

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11月18日



目次

配備およびアップグレードガイドの概要	1
1. 要件	2
1.1. 一般的な要件	2
1.1.1. SUSE Customer Centerアカウントと資格情報	2
1.1.2. SUSE Manager Web UIでサポートされているブラウザ	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. データベースの要件	5
1.2.4. 永続ストレージとパーミッション	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	8
1.3.3. Air-gapped配備	8
1.3.4. ポート	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. ストレージボリュームの準備	13
2. インストールと配備	15
2.1. サーバ	15
2.1.1. 仮想マシンとしてのSUSE Manager '5.0' サーバの配備 - KVM	15
2.1.2. SUSE Manager '5.0' サーバの仮想マシンとしての配備 - VMware	20
2.1.3. SUSE Manager '5.0' サーバの配備	23
2.1.4. SUSE ManagerサーバのAir-gapped配備	31
2.1.5. SUSE Managerサーバとパブリッククラウド	32
2.2. プロキシ	32
2.2.1. 仮想マシンとしてのSUSE Manager '5.0' プロキシの配備	32
2.2.2. SUSE Manager '5.0' プロキシの配備	42
2.2.3. k3sへのコンテナ化されたSUSE Managerプロキシのインストール	51
2.2.4. SUSE ManagerプロキシのAir-gapped配備	54
3. アップグレードと移行	56
3.1. サーバ	56
3.1.1. コンテナ化された環境へのSUSE Managerサーバの移行	56
3.1.2. コンテナの更新	59

3.2. プロキシ	59
3.2.1. プロキシの移行	59
3.2.2. コンテナの更新	61
3.3. クライアント	61
3.3.1. クライアントのアップグレード	61
4. 基本的なサーバ管理	62
4.1. YAMLのカスタム設定とmgradmを使用した配備	62
4.2. コンテナの起動と停止	63
4.3. 永続ストレージボリュームのリスト	63
5. GNU Free Documentation License	66

配備およびアップグレードガイドの概要

Version: '5.0'

このドキュメントではSUSE Managerサーバおよびプロキシを配備およびアップグレードするガイダンスを提供します。ガイダンスは、次のセクションに分かれています。

要件

インストールを開始する前に、ハードウェア、ソフトウェア、ネットワークの要件について説明します。

配備

コンテナとしてのSUSE Managerの配備および初期セットアップのタスクについて説明します。

アップグレードと移行

SUSE Managerのアップグレードと移行について説明します

パブリッククラウド

SUSE Managerをパブリッククラウドのインスタンスに配備することもできます。

パブリッククラウドでのSUSE Managerの使用の詳細については、[Specialized-guides](#) > [Public-cloud-guide](#)を参照してください。

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. SUSE Customer Centerアカウント。このアカウントにより、組織の資格情報と、SLE Micro 5.5およびSUSE Managerのサーバとプロキシの登録キーにアクセスできます。
2. SUSE Manager Web UIでサポートされるブラウザ。
3. 環境のSSL証明書。デフォルトでは、SUSE Manager '5.0' は自己署名証明書を使用します。

次のセクションでは、これらの要件について詳しく説明します。

1.1.1. SUSE Customer Centerアカウントと資格情報

SUSE Manager '5.0' を配備する前に、SUSE Customer Centerでアカウントを作成します。

プロシージャ: 組織の資格情報を取得する

1. Webブラウザで <https://scc.suse.com/login> にアクセスします。
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. **[組織を管理する]** をクリックし、組織名をクリックして一覧から組織を選択します。
5. **[ユーザ]** タブをクリックし、**[組織の資格情報]** サブタブを選択します。
6. SUSE Managerの設定中に使用するログイン情報をメモします。

組織の設定によっては、左側のナビゲーションバーから**[サブスクリプションをアクティブ化する]**メニューを使用してサブスクリプションをアクティブ化する必要が生じる場合もあります。

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. SUSE Manager Web UIでサポートされているブラウザ

Web UIを使用してSUSE Manager環境を管理するには、最新のWebブラウザを実行する必要があります。

SUSE Managerは以下のブラウザでサポートされています。

- SUSE Linux Enterprise Serverに付属する最新の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に付属する最新の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

以下の表は、x86-64、ARM、およびs390xアーキテクチャのSUSE Managerサーバおよびプロキシのハードウェアとソフトウェアの要件を説明しています。

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

SLE Micro 5.5はコンテナホストのオペレーティングシステムであり、空きディスク容量として以下が必要です。

- ベースインストール用に100 GB以上
- およびリポジトリデータ用に130 GB以上

デフォルトでは、SUSE Managerサーバコンテナはパッケージを `/var/lib/containers/storage/volumes/var-spacewalk/` ディレクトリに保存します。このディレクトリのディスク容量がなくなるとリポジトリの同期に失敗します。ミラーリングするクライアントおよびリポジトリに基づいて、`/var/lib/containers/storage/volumes/var-spacewalk/` ディレクトリが必要とする容量を推測します。

ファイルシステムとパーティションの詳細については、[installation-and-upgrade:hardware-requirements.pdf](#)およびこのガイドのインストールと配備のセクションにある詳細なインストール手順を参照してください。

表 1. サーバハードウェアの要件

ハードウェア	詳細	推奨
CPU	x86-64、ARM、またはs390x	専用64ビットCPUコア数は4つ以上
RAM	最小	16 GB
	推奨	32 GB
ディスク容量	/ (ルートディレクトリ)	20 GB
	<code>/var/lib/containers/storage/volumes/var-pgsq1</code>	50 GB以上

ハードウェア	詳細	推奨
	<code>/var/lib/containers/storage/volumes/var-spacewalk</code>	必要な最小ストレージ: 100GB (これは、実装されたチェック機能によって確認されます) * 各SUSE製品およびPackage Hubでは50GB 各Red Hat製品に360 GB
	<code>/var/lib/containers/storage/volumes/var-cache</code>	10 GB以上。SUSE製品あたり100 MB、Red Hatまたは他の製品あたり1 GBを追加します。サーバをサーバ間同期(ISS)に使用する場合は、容量を倍増することを検討してください。

これらのイメージにはデフォルトで20 GBの/`パーティション`があります。SLE Micro 5.5のクラウドイメージの/`パーティション`は5 GB程度です。どちらもSUSE Managerで問題なく動作します。外部ストレージを/`var/lib/containers/storage/volumes`にマウントする限り、SUSE Managerは/`パーティション`上のストレージを必要とせず、使用することはありません。その管理はコンテナホスト自体に任されています。

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。

多数のクライアント管理の詳細については、[Specialized-guides](#) > [Large-deployments](#)を参照してください。

1.2.2. プロキシ要件

表 2. プロキシのハードウェア要件

ハードウェア	詳細	推奨
CPU	x86-64、ARM	専用64ビットCPUコア数は2つ以上
RAM	最小	2 GB
	推奨	8 GB
ディスク容量	/ (ルートディレクトリ)	40 GB以上

ハードウェア	詳細	推奨
	<code>/var/lib/containers/storage/volumes/srv-www</code>	100 GB以上 ストレージ要件は、使用するISOディストリビューションイメージ、コンテナ、およびブートストラップリポジトリの数に合わせて計算する必要があります。
	<code>/var/lib/containers/storage/volumes/var-cache</code> (Squid)	100 GB以上

デフォルトでは、SUSE Managerプロキシコンテナは、`/var/lib/containers/storage/volumes/var-cache/`ディレクトリにパッケージをキャッシュします。容量が不足している場合、プロキシは、使用されていない古いパッケージを削除し、新しいパッケージに置き換えます。

この動作の結果は以下のとおりです。

- プロキシ上の `/var/lib/containers/storage/volumes/var-cache/`ディレクトリの容量を大きくすると、プロキシとSUSE Managerサーバ間のトラフィックが少なくなります。
- プロキシ上の`/var/lib/containers/storage/volumes/var-cache/`ディレクトリをSUSE Managerサーバ上の`/var/lib/containers/storage/volumes/var-spacewalk/`と同じサイズにすることで、最初に同期した後のトラフィック量の増大が防止されます。
- `/var/lib/containers/storage/volumes/var-cache/`ディレクトリは、SUSE Managerサーバ上ではプロキシと比べて小さくできます。サイズの推定のガイドについては、[サーバ要件](#)のセクションを参照してください。

1.2.3. データベースの要件

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。



パフォーマンスの問題が発生する可能性があるため、PostgreSQLデータベースをSUSE Managerからリモートで実行することは推奨されません。このような環境は可能であり、さらには多くの場合安定していますが、何か問題が発生した場合、データ損失のリスクが常にあります。

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. 永続ストレージとパーミッション

永続ボリュームは、コンテナの配備時にデフォルトで作成されます。

ただし、リポジトリとSUSE Managerのデータベースは、別のストレージデバイスに保存することをお勧め

します。このようなセットアップにすると、運用環境でのデータの損失が防止されます。

ストレージデバイスはコンテナを配備する前にセットアップする必要があります。詳細については、[Installation-and-upgrade > Container-management](#)を参照してください。

SUSE Managerでは、3つの異なるボリュームが必要です。

- データベースボリューム: `/var/lib/containers/storage/volumes/var-pgsql`
- チャンネルボリューム: `/var/lib/containers/storage/volumes/var-spacewalk`
- キャッシュ: `/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。

SUSE Managerサーバで、次のコマンドを使用して、利用できるすべてのストレージデバイスを検索します。

```
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。

`mgr-storage-server`コマンドにデバイス名を付けて、データベースおよびリポジトリの場所として外部デバイスを設定します。

```
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。

チャンネルデータとデータベースの両方に同じストレージデバイスを使用できます。これはお勧めしません。その理由は、チャンネルリポジトリが大きくなると、ストレージがいっぱいになり、データベースの一貫性が損なわれるリスクが生じるためです。別々のストレージデバイスを使用すると、パフォーマンスが向上する場合があります。1つのストレージデバイスを使用する場合、1つのデバイス名パラメータを指定して`mgr-storage-server`を実行します。

プロキシをインストールしている場合、`mgr-storage-proxy`コマンドはデバイス名パラメータを1つだけ取り、外部ストレージの場所をSquidキャッシュとして設定します。

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。

`/var/lib/containers/storage/volumes/var-pgsql`の場合:

- オーナー: 読み取り、書き込み、実行

- グループ: 読み取り、実行
- ユーザ: なし

`/var/lib/containers/storage/volumes/var-spacewalk`の場合:

- 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。

ホスト名とDNSの設定の詳細については、<https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-network.html#sec-network-yast-change-host>を参照してください。

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。

DNSサーバの設定の詳細については、<https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-dns.html>を参照してください。

1.3.3. Air-gapped配備

社内ネットワーク上で操作していて、SUSE Customer Centerにアクセスできない場合、**Installation-and-upgrade** > **Container-deployment**を使用できます。

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. ポート

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

ポート番号	プロトコル	使用元	注意
22			ssh-pushおよびssh-push-tunnelの接続メソッドに必要です。
67	TCP/UDP	DHCP	クライアントがサーバからIPアドレスをリクエストしている場合のみ必要です。
69	TCP/UDP	TFTP	自動化されたクライアントのインストールのためにサーバがPXEサーバとして使用されている場合に必要です。
80	TCP	HTTP	一部のブートストラップリポジトリおよび自動化されたインストールのために一時的に必要です。

ポート番号	プロトコル	使用元	注意
443	TCP	HTTPS	Web UI、クライアント、およびサーバとプロキシ(<code>tftpsync</code>)のリクエストを処理します。
4505	TCP	salt	クライアントからの通信リクエストを受け入れるために必要です。クライアントは、接続を開始し、開いたままになり、Saltマスタからのコマンドを受信します。
4506	TCP	salt	クライアントからの通信リクエストを受け入れるために必要です。クライアントは、接続を開始し、開いたままになり、Saltマスタに結果を返します。
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

ポート番号	プロトコル	使用元	注意
80	TCP	HTTP	SUSE Customer Centerで必要です。ポート80はWeb UIを操作するためには使用されません。
443	TCP	HTTPS	SUSE Customer Centerで必要です。
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。

ポート番号	注意
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。
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

ポート番号	プロトコル	使用元	注意
22			ssh-pushおよびssh-push-tunnelの接続メソッドに必要です。プロキシに接続されているクライアントは、サーバへのチェックインを開始し、クライアントにホップします。
67	TCP/UDP	DHCP	クライアントがサーバからIPアドレスをリクエストしている場合のみ必要です。
69	TCP/UDP	TFTP	自動化されたクライアントのインストールのためにサーバがPXEサーバとして使用されている場合に必要です。
443	TCP	HTTPS	Web UI、クライアント、およびサーバとプロキシ(tftpsync)のリクエストを処理します。

