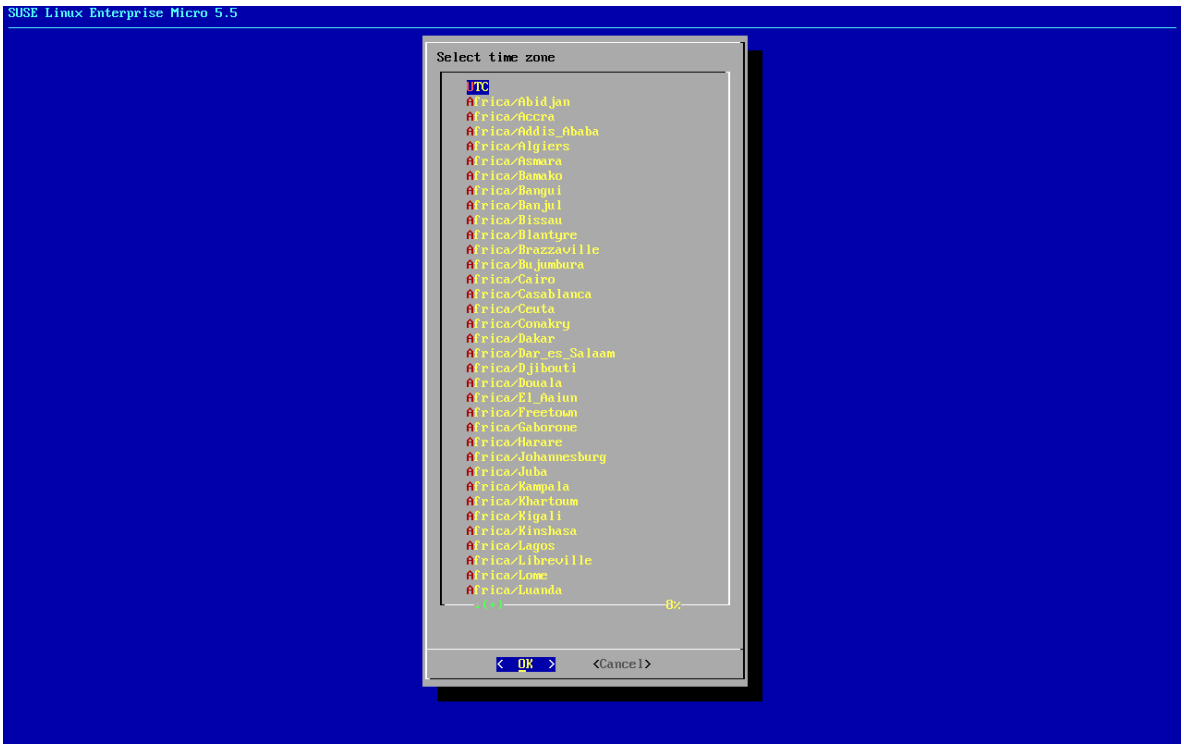
6. Select keyboard layout.



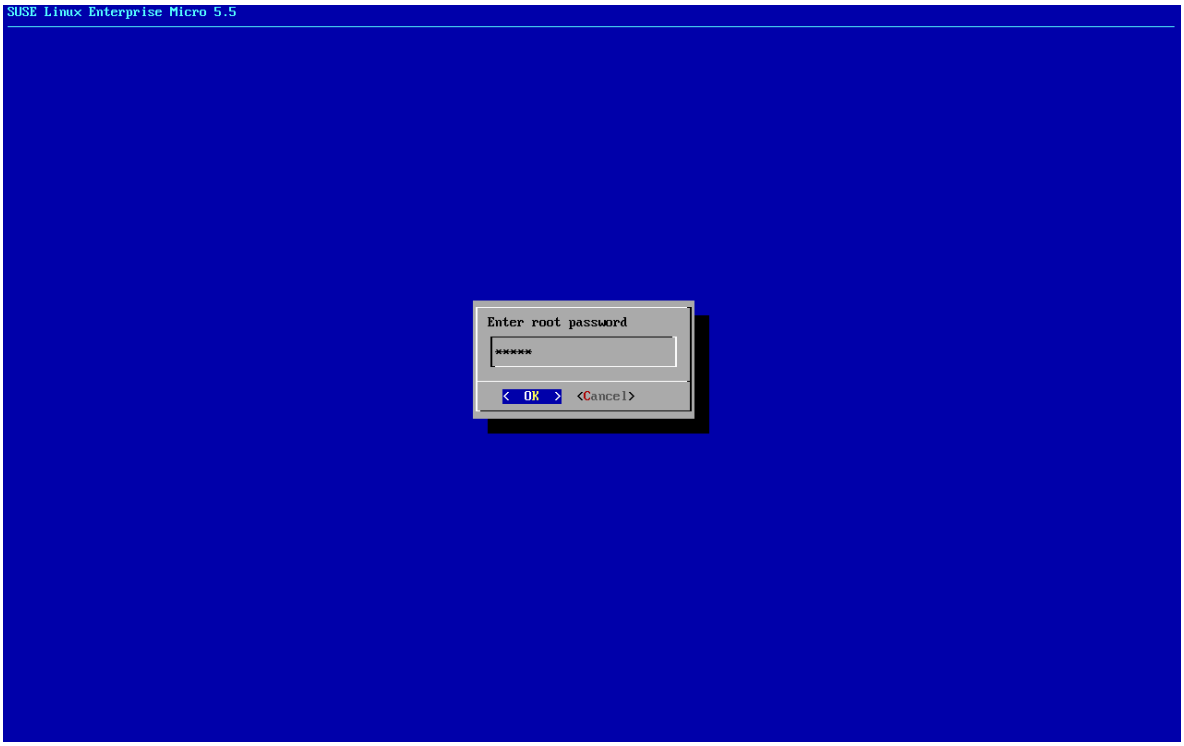
7. Accept the license agreement.



8. Select your time zone.



9. Enter a password for root.



10. When installation completes log in as root.
11. Proceed to the next section.

*) For minimum values, see installation-and-upgrade:hardware-requirements.pdf.

Register SLE Micro and SUSE Manager 5.0 Server

The SLE Micro 5.5 entitlement is included within the SUSE Manager entitlement, so it does not require a separate registration code.

Procedure: Registering SLE Micro and SUSE Manager 5.0

1. Boot the virtual machine.
2. Log in as root.
3. Register SLE Micro with SCC.

```
transactional-update register -r <REGCODE> -e <your_email>
```

4. Reboot.
5. Register SUSE Manager 5.0 with SUSE Customer Center.

```
transactional-update register -p SUSE-Manager-Server/5.0/x86_64 -r <REGCODE>
```

6. Reboot.
7. Update the system:

```
transactional-update
```

8. If updates were applied reboot.
9. This step is optional. However, if custom persistent storage is required for your infrastructure, use the mgr-storage-server tool.
    - For more information, see mgr-storage-server --help. This tool simplifies creating the container storage and database volumes.
    - Use the command in the following manner:

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

      For example:

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

      This command will move the persistent storage volumes at /var/lib/containers/storage/volumes to specified storage devices.

      For more information, see

- **Installation-and-upgrade › Container-management**
- **Administration › Troubleshooting**

10. Run the following command to deploy SUSE Manager:

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

SUSE Manager 5.0 Server Deployment as a Virtual Machine - VMware

This chapter provides the required Virtual Machine settings for deployment of SUSE Manager 5.0 as an Image. VMware will be used as a sandbox for this installation.

Available Images

The preferred method for deploying SUSE Manager 5.0 Server is to use one of the following available images. All tools are included in these images greatly simplifying deployment.

