SUSE Multi-Linux Manager 5.1

管理者ガイド

Chapter 1. 序文

Administration Guide | SUSE Multi-Linux Manager 5.1

このガイドでは、SUSE Multi-Linux Managerサーバの保守、監視、カスタマイズなどの管理タスクについて説明します。

発行日: 2025-12-12

目次

Chapter 2. アクション

クライアントに対するアクションは、さまざまな方法で管理することができます。

- 自動化された定期的なアクションをスケジュールして、指定されたスケジュールでクライアントにhighstateまたは任意のカスタム状態のセットを適用できます。
- 個々のクライアント、システムグループ内のすべてのクライアント、または組織全体に定期的なアクションを適用できます。
- 動作チェーンを作成することにより、特定の順序で実行されるアクションを設定できます。
  - 動作チェーンは事前に作成および編集でき、適切な時間に実行するようにスケジュールできます。
- You can also perform remote commands on one or more of your clients.
  - Remote commands allows you to issue commands to individual clients, or to all clients that match a search term.

2.1. 定期的なアクション

You can apply recurring actions on individual clients, to a system group, or to all clients in an organization.

現在、SUSE Multi-Linux Managerは、次のアクションタイプを定期的なアクションとしてサポートしています。

- **Highstate:** highstateを実行します。
- **カスタム状態:** カスタム状態のセットを実行します。カスタム状態には、SUSE Multi-Linux Managerによって提供される内部状態、またはユーザによって作成された設定チャンネルのいずれかを指定できます。

設定チャンネルの詳細については、**Client-configuration › Configuration-management**を参照してください。

プロシージャ: 新しい定期的なアクションを作成する

1. 個々のクライアントに定期的なアクションを適用するには、［**システム**］に移動し、クライアントをクリックしてスケジュールを設定し、［**定期的なアクション**］タブに移動します。
2. システムグループに定期的なアクションを適用するには、**システム › システムグループ**に移動し、スケジュールを設定するグループを選択して、［**定期的なアクション**］タブに移動します。
3. **[作成]**をクリックします。
4. ［**動作タイプ**］ドロップダウンから動作タイプを選択します。
5. 新しいスケジュールの名前を入力します。
6. 定期的なアクションの頻度を選択します。
   - **毎時:** 各時間の分を入力します。 たとえば、**15**は毎時15分にアクションを実行します。

- **毎日:** 毎日の時間を選択します。 たとえば、**01:00**は、SUSE Multi-Linux Managerサーバのタイムゾーンで、毎日0100にアクションを実行します。
- **毎週:** 指定した時刻に毎週アクションを実行する曜日と時刻を選択します。
- **毎月:** 指定した時刻に毎月アクションを実行する日付と時刻を選択します。
- **独自のクォーツ書式:** 詳細オプションについては、独自のクォーツ文字列を入力します。 たとえば、毎月毎週土曜日の0215に定期的なアクションを実行するには、次のように入力します。

```
0 15 2 ? * 7
```

7. オプション: ［**テストモード**］スイッチを オンに切り替えて、テストモードでスケジュールを実行します。
8. **カスタム状態**タイプのアクションの場合は、利用可能な状態のリストから状態を選択し、**[変更点の保存]**をクリックします。これにより、現在の状態選択のみが保存され、スケジュールは保存されません。
9. 次のペインで、選択した状態をドラッグアンドドロップして実行順序に配置し、**[確認]**をクリックします。
10. **[スケジュールの作成]**をクリックして保存し、既存のスケジュールの完全なリストを表示します。

組織管理者は、組織内のすべてのクライアントに定期的なアクションを設定および編集できます。**ホーム › 組織 › 定期的なアクション**に移動して、組織全体に適用されるすべての定期的なアクションを表示します。

SUSE Multi-Linux Manager管理者は、すべての組織のすべてのクライアントの定期的なアクションを設定および編集できます。**管理 › 組織**に移動し、管理する組織を選択して、**状態 › 定期的なアクション**タブに移動します。

2.2. 動作チェーン

クライアントに対して多数の連続動作を実行する必要がある場合は、順序を確実に反映するための動作チェーンを作成できます。

デフォルトでは、ほとんどのクライアントはコマンドが発行されるとすぐに動作を実行します。 場合によっては、動作に時間がかかることがあります。これは、その後に実行された動作が失敗することを意味します。 たとえば、クライアントに再起動を指示してから2番目のコマンドを発行すると、再起動がまだ行われているため、2番目の動作が失敗する可能性があります。 アクションが正しい順序で実行されるようにするには、動作チェーンを使用します。

トランザクション更新システムの場合、動作チェーンは、再起動動作があるまで単一スナップショット内で実行されます。 これによりいくつかの制限が発生する可能性があります。

詳細については、**Client-configuration › Clients-slemicro**を参照してください。

動作チェーンは、すべてのクライアントで使用できます。動作チェーンには、次の動作を任意の数、任意の順序で含めることができます。

- **システムの詳細 › リモートコマンド**
- **システムの詳細 › システムの再起動をスケジュール**
- **システムの詳細 › 状態 › highstate**
- **システムの詳細 › ソフトウェア › パッケージ › 一覧表示/削除**
- **システムの詳細 › ソフトウェア › パッケージ › インストール**
- **システムの詳細 › ソフトウェア › パッケージ › アップグレード**
- **システムの詳細 › ソフトウェア › パッチ**
- **システムの詳細 › ソフトウェア › ソフトウェアチャンネル**
- **システムの詳細 › 設定**
- **イメージ › ビルド**

動作チェーンはユーザ固有です。 Web UIで動作チェーンを表示するには、動作チェーンを作成した同じユーザとしてサインインする必要があります。

プロシージャ: 新しい動作チェーンの作成

1. SUSE Multi-Linux Manager Web UIで、動作チェーンで実行する最初の動作に移動します。 たとえば、クライアントの［**システムの詳細**］に移動し、**[システムの再起動をスケジュール]**をクリックします。
2. ［**以下に追加**］フィールドをオンにし、追加する動作チェーンを選択します。
   - これが最初の動作チェーンの場合は、［**新しい動作チェーン**］を選択します。
   - 動作チェーンがすでに存在する場合は、リストから選択します。
   - 既存の動作チェーンがすでにあるが、新しい動作チェーンを作成する場合は、作成する新しい動作チェーンの名前の入力を開始します。
3. 動作を確認します。 動作はすぐには実行されず、新しい動作チェーンが作成され、これを確認する青いバーが画面の上部に表示されます。
4. ［**以下に追加**］フィールドをオンにし、追加する動作チェーンの名前を選択して、動作チェーンに動作の追加を続行します。
5. 動作を追加し終えたら、**スケジュール › 動作チェーン**に移動して、リストから動作チェーンを選択します。
6. 動作をドラッグして正しい位置にドロップすることで、動作の順序を変更します。 青いプラス記号をクリックして、動作が実行されるクライアントを表示します。 **[保存]**をクリックして、変更を保存します。
7. 実行する動作チェーンの時刻をスケジュールし、**[保存とスケジュール]**をクリックします。 **[保存]**または**[保存とスケジュール]**のいずれかをクリックせずにページを離れる場合、未保存の変更はすべて破棄されます。

動作チェーン内の1つの動作が失敗すると、動作チェーンが停止し、これ以上の動作は実行されません。

スケジュール › 待機中の動作に移動して、動作チェーンからスケジュール済みの動作を確認できます。

2.3. リモートコマンド

Use this procedure to run a remote command via Salt.

開始する前に、インストールされているオペレーティングシステムに適したツールの子チャンネルにクライアントがサブスクライブされていることを確認してください。 ソフトウェアチャンネルへのサブスクライブの詳細については、**Client-configuration › Channels**を参照してください。

- トランザクション更新システムの場合、リモートコマンドが単一スナップショット内で実行されることを考慮します。これによりいくつかの制限が発生する可能性があります。詳細については、**Client-configuration › Clients-slemicro**を参照してください。
- リモートコマンドはクライアントの**/tmp/**ディレクトリから実行されます。リモートコマンドが正確に機能するようにするには、**noexec**オプションを指定して**/tmp**をマウントしないでください 。詳細については、**Administration › Troubleshooting**を参照してください。
- ［**リモートコマンド**］ページから実行されるすべてのコマンドは、クライアント上でrootとして実行されます。 ワイルドカードを使用して、任意の数のシステムでコマンドを実行できます。 コマンドを発行する前に、必ず十分注意してコマンドを確認してください。

Procedure: Running Remote Commands on Clients

1. **Salt › リモートコマンド**に移動します。
2. 最初のフィールドで、@記号の前に、発行するコマンドを入力します。
3. 2番目のフィールドで、@記号の後に、コマンドを発行するクライアントを入力します。 個々のクライアントの**minion-id**を入力することも、ワイルドカードを使用してクライアントの範囲をターゲットにすることもできます。
4. **[ターゲットの検索]**をクリックして、ターゲットにしたクライアントを確認し、正しい詳細情報を使用していることを確認します。
5. **[コマンドの実行]**をクリックして、ターゲットクライアントにコマンドを発行します。

Chapter 3. Ansibleの統合

Ansible is a tool to manage computer client systems. For more information, see https://www.ansible.com.

SUSE Multi-Linux Manager supports managing Ansible control nodes. For more information, see administration:ansible-setup-control-node.pdf.

The supported version for the Ansible Control Node is Ansible 11.3. It should be obtained from the operating system vendor's official repositories. For example, on SUSE Linux Enterprise 15 SP6 and SP7, Ansible is available through the **Systems Management Module.** For Control Nodes running operating systems other than SUSE Linux Enterprise, use Ansible shipped together with that distribution.

Ansible software is also available for SUSE Multi-Linux Manager Proxy and SUSE Multi-Linux Manager for Retail Branch Server.

3.1. 機能の概要

SUSE Multi-Linux Managerでは、システム管理者がAnsible制御ノードを操作できます。 サポートされる機能は次のとおりです。

- インベントリファイルの検査
- playbookの検出
- playbookの実行

詳細情報:

- インベントリは、管理されたAnsibleノードのソートされたリストです。 インベントリの整理の詳細については、https://docs.ansible.com/ansible/latest/inventory_guide/intro_inventory.htmlを参照してください。
- playbookは、インベントリの管理方法を説明する方法です。 playbookの詳細については、https://docs.ansible.com/ansible/latest/playbook_guide/playbooks_intro.htmlを参照してください。

3.2. 要件と基本設定

To use Ansible features, you need to register the already existing Ansible Control Node to the SUSE Multi-Linux Manager Server. In the Web UI, on the **System Details › Properties** page of the registered system, you must enable the **Ansible Control Node** system type of the **Add-on System Types** list.

Ansible制御ノードシステムタイプを有効にすると、highstateに追加して**ansible**パッケージがシステムにインストールされ、**システムの詳細 › Ansible**タブでAnsible機能が有効になります。

次のステップとして、**システムの詳細 › Ansible › 制御ノード**ページでAnsible playbookディレクトリおよびインベントリファイルへのパスを設定します。 インベントリパスとして、標準のAnsibleインベントリパ

ス**/etc/ansible/hosts**を使用できます。 playbookディレクトリとして、playbookファイルが保存されている制御ノード上の任意のディレクトリを使用できます。 playbookディレクトリには、**.yml**ファイルが含まれているか、**.yml**ファイルを持つサブディレクトリが含まれています。

Ansible制御ノードのインストールと設定については、**Administration › Ansible-setup-control-node**を参照してください。

3.3. インベントリの検査

インベントリパスを定義した後、SUSE Multi-Linux Managerを使用してその内容を検査できます。

プロシージャ: Web UIからのインベントリの検査

1. SUSE Multi-Linux Manager Web UIで、**システムの詳細 › Ansible › インベントリ**に移動します
2. インベントリパスをクリックして、制御ノードのインベントリ検査をリアルタイムで実行します。

3.4. Playbookの検出

playbookディレクトリを定義した後で、**システムの詳細 › Ansible › playbook**ページでplaybookを検出できます。

インベントリの検査と同様に、playbookの検出操作は制御ノード上でリアルタイムに実行されます。

3.5. Playbookの実行

playbookの実行は、**システムの詳細 › Ansible › playbook**ページからスケジュールできます。 実行するplaybookを選択した後で、［**playbookの実行のスケジュール**］ダイアログの［**インベントリパス**］ドロップダウンメニューから実行するインベントリファイルを選択できます。 項目を選択しない場合は、制御ノードで設定されているデフォルトのインベントリが使用されます。 ドロップダウンメニューには、インベントリパスで定義したインベントリと、playbookディレクトリでローカルに検出されたインベントリが表示されます。 これらは、playbookの詳細に［**カスタムインベントリ**］項目として表示されます。 任意のインベントリパスを入力することもできます。

その後、playbookの実行時刻を選択するか、動作チェーンを選択します。 最終的に、SUSE Multi-Linux Managerは制御ノードで動作としてplaybookを実行します。 操作の結果は、動作の詳細ページに表示されます。

3.6. Ansible制御ノードのセットアップ

Ansible制御ノードをセットアップするには、SUSE Multi-Linux Manager Web UIから次のステップを実行します。

クライアントをAnsible制御ノードとして設定するには、そのシステムにAnsibleパッケージがインストールされている必要があります。 通常、Ansibleパッケージは、 オペレーティングシステムベンダの公式レポジトリから取得する必要があります。 たとえば、SUSE Linux Enterprise 15 SP6およびSP7では、Ansibleは、**Systems Management**

> **Module**から入手できます。

プロシージャ: SUSE Linux Enterprise 15 SP6またはSP7システムでのAnsible制御ノードのセットアップ

1. SUSE Multi-Linux Manager Web UIで、**管理 › セットアップウィザード › 製品**に移動し、**SUSE Linux Enterprise Server 15 SP6 x86_64** (以降)と**Systems Management Module**および必要な**Python 3 Module**が選択および同期されていることを確認します。
2. SUSE Linux Enterprise 15 SP6 (またはそれ以降)のクライアントを配備します。
3. SUSE Multi-Linux Manager Web UIで、クライアントの**システム › 概要**ページに移動します。 **ソフトウェア › ソフトウェアチャンネル**を選択し、クライアントを**SUSE Linux Enterprise Server 15 SP6 x86_64** (またはそれ以降のSP)、**Systems Management Module**、および**Python 3 Module**チャンネルにサブスクライブします。
4. クライアントの**詳細 › プロパティ**を選択します。 ［**付属エンタイトルメント**］リストで［**Ansible制御ノード**］を有効にして、**[プロパティの更新]**をクリックします。
5. クライアントの概要ページに移動し、**状態 › highstate**を選択して、**[highstateの適用]**をクリックします。
6. **イベント**タブを選択して、highstateの状態を確認します。

> SUSE Linux Enterprise 15 SP4またはSP5クライアントに新しいAnsibleをインストールする場合は、**Python 3 Module**を有効にする必要があります。

> Ansibleの新しいバージョンでは、古いPythonバージョンを搭載したノードの管理はサポートされなくなりました。 管理対象ノードが依然として古いPythonバージョンをデフォルトとして設定している場合、playbookの実行中に接続エラーや障害が発生する可能性があります。 これに対処するには、可能であれば管理対象ノードのPythonをアップグレードし、Ansibleのインベントリまたは設定で正しいPythonインタープリタを設定する必要があります。

3.6.1. Ansibleインベントリファイルの作成

Ansible統合ツールは、playbookをインベントリファイルとして配備します。 _Table 1_に一覧表示されている個々のオペレーティングシステムごとに1つのインベントリファイルを作成します。

プロシージャ: Ansibleインベントリファイルの作成

1. Ansibleが管理するインベントリファイルにホストを作成して追加します。 Ansibleインベントリのデフォルトパスは、**/etc/ansible/hosts**です。

リスト 1. インベントリの例

```
client240.mgr.example.org
client241.mgr.example.org
client242.mgr.example.org
client243.mgr.example.org ansible_ssh_private_key_file=/etc/ansible/some_ssh_key

[mygroup1]
```

```
client241.mgr.example.org
client242.mgr.example.org

[mygroup2]
client243.mgr.example.org

[all:vars]
ansible_ssh_private_key_file=/etc/ansible/my_ansible_private_key
```

2. SUSE Multi-Linux Manager Web UIで、［**Ansible**］タブから**Ansible › 制御ノード**に移動して、制御ノードにインベントリファイルを追加します。
3. ［**playbookディレクトリ**］セクションで、［**Add a Playbook Directories**］（playbookディレクトリの追加）フィールドに**/usr/share/scap-security-guide/ansible**を追加し、**[保存]**をクリックします。
4. ［**インベントリファイル**］の下の［**インベントリファイルの追加**］フィールドにインベントリファイルの場所を追加し、**[保存]**をクリックします。

リスト 2. 例

```
/etc/ansible/sles15
/etc/ansible/sles12
/etc/ansible/centos7
```

その他のplaybookの例については、https://github.com/ansible/ansible-examplesを参照してください。

3.6.2. Ansibleノードとの通信の確立

プロシージャ: Ansibleノードとの通信の確立

1. インベントリで使用しているSSHキーを作成します。

```
ssh-keygen -f /etc/ansible/my_ansible_private_key
```

2. 生成されたSSHキーをAnsible管理対象クライアントにコピーします。 例:

```
ssh-copy-id -i /etc/ansible/my_ansible_private_key root@client240.mgr.example.org
```

3. 次のように**/etc/ansible/ansible.cfg**で機密鍵を宣言します。

```
private_key_file = /etc/ansible/my_ansible_private_key
```

my_ansible_private_keyを、機密鍵を含むファイルの名前に置き換えます。

4. 制御ノードから次のコマンドを実行して、Ansibleが動作していることをテストします。

```
ansible all -m ping
ansible mygroup1 -m ping
```

```
ansible client240.mgr.example.org -m ping
```

これで修復を実行できます。詳細については、ansible-compliance-as-code.pdfを参照してください。

3.7. コードとしてのコンプライアンス

このドキュメントでは、Ansible　playbookを使用して、コード修復としてコンプライアンスを実行する方法について説明します。

bashスクリプトを使用してコード修復としてコンプライアンスを実行する方法の詳細については、修復を参照してください。

修復を実行するには、Ansible制御ノードにSCAPセキュリティガイドパッケージをインストールする必要があります。

プロシージャ: SCAPセキュリティガイドパッケージのインストール

1. **システム › 概要**から、クライアントを選択します。 次に、**ソフトウェア › パッケージ › インストール**をクリックします。
2. **scap-security-guide**を検索し、ご使用のシステムに適したパッケージをインストールします。　パッケージ配布の要件については、次の表を参照してください。

表 1. SCAPセキュリティガイドパッケージの要件

パッケージ名	サポートされているシステム
scap-security-guide	openSUSE、SLES12、SLES15
scap-security-guide-redhat	CentOS 7、CentOS 8、Fedora、Oracle Linux 7、Oracle Linux 8、RHEL7、RHEL8、RHEL9、Red Hat OpenStack Platform 10、Red Hat OpenStack Platform 13、Red Hat Virtualization 4、Scientific Linux
scap-security-guide-debian	Debian 12
scap-security-guide-ubuntu	Ubuntu 20.04、Ubuntu 22.04

3.7.1. Ansible Playbookを使用した修復

Ansible制御ノードが必要です。 詳細については、**Administration › Ansible-setup-control-node**を参照してください。

次のプロシージャでは、Ansible playbookを使用して修復を実行する方法について説明します。

プロシージャ: Ansible Playbookを使用して修復を実行する

1. 制御ノードのシステムメニューから、**Ansible › playbook**を選択し、playbookをクリックします。例:

```
sle15-playbook-stig.yml
```

2. playbookを実行するには、クライアントの［**インベントリパス**］を選択します。例:

```
/etc/ansible/sles15
```

[Schedule] をクリックします。

3. ［**イベント**］タブで、スケジュールされたイベントのステータスを確認します。

playbookが別のディレクトリにある場合は、［**Ansible制御ノードのセットアップ**］へのリンクをたどって、その追加方法を確認できます。

Chapter 4. 認証方法

SUSE Multi-Linux Managerは、いくつかの異なる認証方法をサポートしています。 このセクションでは、pluggable authentication modules (PAM)およびシングルサインオン(SSO)について説明します。

4.1. シングルサインオン(SSO)による認証

SUSE Multi-Linux Managerは、Security Assertion Markup Language (SAML) 2プロトコルを実装することで、シングルサインオン(SSO)をサポートしています。

シングルサインオンは、ユーザが1組の資格情報を使用して複数のアプリケーションにアクセスできるようにする認証プロセスです。 SAMLは、認証および許可データを交換するためのXMLベースの規格です。 SAML IDサービスプロバイダ(IdP)は、SUSE Multi-Linux Managerなどのサービスプロバイダ(SP)に認証および許可サービスを提供します。 SUSE Multi-Linux Managerは、シングルサインオンを有効にする必要がある3つのエンドポイントを公開します。

SUSE Multi-Linux ManagerのSSOは以下をサポートします。

- SSOを使用したログイン。
- サービスプロバイダが開始したシングルログアウト(SLO)、およびIDサービスプロバイダのシングルログアウトサービス(SLS)を使用してログアウトする。
- アサーションとnameIdの暗号化。
- アサーションの署名。
- AuthNRequest、LogoutRequest、およびLogoutResponderによるメッセージ署名。
- アサーションコンシューマサービスエンドポイントの有効化。
- シングル ログアウト サービス エンドポイントの有効化。
- SPメタデータ(署名可能)の発行。

SUSE Multi-Linux ManagerのSSOは以下をサポートしません。

- IDサービスプロバイダ(IdP)の製品の選択と実装。
- 他の製品のSAMLサポート(各製品のドキュメントで確認してください)。

SSOの実装例については、**Administration › Auth-methods-sso-example**を参照してください。

デフォルトの認証方法からシングルサインオンに変更する場合、新しいSSO資格情報はWeb UIにのみ適用されます。 **mgr-sync**や**spacecmd**などのクライアントツールは、引き続きデフォルトの認証方式でのみ動作します。

4.1.1. 前提条件

開始する前に、これらのパラメータを使用して外部IDサービスプロバイダを設定しておく必要があります。手順については、IdPのドキュメントを確認してください。

IdPユーザとSUSE Multi-Linux Managerユーザのマッピングは SAML:Attributeで指定します。SAML:AttributeはIdPで指定し、SAML認証時にSUSE Multi-Linux Managerに渡す必要があります。この属性には**uid**という名前を付け、ログイン後にマップされたSUSE Multi-Linux Managerユーザを含める必要があります。シングルサインオンを有効にする前に、SUSE Multi-Linux Managerが作成されている必要があります。

以下のエンドポイントが必要です。

- アサーションコンシューマサービス(ACS): SAMLメッセージを受け入れてサービスプロバイダへのセッションを確立するエンドポイント。 SUSE Multi-Linux ManagerのACSのエンドポイントはhttps://server.example.com/rhn/manager/sso/acsです
- シングルログアウトサービス(SLS): IdPからログアウト要求を開始するエンドポイント。 SUSE Multi-Linux ManagerのSLSのエンドポイントはhttps://server.example.com/rhn/manager/sso/slsです
- メタデータ: SAMLのSUSE Multi-Linux Managerメタデータを取得するエンドポイント。 SUSE Multi-Linux Managerのメタデータのエンドポイントはhttps://server.example.com/rhn/manager/sso/metadataです

ユーザ**orgadmin**を使用したIdPによる認証が成功した後で、**orgadmin**ユーザがSUSE Multi-Linux Managerに存在する場合は、**orgadmin**ユーザとしてSUSE Multi-Linux Managerにログインします。

4.1.2. SSOの有効化

SSOの使用は、他のタイプの認証と相互に排他的であり、有効か無効のいずれかです。SSOはデフォルトで無効になっています。

サーバコンテナでステップを実行する前に、**mgrctl term**を使用します。

プロシージャ: SSOの有効化

1. ユーザがまだSUSE Multi-Linux Managerに存在しない場合は、まず作成してください。
2. **/etc/rhn/rhn.conf**を編集して、次の行をファイルの最後に追加します。

```
java.sso = true
```

3. **/usr/share/rhn/config-defaults/rhn_java_sso.conf**で、カスタマイズするパラメータを見つけます。カスタマイズするパラメータを**/etc/rhn/rhn.conf**に挿入し、それらのパラメータの前に**java.sso**を付けます。 たとえば、**/usr/share/rhn/config-defaults/rhn_java_sso.conf**で以下を見つけます。

```
onelogin.saml2.sp.assertion_consumer_service.url = https://YOUR-PRODUCT-HOSTNAME-OR-
IP/rhn/manager/sso/acs
```

カスタマイズするには、オプション名の前に**java.sso.**を付けて、対応するオプションを**/etc/rhn/rhn.conf**に作成します。

```
java.sso.onelogin.saml2.sp.assertion_consumer_service.url = https://YOUR-PRODUCT-
```

```
HOSTNAME-OR-IP/rhn/manager/sso/acs
```

変更する必要があるすべての出現を見つけるには、プレースホルダ**YOUR-PRODUCT**および**YOUR-IDP-ENTITY**をファイル内で検索します。 すべてのパラメータには、その意味についての簡単な説明が含まれています。

4. spacewalkサービスを再起動して変更を取得します。

```
mgradm restart
```

SUSE Multi-Linux ManagerのURLにアクセスすると、認証を要求されたSSO用IdPにリダイレクトされます。認証に成功すると、SUSE Multi-Linux Manager Web UIにリダイレクトされ、認証されたユーザとしてログインします。 SSOを使用したログインで問題が発生した場合は、SUSE Multi-Linux Managerのログで詳細情報を確認してください。

4.1.3. SSOの実装例

この例では、3つのエンドポイントをSUSE Multi-Linux Managerで公開し、Keycloak 21.0.1以降をIDサービスプロバイダ(IdP)として使用することによってSSOが実装されています。

まずKeycloak IdPをインストールしてから、SUSE Multi-Linux Managerサーバを設定します。 次に、エンドポイントをKeycloakクライアントとして追加し、ユーザを作成できます。

この例は、説明のみを目的としています。 SUSEは、サードパーティのIDサービスプロバイダを推奨またはサポートしておらず、Keycloakとは提携していません。 Keycloakのサポートについては、https://www.keycloak.org/を参照してください。

Keycloakは、マシンに直接インストールすることも、コンテナ内で実行することもできます。 この例では、PodmanコンテナでKeycloakを実行します。 Keycloakのインストールの詳細については、https://www.keycloak.org/guides#getting-startedにあるKeycloakのドキュメントを参照してください。

プロシージャ: IDサービスプロバイダの設定

1. Keycloakのドキュメントに従って、PodmanコンテナにKeycloakをインストールします。
2. **-td**引数を使用してコンテナを実行し、プロセスが実行されたままになっていることを確認します。

```
podman run -td --name keycloak -p 8080:8080 -e KEYCLOAK_USER=admin -e
KEYCLOAK_PASSWORD=admin quay.io/keycloak/keycloak:21.0.1
```

3. Keycloak Web UIに**admin**ユーザとしてサインインし、次の詳細情報を使用して認証レルムを作成します。
   - ［**名前**］フィールドに、レルムの名前を入力します。 たとえば、**MLM**。
   - ［**エンドポイント**］フィールドで、［**SAML 2.0 Identity Provider Metadata**］リンクをクリックします。 これにより、SUSE Multi-Linux Manager設定ファイルにコピーするエンドポイントと証明書が表示されるページに移動します。

Keycloakをインストールしてレルムを作成したら、SUSE Multi-Linux Managerサーバを準備できます。

プロシージャ: SUSE Multi-Linux Managerサーバの設定

1. SUSE Multi-Linux Managerサーバで、**/etc/rhn/rhn.conf**設定ファイルを開き、これらのパラメータを編集します。 **<FQDN_MLM>**をSUSE Multi-Linux Managerのインストールの完全修飾ドメイン名に置き換えます。

```
java.sso.onelogin.saml2.sp.entityid                       =
https://<FQDN_MLM>/rhn/manager/sso/metadata
java.sso.onelogin.saml2.sp.assertion_consumer_service.url =
https://<FQDN_MLM>/rhn/manager/sso/acs
java.sso.onelogin.saml2.sp.single_logout_service.url      =
https://<FQDN_MLM>/rhn/manager/sso/sls
```

2. 設定ファイルで、**<FQDN>**をKeycloakサーバの完全修飾ドメイン名に置き換えます。 **<REALM>**を認証レルム に置き換えます。たとえば**MLM**。

```
java.sso.onelogin.saml2.idp.entityid                   =
http://<FQDN_IDP>:8080/realms/<REALM>
java.sso.onelogin.saml2.idp.single_sign_on_service.url =
http://<FQDN_IDP>:8080/realms/<REALM>/protocol/saml
java.sso.onelogin.saml2.idp.single_logout_service.url  =
http://<FQDN_IDP>:8080/realms/<REALM>/protocol/saml
```

3. IdPメタデータで、パブリックx509証明書を探します。 これには http://<FQDN_IDP>:8080/realms/<REALM>/protocol/saml/descriptorの形式が使用されます。 設定ファイルで、IdPのパブリックx509証明書を指定します。

```
java.sso.onelogin.saml2.idp.x509cert = -----BEGIN CERTIFICATE----- <CERTIFICATE>
-----END CERTIFICATE-----
```

以下は、SSOを有効にした後のSUSE Multi-Linux Managerの**rhn.conf**の例です。

```
java.sso = true


# This is the configuration file for Single Sign-On (SSO) via SAMLv2 protocol
# To enable SSO, set java.sso = true in /etc/rhn/rhn.conf
#
# Mandatory changes: search this file for:
# - YOUR-PRODUCT
# - YOUR-IDP-ENTITY
#
# See product documentation and the comments inline in this file for more
# information about every parameter.
#
#
#
#
# If 'strict' is True, then the Java Toolkit will reject unsigned
# or unencrypted messages if it expects them signed or encrypted
# Also will reject the messages if not strictly follow the SAML
#
```

```
# WARNING: In production, this parameter setting parameter MUST be set as "true".
# Otherwise your environment is not secure and will be exposed to attacks.
# Enable debug mode (to print errors)
# Identifier of the SP entity (must be a URI)
java.sso.onelogin.saml2.sp.entityid =
https://MLMserver.example.org/rhn/manager/sso/metadata

# Specifies info about where and how the <AuthnResponse> message MUST be
# returned to the requester, in this case our SP.
# URL Location where the <Response> from the IdP will be returned
java.sso.onelogin.saml2.sp.assertion_consumer_service.url =
https://MLMserver.example.org/rhn/manager/sso/acs

# Specifies info about where and how the <Logout Response> message MUST be
# returned to the requester, in this case our SP.
java.sso.onelogin.saml2.sp.single_logout_service.url =
https://MLMserver.example.org/rhn/manager/sso/sls

# Identifier of the IdP entity (must be a URI)
java.sso.onelogin.saml2.idp.entityid = http://idp.example.org:8080/realms/MLM

# SSO endpoint info of the IdP. (Authentication Request protocol)
# URL Target of the IdP where the SP will send the Authentication Request Message
java.sso.onelogin.saml2.idp.single_sign_on_service.url =
http://idp.example.org:8080/realms/MLM/protocol/saml

# SLO endpoint info of the IdP.
# URL Location of the IdP where the SP will send the SLO Request
java.sso.onelogin.saml2.idp.single_logout_service.url =
http://idp.example.org:8080/realms/MLM/protocol/saml

# Public x509 certificate of the IdP
java.sso.onelogin.saml2.idp.x509cert = -----BEGIN CERTIFICATE-----
MIIClzCCAX8CBgGC+tPbVjANBgkqhkiG9w0BAQsFADAPMQ0wCwYDVQQDDARTVU1BMB4XDTIyMDkwMTIwNTEwNFoXDT
MyMDkwMTIwNTI0NFowDzENMAsG
A1UEAwwEU1VNQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMNSWJAalB5mShTkMBO5mrsOosyheEL8/A
37WvuqDPwwEfm4x0cG7gmMHvONxYXZk+LRyzoQl2sBrNFrbMuwu5dnah5ZSMxQyUu697S280m4vIiegGaFdbgH+g4F
GBu
eSis1ssMzTcES+NUuI7pLkMLNmSQtncESnoL9q2SyeQSwYtr5dz1ydl6IzjwtaWeyQ9EGJNtJtLk3U4+arLPCpHAwq
FAnLO9NeYcRDNUKhNBs1v5mHP+L066PZu1/DkE0mSgy/+qXaS0CgZVKqz8qB+bvHVuAq9W60g1CjqZKbwvPu72p/7+
d8z
9DxXPIZ1uxdqn19q/kLEP2TYLtgQobSHECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAga+raLMJDo/P/yN1Z6SGGocK
227WFqovBiE/mLYlp5Ff0+0jS1US1plSppJ94xOr8j0m7HW0Wu5xCz6oOhzXTEtnfIbeRyr1Rms3BWdxyXgQ9bWUeZ
MWZ
HfDkTbhgRRmjDEwSSfEXRKQNvw41CpnlB36I0++ejgGnjDvH7BbkCaoW55JF5j6DT/WYR0n7MkEl2Ova9CH0e9X7Gn
y8iOAg26oziy06uy3P/lx9Z9RmHnvpvN/Q34SGEq9z/HlQVuP12UPj//iT21Jc17OOZFsZQXlGFTG6bXKmO42W8FdU
DJU
ONoXZgjMb3eC7U691YyeowoqTY7mJKxNPprYY/lL0w== -----END CERTIFICATE-----


# Organization
java.sso.onelogin.saml2.organization.name = SUSE Manager admin
java.sso.onelogin.saml2.organization.displayname = SUSE Manager admin
java.sso.onelogin.saml2.organization.url = https://MLMserver.example.org
java.sso.onelogin.saml2.organization.lang =

# Contacts
java.sso.onelogin.saml2.contacts.technical.given_name = SUSE Manager admin
java.sso.onelogin.saml2.contacts.technical.email_address = MLM@example.org
java.sso.onelogin.saml2.contacts.support.given_name = SUSE Manager admin
java.sso.onelogin.saml2.contacts.support.email_address = MLM@example.org
```

SUSE Multi-Linux Manager エンドポイントをKeycloakに追加できます。 Keycloakはエンドポイントをクラ

イアントと呼びます。

プロシージャ: エンドポイントをクライアントとして追加する

1. Keycloak Web UIで、これらの詳細を使用して新しいクライアントを作成します。
   - ［**Client type**］（クライアントタイプ）フィールドで、［**SAML**］を選択します。
   - ［**クライアントID** ］フィールドに、サーバ設定ファイルで指定されているエンドポイントを**java.sso.onelogin.saml2.idp.entityid**として入力します。 たとえば、https://<FQDN_MLM>/rhn/manager/sso/metadata。
2. ［設定］タブで、これらの詳細を使用してクライアントを微調整します。
   - ［**Sign assertions**］（アサーションに署名する）を［**オン**］に切り替えます。
   - ［**Signature algorithm**］（署名アルゴリズム）フィールドで、［**RSA_SHA1**］を選択します。
   - ［**SAML Signature Key Name**］（SAML署名キー名）フィールドで、［**Key ID**］（キーID）を選択します。
3. ［**キー**］タブで次の操作を行います。
   - ［**Client signature required**］（クライアントの署名が必要）を［**オフ**］に設定します。
4. ［**Advanced**］（詳細）タブの［**Fine Grain SAML Endpoint Configuration**］セクションで、これらの詳細を使用して2つのエンドポイントを追加します。
   - ［**Assertion Consumer Service**］（アサーションコンシューマサービス）フィールドの両方にサーバ設定ファイルで指定されているエンドポイントを**java.sso.onelogin.saml2.sp.assertion_consumer_service.url**として入力します。 たとえば、https://<FQDN_MLM>/rhn/manager/sso/acs。
   - ［**Logout Service**］（ログアウトサービス）フィールドの両方に、サーバ設定ファイルで指定されているエンドポイントを**java.sso.onelogin.saml2.sp.single_logout_service.url**として入力します。 たとえば、https://<FQDN_MLM>/rhn/manager/sso/sls。

エンドポイントをクライアントとして追加したら、クライアントスコープを設定し、KeycloakとSUSE Multi-Linux Managerの間でユーザをマッピングできます。

プロシージャ: クライアントスコープとマッパーを設定する

1. Keycloak Web UIで、**クライアント › Client scopes**（クライアントスコープ）タブに移動し、デフォルトのクライアントスコープとして**role_list**を割り当てます。
2. **Client_scopes › Mappers** （マッパー）タブに移動して、ユーザ属性**uid**のマッパーをデフォルトの値を使用して追加します。 このSAML属性はSUSE Multi-Linux Managerによって想定されています。
3. **Client_scopes › Mappers**（マッパー）に移動し、［**role_list**］ マッパーをクリックします。［**Single Role Attribute**］（単一役割属性）を［**オン**］に設定します。
4. **ユーザ › 管理**セクションに移動し、管理ユーザを作成します。 このユーザは、SUSE Multi-Linux Manager管理ユーザに一致する必要はありません。
5. **ユーザ › Role mappings** （ロールマッピング）タブに移動して、SUSE Multi-Linux Manager管理ユー

ザのユーザ名に一致する値を持つ**uid**属性を追加します。

6. **ユーザ › 資格情報**タブに移動して、SUSE Multi-Linux Manager管理ユーザによって使用されるのと同じパスワードを設定します。 . 変更を保存します。

設定が完了したら、インストールが期待どおりに動作していることをテストできます。 SUSE Multi-Linux Managerサーバを再起動して変更を取得し、SUSE Multi-Linux Manager Web UIに移動します。 インストールが正常に動作している場合は、Keycloak SSOページにリダイレクトされ、ここでは正常に認証できます。

4.2. PAMによる認証

SUSE Multi-Linux Managerは、SSSDを用いることで、pluggable authentication modules (PAM)を使用したネットワークベースの認証システムをサポートしています。 PAM は、SUSE Multi-Linux Managerを集中認証メカニズムと統合できるようにする一連のライブラリであり、複数のパスワードを覚える必要がなくなります。 SUSE Multi-Linux Managerは、LDAP、Kerberos、およびその他のネットワークベースの認証プロトコルをサポートしています。

4.2.1. SSSDの設定

プロシージャ: SSSDの設定

1. SUSE Multi-Linux Manager Web UIで、**ユーザ › ユーザの作成**に移動し、新しいユーザまたは既存のユーザがPAMで認証されるようにします。

   ユーザ名では、英数字に加えて、-、 _、 .、@が許可されています。

2. ［**Pluggable Authentication Modules (PAM)**］チェックボックスをオンにします。
3. サーバコンテナでSSSDを設定します。 SUSE Multi-Linux Managerコンテナホストのコマンドプロンプトで、rootとしてサーバコンテナに入ります。

```
mgrctl term
```

4. コンテナ内で次の手順を実行します。
   a. 設定に従って**/etc/sssd/sssd.conf**を編集します。 例については、administration:auth-methods-pam.pdfを参照してください。
   b. 実行したら、コンテナを終了します。

```
exit
```

5. SUSE Multi-Linux Managerを再起動します。

```
mgradm restart
```

SUSE Multi-Linux Manager Web UIのパスワードを変更すると、SUSE Multi-Linux Managerサーバのローカルパスワードのみが変更されます。 PAMがそのユーザに対して

> 有効になっている場合、ローカルパスワードはまったく使用されない可能性があります。 たとえば、先に記載した例では、Kerberosパスワードは変更されません。 ネットワークサービスのパスワード変更メカニズムを使用して、これらのユーザのパスワードを変更します。

PAMの設定の詳細については、『SUSE Linux Enterprise Serverセキュリティガイド』を参照してください。『セキュリティガイド』には、他のネットワークベースの認証方法でも機能する一般的な例が含まれています。 また、Active Directory (AD)サービスを設定する方法についても説明しています。 詳細については、https://documentation.suse.com/sles/15-SP6/html/SLES-all/part-auth.htmlを参照してください。

4.2.1.1. LDAPとActive Directoryの統合例

Active DirectoryとのLDAP統合については、次の例を使用できます。

コードスニペットで、環境に応じて次のプレースホルダを変更します。

$domain

ドメイン名

$ad_server

$domain $uyuni-hostnameから自動検出されない場合は、ADサーバのFQDN: このADクライアントが認識されるはずのマシンの名前。 設定されていない場合は、**uyuni-server.mgr.internal**になります。

/etc/sssd/sssd.confのスニペットの例:

```
[sssd]
config_file_version = 2
services = nss, pam
domains = $domain

[nss]

[pam]

[domain/$domain]
id_provider = ad
chpass_provider = ad
access_provider = ad
auth_provider = ad

ad_domain = $domain
ad_server = $ad_server
ad_hostname = $uyuni-hostname

ad_gpo_map_network = +susemanager

krb5_keytab = FILE:/etc/rhn/krb5.conf.d/krb5.keytab
krb5_ccname_template = FILE:/tmp/krb5cc_%{uid}
```

Chapter 5. バックアップと復元

This chapter contains information on the files you need to back up. With the built-in backup and restore solution (**mgradm backup**) you create SUSE Multi-Linux Manager backups. Information about restoring from your backups in the case of a system failure completes this chapter.

SUSE Multi-Linux Managerは、データベース、およびインストールされたプログラムと設定に依存しているため、インストールのすべてのコンポーネントをバックアップすることが重要です。 SUSE Multi-Linux Managerインストールを定期的にバックアップして、データ損失を防止し、迅速に回復できるようにしてください。

使用するバックアップ方法にかかわらず、現在のインストールで使用している容量の3倍以上の空き容量が必要です。 容量が不足するとバックアップが失敗する可能性があるため、頻繁に確認してください。

5.1. Disable old method with smdba

Skip this section if you installed SUSE Multi-Linux Manager 5.1 from scratch.

With the advent of the built-in solution, the old method with the **smdba** backup tool is deprecated. If you migrated from an old system with **smdba** to the new solution, you must disable the old funtionality and remove the old backup archives.

Either disable **smdba** before migrating (recommended) or later on the migrated SUSE Multi-Linux Manager 5.1 system.

Procedure: Disabling old method with installed smdba before migration

This procedure only works when smdba is still installed.

Commands are different on SUSE Manager 4.3 (non-containerized installation) or SUSE Manager 5.0 (containerized installation) present (so 5.0 or on 4.3 before migration):

SUSE Manager 4.3

On the command line, as root, execute:

```
smdba backup-hot --enable=off
```

SUSE Manager 5.0

On the command line of the container host, as root, execute:

```
mgrctl exec -- smdba backup-hot --enable=off
```

> This will change **archive_command** in **/var/lib/pgsql/data/postgresql.conf** as follows:
>
> ```
> archive_command = '/bin/true'
> ```

Now your old system is ready to be migrated to SUSE Multi-Linux Manager 5.1.

Procedure: Disabling old method on SUSE Multi-Linux Manager 5.1 after migration

> Use this procedure after migration, when smdba is no longer available.
>
> 1. On the container host, as root, edit **/var/lib/containers/storage/volumes/var-pgsql/_data/postgresql.conf** and set these options:
>
>    ```
>    archive_mode = off
>    archive_command = '/bin/true'
>    ```
>
> 2. Restart the container:
>
>    ```
>    mgradm restart
>    ```

5.2. SUSE Multi-Linux Managerのバックアップ

SUSE Multi-Linux Managerのインストールをバックアップする最も包括的な方法は、**mgradm backup create**コマンドを使用することです。 これにより、バックアップの管理にかかる時間を節約でき、障害発生時に再インストールと再同期をより速く実行できます。 ただし、この方法ではディスク領域がかなり必要になるため、バックアップの実行に時間がかかることがあります。

mgradm backup createコマンドは、ディレクトリへのバックアップを実行します。 このディレクトリは、ローカルストレージでもマウントされたリモートストレージでも構いません。

mgradm backup createコマンドは、バックアップの内容をさまざまな方法でカスタマイズできます。 利用可能なすべてのオプションについては、**mgradm backup create --help**を参照してください。

5.2.1. Full backup of SUSE Multi-Linux Manager

SUSE Multi-Linux Managerのフルバックアップは、次のコンポーネントのバックアップで構成されます。

- SUSE Multi-Linux Managerボリューム
- データベースボリューム
- podmanネットワーク設定
- podmanシークレット
- SUSE Multi-Linux Manager systemdサービス

- SUSE Multi-Linux Managerコンテナイメージ

フルバックアップの作成に要する時間、SUSE Multi-Linux Managerサービスは自動的に停止されます。 このダウンタイムは長くなる可能性があります。 バックアップが完了すると、サービスは自動的に再開されます。

Procedure: Creating full backup with mgradm backup create

1. コンテナホストで、rootとして、次のコマンドでバックアップを作成します。

```
mgradm backup create $path
```

$pathをバックアップ場所へのパスで置き換えます。

5.2.2. Partial backup of SUSE Multi-Linux Manager

mgradm backup createツールを使用すると部分バックアップを作成できます。 個々のボリュームまたはすべてのボリュームをスキップしたり、データベースのバックアップやイメージをスキップしたりすることができます。

特にデータベースのバックアップがスキップされた場合、SUSE Multi-Linux Managerサービスを停止せずにバックアップが作成され、2段階バックアップ手順の1段階として機能します。

Partial backups are only considering a part of the data, and do not take potential dependencies with other parts which may not have been backed up in consideration. Therefore they cannot guarantee backup/restore consistency.

