



SUSE Multi-Linux Manager 5.1

インストールおよびアップ グレードガイド

Chapter 1. 序文

Installation, Deployment and Upgrade | SUSE Multi-Linux Manager 5.1

このガイドでは、SUSE Multi-Linux Managerサーバおよびプロキシを配備、アップグレード、管理するための包括的な手順を段階的に説明します。

以下のセクションで構成されています。

- **要件:** スムーズなセットアップを確実に行うために必要なハードウェア、ソフトウェア、およびネットワークの前提条件を概説します。
- **配備とインストール:** SUSE Multi-Linux Managerをコンテナとして配備し、初期設定を完了する手順を説明します。
- **アップグレードと移行:** ダウンタイムを最小限に抑えながらSUSE Multi-Linux Managerをアップグレードおよび移行するプロセスを詳細に説明します。
- **基本的なサーバ管理:** 基本的なサーバ操作をカバーし、SUSE Multi-Linux Managerを効率的に開始するのに役立ちます。

発行日: 2025-12-12

Copyright © 2011–2025 SUSE LLC and contributors. All rights reserved. この文書は、GNUフリー文書ライセンスのバージョン1.2または(オプションとして)バージョン1.3の条項に従って、複製、頒布、および/または改変が許可されています。ただし、この著作権表示およびライセンスは変更せずに記載すること。ライセンスバージョン1.2のコピーは、**Legal > License**セクションに含まれています。

SUSEの商標については、<https://www.suse.com/company/legal/>を参照してください。その他の第三者のすべての商標は、各社の所有に帰属します。商標記号(®、™など)は、SUSEおよび関連会社の商標を示します。アスタリスク(*)は、第三者の商標を示します。本書のすべての情報は、細心の注意を払って編集されています。しかし、このことは絶対に正確であることを保証するものではありません。SUSE LLC、その関係者、著者、翻訳者のいずれも誤りまたはその結果に対して一切責任を負いかねます。

目次

1. 序文	1
2. 要件	4
2.1. 一般的な要件	4
2.1.1. SUSE Customer Centerアカウントと資格情報	4
2.1.2. SUSE Multi-Linux Manager Web UIでサポートされているブラウザ	4
2.1.3. SSL証明書	5
2.2. ハードウェア要件	5
2.2.1. サーバ要件	5
2.2.2. プロキシ要件	7
2.2.3. スワップ容量	8
2.2.4. データベースの要件	8
2.2.5. 永続ストレージとパーミッション	9
2.2.6. 論理ボリューム管理(LVM)	10
2.3. ネットワーク要件	10
2.3.1. 完全修飾ドメイン名(FQDN)	10
2.3.2. ホスト名とIPアドレス	11
2.3.3. ルータ広告の再有効化	11
2.3.4. HTTPまたはHTTPSのOSIレベル7プロキシの背後での配備	11
2.3.5. Air-gapped配備	12
2.3.6. 必須のネットワークポート	12
2.4. パブリッククラウドの要件	19
2.4.1. ネットワーク要件	19
2.4.2. ストレージボリュームの準備	20
3. インストールと配備	22
3.1. SUSE Multi-Linux Managerサーバのインストール	22
3.1.1. SUSE Multi-Linux Manager 5.1サーバの配備	22
3.1.2. 仮想マシンとしてのSUSE Multi-Linux Manager 5.1サーバの配備 - KVM	34
3.1.3. SUSE Multi-Linux Manager 5.1サーバの仮想マシンとしての配備 - VMware	40
3.1.4. SUSE Multi-Linux ManagerサーバのAir-gapped配備	43
3.1.5. パブリッククラウドの配備	46
3.1.6. PAYGインスタンスの接続	46
3.2. SUSE Multi-Linux Managerプロキシのインストール	49
3.2.1. SUSE Multi-Linux Manager 5.1プロキシの配備	49
3.2.2. クライアントをMLMプロキシに変換する	63
3.2.3. 仮想マシンとしてのSUSE Multi-Linux Managerプロキシの配備 - KVM	67
3.2.4. SUSE Multi-Linux Managerプロキシの仮想マシンとしての配備 - VMware	77
3.2.5. K3sへのSUSE Multi-Linux Manager 5.1プロキシの配備	84
3.2.6. SUSE Multi-Linux ManagerプロキシのAir-gapped配備	88
4. アップグレードと移行	90
4.1. サーバ	90
4.1.1. ディストリビューションのアップグレードとサーバ移行	90
4.1.2. コンテナ化された環境へのSUSE Multi-Linux Managerサーバの移行	97
4.1.3. SUSE Multi-Linux Managerサーバのアップグレード	108
4.2. プロキシ	110
4.2.1. Proxy Migration from 5.0 to 5.1	110
4.2.2. Proxy Migration from 4.3 to 5.1	117
4.2.3. SUSE Multi-Linux Managerプロキシのアップグレード	119
4.3. クライアント	120
4.3.1. クライアントのアップグレード	120
5. 基本的なサーバとプロキシの管理	122
5.1. YAMLのカスタム設定とmgradmを使用した配備	122
5.2. コンテナの起動と停止	123
5.3. SUSE Multi-Linux Managerで使用するコンテナ	123
5.4. 永続コンテナボリューム	124
5.4.1. サーバ	124

5.4.2. プロキシ	126
5.5. mgr-storage-server および mgr-storage-proxy について	126
5.5.1. これらのツールの機能	127
5.5.2. これらのツールが実行*しない*こと	127
5.5.3. インストール後のストレージ管理	127
5.5.4. 使用する場合、使用しない場合	128
5.5.5. 概要	128
6. GNU Free Documentation License	129

Chapter 2. 要件

2.1. 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、SUSE Multi-Linux Managerサーバ、プロキシ、およびRetail Branch Serverの登録キーにアクセスできます。
2. SUSE Multi-Linux 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 Multi-Linux Manager 5.1は自己署名証明書を使用します。



SL Micro 6.1エンタイトルメントは、SUSE Multi-Linux Managerエンタイトルメント内に含まれているため、別途登録キーは必要ありません。

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。

2.1.1. SUSE Customer Centerアカウントと資格情報

SUSE Multi-Linux Manager 5.1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 Multi-Linux 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。

2.1.2. SUSE Multi-Linux 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 Multi-Linux 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 Multi-Linux 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 Multi-Linux ManagerのWeb UIはWindows Internet Explorerでは正しくレンダリングされません。

2.1.3. SSL証明書

SUSE Multi-Linux 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 Multi-Linux 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 Multi-Linux 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。

2.2. ハードウェア要件

以下の表は、x86-64、ARM、ppc64le、およびs390xアーキテクチャのSUSE Multi-Linux 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。



ppc64leまたはs390xアーキテクチャに基づくSUSE Multi-Linux Managerのインストールでは、ネットワークブートクライアントにセキュアブートを使用できません。この制限は、これらのアーキテクチャの両方でshimブートローダが利用できないために存在します。

SUSE Multi-Linux 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。

2.2.1. サーバ要件

SL Micro 6.1またはSUSE Linux Enterprise Server 15 SP7の1つは、コンテナホストのオペレーティングシステムです。

以下では、インストールされているホストオペレーティングシステムであるSUSE Linux Enterprise Serverは、それが重要な場合にのみ明示的に言及されます。それ以外の場合は、SL Microと表記するか、単にホストオペレーティングシステムと表記します。

オペレーティングシステムとしてSL Microを使用するコンテナホストに必要な空きディスク容量は次のとおりです。

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

選択したソフトウェアの量によっては、SUSE Linux Enterprise Serverをオペレーティングシステムとして使

用する場合、ディスク容量がかなり必要になる場合があります。

デフォルトでは、SUSE Multi-Linux Managerサーバコンテナは、ミラーリングされたりポジトリ(パッケージまたは製品)、データベース、およびその他のデータを `/var/lib/containers/storage/volumes/`ディレクトリのサブ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。ミラーリングする予定のクライアントおよびリポジトリの数と種類に基づいて、`/var/lib/containers/storage/volumes/`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、ppc64le、または s390x	専用64ビットCPUコア数は4つ以上
RAM	最小	16GB
	推奨	32GB
ディスク容量	<code>/</code> (ルートディレクトリ)	40GB
	<code>/var/lib/containers/storage/volumes</code>	150GB以上(製品数によって異なります)
	<code>/var/lib/containers/storage/volumes/var-pgsql</code>	50GB以上
スワップ容量	システムは追加のスワップ容量からメリットを得ることができます。SUSEでは、スワップパーティションではなく、スワップファイルの使用を推奨しています。スワップ容量の詳細については、 installation-and-upgrade:hardware-	8~12GB

デフォルトでイメージには40GBの/`パーティション`があります。SL Micro 6.1のクラウドイメージには、わずか5GBの/`パーティション`しかありません。どちらもSUSE Multi-Linux Managerで問題なく動作します。外部ストレージが`/var/lib/containers/storage/volumes`にマウントされている限り、SUSE Multi-Linux Managerは/`パーティション`上のストレージを必要とせず、使用しません。その管理はコンテナホスト自体に委ねられます。



SUSE Multi-Linux 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 Multi-Linux 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。

2.2.2. プロキシ要件

SL Micro 6.1またはSUSE Linux Enterprise Server 15 SP7の1つは、コンテナホストのオペレーティングシステムです。



最低要件は、クライアントが1つある1つのプロキシなど、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、推奨値から開始してください。

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
	推奨	最小値と同じ
RAM	最小	2GB
	推奨	8GB
ディスク容量	/ (ルートディレクトリ)	40GB以上
	<code>/var/lib/containers/storage/volumes</code>	100GB以上
スワップ容量	システムは追加のスワップ容量からメリットを得ることができます。SUSEでは、スワップパーティションではなく、スワップファイルの使用を推奨しています。スワップ容量の詳細については、 installation-and-upgrade:hardware-	4～8GB

デフォルトでは、SUSE Multi-Linux Managerプロキシコンテナは、`/var/lib/containers/storage/volumes/uyuni-proxy-squid-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/uyuni-proxy-squid-cache/`ディレクトリの容量を大きくすると、プロキシとSUSE Multi-Linux 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/uyuni-proxy-squid-cache/`ディレクトリをSUSE Multi-Linux 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/uyuni-proxy-squid-cache/`ディレクトリは、SUSE Multi-Linux

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。



一般的に、SUSEでは、キャッシュディレクトリの値を、利用可能な空き容量の約80%に調整することを推奨しています。**cache_dir**の値は、サーバ上でプロキシ設定を生成する際に設定されます。**squid.conf**で直接オプションを設定することはできません。

2.2.3. スワップ容量

ワークロードはシステムごとに異なります。ワークロードが重い、予測不可能なシステムでは、総RAM量に関わらずスワップ容量を追加することでメリットが得られます。スワップ容量は利用可能な最速のストレージ(例: SSD)に配置することをお勧めします。SUSEではスワップパーティションではなくスワップファイルの使用を推奨しています。

サイズの推奨事項については、上記の表を参照してください。

以下のシェルコマンドスニペットは8GiBスワップファイルを作成します。



Btrfsファイルシステム上のスワップファイルは、そのボリュームのスナップショットの作成を妨げます。以下の例における**/var**はすでにsnapperスナップショットから除外されているため、**/var/swap**を安全に使用できます。

```
## setup swapfile at /var/swap
# run following as a root user

# allocate 8GiB for swap file
fallocate -l 8G /var/swap
# ensure CoW is disabled for the swap file
chattr +C /var/swap
# allow only root access
chmod 600 /var/swap
# make swap file based on allocated file
mkswap /var/swap
# activate swap use for the running system
swapon /var/swap
# activate swap during the next boots
echo "/var/swap swap swap defaults 0 0" >> /etc/fstab
```

2.2.4. 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 Multi-Linux 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 Multi-Linux 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。

2.2.5. 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、ボリュームは1つ以上の個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。これは、コンテナの配備後に実行できません。

ストレージデバイスは最初にコンテナを配備した後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。

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。リポジトリストレージのディスクのサイズは、SUSE Multi-Linux 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。



CobblerまたはPostgreSQLのストレージにNFSを使用しないでください。また、SELinux環境でもNFSを使用しないでください。これらのシナリオはサポートされていません。

SUSE Multi-Linux 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、外部ディスクをストレージの場所に設定し、オプションでデータベース用の独自のディスク上に設定することもできます。

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

例:

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

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。



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。

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。

2.2.6. 論理ボリューム管理(LVM)

すべての種類の仮想マシン(VM)では、LVMは一般的に必要なく、推奨されません。ディスクのセットアップは仮想的であり、ボリュームごとに個別のディスクが可能であり、推奨されます。

その他の配備については、ボリュームごとに個別のディスクも推奨されます。

SUSE Multi-Linux Managerサーバのコンテナホストでは、**mgr-storage-server**コマンドが**/var/lib/containers/storage/volumes**ディレクトリの内容全体を別のディスクに移動し、**/var/lib/containers/storage/volumes**に再マウントします。

オプションで、2つ目のデバイス名を指定した場合、**mgr-storage-server**は**/var/lib/containers/storage/volumes/var-pgsql**データベースディレクトリの内容を別の2つ目のディスクに移動し、**/var/lib/containers/storage/volumes/var-pgsql**に再マウントします。

同様に、SUSE Multi-Linux Managerプロキシのコンテナホストでは、**mgr-storage-proxy**コマンドは、**/var/lib/containers/storage/volumes**ディレクトリの内容全体を別のディスクに移動し、**/var/lib/containers/storage/volumes**に再マウントします。

2.3. ネットワーク要件

このセクションでは、SUSE Multi-Linux 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。



IP転送は、コンテナ化されたインストールによって有効になります。つまり、SUSE Multi-Linux Managerサーバとプロキシはルータとして動作します。この動作はpodmanによって直接実行されます。IP転送が無効になっている場合、Podmanコンテナは実行されません。

ポリシーに従って、SUSE Multi-Linux Manager環境のネットワーク分離を実現することを検討してください。

詳細については、<https://www.suse.com/support/kb/doc/?id=000020166>を参照してください。

2.3.1. 完全修飾ドメイン名(FQDN)

SUSE Multi-Linux 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-SP6/html/SLES-all/cha-network.html#sec-network-yast-change-host>を参照してください。

2.3.2. ホスト名とIPアドレス

SUSE Multi-Linux 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-SP6/html/SLES-all/cha-dns.html>を参照してください。

2.3.3. ルータ広告の再有効化

SUSE Multi-Linux Managerを**mgradm install podman**または**mgrpky install podman**を使用してインストールすると、IPv4とIPv6の転送を有効にするPodmanが設定されます。これは、コンテナの外側から通信を行うために必要です。

ただし、システムで以前に**/proc/sys/net/ipv6/conf/eth0/accept_ra**を**1**に設定していた場合、ルータ広告の使用が停止されます。その結果、ルートがルータ広告経由で取得されなくなり、デフォルトのIPv6ルートが消失します。

IPv6ルーティングの正常な機能を回復するには、次のプロシージャに従います。

プロシージャ: ルータ広告の再有効化

1. **/etc/sysctl.d**にファイルを作成します。例: **99-ipv6-ras.conf**。
2. 次のパラメータと値をファイルに追加します。

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

3. 再起動します。

2.3.4. HTTPまたはHTTPSのOSIレベル7プロキシの背後での配備

一部の環境では、HTTPまたはHTTPSプロキシを介したインターネットアクセスが強制されています。これはSquidサーバなどのサーバが対象となります。このような設定でSUSE Multi-Linux Managerサーバのインターネットアクセスを許可するには、次のように設定する必要があります。

プロシージャ: HTTPまたはHTTPS OSIレベル7プロキシの設定

1. オペレーティングシステムのインターネットアクセスの場合は、必要に応じて**/etc/sysconfig/proxy**を変更します。

```
PROXY_ENABLED="no"  
HTTP_PROXY=""  
HTTPS_PROXY=""
```



```
NO_PROXY="localhost, 127.0.0.1"
```

2. Podmanコンテナのインターネットアクセスの場合は、必要に応じて`/etc/systemd/system/uyuni-server.service.d/custom.conf`を変更します。たとえば、次のように設定します。

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

3. Javaアプリケーションのインターネットアクセスの場合は、必要に応じて`/etc/rhn/rhn.conf`を変更します。コンテナホストで、`mgrctl term`を実行し、サーバコンテナ内でコマンドラインを開きます。

- a. 必要に応じて`/etc/rhn/rhn.conf`を変更します。たとえば、次のように設定します。

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

4. コンテナホストでサーバを再起動して、新しい設定を適用します。

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

2.3.5. 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 Multi-Linux 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:network-requirements.pdf](#)を参照してください。

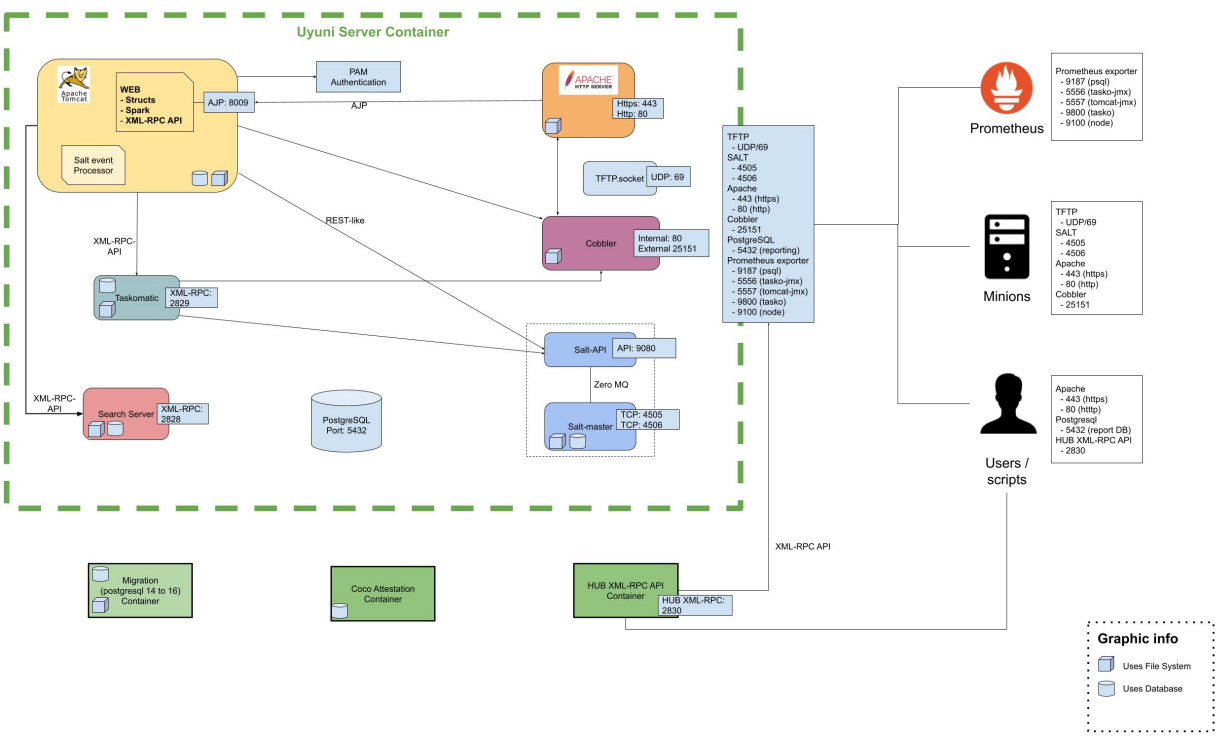
2.3.6. 必須のネットワークポート

このセクションには、SUSE Multi-Linux 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。

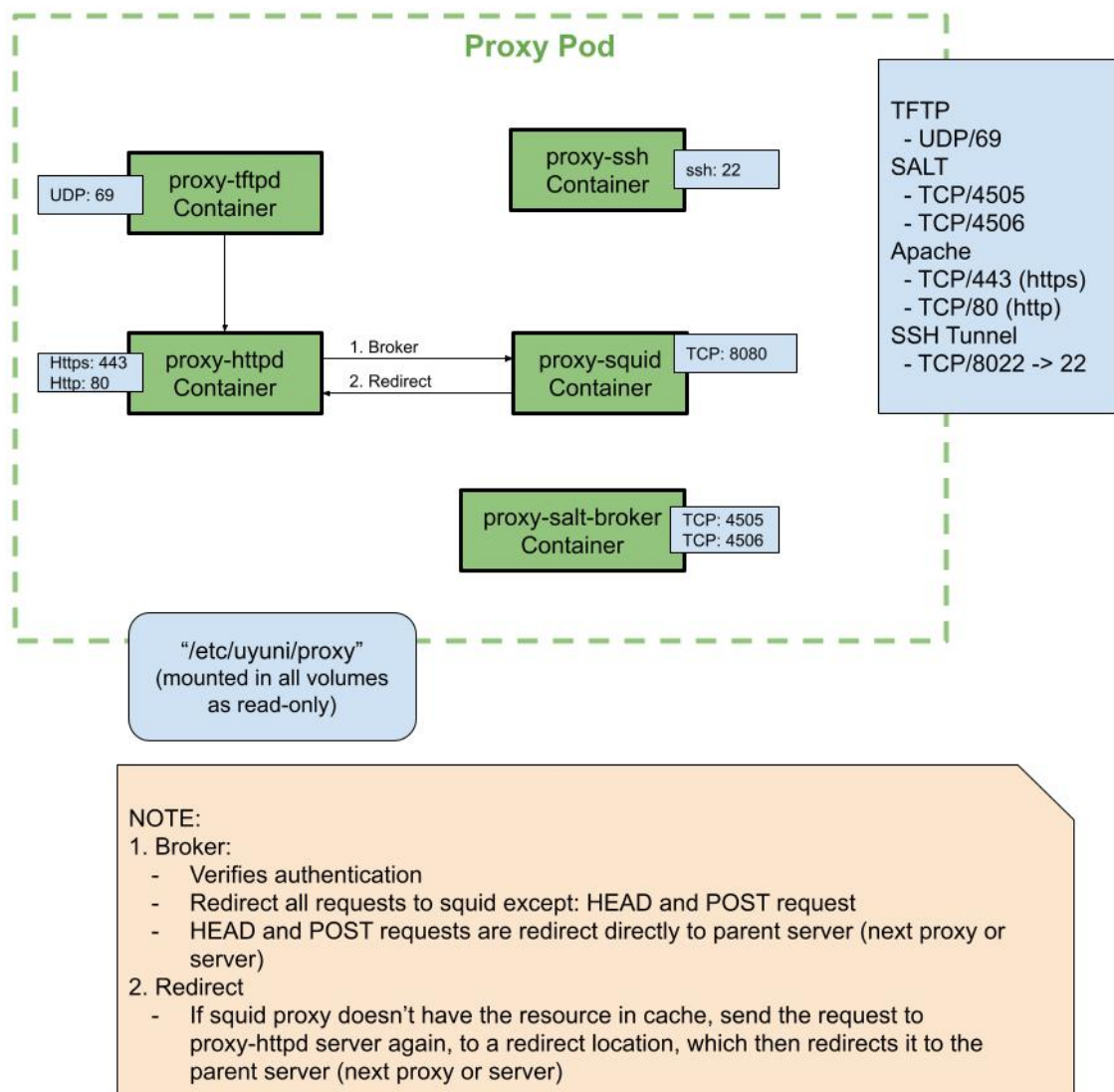
これらのポートすべてを開く必要はありません。サービスの使用に必要なポートのみを開く必要があります。

2.3.6.1. 概要

2.3.6.1.1. サーバ



2.3.6.1.2. プロキシ



2.3.6.2. 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 Multi-Linux 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 Multi-Linux Managerサーバにアクセスできるようになります。

表 3. SUSE Multi-Linux Managerサーバの外部ポートの要件

Port number	Protocol	Used By	Notes
67	TCP/UDP	DHCP	Required only if clients are requesting IP addresses from the server.

