

SUSE Manager '5.0'

インストールおよびアップグレードガイド

2024年07月12日



目次

Deployment and Upgrade Guide Overview	1
1. 要件	2
1.1. 一般的な要件	2
1.1.1. SUSE Customer Center Account and Credentials	2
1.1.2. Supported Browsers for SUSE Manager Web UI	2
1.1.3. SSL証明書	3
1.2. ハードウェア要件	3
1.2.1. サーバ要件	3
1.2.2. プロキシ要件	4
1.2.3. Database Requirement	5
1.2.4. Persistent Storage and Permissions	5
1.3. ネットワーク要件	7
1.3.1. 完全修飾ドメイン名(FQDN)	7
1.3.2. ホスト名とIPアドレス	7
1.3.3. Air-gapped Deployment	8
1.3.4. Ports	8
1.4. パブリッククラウドの要件	12
1.4.1. ネットワーク要件	12
1.4.2. Prepare Storage Volumes	13
2. インストールと配備	14
2.1. サーバ	14
2.1.1. Deploy SUSE Manager '5.0' Server as a Virtual Machine	14
2.1.2. Deploy SUSE Manager '5.0' Server	19
2.1.3. SUSE Manager Server Air-gapped Deployment	27
2.1.4. SUSE Manager Server and the Public Cloud	28
2.2. プロキシ	28
2.2.1. Deploy SUSE Manager '5.0' Proxy as a Virtual Machine	28
2.2.2. Deploy a SUSE Manager '5.0' Proxy	38
2.2.3. k3sでのコンテナ化されたSUSE Managerプロキシのインストール	47
2.2.4. SUSE Manager Proxy Air-gapped Deployment	51
3. アップグレードと移行	52
3.1. サーバ	52
3.1.1. Migrating the SUSE Manager Server to a Containerized Environment	52
3.1.2. Update Containers	54
3.2. プロキシ	55

3.2.1. Proxy Migration	55
3.2.2. Update Containers.....	56
3.3. クライアント.....	57
3.3.1. クライアントのアップグレード	57
4. 基本的なサーバ管理	58
4.1. Custom YAML Configuration and Deployment with <code>mgradm</code>	58
4.2. Starting and Stopping Containers.....	59
4.3. List of persistent storage volumes	59
5. GNU Free Documentation License	62

Deployment and Upgrade Guide Overview

更新: 2024-07-12

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

要件

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

Deployment

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

アップグレードと移行

Describes upgrade and migration of SUSE Manager

Public Cloud

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

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

Chapter 1. 要件

1.1. 一般的な要件

インストールを始める前に、次の項目を確認してください。

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

The following section contains more information on these requirements.

1.1.1. SUSE Customer Center Account and Credentials

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

Procedure: Obtain Your Organization Credentials

1. Navigate to <https://scc.suse.com/login> in your web browser.
2. SCCアカウントにログインするか、またはプロンプトに従い新しいアカウントを作成します。
3. まだ組織に接続していない場合、[**組織に接続する**]をクリックし、組織を入力または検索します。
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. SUSE Managerの設定中に使用するログイン情報をメモします。

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

SCCの使用の詳細については、<https://scc.suse.com/docs/help>を参照してください。

1.1.2. 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:

- SUSE Linux Enterprise Serverとともに出荷される最新のFirefoxブラウザ
- あらゆるオペレーティングシステム上の最新のChromeブラウザ
- Windowsとともに出荷される最新のEdgeブラウザ

Windows Internet Explorerはサポートされていません。 SUSE ManagerのWeb UIはWindows Internet

Explorerでは正しくレンダリングされません。

1.1.3. SSL証明書

SUSE Managerは、SSL証明書を使用して、クライアントが正しいサーバに登録されていることを確認します。デフォルトでは、SUSE Managerは自己署名証明書を使用します。サードパーティCAによって署名された証明書がある場合、それをSUSE Managerインストール環境にインポートできます。

- 自己署名証明書の詳細については、**Administration** > **Ssl-certs-selfsigned**を参照してください。
- インポートした証明書の詳細については、**Administration** > **Ssl-certs-imported**を参照してください。

1.2. ハードウェア要件

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

SUSE Manager for Retailハードウェアの要件については、**Retail** > **Retail-requirements**を参照してください。

1.2.1. サーバ要件

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

For more information about filesystem and partitioning details, see [installation-and-upgrade:hardware-requirements.pdf](#).

表 1. サーバハードウェアの要件

Hardware	Details	Recommendation
CPU	x86-64, ARM, s390x	Minimum 4 dedicated 64-bit CPU cores
RAM	Minimum	16 GB
	Recommended	32 GB
Disk Space	<code>/</code> (root directory)	Minimum 40 GB
	<code>/var/lib/containers/storage/volumes/var-pgsql</code>	Minimum 50 GB

Hardware	Details	Recommendation
	<code>/var/lib/containers/storage/volumes/var-spacewalk</code>	Minimum storage required: 100 GB (this will be verified by the implemented check) * 50 GB for each SUSE product and Package Hub 360 GB for each Red Hat product
	<code>/var/lib/containers/storage/volumes/var-cache</code>	Minimum 10 GB. Add 100 MB per SUSE product, 1 GB per Red Hat or other product. Double the space if the server is an ISS Master.

SUSE Managerのパフォーマンスは、ハードウェアリソース、ネットワーク帯域幅、クライアントとサーバ間の遅延などによって異なります。

経験および使用されているさまざまな配備に基づいて、適切な数のプロキシを備えたSUSE Managerサーバの最適なパフォーマンスを得るためには、単一サーバあたり10,000クライアントを超えないようにすることをお勧めします。クライアント数が10,000を超える場合は、ハブのセットアップに移行し、コンサルティングを利用することを強くお勧めします。微調整と適切な数のプロキシを使用しても、このような多数のクライアントによって、パフォーマンスの問題が生じる可能性があります。

For more information about managing a large number of clients, see **Specialized-guides > Large-deployments**.

1.2.2. プロキシ要件

表 2. プロキシハードウェア要件

Hardware	Details	Recommendation
CPU	x86-64, ARM	Minimum 2 dedicated 64-bit CPU cores
RAM	Minimum	2 GB
	Recommended	8 GB
Disk Space	<code>/</code> (root directory)	Minimum 40 GB

Hardware	Details	Recommendation
	<code>/var/lib/containers/storage/volumes/srv-www</code>	Minimum 100 GB Storage requirements should be calculated for the number of ISO distribution images, containers, and bootstrap repositories you will use.
	<code>/var/lib/containers/storage/volumes/var-cache</code> (Squid)	Minimum 100 GB

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

この動作の結果は以下のとおりです。

- The larger `/var/lib/containers/storage/volumes/var-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/var-cache/` directory on the proxy the same size as `/var/lib/containers/storage/volumes/var-spacewalk/` on the SUSE Manager Server, you avoid a large amount of traffic after the first synchronization.
- The `/var/lib/containers/storage/volumes/var-cache/` directory can be small on the SUSE Manager Server compared to the proxy. For a guide to size estimation, see the [サーバ要件](#) section.

1.2.3. Database Requirement

PostgreSQLはサポートされている唯一のデータベースです。 PostgreSQLデータベースとともにリモートのPostgreSQLデータベースやリモートのファイルシステム(NFS など)を使用することはサポートされていません。つまり、PostgreSQLは、SUSE Managerで使用可能な最速のストレージデバイス上に存在する必要があります。



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.

このような場合、SUSEは支援を提供できないことがあります。

1.2.4. Persistent Storage and Permissions

Persistent volumes are created by default when deploying the container.

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

Storage devices must be set up prior to deploying the container. For more details, see **Installation-and-**

upgrade › Container-management.

SUSE Managerでは、3つの異なるボリュームが必要です。

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

すべてのボリュームで、ファイルシステムの種類にはXFSを使用することをお勧めします。また、オンプレミスインストールでは、論理ボリューム管理(LVM)を使用してディスクを管理することを検討してください。リポジトリストレージのディスクのサイズは、SUSE Managerで管理するディストリビューションおよびチャンネルの数によって決まります。必要サイズを推測するガイドについては、このセクションの表を参照してください。

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

```
hwinfo --disk | grep -E "デバイスファイル:"
```

`lsblk`コマンドを使用して、各デバイスの名前とサイズを表示します。

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

```
mgr-storage-server <channel_devicename> [<database_devicename>]
```

外部ストレージボリュームは、`/manager_storage`および`/pgsql_storage`にマウントされているXFSパーティションとして設定されます。

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 only takes a single device name parameter and will set up the external storage location as the Squid cache.