Procedure: Creating partial backup by skipping database backup

1. コンテナホストで、rootとして、次のコマンドでバックアップを作成します。

```
mgradm backup create --skipdatabase $path
```

$pathをバックアップ場所へのパスで置き換えます。

Procedure: Creating partial backup by skipping a volume

1. コンテナホストで、rootとして、次のコマンドでバックアップを作成します。

```
mgradm backup create --skipvolumes $volumes $path
```

$pathをバックアップ場所へのパスで置き換えます。

Replace **$volumes** by the name of the volume name to be excluded from the backup, or by a comma separated list of volumes to be excluded.

allを使用すると、データベースボリュームを除くすべてのボリュームをスキップします。

5.2.3. 追加ボリュームのバックアップ

mgradm backupコマンドは、SUSE Multi-Linux Managerボリュームの内部リストを使用します。 インストール中に追加のボリュームが設定された場合、またはバックアップに追加のボリュームを追加する必要がある場合は、**--extravolumes $volumes**を使用して指定する必要があります。

Procedure: Creating backup with additional custom volume

1. コンテナホストで、rootとして、次のコマンドでバックアップを作成します。

```
mgradm backup create --extravolumes $volume $path
```

$pathをバックアップ場所へのパスで置き換えます。

$volumesを、バックアップに含めるボリュームの名前、または含めるボリュームのカンマ区切りのリストで置き換えます。

5.2.4. Perform a manual database backup

Procedure: Performing a manual database backup

1. バックアップ用に永続的なストレージ容量を割り当てます。
2. SUSE Multi-Linux Managerコンテナホストのコマンドプロンプトで、rootとして次のコマンドを使用します。

```
mgradm backup create --skipvolumes all --skipconfig --skipimages $path
```

5.3. Restore SUSE Multi-Linux Manager from the existing backup

SUSE Multi-Linux Managerを既存のバックアップから復元すると、復元対象のボリューム、イメージ、および設定のバックアップが列挙されます。バックアップの作成シナリオとは異なり、復元操作では内部のボリュームリストを使用せず、バックアップ内に存在するすべてのボリュームまたはイメージが自動的に検出されます。

復元対象の項目のリストが収集された後で、存在と整合性のチェックが実行されます。存在チェックによ

り、バックアップの復元によって既存のボリューム、イメージ、または設定が誤って上書きされることが防止されます。整合性チェックは、バックアップ項目のチェックサムを計算することで実行されます。

両方のチェックが成功すると、実際のバックアップの復元が実行されます。

SUSE Multi-Linux Managerサービスは、バックアップの復元が完了した後で、自動的に開始されません。

Procedure: Restoring from an existing backup

1. コンテナホストで、rootとして、次のコマンドを使用してSUSE Multi-Linux Managerサーバを再配備します。

```
mgradm stop
mgradm backup restore $path
mgradm start
```

$pathをバックアップ場所へのパスで置き換えます。

バックアップの検証は時間がかかる操作になる可能性があります。バックアップの整合性が他の手段で確保されている場合、**--skipverify**オプションを使用することで検証をスキップできます。

何らかの理由でバックアップに存在するボリュームの復元をスキップする必要がある場合は、**--skipvolumes $volumes**オプションを使用できます。

5.3.1. Recommended steps after restoring a backup

Procedure: Recommended steps after SUSE Multi-Linux Manager restore

1. SUSE Multi-Linux Manager Web UIを使用するか、コンテナ内のコマンドプロンプトで**mgr-sync**ツールを使用して、SUSE Multi-Linux Managerリポジトリを再同期します。 製品を再登録するか、登録およびSSL証明書生成セクションをスキップするかを選択できます。
2. On the container host, check whether you need to restore **/var/lib/containers/storage/volumes/var-spacewalk/_data/packages/**. If **/var/lib/containers/storage/volumes/var-spacewalk/_data/packages/** was not in your backup, you need to restore it. If the source repository is available, you can restore [path]``/var/lib/containers/storage/volumes/var-spacewalk/_data/packages/`u with a complete channel synchronization:

```
mgrctl exec -ti -- mgr-sync refresh --refresh-channels
```

3. Schedule the re-creation of search indexes next time the **rhn-search** service is started.

   This command produces only debug messages, it does not produce error messages.

   On the container host, enter:

```
mgrctl exec -ti -- rhn-search cleanindex
```

Chapter 6. チャンネル管理

チャンネルはソフトウェアパッケージをグループ化する方法です。

SUSE Multi-Linux Managerでは、チャンネルはベースチャンネルと子チャンネルにグループ化され、ベースチャンネルはオペレーティングシステムのタイプ、バージョン、およびアーキテクチャ別にグループ化され、子チャンネルは関連するベースチャンネルと互換性があります。 クライアントがベースチャンネルに割り当てられている場合、そのシステムでは関連する子チャンネルのみをインストールできます。 この方法でチャンネルを編成すると、互換性のあるパッケージのみが各システムにインストールされます。

ソフトウェアチャンネルは、リポジトリを使用してパッケージを提供します。 チャンネルはリポジトリをSUSE Multi-Linux Managerにミラーリングし、パッケージ名やその他のデータはSUSE Multi-Linux Managerデータベースに保存されます。 1つのチャンネルに関連付けられたリポジトリはいくつでも持つことができます。 これらのリポジトリのソフトウェアは、クライアントを適切なチャンネルにサブスクライブすることでクライアントにインストールできます。

クライアントはベースチャンネルにのみ割り当てることができます。 その後、クライアントは、そのベースチャンネルとその子チャンネルのいずれかに関連付けられたリポジトリからパッケージをインストールまたは更新できます。

SUSE Multi-Linux Managerには、SUSE Multi-Linux Managerを実行するために必要なすべてのものを提供する、複数のベンダチャンネルが用意されています。 SUSE Multi-Linux Managerの管理者とチャンネル管理者には、チャンネル管理権限があり、これにより、独自のカスタムチャンネルを作成して管理することができます。 環境で独自のパッケージを使用する場合は、カスタムチャンネルを作成できます。 カスタムチャンネルはベースチャンネルとして使用することも、ベンダベースチャンネルに関連付けることもできます。

カスタムチャンネルの作成の詳細については、**Administration › Custom-channels**を参照してください。

6.1. チャンネル管理

デフォルトでは、すべてのユーザがシステムにチャンネルをサブスクライブできます。 Web UIを使用してチャンネルに制限を実装できます。

プロシージャ: チャンネルへのサブスクライバアクセスの制限

1. SUSE Multi-Linux Manager Web UIで、**ソフトウェア › チャンネルリスト**に移動して、編集するチャンネルを選択します。
2. ［**ユーザごとのサブスクリプション制限**］セクションを見つけて、［**この組織内の指定されたユーザのみがこのチャンネルにサブスクライブできます**］をオンにします。 **[更新]**をクリックして、変更を保存します。
3. ［**サブスクライバ**］タブに移動して、必要に応じてユーザを選択または選択解除します。

6.2. チャンネルの削除

コマンドプロンプトからベンダソフトウェアチャンネルを削除できます。

プロシージャ: ベンダチャンネルを削除する

1. SUSE Multi-Linux Managerサーバのコマンドプロンプトで、rootとして、使用できるベンダチャンネルを一覧にし、削除するチャンネルをメモします。

```
mgr-sync list チャンネル
```

2. チャンネルを削除します。

```
spacewalk-remove-channel -c <channel-name>
```

   - チャンネルを手動で削除する方法の詳細については、**Administration › Removing-channels**を参照してください。
   - カスタムチャンネルの削除については、**Administration › Custom-channels**を参照してください。

6.3. カスタムチャンネル

カスタムチャンネルを使用すると、クライアントを更新するために使用できる、独自のソフトウェアパッケージとリポジトリを作成できます。 また、環境内でサードパーティベンダが提供するソフトウェアを使用することもできます。

このセクションでは、カスタムチャンネルを作成、管理、および削除する方法について詳細に説明します。カスタムチャンネルを作成および管理できるようにするには、管理者権限が必要です。

6.3.1. Creating custom channels and repositories

カスタムチャンネルを作成する前に、関連付けるベースチャンネルと、コンテンツに使用するリポジトリを決定します。

クライアントシステムにインストールする必要があるカスタムソフトウェアパッケージがある場合は、カスタム子チャンネルを作成して管理できます。 システムにチャンネルを割り当てる前に、SUSE Multi-Linux Manager Web UIでチャンネルを作成し、パッケージのリポジトリを作成する必要があります。

クライアントシステムと互換性のないパッケージを含む子チャンネルを作成しないでください。

ベンダによって提供されたパッケージを使用する場合は、ベースチャンネルとしてベンダチャンネルを選択できます。 または［**なし**］を選択して、カスタムチャンネルをベースチャンネルにします。

Procedure: Creating a custom channel

1. SUSE Multi-Linux Manager Web UIで、**ソフトウェア › 管理 › チャンネル**に移動して、**[チャンネルの作成]**をクリックします。

2. ［**ソフトウェアチャンネルの作成**］ページで、チャンネルに名前(たとえば、**My Tools SLES 15 SP1 x86_64**)、およびラベル(たとえば、**my-tools-sles15sp1-x86_64**)を付けます。 ラベルにはスペースまたは大文字を含めないでください。
3. ［**親チャンネル**］ドロップダウンで、関連するベースチャンネル(たとえば、**SLE-Product-SLES15-SP1-Pool for x86_64**)を選択します。 パッケージに互換性のある親チャンネルを選択していることを確認します。
4. ［**アーキテクチャ**］ドロップダウンで、適切なハードウェアアーキテクチャ(たとえば、**x86_64**)を選択します。
5. ご使用の環境に応じて、連絡先の詳細、チャンネルアクセス制御、およびGPGフィールドに追加情報を入力します。
6. **[チャンネルの作成]**をクリックします。

カスタムチャンネルでは、追加のセキュリティ設定が必要になる場合があります。 多くのサードパーティベンダは、GPGを使用してパッケージをセキュリティ保護しています。 カスタムチャンネルでGPGで保護されたパッケージを使用する場合は、メタデータの署名に使用されたGPGキーを信頼する必要があります。 次に、［**メタデータは署名されていますか？**］チェックボックスをオンにして、パッケージメタデータを信頼できるGPGキーと照合します。

リモートチャンネルおよびリポジトリがGPGキーで署名されている場合、これらのGPGキーをインポートして信頼することができます。 たとえば、SUSE Multi-Linux Managerサーバのコマンドラインから**spacewalk-repo-sync**を実行します。

```
/usr/bin/spacewalk-repo-sync -c <channellabelname> -t yum
```

This command and procedure is for temporary GPG key synchronization only. For storing the key permantenly, see this section later on.

基盤となる**zypper**コールは、利用可能な場合はキーをインポートします。 Web UIはこの機能を提供していません。

これは、ミラーするリポジトリが特別な方法で設定されていて、署名の横のリポジトリに「キー」が提供されている場合にのみ機能します 。 これは、Open Build Service (OBS)によって生成されたすべてのリポジトリに該当します。 その他のリポジトリについては、以下で詳述する特別な準備ステップが必要です。

デフォルトでは、新しいチャンネルを作成する際に［**GPGチェックの有効化**］フィールドがオンになっています。 チャンネルにカスタムパッケージとアプリケーションを追加する場合は、このフィールドをオフにして、署名されていないパッケージをインストールできるようにしてください。 パッケージが信頼されていないソースからのものである場合、GPGチェックを無効にするとセキュリティリスクが生じます。

You can only add a repository to the SUSE Multi-Linux Manager with the Web UI if it is a valid software repository. Check in advance that needed repository metadata are available. Tools such as **createrepo**

and **reprepro** are useful in this regard. **mgrpush** can help with pushing a single RPM into a channel without creating a repository.

- For more information on **createrepo_c** see https://manpages.opensuse.org/Leap-15.6/createrepo_c/
- For more information on **reprepro** see https://manpages.opensuse.org/Leap-15.6/reprepro/

Procedure: Adding a software repository

1. SUSE Multi-Linux Manager Web UIで、**ソフトウェア › 管理 › リポジトリ**に移動し、**[リポジトリの作成]**をクリックします。
2. ［**リポジトリの作成**］ページで、リポジトリにラベル(たとえば、**my-tools-sles15sp1-x86_64-repo**)を付けます。
3. ［**リポジトリURL**］フィールドに、**repodata**ファイル(たとえば、file:///opt/mytools/)を含むディレクトリへのパスを指定します。　このフィールドでは、任意の有効なアドレス指定プロトコルを使用できます。
4. ［**メタデータは署名されていますか？**］チェックボックスをオフにします。
5. オプション:　リポジトリでクライアント証明書認証が必要な場合は、SSLフィールドに入力します。
6. **[リポジトリの作成]**をクリックします。

先に示したプロシージャは、ミラーリングするリポジトリが署名の横にあるリポジトリに「キー」を提供する場合にのみ機能します。これはOBSによって生成されたすべてのリポジトリに該当しますが、通常、OBSによって提供されていないオペレーティングシステムの他のリポジトリには該当しません。

使用するリポジトリにGPGキーがない場合は、自分でGPGキーを指定し、GPGキーをキーリングに手動でインポートできます。**gpg**コマンドラインツールを使用して**/var/lib/spacewalk/gpgdir**キーリングにキーをインポートすると、永続的に保存されます。chroot環境が消去されても、キーは保持されます。

Procedure: Creating a software repository with GPG key

1. On the container host, the command to import a key into the keyring, is:

```
mgradm gpg add /path/to/gpg.key
```

2. For more information, see **Client-configuration › Autoinst-owngpgkey**.

uyuni_suite、**uyuni_component**、および**uyuni_arch**のクエリパラメータを使用し

て、Debianの非フラットリポジトリを追加します。

uyuni_suite

必須です。 Debianのドキュメントでは、これは**distribution**とも呼ばれています。 このパラメータでは、aptソースを指定します。 このパラメータを指定しない場合は、元のアプローチが使用されます。パラメータの末尾が/の場合、リポジトリはフラットとして識別されます。

uyuni_component

オプションです。このパラメータは1つのコンポーネントのみを指定できます。コンポーネントを一覧にすることはできません。aptソースエントリでは複数のコンポーネントを指定できますが、Uyuniでは指定できません。代わりに、コンポーネントごとに個別のリポジトリを作成する必要があります。

uyuni_arch

オプションです。 省略すると、データベースからチャンネルのSQLクエリを使用してアーキテクチャ名が計算されます。 チャンネルのアーキテクチャと一致しない場合は、明示的に**uyuni_arch**を指定します(アーキテクチャの命名があいまいな場合があります)。

ここにいくつかの例があります。

表 2. Debian非フラットリポジトリマッピング

タイプ	ソース行 / URL
apt ソース行	**deb** https://pkg.jenkins.io/debian-stable **binary/**
URLマッピング	https://pkg.jenkins.io/debian-stable?uyuni_suite=binary/
aptソース行	**deb** https://deb.debian.org/debian/dists **stable main**
URLマッピング	https://deb.debian.org/debian/dists?uyuni_suite=stable&uyuni_component=main

Debianリポジトリ定義フォーマットに関する情報はこちらをご覧ください。この情報は、https://wiki.debian.org/DebianRepository/Format#Overviewに基づいています。

リポジトリ定義フォーマットは次のとおりです。

```
deb uri suite [コンポーネント1] [コンポーネント2] [...]
```

例:

```
deb https://deb.debian.org/debian/dists stable main
```

または

```
deb https://pkg.jenkins.io/debian-stable binary/
```

スイートと**コンポーネント**のペアごとに、仕様ではベースURL **+ suite + component**に基づいて計算される個別のURLを定義しています。

Procedure: Assigning the repository to a channel

1. **ソフトウェア › 管理 › チャンネル**に移動して、新たに作成されたカスタムチャンネルの名前をクリックし、新しいリポジトリをカスタムチャンネルに割り当てます。
2. ［**リポジトリ**］タブに移動し、チャンネルに割り当てるリポジトリがオンになっていることを確認し、**[リポジトリの保存]**をクリックします。
3. デフォルトでは、同期プロセスはすぐに開始されます。

チャンネルの同期の詳細については、administration:custom-channels.pdfを参照してください。

Procedure: Adding custom channels to an activation key

1. SUSE Multi-Linux Manager Web UIで、**システム › アクティベーションキー**に移動して、カスタムチャンネルを追加するキーを選択します。
2. ［**詳細**］タブの［**子チャンネル**］リストで、関連付けるチャンネルを選択します。 必要に応じて、複数のチャンネルを選択できます。
3. **[アクティベーションキーの更新]**をクリックします。

6.3.2. カスタムチャンネル同期

重要な更新を見逃さないようにするため、SUSEでは、カスタムチャンネルをリモートリポジトリの変更に合わせて最新の状態に保つことをお勧めします。

デフォルトでは、作成したすべてのカスタムチャンネルに対して同期が自動的に行われます。特に、次のことが発生します。

- UIから、または**spacewalk-common-channels**を使用して、リポジトリをチャンネルに追加した後
- 毎日のタスク**mgr-sync-refresh-default**の一部として、すべてのカスタムおよびベンダチャンネルを同期します。

このデフォルトの動作を無効にするには、**/etc/rhn/rhn.conf**に以下を設定します。

```
java.unify_custom_channel_management = 0
```

このプロパティをオフにすると、同期は自動的に実行されません。カスタムチャンネルを最新の状態に保つには、次の操作を行う必要があります。

- ［**同期**］ タブに移動し、**[今すぐ同期]**をクリックして手動で同期し、
- ［**リポジトリ**］タブから自動同期スケジュールを設定します。

プロセス開始時には、チャンネルの同期が終了したかどうかを確認するいくつかの方法があります。

- SUSE Multi-Linux ManagerのWeb UIで、**管理 › セットアップウィザード**に移動し、［**製品**］タブを選択します。 このダイアログには、同期中の各製品の完了バーが表示されます。
- SUSE Multi-Linux ManagerのWeb UIで、**ソフトウェア › 管理 › チャンネル**に移動し、リポジトリに関連付けられているチャンネルをクリックします。 **リポジトリ › 同期**タブに移動します。リポジトリ名の横に［**同期状態**］が表示されます。
- コマンドプロンプトで同期ログファイルを確認します。

  ```
  tail -f /var/log/rhn/reposync/<channel-label>.log
  ```

  同期の進行中に各子チャンネルは独自のログを生成します。 同期が完了したことを確認するには、ベースチャンネルと子チャンネルのログファイルをすべて確認する必要があります。

次のカスタムチャンネル同期オプションが利用できます。

リポジトリから削除されたチャンネル内のパッケージを保持する

これにより、**strict**モードがオフになります。

エラータを同期しない

パッチを同期しません。

最新パッケージのみ同期する

最新のパッケージバージョンのみを同期します。

キックスタート可能なツリーの作成

このオプションは、Kickstartによる自動インストール用にディレクトリツリーを準備します。

エラーが発生したら終了する

エラーが発生した場合、同期を停止します。

これらのオプションはチャンネルごとに永続的に保存されます。**[今すぐ同期]**ボタンをクリックした場合も、同期を実行する前にチャンネルオプションが保存されます。

6.3.3. Add packages and patches to custom channels

既存のチャンネルからクローンを作成せずに新しいカスタムチャンネルを作成する場合、そのチャンネルにはパッケージやパッチは含まれません。 SUSE Multi-Linux Manager Web UIを使用して、必要なパッケージとパッチを追加できます。

カスタムチャンネルには、クローンまたはカスタムのパッケージまたはパッチのみを含めることができ、チャンネルの基本アーキテクチャに一致する必要があります。 カスタムチャンネルに追加されたパッチは、チャンネルに存在するパッケージに適用する必要があります。

Procedure: Adding packages to custom channels

1. SUSE Multi-Linux Manager Web UIで、**ソフトウェア › 管理 › チャンネル**に移動して、［**パッケージ**］タブに移動します。
2. オプション: ［**一覧表示/削除**］タブに移動して、現在チャンネル内にあるすべてのパッケージを表示します。
3. ［**追加**］タブに移動して、チャンネルに新しいパッケージを追加します。
4. パッケージを提供する親チャンネルを選択し、**[パッケージの表示]**をクリックして、リストに入力します。
5. カスタムチャンネルに追加するパッケージをオンにして、**[パッケージの追加]**をクリックします。
6. 選択に問題がなければ、**[追加の確認]**をクリックして、チャンネルにパッケージを追加します。
7. オプション: **ソフトウェア › 管理 › チャンネル**に移動し、**パッケージ › 比較**タブに移動して、現在のチャンネルのパッケージを別のチャンネルのパッケージと比較できます。 2つのチャンネルを同じにするには、**[違いをマージする]**ボタンをクリックし、競合を解決します。

Procedure: Adding patches to a custom channel

1. SUSE Multi-Linux Manager Web UIで、**ソフトウェア › 管理 › チャンネル**に移動して、［**パッチ**］タブに移動します。
2. オプション: ［**一覧表示/削除**］タブに移動して、現在チャンネル内のすべてのパッチを表示します。
3. ［ **追加**］タブに移動し、追加するパッチの種類を選択して、チャンネルに新しいパッチを追加します。

4. パッチを提供する親チャンネルを選択し、[**関連付けられたパッチの表示**]をクリックして、リストに入力します。
5. カスタムチャンネルに追加するパッチをオンにして、[**確認**]をクリックします。
6. 選択に問題がなければ、[**確認**]をクリックして、チャンネルにパッチを追加します。

6.3.4. Manage custom channels

SUSE Multi-Linux Manager管理者とチャンネル管理者は任意のチャンネルを変更または削除できます。

チャンネルを変更または削除する権限を他のユーザに付与するには、**ソフトウェア › 管理 › チャンネル**に移動して、編集するチャンネルを選択します。 ［ **マネージャ**］タブに移動して、権限を付与するユーザをオンにします。 [**更新**]をクリックして、変更を保存します。

一連のクライアントに割り当てられているチャンネルを削除すると、削除されたチャンネルに関連付けられているすべてのクライアントのチャンネル状態が直ちに更新されます。 これは、変更がリポジトリファイルに正確に反映されるようにするためです。

Web UIを使用してSUSE Multi-Linux Managerチャンネルを削除することはできません。 カスタムチャンネルのみを削除できます。

Procedure: Deleting custom channels

1. SUSE Multi-Linux Manager Web UIで、**ソフトウェア › 管理 › チャンネル**に移動して、削除するチャンネルを選択します。
2. [**ソフトウェアチャンネルの削除**]をクリックします。
3. ［**チャンネルの削除**］ページで、削除するチャンネルの詳細を確認し、［**システムのサブスクライブを中止**］チェックボックスをオンにして、まだサブスクライブされている可能性のあるシステムからカスタムチャンネルを削除します。
4. [**チャンネルの削除**]をクリックします。

チャンネルを削除しても、削除されたチャンネルの一部であるパッケージは自動的に削除されません。 チャンネルが削除されたパッケージを更新することはできません。

SUSE Multi-Linux Manager Web UIで、チャンネルに関連付けられていないパッケージを削除できます。 **ソフトウェア › 管理 › パッケージ**に移動して、削除するパッケージをオンにして、[**パッケージの削除**]をクリックします。

6.4. Third-party Channels

SUSE Multi-Linux Manager includes the ability to synchronize the content of optional third-party repositories with some of the products that can be managed by it.

Some third-party GPG keys are included by default in the SUSE Multi-Linux Manager database, and some are not. For third-party keys that are not included, the relevant keys need to be imported when choosing to synchronize such third-party repositories.

To import a GPG key, use the following command syntax, executing the command on the SUSE Multi-Linux Manager host server:

```
mgradm gpg add <path-to-gpg-key-file-or-URL>
```

1. Example: Adding a GPG key from a file:

```
mgradm gpg add repomd.xml.key
```

1. Example: Adding a GPG key from a remote repository using a URL:

```
mgradm gpg add
https://public.dhe.ibm.com/software/server/POWER/Linux/yum/OSS/SLES/15/ppc64le/repodata/repomd.xml.key
```

To list the keys currently held in the SUSE Multi-Linux Manager GPG database, run the following command:

```
mgrctl exec -ti -- gpg --homedir /var/lib/spacewalk/gpgdir --list-keys
```

When installing a package on the client, you may also need to trust the GPG key on the client itself. This requires that the GPG key is also available there.

For more information, see: **Client-configuration › Gpg-keys**.

6.5. チャンネルの削除

この章では、SUSEで提供されているチャンネルをSUSE Multi-Linux Managerから手動で削除する方法、サポート終了製品をクリーンアップする方法、および他の目的のために領域を再利用する方法について説明しています。

6.5.1. チャンネルの削除の準備

チャンネルを削除する前に、削除するチャンネルのラベルを特定する必要があります。これは、Web UIを使用するか、コマンドラインで行うことができます。

- システムが現在サブスクライブしているチャンネルや、サブスクライブする予定のチャンネルを削除しないように注意してください。

- 削除するチャンネルを現在サブスクライブしているシステムがある場合は、そのシステムをアップグレードするか、サブスクリプションを解除するまで、そのチャンネルを削除しないでください。

6.5.1.1. チャンネルのラベルの特定

プロシージャ: Web UIを使用したチャンネルのラベルの特定

1. SUSE Multi-Linux Manager Web UIで、**ソフトウェア › チャンネルリスト › すべて**に移動します。
2. このページに、**Channel Name (チャンネル名)**が表示されます。チャンネル名のリンクを選択すると、**Channel Label (チャンネルのラベル)**のフィールドが表示されます。
3. 削除するチャンネルと子チャンネルを特定します。

プロシージャ: コマンドラインを使用したチャンネルのラベルの特定

1. SUSE Multi-Linux Managerコンテナホストで、次のコマンドを実行して、チャンネルのリストを取得できます。

```
mgrctl exec -ti -- spacewalk-remove-channel -l
```

6.5.1.2. システムのチャンネルのサブスクリプションの確認

プロシージャ: Web UIを使用した、システムのチャンネルのサブスクリプションの確認

1. SUSE Multi-Linux Manager Web UIで、**ソフトウェア › チャンネルリスト › すべて**に移動します。
2. 右側にある［**システム**］列を見つけます。
3. 削除するチャンネルがあるかどうかを［**システム**］列で確認します。

プロシージャ: コマンドラインを使用した、システムのチャンネルのサブスクリプションの確認

1. SUSE Multi-Linux Managerコンテナホストで次のコマンドを実行します。

```
mgrctl exec -ti -- 'spacecmd -- softwarechannel_listsystems <Channel Label>'
```

6.5.2. チャンネルの削除

チャンネルとそのメタデータは、コマンドラインツールでのみ削除できます。 **spacewalk-remove-channel** コマンドは、他のチャンネルから参照されなくなったソフトウェアパッケージを自動的に削除します。 したがって、メタデータはデータベースから、ファイルはストレージメディアから削除されます。

6.5.2.1. 子チャンネルの削除

プロシージャ: コマンドラインを使用した子チャンネルの削除

1. 個々のチャンネルを削除するには、SUSE Multi-Linux Managerコンテナホストで次のコマンドを実行します。

```
mgrctl exec -ti -- spacewalk-remove-channel -c channel-label
```

2. 複数のチャンネルを同時に削除するには、各チャンネルに対して**-c**フラグを使用し、その後に**channel-label**を付けます。 次に例を示します。

```
mgrctl exec -ti -- spacewalk-remove-channel -c channel-label1 -c channel-label2
```

6.5.2.2. 親チャンネルとそのすべての子チャンネルの削除

プロシージャ: 親チャンネルとそのすべての子チャンネルの削除

1. 親チャンネルとすべての子チャンネルを削除するには、**spacewalk-remove-channel**を **-a** オプションを指定して実行し、**parent-channel-label** を **sles12-sp5-pool-x86_64**のようなチャンネルラベルに置き換えます。

```
mgrctl exec -ti -- spacewalk-remove-channel -a parent-channel-label
```

Chapter 7. コンフィデンシャルコンピューティング

Confidential Computingは、ハードウェアベースの高信頼実行環境(TEE)を利用して、使用中のデータを保護できる技術です。TEEとは、データの整合性、データの機密性、およびコードの整合性に対して強化されたレベルのセキュリティを提供する環境のタイプです。

7.1. SUSE Multi-Linux ManagerでのConfidential Computing

TEEの信頼性は認証プロセスによってチェックされます。SUSE Multi-Linux Managerを、登録されているシステムの認証サーバとして使用できます。これにより、このモードで動作しているシステムのレポートページが生成されます。これらのシステムは定期的に認証およびチェックする必要があります。過去のチェックの履歴も保存されており、要求に応じて利用できます。

Confidential Computingの検証は、認証されるシステムが実行されている使用ハードウェアと環境によって異なります。

Confidential Computingの認証はx86_64アーキテクチャでのみ利用できます。

7.2. 要件

Confidential Computingは、次の特性を持つ環境にセットアップできます。

- 認証されるシステム(仮想マシン)がSLES15 SP6であり、SUSE Multi-Linux Managerにブートストラップされる
- ハードウェアに**AMD EPYC Milan CPU**または**AMD EPYC Genoa CPU**が搭載されている必要がある
- BIOSがConfidential Computingの認証を許可するように設定されている必要がある
- ホストOSと仮想化ソフトウェア(KVMおよびlibvirt)でConfidential Computingがサポートされている必要がある

7.3. 制限事項

- SLES15 SP6のConfidential Computingの認証はテクノロジプレビューとして提供されています。
- SUSE Multi-Linux ManagerのConfidential Computingの検証はテクノロジプレビューとして提供されています。
- セキュアブートは認証されますが、現在のところKVMセキュリティブートとSNPゲストは同時に使用できません。

7.4. SUSE Multi-Linux ManagerでのConfidential Computingの使用

Confidential Computingをホストにセットアップして設定する正確な手順については、OSベンダのマニュアルを参照してください。

プロシージャ: SUSE Multi-Linux Managerのインストール中に認証コンテナを有効にする

1. 認証コンテナは、**mgradm install podman**を使用してSUSE Multi-Linux Managerをインストールする際に有効にします。
2. ファイル**mgradm.yaml**に以下を追加します。

```
coco:
    replicas: 1
```

プロシージャ: SUSE Multi-Linux Managerのインストール後に認証コンテナを有効にする

1. インストール後に認証コンテナを有効にするには、コマンドラインパラメータ**mgradm**を使用します。
2. 次のコマンドを実行します。

```
mgradm scale uyuni-server-attestation --replicas 1
```

Procedure: Disabling Attestation Container After the SUSE Multi-Linux Manager Installation

1. すでに有効な認証コンテナを無効にするには、次のコマンドを実行します。

```
mgradm scale uyuni-server-attestation --replicas 0
```

プロシージャ: 認証を有効にする

1. 選択したシステムで、**監査 › Confidential Computing › 設定** (コンフィデンシャルコンピューティング > 設定)に移動します。
2. トグルボタンを選択して認証を有効にします。
3. フィールド**環境タイプ**で、ドロップダウンリストから正しいオプションを選択します。
4. **[保存]**をクリックして、変更を保存します。

プロシージャ: 新しい認証をスケジュールする

1. 選択したシステムで、**監査 › Confidential Computing › List Attestations** (コンフィデンシャルコンピューティング > 認証の一覧)タブに移動します。

2. **[認証のスケジュールを設定する]**をクリックします。新しいフォームが開きます。
3. **指定時刻以降にスケジュール**で、認証の実行時刻を選択します。
4. 必要に応じて、**以下に追加**オプションを選択して、新しく作成した認証を動作チェーンに追加します。
5. **[スケジュール]**をクリックして、新しい認証の実行を保存してスケジュールします。

プロシージャ: システム詳細から検証レポートを表示する

1. 選択したシステムで、**監査 › Confidential Computing › List Attestations** (コンフィデンシャルコンピューティング > 認証の一覧)タブに移動します。
2. 表示するレポートを見つけて選択します。
3. 選択した検証レポートをクリックすると、**概要**タブが開きます。
4. 次のタブ**SEV-SNP**に移動します。
5. 最後に、次のタブ**セキュアブート**に移動します。

プロシージャ: 監査から検証レポートを表示する

1. ナビゲーションバーから、**監査 › Confidential Computing** (コンフィデンシャルコンピューティング) を選択します。
2. メインパネルにすべての認証のリストが表示されます。
3. 表示するレポートを見つけて選択します。

7.4.1. レポートのステータス

認証レポートは次のいずれかのステータスになります。

待機中

これはスケジュールされた認証のデフォルトのステータスです。プロセスがまだ開始されていないか完了していないため、レポートはまだ利用可能ではありません。

成功

スケジュールされた認証によって、表示可能なレポートが作成されると、プロセスのステータスは**成功**になります。

失敗

スケジュールされた認証が失敗し、その結果レポートが作成されない場合、プロセスのステータスは**失敗**になります。

7.5. 関連トピック

Confidential Computingの詳細については、https://www.fortanix.com/platform/confidential-computing-manager/what-is-confidential-computing[こちら]を参照してください。

Chapter 8. コンテンツライフサイクル管理

コンテンツライフサイクル管理では運用クライアントを更新する前にパッケージをカスタマイズおよびテストできます。 これは、限られたメンテナンスウィンドウ中に更新を適用する必要がある場合に特に役立ちます。

コンテンツライフサイクル管理では、ソフトウェアチャンネルをソースとして選択し、必要に応じて環境に合わせて調整して、運用クライアントにインストールする前に徹底的にテストすることがでます。

ベンダチャンネルを直接変更することはできませんが、パッケージとカスタムパッチを追加または削除することで、それらのチャンネルのクローンを作成し、クローンを変更することができます。 これらのクローンチャンネルをテストクライアントに割り当てて、クライアントが期待どおりに動作することを確認できます。

デフォルトでは、クローンベンダチャンネルは元のベンダチャンネルと一致し、依存関係を自動的に選択します。 **/etc/rhn/rhn.conf**に次のオプションを追加することにより、クローンチャンネルの自動選択を無効にできます。

```
java.cloned_channel_auto_selection = false
```

次に、すべてのテストに合格すると、クローンチャンネルを運用サーバにプロモートできます。

これは、ソフトウェアチャンネルがライフサイクルで移動できる一連の環境を通じて実現されます。 ほとんどの環境ライフサイクルには、少なくともテスト環境と運用環境が含まれていますが、必要な数の環境を持つことができます。

このセクションでは、基本的なコンテンツライフサイクル手順、および使用可能なフィルタについて説明します。 より具体的な例については、**Administration › Content-lifecycle-examples**を参照してください。

8.1. コンテンツライフサイクルプロジェクトの作成

コンテンツライフサイクルを設定するには、プロジェクトから開始する必要があります。 プロジェクトでは、ソフトウェアチャンネルソース、パッケージの検索に使用されるフィルタ、およびビルド環境について定義します。

Procedure: Creating a content lifecycle project

1. SUSE Multi-Linux Manager Web UIで、**コンテンツライフサイクル › プロジェクト**に移動し、**[プロジェクトの作成]**をクリックします。
2. ［**ラベル**］フィールドに、プロジェクトのラベルを入力します。 ［**ラベル**］フィールドには、小文字、数字、ピリオド、ハイフン、およびアンダースコアのみを入力できます。
3. ［**名前**］フィールドに、プロジェクトのわかりやすい名前を入力します。

4. [作成]ボタンをクリックして、プロジェクトを作成し、プロジェクトページに戻ります。
5. [Attach/Detach Sources]（ソースの割り当て/取り外し）をクリックします。
6. ［ソース］ダイアログで、ソースタイプを選択し、プロジェクトの ベースチャンネルを選択します。 チャンネルが必須か推奨されるかに関する情報を含め、選択したベースチャンネルで使用可能な子チャンネルが表示されます。
7. 必要な子チャンネルをオンにし、[保存]をクリックして、プロジェクトページに戻ります。 選択したソフトウェアチャンネルが表示されているはずです。
8. [フィルタの割り当て／取り外し]をクリックします。
9. ［フィルタ］ダイアログで、プロジェクトに割り当てるフィルタを選択します。 新しいフィルタを作成するには、[新しいフィルタの作成]をクリックします。
10. [環境の追加]をクリックします。
11. ［環境ライフサイクル］ダイアログで、最初の環境に、名前、ラベル、および説明を付けて、[保存]をクリックします。 ［ラベル］フィールドには、小文字、数字、ピリオド、ハイフン、およびアンダースコアのみを入力できます。
12. ライフサイクルのすべての環境が完了するまで、環境の作成を続行します。 作成時に［前に挿入］フィールドで環境を選択することで、ライフサイクルの環境の順序を選択できます。

8.2. Filter types

SUSE Multi-Linux Managerでは、プロジェクトの構築に使用するコンテンツを制御するために、さまざまなタイプのフィルタを作成できます。 フィルタを使用すると、ビルドに含めるパッケージまたはビルドから除外するパッケージを選択できます。 たとえば、すべてのカーネルパッケージを除外したり、一部のパッケージの特定のリリースのみを含めることができます。

サポートされているフィルタは次のとおりです。

- パッケージのフィルタリング
  - by name（名前別）
  - by name, epoch, version, release, and architecture（名前、エポック、バージョン、リリース、

およびアーキテクチャ別）
    - by provided name（指定された名前別）
- パッチフィルタリング
    - by advisory name（アドバイザリ名別）
    - by advisory type（アドバイザリタイプ別）
    - by synopsis（概要別）
    - by keyword（キーワード別）
    - by date（日付別）
    - by affected package（影響を受けるパッケージ別）
- モジュール
    - by stream（ストリーム別）

パッケージの依存は、コンテンツのフィルタリング中には解決されません。

フィルタで使用できるマッチャーは複数あります。 使用できるマッチャーは、選択したフィルタ タイプによって異なります。

使用できるマッチャーは次のとおりです。

- 含む
- 一致（正規表現の形式を取る必要があります）
- 等しい
- 新しい
- 新しいか等しい
- 古いか等しい
- 古い
- 新しいか等しい

8.2.1. Filter rule parameter

各フィルタには**許可**または**拒否**のいずれかに設定できる**rule**パラメータがあります。 フィルタは次のように処理されます。

- パッケージまたはパッチが**拒否**フィルタを満たす場合は、結果から除外されます。
- パッケージまたはパッチが**許可**フィルタを満たす場合は、結果に含まれます（**拒否**フィルタによって除外された場合でも）。パッケージに対する**許可**フィルタはパッケージフィルタでのみ動作し、パッチに対する**許可**フィルタはパッチフィルタでのみ動作します。つまり、パッケージフィルタでは、パッチフィルタで除外されたパッケージを再び追加することはできません。また、パッケージフィルタで除外されたパッチを再び追加することもできません。

この動作は、一般的な **拒否** フィルタを使用して多数のパッケージまたはパッチを除外し、特定の **許可** フィルタで特定のパッケージまたはパッチを「チェリーピック」する場合に役立ちます。

コンテンツフィルタは組織内でグローバルなものであり、プロジェクト間で共有できます。

プロジェクトにすでに構築されたソースが含まれている場合、環境を追加すると、既存のコンテンツが自動的に入力されます。 コンテンツは、サイクルの以前の環境から引き出されます（存在していた場合）。 以前の環境がない場合は、プロジェクトソースが再度構築されるまで空のままになります。

8.3. Filter templates

いくつかの一般的なシナリオでフィルタの作成を支援するため、SUSE Multi-Linux Managerにはフィルタテンプレートが用意されています。 これらのテンプレートを適用すると、特定のユースケースに合わせてカスタマイズされた一連のフィルタを事前に作成できます。

このセクションでは、使用可能なテンプレートとその使用方法について説明します。

8.3.1. Live patching based on a SUSE product

ライブパッチ処理を含むプロジェクトでは、ライブパッチパッケージのみがクライアントに更新として提供されるように、定期的な将来のカーネルパッケージを除外する必要があります。 一方で、システムの整合性を維持するために、すでにインストールされている通常のカーネルパッケージを含める必要があります。

このテンプレートを適用すると、この動作を実現するために必要な3つのフィルタが作成されます。

- ベースカーネルバージョンと同じ**kernel-default**パッケージを含むパッチを許可する
- **reboot_suggested**キーワードを含むパッチを拒否する
- **installhint(reboot-needed)**という名前を提供するパッケージを含むパッチを拒否する

ライブパッチ処理プロジェクトの設定方法の詳細については、administration:content-lifecycle-examples.pdfを参照してください。

プロシージャ: テンプレートの適用

1. SUSE Multi-Linux Manager Web UIで、**コンテンツライフサイクル › フィルタ**に移動して、[**Create Filter**]（フィルタの作成）をクリックします。
2. ダイアログで、[**テンプレートを使用する**]をクリックします。それに応じて入力が変更されます。
3. ［**プレフィクス**］フィールドに名前のプレフィクスを入力します。 この値は、テンプレートによって作成された個々のフィルタの名前の前に追加されます。 テンプレートがプロジェクトのコンテキストで適用されてい

る場合、このフィールドにはプロジェクトラベルが事前に入力されます。

4. ［**テンプレート**］フィールドで、［**SUSE製品に基づくライブパッチ処理**］を選択します。
5. ［**製品**］フィールドで、ライブパッチ処理を設定する製品を選択します。
6. ［**カーネル**］フィールドで、選択した製品で使用可能なバージョンのリストからカーネルバージョンを選択します。以降の通常のカーネルパッチを拒否するフィルタは、このバージョンに基づきます。
7. **[保存]**をクリックして、フィルタを作成します。
8. **コンテンツライフサイクル › プロジェクト**に移動して、プロジェクトを選択します。
9. **[フィルタの割り当て／取り外し]**をクリックします。
10. 指定したプレフィクスを持つフィルタを3つ選択し、**[保存]**をクリックします。

8.3.2. システムに基づくライブパッチ処理

特定の登録済みシステムにインストールされているカーネルバージョンに基づいてライブパッチ処理プロジェクトを設定する場合、「システムに基づくライブパッチ処理」テンプレートを使用できます。

このテンプレートを適用すると、この動作を実現するために必要な3つのフィルタが作成されます。

- ベースカーネルバージョンと同じ**kernel-default**パッケージを含むパッチを許可する
- **reboot_suggested**キーワードを含むパッチを拒否する
- **installhint(reboot-needed)**という名前を提供するパッケージを含むパッチを拒否する

ライブパッチ処理プロジェクトの設定方法の詳細については、administration:content-lifecycle-examples.pdfを参照してください。

プロシージャ: テンプレートの適用

1. SUSE Multi-Linux Manager Web UIで、**コンテンツライフサイクル › フィルタ**に移動して、**[Create Filter]**（フィルタの作成）をクリックします。
2. ダイアログで、**[テンプレートを使用する]**をクリックします。 それに応じて入力が変更されます。

3. ［**プレフィクス**］フィールドに、名前のプレフィクスを入力します。 この値はテンプレートによって作成されたすべてのフィルタの名前の前に追加されます。 テンプレートがプロジェクトのコンテキストで適用されている場合は、このフィールドにはプロジェクトラベルが事前に入力されます。
4. ［**テンプレート**］フィールドで、［**固有のシステムに基づくライブパッチ処理**］を選択します。
5. ［**システム**］フィールドで、リストからシステムを選択するか、システム名の入力を開始して、オプションを絞り込みます。
6. ［**カーネル**］フィールドで、選択したシステムにインストールされているバージョンのリストからカーネルバージョンを選択します。 以降の通常のカーネルパッチを拒否するフィルタは、このバージョンに基づきます。
7. **[保存]**をクリックして、フィルタを作成します。
8. **コンテンツライフサイクル › プロジェクト**に移動して、プロジェクトを選択します。
9. **[フィルタの割り当て／取り外し]**をクリックします。
10. 指定したプレフィクスを持つフィルタを3つ選択し、**[保存]**をクリックします。

8.3.3. デフォルトのAppStreamモジュール

プロジェクトに含まれているモジュラーリポジトリですべてのモジュールを使用できるようにする場合は、このフィルタテンプレートを使用してモジュールを自動的に追加できます。

このテンプレートを適用すると、モジュールごとにAppStreamフィルタとそのデフォルトストリームが作成されます。

このプロセスがプロジェクトのページから実行された場合、フィルタは自動的にプロジェクトに追加されます。追加されない場合は、作成されたフィルタを**コンテンツライフサイクル › フィルタ**に一覧表示し、必要に応じて任意のプロジェクトに追加できます。

個々のフィルタを編集して別のモジュールストリームを選択したり、ターゲットリポジトリからそのモジュールを除外するために完全に削除したりできます。

すべてのモジュールストリームが相互に互換性があるわけではないため、個々のストリームを変更すると、モジュール間依存関係を正常に解決できない可能性があります。 この場合、プロジェクトの詳細ページのフィルタペインに問題を説明するエラーが表示さ

れ、すべてのモジュールの選択が互換性を持つようになるまでビルドボタンは無効になります。

Red Hat Enterprise Linux 9以降、モジュールには定義済みのデフォルトストリームがありません。 したがって、Red Hat Enterprise Linux 9のソースでこのテンプレートを使用しても効果はありません。

AppStreamリポジトリをコンテンツライフサイクル管理で設定する方法の詳細については、administration:content-lifecycle-examples.pdfを参照してください。

プロシージャ: テンプレートの適用

1. SUSE Multi-Linux ManagerのWeb UIで、**Content Lifecycle › Projects**に移動し、プロジェクトを選択します。
2. ［**フィルタ**］セクションで、**[フィルタの割り当て／取り外し]**をクリックし、**[新しいフィルタの作成]**をクリックします。
3. ダイアログで、**[テンプレートを使用する]**をクリックします。 それに応じて入力が変更されます。
4. ［**プレフィクス**］フィールドに、名前のプレフィクスを入力します。 この値はテンプレートによって作成されたすべてのフィルタの名前の前に追加されます。 テンプレートがプロジェクトのコンテキストで適用されている場合は、このフィールドにはプロジェクトラベルが事前に入力されます。
5. ［**テンプレート**］フィールドで、［**デフォルトのAppStreamモジュール**］を選択します。
6. ［**チャンネル**］フィールドで、モジュールを取得するモジュラーチャンネルを選択します。このドロップダウンには、モジュラーチャンネルのみが表示されます。
7. **[保存]**をクリックして、フィルタを作成します。
8. ［**フィルタ**］セクションまでスクロールして、新しく割り当てられたAppStreamフィルタを確認します。
9. 個々のフィルタを編集/削除して、ニーズに合わせてプロジェクトを調整できます。

8.4. Build a content lifecycle project

プロジェクトを作成し、環境を定義し、ソースとフィルタを割り当てたら、初めてプロジェクトを構築でき

ます。

構築によって、割り当てられたソースにフィルタが適用され、プロジェクトの最初の環境にそれらが複製されます。

複数のコンテンツプロジェクトのソースとして同じベンダチャンネルを使用できます。　この場合、SUSE Multi-Linux Managerはクローンチャンネルごとに新しいパッチクローンを作成しません。 代わりに、1つのパッチクローンがすべてのクローンチャンネル間で共有されます。 これにより、パッチが撤回された場合やパッチ内のパッケージが変更された場合など、ベンダがパッチを変更すると問題が発生する可能性があります。　コンテンツプロジェクトの1つを構築すると、コンテンツプロジェクトの他の環境や組織内の他のコンテンツプロジェクトチャンネルにチャンネルがある場合でも、クローンパッチを共有するすべてのチャンネルがデフォルトでオリジナルと同期されます。 この動作は、組織の設定で自動パッチ同期をオフにすることで変更できます。 パッチを共有しているすべてのチャンネルのパッチを後で手動で同期するには、**ソフトウェア › 管理 › チャンネル**に移動し、同期するチャンネルをクリックして、［**同期**］サブタブに移動します。パッチを手動で同期しても、パッチを共有するすべての組織チャンネルに影響します。

Procedure: Building a content lifecycle project

1. SUSE Multi-Linux Manager Web UIで、**コンテンツライフサイクル › プロジェクト**に移動し、構築するプロジェクトを選択します。

   プロジェクトを構築する前に、利用可能な環境があることを確認してください。

2. 割り当てられたソースとフィルタを確認し、**[ビルド]**をクリックします。
3. このビルドの変更または更新を説明するバージョンメッセージを提供します。
4. ［**環境ライフサイクル**］セクションでビルドの進行状況を監視できます。

ビルドが完了すると、環境バージョンが1つ増え、ソフトウェアチャンネルなどのビルドソースをクライアントに割り当てることができます。

8.5. Promote environments

プロジェクトが構築されると、構築されたソースを順次、環境にプロモートできます。

Procedure: Promoting environments

1. SUSE Multi-Linux Manager Web UIで、**コンテンツライフサイクル › プロジェクト**に移動し、作業するプロジェクトを選択します。
2. ［**環境ライフサイクル**］セクションで、後継環境にプロモートする環境を見つけ、**[Promote]**（プロモート）をクリックします。

3. ［**環境ライフサイクル**］セクションでビルドの進行状況を監視できます。

8.6. Assign clients to environments

コンテンツライフサイクルプロジェクトを構築およびプロモートすると、SUSE Multi-Linux Managerはソフトウェアチャンネルのツリーを作成します。 クライアントを環境に追加するには、クライアントの［**システムの詳細**］ページの**ソフトウェア › ソフトウェアチャンネル**を使用して、ベースソフトウェアチャンネルと子ソフトウェアチャンネルをクライアントに割り当てます。