Images for SUSE Manager 5.0 are available at SUSE Manager 5.0 VM images.

Customized SUSE Manager 5.0 VM images are provided only for SLE Micro 5.5. To run the product on SUSE Linux Enterprise Server 15 SP6, use the standard SUSE Linux Enterprise Server 15 SP6 installation media available at https://www.suse.com/download/sles/ and enable the SUSE Manager 5.0 extensions on top of it.

For more information on preparing raw images, see:

- https://documentation.suse.com/en-us/sle-micro/5.5/single-html/SLE-Micro-deployment/#sec-raw-preparation
- https://documentation.suse.com/en-us/sle-micro/5.5/single-html/SLE-Micro-deployment/#cha-images-procedure

For additional information on the self install images, see:

- https://documentation.suse.com/en-us/sle-micro/5.5/single-html/SLE-Micro-deployment/#cha-selfinstal-procedure

Table 11. Available Server Images

Architecture	Image Format
aarch64	qcow2, vmdk
x86_64	qcow2, vmdk, raw, Self Installer
ppc64le	raw, Self Installer
s390x *	qcow2, raw

* Two storage options are available for s390x: CDL DASD and FBA.

SUSE Manager Virtual Machine Settings - VMware

This sections describes VMware configurations, focusing on the creation of an extra virtual disk essential for the SUSE Manager storage partition within VMware environments.

Procedure: Creating the VMware Virtual Machine

1. Download SUSE Manager Server .vmdk file then transfer a copy to your VMware storage.
2. Make a copy of uploaded .vmdk file using VMware web interface. This will convert provided .vmdk file to the format suitable for vSphere hypervisor.
3. Create and name a new virtual machine based on the Guest OS Family Linux and Guest OS Version SUSE Linux Enterprise 15 (64-bit).
4. Add an additional Hard Disk 2 of 500 GB (or more).
5. Configure RAM and number of CPUs with minimum values. *)
6. Set the network adapter as required.
7. Power on the VM, and follow firstboot dialogs (keyboard layout, license agreement, time zone, password for root).
8. When installation completes log in as root.
9. Proceed to the next section.

*) For minimum values, see installation-and-upgrade:hardware-requirements.pdf.

Register SLE Micro and SUSE Manager 5.0 Server

Before starting obtain your SUSE Manager Registration Code from SUSE Customer Center - https://scc.suse.com.

The SLE Micro 5.5 entitlement is included within the SUSE Manager entitlement, so it does not require a separate registration code.

Procedure: Registering SLE Micro and SUSE Manager 5.0

1. Boot the virtual machine.
2. Log in as root.
3. Register SLE Micro with SCC.

```
transactional-update register -r <REGCODE> -e <your_email>
```

4. Reboot.
5. Register SUSE Manager 5.0 with SUSE Customer Center.

```
transactional-update register -p SUSE-Manager-Server/5.0/x86_64 -r <REGCODE>
```

6. Reboot
7. Update the system:

```
transactional-update
```

8. If updates were applied reboot.
9. This step is optional. However, if custom persistent storage is required for your infrastructure, use the mgr-storage-server tool.
    - For more information, see mgr-storage-server --help. This tool simplifies creating the container storage and database volumes.
    - Use the command in the following manner:

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

For example:

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

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

For more information, see

- **Installation-and-upgrade › Container-management**
- **Administration › Troubleshooting**

10. Run the following command to deploy SUSE Manager:

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

SUSE Manager Server Air-gapped Deployment

What is Air-gapped Deployment?

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

At the moment, air-gapped deployment is available only on SLE Micro.

Deployments

SUSE Manager supports two deployment variants.

Deploy with Virtual Machine

The recommended installation method is using the provided SUSE Manager Virtual Machine Image option, since all the needed tools and container images are pre-loaded and will work out of the box.

For more information about installing SUSE Manager Server Virtual Machine, see Deploy Server as a Virtual Machine.

To upgrade SUSE Manager Server, users should upgrade all packages in the system and follow the procedures defined in Server Upgrade.

Deploy SUSE Manager on SLE Micro

SUSE Manager also provides all the needed container images in RPM's that can be installed on the system.

User should make the needed RPM available on the internal network. That can be done by using a second SUSE Manager Server or an RMT server.

Procedure: Install SUSE Manager on SLE Micro in air-gapped deployment

1. Install SLE Micro.
2. Update the system.

3. Install tools packages and image packages (replace $ARCH$ with the correct architecture).

```
transactional-update pkg install mgradm* mgrctl* suse-manager-5.0-$ARCH$-
server-*
```

4. Reboot.

5. Deploy SUSE Manager with mgradm.

For more detailed information about installing SUSE Manager Server on SLE Micro, see Deploy Server as a Virtual Machine.

To upgrade SUSE Manager Server, users should upgrade all packages in the system and follow the procedures defined in Server Upgrade.

PTFs

The PTF images are not available as packages. This means that they should be pulled using podman on a machine with internet access, then saved in an archive, transferred to the air-gapped machine and loaded there.

Procedure: Pulling the image on a machine with internet access

1. Install podman.

2. Authenticate against the SUSE Registry using the SCC credentials:

```
set +o history
echo SCC_MIRRORING_PASSWORD | podman login -u "SCC_MIRRORING_USER" --password
-stdin registry.suse.com
set -o history
```

3. Create a /tmp/ptf-images temporary file with the URL of the PTF images, one per line. In most of the cases only the server image is needed and it can be created with a command like the following, after replacing the SCC_USERID and PTFID values.

```
SCC_USERID=aXXXX
PTFID=12345
echo
"registry.suse.com/a/$SCC_USERID/$PTFID/suse/manager/5.0/x86_64/server:latest-
ptf-$PTFID" >>/tmp/ptf-images
```

4. Pull each of the container images of the PTF and save them in a tar archive.

```
for image in `cat /tmp/ptf-images`; do
    podman pull $image
done
podman save -o /tmp/ptf-images.tar `cat /tmp/ptf-images`
```

5. Transfer the /tmp/ptf-images.tar images archive on the server to patch.

Procedure: Loading the images on the server to patch

1. Ensure the ptf-images.tar file is available on the server.
2. Load the images from the archive:

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

3. Install the PTF as it would be done on a connected machine, using command:

```
mgradm support ptf podman [--test|--ptf] NUMBER --user SCC_ACCOUNT
```

Because the images are already loaded they will not be pulled.

Public Cloud Deployment

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

For more information about using SUSE Manager in the public cloud, see **Specialized-guides › Public-cloud-guide**.

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 SCC organization credentials.

Before using PAYG feature make sure that:

- 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 SCC account is required. Enter your valid SCC credentials in **Admin › Setup Wizard › Organization Credentials**. This account is required for accessing the SUSE Manager client tools for boostrapping 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.

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 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 SUSE Linux Enterprise Server 15 SP1 product installed, SUSE Linux Enterprise Server 15 SP2, SUSE Linux Enterprise Server 15 SP3, SUSE Linux Enterprise Server 15 SP4 and SUSE Linux Enterprise Server 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 SCC 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.

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 not reachable, the credential update process will fail.

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 [proc-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

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**.

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.

2.2. Install SUSE Manager Proxy

There are various scenarios to deploy a SUSE Manager Proxy. All these scenarios presume you have already successfully deployed a SUSE Manager 5.0 Server.

SUSE Manager 5.0 Proxy Deployment

This guide outlines the deployment process for the SUSE Manager 5.0 Proxy container on SLE Micro 5.5 or SUSE Linux Enterprise Server 15 SP6. This guide presumes you have already successfully deployed a SUSE Manager 5.0 Server.