Port number	Protocol	Used By	Notes
69	TCP/UDP	TFTP	Required if server is used as a PXE server for automated client installation.
80	TCP	HTTP	Required temporarily for some bootstrap repositories and automated installations.
443	TCP	HTTPS	Serves the Web UI, client, and server and proxy (tftpsync) requests.
4505	TCP	salt	Required to accept communication requests from clients. The client initiates the connection, and it stays open to receive commands from the Salt master.
4506	TCP	salt	Required to accept communication requests from clients. The client initiates the connection, and it stays open to report results back to the Salt master.
5432	TCP	PostgreSQL	Required to access the reporting database.
5556	TCP	Prometheus	Required for scraping Taskomatic JMX metrics.
5557	TCP	Prometheus	Required for scraping Tomcat JMX metrics.
9100	TCP	Prometheus	Required for scraping Node exporter metrics.
9187	TCP	Prometheus	Required for scraping PostgreSQL metrics.
9800	TCP	Prometheus	Required for scraping Taskomatic metrics.
25151	TCP	Cobbler	

2.3.6.3. 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 Multi-Linux 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 Multi-Linux 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 Multi-Linux 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が必要です。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が必要です。
25151	TCP	Cobbler	

2.3.6.4. 内部サーバポート

内部ポートは、SUSE Multi-Linux 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 Multi-Linux 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す。
25151	CobblerのXMLRPC API
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
```

2.3.6.5. 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 Multi-Linux 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 Multi-Linux Managerプロキシにアクセスできるようになります。

表 6. SUSE Multi-Linux 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			ユーザがSalt SSHを使用してプロキシホストを管理する場合にのみ必要です。
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。
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。
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。
8022			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。

2.3.6.6. 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 Multi-Linux 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 Multi-Linux 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 Multi-Linux 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。
4505	TCP	Salt	Saltマスターに直接またはプロキシ経由で接続する必要があります。
4506	TCP	Salt	Saltマスターに直接またはプロキシ経由で接続する必要があります。

2.3.6.7. 外部クライアントポート

SUSE Multi-Linux Managerサーバとそのクライアントの間に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 Multi-Linux 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。
443	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。
4505	送信	TCP	Saltマスターに直接またはプロキシ経由で接続する必要があります。
4506	送信	TCP	Saltマスターに直接またはプロキシ経由で接続する必要があります。
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ノードエクスポータに必要です。
9117	送信	TCP	Prometheus Apacheエクスポータに必要です。
9187	送信	TCP	Prometheus PostgreSQLに必要です。

2.3.6.8. 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 Multi-Linux 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
- installer-updates.suse.com
- registry.suse.com
- registry-storage.suse.com
- opensuse.org

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

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

指定したURLとそれに関連するIPアドレスをホワイトリストに登録する方法の詳細については、次の記事を参照してください: [ファイアウォール内および/またはプロキシ経由でSUSE Customer CenterとSUSEレジストリにアクセスする](#)。

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。

2.4. 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 Multi-Linux 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。

始める前に、考慮事項を次に示します。

- SUSE Multi-Linux 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 Multi-Linux 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 Multi-Linux 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 Multi-Linux 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。

2.4.1. ネットワーク要件

パブリッククラウドでSUSE Multi-Linux 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。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 Multi-Linux Managerを実行するということは、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 Multi-Linux 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 Multi-Linux 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 Multi-Linux 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。

2.4.2. ストレージボリュームの準備

リポジトリとSUSE Multi-Linux 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 Multi-Linux 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 Multi-Linux 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 Multi-Linux 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 Multi-Linux 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 Multi-Linux 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。

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 3. インストールと配備

3.1. SUSE Multi-Linux Managerサーバのインストール

SUSE Multi-Linux Managerサーバを配備するさまざまなシナリオがあります。

3.1.1. SUSE Multi-Linux Manager 5.1サーバの配備

このガイドでは、SL Micro 6.1またはSUSE Linux Enterprise Server 15 SP7にSUSE Multi-Linux Manager 5.1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。

3.1.1.1. SUSE Multi-Linux Managerのハードウェア要件

次の表に、SUSE Multi-Linux 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 9. 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	SL Micro 6.1または SUSE Linux Enterprise Server 15 SP7
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	200GB
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:	8〜12GB

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SL Micro 6.1またはSUSE Linux Enterprise Server 15 SP7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:

- **mlm.example.com**
- **mlm.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。

3.1.1.2. 永続ボリューム

SUSE Multi-Linux Manager 5.1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。ここには、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 Multi-Linux 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、SL Micro 6.1でサポートされているファイルシステムであればどれも動作可能)。

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 Multi-Linux 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。

3.1.1.3. SUSE Multi-Linux Managerサーバホストの準備

SUSE Multi-Linux ManagerはSL Micro 6.1またはSUSE Linux Enterprise Server 15 SP7に配備できます。SL Microはトランザクションシステムであり、SUSE Linux Enterprise Serverはフルサーバオペレーティングシステムです。

決定に応じて、[installation-and-upgrade:container-deployment/mlm/server-deployment-mlm.pdf](#)または[installation-and-upgrade:container-deployment/mlm/server-deployment-mlm.pdf](#)を続行し、選択されていないセクションをスキップしてください。

3.1.1.3.1. SLE Micro 6.1ホストの準備

インストールメディアのダウンロード

Procedure: Downloading the installation media

1. <https://www.suse.com/download/sle-micro/>でSL Micro 6.1のインストールメディアを見つけて、適切なメディアファイルをダウンロードします。
2. 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。

SL Micro 6.1のインストール

マシン(仮想または物理)の準備の詳細については、[SL Micro配備ガイド](#)を参照してください。

プロシージャ: SL Micro 6.1のインストール

1. SLE Micro 6.1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。
2. システムをブートまたは再起動します。
3. 矢印キーを使用してインストールを選択します。
4. キーボードと言語を調整します。
5. 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。
6. 次へをクリックして続行します。

7. 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。



SUSE Multi-Linux Manager 5.1コンテナは拡張機能としてインストールされます。以下のリストから必要な特定の拡張機能に応じて、それぞれに追加のSUSE Customer Center登録コードが必要です。

- SUSE Multi-Linux Manager 5.1サーバ
- SUSE Multi-Linux Manager 5.1プロキシ
- SUSE Multi-Linux Manager 5.1 Retail Branch Server



SL Micro 6.1エンタイトルメントは、SUSE Multi-Linux Managerエンタイトルメント内に含まれているため、別途登録コードは必要ありません。

8. SUSE Customer Centerの電子メールアドレスを入力します。
9. SL Micro 6.1の登録コードを入力します。
10. **次へ**をクリックして続行します。
11. プロキシをインストールするにはSUSE Multi-Linux Manager 5.1プロキシ拡張機能、サーバをインストールするにはSUSE Multi-Linux Manager 5.1サーバ拡張機能の**チェックボックス**を選択します。
12. **次へ**をクリックして続行します。
13. SUSE Multi-Linux Manager 5.1拡張機能の登録コードを入力します。
14. **[次へ]**をクリックして続行します。
15. NTP設定ページで、**[次へ]**をクリックします。
16. **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。
17. 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SL Micro 6.1とSUSE Multi-Linux Manager 5.1のインストールが完了しました。

オプション: コマンドラインからの登録

SL Micro 6.1のインストール中にSUSE Multi-Linux Manager 5.1を拡張機能として追加した場合は、このプロセス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、SL Micro 6.1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、SL Micro 6.1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。



次のステップでは、SUSE Multi-Linux Manager 5.1拡張機能を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アーキテクチャを登録する場合は、正しい登録コードを使用してください。

Procedure: Registering from the command line

1. 次のコマンドで利用可能な拡張機能を一覧表示します。

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

2. 利用可能な拡張機能のリストから、インストールしたい拡張機能を選択します。

- a. サーバをインストールする場合は、次のコマンドで SUSE Multi-Linux Manager Server Extension 5.1 x86_64の登録コードを使用します。

```
transactional-update register -p Multi-Linux-Manager-Server/5.1/x86_64 -r <reg_code>
```

- b. プロキシをインストールする場合は、次のコマンドでSUSE Multi-Linux Manager Proxy Extension 5.1 x86_64の登録コードを使用します。

```
transactional-update register -p Multi-Linux-Manager-Proxy/5.1/x86_64 -r <reg_code>
```

3. 再起動します。

システムの更新

Procedure: Updating the system

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。



SL Microはデフォルトで自己更新するように設計されており、更新を適用すると再起動します。ただし、SUSE Multi-Linux Manager環境ではこの動作は望ましくありません。サーバの自動更新を防ぐには、SUSE Multi-Linux Managerでブートストラッププロセス中にtransactional-updateのタイマを無効にします。

SL 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を有効にします。

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

配備を続行するには、[installation-and-upgrade:container-deployment/mlm/server-deployment-mlm.pdf](#)を参照してください。

3.1.1.3.2. Prepare SUSE Linux Enterprise Server 15 SP7 host

または、SUSE Linux Enterprise Server 15 SP7にSUSE Multi-Linux Managerを配備することもできます。

The following procedures describe the main steps of the installation process.

Install SUSE Multi-Linux Manager extensions on SUSE Linux Enterprise Server

Procedure: Installing SUSE Multi-Linux Manager Extensions on SUSE Linux Enterprise Server

1. <https://www.suse.com/download/sles/>でSUSE Linux Enterprise Server 15 SP7 .isoを見つけてダウンロードします。
2. ホストオペレーティングシステム(SUSE Linux Enterprise Server 15 SP7)と拡張機能の両方の登録コードがあることを確認します。
3. SUSE Linux Enterprise Server 15 SP7のインストールを開始します。
 - a. **Language, Keyboard and Product Selection**（言語、キーボードおよび製品の選択）で、インストールする製品を選択します。
 - b. **ライセンス契約**で契約を読み、**[I Agree to the License Terms**（ライセンス条項に同意します）にチェックを付けます。
4. 登録方法を選択します。この例では、SUSEカスタマーセンターにサーバを登録します。
5. SUSE Customer Centerの電子メールアドレスを入力します。
6. SUSE Linux Enterprise Server 15 SP7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。



SUSE Linux Enterprise Server 15 SP7には、有効なSUSE Linux Enterprise Serverサブスクリプションと対応する登録コードが必要であり、この画面で入力する必要があることに注意してください。以下でSUSE Multi-Linux Manager拡張機能の登録コードを入力する必要があります。

8. 拡張とモジュールの選択で、以下にチェックを付けます。

- サーバをインストールするにはSUSE Multi-Linux Managerサーバ拡張機能を選択し、プロキシをインストールするにはSUSE Multi-Linux Managerプロキシ拡張機能を選択します。
- ベースシステムモジュール
- Containersモジュール

9. 次へをクリックして続行します。

10. SUSE Multi-Linux Manager 5.1拡張機能の登録コードを入力します。

11. [次へ]をクリックして続行します。

12. インストールを完了します。

13. インストールが完了したら、rootとして新しくインストールしたサーバにログインします。

14. システムを更新します(オプション。インストール時にシステムが更新をダウンロードするように設定されていない場合)。

```
zypper up
```

15. 再起動します。

オプション: コマンドラインからの登録

If you added SUSE Multi-Linux Manager 5.1 as an extension during SUSE Linux Enterprise Server installation then you can skip this procedure.

However, optionally you may skip registration during SUSE Linux Enterprise Server installation by selecting the [**Skip Registration**] button. This section provides steps on registering your products after SUSE Linux Enterprise Server installation.



The following steps register a SUSE Multi-Linux Manager 5.1 extension with the x86-64 architecture and thus require a registration code for the x86-64 architecture.

To register ARM or s390x architectures use the correct registration code.

Procedure: Registering from the command line

1. 次のコマンドで利用可能な拡張機能を一覧表示します。

```
SUSEConnect --list-extensions
```

From the list of available extensions, select the one you wish to install. If installing the Server, use your SUSE Multi-Linux Manager Server Extension 5.1 x86_64 registration code. For example for SUSE Linux Enterprise 15 SP7, use the following commands:

```
SUSEConnect -r <regcode>
SUSEConnect -p sle-module-containers/15.7/x86_64
SUSEConnect -p Multi-Linux-Manager-Server-SLE/5.1/x86_64 -r <regcode>
```

- If installing the Proxy, use your SUSE Multi-Linux Manager Proxy Extension 5.1 x86_64 registration code with the following command:

```
SUSEConnect -p Multi-Linux-Manager-Proxy-SLE/5.1/x86_64 -r <regcode>
```

Install and enable podman

Procedure: Installing podman

1. Log in as root and install the product package.

- On the server:

```
zypper in podman
zypper in -t product SUSE-Multi-Linux-Manager-Server
```

- On the proxies:

```
zypper in podman
zypper in -t product SUSE-Multi-Linux-Manager-Proxy
```



Make sure that package **podman** is installed. Additionally, on the server **mgradm** and **mgradm-bash-completion** or on the proxies, **mgrpky** and **mgrpky-bash-**

completion also need to be installed.

2. システムを再起動するか、次のコマンドを実行してPodmanサービスを起動します。

```
systemctl enable --now podman.service
```

配備を続行するには、[installation-and-upgrade:container-deployment/mlm/server-deployment-mlm.pdf](#)を参照してください。

3.1.1.4. 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**

3.1.1.5. mgradmを使用したSUSE Multi-Linux Managerの配備

自己署名証明書の代わりに、サードパーティSSL証明書を使用する場合は、以下の配備プロシージャの実行時にインポートします。



サードパーティSSL証明書の要件の詳細については、**Administration › Ssl-certs-imported**を参照してください。



SUSE Multi-Linux Manager server hosts that are hardened for security may restrict execution of files from the **/tmp** folder. In such cases, as a workaround, export the

TMPDIR environment variable to another existing path before running **mgradm**.

例:

```
export TMPDIR=/path/to/other/tmp
```

SUSE Multi-Linux Managerの更新では、この回避策が不要になるようにツールが変更されます。

プロシージャ: mgradmを使用してSUSE Multi-Linux Manager 5.1を配備する

1. rootとしてログインします。
2. Deploy SUSE Multi-Linux Manager.



If you use VM images as a migration target, here as the last step, execute the command **mgradm migrate** instead of **mgradm install**.

Execute one of the following commands, depending on the SSL certificate variant (self-signed or third-party). Replace **<FQDN>** with your fully qualified domain name of the SUSE Multi-Linux Manager Server:

- SUSE Multi-Linux Managerで提供される自己署名証明書を使用する場合:

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

- サードパーティSSL証明書フラグを使用してSSL証明書をインポートする場合(これらすべての証明書が必要なわけではない場合は例を調整可能):

```
mgradm install podman <FQDN> \
--ssl-ca-intermediate <strings> \
--ssl-ca-root <string> \
--ssl-server-cert <string> \
--ssl-server-key <string> \
--ssl-db-ca-intermediate <strings> \
--ssl-db-ca-root <string> \
--ssl-db-cert <string> \
--ssl-db-key <string>
```

詳細については、**mgradm install podman --help**を参照してください。



実行したコマンドが失敗する場合は、SUSE Multi-Linux Manager 5.1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 Multi-Linux Manager 5.1の登録キーを使用します。

3. 入力を求められたら、CAキー(認証局)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。

このガイドでは、SUSE Multi-Linux Manager 5.1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。

3.1.1.6. SUSE Customer CenterへのSUSE Multi-Linux Manager 5.1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 Multi-Linux 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 Multi-Linux 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 Customer Center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.

- 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ットが提供されます。

- 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 Multi-Linux

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 Multi-Linux 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アソースをSUSE Multi-Linux 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 Multi-Linux 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 Multi-Linux Manager 5.1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。

3.1.1.7. 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
```

3.1.2. 仮想マシンとしてのSUSE Multi-Linux Manager 5.1サーバの配備 - KVM

この章では、SUSE Multi-Linux Manager 5.1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。

3.1.2.1. 利用可能なイメージ



SUSE Multi-Linux Manager 5.1サーバ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 Multi-Linux Manager 5.1のイメージは[SUSE Multi-Linux Manager 5.1 VM images](#)で入手できます。



カスタマイズされたSUSE Multi-Linux Manager 5.1 VMイメージは、SL Micro 6.1にのみ提供されます。SUSE Linux Enterprise Server 15 SP7で製品を実行するには、<https://www.suse.com/download/sles/>で入手可能な標準のSUSE Linux Enterprise Server 15 SP7インストールを使用し、その上でSUSE Multi-Linux Manager 5.1拡張機能を有効にします。

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。

3.1.2.2. 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、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 Multi-Linux Manager-Server.x86_64-5.1.*.qcow2
メモリ:	最小*)
CPU:	最小*)
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