新たに追加されたクローンチャンネルはクライアントに自動的に割り当てられません。ソースを追加またはプロモートする場合は、チャンネル割り当てを手動で確認して更新する必要があります。

自動割り当ては、今後のバージョンでSUSE Multi-Linux Managerに追加される予定です。

8.7. コンテンツライフサイクル管理の例

このセクションでは、コンテンツライフサイクル管理の使用方法の一般的な例をいくつか示します。 これらの例を使用して、独自にカスタマイズされた実装を構築します。

8.7.1. 月次パッチサイクルのプロジェクトの作成

月次パッチサイクルのプロジェクト例は、以下で構成されます。

- **By Date**（日付別）フィルタの作成
- プロジェクトへのフィルタの追加
- 新しいプロジェクトビルドへのフィルタの適用
- プロジェクトからのパッチの除外
- プロジェクトにパッチを含める

8.7.1.1. By Date（日付別）フィルタの作成

指定した日付以降にリリースされたすべてのパッチは**By Date**（日付別）フィルタによって除外されます。このフィルタは、月次パッチサイクルに従うコンテンツライフサイクルプロジェクトに役立ちます。

Procedure: Creating the By Date filter

1. SUSE Multi-Linux Manager Web UIで、**コンテンツライフサイクル › フィルタ**に移動して、**[Create Filter]**（フィルタの作成）をクリックします。
2. ［**フィルタ名**］フィールドに、フィルタの名前を入力します。 たとえば、**Exclude patches by date**（日付別にパッチを除外する）。

3. ［**フィルタタイプ**］フィールドで、［**Patch (Issue date)**］（パッチ(発行日)）を選択します。
4. ［**マッチャー**］フィールドでは、［**later or equal**］（それ以降）が自動選択されます。
5. 日時を選択します。
6. [**保存**]をクリックします。

8.7.1.2. Add a filter to the project

Procedure: Adding a filter to a project

1. SUSE Multi-Linux Manager Web UIで、**コンテンツライフサイクル › プロジェクト**に移動して、リストからプロジェクトを選択します。
2. [**フィルタの割り当て／取り外し**]リンクをクリックして、すべての使用可能なフィルタを表示します
3. 新しい［**Exclude patches by date**］（日付別にパッチを除外する）を選択します。
4. [**保存**]をクリックします。

8.7.1.3. Apply a filter to a new project build

新しいフィルタがフィルタリストに追加されますが、プロジェクトに適用する必要があります。 フィルタを適用するには、最初の環境を構築する必要があります。

Procedure: Using the filter

1. [**ビルド**]をクリックして、最初の環境を構築します。
2. オプション: メッセージを追加します。 メッセージを使用して、ビルド履歴を追跡できます。
3. テストサーバで新しいチャンネルを使用して、フィルタが正しく機能していることを確認します。
4. [**Promote**]（プロモート）をクリックして、次の環境にコンテンツを移動します。 多数のフィルタがある場合、または非常に複雑な場合は、ビルドに時間がかかります。

8.7.1.4. Exclude a patch from the project

テストは、問題を発見するのに役立つ場合があります。 問題が見つかった場合は、**by date**（日付別）フィルタの前にリリースされた問題のパッチを除外します。

Procedure: Excluding a patch

1. SUSE Multi-Linux Manager Web UIで、**コンテンツライフサイクル › フィルタ**に移動して、**[Create Filter]**（フィルタの作成）をクリックします。
2. ［ **フィルタ名**］フィールドに、フィルタの名前を入力します。 たとえば、［**Exclude openjdk patch**］（openjdkパッチの除外）。
3. ［**フィルタタイプ**］フィールドで、［**Patch (Advisory Name)**］（パッチ(アドバイザリ名)）を選択します。
4. ［ **マッチャー**］フィールドで、［**等しい**］を選択します。
5. ［**アドバイザリ名**］フィールドに、アドバイザリの名前を入力します。 たとえば、**SUSE-15-2019-1807**。
6. **[保存]**をクリックします。
7. **コンテンツライフサイクル › プロジェクト**に移動して、プロジェクトを選択します。
8. **[フィルタの割り当て／取り外し]**リンクをクリックして、［**Exclude openjdk patch**］（openjdkパッチの除外）を選択し、**[保存]**をクリックします。

[ビルド]ボタンを使用してプロジェクトを再構築すると、新しいフィルタが、以前に追加した［ **by date**］（日付別）フィルタとともに使用されます。

8.7.1.5. Include a patch in the project

この例では、セキュリティアラートを受信しています。 重要なセキュリティパッチが、現在作業している月の最初の日から数日後にリリースされました。 新しいパッチの名前は**SUSE-15-2019-2071**です。 この新しいパッチを環境に含める必要があります。

［**許可**］フィルタ規則は、［**拒否**］フィルタ規則の除外機能を上書きします。 詳細については、**Administration › Content-lifecycle**を参照してください。

Procedure: Including a patch in a project

1. SUSE Multi-Linux Manager Web UIで、**コンテンツライフサイクル › フィルタ**に移動して、**[Create Filter]**（フィルタの作成）をクリックします。
2. ［**フィルタ名**］フィールドに、フィルタの名前を入力します。 たとえ

ば、**Include kernel security fix**（カーネルセキュリティ修正を含める）。

3. ［**フィルタタイプ**］フィールドで、［**Patch (Advisory Name)**］（パッチ(アドバイザリ名)）を選択します。
4. ［**マッチャー**］フィールドで、［**等しい**］を選択します。
5. ［**アドバイザリ名**］フィールドに、「**SUSE-15-2019-2071**」と入力し、［**許可**］をオンにします。
6. **[保存]**をクリックして、フィルタを保存します。
7. **コンテンツライフサイクル › プロジェクト**に移動して、リストからプロジェクトを選択します。
8. **[フィルタの割り当て／取り外し]**をクリックして、［**Include kernel security patch**］（カーネルセキュリティパッチを含める）を選択します。
9. **[保存]**をクリックします。
10. **[ビルド]**をクリックして、環境を再構築します。

8.7.2. Update an existing monthly patch cycle

月次パッチサイクルが完了すると、次の月のパッチサイクルを更新できます。

Procedure: Updating a monthly patch cycle

1. ［**by date**］（日付別）フィールドで、フィルタの日付を次の月に変更します。　または、新しいフィルタを作成して、プロジェクトへの割り当てを変更します。
2. **SUSE-15-2019-1807**の除外フィルタをプロジェクトから取り外すことができるかどうか確認します。　この問題を解決するために使用できる新しいパッチがある場合があります。
3. 以前に追加した［**許可**］フィルタを取り外します。 パッチはデフォルトで含まれています。
4. プロジェクトを再構築して、来月のパッチを適用した新しい環境を作成します。

8.7.3. Enhance a project with live patching

このセクションでは、ライブパッチ処理用の環境を作成するためのフィルタの設定について説明します。

When you are preparing to use live patching, there are some important considerations:

- システムでカーネルバージョンを1つだけ使用してください。 ライブパッチ処理パッケージは、特定のカーネルとともにインストールされます。
- ライブパッチ処理の更新は、1つのパッチとして出荷されます。
- 新しいシリーズのライブパッチ処理カーネルを開始するカーネルパッチごとに、**要再起動**フラグが表示されます。 これらのカーネルパッチには、ライブパッチ処理ツールが付属しています。 それらをインストールしたら、翌年になる前に少なくとも1回システムを再起動する必要があります。
- インストール済みカーネルバージョンに一致するライブパッチ更新のみをインストールします。
- ライブパッチは、スタンドアロンパッチとして提供されます。 現在インストールされているカーネルバージョンよりも新しいカーネルバージョンの通常のカーネルパッチをすべて除外する必要があります。

8.7.3.1. Exclude packages with a higher kernel version

この例では、**SUSE-15-2019-1244**パッチでシステムを更新します。 このパッチには、**kernel-default-4.12.14-150.17.1-x86_64**が含まれています。

より新しいバージョンの**kernel-default**と**kernel-default-base**を含むすべてのパッチを除外する必要があります。

Procedure: Excluding packages with a higher kernel version

1. SUSE Multi-Linux Manager Web UIで、**コンテンツライフサイクル › フィルタ**に移動して、**[Create Filter]**（フィルタの作成）をクリックします。
2. ［**フィルタ名**］フィールドに、フィルタの名前を入力します。 たとえば、**Exclude kernel greater than 4.12.14-150.17.1**（4.12.14-150.17.1より新しいカーネルを除外する）。
3. ［**フィルタタイプ**］フィールドで、［**Patch (Contains Package)**］（パッチ(パッケージを含む)）を選択します。
4. ［**マッチャー**］フィールドで、［**version greater than**］（指定したものより新しいバージョン）を選択します。
5. ［**パッケージ名**］フィールドに、「**kernel-default**」と入力します。
6. ［**エポック**］フィールドを空のままにします。
7. ［**バージョン**］フィールドに、「**4.12.14**」と入力します。

8. ［**リリース**］フィールドに、「**150.17.1**」と入力します。
9. **[保存]**をクリックして、フィルタを保存します。
10. **コンテンツライフサイクル › プロジェクト**に移動して、プロジェクトを選択します。
11. **[フィルタの割り当て／取り外し]**をクリックします。
12. ［**Exclude kernel greater than 4.12.14-150.17.1**］（4.12.14-150.17.1より新しいカーネルを除外する）を選択して、**[保存]**をクリックします。

kernel-default-baseパッケージについても、この手順を繰り返す必要があります。

[ビルド]をクリックすると、新しい環境が作成されます。 新しい環境には、インストールしたバージョンまでのすべてのカーネルパッチが含まれています。

より新しいカーネルバージョンのすべてのカーネルパッチは削除されます。 ライブパッチ処理カーネルは、シリーズの最初でない限り、引き続き使用できます。

このプロシージャはフィルタテンプレートを使用して自動化できます。 ライブパッチ処理フィルタテンプレートの適用方法の詳細については、administration:content-lifecycle.pdfを参照してください。

8.7.4. Switch to a new kernel version for live patching

Live patching for a specific kernel version is only available for one year. After one year you must update the kernel on your systems. Execute these environment changes:

Procedure: Switch to a new kernel version

1. アップグレードするカーネルバージョンを決定します。 例: **4.12.14-150.32.1**
2. 新しいカーネルバージョンフィルタを作成します。
3. Detach all previous Live Patching filters associated with the old kernel.
4. Attach the new kernel version filter.
5. **[ビルド]**をクリックして、環境を再構築します。

Once the build is complete, you must immediately re-attach the two filters which:

- **reboot_suggested**キーワードを含むパッチを拒否する
- **installhint(reboot-needed)**という名前を提供するパッケージを含むパッチを拒否する

The new environment contains all kernel patches up to the new kernel version you selected. You need to reboot systems after they have performed the upgrade. The new kernel remains valid for one year. All packages installed during the year match the current live patching kernel filter.

8.7.5. AppStream filters

コンテンツライフサイクル管理プロジェクトでは、AppStreamフィルタを使用して、モジュラーリポジトリを通常のリポジトリに変換できます。これはパッケージをリポジトリに保持し、モジュールのメタデータを削除することにより行われます　。その結果作成されたリポジトリは、通常のリポジトリと同じ方法でSUSE Multi-Linux Managerで使用できます。

したがって、このプロセスはAppStreamリポジトリを操作するために必須ではありません。

AppStreamフィルタはターゲットリポジトリに含める単一のモジュールストリームを選択します。 複数のフィルタを追加して、複数のモジュールストリームを選択できます。

CLMプロジェクトでAppStreamフィルタを使用しない場合は、モジュラーソースのモジュールメタデータは未加工のままで、ターゲットリポジトリには同じモジュールメタデータが含まれます。 CLMプロジェクトで少なくとも1つのAppStreamフィルタが有効になっている限り、すべてのターゲットリポジトリが通常のリポジトリに変換されます。

場合によっては、どのモジュールのパッケージも含めずに通常のリポジトリを構築したい場合があります。これを行うには、マッチャー　**なし　(モジュール化を無効にする)**を使用して　AppStreamフィルタを追加します。 これにより、ターゲットリポジトリ内のすべてのモジュールが無効になります。 これは、ほとんどのモジュールのデフォルトバージョンが通常のパッケージとしてAppStreamリポジトリにすでに含まれている、Red Hat Enterprise Linux 9のクライアントに特に役立ちます。

AppStreamフィルタを使用するには、**Red Hat Enterprise Linux AppStreams**などのモジュラーリポジトリを含むCLMプロジェクトが必要です。 開始する前に、必要なモジュールがソースとして含まれていることを確認してください。

Procedure: Using AppStream filters

1. SUSE Multi-Linux Manager Web UIで、Red Hat Enterprise Linux 8または9 CLMプロジェクトに移動します。 プロジェクトにAppStreamチャンネルが含まれていることを確認します。
2. **[Create Filter]** (フィルタの作成)をクリックし、次のパラメータを使用します。
   - ［**フィルタ名**］フィールドには、新しいフィルタの名前を入力します。
   - ［**フィルタタイプ**］フィールドで、［**Module (Stream)**］（モジュール(ストリーム)）を選択します。
   - ［**マッチャー**］フィールドで、［**等しい**］を選択します。

- ［**モジュール名**］フィールドに、モジュール名を入力します。 たとえば、**postgresql**。
- ［**ストリーム**］フィールドに、目的のストリームの名前を入力します。 たとえば、**10**。 このフィールドを空のままにする場合、モジュールのデフォルトのストリームが選択されます。

3. **[保存]**をクリックして、新しいフィルタを作成します。
4. **コンテンツライフサイクル › プロジェクト**に移動して、プロジェクトを選択します。
5. **[フィルタの割り当て／取り外し]**をクリックし、新しいAppStreamフィルタを選択して、**[保存]**をクリックします。

［**Create/Edit Filter**］（フィルタの作成/編集）フォームのブラウズ機能を使用して、モジュラーチャンネルで使用可能なモジュールストリームのリストからモジュールを選択できます。

Procedure: Browsing available module streams

1. SUSE Multi-Linux Manager Web UIで、Red Hat Enterprise Linux 8または9 CLMプロジェクトに移動します。 プロジェクトにAppStreamチャンネルが含まれていることを確認します。
2. **[Create Filter]** (フィルタの作成)をクリックし、次のパラメータを使用します。
   - ［**フィルタ名**］フィールドには、新しいフィルタの名前を入力します。
   - ［**フィルタタイプ**］フィールドで、［**Module (Stream)**］（モジュール(ストリーム)）を選択します。
   - ［**マッチャー**］フィールドで、［**等しい**］を選択します。
3. ［**Browse available modules**］（使用可能なモジュールをブラウズ）をクリックして、すべてのモジュラーチャンネルを表示します。
4. モジュールとストリームをブラウズするチャンネルを選択します。
   - ［**モジュール名**］フィールドで、検索するモジュール名の入力を開始するか、リストから選択します。
   - ［**ストリーム**］フィールドで、検索するストリーム名の入力を開始するか、リストから選択します。

チャンネル選択はモジュールのブラウズのみを目的としています。 選択したチャンネル

> はフィルタとともに保存されず、CLMプロセスには影響しません。

ターゲットリポジトリに含める他のモジュールストリーム用に追加のAppStreamフィルタを作成できます。選択したストリームが依存するモジュールストリームは自動的に含まれます。

> 競合する、互換性のない、または欠落しているモジュールストリームを指定しないように注意してください。　たとえば、同じモジュールから2つのストリームを選択すると無効になります。

Procedure: Disabling modularity

1. SUSE Multi-Linux Manager Web UIで、Red Hat Enterprise Linux 8または9 CLMプロジェクトに移動します。 プロジェクトにAppStreamチャンネルが含まれていることを確認します。
2. **[Create Filter]** (フィルタの作成)をクリックし、次のパラメータを使用します。
   - ［**フィルタ名**］フィールドには、新しいフィルタの名前を入力します。
   - ［**フィルタタイプ**］フィールドで、［**Module (Stream)**］（モジュール(ストリーム)）を選択します。
   - ［**マッチャー**］フィールドで、［**なし (モジュール化を無効にする)**］を選択します。
3. **[保存]**をクリックして、新しいフィルタを作成します。
4. **コンテンツライフサイクル › プロジェクト**に移動して、プロジェクトを選択します。
5. **[フィルタの割り当て／取り外し]**をクリックし、新しいAppStreamフィルタを選択して、**[保存]**をクリックします。

これにより、モジュールに属するパッケージを除いて、モジュールのメタデータがターゲットリポジトリから効率的に削除されます。

Web UIの**[ビルド]**ボタンを使用してCLMプロジェクトを構築する場合、ターゲットリポジトリは、選択したモジュールストリームからのパッケージを含む、モジュールを含まない通常のリポジトリです。

> Red Hat Enterprise Linux 8のプロジェクトでモジュール化を完全に無効にすると、一部のモジュールが Red Hat Enterprise Linux 8での正常な動作に不可欠であるため、環境に不具合が生じる可能性があります。

Chapter 9. コンテンツのステージング

ステージングは、クライアントがインストール前にパッケージを事前にダウンロードするために使用されます。 これにより、パッケージのインストールをスケジュールされたらすぐに開始できるため、メンテナンスウィンドウに必要な時間を短縮できます。

9.1. コンテンツステージングの有効化

組織全体のコンテンツステージングを管理できます。 SUSE Multi-Linux Manager Web UIで、**管理 › 組織**に移動して、使用可能な組織のリストを表示します。 組織の名前をクリックし、［**ステージングコンテンツの有効化**］ ボックスをオンにして、この組織のクライアントがパッケージデータをステージングできるようにします。

組織を作成および管理するには、SUSE Multi-Linux Manager管理者としてログインする必要があります。

/etc/sysconfig/rhn/up2dateを編集し、次の行を追加または編集して、コマンドプロンプトでステージングを有効にすることもできます。

```
stagingContent=1
stagingContentWindow=24
```

stagingContentWindowパラメータは時間単位で表される時間値で、ダウンロードの開始時間を決定します。 これは、スケジュールされたインストールまたは更新時間までの時間数です。 この例では、インストール時間の24時間前にコンテンツがダウンロードされます。 ダウンロードの開始時間は、システムで選択した連絡方法によって異なります。

次回、アクションがスケジュールされると、パッケージは自動的にダウンロードされますが、インストールはされません。 スケジュールされた時間に、ステージングされたパッケージがインストールされます。

9.2. コンテンツステージングの設定

コンテンツステージングを設定するために使用される次の2つのパラメータがあります。

- **salt_content_staging_advance**は、コンテンツステージングウィンドウが開くまでの時間です(時間単位)。 これは、インストールが開始されるまでの時間数で、この時間に達するとパッケージのダウンロードを開始できます。
- **salt_content_staging_window**は、コンテンツステージングウィンドウの期間(時間単位)です。 これは、インストールが開始されるまでにクライアントがパッケージをステージングする必要がある時間数です。

たとえば **salt_content_staging_advance**が6時間に設定されていて、**salt_content_staging_window**が2時間に設定されている場合、ステージングウィンドウはインストール時間の6時間前に開き、2時間開いたままになります。 インストールが開始されるまで、残りの4時間以内にパッケージはダウンロードされません。

salt_content_staging_advanceおよび**salt_content_staging_window**の両方に同じ値を設定する場合、イ

ンストールが開始されるまでパッケージをダウンロードできます。

/usr/share/rhn/config-defaults/rhn_java.confで、コンテンツステージングパラメータを設定します。

デフォルト値:

- **salt_content_staging_advance: 8 hours**
- **salt_content_staging_window: 8 hours**

これらのパラメータを正しく機能させるには、コンテンツステージングを有効にする必要があります。

Chapter 10. 切断されたセットアップ

SUSE Multi-Linux Managerは、インターネット接続できない場合は、切断された環境で使用できます。

リポジトリミラーリングツール(RMT)はSUSE Linux Enterprise 15以降で使用できます。 RMTは、古いSUSE Linux Enterpriseインストールで使用できる、サブスクリプション管理ツール(SMT)に代わるものです。

切断されたSUSE Multi-Linux Managerセットアップでは、RMTまたはSMTは外部ネットワークを使用してSUSE Customer Centerに接続します。 すべてのソフトウェアチャンネルとリポジトリは、リムーバブルストレージデバイスに同期されます。 その後、ストレージデバイスを使用して、切断されたSUSE Multi-Linux Managerのインストールを更新できます。

このセットアップにより、SUSE Multi-Linux Managerのインストールをオフラインで、切断された環境のままにできます。

SUSE Multi-Linux Managerサーバを直接管理するには、RMTまたはSMTインスタンスを使用する必要があります。 カスケードで2番目のRMTまたはSMTインスタンスを管理するために使用することはできません。

RMTの詳細については、https://documentation.suse.com/sles/15-SP6/html/SLES-all/book-rmt.htmlを参照してください。

10.1. SCCからチャンネルとリポジトリを同期する

10.1.1. RMTの同期

SUSE Linux Enterprise 15インストールでRMTを使用して、SUSE Linux Enterprise 12以降を実行しているクライアントを管理できます。

SUSE Multi-Linux Managerのインストールごとに専用RMTインスタンスを設定することをお勧めします。

プロシージャ: RMTの設定

1. RMTインスタンスで、RMTパッケージをインストールします。

```
zypper in rmt-server
```

2. YaSTを使用してRMTを設定します。

```
yast2 rmt
```

3. プロンプトに従ってインストールを完了します。

RMTの設定の詳細については、https://documentation.suse.com/sles/15-SP6/html/SLES-all/book-rmt.htmlを参照してください。

プロシージャ: RMTとSCCの同期

1. RMTインスタンスで、組織で使用可能なすべての製品とリポジトリを一覧にします。

```
rmt-cli products list --all
rmt-cli repos list --all
```

2. 組織で使用可能なすべての更新を同期します。

```
rmt-cli sync
```

systemdを使用して定期的に同期するようにRMTを設定することもできます。

3. 必要な製品を有効にします。 たとえば、SLES 15を有効にするには、次のようにします。

```
rmt-cli product enable sles/15/x86_64
```

4. リムーバブルストレージに同期されたデータをエクスポートします。 この例では、ストレージメディアは**/mnt/usb**にマウントされます。

```
rmt-cli export data /mnt/usb
```

5. リムーバブルストレージに有効なリポジトリをエクスポートします。

```
rmt-cli export settings /mnt/usb
rmt-cli export repos /mnt/usb
```

外部ストレージが、RMTユーザが書き込み可能なディレクトリにマウントされていることを確認します。 RMTユーザ設定は、**/etc/rmt.conf**の**cli**セクションで変更できます。

10.1.2. SMTの同期

SMTはSUSE Linux Enterprise 12に含まれ、SUSE Linux Enterprise 10以降を実行しているクライアントを管理するために使用できます。

SMTでは、リポジトリとパッケージを同期するために、SMTインスタンス上にローカルミラーディレクトリを作成する必要があります。

SMTのインストールおよび設定に関する詳細については、https://documentation.suse.com/sles/12-SP5/html/SLES-all/book-smt.htmlを参照してください。

プロシージャ: SMTとSCCの同期

1. SMTインスタンスで、データベース置換ファイルを作成します。

```
smt-sync --createdbreplacementfile /tmp/dbrepl.xml
```

2. 同期されたデータをリムーバブルストレージにエクスポートします。この例では、ストレージメディアは**/mnt/usb**にマウントされます。

```
smt-sync --todir /mnt/usb
smt-mirror --dbreplfile /tmp/dbrepl.xml --directory /mnt/usb \
           --fromlocalsmt -L /var/log/smt/smt-mirror-export.log
curl https://scc.suse.com/multi-linux-manager/product_tree.json -o
/mnt/usb/product_tree.json
```

外部ストレージがRMTユーザによって書き込み可能なディレクトリにマウントされていることを確認します。 **/etc/smt.conf**のSMTユーザ設定を変更できます。

10.2. 必須チャンネル

SUSE Multi-Linux Managerが指定されたチャンネルを同期できるようにするには、対応するSUSE Multi-Linux Managerクライアントツールチャンネルが必要です。 これらのチャンネルが有効でない場合、SUSE Multi-Linux Managerはその製品を検出できない場合があります。

次のコマンドを実行して、これらの必須チャンネルを有効にします。

SLES 12およびSLES for SAPやSLE HPCなどのSLES 12に基づく製品

RMT: **rmt-cli products enable sle-manager-tools/12/x86_64**

SMT: **smt repos -p sle-manager-tools,12,x86_64**

SLES 15およびSLES for SAPやSLE HPCなどのSLES 15に基づく製品

RMT: **rmt-cli products enable sle-manager-tools/15/x86_64**

SMT: **smt repos -p sle-manager-tools,15,x86_64**

次に、チャンネルをミラーリングしてエクスポートします。

他のディストリビューションまたはアーキテクチャを有効にすることができます。 製品チャンネルまたはリポジトリのミラーリングを有効にする方法の詳細については、次のドキュメントを参照してください。

RMT

https://documentation.suse.com/sles/15-SP6/html/SLES-all/cha-rmt-mirroring.html#sec-rmt-mirroring-enable-disable

SMT

https://documentation.suse.com/sles/12-SP5/single-html/SLES-smt/index.html#smt-mirroring-manage-domirror

10.3. 切断されたサーバ

SUSE Multi-Linux Managerを切断されたサーバとして設定するには、 Air-gapped配備の手順に従ってください。

10.3.1. 配備

提供されたイメージを使用して、切断されたサーバを仮想マシン(VM)として配備することをお勧めします。SUSE Multi-Linux Managerサーバ のAir-gapped配備については、**Installation-and-upgrade › Container-deployment**を参照してください。

--mirrorオプションを指定して最後のコマンドを実行し、 **</media/disk>**をマウントポイントに置き換えることを忘れないでください。

```
mgradm install podman --mirror </media/disk>
```

10.3.2. 同期

SUSE Customer Centerデータでロードされたリムーバブルメディアがある場合は、それを使用して切断されたサーバを同期できます。

同期に使用するリムーバブルメディアは常に同じマウントポイントで使用できる必要があります。 ストレージメディアがマウントされていない場合は、同期をトリガしないでください。 これにより、データが破損します。

プロシージャ: 切断されたサーバの同期

1. Tomcatサービスを再起動します。

```
mgrctl exec -ti -- systemctl restart tomcat
```

2. ローカルデータを更新します。

```
mgrctl exec -ti -- mgr-sync refresh
```

3. 同期を実行します。

```
mgrctl exec -ti -- mgr-sync list channels
mgrctl exec -ti -- mgr-sync add channel channel-label
```

server.susemanager.fromdirが設定されている場合、SUSE Multi-Linux Manager はSUSE Customer Center資格情報が有効かどうかを確認できないことに注意してください。 代わりに、警告サインが表示され、SCCオンラインチェックは実行されません。

切断されたセットアップの代替案として、サーバ間同期(ISS)を使用してサーバ間でコンテンツをコピーする方法があります。 詳細については、**Specialized-guides › Large-deployments**を参照してください。

Chapter 11. ディスク容量管理

ディスク容量が不足すると、SUSE Multi-Linux Managerデータベースとファイル構造に深刻な影響を及ぼす可能性があり、場合によっては回復できなくなります。

SUSE Multi-Linux Managerは、空きディスク容量のために一部のディレクトリを監視します。 監視するディレクトリと作成される警告を変更できます。 すべての設定は、**/etc/rhn/rhn.conf**設定ファイルで行われます。

監視対象ディレクトリのいずれかの使用可能容量が警告しきい値を下回ると、設定された電子メールアドレスにメッセージが送信され、サインインページの上部に通知が表示されます。

11.1. 監視対象ディレクトリ

デフォルトでは、SUSE Multi-Linux Managerは以下のディレクトリを監視します。

- **/var/lib/pgsql**
- **/var/spacewalk**
- **/var/cache**
- **/srv**

監視するディレクトリは、**spacecheck_dirs**パラメータで変更できます。 スペースで区切って、複数のディレクトリを指定できます。

例:

```
spacecheck_dirs = /var/lib/pgsql /var/spacewalk /var/cache /srv
```

For more information about volumes, see **Installation-and-upgrade › Container-management**.

11.2. しきい値

デフォルトでは、SUSE Multi-Linux Managerは、監視対象ディレクトリで使用可能な合計容量の10%未満になると警告を作成します。 また、監視対象ディレクトリの空き容量が5%未満になると、クリティカルアラートが作成されます。

これらのアラートしきい値は**spacecheck_free_alert**および**spacecheck_free_critical**パラメータを使用して変更できます。

例:

```
spacecheck_free_alert = 10
spacecheck_free_critical = 5
```

11.3. サービスのシャットダウン

デフォルトでは、クリティカルアラートしきい値に達すると、SUSE Multi-Linux Managerはspacewalkサービスをシャットダウンします。

この動作は、**spacecheck_shutdown**パラメータで変更できます。 **true**の値はシャットダウン機能を有効にします。 その他の値は無効にします。

例:

```
spacecheck_shutdown = true
```

11.4. スペースチェックの無効化

スペースチェックツールはデフォルトで有効になっています。 次のコマンドを使用して完全に無効にできます。

```
systemctl stop spacewalk-diskcheck.timer
systemctl disable spacewalk-diskcheck.timer
```

spacewalk-diskcheck.timerを無効にすると、アラートのしきい値に達した場合に定期的な電子メールアラートが停止しますが、警告通知はサインインページの上部に表示されます。

Chapter 12. イメージの構築と管理

12.1. イメージの構築の概要

SUSE Multi-Linux Managerでは、システム管理者はコンテナおよびOSイメージを構築し、結果をイメージストアにプッシュできます。

プロシージャ: イメージの構築とプッシュ

1. イメージストアを定義します。
2. イメージプロファイルを定義し、それをソース(gitリポジトリまたはディレクトリのいずれか)に関連付けます。
3. イメージを構築します。
4. イメージをイメージストアにプッシュします。

SUSE Multi-Linux Managerでは、次の2つのビルドタイプ(DockerfileおよびKiwiビルドタイプ)をサポートしています。 Kiwiビルドタイプは、システムイメージ、仮想イメージ、およびその他のイメージの構築に使用されます。

The image store for the Kiwi build type is pre-defined as a file system directory in the **srv-www** volume.

The image files can be downloaded from https://MANAGER-HOST/os-images/ORGANIZATION-ID/FILE-NAME. The exact location can be determined from the image details page.

12.2. コンテナイメージ

12.2.1. 要件

コンテナ機能は、SUSE Linux Enterprise Server 12以降を実行しているSaltクライアントで使用できます。開始する前に、ご使用の環境が次の要件を満たしていることを確認してください。

- Dockerfileと設定スクリプトを含む発行済みのgitリポジトリ。 リポジトリはパブリックにもプライベートにもでき、GitHub、GitLab、またはBitBucketでホストする必要があります。
- Dockerレジストリなどの適切に設定されたイメージストア。

コンテナの詳細については、https://documentation.suse.com/container/all/html/Container-guide/を参照してください。

12.2.2. 構築ホストの作成

SUSE Multi-Linux Managerでイメージを構築するには、構築ホストを作成して設定する必要があります。 コンテナビルドホストは、SUSE Linux Enterprise 12以降を実行しているSaltクライアントです。 このセクションでは、構築ホストの初期設定について説明します。

構築ホスト上のオペレーティングシステムは、ターゲットイメージ上のオペレーティングシステムと一致する必要があります。

たとえば、SUSE Linux Enterprise Server 15 (SP2以降)のOSバージョンを実行している構築ホスト上にSUSE Linux Enterprise Server 15ベースのイメージを構築します。 SUSE Linux Enterprise Server 12 SP5またはSUSE Linux Enterprise Server 12 SP4 OSバージョンを実行している構築ホスト上にSUSE Linux Enterprise Server 12ベースのイメージを構築します。

クロスアーキテクチャビルドはサポートされていません。

SUSE Multi-Linux Manager Web UIから、次のステップを実行して、構築ホストを設定します。

プロシージャ: ホストの構築

1. **システム › システム**概要ページから、構築ホストとして指定されるSaltクライアントを選択します。
2. 選択したクライアントの［**システムの詳細**］ページから、コンテナモジュールを割り当てます。 **ソフトウェア › ソフトウェアチャンネル**に移動して、コンテナモジュール(たとえば、［**SLE-Module-Containers15-Pool**］と［**SLE-Module-Containers15-Updates**］)を有効にします。 **[次へ]**で続行します。
3. ［**ソフトウェアチャンネルの変更**］をスケジュールし、**[確認]**をクリックします。
4. ［**システムの詳細**］タブから、**プロパティ**ページを選択し、［**付属エンタイトルメント**］リストから**コンテナビルドホスト**を有効にします。 **[プロパティの更新]**をクリックして確定します。
5. **highstate**を適用して必要なすべてのパッケージをインストールします。 システムの詳細タブで、**状態 › highstate**を選択し、**[highstateの適用]**をクリックします。 または、SUSE Multi-Linux Managerサーバのコマンドラインから**highstate**を適用します。

```
salt '$your_client' state.highstate
```

12.2.3. コンテナ用アクティベーションキーの作成

SUSE Multi-Linux Managerを使用して構築されたコンテナは、イメージを構築するときに、アクティベーションキーに関連付けられたチャンネルをリポジトリとして使用します。 このセクションでは、この目的のためにアドホックアクティベーションキーを作成する方法について説明します。

コンテナを構築するには、**SUSE Manager Default**以外のチャンネルに関連付けられているアクティベーションキーが必要です。

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**を選択します。
2. **[キーの作成]**をクリックします。
3. ［**説明**］と［**キー**］名を入力します。　ドロップダウンメニューを使用してこのキーと関連付ける［**ベースチャンネル**］を選択します。
4. **[アクティベーションキーの作成]**で確定します。

詳細については、**Client-configuration › Activation-keys**を参照してください。

12.2.4. イメージストアの作成

All built images are pushed to an image store. This section contains information about creating an image store. Image store is generally referenced as a registry.

プロシージャ: イメージストアの作成

1. **イメージ › ストア**を選択します。
2. ［**作成**］をクリックして、新しいストアを作成します。
3. ［**ストアの種類**］から正しい種類を選択します。
4. ［**ラベル**］フィールドにイメージストアの名前を定義します。
5. コンテナレジストリホスト(内部か外部)の完全修飾ドメイン名(FQDN)として、［**URI**］フィールドに入力して、イメージレジストリへのパスを指定します。

   ```
   registry.example.com
   ```

   レジストリURI を使用して、すでに使用されているレジストリのイメージストアを指定することもできます。

   ```
   registry.example.com:5000/myregistry/myproject
   ```

6. **[作成]**をクリックして、新しいイメージストアを追加します。

12.2.5. イメージプロファイルの作成

すべてのコンテナイメージは、構築手順を含む、イメージプロファイルを使用して構築されます。　このセクションでは、SUSE Multi-Linux Manager Web UIでイメージプロファイルを作成する方法について説明します。

プロシージャ: イメージプロファイルの作成

1. イメージプロファイルを作成するには、**イメージ › プロファイル**を選択し、**[作成]**をクリックします。
2. ［**ラベル**］フィールドに入力して、イメージプロファイルの名前を指定します。

コンテナイメージタグが**myproject/myimage**などの形式である場合は、イメージストアのレジストリURIに**/myproject**サフィックスが含まれていることを確認します。

3. ［**イメージタイプ**］として［**Dockerfile**］を使用します。
4. ドロップダウンメニューを使用して、［**ターゲットのイメージストア**］フィールドからレジストリを選択します。
5. ［**パス**］フィールドに、GitHub、GitLab、またはBitBucketリポジトリのURLを入力します。 パスは構築ホスト上のローカルディレクトリにすることもできます。 URLは**http**、**https**、またはトークン認証URLである必要があります。 GitHubまたはGitLabの場合は、以下の形式のいずれかを使用します。

GitHubパスオプション

- GitHubシングルユーザプロジェクトリポジトリ

```
https://github.com/USER/project.git#branchname:folder
```

- GitHub組織プロジェクトリポジトリ

```
https://github.com/ORG/project.git#branchname:folder
```

- GitHubトークン認証

  gitリポジトリがプライベートな場合、認証を含むようにプロファイルのURLを変更します。 GitHubトークンで認証するには次のURL形式を使用します。

```
https://USER:<AUTHENTICATION_TOKEN>@github.com/USER/project.git#master:/container/
```

- GitLabシングルユーザプロジェクトリポジトリ

```
https://gitlab.example.com/USER/project.git#master:/container/
```

- GitLabグループプロジェクトリポジトリ

```
https://gitlab.example.com/GROUP/project.git#master:/container/
```

- GitLabトークン認証

  gitリポジトリがプライベートで、パブリックにアクセスできない場合は、認証を含むようにプロファイルのgit　URLを変更する必要があります。 GitLabトークンで認証するには、次のURL形式を使用します。

```
https://gitlab-ci-
token:<AUTHENTICATION_TOKEN>@gitlab.example.com/USER/project.git#master:/co
ntainer/
```

> gitブランチを指定しない場合は、デフォルトで**master**ブランチが使用されます。　**folder**が指定されていない場合、イメージソース(Dockerfileソース)はGitHubまたはGitLabチェックアウトのルートディレクトリにあると想定されます。

6. ［**アクティベーションキー**］を選択します。　アクティベーションキーは、プロファイルを使用するイメージが正しいチャンネルとパッケージに確実に割り当てられるようにします。

> アクティベーションキーをイメージプロファイルに関連付けると、プロファイルを使用するすべてのイメージで正しいソフトウェアチャンネルとチャンネル内のすべてのパッケージが確実に使用されるようになります。

7. **[作成]**ボタンをクリックします。

12.2.5.1. Dockerfileソースの例

再利用できるイメージプロファイルはhttps://github.com/SUSE/manager-build-profilesで公開されています。

> **ARG**パラメータは、構築されたイメージがSUSE Multi-Linux Managerが提供する目的の

リポジトリに関連付けられていることを確認します。 **ARG**パラメータを使用すると、構築ホスト自体で使用されるSUSE Linux Enterprise Serverのバージョンとは異なる可能性のあるSUSE Linux Enterprise Serverのイメージバージョンを構築することもできます。

例: リポジトリファイルを示す**ARG repo**パラメータと**echo**コマンドは、目的のチャンネルバージョンの正しいパスを作成し、リポジトリファイルに挿入します。

リポジトリは、イメージプロファイルに割り当てたアクティベーションキーによって決定されます。

```
FROM registry.example.com/sles12sp2
MAINTAINER Tux Administrator "tux@example.com"

### Begin: These lines are required for use with {productname}

ARG repo
ARG cert

# Add the correct certificate
RUN echo "$cert" > /etc/pki/trust/anchors/RHN-ORG-TRUSTED-SSL-CERT.pem

# Update certificate trust store
RUN update-ca-certificates

# Add the repository path to the image
RUN echo "$repo" > /etc/zypp/repos.d/susemanager:dockerbuild.repo

### End: These lines are required for use with {productname}

# Add the package script
ADD add_packages.sh /root/add_packages.sh

# Run the package script
RUN /root/add_packages.sh

# After building remove the repository path from image
RUN rm -f /etc/zypp/repos.d/susemanager:dockerbuild.repo
```

12.2.5.2. カスタム情報のキーと値のペアをDocker buildargsとして使用する

カスタム情報のキーと値のペアを割り当てて、イメージプロファイルに情報を添付できます。 さらに、これらのキーと値のペアは、Dockerビルドコマンドに**buildargs**として渡されます。

使用可能なカスタム情報キーと追加のキーの作成に関する詳細については、**Reference › Systems**を参照してください。

12.2.6. イメージの構築

イメージを構築するには、2つの方法があります。 1つ目は、最初から作成する方法です。 これを行うには、左側のナビゲーションバーから**イメージ › ビルド**を選択するか、**イメージ › プロファイル**リストのビルドアイコンをクリックして、プロシージャに従います。

プロシージャ: イメージの構築

1. **イメージ › ビルド**を選択します。
2. デフォルトの**latest**(コンテナにのみ関連する)以外のバージョンを使用する場合は、別のタグ名を追加します。
3. ［**Build Profile**］（ビルドプロファイル）と［**構築ホスト**］を選択します。

   ビルドフィールドの右側にある［**プロファイル概要**］に注目します。　ビルドプロファイルを選択すると、選択したプロファイルに関する詳細情報がこの領域に表示されます。

4. ビルドをスケジュールするには、**[ビルド]**ボタンをクリックします。

12.2.7. イメージの取り込み

The second way to get an image is to import and inspect arbitrary images. To do that, select **Images › Image List** from the left navigation bar. Complete the text boxes of the **Import** dialog. When it has processed, the imported image is listed on the **Image List** page.

プロシージャ: イメージの取り込み

1. **イメージ › イメージリスト**から、**[取り込み]**をクリックして、［**イメージの取り込み**］ダイアログを開きます。
2. ［**イメージの取り込み**］ダイアログで、次のフィールドに入力します。

   イメージストア

   検査のためにイメージがプルされるレジストリ。

   イメージ名

   レジストリのイメージの名前。

   イメージバージョン

   レジストリのイメージのバージョン。

   構築ホスト

   イメージをプルして検査する構築ホスト。

アクティベーションキー

イメージが検査されるソフトウェアチャンネルへのパスを提供するアクティベーションキー。

3. 確定するには、**[取り込み]**をクリックします。

イメージのエントリがデータベースに作成され、SUSE Multi-Linux Managerの**Inspect Image**（イメージの検査）アクションがスケジュールされます。

処理が完了すると、取り込まれたイメージが**イメージリスト**に表示されます。 イメージが取り込まれたことを示す異なるアイコンが［**ビルド**］列に表示されます。 取り込まれたイメージのステータスアイコンはイメージの［**概要**］タブにも表示されます。

12.2.8. トラブルシューティング

12.2.8.1. イメージの検査

ベースコンテナイメージ(BCI)には、それを実行するためのすべてのソフトウェアが付属していますが、BCIは軽量であるため、検査に必要なすべてのツールとライブラリが付属していない場合があります。

コンテナイメージを検査する際に、次のようなエラーメッセージが表示されることがあります。

```
libssl.so.1.1: cannot open shared object file: No such file or directory
```

BCIは、コンテナ構築ホストと検査にSalt Bundleを使用する以外のシナリオでも使用できますが、検査を実行する必要がある場合は、事前に必要なソフトウェアをすべて追加しておく必要があります。

このような問題を回避するには、**libopenssl**を**Dockerfile**を含むイメージに追加し、イメージを再構築する必要があります。

同じことが**libexpat**でも起こる可能性があります。

12.2.8.2. General issues

イメージを操作する場合の既知の問題がいくつかあります。

- レジストリまたはgitリポジトリにアクセスするためのHTTPS証明書はカスタム状態ファイルによってクライアントに配備する必要があります。
- Dockerを使用したSSH gitアクセスは現在サポートされていません。

12.3. OS images

OSイメージは、Kiwiビルトシステムによって構築されます。 出力イメージはカスタマイズ可能で、PXE、QCOW2、LiveCD、またはその他のタイプのイメージにすることがきます。

Kiwiビルドシステムの詳細については、Kiwiのドキュメントを参照してください。

12.3.1. 要件

Kiwiイメージ構築機能は、SUSE Linux Enterprise Server 12およびSUSE Linux Enterprise Server 11を実行しているSaltクライアントで利用できます。

Kiwiイメージ設定ファイルおよび設定スクリプトは、以下の場所のいずれかからアクセスできる必要があります。

- Gitリポジトリ
- HTTPまたはHTTPSでホストされたtarアーカイブ
- 構築ホスト上のローカルディレクトリ

gitで提供される完全なKiwiリポジトリの例については、https://github.com/SUSE/manager-build-profiles/tree/master/OSImageを参照してください。

Kiwiで構築されたOSイメージを実行しているホストには、少なくとも1GBのRAMが必要です。 ディスク容量は、イメージの実際のサイズによって異なります。 詳細については、基になるシステムのドキュメントを参照してください。

12.3.2. 構築ホストの作成

SUSE Multi-Linux Managerであらゆる種類のイメージを構築するには、構築ホストを作成して設定します。OSイメージ構築ホストは、SUSE Linux Enterprise Server 15 (SP2以降)またはSUSE Linux Enterprise Server 12 (SP4以降)で実行されているSaltクライアントです。

このプロシージャでは、構築ホストの初期設定について説明します。

構築ホスト上のオペレーティングシステムは、ターゲットイメージ上のオペレーティングシステムと一致する必要があります。

たとえば、SUSE Linux Enterprise Server 15 (SP2以降)のOSバージョンを実行している構築ホスト上にSUSE Linux Enterprise Server 15ベースのイメージを構築します。 SUSE Linux Enterprise Server 12 SP5またはSUSE Linux Enterprise Server 12 SP4 OSバージョンを実行している構築ホスト上にSUSE Linux Enterprise Server 12ベースのイメージを構築します。

クロスアーキテクチャビルドはできません。 たとえば、SUSE Linux Enterprise Server 15 SP3を実行しているRaspberry PI (aarch64アーキテクチャ)構築ホストにRaspberry PI SUSE Linux Enterprise Server 15 SP3を構築する必要があります。

プロシージャ: SUSE Multi-Linux Manager Web UIでの構築ホストの設定

1. **システム › 概要**ページから構築ホストとして指定するクライアントを選択します。

2. **システムの詳細 › プロパティ**タブに移動して、［**付属エンタイトルメント**］>［**OSイメージビルドホスト**］ボックスにチェックを付けます。
3. **[プロパティの更新]**で確定します。
4. **システムの詳細 › ソフトウェア › ソフトウェアチャンネル**に移動し、構築ホストのバージョンに応じて必要なソフトウェアのチャンネルを有効にします。
   - SUSE Linux Enterprise Server 12構築ホストでは、SUSE Multi-Linux Managerクライアントツール(**SLE-Manager-Tools12-Pool**と**SLE-Manager-Tools12-Updates**)が必要です。
   - SUSE Linux Enterprise Server 15構築ホストでは、SUSE Linux Enterprise Serverモジュール**SLE-Module-DevTools15-SP4-Pool**と**SLE-Module-DevTools15-SP4-Updates**が必要です。
   - スケジュールを設定して**[確認]**をクリックします。
5. **highstate**を適用してKiwiと必要なすべてのパッケージをインストールします。 システムの詳細ページで、**状態 › highstate**を選択し、**[highstateの適用]**をクリックします。 または、SUSE Multi-Linux Managerサーバのコマンドラインからhighstateを適用します。

```
salt '$your_client' state.highstate
```

12.3.2.1. SUSE Multi-Linux Manager web server public certificate RPM

構築ホストのプロビジョニングでは、SUSE Multi-Linux Manager証明書RPMを構築ホストにコピーします。この証明書はSUSE Multi-Linux Managerによって提供されるリポジトリにアクセスするために使用されます。

証明書は、**mgr-package-rpm-certificate-osimage**パッケージスクリプトでRPMにパッケージ化されます。パッケージスクリプトは新しいSUSE Multi-Linux Managerのインストール中に自動的に呼び出されます。

spacewalk-certs-toolsパッケージをアップグレードすると、アップグレードシナリオではデフォルト値を使用してパッケージスクリプトが呼び出されます。 ただし、証明書パスが変更された場合や使用できない場合は、アップグレードプロシージャの完了後に、**--ca-cert-full-path <path_to_certificate>**を使用してパッケージスクリプトを手動で呼び出します。

12.3.2.2. パッケージスクリプトの呼び出し例

```
/usr/sbin/mgr-package-rpm-certificate-osimage --ca-cert-full-path /root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT
```

証明書を含むRPMパッケージは、次のようなsalt-accessibleディレクトリに保存されます。

```
/usr/share/susemanager/salt/images/rhn-org-trusted-ssl-cert-osimage-1.0-1.noarch.rpm
```

証明書を含むRPMパッケージは、ローカル構築ホストリポジトリで提供されます。

```
/var/lib/Kiwi/repo
```

ビルドソースに SUSE Multi-Linux Manager SSL証明書を含むRPMパッケージを指定し、Kiwiの設定に**bootstrap**セクションの必須パッケージとして**rhn-org-trusted-ssl-cert-osimage**が含まれていることを確認します。

リスト 3. config.xml

```
...
  <packages type="bootstrap">
    ...
    <package name="rhn-org-trusted-ssl-cert-osimage"
bootinclude="true"/>
  </packages>
...
```

12.3.3. Create an activation key for OS images

イメージの構築時にOSイメージがリポジトリとして使用できるチャンネルに関連付けられたアクティベーションキーを作成します。

アクティベーションキーはOSイメージの構築に必須です。

To build OS Images, you need an activation key that is associated with a channel other than **Default** activation key.