SUSE Managerサーバおよびプロキシのディスクパーティションを作成する場合、パーミッションを正しく設定してください。

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

- オーナー: 読み取り、書き込み、実行
- Group: Read, Execute
- ユーザ: なし

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

- オーナー: 読み取り、書き込み、実行
- グループ: 読み取り、書き込み、実行
- ユーザ: 読み取り、実行

次のコマンドでパーミッションを確認してください。

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

出力は次のようになります。

```
/var/lib/containers/storage/volumes/var-pgsql:
total 0
drwxr-x--- 1 10556 10556 48 Apr 19 14:33 _data

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

必要に応じて、次のコマンドでパーミッションを変更します。

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

オーナーでは次のコマンドを使用します。

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

1.3. ネットワーク要件

このセクションでは、SUSE Managerのネットワークとポートの要件について詳しく説明します。

1.3.1. 完全修飾ドメイン名(FQDN)

SUSE Managerサーバは、そのFQDNを正しく解決する必要があります。FQDNを解決できない場合、多数のコンポーネントで重大な問題の原因になる場合があります。

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

1.3.2. ホスト名とIPアドレス

SUSE Managerのドメイン名をそのクライアントで解決できることを確認するには、サーバとクライアントの両方のマシンを動作中のDNSサーバに接続する必要があります。リバース参照が正しく設定されていることも確認する必要があります。

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

1.3.3. Air-gapped Deployment

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

運用環境では、SUSE Managerサーバおよびクライアントはファイアウォールを常に使用する必要があります。必要なポートの一覧は、**Installation-and-upgrade > Ports**を参照してください。

1.3.4. Ports

このセクションには、SUSE Manager内でのさまざまな通信に使用するポートの一覧が記載されています。

これらのポートすべてを開く必要はありません。 サービスの使用に必要なポートのみを開く必要があります。

1.3.4.1. 外部の着信サーバポート

未許可アクセスからサーバを保護するためにSUSE Managerサーバでファイアウォールを設定するには、外部の着信ポートが開いている必要があります。

これらのポートを開くと、外部ネットワークトラフィックがSUSE Managerサーバにアクセスできるようになります。

表 3. SUSE Managerサーバの外部ポートの要件

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

Port number	Protocol	Used By	Notes
4506	TCP	salt	Required to accept communication requests from clients. The client initiates the connection, and it stays open to report results back to the Salt master.
25151	TCP	Cobbler	

1.3.4.2. 外部の送信サーバポート

サーバからアクセスできるアクセス先を制限するためにSUSE Managerサーバでファイアウォールを設定するには、外部の送信ポートが開いている必要があります。

次のポートを開くと、SUSE Managerサーバからのネットワークトラフィックで外部サービスに通信できます。

表 4. SUSE Managerサーバの外部ポートの要件

Port number	Protocol	Used By	Notes
80	TCP	HTTP	Required for SUSE Customer Center. Port 80 is not used to serve the Web UI.
443	TCP	HTTPS	Required for SUSE Customer Center.
25151	TCP	Cobbler	

1.3.4.3. 内部サーバポート

内部ポートは、SUSE Managerサーバによって内部で使用されます。内部ポートはlocalhostのみからアクセスできます。

ほとんどの場合、これらのポートを調整する必要はありません。

表 5. SUSE Managerサーバの内部ポートの要件

ポート番号	注意
2828	サテライト検索APIであり、TomcatとTaskomaticのRHNアプリケーションで使用されます。
2829	Taskomatic APIであり、TomcatのRHNアプリケーションで使用されます。
8005	Tomcatのシャットダウンポート。
8009	TomcatからApache HTTPD (AJP)。
8080	TomcatからApache HTTPD (HTTP)。
9080	Salt-APIであり、TomcatとTaskomaticのRHNアプリケーションで使用されません。

ポート番号	注意
32000	Taskomaticおよびサテライト検索を実行する仮想マシン(JVM)へのTCP接続用のポート。

ポート32768以上は一時ポートとして使用されます。 これらは、TCP接続の受信に最も頻繁に使用されます。 TCP接続リクエストが受信されると、送信元はこれらの一時ポート番号のいずれかを選択して、宛先ポートと照合します。

次のコマンドを使用して、一時ポートであるポートを確認できます。

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

1.3.4.4. 外部の着信プロキシポート

未許可アクセスからプロキシを保護するためにSUSE Managerプロキシでファイアウォールを設定するには、外部の着信ポートが開いている必要があります。

これらのポートを開くと、外部ネットワークトラフィックがSUSE Managerプロキシにアクセスできるようになります。

表 6. SUSE Managerプロキシの外部ポートの要件

Port number	Protocol	Used By	Notes
22			Required for ssh-push and ssh-push-tunnel contact methods. Clients connected to the proxy initiate check in on the server and hop through to clients.
67	TCP/UDP	DHCP	Required only if clients are requesting IP addresses from the server.
69	TCP/UDP	TFTP	Required if the server is used as a PXE server for automated client installation.
443	TCP	HTTPS	Web UI, client, and server and proxy (<code>tftpsync</code>) requests.
4505	TCP	salt	Required to accept communication requests from clients. The client initiates the connection, and it stays open to receive commands from the Salt master.
4506	TCP	salt	Required to accept communication requests from clients. The client initiates the connection, and it stays open to report results back to the Salt master.

1.3.4.5. 外部の送信プロキシポート

プロキシからアクセスできるアクセス先を制限するためにSUSE Managerプロキシでファイアウォールを設定するには、外部の送信ポートが開いている必要があります。

次のポートを開くと、SUSE Managerプロキシからのネットワークトラフィックで外部サービスに通信できます。

表 7. SUSE Managerプロキシの外部ポートの要件

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

1.3.4.6. 外部クライアントポート

SUSE Managerサーバとそのクライアントの間でファイアウォールを設定するには、外部クライアントポートが開いている必要があります。

ほとんどの場合、これらのポートを調整する必要はありません。

表 8. SUSE Managerクライアントの外部ポートの要件

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

1.3.4.7. 必要なURL

クライアントを登録して更新を実行するためにSUSE Managerがアクセスできる必要があるURLがあります。ほとんどの場合、次のURLにアクセスできれば十分です。

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

SUSE以外のクライアントを使用している場合、該当するオペレーティングシステム用の特定のパッケージを

提供するその他のサーバにもアクセスできる必要がある場合があります。たとえば、Ubuntuクライアントがある場合、Ubuntuサーバにアクセスできる必要があります。

SUSE以外のクライアントでファイアウォールアクセスのトラブルシューティングを行う方法の詳細については、**Administration > Troubleshooting**を参照してください。

1.4. パブリッククラウドの要件

このセクションは、パブリッククラウドインフラストラクチャにSUSE Managerをインストールする要件について説明します。Amazon EC2、Google Compute Engine、およびMicrosoft Azureではテストを実施済みですが、若干の差異はあってもその他のプロバイダにも当てはまるはずですが。

始める前に、考慮事項を次に示します。

- SUSE Manager設定プロシージャは、正引きで確認された逆引きDNS参照を実行します。設定プロシージャが完了してSUSE Managerが期待どおりに動作するためには、この参照が成功する必要があります。SUSE Managerを設定する前に、ホスト名とIPの設定を実行することが重要です。
- SUSE Managerサーバとプロキシのインスタンスは、DNSエントリを介した制御を提供するネットワーク設定で実行する必要がありますが、大規模インターネットからはアクセスできません。
- このネットワーク設定内では、DNSの解決を提供する必要があります。`hostname -f`は、完全修飾ドメイン名(FQDN)を返す必要があります。
- DNSの解決は、クライアントを接続するためにも重要です。
- DNSは、選択したクラウドフレームワークに依存しています。詳細な手順については、クラウドプロバイダのドキュメントを参照してください。
- 外部仮想ディスクでソフトウェアリポジトリ、サーバデータベース、およびプロキシsquidキャッシュを探すことをお勧めします。こうすることによって、インスタンスが予期せず終了した場合のデータ損失が防止されます。このセクションでは、外部仮想ディスクの設定方法の手順について説明します。

1.4.1. ネットワーク要件

パブリッククラウドでSUSE Managerを使用するとき、制約のあるネットワークを使用する必要があります。適切なファイアウォール設定でVPCプライベートサブネットを使用することをお勧めします。指定したIP範囲にあるマシンのみがインスタンスにアクセスできる必要があります。



パブリッククラウド上でSUSE Managerを実行するという事は、堅牢なセキュリティ対策を実装することを意味します。インスタンスへのアクセスを制限、フィルタ、監視、監査することが不可欠です。SUSEは、適切な境界セキュリティが欠如しているグローバルにアクセス可能なSUSE Managerインスタンスを使用しないことを強くお勧めします。

SUSE ManagerのWeb UIにアクセスするには、ネットワークアクセス制御を設定するときにHTTPSを許可します。そうすると、SUSE ManagerのWeb UIにアクセスできます。

EC2およびAzureでは、新しいセキュリティグループを作成し、HTTPSの着信および受信のルールを追加します。GCEでは、**[ファイアウォール]** セクションで **[HTTPSトラフィックを許可する]** ボックスにチェック

を付けます。

1.4.2. Prepare Storage Volumes

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

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



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

リポジトリストレージのディスクのサイズは、SUSE Managerで管理するディストリビューションおよびチャンネルの数によって決まります。仮想ディスクを接続すると、Unixデバイスノードとしてインスタンスに表示されます。デバイスノードの名前は、選択インスタンスの種類とプロバイダによって異なります。

SUSE Managerサーバのルートボリュームが100 GB以上であることを確認してください。500 GB以上のストレージディスクを追加し、可能な場合にはSSDストレージを選択します。SUSE Managerサーバのクラウドイメージは、スクリプトを使用して、インスタンス起動時にこの個別ボリュームを割り当てます。

インスタンスを起動すると、SUSE Managerサーバにログインし、次のコマンドを使用して、利用可能なすべてのストレージデバイスを検索できます。