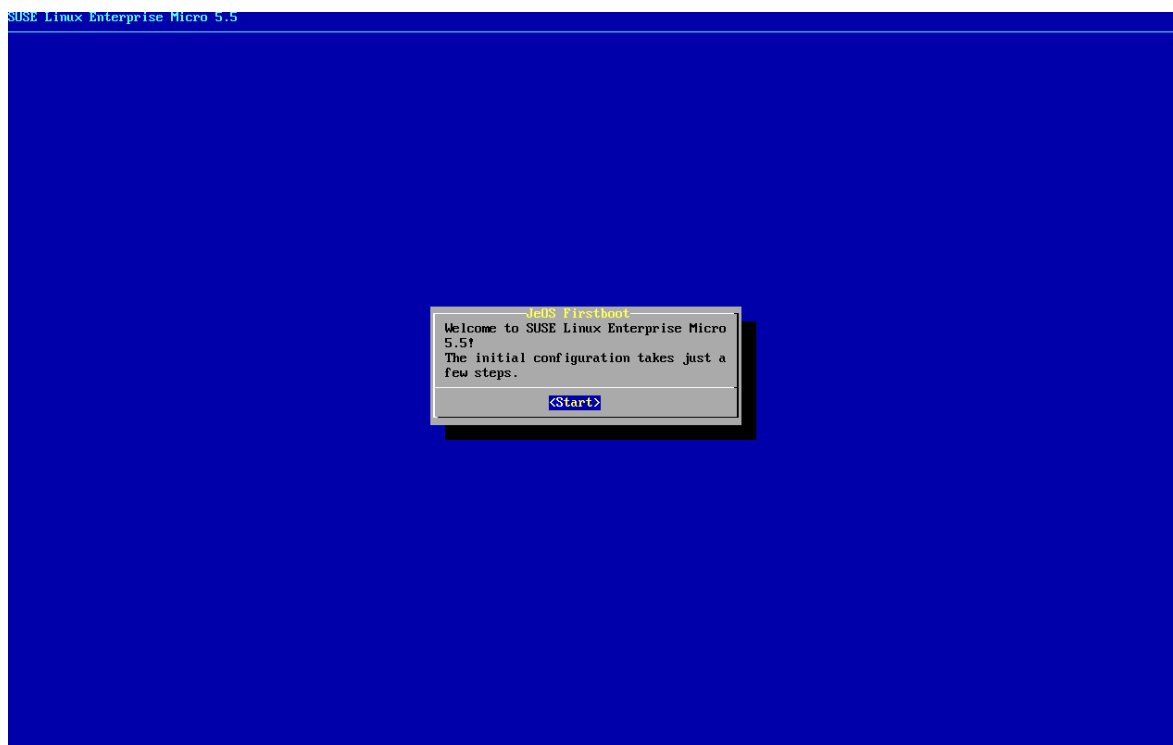
*) 最小値については、[installation-and-upgrade:hardware-requirements.pdf](#)を参照してください。

3.1.2.3. KVMの初期セットアップ

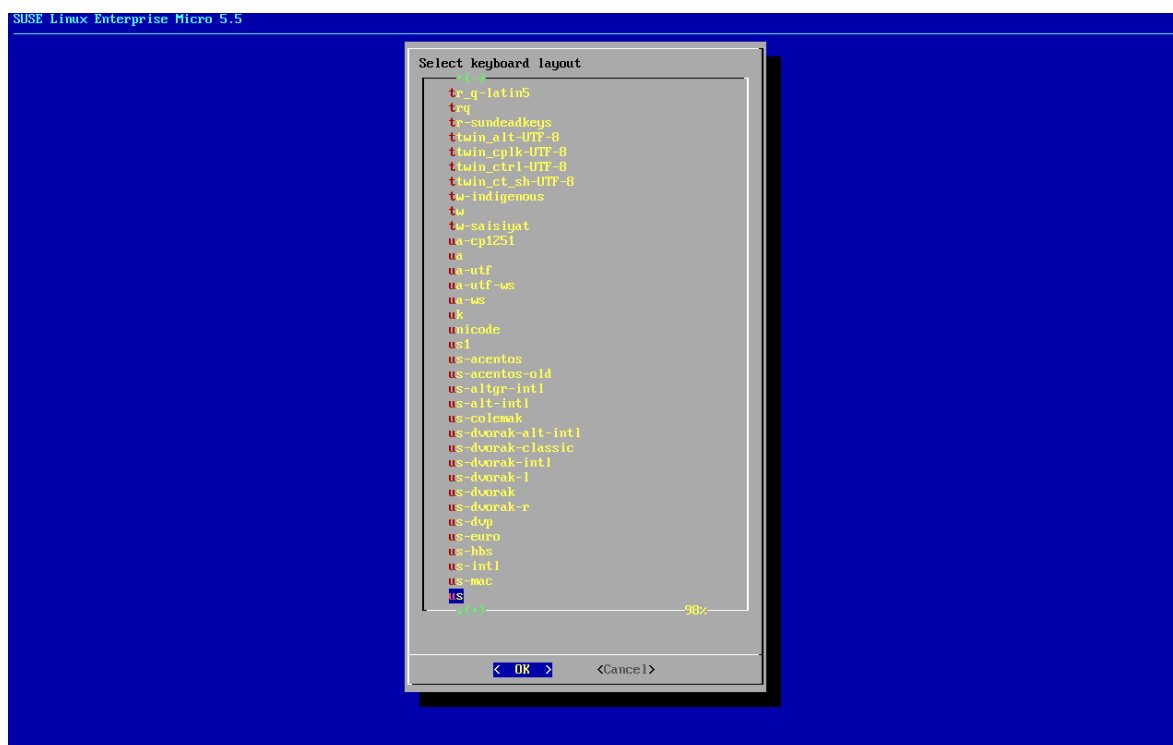
プロシージャ: 初期セットアップを作成する

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。
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。

SUSE Linux Enterprise Micro 5.5

End User License Agreement for SUSE Products
 PLEASE READ THIS AGREEMENT CAREFULLY. BY PURCHASING, INSTALLING, DOWNLOADING OR OTHERWISE USING THE SOFTWARE (INCLUDING ITS COMPONENTS), YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE WITH THESE TERMS, YOU ARE NOT PERMITTED TO DOWNLOAD, INSTALL OR USE THE SOFTWARE AND YOU SHOULD NOTIFY THE PARTY FROM WHICH YOU PURCHASED THE SOFTWARE TO OBTAIN A REFUND. AN INDIVIDUAL ACTING ON BEHALF OF AN ENTITY REPRESENTS THAT HE OR SHE HAS THE AUTHORITY TO ENTER INTO THIS AGREEMENT ON BEHALF OF THAT ENTITY.

This End User License Agreement ("Agreement") is a legal agreement between You (an entity or a person) and SUSE LLC ("Licensor"). SUSE (including Rancher) software products for which You have acquired licenses, any media or reproductions (physical or virtual) and accompanying documentation (collectively the "Software") are protected by the copyright laws and treaties of the United States ("U.S.") and other countries and is subject to the terms of this Agreement. If the laws of Your principal place of business require contracts to be in the local language to be enforceable, such local language version may be obtained from Licensor upon written request and shall be deemed to govern Your purchase of licenses to the Software. Any add-on, extension, update, mobile application, module, adapter or support release to the Software that You may download or receive that is not accompanied by a license agreement is Software and is governed by this Agreement. If the Software is an update or support release, then You must have validly licensed the version and quantity of the Software being updated or supported in order to install or use the update or support release.

Licensed Use
 Open Source
 Nothing in this Agreement shall restrict, limit or otherwise affect any rights or obligations You may have, or conditions to which You may be subject, under any applicable open source licenses to any open source code contained in the Software. The Software may include or be bundled with other software programs licensed under different terms and/or licensed by a third party other than Licensor. Use of any software programs accompanied by a separate license agreement is governed by that separate license agreement.

Subscription Services and Support
 Licensor has no obligation to provide maintenance or support unless You purchase a subscription offering that expressly includes such services. Licensor sells subscription offerings for the Software

(C) 18

< EXIT >

8. タイムゾーンを選択します。

SUSE Linux Enterprise Micro 5.5

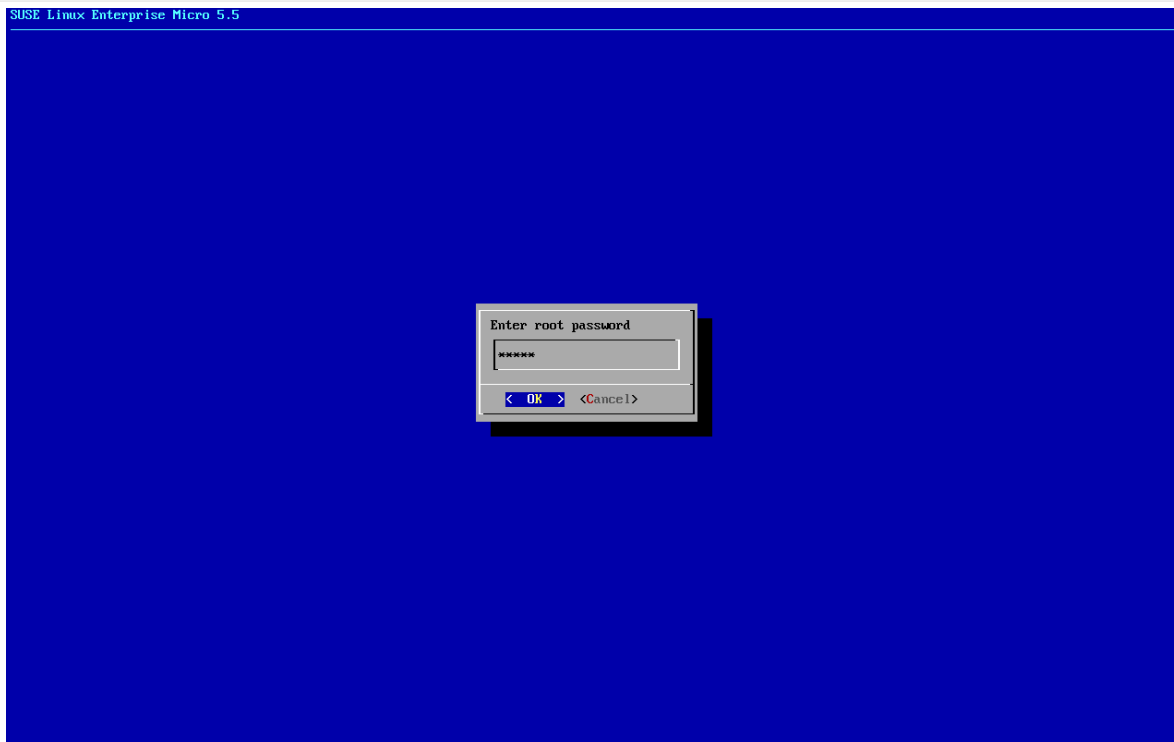
Select time zone

UTC
 Africa/Abidjan
 Africa/Accra
 Africa/Addis_Ababa
 Africa/Algiers
 Africa/Asmara
 Africa/Bamako
 Africa/Bangui
 Africa/Banjul
 Africa/Bissau
 Africa/Blantyre
 Africa/Brazzaville
 Africa/Bujumbura
 Africa/Cairo
 Africa/Casablanca
 Africa/Ceuta
 Africa/Conakry
 Africa/Dakar
 Africa/Dar_es_Salaam
 Africa/Djibouti
 Africa/Douala
 Africa/El_Aaiun
 Africa/Freetown
 Africa/Gaborone
 Africa/Harare
 Africa/Johannesburg
 Africa/Juba
 Africa/Kampala
 Africa/Khartoum
 Africa/Kigali
 Africa/Kinshasa
 Africa/Lagos
 Africa/Libreville
 Africa/Lome
 Africa/Luanda

(C) 0

< OK > <Cancel>

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。

3.1.2.4. SL MicroおよびSUSE Multi-Linux Manager 5.1サーバの登録



SL Micro 6.1エンタイトルメントは、SUSE Multi-Linux Managerエンタイトルメント内に含まれているため、別途登録コードは必要ありません。

SUSE Multi-Linux Manager server hosts that are hardened for security may restrict execution of files from the **/tmp** folder. In such cases, as a workaround, export the **TMPDIR** environment variable to another existing path before running **mgradm**.



例:

```
export TMPDIR=/path/to/other/tmp
```

SUSE Multi-Linux Managerの更新では、この回避策が不要になるようにツールが変更されます。

プロシージャ: SL MicroおよびSUSE Multi-Linux Manager 5.1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 Multi-Linux Manager 5.1を登録します。

```
transactional-update register -p Multi-Linux-Manager-Server/5.1/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。
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。

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>]
```

例:

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



このコマンドは、**/var/lib/containers/storage/volumes**にある永続ストレージボリュームを指定されたストレージデバイスに移動します。

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. Deploy SUSE Multi-Linux Manager.



If you use VM images as a migration target, here as the last step, execute the command **mgradm migrate** instead of **mgradm install**.

Execute one of the following commands, depending on the SSL certificate variant (self-signed or third-party). Replace **<FQDN>** with your fully qualified domain name of the SUSE Multi-Linux Manager Server:

- SUSE Multi-Linux Managerで提供される自己署名証明書を使用する場合:

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

- サードパーティSSL証明書フラグを使用してSSL証明書をインポートする場合(これらすべての証明書が必要なわけではない場合は例を調整可能):

```
mgradm install podman <FQDN> \
--ssl-ca-intermediate <strings> \
--ssl-ca-root <string> \
--ssl-server-cert <string> \
--ssl-server-key <string> \
--ssl-db-ca-intermediate <strings> \
--ssl-db-ca-root <string> \
--ssl-db-cert <string> \
--ssl-db-key <string>
```

詳細については、**mgradm install podman --help**を参照してください。

3.1.3. SUSE Multi-Linux Manager 5.1サーバの仮想マシンとしての配備 - VMware

この章では、SUSE Multi-Linux Manager 5.1 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。

3.1.3.1. 利用可能なイメージ



SUSE Multi-Linux Manager 5.1サーバ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 Multi-Linux Manager 5.1のイメージは[SUSE Multi-Linux Manager 5.1 VM images](#)で入手できます。



カスタマイズされたSUSE Multi-Linux Manager 5.1 VMイメージは、SL Micro 6.1にのみ提供されます。SUSE Linux Enterprise Server 15 SP7で製品を実行するには、<https://www.suse.com/download/sles/>で入手可能な標準のSUSE Linux Enterprise Server 15 SP7インストールを使用し、その上でSUSE Multi-Linux Manager 5.1拡張機能を有効にします。



生イメージの準備の詳細については、[https://documentation.suse.com/sle-micro/6.1/html/Micro-deployment-raw-images-virtual-machines/index.html#deployment-preparing-configuration-device\[\]](https://documentation.suse.com/sle-micro/6.1/html/Micro-deployment-raw-images-virtual-machines/index.html#deployment-preparing-configuration-device[])を参照してください。

セルフインストールイメージの詳細については、<https://documentation.suse.com/sle-micro/6.1/html/Micro-deployment-selfinstall-images/index.html>を参照してください。

表 11. 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

アーキテクチャ	イメージの形式
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。

3.1.3.2. SUSE Multi-Linux Manager 仮想マシン設定 - VMware

このセクションでは、VMware環境内のSUSE Multi-Linux 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 Multi-Linux 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インター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**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数を最小値で設定します。*)
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。

*) 最小値については、[installation-and-upgrade:hardware-requirements.pdf](#)を参照してください。

3.1.3.3. SL MicroおよびSUSE Multi-Linux Manager 5.1サーバの登録

開始する前に、SUSE Customer Center (<https://scc.suse.com>)からSUSE Multi-Linux Manager登録コードを入手してください。



SL Micro 6.1エンタイトルメントは、SUSE Multi-Linux Managerエンタイトルメント内に含まれているため、別途登録コードは必要ありません。



SUSE Multi-Linux Manager server hosts that are hardened for security may restrict execution of files from the **/tmp** folder. In such cases, as a workaround, export the **TMPDIR** environment variable to another existing path before running **mgradm**.

例:

```
export TMPDIR=/path/to/other/tmp
```

SUSE Multi-Linux Managerの更新では、この回避策が不要になるようにツールが変更されます。

プロシージャ: SL MicroおよびSUSE Multi-Linux Manager 5.1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 Multi-Linux Manager 5.1を登録します。

```
transactional-update register -p Multi-Linux-Manager-Server/5.1/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。

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>]
```

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. Deploy SUSE Multi-Linux Manager.



If you use VM images as a migration target, here as the last step, execute the command **mgradm migrate** instead of **mgradm install**.

Execute one of the following commands, depending on the SSL certificate variant (self-signed or third-party). Replace **<FQDN>** with your fully qualified domain name of the SUSE Multi-Linux Manager Server:

- SUSE Multi-Linux Managerで提供される自己署名証明書を使用する場合:

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

- サードパーティSSL証明書フラグを使用してSSL証明書をインポートする場合(これらすべての証明書が必要なわけではない場合は例を調整可能):

```
mgradm install podman <FQDN> \
--ssl-ca-intermediate <strings> \
--ssl-ca-root <string> \
--ssl-server-cert <string> \
--ssl-server-key <string> \
--ssl-db-ca-intermediate <strings> \
--ssl-db-ca-root <string> \
--ssl-db-cert <string> \
--ssl-db-key <string>
```

詳細については、**mgradm install podman --help**を参照してください。

3.1.4. SUSE Multi-Linux ManagerサーバのAir-gapped配備

3.1.4.1. What is Air-gapped deployment?

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。

3.1.4.2. 配備

SUSE Multi-Linux Managerは2つの配備バリエーションをサポートしています。

3.1.4.2.1. 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 Multi-Linux Managerの仮想マシンイメージ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 Multi-Linux 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 Multi-Linux 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必要があります。

3.1.4.2.2. SL MicroにSUSE Multi-Linux Managerを配備する

SUSE Multi-Linux 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。



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

Procedure: Install SUSE Multi-Linux Manager on SL Micro in air-gapped deployment

1. SL Microをインストールします。
2. システムを更新します。
3. Install tools packages and image packages (replace \$ARCH\$ with the correct architecture).

```
transactional-update pkg install mgradm* mgrctl* suse-multi-linux-manager-5.1-$ARCH$-server-*
```

4. 再起動します。
5. **mgradm**を使用してSUSE Multi-Linux Managerを配備します。

SL MicroにSUSE Multi-Linux 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 Multi-Linux 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必要があります。

3.1.4.3. PTF

PTFイメージはパッケージとして利用できません。つまり、インターネットアクセスが可能なマシンで**podman**を使用してイメージをプルしてから、アーカイブに保存し、エアギャップマシンに転送して、そこでロードする必要があります。

プロシージャ: インターネットアクセスが可能なマシン上でイメージをプルする

1. **podman**をインストールします。

2. SCC資格情報を使用して、SUSEレジストリに対して認証します。

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

3. PTFイメージのURLを1行に1つずつ記述した/tmp/ptf-imagesという一時ファイルを作成します。ほとんどのケースではサーバイメージのみが必要であり、以下のようなコマンドを使用してSCC_USERIDとPTFIDの値を置き換えて作成できます。

```
SCC_USERID=aXXXX
PTFID=12345
echo "registry.suse.com/a/$SCC_USERID/$PTFID/suse/multi-linux-
manager/5.1/x86_64/server:latest-ptf-$PTFID" >>/tmp/ptf-images
```

4. PTFの各コンテナイメージをプルしてから、tarアーカイブに保存します。

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

5. パッチを適用するサーバに/tmp/ptf-images.tarイメージアーカイブを転送します。

プロシージャ: パッチを適用するサーバにイメージをロードする

1. ptf-images.tarファイルがサーバで利用可能であることを確認します。
2. アーカイブからイメージをロードします。

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

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

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

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

3.1.5. パブリッククラウドの配備

パブリッククラウドでは、SUSE Multi-Linux 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 Multi-Linux 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。

3.1.6. PAYGインスタンスの接続

大手パブリッククラウドプロバイダ3社(AWS、GCP、Azure)では、SUSEは、

- SLES、SLES for SAPなどのカスタマイズされたPAYG製品イメージを提供します。
- PAYGとして利用可能な製品のリポジトリをミラーリングするリージョンごとのRMTサーバを運用します

このドキュメントでは、既存のPAYGインスタンスをSUSE Multi-Linux Managerサーバに接続する方法について説明し、インスタンスからの資格情報の収集に関する基本的な情報を提供します。 この接続の目的は、認証データを抽出して、SUSE Multi-Linux ManagerサーバがクラウドRMTホストに接続できるようにすることです。 これにより、SUSE Multi-Linux ManagerサーバはSCC組織資格情報ではまだ利用できないRMTホスト上の製品にアクセスできるようになります。

PAYG機能を使用する前に、以下のことを確認してください。

- PAYGインスタンスが正しいSUSE製品イメージ(例: SLES、SLES for SAP、SLE HPC)から起動され、目的のリポジトリにアクセスできる
- SUSE Multi-Linux Managerサーバが直接または要塞経由でPAYGインスタンス(理想的には同じリージョン内)に接続できる
- 基本的なSCCアカウントが必要です。有効なSCC資格情報を**管理**→**セットアップウィザード**→**組織の資格情報**に入力します。 このアカウントは、PAYGインスタンスに関係なく、ブーストラッピング用のSUSE Multi-Linux Managerクライアントツールにアクセスするために必要です。
- PAYGインスタンスをSUSE Managerにブーストラップする場合、SUSE ManagerはそのPAYGリポジトリを無効にしてから、RMTサーバからのデータをミラーリングした場所からリポジトリを追加します。最終的な結果は、PAYGインスタンスがRMTサーバからSUSE Managerサーバ自体を介して同じリポジトリを取得することになります。 もちろん、リポジトリは主にSCCから引き続きセットアップできます。

3.1.6.1. PAYGインスタンスを接続する

プロシージャ: 新しいPAYGインスタンスを接続する

1. SUSE Multi-Linux ManagerのWeb UIで、**管理**→**セットアップウィザード**→**PAYG**に移動し、**[PAYGの追加]**をクリックします。
2. ページセクション **[PAYGの接続の説明]** から始めます。
3. **[説明]** フィールドに、説明を追加します。