SLE Micro is only supported as regular minion (default contact method) for the time being. We are working on managing it as Salt SSH client (salt-ssh contact method), too.

To successfully deploy, you will perform the following actions:

Procedure: Deploying Proxy

1. Review hardware requirements.
2. Synchronize the SLE Micro 5.5 or SUSE Linux Enterprise Server 15 SP6 parent channel and the proxy extension child channel on the server.

3. Install SLE Micro or SUSE Linux Enterprise Server on a bare-metal machine.
4. During the installation, register SLE Micro or SUSE Linux Enterprise Server along with the SUSE Manager Proxy extension.
5. Create a Salt activation key.
6. Bootstrap the proxy as a client with the default connection method.
7. Generate a proxy configuration.
8. Transfer the proxy configuration from server to proxy.
9. Use the proxy configuration to register the client as a proxy with SUSE Manager.

Supported operating system for the Proxy Container Host

The supported operating system for the container host are SLE Micro 5.5 and SUSE Linux Enterprise Server 15 SP6.

Container host

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

Hardware Requirements for the Proxy

For more information about hardware requirements for deploying SUSE Manager Proxy, see installation-and-upgrade:hardware-requirements.pdf.

Synchronize the Parent and Proxy Extension Child Channels

This section presumes that you have already entered your organization credentials under the **Admin › Setup Wizard › Organization Credentials** in the server's Web UI. Products are listed on the **Admin › Setup Wizard › Products** page. This channel must be fully synchronized on the server, with the child channel Proxy as an extension option selected.

Procedure: Synchronizing the Proxy Parent Channel and Proxy Extension

1. In the SUSE Manager Web UI select **Admin › Products**.
2. From the products page enter SLE Micro or SUSE Linux Enterprise Server in the filter field.
3. Next use the drop-down to select the required architecture. For this example x86-64.
4. In the Product Description field select the SLE Micro 5.5 or SUSE Linux Enterprise Server 15 SP6 checkbox then use the drop-down to select the SUSE Manager Proxy Extension 5.0 x86_64 extension.
5. Click the **[Add products]** button.
6. Wait for the synchronization to complete.

Prepare SUSE Manager Proxy Host

In the following subsections, you either prepare the proxy host with SLE Micro or SUSE Linux Enterprise Server.

Unresolved directive in modules/installation-and-upgrade/pages/container-deployment/suma/proxy-deployment-suma.adoc - include::../../partials/container-deployment/prepare-micro-host.adoc[leveloffset=+1]

To continue with deployment, see installation-and-upgrade:container-deployment/suma/proxy-deployment-suma.pdf.

Unresolved directive in modules/installation-and-upgrade/pages/container-deployment/suma/proxy-deployment-suma.adoc - include::../../partials/container-deployment/prepare-sles-host.adoc[leveloffset=+1]

To continue with deployment, see installation-and-upgrade:container-deployment/suma/proxy-deployment-suma.pdf.

Configure Custom Persistent Storage

Configuring persistent storage is optional, but it is the only way to avoid serious trouble with container full disk conditions. If custom persistent storage is required for your infrastructure, use the mgr-storage-proxy tool.

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

Use the command in the following manner:

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

For example:

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

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

For more information, see

- **Installation-and-upgrade › Container-management**
- **Administration › Troubleshooting**

Unresolved directive in modules/installation-and-upgrade/pages/container-deployment/suma/proxy-deployment-suma.adoc - include::../../partials/container-deployment/actkey-bootstrap-proxy-suma.adoc[]

Unresolved directive in modules/installation-and-upgrade/pages/container-deployment/suma/proxy-deployment-suma.adoc - include::../../partials/container-deployment/bootstrap-proxy-client.adoc[]

Unresolved directive in modules/installation-and-upgrade/pages/container-deployment/suma/proxy-deployment-suma.adoc - include::../../partials/container-deployment/generate_proxy_config.adoc[]

Unresolved directive in modules/installation-and-upgrade/pages/container-deployment/suma/proxy-deployment-suma.adoc - include::../../partials/container-deployment/transfer_proxy_config.adoc[]

Start the SUSE Manager Proxy

Container can now be started with the mgrpxy command:

Procedure: Starting and Checking Proxy Status

1. Start the proxy by calling:

```
mgrpxy start
```

2. Check container status by calling:

```
mgrpxy status
```

Five SUSE Manager Proxy containers should be present and should be part of the proxy-pod container pod:

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

Use a Custom Container Image for a Service

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

For example:

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

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

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

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

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

SUSE Manager Proxy Deployment as a Virtual Machine - KVM

This chapter provides the Virtual Machine settings for deployment of SUSE Manager 5.0 Proxy as an image. KVM will be combined with Virtual Machine Manager (virt-manager) as a sandbox for this installation.

Available Images

The preferred method for deploying SUSE Manager Proxy is to use one of the following available images. All tools are included in these images simplifying deployment.

Images for SUSE Manager 5.0 Proxy are available at SUSE Manager 5.0 VM images.

Customized SUSE Manager 5.0 VM images are provided only for SLE Micro 5.5. To run the product on SUSE Linux Enterprise Server 15 SP6, use the standard SUSE Linux Enterprise Server 15 SP6 installation media available at https://www.suse.com/download/sles/ and enable the SUSE Manager 5.0 extensions on top of it.

For more information on preparing raw images, see:

- https://documentation.suse.com/en-us/sle-micro/5.5/single-html/SLE-Micro-deployment/#sec-raw-preparation
- https://documentation.suse.com/en-us/sle-micro/5.5/single-html/SLE-Micro-deployment/#cha-images-procedure

For additional information on the self install images, see:

- https://documentation.suse.com/en-us/sle-micro/5.5/single-html/SLE-Micro-deployment/#cha-selfinstal-procedure

Table 12. Available Proxy Images

Architecture	Image Format
aarch64	qcow2, vmdk
x86_64	qcow2, vmdk, raw, Self Installer

Virtual Machine Manager (virt-manager) Settings

Enter the following settings when creating a new virtual machine using **virt-manager**.

This table specifies the minimum requirements. These are suitable for a quick test installation, such as a proxy with one client.

If you want to use a production environment and need background information about disk space, see **Installation-and-upgrade › Hardware-requirements**.

KVM Settings	
Installation Method	Import Existing Disk Image
OS:	Linux
Version:	SUSE Manager-Proxy.x86_64-5.0.0-*.qcow2

KVM Settings	
Memory:	Minimum *)
CPU's:	Minimum *)
Storage Format:	.qcow2 40 GB (Default) Root Partition
Name:	test-setup
Network	Bridge br0

*) For minimum values, see installation-and-upgrade:hardware-requirements.pdf.