```
hwinfo --disk | grep -E "デバイスファイル:"
```

選択したデバイスがわからない場合、`lsblk`コマンドを使用して、各デバイスの名前およびサイズを確認します。探している仮想ディスクのサイズと一致している名前を選択します。

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>
```

ストレージボリュームおよびパーティションの設定(推奨最小サイズを含む)の詳細については、[Installation-and-upgrade > Hardware-requirements](#)を参照してください。

Chapter 2. インストールと配備

2.1. サーバ

2.1.1. Deploy SUSE Manager '5.0' Server as a Virtual Machine

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.



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.

2.1.1.1. Available Images

Images for SUSE Manager '5.0' are available at [SUSE Manager '5.0' VM images](#).



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>

表 9. 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.

2.1.1.2. 仮想マシンマネージャ(virt-manager)の設定

virt-manager を使用して、新しい仮想マシンを作成するときに、次の設定を入力します。



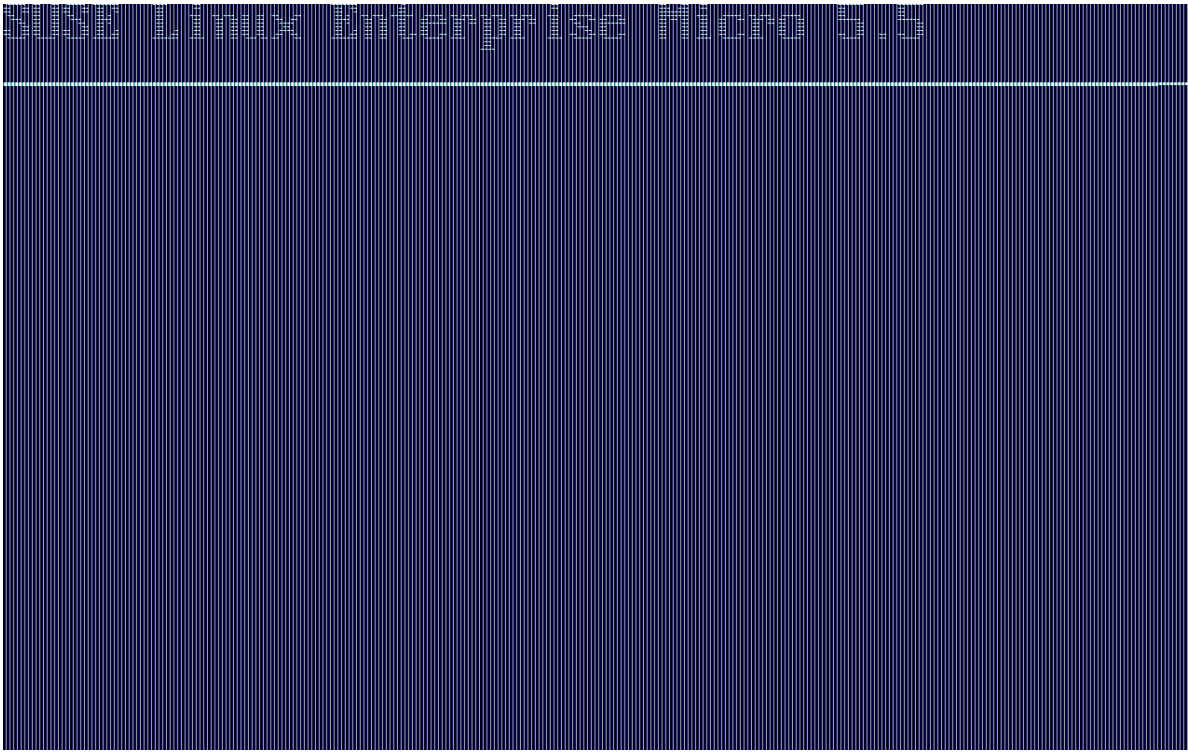
次の表では、最低要件を指定しています。 これらは、1つのクライアントがあるサーバなど、クイックテストインストールに適しています。 運用環境を使用する場合、[Installation-and-upgrade > Hardware-requirements](#)にリストされている要件を確認してください。

KVM Settings	
Installation Method	Import Existing Disk Image
OS:	Linux
Version:	SUSE Manager-Server.x86_64-5.0.0-Build16.10.qcow2
Memory:	16 GB
CPU' s:	4
Storage Format:	.qcow2 100 GB (Default) Root Partition
Name:	test-setup
Network	Bridge br0

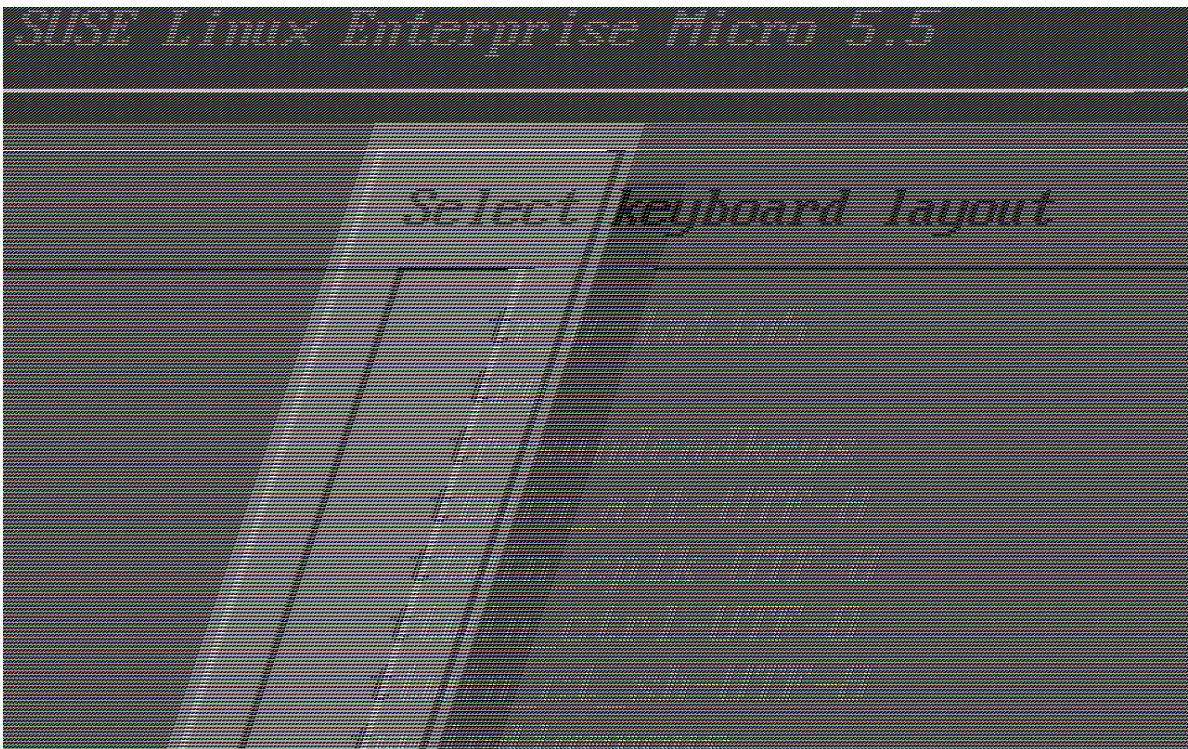
2.1.1.3. Initial KVM Setup

Procedure: Creating Initial Setup

1. ダウンロードしたMinimal KVMイメージを使用して新しい仮想マシンを作成し、**[Import existing disk image]**（既存のディスクイメージをインポート）を選択します。
2. Configure RAM and number of CPUs (at least 16 GB RAM and 4 CPUs).
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.