4. ページセクション **「インスタンスSSH接続データ」** に移動します。
5. **「ホスト」** フィールドに、SUSE Multi-Linux Managerから接続するインスタンスのDNSまたはIPアドレスを入力します。
6. **「SSHポート」** フィールドに、ポート番号を入力するか、デフォルト値22を使用します。
7. **「ユーザ」** フィールドに、クラウドで指定されているユーザ名を入力します。
8. **「パスワード」** フィールドに、パスワードを入力します。
9. **「SSH機密鍵」** フィールドに、インスタンスキーを入力します。
10. **「SSH機密鍵のパスフレーズ」** フィールドに、キーパスフレーズを入力します。



認証キーは常にPEM形式である必要があります。

インスタンスに直接接続していないが、SSH要塞を介して接続している場合は、[プロシージャ: SSH要塞接続データを追加する](#)に進みます。

それ以外の場合は、[プロシージャ: PAYGの接続を完了する](#)に進みます。

プロシージャ: SSH要塞接続データを追加する

1. ページセクション **「要塞SSH接続データ」** に移動します。
2. **「ホスト」** フィールドに、要塞のホスト名を入力します。
3. **「SSHポート」** フィールドに、要塞のポート番号を入力します。
4. **「ユーザ」** フィールドに、要塞のユーザ名を入力します。
5. **「パスワード」** フィールドに、要塞のパスワードを入力します。
6. **「SSH機密鍵」** フィールドに、要塞キーを入力します。
7. **「SSH機密鍵のパスフレーズ」** フィールドに、要塞キーのパスフレーズを入力します。

[プロシージャ: PAYGの接続を完了する](#)を使用してセットアッププロセスを完了します。

プロシージャ: PAYGの接続を完了する

1. 新しいPAYG接続データの追加を完了するには、**「作成」**をクリックします。
2. PAYG接続データの**「詳細」** ページに戻ります。 更新された接続ステータスは、**「情報」** という名前の上部セクションに表示されます。
3. 接続ステータスは、**「管理 > セットアップウィザード > Pay-as-you-go」** 画面にも表示されます。
4. インスタンスの認証データが正しい場合、**「ステータス」** 列に「資格情報が正常に更新されました」と表示されます。



いずれかの時点で無効なデータが入力されると、新しく作成されたインスタンスが**「管理 > セットアップウィザード > PAYG」** に表示され、**「ステータス」** 列にエラーメッセージが表示されます。

サーバで認証データが利用可能になるとすぐに、利用可能な製品のリストが更新されます。

利用可能な製品は、PAYGインスタンスにインストールされているものと同じ製品ファミリーおよびアーキテクチャのすべてのバージョンです。たとえば、インスタンスにSUSE Linux Enterprise Server 15 SP1製品がインストールされている場合、SUSE Linux Enterprise Server 15 SP2、SUSE Linux Enterprise Server 15 SP3、SUSE Linux Enterprise Server 15 SP4、およびSUSE Linux Enterprise Server 15 SP5が **管理 > セットアップウィザード > 製品** に自動的に表示されます。

製品が利用可能として表示されたら、ユーザは、製品名の横にあるチェックボックスを選択し **[製品の追加]** をクリックして、SUSE Multi-Linux Managerに製品を追加できます。

成功メッセージの後、**ソフトウェア > チャンネル一覧 > すべて** に移動して、Web UIで新しく追加されたチャンネルを確認できます。

各チャンネルの同期の進行状況を監視するには、SUSE Multi-Linux Managerサーバの `/var/log/rhn/reposync` ディレクトリにあるログファイルを確認します。



PAYGインスタンスとSCCサブスクリプションの1つによって製品が提供されている場合、その製品は製品リストに1回のみ表示されます。

その製品に属するチャンネルが同期されている場合でも、データはSCCサブスクリプションからのものであり、従量課金制インスタンスからのものではない可能性があります。

3.1.6.2. インスタンス資格情報収集ステータス

SUSE Multi-Linux Managerサーバは、インスタンスから収集された資格情報を使用してRMTサーバに接続し、reposyncを使用してパッケージをダウンロードします。これらの資格情報は、taskomaticにより、定義されたSSH接続データを使用して10分ごとに更新されます。RMTサーバへの接続では、常にPAYGインスタンスから収集された最新の既知の認証資格情報が使用されます。

PAYGインスタンスの資格情報収集のステータスは、**[ステータス]** 列またはインスタンスの詳細ページに表示されます。インスタンスに到達できない場合、資格情報の更新プロセスは失敗します。

インスタンスに到達できない場合、資格情報の更新プロセスは失敗し、2回目に更新が失敗すると資格情報は無効になります。資格情報が無効な場合、チャンネルの同期は失敗します。これを避けるには、接続されているインスタンスの実行状態を維持します。

PAYGインスタンスは、SSH接続データが明示的に削除されない限り、SUSE Multi-Linux Managerサーバに接続されたままになります。インスタンスへのSSH接続データを削除するには、[\[proc-deleting-connection-data-to-instance\]](#)を使用します。

PAYGインスタンスは、SUSE Multi-Linux Managerサーバから常にアクセスできるとは限りません。

- インスタンスが存在するが停止している場合は、最新の既知の資格情報を使用してインスタンスへの接続が試行されます。資格情報が有効である期間は、クラウドプロバイダによって異なります。
- インスタンスが存在しなくなったが、SUMAに登録されている場合、その資格情報は無効になり、認証は失敗します。エラーメッセージは **[ステータス]** 列に表示されます。



エラーメッセージは、インスタンスが使用できないことを示すだけです。インスタンスのステータスに関する詳細な診断は、クラウドプロバイダで実行する必要があります。



PAYGインスタンスで次のアクションまたは変更を行うと、資格情報が機能しなくなります。 * zypper資格情報ファイルの削除 * インポートした証明書の削除 * `/etc/hosts`からのクラウド固有エントリの削除

3.1.6.3. PAYGシステムをクライアントとして登録する

資格情報をSaltクライアントとして収集する場所からPAYGインスタンスを登録できます。 インスタンスには有効なクラウド接続が登録されている必要があります。登録されていないとチャンネルにアクセスできません。ユーザがクラウドパッケージを削除すると、資格情報の収集が機能しなくなる場合があります。

最初にPAYGインスタンスを設定して、認証データを収集し、チャンネルを同期できるようにします。

残りのプロセスは、パブリッククラウド以外のクライアントの場合と同じで、チャンネルの同期、ブートストラップスクリプトの自動作成、アクティベーションキーの作成、および登録の開始で構成されます。

クライアントの登録の詳細については、**Client-configuration** > **Registration-overview**を参照してください。

3.1.6.4. トラブルシューティング

資格情報の確認

- スクリプトが資格情報の収集に失敗した場合、ログとWeb UIに適切なエラーメッセージが表示されます。
- 資格情報が機能しない場合は、**reposync**に適切なエラーが表示されます。

registercloudguestを使用する

- パブリッククラウド更新インフラストラクチャへの**registercloudguest**接続を更新または変更しても、資格情報の使用に支障はありません。
- cloudquestコマンドを使用して新しいクラウド接続が登録されていない場合、**registercloudguest --clean**を実行すると問題が発生します。

3.2. SUSE Multi-Linux Managerプロキシのインストール

SUSE Multi-Linux Managerプロキシを配備するさまざまなシナリオがあります。これらのシナリオはすべて、すでにSUSE Multi-Linux Manager 5.1サーバが正常に配備済みであることを前提としています。

3.2.1. SUSE Multi-Linux Manager 5.1プロキシの配備

このガイドでは、SL Micro 6.1またはSUSE Linux Enterprise Server 15 SP7上のSUSE Multi-Linux Manager 5.1プロキシコンテナの配備プロセスについて説明します。このガイドでは、SUSE Multi-Linux Manager 5.1サーバが正常に配備済みであることを想定しています。



SL Microは当面、通常のminion (デフォルト接続メソッド)としてのみサポートされます。SUSEでは、これを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取り組んでいます。

正常に配備するには、次のアクションを実行します。

プロシージャ: プロキシを配備する

1. ハードウェア要件を確認します。
2. SL Micro 6.1またはSUSE Linux Enterprise Server 15 SP7親チャンネルとサーバ上の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SL MicroまたはSUSE Linux Enterprise Serverをインストールします。
4. インストール時に、SL MicroまたはSUSE Linux Enterprise ServerをSUSE Multi-Linux Manager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 Multi-Linux 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SL Micro 6.1とSUSE Linux Enterprise Server 15 SP7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。

3.2.1.1. プロキシのハードウェア要件

SUSE Multi-Linux Managerプロキシを配備するためのハードウェア要件の詳細については、[installation-and-upgrade:hardware-requirements.pdf](#)を参照してください。

3.2.1.2. 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。

プロシージャ: 親チャンネルとプロキシ拡張機能の同期

1. SUSE Multi-Linux 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「SL Micro」または「SUSE Linux Enterprise Server」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 [SL Micro 6.1] または [SUSE Linux Enterprise Server 15 SP7] チェックボックスをオンにし、ドロップダウンを使用して **SUSE Multi-Linux Manager Proxy Extension 5.1 x86_64** 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。

3.2.1.3. SUSE Multi-Linux Managerプロキシホストの準備

以下のサブセクションで、SLE MicroまたはSUSE Linux Enterprise Serverを使用してプロキシホストを準備します。

3.2.1.3.1. SLE Micro 6.1ホストの準備

インストールメディアのダウンロード

Procedure: Downloading the installation media

1. <https://www.suse.com/download/sle-micro/>でSL Micro 6.1のインストールメディアを見つけて、適切なメディアファイルをダウンロードします。
2. 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。

SL Micro 6.1のインストール

マシン(仮想または物理)の準備の詳細については、[SL Micro配備ガイド](#)を参照してください。

プロシージャ: SL Micro 6.1のインストール

1. SLE Micro 6.1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。
2. システムをブートまたは再起動します。
3. 矢印キーを使用してインストールを選択します。
4. キーボードと言語を調整します。
5. 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。
6. 次へをクリックして続行します。
7. 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。



SUSE Multi-Linux Manager 5.1コンテナは拡張機能としてインストールされます。以下のリストから必要な特定の拡張機能に応じて、それぞれに追加のSUSE Customer Center登録コードが必要です。

- SUSE Multi-Linux Manager 5.1サーバ
- SUSE Multi-Linux Manager 5.1プロキシ
- SUSE Multi-Linux Manager 5.1 Retail Branch Server



SL Micro 6.1エンタイトルメントは、SUSE Multi-Linux Managerエンタイトルメント内に含まれているため、別途登録コードは必要ありません。

8. SUSE Customer Centerの電子メールアドレスを入力します。
9. SL Micro 6.1の登録コードを入力します。
10. 次へをクリックして続行します。
11. プロキシをインストールするにはSUSE Multi-Linux Manager 5.1プロキシ拡張機能、サーバをインストールするにはSUSE Multi-Linux Manager 5.1サーバ拡張機能のチェックボックスを選択します。

12. 次へをクリックして続行します。
13. SUSE Multi-Linux Manager 5.1拡張機能の登録コードを入力します。
14. [次へ]をクリックして続行します。
15. NTP設定ページで、[次へ]をクリックします。
16. 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。
17. 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SL Micro 6.1とSUSE Multi-Linux Manager 5.1のインストールが完了しました。

オプション: コマンドラインからの登録

SL Micro 6.1のインストール中にSUSE Multi-Linux Manager 5.1を拡張機能として追加した場合は、このプロセス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、SL Micro 6.1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、SL Micro 6.1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。



次のステップでは、SUSE Multi-Linux Manager 5.1拡張機能を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アーキテクチャを登録する場合は、正しい登録コードを使用してください。

Procedure: Registering from the command line

1. 次のコマンドで利用可能な拡張機能を一覧表示します。

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

2. 利用可能な拡張機能のリストから、インストールしたい拡張機能を選択します。

- a. サーバをインストールする場合は、次のコマンドで SUSE Multi-Linux Manager Server Extension 5.1 x86_64の登録コードを使用します。

```
transactional-update register -p Multi-Linux-Manager-Server/5.1/x86_64 -r <reg_code>
```

- b. プロキシをインストールする場合は、次のコマンドでSUSE Multi-Linux Manager Proxy Extension 5.1 x86_64の登録コードを使用します。

```
transactional-update register -p Multi-Linux-Manager-Proxy/5.1/x86_64 -r
```

```
<reg_code>
```

3. 再起動します。

システムの更新

Procedure: Updating the system

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。



SL Microはデフォルトで自己更新するように設計されており、更新を適用すると再起動します。ただし、SUSE Multi-Linux Manager環境ではこの動作は望ましくありません。サーバの自動更新を防ぐには、SUSE Multi-Linux Managerでブートストラッププロセス中にtransactional-updateのタイマを無効にします。

SL 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を有効にします。

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

配備を続行するには、[installation-and-upgrade:container-deployment/mlm/proxy-deployment-mlm.pdf](#)を参照してください。

3.2.1.3.2. Prepare SUSE Linux Enterprise Server 15 SP7 host

または、SUSE Linux Enterprise Server 15 SP7にSUSE Multi-Linux Managerを配備することもできます。

The following procedures describe the main steps of the installation process.

Install SUSE Multi-Linux Manager extensions on SUSE Linux Enterprise Server

Procedure: Installing SUSE Multi-Linux Manager Extensions on SUSE Linux Enterprise Server

1. <https://www.suse.com/download/sles/>でSUSE Linux Enterprise Server 15 SP7 **.iso**を見つけてダウンロードします。
2. ホストオペレーティングシステム(SUSE Linux Enterprise Server 15 SP7)と拡張機能の両方の登録コードがあることを確認します。

3. SUSE Linux Enterprise Server 15 SP7のインストールを開始します。
 - a. **Language, Keyboard and Product Selection**（言語、キーボードおよび製品の選択）で、インストールする製品を選択します。
 - b. **ライセンス契約**で契約を読み、**[I Agree to the License Terms**（ライセンス条項に同意します）にチェックを付けます。
4. 登録方法を選択します。この例では、SUSEカスタマーセンターにサーバを登録します。
5. SUSE Customer Centerの電子メールアドレスを入力します。
6. SUSE Linux Enterprise Server 15 SP7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。



SUSE Linux Enterprise Server 15 SP7には、有効なSUSE Linux Enterprise Serverサブスクリプションと対応する登録コードが必要であり、この画面で入力する必要があることに注意してください。以下でSUSE Multi-Linux Manager拡張機能の登録コードを入力する必要があります。

8. **拡張とモジュールの選択**で、以下にチェックを付けます。
 - サーバをインストールするにはSUSE Multi-Linux Managerサーバ拡張機能を選択し、プロキシをインストールするにはSUSE Multi-Linux Managerプロキシ拡張機能を選択します。
 - ベースシステムモジュール
 - Containersモジュール
9. **次へ**をクリックして続行します。
10. SUSE Multi-Linux Manager 5.1拡張機能の登録コードを入力します。
11. **[次へ]**をクリックして続行します。
12. インストールを完了します。
13. インストールが完了したら、rootとして新しくインストールしたサーバにログインします。

14. システムを更新します(オプション。インストール時にシステムが更新をダウンロードするように設定されていない場合)。

```
zypper up
```

15. 再起動します。

オプション: コマンドラインからの登録

If you added SUSE Multi-Linux Manager 5.1 as an extension during SUSE Linux Enterprise Server installation then you can skip this procedure.

However, optionally you may skip registration during SUSE Linux Enterprise Server installation by selecting the **[Skip Registration]** button. This section provides steps on registering your products after SUSE Linux Enterprise Server installation.



The following steps register a SUSE Multi-Linux Manager 5.1 extension with the x86-64 architecture and thus require a registration code for the x86-64 architecture.

To register ARM or s390x architectures use the correct registration code.

Procedure: Registering from the command line

1. 次のコマンドで利用可能な拡張機能を一覧表示します。

```
SUSEConnect --list-extensions
```

From the list of available extensions, select the one you wish to install. If installing the Server, use your SUSE Multi-Linux Manager Server Extension 5.1 x86_64 registration code. For example for SUSE Linux Enterprise 15 SP7, use the following commands:

```
SUSEConnect -r <regcode>
SUSEConnect -p sle-module-containers/15.7/x86_64
SUSEConnect -p Multi-Linux-Manager-Server-SLE/5.1/x86_64 -r <regcode>
```

- If installing the Proxy, use your SUSE Multi-Linux Manager Proxy Extension 5.1 x86_64 registration code with the following command:

```
SUSEConnect -p Multi-Linux-Manager-Proxy-SLE/5.1/x86_64 -r <regcode>
```

Install and enable podman

Procedure: Installing podman**1. Log in as root and install the product package.**

- On the server:

```
zypper in podman
zypper in -t product SUSE-Multi-Linux-Manager-Server
```

- On the proxies:

```
zypper in podman
zypper in -t product SUSE-Multi-Linux-Manager-Proxy
```



Make sure that package **podman** is installed. Additionally, on the server **mgradm** and **mgradm-bash-completion** or on the proxies, **mgrpky** and **mgrpky-bash-completion** also need to be installed.

2. システムを再起動するか、次のコマンドを実行してPodmanサービスを起動します。

```
systemctl enable --now podman.service
```

配備を続行するには、[installation-and-upgrade:container-deployment/mlm/proxy-deployment-mlm.pdf](#)を参照してください。

3.2.1.4. 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。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**ツールを使用してください。

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](#)

3.2.1.5. プロキシのアクティベーションキーの作成

プロシージャ: 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 6.1またはSUSE Linux Enterprise Server 15 SP7を親チャンネルとして使用して、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。

3.2.1.6. 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

プロシージャ: 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. オペレーティングシステムがSL Microの場合は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SL Microの場合は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。

プロシージャ: 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. オペレーティングシステムがSL Microの場合はプロキシホストを再起動します。

3.2.1.7. プロキシ設定の生成

SUSE Multi-Linux Managerプロキシの設定アーカイブはSUSE Multi-Linux 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。

For the containerized SUSE Multi-Linux Manager Proxy, you must build a new proxy configuration file and then redeploy the container for the changes to take effect. This is the process for updating settings, including the SSL certificate.



Podmanの配備では、このプロキシ設定を生成する前に、SUSE Multi-Linux ManagerプロキシのコンテナホストをSUSE Multi-Linux 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。



Peripheral servers are always using third-party SSL certificates. If the hub server has generated the certificates for the peripheral server, it needs to generate the certificate of each proxy too.

On the hub server, run the following command.

```
mgrctl exec -ti -- rhn-ssl-tool --gen-server --dir="/root/ssl-build"
--set-country="COUNTRY" \
--set-state="STATE" --set-city="CITY" --set-org="ORGANIZATION" \
--set-org-unit="ORGANIZATION UNIT" --set-email="name@example.com" \
--set-hostname=PROXY --set-cname="proxy.example.com"
```

The files to use will be

1. **/root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT** as the root CA,
2. **/root/ssl-build/<hostname>/server.crt** as the proxy certificate and
3. **/root/ssl-build/<hostname>/server.key** as the proxy certificate's key.

3.2.1.7.1. 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 Multi-Linux Managerサーバまたは別のSUSE Multi-Linux 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 Multi-Linux 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 80% of available storage for the containers.