ポート番号	プロトコル	使用元	注意
4505	TCP	salt	クライアントからの通信リクエストを受け入れるために必要です。クライアントは、接続を開始し、開いたままになり、Saltマスタからのコマンドを受信します。
4506	TCP	salt	クライアントからの通信リクエストを受け入れるために必要です。クライアントは、接続を開始し、開いたままになり、Saltマスタに結果を返します。

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

ポート番号	プロトコル	使用元	注意
80			サーバにアクセスするために使用します。
443	TCP	HTTPS	SUSE Customer Centerで必要です。

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

ポート番号	方向	プロトコル	注意
22	着信	SSH	ssh-pushおよびssh-push-tunnelの接続メソッドに必要です。
80	送信		サーバまたはプロキシにアクセスするために使用します。
9090	送信	TCP	Prometheusユーザインターフェースに必要です。
9093	送信	TCP	Prometheus警告マネージャに必要です。
9100	送信	TCP	Prometheusノードエクスポートに必要です。
9117	送信	TCP	Prometheus Apacheエクスポートに必要です。

ポート番号	方向	プロトコル	注意
9187	送信	TCP	Prometheus PostgreSQLに必要です。

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。
- 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キャッシュは外部仮想ディスクに配置する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に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を使用する場合は、制限付きのネットワークを使用する必要があります。

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. ストレージボリュームの準備

リポジトリとSUSE Managerのデータベースは、ルートボリュームとは別のストレージデバイスに保存することをお勧めします。こうするとデータの損失が防止され、パフォーマンスが向上する可能性があります。

SUSE Managerコンテナはデフォルトのストレージの場所を利用します。これらの場所は、カスタムストレージ用の配備前に設定する必要があります。詳細については、**Installation-and-upgrade** > **Container-management**を参照してください



パブリッククラウドへのインストールでは論理ボリューム管理(LVM)を使用しないでください。

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。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。

```
hwdisk --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。

`mgr-storage-server`コマンドを使用して外部ディスクを設定できます。設定すると、XFSパーティションが`/manager_storage`にマウントされ、データベースおよびリポジトリの場所として使用されます。


```
/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. 仮想マシンとしてのSUSE Manager '5.0' サーバの配備 - KVM

この章では、SUSE Manager '5.0' をイメージとして配備するために必要な仮想マシン設定について説明します。このインストールでは、KVMを仮想マシンマネージャ(virt-manager)と組み合わせてサンドボックスとして使用します。

2.1.1.1. 利用可能なイメージ



SUSE Manager '5.0' サーバを配備するために推奨される方法は、利用可能な次のイメージの1つを使用することです。これらのイメージにはすべてのツールが含まれており、配備が大幅に容易になります。

SUSE Manager '5.0' のイメージは[SUSE Manager '5.0' VM images](#)で入手できます。



生イメージの準備の詳細については、以下を参照してください。

- <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>

セルフインストールイメージの詳細については、以下を参照してください。

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

表 9. 利用可能なサーバイメージ

アーキテクチャ	イメージの形式
aarch64	qcow2、vmdk
x86_64	qcow2、vmdk、raw、セルフインストーラ
ppc64le	raw、セルフインストーラ
s390x *	qcow2、raw

* s390xでは、CDL DASDとFBAの2つのストレージオプションが利用可能です。

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。



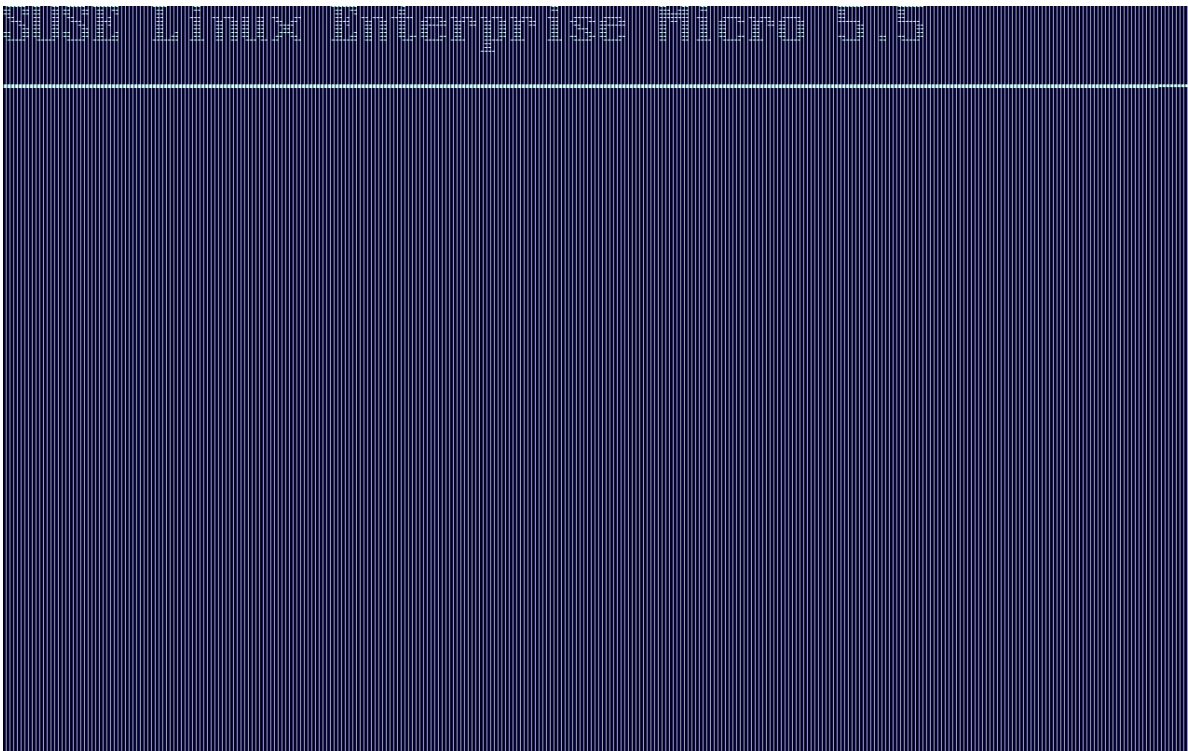
次の表は、最低要件を指定しています。これらは、クライアントが1つある1つのサーバなど、テスト用の簡易的なインストールに適しています。運用環境を使用する場合、特にディスク容量に関する背景情報が必要な場合は、**Installation-and-upgrade Hardware-requirements**を参照してください。

KVMの設定	
インストール方法	既存のディスクイメージのインポート
OS:	Linux
バージョン:	SUSE Manager-Server.x86_64-5.0.0-Build16.10.qcow2
メモリ:	16 GB
CPU数:	4
ストレージフォーマット:	.qcow2 100GB (デフォルト)ルートパーティション
名前:	test-setup
ネットワーク	Bridge br0

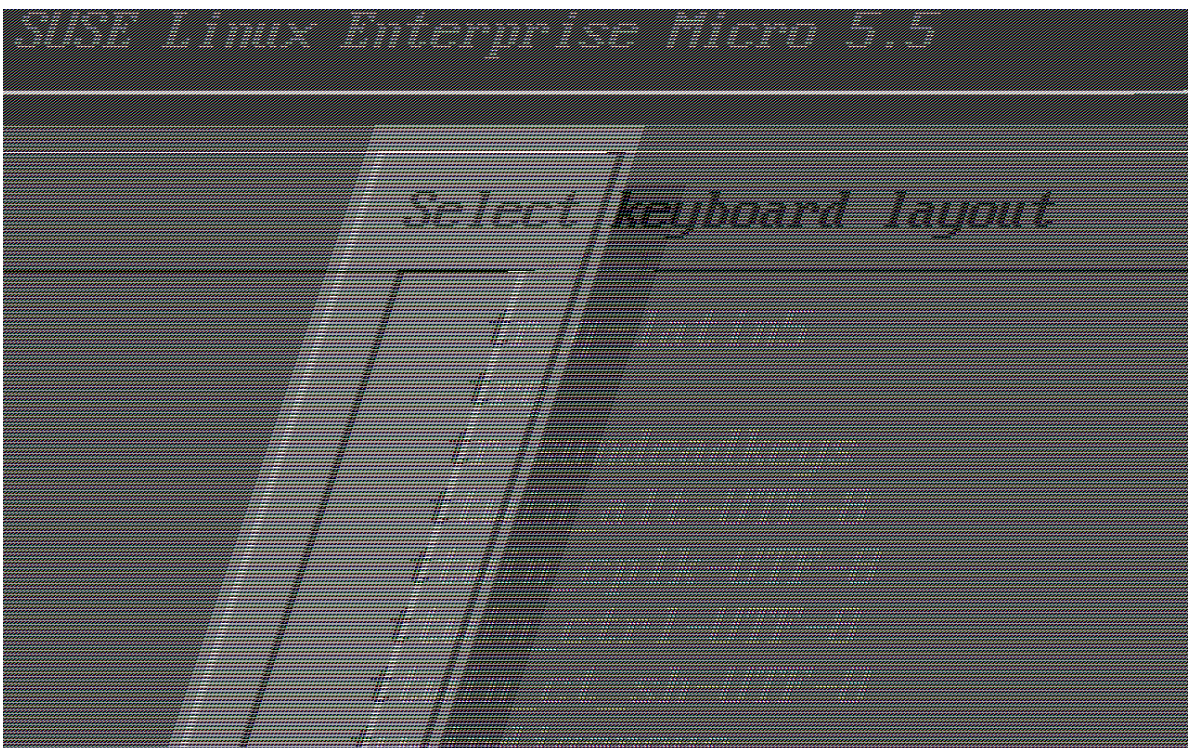
2.1.1.3. KVMの初期セットアップ

プロシージャ: 初期セットアップを作成する

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. RAMおよびCPU数を設定します(少なくとも16GBのRAMおよび4つのCPU)。
3. KVMマシンに名前を付けます。
4. **[Begin Installation]** (インストールの開始) をクリックし、イメージからブートします。
5. **[JeOS Firstboot]** の画面で、**[Start]** を選択して続行します。



6. キーボードレイアウトを選択します。



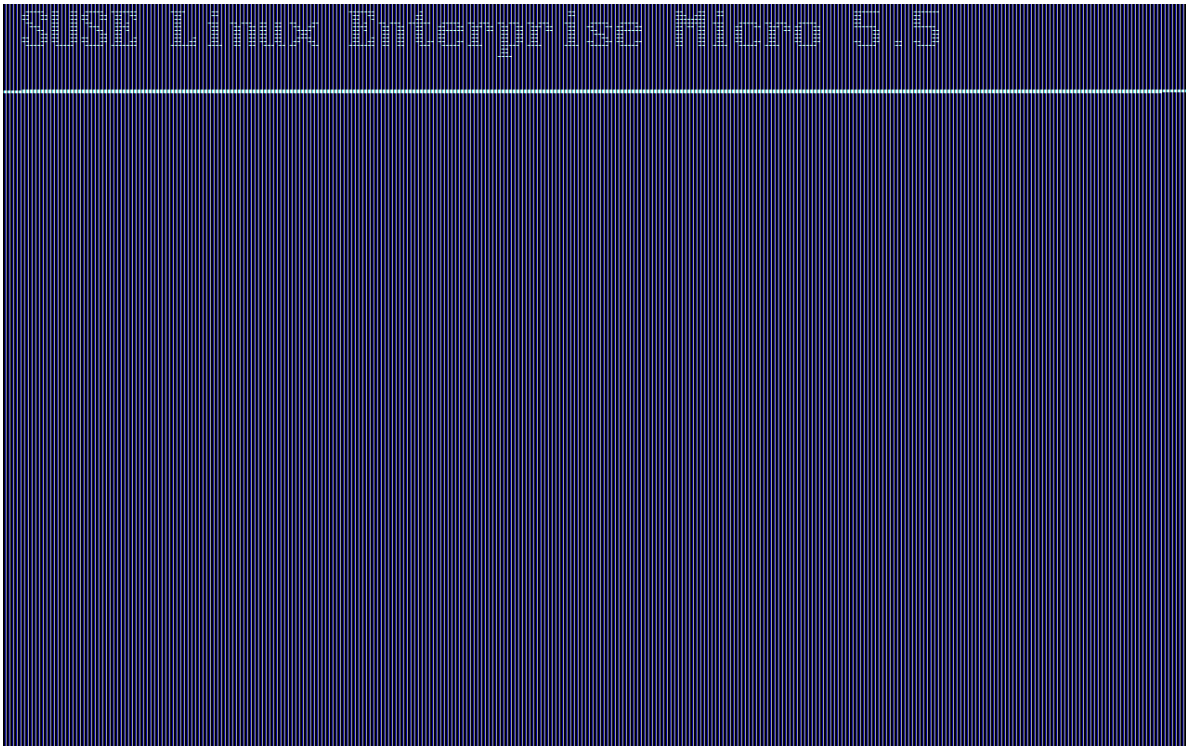
7. ライセンス契約に同意します。



8. タイムゾーンを選択します。



9. rootのパスワードを入力します。

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 dark with a light-colored grid pattern.