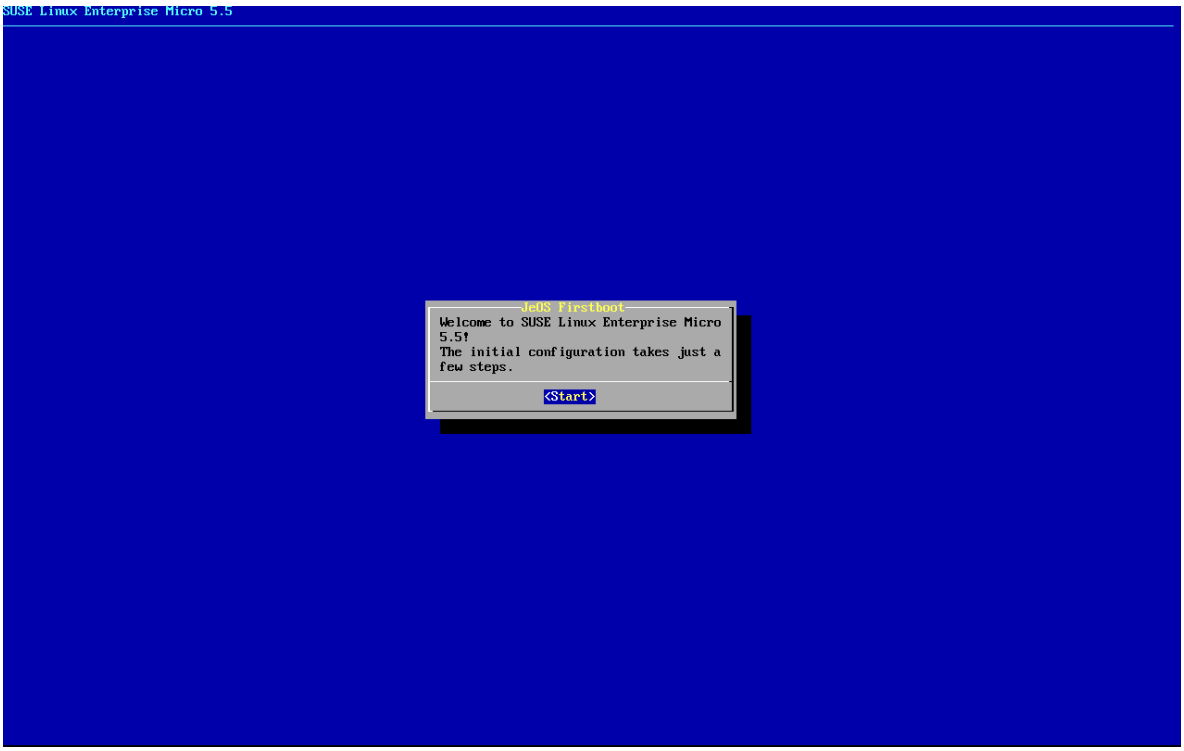
/var/lib/containers/storage/volumes Minimum 100 GB. Storage requirements should be calculated for the number of ISO distribution images, containers, and bootstrap repositories you will use.

Initial KVM Setup

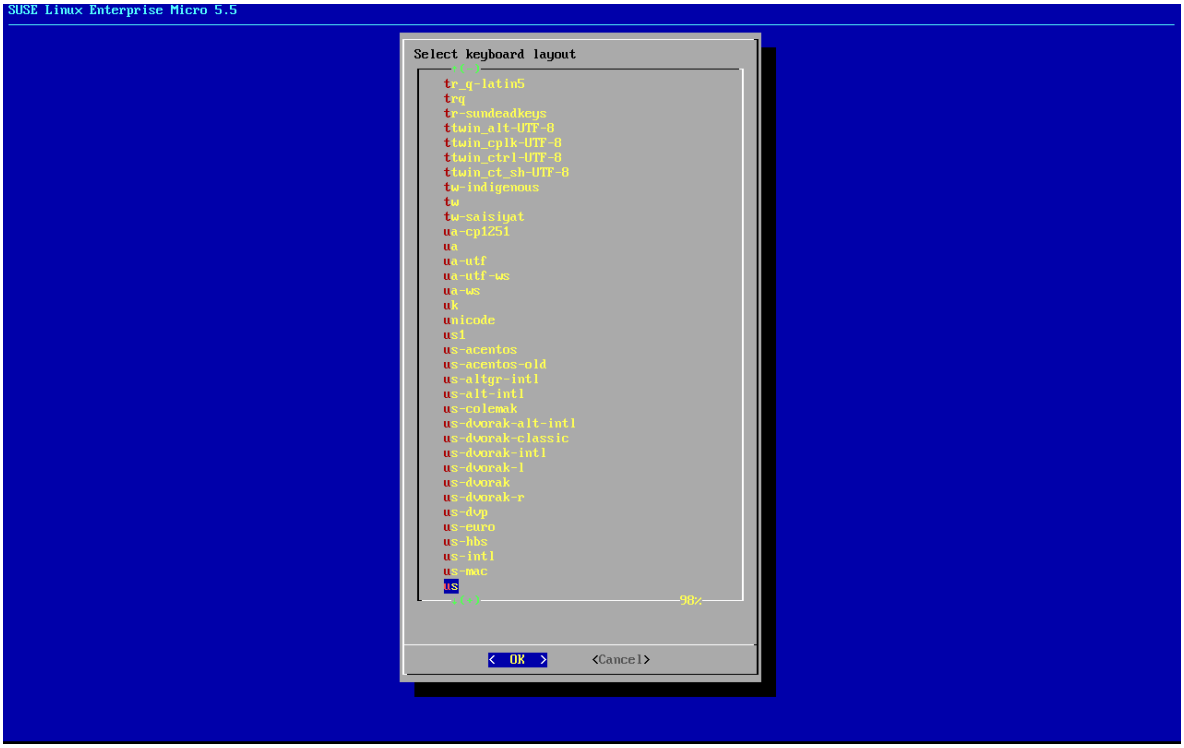
For settings, see installation-and-upgrade:container-deployment/suma/proxy-deployment-vm-suma.pdf.

Procedure: Creating Initial Setup

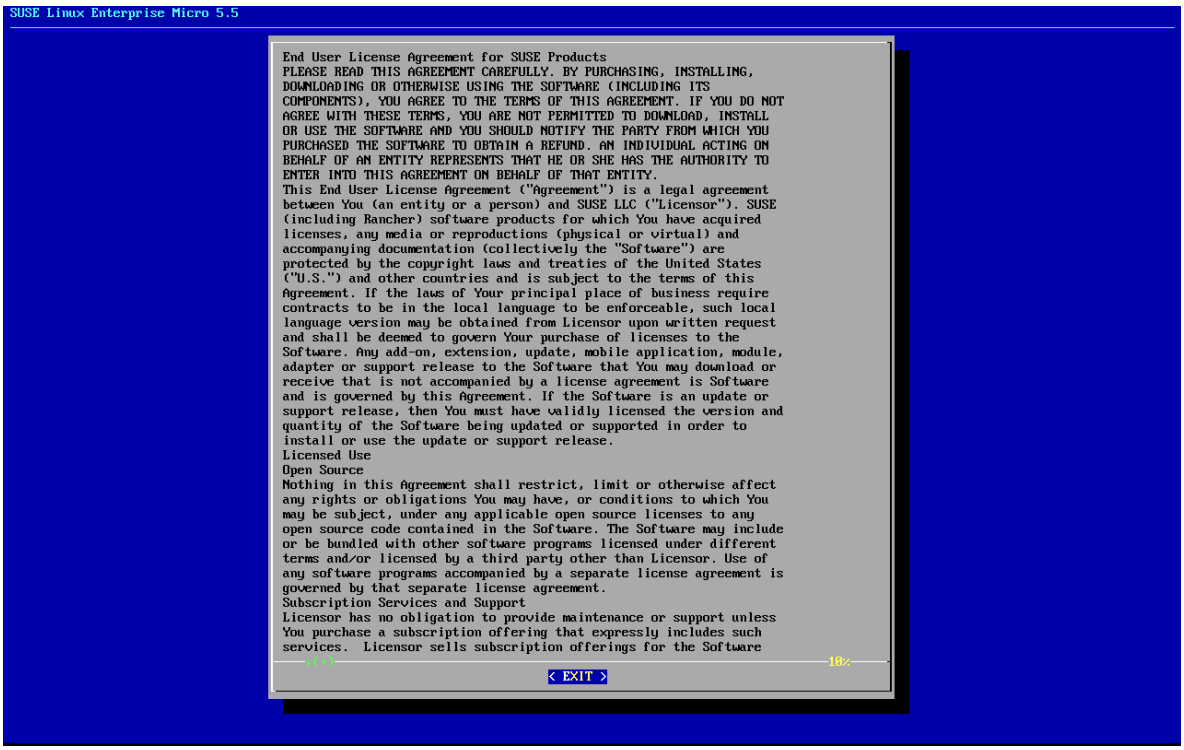
1. Create a new virtual machine using the downloaded Minimal KVM image and select Import existing disk image.
2. Configure RAM and number of CPUs with minimum values. *)
3. Name your KVM machine and select the Customize configuration before install check box.
4. Click **[Begin Installation]** to boot from the image.
5. At the JeOS Firstboot screen select start to continue.