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 Multi-Linux 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 Multi-Linux 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。

6. [生成]をクリックして、SUSE Multi-Linux 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。
7. 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。

3.2.1.7.2. spacecmdと自己署名証明書を使用したプロキシ設定の生成

`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`と自己署名証明書を使用してプロキシ設定を生成する

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 .
```

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

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

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. Execute the following commands, 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. If your setup uses an intermediate CA, copy it as well and include it in the command with the `-i` option (can be provided multiple times if needed):

```
mgrctl cp intermediateCA.pem server:/tmp/intermediateCA.pem
mgrctl exec -ti 'spacecmd proxy_container_config -- -p 8022 -i
/tmp/intermediateCA.pem pxy.example.com srv.example.com 2048 email@example.com
/tmp/ca.crt /tmp/proxy.crt /tmp/proxy.key -o /tmp/config.tar.gz'
```

4. 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 .
```

3.2.1.8. 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. まだ実行していない場合は、前のステップで生成された設定アーカイブ (`config.tar.gz`) をサーバコンテナからサーバホストにコピーします。

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

2. まだ実行していない場合は、サーバホスト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. プロキシホストで、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。

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

3.2.1.9. SUSE Multi-Linux Managerプロキシの起動

`mgrpky` 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。

```
mgrpky 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。

```
mgrpky status
```

5つのSUSE Multi-Linux Managerプロキシコンテナが存在し、また、**proxy-pod**コンテナポッドの一部である必要があります。

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

3.2.1.10. 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 Multi-Linux 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。

例:

```
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-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。

```
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。

3.2.2. クライアントをMLMプロキシに変換する

3.2.2.1. 概要

この章では、Web UIを使用してクライアントシステムをSUSE Multi-Linux Managerプロキシに変換する方法を説明します。

プロキシホストシステムがすでにブートストラップされており、ベースオペレーティングシステムチャンネル(SUSE Linux Enterprise Server 15 SP7やSL Micro 6.1など)およびプロキシ拡張機能チャンネルにサブスクライブされていることが前提となります。

クライアントのオンボーディングの詳細については、[Client-configuration](#) > [Registration-overview](#)を参照してください。

3.2.2.2. 要件

変換を開始する前に、以下の要件が満たされていることを確認します。

3.2.2.2.1. サポートされているシステム

以下のオペレーティングシステムのみが現在プロキシ変換にサポートされています。

- SUSE Linux Enterprise Server 15 SP7
- SL Micro 6.1

3.2.2.2.2. クライアントは以下を満たしている必要があります

- SUSE Multi-Linux Managerにすでにオンボーディング済みであること
- ネットワーク経由でアクセス可能であること
- 適切なプロキシ拡張機能チャンネルにサブスクライブされていること:
 - SUSE Multi-Linux Manager Proxy Extension 5.1 (アーキテクチャが一致していること)

3.2.2.3. 準備

プロキシ変換を進める前に、変換プロセス中の中断を回避するため、以下の準備が完了していることを確認してください。

3.2.2.3.1. SSL証明書

プロキシと他のコンポーネント間の通信をセキュリティで保護するために、有効なSSL証明書が必要です。

以下のものがが必要です。

- SUSE Multi-Linux Managerサーバ上の証明書に署名した認証局(CA)の公開証明書
- プロキシの証明書。
- プロキシ証明書に対応する機密鍵。



CAが中間証明書チェーンを使用している場合は、すべて中間証明書も含める必要があります。

サードパーティ証明書を使用していない場合は、SUSE Multi-Linux Managerコンテナ内の`rhn-ssl-tool`を使用して生成できます。

プロキシ証明書を生成する

1. SUSE Multi-Linux Managerサーバホストで、次のコマンドを実行します。

```
mgrctl exec -ti -- rhn-ssl-tool --gen-server \
  --set-hostname="<PROXY-FQDN>" \
  --dir="/root/ssl-build"
```

他のパラメータの詳細については、**Administration > Ssl-certs-selfsigned**を参照してください。

2. SUSE Multi-Linux Managerサーバホストに証明書を転送します。

```
mgrctl cp server:/root/ssl-build/<PROXY-FQDN>/server.crt /root/proxycert.pem
mgrctl cp server:/root/ssl-build/<PROXY-FQDN>/server.key /root/proxykey.pem
mgrctl cp server:/root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT /root/rootca.pem
```



証明書とキーファイルが生成された正確なフォルダを確認するには、次のコマンドでディレクトリを一覧表示できます。

```
mgrctl exec -ti -- ls -ltd /root/ssl-build/*/
```

3. SUSE Multi-Linux Managerサーバホストからローカルマシンまたは他のターゲットシステムに証明書を転送します。

```
scp <MLM-FQDN>:/root/proxycert.pem ./
scp <MLM-FQDN>:/root/proxykey.pem ./
scp <MLM-FQDN>:/root/rootca.pem ./
```

3.2.2.3.2. パッケージの準備

コンテナイメージをRPMパッケージとして配備することをお勧めします。次のパッケージがクライアントにインストールされていることを確認してください。

- suse-multi-linux-manager-5.1-<ARCH>-proxy-httpd-image
- suse-multi-linux-manager-5.1-<ARCH>-proxy-salt-broker-image
- suse-multi-linux-manager-5.1-<ARCH>-proxy-squid-image
- suse-multi-linux-manager-5.1-<ARCH>-proxy-ssh-image
- suse-multi-linux-manager-5.1-<ARCH>-proxy-tftpd-image

これらのパッケージはWeb UIから、**[ソフトウェア] > [パッケージ] > [インストール]** タブに移動し、上記のパッケージを検索して、インストールすることでインストールできます。

Air-gapped配備の詳細については、**Installation-and-upgrade > Container-deployment**を参照してください。

3.2.2.4. プロキシクライアントのセットアップ

1. クライアントの**[概要]** ページに移動します。
2. **[プロキシへの変換]** ボタンをクリックします。

プロキシ設定フォームにリダイレクトされたことを確認します。

このページには後で **[詳細]** > **[プロキシ]** > **[設定]** タブからアクセスできます。

3. Web UIで、**プロキシ** > **設定**に移動し、必要なデータを入力します。

プロシージャ: プロキシの設定

- a. **[親FQDN]** フィールドに、親サーバまたはプロキシの完全修飾ドメイン名を入力します。
 - b. **[プロキシSSHポート]** フィールドに、SSHサービスがSUSE Multi-Linux Managerプロキシでリスニングしている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。
 - c. **[Squidの最大キャッシュサイズ]** フィールドに、Squidキャッシュの最大許容サイズをギガバイト単位で入力します。
 - d. **[プロキシ管理者の電子メール]** フィールドに、管理者の電子メールアドレスを入力します。
 - e. **[証明書]** セクションに、準備ステップで取得した SUSE Multi-Linux Managerプロキシの証明書を指定します。
 - f. **[ソース]** セクションで、2つのオプション(**[RPM]** または **[レジストリ]**)のいずれかを選択します。
 - **[RPM]** オプション、はエアギャップ環境または制限された環境に推奨されます。 The **Registry** option can be used if connectivity to the container image registry is available. + If selected, you will be prompted to choose between two sub-options: **Simple** or **Advanced**.
 - **[単純]** を選択した場合は、 **[レジストリURL]** と **[コンテナタグ]** フィールドに値を入力します。
 - **[レジストリURL]** には、 **registry.suse.com/suse/multi-linux-manager/5.1/x86_64**を使用します。
 - ドロップダウンリストからタグを選択します。
 - **[詳細]** を選択する場合は、フォームの追加セクションが表示されます。
 - 個々のコンテナURLフィールドには、レジストリ**registry.suse.com/suse/multi-linux-manager/5.1/x86_64**に続いて、対応するサフィックス(例: **proxy-httpd** または **salt-broker**)を使用します。
 - ドロップダウンリストからタグを選択します。
4. すべてのフィールドが入力されたら、**[適用]**をクリックして設定を適用し、プロキシインストールタスクをスケジュールします。

3.2.2.5. プロキシの有効化の確認

クライアントのイベント履歴をチェックして、タスクの成功を確認します。

(オプション)プロキシのHTTPエンドポイントにアクセスして、ようこそページが表示されることを確認します。

3.2.3. 仮想マシンとしてのSUSE Multi-Linux Managerプロキシの配備 - KVM

この章では、SUSE Multi-Linux Manager 5.1プロキシ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。

3.2.3.1. 利用可能なイメージ



SUSE Multi-Linux Manager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。これらのイメージにはすべてのツールが含まれており、配備が容易になります。

SUSE Multi-Linux Manager 5.1プロキシのイメージは[SUSE Multi-Linux Manager 5.1 VM images](#)で入手できます。



カスタマイズされたSUSE Multi-Linux Manager 5.1 VMイメージは、SL Micro 6.1にのみ提供されます。SUSE Linux Enterprise Server 15 SP7で製品を実行するには、<https://www.suse.com/download/sles/>で入手可能な標準のSUSE Linux Enterprise Server 15 SP7インストールを使用し、その上でSUSE Multi-Linux Manager 5.1拡張機能を有効にします。



生イメージの準備の詳細については、[https://documentation.suse.com/sle-micro/6.1/html/Micro-deployment-raw-images-virtual-machines/index.html#deployment-preparing-configuration-device\[\]](https://documentation.suse.com/sle-micro/6.1/html/Micro-deployment-raw-images-virtual-machines/index.html#deployment-preparing-configuration-device[])を参照してください。

セルフインストールイメージの詳細については、<https://documentation.suse.com/sle-micro/6.1/html/Micro-deployment-selfinstall-images/index.html>を参照してください。

表 12. 利用可能なプロキシイメージ

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

3.2.3.2. 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つのプロキシなど、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、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 Multi-Linux Manager-Proxy.x86_64-5.1.*.qcow2
メモリ:	最小*)
CPU:	最小*)
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

*) 最小値については、[installation-and-upgrade:hardware-requirements.pdf](#)を参照してください。



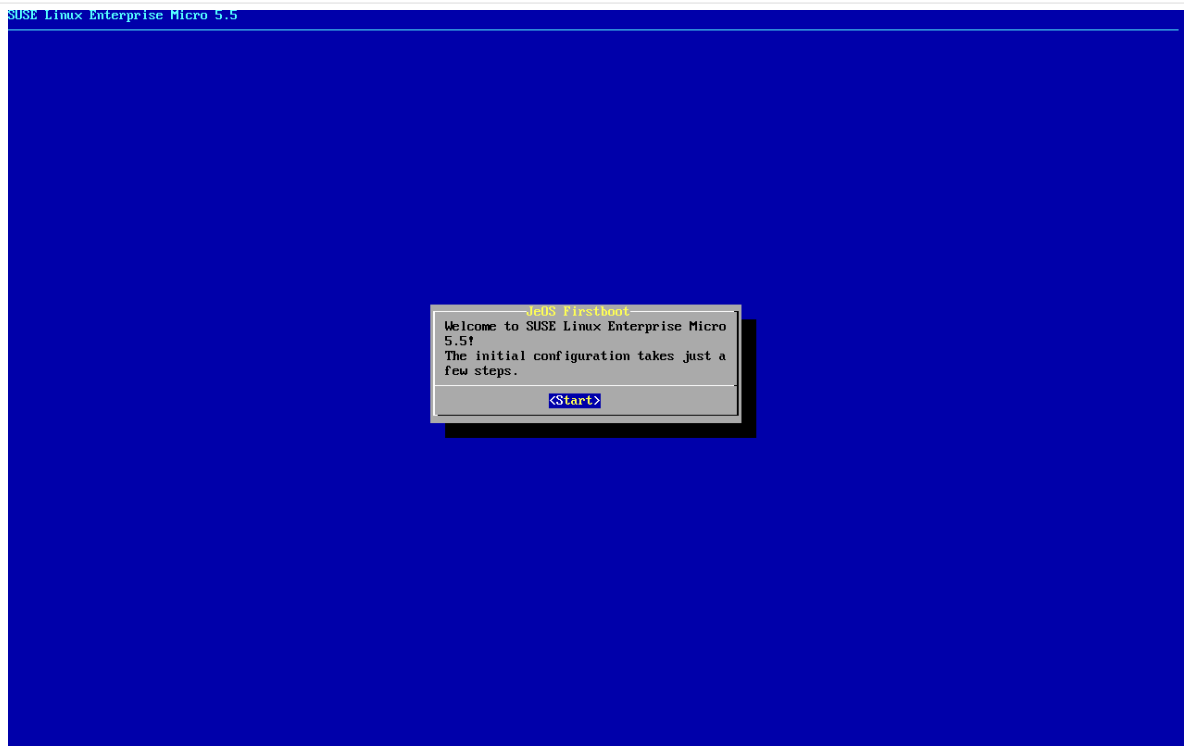
/var/lib/containers/storage/volumes 100GB以上。ストレージ要件は、使用するISOディストリビューションイメージ、コンテナ、およびブートストラップリポジトリの数に合わせて計算する必要があります。

3.2.3.3. KVMの初期セットアップ

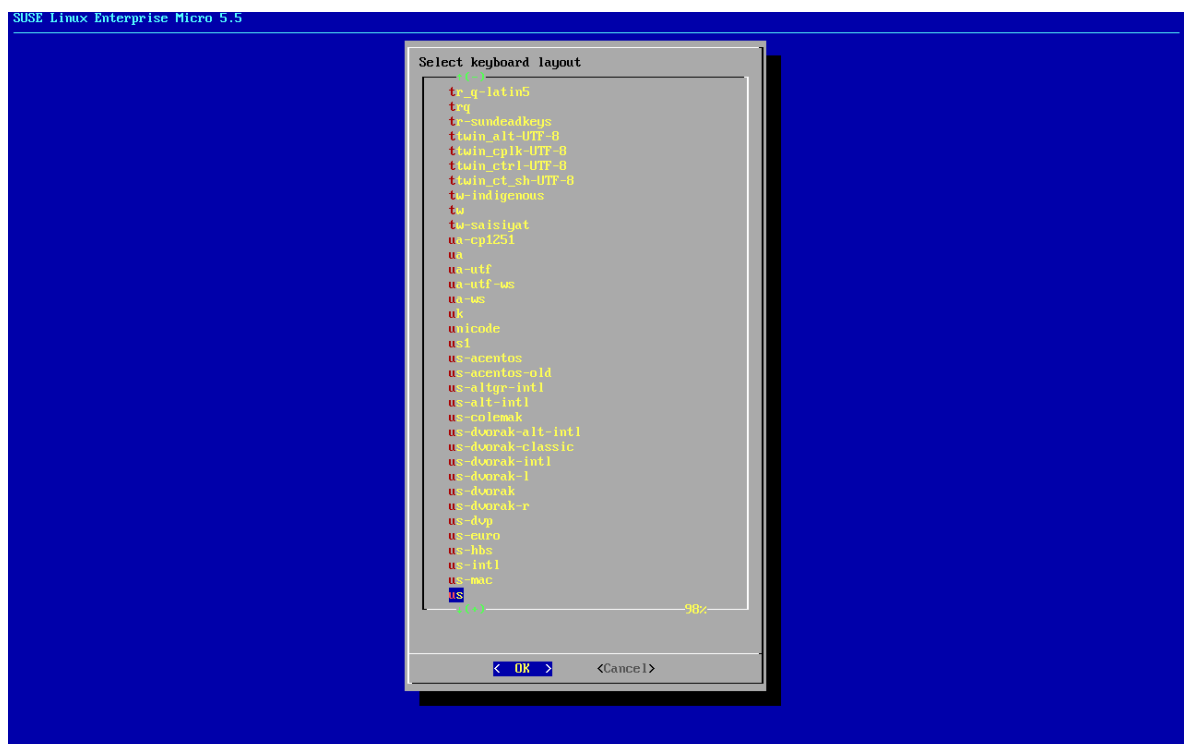
設定については、[installation-and-upgrade:container-deployment/mlm/proxy-deployment-vm-mlm.pdf](#)を参照してください。

プロシージャ: 初期セットアップを作成する

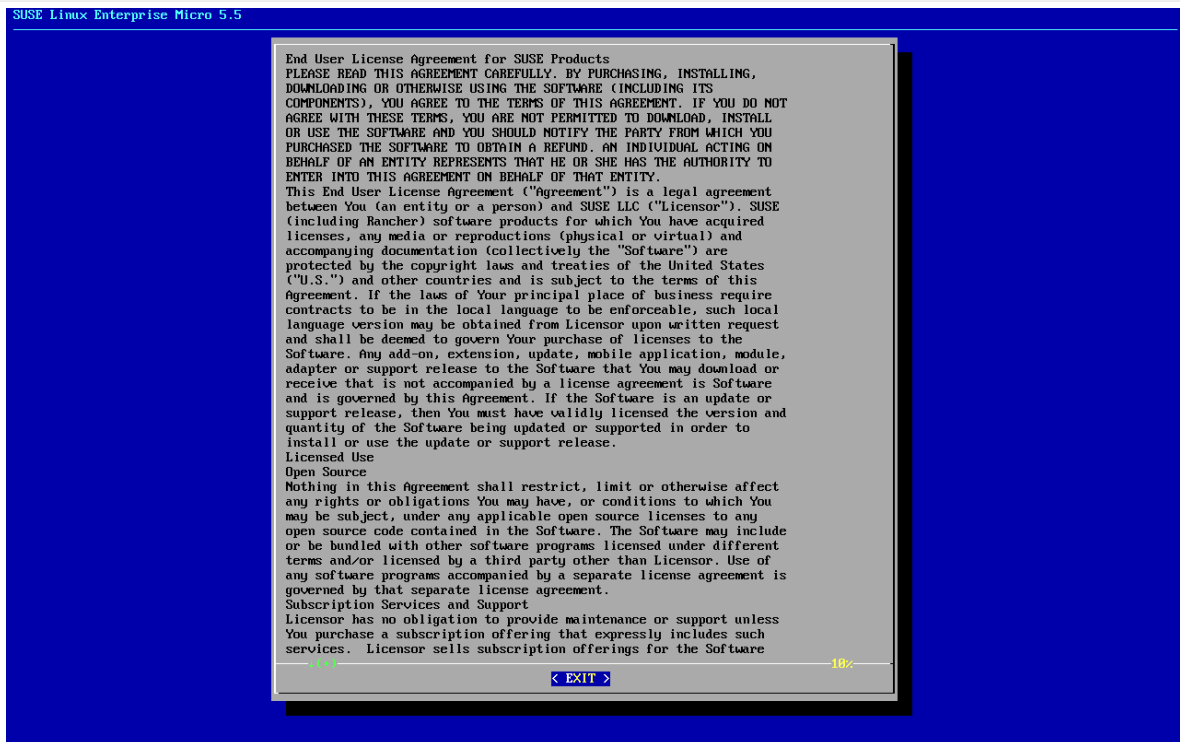
1. ダウンロードしたMinimal KVMイメージを使用して新しい仮想マシンを作成し、**[Import existing disk image]**（既存のディスクイメージをインポート）を選択します。
2. RAMおよびCPU数を最小値で設定します。*)
3. KVMマシンに名前を付け、**[Customize configuration before install]**（インストール前に設定をカスタマイズ）チェックボックスを選択します。
4. **[Begin Installation]**（インストールの開始）をクリックし、イメージからブートします。
5. **[JeOS Firstboot]** の画面で、**[Start]** を選択して続行します。



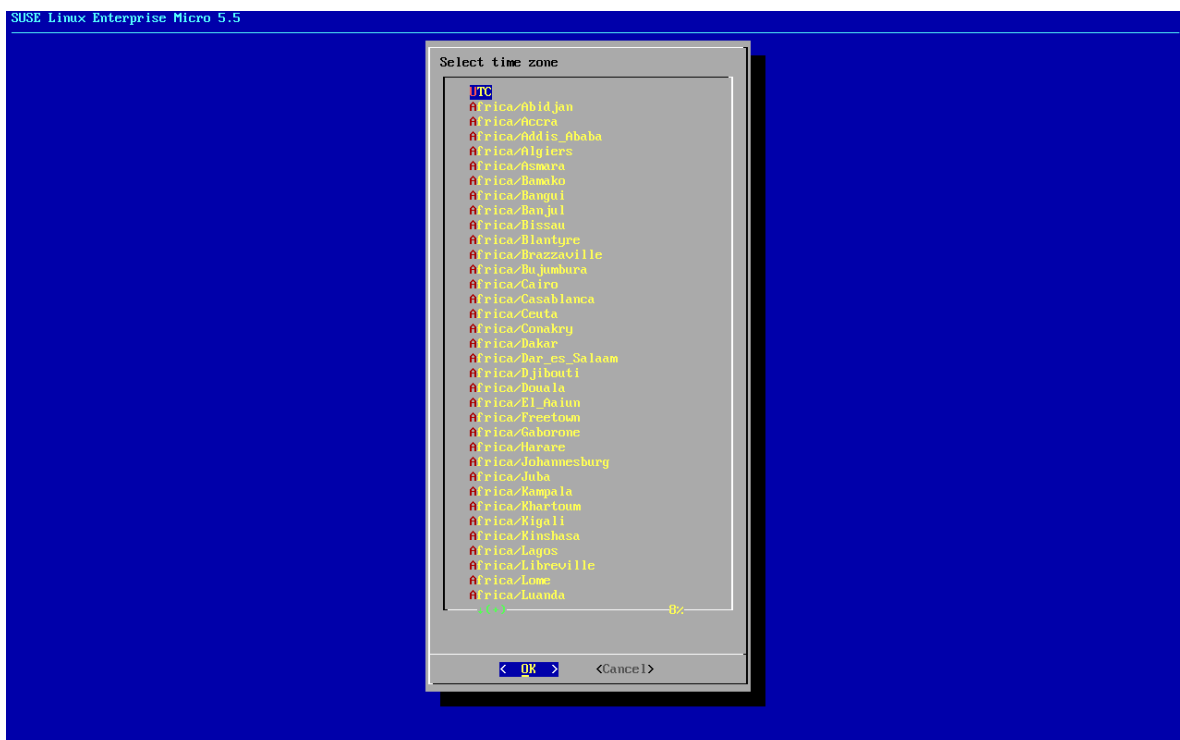
6. キーボードレイアウトを選択します。



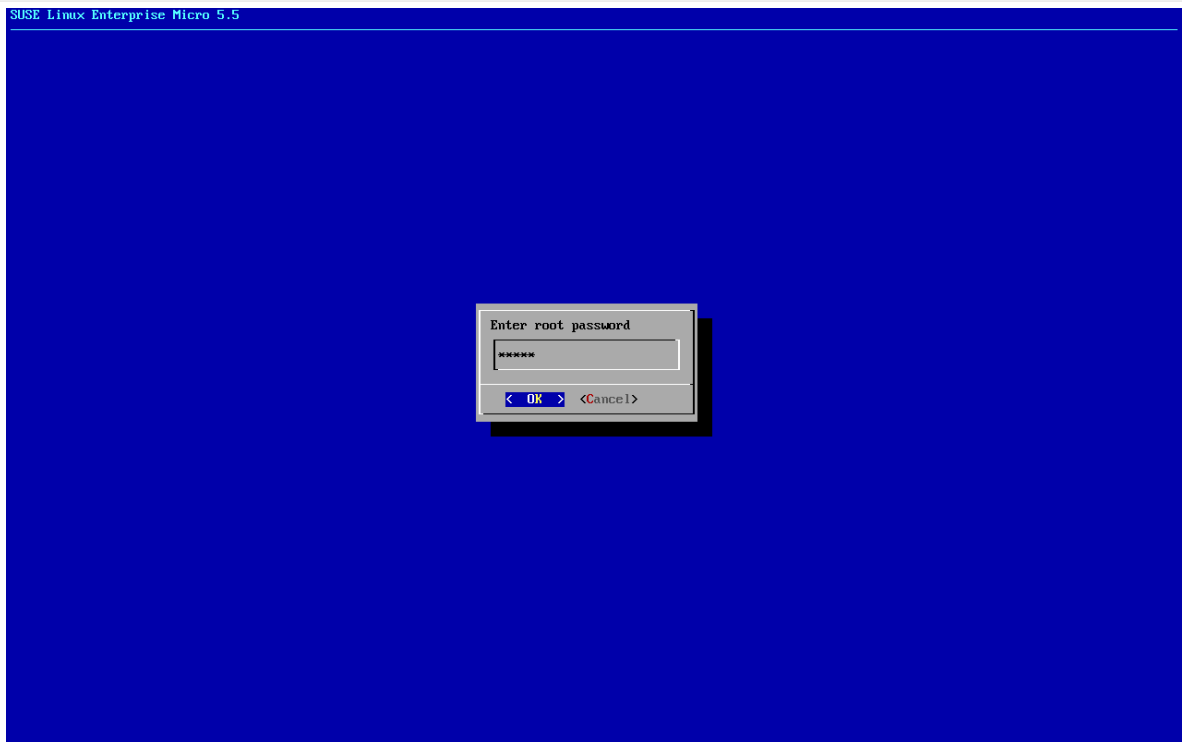
7. ライセンス契約に同意します。



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。

*) 最小値については、[installation-and-upgrade:hardware-requirements.pdf](#)を参照してください。

3.2.3.4. SL MicroおよびSUSE Multi-Linux Manager 5.1プロキシの登録

プロシージャ: SL MicroおよびSUSE Multi-Linux Manager 5.1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 Multi-Linux Manager 5.1プロキシを登録します。