10. インストールが完了したら、rootとしてログインします。
11. 次のセクションに進みます。

2.1.1.4. SL MicroおよびSUSE Manager '5.0' サーバの登録

プロシージャ: SL MicroおよびSUSE Manager '5.0' を登録する

1. 仮想マシンをブートします。
2. `root`としてログインします。
3. SCCでSL Microを登録します。

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

4. 再起動します。
5. SUSE Customer CenterでSUSE Manager '5.0' を登録します。

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

6. 再起動
7. システムを更新します。

```
transactional-update
```

8. 更新が適用されていた場合は再起動します。

9. このステップはオプションです。ただし、ご使用のインフラストラクチャでカスタム永続ストレージが必要な場合は、`mgr-storage-server` ツールを使用します。詳細については、`mgr-storage-server --help` を参照してください。このツールを使用すると、コンテナストレージとデータベースボリュームの作成が容易になります。

- このコマンドは次のように使用します。

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

例:

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

このコマンドは、`/var/lib/containers/storage/volumes` に永続ストレージを作成します。



詳細については、以下を参照してください。

- [Installation-and-upgrade > Container-management](#)
- [Administration > Troubleshooting](#)

10. 次のコマンドを実行してSUSE Managerを配備します。

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

2.1.2. SUSE Manager '5.0' サーバの仮想マシンとしての配備 - VMware

この章では、SUSE Manager '5.0' をイメージとして配備するために必要な仮想マシン設定について説明します。このインストールでは、VMwareをサンドボックスとして使用します。

2.1.2.1. 利用可能なイメージ



SUSE Manager '5.0' サーバを配備するために推奨される方法は、利用可能な次のイメージの1つを使用することです。これらのイメージにはすべてのツールが含まれており、配備が大幅に容易になります。

SUSE Manager '5.0' のイメージは [SUSE Manager '5.0' VM images](#) で入手できます。

生イメージの準備の詳細については、以下を参照してください。



- <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>

セルフインストールイメージの詳細については、以下を参照してください。

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

表 10. 利用可能なサーバイメージ

アーキテクチャ	イメージの形式
aarch64	qcow2、vmdk
x86_64	qcow2、vmdk、raw、セルフインストーラ
ppc64le	raw、セルフインストーラ
s390x *	qcow2、raw

* s390xでは、CDL DASDとFBAの2つのストレージオプションが利用可能です。

2.1.2.2. SUSE Manager 仮想マシン設定 - VMware

このセクションでは、VMware環境内のSUSE Managerストレージパーティションに不可欠な追加の仮想ディスクの作成に重点を置いて、VMware設定について説明します。

プロシージャ: VMware仮想マシンを作成する

1. SUSE Manager Server **.vmdk** ファイルをダウンロードし、コピーをVMwareストレージに移動します。
2. VMware Webインタフェースを使用して、アップロードされた**.vmdk** ファイルのコピーを作成します。これにより、提供された**.vmdk** ファイルがvSphereハイパーバイザーに適した形式に変換されます。
3. ゲストOSファミリーLinuxおよびゲストOSバージョンSUSE Linux Enterprise 15 (64ビット)に基づいて、新しい仮想マシンを作成し、名前を付けます。
4. 500GB以上の**Hard Disk 2**を追加します。
5. RAMおよびCPU数を設定します(少なくとも16GBのRAMおよび4つのCPU)。
6. 必要に応じてネットワークアダプタを設定します。
7. VMの電源を入れ、firstbootダイアログ(キーボードレイアウト、ライセンス契約、タイムゾーン、rootのパスワード)に従います。
8. インストールが完了したら、rootとしてログインします。
9. 次のセクションに進みます。

2.1.2.3. SL MicroおよびSUSE Manager '5.0' サーバの登録

開始する前に、SUSEカスタマーセンター(<https://scc.suse.com>)からSUSE Manager登録コードを入手してください。

プロシージャ: SL MicroおよびSUSE Manager '5.0' を登録する

1. 仮想マシンをブートします。
2. `root`としてログインします。
3. SCCでSL Microを登録します。

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

4. 再起動します。
5. SUSE Customer CenterでSUSE Manager '5.0' を登録します。

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

6. 再起動
7. システムを更新します。

```
transactional-update
```

8. 更新が適用されていた場合は再起動します。
9. このステップはオプションです。ただし、ご使用のインフラストラクチャでカスタム永続ストレージが必要な場合は、`mgr-storage-server`ツールを使用します。詳細については、`mgr-storage-server --help`を参照してください。このツールを使用すると、コンテナストレージとデータベースボリュームの作成が容易になります。
 - このコマンドは次のように使用します。

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

例:

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



このコマンドは、`/var/lib/containers/storage/volumes`に永続ストレージを作成します。

詳細については、以下を参照してください。

- [Installation-and-upgrade > Container-management](#)
- [Administration > Troubleshooting](#)

10. 次のコマンドを実行してSUSE Managerを配備します。

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

2.1.3. SUSE Manager '5.0' サーバの配備

このガイドでは、SLE Micro 5.5にSUSE Manager '5.0' コンテナをインストールして設定する方法について説明します。

2.1.3.1. SUSE Managerのハードウェア要件

次の表に、SUSE Managerサーバをベースメタルマシンに配備するためのソフトウェアおよびハードウェアの要件を示します。このガイドの目的のためには、マシンに16 GBのRAMと200 GB以上のディスク容量が必要です。ディスク容量に関する背景情報については、[Installation-and-upgrade](#) > [Hardware-requirements](#)を参照してください。

表 11. ソフトウェアおよびハードウェアの要件

ソフトウェアおよびハードウェア	推奨
オペレーティングシステム:	SLE Micro 5.5
アーキテクチャ	x86-64、ARM、s390x、ppc64le
プロセッサ: (CPU)	最低4つの64ビットCPUコア
RAM:	16 GB
ディスク容量:	200 GB
チャンネル要件	SUSEまたはopenSUSE製品では50GB Red Hat製品では360GB
スワップ容量:	3 GB

サーバコンテナホストでサポートされるオペレーティングシステム

コンテナホストでサポートされているオペレーティングシステムはSLE Micro 5.5です。

コンテナホスト



コンテナホストは、コンテナを管理および配備できるPodmanなどのコンテナエンジンを搭載したサーバです。これらのコンテナは、アプリケーションと、ライブラリなどの重要な部品を保持していますが、完全なオペレーティングシステムは保持しないため軽量です。このセットアップにより、アプリケーションは異なる環境でも同じように動作します。CPU、メモリ、ストレージなど、これらのコンテナに必要なリソースはコンテナホストが提供します。

サーバの配備では、必ず完全修飾ドメイン名(FQDN)を使用する必要があります。ルータまたはネットワークにFQDNのDNSの自動プロビジョニング機能がない場合は、配備プロセスは正常に続行されません。FQDNは通常、<host>.<domain>.comの形式に従います。

例:

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

詳細については、[Installation-and-upgrade > Network-requirements](#)のネットワーク要件のセクションを参照してください。

2.1.3.2. 永続ボリューム

SUSE Manager '5.0' では、必要な永続ボリュームがデフォルトで定義されます。これらのボリュームは、まだ存在しない場合、`mgradm`ツールによってインストール中に作成されます。

これらのボリュームは`/var/lib/containers/storage/volumes/`に作成されます。`Podman`はボリュームをデフォルトでここに保存します。

推奨事項

外部ストレージデバイスをこのディレクトリにマウントすると、ストレージを簡単に利用できます。ここでは、PostgreSQLデータベース、リポジトリのバイナリパッケージ、キャッシュ、オペレーティングシステムのイメージ、自動インストールディストリビューション、および設定ファイルが保存されるため、次の3つの推奨事項があります。

高速なストレージ

このマウントポイントはNVMeまたはSSDクラスのデバイスにするのが理想的です。低速なストレージはSUSE Managerのパフォーマンスに悪影響を及ぼします。

大容量

管理するLinuxディストリビューションまたはアーキテクチャが複数ある場合、このディレクトリの推奨最小サイズは300 GB以上です。

推奨されるファイルシステム

XFS (ただし、SLE Micro 5.5でサポートされているファイルシステムであればどれでも動作可能)。

オプション

ボリュームのカスタムストレージを提供できます。そのためには、`/var/lib/containers/storage/volumes/var-spacewalk`など、ボリューム内の予期されるボリュームパスにディスクをマウントします。これにより、SUSE Managerの配備の複雑さが増し、推奨されるデフォルトのストレージで提供される回復性に影響する可能性があります。

コンテナ内の永続ボリュームのリストについては、[Installation-and-upgrade](#) > [Container-management](#)を参照してください。

2.1.3.3. SLE Micro 5.5のインストール

プロシージャ: インストールメディアをダウンロードする

1. <https://www.suse.com/download/sle-micro/>でSLE Micro 5.5のインストールメディアを見つけます。
2. [SLE-Micro-5.5-DVD-x86_64-GM-Media1.iso](#)をダウンロードします。
3. インストール用のDVDまたはUSBフラッシュドライブ(ダウンロードした.isoイメージを含む)を準備します。
4. SLE Micro 5.5のインストールイメージを含むDVDまたはUSBフラッシュドライブ(USBディスクまたはキー)を挿入します。
5. システムをブートまたは再起動します。

マシン(仮想または物理)の準備の詳細については、[SLE Micro 5.5 Deployment Guide](#)を参照してください。

プロシージャ: SLE Micro 5.5のインストール

1. 矢印キーを使用して**インストール**を選択します。
2. キーボードと言語を調整します。
3. **チェックボックス**をクリックしてライセンス契約に同意します。
4. **次へ**をクリックして続行します。
5. 登録方法を選択します。この例では、SUSE Customer Centerを使用してサーバを登録します。

インストール中にSUSE Managerを拡張機能として登録する

SUSE Manager '5.0' のコンテナは拡張機能としてインストールされます。したがって、SLE Micro 5.5のSUSE Customer Center登録コードを入手するほかに、次の拡張機能用のSUSE Customer Center登録コードも必要です。



- SUSE Manager '5.0' サーバ
- SUSE Manager '5.0' プロキシ
- Retail Branch Server

6. SUSE Customer Centerの電子メールアドレスを入力します。
7. SLE Micro 5.5の登録コードを入力します。
8. **次へ**をクリックして続行します。
9. SUSE Manager '5.0' サーバ拡張機能の**チェックボックス**をオンにします。
10. **次へ**をクリックして続行します。

11. SUSE Manager '5.0' サーバ拡張機能の登録コードを入力します。
12. [次へ]をクリックして続行します。
13. **NTP設定** ページで、[次へ]をクリックします。
14. **Authentication for the System (システムの認証)** ページで、rootユーザのパスワードを入力します。Click [次へ]をクリックします。
15. **インストール設定** ページで、[インストール]をクリックします。

これで、拡張機能としてのSLE Micro 5.5とSUSE Manager '5.0' のインストールが完了しました。

2.1.3.3.1. コマンドラインからの登録(オプション)

SLE Micro 5.5のインストール中にSUSE Manager '5.0' を拡張機能として追加した場合は、このステップはスキップして構いません。ただし、オプションで、[登録を行わずに次へ進む]ボタンを選択することにより、SLE Micro 5.5のインストール中に登録をスキップできます。このセクションでは、SLE Micro 5.5のインストール後に製品を登録するステップについて説明します。

プロシージャ: インストール後の製品の登録

1. SLE Micro 5.5をコマンドラインからSUSE Customer Centerに登録し、コンテナホストで次のコマンドを実行します。

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

2. SUSE Customer Centerアカウントから取得した登録コードをSLE Micro 5.5に使用します。



次の手順では、サーバをx86-64アーキテクチャに登録します。そのため、x86-64アーキテクチャの登録コードが必要になります。ARMまたはs390xアーキテクチャに登録する場合は、正しい登録コードを使用してください。

