

Uyuni 2026.01

# 管理者ガイド



U Y U N I

# 章 1. 序文

Administration Guide + Uyuni 2026.01

このガイドでは、Uyuni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: 2026-01-28

+ + + + + + + + + + + + + + + + + + + +

# 目次

|  |    |
|--|----|
| 1. 序文 .....  | 1  |
| 2. 動作 .....  | 8  |
| 2.1. 定期的なアクション                                     | 8  |
| 2.2. 動作チェーン  | 9  |
| 2.3. リモートコマンド                                      | 11 |
| 3. Ansibleの統合 .....                                | 12 |
| 3.1. 機能の概要   | 12 |
| 3.2. 要件と基本設定                                       | 12 |
| 3.3. インベントリの検査                                     | 13 |
| 3.4. Playbookの検出                                   | 13 |
| 3.5. Playbookの実行                                   | 13 |
| 3.6. Ansible制御ノードのセットアップ                           | 13 |
| 3.6.1. Ansibleインベントリファイルの作成                        | 14 |
| 3.6.2. Ansibleノードとの通信の確立                           | 15 |
| 3.7. コードとしてのコンプライアンス                               | 16 |
| 3.7.1. Ansible Playbookを使用した修復                     | 17 |
| 4. 認証方法 .....                                      | 18 |
| 4.1. シングルサインオン(SSO)による認証                           | 18 |
| 4.1.1. 前提条件  | 18 |
| 4.1.2. SSOの有効化                                     | 19 |
| 4.1.3. SSOの実装例                                     | 20 |
| 4.2. PAMによる認証                                      | 24 |
| 4.2.1. SSSDの設定                                     | 24 |
| 5. バックアップと復元 .....                                 | 26 |
| 5.1. smdbaを使用した古い方法を無効にする                          | 26 |
| 5.2. Uyuniのバックアップ                                  | 27 |
| 5.2.1. Uyuniのフルバックアップ                              | 27 |
| 5.2.2. Uyuniの部分バックアップ                              | 28 |
| 5.2.3. 追加ボリュームのバックアップ                              | 29 |
| 5.2.4. データベースの手動バックアップの実行                          | 29 |
| 5.3. 既存のバックアップからUyuniを復元する                         | 29 |
| 5.3.1. バックアップ復元後の推奨されるステップ                         | 30 |
| 6. チャンネル管理 .....                                   | 32 |
| 6.1. チャンネル管理                                       | 32 |
| 6.2. チャンネルの削除                                      | 32 |
| 6.3. カスタムチャンネル                                     | 33 |
| 6.3.1. Creating custom channels and repositories   | 33 |
| 6.3.2. カスタムチャンネル同期                                 | 37 |
| 6.3.3. Add packages and patches to custom channels | 38 |
| 6.3.4. Manage custom channels                      | 40 |
| 6.4. サードパーティチャンネル                                  | 40 |
| 7. コンフィデンシャルコンピューティング .....                        | 42 |
| 7.1. UyuniでのConfidential Computing                 | 42 |
| 7.2. 要件  | 42 |
| 7.3. 制限事項  | 42 |
| 7.4. UyuniでのConfidential Computingの使用              | 42 |
| 7.4.1. レポートのステータス                                  | 44 |
| 7.5. 関連トピック  | 44 |
| 8. コンテンツライフサイクル管理 .....                            | 45 |
| 8.1. コンテンツライフサイクルプロジェクトの作成                         | 45 |
| 8.2. フィルタタイプ                                       | 46 |
| 8.2.1. フィルタの rule パラメータ                            | 47 |