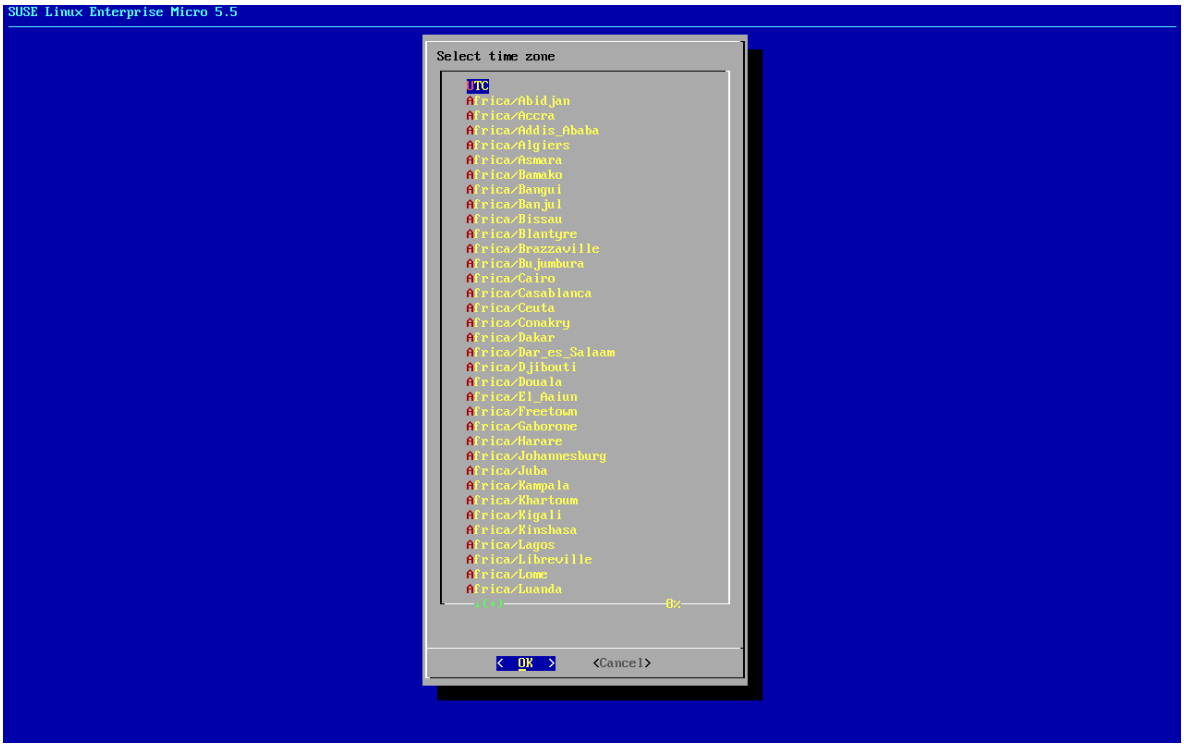
6. Select keyboard layout.



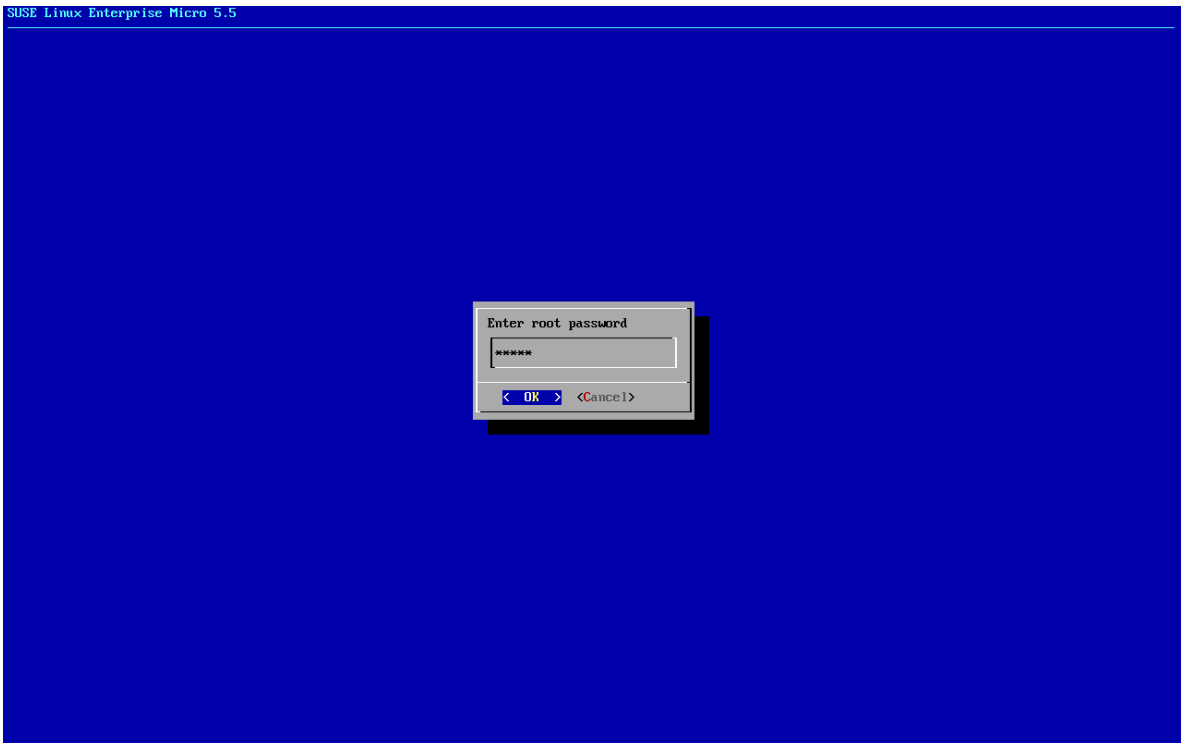
7. Accept the license agreement.



8. Select your time zone.



9. Enter a password for root.



10. When installation completes log in as root.
11. Proceed to the next section.

*) For minimum values, see installation-and-upgrade:hardware-requirements.pdf.

Unresolved directive in modules/installation-and-upgrade/pages/container-deployment/suma/proxy-deployment-vm-suma.adoc - include::../../partials/container-deployment/register-proxy-suma.adoc[]

Unresolved directive in modules/installation-and-upgrade/pages/container-deployment/suma/proxy-deployment-vm-suma.adoc - include::../../partials/container-deployment/actkey-bootstrap-proxy-suma.adoc[]

Unresolved directive in modules/installation-and-upgrade/pages/container-deployment/suma/proxy-deployment-vm-suma.adoc - include::../../partials/container-deployment/generate_proxy_config.adoc[]

Unresolved directive in modules/installation-and-upgrade/pages/container-deployment/suma/proxy-deployment-vm-suma.adoc - include::../../partials/container-deployment/transfer_proxy_config.adoc[]

Unresolved directive in modules/installation-and-upgrade/pages/container-deployment/suma/proxy-deployment-vm-suma.adoc - include::../../partials/container-deployment/start_proxy.adoc[]

Using a Custom Container Image for a Service

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

ending with -tag and -image.