3. 次に、**SUSE Manager Server Extension 5.0 x86_64**拡張機能を追加します。次のコマンドを使用して、利用可能な拡張機能を一覧表示します。

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

4. 次のコマンドで**SUSE Manager Server Extension 5.0 x86_64**の登録コードを使用します。

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

5. 再起動します。

2.1.3.3.2. システムの更新

1. **root**としてログインします。
2. **transactional-update**を実行します。

```
transactional-update
```

3. 再起動します。

2.1.3.3.3. カスタム永続ストレージの設定

永続ストレージの設定はオプションですが、コンテナのディスクがいっぱいになった状態での深刻な問題を回避する唯一の方法です。mgr-storage-server ツールを使用してカスタム永続ストレージを設定することを強くお勧めします。

詳細については、`mgr-storage-server --help`を参照してください。このツールを使用すると、コンテナストレージとデータベースボリュームの作成が容易になります。

+ このコマンドは次のように使用します。

+

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

+ 例:

+

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

+



このコマンドは、`/var/lib/containers/storage/volumes`に永続ストレージを作成します。

詳細については、以下を参照してください。

- [Installation-and-upgrade › Container-management](#)
- [Administration › Troubleshooting](#)

2.1.3.4. mgradmを使用した配備

プロシージャ: mgradmを使用してSUSE Manager '5.0' を配備する

1. rootとしてログインします。
2. 次のコマンドを、`<suma.example.com>`を完全修飾ドメイン名に置き換えて入力します。

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

上記のコマンドが失敗する場合は、SUSE Manager '5.0' が登録済みであることを確認してください。インストール時に登録をスキップし、ここでコマンドラインから登録する必要がある場合は、次のステップに従ってレジストリにログインします。



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

入力を求められたら、SUSE Manager '5.0' の登録キーを使用します。

3. 入力を求められたら、証明書と管理者アカウントのパスワードを入力します。



管理者アカウントのパスワードは長さ5文字以上、48文字未満である必要があります。

4. [**Enter (入力)**]を押します。
5. 管理者アカウントの電子メールアドレスを入力します。[**Enter (入力)**]を押します。
6. 配備が完了するまで待ちます。
7. ブラウザを開き、サーバのFQDNに進みます。
8. ユーザ名(デフォルトはadmin)と、配備プロセス中に設定したパスワードを入力します。

SLE Microはデフォルトで自動的に自己更新するように設計されており、更新が適用されると再起動します。ただし、この動作はSUSE Manager環境では望ましくありません。サーバの自動更新を防ぐために、SUSE Managerでは、ブートストラッププロセス中にトランザクション型更新のタイマーが無効化されます。



SLE Microのデフォルトの動作を使用したい場合は、次のコマンドを実行してタイマーを有効にします。

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

このガイドでは、SUSE Manager '5.0' サーバをコンテナとして配備します。次のセクションに進み、SUSE Customer Centerと同期するために組織の資格情報を追加します。

2.1.3.5. SUSE Customer CenterへのSUSE Manager '5.0' の接続

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. ブラウザを開き、サーバのFQDNに進みます。
2. ユーザ名(デフォルトはadmin)と、配備プロセス中に設定したパスワードを入力します。
3. SUSE ManagerのWeb UIで、**管理** > **セットアップウィザード**を選択します。

4. [\[セットアップウィザード\]](#) 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. ブラウザでSUSE Customer Centerにアクセスします。
7. 左側のナビゲーションから自分の組織を選択します。
8. ページの上部から [\[ユーザ\]](#) タブを選択し、[\[組織の資格情報\]](#) を選択します。
9. [ミラーリング資格情報](#) をメモします。
10. SUSE ManagerのWeb UIに戻り [\[ユーザ名\]](#) と [\[パスワード\]](#) に入力し、[\[保存\]](#) を押して確定します。

緑色のチェックマークアイコンで資格情報を確認したら、[プロシージャ: SUSE Customer Centerと同期する](#)に進みます。

プロシージャ: SUSE Customer Centerと同期する

1. Web UIで、[管理](#) > [セットアップウィザード](#) に移動します。
2. [\[セットアップウィザード\]](#) ページから [\[SUSE製品\]](#) タブを選択します。以前にSUSE Customer Centerで登録したことがある場合、製品の一覧が表に入力され始めます。この操作には数分かかる場合があります。右側の [\[SUSEカスタマーセンターから製品カタログを更新\]](#) セクションで、操作の進行状況を監視できます。この表は、アーキテクチャ、チャンネル、状態の各情報を一覧表示します。詳細については、[Reference > Admin](#)を参照してください。

Setup Wizard

HTTP Proxy Organization Credentials **SUSE Products**

Filter by product Description Filter by architecture 25 items per page

Items 1 - 25 of 94

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

Page 1 of 4

First Prev Next Last

← Prev 3 of 3

Refresh the product catalog from SUSE Customer Center

Channels
Channel Families
Products
Product Channels
Subscriptions

Refresh

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

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

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

3. 表示されている製品のリストをフィルタするには、**[製品説明でフィルタ]** および **[アーキテクチャでフィルタ]** を使用します。**[製品]** ページに一覧表示されたチャンネルによって、クライアントのリポジトリが提供されます。
- 各チャンネルの左側にあるチェックボックスをオンにして、チャンネルをSUSE Managerに追加します。説明の左にある矢印をクリックして、製品を展開し、使用できるモジュールを一覧表示します。
 - ページの上部の**[製品の追加]** をクリックして、製品の同期を開始します。

チャンネルを追加した後、SUSE Managerは、チャンネルの同期をスケジュールします。この処理には時間がかかる場合があります。その理由は、SUSE Customer CenterにあるSUSEリポジトリからサーバのローカル/`/var/lib/containers/storage/volumes/var-spacewalk/`ディレクトリにチャンネルソフトウェアソースをSUSE Managerでコピーするためです。

チャンネルが完全に同期されると、そのブートストラップリポジトリが自動的に生成されます。このステップは、クライアントを正常にブートストラップし、チャンネルの同期と配布がクライアント側で正常に機能していることを確認するために非常に重要です。これで、SUSE Managerのインストールと設定、およびクライアントのブートストラップに必要なチャンネルの準備は完了です。

チャンネル同期プロセスが完了したら、SUSE Manager '5.0' プロキシまたは他のクライアントの登録に進むことができます。

詳細手順については、[Client-configuration > Registration-overview](#)を参照してください。

2.1.3.6. 管理のためにコンテナに移動する

コンテナ内のシェルに移動するには、コンテナホストで次のコマンドを実行します。

```
mgrctl term
```

2.1.4. SUSE ManagerサーバのAir-gapped配備

2.1.4.1. Air-gapped配備とは何ですか？

Air-gapped配備とは、安全ではないネットワーク、特にインターネットから物理的に隔離されたネットワークシステムをセットアップおよび運用することです。この種の配備は、一般的に高度なセキュリティ環境で使用されます。たとえば、軍事施設、金融システム、重要インフラストラクチャ、機密データを取り扱って外部の脅威から保護する必要がある場所などです。

2.1.4.2. 配備

SUSE Managerは2つの配備バリエーションをサポートしています。

2.1.4.2.1. 仮想マシンでの配備

推奨されるインストール方法は、提供されているSUSE Managerの仮想マシンイメージのオプションを使用する方法です。必要なツールとコンテナイメージがすべてプリロードされていて、すぐに動作するためです。

SUSE Managerサーバ仮想マシンのインストールの詳細については、[仮想マシンとしてのサーバの配備](#)を参照してください。

SUSE Managerサーバをアップグレードするには、システム内のすべてのパッケージをアップグレードし、[サーバのアップグレード](#)で定義されている手順に従うことをお勧めします。

2.1.4.2.2. SLE MicroにSUSE Managerを配備する

SUSE Managerでは、必要なコンテナイメージはすべてRPMでも提供されており、このイメージをシステムにインストールすることができます。



ユーザは必要なRPMを内部のネットワーク上で利用できるようにする必要があります。そのためには、2つ目のSUSE ManagerサーバまたはRMTサーバを使用します。

プロシージャ: Air-gappedでSLE MicroにSUSE Managerをインストールする

1. SLE Microのインストール
2. システムの更新
3. ツールのパッケージとイメージのパッケージをインストールします(\$ARCH\$は適切なアーキテクチャに置き換えます)。

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

4. 再起動します。
5. mgradmを使用したSUSE Managerの配備

SLE MicroにSUSE Managerサーバをインストールする方法の詳細については、[仮想マシンとしてのサーバの配備](#)を参照してください。

SUSE Managerサーバをアップグレードするには、システム内のすべてのパッケージをアップグレードし、[サーバのアップグレード](#)で定義されている手順に従うことをお勧めします。

2.1.5. SUSE Managerサーバとパブリッククラウド

パブリッククラウドでは、SUSE ManagerはBring-your-own-subscription (BYOS)モデルまたはPay-as-you-go (PAYG)に基づいて提供されます。

パブリッククラウドでのSUSE Managerの使用の詳細については、[Specialized-guides](#) > [Public-cloud-guide](#)を参照してください。

2.2. プロキシ

2.2.1. 仮想マシンとしてのSUSE Manager '5.0' プロキシの配備

この章では、SUSE Manager '5.0' をイメージとして配備するための仮想マシンの設定について説明します。このインストールでは、KVMを仮想マシンマネージャ(virt-manager)と組み合わせてサンドボックスとして使用します。



SUSE Manager '5.0' プロキシを配備する際に推奨される方法は、利用可能な次のイメージの1つを使用することです。これらのツールにはすべてのツールが含まれており、配備が大幅に容易になります。

2.2.1.1. 利用可能なイメージ

SUSE Manager '5.0' のイメージはSUSE Manager '5.0' VM imagesで入手できます。

表 12. 利用可能なプロキシイメージ

アーキテクチャ	イメージのフォーマット
aarch64	qcow2、vmdk
x86_64	qcow2、vmdk、raw、セルフインストーラ

生イメージの準備の詳細については、以下を参照してください。

- <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>

セルフインストーライメージの詳細については、以下を参照してください。

- <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。

次の表は、最低要件を指定しています。これらは、クライアントが1つある1つのサーバなど、テスト用の簡易的なインストールに適しています。運用環境を使用する場合は、**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. プロキシのハードウェア要件

次の表に、SUSE Managerプロキシを配備するためのハードウェア要件を示します。

KVMの設定	
インストール方法	既存のディスクイメージのインポート
OS:	Linux
バージョン:	SUSE Manager-Proxy.x86_64-5.0.0-Build16.12.qcow2
メモリ:	2 GB

KVMの設定	
CPU:	2
ストレージフォーマット:	.qcow2 40 GB (デフォルト)ルートパーティション
名前:	test-setup
ネットワーク	Bridge br0



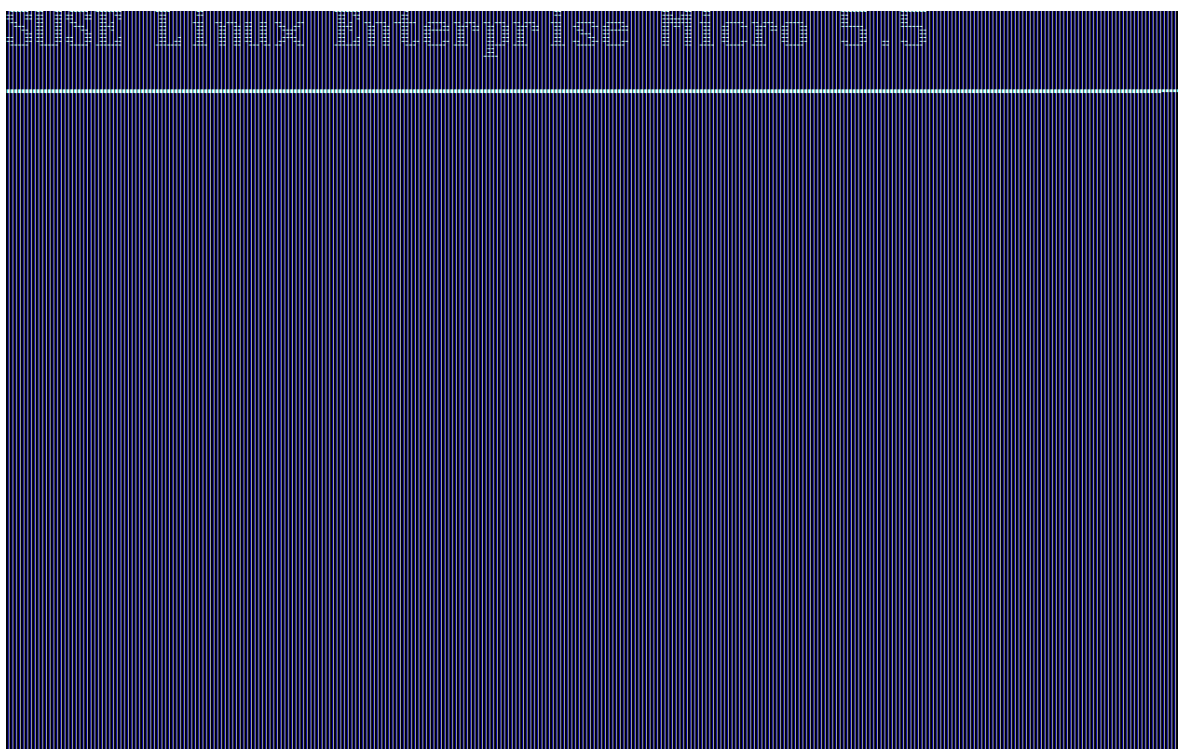
`/var/lib/containers/storage/volumes/srv-www` 100 GB以上、ストレージ要件は、使用するISOディストリビューションイメージ、コンテナ、およびブートストラップリポジトリの数に合わせて計算する必要があります。