|                                     |           |
|-------------------------------------|-----------|
| 8.3. フィルタテンプレート                     | 48        |
| 8.3.1. SUSE製品に基づくライブパッチ処理           | 48        |
| 8.3.2. システムに基づくライブパッチ処理             | 49        |
| 8.3.3. デフォルトのAppStreamモジュール         | 50        |
| 8.4. コンテンツライフサイクルプロジェクトの構築          | 52        |
| 8.5. 環境のプロモート                       | 52        |
| 8.6. 環境にクライアントを割り当てる                | 53        |
| 8.7. コンテンツライフサイクル管理の例               | 53        |
| 8.7.1. 月次パッチサイクルのプロジェクトの作成          | 53        |
| 8.7.2. 既存の月次パッチサイクルの更新              | 56        |
| 8.7.3. ライブパッチ処理でプロジェクトを強化           | 57        |
| 8.7.4. ライブパッチ処理用の新しいカーネルバージョンに切り替える | 58        |
| 8.7.5. AppStreamフィルタ                | 59        |
| <b>9. コンテンツのステージング</b>              | <b>63</b> |
| 9.1. コンテンツステージングの有効化                | 63        |
| 9.2. コンテンツステージングの設定                 | 63        |
| <b>10. 切断されたセットアップ</b>              | <b>65</b> |
| 10.1. SCCからチャンネルとリポジトリを同期する         | 65        |
| 10.1.1. RMTの同期                      | 65        |
| 10.1.2. SMTの同期                      | 66        |
| 10.2. 必須チャンネル                       | 67        |
| 10.3. 切断されたサーバ                      | 67        |
| 10.3.1. 配備                          | 68        |
| 10.3.2. 同期                          | 68        |
| <b>11. ディスク容量管理</b>                 | <b>69</b> |
| 11.1. 監視対象ディレクトリ                    | 69        |
| 11.2. しきい値                          | 69        |
| 11.3. サービスのシャットダウン                  | 70        |
| 11.4. スペースチェックの無効化                  | 70        |
| <b>12. イメージの構築と管理</b>               | <b>71</b> |
| 12.1. イメージの構築の概要                    | 71        |
| 12.2. コンテナイメージ                      | 71        |
| 12.2.1. 要件                          | 71        |
| 12.2.2. 構築ホストの作成                    | 71        |
| 12.2.3. コンテナ用アクティベーションキーの作成         | 72        |
| 12.2.4. イメージストアの作成                  | 73        |
| 12.2.5. イメージプロファイルの作成               | 73        |
| 12.2.6. イメージの構築                     | 76        |
| 12.2.7. イメージの取り込み                   | 77        |
| 12.2.8. トラブルシューティング                 | 78        |
| 12.3. OSイメージ                        | 78        |
| 12.3.1. 要件                          | 79        |
| 12.3.2. 構築ホストの作成                    | 79        |
| 12.3.3. OSイメージ用アクティベーションキーの作成       | 81        |
| 12.3.4. イメージストアの作成                  | 81        |
| 12.3.5. イメージプロファイルの作成               | 82        |
| 12.3.6. イメージの構築                     | 84        |
| 12.3.7. トラブルシューティング                 | 85        |
| 12.3.8. 制限事項                        | 86        |
| 12.4. ビルドイメージのリスト                   | 86        |
| <b>13. インフラストラクチャ保守タスク</b>          | <b>87</b> |
| 13.1. サーバ                           | 87        |
| 13.1.1. クライアントツール                   | 87        |
| 13.2. サーバ間同期スレーブサーバ                 | 87        |
| 13.3. モニタリングサーバ                     | 88        |
| 13.4. プロキシ                          | 88        |
| <b>14. Uyuniによるライブパッチ処理</b>         | <b>89</b> |