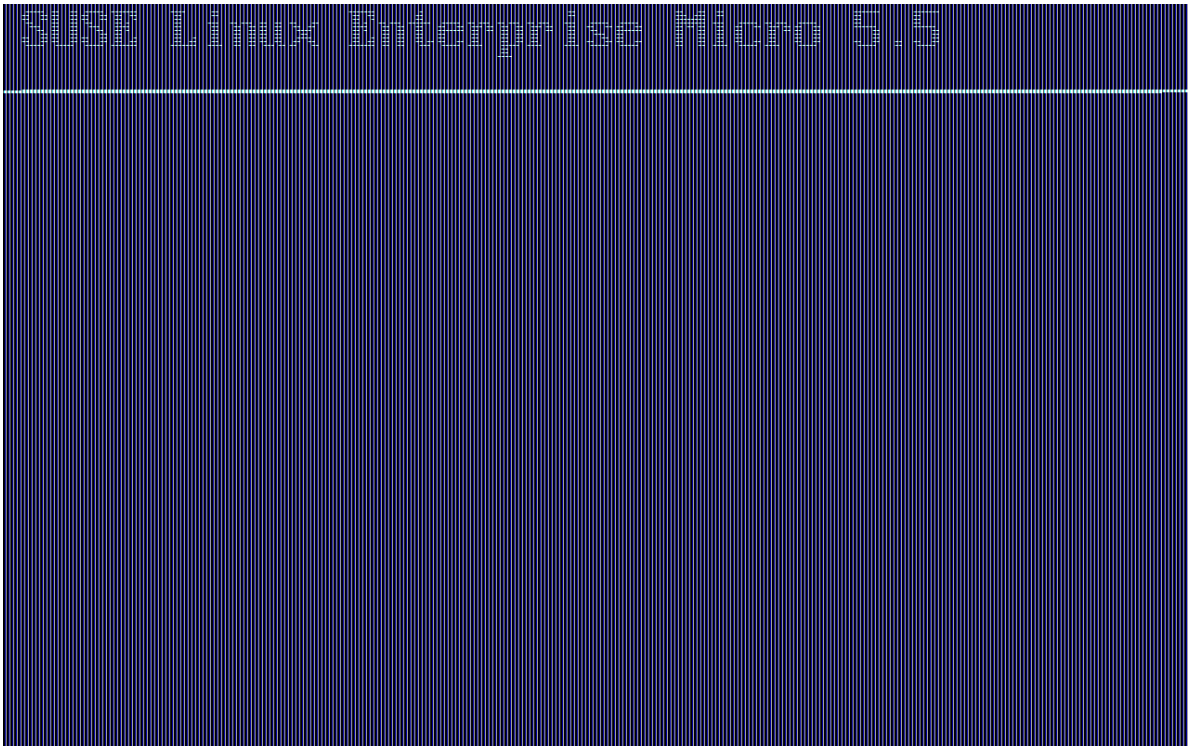
7. Accept the license agreement.



8. Select your time zone.



9. Enter a password for root.

A screenshot of the SUSE Linux Enterprise Micro 5.0 boot screen. The text "SUSE Linux Enterprise Micro 5.0" is displayed in a monospaced font at the top of the screen. The background is a dark blue/black color with a light blue/white grid pattern.

10. Once installation completes login as root.
11. Proceed to the next section.

2.1.1.4. Register SL Micro and SUSE Manager '5.0' Server

Procedure: Registering SL Micro and SUSE Manager '5.0'

1. Boot the virtual machine.
2. `root`としてログインします。
3. Register SL Micro with SCC.

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

4. 再起動します。
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**.

10. Otherwise run the following command to deploy SUSE Manager:

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

2.1.2. Deploy SUSE Manager '5.0' Server

This guide shows you how to install and configure a SUSE Manager '5.0' container on SLE Micro 5.5.

2.1.2.1. 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.

表 10. ソフトウェアおよびハードウェアの要件

Software and Hardware	Recommended
Operating System:	SLE Micro 5.5
Architecture	x86-64, ARM, s390x, ppc64le
Processor: (CPU)	Minimum of four (4) 64-bit CPU cores
RAM:	16 GB
Disk Space:	200 GB

Software and Hardware	Recommended
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.

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**.

2.1.2.2. 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. Since 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**.

2.1.2.3. SLE Micro 5.5 Installation

Procedure: Download the Installation Media

1. Locate the SLE Micro 5.5 installation media at <https://www.suse.com/download/sle-micro/>.
2. You will need an account with SUSE Customer Center and must be logged in to download the ISO image.
3. Download `SLE-Micro-5.5-DVD-x86_64-GM-Media1.iso`.
4. Prepare a DVD or USB flash drive for installation.
5. Insert the DVD or USB flash drive (USB disk or key) containing the installation image for SLE Micro 5.5.
6. Boot or reboot your system.

For more information about preparing your machines (virtual or physical), see [SLE Micro 5.5 Deployment Guide](#).

Procedure: SLE Micro 5.5 Installation

1. Use the arrow keys to select **Installation**.
2. Adjust keyboard and language.
3. Click the **checkbox** to accept the license agreement.
4. Click **Next** to continue.
5. Select the registration method. For this example, we will register the server with SUSE Customer Center.

Registering SUSE Manager as an Extension during Installation

The SUSE Manager '5.0' container is installed as an extension. Therefore, in addition to acquiring SUSE Customer Center registration codes for SLE Micro 5.5, you will also need SUSE Customer Center registration codes for the following extensions:



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

The following section uses a registration code for the x86-64 architecture. To register ARM or s390x architectures replace with the correct registration code.

6. Enter your SUSE Customer Center email address.
7. Enter your registration code for SLE Micro 5.5.
8. Click **Next** to continue.
9. On the **Extension and Module Selection** page, uncheck the **Hide Development Versions** checkbox.
10. Select the SUSE Manager '5.0' Server extension **Checkbox**.
11. Click **Next** to continue.
12. Enter your SUSE Manager '5.0' Server extension registration code.
13. [次へ]をクリックして続行します。
14. On the **NTP Configuration** page click [**Next**].
15. On the **Authentication for the System** page enter a password for the root user. Click [**Next**].
16. On the **Installation Settings** page click [**Install**].

This concludes installation of SLE Micro 5.5 and SUSE Manager '5.0' as an extension.

2.1.2.3.1. Registration from the Command Line (Optional)

If you added SUSE Manager '5.0' as an extension during SLE Micro 5.5 installation then you can skip this step. However, optionally you may skip registration during SLE Micro 5.5 installation by selecting the [**Skip Registration**] button. This section provides steps on registering your products after SLE Micro 5.5 installation.

Procedure: Post Installation Product Registration

1. Register SLE Micro 5.5 to SUSE Customer Center from the command line run the following commands on the container host:

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

2. Use the registration code you obtained from your SUSE Customer Center account for SLE Micro 5.5.



The following section uses a registration code for the x86-64 architecture. To register ARM or s390x architectures replace it with the correct registration code.

3. Next add the **SUSE Manager Server Extension 5.0 x86_64 (Beta)** Extension. List available extensions with the following command:

```
transactional-update --quiet register --list-extensions
```

4. Use your **SUSE Manager Server Extension 5.0 x86_64** registration code with the following command:

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

5. 再起動します。

2.1.2.3.2. Update the system

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

```
transactional-update
```

3. 再起動します。

2.1.2.3.3. Configure Custom Persistent Storage

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

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

+ Use the command in the following manner:

+

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

+ For example:

+

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

+



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

For more information, see [Installation-and-upgrade › Container-management](#).