```
transactional-update register -p Multi-Linux-Manager-Proxy/5.1/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。
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**にある永続ストレージボリュームを指定されたストレージデバイスに移動します。

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](#)

3.2.3.5. プロキシのアクティベーションキーの作成

プロシージャ: 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 6.1またはSUSE Linux Enterprise Server 15 SP7を親チャンネルとして使用して、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。

3.2.3.6. プロキシ設定の生成

SUSE Multi-Linux Managerプロキシの設定アーカイブはSUSE Multi-Linux 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。

For the containerized SUSE Multi-Linux Manager Proxy, you must build a new proxy configuration file and then redeploy the container for the changes to take effect. This is the process for updating settings,

including the SSL certificate.



Podmanの配備では、このプロキシ設定を生成する前に、SUSE Multi-Linux ManagerプロキシのコンテナホストをSUSE Multi-Linux 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。



Peripheral servers are always using third-party SSL certificates. If the hub server has generated the certificates for the peripheral server, it needs to generate the certificate of each proxy too.

On the hub server, run the following command.

```
mgrctl exec -ti -- rhn-ssl-tool --gen-server --dir="/root/ssl-build"
--set-country="COUNTRY" \
--set-state="STATE" --set-city="CITY" --set-org="ORGANIZATION" \
--set-org-unit="ORGANIZATION UNIT" --set-email="name@example.com" \
--set-hostname=PROXY --set-cname="proxy.example.com"
```

The files to use will be

1. `/root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT` as the root CA,
2. `/root/ssl-build/<hostname>/server.crt` as the proxy certificate and
3. `/root/ssl-build/<hostname>/server.key` as the proxy certificate's key.

3.2.3.6.1. 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 Multi-Linux Managerサーバまたは別のSUSE Multi-Linux 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 Multi-Linux 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 80% of available storage for the containers.



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 Multi-Linux 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 Multi-Linux 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。

6. [生成]をクリックして、SUSE Multi-Linux 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。
7. 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。

3.2.3.6.2. spacecmdと自己署名証明書を使用したプロキシ設定の生成

`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と自己署名証明書を使用してプロキシ設定を生成する

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 .
```

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

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

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. Execute the following commands, 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. If your setup uses an intermediate CA, copy it as well and include it in the command with the **-i** option (can be provided multiple times if needed):

```
mgrctl cp intermediateCA.pem server:/tmp/intermediateCA.pem
mgrctl exec -ti 'spacecmd proxy_container_config -- -p 8022 -i
/tmp/intermediateCA.pem pxy.example.com srv.example.com 2048 email@example.com
/tmp/ca.crt /tmp/proxy.crt /tmp/proxy.key -o /tmp/config.tar.gz'
```

4. 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 .
```

3.2.3.7. 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。

プロシージャ: プロキシ設定をコピーする

1. まだ実行していない場合は、前のステップで生成された設定アーカイブ (`config.tar.gz`) をサーバコンテナからサーバホストにコピーします。

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

2. まだ実行していない場合は、サーバホスト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. プロキシホストで、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
```

3.2.3.8. SUSE Multi-Linux Manager 5.1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
```

5つのSUSE Multi-Linux Managerプロキシコンテナが存在し、また、**proxy-pod**コンテナポッドの一部である必要があります。

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

3.2.3.8.1. 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 Multi-Linux 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-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。

```
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。

3.2.4. SUSE Multi-Linux Managerプロキシの仮想マシンとしての配備 - VMware

この章では、SUSE Multi-Linux Manager 5.1プロキシ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。

3.2.4.1. 利用可能なイメージ



SUSE Multi-Linux Manager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。これらのイメージにはすべてのツールが含まれており、配備が容易になります。

SUSE Multi-Linux Manager 5.1プロキシのイメージは[SUSE Multi-Linux Manager 5.1 VM images](#)で入手できます。



カスタマイズされたSUSE Multi-Linux Manager 5.1 VMイメージは、SL Micro 6.1にのみ提供されます。SUSE Linux Enterprise Server 15 SP7で製品を実行するには、<https://www.suse.com/download/sles/>で入手可能な標準のSUSE Linux Enterprise Server 15 SP7インストールを使用し、その上でSUSE Multi-Linux Manager 5.1拡張機能を有効にします。



生イメージの準備の詳細については、[https://documentation.suse.com/sle-micro/6.1/html/Micro-deployment-raw-images-virtual-machines/index.html#deployment-preparing-configuration-device\[\]](https://documentation.suse.com/sle-micro/6.1/html/Micro-deployment-raw-images-virtual-machines/index.html#deployment-preparing-configuration-device[])を参照してください。

セルフインストールイメージの詳細については、<https://documentation.suse.com/sle-micro/6.1/html/Micro-deployment-selfinstall-images/index.html>を参照してください。

表 13. 利用可能なプロキシイメージ

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

3.2.4.2. 仮想マシン設定 - VMware

このセクションでは、VMware環境内のSUSE Multi-Linux Managerプロキシ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。



このセクションでは、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つのプロキシなど、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、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。

プロシージャ: VMware仮想マシンを作成する

1. SUSE Multi-Linux Managerプロキシ.vmdkファイルをダウンロードし、コピーをVMwareストレージに転送します。
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. 100GB以上の**Hard Disk 2**を追加します。
5. RAMおよびCPU数を最小値で設定します。*)
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。

*) 最小値については、[installation-and-upgrade:hardware-requirements.pdf](#)を参照してください。

3.2.4.3. SL MicroおよびSUSE Multi-Linux Manager 5.1プロキシの登録

プロシージャ: SL MicroおよびSUSE Multi-Linux Manager 5.1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 Multi-Linux Manager 5.1プロキシを登録します。

```
transactional-update register -p Multi-Linux-Manager-Proxy/5.1/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。
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**にある永続ストレージボリュームを指定されたストレージデバイスに移動します。



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**

3.2.4.4. プロキシのアクティベーションキーの作成

プロシージャ: 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 6.1またはSUSE Linux Enterprise Server 15 SP7を親チャンネル

として使用して、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。

3.2.4.5. プロキシ設定の生成

SUSE Multi-Linux Managerプロキシの設定アーカイブはSUSE Multi-Linux 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。

For the containerized SUSE Multi-Linux Manager Proxy, you must build a new proxy configuration file and then redeploy the container for the changes to take effect. This is the process for updating settings, including the SSL certificate.



Podmanの配備では、このプロキシ設定を生成する前に、SUSE Multi-Linux ManagerプロキシのコンテナホストをSUSE Multi-Linux 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。



Peripheral servers are always using third-party SSL certificates. If the hub server has generated the certificates for the peripheral server, it needs to generate the certificate of each proxy too.

On the hub server, run the following command.

```
mgrctl exec -ti -- rhn-ssl-tool --gen-server --dir="/root/ssl-build"
--set-country="COUNTRY" \
--set-state="STATE" --set-city="CITY" --set-org="ORGANIZATION" \
--set-org-unit="ORGANIZATION UNIT" --set-email="name@example.com" \
--set-hostname=PROXY --set-cname="proxy.example.com"
```

The files to use will be

1. `/root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT` as the root CA,
2. `/root/ssl-build/<hostname>/server.crt` as the proxy certificate and
3. `/root/ssl-build/<hostname>/server.key` as the proxy certificate's key.

3.2.4.5.1. 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 Multi-Linux Managerサーバまたは別のSUSE Multi-Linux 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 Multi-Linux 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 80% of available storage for the containers.



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 Multi-Linux 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 Multi-Linux 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。

6. [生成]をクリックして、SUSE Multi-Linux 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。

7. 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。

3.2.4.5.2. spacecmdと自己署名証明書を使用したプロキシ設定の生成

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と自己署名証明書を使用してプロキシ設定を生成する

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 .
```

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

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

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. Execute the following commands, 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. If your setup uses an intermediate CA, copy it as well and include it in the command with the `-i` option (can be provided multiple times if needed):

```
mgrctl cp intermediateCA.pem server:/tmp/intermediateCA.pem
```

```
mgrctl exec -ti 'spacecmd proxy_container_config -- -p 8022 -i /tmp/intermediateCA.pem pxy.example.com srv.example.com 2048 email@example.com /tmp/ca.crt /tmp/proxy.crt /tmp/proxy.key -o /tmp/config.tar.gz'
```

4. 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 .
```

3.2.4.6. 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. まだ実行していない場合は、前のステップで生成された設定アーカイブ (`config.tar.gz`) をサーバコンテナからサーバホストにコピーします。

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

2. まだ実行していない場合は、サーバホスト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. プロキシホストで、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
```

3.2.4.7. SUSE Multi-Linux Manager 5.1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
```


5つのSUSE Multi-Linux Managerプロキシコンテナが存在し、また、**proxy-pod**コンテナポッドの一部である必要があります。

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

3.2.4.7.1. 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 Multi-Linux 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-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。

```
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。

3.2.5. K3sへのSUSE Multi-Linux Manager 5.1プロキシの配備

3.2.5.1. K3sのインストール



SUSE Multi-Linux Managerプロキシは、シングルノードクラスタのSL 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 -
```

3.2.5.2. 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。

mgrpxyおよび**helm**パッケージはSUSE Multi-Linux Managerプロキシの製品リポジトリで利用可能です。

1. インストールするには、次のコマンドを実行します。

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

2. 再起動

3.2.5.2.1. 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

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 Multi-Linux Managerサーバまたは別のSUSE Multi-Linux 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 Multi-Linux 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 80% of available storage for the containers.



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 Multi-Linux 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 Multi-Linux 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。

6. **[生成]**をクリックして、SUSE Multi-Linux 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。
7. 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。

3.2.5.2.2. spacecmdと自己署名証明書を使用したプロキシ設定の生成

`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と自己署名証明書を使用してプロキシ設定を生成する

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 .
```

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

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

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. Execute the following commands, 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. If your setup uses an intermediate CA, copy it as well and include it in the command with the -i option (can be provided multiple times if needed) :

```
mgrctl cp intermediateCA.pem server:/tmp/intermediateCA.pem
mgrctl exec -ti 'spacecmd proxy_container_config -- -p 8022 -i
/tmp/intermediateCA.pem pxy.example.com srv.example.com 2048 email@example.com
/tmp/ca.crt /tmp/proxy.crt /tmp/proxy.key -o /tmp/config.tar.gz'
```

4. 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 .
```

3.2.5.3. SUSE Multi-Linux ManagerプロキシHelmチャートの配備

SUSE Multi-Linux 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 Multi-Linux 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。

```
mgrpxy 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。

3.2.6. SUSE Multi-Linux ManagerプロキシのAir-gapped配備

3.2.6.1. 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。



現時点では、Air-gapped配備はSL Microでのみ利用可能です。

3.2.6.2. 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 Multi-Linux Managerの仮想マシンイメージ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 Multi-Linux 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 Multi-Linux 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。

3.2.6.3. SL MicroにSUSE Multi-Linux Managerを配備する

SUSE Multi-Linux 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SL MicroにSUSE Multi-Linux Managerをインストールする

1. SL Microをインストールします。
2. SUSE Multi-Linux 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と置き換えます)。

```
transactional-update pkg install mgrpxy* mgrctl* suse-multi-linux-manager-5.1-$ARCH$-proxy-*
```

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

SL MicroにSUSE Multi-Linux 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 Multi-Linux 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 4. アップグレードと移行

4.1. サーバ

4.1.1. ディストリビューションのアップグレードとサーバ移行



- SUSE Multi-Linux Manager 5.0 must be stopped before the upgrade.
- SUSE Multi-Linux Manager 5.0 is not supported on top of SL Micro 6.1 & SUSE Linux Enterprise Server 15 SP7 as host OS.

SUSE Multi-Linux Manager server hosts that are hardened for security may restrict execution of files from the **/tmp** folder. In such cases, as a workaround, export the **TMPDIR** environment variable to another existing path before running **mgradm**.



例:

```
export TMPDIR=/path/to/other/tmp
```

SUSE Multi-Linux Managerの更新では、この回避策が不要になるようにツールが変更されます。

SSL certificates are needed at a later stage. If not using the self-signed generated CA and certificates, ensure you have the following before starting:

- 認証局(CA) SSLパブリック証明書。 CAチェーンを使用している場合は、すべての中間CAも使用できる必要があります。
- An SSL database private key.
- An SSL database certificate.

すべてのファイルがPEM形式である必要があります。

SSLサーバ証明書のホスト名は、配備先マシンの完全修飾ホスト名と一致している必要があります。 ホスト名は、証明書の**X509v3 Subject Alternative Name**セクションで設定できます。 環境で必要な場合は、複数のホスト名を一覧にすることもできます。 サポートされているキーの種類は、**RSA**と**EC** (Elliptic Curve)です。



Database SSL certificate requires **reportdb** and **db** and the FQDN used to access the report database as **Subject Alternative Name**.

During a migration the server SSL certificate and CA chain are copied from the source server, meaning that only the database certificates are required



SUSE Multi-Linux Manager 5.0 peripheral servers are always using third-party SSL certificates. If the hub server has generated the certificates for the peripheral server, it needs to generate the certificate for the peripheral database too.

On the hub server, run the following command for each of the peripheral server to migrate.

```
mgrctl exec -ti -- rhn-ssl-tool --gen-server --dir="/root/ssl-build"
--set-country="COUNTRY" \
--set-state="STATE" --set-city="CITY" --set-org="ORGANIZATION" \
--set-org-unit="ORGANIZATION UNIT" --set-email="name@example.com" \
--set-hostname=<hostname>-reportdb --set-cname="example.com" --set
-cname=db --set-cname=reportdb
```

The files to use will be inside the server container and need to be copied to the new peripheral server host:

1. `/root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT` as the root CA,
2. `/root/ssl-build/<hostname>-reportdb/server.crt` as the db certificate and
3. `/root/ssl-build/<hostname>-reportdb/server.key` as the db certificate's key.

4.1.1.1. Client tools rebranding

SUSE Multi-Linux Manager 5.1では、サポート対象のすべてのオペレーティングシステム向けに、ブランド変更されたクライアントツールセットが導入されています。この移行はシームレスに行われ、新しい製品同期を実行するユーザは、更新されたチャンネル名にのみ気づくはずです。

Channels named **SUSE Manager Client Tools for XYZ**, used by clients previously registered with SUSE Multi-Linux Manager 4.3 or 5.0, are no longer available in version 5.1 and will no longer receive updates in 5.1.

移行後もレガシチャンネルは既存のクライアントに割り当てられたままですが、対応するリポジトリは削除されています。

継続的な更新を確実に行うには、ユーザは以下の操作を実行する必要があります。

- Mirror the new **SUSE Multi-Linux Manager Client Tools for XYZ** channels for the relevant products and assign them to the appropriate clients.
- Unassign the outdated **SUSE Manager Client Tools for XYZ** channels.

これにより、古いクライアントツールに基づくCLMプロジェクトも適宜調整する必要があります。

For example workflow, see **Common-workflows > Workflow-switch-to-new-client-tools-channels**.

4.1.1.2. SLE Micro 5.5からSL Micro 6.1

このドキュメントでは、SUSE Multi-Linux Manager 5.0 Serverが配備されたSLE Micro 5.5ホストをSL Micro 6.1にアップグレードし、SUSE Multi-Linux Manager 5.1に移行するためのテスト済みプロシージャについて説明します。

4.1.1.2.1. 前提条件

- SUSE Multi-Linux Manager 5.0がSLE Micro 5.5にインストールされ、実行されている。
- システムは登録済みであり、SCCにアクティブなサブスクリプションがある。

4.1.1.2.2. Distribution upgrade and server migration

プロシージャ: SUSE Multi-Linux Manager 5.0からSUSE Multi-Linux Manager 5.1への移行

1. Verify current product status.

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

Confirm:

- ベースOS: **SUSE Linux Enterprise Micro 5.5**
- 拡張機能: **SUSE Manager Server 5.0拡張機能**

2. Ensure the system is updated.

```
transactional-update patch
```

- If patches were applied, stop the server and then reboot the system before proceeding to migration:

```
mgradm stop  
reboot
```

- 更新が見つからなかった場合、移行ステップに直接進むことができます。

3. Start the migration.

```
transactional-update migration --auto-agree-with-licenses --gpg-auto-import  
-keys
```

プロンプトに従って、**SUSE Linux Micro 6.1**および**SUSE Multi-Linux Manager Server Extension 5.1**への利用可能な移行を選択します。

4. Stop the server and then reboot to apply changes.

```
mgradm stop
```

```
reboot
```

5. Perform post-reboot checks.

アップグレードされたOSとSUSE Multi-Linux Manager拡張機能を確認します。

```
cat /etc/os-release  
SUSEConnect --status-text
```

以下が表示されるはずです。

- **PRETTY_NAME="SUSE Linux Micro 6.1"**
- **SUSE Multi-Linux Manager Server 5.1 Extension**

Enable root SSH access (if required). SL Micro 6.1 disables root login via SSH by default. Edit `/etc/ssh/sshd_config.d/sshd.conf`:

```
PermitRootLogin yes
```

サービスを再起動します。

```
systemctl restart sshd
```

詳細については、**Administration › Troubleshooting**を参照してください。

6. Verify SUSE Multi-Linux Manager tools

```
mgradm --version
```

予想される出力:

- Version **5.1.11** or higher
- References **5.1.0** or higher

7. Upgrade server containers.