|   |            |
|---|------------|
| 14.1. ライブパッチ処理用のチャンネルの設定                                  | 89         |
| 14.1.1. ライブパッチ処理用のspacewalk-manage-channel-lifecycleを使用する | 89         |
| 14.2. SLES 15でのライブパッチ処理                                   | 91         |
| 14.3. SLES 12でのライブパッチ処理                                   | 92         |
| <b>15. メンテナスウィンドウ</b>                                     | <b>94</b>  |
| 15.1. メンテナススケジュールタイプ                                      | 96         |
| 15.2. 制限されたアクションと制限されないアクション                              | 97         |
| <b>16. mgr-syncの使用</b>                                    | <b>98</b>  |
| <b>17. PrometheusとGrafanaを使用したモニタリング</b>                  | <b>100</b> |
| 17.1. 要件  | 100        |
| 17.2. PrometheusとGrafana                                  | 100        |
| 17.2.1. Prometheus  | 100        |
| 17.2.2. Prometheus Exporters                              | 101        |
| 17.2.3. Grafana   | 101        |
| 17.3. モニタリングサーバの設定  | 101        |
| 17.3.1. Prometheusのインストール                                 | 101        |
| 17.3.2. Grafanaのインストール                                    | 103        |
| 17.4. Uyuniのモニタリングの設定                                     | 106        |
| 17.4.1. サーバ自己監視   | 106        |
| 17.4.2. 管理対象システムの監視                                       | 109        |
| 17.4.3. Grafanaパスワードの変更                                   | 110        |
| 17.5. ネットワーク境界  | 110        |
| 17.5.1. リバースプロキシのセットアップ                                   | 111        |
| 17.6. セキュリティ  | 112        |
| 17.6.1. TLS証明書の生成   | 112        |
| <b>18. 組織</b>   | <b>114</b> |
| 18.1. 組織の管理   | 114        |
| 18.1.1. 組織ユーザ   | 115        |
| 18.1.2. 組織の作成   | 115        |
| 18.1.3. 組織の設定   | 115        |
| 18.2. 状態の管理   | 115        |
| 18.2.1. 設定チャンネルの管理  | 115        |
| <b>19. パッチ管理</b>  | <b>116</b> |
| 19.1. 撤回されたパッチ  | 116        |
| 19.1.1. チャンネルクローン   | 116        |
| 19.1.2. パッチの共有  | 117        |
| <b>20. UyuniのPTFsの使用</b>                                  | <b>118</b> |
| 20.1. PTFパッケージについて  | 118        |
| 20.2. PTFパッケージのインストール                                     | 118        |
| 20.3. PTFのインストール後   | 119        |
| 20.4. パッチ適用済みバージョンのパッケージの削除                               | 120        |
| 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                     | 120        |
| <b>21. レポートの生成</b>  | <b>121</b> |
| 21.1. <b>spacewalk-report</b> の使用                         | 121        |
| 21.2. <b>spacewalk-report</b> およびレポーティングデータベース            | 121        |
| 21.3. 使用可能なレポートのリスト                                       | 122        |
| <b>22. セキュリティ</b>   | <b>128</b> |
| 22.1. 監査  | 128        |
| 22.1.1. CVE監査   | 128        |
| 22.1.2. OVAL  | 129        |
| 22.1.3. CVEステータス  | 131        |
| 22.2. クライアントをマスター検証指紋に設定する                                | 132        |
| 22.3. ミラーソースパッケージ   | 133        |
| 22.4. OpenSCAPによるシステムセキュリティ                               | 133        |
| 22.4.1. SCAPについて  | 134        |

|   |            |
|---|------------|
| 22.4.2. SCAPスキャンのためのクライアントの準備                           | 134        |
| 22.4.3. OpenSCAPコンテンツファイル                               | 135        |
| 22.4.4. OpenSCAPプロファイルの検索                               | 136        |
| 22.4.5. 監査スキャンの実行                                       | 137        |
| 22.4.6. スキャン結果  | 138        |
| 22.4.7. 修復  | 139        |
| 22.5. リポジトリメタデータ  | 143        |
| <b>23. ロールベースのアクセス制御(RBAC)</b>                          | <b>146</b> |
| 23.1. RBACの主要概念   | 146        |
| 23.2. Uyuniでのユーザロール                                     | 146        |
| 23.2.1. 事前定義済みロール                                       | 146        |
| 23.2.2. 追加のロールの定義                                       | 146        |
| 23.3. きめ細かなアクセスのためのネームスペース                              | 147        |
| 23.4. RBACの管理   | 147        |
| 23.4.1. APIを介したRBACの管理                                  | 148        |
| 23.5. RBACベストプラクティス                                     | 148        |
| <b>24. SSL証明書</b>                                       | <b>149</b> |
| 24.1. UyuniコンテナへのSSL証明書の提供                              | 150        |
| 24.1.1. Podman  | 150        |
| 24.2. 自己署名SSL証明書  | 150        |
| 24.2.1. 既存のサーバ証明書の再作成                                   | 151        |
| 24.2.2. 新しいCAおよびサーバ証明書の作成                               | 151        |
| 24.3. SSL証明書のインポート                                      | 152        |
| 24.3.1. 新しいインストール用証明書のインポート                             | 152        |
| 24.3.2. Import certificates for new proxy installations | 153        |
| 24.3.3. Replace certificates                            | 153        |
| 24.3.4. HTTP Strict Transport Security                  | 155        |
| <b>25. サブスクリプションマッチング</b>                               | <b>157</b> |
| 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                           | 158        |
| <b>26. タスクスケジュール</b>                                    | <b>159</b> |
| 26.1. 事前定義済みのタスクバンチ                                     | 160        |
| <b>27. 変更ログの調整</b>                                      | <b>164</b> |
| <b>28. ユーザー</b>   | <b>165</b> |
| 28.1. パスワード要件   | 165        |
| 28.2. アカウントの無効化と削除                                      | 166        |
| 28.3. ユーザロール  | 166        |
| 28.4. 追加ロールの作成  | 167        |
| 28.5. ユーザ許可とシステム  | 167        |
| 28.6. ユーザとチャンネルの許可                                      | 168        |
| 28.7. ユーザのデフォルト言語                                       | 168        |
| 28.7.1. ユーザデフォルトのインターフェーステーマ                            | 169        |
| <b>29. サポート</b>   | <b>171</b> |
| 29.1. サービスリクエスト番号の作成                                    | 171        |
| 29.2. UyuniからSUSEにサポートデータを収集してアップロードする                  | 171        |
| <b>30. トラブルシューティング</b>                                  | <b>173</b> |
| 30.1. 自動インストールのトラブルシューティング                              | 173        |
| 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                | 173        |
| 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                 | 174        |
| 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               | 174        |
| 30.5. 破損したリポジトリのトラブルシューティング                             | 175        |
| 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                   | 175        |
| 30.7. FQDNS grainの無効化のトラブルシューティング                       | 176        |
| 30.8. ディスク容量のトラブルシューティング                                | 177        |
| 30.9. ファイアウォールのトラブルシューティング                              | 177        |
| 30.10.  | 177        |