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

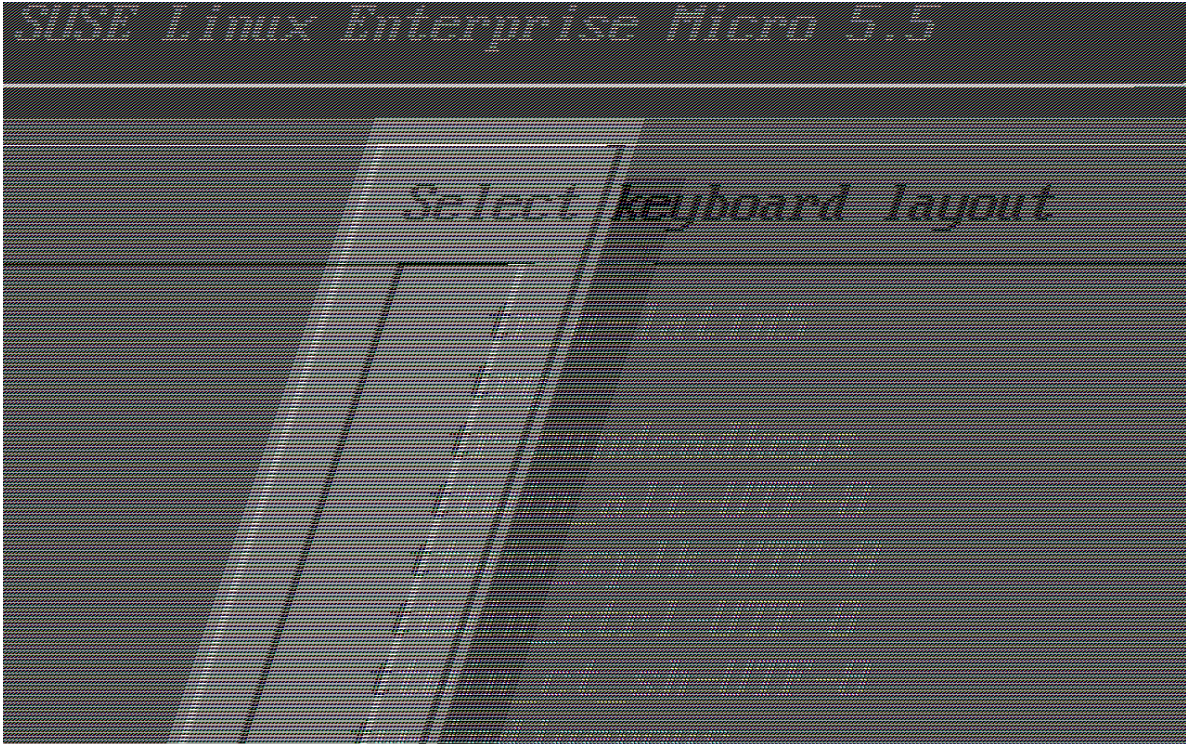
2.2.1.4. KVMの初期セットアップ

プロシージャ: 初期セットアップを作成する

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. RAMおよびCPU数を設定します(少なくとも16GBのRAMおよび4つのCPU)。
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. `[Begin Installation]` (インストールの開始) をクリックし、イメージからブートします。
5. `[JeOS Firstboot]` の画面で、`[Start]` を選択して続行します。



6. キーボードレイアウトを選択します。



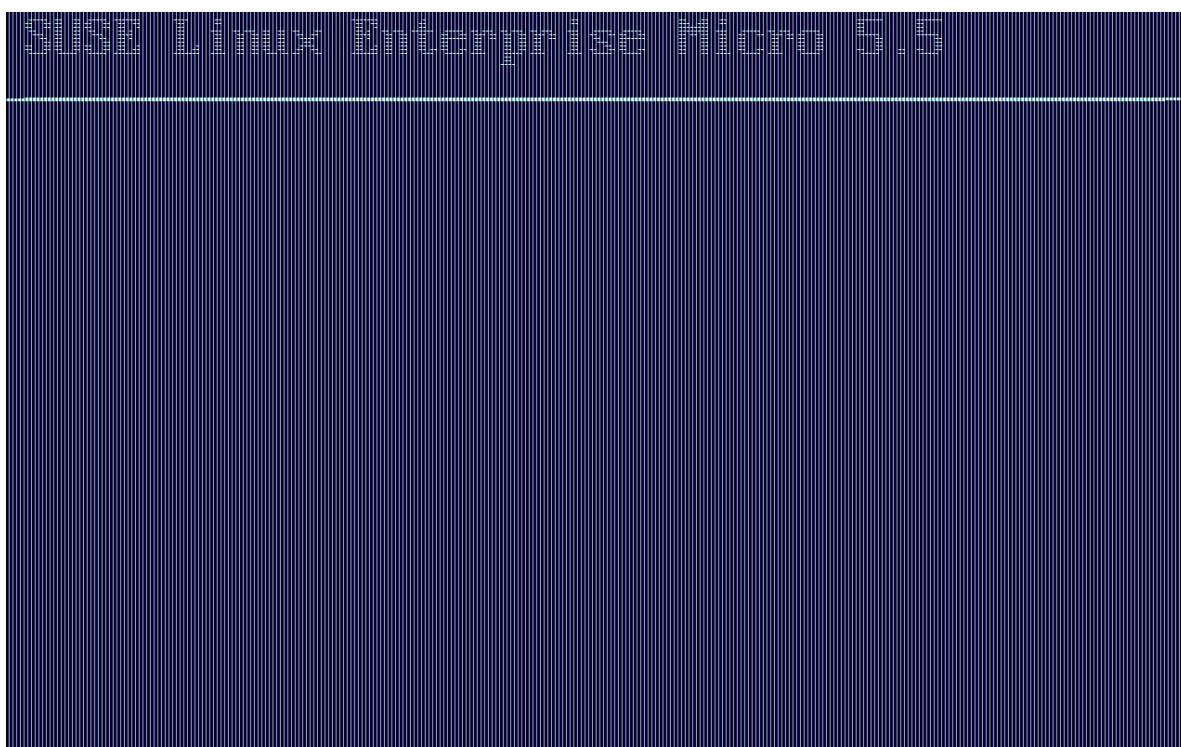
7. ライセンス契約に同意します。



8. タイムゾーンを選択します。



9. rootのパスワードを入力します。



10. インストールが完了したら、rootとしてログインします。

11. 次のセクションに進みます。

2.2.1.5. SL MicroおよびSUSE Manager '5.0' の登録

プロシージャ: SL MicroおよびSUSE Manager '5.0' プロキシを登録する

1. 仮想マシンをブートします。
2. `root`としてログインします。
3. SCCでSL Microを登録します。

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

4. 再起動します。
5. SUSE Customer CenterでSUSE Manager '5.0' を登録します。

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

6. 再起動します。
7. システムを更新します。

```
transactional-update
```

8. 更新が適用されていた場合は再起動します。

2.2.1.6. プロキシのアクティベーションキーの作成

SUSE Managerサーバ上で、プロキシのアクティベーションキーを作成します。

タスク: アクティベーションキーの作成

1. システム > アクティベーションキーに移動し、[**キーの作成**]をクリックします。
2. SL Micro 5.5を親ホストとしてプロキシホストのアクティベーションキーを作成します。このキーには、推奨されるすべてのチャンネルと、拡張機能としてのプロキシの子チャンネルが含まれる必要があります。
3. 続行して、プロキシホストをMinionとしてブートストラップします。

2.2.1.7. プロキシホストのブートストラップ

タスク: プロキシホストのブートストラップ

1. システム > ブートストラップを選択します。
2. プロキシホストのフィールドに入力します。
3. ドロップダウンから、前のステップで作成したアクティベーションキーを選択します。
4. Click [**ブートストラップ**]をクリックします。
5. ブートストラッププロセスが完了するまで待ちます。Saltメニューをチェックして、Saltキーが一覧表

示されていて受け入れられていることを確認します。

6. プロキシホストを再起動します。
7. すべてのイベントが終了したら、**システム**の一覧からホストを選択して2回目の再起動をトリガし、オンボーディングを完了します。

タスク: プロキシホストの更新

1. **システム**の一覧からホストを選択し、すべてのパッチを適用してホストを更新します。
2. プロキシホストを再起動します。

2.2.1.8. プロキシ設定の生成

SUSE Managerプロキシの設定アーカイブはSUSE Managerサーバによって生成されます。追加のプロキシごとに専用の設定アーカイブが必要です。



2 GBはプロキシSquidのデフォルトのキャッシュサイズを表します。これは環境に合わせて調整する必要があります。



Podmanの配備では、このプロキシ設定を生成する前に、SUSE ManagerプロキシのコンテナホストをSUSE Managerサーバにクライアントとして登録する必要があります。

プロキシFQDNを使用して、登録済みのクライアントではないプロキシコンテナ設定を生成すると(Kubernetesのユースケースと同様)、新しいシステムエントリがシステム一覧に表示されます。この新しいエントリは、以前に入力されたプロキシFQDN値の下に表示され、**外部**システムタイプになります。

2.2.1.8.1. Web UIを使用したプロキシ設定の生成

プロシージャ: Web UIを使用してプロキシコンテナ設定を生成する

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. [**Squidの最大キャッシュサイズ[MB]**] フィールドタイプで、Squidキャッシュの最大許容サイズ。コンテナで使用可能なストレージの最大60%で使用することを推奨します。



2 GBはプロキシSquidのデフォルトのキャッシュサイズを表します。これは、環境に合わせて調整する必要があります。



[**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)証明書とみ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。

+ サーバによって生成されたCA証明書は、`/var/lib/containers/storage/volumes/root/_data/ssl-build`ディレクトリに保存されます。

+ 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. **[生成]**をクリックして、SUSE Managerサーバに新しいプロキシFQDNを登録し、コンテナホストの詳細を含む設定アーカイブ(`config.tar.gz`)を生成します。
2. しばらくすると、ダウンロードするファイルが表示されます。このファイルをローカルに保存します。

 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. spacecmdと自己署名証明書を使用したプロキシ設定ファイルの生成

プロシージャ: spacecmdと自己署名証明書を使用してプロキシ設定を生成する

spacecmdを使用してプロキシ設定を生成できます。

1. SSHでコンテナホストに接続します。
2. 次のコマンドを実行してサーバとプロキシFQDNを置き換えます。

```
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. 生成された設定をサーバコンテナからコピーします。

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

2.2.1.8.3. spacecmdとカスタム証明書を使用したプロキシ設定の生成

デフォルトの自己署名証明書ではなくカスタム証明書に対してspacecmdを使用して、プロキシ設定を生成できます。

プロシージャ: spacecmdとカスタム証明書を使用してプロキシ設定を生成する

1. サーバコンテナホストにSSHで接続します。
2. 次のコマンドを実行してサーバとプロキシFQDNを置き換えます。

```
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. 生成された設定をサーバコンテナからコピーします。

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

2.2.1.9. カスタム永続ストレージの設定

このステップはオプションです。ただし、ご使用のインフラストラクチャにカスタム永続ストレージが必要な場合は、`mgr-storage-proxy`ツールを使用します。

詳細については、`mgr-storage-proxy --help`を参照してください。このツールを使用すると、コンテナストレージとSquidキャッシュボリュームの作成が容易になります。

+ このコマンドは次のように使用します。

+

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

+ 例:

+

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

+



このコマンドは、`/var/lib/containers/storage/volumes`に永続ストレージを作成します。

詳細については、以下を参照してください。

- [Installation-and-upgrade](#) › [Container-management](#)
- [Administration](#) › [Troubleshooting](#)

2.2.1.10. プロキシ設定の転送

Web UIによって設定アーカイブが生成されます。このアーカイブをプロキシコンテナホストで利用できるようにする必要があります。

プロシージャ: プロキシ設定をコピーする

1. サーバコンテナからサーバのホストOSにファイルをコピーします。

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

2. サーバのホストOSからプロキシホストにファイルをコピーします。

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

3. 次のコマンドを使用してプロキシをインストールします。

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

2.2.1.11. SUSE Manager '5.0' プロキシの起動

`mgrpxy`コマンドを使用してコンテナを起動できます。

プロシージャ: プロキシを起動してステータスを確認する

1. 次のコマンドを呼び出してプロキシを起動します。

```
mgrpxy start
```

2. 次のコマンドを呼び出してコンテナのステータスを確認します。

```
mgrpxy status
```

次の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

また、`proxy-pod`コンテナポッドの一部である必要があります。

2.2.1.11.1. サービスにカスタムコンテナイメージを使用する

デフォルトでは、SUSE Managerプロキシスイートは、その各サービスに対して同じイメージバージョンとレジストリパスを使用するように設定されています。ただし、末尾に`-tag`および`-image`を指定してインストールパラメータを使用し、特定のサービスのデフォルト値を上書きすることは可能です。

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
```

これは、`httpd`サービスの設定ファイルを調整してから再起動します。`registry.opensuse.org/uyuni/proxy-httpd`は使用するイメージ、`0.1.0`はバージョンタグです。

値をデフォルトにリセットするには、これらのパラメータを指定せずにもう一度`install`コマンドを実行します。

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

このコマンドは、すべてのサービスの設定をグローバルデフォルトにリセットして再ロードします。

2.2.2. SUSE Manager '5.0' プロキシの配備

このガイドでは、SUSE Manager '5.0' プロキシの配備プロセスの概要を説明します。このガイドでは、SUSE Manager '5.0' サーバが既に正常に配備済みであることを想定しています。



現時点では、SLE Microは正規のminionとして(デフォルト接続メソッド)のみサポートされています。Salt SSHクライアント(`salt-ssh`接続メソッド)としても管理できるように目指しています。

正常に配備するには、次のアクションを実行します。

タスク: プロキシの配備

1. ハードウェア要件を確認します。

2. サーバ上でSLE Micro 5.5の親チャンネルとプロキシ拡張機能の子チャンネルを同期します。
3. ベアメタルマシンにSLE Micro 5.5をインストールします。
4. インストール時に、SLE Micro 5.5をSUSE Manager '5.0' プロキシ拡張機能とともに登録します。
5. Saltのアクティベーションキーを作成します。
6. **デフォルト**接続メソッドを使用して、プロキシをクライアントとしてブートストラップします。
7. プロキシ設定を生成します。
8. サーバからプロキシにプロキシ設定を転送します。
9. プロキシ設定を使用して、クライアントをSUSE Managerにプロキシとして登録します。

プロキシコンテナホストでサポートされるオペレーティングシステム

コンテナホストでサポートされているオペレーティングシステムはSLE Micro 5.5です。



コンテナホスト

コンテナホストは、コンテナを管理および配備できるPodmanなどのコンテナエンジンを搭載したサーバです。これらのコンテナは、アプリケーションと、ライブラリなどの重要な部品を保持していますが、完全なオペレーティングシステムは保持しないため軽量です。このセットアップにより、アプリケーションは異なる環境でも同じように動作します。CPU、メモリ、ストレージなど、これらのコンテナに必要なリソースはコンテナホストが提供します。

2.2.2.1. プロキシのハードウェア要件

次の表に、SUSE Managerプロキシを配備するためのハードウェア要件を示します。

表 13. プロキシのハードウェア要件

ハードウェア	詳細	推奨
CPU	x86-64、ARM	専用64ビットCPUコア数は2つ以上
RAM	最小	2 GB
	推奨	8 GB
ディスク容量	/(ルートディレクトリ)	40 GB以上
	<code>/var/lib/containers/storage/volumes/srv-www</code>	100 GB以上。ストレージ要件は、使用するISOディストリビューションイメージ、コンテナ、およびブートストラップリポジトリの数に合わせて計算する必要があります。
	<code>/var/lib/containers/storage/volumes/var-cache</code> (Squid)	100 GB以上

2.2.2.2. 親とプロキシ拡張機能の子チャンネルの同期

このセクションは、サーバのWeb UIの**管理** > **セットアップウィザード** → **組織の資格情報**で組織の資格情報を入力済みであることを想定しています。製品は、**管理** > **セットアップウィザード** → **製品**ページに一覧表示されます。このチャンネルは、子チャンネルの **[Proxy as an extension (プロキシを子チャンネルとして)]** オプションを選択した状態で、サーバ上で完全に同期する必要があります。

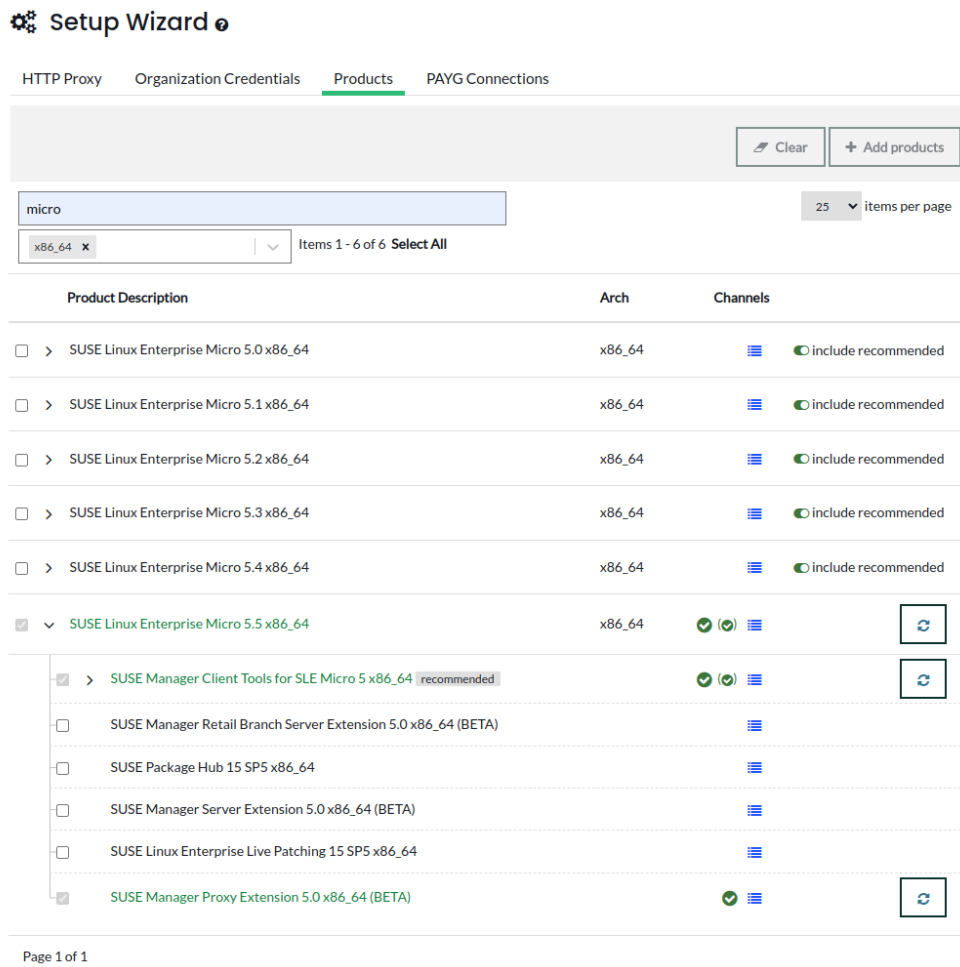


図 1. プロキシのSUSE Manager '5.0' のチャンネル同期

タスク: プロキシの親チャンネルとプロキシ拡張機能の同期

1. SUSE ManagerのWeb UIで、**管理** > **製品**を選択します。
2. [製品] ページから、[フィルタ] フィールドに「SLE Micro」と入力します。
3. 続いて、ドロップダウンを使用して必要なアーキテクチャを選択します。この例では、[x86-64] を選択します。
4. **製品説明**フィールドで、SLE Micro 5.5のチェックボックスをオンにしてから、ドロップダウンを使用して**SUSE Manager Proxy Extension 5.0 x86_64 BETA**拡張機能を選択します。
5. **[製品の追加]**をクリックします。
6. 同期が完了するまで待ちます。

2.2.2.3. SLE Micro 5.5のインストール

タスク: インストールメディアのダウンロード

1. <https://www.suse.com/download/sle-micro/>でSLE Micro 5.5のインストールメディアを見つけます。
2. ISOをダウンロードするには、SUSE Customer Centerのアカウントが必要で、ログインしている必要があります。
3. [SLE-Micro-5.5-DVD-x86_64-GM-Media1.iso](#)をダウンロードします。
4. インストール用のUSBフラッシュディスクまたはDVDを準備します。
5. SLE Micro 5.5のインストールイメージを含むDVDまたは起動可能なUSBスティックを挿入します。
6. システムをブートまたは再起動します。

マシンのOS (仮想または物理)の準備に関する詳しいドキュメントについては、[SLE Micro 5.5 Deployment Guide](#)を参照してください。

タスク: SLE Micro 5.5のインストール

1. 矢印キーを使用して**インストール**を選択します。
2. キーボードと言語を調整します。**チェックボックス**をクリックしてライセンス契約に同意します。
3. **次へ**をクリックして続行します。
4. 登録方法を選択します。この例では、SUSE Customer Centerでサーバを登録します。

拡張機能としてのSUSE Manager '5.0' プロキシ



SUSE Manager '5.0' プロキシは拡張機能として登録されます。したがって、SLE Micro 5.5のSUSE Customer Center登録キーを入手するほかに、次の拡張機能用のSUSE Customer Center登録コードも必要です。

- SUSE Manager '5.0' プロキシ

5. SUSE Customer Centerの電子メールアドレスを入力します。
6. SLE Micro 5.5の登録コードを入力します。
7. **次へ**をクリックして続行します。
8. **拡張とモジュールの選択**ページで、**開発版を隠す**チェックボックスをオフにします。
9. SUSE Manager '5.0' プロキシ拡張機能の**チェックボックス**をオンにします。
10. **次へ**をクリックして続行します。
11. SUSE Manager '5.0' プロキシ拡張機能の登録コードを入力します。
12. **[次へ]**をクリックして続行します。
13. **NTP設定**ページで、**[次へ]**をクリックします。
14. **Authentication for the System**ページで、rootユーザのパスワードを入力します。Click **[次へ]**をクリ

ックします。

15. **インストール設定** ページで、**[インストール]** をクリックします。

これにより、拡張機能としてのSLE Micro 5.5およびSUSE Manager '5.0' プロキシのインストールが終了します。

2.2.2.3.1. システムの更新

タスク: システムの更新

1. **root**としてログインします。
2. **transactional-update**を実行します。