2.1.2.4. Deploy with mgradm

Procedure: Deploy 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 a certificate and administrator account password when prompted.



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

4. Press **[Enter]**.
5. 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.



SLE Micro is designed to update itself automatically by default and will reboot after applying updates. However, this behavior is not desirable for the SUSE Manager environment. To prevent automatic updates on your server, we recommend disabling the transactional-update timer.

You can disable the timer by running the following command:

```
systemctl disable --now transactional-update.timer
```

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.

2.1.2.5. Connect SUSE Manager '5.0' to SUSE Customer Center

このセクションでは、Web UIからSCCと同期を取り、最初のクライアントチャンネルを追加する方法について説明します。

プロシージャ: 組織の資格情報の入力

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. [セッアップウィザード] ページから、[組織の資格情報] タブを選択します。
5. [Add a new credential] (新しい資格情報の追加) をクリックします。
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 [プロシージャ: SUSE Customer Centerとの同期](#).

プロシージャ: SUSE Customer Centerとの同期

1. Web UIで、**管理** > **セッアップウィザード**に移動します。
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**.

The screenshot shows the 'Setup Wizard' interface for 'SUSE Products'. It features a table with the following columns: Product Description, Arch, and Channels. The table lists various SUSE products, including Open Enterprise Server 2018, RHEL Expanded Support 5 and 6, SUSE Container as a Service Platform 1.0 and 2.0, and SUSE Linux Enterprise Desktop 11, 12, and 15. The 'SUSE Linux Enterprise Desktop 15' product is highlighted in green and shows a progress bar at 100%. To the right of the table, there is a sidebar with a 'Refresh' button and a section titled 'Why aren't all SUSE products displayed in the list?' which explains that products are linked to organization credentials and subscriptions.

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](#).

2.1.2.6. Entering the container for management

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

```
mgrctl term
```

2.1.3. SUSE Manager Server Air-gapped Deployment

2.1.3.1. What is air-gapped deployment?

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

2.1.3.2. 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](#).

2.1.3.3. 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

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. 再起動します。
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](#).

2.1.4. SUSE Manager Server and the Public Cloud

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

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

2.2. プロキシ

2.2.1. Deploy SUSE Manager '5.0' Proxy as a Virtual Machine

This chapter provides the 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.



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

2.2.1.1. Available Images

Images for SUSE Manager '5.0' are available at [SUSE Manager '5.0' VM images](#).

表 11. Available Proxy Images

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

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>

2.2.1.2. 仮想マシンマネージャ(virt-manager)の設定

virt-manager を使用して、新しい仮想マシンを作成するときに、次の設定を入力します。

次の表では、最低要件を指定しています。 これらは、1つのクライアントがあるサーバなど、クイックテストインストールに適しています。 運用環境を使用する場合、**Installation-and-upgrade > Hardware-requirements** にリストされている要件を確認してください。

2.2.1.3. Hardware Requirements for the Proxy

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

KVM Settings	
Installation Method	Import Existing Disk Image
OS:	Linux
Version:	SUSE Manager-Proxy.x86_64-5.0.0-Build16.12.qcow2
Memory:	2 GB
CPU' s:	2
Storage Format:	.qcow2 40 GB (Default) Root Partition
Name:	test-setup
Network	Bridge br0

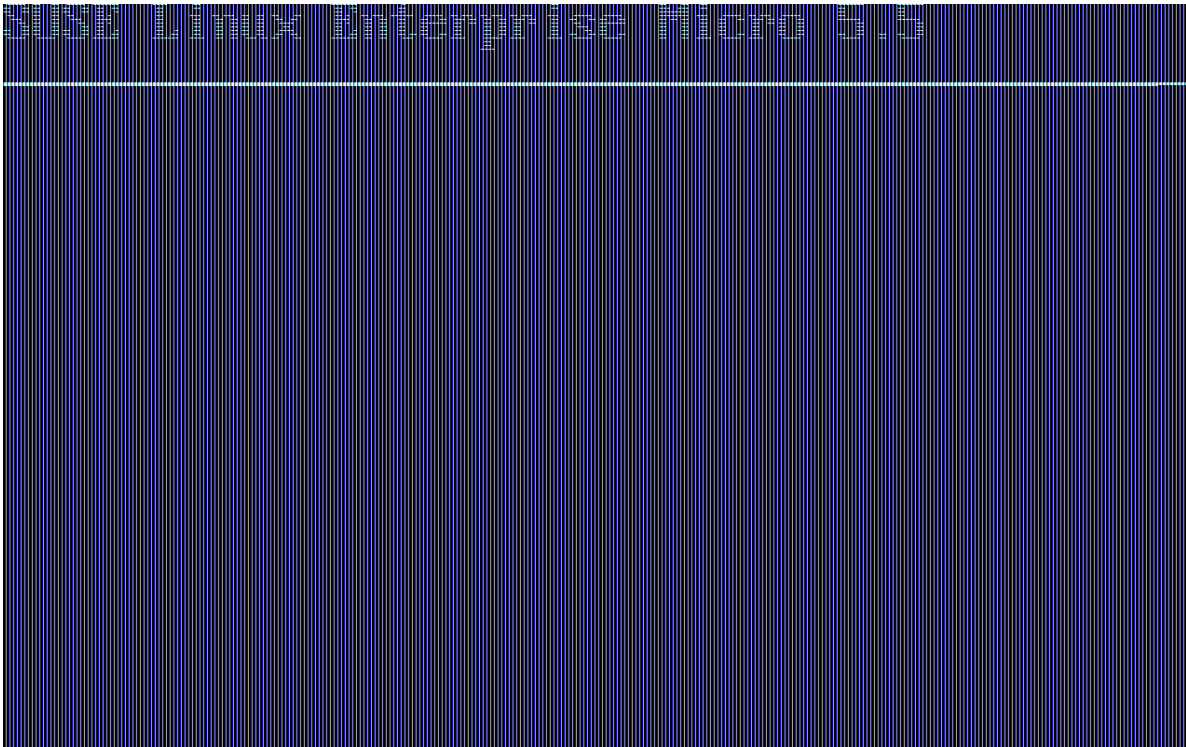
`/var/lib/containers/storage/volumes/srv-www` Minimum 100 GB, Storage requirements should be calculated for the number of ISO distribution images, containers, and bootstrap repositories you will use.