---

|   |     |
|---|-----|
| WAN接続を介したUyuni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   | 178 |
| 30.11. 無効なクライアントのトラブルシューティング                    | 180 |
| 30.12. サーバ間同期のトラブルシューティング                       | 181 |
| 30.13. ローカル発行者証明書のトラブルシューティング                   | 182 |
| 30.14. ログインタイムアウトのトラブルシューティング                   | 182 |
| 30.15. メール設定のトラブルシューティング                        | 183 |
| 30.16. 大量のMachine_idの重複                         | 183 |
| 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         | 184 |
| 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     | 184 |
| 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               | 184 |
| 30.20. 通知のトラブルシューティング                           | 185 |
| 30.21. パッケージの不整合のトラブルシューティング                    | 185 |
| 30.22. 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            | 185 |
| 30.23. プロキシの接続およびFQDNのトラブルシューティング               | 186 |
| 30.24. 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                | 186 |
| 30.25. SL Microへのリモートルートログイン                    | 189 |
| 30.26. 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               | 190 |
| 30.27. 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 | 190 |
| 30.28. 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      | 190 |
| 30.29. Uyuniサーバの名前変更のトラブルシューティング                | 191 |
| 30.29.1. Rename server                          | 191 |
| 30.29.2. プロキシの再設定                               | 193 |
| 30.30. RPC接続タイムアウトのトラブルシューティング                  | 193 |
| 30.31. 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    | 194 |
| 30.32. 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          | 195 |
| 30.33. 同期のトラブルシューティング                           | 196 |
| 30.34. Taskomaticのトラブルシューティング                   | 197 |
| 30.35. 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           | 198 |
| 31. GNU Free Documentation License .....        | 199 |



## 章 2. 動作

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。
- また、1つ以上のクライアントに対してリモートコマンドを実行することもできます。
  - リモートコマンドを使用すると、個々のクライアント、または検索語に一致するすべてのクライアントにコマンドを発行できます。

### 2.1. 定期的なアクション

個々のクライアント、システムグループ、また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適用することができます。

現在、Uyuni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、Uyuni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、Uyuni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。
- **独自のクオーツ書式:** 詳細オプションについては、独自のクオ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。

Uyuni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**および**Client-configuration** > **Clients-opensuseleapmicro**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. Uyuni 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

このプロシージャを使用して、Saltを介してリモートコマンドを実行します。

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](#)および[Client-configuration > Clients-opensuseleapmicro](#)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

- Salt > リモートコマンドに移動します。
- 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。
- 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。
- [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。
- [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。