プロシージャ: アクティベーションキーの作成

1. Web UIで、**システム › アクティベーションキー**を選択します。
2. ［**キーの作成**］をクリックします。
3. ［**説明**］、［**キー**］の名前を入力し、ドロップダウンボックスを使用してキーに関連付ける［**ベースチャンネル**］を選択します。
4. [**アクティベーションキーの作成**]で確定します。

詳細については、**Client-configuration › Activation-keys**を参照してください。

12.3.4. イメージストアの作成

OS Images can require a significant amount of storage space. By default, the image store is using the **srv-**

www volume.

システム、仮想、およびその他のイメージの構築に使用されるKiwiビルドタイプのイメージストアは、まだサポートされていません。

The image files can be downloaded from https://MANAGER-HOST/os-images/ORGANIZATION-ID/FILE-NAME. The exact location can be determined from the image details page.

12.3.5. イメージプロファイルの作成

Web UIを使用してイメージプロファイルを管理します。

プロシージャ: イメージプロファイルの作成

1. イメージプロファイルを作成するには、**イメージ › プロファイル**から選択し、**[作成]**をクリックします。
2. ［**ラベル**］フィールドに、**イメージプロファイル**の名前を入力します。
3. ［**イメージタイプ**］として［**Kiwi**］を使用します。
4. イメージストアは自動的に選択されます。
5. Kiwi設定ファイルを含むディレクトリに［**設定URL**］を入力します。 たとえば、https://github.com/SUSE/manager-build-profiles#master:OSImage/SLE-Micro54などのgit URIです。 その他のオプションは、HTTPまたはHTTPSでホストされたtarアーカイブ、または構築ホスト上のローカルディレクトリです。 詳細については、このセクションの最後にあるソースフォーマットオプションを参照してください。
6. 必要に応じて［**Kiwiオプション**］を入力します。 Kiwi設定ファイルで複数のプロファイルが指定されている場合、**--profile <name>**を使用してアクティブなプロファイルを選択します。 他のオプションについては、Kiwiのドキュメントを参照してください。
7. ［**アクティベーションキー**］を選択します。 アクティベーションキーにより、プロファイルを使用したイメージが正しいチャンネルとパッケージに確実に割り当てられます。

アクティベーションキーをイメージプロファイルに関連付け、イメージプロファイルで正しいソフトウェアチャンネルとパッケージが使用されるようにします。

8. [**作成**]ボタンで確定します。

ソースフォーマットオプション

- リポジトリへのgit/HTTP(S) URL

  構築するイメージのソースを含むパブリックまたはプライベートgitリポジトリへのURL。　リポジトリのレイアウトによって、URLは次のようになります。

```
https://github.com/SUSE/manager-build-profiles
```

  URLの#文字の後にブランチを指定できます。　この例では、**master**ブランチを使用します。

```
https://github.com/SUSE/manager-build-profiles#master
```

  :文字の後のイメージソースを含むディレクトリを指定できます。　この例では、**OSImage/POS_Image-JeOS6**を使用します。

```
https://github.com/SUSE/manager-build-profiles#master:OSImage/POS_Image-JeOS6
```

- tarballアーカイブへのHTTP(S) URL

  Webサーバでホストされているtarアーカイブへの URL　(圧縮または非圧縮)。

```
https://myimagesourceserver.example.org/MyKiwiImage.tar.gz
```

- 構築ホスト上のディレクトリへのパス

  Kiwiビルドシステムソースを含むディレクトリへのパスを入力します。このディレクトリは選択した構築ホスト上に存在する必要があります。

```
/var/lib/Kiwi/MyKiwiImage
```

12.3.5.1. Kiwiソースの例

Kiwiソースは少なくとも **config.xml**で構成されています 。 通常、**config.sh**と**images.sh**も存在します。 ソースには**root**サブディレクトリの下の最終イメージにインストールするファイルも含めることができます。

Kiwiビルドシステムについては、Kiwiのドキュメントを参照してください。

SUSEでは、SUSE/manager-build-profilesパブリックGitHubリポジトリで、完全に機能するイメージソースの例を提供しています。

リスト 4. JeOS config.xmlの例

```
<?xml version="1.0" encoding="utf-8"?>

<image schemaversion="6.1" name="POS_Image_JeOS6">
    <description type="system">
        <author>Admin User</author>
        <contact>noemail@example.com</contact>
        <specification>SUSE Linux Enterprise 12 SP3 JeOS</specification>
    </description>
    <preferences>
        <version>6.0.0</version>
        <packagemanager>zypper</packagemanager>
        <bootsplash-theme>SLE</bootsplash-theme>
        <bootloader-theme>SLE</bootloader-theme>

        <locale>en_US</locale>
        <keytable>us.map.gz</keytable>
        <timezone>Europe/Berlin</timezone>
        <hwclock>utc</hwclock>

        <rpm-excludedocs>true</rpm-excludedocs>
        <type boot="saltboot/suse-SLES12" bootloader="grub2" checkprebuilt="true"
compressed="false" filesystem="ext3" fsmountoptions="acl" fsnocheck="true" image="pxe"
kernelcmdline="quiet"></type>
    </preferences>
    <!--    CUSTOM REPOSITORY
    <repository type="rpm-dir">
      <source path="this://repo"/>
    </repository>
    -->
    <packages type="image">
        <package name="patterns-sles-Minimal"/>
        <package name="aaa_base-extras"/> <!-- wouldn't be SUSE without that ;-) -->
        <package name="kernel-default"/>
        <package name="venv-salt-minion"/>
        ...
    </packages>
    <packages type="bootstrap">
        ...
        <package name="sles-release"/>
        <!-- this certificate package is required to access {productname} repositories
             and is provided by {productname} automatically -->
        <package name="rhn-org-trusted-ssl-cert-osimage" bootinclude="true"/>

    </packages>
    <packages type="delete">
        <package name="mtools"/>
        <package name="initviocons"/>
        ...
    </packages>
</image>
```

12.3.6. イメージの構築

There are two ways to build or get an image using the Web UI. Either select **Images › Build**, or click the build icon in the **Images › Profiles** list.

プロシージャ: イメージの構築

1. **イメージ › ビルド**を選択します。
2. デフォルトの**latest**　(コンテナのみに適用)以外のバージョンが必要な場合は別のタグ名を追加します。
3. ［**イメージプロファイル**］および［**構築ホスト**］を選択します。

［**プロファイル概要**］がビルドフィールドの右側に表示されます。　ビルドプロファイルを選択したら、選択したプロファイルに関する詳細情報がここに表示されます。

4. ビルドをスケジュールするには、**[ビルド]**ボタンをクリックします。

ビルドサーバは、イメージ構築プロセス中にどのような形式のオートマウンタも実行できません。 必要に応じて、Gnomeセッションがrootとして実行されていないことを確認します。　オートマウンタが実行されている場合、イメージのビルドは正常に終了しますが、イメージのチェックサムが異なるためエラーが発生します。

イメージが正常に構築されると、検査フェーズが開始されます。　検査フェーズ中に、SUSE　Multi-Linux Managerではイメージに関する情報を収集します。

- イメージにインストールされているパッケージのリスト
- イメージのチェックサム
- イメージタイプと他のイメージの詳細

構築されたイメージタイプが**PXE**の場合は、Saltピラーも生成されます。　イメージのピラーはデータベースに保存され、Saltサブシステムは生成されたイメージに関する詳細にアクセスできます。　詳細には、イメージファイルの場所と提供場所、イメージのチェックサム、ネットワークブートに必要な情報などが含まれます。

生成されたピラーはすべての接続されているクライアントで使用できます。

12.3.7. トラブルシューティング

イメージを構築するには、いくつかの依存ステップが必要です。　ビルドが失敗した場合は、Salt状態の結果とビルドログを調査することで、失敗の原因を特定できます。　ビルドが失敗した場合は、次のチェックを実行できます。

- 構築ホストがビルドソースにアクセスできる
- 構築ホストとSUSE Multi-Linux Managerサーバの両方にイメージ用の十分なディスク容量がある
- アクティベーションキーには正しいチャンネルが関連付けられている
- 使用されるビルドソースが有効である
- SUSE Multi-Linux Managerのパブリック証明書を含むRPMパッケージは最新で**/usr/share/susemanager/salt/images/rhn-org-trusted-ssl-cert-osimage-1.0-1.noarch.rpm**から入手できます。 パブリック証明書RPMを更新する方法の詳細については、構築ホストの作成を参照してください。

12.3.8. 制限事項

このセクションには、イメージを操作するときのいくつかの既知の問題が含まれています。

- HTTPソースまたはgitリポジトリへのアクセスに使用されるHTTPS証明書は、カスタム状態ファイルによってクライアントに配備するか、手動で設定する必要があります。
- Kiwiベースのイメージの取り込みはサポートされていません。

12.4. ビルドイメージのリスト

使用できるビルドイメージを一覧にするには、**イメージ › イメージリスト**を選択します。 すべてのイメージのリストが表示されます。

イメージに関する表示されたデータには、イメージの［**名前**］、その［**バージョン**］、［**リビジョン**］、およびビルドの［**ステータス**］が含まれます。 また、イメージに使用できる可能性のあるパッチやパッケージの更新のリストを使用してイメージの更新ステータスを確認することもできます。

OSイメージの場合、［**名前**］および［**バージョン**］フィールドはkiwiソースから作成され、ビルドが成功したときに更新されます。 ビルド中またはビルドが失敗した後は、これらのフィールドにはプロファイル名に基づく一時的な名前が表示されます。

［**リビジョン**］はビルドが成功するたびに自動的に増えます。OSイメージの場合、複数のリビジョンがストア内に共存できます。

コンテナイメージの場合、ストアには最新リビジョンのみが保持されます。 以前のリビジョン(パッケージ、パッチなど)に関する情報は保存され、［**非推奨の表示**］チェックボックスを使用して一覧にすることができます。

イメージの**[詳細]**ボタンをクリックすると、詳細ビューが表示されます。 詳細ビューには、関連するパッチの正確なリスト、イメージ内にインストールされたすべてのパッケージのリスト、およびビルドログが含まれます。

[削除]ボタンをクリックすると、リストからイメージが削除されます。 また、関連するピラー、OSイメージストアからのファイル、および非推奨のリビジョンも削除されます。

パッチおよびパッケージリストは、ビルド後の検査状態が正常だった場合にのみ使用で

きます。

Chapter 13. インフラストラクチャ保守タスク

スケジュールされたダウンタイム期間で作業する場合、SUSE Multi-Linux Managerサーバの重要なダウンタイムの前、その最中、およびその後に行う必要があるすべての作業を覚えておくことが困難な場合があります。 サーバ間同期スレーブサーバやSUSE Multi-Linux Managerプロキシなどの SUSE Multi-Linux Managerサーバ関連のシステムも影響を受けるため、考慮する必要があります。

SUSEでは、常にSUSE Multi-Linux Managerインフラストラクチャを更新し続け続けることをお勧めします。 これには、サーバ、プロキシ、構築ホストが含まれます。 SUSE Multi-Linux Managerサーバを更新し続けないと、必要な場合に環境の一部を更新できない場合があります。

このセクションには、ダウンタイム期間のチェックリストと、各ステップの実行に関する詳細情報へのリンクが含まれています。

13.1. サーバ

プロシージャ: サーバの確認

1. 最新の更新を適用します。
2. 必要に応じて、最新のサービスパックにアップグレードします。
3. **spacewalk-service status**を実行し、必要なすべてのサービスが稼働しているかどうかを確認します。

パッケージ マネージャを使用して更新をインストールできます。

- YaSTの詳細については、https://documentation.suse.com/sles/15-SP6/html/SLES-all/cha-onlineupdate-you.htmlを参照してください。
- zypperの設定の詳細については、https://documentation.suse.com/sles/15-SP6/html/SLES-all/cha-sw-cl.html#sec-zypperを参照してください。

デフォルトでは、SUSE Multi-Linux Managerサーバに対していくつかの更新チャンネルが設定され、有効になっています。 新規および更新されたパッケージは自動的に使用可能になります。

SUSE Multi-Linux Managerを最新のままにするには、SUSE Customer Centerに直接接続するか、Repository Management Tool (RMT)を使用します。 RMTは、切断された環境のローカルインストールソースとして使用できます。

次のコマンドを使用して、更新チャンネルがご使用のシステムで使用できることを確認できます。

```
zypper lr
```

出力は次のようになります。

```
Name                                                | Enabled | GPG Check | Refresh
----------------------------------------------------+---------+-----------+--------
SLE-Module-Basesystem15-SP4-Pool                    | Yes     | (r ) Yes  | No
SLE-Module-Basesystem15-SP4-Updates                 | Yes     | (r ) Yes  | Yes
```

```
SLE-Module-Python2-15-SP4-Pool                    | Yes     | (r ) Yes  | No
SLE-Module-Python2-15-SP4-Updates                 | Yes     | (r ) Yes  | Yes
SLE-Product-SUSE-Manager-Server-4.3-Pool          | Yes     | (r ) Yes  | No
SLE-Product-SUSE-Manager-Server-4.3-Updates       | Yes     | (r ) Yes  | Yes
SLE-Module-SUSE-Manager-Server-4.3-Pool           | Yes     | (r ) Yes  | No
SLE-Module-SUSE-Manager-Server-4.3-Updates        | Yes     | (r ) Yes  | Yes
SLE-Module-Server-Applications15-SP4-Pool         | Yes     | (r ) Yes  | No
SLE-Module-Server-Applications15-SP4-Updates      | Yes     | (r ) Yes  | Yes
SLE-Module-Web-Scripting15-SP4-Pool               | Yes     | (r ) Yes  | No
SLE-Module-Web-Scripting15-SP4-Updates            | Yes     | (r ) Yes  | Yes
```

SUSE Multi-Linux Managerは、新しいパッケージを提供するために保守更新(MU)をリリースします。保守更新は、新しいバージョン番号で示されます。たとえば、メジャーリリース4.3は、MUがリリースされると4.3.1にインクリメントされます。

Web UIのナビゲーションバーの下部を参照して、実行中のバージョンを確認できます。 **api.getVersion()** XMLRPC APIコールでバージョン番号をフェッチすることもできます。

13.1.1. クライアントツール

When the server is updated consider updating some tools on the clients, too. Updating **venv-salt-minion**, **zypper**, and other related management package on clients is not a strict requirement, but it is a best practice in general. For example, a maintenance update on the server might introduce a major new Salt version. Then Salt clients continue to work but might experience problems later on. To avoid this SUSE makes sure that **venv-salt-minion** will always be updated safely.

13.2. サーバ間同期スレーブサーバ

サーバ間同期スレーブサーバを使用している場合は、SUSE Multi-Linux Managerサーバ更新が完了した後で更新してください。

詳細については、**Specialized-guides › Large-deployments**を参照してください。

13.3. モニタリングサーバ

Prometheusにモニタリングサーバを使用している場合は、SUSE Multi-Linux Managerサーバの更新が完了した後で更新してください。

モニタリングの詳細については、**Administration › Monitoring**を参照してください。

13.4. プロキシ

プロキシは、SUSE Multi-Linux Managerサーバの更新が完了したらすぐに更新する必要があります。

一般的に、別のバージョンのサーバに接続されたプロキシの実行はサポートされていません。 唯一の例外は、サーバが最初に更新されることが予想される更新期間の場合で、プロキシは以前のバージョンを一時的に実行できます。

常に、最初にサーバをアップグレードしてから任意のプロキシをアップグレードしてく

ださい。

Chapter 14. SUSE Multi-Linux Managerによるライブパッチ処理

カーネル更新を実行するには、通常、システムの再起動が必要です。共通脆弱性識別子(CVE)パッチはできるだけ早く適用する必要がありますが、ダウンタイムを許容できない場合は、ライブパッチ処理を使用してこれらの重要な更新を挿入し、再起動の必要性をスキップできます。

ライブパッチ処理を設定するプロシージャはSLES 12とSLES 15ではわずかに異なります。 このセクションでは両方のプロシージャについて説明します。

14.1. ライブパッチ処理用のチャンネルの設定

完全なカーネルパッケージを更新するたびに再起動が必要です。 したがって、ライブパッチ処理を使用しているクライアントは、割り当てられているチャンネルで新しいカーネルを使用できないことが重要です。 ライブパッチ処理を使用しているクライアントは、ライブパッチ処理チャンネルで実行中のカーネルの更新を取得します。

ライブパッチ処理用のチャンネルを管理するには次の2つの方法があります。

コンテンツライフサイクル管理を使用して製品ツリーのクローンを作成し、実行中のバージョンより新しいカーネルバージョンを削除します。 このプロシージャは、administration:content-lifecycle-examples.pdfで説明されています。 これは推奨される解決策です。

または、**spacewalk-manage-channel-lifecycle**ツールを使用します。 このプロシージャはより手動であり、Web UIと同様にコマンドラインツールが必要です。 このプロシージャはSLES 15 SP5のこのセクションで説明されていますが、SLE 12 SP4以降でも機能します。

14.1.1. ライブパッチ処理用のspacewalk-manage-channel-lifecycleを使用する

spacewalk-manage-channel-lifecycleは廃止され、今後のリリースで削除される予定です。代わりに、サポート対象で機能豊富なコンテンツライフサイクル管理(CLM) APIに切り替えることをお勧めします。

複製されたベンダチャンネルは、開発の場合は**dev**、運用の場合は**testing**または**prod**で始まる必要があります。 このプロシージャでは**dev**クローンチャンネルを作成し、そのチャンネルを**testing**にプロモートさせます。

プロシージャ: ライブパッチ処理チャンネルの複製

1. クライアントのコマンドプロンプトで、rootとして、現在のパッケージチャンネルツリーを取得します。

```
# spacewalk-manage-channel-lifecycle --list-channels
Spacewalk Username: admin
Spacewalk Password:
Channel tree:
```

```
1. sles15-sp7-pool-x86_64
     \__ sle-live-patching15-pool-x86_64-sp7
     \__ sle-live-patching15-updates-x86_64-sp7
     \__ sle-manager-tools15-pool-x86_64-sp7
     \__ sle-manager-tools15-updates-x86_64-sp7
     \__ sles15-sp7-updates-x86_64
```

2. **spacewalk-manage-channel**コマンド　に**init**引数を指定して、元のベンダチャンネルの新しい開発クローンを自動的に作成します。

```
spacewalk-manage-channel-lifecycle --init -c sles15-sp7-pool-x86_64
```

3. **dev-sles15-sp7-updates-x86_64**がチャンネルリストで使用できることを確認します。

作成した**dev**クローンチャンネルを確認し、再起動が必要なカーネル更新をすべて削除します。

プロシージャ: クローンチャンネルから非ライブカーネルパッチを削除する

1. **システム › システム一覧**からクライアントを選択し、［**カーネル**］フィールドに表示されるバージョンをメモして、現在のカーネルバージョンを確認します。
2. SUSE Multi-Linux Manager Web UIで、**システム › 概要**からクライアントを選択し、**ソフトウェア › 管理 › チャンネル**タブに移動して、**dev-sles15-sp7-updates-x86_64**を選択します。　［**パッチ**］タブに移動して、**[パッチの一覧表示／削除]**をクリックします。
3. 検索バーに「**カーネル**」と入力し、クライアントが現在使用しているカーネルに一致するカーネルバージョンを特定します。
4. 現在インストールされているカーネルより新しいすべてのカーネルバージョンを削除します。

これでチャンネルにライブパッチ処理を適用するように設定され、**testing**にプロモートできるようになりました。　このプロシージャでは、ライブパッチ処理の子チャンネルもクライアントに追加し、適用できるように準備します。

プロシージャ: ライブパッチ処理チャンネルのプロモート

1. クライアントのコマンドプロンプトで、**root**として、**dev-sles15-sp7-pool-x86_64**チャンネルを新しい**testing**チャンネルにプロモートして複製します。

```
# spacewalk-manage-channel-lifecycle --promote -c dev-sles15-sp7-pool-x86_64
```

2. SUSE Multi-Linux Manager Web UIで、**システム › 概要**からクライアントを選択し、**ソフトウェア › ソフトウェアチャンネル**タブに移動します。
3. 新しい**test-sles15-sp7-pool-x86_64**カスタムチャンネルを確認してベースチャンネルを変更し、両方の対応するライブパッチ処理の子チャンネルを確認します。
4. **[次へ]**をクリックして、詳細が正しいことを確認して、**[確認]**をクリックして、変更を保存します。

これで、使用できるCVEパッチを選択して表示し、ライブパッチ処理でこれらの重要なカーネル更新を適用できるようになりました。

14.2. SLES 15でのライブパッチ処理

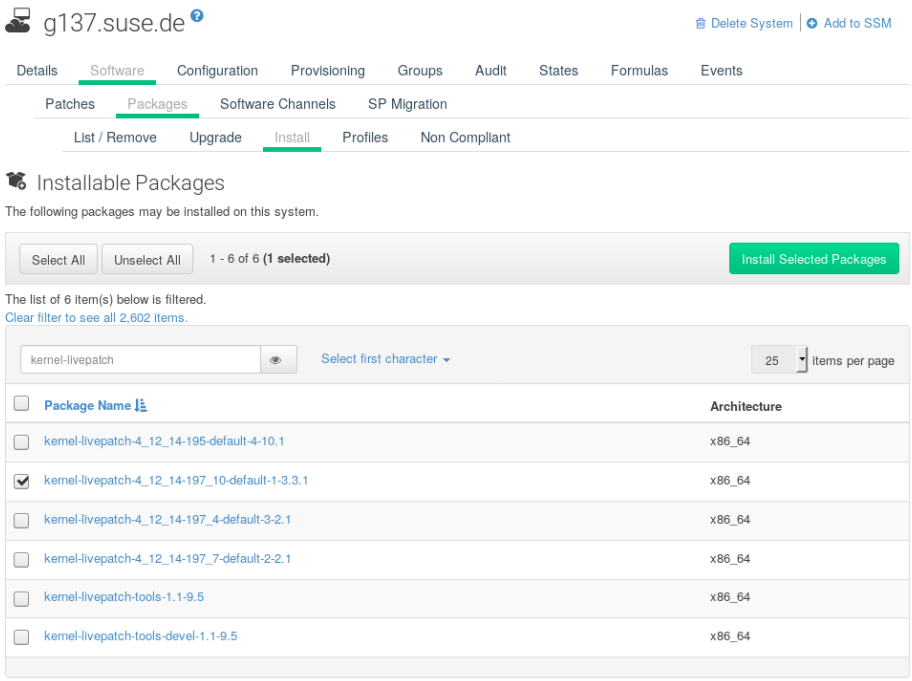
SLES 15以降のシステムでは、ライブパッチ処理は**klp livepatch**ツールで管理されます。

開始する前に、以下を確認します。

- SUSE Multi-Linux Managerが完全に更新されている。
- SLES 15 (SP1以降)を実行している1つ以上のSaltクライアントがある。
- SLES 15 SaltクライアントはSUSE Multi-Linux Managerに登録されている。
- ライブパッチ処理の子チャンネルを含む、アーキテクチャに適したSLES 15チャンネルにアクセスできる。
- クライアントが完全に同期されている。
- クライアントをライブパッチ処理用に準備されているクローンチャンネルに割り当てる。 準備の詳細については、**Administration › Live-patching-channel-setup**を参照してください。

プロシージャ: ライブパッチ処理の設定

1. **システム › 概要**からライブパッチ処理で管理するクライアントを選択し、**ソフトウェア › パッケージ › インストール**タブに移動します。 **kernel-livepatch**パッケージを検索して、インストールします。



2. highstateを適用してライブパッチ処理を有効にし、クライアントを再起動します。
3. ライブパッチ処理で管理するクライアントごとに繰り返します。
4. ライブパッチ処理が正しく有効化されていることを確認するには、**システム › システム一覧**からクライアントを選択し、［**カーネル**］フィールドに **ライブパッチ**が表示されていることを確認します。

プロシージャ: ライブパッチのカーネルへの適用

1. SUSE Multi-Linux Manager Web UIで、**システム › 概要**からクライアントを選択します。 画面の上部のバナーに、クライアントに使用できる重要なパッケージ数と、重要ではないパッケージ数が表示されます。
2. **[重大]** をクリックすると、使用可能な重大なパッチのリストが表示されます。
3. ［**Important: Security update for the Linux kernel**］（重要: Linuxカーネル用のセキュリティ更新）という概要のパッチを選択します。 セキュリティバグには該当する場合はCVE番号も含まれます。
4. オプション: 適用するパッチのCVE番号がわかっている場合は、**監査 › CVE監査**で検索し、必要なクライアントにパッチを適用します。

- すべてのカーネルパッチがライブパッチであるわけではありません。 非ライブカーネルパッチは［**セキュリティ**］ シールドアイコンの横にある［**要再起動**］アイコンで示されます。これらのパッチでは常に再起動が必要です。
- ライブパッチを適用することで、すべてのセキュリティ問題を修正できるわけではありません。 一部のセキュリティ問題は、カーネルの完全な更新を適用することによってのみ修正でき、再起動が必要です。 これらの問題に割り当てられたCVE番号は、ライブパッチには含まれていません。 CVE監査では、この要件が表示されます。

14.3. SLES 12でのライブパッチ処理

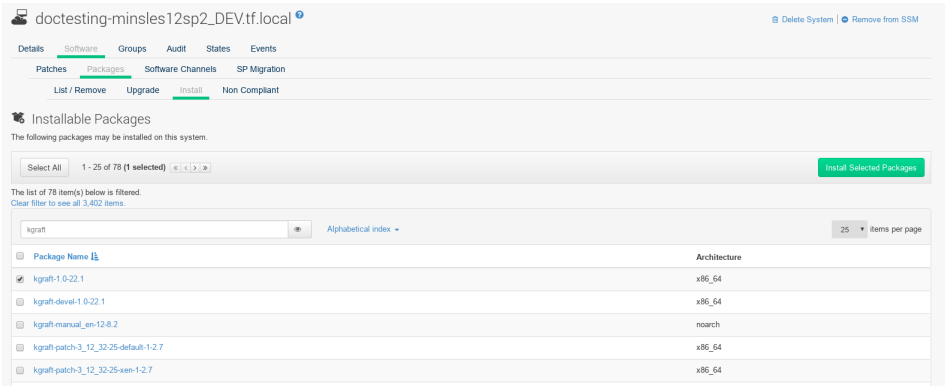
SLES 12システムでは、ライブパッチ処理はkGraftで管理されます。 kGraftの使用に関する詳細については、https://documentation.suse.com/sles/12-SP5/html/SLES-all/cha-kgraft.htmlを参照してください。

開始する前に、以下を確認します。

- SUSE Multi-Linux Managerが完全に更新されている。
- SLES 12 (SP1以降)を実行している1つ以上のSaltクライアントがある。
- SLES 12 SaltクライアントがSUSE Multi-Linux Managerに登録されている。
- ライブパッチ処理の子チャンネルを含む、アーキテクチャに適したSLES 12チャンネルにアクセスできる。
- クライアントが完全に同期されている。
- クライアントをライブパッチ処理用に準備されているクローンチャンネルに割り当てる。 準備の詳細については、**Administration › Live-patching-channel-setup**を参照してください。

プロシージャ: ライブパッチ処理の設定

1. **システム › 概要**からライブパッチ処理を使用して管理するクライアントを選択し、システムの詳細ページで、**ソフトウェア › パッケージ › インストール**タブに移動します。 **kgraft**パッケージを検索して、インストールします。



2. highstateを適用してライブパッチ処理を有効にし、クライアントを再起動します。
3. ライブパッチ処理で管理するクライアントごとに繰り返します。
4. ライブパッチ処理が正常に有効化されていることを確認するには、**システム › システム一覧**からクライアントを選択し、［**ライブパッチ処理**］が［**カーネル**］フィールドに表示されていることを確認します。

プロシージャ: ライブパッチのカーネルへの適用

1. SUSE Multi-Linux Manager Web UIで、**システム › 概要**からクライアントを選択します。 画面の上部のバナーに、クライアントに使用できる重要なパッケージ数と、重要ではないパッケージ数が表示されます。
2. **[重大]** をクリックすると、使用可能な重大なパッチのリストが表示されます。
3. ［**Important: Security update for the Linux kernel**］（重要: Linuxカーネル用のセキュリティ更新）という概要のパッチを選択します。 セキュリティバグには該当する場合はCVE番号も含まれます。
4. オプション: 適用するパッチのCVE番号がわかっている場合は、**監査 › CVE監査**で検索し、必要なクライアントにパッチを適用します。

- すべてのカーネルパッチがライブパッチであるわけではありません。 非ライブカーネルパッチは［**セキュリティ**］ シールドアイコンの横にある［**要再起動**］アイコンで示されます。これらのパッチでは常に再起動が必要です。
- ライブパッチを適用しても、すべてのセキュリティ問題を修正できるわけではありません。 一部のセキュリティの問題は、カーネルの完全な更新を適用することでのみ修正でき、再起動が必要です。 これらの問題に割り当てられたCVE番号は、ライブパッチには含まれていません。 CVE監査ではこの要件が表示されます。

Chapter 15. メンテナンスウィンドウ

SUSE Multi-Linux Managerのメンテナンスウィンドウ機能を使用すると、スケジュールされたメンテナンスウィンドウ期間中にアクションを実行するようにスケジュールできます。 メンテナンスウィンドウスケジュールを作成してクライアントに適用すると、指定した期間外に一部のアクションを実行できなくなります。

メンテナンスウィンドウは、システムロックとは異なる方法で動作します。 システムロックは必要に応じてオンまたはオフに切り替えられますが、メンテナンスウィンドウではアクションを許可する期間が定義されます。 また、許可されたアクションと制限されたアクションが異なります。 システムロックの詳細については、**Client-configuration › System-locking**を参照してください。

メンテナンスウィンドウには、カレンダーとスケジュールの両方が必要です。 カレンダーは、定期的なイベントを含むメンテナンスウィンドウイベントの日付と時刻を定義し、**ical**形式にする必要があります。 スケジュールは、カレンダーで定義されたイベントを使用して、メンテナンスウィンドウを作成します。 スケジュールを作成する前に、アップロード用の**ical**ファイルを作成するか、**ical**ファイルにリンクしてカレンダーを作成する必要があります。

スケジュールを作成したら、SUSE Multi-Linux Managerサーバに登録されているクライアントに割り当てることができます。 メンテナンススケジュールが割り当てられているクライアントは、メンテナンスウィンドウ以外に制限されたアクションを実行できません。

制限されたアクションによってクライアントが大幅に変更され、クライアントの実行を停止させる可能性があります。 制限されたアクションの例は次のとおりです。

- パッケージのインストール
- クライアントのアップグレード
- 製品の移行
- Highstate application

制限されたアクションは、安全であるとみなされ、クライアントに問題が発生する可能性が低いマイナーアクションです。 制限されたアクションの例は次のとおりです。

- パッケージプロファイルの更新
- ハードウェアの更新
- ソフトウェアチャンネルのサブスクライブ

開始する前に、アップロード用の**ical**ファイルを作成するか、**ical**ファイルにリンクしてカレンダーを作成する必要があります。 **ical**ファイルは、Microsoft Outlook、Google Calendar、KOrganizerなどのお好みのカレンダーツールで作成できます。

プロシージャ: 新しいメンテナンスカレンダーのアップロード

1. SUSE Multi-Linux Manager Web UIで、**スケジュール › メンテナンスウィンドウ › カレンダー**に移動し、**[作成]**をクリックします。

2. ［**カレンダー名**］セクションに、カレンダーの名前を入力します。
3. **ical**ファイルへのURLを指定するか、ファイルを直接アップロードします。
4. **[Create Calendar]**（カレンダーの作成）をクリックして、カレンダーを保存します。

プロシージャ: 新しいスケジュールの作成

1. SUSE Multi-Linux Manager Web UIで、**スケジュール › メンテナンスウィンドウ › スケジュール**に移動して、**[作成]**をクリックします。
2. ［**スケジュール名**］セクションに、スケジュールの名前を入力します。
3. オプション: **ical**ファイルに複数のスケジュールに適用するイベントが含まれている場合は、［**マルチ**］をオンにします。
4. このスケジュールに割り当てるカレンダーを選択します。
5. **[スケジュールの作成]**をクリックして、スケジュールを保存します。

プロシージャ: スケジュールをクライアントに割り当てる

1. SUSE Multi-Linux Manager Web UIで、**システム › システム一覧**に移動して、スケジュールに割り当てるクライアントを選択し、［**System Properties**］（システムのプロパティ）パネルを見つけて、**[これらのプロパティを編集します]**をクリックします。 または、**システム › システムセットマネージャ**に移動し、**その他 › メンテナンスウィンドウ**タブを使用して、システムセットマネージャからクライアントを割り当てることができます。
2. ［**システムの詳細を編集**］ページで、［**メンテナンススケジュール**］フィールドを見つけて、割り当てるスケジュールの名前を選択します。
3. **[プロパティの更新]**をクリックし、メンテナンススケジュールを割り当てます。

新しいメンテナンススケジュールをクライアントに割り当てると、クライアントですでにいくつかの制限されたアクションがスケジュールされている可能性があり、これらが新しいメンテナンススケジュールと競合する可能性があります。 この場合は、Web UIにエラーが表示され、スケジュールをクライアントに割り当てることができません。 この問題を解決するには、スケジュールを割り当てるときに、**[影響する動作のキャンセル]**オプションをオンにします。 これにより、新しいメンテナンススケジュールと競合する、以前にスケジュールされた動作がすべてキャンセルされます。

メンテナンスウィンドウを作成したら、メンテナンスウィンドウ中に実行される、パッケージの更新などの制限されたアクションをスケジュールできます。

プロシージャ: パッケージのアップグレードのスケジュール

1. SUSE Multi-Linux Manager Web UIで、**システム › システム一覧**に移動して、アップグレードするクライアントを選択し、**ソフトウェア › パッケージ › アップグレード**タブに移動します。
2. リストからアップグレードするパッケージを選択し、**[パッケージのアップグレード]**をクリックします。
3. ［**メンテナンスウィンドウ**］フィールドで、クライアントがアップグレードの実行に使用するメンテナ

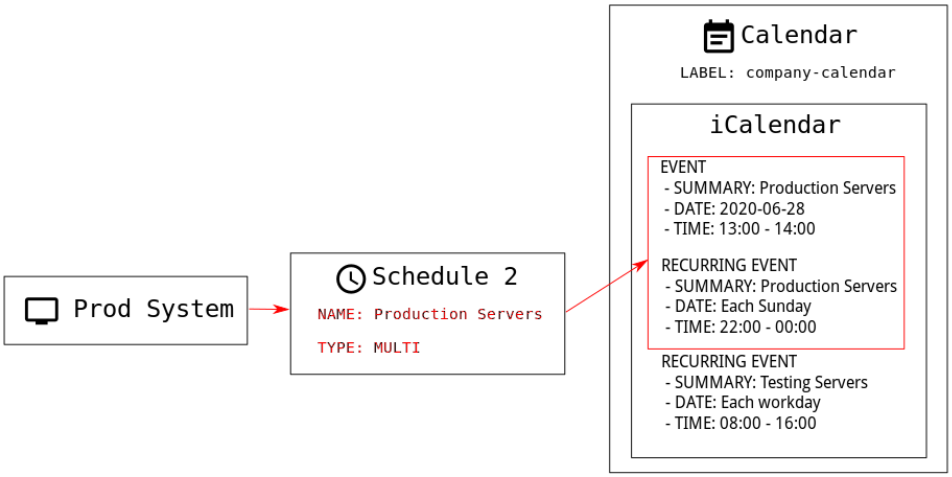
ンスウィンドウを選択します。

4. **[確認]**をクリックして、パッケージのアップグレードをスケジュールします。

15.1. メンテナンススケジュールタイプ

カレンダーを作成すると、1回限りのイベントまたは繰り返し発生するイベントのいずれかを含むイベントが多数含まれます。 各イベントには［**概要**］フィールドが含まれます。 1つのカレンダーに対して複数のメンテナンススケジュールを作成する場合は、［**概要** ］フィールドを使用して、それぞれのイベントを指定できます。

たとえば、運用サーバのスケジュールを作成し、テストサーバに別のスケジュールを作成したい場合があります。 この場合、運用サーバのイベントには**SUMMARY: Production Servers** を指定し、テストサーバのイベントには**SUMMARY: Testing Servers** を指定します。



スケジュールには、シングルとマルチの2つのタイプがあります。 カレンダーに複数のスケジュールに適用されるイベントが含まれている場合は［**マルチ**］を選択し、カレンダーファイルで使用した［**概要**］フィールドに従ってスケジュールに名前を付ける必要があります。

プロシージャ: マルチスケジュールの作成

1. SUSE Multi-Linux Manager Web UIで、**スケジュール › メンテナンスウィンドウ › スケジュール**に移動して、**[作成]**をクリックします。
2. ［**スケジュール名**］セクションに、スケジュールの名前を入力します。 カレンダーの［**概要**］フィールドに一致していることを確認します。
3. ［**マルチ**］オプションをオンにします。
4. このスケジュールに割り当てるカレンダーを選択します。
5. **[スケジュールの作成]**をクリックして、スケジュールを保存します。
6. 次のスケジュールを作成するには、**[作成]**をクリックします。
7. ［**スケジュール名**］セクションに、2番目のスケジュールの名前を入力します。 2番目のカレンダーの［**概要**］フィールドに一致していることを確認します。

8. ［**マルチ**］オプションをオンにします。
9. **[スケジュールの作成]**をクリックして、スケジュールを保存します。
10. 作成する必要がある各スケジュールごとに繰り返します。

15.2. 制限されたアクションと制限されないアクション

このセクションには、制限されたアクションと制限されないアクションのリスト全体が含まれています。

制限されたアクションにより、クライアントが大幅に変更され、クライアントの実行が停止する可能性があります。 制限されたアクションは、メンテナンスウィンドウ中にのみ実行できます。 制限されたアクションは次のとおりです。

- パッケージ操作(たとえば、パッケージのインストール、更新、または削除)
- パッチの更新
- クライアントの再起動
- トランザクションのロールバック
- 設定管理の変更タスク
- Applying a highstate
- 自動インストールと再インストール
- リモートコマンド
- 製品移行
- クラスター操作

It is possible to run remote commands directly at any time by navigating to **Salt › Remote Commands**. This applies whether or not the client is in a maintenance window. For more information about remote commands, see **Administration › Actions**.

制限されないアクションは、安全であるとみなされ、クライアントに問題が発生する可能性が少ないマイナーアクションです。 アクションが制限されない場合、定義では、無制限であり、いつでも実行できます。

Chapter 16. mgr-syncの使用

mgr-syncツールは、コマンドプロンプトで使用されます。 Web UIでは必ずしも使用できるとは限らないSUSE Multi-Linux Managerを使用するための機能を提供します。 **mgr-sync**の主な用途は、SUSE Customer Centerへの接続、製品およびパッケージ情報の取得、SUSE Multi-Linux Managerサーバと同期するためのチャンネルの準備です。

このツールは、SUSEサポートサブスクリプションで使用するように設計されています。
openSUSE、CentOS、Ubuntuなどのオープンソースディストリビューションには必要ありません。

mgr-syncに使用できるコマンドおよび引数を以下の表に一覧表示しています。 **mgr-sync**コマンドには次の構文を使用します。

```
mgr-sync [-h] [--version] [-v] [-s] [-d {1,2,3}] {list,add,refresh,delete}
```

表 3. mgr-syncコマンド

コマンド	説明	使用例
list	チャンネル、組織の資格情報、または製品を一覧表示する	**mgr-sync list channels**
add	チャンネル、組織の資格情報、または製品を追加する	**mgr-sync add channel <channel_name>**
refresh	製品、チャンネル、およびサブスクリプションのローカルコピーを更新する	**mgr-sync refresh**
delete	ローカルシステムから既存のSCC組織の資格情報を削除する	**mgr-sync delete credentials**
sync	指定されたチャンネルを同期するか、空白のままの場合は尋ねる	**mgr-sync sync channel <channel_name>**

コマンドに固有のオプションの全リストを表示するには、次のコマンドを使用します。

```
mgr-sync <command> --help
```

表 4. mgr-syncオプション引数

オプション	短縮オプション	説明	使用例
help	**h**	コマンドの使用方法とオプションを表示する	**mgr-sync --help**
version	N/A	現在インストールされているバージョンの**mgr-sync**を表示する	**mgr-sync --version**

オプション	短縮オプション	説明	使用例
verbose	**v**	詳細な出力を提供する	**mgr-sync --verbose refresh**
store-credentials	**s**	資格情報をローカルの隠しファイルに保存する	**mgr-sync --store -credentials**
debug	**d**	追加のデバッグ情報をログに記録する。レベル1、2、3が必要です。3は、最も多くのデバッグ情報を提供します。	**mgr-sync -d 3 refresh**
no-sync	N/A	**add** コマンドと一緒に使用して、同期を開始せずに製品またはチャンネルを追加する	**mgr-sync --no-sync add <channel_name>**

mgr-syncのログは次の場所にあります。

- **/var/lib/containers/storage/volumes/var-log/_data/rhn/mgr-sync.log**
- **/var/lib/containers/storage/volumes/var-log/_data/rhn/rhn_web_api.log**

Chapter 17. PrometheusとGrafanaを使用したモニタリング

PrometheusとGrafanaを使用して、SUSE Multi-Linux Manager環境を監視できます 。SUSE Multi-Linux Managerサーバとプロキシはself-health metricsを提供できます。また、Saltクライアント上に多数のPrometheus exportersをインストールして管理することもできます。

17.1. 要件

PrometheusとGrafanaパッケージは以下のSUSE Multi-Linux Managerクライアントツールに含まれています。

- SUSE Linux Enterprise 12
- SUSE Linux Enterprise 15
- openSUSE Leap 15.x

上記のクライアントのみがモニタリングサーバとしてサポートされます。

SUSE Multi-Linux Managerサーバとは別のマシンにPrometheusとGrafanaをインストールする必要があります。 管理対象のSalt SUSEクライアントをモニタリングサーバとして使用することをお勧めします。

Prometheusはプルメカニズムを使用してメトリックをフェッチするため、サーバは監視対象クライアントへのTCP接続を確立できる必要があります。 クライアントには対応するオープンポートがあり、ネットワークを介して到達できる必要があります。 または、リバースプロキシを使用して接続を確立することもできます。

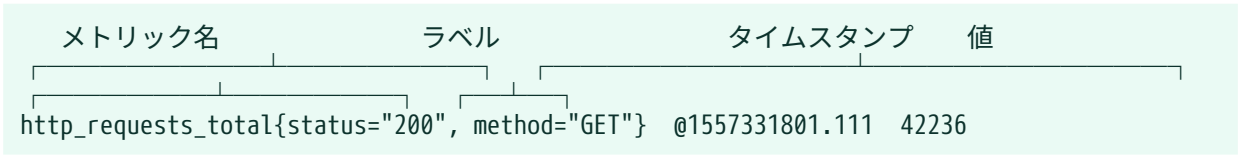
監視するクライアントごとに、モニタリングアドオンサブスクリプションが必要です。 SUSE Customer Centerにアクセスして、SUSE Multi-Linux Managerのサブスクリプションを管理してください。

17.2. PrometheusとGrafana

17.2.1. Prometheus

Prometheusはオープンソースのモニタリングツールで、リアルタイムメトリックを時系列データベースに記録するために使用されます。 メトリックはHTTP経由でプルされるため、高いパフォーマンスと拡張性が実現します。

Prometheusメトリックは時系列データ、または同じグループやディメンションに属するタイムスタンプ付きの値です。 メトリックはその名前とラベルセットで固有に識別されます。



監視対象の各アプリケーションまたはシステムは、コードインストルメンテーションまたはPrometheus exportersを使用して、上記の形式でメトリックを公開する必要があります。

17.2.2. Prometheus exporters

Exportersは、サードパーティシステムからメトリックをPrometheusメトリックとしてエクスポートするのに役立つライブラリです。 Exportersは、Prometheusメトリックを直接使用して特定のアプリケーションまたはシステムをインストルメントできない場合に役立ちます。 複数のexportersを監視対象ホスト上で実行して、ローカルメトリックをエクスポートできます。

Prometheusコミュニティは公式exportersのリストを提供し、さらに多くのものをコミュニティの貢献として見つけることができます。 詳細およびexportersの詳細なリストについては、https://prometheus.io/docs/instrumenting/exporters/を参照してください。

17.2.3. Grafana

Grafanaは、データの視覚化、モニタリング、および分析を行うためのツールです。 一定期間の特定のメトリックを表すパネルを使用してダッシュボードを作成するために使用されます。 Grafanaは通常、Prometheusと一緒に使用されますが、Elasticsearch、MySQL、PostgreSQL、Influx DBなどの他のデータソースもサポートしています。 Grafanaの詳細については、https://grafana.com/docs/を参照してください。

17.3. Set up the monitoring server

モニタリングサーバを設定するには、PrometheusとGrafanaをインストールして設定する必要があります。

SUSEクライアントのみがモニタリングサーバとしてサポートされます。 完全なリストについては、administration:monitoring.pdfを参照してください。

17.3.1. Prometheusのインストール

モニタリングサーバがSaltクライアントの場合、SUSE Multi-Linux Manager Web UIを使用してPrometheusパッケージをインストールできます。 インストールできない場合は、モニタリングサーバに手動でパッケージをダウンロードしてインストールできます。 Prometheusソフトウェアは、SUSE Multi-Linux Managerプロキシおよび SUSE Multi-Linux Manager for Retailブランチサーバでも使用できます。

- To access a shell inside the SUSE Multi-Linux Manager Server container run **mgrctl term** on the container host, or to execute one command run **mgrctl exec <options> — <command>**.
- To copy files from inside the container to the container host use **mgrctl cp**.