`/var/lib/containers/storage/volumes/var-cache` (Squid) Minimum 100 GB

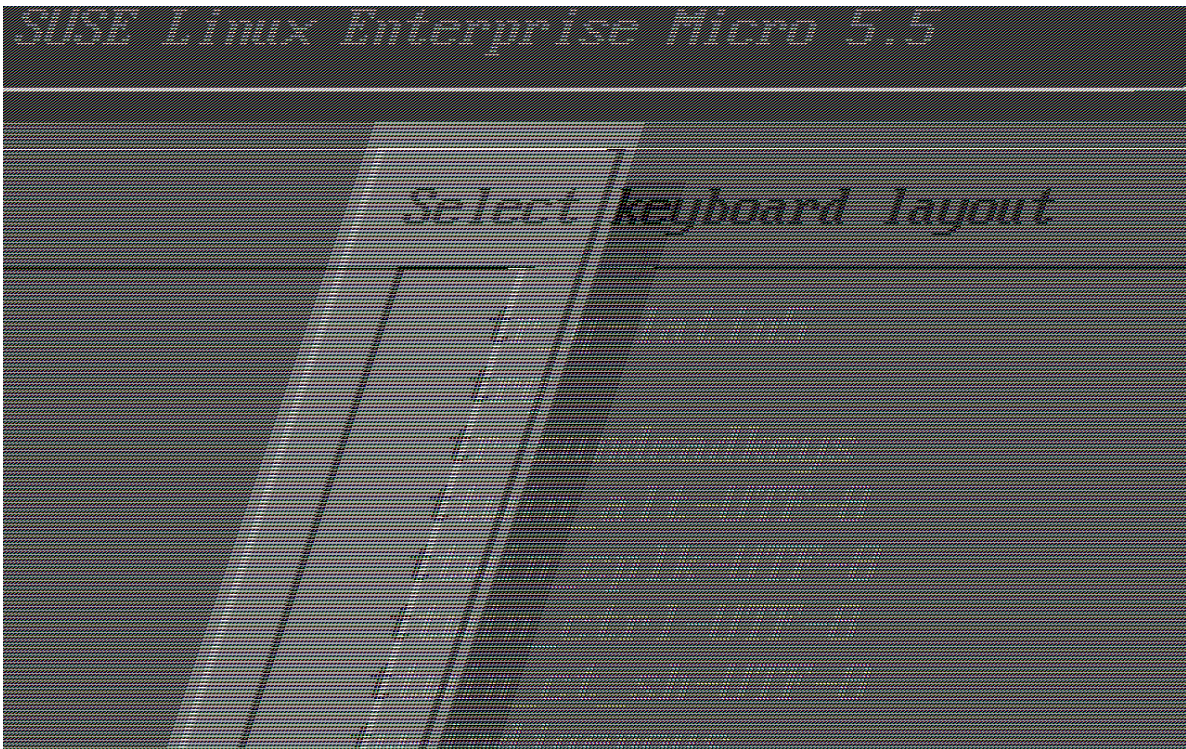
2.2.1.4. Initial KVM Setup

Procedure: Creating Initial Setup

1. ダウンロードしたMinimal KVMイメージを使用して新しい仮想マシンを作成し、`[Import existing disk image]`（既存のディスクイメージをインポート）を選択します。
2. Configure RAM and number of CPUs (at least 16 GB RAM and 4 CPUs).
3. KVMマシンに名前を付け、`[Customize configuration before install]`（インストール前に設定をカスタマイズ）チェックボックスを選択します。
4. Click `[Begin Installation]` to boot from the image.
5. At the JeOS Firstboot screen select start to continue.



6. Select keyboard layout.



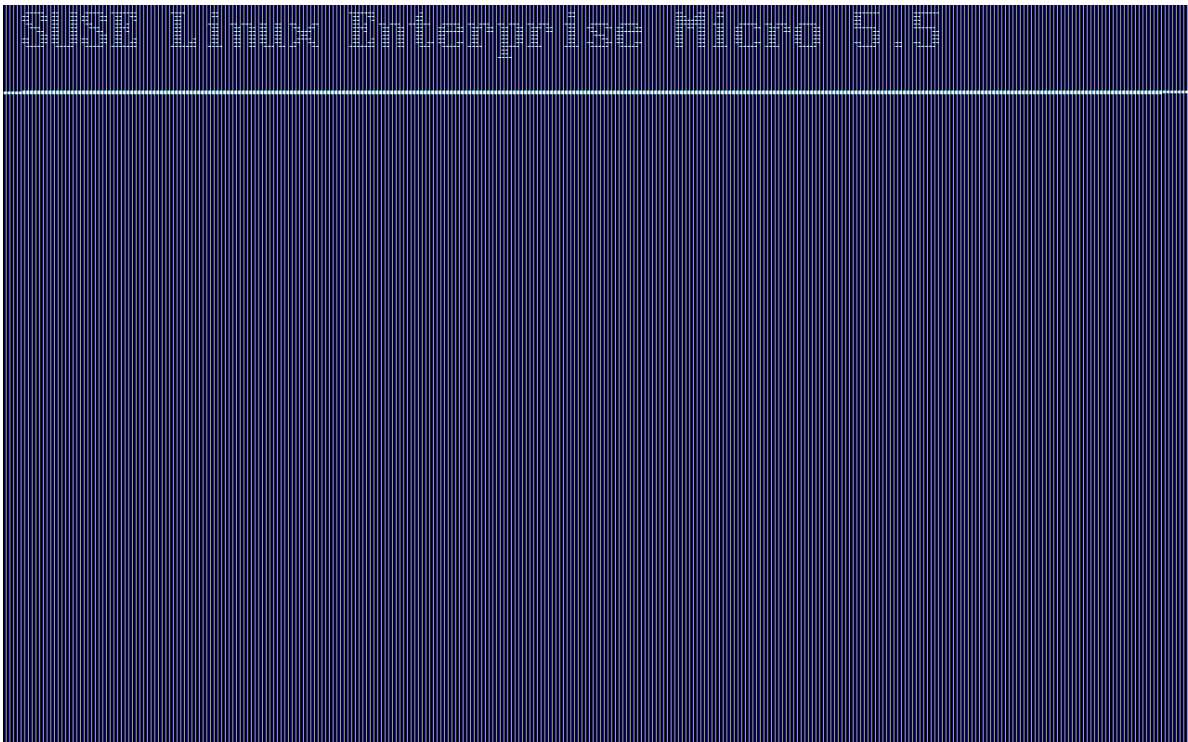
7. Accept the license agreement.



8. Select your time zone.



9. Enter a password for root.



10. Once installation completes login as root.
11. Proceed to the next section.

2.2.1.5. Register SL Micro and SUSE Manager '5.0'

Procedure: Registering SL Micro and SUSE Manager '5.0' Proxy

1. Boot the virtual machine.
2. `root`としてログインします。
3. Register SL Micro with SCC.

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

4. 再起動します。
5. Register SUSE Manager '5.0' with SUSE Customer Center.

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

6. 再起動します。
7. Update the system:

```
transactional-update
```

8. If updates were applied reboot.

2.2.1.6. Create an Activation Key for the Proxy

On the SUSE Manager server, create an activation key for the Proxy.

Task: Create an Activation Key

1. Navigate to **Systems** > **Activation Keys**, and click [**Create key**].
2. Create an activation key for the proxy host with SL Micro 5.5 as the parent channel. This key should include all recommended channels and the Proxy as an extension child channel.
3. Proceed to bootstrapping the proxy host as a minion.

2.2.1.7. Bootstrap the Proxy Host

Task: Bootstrap the Proxy Host

1. Select **Systems** > **Bootstrapping**.
2. Fill in the fields for your proxy host.
3. Select the Activation key created in the previous step from the dropdown.
4. Click [**Bootstrap**].
5. Wait for the Bootstrap process to complete successfully. Check the **Salt** menu and confirm the Salt key is listed and accepted.

6. Reboot the proxy host.
7. Select the host from the **System** list and trigger a second reboot after all events are finished to conclude the onboarding.

Task: Update the Proxy Host

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

2.2.1.8. Generate the Proxy Configuration

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



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



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

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

2.2.1.8.1. Generate the Proxy Configuration with Web UI

Procedure: Generating a Proxy Container Configuration using Web UI

1. Web UIで、**システム > プロキシの設定**に移動し、必要なデータを入力します。
2. **[プロキシFQDN]** フィールドに、プロキシの完全修飾ドメイン名を入力します。
3. **[親FQDN]** フィールドに、SUSE Managerサーバまたは別のSUSE Managerプロキシの完全修飾ドメイン名を入力します。
4. **[プロキシSSHポート]** フィールドに、SSHサービスがSUSE ManagerプロキシでリスンしているSSHポートを入力します。デフォルトの8022を維持することをお勧めします。
5. In the **Max Squid cache size [MB]** field type maximal allowed size for Squid cache. Recommended is to use at most 60% of available storage for the containers.



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



[SSL証明書] 選択リストで、SUSE Managerプロキシ用に新しいサーバ証明書を生成するか、既存のサーバ証明書を使用するかを選択します。生成された証明書は、SUSE Manager組み込みの(自己署名)証明書と見なすことができます。

+ 選択に応じて、新しい証明書を生成するための署名CA証明書へのパス、またはプロキシ証明書として使用される既存の証明書とそのキーへのパスのいずれかを指定します。

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

+ 既存の証明書またはカスタム証明書、および企業証明書と中間証明書の概念の詳細については、**Administration** > **Ssl-certs-imported**を参照してください。

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

 Container Based Proxy Configuration 

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

Proxy FQDN *:

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

Proxy SSH port:
Port range: 1 - 65535

Max Squid cache size (MB) *:

Proxy administrator email *:


SSL certificate *: Create Use existing

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

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

The CA private key password *:

SSL Certificate data

Alternate CNAMES 

2-letter country code:

State:

City:

Organization:

Organization Unit:

Email:

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

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

You can generate a Proxy configuration using spacecmd.