For example, use it like this:

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

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

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

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

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

SUSE Manager Proxy Deployment as a Virtual Machine - VMware

This chapter provides the Virtual Machine settings for deployment of SUSE Manager 5.0 Proxy as an image. VMware will be used as a sandbox for this installation.

Available Images

The preferred method for deploying SUSE Manager Proxy is to use one of the following available images. All tools are included in these images simplifying deployment.

Images for SUSE Manager 5.0 Proxy are available at SUSE Manager 5.0 VM images.

Customized SUSE Manager 5.0 VM images are provided only for SLE Micro 5.5. To run the product on SUSE Linux Enterprise Server 15 SP6, use the standard SUSE Linux Enterprise Server 15 SP6 installation media available at https://www.suse.com/download/sles/ and enable the SUSE Manager 5.0 extensions on top of it.

For more information on preparing raw images, see:

- https://documentation.suse.com/en-us/sle-micro/5.5/single-html/SLE-Micro-deployment/#sec-raw-preparation
- https://documentation.suse.com/en-us/sle-micro/5.5/single-html/SLE-Micro-deployment/#cha-images-procedure

For additional information on the self install images, see:

- https://documentation.suse.com/en-us/sle-micro/5.5/single-html/SLE-Micro-deployment/#cha-selfinstal-procedure

Table 13. Available Proxy Images

Architecture	Image Format
aarch64	qcow2, vmdk
x86_64	qcow2, vmdk, raw, Self Installer

Virtual Machine Settings - VMware

This section describes VMware configurations, focusing on the creation of an extra virtual disk essential for the SUSE Manager Proxy storage partition within VMware environments.

This section specifies the minimum requirements. These are suitable for a quick test installation, such as a proxy with one client.

If you want to use a production environment and need background information about disk space, see **Installation-and-upgrade › Hardware-requirements**.

Procedure: Creating the VMware Virtual Machine

1. Download SUSE Manager Proxy .vmdk file then transfer a copy to your VMware storage.
2. Make a copy of uploaded .vmdk file using VMware web interface. This will convert provided .vmdk file to the format suitable for vSphere hypervisor.
3. Create and name a new virtual machine based on the Guest OS Family Linux and Guest OS Version SUSE Linux Enterprise 15 (64-bit).
4. Add an additional Hard Disk 2 of 100 GB (or more).
5. Configure RAM and number of CPUs with minimum values. *)
6. Set the network adapter as required.
7. Power on the VM, and follow firstboot dialogs (keyboard layout, license agreement, time zone, password for root).
8. When installation completes log in as root.
9. Proceed to the next section.

*) For minimum values, see installation-and-upgrade:hardware-requirements.pdf.

Unresolved directive in modules/installation-and-upgrade/pages/container-deployment/suma/proxy-deployment-vmdk-suma.adoc - include::../../partials/container-deployment/register-proxy-suma.adoc[]

Unresolved directive in modules/installation-and-upgrade/pages/container-deployment/suma/proxy-deployment-vmdk-suma.adoc - include::../../partials/container-deployment/actkey-bootstrap-proxy-suma.adoc[]

Unresolved directive in modules/installation-and-upgrade/pages/container-deployment/suma/proxy-deployment-vmdk-suma.adoc - include::../../partials/container-deployment/generate_proxy_config.adoc[]

Unresolved directive in modules/installation-and-upgrade/pages/container-deployment/suma/proxy-deployment-vmdk-suma.adoc - include::../../partials/container-deployment/transfer_proxy_config.adoc[]

Unresolved directive in modules/installation-and-upgrade/pages/container-deployment/suma/proxy-deployment-vmdk-suma.adoc - include::../../partials/container-deployment/start_proxy.adoc[]

Using a Custom Container Image for a Service

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

For example, use it like this:

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

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

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

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

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

SUSE Manager 5.0 Proxy Deployment on K3s

Installing K3s

SUSE Manager Proxy is supported on K3s running on top of SLE Micro in a single node cluster. If you need to deploy it in any other Kubernetes environment, please contact support for evaluation.

On the container host machine, install K3s (replace <K3S_HOST_FQDN> with the FQDN of your K3s host):

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

Installing Tools

The installation requires the mgrpxy and helm packages.

The mgrpxy and helm packages are available in the SUSE Manager Proxy product repositories.

1. To install it run:

```
transactional-update pkg install helm mgrpxy
```

2. Reboot

Unresolved directive in modules/installation-and-upgrade/pages/container-deployment/suma/proxy-k3s-deployment-suma.adoc - include::../../partials/container-deployment/generate_proxy_config.adoc[tags=generate-proxy-config-section]

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.

SUSE Manager Proxy Air-gapped Deployment

What is air-gapped deployment?

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

At the moment, air-gapped deployment is available only on SLE Micro.

Deploy with Virtual Machine

The recommended installation method is using the provided SUSE Manager Virtual Machine Image option, since all the needed tools and container images are pre-loaded and will work out of the box.

For more information about installing SUSE Manager Proxy Virtual Machine, see Deploy Proxy as a Virtual Machine.

To upgrade SUSE Manager Proxy, users should follow the procedures defined in Proxy Upgrade.

Deploy SUSE Manager on SLE Micro

SUSE Manager also provides all the needed container images in RPM's that can be installed on the system.

Procedure: Install SUSE Manager on SLE Micro in Air-gapped

1. Install SLE Micro.
2. Bootstrap the Proxy Host OS as a Client on SUSE Manager Server.
3. Update the system.
4. Install tools packages and image packages (replace $ARCH$ with the correct architecture)

```
transactional-update pkg install mgrpxy* mgrctl* suse-manager-5.0-$ARCH$-proxy-*
```

5. Reboot.
6. Deploy SUSE Manager with mgrpxy.

For more detailed information about installing SUSE Manager Proxy on SLE Micro, see Deploy Proxy as a Virtual Machine.

To upgrade SUSE Manager Proxy, users should follow the procedures defined in Proxy Upgrade.

Chapter 3. Upgrade and Migration

3.1. Server

SUSE Manager Server Migration to a Containerized Environment

Requirements and Considerations

General

- To migrate a SUSE Manager 4.3 Server to a container, you require a new machine with SLE Micro 5.5 or SUSE Linux Enterprise Server 15 SP6, and mgradm installed.
- An in-place migration from SUSE Manager 4.3 to 5.0 is not supported, regardless of whether the chosen host operating system is SLE Micro 5.5 or SUSE Linux Enterprise Server 15 SP6.
- Before migrating from SUSE Manager 4.3 to 5.0, any existing traditional clients including the traditional proxies must be migrated to Salt.
  - For more information about migrating traditional SUSE Manager 4.3 clients to Salt clients, see https://documentation.suse.com/suma/4.3/en/suse-manager/client-configuration/contact-methods-migrate-traditional.html.
- Traditional contact protocol is no longer supported in SUSE Manager 5.0 and later.

This guide only covers the migration from SUSE Manager 4.3 to 5.0. Migrating an existing SUSE Manager 5.0 instance to the same version while switching the host operating system from SLE Micro 5.5 to SUSE Linux Enterprise Server 15 SP6, or vice versa, is not handled by the mgradm migrate command.

GPG Keys

- Self trusted GPG keys are not migrated.
- GPG keys that are trusted in the RPM database only are not migrated. Thus synchronizing channels with spacewalk-repo-sync can fail.
- The administrator must migrate these keys manually from the 4.3 installation to the container host after the actual server migration.