# 章 3. Ansibleの統合

Ansibleは、コンピュータクライアントシステムを管理するためのツールです。  
詳しくは、<https://www.ansible.com>を参照してください。

Uyuniは、Ansible制御ノードの管理をサポートしています。 詳細については、[administration:ansible-setup-control-node.pdf](#)を参照してください。

Ansible制御ノードのサポートされているバージョンはAnsible 11.3です。 これ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。SUSE Linux Enterprise以外のオペレーティングシステムを実行している制御ノードでは、そのディストリビューションに同梱されているAnsibleを使用してください。

Ansibleソフトウェアは、UyuniプロキシおよびUyuni for Retailプランチサーバでも使用できます。

## 3.1. 機能の概要

Uyuni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](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](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

Ansible機能を使用するには、既存のAnsible制御ノードをUyuniサーバに登録する必要があります。 Web UIの登録されているシステムの**システムの詳細** → **プロパティ**ページで、 [付属エンタイトルメント] リストの**Ansible制御ノード**システムタイプを有効にする必要があります。

**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、Uyuni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. Uyuni 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、Uyuni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、Uyuni Web UIから次のステップを実行します。

- i** 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。

## Procedure: Setting up Ansible Control Node on a SUSE Linux Enterprise 15 SP6 or SP7 system

1. Uyuni 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. Uyuni 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。表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. Uyuni 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

#### Procedure: Establishing communication with Ansible Nodes

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_public_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。

### プロジェクト: 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 |

| パッケージ名                     | サポートされているシステム  |
|----------------------------|--|
| 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。

# 章 4. 認証方法

Uyuni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

Uyuni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、Uyuni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。 Uyuni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。

Uyuni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。

Uyuni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ユーザーとUyuniユーザーのマッピングはSAML:Attributeで指定します。SAML:AttributeはIdPで指定し、SAML認証時にUyuni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Uyuniユーザー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、Uyuni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。 Uyuni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。 Uyuni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Uyuniメタデータを取得するエンドポイント。 Uyuni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Uyuniに存在する場合は、`orgadmin`ユーザとしてUyuni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

- ユーザがまだUyuniに存在しない場合は、まず作成してください。
- `/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
```

- `/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。

- spacewalkサービスを再起動して変更を取得します。

```
mgradm restart
```

Uyuni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、Uyuni 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、Uyuni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Uyuni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、Uyuni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

- 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。
- 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
```

- 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、Uyuni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、Uyuniサーバを準備できます。

## プロセッジヤ: Uyuniサーバの設定

- Uyuni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Uyuni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
```

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

- 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/realm/<REALM>/protocol/saml/descriptor](http://<FQDN_IDP>:8080/realm/<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Uyuni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+tPbVjANBgkqhkiG9w0BAQsFADAMQ0wCwYDVQQDARTVU1BMB4XDTIyMDkwMTIwNTEwNFoXDT
MyMDkwMTIwNTI0NFowDzENMAsg
A1UEAwwEU1VNQTCASIwDQYJKoZIhvNAQEBBQADggEPADCCAQoCggEBAMNSWJAa1B5mShTkMB05mrs0osyheEL8/A
37WvuqDPwwEf m4x0cG7gmMHvONxYZk+LRyoQ12sBrNFrbMuwu5dnah5ZSMxQyUu697S280m4vIiegGaFdbgH+g4F
GBu
eSis1ssMzTcES+NUuI7pLkMLNmSQtn cESnoL9q2Sy eQSwYtr5dz1ydl6IzjwtaWeyQ9EGJNtJtlk3U4+arLPCpHAwq
FA nL09NeYcRDNUK hNBs1v5mHP+L066PZu1/DkE0mSgy/+qXaS0CgZVKqz8qB+bvHVuAq9W60g1CjqZKbwvPu72p/7+
d8z
9DxXPIZ1uxdq n19q/kLEP2TYLtgQobSHECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAg a+r aLMJD o/P/yN1Z6SGGocK
227WFqovBiE/mLYlp5Ff0+0jS1US1p1SppJ94x0r8j0m7HW0Wu5xCz6o0hzXTEt nfIBeRyr1Rms3BWdxyXgQ9bWUeZ
MWZ
HfDkTbhgRRmjDEwSSfEXRKQNvw41Cpn lB36I0++ejgGnjDvH7BbkCaoW55JF5j6DT/WYR0n7MkE120va9CH0e9X7Gn
y8i0Ag26oziy06uy3P/lx9Z9RmHnvpvN/Q34SG6Eq9z/HlQVuP12UPj//i T21Jc1700ZFsZQX1GFTG6bXKm042W8FdU
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