```
mgradm upgrade podman
```

プロンプトに従い、新しい5.1.0コンテナをプルして設定します。

8. Check the running containers:

```
podman ps
```

以下が表示されるはずです。

- **server:5.1.0** or higher
- **server-postgresql:5.1.0** or higher



Errors for missing services like **uyuni-db** or **saline** during upgrade can be ignored if not installed previously.

4.1.1.2.3. Migration complete

The system is now running SUSE Multi-Linux Manager 5.1 on SL Micro 6.1. Validate your setup before resuming production operations. If you have a SUSE Multi-Linux Manager 5.0 proxy connected to this server, proceed to the **Installation-and-upgrade > Container-deployment** guide to upgrade the proxy host.

4.1.1.2.4. データベースバックアップボリューム

mgradm migrationまたは**mgradm upgrade**を使用したサーバ移行またはアップグレードにより、データベースバックアップを含むボリュームを作成できます。

PostgreSQLデータベースのバージョンを上げる際には、アップグレードを実行する前に古いデータベースを別の場所に保存する必要があります。この目的のために、**mgradm**はボリューム**var-pgsql-backup**を動的に作成します。移行またはアップグレードが完了し、ユーザが新しいシステムが期待通りに動作することを確認したら、このボリュームは安全に削除できます。

4.1.1.3. SUSE Linux Enterprise Server 15 SP6から15 SP7

このドキュメントでは、SUSE Multi-Linux Manager 5.0 Serverが配備されたSUSE Linux Enterprise Server 15 SP6ホストをSUSE Multi-Linux Manager 5.1を備えたSUSE Linux Enterprise Server 15 SP7にアップグレードするためのテスト済みプロシージャについて説明します。

4.1.1.3.1. 前提条件

- SUSE Multi-Linux Manager 5.0がSUSE Linux Enterprise Server 15 SP6 にインストールされ、実行されている。
- システムはSUSEカスタマーセンター(SCC)に登録済みで、有効なサブスクリプションがある。
- 続行する前にバックアップ作成されていることを確認する。

4.1.1.3.2. Distribution upgrade and server migration

プロシージャ: SUSE Multi-Linux Manager 5.0からSUSE Multi-Linux Manager 5.1への移行

1. Verify current product status.

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

Confirm:

- Base OS: **SUSE Linux Enterprise Server 15 SP6**
- Extension: **SUSE Manager Server 5.0 Extension**

2. Apply all system patches.

```
zypper patch
```

3. Stop the server, and then reboot if the update stack was updated.

```
mgradm stop  
reboot
```

4. Launch the Zypper migration tool.

```
zypper migration
```

Zypperは、可能な移行ターゲットと詳細を表示します。

5. 適切なターゲットを選択し、プロンプトに従って移行を実行します。
6. After the migration completes, stop the server and then reboot the system.

```
mgradm stop  
reboot
```

7. Perform post-reboot checks:

Verify upgraded OS and SUSE Multi-Linux Manager extension.

```
cat /etc/os-release  
SUSEConnect --status-text
```

以下が表示されるはずですが。

- **VERSION="15-SP7"**
- **SUSE Multi-Linux Manager Server 5.1 Extension for SLE**

8. Verify SUSE Multi-Linux Manager tools version.

```
mgradm --version
```

予想される出力:

- Version **5.1.11** or higher
- Image tag **5.1.0** or higher

9. Upgrade the server containers.

```
mgradm upgrade podman
```

プロンプトに従って新しいコンテナイメージを取得し、環境を再設定します。

10. Check the running containers.

```
podman ps
```

予想されるコンテナ:

- **server:5.1.0** or higher
- **server-postgresql:5.1.0** or higher

4.1.1.3.3. Migration complete

The system is now running SUSE Multi-Linux Manager 5.1 on SUSE Linux Enterprise Server 15 SP7. Validate your setup before resuming production operations. If you have a SUSE Multi-Linux Manager 5.0 proxy connected to this server, proceed with **Installation-and-upgrade › Container-deployment**.

4.1.1.3.4. データベースバックアップボリューム

mgradm migrationまたは**mgradm upgrade**を使用したサーバ移行またはアップグレードにより、データベースバックアップを含むボリュームを作成できます。

PostgreSQLデータベースのバージョンを上げる際には、アップグレードを実行する前に古いデータベースを別の場所に保存する必要があります。この目的のために、**mgradm**はボリューム**var-pgsql-backup**を動的に

作成します。移行またはアップグレードが完了し、ユーザが新しいシステムが期待通りに動作することを確認したら、このボリュームは安全に削除できます。

4.1.2. コンテナ化された環境へのSUSE Multi-Linux Managerサーバの移行

4.1.2.1. Requirements and considerations

4.1.2.1.1. General requirements

- SUSE Multi-Linux Manager 4.3サーバをコンテナに移行するには、SL Micro 6.1またはSUSE Linux Enterprise Server 15 SP7と**mgradm**がインストールされた新しいマシンが必要です。
- 選択したホストオペレーティングシステムがSL Micro 6.1またはSUSE Linux Enterprise Server 15 SP7のいずれであっても、SUSE Multi-Linux Manager 4.3 から5.1へのインプレース移行はサポートされていません。

Before migrating from SUSE Multi-Linux Manager 4.3 to 5.1, any existing traditional clients including the traditional proxies must be migrated to Salt. For more information about migrating traditional SUSE Multi-Linux Manager 4.3 clients to Salt clients, see [Migrate Traditional Clients to Salt Clients](#).

- 従来の接続プロトコルは、SUSE Multi-Linux Manager 5.0以降ではサポートされなくなりました。



This guide only covers the migration from SUSE Multi-Linux Manager 4.3 to 5.1.

Migrating an existing SUSE Multi-Linux Manager 5.1 instance to the same version while switching the host operating system from SL Micro 6.1 to SUSE Linux Enterprise Server 15 SP7, or vice versa, is not handled by the **mgradm migrate** command.

4.1.2.1.2. ホスト名

- Current migration procedure does not include functionality for renaming hostnames. As a result, fully qualified domain name (FQDN) of the new server will remain the same as that of the old server.
- 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。



After the migration, it is necessary to manually update the DHCP and DNS records to point to the new server.

4.1.2.1.3. GPG keys

- Self-trusted GPG keys are not migrated.
- GPG keys that are trusted in the RPM database only are not migrated. Thus, synchronizing channels with **spacewalk-repo-sync** can fail.
- 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。

Procedure: Manual migration of the 4.3 GPG keys to the new server

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。

4.1.2.1.4. SSL certificates

SSL certificates are needed at a later stage. If not using the self-signed generated CA and certificates, ensure you have the following before starting:

- 認証局(CA) SSLパブリック証明書。 CAチェーンを使用している場合は、すべての中間CAも使用できる必要があります。
- An SSL database private key.
- An SSL database certificate.

すべてのファイルがPEM形式である必要があります。

SSLサーバ証明書のホスト名は、配備先マシンの完全修飾ホスト名と一致している必要があります。 ホスト名は、証明書の **X509v3 Subject Alternative Name** セクションで設定できます。 環境で必要な場合は、複数のホスト名を一覧にすることもできます。 サポートされているキーの種類は、**RSA**と**EC** (Elliptic Curve)です。



Database SSL certificate requires **reportdb** and **db** and the FQDN used to access the report database as **Subject Alternative Name**.

During a migration the server SSL certificate and CA chain are copied from the source server, meaning that only the database certificates are required

4.1.2.2. 移行

4.1.2.2.1. Prepare SUSE Multi-Linux Manager 5.1 server host



準備されたSL Micro 6.1またはSUSE Linux Enterprise Server 15 SP7システムにSUSE Multi-Linux Managerを事前にインストールしないでください。

移行プロセスは、サーバのインストールを自動的に実行するように設計されています。 **mgradm install**を実行してから**mgradm migrate**を実行することはサポートされておらず、サポートされていないシステム状態を引き起こします。

以下のステップでは、ホストシステムの準備のみを行い、実際のSUSE Multi-Linux Manager 5.1サーバのインストールは行いません。

You can use VM images based on SL Micro 6.1 as a migration target. In such a scenario, you can prepare the host system as described in

- [Installation-and-upgrade › Container-deployment](#)

または

- **Installation-and-upgrade › Container-deployment.**

However, at the end the last step is executing the command **mgradm migrate <FQDN>** instead of **mgradm install <FQDN>**.

SLE Micro 6.1ホストの準備

インストールメディアのダウンロード

Procedure: Downloading the installation media

1. <https://www.suse.com/download/sle-micro/>でSL Micro 6.1のインストールメディアを見つけて、適切なメディアファイルをダウンロードします。
2. 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。

SL Micro 6.1のインストール

マシン(仮想または物理)の準備の詳細については、[SL Micro配備ガイド](#)を参照してください。

プロシージャ: SL Micro 6.1のインストール

1. SLE Micro 6.1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。
2. システムをブートまたは再起動します。
3. 矢印キーを使用してインストールを選択します。
4. キーボードと言語を調整します。
5. 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。
6. 次へをクリックして続行します。
7. 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。



SUSE Multi-Linux Manager 5.1コンテナは拡張機能としてインストールされます。以下のリストから必要な特定の拡張機能に応じて、それぞれに追加のSUSE Customer Center登録コードが必要です。

- SUSE Multi-Linux Manager 5.1サーバ

- SUSE Multi-Linux Manager 5.1プロキシ
- SUSE Multi-Linux Manager 5.1 Retail Branch Server



SL Micro 6.1エンタイトルメントは、SUSE Multi-Linux Managerエンタイトルメント内に含まれているため、別途登録コードは必要ありません。

8. SUSE Customer Centerの電子メールアドレスを入力します。
9. SL Micro 6.1の登録コードを入力します。
10. 次へをクリックして続行します。
11. プロキシをインストールするにはSUSE Multi-Linux Manager 5.1プロキシ拡張機能、サーバをインストールするにはSUSE Multi-Linux Manager 5.1サーバ拡張機能のチェックボックスを選択します。
12. 次へをクリックして続行します。
13. SUSE Multi-Linux Manager 5.1拡張機能の登録コードを入力します。
14. [次へ]をクリックして続行します。
15. NTP設定ページで、[次へ]をクリックします。
16. 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。
17. 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SL Micro 6.1とSUSE Multi-Linux Manager 5.1のインストールが完了しました。

オプション: コマンドラインからの登録

SL Micro 6.1のインストール中にSUSE Multi-Linux Manager 5.1を拡張機能として追加した場合は、このプロセス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、SL Micro 6.1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、SL Micro 6.1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。



次のステップでは、SUSE Multi-Linux Manager 5.1拡張機能を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アーキテクチャを登録する場合は、正しい登録コードを使用してください。

Procedure: Registering from the command line

1. 次のコマンドで利用可能な拡張機能を一覧表示します。

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

2. 利用可能な拡張機能のリストから、インストールしたい拡張機能を選択します。

- a. サーバをインストールする場合は、次のコマンドで SUSE Multi-Linux Manager Server Extension 5.1 x86_64の登録コードを使用します。

```
transactional-update register -p Multi-Linux-Manager-Server/5.1/x86_64 -r <reg_code>
```

- b. プロキシをインストールする場合は、次のコマンドで SUSE Multi-Linux Manager Proxy Extension 5.1 x86_64の登録コードを使用します。

```
transactional-update register -p Multi-Linux-Manager-Proxy/5.1/x86_64 -r <reg_code>
```

3. 再起動します。

システムの更新

Procedure: Updating the system

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。



SL Microはデフォルトで自己更新するように設計されており、更新を適用すると再起動します。ただし、SUSE Multi-Linux Manager環境ではこの動作は望ましくありません。サーバの自動更新を防ぐには、SUSE Multi-Linux Managerでブートストラッププロセス中にtransactional-updateのタイマを無効にします。

SL 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を有効にします。

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

Prepare SUSE Linux Enterprise Server 15 SP7 host

または、SUSE Linux Enterprise Server 15 SP7にSUSE Multi-Linux Managerを配備することもできます。

The following procedures describe the main steps of the installation process.

Install SUSE Multi-Linux Manager extensions on SUSE Linux Enterprise Server

Procedure: Installing SUSE Multi-Linux Manager Extensions on SUSE Linux Enterprise Server

1. <https://www.suse.com/download/sles/>でSUSE Linux Enterprise Server 15 SP7 .isoを見つけてダウンロードします。
2. ホストオペレーティングシステム(SUSE Linux Enterprise Server 15 SP7)と拡張機能の両方の登録コードがあることを確認します。
3. SUSE Linux Enterprise Server 15 SP7のインストールを開始します。
 - a. **Language, Keyboard and Product Selection**（言語、キーボードおよび製品の選択）で、インストールする製品を選択します。
 - b. **ライセンス契約**で契約を読み、**[I Agree to the License Terms**（ライセンス条項に同意します）にチェックを付けます。
4. 登録方法を選択します。この例では、SUSEカスタマーセンターにサーバを登録します。
5. SUSE Customer Centerの電子メールアドレスを入力します。
6. SUSE Linux Enterprise Server 15 SP7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。



SUSE Linux Enterprise Server 15 SP7には、有効なSUSE Linux Enterprise Serverサブスクリプションと対応する登録コードが必要であり、この画面で入力する必要があることに注意してください。以下でSUSE Multi-Linux Manager拡張機能の登録コードを入力する必要があります。

8. **拡張とモジュールの選択**で、以下にチェックを付けます。

- サーバをインストールするにはSUSE Multi-Linux Managerサーバ拡張機能を選択し、プロキシをインストールするにはSUSE Multi-Linux Managerプロキシ拡張機能を選択します。
- ベースシステムモジュール
- Containersモジュール

9. 次へをクリックして続行します。

10. SUSE Multi-Linux Manager 5.1拡張機能の登録コードを入力します。

11. [次へ]をクリックして続行します。

12. インストールを完了します。

13. インストールが完了したら、rootとして新しくインストールしたサーバにログインします。

14. システムを更新します(オプション。インストール時にシステムが更新をダウンロードするように設定されていない場合)。

```
zypper up
```

15. 再起動します。

オプション: コマンドラインからの登録

If you added SUSE Multi-Linux Manager 5.1 as an extension during SUSE Linux Enterprise Server installation then you can skip this procedure.

However, optionally you may skip registration during SUSE Linux Enterprise Server installation by selecting the [**Skip Registration**] button. This section provides steps on registering your products after SUSE Linux Enterprise Server installation.



The following steps register a SUSE Multi-Linux Manager 5.1 extension with the x86-64 architecture and thus require a registration code for the x86-64 architecture.

To register ARM or s390x architectures use the correct registration code.

Procedure: Registering from the command line

1. 次のコマンドで利用可能な拡張機能を一覧表示します。

```
SUSEConnect --list-extensions
```

From the list of available extensions, select the one you wish to install.

If installing the Server, use your SUSE Multi-Linux Manager Server Extension 5.1 x86_64 registration code. For example for SUSE Linux Enterprise 15 SP7, use the following commands:

```
SUSEConnect -r <regcode>
SUSEConnect -p sle-module-containers/15.7/x86_64
SUSEConnect -p Multi-Linux-Manager-Server-SLE/5.1/x86_64 -r <regcode>
```

- If installing the Proxy, use your SUSE Multi-Linux Manager Proxy Extension 5.1 x86_64 registration code with the following command:

```
SUSEConnect -p Multi-Linux-Manager-Proxy-SLE/5.1/x86_64 -r <regcode>
```

Install and enable podman

Procedure: Installing podman

1. Log in as root and install the product package.

- On the server:

```
zypper in podman
zypper in -t product SUSE-Multi-Linux-Manager-Server
```

- On the proxies:

```
zypper in podman
zypper in -t product SUSE-Multi-Linux-Manager-Proxy
```



Make sure that package **podman** is installed. Additionally, on the server **mgradm** and **mgradm-bash-completion** or on the proxies, **mgrpky** and **mgrpky-bash-completion** also need to be installed.

2. システムを再起動するか、次のコマンドを実行してPodmanサービスを起動します。

```
systemctl enable --now podman.service
```

4.1.2.2.2. SSH connection preparation

このステップを使用すると、新しいSUSE Multi-Linux Manager 5.1サーバが既存の4.3サーバにパスワードを必要とせずにSSH経由で接続できるようになります。このステップには、SSHキーの生成と設定、SSHエージェントのセットアップ、および公開鍵の古いサーバへのコピーが含まれます。このセットアップは、手動

による介入なしに移行プロセスを実行するために必要です。

プロシージャ: SSH接続を準備する

1. **root**に対して、新しい5.1サーバ上にSSHキーが存在することを確認します。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. パスワードを要求しない4.3サーバへの接続のために、新しいサーバ上でSSH設定とエージェントを準備する必要があります。

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



パスワードを要求しない接続を確立するために、移行スクリプトは新しいサーバで実行されているSSHエージェントに依存します。この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。その後、`ssh-add`に続けて機密鍵へのパスを指定し、実行中のエージェントにSSHキーを追加します。このプロセス中に、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 Multi-Linux 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 Multi-Linux 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ないことも確認します。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。

4.1.2.2.3. Perform the migration

When planning your migration from SUSE Manager 4.3 to SUSE Multi-Linux Manager 5.1, ensure that your target instance meets or exceeds the specifications of the old setup.

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。



SUSE Multi-Linux Manager server hosts that are hardened for security may restrict execution of files from the `/tmp` folder. In such cases, as a workaround, export the **TMPDIR** environment variable to another existing path before running **mgradm**.

例:

```
export TMPDIR=/path/to/other/tmp
```

SUSE Multi-Linux Managerの更新では、この回避策が不要になるようにツールが変更されます。

When migrating from SUSE Manager 4.3, you will be prompted for the **Password for the CA key to generate**. It is essential to enter the same CA password that was used in your SUSE Manager 4.3 installation.



Entering the wrong password will result in a failure to generate the database certificate and will cause the migration to abort with the following error:

```
Error: cannot configure db container: Cannot generate database
certificate: CA validation failed!
```

Make sure the correct CA password is available before starting the migration process.

Procedure: Performing the migration

1. 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。**mgr-storage-server**の詳細については、[installation-and-upgrade:hardware-requirements.pdf](#)を参照してください。
2. Execute the following command to migrate and set up a new SUSE Multi-Linux Manager 5.1 server. Replace `<oldserver.fqdn>` with the FQDN of the 4.3 server:



移行プロセスを開始する前に、4.3サーバを必ずアップグレードして、利用可能なすべての更新を適用してください。また、不要なチャンネルを削除すると、全体的な移行時間を短縮できます。



The migration can take a very long time depending on the amount of data that needs to be replicated. To reduce downtime it is possible to run the migration multiple times in a process of initial replication, re-replication, or final replication and switch over while all the services on the old 4.3 server can stay up and running.

Only during the final migration, the processes on the old 4.3 server need to be stopped.

For all non-final replications add the parameter **--prepare** to prevent the automatic stopping of services on the old 4.3 server.

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

Procedure: Final migration

1. Stop the SUSE Manager services on 4.3 Server:

```
spacewalk-service stop
```

2. 4.3サーバ上のPostgreSQLサービスを停止します。

```
systemctl stop postgresql
```

3. Perform the final migration on SUSE Multi-Linux Manager 5.1 Server

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

4. 信頼されているSSL CA証明書を移行します。

Migration of the certificates

Trusted SSL CA certificates that were installed as part of an RPM and stored on SUSE Multi-Linux 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 SUSE Manager 4.3 server after the migration.

Procedure: Migrating the certificates

1. Copy the file from the SUSE Manager 4.3 Server to the new SUSE Multi-Linux Manager 5.1 Server. 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。

```
mgrctl 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5.1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FQDNとIPアドレスを使用する必要があります。

クライアントにminionの最新バージョンがインストールされている場合、IPアドレスの調整は不要です。新しいバージョンではFQDNのみを使用してサーバに自動的に再接続できるためです。

4.1.2.3. Client tools rebranding

SUSE Multi-Linux Manager 5.1 introduces a rebranded set of client tools for all supported operating systems. This transition is seamless, and users performing a new product synchronization should only notice the updated channel names.

Channels named **SUSE Manager Client Tools for XYZ**, used by clients previously registered with SUSE Multi-Linux Manager 4.3 or 5.0, are no longer available in version 5.1 and will no longer receive updates in 5.1.

移行後もレガシチャンネルは既存のクライアントに割り当てられたままですが、対応するリポジトリは削除されています。

継続的な更新を確実に行うには、ユーザは以下の操作を実行する必要があります。

- Mirror the new **SUSE Multi-Linux Manager Client Tools for XYZ** channels for the relevant products and assign them to the appropriate clients.
- Unassign the outdated **SUSE Manager Client Tools for XYZ** channels.

これにより、古いクライアントツールに基づくCLMプロジェクトも適宜調整する必要があります。

For example workflow, see **Common-workflows > Workflow-switch-to-new-client-tools-channels**.

4.1.3. SUSE Multi-Linux Managerサーバのアップグレード

Before running the upgrade command, it is required to update the host operating system. Updating the host operating system will also result in the update of the SUSE Multi-Linux Manager tooling such as the **mgradm** tool.

プロシージャ: サーバのアップグレード

1. **zypper**を使用してソフトウェアリポジトリを更新します。

```
zypper ref
```

2. ホストオペレーティングシステムに応じて、以下のステップに進みます。

SL Microなどのトランザクションシステムの場合:

1. **transactional-update**を使用して利用可能な更新を適用します。

```
transactional-update
```

2. 更新が適用されたら、**reboot**を実行して再起動します。

SUSE Linux Enterprise Serverの場合:

zypperを使用してインストールされたソフトウェアを更新します。

```
zypper up
```

3. SUSE Multi-Linux Manager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。

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

```
podman image prune -a
```

Upgrading with third-party SSL certificate

If you are using third-party certificates, the database container needs to have an SSL certificate with the following Subject Alternate Names (SANs):

- **db**
- **reportdb**



- the externally facing fully qualified domain name

The same certificate can be used for both the main container and the database one, but it needs to have those SANs too.