Procedure: Manual Migration of the 4.3 GPG Keys to New Server

1. Copy the keys from the 4.3 server to the container host of the new server.
2. Later, add each key to the migrated server with the command mgradm gpg add <PATH_TO_KEY_FILE>.

Migration

Prepare SUSE Manager 5.0 Server Host

Do not pre-install SUSE Manager on the prepared SLE Micro 5.5 or SUSE Linux Enterprise Server 15 SP6 system. The migration process is designed to perform the server installation automatically. Running `mgradm install` and then `mgradm migrate` is not supported and will lead to an unsupported system state.

In the following steps, we are only preparing the host system, not installing the actual SUSE Manager 5.0 Server.

Unresolved directive in modules/installation-and-upgrade/pages/container-deployment/suma/server-migration-suma.adoc - include::../../partials/container-deployment/prepare-micro-host.adoc[leveloffset=+2]

Unresolved directive in modules/installation-and-upgrade/pages/container-deployment/suma/server-migration-suma.adoc - include::../../partials/container-deployment/prepare-sles-host.adoc[leveloffset=+2]

SSH Connection Preparation

This step ensures that the new SUSE Manager 5.0 Server can connect to the existing 4.3 Server over SSH without requiring a password. It involves generating and configuring SSH keys, setting up an SSH agent, and copying the public key to the old server.

This setup is required for the migration process to run without manual intervention.

Procedure: Preparing the SSH Connection

1. Ensure that for root an SSH key exists on the new 5.0 server. If a key does not exist, create it with:

```
ssh-keygen -t rsa
```

2. The SSH configuration and agent should be ready on the new server for a connection to the 4.3 server that does not prompt for a password.

```
eval $(ssh-agent); ssh-add
```

To establish a connection that does not prompt for a password, the migration script relies on an SSH agent running on the new 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` followed by the path to the private key. You will be prompted to enter the password for the private key during this process.

3. Copy the public SSH key to the SUSE Manager 4.3 Server (<oldserver.fqdn>) with ssh-copy-id. Replace <oldserver.fqdn> with the FQDN of the 4.3 server:

```
ssh-copy-id <old server.fqdn>
```

The SSH key will be copied into the old server's ~/.ssh/authorized_keys file. For more information, see the ssh-copy-id manpage.

4. Establish an SSH connection from the new server to the old SUSE Manager Server to check that no password is needed. Also there must not by any problem with the host fingerprint. In case of trouble, remove old fingerprints from the ~/.ssh/known_hosts file. Then try again. The fingerprint will be stored in the local ~/.ssh/known_hosts file.

Perform the Migration

When planning your migration from SUSE Manager 4.3 to SUSE Manager 5.0, ensure that your target instance meets or exceeds the specifications of the old setup.

This includes, but is not limited to, memory (RAM), CPU Cores, Storage, and Network Bandwidth.

Procedure: Performing the Migration

1. This step is optional. If custom persistent storage is required for your infrastructure, use the mgr-storage-server tool. For more information about mgr-storage-server, see installation-and-upgrade:hardware-requirements.pdf.
2. Execute the following command to install a new SUSE Manager server. Replace <oldserver.fqdn> with the FQDN of the 4.3 server:

Make sure to upgrade your 4.3 server and apply all available updates before starting the migration process. Additionally, remove any unnecessary channels to help reduce the overall migration time.

The migration can take a very long time depending on the amount of data that needs to be replicated. To reduce downtime it is possible to run the migration multiple times in a process of initial replication, re-replication, or final replication and switch over while all the services on the old server can stay up and running.

Only during the final migration the processes on the old server need to be stopped.

For all non-final replications add the parameter --prepare to prevent the automatic stopping the services on the old server. For example on SUSE Manager server:

```
mgradm migrate podman <oldserver.fqdn> --prepare
```

Procedure: Final Migration

1. Stop the SUSE Manager services on 4.3 Server:

```
spacewalk-service stop
```

2. Stop the PostgreSQL service on 4.3 Server:

```
systemctl stop postgresql
```

3. Perform the migration on SUSE Manager server

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

4. Migrate trusted SSL CA certificates.

Migration of the Certificates

Trusted SSL CA certificates that were installed as part of an RPM and stored on SUSE Manager 4.3 in the /usr/share/pki/trust/anchors/ directory will not be migrated. Because SUSE does not install RPM packages in the container, the administrator must migrate these certificate files manually from the 4.3 installation after the migration.

Procedure: Migrating the Certificates

1. Copy the file from the 4.3 server to the new server. For example, as /local/ca.file.
2. Copy the file into the container with:

```
mgrctl cp /local/ca.file server:/etc/pki/trust/anchors/
```

After successfully running the mgradm migrate command, the Salt setup on all clients will still point to the old 4.3 server.

To redirect them to the 5.0 server, it is required to rename the new server at the infrastructure level (DHCP and DNS) to use the same FQDN and IP address as 4.3 server.

Server Upgrade

Before running the upgrade command, it is required to upgrade the mgradm tool first.

Procedure: Upgrading Server

1. Refresh software repositories with zypper:

```
zypper ref
```

2. Apply available updates:

   a. For SLE Micro:

   ```
   transactional-update
   ```

   If updates were applied, reboot.

   b. For SUSE Linux Enterprise Server:

   ```
   zypper up
   ```

3. The SUSE Manager Server container can be updated using the following command:

   ```
   mgradm upgrade podman
   ```

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

4. Clean up the unused container images to free disk space:

   ```
   podman image prune -a
   ```

> **Upgrading to specific version**
>
> If you do not specify the tag parameter, it will default to upgrading to the most recent version. To upgrade to a specific version, provide the tag parameter with the desired image tag.

For more information on the upgrade command and its parameters, use the following command:

```
mgradm upgrade podman -h
```

For air-gapped installations, first upgrade the container RPM packages, then run the mgradm command.

3.2. Proxy

Proxy Migration

In SUSE Manager 4.3, the proxy can be deployed using three different methods: RPM based, containerized running on podman or k3s.

In SUSE Manager 5.0, management of the containerized proxy running with podman was re-designed and made simpler with the mgrpxy tool. At the same time, RPM based support was removed, and only the containerized version running with podman or k3s is supported.

This section describes migrating from Proxy 4.3 using the mgrpxy tool.

An in-place migration from SUSE Manager 4.3 to 5.0 is unsupported. The host operating system has changed from SUSE Linux Enterprise Server 15 SP4 to SLE Micro 5.5 or SUSE Linux Enterprise Server 15 SP6.

The traditional contact protocol is no longer supported in SUSE Manager 5.0 and later. Before migrating from SUSE Manager 4.3 to 5.0, any existing traditional clients including the traditional proxies must be migrated to Salt.

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

Deploy a New SUSE Manager Proxy

Because in-place migration is not supported, the users must deploy a new SUSE Manager proxy with a new FQDN.

For more information about installing SUSE Manager Proxy, see **Installation-and-upgrade › Install-proxy**.

Migrate Clients to the New Proxy

Before migrating the clients, ensure that the new proxy is already deployed and fully functional.

Procedure: Migrating Client Between Proxies

1. Log in to the SUSE Manager Server Web UI.
2. From the left navigation, select **Systems › Systems List**.
3. Navigate to the old 4.3 proxy page, and click the Proxy tab.

4. Select all systems to "SSM".
5. From the left navigation, select **Systems › System Set Manager**.
6. Select the sub-menu **Misc › Proxy**.
7. From the drop-down select the new proxy to migrate to.
8. Click **[Change Proxy]**.

All selected clients will now be migrated to the new proxy. You can check the schedule progress to verify if all clients were successfully migrated.

After a few minutes, the clients will start to show up the new connection path. When all clients have the connection path under the new proxy, the old 4.3 proxy system is not needed anymore and can be removed.