Prometheusはデータの保存にPOSIXファイルシステムを想定しています。 非POSIX準拠ファイルシステムはサポートされていません。 NFSファイルシステムはサポートされていません。

Procedure: Installing Prometheus using the Web UI

1. SUSE Multi-Linux Manager Web UIで、Prometheusをインストールするシステムの詳細ページを開き、［**Formula**］タブに移動します。
2. ［**Prometheus**］チェックボックスをオンにして、モニタリング式を有効にし、**[保存]**をクリックします。
3. 上部メニューの［**Prometheus**］タブに移動します。
4. ［**SUSE Multi-Linux Manager サーバ**］セクションに、有効なSUSE Multi-Linux Manager API資格情報を入力します。 入力した資格情報でモニタリングするシステムセットにアクセスできることを確認してください。
5. 必要に応じて、他の設定オプションをカスタマイズします。
6. **[Save Formula]**（Formulaの保存）をクリックします。
7. highstateを適用し、正常に完了したことを確認します。
8. Prometheusインタフェースが正しくロードされることを確認します。ブラウザで、ポート9090で、PrometheusがインストールされているサーバのURLに移動します(たとえば、http://example.com:9090)。

モニタリング式の詳細については、**Specialized-guides › Salt**を参照してください。

Procedure: Manually installing and configuring Prometheus

1. モニタリングサーバで、**golang-github-prometheus-prometheus**パッケージをインストールします。

```
zypper in golang-github-prometheus-prometheus
```

2. Prometheusサービスを有効にします。

```
systemctl enable --now prometheus
```

3. Check that the Prometheus interface loads correctly. In your browser, navigate to the URL of the server where Prometheus is installed, on port 9090 (for example, http://example.com:9090).
4. Open the configuration file at **/etc/prometheus/prometheus.yml** and add this configuration information. Replace **server.url** with your SUSE Multi-Linux Manager server URL and adjust **username** and **password** fields to match

your SUSE Multi-Linux Manager credentials.

```
# {productname} self-health metrics
scrape_configs:
- job_name: 'mgr-server'
  static_configs:
    - targets:
      - 'server.url:9100'  # Node exporter
      - 'server.url:9187'  # PostgreSQL exporter
      - 'server.url:5556'  # JMX exporter (Tomcat)
      - 'server.url:5557'  # JMX exporter (Taskomatic)
      - 'server.url:9800'  # Taskomatic
    - targets:
      - 'server.url:80'    # Message queue
      labels:
        __metrics_path__: /rhn/metrics

# Managed systems metrics:
- job_name: 'mgr-clients'
  uyuni_sd_configs:
   - server: "http://server.url"
     username: "admin"
     password: "admin"
  relabel_configs:
   - source_labels: [__meta_uyuni_exporter]
     target_label: exporter
   - source_labels: [__address__]
     replacement: "No group"
     target_label: groups
   - source_labels: [__meta_uyuni_groups]
     regex: (.+)
     target_label: groups
   - source_labels: [__meta_uyuni_minion_hostname]
     target_label: hostname
   - source_labels: [__meta_uyuni_primary_fqdn]
     regex: (.+)
     target_label: hostname
   - source_labels: [hostname, __address__]
     regex: (.*);.*:(.*)
     replacement: ${1}:${2}
     target_label: __address__
   - source_labels: [__meta_uyuni_metrics_path]
     regex: (.+)
     target_label: __metrics_path__
   - source_labels: [__meta_uyuni_proxy_module]
     target_label: __param_module
   - source_labels: [__meta_uyuni_scheme]
     target_label: __scheme__
```

5. 設定ファイルを保存します。
6. Prometheusサービスを再起動します。

```
systemctl restart prometheus
```

Prometheus設定オプションの詳細については、https://prometheus.io/docs/prometheus/latest/configuration/configuration/にある公式Prometheusドキュメントを参照してください。

17.3.2. Grafanaのインストール

モニタリングサーバがSUSE　Multi-Linux　Managerで管理されているクライアントの場合は、SUSE　Multi-Linux　ManagerのWeb UIを使用してGrafanaパッケージをインストールできます。それ以外の場合は、モニタリングサーバにパッケージを手動でダウンロードしてインストールできます。

GrafanaはSUSE Multi-Linux Managerプロキシでは使用できません。

Procedure: Installing Grafana using the Web UI

1. SUSE Multi-Linux Manager Web UIで、Grafanaがインストールされるシステムの詳細ページを開き、［**Formula**］タブに移動します。
2. ［**Grafana**］チェックボックスをオンにして、モニタリング式を有効にし、**[保存]**をクリックします。
3. 上部メニューの［**Grafana**］タブに移動します。
4. ［**Enable and configure Grafana**］（Grafanaの有効化と設定）セクションに、Grafanaにログインするために使用する管理者資格情報を入力します。
5. ［**Datasources**］（データソース）セクションで、Prometheus　URLフィールドがPrometheusが実行されているシステムを指していることを確認します。
6. 必要に応じて、他の設定オプションをカスタマイズします。
7. **[Save Formula]**（Formulaの保存）をクリックします。
8. highstateを適用し、正常に完了したことを確認します。
9. Grafanaインタフェースが正しくロードされていることを確認します。ブラウザで、ポート3000で、GrafanaがインストールされているサーバのURLに移動します(たとえば、http://example.com:3000)。
    - Ensure that port 3000 is open on the firewall to successfully access Grafana

SUSE Multi-Linux Managerには、サーバのセルフヘルス、基本的なクライアントモニタリングなどのためのダッシュボードがあらかじめ構築されています。　プロビジョニングするダッシュボードは、式の設定ページで選択できます。

Procedure: Manually installing Grafana

1. **grafana**パッケージをインストールします。

```
zypper in grafana
```

2. Grafanaサービスを有効にします。

```
systemctl enable --now grafana-server
```

3. ブラウザで、ポート3000で、GrafanaがインストールされているサーバのURLに移動します(たとえば、http://example.com:3000)。
    - Ensure that port 3000 is open on the firewall to successfully access Grafana.
4. ログインページで、ユーザ名とパスワードに**admin**と入力します。
5. Click **[Log in]**. If login is successful, then you will see a prompt to change the password.
6. プロンプトで**[OK]**をクリックし、パスワードを変更します。
7. サイドメニューの歯車アイコンにカーソルを移動すると、設定オプションが表示されます。
8. **[Data sources]**（データソース）をクリックします。
9. **[Add data source]**（データソースの追加） をクリックすると、サポートされているすべてのデータソースのリストが表示されます。
10. Prometheusデータソースを選択します。
11. Prometheusサーバの正しいURLを指定してください。
12. **[Save & test]**（保存とテスト）をクリックします。
13. ダッシュボードをインポートするには、サイドメニューの**[+]**アイコンをクリックし、**[取り込み]**をクリックします。
14. SUSE Multi-Linux Managerサーバの概要については、ダッシュボードID: **17569**をロードします。
15. SUSE Multi-Linux Managerクライアントの概要については、ダッシュボードID: **17570**をロードします。

- モニタリング式の詳細については、**Specialized-guides** › **Salt**を参照してください。
- Grafanaを手動でインストールおよび設定する方法の詳細については、https://grafana.com/docsを参照してください。

17.4. Configure SUSE Multi-Linux Manager monitoring

SUSE Multi-Linux Manager 4以降では、サーバがPrometheus self-health metricsを公開できるようにして、クライアントシステムにexportersをインストールして設定することもできます。

17.4.1. Server self-monitoring

Server self-health metricsは、ハードウェア、オペレーティングシステム、およびSUSE Multi-Linux Managerの内部を対象としています。 これらのメトリックは、Prometheus exportersと組み合わされた、Javaアプリケーションのインストルメンテーションによって利用可能になります。

以下のexporterパッケージはSUSE Multi-Linux Managerサーバに同梱されています。

- Node exporter: **golang-github-prometheus-node_exporter**。
  - https://github.com/prometheus/node_exporterを参照してください。
- PostgreSQL exporter: **prometheus-postgres_exporter**。
  - https://github.com/wrouesnel/postgres_exporterを参照してください。
- JMX exporter: **prometheus-jmx_exporter**。
  - https://github.com/prometheus/jmx_exporterを参照してください。

以下のexporterパッケージはSUSE Multi-Linux Managerプロキシに同梱されています。

- Node exporter: **golang-github-prometheus-node_exporter**。
  - https://github.com/prometheus/node_exporterを参照してください。

- Squid exporter: **golang-github-boynux-squid_exporter**。
  - https://github.com/boynux/squid-exporterを参照してください。

exporterパッケージはSUSE　Multi-Linux　Managerサーバおよびプロキシに事前インストールされていますが、各systemdデーモンはデフォルトで無効になっています。

Procedure: Enabling self-monitoring

1. SUSE Multi-Linux Manager Web UIで、**管理 › マネージャ設定 › モニタリング**に移動します。
2. **[Enable services]**（サービスの有効化）をクリックします。
3. TomcatとTaskomaticを再起動します。
4. ポート9090で、PrometheusサーバのURLに移動します(たとえば、http://example.com:9090)。
5. Prometheus　UIで、**ステータス　›　Targets（ターゲット）**に移動して、**mgr-server**グループのすべてのエンドポイントが起動していることを確認します。
6. Web UIを使用してGrafanaもインストールしている場合、サーバインサイトがSUSE Multi-Linux Managerサーバダッシュボードの管理[Manager Configuration > Monitoring (マネージャの設定 > モニタリング)]に表示されます。

Web UIを使用して有効にできるのは、サーバのセルフヘルスモニタリングだけです。 プロキシのメトリックは、Prometheusによって自動的に収集されません。　プロキシでセルフヘルスモニタリングを有効にするには、exportersを手動でインストールして有効にする必要があります。

以下の関連メトリックがSUSE Multi-Linux Managerサーバに収集されます。

表 5. サーバ統計(ポート80)

メトリック	タイプ	説明
uyuni_all_systems	ゲージ	全システムの数
uyuni_virtual_systems	ゲージ	仮想システムの数
uyuni_inactive_systems	ゲージ	休止中のシステムの数
uyuni_outdated_systems	ゲージ	旧式パッケージを持つシステムの数

表 6. PostgreSQL exporter (ポート9187)

メトリック	タイプ	説明
pg_stat_database_tup_fetched	カウンタ	クエリによってフェッチされた行数
pg_stat_database_tup_inserted	カウンタ	クエリによって挿入された行数
pg_stat_database_tup_updated	カウンタ	クエリによって更新された行数
pg_stat_database_tup_deleted	カウンタ	クエリによって削除された行数
mgr_serveractions_completed	ゲージ	完了したアクションの数
mgr_serveractions_failed	ゲージ	失敗したアクションの数
mgr_serveractions_picked_up	ゲージ	ピックアップされたアクションの数
mgr_serveractions_queued	ゲージ	キューに入れられたアクションの数

表 7. JMX exporter (Tomcatポート5556、Taskomaticポート5557)

メトリック	タイプ	説明
java_lang_Threading_ThreadCount	ゲージ	アクティブなスレッドの数
java_lang_Memory_HeapMemoryUsage_used	ゲージ	現在のヒープメモリ使用量

表 8. サーバメッセージキュー(ポート80)

メトリック	タイプ	説明
message_queue_thread_pool_threads	カウンタ	これまでに作成されたメッセージキュースレッドの数
message_queue_thread_pool_threads_active	ゲージ	現在アクティブなメッセージキュースレッドの数
message_queue_thread_pool_task_count	カウンタ	これまでに送信されたタスクの数
message_queue_thread_pool_completed_task_count	カウンタ	これまでに完了したタスクの数

表 9. Salt Queue (ポート80)

メトリック	タイプ	説明
salt_queue_thread_pool_size	ゲージ	Saltキューごとに作成されたスレッドの数
salt_queue_thread_pool_active_threads	ゲージ	キューごとに現在アクティブなSaltスレッドの数
salt_queue_thread_pool_task_total	カウンタ	キューごとに送信されたタスクの数

メトリック	タイプ	説明
salt_queue_thread_pool_completed_task_total	カウンタ	キューごとに完了したタスクの数

すべてのsalt_queue値には、キュー番号を値として持つ「queue」という名前のラベルがあります。

表 10. Taskomaticスケジューラ(ポート9800)

メトリック	タイプ	説明
taskomatic_scheduler_threads	カウンタ	これまでに作成されたスケジューラスレッドの数
taskomatic_scheduler_threads_active	ゲージ	現在アクティブなスケジューラスレッドの数
taskomatic_scheduler_completed_task_count	カウンタ	これまでに完了したタスクの数

17.4.2. Monitoring managed systems

Prometheus metrics exporters can be installed and configured on Salt clients using formulas. The packages are available from the SUSE Multi-Linux Manager client tools channels, and can be enabled and configured directly in the SUSE Multi-Linux Manager Web UI.

これらのexportersは管理対象システムにインストールできます。

- Node exporter: **golang-github-prometheus-node_exporter**。
  - https://github.com/prometheus/node_exporterを参照してください。
- PostgreSQL exporter: **prometheus-postgres_exporter**。
  - https://github.com/wrouesnel/postgres_exporterを参照してください。
- Apache exporter: **golang-github-lusitaniae-apache_exporter**。
  - https://github.com/Lusitaniae/apache_exporterを参照してください。

On SL Micro, only the Node exporter and the Blackbox exporter are available.

exporterをインストールして設定したら、Prometheusを使用して監視対象システムからメトリックを収集できます。Web UIを使用してモニタリングサーバを設定している場合、メトリック収集は自動的に行われます。

Procedure: Configuring Prometheus exporters on a client

1. SUSE Multi-Linux Manager Web UIで、監視対象のクライアントの詳細ページを開き、**Formula**タブに移動します。
2. ［**Prometheus Exporters**］ formulaで、［**有効**］チェックボックスをオンにし

ます。

3. [保存]をクリックします。
4. **Formula › Prometheus Exporters**タブに移動します。
5. 有効にするexportersを選択し、必要に応じて引数をカスタマイズします。 ［アドレス］フィールドは、コロンで始まるポート番号(**:9100**)か、完全に解決可能なアドレス(**example:9100**)のいずれかを受け入れます。
6. [**Save Formula**]（Formulaの保存）をクリックします。
7. highstateを適用します。

The following ports need to be enabled and not blocked by the firewall:

- on the monitor: 9090/tcp
- on the monitored system: 9100/tcp, 9117/tcp, and 9187/tcp

モニタリング式は、対応するグループ内の個々のシステムに使用されているのと同じ設定を適用することによって、システムグループにも設定できます。

モニタリング式の詳細については、**Specialized-guides › Salt**を参照してください。

17.4.3. Change Grafana password

Grafanaパスワードを変更するには、Grafanaのドキュメントに記載されているステップに従います。

- https://grafana.com/docs/grafana/latest/administration/user-management/user-preferences/#change-your-grafana-password

Grafana管理者パスワードを紛失した場合は、次のコマンドで**root**としてリセットできます。

```
grafana-cli --configOverrides cfg:default.paths.data=/var/lib/grafana --homepath
/usr/share/grafana admin reset-admin-password <new_password>
```

17.5. Network boundaries

Prometheusはプルメカニズムを使用してメトリックをフェッチするため、サーバは監視対象クライアントとのTCP接続を確立できる必要があります。 デフォルトでは、Prometheusは次のポートを使用します。

- Node exporter: 9100
- PostgreSQL exporter: 9187
- Apache exporter: 9117

さらに、Prometheusを実行するホストとは異なるホストでAlertmanagerを実行している場合は、ポー

ト9093も開く必要があります。AlertmanagerはPrometheusソリューションの一部であり、Prometheusサーバインスタンスなどのクライアントアプリケーションによって送信されるアラートを処理します。Alertmanagerの詳細については、https://prometheus.io/docs/alerting/latest/alertmanager/を参照してください。

クラウドインスタンスにインストールされているクライアントの場合、モニタリングサーバにアクセスできるセキュリティグループに必要なポートを追加できます。

または、Prometheusインスタンスをexportersのローカルネットワークにデプロイし、フェデレーションを設定することもできます。 これにより、メインのモニタリングサーバはローカルのPrometheusインスタンスから時系列をスクレイピングできます。 この方法を使用する場合は、Prometheus APIポート(9090)を開くだけで済みます。

Prometheusフェデレーションの詳細については、https://prometheus.io/docs/prometheus/latest/federation/を参照してください。

ネットワーク境界から要求をプロキシすることもできます。 PushProxのようなツールは、プロキシとクライアントをネットワークバリアの両側に配備し、PrometheusがNATなどのネットワークトポロジ全体で動作できるようにします。

PushProxの詳細については、https://github.com/RobustPerception/PushProxを参照してください。

17.5.1. Reverse proxy setup

Prometheusはプルメカニズムを使用してメトリックをフェッチするため、サーバは監視対象クライアント上の各exporter へのTCP接続を確立できる必要があります。 ファイアウォール設定を簡素化するため、exportersにリバースプロキシを使用して、単一のポートですべてのメトリックを公開できます。

Procedure: Installing Prometheus exporters with reverse proxy

1. SUSE Multi-Linux Manager Web UIで、監視対象のシステムの詳細ページを開き、［**Formula**］タブに移動します。
2. ［**Prometheus Exporters**］チェックボックスをオンにして、exporters formulaを有効にし、**[保存]**をクリックします。
3. 上部メニューの［**Prometheus Exporters**］タブに移動します。
4. Check the **Enable reverse proxy** option, and enter a valid reverse proxy port number. For example, **9999**.
   - Ensure that port 9999/tcp is open on the firewall.
5. 必要に応じて他のexportersをカスタマイズします。
6. **[Save Formula]**（Formulaの保存）をクリックします。

7. highstateを適用し、正常に完了したことを確認します。

モニタリング式の詳細については、**Specialized-guides › Salt**を参照してください。

17.6. セキュリティ

PrometheusサーバとPrometheus node exporterは、TLS暗号化と認証でエンドポイントを保護するための組み込みメカニズムを提供します。 SUSE Multi-Linux Manager Web UIは、関連するすべてのコンポーネントの設定を簡素化します。 TLS証明書は、ユーザが提供して配備する必要があります。 SUSE Multi-Linux Managerでは、次のセキュリティモデルを有効にします。

- Node exporter: TLS暗号化とクライアント証明書ベースの認証
- Prometheus: TLS暗号化と基本認証

利用可能なすべてのオプションの設定の詳細については、**Specialized-guides › Salt**を参照してください。

17.6.1. TLS証明書の生成

デフォルトでは、SUSE Multi-Linux Managerはモニタリング設定を保護するための証明書を提供しません。セキュリティを提供するために、自己署名された、またはサードパーティの認証局(CA)によって署名されたカスタム証明書を生成またはインポートできます。

このセクションでは、SUSE Multi-Linux Manager CAで自己署名したPrometheusおよびNode exporter minionsのクライアント/サーバ証明書を生成する方法について説明します。

プロシージャ: サーバ/クライアントTLS証明書の作成

1. At the command prompt of the SUSE Multi-Linux Manager container host, as root, run the following commands:

   a. To generate certificate files, run the following command.

      Ensure that the **set-cname** parameter is the fully qualified domain name (FQDN) of your Salt client. You can use the the **set-cname** parameter multiple times if you require multiple aliases:

```
mgrctl exec -ti -- mgr-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="minion.example.com" --set-cname="minion.example.com" --no
-rpm
```

      Resulting in:

```
Generating the web server's SSL private key: /root/ssl-
build/minion/server.key
Generating web server's SSL certificate request: /root/ssl-
build/minion/server.csr
Generating/signing web server's SSL certificate: server.crt
```

b. Copy **server.crt** and **server.key** files from the server container to the host:

```
mgrctl cp server:/root/ssl-build/minion/server.key server.key
mgrctl cp server:/root/ssl-build/minion/server.crt server.crt
```

c. Copy **server.crt** and **server.key** files from the host to the monitoring client:

```
ssh minion.example.com 'mkdir /etc/ssl/mlm-server-certs'
scp /root/server.* minion.example.com:/etc/ssl/mlm-server-certs
ssh minion.example.com 'chmod go+r /etc/ssl/mlm-server-certs/server.*; ls
-la /etc/ssl/mlm-server-certs'
```

2. To configure Salt formulars, enter the directory names specified in the previous steps.

   formular server Server Certificate /etc/ssl/mlm-server-certs/server.crt Server Key /etc/ssl/mlm-server-certs/server.key

   a. formular minion

Chapter 18. 組織

組織は、SUSE Multi-Linux Manager内でユーザのアクセスと許可を管理するために使用されます。

ほとんどの環境では、単一の組織で十分です。 ただし、より複雑な環境では、複数の組織が必要な場合があります。 ビジネス内の物理的な場所ごとに、またはさまざまなビジネス機能ごとに組織を設定したい場合があります。

組織を作成したら、ユーザを作成して組織に割り当てることができます。 次に、組織レベルで許可を割り当てることができます。 この許可は、組織に割り当てられたすべてのユーザにデフォルトで適用されます。

PAMやシングルサインオンなど、新しい組織の認証方法を設定することもできます。 認証の詳細については、**Administration › Auth-methods**を参照してください。

組織を作成および管理するには、SUSE Multi-Linux Manager管理者としてログインする必要があります。

プロシージャ: 新しい組織の作成

1. SUSE Multi-Linux Manager Web UIで、**管理 › 組織**に移動して、**[組織の作成]**をクリックします。
2. ［**組織の作成**］ダイアログで、次のフィールドに入力します。
   - ［**Organization Name**］（組織名）フィールドに、新しい組織の名前を入力します。 名前は3～128文字である必要があります。
   - ［**希望のログイン**］フィールドに、組織の管理者に使用するログイン名を入力します。 これは新しい管理者アカウントである必要があります。現在サインインしている組織を含め、既存の管理者アカウントを使用して、新しい組織にサインインすることはできません。
   - ［**希望のパスワード**］フィールドに、新しい組織の管理者のパスワードを入力します。 ［**パスワードの確認**］フィールドにパスワードを再度入力して確認します。 パスワードの強度はパスワードフィールドの下の色付きバーで示されます。
   - ［**電子メール** ］フィールドに、新しい組織の管理者の電子メールアドレスを入力します。
   - ［**ファーストネーム(名)**］フィールドで、挨拶文を選択し、新しい組織の管理者の名前を入力します。
   - ［**ラストネーム(姓)**］フィールドに、新しい組織の管理者の姓を入力します。
3. **[組織の作成]**をクリックします。

18.1. 組織の管理

SUSE Multi-Linux Manager Web UIで、**管理 › 組織**に移動して、利用可能な組織のリストを表示します。 管理する組織の名前をクリックします。

管理 › 組織セクションから、組織のユーザ、信頼、設定、および状態を管理するタブにアクセスできます。

組織を管理できるのは管理者のみです。 組織を管理するには、変更する組織の正しい管

> 理者としてサインインしていることを確認してください。

18.1.1. 組織ユーザ

［**ユーザ**］タブに移動して、組織に関連付けられているすべてのユーザとそのロールのリストを表示します。 ユーザ名をクリックすると、ユーザを追加、変更、または削除する［**ユーザ**］メニューに移動します。

18.1.2. 信頼されている組織

［**信頼**］タブに移動して、信頼されている組織を追加または削除します。 組織間で信頼を確立することにより、それらの組織間でコンテンツを共有し、ある組織から別の組織にクライアントを転送できるようになります。

18.1.3. 組織の設定

［**設定**］タブに移動し、組織の設定を管理します。 これには、ステージングされたコンテンツの使用、および SCAPファイルの使用が含まれます。

コンテンツステージングの詳細については、**Administration › Content-staging**を参照してください。

OpenSCAPの詳細については、**Reference › Audit**を参照してください。

18.2. 状態の管理

［**状態**］タブに移動して、組織のすべてのクライアントのSalt状態を管理します。 状態を使用すると、グローバルセキュリティポリシーを定義したり、すべてのクライアントに共通の管理ユーザを追加したりできます。

Salt状態の情報については、**Specialized-guides › Salt**を参照してください。

18.2.1. 設定チャンネルの管理

組織全体に適用する設定チャンネルを選択できます。 設定チャンネルは、SUSE Multi-Linux Manager Web UIで**設定 › チャンネル**に移動して作成できます。 SUSE Multi-Linux Manager Web UIを使用して組織に設定チャンネルを適用します。

プロシージャ: 組織への設定チャンネルの適用

1. SUSE Multi-Linux Manager Web UIで、**ホーム › 所属企業/組織 › 設定チャンネル**に移動します。
2. 検索機能を使用して、名前でチャンネルを見つけます。
3. 適用するチャンネルをオンにし、**[変更点の保存]**をクリックします。 これにより、データベースに保存されますが、チャンネルに変更は適用されません。
4. **[適用]**をクリックして変更を適用します。 これにより、組織内のすべてのクライアントに変更が適用されるようにタスクがスケジュールされます。

Chapter 19. パッチ管理

この章では、パッチ管理に関連するさまざまなトピックについて説明します。

19.1. 撤回されたパッチ

ベンダから新しいパッチがリリースされると、テストで特定されなかったいくつかのシナリオでは、パッチに望ましくない副作用(セキュリティ、安定性)が生じる可能性があります。 これが発生すると(非常にまれ)、ベンダは通常、新しいパッチをリリースします。このパッチには、そのベンダが実施している内部プロセスによっては、数時間または数日かかる場合があります。

SUSEでは、「撤回されたパッチ」と呼ばれる新しいメカニズム(2021年)を導入し、このようなパッチのアドバイザリステータスを(「最終」または「安定」ではなく)「撤回」に設定することで、ほぼ即座にこのようなパッチを取り消します。

アドバイザリステータス属性が「撤回」に設定されている場合、パッチは「撤回」されています。パッケージが「撤回された」パッチに属している場合、そのパッケージは「撤回」されています。

撤回されたパッチまたはパッケージは、SUSE Multi-Linux Managerのシステムにはインストールできません。 撤回されたパッケージをインストールする唯一の方法は、**zypper install**を使用して手動で実行し、正確なパッケージバージョンを指定することです。 例:

```
zypper install vim-8.0.1568-5.14.1
```

パッチおよびパッケージの撤回ステータスは、SUSE Multi-Linux ManagerのWeb UIの⊗アイコンで示されます。たとえば、以下を参照してください。

- チャンネルのパッケージのリスト
- チャンネルのパッチのリスト

システムにインストールされているパッチまたはパッケージが撤回されると、そのシステムのインストール済みパッケージリストに⊗アイコンも表示されます。SUSE Multi-Linux Managerでは、このようなパッチまたはパッケージをダウングレードする方法は提供されていません。

19.1.1. チャンネルクローン

複製されたチャンネルを使用する場合は、元のチャンネルからクローンへの撤回されたアドバイザリステータスの伝播に注意する必要があります。

ベンダチャンネルを組織に複製すると、チャンネルパッチも複製されます。

ベンダがチャンネル内のパッチを撤回し、SUSE Multi-Linux Managerがこのチャンネルを同期する(たとえば、夜間ジョブと同期する)と、「撤回」属性はクローンパッチに伝播されず、クローンチャンネルにサブスクライブされたクライアントによって監視されません。 属性をクローンチャンネルに伝播するには、次のいずれかの方法を使用します。

- パッチ同期(**ソフトウェア › 管理 › cloned channel （クローンチャンネル） › パッチ › 同期**)。この機能を使用すると、クローンチャンネルのパッチの属性をオリジナルに合わせることができます。
- コンテンツライフサイクル管理。コンテンツライフサイクル管理のコンテキストでのクローンチャンネルの詳細については、**Client-configuration › Channels**を参照してください。

19.1.2. パッチの共有

組織内で複数のベンダチャンネルのクローンを作成する場合、パッチは複数回複製されるのではなく、クローンチャンネル間で共有されます。 その結果、(パッチ同期機能または先述のコンテンツライフサイクル管理を使用して)複製されたパッチを同期すると、複製されたパッチを使用するすべてのチャンネルでその変更が確認されます。

例:

1. 2つのコンテンツライフサイクル管理プロジェクト**prj1**と**prj2**を検討します。
2. これらのプロジェクトの両方に2つの環境 **dev**と**test**があります。
3. これらのプロジェクトの両方にソースチャンネルとして設定されたベンダチャンネルがあります。
4. このシナリオのすべてのチャンネル(合計4つのクローンチャンネル)は、ベンダチャンネルの最新の状態に合わせて調整されます。
5. ベンダがソースチャンネル内のパッチを撤回し、夜間ジョブがそのパッチをSUSE Multi-Linux Managerに同期します。
6. 4つのチャンネルのいずれも、パッチを直接使用するのではなく、パッチクローンを使用しているため、この変更を認識しません。
7. パッチを同期するとすぐに(これら2つのプロジェクトのいずれかを構築するか、または4つのクローンチャンネルのいずれかでパッチ同期機能を使用する)、パッチの共有により、**すべて**のクローンチャンネルがそのパッチを撤回されたものと認識します。

Chapter 20. SUSE Multi-Linux ManagerのPTFsの使用

SUSEでは、お客様に直接出荷される現在サポートされているすべてのソリューションに対して一時的な修正を提供しています。 これらのPTFs (プログラムの一時的な修正)は、SUSE Multi-Linux Managerで同期できるリポジトリとして利用できるようになりました。

20.1. PTFパッケージについて

PTFパッケージはプロキシパッケージを介してインストールされ、**ptf-xxxxxx**という名前が付けられます。ここで、xxxxxxはパッケージのバージョンではなく、パッケージの番号と名前の一部です。

これらは、ソフトウェアに修正が含まれていることがわかっている正しいバージョンのパッケージに依存します。このタイプのパッケージは次のとおりです。

- 誤ってインストールすることはできません(つまり、zypper更新はインストールを推奨しません)。
- 誤って削除することはできません(つまり、ユーザがzypperコマンドラインで明示的に指定しない限り、新しいパッケージバージョンはPTFバージョンに置き換わりません)。
- PTFによって以前に解決された特定の問題に新しいバージョンが対処することがわかっている場合にのみ更新されます。
- システムにすでにインストールされているパッケージのみを更新します(つまり、ソフトウェアが複数のパッケージに分割されている場合、PTFは現在システムにインストールされているパッケージのみを置き換えます)。

サポートケース調査の過程で、パッケージの正しいIDと、影響を受けるサービスの配備/再起動方法についての指示がSUSEサポートによって提供されます。

20.2. PTFパッケージのインストール

PTFパッケージは現在、SLE 12およびSLE 15ベースのシステムでのみサポートされています。他のバージョンまたはオペレーティングシステムにはこの機能がないため、ページは表示されません。

Access to PTF channels via SUSE Multi-Linux Manager needs to be requested from L3 support.

プロシージャ: コマンドラインを使用してPTFリポジトリを有効にし、同期する

1. コンソールで、**mgr-sync refresh**と入力します。
2. 「**mgr-sync list channel**」と入力し、SCCアカウント名とその名前の**ptfs**で始まるチャンネルを探します。 例: **a123456-sles-15.3-ptfs-x86_64**。
3. **mgr-sync add channel <label>**を使用してPTFチャンネルを有効にします。

このチャンネルは現在使用可能になり、同じベースチャンネルを使用しているすべてのシステムに追加でき

ます。

PTFパッケージは、システムの更新時に自動的には選択されないため、明示的にインストールする必要があります。SUSEカスタマーサポートは、特定の問題を修正するためのPTF番号を提供しています。この番号を使用して、PTFリストでプロキシパッケージを特定できます。SUSE Multi-Linux ManagerのWeb UIには、インストールできるPTFが提供されているすべてのシステム用に、PTFを一覧にしたページがあります。

プロシージャ: SUSE Multi-Linux ManagerのWeb UIを使用したPTFリポジトリの有効化および同期

1. SUSE Multi-Linux ManagerのWeb UIで、**管理 › セットアップウィザード › 製品**に移動し、PTFリポジトリを有効にする製品を探します。
2. 製品同期ステータスの横にある**[製品チャンネルの表示]**をクリックします。
3. 製品の必須チャンネルとオプションチャンネルを一覧表示したポップアップが表示されます。
4. オプションのチャンネルリストで、自分のSCCアカウント名と**ptfs**で名前が始まるチャンネルを探します。 例: **a123456-sles-15.3-ptfs-x86_64**。
5. チャンネル名の横にあるチェックボックスを使用してチャンネルを選択し、**[確認]**をクリックして同期をスケジュールします。

オプションチャンネルを追加できるようにするには、製品をインストールする必要があることに注意してください。

プロシージャ: PTFパッケージのインストール

1. SUSE Multi-Linux Manager Web UIで、**システム › システム一覧**に移動して、PTFをインストールするクライアントを選択します。
2. **システム › ソフトウェア › パッケージ › ソフトウェアチャンネル**に移動し、**PTF channel**（PTFチャンネル）を選択します。
3. **[次へ]**、［**ソフトウェアチャンネルの変更確認**］、**[確認]**をクリックします。
4. チャンネルの割り当てが完了しているかどうかを確認するには、**システム › Events › History (イベント › 履歴)**に移動して結果を確認します。
5. **システム › ソフトウェア › PTFs › インストール**サブタブに移動します。
6. インストールするPTFパッケージを選択します。
7. **[PTFのインストール]**、［**Program Temporary Fixes (PTFs)インストールの確認**］、**[確認]**をクリックします。
8. PTFのインストール結果を確認するには、**システム › Events › History (イベント › 履歴)**に移動します。

APIを使用してPTFをインストールする必要がある場合は、プロキシパッケージ名とともに通常の**system.schedulePackageInstall** APIを使用できます。

20.3. PTFのインストール後

PTFを確認して報告された問題に対処すると、更新されたパッケージは、通常のメンテナンス更新として更新リポジトリで広く配布される前に、今後のメンテナンス更新に含める対象として追跡されます。

この修正を含む定期的な更新がリリースされると、PTFの更新バージョンもアカウント固有のPTFリポジトリにリリースされます。　更新されたPTFにより厳密な依存関係が削除され、更新を再度インストールできるようになります。

PTFの修正を含む保守更新の置き換えは、標準のパッケージ更新またはパッチのインストールによって自動的に行われます。

20.4. パッチ適用済みバージョンのパッケージの削除

PTFをアンインストールする必要があり、パッチが適用されていないバージョンのパッケージをシステムにインストールする必要がある場合、単純なパッケージ削除は使用できません。　PTFパッケージは、標準パッケージリストページでは選択できません。

プロシージャ: PTFパッケージの削除

1. SUSE Multi-Linux Manager Web UIで、**システム › システム一覧**に移動して、PTFを削除するクライアントを選択します。
2. **システム › ソフトウェア › PTFs › 一覧表示/削除**サブタブに移動します。
3. 削除するPTFパッケージを選択します。
4. **[PTFsの削除]**をクリックし、［**Program Temporary Fixes (PTFs)削除の確認**］ページで、**[確認]**をクリックします。
5. 結果を確認するには、**システム › イベント › 履歴**に移動します。

PTFを削除するには、特別なバージョンの**libzypp**と**zypper**をクライアントシステムにインストールする必要があります。**removeptf**がサポートされているかどうかを確認するには、**zypper --help**を確認します。［**List/Remove (リスト/削除)**］タブは、この条件を満たしている場合にのみ表示されます。

APIを使用してPTFを削除する必要がある場合は、プロキシパッケージ名とともに通常の**system.schedulePackageRemove** APIを使用できます。

20.5. クライアント上のパッチ適用済みバージョンのパッケージを削除する

コンソールを使用してPTFをクライアント上で直接削除する必要がある場合、特別なコマンド**zypper removeptf**を使用する必要があります。他の方法はすべて、エラーになるか、重要なパッケージがシステムから削除されてシステムが使用不能になるなどの望まない動作を招く可能性があります。

Chapter 21. レポートの生成

SUSE Multi-Linux Managerでは、ユーザがさまざまなレポートを作成できます。 これらのレポートはサブスクライブしたシステム、ユーザ、および組織のインベントリを取得するのに役立ちます。 レポートの使用は、特に多数のシステムを管理している場合は、SUSE Multi-Linux Manager Web UIから手動で情報を収集するより簡単な場合が多いです。

コマンドラインツール**spacewalk-report**を使用して事前設定されたレポートを生成することができますが、**Specialized-guides › Large-deployments**を導入することで、完全にカスタマイズされたレポートを生成することもできます。 これは、SQL言語をサポートする任意のレポーティングツールをレポーティングデータベースに接続し、データを直接抽出することで実現できます。 データの可用性と構造の詳細については、レポーティングデータベーススキーマのドキュメントを参照してください。

21.1. spacewalk-reportの使用

サーバコンテナでステップを実行する前に、**mgrctl term**を使用します。

レポートを生成するには、**spacewalk-reports**パッケージをインストールしている必要があります。**spacewalk-report**コマンドを使用すると、SUSE Multi-Linux Manager全体のコンテンツ、システム、およびユーザリソースに関するレポートを整理して表示できます。

Specialized-guides › Large-deploymentsの導入により、**spacewalk-report**はデフォルトでレポーティングデータベースからデータを収集するようになりました。 詳細については**spacewalk-report**およびレポーティングデータベースを参照してください。

次に関するレポートを生成できます。

システムインベントリ

SUSE Multi-Linux Managerに登録されているすべてのシステムを一覧にします。

パッチ

登録されているシステムに関連するすべてのパッチを一覧にします。重大度、および特定のパッチに適用されるシステムでパッチをソートできます。

ユーザー

すべての登録済みユーザおよび特定のユーザに関連するすべてのシステムを一覧にします。

CSV形式でレポートを取得するには、サーバのコマンドプロンプトで次のコマンドを実行します。

```
spacewalk-report <report_name>
```

21.2. spacewalk-reportおよびレポーティングデータベース

spacewalk-reportは、デフォルトで新しいレポーティングデータベースを使用してデータを抽出します。 これは、新しく生成されたレポートには、データの構造と形式にいくつかの相違があることを意味します。 す

べてのレポートに共通する相違点は次のとおりです。

- レポートデータはリアルタイムでは変更されず、スケジュールされたタスクの実行によってのみ更新されます。
- データの重複が削除され、以前は「多値」とみなされていた列には、**;**で区切られた複数の値が含まれるようになりました。 これはまた、コマンドラインオプション**--multival-on-rows**と **--multival-separator**が新しいレポートには適用されなくなったことも意味します。これは、これらの動作がデフォルトになったためです。
- すべてのレポートで、新しい列の**mgm_id**と**synced_date**が導入され、ハブシナリオの管理サーバと、アプリケーションデータベースから情報が最後に更新された時刻を識別します。
- すべてのブール値は、**1**/**0**値ではなく、**True**/**False**で表されるようになりました。
- 列**org_id**は、数値識別子ではなく組織名を含む、**organization** に置き換えられました。
- 「サーバ」という用語は「システム」に置き換えられました。 したがって、たとえば、列**server_id**は**system_id**と呼ばれるようになりました。

レポート固有の変更については、使用可能なレポートのリストを参照してください。

この変更された動作によって問題が発生した場合、新しいオプション**--legacy-report**を使用して、アプリケーションデータベースに対して実行される古いレポートにフォールバックできます。

hubレポートの詳細については、**Specialized-guides › Large-deployments** を参照してください。

21.3. 使用可能なレポートのリスト

この表は、使用可能なレポートを一覧表示します。

表 11. spacewalk-reportレポート

Report	Invoked as	Description	Uses reporting database	Specific differences
Actions	**actions**	All actions.	Yes	The column **id** is now called **action_id**
Activation Keys	**activation-keys**	All activation keys, and the entitlements, channels, configuration channels, system groups, and packages associated with them.	No	

Report	Invoked as	Description	Uses reporting database	Specific differences
Activation Keys: Channels	**activation-keys-channels**	All activation keys and the entities associated with each key.	No	
Activation Keys: Configuration	**activation-keys-config**	All activation keys and the configuration channels associated with each key.	No	
Activation Keys: Server Groups	**activation-keys-groups**	All activation keys and the system groups associated with each key.	No	
Activation Keys: Packages	**activation-keys-packages**	All activation keys and the packages each key can deploy.	No	
Channel Packages	**channel-packages**	All packages in a channel.	Yes	
Channel Report	**channels**	Detailed report of a given channel.	Yes	
Cloned Channel Report	**cloned-channels**	Detailed report of cloned channels.	Yes	
Configuration Files	**config-files**	All configuration file revisions for all organizations, including file contents and file information.	No	
Latest Configuration Files	**config-files-latest**	The most recent configuration file revisions for all organizations, including file contents and file information.	No	

Report	Invoked as	Description	Uses reporting database	Specific differences
Custom Channels	**custom-channels**	Channel metadata for all channels owned by specific organizations.	Yes	The column **id** is now called **channel_id**
Custom Info	**custom-info**	Client custom information.	Yes	
Patches in Channels	**errata-channels**	All patches in channels.	Yes	
Patches Details	**errata-list**	All patches that affect registered clients.	Yes	
All patches	**errata-list-all**	All patches.	No	
Patches for Clients	**errata-systems**	Applicable patches and any registered clients that are affected.	Yes	
Host Guests	**host-guests**	Host and guests mapping.	Yes	
Inactive Clients	**inactive-systems**	Inactive clients.	Yes	The mandatory parameter is now called **threshold**.
System Inventory	**inventory**	Clients registered to the server, together with hardware and software information.	Yes	The column **osad_status** has been removed.
Kickstart Scripts	**kickstart-scripts**	All kickstart scripts, with details.	No	
Kickstart Trees	**kickstartable-trees**	Kickstartable trees.	No	"
All Upgradable Versions	**packages-updates-all**	All newer package versions that can be upgraded.	Yes	
Newest Upgradable Version	**packages-updates-newest**	Newest package versions that can be upgraded.	Yes	

Report	Invoked as	Description	Uses reporting database	Specific differences
Proxy Overview	**proxies-overview**	All proxies and the clients registered to each.	Yes	
Repositories	**repositories**	All repositories, with their associated SSL details, and any filters.	No	
Result of SCAP	**scap-scan**	Result of OpenSCAP **sccdf** evaluations.	Yes	
Result of SCAP	**scap-scan-results**	Result of OpenSCAP **sccdf** evaluations, in a different format.	Yes	
System Data	**splice-export**	Client data needed for splice integration.	No	
System Currency	**system-currency**	Number of available patches for each registered client.	No	
System Extra Packages	**system-extra-packages**	All packages installed on all clients that are not available from channels the client is subscribed to.	Yes	
System Groups	**system-groups**	System groups.	Yes	
Activation Keys for System Groups	**system-groups-keys**	Activation keys for system groups.	No	
Systems in System Groups	**system-groups-systems**	Clients in system groups.	Yes	
System Groups Users	**system-groups-users**	System groups and users that have permissions on them.	No	
System Hardware	**system-hardware**	System hardware information.	No	

Report	Invoked as	Description	Uses reporting database	Specific differences
History: System	**system-history**	Event history for each client.	Yes	
History: Channels	**system-history-channels**	Channel event history.	Yes	
History: Configuration	**system-history-configuration**	Configuration event history.	Yes	The column **created_date** has been removed.
History: Entitlements	**system-history-entitlements**	System entitlement event history.	Yes	
History: Errata	**system-history-errata**	Errata event history.	Yes	The column **created_date** has been removed.
History: Kickstart	**system-history-kickstart**	Kickstart event history.	Yes	The column **created_date** has been removed.
History: Packages	**system-history-packages**	Package event history.	Yes	The column **created_date** has been removed.
History: SCAP	**system-history-scap**	OpenSCAP event history.	Yes	The column **created_date** has been removed.
MD5 Certificates	**system-md5-certificates**	All registered clients using certificates with an MD5 checksum.	No	
Installed Packages	**system-packages-installed**	Packages installed on clients.	Yes	
System Profiles	**system-profiles**	All clients registered to the server, with software and system group information.	No	
Users	**users**	All users registered to SUSE Multi-Linux Manager.	Yes	The column **organization_id** has been removed.

Report	Invoked as	Description	Uses reporting database	Specific differences
MD5 Users	**users-md5**	All users for all organizations using MD5 encrypted passwords, with their details and roles.	Yes	The column **organization_id** has been removed.
Systems administered	**users-systems**	Clients that individual users can administer.	Yes	The column **organization_id** has been removed.