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

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

3. Copy the generated configuration from the server container:

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

2.2.1.8.3. Generate the Proxy Configuration with spacecmd and Custom Certificate

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

Procedure: Generating Proxy Configuration with spacecmd and Custom Certificate

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

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

3. Copy the generated configuration from the server container:

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

2.2.1.9. Configure Custom Persistent Storage

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

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

+ Use the command in the following manner:

+

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

+ For example:

+

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

+



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

For more information, see [Installation-and-upgrade > Container-management](#).

2.2.1.10. Transfer the Proxy Configuration

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

Procedure: Copying the Proxy Configuration

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

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

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

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

3. Install the Proxy with:

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

2.2.1.11. Start the SUSE Manager '5.0' Proxy

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

Procedure: Start and Check Proxy Status

1. Start the Proxy by calling:

```
mgrpky start
```

2. Check container status by calling:

```
mgrpky status
```

5つのSUSE Managerプロキシコンテナが存在する必要があります。

- proxy-salt-broker

- proxy-httpd
- proxy-tftpd
- proxy-squid
- proxy-ssh

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

2.2.1.11.1. 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`.

たとえば、次のように使用します。

```
mgrpky 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:

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

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

2.2.2. Deploy a SUSE Manager '5.0' Proxy

This guide outlines the deployment process for the SUSE Manager '5.0' Proxy. 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:

Task: Proxy Deployment

1. Review hardware requirements.
2. Synchronize the SLE Micro 5.5 parent channel and the proxy extension child channel on the server.
3. Install SLE Micro 5.5 on a bare-metal machine.
4. During the installation, register SLE Micro 5.5 along with the SUSE Manager '5.0' 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 is SLE Micro 5.5.

Container host



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

2.2.2.1. Hardware Requirements for the Proxy

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

表 12. プロキシハードウェア要件

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

2.2.2.2. Sync 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 Servers 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.

Setup Wizard

HTTP Proxy Organization Credentials **Products** PAYG Connections

Clear + Add products

micro 25 items per page

x86_64 Items 1 - 6 of 6 Select All

Product Description	Arch	Channels
<input type="checkbox"/> > SUSE Linux Enterprise Micro 5.0 x86_64	x86_64	<input checked="" type="checkbox"/> include recommended
<input type="checkbox"/> > SUSE Linux Enterprise Micro 5.1 x86_64	x86_64	<input checked="" type="checkbox"/> include recommended
<input type="checkbox"/> > SUSE Linux Enterprise Micro 5.2 x86_64	x86_64	<input checked="" type="checkbox"/> include recommended
<input type="checkbox"/> > SUSE Linux Enterprise Micro 5.3 x86_64	x86_64	<input checked="" type="checkbox"/> include recommended
<input type="checkbox"/> > SUSE Linux Enterprise Micro 5.4 x86_64	x86_64	<input checked="" type="checkbox"/> include recommended
<input checked="" type="checkbox"/> > SUSE Linux Enterprise Micro 5.5 x86_64	x86_64	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> > SUSE Manager Client Tools for SLE Micro 5 x86_64 <small>recommended</small>		<input checked="" type="checkbox"/>
<input type="checkbox"/> > SUSE Manager Retail Branch Server Extension 5.0 x86_64 (BETA)		
<input type="checkbox"/> > SUSE Package Hub 15 SP5 x86_64		
<input type="checkbox"/> > SUSE Manager Server Extension 5.0 x86_64 (BETA)		
<input type="checkbox"/> > SUSE Linux Enterprise Live Patching 15 SP5 x86_64		
<input checked="" type="checkbox"/> > SUSE Manager Proxy Extension 5.0 x86_64 (BETA)		<input checked="" type="checkbox"/>

Page 1 of 1

📌 1. SUSE Manager '5.0' Channel Sync for Proxy

Task: Sync 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 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 checkbox then use the drop-down to select the **SUSE Manager Proxy Extension 5.0 x86_64 BETA** extension.
5. Click the **[Add products]** button.
6. Wait for the synchronization to complete.

2.2.2.3. SLE Micro 5.5 Installation

Task: Download the Installation Media

1. Locate the SLE Micro 5.5 installation media at <https://www.suse.com/download/sle-micro/>.
2. You will need an account with SUSE Customer Center and must be logged in to download the ISO.

3. Download [SLE-Micro-5.5-DVD-x86_64-GM-Media1.iso](#).
4. Prepare a USB flash disk or DVD for installation.
5. Insert a DVD or a bootable USB stick containing the installation image for SLE Micro 5.5.
6. Boot or reboot your system.

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

Task: SLE Micro 5.5 Installation

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



SUSE Manager '5.0' Proxy as an extension

The SUSE Manager '5.0' Proxy is registered as an extension. Therefore, in addition to acquiring an SUSE Customer Center registration key for SLE Micro 5.5, you will also need an SUSE Customer Center registration code for the following extension:

- SUSE Manager '5.0' Proxy

5. Enter your SUSE Customer Center Email address.
6. Enter your registration code for SLE Micro 5.5.
7. Click **Next** to continue.
8. On the **Extension and Module Selection** page uncheck the **Hide Development Versions** checkbox.
9. Select the SUSE Manager '5.0' Proxy extension **Checkbox**.
10. Click **Next** to continue.
11. Enter your SUSE Manager '5.0' Proxy extension registration code.
12. [**次へ**]をクリックして続行します。
13. On the **NTP Configuration** page click [**Next**].
14. On the **Authentication for the System** page enter a password for the root user. Click [**Next**].
15. On the **Installation Settings** page click [**Install**].

This finalizes installation of SLE Micro 5.5 and SUSE Manager '5.0' Proxy as an extension.

2.2.2.3.1. Update the System

Task: Update the System

1. Login as **root**.
2. Run **transactional-update**:

```
transactional-update
```

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



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

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

6. Reboot the system.

2.2.2.3.2. Configure Custom Persistent Storage

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

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

+ Use the command in the following manner:

+

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

+ For example:

+

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

+



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

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

2.2.2.4. Create an Activation Key for the Proxy

Task: Create an Activation Key

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

2.2.2.5. Bootstrap the Proxy Host as a Client

Task: Bootstrap the Proxy Host

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

Task: Update the Proxy Host

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

2.2.2.6. Generate the Proxy Configuration

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



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



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

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

2.2.2.6.1. Generate the Proxy Configuration with Web UI

Procedure: Generating a Proxy Container Configuration using Web UI

1. Web UIで、**システム** > **プロキシの設定**に移動し、必要なデータを入力します。
2. [**プロキシFQDN**] フィールドに、プロキシの完全修飾ドメイン名を入力します。
3. [**親FQDN**] フィールドに、SUSE Managerサーバまたは別のSUSE Managerプロキシの完全修飾ドメイン名を入力します。
4. [**プロキシSSHポート**] フィールドに、SSHサービスがSUSE ManagerプロキシでリスンしているSSHポートを入力します。デフォルトの8022を維持することをお勧めします。
5. In the **Max Squid cache size [MB]** field type maximal allowed size for Squid cache. Recommended is to use at most 60% of available storage for the containers.



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

[**SSL証明書**] 選択リストで、SUSE Managerプロキシ用に新しいサーバ証明書を生成するか、既存のサーバ証明書を使用するかを選択します。生成された証明書は、SUSE Manager組み込みの(自己署名)証明書と見なすことができます。

+ 選択に応じて、新しい証明書を生成するための署名CA証明書へのパス、またはプロキシ証明書として使用される既存の証明書とそのキーへのパスのいずれかを指定します。

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

+ 既存の証明書またはカスタム証明書、および企業証明書と中間証明書の概念の詳細については、**Administration** > **Ssl-certs-imported**を参照してください。

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

Container Based Proxy Configuration ?

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

Proxy FQDN *:

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

Proxy SSH port:
Port range: 1 - 65535

Max Squid cache size (MB) *:

Proxy administrator email *:

SSL certificate *: Create Use existing

CA certificate to use to sign the SSL certificate in PEM format *:

CA private key to use to sign the SSL certificate in PEM format *:

The CA private key password *:

SSL Certificate data

Alternate CNAMES

2-letter country code:

State:

City:

Organization:

Organization Unit:

Email:

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

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

You can generate a Proxy configuration using spacecmd.

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

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

3. Copy the generated configuration from the server container:

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

2.2.2.6.3. Generate the Proxy Configuration with spacecmd and Custom Certificate

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

Procedure: Generating Proxy Configuration with spacecmd and Custom

Certificate

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

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

3. Copy the generated configuration from the server container:

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

2.2.2.7. Transfer the Proxy Configuration

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

Task: Copy the Proxy Configuration

1. Copy the configuration archive (config.tar.gz) generated in the previous step to the Proxy host:

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

2. Install the Proxy with:

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

2.2.2.8. Start the SUSE Manager '5.0' Proxy

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

Task: Start and Check Proxy Status

1. Start the Proxy by calling:

```
mgrpky start
```

2. Check container status by calling:

```
mgrpky status
```

5つのSUSE Managerプロキシコンテナが存在する必要があります。

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

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

2.2.2.8.1. Using 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`.

たとえば、次のように使用します。

```
mgrpky 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:

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

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

2.2.3. k3sでのコンテナ化されたSUSE Managerプロキシのインストール

2.2.3.1. k3sのインストール



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 -
```

2.2.3.2. Installing tools

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

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



Containersモジュールがhelmをインストールするために必要です。

1. To install them run:

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

2. Reboot

2.2.3.3. Generate the Proxy Configuration

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



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



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

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

2.2.3.3.1. Generate the Proxy Configuration with Web UI

Procedure: Generating a Proxy Container Configuration using Web UI

1. Web UIで、**システム > プロキシの設定**に移動し、必要なデータを入力します。
2. **[プロキシFQDN]** フィールドに、プロキシの完全修飾ドメイン名を入力します。
3. **[親FQDN]** フィールドに、SUSE Managerサーバまたは別のSUSE Managerプロキシの完全修飾ドメイン名を入力します。
4. **[プロキシSSHポート]** フィールドに、SSHサービスがSUSE ManagerプロキシでリスンしているSSHポートを入力します。デフォルトの8022を維持することをお勧めします。
5. In the **Max Squid cache size [MB]** field type maximal allowed size for Squid cache. Recommended is to use at most 60% of available storage for the containers.



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



[SSL証明書] 選択リストで、SUSE Managerプロキシ用に新しいサーバ証明書を生成するか、既存のサーバ証明書を使用するかを選択します。生成された証明書は、SUSE Manager組み込みの(自己署名)証明書と見なすことができます。

+ 選択に応じて、新しい証明書を生成するための署名CA証明書へのパス、またはプロキシ証明書として使用される既存の証明書とそのキーへのパスのいずれかを指定します。

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

+ 既存の証明書またはカスタム証明書、および企業証明書と中間証明書の概念の詳細については、**Administration** > **Ssl-certs-imported**を参照してください。

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

 Container Based Proxy Configuration 

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

Proxy FQDN *:

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

Proxy SSH port:
Port range: 1 - 65535

Max Squid cache size (MB) *:

Proxy administrator email *:


SSL certificate *: Create Use existing

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

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

The CA private key password *:

SSL Certificate data

Alternate CNAMES 

2-letter country code:

State:

City:

Organization:

Organization Unit:

Email:

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

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

You can generate a Proxy configuration using spacecmd.

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

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

3. Copy the generated configuration from the server container:

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

2.2.3.3.3. Generate the Proxy Configuration with spacecmd and Custom Certificate

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

Procedure: Generating Proxy Configuration with spacecmd and Custom Certificate

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

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

3. Copy the generated configuration from the server container:

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

2.2.3.4. SUSE Manager プロキシhelmチャートの配備

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:

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

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

2.2.4. SUSE Manager Proxy Air-gapped Deployment

2.2.4.1. What is air-gapped deployment?

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

2.2.4.2. 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](#).

2.2.4.3. 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. 再起動します。
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. アップグレードと移行

3.1. サーバ

3.1.1. Migrating the SUSE Manager Server to a Containerized Environment

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

An in-place migration from SUSE Manager 4.3 to 5.0 will remain unsupported because of the change of the underlying operating system from SUSE Linux Enterprise Server 15 SP4 to SLE Micro 5.5.



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 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>.

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 **after migration**:

1. Copy the keys from the source server to the container host of the destination server.
2. Add the keys to the container with `mgradm gpg add ...`.

The current migration procedure does not include functionality for renaming hostnames. As a result, the fully qualified domain name (FQDN) of the destination server will remain the same as that of the source server. Additionally, the IP address must remain unchanged to ensure that the minions can contact the server. Consequently, after the migration, it will be necessary to manually update the DHCP and DNS records to point to the new server.

3.1.1.1. Initial Preparation on the Old 4.3 Server

Procedure: Initial preparation on the 4.3 server

1. Stop the SUSE Manager services:

```
spacewalk-service stop
```

2. Stop the PostgreSQL service:

```
systemctl stop postgresql
```

3.1.1.2. Prepare the SSH Connection

Procedure: Preparing the SSH connection

1. The SSH configuration and agent should be ready on the new '5.0' server for a passwordless connection to the 4.3 server.



To establish a passwordless connection, the migration script relies on an SSH agent running on the '5.0' server. If the agent is not active yet, initiate it by running `eval $(ssh-agent)`. Then, add the SSH key to the running agent with `ssh-add /path/to/the/private/key`. You will be prompted to enter the password for the private key during this process.

2. The migration script only uses the 4.3 server's FQDN in the SSH command.
3. This means that every other configuration required to connect, needs to be defined in the `~/.ssh/config` file.

3.1.1.3. 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 your current setup. This includes, but is not limited to, **Memory (RAM)**, **CPU Cores**, **Storage**, **Network Bandwidth**, etc.

Procedure: Performing the Migration

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**.

1. Execute the following command to install a new SUSE Manager server, replacing `<oldserver.fqdn>` with the appropriate FQDN of the 4.3 server:

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

Trusted SSL CA certificates that were installed as part of an RPM and store 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 migration**:



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

```
mgradm 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 Fully Qualified Domain Name and IP address as 4.3 server.

3.1.2. Update Containers

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

1. One can do so by running the following command:

```
transactional-update
```

2. If updates were applied, `reboot`.
3. The SUSE Manager '5.0' 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.

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. プロキシ

3.2.1. 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 due to the HostOS change from SUSE Linux Enterprise Server 15 SP4 to SLE Micro 5.5.

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 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>

3.2.1.1. 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 [Deploy Proxy as a Virtual Machine](#).

3.2.1.2. 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 system 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 on [**Change Proxy**].
9. After this action, minions will be migrated to the new proxy.
10. You can check the schedule progress to verify if all systems were successfully migrated.

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

3.2.2. Update Containers

Before running the upgrade command, it is recommended to upgrade the `mgrpky` tool first.

1. One can do so by running the following command:

```
transactional-update
```

2. If updates were applied, `reboot`.
3. The SUSE Manager '5.0' Proxy containers running on `podman` can be updated using the following command:

```
mgrpky upgrade podman
```

Those running on a Kubernetes cluster can update using:

```
mgrpky upgrade kubernetes
```



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.



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 `mgradm` command.

3.3. クライアント

3.3.1. クライアントのアップグレード

クライアントは、基盤となるオペレーティングシステムのバージョン設定システムを使用します。 SUSEオペレーティングシステムを使用するクライアントの場合、SUSE ManagerのWeb UI内でアップグレードを実行できます。

クライアントのアップグレードの詳細については、[Client-configuration](#) > [Client-upgrades](#)を参照してください。

Chapter 4. 基本的なサーバ管理

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. List of persistent storage volumes

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

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



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

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

表 13. Persistent Volumes: Podman Default Storage

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

表 14. Persistent Volumes: root

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

表 15. Persistent Volumes: var/

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

表 16. Persistent Volumes: srv/

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

表 17. Persistent Volumes: etc/

Volume Name	Volume Directory
etc-apache2	<code>/etc/apache2</code>

4.3. List of persistent storage volumes

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

Chapter 5. GNU Free Documentation License

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

0. PREAMBLE

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

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

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

1. APPLICABILITY AND DEFINITIONS

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

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

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

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

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

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

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

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

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

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

2. VERBATIM COPYING

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

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

3. COPYING IN QUANTITY

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

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

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

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

4. MODIFICATIONS

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

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

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

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

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

5. COMBINING DOCUMENTS

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

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

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

6. COLLECTIONS OF DOCUMENTS

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

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

7. AGGREGATION WITH INDEPENDENT WORKS

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

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

8. TRANSLATION

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

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

9. TERMINATION

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

10. FUTURE REVISIONS OF THIS LICENSE

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

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

ADDENDUM: How to use this License for your documents

Copyright (c) YEAR YOUR NAME.

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