In order to pass the new certificate to the upgrade command, use the `--ssl-db-ca-root`, `--ssl-db-cert` and `--ssl-db-key` parameters.

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。

4.1.3.1. データベースバックアップボリューム

mgradm migrationまたは**mgradm upgrade**を使用したサーバ移行またはアップグレードにより、データベースバックアップを含むボリュームを作成できます。

PostgreSQLデータベースのバージョンを上げる際には、アップグレードを実行する前に古いデータベースを別の場所に保存する必要があります。この目的のために、**mgradm**はボリューム**var-pgsql-backup**を動的に作成します。移行またはアップグレードが完了し、ユーザが新しいシステムが期待通りに動作することを確認したら、このボリュームは安全に削除できます。

4.2. プロキシ

4.2.1. Proxy Migration from 5.0 to 5.1

4.2.1.1. 概要

このドキュメントは、**SUSE Multi-Linux Manager**で管理される環境において、**ホストオペレーティングシステムとプロキシ拡張機能の両方を移行するためのテスト済みかつ検証済みのプロシージャ**を提供します。特に、**SUSE Multi-Linux Manager Proxy 5.0**を配備したシステムを対象としています。

対象となるアップグレードシナリオは次のとおりです。

- **SUSE Linux Enterprise Micro (SLE Micro) 5.5からSLE Micro 6.1への移行**
- **SUSE Linux Enterprise Server (SLES) 15 SP6からSLES 15 SP7への移行**
- **SUSE Multi-Linux Managerプロキシ拡張機能のバージョン5.0からバージョン5.1へのアップグレード**



Before migrating the proxy, it is required to first migrate the SUSE Manager 5.0 Server to SUSE Multi-Linux Manager 5.1.

4.2.1.2. SLE Micro 5.5からSL Micro 6.1

このセクションでは、SUSE Multi-Linux Manager 5.0プロキシが配備されたSLE Micro 5.5ホストをSUSE Multi-Linux Manager 5.1プロキシを備えたSL Micro 6.1にアップグレードするためのテスト済みプロシージャについて説明します。

4.2.1.2.1. 前提条件

- SUSE Multi-Linux Manager 5.0プロキシがSLE Micro 5.5にインストールされ、実行されている。
- プロキシシステムがSUSE Multi-Linux Managerサーバに登録されている。

4.2.1.2.2. Distribution upgrade and proxy migration

Procedure: Migrate SUSE Multi-Linux Manager 5.0 Proxy to SUSE Multi-Linux Manager 5.1 Proxy

1. Verify System and SUSE Multi-Linux Manager Tools version.

```
cat /etc/os-release  
mgrpxy --version
```

Confirm:

- Operating System: **SLE Micro 5.5**
- Tools version: **mgrpxy version 0.1.29** or higher

2. Check running containers.

```
podman ps
```

以下のコンテナが実行されていることを確認します。

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

3. Synchronize the new Proxy Products in SUSE Multi-Linux Manager Server. For more information, see **Client-configuration › Products**.

Web UIを使用して同期します。

- SUSE Linux Micro 6.1
- SUSE Multi-Linux Manager Proxy Extension 5.1

4. Perform proxy product migration. For more information, see **Client-configuration › Client-upgrades-product-migration**.

Navigate to the proxy system and select **Systems › Overview › Software › Product Migration**.

Migrate from

- SLE Micro 5.5 + SUSE Manager Proxy 5.0 Extension

to

- SL Micro 6.1 + SUSE Multi-Linux Manager Proxy Extension 5.1



必要であることが確認されていない限り、プロンプトが表示されたときにオプションのチャンネルを**選択しないでください**。



It is recommended to do a dry-run first before performing the actual migration.

5. Monitor the migration action.

You can follow the process under **Systems › Details › Events** tab in the Web UI.

6. After the upgrade completes, stop the proxy container and then reboot the system.

```
mgrpxy stop
reboot
```

7. Perform post-reboot checks.

アップグレードされたOSとSUSE Multi-Linux Manager拡張機能を確認します。

```
cat /etc/os-release
SUSEConnect --status-text
```

以下が表示されるはずです。

- **PRETTY_NAME="SUSE Linux Micro 6.1"**
- **SUSE Multi-Linux Manager Proxy 5.1 Extension**

8. Verify SUSE Multi-Linux Manager tools version.

```
mgrpky --version
```

予想される出力:

- **mgrpky version 5.1.11 or higher**

9. ルートSSHアクセスを有効化します(必要な場合)。SL Micro 6.1ではデフォルトでSSH経由のルートログインが無効化されています。`/etc/ssh/sshd_config.d/sshd.conf`を編集します。

```
PermitRootLogin yes
```

サービスを再起動します。

```
systemctl restart sshd
```

詳細については、**Administration › Troubleshooting**を参照してください。

10. Install the new proxy container images as RPM packages.

```
transactional-update pkg install suse-multi-linux-manager-5.1-x86_64-proxy*
```

11. Reboot the P-roxy.

12. Upgrade proxy containers and restart them.

```
mgrpky upgrade podman
mgrpky stop
mgrpky start
```

13. Confirm proxy containers are operational.

```
podman ps
```

All expected proxy containers should be up and running:

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

4.2.1.2.3. Migration complete

プロキシホストシステムは現在、更新されたSUSE Multi-Linux Manager 5.1プロキシパッケージと、同期された製品チャンネルを備えたSL Micro 6.1を実行しています。

4.2.1.3. SUSE Linux Enterprise Server 15 SP6から15 SP7

This section provides the procedure to upgrade a SUSE Linux Enterprise Server SP6 host deployed with SUSE Multi-Linux Manager 5.0 Proxy to SUSE Linux Enterprise Server SP7 with SUSE Multi-Linux Manager 5.1 Proxy.

4.2.1.3.1. 前提条件

- SUSE Multi-Linux Manager Proxy 5.0がSUSE Linux Enterprise Server 15 SP6にインストールされ、実行されている。
- プロキシシステムがSUSE Multi-Linux Managerサーバに登録されている。

4.2.1.3.2. Distribution upgrade and proxy migration

Procedure: Update SUSE Multi-Linux Manager Proxy components on SUSE Linux Enterprise Server 15 SP6

1. Verify operating system and SUSE Multi-Linux Manager tools version.

```
cat /etc/os-release
mgrpxy --version
```

Confirm:

- Operating System: **SUSE Linux Enterprise Server 15 SP6**

- Tools version: **mgrpxy version 0.1.29** or higher

2. List running proxy containers.

```
podman ps
```

次のコンテナが実行されていることを確認します。

- **proxy-salt-broker**
- **proxy-httpd**
- **proxy-squid**
- **proxy-tftpd**
- **proxy-ssh**
- サポートインフラストラクチャコンテナ

3. Synchronize the new proxy products in SUSE Multi-Linux Manager Server. For more information see **Client-configuration › Products**.

Using the Web UI, synchronize the following:

- **SUSE Linux Enterprise Server 15 SP7**
 - **SUSE Multi-Linux Manager Proxy Extension for SLE 5.1**



Proxy extensions are listed under **Basesystem Module 15 SP7` > `Containers Module 15 SP7**.

4. Perform proxy product migration. For more information, see **Client-configuration › Client-upgrades-product-migration**.

Navigate to the proxy system and select **Systems › Overview › Software › Product Migration**.

Migrate from

- **SUSE Linux Enterprise Server 15 SP6 + SUSE Manager Proxy Extension 5.0**

to

- **SUSE Linux Enterprise Server 15 SP7 + SUSE Multi-Linux Manager Proxy Extension for SLE 5.1**



必要であることが確認されていない限り、プロンプトが表示されたときにオプションのチャンネルを**選択しないでください**。



It is recommended to do a dry-run first before performing the actual migration.

5. Monitor the migration action.

You can follow the process under **Systems › Details › Events** tab in the Web UI.

6. After the upgrade completes, stop the proxy container and then reboot the system.

```
mgrpxy stop
reboot
```

7. Perform post-reboot checks:

Verify upgraded OS and SUSE Multi-Linux Manager extension.

```
cat /etc/os-release
SUSEConnect --status-text
```

以下が表示されるはずです。

- **PRETTY_NAME="SUSE Linux Enterprise Server 15 SP7"**
- **SUSE Multi-Linux Manager Proxy 5.1 Extension for SLE**

8. Verify SUSE Multi-Linux Manager tools version.

```
mgrpxy --version
```

予想される出力:

- **mgrpxy version 5.1.11 or higher**

9. Install the new proxy container images as RPM packages.

```
zypper install suse-multi-linux-manager-5.1-x86_64-proxy*
```

10. Upgrade proxy containers and restart them.

```
mgrpky upgrade podman  
mgrpky stop  
mgrpky start
```

11. Confirm proxy containers are operational.

```
podman ps
```

All expected proxy containers should be up and running:

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

4.2.1.3.3. Migration complete

プロキシホストシステムは現在、更新された SUSE Multi-Linux Manager 5.1プロキシパッケージと、同期された製品チャンネルを備えたSUSE Linux Enterprise Server 15 SP7を実行しています。

4.2.2. Proxy Migration from 4.3 to 5.1

4.2.2.1. Requirements and considerations

- To migrate a SUSE Manager 4.3 Proxy to SUSE Multi-Linux Manager 5.1, you require a new machine with SL Micro 6.1 or SUSE Linux Enterprise Server 15 SP7 and **mgrpky** installed.
- An in-place migration from SUSE Manager 4.3 to 5.1 is not supported, regardless of whether the chosen host operating system is SL Micro 6.1 or SUSE Linux Enterprise Server 15 SP7.

Before migrating from SUSE Manager 4.3 to 5.1, any existing traditional clients including the traditional proxies must be migrated to Salt. For more information about migrating traditional SUSE Multi-Linux 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>.

- 従来の接続プロトコルは、SUSE Multi-Linux Manager 5.0以降ではサポートされなくなりました。

Before migrating a SUSE Manager 4.3 Proxy to SUSE Multi-Linux Manager 5.1, the SUSE Manager 4.3 Server needs to be migrated first, see **Installation-and-upgrade › Container-deployment**.

4.2.2.2. 概要

In SUSE Multi-Linux Manager 4.3, the proxy can be deployed using three different methods:

- RPM based
- containerized running on Podman
- containerized running on k3s

In SUSE Multi-Linux Manager 5.1, RPM based support was removed, and only the containerized version running with podman or k3s is supported. Furthermore, the management of the containerized proxy running with Podman was re-designed and made simpler with the **mgrpky** tool.

4.2.2.3. Deploy a new SUSE Multi-Linux Manager 5.1 proxy

Because an in-place migration is not supported, a deployment of a new SUSE Multi-Linux Manager proxy with a new FQDN is required. For more information on deploying a new proxy on SL Micro 6.1 or SUSE Linux Enterprise Server 15 SP7 see **Installation-and-upgrade › Install-proxy**.

4.2.2.4. Migrate clients to the new proxy



Before migrating the clients, ensure that the new SUSE Multi-Linux Manager 5.1 Proxy is already deployed and fully functional.

Procedure: Migrating clients from the old to the new proxy

1. SUSE Multi-Linux 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。

選択したすべてのクライアントが新しいプロキシに移行されます。スケジュールの進行状況をチェックして、すべてのクライアントが正常に移行されたかどうかを確認できます。

After a few minutes, the clients will start to show the new connection path. When all clients have the


connection path under the new proxy, the old SUSE Manager 4.3 Proxy system is not needed anymore and can be removed.

4.2.2.5. TFTPファイルの同期

コンテナ化されたプロキシは、tftprootファイルの転送にtftpsyncメカニズムを使用しません。代わりにこれらのファイルは、要求に応じて透過的にダウンロードされキャッシュされます。

cobbler syncの実行中の誤検知エラーを防ぐため、移行された4.3プロキシをtftpsyncメカニズムから削除する必要があります。

以前にTFTPファイルを受信するように4.3プロキシを設定していた場合は、以下の設定オプションのいずれかが必要です。

 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
```

In the SUSE Multi-Linux Manager 5.1 server container, run **configure-tftpsync.sh** with the list of remaining 4.3 proxies as arguments. If no 4.3 proxies remain, run **configure-tftpsync.sh** with no arguments.

In the SUSE Multi-Linux Manager 5.1 server container, manually remove the relevant proxy from the **proxies** setting in the **/etc/cobbler/settings.yaml** file. If there are no 4.3 proxies remaining, then manually remove the **proxies** list completely.

4.2.3. SUSE Multi-Linux Managerプロキシのアップグレード

Before running the upgrade command, it is required to update the host operating system. Updating the host operating system will also result in the update of the SUSE Multi-Linux Manager tooling such as the **mgrpxy** tool.

Procedure: Upgrading Proxy

1. **zypper**を使用してソフトウェアリポジトリを更新します。

```
zypper ref
```

2. ホストオペレーティングシステムに応じて、以下のステップに進みます。

SL Microなどのトランザクションシステムの場合:

1. **transactional-update**を使用して利用可能な更新を適用します。

```
transactional-update
```

2. 更新が適用されたら、**reboot**を実行して再起動します。

SUSE Linux Enterprise Serverの場合:

zypperを使用してインストールされたソフトウェアを更新します。

```
zypper up
```

3. **podman**上で実行されるSUSE Multi-Linux Manager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。

```
mgrpky upgrade podman
```



または、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。

```
mgrpky upgrade kubernetes
```

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

```
podman image prune -a
```

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

-  特定のバージョンにアップグレードする際に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。
- 通常の状況下では、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**mgrpky upgrade podman**コマンドを実行します。

4.3. クライアント

4.3.1. 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 Multi-Linux 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 5. 基本的なサーバとプロキシの管理

5.1. 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 Multi-Linux 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。

5.2. コンテナの起動と停止

次のコマンドを使用して、SUSE Multi-Linux Manager 5.1サーバコンテナを再起動、起動、および停止できます。

SUSE Multi-Linux Manager 5.1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
```

5.3. SUSE Multi-Linux Managerで使用されるコンテナ

以下は、SUSE Multi-Linux Manager 5.1で使用されるコンテナのリストです。

表 14. サーバコンテナ

コンテナ名	説明
uyuni-server	主な製品コンテナ
uyuni-db	製品のデータベースコンテナ
uyuni-hub-xmlrpc	ハブ配備用のXML-RPCゲートウェイ
uyuni-server-attestation	サーバCOCO認証

コンテナ名	説明
uyuni-saline	Salt 可観測性のためのSalineコンテナ
uyuni-server-migration	移行ヘルパーコンテナ

表 15. プロキシコンテナ

コンテナ名	説明
uyuni-proxy-httpd	すべてのHTTP通信を処理する主なプロキシコンテナ
uyuni-proxy-squid	Squidキャッシュ
uyuni-proxy-salt-broker	Saltフォワーダ
uyuni-proxy-ssh	SSHフォワーダ
uyuni-proxy-tftpd	TFTPDからHTTPへのトランスレータおよびフォワーダ

5.4. 永続コンテナボリューム

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 Multi-Linux Manager 5.1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。

5.4.1. サーバ

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

表 16. 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	/var/lib/containers/storage/volumes/

表 17. 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	/root

表 18. 永続ボリューム: var/

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

表 19. 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	/srv/salt
srv-www	/srv/www/
srv-tftpboot	/srv/tftpboot
srv-formulametadata	/srv/formula_metadata
srv-pillar	/srv/pillar
srv-susemanager	/srv/susemanager
srv-spacewalk	/srv/spacewalk

表 20. 永続ボリューム: etc/

Volume Name	Volume Directory
etc-apache2	/etc/apache2
etc-rhn	/etc/rhn
etc-systemd-multi	/etc/systemd/system/multi-user.target.wants
etc-systemd-sockets	/etc/systemd/system/sockets.target.wants
etc-salt	/etc/salt
etc-sssd	/etc/sssd
etc-tomcat	/etc/tomcat
etc-cobbler	/etc/cobbler
etc-sysconfig	/etc/sysconfig
etc-postfix	/etc/postfix

Volume Name	Volume Directory
ca-cert	/etc/pki/trust/anchors

表 21. Persistent Volumes: run/

Volume Name	Volume Directory
run-salt-master	/run/salt/master

5.4.2. プロキシ

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

表 22. 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	/var/lib/containers/storage/volumes/

表 23. 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
uyuni-proxy-tftpboot	/srv/tftpboot

表 24. 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
uyuni-proxy-rhn-cache	/var/cache/rhn
uyuni-proxy-squid-cache	/var/cache/squid

5.5. mgr-storage-serverおよびmgr-storage-proxyについて

mgr-storage-serverおよび**mgr-storage-proxy**は、SUSE Multi-Linux Manager 5.0以降で提供されるヘルパースクリプトです。

これらはSUSE Multi-Linux Managerサーバおよびプロキシのストレージを設定するように設計されています。

スクリプトはディスクデバイスを引数として受け取ります。**mgr-storage-proxy**にはストレージディスクデバイス用の引数が1つ必要です。**mgr-storage-server**にはストレージディスクデバイスが必要であり、オプションで専用データベースディスクデバイス用の2番目の引数を受け取ることができます。通常のストレージとデータベースストレージは同一ディスク上に配置可能ですが、パフォーマンスの向上と管理の容易性を確保するため、データベースは専用の高性能ディスクに配置することをお勧めします。

5.5.1. これらのツールの機能

mgr-storage-serverと**mgr-storage-proxy**の両方が標準のストレージセットアップ操作を実行します。

- 提供されたストレージデバイスを検証します。
- デバイスが空で使用に適していることを確認します。
- 指定されたデバイス上にXFSファイルシステムを作成します。
- データ移行のためデバイスを一時的にマウントします。
- 関連するストレージディレクトリを新しいデバイスに移動します。
- ブート時にストレージが自動的にマウントされるように、**/etc/fstab**にエントリを作成します。
- デバイスを最終的な場所で再マウントします。

表 25. 追加のツール固有の動作

mgr-storage-server	<ul style="list-style-type: none"> • オプションでデータベースストレージ用の個別のデバイスをサポートします。 • 移行中にSUSE Managerサービスを停止し、その後再起動します。Podmanボリュームディレクトリ/var/lib/containers/storage/volumesを準備済みストレージに移動し、オプションで/var/lib/containers/storage/volumes/var-pgsqlを準備済みデータベースストレージに移動します。
mgr-storage-proxy	<ul style="list-style-type: none"> • プロキシストレージのみに焦点を当てます(データベースストレージはサポートしていません)。 • 移行中にプロキシサービスを停止し、再起動します。 • podmanボリュームディレクトリ/var/lib/containers/storage/volumesを準備済みストレージに移動します。



どちらのツールも標準的なLinuxストレージ操作を自動化します。Linux管理者が手動で行う範囲を超えた、隠れたロジックやカスタムロジックはありません。

5.5.2. これらのツールが実行*しない*こと

- LVMボリュームを作成または管理*しません*。
- RAIDや複雑なストレージトポロジを設定*しません*。
- セットアップ後に通常のLinuxツールを使用したストレージの管理を妨げる*ことはありません*。
- 動的なサイズ変更や拡張機能は提供*しません*。これらは標準的なLinuxストレージツールで処理する必要があります。

5.5.3. インストール後のストレージ管理

ストレージが設定されると、標準的なLinuxコマンドを使用して安全に管理できます。

5.5.3.1. 例

リスト 1. 例1: LVMを使用する場合のストレージの拡張

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

例2: 大容量ディスクへの移行

1. 新規ディスクを追加してフォーマットします。
2. 一時的にマウントします。
3. `rsync`を使用してデータをコピーします。
4. `/etc/fstab`を更新します。
5. 正しい場所に再マウントします。

5.5.4. 使用する場合、使用しない場合



ストレージセットアップに変更を行う前に、必ずバックアップを取ってください。

- これらのツールは初期ストレージセットアップ中、またはツールがデータ移行と`/etc/fstab`の更新を処理することが想定される新しいストレージへの移行時に*のみ*使用します。
- ストレージのサイズ変更や拡張のためにこれらのスクリプトを再実行*しない*でください。このような操作には標準的なLinuxツール(**lvextend**、**xfs_growfs**など)を使用してください。

5.5.5. 概要

mgr-storage-serverおよび**mgr-storage-proxy**は、標準的なLinuxストレージ手法を使用して、SUSE Multi-Linux Managerコンポーネントの初期永続化ストレージセットアップを自動化するのに役立ちます。これらは、その後の標準的なストレージ管理を制限したり妨げたりすることはありません。

セットアップ後は、使い慣れたLinuxツールを使用してストレージの管理を続行してください。



データベースボリュームがいっぱいになると、システム動作に重大な問題を引き起こす可能性があります。ディスク使用量の通知はまだコンテナ化された環境には適応されていないため、ユーザはPodmanボリューム自体で使用するディスク容量を、GrafanaやPrometheusなどのツールまたは他の好ましい方法で監視することをお勧めします。**/var/lib/containers/storage/volumes/**の下にあるvar-pgsqlボリュームに特に注意してください。

Chapter 6. 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".