```
transactional-update
```

3. システムを再起動します。
4. rootとしてログインします。
5. コンテナユーティリティをインストールします。



または、**mgrpky-zsh-completion**または**mgrpky-fish-completion**をインストールできます。

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

6. システムを再起動します。

2.2.2.3.2. カスタム永続ストレージの設定

このステップはオプションです。ただし、ご使用のインフラストラクチャにカスタム永続ストレージが必要な場合は、**mgr-storage-proxy**ツールを使用します。

詳細については、**mgr-storage-proxy --help**を参照してください。このツールを使用すると、コンテナストレージとSquidキャッシュボリュームの作成が容易になります。

+ このコマンドは次のように使用します。

+

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

+ 例:

+

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

+

このコマンドは、`/var/lib/containers/storage/volumes`に永続ストレージを作成します。



詳細については、以下を参照してください。

- [Installation-and-upgrade > Container-management](#)
- [Administration > Troubleshooting](#)

2.2.2.4. プロキシのアクティベーションキーの作成

タスク: アクティベーションキーの作成

1. システム > アクティベーションキーに移動し、[**キーの作成**]をクリックします。
2. SLE Micro 5.5を親チャンネルとして、プロキシホストのアクティベーションキーを作成します。このキーには、推奨されるすべてのチャンネルと、拡張機能としてのプロキシの子チャンネルが含まれる必要があります。
3. 続行して、プロキシホストを**デフォルト**クライアントとしてブートストラップします。

2.2.2.5. クライアントとしてのプロキシホストのブートストラップ

タスク: プロキシホストのブートストラップ

1. システム > **ブートストラップ**を選択します。
2. プロキシホストのフィールドに入力します。
3. ドロップダウンから、前のステップで作成したアクティベーションキーを選択します。
4. Click [**ブートストラップ**]をクリックします。
5. ブートストラッププロセスが完了するまで待ちます。 **Salt**メニューをチェックし、Saltキーが一覧表示されていて受け入れられていることを確認します。
6. プロキシホストを再起動します。
7. すべてのイベントが終了したら、**システム**の一覧からホストを選択して2回目の再起動をトリガし、オンボーディングを完了します。

タスク: プロキシホストの更新

1. **システム**の一覧からホストを選択し、すべてのパッチを適用してホストを更新します。
2. プロキシホストを再起動します。

2.2.2.6. プロキシ設定の生成

SUSE Managerプロキシの設定アーカイブはSUSE Managerサーバによって生成されます。追加のプロキシごとに専用の設定アーカイブが必要です。



2 GBはプロキシSquidのデフォルトのキャッシュサイズを表します。これは環境に合わせて調整する必要があります。



Podmanの配備では、このプロキシ設定を生成する前に、SUSE ManagerプロキシのコンテナホストをSUSE Managerサーバにクライアントとして登録する必要があります。

プロキシFQDNを使用して、登録済みのクライアントではないプロキシコンテナ設定を生成すると(Kubernetesのユースケースと同様)、新しいシステムエントリがシステム一覧に表示されます。この新しいエントリは、以前に入力されたプロキシFQDN値の下に表示され、**外部**システムタイプになります。

2.2.2.6.1. Web UIを使用したプロキシ設定の生成

プロシージャ: Web UIを使用してプロキシコンテナ設定を生成する

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. [**Squidの最大キャッシュサイズ[MB]**] フィールドタイプで、Squidキャッシュの最大許容サイズ。コンテナで使用可能なストレージの最大60%でを使用することを推奨します。



2 GBはプロキシSquidのデフォルトのキャッシュサイズを表します。これは、環境に合わせて調整する必要があります。

[**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)証明書とみ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。

+ サーバによって生成されたCA証明書は、`/var/lib/containers/storage/volumes/root/_data/ssl-build`ディレクトリに保存されます。

+ 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. [**生成**]をクリックして、SUSE Managerサーバに新しいプロキシFQDNを登録し、コンテナホストの詳細を含む設定アーカイブ(`config.tar.gz`)を生成します。
2. しばらくすると、ダウンロードするファイルが表示されます。このファイルをローカルに保存します。

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. spacecmdと自己署名証明書を使用したプロキシ設定ファイルの生成

プロシージャ: spacecmdと自己署名証明書を使用してプロキシ設定を生成する

spacecmdを使用してプロキシ設定を生成できます。

1. SSHでコンテナホストに接続します。
2. 次のコマンドを実行してサーバとプロキシFQDNを置き換えます。

```
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. 生成された設定をサーバコンテナからコピーします。

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

2.2.2.6.3. spacecmdとカスタム証明書を使用したプロキシ設定の生成

デフォルトの自己署名証明書ではなくカスタム証明書に対してspacecmdを使用して、プロキシ設定を生成できます。

プロシージャ: spacecmdとカスタム証明書を使用してプロキシ設定を生成する

1. サーバコンテナホストにSSHで接続します。
2. 次のコマンドを実行してサーバとプロキシFQDNを置き換えます。

```
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. 生成された設定をサーバコンテナからコピーします。

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

2.2.2.7. プロキシ設定の転送

Web UIによって設定アーカイブが生成されます。このアーカイブをプロキシコンテナホストで利用できるようにする必要があります。

タスク: プロキシ設定のコピー

1. 前のステップで生成された設定アーカイブ(`config.tar.gz`)をプロキシホストにコピーします。

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

2. 次のコマンドを使用してプロキシをインストールします。

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

2.2.2.8. SUSE Manager '5.0' プロキシの起動

`mgrpxy`コマンドを使用してコンテナを起動できます。

タスク: プロキシの起動とステータスの確認

1. 次のコマンドを呼び出してプロキシを起動します。

```
mgrpxy start
```

2. 次のコマンドを呼び出してコンテナのステータスを確認します。

```
mgrpxy status
```

次の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

また、`proxy-pod`コンテナポッドの一部である必要があります。

2.2.2.8.1. サービスにカスタムコンテナイメージを使用する

デフォルトでは、SUSE Managerプロキシスイートは、そのサービスごとに同じイメージバージョンとレジストリパスを使用するように設定されています。ただし、`-tag`および`-image`で終わるインストールパラメータを使用して、特定のサービスのデフォルト値を上書きすることは可能です。

たとえば、次のように使用します。

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

これは、httpdサービスの設定ファイルを調整してから再起動します。`registry.opensuse.org/uyuni/proxy-httpds`は使用するイメージ、`0.1.0`はバージョンタグです。

値をデフォルトにリセットするには、これらのパラメータを指定せずにもう一度installコマンドを実行します。

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

このコマンドは、すべてのサービスの設定をグローバルデフォルトにリセットして再ロードします。

2.2.3. k3sへ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プロキシは、シングルノードクラスタのSLE Micro上で実行されるk3sでサポートされます。他のKubernetes環境に配備する必要がある場合は、サポートに連絡して評価を依頼してください。

コンテナホストマシンにk3sをインストールします(<K3S_HOST_FQDN>はk3sホストのFQDNに置き換えます)。

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

2.2.3.2. ツールのインストール

インストールにはmgrpxyパッケージとhelmパッケージが必要です。

For Helm, you can install it using the installer script:

```
curl -fsSL -o get_helm.sh https://raw.githubusercontent.com/helm/helm/main/scripts/get-helm-3
chmod 700 get_helm.sh
./get_helm.sh
```

For more information, see <https://helm.sh/docs/intro/install/#from-script>.

The `mgrpxy` package is available in the SUSE Manager Proxy product repositories. To install it run:

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

- 再起動

2.2.3.2.1. Web UIを使用したプロキシ設定の生成

プロシージャ: Web UIを使用してプロキシコンテナ設定を生成する

- 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。
- [**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。
- [**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。
- [**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。
- [**Squidの最大キャッシュサイズ[MB]**] フィールドタイプで、Squidキャッシュの最大許容サイズ。コンテナで使用可能なストレージの最大60%で使用することを推奨します。



2 GBはプロキシSquidのデフォルトのキャッシュサイズを表します。これは、環境に合わせて調整する必要があります。

[**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)証明書とみ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。

+ サーバによって生成されたCA証明書は、`/var/lib/containers/storage/volumes/root/_data/ssl-build`ディレクトリに保存されます。

+ 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。

- [**生成**]をクリックして、SUSE Managerサーバに新しいプロキシFQDNを登録し、コンテナホストの詳細を含む設定アーカイブ(`config.tar.gz`)を生成します。
- しばらくすると、ダウンロードするファイルが表示されます。このファイルをローカルに保存します。

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:

2.2.3.2.2. spacecmdと自己署名証明書を使用したプロキシ設定ファイルの生成

プロシージャ: spacecmdと自己署名証明書を使用してプロキシ設定を生成する

spacecmdを使用してプロキシ設定を生成できます。

1. SSHでコンテナホストに接続します。
2. 次のコマンドを実行してサーバとプロキシFQDNを置き換えます。

```
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. 生成された設定をサーバコンテナからコピーします。

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

2.2.3.2.3. spacecmdとカスタム証明書を使用したプロキシ設定の生成

デフォルトの自己署名証明書ではなくカスタム証明書に対してspacecmdを使用して、プロキシ設定を生成できます。

プロシージャ: spacecmdとカスタム証明書を使用してプロキシ設定を生成する

1. サーバコンテナホストにSSHで接続します。
2. 次のコマンドを実行してサーバとプロキシFQDNを置き換えます。

```
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. 生成された設定をサーバコンテナからコピーします。

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

2.2.3.3. SUSE Managerプロキシhelmチャートの配備

SUSE Managerプロキシポッドで使用するボリュームのストレージを設定するには、次のクレームに対して永続ボリュームを定義します。ストレージ設定をカスタマイズしない場合は、k3sによって自動的にストレージボリュームが作成されます。

永続ボリュームのクレームの名前は次のとおりです。

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

Installation-and-upgrade > Container-deploymentに記載されているように、SUSE Managerプロキシの設定を作成します。設定tar.gzファイルをコピーしてインストールします。

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

詳細については、<https://kubernetes.io/docs/concepts/storage/persistent-volumes/> (kubernetes)または<https://rancher.com/docs/k3s/latest/en/storage/> (k3s)のドキュメントを参照してください。

2.2.4. SUSE ManagerプロキシのAir-gapped配備

2.2.4.1. Air-gapped配備とは

Air-gapped配備とは、安全ではないネットワーク、特にインターネットから物理的に隔離されたネットワークシステムをセットアップおよび運用することです。この種の配備は、一般的に高度なセキュリティ環境で使用されます。たとえば、軍事施設、金融システム、重要インフラストラクチャ、機密データを取り扱っていて外部の脅威から保護する必要がある場所などです。

2.2.4.2. 仮想マシンでの配備

推奨されるインストール方法は、提供されているSUSE Managerの仮想マシンイメージのオプションを使用

する方法です。必要なツールとコンテナイメージがすべてプリロードされていて、すぐに動作するためです。

SUSE Managerプロキシ仮想マシンのインストールの詳細については、[仮想マシンとしてのプロキシの配備](#)を参照してください。

SUSE Managerプロキシをアップグレードするには、[プロキシのアップグレード](#)で定義されている手順に従う必要があります。

2.2.4.3. SLE MicroにSUSE Managerを配備する

SUSE Managerでは、必要なコンテナイメージはすべてRPMでも提供されており、このイメージをシステムにインストールすることができます。

プロシージャ: Air-gappedでSLE MicroにSUSE Managerをインストールする

1. SLE Microをインストールします。
2. SUSE Managerサーバ上のクライアントとしてプロキシホストOSをブートストラップします。
3. システムを更新します。
4. ツールのパッケージとイメージのパッケージをインストールします(\$ARCH\$は適切なアーキテクチャに置き換えます)。

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

5. 再起動します。
6. mgrpxyを使用してSUSE Managerを配備します。

SLE MicroにSUSE Managerプロキシをインストールする方法の詳細については、[仮想マシンとしてのプロキシの配備](#)を参照してください。

SUSE Managerプロキシをアップグレードするには、[プロキシのアップグレード](#)で定義されている手順に従う必要があります。

Chapter 3. アップグレードと移行

3.1. サーバ

3.1.1. コンテナ化された環境へのSUSE Managerサーバの移行

SUSE Manager 4.3サーバをコンテナに移行するには、SLE Micro 5.5と`mgradm`がインストールされた新しいマシンが必要です。

基盤となるオペレーティングシステムがSUSE Linux Enterprise Server 15 SP4からSLE Micro 5.5に変更されたため、SUSE Manager 4.3から5.0へのインプレース移行は今後もサポートされないままです。



従来の接続プロトコルは、SUSE Manager 5.0移行ではサポートされなくなりました。Before migrating from SUSE Manager 4.3から'5.0'に移行する前に、従来のプロキシを含む既存の従来のクライアントをSaltに移行する必要があります。

従来のSUSE Manager 4.3クライアントからSaltクライアントへの移行については、<https://documentation.suse.com/suma/4.3/en/suse-manager/client-configuration/contact-methods-migrate-traditional.html>を参照してください。

自己信頼GPGキーは移行されません。RPMデータベースで信頼されているGPGキーのみが移行されます。したがって、`spacewalk-repo-sync`でチャンネルを同期すると失敗する可能性があります。



管理者は、サーバを実際に移行した後にこれらのキーを4.3のインストールからコンテナホストに手動で移行する必要があります。

1. 4.3サーバから新しいサーバのコンテナホストにキーをコピーします。
2. その後、コマンド`mgradm gpg add <PATH_TO_KEY_FILE>`を使用して、移行したサーバに各キーを追加します。

現在の移行手順には、ホスト名を変更するための機能が含まれていません。そのため、新しいサーバの完全修飾ドメイン名(FQDN)は古いサーバのFQDNと同じままです。さらに、クライアントがサーバに確実に接続できるよう、IPアドレスは変更しないままにする必要があります。移行後に、新しいサーバを指すようにDHCPとDNSレコードを手動で更新する必要があります。

3.1.1.1. 古い4.3サーバでの初期準備

プロシージャ: 4.3サーバでの初期準備

1. SUSE Managerサービスを停止します。