個々のレポートに関する詳細については、オプション**--info**または**--list-fields-info**およびレポート名を指定して、**spacewalk-report**を実行します。 これにより、レポートに使用可能なフィールドの説明とリストが表示されます。

プログラムの呼び出しとオプションの詳細については、**spacewalk-report(8)**マニュアルページ、および**spacewalk-report**コマンドの**--help**パラメータを参照してください。

Chapter 22. セキュリティ

22.1. 監査

SUSE Multi-Linux Managerでは、一連の監査タスクを通じてクライアントを追跡できます。 クライアントがすべてのパブリックセキュリティパッチ(CVE)を適用して最新の状態になっていることを確認し、サブスクリプションマッチングを実行して、OpenSCAPを使用して仕様のコンプライアンスを確認できます。

SUSE Multi-Linux Manager Web UIで、［**監査**］に移動して、監査タスクを実行します。

22.1.1. CVE監査

CVE (共通脆弱性識別子)は、一般に知られているセキュリティの脆弱性に対する修正です。

CVEが利用可能になったらすぐにクライアントに適用する必要があります。

各CVEには、識別番号、脆弱性の説明、および詳細情報へのリンクが含まれています。 CVE識別番号は、**CVE-YEAR-XXXX**の形式を使用します。

SUSE Multi-Linux Manager Web UIで、**監査 › CVE監査**に移動して、すべてのクライアントとその現在のパッチステータスのリストを表示します。

デフォルトでは、パッチデータは毎日23:00に更新されます。 CVE監査を開始する前に、データを更新して最新のパッチが適用されていることを確認することをお勧めします。

プロシージャ: パッチデータの更新

1. SUSE Multi-Linux Manager Web UIで、**管理 › タスクスケジュール**に移動し、**cve-server-channels-default**スケジュールを選択します。
2. **[cve-server-channels-bunch]**をクリックします。
3. **[一回のみの実行スケジュール]**をクリックして、タスクをスケジュールします。 CVE監査を続行する前に、タスクを完了させてください。

プロシージャ: パッチステータスの確認

1. SUSE Multi-Linux Manager Web UIで、**監査 › CVE監査**に移動します。
2. 特定のCVEのパッチステータスを確認するには、［**CVE番号**］フィールドにCVE IDを入力します。
3. 検索するパッチステータスを選択するか、すべてのステータスをオンのままにしてすべてを検索します。
4. **[監査サーバ]**をクリックしてすべてのシステムを確認するか、**[監査イメージ]**をクリックしてすべてのイメージを確認します。

このページで使用されるパッチステータスアイコンの詳細については、**Reference › Audit**を参照してください。

各システムについて、［**アクション**］列には、脆弱性に対処するために実行する必要がある情報が表示されます。 該当する場合は、候補チャンネルまたはパッチのリストも表示されます。 さらにバッチ処理を行うためにシステムを［**システムセット**］に割り当てることもできます。

SUSE Multi-Linux Manager APIを使用して、クライアントのパッチステータスを確認できます。 **audit.listSystemsByPatchStatus** APIメソッドを使用します。 このメソッドの詳細については、『SUSE Multi-Linux Manager API ガイド』を参照してください。

22.1.2. OVAL

チャンネルデータからCVE情報を取得する機能に加え、SUSE Multi-Linux Managerには現在、OVALファイルからCVEの詳細をフェッチする実験的な機能が含まれています。 この機能は現在、**テクノロジプレビュー**として提供されています。

ユーザは、この機能を試してフィードバックを共有することが推奨されます。 ただし、テスト環境での徹底的なテストを行わずに、運用環境で使用することは推奨されません。

CVE監査操作は、チャンネルとOVAL (Open Vulnerability and Assessment Language)という2つの主要なデータソースに依存しています。 これらの2つのソースは、CVE監査を実施するためのメタデータを提供し、それぞれが異なる目的を果たします。

チャンネル

チャンネルには、パッチを含む更新されたソフトウェアパッケージが含まれており、脆弱性に対処するために必要な重要なパッチに関する洞察を提供します。

OVAL (テクノロジプレビュー)

対照的に、OVALデータは、脆弱性そのものに関する情報、およびシステムをCVEに対して脆弱にするパッケージに関する情報を提供します。

CVE監査はチャンネルデータのみを使用して実施できますが、OVALデータを同期させることで、特に、ゼロデイ脆弱性や部分的にパッチが適用された脆弱性に関連するケースで、結果の精度が向上します。

OVALデータはチャンネルデータよりもはるかに軽量です。 たとえば、openSUSE Leap 15.4のOVALデータは約50MB です。

OVALデータを同期しただけで、すでに CVE 監査を実施し、システムがCVEに対して脆弱かどうかを確認できます。ただし、パッチはチャンネルから取得されるため、パッチを適用することはできません。

OVAL機能の主な特徴は次のとおりです。

- **デフォルトで無効化**: この機能はデフォルトでオフになっており、ユーザが設定ファイル**rhn.conf**を更新し、関連するサービスを再起動することで明示的に有効化する必要があります。
- **元に戻せる**: 問題が発生した場合、ユーザは標準のチャンネルベースのCVE監査に戻すことができます。

- **パフォーマンスに関する考慮事項**:　初期テストは実施済みですが、パフォーマンスに関する懸念がまだあり、さらなる最適化が必要になる場合があります。
- デフォルトでは、OVALデータは毎日23:00に更新されます。　CVE監査を開始する前に、データを更新して最新の脆弱性メタデータが適用されていることを確認することをお勧めします。

プロシージャ: OVALデータサポートを有効にする

1. Add or modify the following setting in file **/etc/rhn/rhn.conf** in the container:

```
java.cve_audit.enable_oval_metadata=true
```

2. TomcatおよびTaskomaticサービスを再起動します。

```
systemctl restart tomcat taskomatic
```

問題が発生し、デフォルトの動作に戻す必要がある場合は、次のように設定してこの機能を無効にしてください。

プロシージャ: OVALデータサポートの無効化

1. **rhn.conf**に次の設定を追加または編集します。

```
java.cve_audit.enable_oval_metadata=false
```

2. TomcatおよびTaskomaticサービスを再起動します。

```
systemctl restart tomcat taskomatic
```

プロシージャ: OVALデータの更新

1. SUSE Multi-Linux Manager Web UIで、**管理 › タスクスケジュール**に移動し、**oval-data-sync-default**スケジュールを選択します。
2. **[oval-data-sync-bunch]**をクリックします。
3. **[1 回のみの実行スケジュール]**をクリックして、タスクをスケジュールします。

CVE監査を続行する前に、タスクを完了させてください。

22.1.2.1. CPEの収集

特定のクライアントに適用される脆弱性を正確に特定するには、そのクライアントが使用しているオペレーティングシステム製品を特定する必要があります。そのため、クライアントのCPE　(Common　Platform Enumeration)をsalt grainとして収集し、データベースに保存します。

新規登録されたクライアントのCPEは、自動的に収集され、データベースに保存されます。　ただし、既存の

クライアントについては、少なくとも1回**パッケージリストの更新**アクションを実行する必要があります。

プロシージャ: パッケージリストの更新

1. SUSE Multi-Linux Manager Web UIで、**システム › システム一覧 › すべて**に移動して、クライアントを選択します。
2. ［**ソフトウェア**］タブに移動し、［**パッケージ**］サブタブを選択します。
3. **[Update Packages List]**（パッケージリストの更新）をクリックして、クライアントのCPEを収集します。

22.1.2.2. OVALソース

OVALデータの完全性と最新性を確保するため、SUSE Multi-Linux Managerは、すべての製品の公式メンテナーから提供されるOVALデータを排他的に使用します。以下に、OVALデータソースのリストを示します。

表 12. OVALソース

製品	ソースURL
openSUSE Leap	https://ftp.suse.com/pub/projects/security/oval
openSUSE Leap Micro	
SUSE Linux Enterprise Server	
SUSE Linux Enterprise Desktop	
SUSE Linux Enterprise Micro	
RedHat Enterprise Linux	https://www.redhat.com/security/data/oval/v2
Debian	https://www.debian.org/security/oval
Ubuntu	https://security-metadata.canonical.com/oval

OVALメタデータは、CVE監査でクライアントのサブセット、すなわち、openSUSE Leap、SUSEエンタープライズ製品、RHEL、Debian、またはUbuntuを使用するクライアントのみに使用されます。これは、他の製品にはOVAL脆弱性定義メタデータが存在しないためです。

22.1.3. CVEステータス

クライアントのCVEステータスは通常、**影響を受けています**、**影響を受けません**、または**パッチ適用済み**のいずれかです。 これらのステータスは、SUSE Multi-Linux Managerで使用できる情報にのみ基づいています。

SUSE Multi-Linux Manager内で、次の定義が適用されます。

特定の脆弱性の影響を受けるシステム

脆弱性がマークされた関連パッチ内の同じパッケージのバージョンより前のバージョンのパッケージがインストールされているシステム。

特定の脆弱性の影響を受けないシステム

脆弱性がマークされた関連パッチにも含まれているパッケージがインストールされていないシステム。

特定の脆弱性に対するパッチが適用されたシステム

脆弱性がマークされた関連パッチ内の同じパッケージのバージョン以上のバージョンのパッケージがインストールされているシステム。

関連パッチ

関連するチャンネルでSUSE Multi-Linux Managerによって知られているパッチ。

関連するチャンネル

システムに割り当てられたSUSE Multi-Linux Managerによって管理されるチャンネル、システムに割り当てられたクローンチャンネルのオリジナルチャンネル、システムにインストールされている製品にリンクされたチャンネル、またはシステムの過去または将来のサービスパックチャンネル。

SUSE Multi-Linux Manager内で使用されている定義のため、状況によってはCVE監査結果が正しくない場合があります。 たとえば、管理されていないチャンネル、管理されていないパッケージ、または準拠していないシステムが誤って報告される可能性があります。

22.2. クライアントをマスター検証指紋に設定する

高度に安全なネットワーク設定では、Saltクライアントが特定のマスターに接続していることを確認したい場合があります。クライアントからマスターへの検証を設定するには、Salt Minionの設定ファイル内にマスターの指紋を入力します。

- クライアントでSalt Minionを使用している場合、**/etc/salt/minion.d/custom.conf**
- クライアントでSalt Bundleを使用している場合、**/etc/venv-salt-minion/minion.d/custom.conf**

その後、次のプロシージャに従います。

サーバコンテナ内でシェルにアクセスするには、コンテナホストで**mgrctl term**を実行します。

プロシージャ: マスターの指紋をクライアントに追加する

1. マスターのコマンドプロンプトで、rootとして、次のコマンドを使用して、**master.pub**の指紋を見つけます。

```
salt-key -F master
```

クライアントで、**/etc/salt/minion.d/custom.conf**または**/etc/venv-salt-minion/minion.d/custom.conf**設定ファイルを開きます。次の行を、指紋の例を置き換えてマスターの指紋に追加します。

```
master_finger: 'ba:30:65:2a:d6:9e:20:4f:d8:b2:f3:a7:d4:65:11:13'
```

2. サービスを再起動します。salt-minionの場合は、次のコマンドを実行します。

```
systemctl restart salt-minion
```

3. または、venv-salt-minionの場合は、次のコマンドを実行します。

```
systemctl restart venv-salt-minion
```

Salt Bundleの詳細については、**Client-configuration › Contact-methods-saltbundle**を参照してください。

クライアントからのセキュリティの設定については、https://docs.saltproject.io/en/latest/ref/configuration/minion.htmlを参照してください。

22.3. ミラーソースパッケージ

独自のパッケージをローカルに構築する場合、または法的な理由でパッケージのソースコードが必要な場合は、SUSE Multi-Linux Managerサーバ上のソースパッケージをミラーリングできます。

ソースパッケージをミラーリングすると、大量のディスク容量が消費される可能性があります。

サーバコンテナでステップを実行する前に、**mgrctl term**を使用します。

プロシージャ: ソースパッケージのミラーリング

1. **/etc/rhn/rhn.conf**設定ファイルを開いて、次の行を追加します。

```
server.sync_source_packages = 1
```

2. Spacewalkサービスを再起動して、変更を取得します。

```
mgradm restart
```

現在、この機能はすべてのリポジトリに対してグローバルにのみ有効にできます。 ミラーリングに個々のリポジトリを選択することはできません。

この機能を有効にすると、次のリポジトリ同期後に、ソースパッケージがSUSE Multi-Linux Manager Web UIで使用できるようになります。 これらはバイナリパッケージのソースとして表示され、Web UIから直接ダウンロードできます。 Web UIを使用して、ソースパッケージをクライアントにインストールすることはできません。

22.4. OpenSCAPによるシステムセキュリティ

SUSE Multi-Linux ManagerはOpenSCAPを使用してクライアントを監査します。 任意のクライアントのコンプライアンススキャンをスケジュールして表示できます。

22.4.1. SCAPについて

Security Content Automation Protocol (SCAP)は、コミュニティのアイデアから派生した相互運用可能な仕様を統合したものです。 これは、エンタープライズシステムのシステムセキュリティを維持するために、National Institute of Standards and Technology (NIST)によって維持されている一連の仕様です。

SCAPは、システムのセキュリティを維持するための標準化されたアプローチを提供するために作成されました。また、使用される標準は、コミュニティや企業のビジネスニーズを満たすために継続的に変更されます。 新しい仕様はNISTのSCAPリリースサイクルによって管理され、一貫性のある再現可能な改訂ワークフローを提供します。 詳細については、以下を参照してください。

- https://csrc.nist.gov/projects/security-content-automation-protocol
- https://www.open-scap.org/features/standards/
- https://ncp.nist.gov/repository?scap

SUSE Multi-Linux ManagerはOpenSCAPを使用してSCAP仕様を実装します。 OpenSCAPは、Extensible Configuration Checklist Description Format (XCCDF)を利用した監査ツールです。 XCCDFは、チェックリストの内容を表現する標準的な方法であり、セキュリティチェックリストを定義します。また、Common Platform Enumeration (CPE)、Common Configuration Enumeration (CCE)、Open Vulnerability and Assessment Language (OVAL)などの他の仕様と組み合わせて、SCAP検証済みの製品で処理できるSCAP表現のチェックリストを作成します。

OpenSCAPはSUSEセキュリティチームが作成したコンテンツを使用して、パッチの存在を確認します。 OpenSCAPは、システムセキュリティ設定をチェックし、標準と仕様に基づいたルールを使用して、システムに侵害の兆候がないかどうかを検査します。 SUSEセキュリティチームの詳細については、https://www.suse.com/support/securityを参照してください。

22.4.2. Prepare clients for an SCAP scan

開始する前に、SCAPスキャン用にクライアントシステムを準備する必要があります。

OpenSCAP監査は、SSH接続メソッドを使用するSaltクライアントでは使用できません。

スキャンクライアントは、スキャンするクライアントのメモリと計算能力を大量に消費する可能性があります。 Red Hatクライアントの場合、スキャンする各クライアントで少なくとも2GBのRAMが使用可能であることを確認してください。

開始する前にOpenSCAPスキャナとSCAPセキュリティガイド(コンテンツ)パッケージをインストールしてください。オペレーティングシステムに応じて、これらのパッケージはベースオペレーティングシステムまたはSUSE Multi-Linux Managerクライアントツールのいずれかに含まれています。

次の表に、必要なパッケージを一覧表示します。

表 13. OpenSCAPパッケージ

オペレーティングシステム	スキャナ	コンテンツ
SLES	openscap-utils	scap-security-guide
openSUSE	openscap-utils	scap-security-guide
RHEL	openscap-utils	scap-security-guide-redhat
CentOS	openscap-utils	scap-security-guide-redhat
Oracle Linux	openscap-utils	scap-security-guide-redhat
Ubuntu	libopenscap8	scap-security-guide-ubuntu
Debian	libopenscap8	scap-security-guide-debian

RHEL 7および互換システムでは、**scap-security-guide**パッケージが提供されています。このパッケージには、古い内容が含まれています。 SUSE Multi-Linux Managerクライアントツールにある**scap-security-guide-redhat**パッケージを使用することをお勧めします。

SUSEは、異なるOpenSCAPプロファイル用の **scap-security-guide**パッケージを提供しています。 **scap-security-guide**の現在のバージョンでは、SUSEは次のプロファイルをサポートしています。

- SUSE Linux Enterprise Server 12および15のDISA STIGプロファイル
- SUSE Linux Enterprise Server 12および15のANSSI-BP-028プロファイル
- SUSE Linux Enterprise Server 12および15のPCI-DSSプロファイル
- SUSE Linux Enterprise Server 15のHIPAAプロファイル
- SUSE Linux Enterprise Server 12および15のCISプロファイル
- SUSE Linux Enterprise Server for SAP Applications 15のパブリッククラウドイメージ用の強化
- SUSE Linux Enterprise 15用のパブリッククラウドの強化
- SLE 12および15の標準のシステムセキュリティプロファイル

このリストに記載されていない他のプロファイルは、コミュニティが提供するものであり、SUSEによって公式にサポートされていません。

SUSE以外のオペレーティングシステムの場合、含まれるプロファイルはコミュニティが提供します。 これらはSUSEによって公式にサポートされていません。

22.4.3. OpenSCAP content files

OpenSCAPは、SCAPコンテンツファイルを使用してテストルールを定義します。 これらのコンテンツファ

イルは、XCCDFまたはOVAL標準に基づいて作成されます。 『SCAPセキュリティガイド』に加えて、公開されているコンテンツファイルをダウンロードして、要件に合わせてカスタマイズできます。 デフォルトのコンテンツファイルテンプレート用のSCAPセキュリティガイドパッケージをインストールできます。 または、XCCDFまたはOVALに精通している場合は、独自のコンテンツファイルを作成できます。

テンプレートを使用してSCAPコンテンツファイルを作成することをお勧めします。 独自のカスタムコンテンツファイルを作成して使用する場合は、自己責任で作成してください。 カスタムコンテンツファイルを使用してシステムが破損した場合、SUSEのサポートを受けられない可能性があります。

コンテンツファイルを作成したら、ファイルをクライアントに転送する必要があります。 これは、物理的なストレージメディアを使用して他のファイルを移動するのと同じ方法で行うことができます。または、Salt（たとえば、salt-cpやSalt File Server)、**ftp**や**scp**を使用してネットワークを介して移動することもできます。

SUSE Multi-Linux Managerで管理しているクライアントにコンテンツファイルを配布するパッケージを作成することをお勧めします。 パッケージの整合性を確認するために、パッケージに署名して検証することができます。 詳細については、**Administration › Custom-channels**を参照してください。

22.4.4. OpenSCAPプロファイルの検索

オペレーティングシステムによって、使用可能なOpenSCAPコンテンツファイルとプロファイルが異なります。 1つのコンテンツファイルに複数のプロファイルを含めることができます。

RPMベースのオペレーティングシステムでは、次のコマンドを使用して、使用可能なSCAPファイルの場所を決定します。

```
rpm -ql <scap-security-guide-package-name-from-table>
```

DEBベースのオペレーティングシステムでは、次のコマンドを使用して、使用可能なSCAPファイルの場所を決定します。

```
dpkg -L <scap-security-guide-package-name-from-table>
```

ニーズに合う1つの SCAPコンテンツファイルを特定したら、クライアントに使用可能なプロファイルを一覧にします。

```
oscap info /usr/share/xml/scap/ssg/content/ssg-sle15-ds.xml
Document type: Source Data Stream
Imported: 2021-03-24T18:14:45

Stream: scap_org.open-scap_datastream_from_xccdf_ssg-sle15-xccdf-1.2.xml
Generated: (null)
Version: 1.2
Checklists:
        Ref-Id: scap_org.open-scap_cref_ssg-sle15-xccdf-1.2.xml
                Status: draft
                Generated: 2021-03-24
                Resolved: true
                Profiles:
```

```
                        Title: CIS SUSE Linux Enterprise 15 Benchmark
                                Id: xccdf_org.ssgproject.content_profile_cis
                        Title: Standard System Security Profile for SUSE Linux Enterprise
15
                                Id: xccdf_org.ssgproject.content_profile_standard
                        Title: DISA STIG for SUSE Linux Enterprise 15
                                Id: xccdf_org.ssgproject.content_profile_stig
                Referenced check files:
                        ssg-sle15-oval.xml
                                system: http://oval.mitre.org/XMLSchema/oval-definitions-5
                        ssg-sle15-ocil.xml
                                system: http://scap.nist.gov/schema/ocil/2

https://ftp.suse.com/pub/projects/security/oval/suse.linux.enterprise.15.xml
                                system: http://oval.mitre.org/XMLSchema/oval-definitions-5
Checks:
        Ref-Id: scap_org.open-scap_cref_ssg-sle15-oval.xml
        Ref-Id: scap_org.open-scap_cref_ssg-sle15-ocil.xml
        Ref-Id: scap_org.open-scap_cref_ssg-sle15-cpe-oval.xml
Dictionaries:
        Ref-Id: scap_org.open-scap_cref_ssg-sle15-cpe-dictionary.xml
```

スキャンを実行するためのファイルパスとプロファイルをメモします。

22.4.5. Perform an audit scan

コンテンツファイルをインストールまたは転送したら、監査スキャンを実行できます。 監査スキャンは、SUSE Multi-Linux Manager Web UIを使用してトリガできます。 SUSE Multi-Linux Manager APIを使用して、定期的なスキャンをスケジュールすることもできます。

Procedure: Running an audit scan from the Web UI

1. SUSE Multi-Linux Manager Web UIで、**システム › システム一覧**に移動して、スキャンするクライアントを選択します。
2. ［**監査**］タブ、および［**スケジュール**］サブタブに移動します。
3. ［**XCCDFドキュメントへのパス**］フィールドに、クライアントで使用するSCAPテンプレートとプロファイルのパラメータを入力します。 例:
   - **Command**: /usr/bin/oscap xccdf eval
   - **Command-line arguments**: --profile xccdf_org.ssgproject.content_profile_stig
   - **Path to XCCDF document**: /usr/share/xml/scap/ssg/content/ssg-sle15-ds.xml

--fetch-remote-resourcesパラメータを使用する場合は、大量のRAMが必要です。 さらに、**file_recv_max_size**の値を増やす必要がある場合があります。

4. スキャンは、クライアントの次にスケジュールされた同期時に実行されます。

XCCDFコンテンツファイルはリモートシステムで実行される前に検証されます。 コンテンツファイルに無効な引数が含まれている場合は、テストに失敗します。

Procedure: Running an audit scan from the API

1. 開始する前に、スキャンするクライアントにPythonおよびXML-RPCライブラリがインストールされていることを確認します。
2. 既存のスクリプトを選択するか、**system.scap.scheduleXccdfScan**を使用してシステムスキャンをスケジュールするスクリプトを作成します。 例:

```
#!/usr/bin/python3
import xmlrpc.client
client = xmlrpc.client.ServerProxy('https://server.example.com/rpc/api')
key = client.auth.login('username', 'password')
client.system.scap.scheduleXccdfScan(key, <1000010001>,
    '<path_to_xccdf_file.xml>',
    '--profile <profile_name>')
client.auth.logout(session_key)
```

この例では:

- **<1000010001>**はシステムID (sid)です。
- **<path_to_xccdf_file.xml>** is the path to the content file location on the client. For example, **/usr/share/xml/scap/ssg/content/ssg-sle15-ds.xml.**
- **<profile_name>**は**oscap**コマンドの追加の引数です。 たとえば、**united_states_government_configuration_baseline** (USGCB)を使用します。

3. コマンドプロンプトから、スキャンするクライアント上でスクリプトを実行します。

22.4.6. Scan results

実行したスキャンに関する情報は、SUSE Multi-Linux Manager Web UIにあります。 結果の表を表示するには、**監査 › OpenSCAP › 全スキャン**に移動します。 この表のデータの詳細については、**Reference › Audit**を参照してください。

スキャンに関する詳細情報を使用できるようにするには、クライアントで有効にする必要があります。 SUSE Multi-Linux Manager Web UIで、**管理 › 組織**に移動し、クライアントが属する組織をクリックします。 ［**設定**］タブに移動し、［**詳細なSCAPファイルのアップロードを有効にする**］オプションをオンにします。 有効にすると、スキャンごとに、追加情報を含む追加のHTMLファイルが生成されます。 結果には、次のよ

うな追加の行が表示されます。

```
Detailed Results: xccdf-report.html xccdf-results.xml scap-yast2sec-oval.xml.result.xml
```

コマンドラインからスキャン情報を取得するには、**spacewalk-report**コマンドを使用します。

```
spacewalk-report system-history-scap
spacewalk-report scap-scan
spacewalk-report scap-scan-results
```

SUSE Multi-Linux Manager APIを使用して、**system.scap**ハンドラを使用して結果を表示することもできます。

22.4.7. 修復

クライアントシステムを強化するために、修復用のBashスクリプトとAnsible playbookが同じSCAPセキュリティガイドパッケージで提供されます。 例:

リスト 5. bashスクリプト

```
/usr/share/scap-security-guide/bash/sle15-script-cis.sh
/usr/share/scap-security-guide/bash/sle15-script-standard.sh
/usr/share/scap-security-guide/bash/sle15-script-stig.sh
```

リスト 6. Ansible playbook

```
/usr/share/scap-security-guide/ansible/sle15-playbook-cis.yml
/usr/share/scap-security-guide/ansible/sle15-playbook-standard.yml
/usr/share/scap-security-guide/ansible/sle15-playbook-stig.yml
```

クライアントシステムでAnsibleを有効にした後、リモートコマンドまたはAnsibleを使用して実行できます。

22.4.7.1. Bashスクリプトを使用して修復を実行する

scap-security-guideパッケージをすべてのターゲットシステムにインストールします。 詳細については、**Administration › Ansible-setup-control-node**を参照してください。

パッケージ、チャンネル、スクリプトは、オペレーティングシステムと配布ごとに異なります。 修復Bashスクリプトの例セクションに例を一覧表示しています。

22.4.7.1.1. リモートコマンドとして単一システムでBashスクリプトを実行する

単一システムでリモートコマンドとしてBashスクリプトを実行します。

1. **システム › 概要**タブから、インスタンスを選択します。 次に、**詳細 › リモートコマンド**で、Bashスクリプトを次のように記述します。

```
#!/bin/bash
chmod +x -R /usr/share/scap-security-guide/bash
/usr/share/scap-security-guide/bash/sle15-script-stig.sh
```

2. **[Schedule]** をクリックします。

配布とバージョンの間でフォルダ名とスクリプト名が変わります。 修復Bashスクリプトの例セクションに例を一覧表示しています。

22.4.7.1.2. 複数のシステムでシステムセットマネージャを使用してbashスクリプトを実行する

複数のシステムでリモートコマンドとして一度にBashスクリプトを実行します。

1. システムグループが作成されたら［**システムグループ**］をクリックし、テーブルから［**SSM で 使用**］を選択します。
2. ［**システムセットマネージャ**］から、**その他 › リモートコマンド**の下で、次のようなBashスクリプトを記述します。

```
#!/bin/bash
chmod +x -R /usr/share/scap-security-guide/bash
/usr/share/scap-security-guide/bash/sle15-script-stig.sh
```

3. **[Schedule]** をクリックします。

22.4.7.2. 修復Bashスクリプトの例

22.4.7.2.1. SUSE Linux Enterprise openSUSEおよび亜種

SUSE Linux EnterpriseおよびopenSUSEスクリプトデータの例。

パッケージ

scap-security-guide

チャンネル

- SLE12: SLES12 Updates
- SLE15: SLES15 Module Basesystem Updates

Bashスクリプトディレクトリ

/usr/share/scap-security-guide/bash/

Bashスクリプト

```
opensuse-script-standard.sh
sle12-script-standard.sh
sle12-script-stig.sh
sle15-script-cis.sh
sle15-script-standard.sh
sle15-script-stig.sh
```

22.4.7.2.2. Red Hat Enterprise LinuxおよびCentOS Bashスクリプトデータ

Red Hat Enterprise LinuxおよびCentOSスクリプトデータの例。

centos7-updatesの**scap-security-guide**には、Red Hat Enterprise Linuxスクリプトのみが含まれています。

パッケージ

scap-security-guide-redhat

チャンネル

- SUSE Managerツール

Bashスクリプトディレクトリ

/usr/share/scap-security-guide/bash/

Bashスクリプト

```
centos7-script-pci-dss.sh
centos7-script-standard.sh
centos8-script-pci-dss.sh
centos8-script-standard.sh
fedora-script-ospp.sh
fedora-script-pci-dss.sh
fedora-script-standard.sh
ol7-script-anssi_nt28_enhanced.sh
ol7-script-anssi_nt28_high.sh
ol7-script-anssi_nt28_intermediary.sh
ol7-script-anssi_nt28_minimal.sh
ol7-script-cjis.sh
ol7-script-cui.sh
ol7-script-e8.sh
ol7-script-hipaa.sh
ol7-script-ospp.sh
ol7-script-pci-dss.sh
ol7-script-sap.sh
ol7-script-standard.sh
ol7-script-stig.sh
ol8-script-anssi_bp28_enhanced.sh
ol8-script-anssi_bp28_high.sh
ol8-script-anssi_bp28_intermediary.sh
ol8-script-anssi_bp28_minimal.sh
ol8-script-cjis.sh
ol8-script-cui.sh
ol8-script-e8.sh
ol8-script-hipaa.sh
ol8-script-ospp.sh
ol8-script-pci-dss.sh
ol8-script-standard.sh
rhel7-script-anssi_nt28_enhanced.sh
rhel7-script-anssi_nt28_high.sh
rhel7-script-anssi_nt28_intermediary.sh
rhel7-script-anssi_nt28_minimal.sh
rhel7-script-C2S.sh
rhel7-script-cis.sh
rhel7-script-cjis.sh
rhel7-script-cui.sh
rhel7-script-e8.sh
rhel7-script-hipaa.sh
```

```
rhel7-script-ncp.sh
rhel7-script-ospp.sh
rhel7-script-pci-dss.sh
rhel7-script-rhelh-stig.sh
rhel7-script-rhelh-vpp.sh
rhel7-script-rht-ccp.sh
rhel7-script-standard.sh
rhel7-script-stig_gui.sh
rhel7-script-stig.sh
rhel8-script-anssi_bp28_enhanced.sh
rhel8-script-anssi_bp28_high.sh
rhel8-script-anssi_bp28_intermediary.sh
rhel8-script-anssi_bp28_minimal.sh
rhel8-script-cis.sh
rhel8-script-cjis.sh
rhel8-script-cui.sh
rhel8-script-e8.sh
rhel8-script-hipaa.sh
rhel8-script-ism_o.sh
rhel8-script-ospp.sh
rhel8-script-pci-dss.sh
rhel8-script-rhelh-stig.sh
rhel8-script-rhelh-vpp.sh
rhel8-script-rht-ccp.sh
rhel8-script-standard.sh
rhel8-script-stig_gui.sh
rhel8-script-stig.sh
rhel9-script-pci-dss.sh
rhosp10-script-cui.sh
rhosp10-script-stig.sh
rhosp13-script-stig.sh
rhv4-script-pci-dss.sh
rhv4-script-rhvh-stig.sh
rhv4-script-rhvh-vpp.sh
sl7-script-pci-dss.sh
sl7-script-standard.sh
```

22.4.7.2.3. Ubuntu Bashスクリプトデータ

Ubuntuスクリプトデータの例。

パッケージ

scap-security-guide-ubuntu

チャンネル

- SUSE Managerツール

Bashスクリプトディレクトリ

/usr/share/scap-security-guide/

Bashスクリプト

```
ubuntu1804-script-anssi_np_nt28_average.sh
ubuntu1804-script-anssi_np_nt28_high.sh
ubuntu1804-script-anssi_np_nt28_minimal.sh
ubuntu1804-script-anssi_np_nt28_restrictive.sh
ubuntu1804-script-cis.sh
ubuntu1804-script-standard.sh
```

```
ubuntu2004-script-standard.sh
```

22.4.7.2.4. Debian Bashスクリプトデータ

Debianスクリプトデータの例。

パッケージ

scap-security-guide-debian

チャンネル

- SUSE Managerツール

Bashスクリプトディレクトリ

/usr/share/scap-security-guide/bash/

Bashスクリプト

```
# Debian 12
debian12-script-anssi_np_nt28_average.sh
debian12-script-anssi_np_nt28_high.sh
debian12-script-anssi_np_nt28_minimal.sh
debian12-script-anssi_np_nt28_restrictive.sh
debian12-script-standard.sh
```

22.5. リポジトリメタデータ

リポジトリメタデータを署名できるようにするにはカスタムGPGキーが必要です。

サーバコンテナ内でシェルにアクセスするには、コンテナホストで**mgrctl term**を実行します。

プロシージャ: カスタムGPGキーの生成

1. rootユーザとして、**gpg**コマンドを使用して、新しいキーを生成します。

```
mgrctl exec -- gpg --full-generate-key
```

2. プロンプトが表示されたら、サイズが2048ビットの**RSA**をキータイプとして選択し、キーの適切な有効期限を選択します。 新しいキーの詳細を確認して、「**y**」と入力して確定します。
3. プロンプトが表示されたら、キーに関連付けられた名前と電子メールアドレスを入力します。 必要に応じて、キーの識別に役立つコメントを追加することもできます。 ユーザIDに問題がなければ、「**O** 」と入力して確定します。
4. プロンプトが表示されたら、キーを保護するパスフレーズを入力します。
5. キーは自動的にキーリングに追加されます。 キーリングにキーを一覧表示して確認できます。

```
gpg --list-keys
```

6. テキストエディタでファイルを開き、次の行を追加して、キーリングのパスワードを**/etc/rhn/signing.conf**設定ファイルに追加します。

```
GPGPASS="password"
```

GPGキーの更新については、**Administration › Troubleshooting**を参照してください。

mgr-sign-metadata-ctlコマンドを使用してコマンドラインでメタデータ署名を管理できます。

プロシージャ: メタデータ署名の有効化

1. 使用するキーの短い識別子を知っている必要があります。 使用可能な公開鍵を短い形式で一覧表示できます。

```
mgrctl exec -- gpg --keyid-format short --list-keys
...
pub   rsa4096/3E7BFE0A 2019-04-02 [SC] [expires: 2029-04-01]
      A43F9EC645ED838ED3014B035CFA51BF3E7BFE0A
uid         [ultimate] SUSE Manager
sub   rsa4096/118DE7FF 2019-04-02 [E] [expires: 2029-04-01]
```

2. **mgr-sign-metadata-ctl**コマンドを使用してメタデータ署名を有効化します。

```
mgrctl exec -- mgr-sign-metadata-ctl enable 3E7BFE0A
OK. Found key 3E7BFE0A in keyring.
DONE. Set key 3E7BFE0A in /etc/rhn/signing.conf.
DONE. Enabled metadata signing in /etc/rhn/rhn.conf.
DONE. Exported key 3E7BFE0A to /srv/susemanager/salt/gpg/mgr-keyring.gpg.
DONE. Exported key 3E7BFE0A to /var/spacewalk/gpg/<KEY_NAME>.key.
NOTE. For the changes to become effective run:
   mgr-sign-metadata-ctl regen-metadata
```

3. このコマンドを使用して設定が正しいことを確認できます。

```
mgrctl exec -- mgr-sign-metadata-ctl check-config
```

4. サービスを再起動し、メタデータの再生成をスケジュールして変更を取得します。

```
mgrctl exec -- mgr-sign-metadata-ctl regen-metadata
```

mgr-sign-metadata-ctlコマンドを使用して他のタスクを実行することもできます。 **mgr-sign-metadata-ctl --help**を使用して、完全なリストを表示します。

リポジトリメタデータ署名はグローバルオプションです。 有効にすると、サーバ上のすべてのソフトウェアチャンネルで有効になります。 これは、サーバに接続されているすべてのクライアントが、パッケージをインストールまたは更新できるようにするために、新しいGPGキーを信頼する必要があることを意味します。

プロシージャ: クライアントへのGPGキーのインポート

1. GPGキーをクライアントに配備すると、salt状態で動作します。
2. SUSE Multi-Linux Manager Web UIを使用してhighstateを適用します。

GPGキーのトラブルシューティングの詳細については、**Administration › Troubleshooting**を参照してください。

Chapter 23. ロールベースのアクセス制御(RBAC)

ロールベースのアクセス制御(RBAC)は、割り当てられたロールに基づいて、許可されたユーザのみがリソースにアクセスできるようにするセキュリティ手法です。SUSE Multi-Linux Managerでは、RBACによりユーザは明示的に許可されたアクションやリソースへのアクセスのみを実行できるようになり、セキュリティが強化され、管理が簡素化されます。

RBACのコア原則は次のとおりです。

- **最小権限の原則:** ユーザがタスクを実行するために必要なアクセス権のみを付与する。
- **きめ細かな制御:** 特定の機能に対してきめ細かな制御を提供する。
- **職務の分離:** 単一ユーザが重要なプロセスに対して過度に制御することを防止する。
- **監査可能性:** ユーザのアクションと許可を明確に追跡できるようにする。

23.1. RBACの主要概念

効果的なRBAC管理には、以下のコア概念を理解することが重要です。

- **Role:** A collection of permissions defining a specific set of capabilities within SUSE Multi-Linux Manager.

  Roles are assigned to users, granting the user aggregated permissions.

- **許可:** SUSE Multi-Linux Manager内で特定のアクションを実行したり、特定のWebページにアクセスしたり、特定のAPIエンドポイントを呼び出したりするためのアトミック認可。SUSE Multi-Linux Managerでは、許可はネームスペースとそのアクセスモードによって表されます。
- **ユーザ:** SUSE Multi-Linux Managerとやり取りする個々のアカウント。ユーザには1つ以上のロールが割り当てられます。
- **ネームスペース:** ツリーのような構造で構成された、アクセス制御のきめ細かな単位。ほとんどのネームスペースには、明確な「表示」モードまたは「変更」モードがあります。

23.2. SUSE Multi-Linux Managerでのユーザロール

SUSE Multi-Linux Managerでは、事前定義されたロールを提供し、オプションで、他のロールの組み合わせを継承して追加のカスタムロールを定義することもできます。

23.2.1. 事前定義済みロール

事前定義済みロールとその説明の完全なリストについては、administration:users.pdfを参照してください。

23.2.2. 追加のロールの定義

追加のロールを定義するには、次の操作を実行できます。

- 許可を継承する既存のロールを複数選択する。
- アクセスを許可する追加のネームスペースを指定する。

23.3. きめ細かなアクセスのためのネームスペース

ネームスペースはツリーのような構造で構成された、きめ細かなアクセス制御を提供します。ほとんどのネームスペースでは、ネームスペース内のアクセスは「表示」モードと「変更」モードによってさらに細分化されます。

表 14. 例: イメージ管理のネームスペースとアクセスモード

ネームスペース	アクセスモード	説明
cm.build	変更	コンテナまたはKiwiイメージを構築します
cm.image.import	変更	登録済みイメージストアからコンテナイメージを取り込みます
cm.image.list	表示	すべてのイメージを一覧表示します
cm.image.list	変更	イメージを削除します
cm.image.overview	表示	イメージの詳細、パッチ、パッケージ、構築ログ、クラスタ情報を表示します
cm.image.overview	変更	イメージを検査、再構築、削除します
cm.profile.details	表示	イメージプロファイルの詳細を表示します
cm.profile.details	変更	イメージプロファイルを作成し、プロファイルの詳細を編集します
cm.profile.list	表示	すべてのイメージプロファイルを一覧表示します
cm.profile.list	変更	イメージプロファイルを削除します
cm.store.details	表示	イメージストアの詳細を表示します
cm.store.details	変更	イメージストアを作成し、ストアの詳細を編集します
cm.store.list	表示	すべてのイメージストアを一覧表示します
cm.store.list	変更	イメージストアを削除します

ネームスペースとその説明の包括的なリストは、**access.listNamespaces** APIメソッドを呼び出すことで取得できます。 リクエストおよび応答形式を含む詳細については、SUSE Multi-Linux Manager APIドキュメントを参照してください。

23.4. RBACの管理

RBACロールと許可の管理は現在、APIを通じてのみ可能です。 Web UIを介してユーザにロールを割り当てるには、 **Administration › Users**を参照してください。

23.4.1. APIを介したRBACの管理

SUSE Multi-Linux Manager APIは、ロール、許可、およびユーザの割り当てをプログラムで管理するためのメソッドを提供します。

23.4.1.1. アクセスAPI

これらのAPIメソッドは、ロールとそれに関連するアクセスを管理します。

- **listNamespaces**: SUSE Multi-Linux Managerで利用可能なネームスペース、アクセスモード、およびそれらの説明を一覧表示します。
- **listPermissions**: ロールに許可されているネームスペースを一覧表示します。
- **listRoles**: SUSE Multi-Linux Manager内の既存のロールを一覧表示します。
- **createRole**: 新しいロールを作成します。オプションで既存のロールから許可をコピーします。
- **deleteRole**: ロールを削除します。
- **grantAccess**: ネームスペースへのアクセスを許可します。
- **revokeAccess**: ネームスペースへのアクセスを取り消します。

23.4.1.2. ユーザAPI

以下のAPIメソッドはユーザとロールの割り当てを管理します。

- **listPermissions**: ユーザの有効な許可を一覧表示します。
- **listRoles**: ユーザの割り当てられたロールを一覧表示します。
- **addRole**: ユーザにロールを割り当てます。
- **removeRole**: ユーザからロールを削除します。

リクエストおよび応答形式を含む詳細なAPIドキュメントについては、SUSE Multi-Linux Manager APIリファレンスを参照してください。

23.5. RBACベストプラクティス

これらのベストプラクティスに従うことで、安全で、効率的で、管理しやすいRBAC環境を維持できます。

- **最小権限の原則:** 職務を遂行するために必要な最小限の許可をユーザに常に付与します。過度に広範な許可は避けてください。
- **定期的なレビュー:** ユーザに割り当てられたロールと許可を定期的にレビューして、それらが依然とし

て適切であり、現在のセキュリティポリシーに準拠していることを確認します。

- **ロールの文書化:** 作成する各カスタムロールの目的と許可を明確に文書化します。
- **職務の分離:** 単一ユーザが重要なプロセスに対して過度に制御することを防止するため、職務の分離を強制するロールを実装します。

Chapter 24. SSL証明書

SUSE Multi-Linux Managerでは、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。

SSLを使用してSUSE Multi-Linux Managerサーバに登録するすべてのクライアントは、サーバ証明書に対して検証することにより、適切なサーバに接続していることを確認します。 このプロセスはSSLハンドシェークと呼ばれます。

SSLハンドシェーク中に、クライアントはサーバ証明書のホスト名が予期しているホスト名と一致することを確認します。 クライアントは、サーバ証明書が信頼できるかどうかも確認する必要があります。

認証局(CA)は、他の証明書に署名するために使用される証明書です。 証明書が有効であるとみなされ、クライアントが証明書と正常に照合できるようにするには、すべての証明書が認証局(CA)によって署名されている必要があります。

SSL認証が正しく機能するためには、クライアントがルートCAを信頼する必要があります。 これは、ルートCAがすべてのクライアントにインストールされる必要があることを意味します。

SSL認証のデフォルトの方法は、SUSE Multi-Linux Managerで自己署名証明書を使用することです。 この場合、SUSE Multi-Linux Managerはすべての証明書を生成し、ルートCAはサーバ証明書に直接署名しています。

別の方法は、中間CAを使用する方法です。 この場合、ルートCAは中間CAに署名します。 中間CAは任意の数の他の中間CAに署名することができ、最後のCAはサーバ証明書に署名します。 これはチェーン証明書と呼ばれます。

チェーン証明書で中間CAを使用している場合は、ルートCAがクライアントにインストールされ、サーバ証明書がサーバにインストールされます。 SSLハンドシェーク中に、クライアントはルートCAとサーバ証明書の間の中間証明書のチェーン全体を検証できる必要があります。そのため、クライアントはすべての中間証明書にアクセスできる必要があります。

これを実現するには、主に2つの方法があります。 以前のバージョンのSUSE Multi-Linux Managerでは、デフォルトですべての中間CAがクライアントにインストールされます。 ただし、サーバ上でサービスを設定してクライアントに提供することも可能です。 この場合、SSLハンドシェーク中に、サーバはサーバ証明書とすべての中間CAを提示します。 このメカニズムは現在、デフォルト設定として使用されています。

デフォルトでは、SUSE Multi-Linux Managerは中間CAなしの自己署名証明書を使用します。 セキュリティを強化するために、サードパーティのCAを手配して証明書に署名できます。 サードパーティのCAは、証明書に含まれる情報が正しいことを確認するためにチェックを実行します。 通常、このサービスには年会費がかかります。 サードパーティのCAを使用すると、証明書のスプーフィングが難しくなり、インストールに対する保護が強化されます。 サードパーティのCAによって署名された証明書がある場合は、SUSE Multi-Linux Managerのインストール環境にインポートできます。

このマニュアルでは、SSL証明書の使用について2つのステップで説明します。

1. SUSE Multi-Linux Managerツールを使用して自己署名証明書を作成する方法

2. SUSE Multi-Linux Managerサーバまたはプロキシに証明書を配備する方法

証明書が独自のPKIや外部PKIなどのサードパーティのインスタンスによって提供されている場合は、ステップ1をスキップできます。

- 自己署名証明書の作成の詳細については、**Administration › Ssl-certs-selfsigned**を参照してください。
- 証明書のインポートの詳細については、**Administration › Ssl-certs-imported**を参照してください。

24.1. SUSE Multi-Linux Managerコンテナへの SSL証明書の提供

24.1.1. Podman

SSL証明書はpodmanシークレットとして保存され、それぞれのコンテナに割り当てられます。 Podman SSLシークレットは次のとおりです。

- CA証明書
  - uyuni-ca
  - uyuni-db-ca
- サーバ証明書とキー
  - uyuni-cert
  - uyuni-key
- データベース証明書とキー
  - uyuni-db-cert
  - uyuni-db-key

24.2. 自己署名SSL証明書

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。 この場合、証明書はSUSE Multi-Linux Managerによって作成され、署名されます。 この方法では、証明書の詳細が正しいことを保証するために独立した認証局を使用しません。 サードパーティCAは、証明書に含まれる情報が正しいことを確認するためにチェックを実行します。

- サードパーティCA証明書の詳細については、**Administration › Ssl-certs-imported**を参照してください。
- 証明書の置き換え方法の詳細については、administration:ssl-certs-imported.pdfを参照してください。

このセクションでは、新規または既存のインストールで自己署名証明書を作成または再作成する方法について説明します。

SSLキーおよび証明書のホスト名はそれらを配備するマシンの完全修飾ホスト名に一致する必要があります。

24.2.1. 既存のサーバ証明書の再作成

既存の証明書の有効期限が切れているか、何らかの理由で動作を停止している場合は、既存のCAから新しいサーバ証明書を生成できます。

プロシージャ: 既存のサーバ証明書の再作成

1. SUSE Multi-Linux Managerコンテナホストのコマンドプロンプトで、サーバ証明書を再生成します。

```
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="susemanager.example.com" --set-cname="example.com"
```

set-cnameパラメータがSUSE Multi-Linux Managerサーバの完全修飾ドメイン名であることを確認します。 複数のエイリアスが必要な場合は複数回、**set-cname**パラメータを使用できます。

機密鍵とサーバ証明書はサーバコンテナ内のディレクトリ**/root/ssl-build/susemanager/**に**server.key**と**server.crt**として検索できます。 最後のディレクトリの名前は、**--set-hostname**オプションで使用されるホスト名に依存します。

コンテナのホストpodmanシークレットを更新して、新しい証明書とキーを配備またはインポートします。生成されたばかりの証明書をインポートする方法の詳細については、administration:ssl-certs-imported.pdfを参照してください。

24.2.2. 新しいCAおよびサーバ証明書の作成

ルートCAを置き換える必要がある場合は注意してください。 サーバとクライアントの間の信頼チェーンを切断する可能性があります。 その場合は、管理ユーザがすべてのクライアントにログインしてCAを直接配備する必要があります。

プロシージャ: 新しい証明書の作成

1. SUSE Multi-Linux Managerコンテナホストのコマンドプロンプトで、古い証明書ディレクトリを新しい場所に移動します。

```
mgrctl exec -- mv /root/ssl-build /root/old-ssl-build
```

2. 新しいCA証明書を生成します。

```
mgrctl exec -ti -- rhn-ssl-tool --gen-ca --dir="/root/ssl-build" --set
-country="COUNTRY" \
--set-state="STATE" --set-city="CITY" --set-org="ORGANIZATION" \
--set-org-unit="ORGANIZATION UNIT" --set-common-name="SUSE Manager CA Certificate" \
--set-email="name@example.com"
```

3. 新しいサーバ証明書を生成します。

```
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="susemanager.example.top" --set-cname="example.com"
```

set-cnameパラメータがSUSE Multi-Linux Managerサーバの完全修飾ドメイン名であることを確認します。 複数のエイリアスが必要な場合は複数回、**set-cname**パラメータを使用できます。

ホスト名とcnameを使用して、各プロキシのサーバ証明書も生成する必要があります。

24.3. SSL証明書のインポート

このセクションでは、新しいSUSE Multi-Linux Managerのインストールに SSL証明書を設定する方法、および既存の証明書を置き換える方法について説明します。

開始する前に、以下があることを確認します。

- 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。
- SSLサーバ秘密鍵
- SSLサーバ証明書
- SSLデータベース機密鍵
- SSLデータベース証明書

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。

データベースSSL証明書では、**reportdb**と**db**が**Subject Alternative Name**として必要です。

Third-party authorities commonly use intermediate CAs to sign requested server certificates. In this case, all CAs in the chain are required to be available. The **mgrdadm** commands are taking care of ordering the certificates. Ideally, the root CA should be in its own file. The server certificate file should contain the server certificate first, followed by all intermediate CA certificates in order.

24.3.1. 新しいインストール用証明書のインポート

By default, SUSE Multi-Linux Manager uses a self-signed certificate. Certificates can be imported with third-party certificates at the installation time.

Procedure: Importing certificates on a new SUSE Multi-Linux Manager server

1. **Installation-and-upgrade › Install-server**の手順に従ってSUSE Multi-Linux Managerサーバを配備します。必ず、正しいファイルをパラメータとして**mgradm install podman**に渡してください。パラメータは次のとおりです。

```
サードパーティSSL証明書フラグ:
      --ssl-ca-intermediate文字列    中間CA証明書のパス
      --ssl-ca-root文字列             ルートCA証明書のパス
      --ssl-server-cert文字列         サーバ証明書のパス
      --ssl-server-key文字列          サーバキーのパス
      --ssl-db-ca-intermediate文字列 データベースの中間CA証明書のパス
(サーバの証明書と異なる場合)
      --ssl-db-ca-root文字列          データベースのルートCA証明書のパス
(サーバの証明書と異なる場合)
      --ssl-db-cert string            データベース証明書のパス
      --ssl-db-key string             データベースキーのパス
```

Intermediate CAs can either be available in the file which is specified with **--ssl-ca-root**, or specified as extra options with **--ssl-ca-intermediate**. The **--ssl-ca-intermediate** option can be specified multiple times.