TFTP files synchronization

Containerized proxies do not use tftpsync mechanism to transfer tftproot files. Instead these files are transparently downloaded and cached on demand.

To prevent false positive errors during cobbler sync run, migrated 4.3 proxies need to be removed from tftpsync mechanism.

If you previously configured a 4.3 proxy to receive TFTP files, one of the following configuration option is required:

- In the server container, run configure-tftpsync.sh with the list of remaining 4.3 proxies as arguments. If no 4.3 proxies remain, run configure-tftpsync.sh with no arguments.
- In the server container, manually remove the relevant proxy from the proxies setting in the /etc/cobbler/settings.yaml file. If there are no 4.3 proxies remaining, then manually remove the proxies list completely.

Proxy Upgrade

Before running the upgrade command, it is required to upgrade the mgrpxy tool first.

Procedure: Upgrading Proxy

1. Refresh software repositories with zypper:

```
zypper ref
```

2. Apply available updates:

a. For SLE Micro:

```
transactional-update
```

If updates were applied, reboot.

b. For SUSE Linux Enterprise Server:

```
zypper up
```

3. The SUSE Manager 5.0 Proxy containers running on podman can be updated using the following command:

```
mgrpxy upgrade podman
```

4. Or, those running on a Kubernetes cluster can update using:

```
mgrpxy upgrade kubernetes
```

5. On podman, clean up the unused container images to free disk space:

```
podman image prune -a
```

On Kubernetes the image cleanup is handled automatically, or it depends on the Kubernetes distribution.

If you do not specify the tag parameter when upgrading to specific version, it will default to upgrading to the most recent version. To upgrade to a specific version, provide the tag parameter with the desired image tag.

While there is an option to upgrade a specific container using its specific tag, this feature is intended for applying PTFs only. We highly recommend using the same tag for all proxy containers to ensure consistency under normal circumstances.

For air-gapped installations, first upgrade the container RPM packages, then run the mgrpxy upgrade podman command.

3.3. Clients

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 4. Basic Server and Proxy Management

4.1. 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, as root, run the following command. Entering your server's FQDN is optional.

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

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

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

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

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

4.2. 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
```

4.3. Containers used by SUSE Manager

Below is a list of containers used by SUSE Manager 5.0.

Table 14. Server Containers

Container Name	Description
uyuni-server	Main product container
uyuni-hub-xmlrpc	XML-RPC gateway for Hub deployment

Container Name	Description
uyuni-server-attestation	Server COCO attestation
uyuni-server-migration	Migration helper container

Table 15. Proxy Containers

Container Name	Description
uyuni-proxy-httpd	Main proxy container handling all HTTP communication
uyuni-proxy-squid	Squid cache
uyuni-proxy-salt-broker	Salt forwarder
uyuni-proxy-ssh	SSH forwarder
uyuni-proxy-tftpd	TFTPd to HTTP translator and forwarder

4.4. 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.

Server

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

Table 16. Persistent Volumes: Podman Default Storage

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

Table 17. Persistent Volumes: root

Volume Name	Volume Directory
root	/root

Table 18. Persistent Volumes: var/

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

Table 19. Persistent Volumes: srv/

Volume Name	Volume Directory
srv-salt	/srv/salt
srv-www	/srv/www/
srv-tftpboot	/srv/tftpboot
srv-formulametadata	/srv/formula_metadata
srv-pillar	/srv/pillar
srv-susemanager	/srv/susemanager
srv-spacewalk	/srv/spacewalk

Table 20. 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

Volume Name	Volume Directory
etc-salt	/etc/salt
etc-sssd	/etc/sssd
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

Proxy

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

Table 21. Persistent Volumes: Podman Default Storage

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

Table 22. Persistent Volumes: srv/

Volume Name	Volume Directory
uyuni-proxy-tftpboot	/srv/tftpboot

Table 23. Persistent Volumes: var/

Volume Name	Volume Directory
uyuni-proxy-rhn-cache	/var/cache/rhn
uyuni-proxy-squid-cache	/var/cache/squid

4.5. Understanding mgr-storage-server and mgr-storage-proxy

They are designed to configure storage for SUSE Manager Server and Proxy.

The scripts take disk devices as arguments. mgr-storage-proxy requires a single argument for the storage disk

device. mgr-storage-server requires a storage disk device and can optionally accept a second argument for a dedicated database disk device. While both normal and database storage can reside on the same disk, it is advisable to place the database on a dedicated, high-performance disk to ensure better performance and easier management.

What these tools do

Both mgr-storage-server and mgr-storage-proxy perform standard storage setup operations:

- Validate the provided storage devices.
- Ensure that devices are empty and suitable for use.
- Create XFS filesystems on the specified devices.
- Mount the devices temporarily for data migration.
- Move the relevant storage directories to the new devices.
- Create entries in /etc/fstab so that the storage mounts automatically on boot.
- Remount the devices at their final locations.

Table 24. Additional tool-specific behavior

mgr-storage-server	• Optionally supports a separate device for database storage. • Stops SUSE Manager services during migration, restarts them afterward. • Moves Podman volumes directory /var/lib/containers/storage/volumes to the prepared storage, and optionally /var/lib/containers/storage/volumes/var-pgsql to the prepared database storage.
mgr-storage-proxy	• Focuses only on proxy storage (no database storage support). • Stops and restarts the proxy service during migration. • Moves podman volumes directory /var/lib/containers/storage/volumes to the prepared storage.

Both tools automate standard Linux storage operations. There is no hidden or custom logic beyond what a Linux administrator would do manually.

What these tools do **not** do

- They do **not** create or manage LVM volumes.
- They do **not** configure RAID or complex storage topologies.

- They do **not** prevent you from managing storage using normal Linux tools after setup.
- They do **not** provide dynamic resizing or expansion capabilities — these must be handled using standard Linux storage tools.

Post-installation storage management

Once storage has been configured, you can safely manage it using standard Linux commands.

Examples

Listing 1. Example 1: Extending storage if using LVM

```
lvextend -L +10G /dev/your_vg/your_lv
xfs_growfs /var/lib/containers/storage/volumes
```

Example 2: Migrating to a larger disk

1. Add and format the new disk.
2. Mount it temporarily.
3. Use rsync to copy data.
4. Update /etc/fstab.
5. Remount at the correct location.

When to use, or not use

Always take a backup before making changes to your storage setup.

- Use these tools **only** during initial storage setup or when migrating to new storage where the tool is expected to handle data migration and update /etc/fstab.
- Do **not** rerun these scripts for resizing or expanding storage. Use standard Linux tools (e.g., lvextend, xfs_growfs) for such operations.

Summary

mgr-storage-server and mgr-storage-proxy help automate the initial persistent storage setup for SUSE Manager components using standard Linux storage practices. They do not limit or interfere with standard storage management afterward.

After setup, continue managing your storage using familiar Linux tools.

A full database volume can cause significant issues with system operation. As disk usage

notifications have not yet been adapted for containerized environments, users are encouraged to monitor the disk space used by Podman volumes themselves, either through tools such as Grafana, Prometheus, or any other preferred method. Pay particular attention to the var-pgsql volume, located under /var/lib/containers/storage/volumes/.

Chapter 5. GNU Free Documentation License

Copyright © 2000, 2001, 2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these

sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other

respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
Copyright (c) YEAR YOUR NAME.
   Permission is granted to copy, distribute and/or modify this document
   under the terms of the GNU Free Documentation License, Version 1.2
   or any later version published by the Free Software Foundation;
   with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
   A copy of the license is included in the section entitled "GNU
   Free Documentation License".
```