```
spacewalk-service stop
```

2. PostgreSQLサービスを停止します。

```
systemctl stop postgresql
```

3.1.1.2. SSH接続の準備



SLE Micro 5.5とmgradmがインストールされている必要があります。このサーバにSUSE Managerを事前インストールしないでください。移行プロセスでは、サーバのインストールが行われます。

プロシージャ: SSH接続を準備する

1. rootに対して、新しい'5.0'サーバ上にSSHキーが存在することを確認します。キーが存在しない場合は、次のコマンドを使用して作成します。

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

2. SSHの設定とエージェントが、4.3サーバにパスワードなしで接続する準備ができている必要があります。



パスワードレス接続を確立するために、移行スクリプトは、SSHエージェントが新しいサーバ上で実行されていることに依存します。エージェントがまだアクティブではない場合は、`eval $(ssh-agent)`を実行して開始します。次に、`ssh-add`をその後に機密鍵のパスを指定して実行し、実行されているエージェントにSSHキーを追加します。この処理中に機密鍵のパスワードの入力を求められます。

3. `ssh-copy-id`を使用して、SSH公開鍵をSUSE Manager 4.3サーバ(<oldserver.fqdn>)にコピーします。<oldserver.fqdn>は、4.3サーバのFQDNに置き換えてください。

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

SSHキーは、古いサーバの`~/.ssh/authorized_keys`ファイルにコピーされます。詳細については、`ssh-copy-id`のマニュアルページを参照してください。

4. 新しいサーバから古いSUSE ManagerサーバへのSSH接続を確立し、パスワードが不要であることを確認します。また、ホストの指紋に問題があってはなりません。問題がある場合は、古い指紋を`~/.ssh/known_hosts`ファイルから削除して、もう一度実行します。指紋はローカルの`~/.ssh/known_hosts`ファイルに保存されます。

3.1.1.3. 移行の実行



SUSE Manager 4.3からSUSE Manager 5.0への移行を計画する際には、ターゲットのインスタンスが古いセットアップの仕様を満たしているか上回っていることを確認してください。これには、メモリ(RAM)、CPUコア、ストレージ、ネットワーク帯域幅が含まれますが、これらに限定されません。

プロシージャ: 移行を実行する

このステップはオプションです。ご使用のインフラストラクチャにカスタムの永続ストレージが必要な場合は、`mgr-storage-server` ツールを使用します。詳細については、`mgr-storage-server --help` を参照してください。このツールを使用すると、コンテナストレージとデータベースボリュームの作成が容易になります。

- このコマンドは次のように使用します。

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

例:

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



このコマンドは、`/var/lib/containers/storage/volumes` に永続ストレージを作成します。

詳細については、[Installation-and-upgrade > Container-management](#) を参照してください。

1. 次のコマンドを実行して、新しい SUSE Manager サーバをインストールします。`<oldserver.fqdn>` は 4.3 サーバの FQDN に置き換えてください。

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

2. 信頼されている SSL CA 証明書を移行します。

RPMの一部としてインストールされ、SUSE Manager 4.3 の `/usr/share/pki/trust/anchors/` ディレクトリに保存されていた信頼済み SSL CA 証明書は移行されません。SUSEでは、RPMパッケージはコンテナ内にインストールされないため、これらの証明書は、移行後に管理者が次の手順で4.3のインストールから手動で移行する必要があります。



1. 4.3サーバから新しいサーバにファイルをコピーします。たとえば、`/local/ca.file` です。
2. 次のコマンドを使用してファイルをコンテナにコピーします。

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

`mgradm migrate` コマンドの実行が正常に完了した後も、すべてのクライアント上のSaltのセットアップはまだ古い4.3サーバを指したままです。



これらを'5.0'サーバにリダイレクトするために、新しいサーバの名前をインフラストラクチャレベル(DHCPおよびDNS)で変更し、4.3サーバと同じ完全修飾ドメイン名とIPアドレスを使用するようにする必要があります。

3.1.2. コンテナの更新

`upgrade` コマンドを実行する前に、まず `mgradm` ツールをアップグレードすることをお勧めします。

1. そのためには、次のコマンドを実行します。

```
transactional-update
```

2. 更新が適用されたら、`reboot` を実行して再起動します。
3. SUSE Manager '5.0' サーバコンテナは、次のコマンドを使用して更新できます。

```
mgradm upgrade podman
```

このコマンドは、コンテナのステータスを最新に更新してサーバを再起動します。

特定のバージョンへのアップグレード



タグパラメータを指定しない場合、デフォルトで最新バージョンにアップグレードされます。特定のバージョンにアップグレードするには、タグパラメータと目的のイメージタグを指定します。

`upgrade` コマンドとそのパラメータの詳細については、次のコマンドを使用します。

```
mgradm upgrade podman -h
```

Air-gappedインストールでは、まずコンテナのRPMパッケージをアップグレードし、その後 `mgradm` コマンドを実行します。

3.2. プロキシ

3.2.1. プロキシの移行

SUSE Manager 4.3では、RPMベース、Podman上でのコンテナ化、またはk3s上でのコンテナ化の3つの方法を使用してプロキシを配備できます。

SUSE Manager '5.0' では、Podmanで実行されるコンテナ化されたプロキシの管理が再設計され、`mgrpxy` ツールで簡単に管理できるようになりました。同時に、RPMベースのサポートは削除され、Podmanまたはk3s

で実行されるコンテナ化されたバージョンのみがサポートされるようになりました。

このセクションでは、`mgrpxy` ツールを使用したプロキシ4.3からの移行について説明します。



ホストOSがSUSE Linux Enterprise Server 15 SP4からSLE Micro 5.5に変更されたため、SUSE Manager 4.3から5.0へのインプレース移行はサポートされません。

従来の接続プロトコルは、SUSE Manager 5.0移行ではサポートされなくなりました。Before migrating from SUSE Manager 4.3から'5.0' に移行する前に、従来のプロキシを含む既存の従来のクライアントをSaltに移行する必要があります。

従来のSUSE Manager 4.3クライアントからSaltクライアントへの移行については、<https://documentation.suse.com/suma/4.3/en/suse-manager/client-configuration/contact-methods-migrate-traditional.html>を参照してください。

3.2.1.1. 新しいSUSE Managerプロキシの配備

インプレース移行はサポートされていないため、新しいFQDNを使用して新しいSUSE Managerプロキシを配備する必要があります。

- SUSE Managerプロキシの詳細については、[仮想マシンとしてのプロキシの配備](#)を参照してください。

3.2.1.2. 新しいプロキシへのクライアントの移行



クライアントを移行する前に、新しいプロキシが配備済みで完全に機能することを確認します。

プロシージャ: プロキシ間でクライアントを移行する

1. SUSE ManagerサーバのWeb UIにログインします。
2. 左側のナビゲーションから、:システム[システム一覧]を選択します。
3. 古い4.3プロキシのページに移動し、[**プロキシ**] タブを選択します。
4. 「SSM」に対するすべてのシステムを選択します。
5. 左側のナビゲーションから、**システム** > **システムセットマネージャ**を選択します。
6. サブメニューの**その他** > **プロキシ**を選択します。
7. ドロップダウンから、移行先の新しいプロキシを選択します。
8. [**プロキシの変更**]をクリックします。
9. このアクションの後、Minionsが新しいプロキシに移行されます。
10. スケジュールの進行状況をチェックして、すべてのシステムが正常に移行されたかどうかを確認できます。

数分後、マシンに新しい接続パスが表示され始めます。すべてのマシンに新しいプロキシ下の接続パスが設

定されたら、古い4.3のプロキシのマシンは不要なので削除できます。

3.2.2. コンテナの更新

upgradeコマンドを実行する前に、先にmgrpxyツールをアップグレードすることをお勧めします。

1. そのためには、次のコマンドを実行します。

```
transactional-update
```

2. 更新が適用されたら、`reboot`を実行して再起動します。
3. `podman`上で実行されるSUSE Manager '5.0' プロキシコンテナは、次のコマンドを使用して更新できます。

```
mgrpxy upgrade podman
```

Kubernetesクラスタ上で実行されるプロキシコンテナは、次のコマンドを使用して更新できます。

```
mgrpxy upgrade kubernetes
```

特定のバージョンへのアップグレード



タグパラメータを指定しない場合、デフォルトで最新バージョンにアップグレードされます。特定のバージョンにアップグレードするには、タグパラメータと目的のイメージタグを指定します。



特定のタグを使用して特定のコンテナをアップグレードするオプションはありますが、この機能はPTFの適用のみを意図しています。通常の状態では、すべてのプロキシコンテナに同じタグを使用して一貫性を確保することを強くお勧めします。

Air-gappedインストールでは、まずコンテナのRPMパッケージをアップグレードし、その後`mgradm`コマンドを実行します。

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. YAMLのカスタム設定とmgradmを使用した配備

カスタムのmgradm.yamlファイルを作成し、配備時にmgradmツールでこのファイルを利用することができます。



コマンドラインパラメータまたはmgradm.yaml設定ファイルで基本的な変数が指定されていない場合、mgradmによって入力を求められます。

セキュリティのため、コマンドラインパラメータを使用してパスワードを指定するのは避けることをお勧めします。代わりに、適切なパーミッションで設定ファイルを使用します。

プロシージャ: カスタム設定ファイルを使用してPodmanでSUSE Managerコンテナを配備する

1. 次の例のようなmgradm.yamlという名前の設定ファイルを準備します。

```
# データベースのパスワード。デフォルトでランダムに生成されます
db:
  password: MySuperSecretDBPass

# CA証明書のパスワード
ssl:
  password: MySuperSecretSSLPassword

# SUSEカスタマーセンターの資格情報
scc:
  user: ccUsername
  password: ccPassword

# 組織名
organization: YourOrganization

# 通知を送信する電子メールアドレス
emailFrom: notifications@example.com

# 管理者アカウントの詳細
admin:
  password: MySuperSecretAdminPass
  login: LoginName
  firstName: Admin
  lastName: Admin
  email: email@example.com
```

2. 端末からrootとして次のコマンドを実行します。サーバのFQDNの入力はオプションです。

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

コンテナはsudoまたはrootとして配備する必要があります。このステップを省略すると、端末に次のエラーが表示されます。



```
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. 配備が完了するまで待ちます。
4. ブラウザを開き、FQDNまたはIPアドレスの入力に進みます。

このセクションでは、YAMLのカスタム設定を使用してSUSE Manager '5.0' サーバコンテナを配備する方法について学びました。

4.2. コンテナの起動と停止

次のコマンドを使用して、SUSE Manager '5.0' サーバコンテナを再起動、起動、および停止できます。

SUSE Manager '5.0' サーバを再起動(**restart**)するには、次のコマンドを実行します。

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

サーバを起動(**start**)するには、次のコマンドを実行します。

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

サーバを停止(**stop**)するには、次のコマンドを実行します。

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

4.3. 永続ストレージボリュームのリスト

コンテナ内で行った変更は保持されません。永続ボリュームの外部で加えた変更は破棄されます。以下にSUSE Manager '5.0' の永続ボリュームのリストを示します。

デフォルトのボリュームの場所をカスタマイズするには、`podman volume create`コマンドを使用して、ポッドの最初の起動前に、必要なボリュームを作成するようにします。



この表は、Helmチャートおよびsystemctlサービス定義の両方で示されているボリュームマッピングに正確に従っています。

次のボリュームは、Podmanのデフォルトのストレージの場所に保存されます。

表 14. 永続ボリューム: Podmanのデフォルトストレージ

ボリューム名	ボリュームディレクトリ
Podman Storage	<code>/var/lib/containers/storage/volumes/</code>

表 15. 永続ボリューム: root

ボリューム名	ボリュームディレクトリ
root	<code>/root</code>

表 16. 永続ボリューム: var/

ボリューム名	ボリュームディレクトリ
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 17. 永続ボリューム: srv/

ボリューム名	ボリュームディレクトリ
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 18. 永続ボリューム: etc/

ボリューム名	ボリュームディレクトリ
etc-apache2	<code>/etc/apache2</code>

ボリューム名	ボリュームディレクトリ
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-sssd	/etc/sssd
etc-tomcat	/etc/tomcat
etc-cobbler	/etc/cobbler
etc-sysconfig	/etc/sysconfig
etc-tls	/etc/pki/tls
etc-postfix	/etc/postfix
ca-cert	/etc/pki/trust/anchors

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".