24.3.2. Import certificates for new proxy installations

The proxy certificates are embedded in the generated configuration. In order to use a third-party certificate, it needs to be provided during the configuration.

Procedure: Importing certificates on a new SUSE Multi-Linux Manager Proxy

1. **Installation-and-upgrade › Install-proxy**の手順に従って、SUSE Multi-Linux Managerプロキシをインストールします。
2. プロンプトに従ってセットアップを完了します。

Use the same certificate authority (CA) to sign all certificates for servers and proxies. Certificates signed with different CAs do not match.

24.3.3. Replace certificates

You can replace active certificates on your SUSE Multi-Linux Manager installation with a new certificate. There are two cases to consider: replacing only the server or database certificate, and replacing the root CA.

Replacing the root certificate requires more time and planning to avoid disruption as all the registered

proxies and systems will need to have the new CA in their database before switching to it at the server level.

When using third-party certificates signed by an intermediate CA, the intermediate CA certificates need to be appended to the server or database certificate file.

The order is important: first comes the server certificate, then the CAs from the one which signed the certificate to the one signed by the root CA. The root CA certificate should not be appended to the server certificate file.

Procedure: Replacing all existing certificates

1. The following considers that you have **root-ca.pem**, **intermediate-ca1.pem**, **intermediate-ca2.pem**, **server.pem** and **server.key** files. It may be different depending on the number of intermediate CAs in the server certificate signature chain.
2. Combine the intermediate CAs and server certificates. The order matters, the server must be first and the intermediate CAs in order. Do not add the root CA last into the chain as it will be passed separately to **uyuni-ca** and **uyuni-db-ca** secrets. If there is no intermediate CA, then you can use the **server.pem** instead of the combined file in the next steps.

```
cat server.pem intermediate-ca1.pem intermediate-ca2.pem >combined-server.pem
```

3. On the SUSE Multi-Linux Manager container host, at the command prompt, recreate podman certificate secrets passing the files paths:

```
podman secret create --replace uyuni-ca $path_to_ca_certificate
podman secret create --replace uyuni-cert $path_to_combined_server_certificate
podman secret create --replace uyuni-key $path_to_server_key

podman secret create --replace uyuni-db-ca $path_to_database_ca_certificate
podman secret create --replace uyuni-db-cert
$path_to_combined_database_certificate
podman secret create --replace uyuni-db-key $path_to_database_key
```

Procedure: Restarting the server

1. コンテナホストで、サーバを再起動して変更を取得します。

```
mgradm restart
```

プロキシを使用している場合は、各プロキシのホスト名とcnameを使用して、各プロキシ用のサーバ証明書RPMを生成する必要があります。 新しい設定tarballを生成して配備します。

詳細については、installation-and-upgrade:container-deployment/mlm/proxy-deployment-

mlm.pdfを参照してください。

If the Root CA was changed, it needs to get deployed to all the clients connected to SUSE Multi-Linux Manager. This is ideally done in advance to minimize the disruption.

If the CA certificate was updated, a RPM file with Kiwi certificate needs to be repackaged.

On the SUSE Multi-Linux Manager Server container host, execute following command:

```
mgrctl exec mgr-package-rpm-certificate-osimage
```

After that, apply highstate on the Image Build hosts to deploy the new certificates for Kiwi to use.

Procedure: Deploying the root CA on clients

1. SUSE Multi-Linux Manager Web UIで、**システム › 概要**に移動します。
2. すべてのクライアントをチェックして、システムセットマネージャに追加します。
3. **システム › システムセットマネージャ › 概要**に移動します。
4. ［**状態**］フィールドで、**[適用]**をクリックして、システムの状態を適用します。
5. ［**highstate**］ページで、**[highstateの適用]**をクリックして、クライアントに変更を伝播します。

24.4. HTTP Strict Transport Security

HTTP Strict Transport Security (HSTS)は、プロトコルダウングレード攻撃やクッキーハイジャックなどの中間者攻撃からWebサイトを保護するのに役立つポリシーメカニズムです。

On SUSE Multi-Linux Manager, HSTS is enabled by default. If you need to disable it on the server, follow this procedure:

Procedure: Disabling HSTS on the server

1. On the server container host, as root, execute the following command to create a new configuration file with setting **max-age=0**:

```
mgrctl exec -- \
  echo 'Header always set Strict-Transport-Security "max-age=0;
includeSubDomains"' \
```

```
  > /etc/apache2/conf.d/zz-spacewalk-www-hsts.conf
```

2. 次のコマンドでApacheを再起動します。

```
mgrctl exec -- systemctl restart apache2
```

If you need to disable it on the proxy, follow this procedure:

Procedure: Disabling HSTS on the proxy

1. On the server container host, as root, execute the following command to create a new configuration file with setting **max-age=0**:

```
echo 'Header always set Strict-Transport-Security "max-age=0;
includeSubDomains' \
  > /etc/uyuni/custom-httpd.conf
```

2. 次のコマンドを実行します。

```
mgrpxy install podman --tuning-httpd /etc/uyuni/custom-httpd.conf config.tar.gz
```

新しい設定ファイルに**<filename>.conf**という名前を付ける場合は、適切なタイミングでロードされるようにしてください。 たとえば、**spacewalk-www.conf**で定義されたものを上書きするには、新しいファイルがアルファベット順でこのファイルの後にある必要があります。 Apacheがファイルをロードする方法の詳細については、https://httpd.apache.org/docsを参照してください。

SUSE Multi-Linux Managerで生成されたデフォルトのSSL証明書または自己署名証明書を使用してHSTSを有効にすると、このような証明書に署名するために使用されたCAがブラウザによって信頼されていない限り、ブラウザはHTTPSでの接続を拒否します。 SUSE Multi-Linux Managerで生成されたSSL証明書を使用している場合は、http://<SERVER-HOSTNAME>/pub/RHN-ORG-TRUSTED-SSL-CERTにあるファイルをすべてのユーザのブラウザにインポートすることでこの証明書を信頼することができます。

Chapter 25. サブスクリプションマッチング

SUSE製品にはSUSE Customer Center (SCC)によって管理されるサブスクリプションが必要です。 SUSE Multi-Linux Managerは、SCCアカウントに対して登録済みの全クライアントのサブスクリプションステータスをチェックする夜間レポートを実行します。 このレポートには、どのクライアントがどのサブスクリプションを使用しているか、残りのサブスクリプション数と使用できるサブスクリプション数、および現在のサブスクリプションがないクライアントに関する情報が表示されます。

監査 › サブスクリプションマッチングに移動して、レポートを表示します。

［**Subscriptions Report**］（サブスクリプションレポート）タブには、現在のサブスクリプションと期限切れサブスクリプションに関する情報が表示されます。

［**Unmatched Products Report**］（一致しない製品レポート）タブには、現在のサブスクリプションがないクライアントのリストが表示されます。 これには、一致できなかったクライアント、SUSE Multi-Linux Managerに現在登録されていないクライアントが含まれます。 このレポートには、製品名とまだ一致していないシステムの数が含まれます。

［**ピン**］タブでは、関連するサブスクリプションに個々のクライアントを関連付けることができます。 これは、サブスクリプションマネージャがクライアントをサブスクリプションに自動的に正常に関連付けない場合に特に役立ちます。

［**メッセージ**］タブには、マッチングプロセス中にサブスクリプションマッチャーによって生成されたすべてのメッセージが表示されます。 これらは、結果を理解し、マッチングを改善するのに役立つ情報を提供します。

レポートは.csv形式でダウンロードすることも、コマンドプロンプトから**/var/lib/spacewalk/subscription-matcher/**ディレクトリでアクセスすることもできます。

デフォルトでは、サブスクリプションマッチャーは毎日午前0時に実行されます。 これを変更するには、**管理 › タスクスケジュール**に移動し、［**gatherer-matcher-default**］をクリックします。 必要に応じてスケジュールを変更し、**[スケジュールの更新]**をクリックします。

レポートは現在のクライアントと現在のサブスクリプションしか一致させることができないため、一致が時間の経過とともに変化することがあります。 同じクライアントが常に同じサブスクリプションと一致するわけではありません。 これは、新規クライアントの登録または登録解除、もしくはサブスクリプションの追加または期限切れが原因である可能性があります。

サブスクリプションマッチャーは、アカウント内のサブスクリプションの条項によって制限される、不一致の製品数を自動的に減らそうとします。 ただし、不完全なハードウェア情報、不明な仮想マシンホストの割り当て、または不明なパブリッククラウドで実行されているクライアントがある場合は、利用可能なサブスクリプションが十分でないことがマッチャーに表示されることがあります。 正確性を確保するために、常にSUSE Multi-Linux Managerに含まれるクライアントに関する完全なデータがあることを確認してください。

サブスクリプションマッチャーは、常にクライアントとサブスクリプションを正確に一致させるとは限りません。 これは監査に代わるものではありません。

25.1. クライアントをサブスクリプションにピン設定する

サブスクリプションマッチャーが特定のクライアントと正しいサブスクリプションを自動的に一致させない場合は、それらを手動でピン設定することができます。 ピンを作成すると、サブスクリプションマッチャーは特定のサブスクリプションを特定のシステムまたはシステムのグループと一致させることを優先します。

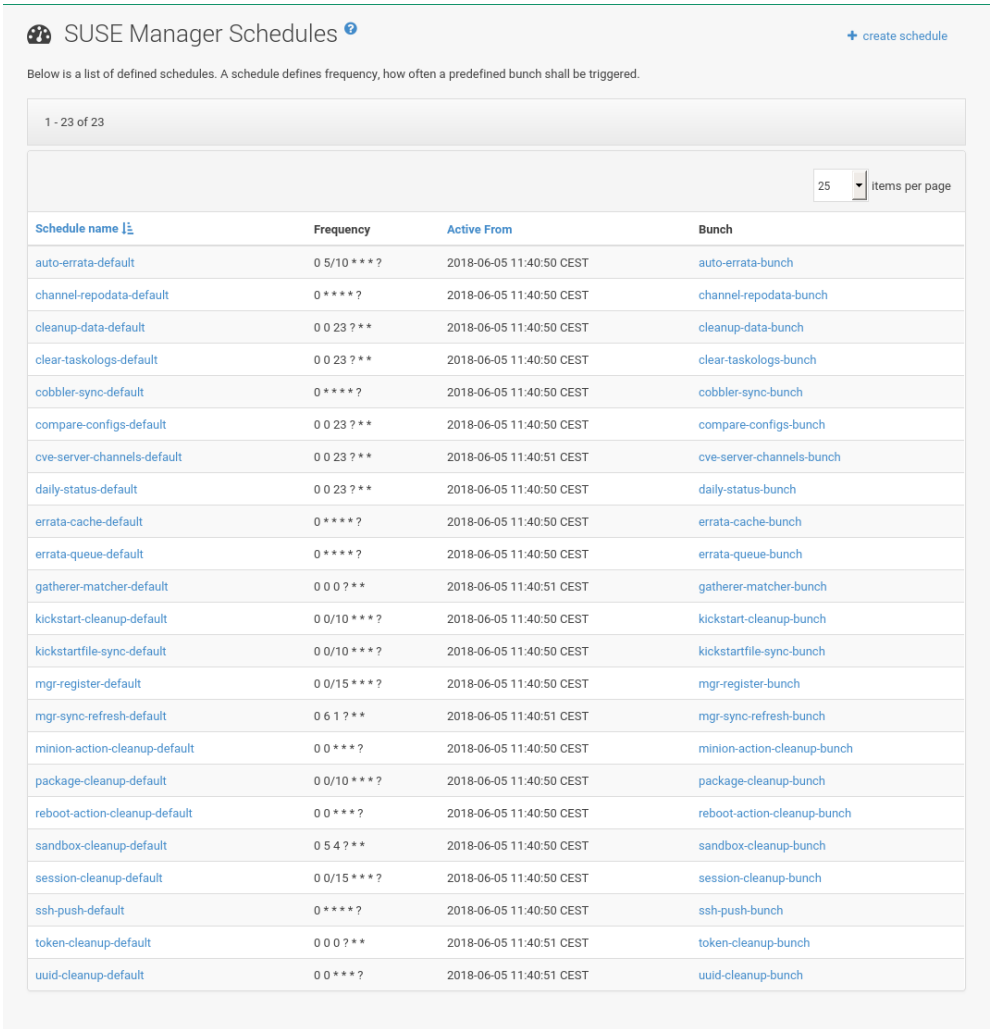
ただし、マッチャーは常にピンを尊重するわけではありません。 これは、利用可能なサブスクリプション、およびサブスクリプションをクライアントに適用できるかどうかによって異なります。 さらに、サブスクリプションの条項に違反する一致が発生した場合、またはピンが無視された場合にマッチャーがより正確な一致を検出した場合、ピンは無視されます。

新しいピンを追加するには、**[ピンの追加]**をクリックし、ピンを設定するクライアントを選択します。

定期的に、または多数のクライアントにピンの設定を使用することはお勧めしません。 Subscription Matcherツールは、一般的にほとんどのインストールに十分な精度があります。

Chapter 26. タスクスケジュール

事前定義されたすべてのタスクバンチは、**管理者 › タスクスケジュール**の下に一覧表示されます。



Schedule name	Frequency	Active From	Bunch
auto-errata-default	0 5/10 * * * ?	2018-06-05 11:40:50 CEST	auto-errata-bunch
channel-repodata-default	0 * * * * ?	2018-06-05 11:40:50 CEST	channel-repodata-bunch
cleanup-data-default	0 0 23 ? * *	2018-06-05 11:40:50 CEST	cleanup-data-bunch
clear-taskologs-default	0 0 23 ? * *	2018-06-05 11:40:50 CEST	clear-taskologs-bunch
cobbler-sync-default	0 * * * * ?	2018-06-05 11:40:50 CEST	cobbler-sync-bunch
compare-configs-default	0 0 23 ? * *	2018-06-05 11:40:50 CEST	compare-configs-bunch
cve-server-channels-default	0 0 23 ? * *	2018-06-05 11:40:51 CEST	cve-server-channels-bunch
daily-status-default	0 0 23 ? * *	2018-06-05 11:40:50 CEST	daily-status-bunch
errata-cache-default	0 * * * * ?	2018-06-05 11:40:50 CEST	errata-cache-bunch
errata-queue-default	0 * * * * ?	2018-06-05 11:40:50 CEST	errata-queue-bunch
gatherer-matcher-default	0 0 0 ? * *	2018-06-05 11:40:51 CEST	gatherer-matcher-bunch
kickstart-cleanup-default	0 0/10 * * * ?	2018-06-05 11:40:50 CEST	kickstart-cleanup-bunch
kickstartfile-sync-default	0 0/10 * * * ?	2018-06-05 11:40:50 CEST	kickstartfile-sync-bunch
mgr-register-default	0 0/15 * * * ?	2018-06-05 11:40:50 CEST	mgr-register-bunch
mgr-sync-refresh-default	0 6 1 ? * *	2018-06-05 11:40:51 CEST	mgr-sync-refresh-bunch
minion-action-cleanup-default	0 0 * * * ?	2018-06-05 11:40:50 CEST	minion-action-cleanup-bunch
package-cleanup-default	0 0/10 * * * ?	2018-06-05 11:40:50 CEST	package-cleanup-bunch
reboot-action-cleanup-default	0 0 * * * ?	2018-06-05 11:40:50 CEST	reboot-action-cleanup-bunch
sandbox-cleanup-default	0 5 4 ? * *	2018-06-05 11:40:50 CEST	sandbox-cleanup-bunch
session-cleanup-default	0 0/15 * * * ?	2018-06-05 11:40:50 CEST	session-cleanup-bunch
ssh-push-default	0 * * * * ?	2018-06-05 11:40:50 CEST	ssh-push-bunch
token-cleanup-default	0 0 0 ? * *	2018-06-05 11:40:51 CEST	token-cleanup-bunch
uuid-cleanup-default	0 0 * * * ?	2018-06-05 11:40:51 CEST	uuid-cleanup-bunch

SUSE Multi-Linux Manager Schedules（SUSE Multi-Linux Managerスケジュール） › スケジュール名をクリックして、**スケジュール名 › 基本的なスケジュール詳細**を開き、無効にしたり、頻度を変更したりできます。

[Edit Schedule]（スケジュールの編集）をクリックして、設定でスケジュールを更新します。

スケジュールを無効化するには、右上隅の**[スケジュールの無効化]**をクリックします。

SUSE Multi-Linux Managerが正常に動作するために不可欠であるため、スケジュールが必要であると確信している場合にのみ、スケジュールを無効化してください。

タスクが無効化されても、リストには表示されます。 **SUSE Multi-Linux Managerスケジュール › スケジュール名**をクリックする場合、**[スケジュールを有効化する]**をクリックして、ジョブを再度有効化できます。

バンチ名をクリックすると、そのバンチタイプのランとそのステータスのリストが表示されます。

開始時間のリンクをクリックすると、**スケジュール名 › 基本的なスケジュール詳細**に戻ります。

26.1. 事前定義済みのタスクバンチ

次の事前定義済みのタスクバンチはデフォルトでスケジュールされており、設定できます。

auto-errata-default

必要に応じて自動エラータ更新をスケジュールします。

channel-repodata-default

リポジトリメタデータファイルを(再)生成します。

cleanup-data-default

古いパッケージ変更ログをクリーンアップし、データベースから時系列データを監視します。

clear-taskologs-default

ジョブタイプに応じて、指定した日数よりも古いタスクエンジン(taskomatic)履歴データをデータベースからクリアします。

cobbler-sync-default

SUSE Multi-Linux ManagerからCobblerに配布データとプロファイルデータを同期します。 Cobblerによる自動インストールの詳細については、**Client-configuration › Autoinst-intro**を参照してください。

compare-configs-default

設定チャンネルに保存されている設定ファイルと、すべての設定対応サーバに保存されているファイルを比較します。 比較を確認するには、**システム**タブをクリックし、対象のシステムを選択します。 **設定 › ファイルの比較**に移動します。 詳細については、reference:systems/system-details/sd-configuration.pdfを参照してください。

cve-server-channels-default

監査 › CVE監査ページに結果を表示するために使用される、事前に計算された内部CVEデータを更新します。 **監査 › CVE監査**ページの検索結果は、このスケジュールの最後の実行に更新されます。 詳細については、**Reference › Audit**を参照してください。

daily-status-default

関連するアドレスに日次レポート電子メール を送信します。 特定のユーザの通知を設定する方法の詳細については、**Reference › Users**を参照してください。

errata-advisory-map-sync-default

内部のSUSEパッチベンダアドバイザリーデータベーステーブルを更新します。 利用可能な場合は、SUSEによって提供される元のアドバイザリーが各パッチ詳細の［ベンダアドバイザリー］セクションに表示されます。

errata-cache-default

各サーバの更新が必要なパッケージを検索するために使用される、内部パッチキャッシュデータベーステーブルを更新します。 また、これにより、特定のパッチに関心がある可能性のあるユーザに通知メールが送信されます。 パッチの詳細については、**Reference › Patches**を参照してください。

errata-queue-default

自動更新(パッチ)を受信するように設定されているサーバのキューに入れます。

gatherer-matcher-default

仮想ホストマネージャで設定されたVirtual Host Gathererを実行して、仮想ホストデータを収集します。更新されたデータが利用可能になると、Subscription Matcherジョブが実行されます。

kickstart-cleanup-default

古いKickstartセッションデータをクリーンアップします。

kickstartfile-sync-default

設定ウィザードによって作成されたKickstartプロファイルに対応するCobblerファイルを生成します。

mgr-forward-registration-default

SUSE Customer Centerとクライアント登録データを同期します。 デフォルトでは、新規、変更済み、または削除済みクライアントデータが転送されます。 **/etc/rhn/rhn.conf**で同期セットを無効にするには、次のコマンドを実行します。

```
server.susemanager.forward_registration = 0
```

SCCとのデータ同期を無効にすると、RMT、SMT、SUSE Multi-Linux Manager、およびSCCに直接登録されたクライアント間の管理対象クライアントの可視性が低下します。

データの同期により、登録されたすべてのクライアントの統一されたビューが確保されます。

オプトアウトの理由を共有して、サービス向上にご協力ください

mgr-sync-refresh-default

SUSE Customer Centerと同期します(**mgr-sync-refresh**)。 デフォルトでは、すべてのカスタムチャンネルもこのタスクの一部として同期されます。 カスタムチャンネル同期の詳細については、administration:custom-channels.pdfを参照してください。

minion-action-chain-cleanup-default

古い動作チェーンデータをクリーンアップします。

minion-action-cleanup-default

ファイルシステムから古いクライアントアクションデータを削除します。 最初に、Saltジョブキャッシュに保存されている対応する結果を検索して、未完了の可能性のあるアクションを完了しようとしま

す。　サーバがアクションの結果を見逃した場合、未完了のアクションが発生する可能性があります。アクションが正常に完了した場合は、実行されたスクリプトファイルなどのアーティファクトが削除されます。

minion-checkin-default

クライアントに対して定期的なチェックインを実行します。

notifications-cleanup-default

期限切れの通知メッセージをクリーンアップします。

oval-data-sync-default

CVE監査クエリの精度を向上させるために必要なOVALデータを生成します。

package-cleanup-default

ファイルシステムから古いパッケージファイルを削除します。

reboot-action-cleanup-default

6時間以上待機中の再起動アクションは失敗としてマークされ、関連データがデータベースからクリーンアップされます。　再起動アクションのスケジュール設定の詳細については、reference:systems/system-details/sd-provisioning.pdfを参照してください。

sandbox-cleanup-default

sandbox_lifetime　設定パラメータ(デフォルトでは3日)よりも古いサンドボックス設定ファイルとチャンネルをクリーンアップします。　サンドボックスファイルは、システムまたは開発中のファイルからインポートされたファイルです。　詳細については、reference:systems/system-details/sd-configuration.pdfを参照してください。

session-cleanup-default

古いWebインタフェースセッションをクリーンアップします。通常は、ユーザがログインし、ログアウトする前にブラウザを閉じたときに一時的に保存されるデータです。

ssh-service-default

クライアントが**SSH Push**の接続メソッドで設定されている場合、SSH経由でSUSE Multi-Linux Managerにチェックインするようにクライアントにプロンプトを表示します。また、再起動後に動作チェーンを再開します。

system-overview-update-queue-default

システム概要データを更新します。

system-profile-refresh-default

すべてのシステムでハードウェアの更新を実行します。　これは毎月のみ発生し、SUSE　Multi-Linux Managerサーバの負荷が増加する可能性があります。　ジョブは**Specialized-guides › Salt**を使用します。 バッチサイズの調整については、specialized-guides:large-deployments/tuning.pdfを参照してください。

token-cleanup-default

Saltクライアントがパッケージとメタデータをダウンロードするために使用する期限切れのリポジトリトークンを削除します。

update-payg-default

構成されたPAYGのクラウドインスタンスから認証データを収集します。

update-reporting-default

ローカルレポーティングデータベースを更新します。

update-reporting-hub-default

周辺機器SUSE Multi-Linux Managerサーバからすべてのレポーティングデータを収集し、ハブレポーティングデータベースを更新します。

update-system-overview-default

システム概要データが最新であることを定期的に確認します。

uuid-cleanup-default

古いUUIDレコードをクリーンアップします。

Chapter 27. 変更ログの調整

一部のパッケージには、変更ログエントリの長いリストがあります。 このデータはデフォルトでダウンロードされますが、必ずしも保持すべき役立つ情報とは限りません。 ダウンロードする変更ログのメタデータ量を制限し、ディスク容量を節約するために、ディスクに保持するエントリ数を制限できます。

サーバコンテナでステップを実行する前に、**mgrctl term**を使用します。

この設定オプションは、**/etc/rhn/rhn.conf**設定ファイルにあります。パラメータのデフォルトは**20**です。この値を**0**に変更すると、無制限の数のエントリが提供されます。

```
java.max_changelog_entries = 20
```

このパラメータを設定すると、新しいパッケージが同期されるときにのみ有効になります。

このパラメータを変更した後で、**mgradm restart**を使用してサービスを再起動します。

キャッシュされたデータを削除して再生成し、古いデータを削除したい場合があります。

キャッシュされたデータの削除と再生成には時間がかかる場合があります。 使用するチャンネル数と削除するデータ量に応じて、数時間かかる可能性があります。 タスクはTaskomaticによってバックグラウンドで実行されるため、操作が完了するまでSUSE Multi-Linux Managerを使用し続けることができますが、多少のパフォーマンスの低下が予想されます。

コマンドラインからキャッシュされたデータを削除して、再生成を要求できます。

```
spacewalk-sql -i
```

次に、SQLデータベースプロンプトで、次のように入力します。

```
DELETE FROM rhnPackageRepodata;
INSERT INTO rhnRepoRegenQueue (id, CHANNEL_LABEL, REASON, FORCE)
(SELECT sequence_nextval('rhn_repo_regen_queue_id_seq'),
        C.label,
        'cached data regeneration',
        'Y'
        FROM rhnChannel C);
\q
```

Chapter 28. ユーザー

SUSE Multi-Linux Manager管理者は新しいユーザの追加、許可の付与、ユーザの無効化または削除を行うことができます。 多数のユーザを管理している場合は、ユーザをシステムグループに割り当てて、グループレベルで許可を管理できます。 言語やテーマのデフォルトなど、Web UIのシステムデフォルトを変更することもできます。

［**ユーザ**］メニューは、SUSE Multi-Linux Manager管理者アカウントでログインしている場合にのみ使用できます。

SUSE Multi-Linux Managerユーザを管理するには、ユーザ[ユーザ一覧 > すべて]に移動し、SUSE Multi-Linux Managerサーバのすべてのユーザを表示します。 リスト内の各ユーザにはユーザ名、リアル名、割り当てられたロール、ユーザが最後に署名した日付、ユーザの現在のステータスが表示されます。 **[ユーザの作成]**をクリックして、新しいユーザアカウントを作成します。 ユーザ名をクリックして、［**ユーザの詳細**］ページに移動します。

新規ユーザを組織に追加するには、**[ユーザの作成]**をクリックして、新しいユーザの詳細を確認し、**[ログインの作成]**をクリックします。

28.1. パスワード要件

SUSE Multi-Linux Managerは、デフォルト値が選択された状態で出荷されます。

すべての新しいユーザパスワードが組織のセキュリティ基準に確実に準拠するように、SUSE Multi-Linux Manager管理者にはパスワード作成ルールを強制するオプションがあります。

Web UIで、**管理 › マネージャ設定 › パスワードポリシー**に移動し、パスワード要件を定義します。 次のフィールドの組み合わせを使用します。

最小パスワード長

このフィールドを使用して、パスワードの最小長を定義します。

最大パスワード長

このフィールドを使用して、パスワードの最大長を定義します。

数字が必要

このフィールドを使用して、パスワードに数字(0〜9)を含める必要があるかどうかを指定します。

小文字が必要

このフィールドを使用して、パスワードに小文字(a〜z)を含める必要があるかどうかを指定します。

大文字が必要

このフィールドを使用して、パスワードに大文字(A〜Z)を含める必要があるかどうかを指定します。

連続文字を制限

このフィールドを使用して、連続文字が制限されるかどうかを指定します。

特殊文字が必要

このフィールドを使用して、パスワードに特殊文字を含める必要があるかどうかを指定します。

使用できる特殊文字

このフィールドは、**特殊文字が必要**が選択されている場合のみ有効になります。 このフィールドを使用して、使用できる特殊文字を指定します。たとえば、**!@#$%&***など。

Restrict Character Occurences (文字の出現を制限する)

このフィールドを使用して、制限される文字の出現を指定します。

Max Character Occurences (最大文字出現回数)

このフィールドを使用して、最大文字出現回数を指定します。

[保存]をクリックして、変更したパスワード設定を保存します。

[リセット]を使用すると、すべての設定をデフォルトに戻すことができます。

SUSE Multi-Linux Managerは、次のデフォルト値で出荷されます。

- 最小パスワード長: 4
- 最大パスワード長: 32
- 大文字が必要: チェック済み

28.2. アカウントの無効化と削除

ユーザアカウントが不要になった場合は、無効化または削除できます。 無効化されたユーザアカウントは、いつでも再有効化できます。 削除されたユーザアカウントは表示されず、取得できません。

ユーザは独自のアカウントを無効化できます。 ただし、ユーザに管理者ロールがある場合は、アカウントを無効化する前に、ロールを削除する必要があります。

無効化されたユーザはSUSE Multi-Linux Manager Web UIにログインしたり、アクションをスケジュール したりできません。 無効化の前にユーザによってスケジュールされたアクションは、アクションキューに残ります。 無効化されたユーザはSUSE Multi-Linux Manager管理者によって再有効化できます。

28.3. ユーザロール

ユーザには複数のロールを割り当てることができます。また、任意のロールを保持するユーザは、いつでも複数存在することができます。 常に少なくとも1人の有効なSUSE Multi-Linux Manager管理者が必要です。

SUSE Multi-Linux Manager管理者ロールを除く、ユーザのロールを変更するには、**ユーザ › ユーザー覧 › す**

べてに移動して、変更するユーザを選択し、必要に応じて管理者ロールをオンまたはオフにします。

ユーザのSUSE Multi-Linux Manager管理者ロールを変更するには、**管理 › ユーザ**に移動して、必要に応じて、［**SUSE Multi-Linux Manager管理者?**］をオンまたはオフにします。

表 15. ユーザロールの許可

ロール名	説明
SUSE Multi-Linux Manager管理者	他のユーザの権限の変更を含む、すべての機能を実行できます。
組織管理者	アクティベーションキー、設定、チャンネル、およびシステムグループを管理します。
アクティベーションキー管理者	アクティベーションキーを管理します。
イメージ管理者	イメージプロファイル、ビルド、およびストアを管理します。
設定管理者	システム設定を管理します。
チャンネル管理者	チャンネルをグローバルにサブスクライブ可能にしたり、新しいチャンネルを作成したりするなど、ソフトウェアチャンネルを管理します。
システムグループ管理者	システムグループの作成と削除、既存のグループへのクライアントの追加、グループへのユーザアクセスの管理など、システムグループを管理します。
標準ユーザ	標準レベルのアクセスを提供します。新規作成されたユーザは自動的にこのロールに割り当てられます。

28.4. 追加ロールの作成

SUSE Multi-Linux Managerのロールベースのアクセス制御では、追加ロールを作成して、ユーザ許可を微調整できます。 ロールの管理方法の詳細については、**Administration › Role-based-access-control**を参照してください。

28.5. ユーザ許可とシステム

クライアントを管理するシステムグループを作成している場合は、管理するグループをユーザに割り当てることができます。

ユーザをシステムグループに割り当てるには、**ユーザ › ユーザー覧**に移動して、編集するユーザ名をクリックし、［**システムグループ**］タブに移動します。 割り当てるグループをオンにして、**[デフォルトの更新]**をクリックします。

ユーザの1つ以上のデフォルトのシステムグループを選択することもできます。 ユーザが新しいクライアン

トを登録すると、デフォルトで選択したシステムグループに割り当てられます。　これにより、ユーザは新たに登録されたクライアントに直ちにアクセスできます。

外部グループを管理するには、**ユーザ › システムグループ設定**に移動して、［**外部認証** ］タブに移動します。 **［外部グループの作成］** をクリックして、新しい外部グループを作成します。 グループに名前を付けて、適切なシステムグループに割り当てます。

システムグループの詳細については、**Reference › Systems**を参照してください。

ユーザが管理できる個々のクライアントを確認するには、**ユーザ › ユーザー覧**に移動し、編集するユーザ名をクリックして、［**システム**］タブに移動します。 一括タスクを実行するには、リストからクライアントを選択し、システムセットマネージャに追加します。

システムセットマネージャの詳細については、**Client-configuration › System-set-manager**を参照してください。

28.6. ユーザとチャンネルの許可

チャンネルからコンテンツを消費するサブスクライバとして、またはチャンネル自体を管理できる管理者として、ユーザを組織内のソフトウェアチャンネルに割り当てることができます。

ユーザをチャンネルにサブスクライブするには、**ユーザ › ユーザー覧**に移動し、編集するユーザ名をクリックして、**チャンネルの権限 › サブスクリプション**タブに移動します。 割り当てるチャンネルをオンにして、**[許可の更新]**をクリックします。

ユーザにチャンネル管理許可を付与するには、**ユーザ › ユーザー覧**に移動し、編集するユーザ名をクリックして、**チャンネルの権限 › 管理**タブに移動します。 割り当てるチャンネルをオンにして、**[許可の更新]**をクリックします。

リスト内の一部のチャンネルはサブスクライブできない場合があります。 これは通常、ユーザ管理者のステータス、またはチャンネルのグローバル設定が原因です。

28.7. ユーザのデフォルト言語

新しいユーザを作成するときに、Web UIで使用する言語を選択できます。 ユーザを作成した後で、**ホーム › 設定**に移動して、言語を変更できます。

デフォルト言語は、**rhn.conf**設定ファイルで設定されます。　デフォルト言語を変更するには、**/etc/rhn/rhn.conf**ファイルを開いて、次の行を追加または編集します。

```
web.locale = <LANGCODE>
```

パラメータが設定されていない場合、デフォルト言語は**en_US**です。

SUSE Multi-Linux Managerで使用可能な言語は次のとおりです。

表 16. 使用可能な言語コード

言語コード	言語	ダイアレクト
en_US	英語	米国
zh_CN	中国語	本土、簡体字

28.7.1. ユーザデフォルトのインタフェーステーマ

デフォルトでは、SUSE Multi-Linux Manager Web UIはインストールした製品に適切なテーマを使用します。 テーマを変更して、UyuniまたはSUSE Multi-Linux Managerの色を反映できます。 SUSE Multi-Linux Managerのテーマでは、ダークオプションも使用できます。

rhn.conf設定ファイルでデフォルトのテーマを変更できます。 デフォルトのテーマを変更するには、**/etc/rhn/rhn.conf**ファイルを開いて、次の行を追加または編集します。

```
web.theme_default = <THEME>
```

表 17. 使用可能なWebUIテーマ

テーマ名	色	スタイル
suse-light	SUSE Multi-Linux Manager	ライト
suse-dark	SUSE Multi-Linux Manager	ダーク
uyuni	Uyuni	ライト

Chapter 29. Support

When you manage systems in SUSE Multi-Linux Manager where you are entitled for support from SUSE, you can get the support data like **supportconfig** or **sosreport**. You will get the data from the managed client and upload it directly to SUSE Global Technical Support.

29.1. Create a service request number

Before handing over the support data to Global Technical Support, you need to generate a service request number first.

To create a service request, go to https://scc.suse.com/support/requests and follow the instructions on the screen. Write down the service request number.

Privacy statement

SUSE treats system reports as confidential data. For details about the SUSE privacy commitment, see https://www.suse.com/company/policies/privacy/.

29.2. Collect and upload support data from SUSE Multi-Linux Manager to SUSE

Procedure: Collecting support data and uploading with the SUSE Multi-Linux Manager Web UI

1. In the SUSE Multi-Linux Manager Web UI, navigate to **Systems › System List › All** and select the client which support data should be added to the case.
2. Then navigate to the **Details** tab and select the **Support** sub-tab.
3. In the field **Support Case Number** enter the service request number created above.
4. In the field **Upload Region** select option **EU** or **US** depending on the server where you want to upload your data.
5. In the field **Command-line Arguments** you can enter options for tool which is used to collect the data from the target system. Which tool will be used can be found in the tip below this field.
6. In the field **Earliest** select the time of running this action.
7. Click button [**Schedule**]. The action is scheduled and will be executed defined time. It will collect the data from the client and upload it directly to the upload server.

Supported Products where support data can be collected:

- SUSE Multi-Linux Managerプロキシ
- SUSE Multi-Linux Manager Server when it is registered as Peripheral Server in a Hub Scenario
- all SUSE Linux Enterprise Server and openSUSE clients
- SUSE Liberty and compatible clients
- Ubuntu clients
- Debian clients

To upload the support data from the main SUSE Multi-Linux Manager Server please still use **mgradm support config** from the container host.

Chapter 30. トラブルシューティング

このセクションには、SUSE Multi-Linux Managerで発生する可能性のある共通の問題、およびそれらの問題を解決するためのソリューションが含まれています。

パブリッククラウドに固有のトラブルシューティングのトピックについては別途説明します。

パブリッククラウドのトラブルシューティングについては、**Specialized-guides › Public-cloud-guide**を参照してください。

30.1. 自動インストールのトラブルシューティング

通信にプレーンなSalt (salt-minion)実装を使用する場合は、必要なすべてのソフトウェア(ソフトウェアパッケージ)が設定済みクライアントチャンネルで適切に利用できることを各自で確認する必要があります。 この実装をSUSE Multi-Linux Managerと一緒に使用することは推奨されません。

デフォルトのSalt Bundle (venv-salt-minion)実装では、クライアントベースチャンネルと互換性のある子チャンネルとしてクライアントツールチャンネルのみが必要です。 必要なすべてのパッケージはSalt Bundleの一部となります。

- 自動インストールプロファイルのベースチャンネルに関するクライアントツールソフトウェアチャンネルを組織およびユーザで使用できることを確認します。
- ツールチャンネルが子チャンネルとしてSUSE Multi-Linux Managerで使用できることを確認します。
- プレーンなSalt (salt-minion)実装を使用する場合のみ、関連するチャンネルで、必要なパッケージと依存関係が使用可能であることも確認します。

30.2. サポート終了製品のブートストラップリポジトリのトラブルシューティング

サポートされている製品を同期するとき、ブートストラップリポジトリは、自動的に作成され、SUSE Multi-Linux Managerサーバに再生成されます。 製品がサポート終了になり、サポートされなくなったが、製品の使用を継続する場合、ブートストラップリポジトリを手動で作成する必要があります。

ブートストラップリポジトリの詳細については、**Client-configuration › Bootstrap-repository**を参照してください。

プロシージャ: サポート終了製品のブートストラップリポジトリの作成

1. SUSE Multi-Linux Managerコンテナホストのコマンドプロンプトで、rootとしてサーバコンテナに入ります。

```
mgrctl term
```

2. コンテナ内で次の手順を実行します。

a. **--force**オプションを指定して使用可能なサポート対象外のブートストラップリポジトリの一覧を表示してください。たとえば下記のようになります:

```
mgr-create-bootstrap-repo --list --force
1. SLE-12-SP2-x86_64
2. SLE-12-SP3-x86_64
```

b. 製品ラベルとして適切なリポジトリ名を使用して、ブートストラップリポジトリを作成します。

```
mgr-create-bootstrap-repo --create SLE-12-SP2-x86_64 --force
```

ブートストラップリポジトリを手動で作成しない場合、必要な製品およびブートストラップリポジトリでLTSSが使用できるかどうかを確認できます。

30.3. クライアントが複製したSaltクライアントのトラブルシューティング

ハイパーバイザ複製ユーティリティを使用していて、複製したSaltクライアントを登録しようすると、次のエラーが発生します。

```
残念ながら、このシステムは見つかりませんでした。
```

新しい複製システムのマシンIDが既存の登録済みシステムのマシンIDと同じことが原因です。 マシンIDを手動で調整してエラーに対処すると、複製したシステムを正常に登録できます。

詳細および手順については、**Administration › Troubleshooting**を参照してください。

30.4. 「ディスクがいっぱいになったコンテナ」イベントのトラブルシューティング

コンテナの永続ストレージメディアとしてマウントされた専用ディスクのストレージ領域が不足した場合は、緊急アクションが必要になります。

ストレージメディアのサイズ変更に関する問題を解決するには、次の手順に従います。 コンテナホスト上で、**root**として一覧にされているコマンドをすべて実行します。

プロシージャ: ストレージメディアのサイズ変更

1. ディスクのサイズを増やします。 取るべきアクションは、インストールシナリオによって異なります。
2. ディスクがパーティション設定されている場合(たとえば、ディスク**/dev/vdb**に**/dev/vdb1**がある場合)、次のコマンドを実行します。

   次のコマンドを実行します。

   a. **parted /dev/vdb**

b. **(parted) print**

c. **(parted) resizepart NUMBER 100%**ここで **NUMBER**は**print**コマンドで表示されるパーティション番号です(たとえば、**/dev/vdb1**の場合は**1**)

d. **(parted) quit**

3. ファイルシステムのサイズを変更します。 たとえば、XFSファイルシステムの場合、次のコマンドを実行します。

```
xfs_growfs /dev/vdb1
```

手順を完了すると、XFSファイルシステムがディスク上の使用可能な容量をすべて使用しているはずです。

30.5. 破損したリポジトリのトラブルシューティング

リポジトリメタデータファイルの情報が破損したり、古くなったりする可能性があります。 これにより、クライアントの更新で問題が発生する可能性があります。 これは、ファイルを削除して再生成することで修正できます。 新しいリポジトリデータファイルを使用すると、更新が期待どおりに動作するはずです。

プロシージャ: 破損したリポジトリデータの解決

1. **/var/cache/rhn/repodata/<channel-label>**からすべてのファイルを削除します。 チャンネルラベルがわからない場合は、SUSE Multi-Linux Manager Web UIで**ソフトウェア › チャンネル › チャンネルラベル**に移動して検索できます。
2. コンテナホストで、コマンドラインから、次のコマンドを実行してコンテナ内のファイルを再生成します。

```
mgrctl exec -ti -- spacecmd softwarechannel_regenerateyumcache <channel-label>
```

30.6. パッケージが競合するカスタムチャンネルのトラブルシューティング

パッケージが競合するカスタムチャンネルを設定する場合、ブートストラップリポジトリの作成などの機能が未定義の動作を引き起こし、クライアントの登録に失敗する可能性があります。

たとえば、バージョン番号がより新しい競合するパッケージがブートストラップリポジトリに含まれる可能性があります。 このようなパッケージ(たとえば、**python3-zmq**や**zeromq**)により、ブートストラップリポジトリの作成が破損したり、クライアントのブートストラップ中に問題が発生する可能性があります。

カスタムチャンネル(たとえば、EPELチャンネル)が親ベンダチャンネルの下に追加されると、パッケージの競合に関する問題を直接解決できません。 これを解決する方法は、カスタムチャンネルをベンダチャンネルから分離する方法です。 カスタムチャンネルを別のツリーで作成する必要があります。 カスタムチャンネルを子として配信する必要がある場合は、このような環境をコンテンツライフサイクル管理(CLM)を使用して作成できます。 CLMプロジェクトのソースは別のツリーからそこに追加できます。 このようなアプローチを使用すると、カスタムチャンネルは構築された環境内で親の下に維持されます。 ただし、ベンダチャンネルツリーはカスタムチャンネルとブートストラップリポジトリなしで維持されます。 その後、クライアントの

登録は正しく機能します。

競合するパッケージ(salt、zeromqなど)を持つカスタムチャンネルを子チャンネルとして作成する場合は、次のステップに従うことで問題を回避できます。

プロシージャ: カスタムチャンネルで競合するパッケージを回避する

1. カスタムチャンネルを親チャンネルから子チャンネルとして削除します。 詳細については、administration:custom-channels.pdfを参照してください。
2. 別のツリーでカスタムチャンネルを作成します。 詳細については、administration:custom-channels.pdfを参照してください。 コンテンツライフサイクル管理(CLM)内で子チャンネルとしてカスタムチャンネルを取得するには、次の手順に従います。
   - SUSE Multi-Linux ManagerのWeb UIで、**コンテンツライフサイクル**に移動し、**[プロジェクトの作成]**をクリックします。 ［**名前**］と［**ラベル**］に入力します。
   - ソースをプロジェクトに割り当てます。 必要なベンダチャンネルとカスタムチャンネルを使用します。 (CentOS8を使用した共有例)
   - プロジェクトに環境を追加します。 たとえば、CentOS8を使用します。
   - 環境を構築するには、**[ビルド]**ボタンをクリックします。 これにより、アクティベーションキーに関連付けて、クライアントのブートストラップに使用できるベンダチャンネルとカスタムチャンネルを備えた環境が作成されます。
3. 重要なメモ: CLMプロジェクトでは、問題のあるパッケージや競合するパッケージを除外するフィルタを追加することをお勧めします。 これを追加しないと、より新しいバージョン番号の競合するパッケージがクライアントの更新中にインストールされます。 フィルタリングの詳細については administration:content-lifecycle-examples.pdfを参照してください。
4. 最新のパッチをCLM環境(ベンダチャンネルおよびカスタムチャンネルを使用)に取得するには、プロジェクトの**[ビルド]**ボタンをクリックします。 これは、環境を再構築するために必要です。
   - CLM の詳細については、**Administration › Content-lifecycle** を参照してください。

> Extra Packages for Enterprise Linux (EPEL)を直接Red Hat Enterprise Linuxクライアント(または互換性のあるSUSE Liberty Linux、CentOS、Oracle Linuxなど)上で使用すると、EPELからSaltパッケージがインストールされます。この場合、SUSE Multi-Linux Managerで提供されているSaltパッケージで利用可能な一部の機能がインストールされません。これが特に重要な理由は、ブートストラップリポジトリにSUSE以外のSaltパッケージが含まれる結果になるためです。したがって、これはサポート対象外のシナリオです。
>
> EPELリポジトリを有効にする必要がある場合は、事前にEPELからSaltパッケージをフィルタで除外してください(たとえば、**ソフトウェア › 管理 › チャンネル › EPEL › パッケージ**でSaltパッケージを削除します)。

30.7. FQDNS grainの無効化のトラブルシューティング

FQDNS grainは、システムのすべての完全修飾DNSサービスのリストを返します。 この情報の収集は、通

常、高速プロセスですが、DNS設定が間違っていると、長時間かかる可能性があります。　場合によっては、クライアントが無応答またはクラッシュする場合があります。

この問題を回避するには、Saltフラグを使用してFQDNS grainを無効にできます。 grainを無効にした場合、ネットワークモジュールを使用して、FQDNSサービスを提供できます。この場合、クライアントが無応答になるリスクはありません。

この操作は、古いSaltクライアントにのみ適用されます。　最近Saltクライアントを登録した場合、FQDNS grainはデフォルトで無効になっています。

SUSE Multi-Linux Managerサーバのコマンドプロンプトで、次のコマンドを使用してFQDNS grainを無効にします。

```
salt '*' state.sls util.mgr_disable_fqdns_grain
```

このコマンドを実行すると、各クライアントが再起動され、サーバが処理する必要があるSaltイベントが生成されます。 クライアント数が多い場合、バッチモードでコマンドを実行できます。

```
salt --batch-size 50 '*' state.sls util.mgr_disable_fqdns_grain
```

バッチコマンドの実行完了を待機します。 `Ctrl` + `C` でプロセスを中断しないでください。

30.8. ディスク容量のトラブルシューティング

ディスク容量が不足すると、SUSE Multi-Linux Managerデータベースとファイル構造に重大な影響を及ぼす可能性があり、ほとんどの場合、回復できません。 SUSE Multi-Linux Managerでは特定のディレクトリの空き容量を監視し、設定可能なアラートを用意しています。　スペース管理の詳細については、**Administration › Space-management**を参照してください。

一般的に、コンテナボリュームはホストファイルシステムと容量を共有します。**btrfs**ファイルシステムがいっぱいになった場合、ファイルを削除できなくなる可能性があります。これを解決するために、**btrfs device add**コマンドを使用して、小容量のストレージを一時的にファイルシステムに追加できます。これにより、ファイルを削除して容量を増やし、ファイルシステムをさらにメンテナンスできるようになります。メンテナンスが完了したら、**btrfs device delete**を使用して一時ストレージを削除できます。このトピックの詳細については、https://www.suse.com/support/kb/doc/?id=000018779を参照してください。

使用されていないソフトウェアチャンネルを削除することにより、ディスク容量を回復できます。

- ベンダチャンネルの削除方法については、**Administration › Channel-management**を参照してください。
- カスタムチャンネルの削除方法については、**Administration › Custom-channels**を参照してください。

カスタムチャンネルが同期される頻度を確認することもできます。　カスタムチャンネル同期の処理方法については、administration:custom-channels.pdfを参照してください。

未使用のアクティベーションキー、コンテンツライフサイクルプロジェクト、およびクライアント登録をクリーンアップすることで、ディスク容量を回復することもできます。 また、冗長なデータベースエントリを削除することもできます。

プロシージャ: 冗長なデータベースエントリの解決

1. **spacewalk-data-fsck**コマンドを使用して、冗長なデータベースエントリを一覧にします。
2. **spacewalk-data-fsck --remove**コマンドを使用して削除します。

30.9. ファイアウォールのトラブルシューティング

送信トラフィックをブロックするファイアウォールを使用している場合は、**REJECT**または**DROP**のいずれかのネットワーク要求を実行できます。 **DROP**に設定されている場合、SUSE Customer Centerとの同期がタイムアウトする可能性があります。

これは、同期プロセスがSUSE Customer Centerだけではなく、SUSE以外のクライアント用のパッケージを提供するサードパーティリポジトリにアクセスする必要があるために発生します。 SUSE Multi-Linux Managerサーバがこれらのリポジトリに到達して有効であることを確認しようとすると、ファイアウォールは要求をドロップし、同期はタイムアウトするまで応答を待ち続けます。

これが発生する場合、同期が失敗するまで長時間かかり、SUSE以外の製品が製品リストに表示されません。

この問題はさまざまな方法で修正できます。

最も簡単な方法は、SUSE以外のリポジトリで必要なURLへのアクセスを許可するようにファイアウォールを設定することです。 これにより、同期プロセスがURLに到達し、正常に完了することができます。

外部トラフィックを許可できない場合は、SUSE Multi-Linux Managerからの**REJECT**(**DROP**ではない)要求を行うようにファイアウォールを設定してください。 これにより、サードパーティURLへの要求が拒否されるため、同期はタイムアウトではなく早期に失敗し、製品はリストに表示されません。

ファイアウォールへの設定アクセス権がない場合は、代わりにSUSE Multi-Linux Managerサーバに別のファイアウォールを設定することを検討してください。

30.10. WAN接続を介したSUSE Multi-Linux Managerサーバとプロキシ間の長い同期時間に関するトラブルシューティング

WebUIで、あるいはディストリビューションまたはシステム設定へのAPIコールを介して実行される変更によっては、SUSE Multi-Linux ManagerサーバからSUSE Multi-Linux Managerプロキシシステムにファイルを転送するために、**cobbler sync**コマンドが必要になる場合があります。これを実現するために、Cobblerは**/etc/cobbler/settings**で指定されたプロキシのリストを使用します。

cobbler syncは、その設計上、変更されたファイルや最近追加されたファイルのみを同期することはできません。

代わりに、**cobbler sync**を実行すると、**/etc/cobbler/settings**で設定された指定のすべてのプロキシに**/srv/tftpboot**ディレクトリの完全同期がトリガされます。また、関連するシステム間のWAN接続の遅延によっても影響を受けます。

/var/log/cobbler/のログによると、同期のプロセスが完了するまでにかなりの時間がかかる場合があります。

たとえば、次の日時に開始したとします。

```
Thu Jun  3 14:47:35 2021 - DEBUG | running python triggers from
/var/lib/cobbler/triggers/task/sync/pre/*
Thu Jun  3 14:47:35 2021 - DEBUG | running shell triggers from
/var/lib/cobbler/triggers/task/sync/pre/*
```

そして、次の日時に終了したとします。

```
Thu Jun  3 15:18:49 2021 - DEBUG | running shell triggers from
/var/lib/cobbler/triggers/task/sync/post/*
Thu Jun  3 15:18:49 2021 - DEBUG | shell triggers finished successfully
```

転送量は約1.8GBでした。 転送には30分ほどかかりました。

比較すると、**/srv/tftpboot**と同じサイズの大きな単一ファイルのコピーは、数分以内に完了します。

SUSE Multi-Linux Managerサーバとプロキシ間でファイルをコピーするために**rsync**ベースのアプローチに切り替えると、転送時間と待機時間を短縮できる場合があります。

このタスクを実行するためのスクリプトは、https://suse.my.salesforce.com/sfc/p/1i000000gLOd/a/1i000000ll5B/B2AmvIJN2_JsAyjTQzCVP_x5ioVgd0bYN9X9NpMugS8でダウンロードできます。

このスクリプトはコマンドラインオプションを受け入れません。 スクリプトを実行する前に、手動で編集し、**MLMHOSTNAME**、**MLMIP**、および**MLMPROXY1**変数を正しく設定して、スクリプトが正しく機能するようにする必要があります。

スクリプトの個々の調整に利用可能なサポートはありません。 スクリプトと内部のコメントは、プロセスの概要と考慮すべきステップを提供することを目的としています。 さらにサポートが必要な場合は、SUSEコンサルティングにお問い合わせください。

スクリプトを使用した提案されるアプローチは、次の環境で役立ちます。

- SUSE Multi-Linux Managerプロキシシステムが WAN接続を介して接続されている。
- **/srv/tftpboot**に多数のディストリビューション用ファイルおよびクライアントPXEブートファイル(合計数千ファイル)が含まれている。
- **/etc/cobbler/settings**の任意のプロキシは無効になっているが、それ以外の場合、SUSE Multi-Linux Managerは引き続きプロキシとコンテンツを同期する。

```
#proxies:
```

```
# - "MLMproxy.MLMproxy.test"
# - "MLMproxy2.MLMproxy.test"
```

プロシージャ: 新しい同期速度の分析

1. SUSE Multi-Linux Managerと関連するシステム間のTCPトラフィックのダンプを取得します。
   - SUSE Multi-Linux Managerサーバの場合:

     ```
     tcpdump -i ethX -s 200 host <ip-address-of-susemanagerproxy> and not ssh
     ```

   - SUSE Multi-Linux Managerプロキシの場合:

     ```
     tcpdump -i ethX -s 200 host <ip-address-of-susemanager> and not ssh
     ```

   - これにより、分析を実行するのに十分な200のパッケージサイズのみがキャプチャされます。
   - プロキシと通信するためにSUSE Multi-Linux Managerが使用する各ネットワークインタフェースにehtXを調整します。
   - 最後に、さらにパッケージ数を削減するため、ssh通信はキャプチャされません。
2. **cobbler sync**を開始します。
   - 同期を強制するため、最初にCobbler jsonキャッシュファイルを削除してから、**cobbler sync**を発行します。

     ```
     rm /var/lib/cobbler/pxe_cache.json
     cobbler sync
     ```

3. **cobbler sync**が終了したら、TCPdumpsを停止します。
4. Wiresharkを使用してTCPdumpsを開き、［**Statistics（統計）** > **Conversations（対話）**］に移動して、ダンプが分析されるのを待ちます。
5. TCPタブに切り替えます。 このタブに表示される数は、SUSE Multi-Linux ManagerサーバとSUSE Multi-Linux Managerプロキシ間でキャプチャされた合計対話数を示しています。
6. ［**Duration**］（期間）列を探します。
   - 昇順にソートして開始し、ファイルの転送にかかった最小時間を確認します。
   - 降順にソートして続行し、カーネルやinitrdの転送など、大きなファイルの最大値を確認します。

     ポート4505と4506はSalt通信に使用されるため無視してください。

TCPdumpsの分析では、SUSE Multi-Linux Managerサーバからプロキシへの、サイズが約1800バイトの小さなファイルの転送に約0.3秒かかったことを示しています。

大きなファイルは多くありませんでしたが、小さなファイルの数が多いため、転送されるファイルごとに新しいTCP接続が作成され、確立された接続数が多くなりました。

したがって、最小転送時間と必要な接続数(たとえば、約5000)がわかれば、転送時間全体の概算推定時間が得られます(5000 * 0.3 / 60 = 25分)。

30.11. 無効なクライアントのトラブルシューティング

Taskomaticジョブは、クライアントが接続されていることを確認するため、クライアントに定期的にpingを送信します。　クライアントが24時間以上Taskomaticのチェックインに応答しない場合は、無効であるとみなされます。 Web UIで無効なクライアントのリストを表示するには、**システム › システム一覧 › 無効**に移動します。

クライアントはさまざまな理由で無効になる可能性があります。

- クライアントにSUSE Multi-Linux Managerサービスへのエンタイトルメントが付与されていない。
- クライアントがHTTPS接続を許可しないファイアウォールの背後にある。
- クライアントが誤って設定されたプロキシの背後にある。
- クライアントが異なるSUSE Multi-Linux Managerサーバと通信しているか、接続が正しく設定されていない。
- クライアントがSUSE Multi-Linux Managerサーバと通信できるネットワーク内にない。
- ファイアウォールがクライアントとSUSE Multi-Linux Managerサーバ間のトラフィックをブロックしている。
- Taskomaticが正しく設定されていない。

サーバへのクライアント接続の詳細については、**Client-configuration › Contact-methods-intro**を参照してください。

ポート設定の詳細については、installation-and-upgrade:network-requirements.pdfを参照してください。

ファイアウォールのトラブルシューティングの詳細については、**Administration › Troubleshooting**を参照してください。

30.12. サーバ間同期のトラブルシューティング

サーバ間同期では、キャッシュを使用してISSマスターとスレーブを管理します。　これらのキャッシュには、無効なエントリを作成するバグが発生する可能性があります。　この場合、キャッシュがまだ無効なエントリを使用しているため、バグを解決するバージョンに更新した後でもバグが表示される可能性があります。　新しいバージョンのISSにアップグレードしても問題が解決しない場合は、すべてのキャッシュをクリアして、問題の原因となる古いエントリがないことを確認します。

キャッシュエラーにより、さまざまなエラーで同期が失敗する可能性がありますが、エラーメッセージは通常、次のような内容をレポートします。

```
consider removing satellite-sync cache at /var/cache/rhn/satsync/* and re-run satellite-
```

```
sync with same options.
```

これを解決するには、ISSマスターとISSスレーブでキャッシュを削除して、同期が正常に完了するようにします。

サーバコンテナ内でシェルにアクセスするには、コンテナホストで**mgrctl term**を実行します。

プロシージャ: ISSキャッシュエラーの解決

1. ISSマスターのコマンドプロンプトで、rootとして、マスターのキャッシュファイルを削除します。

```
rm -rf /var/cache/rhn/xml-*
```

2. サービスを再起動します。

```
rcapache2 restart
```

3. ISSマスターのコマンドプロンプトで、rootとして、スレーブのキャッシュファイルを削除します。

```
rm -rf /var/cache/rhn/satsync/*
```

4. サービスを再起動します。

```
rcapache2 restart
```

30.13. ローカル発行者証明書のトラブルシューティング

一部の古いブートストラップスクリプトは、ローカル証明書へのリンクを間違った場所に作成します。 これにより、zypperはローカルの発行者証明書に関する**Unrecognized error**を返します。 **/etc/ssl/certs/**ディレクトリをチェックすることにより、ローカル発行者証明書へのリンクが正しく作成されていることを確認できます。 この問題が発生した場合は、zypperが期待どおりに動作するようにブートストラップスクリプトを更新することを検討する必要があります。

30.14. ログインタイムアウトのトラブルシューティング

デフォルトでは、SUSE Multi-Linux Manager Web UIはユーザに30分後に再度ログインするように要求します。 環境によっては、ログインタイムアウトの値を調整したい場合があります。

値を調整するには、**rhn.conf**と **web.xml**の両方で変更する必要があります。 **/etc/rhn/rhn.conf**で秒単位の値、**web.xml**で分単位の値を設定してください。 この 2つの値は同じ時間に等しくなる必要があります。

たとえば、タイムアウト値を1時間に変更するには、**rhn.conf**の値を3600秒に設定し、**web.xml**の値を60分に設定します。

プロシージャ: Web UIログインタイムアウト値の調整

1. コンテナホストで、サーバコンテナ内でコマンドラインを開きます。

```
mgrctl term
```

   a. **/etc/rhn/rhn.conf**を開いて、次の行を追加または編集して、秒単位の新しいタイムアウト値を含めます。

```
web.session_database_lifetime = <Timeout_Value_in_Seconds>
```

   b. ファイルを保存して閉じます。

   c. **/etc/tomcat/web.xml**を開いて、次の行を追加または編集して、分単位の新しいタイムアウト値を含めます。

```
<session-timeout>Timeout_Value_in_Minutes</session-timeout>
```

   d. ファイルを保存して閉じます。

2. 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
```

30.15. メール設定のトラブルシューティング

安全なメール通信にするため、認証を有効にし、ユーザ名とパスワードを定義して、**/etc/rhn/rhn.conf**で**SSL**または**STARTLS**を有効にすることができます。

```
java.smtp_server = string (default: localhost)
java.smtp_port = integer (default: 25)
java.smtp_auth = true/false (default: false)
java.smtp_ssl = true/false (default: false)
java.smtp_starttls = true/false (default: false)
java.smtp_user = string (default: null)
java.smtp_pass = string (default: null)
```

SMTPサーバ通信の接続タイムアウトを増やすには、**/etc/rhn/rhn.conf**で次のパラメータを設定できます:

```
java.smtp_timeout = integer (デフォルト: 5000)
java.smtp_connection_timeout = integer (デフォルト: 5000)
java.smtp_write_timeout = integer (デフォルト: 5000)
```

30.16. Mass Machine_id Duplication

SUSE Multi-Linux Managerを使用して仮想マシンを管理している場合は、仮想マシンのクローンを作成すると役立つ場合があります。 クローンとは、既存のディスクの正確なコピーであるプライマリディスクを使用

する仮想マシンのことです。

仮想マシンのクローンを作成すると時間を大幅に節約できますが、ディスク上の識別情報が重複しているために問題が発生する可能性があります。

If you try to register two machine where one is the clone of the other, you probably want SUSE Multi-Linux Manager to register them as two separate clients. However, if the machine ID in both the original client and the clone is the same, SUSE Multi-Linux Manager registers both clients as one system, and the data is overwritten one the second machine is registered.

This can be resolved by changing the machine ID of the clone, so that SUSE Multi-Linux Manager recognizes them as two different clients. For more information and instructions on how to change machine ID, see **Administration › Troubleshooting**.

However, in some situations, it is neither feasible nor practical to change the machine ID on all systems, as this could disrupt other applications that depend on the existing machine IDs. In those cases, a option is available where a fake machine ID is generated to be used in the context of SUSE Multi-Linux Manager.

Procedure: Generating machine ID for SUSE Multi-Linux Manager at registration time

1. Create a Bootstrap script (skip this step if you already have it) For more information, see **Client-configuration › Registration-bootstrap**.
2. Open the file and change the parameter:

```
GENERATE_OWN_MACHINEID=1
```

3. Start using your bootstrap strict, and machine ID will not collide anymore.

30.17. noexecで/tmpをマウントする場合のトラブルシューティング

Saltはクライアントのファイルシステム上の**/tmp**からリモートコマンドを実行します。 したがって、**noexec**オプションを指定して**/tmp**をマウントしないでください。 この問題を解決する別の方法は、一時ディレクトリパスをSaltサービスに指定された**TMPDIR**環境変数で上書きして、**noexec**オプションが設定されていないディレクトリを指すようにすることです。 Salt Bundleを使用する場合はsystemdドロップイン設定ファイル**/etc/systemd/system/venv-salt-minion.service.d/10-TMPDIR.conf**を使用し、クライアントで**salt-minion**を使用する場合は**/etc/systemd/system/salt-minion.service.d/10-TMPDIR.conf**を使用することをお勧めします。 ドロップイン設定ファイルの内容の例を次に示します。

```
[Service]
Environment=TMPDIR=/var/tmp
```

30.18. noexecで/var/tmpをマウントする場合のトラブルシューティング

Salt SSHは、**/var/tmp**を使用して、Salt Bundleを配備し、バンドルされたPythonを使用してクライアント上でSaltコマンドを実行しています。 したがって、**noexec**オプションを指定して**/var/tmp**をマウントしないでください。 ブートストラッププロセスがクライアントに到達するためにSalt SSHを使用しているため、**/var/tmp**が**noexec**オプションでマウントされたクライアントをWeb UIでブートストラップすることはできません。

30.19. 十分なディスク容量がない場合のトラブルシューティング

移行を開始する前に、使用できるディスク容量を確認してください。 別々のXFSファイルシステムで**/var/spacewalk**と**/var/lib/pgsql**を探すことをお勧めします。

別々のファイルシステムを設定している場合、**/etc/fstab**を編集し、**/var/lib/pqsql**サブボリュームを削除します。 サーバを再起動して変更を取得します。

アップグレードの問題の詳細については、移行ログファイルを確認してください。 ログファイルは、アップグレードしているシステムの**/var/log/rhn/migration.log**にあります。

30.20. 通知のトラブルシューティング

通知メッセージのデフォルトの有効期間は30日です。その期間が過ぎると、メッセージは読み込みステータスに関係なくデータベースから削除されます。 この値を変更するには、**/etc/rhn/rhn.conf**で次の行を追加または編集します。

```
java.notifications_lifetime = 30
```

通知タイプを有効または無効にするには、**/etc/rhn/rhn.conf**で次のように行を追加または編集します。

```
java.notifications_type_disabled = OnboardingFailed,ChannelSyncFailed,\
  ChannelSyncFinished,CreateBootstrapRepoFailed,StateApplyFailed,\
  PaygAuthenticationUpdateFailed,EndOfLifePeriod,SubscriptionWarning
```

デフォルト設定と設定オプションについては、**usr/share/rhn/config-defaults/rhn_java.conf**テンプレートファイルを参照してください。

30.21. OESリポジトリの有効化のトラブルシューティング

SUSE Multi-Linux ManagerサーバでOpen Enterprise Server (OES)を有効にするには、説明されているプロシージャに従います。

プロシージャ: OESリポジトリの有効化

1. OESにアクセスできるMicrofocusからのミラー資格情報があることを確認します。
2. SUSE Multi-Linux Managerサーバにログインします。
3. ［**管理 > セットアップウィザード > 組織の資格情報**］に移動します。
4. すでにSUSE Multi-Linux ManagerのSUSE資格情報があることを確認します。
5. 新規追加のオプションを選択し、Microfocus資格情報を入力します。
6. ［**管理 > セットアップウィザード > 組織の資格情報**］に移動して、更新操作が完了するのを待ちます。
7. OESは更新された製品リストに表示されます。 これで、他の製品のように、有効にできるようになりました。

OESの詳細については、https://www.microfocus.com/documentation/open-enterprise-server/を参照してください。

30.22. パッケージの不整合のトラブルシューティング

クライアント上のパッケージがロックされている場合、SUSE Multi-Linux Managerサーバは適用可能なパッチのセットを正しく判断できない場合があります。 この場合、パッケージの更新はWeb UIで使用できますが、クライアントには表示されず、クライアントを更新しようとすると失敗します。 パッケージのロックと除外リストをチェックして、クライアント上でパッケージがロックされているか除外されているかを判断します。

クライアント上で、パッケージのロックと除外リストをチェックして、パッケージがロックされているか、除外されているかを判断します。

- 拡張サポートプラットフォームでは、**/etc/yum.conf**をチェックして、**exclude=**を検索します。
- SUSE Linux EnterpriseおよびopenSUSEでは、**zypper locks**コマンドを使用します。

30.23. grainを開始イベントに渡す場合のトラブルシューティング

Saltクライアントは、起動するたびに、**machine_id** grainをSUSE Multi-Linux Managerに渡します。SUSE Multi-Linux Managerは、このgrainを使用して、クライアントが登録されたかどうかを判定します。 このプロセスでは、同期Saltコールが必要です。同期Saltコールは、その他のプロセスをブロックするため、多数のクライアントを同時に起動する場合、大幅な遅延が発生する可能性があります。

この問題を克服するために、別々の同期Saltコールを回避するための新しい機能がSaltに導入されました。

この機能を使用するには、この機能をサポートしているクライアントのクライアント設定に設定パラメータを追加できます。

このプロセスを簡単にするには、**mgr_start_event_grains.sls**ヘルパーSaltの状態を使用します。

この操作は、登録済みのクライアントにのみ適用されます。 最近Saltクライアントを登録した場合、この設定パラメータはデフォルトで追加されています。

SUSE Multi-Linux Managerサーバのコマンドプロンプトで、次のコマンドを使用して**start_event_grains**設定ヘルパーを有効にします。

```
salt '*' state.sls util.mgr_start_event_grains
```

このコマンドを実行すると、必要な設定がクライアントの設定ファイルに追加され、クライアントを再起動したときに適用されます。 クライアント数が多い場合、バッチモードでコマンドを実行できます。

```
salt --batch-size 50 '*' state.sls mgr_start_event_grains
```

30.24. プロキシの接続およびFQDNのトラブルシューティング

プロキシ経由で接続されているクライアントがWeb UIに表示されることがありますが、そのようなクライアントがプロキシ経由で接続されていることは示されません。 完全修飾ドメイン名(FQDN)を使用して接続していない場合、SUSE Multi-Linux Managerでプロキシが認識されないと、この動作が発生することがあります。

この動作を修正するには、プロキシのクライアント設定ファイルでgrainとして追加のFQDNを指定します。

```
grains:
  susemanager:
     custom_fqdns:
       - name.one
       - name.two
```

30.25. クローンクライアントの登録のトラブルシューティング

SUSE Multi-Linux Managerを使用して仮想マシンを管理している場合は、仮想マシンのクローンを作成すると役立つ場合があります。 クローンとは、既存のディスクの正確なコピーであるプライマリディスクを使用する仮想マシンのことです。

仮想マシンのクローンを作成すると時間を大幅に節約できますが、ディスク上の識別情報が重複しているために問題が発生する可能性があります。

すでに登録されているクライアントがある場合は、そのクライアントのクローンを作成してから、クローンを登録しようとすると、おそらく、SUSE Multi-Linux Managerでそれらを2つの別々のクライアントとして登録する必要があります。 ただし、元のクライアントとクローンのマシンIDが同じ場合、SUSE Multi-Linux Managerは両方のクライアントを1つのシステムとして登録し、既存のクライアントデータはクローンのデータで上書きされます。

これは、SUSE Multi-Linux Managerが2つの別のクライアントとして認識できるように、クローンのマシンIDを変更することで解決できます。

このプロシージャの各ステップはクローンクライアントで実行されます。 このプロシー

> ジャではSUSE Multi-Linux Managerに登録されたままである、元のクライアントを操作しません。

プロシージャ: 複製されたSaltクライアントでの重複するマシンIDを解決する

1. **Initial System Configuration**
   a. クローンマシンで、ホスト名とIPアドレスを変更します。 **/etc/hosts**に加えられた変更と正しいホストエントリが含まれていることを確認します。
2. **Resolving Duplicate Machine IDs**
   a. For distributions that support systemd:
      i. If your machines have the same machine ID, as root, delete the files on each duplicated client and re-create it:

```
rm /etc/machine-id
rm /var/lib/dbus/machine-id
rm /var/lib/zypp/AnonymousUniqueId
dbus-uuidgen --ensure
systemd-machine-id-setup
```

      ii. If the cloned machine also has a folder in **/var/log/journal/** it needs to be renamed accordingly to the new machine ID. If names do not match, **journalctl** could not retrieve any log and **podman logs** would not show anything.

```
mv /var/log/journal/* /var/log/journal/$(cat /etc/machine-id)
```

   b. For distributions that do not support systemd:
      i. As root, generate a machine ID from dbus:

```
rm /var/lib/dbus/machine-id
rm /var/lib/zypp/AnonymousUniqueId
dbus-uuidgen --ensure
```

> ○ If you are cloning a Red Hat Enterprise Linux 8.10 server that will later be liberated to SUSE Liberty Linux, you must perform extra steps to fix the kernel configuration files.
>
> Red Hat Enterprise Linux uses the machine ID to

generate kernel entries in **/boot/loader/entries**. Not performing these steps will result in a mix of old and new kernel entries after the liberation, as SUSE Liberty Linux kernels will create new entries instead of replacing the old ones.

- After changing the machine ID and before liberating, run:

```
sudo rm -rf /boot/loader/entries/
sudo for ver in $(rpm -q kernel --qf '%{VERSION}-
%{RELEASE}.%{ARCH}\n'); do echo "Reinstalling kernel
$ver..."; sudo kernel-install add $ver /lib/modules/$ver;
done
sudo grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
```

- For more information and example on liberating Red Hat Enterprise Linux 8.10 server, see **Common-workflows › Workflow-liberate-rhel-with-secureboot**.

3. **Reconfiguring Salt Clients**

   a. If your clients still have the same Salt client ID, delete the **minion_id** file on each client (FQDN is used when it is regenerated on client restart).

      i. For Salt Minion clients:

```
rm /etc/salt/minion_id
rm -rf /etc/salt/pki
```

      ii. Salt Bundleクライアントの場合:

```
rm /etc/venv-salt-minion/minion_id
rm -rf /etc/venv-salt-minion/pki
```

   b. Delete accepted keys from the onboarding page and the system profile from SUSE Multi-Linux Manager, and restart the client with.

      i. For Salt Minion clients:

```
service salt-minion restart
```

ii. Salt Bundleクライアントの場合:

```
service venv-salt-minion restart
```

c. クライアントを再登録します。各クライアントは異なる**/etc/machine-id**を持つようになり、［**システムの概要**］ページに正しく表示されるはずです。

30.26. SL Microへのリモートルートログイン

For enhanced security, new installations of SL Micro 6.1 and later do not allow password-based remote root login anymore, which affects server and proxy container hosts running on SL Micro and managed SL Micro clients. Also, SLE Micro 5.5 clients with password-based remote root login which will when be migrated to 6.1/6.2 will suddenly lose this access and must be newly configured. For more information, see SL Micro Release Notes 6.1 (https://www.suse.com/releasenotes/x86_64/SL-Micro/6.1/index.html#jsc-SMO-405).

SUSE Multi-Linux ManagerプロキシなどのSUSE Multi-Linux Managerコンポーネントを配備する際に、デフォルトで、パスワードベースのリモートルートログインが必要です。 パスワードベースのリモートルートログインは次のステップで有効化できます。

プロシージャ: SL Microでのパスワードを使用したSSHルートログインの有効化

You can enable SSH root login in two different ways. Either of them will work; choose the one that best fits your setup.

Option A: Use the preconfigured package

1. Install the package **openssh-server-config-rootlogin** from the UI/API on the client.
2. Reboot the container host to activate the new configuration either from UI or from terminal

Option B: Edit the SSH configuration manually

1. Add a drop-in config **/etc/ssh/sshd_config.d/permit_root.conf** file, with the following content:

```
PermitRootLogin yes
```

2. Reload the SSH server configuration

```
systemctl reload sshd
```

3. If connected using SSH, before disconnecting from the server, validate the SSH server is working correctly by opening a new SSH connection.

transactional-updateの詳細については、https://documentation.suse.com/sle-micro/6.1/html/Micro-transactional-updates/を参照してください。

30.27. 削除されたクライアントの登録のトラブルシューティング

サーバコンテナでステップを実行する前に、**mgrctl term**を使用します。

削除された(登録解除された)クライアントを新しく登録できないことがあります。この問題を解決するには、再登録をもう一度試みる前に、SUSE Multi-Linux Managerサーバ(Saltマスター)上で一部のSaltキャッシュファイルを削除する必要があります。

```
rm /var/cache/salt/master/thin/version
rm /var/cache/salt/master/thin/thin.tgz
```

30.28. Web UIからの登録が失敗し、エラーが表示されない場合のトラブルシューティング

Web UIからの初期登録では、すべてのSaltクライアントがSalt SSHを使用しています。

その性質上、Salt SSHクライアントはサーバにエラーを報告しません。

ただし、Salt SSHクライアントは、エラーを検査できるログを**/var/log/salt-ssh.log**にローカルに保存します。

30.29. Red Hat CDNチャンネルと複数の証明書のトラブルシューティング

Red Hatコンテンツデリバリネットワーク(CDN)チャンネルは複数の証明書を提供することがありますが、SUSE Multi-Linux Manager Web UIは単一の証明書しかインポートできません。 CDNがSUSE Multi-Linux Manager Web UIで認識されている証明書とは異なる証明書を提示した場合、証明書が正確であっても検証が失敗し、リポジトリへのアクセスパーミッションが拒否されます。 次のようなエラーメッセージが生じます。

```
[error] (エラー)
Repository '<repo_name>' is invalid. (リポジトリ'<repo_name>'は無効です。)
<repo.pem> Valid metadata not found at specified URL (有効なメタデータが指定されている
URLで見つかりませんでした)
History: (履歴:)
 - [|] Error trying to read from '<repo.pem>' (
'<repo.pem>'からの読み込み時にエラーが発生しました)
 - Permission to access '<repo.pem>' denied. ('<repo.pem>'へのアクセスが拒否されました。)
Please check if the URIs defined for this repository are pointing to a valid
repository. (このリポジトリ用に定義されているURIが有効なリポジトリを指しているかどうかを確
```

```
認してください。)
Skipping repository '<repo_nam' because of the above error.
(上記エラーのため、リポジトリ'<repo_name>'をスキップします。)
Could not refresh the repositories because of
errors.(エラーが発生したため、リポジトリを更新できませんでした。)
HH:MM:SS RepoMDError: Cannot access repository. Maybe repository GPG keys are not
imported (HH:MM:SS RepoMDError: リポジトリにアクセスできません。リポジトリ
GPGキーがインポートされていない可能性があります)
```

この問題を解決するには、すべての有効な証明書を1つの**.pem**ファイルにマージし、SUSE Multi-Linux Managerで使用する証明書を再作成します。

手順: 複数のRed Hat CDN証明書の解決

1. Red Hat クライアントのコマンドプロンプトで、rootとして、**/etc/pki/entitlement/**からすべての現行の証明書を単一の **rh-cert.pem**ファイルに収集します。

```
cat 866705146090697087.pem 3539668047766796506.pem redhat-entitlement-authority.pem >
rh-cert.pem
```

2. **/etc/pki/entitlement/**からすべての現行のキーを単一の**rh-key. pem**ファイルに収集します。

```
cat 866705146090697087-key.pem 3539668047766796506-key.pem > rh-key.pem
```

次に、**Client-configuration › Clients-rh-cdn**の手順に従って、新しい証明書をSUSE Multi-Linux Managerサーバにインポートできます。

30.30. SUSE Multi-Linux Managerサーバの名前変更のトラブルシューティング

SUSE Multi-Linux Managerサーバのホスト名をローカルで変更する場合は、SUSE Multi-Linux Managerインストールが適切に機能しなくなります。 これは、変更がデータベースで行われていないため、変更がクライアントとプロキシに伝播されないためです。

30.30.1. サーバの名前変更

If you need to change the hostname of the SUSE Multi-Linux Manager Server, you can do so using the **mgradm server rename** command. This command updates the settings in the PostgreSQL database and the internal structures of SUSE Multi-Linux Manager.

30.30.1.1. サーバ設定

The command takes no mandatory parameter, but can take the new hostname if it is not the one from the container host.

In case any SSL certificate needs to be generated to match the new hostname, the SSL CA password needs to be provided. This is safely achieved using a configuration file

Procedure: Prepare the configuration file for the SSL CA password

1. Write a **config.yaml** file with content like the following:

```
ssl:
  password: "<THE CA PASSWORD>"
```

プロシージャ: SUSE Multi-Linux Managerサーバの名前変更

1. システムレベルのサーバのネットワーク設定を、DNSサーバでローカルおよびリモートで変更します。 逆引き名前解決のための設定を指定する必要もあります。 ネットワーク設定の変更は、他のシステムの名前変更と同じ方法で実行されます。
2. SUSE Multi-Linux Managerサーバを再起動して、新しいネットワーク構成を使用し、ホスト名が変更されていることを確認します。
3. On the container host, from the command line, execute the following command. Add **-c config.yaml** if you created the file to store the SSL CA password:

```
mgradm server rename
```

   If the new hostname is not resolvable, the command fails.

The renaming procedure also takes place during the restart of the server container. The logs can be found by running this command:

```
mgrctl exec -ti -- journalctl -u uyuni-update-config
```

Be aware that this command triggers a refresh of the pillar data for all Salt clients when restarting the server container: the time it takes to run depends on the number of registered clients.

30.30.1.2. 直接管理されているクライアントの再設定

クライアントがSUSE Multi-Linux Managerプロキシを介して管理されている場合は、この手順をスキップします。

次のプロシージャを使用して、直接管理されているクライアントを再設定し、新しいホスト名とIPアドレスを認識させるようにします。

プロシージャ: 直接管理されているクライアントの再設定

1. すべてのクライアントのSaltクライアント設定ファイルで、新しいSaltマスター(SUSE Multi-Linux Managerサーバ)の名前を指定します。 ファイル名は **/etc/venv-salt-minion/minion.d/susemanager.conf**です。Salt Bundleを使用しない場合は、**/etc/salt-minion/minion.d/susemanager.conf**です。

```
master: <new_hostname>
```

2. すべてのクライアントで、Saltサービスを再起動します。 次コマンドを実行します。

```
systemctl restart venv-salt-minion
```

または、Salt Bundleを使用しない場合は、次のコマンドを実行します。

```
systemctl restart salt-minion
```

30.30.1.3. highstateを適用したクライアント接続

最後に、ホスト名がSaltクライアント設定に完全に伝播されるようにするには、highstateを適用します。 highstateを適用すると、リポジトリURLのホスト名が更新されます。

30.30.2. プロキシの再設定

すべてのプロキシを再設定する必要があります。 新しいサーバ証明書とキーをプロキシにコピーする必要があります。 詳細については、**Installation-and-upgrade › Install-proxy**を参照してください。

プロキシ経由でPXEブートを使用する場合は、プロキシの設定を確認する必要があります。 コンテナ化されていないSUSE Multi-Linux Managerプロキシ4.3経由でPXEブートを使用する場合は、**tftpsync**を再設定する必要があります。

コンテナホストで、次のコマンドを実行します。

```
mgrctl exec -ti -- configure-tftpsync.sh
```

30.31. RPC接続タイムアウトのトラブルシューティング

RPC接続は、ネットワークが低速になったり、ネットワークリンクがダウンしたりするためにタイムアウトすることがあります。 その結果、パッケージのダウンロードやバッチジョブがハングしたり予想よりも時間がかかります。 設定ファイルを編集することで、RPC接続にかかる最大時間を調整できます。 ただし、これではネットワークの問題は解決されず、プロセスがハングするのではなく失敗します。

プロシージャ: RPC接続タイムアウトの解決

1. SUSE Multi-Linux Managerサーバで、**/etc/rhn/rhn.conf**ファイルを開いて、最大タイムアウト値(秒単位)を設定します。

```
server.timeout =`number`
```

On the SUSE Multi-Linux Manager Proxy, open the **/etc/uyuni/proxy/config.yaml** file and set a maximum timeout value (in seconds). The proxy containers need to be restarted for the change to be effective:

```
timeout: `number`
```

2. zypperを使用するSUSE Linux Enterprise Serverクライアントで、**/etc/zypp/zypp.conf**ファイルを開い

て、最大タイムアウト値(秒単位)を設定します。

```
## Valid values:  [0,3600]
## Default value: 180
download.transfer_timeout = 180
```

3. yumを使用するRed Hat Enterprise Linuxクライアントで、**/etc/yum.conf**ファイルを開いて、最大タイムアウト値(秒単位)を設定します。

```
timeout =`number`
```

RPCタイムアウトを**180**秒未満に制限する場合は、完全に正常な操作が中断されるリスクがあります。

30.32. ダウンと表示されるSaltクライアントとDNS設定のトラブルシューティング

Saltクライアントが実行されている場合でも、パッケージの更新や状態の適用などのアクションは、次のメッセージで失敗としてマークされる可能性があります。

```
Minionがダウンしているか、接続できませんでした。
```

この場合、アクションのスケジュールを変更してみてください。スケジュールの変更が成功した場合、問題の原因はDNS設定の誤りである可能性があります。

サーバコンテナ内でシェルにアクセスするには、コンテナホストで**mgrctl term**を実行します。

Saltクライアントが再起動されたとき、または grainが更新された場合、クライアントはFQDN grainを計算し、grainが処理されるまで応答しません。SUSE Multi-Linux Managerサーバでスケジュールされたアクションが実行される場合、SUSE Multi-Linux Managerサーバは、実際のアクションの前にクライアントに対して**test.ping**を実行し、クライアントが実際に実行されていてアクションをトリガできることを確認します。

デフォルトでは、SUSE Multi-Linux Managerサーバは**test.ping**コマンドからの応答を取得するために5秒間待機します。5秒以内に応答が受信されない場合、アクションは失敗に設定され、クライアントがダウンしているか、接続できなかったというメッセージが表示されます。

これを修正するには、クライアントのDNS解決を修正して、クライアントがFQDNの解決中に5秒間スタックしないようにします。

これができない場合は、SUSE Multi-Linux Managerサーバ上の**/etc/rhn/rhn.conf**ファイルの**java.salt_presence_ping_timeout**の値を4より大きい値に増やしてみてください。

例:

```
mgrctl term
```

```
vim /etc/rhn/rhn.conf
java.salt_presence_ping_timeout = 6
```

その後、次のコマンドを実行します。

```
mgradm restart
```

この値を大きくすると、minionに到達できないのかminionが応答しないのかをSUSE Multi-Linux Managerサーバが確認するのに時間がかかり、SUSE Multi-Linux Managerサーバの全体的な速度が低下したり応答しなくなったりします。

30.33. スキーマのアップグレードが失敗する場合のトラブルシューティング

スキーマのアップグレードに失敗すると、データベースのバージョン確認およびその他すべてのspacewalkサービスが開始されません。詳細および続行する方法のヒントについては、**mgradm start**を実行してください。

サーバコンテナ内でシェルにアクセスするには、コンテナホストで**mgrctl term**を実行します。

バージョン確認をコンテナ上で直接実行することもできます。

```
systemctl status uyuni-check-database.service
```

または

```
journalctl -u uyuni-check-database.service
```

一般的な　**mgradm**コマンドを実行しない場合、これらのコマンドを実行するとデバッグ情報が出力されます。

30.34. 同期のトラブルシューティング

同期はさまざまな理由で失敗する可能性があります。　接続問題に関する詳細情報を取得するには、次のコマンドを実行します。

```
export URLGRABBER_DEBUG=DEBUG
spacewalk-repo-sync -c <channelname> <options> > /var/log/spacewalk-repo-sync-$(date +%F-%R).log 2>&1
```

/var/log/zypper.logにあるZypperによって作成されたログを確認することもできます。

GPGキーの不一致

SUSE Multi-Linux Managerはサードパーティの GPGキーを自動的に信頼しません。　パッケージ同期が失

敗する場合は、信頼されていないGPGキーが原因である可能性があります。 この場合は、**/var/log/rhn/reposync**を開いて、次のようなエラーを検索することで確認できます。

```
['/usr/bin/spacewalk-repo-sync', '--channel', 'sle-12-sp1-ga-desktop-
nvidia-driver-x86_64', '--type', 'yum', '--non-interactive']
RepoMDError: Cannot access repository. Maybe repository GPG keys are not imported
```

この問題を解決するには、SUSE Multi-Linux ManagerにGPGキーをインポートする必要があります。GPGキーのインポートの詳細については、**Administration › Repo-metadata**を参照してください。

spacewalk-repo-syncからのGPGキーの削除

リポジトリのGPGキー が**spacewalk-repo-sync**を使用して手動でインポートされ、このキーが不要になった場合(たとえば、キーが侵害された場合や、テスト目的専用で使用された場合)、次のコマンドを使用して、**spacewalk-repo-sync**によって使用されるzypper RPMデータベースから削除できます。

```
rpm --dbpath=/var/lib/spacewalk/reposync/root/var/lib/rpm/ -e gpg-pubkey-*
```

ここで、**gpg-pubkey-***は削除されるGPGキーの名前です。

GPGキーの更新

GPGキーを更新する場合は、まず古いキーを削除してから、新しいキーを生成してインポートします。

チェックサムの不一致

チェックサムが失敗すると、**/var/log/rhn/reposync/*.log**ログファイルに次のようなエラーが表示される場合があります。

```
Repo Sync Errors: (50, u'checksums did not match
326a904c2fbd7a0e20033c87fc84ebba6b24d937 vs
afd8c60d7908b2b0e2d95ad0b333920aea9892eb', 'Invalid information uploaded
to the server')
The package microcode_ctl-1.17-102.57.62.1.x86_64 which is referenced by
patch microcode_ctl-8413 was not found in the database. This patch has
been skipped.
```

-Yオプションを使用して、コマンドラインプロンプトから同期を実行することで、このエラーを解決できます。

```
spacewalk-repo-sync --channel <channelname> -Y
```

このオプションはローカルにキャッシュされたチェックサムに依存するのではなく、同期前にリポジトリデータを検証します。

接続タイムアウト

ダウンロードが次のエラーでタイムアウトする場合:

```
28, 'Operation too slow. Less than 1000 bytes/sec transferred the last 300 seconds
```

このエラーは、**/etc/rhn/rhn.conf**で**reposync_timeout**と**reposync_minrate**の設定値を指定することで解決できます。 デフォルトでは、300秒で1秒あたり1000バイト未満の転送が行われると、ダウンロードが中止されます。 **reposync_minrate**で1秒あたりのバイト数を調整でき、**reposync_timeout**で待機する秒数を調整できます。

reposyncの実行中にキーを手動で信頼する

reposyncの実行時に、GPGキーを手動で承認する必要がある場合があります。 例:

```
# spacewalk-repo-sync -c nvidia-compute-sle-15-x86_64-we-sp3
17:07:40 ======================================
17:07:40 | Channel: nvidia-compute-sle-15-x86_64-we-sp3
17:07:40 ======================================
17:07:40 Sync of channel started.
New repository or package signing key received:
  Repository:       nvidia-compute-sle-15-x86_64-we-sp3
  Key Fingerprint:  610C 7B14 E068 A878 070D A4E9 9CD0 A493 D42D 0685
  Key Name:         cudatools <cudatools@nvidia.com>
  Key Algorithm:    RSA 4096
  Key Created:      Thu Apr 14 16:04:01 2022
  Key Expires:      (does not expire)
  Rpm Name:         gpg-pubkey-d42d0685-62589a51
    Note: Signing data enables the recipient to verify that no modifications occurred
after the data
    were signed. Accepting data with no, wrong or unknown signature can lead to a
corrupted system
    and in extreme cases even to a system compromise.
    Note: A GPG pubkey is clearly identified by its fingerprint. Do not rely on the
key's name. If
    you are not sure whether the presented key is authentic, ask the repository
provider or check
    their web site. Many providers maintain a web page showing the fingerprints of the
GPG keys they
    are using.
Do you want to reject the key, trust temporarily, or trust always? [r/t/a/?] (r):
```

30.35. Taskomaticのトラブルシューティング

リポジトリメタデータの再生成は比較的集中的なプロセスであるため、Taskomaticが完了するまでに数分かかる可能性があります。 また、Taskomaticがクラッシュした場合、リポジトリメタデータの再生成が中断される可能性があります。

サーバコンテナ内でシェルにアクセスするには、コンテナホストで**mgrctl term**を実行します。

Taskomatic がまだ実行されている場合、またはプロセスがクラッシュした場合は、Web UIでパッケージ更新が使用可能に見える場合がありますが、クライアントに表示されず、クライアントを更新しようとすると失敗します。 この場合、**zypper ref**コマンドを使用すると、次のようなエラーが表示されます。

```
Valid metadata not found at specified URL
```

これを修正するには、Taskomaticがまだリポジトリメタデータを生成中であるか、またはクラッシュが発生した可能性があるかどうかを判断します。 クライアントの更新が正しく実行されるように、メタデータの再生成が完了するまで待つか、クラッシュ後にTaskomaticを再起動します。

プロシージャ: Taskomaticの問題の解決

1. SUSE Multi-Linux Managerサーバで、**/var/log/rhn/rhn_taskomatic_daemon.log**ファイルを確認して、メタデータ再生成プロセスがまだ実行されているか、クラッシュが発生したかどうかを判断します。
2. taskomaticを再起動します。

```
service taskomatic restart
```

3. Taskomaticログファイルで、次のような開始および終了行を検索することで、メタデータ再生成に関連するセクションを特定できます。

```
<YYYY-DD-MM> <HH:MM:SS>,174 [Thread-584] INFO
com.redhat.rhn.taskomatic.task.repomd.RepositoryWriter - Generating new repository
metadata for channel 'cloned-2018-q1-sles12-sp3-updates-x86_64'(sha256) 550 packages,
140 errata

...

<YYYY-DD-MM> <HH:MM:SS>,704 [Thread-584] INFO
com.redhat.rhn.taskomatic.task.repomd.RepositoryWriter - Repository metadata
generation for 'cloned-2018-q1-sles12-sp3-updates-x86_64' finished in 4 seconds
```

30.36. Web UIの読み込みが失敗する場合のトラブルシューティング

移行後、Web UIが読み込まれない場合があります。 新しいシステムのホスト名およびIPアドレスが古いシステムと同じ場合、通常、このエラーはブラウザのキャッシュが原因です。 この重複によって一部のブラウザが混乱する可能性があります。

この問題は、キャッシュをクリアしてページを再読み込みすると解決します。 ほとんどのブラウザでは、この操作は、`Ctrl` + `F5` を押すことで実行できます。

Chapter 31. GNU Free Documentation License

0. PREAMBLE

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

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

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

1. APPLICABILITY AND DEFINITIONS

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

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

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

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections

then there are none.

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

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

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

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

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

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

2. VERBATIM COPYING

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

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

3. COPYING IN QUANTITY

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

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

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

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

4. MODIFICATIONS

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

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

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

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

D. Preserve all the copyright notices of the Document.

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

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

below.

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

H. Include an unaltered copy of this License.

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

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

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

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

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

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

O. Preserve any Warranty Disclaimers.

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

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

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

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

5. COMBINING DOCUMENTS

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

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

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

6. COLLECTIONS OF DOCUMENTS

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

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

7. AGGREGATION WITH INDEPENDENT WORKS

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

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

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this

License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

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

9. TERMINATION

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

10. FUTURE REVISIONS OF THIS LICENSE

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

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

ADDENDUM: How to use this License for your documents

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