```

Uyuni 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](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](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](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Uyuniの間でユーザをマッピングできます。

## プロジェクト: 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Uyuni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、Uyuni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、Uyuni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、Uyuni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。 Uyuniサーバを再起動して変更を取得し、Uyuni 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

Uyuni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、Uyuni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。 Uyuni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. Uyuni 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。 Uyuni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. Uyuniを再起動します。

```
mgradm restart
```



Uyuni Web UIのパスワードを変更すると、Uyuni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

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}
```

# 章 5. バックアップと復元

この章では、バックアップが必要なファイルに関する情報について説明します。組み込みのバックアップと復元ソリューション(**mgradm backup**)を使用して、Uyuniのバックアップを作成します。この章の最後に、システム障害が発生した場合のバックアップからの復元に関する情報について説明します。

Uyuni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。Uyuni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. smdbaを使用した古い方法を無効にする

Uyuni 2026.01を最初からインストールした場合は、このセクションをスキップしてください。



組み込みソリューションの登場により、**smdba**バックアップツールを使用した古い方法は非推奨となりました。**smdba**を使用する古いシステムから新しいソリューションに移行した場合は、古い機能を無効にして、古いバックアップアーカイブを削除する必要があります。

移行前に**smdba**を無効にするか(推奨)、移行後のUyuni 2026.01システムで無効にしてください。

### プロシージャ: 移行前にインストール済みのsmdbाを使用した古い方法を無効にする

このプロシージャは、smdbाがまだインストールされている場合にのみ機能します。

1. コンテナホストのコマンドラインで、rootとして次のコマンドを実行します。

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

これにより、`/var/lib/pgsql/data/postgresql.conf`の`archive_command`が次のように変更されます。

```
archive_command = '/bin/true'
```

これで、古いシステムをUyuni 2026.01に移行する準備が整いました。

## プロシージャ: 移行後にUyuni 2026.01における古い方法を無効にする

smdbaが利用できなくなっている場合は、移行後にこのプロシージャを使用します。

- コンテナホストで、rootとして/var/lib/containers/storage/volumes/var-pgsql/\_data/postgresql.confを編集し、以下のオプションを設定します。

```
archive_mode = off
archive_command = '/bin/true'
```

- コンテナを再起動します。

```
mgradm restart
```

## 5.2. Uyuniのバックアップ

Uyuni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. Uyuniのフルバックアップ

Uyuni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。

- Uyuni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
- Uyuni systemdサービス
- Uyuni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、Uyuni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。

## プロシージャ: `mgradm backup create`を使用したフルバックアップの作成

- 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. Uyuniの部分バックアップ

`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、Uyuni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。



部分バックアップはデータの一部のみを対象としており、バックアップされていない可能性のある他の部分との潜在的な依存関係を考慮していません。したがって、バックアップ/復元の一貫性を保証できません。

## プロシージャ: データベースバックアップをスキップして部分バックアップを作成する

- 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。

## プロシージャ: ボリュームをスキップして部分バックアップを作成する

- 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。

`$volumes`を、バックアップから除外するボリュームの名前、または除外するボリュームのカンマ区切りのリストで置き換えます。

**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、Uyuni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。

#### プロシージャ: 追加のカスタムボリュームを使用したバックアップの作成

- 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. データベースの手動バックアップの実行

#### プロシージャ: データベースの手動バックアップの実行

- 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。
- Uyuni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. 既存のバックアップからUyuniを復元する

Uyuni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。

**!** Uyuni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。

## プロシージャ: 既存のバックアップからの復元

- コンテナホストで、rootとして、次のコマンドを使用してUyuniサーバーを再配備します。

```
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. バックアップ復元後の推奨されるステップ

#### プロシージャ: Uyuniの復元後の推奨されるステップ

- Uyuni 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、Uyuni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。
- 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
```

- 次回**rhn-search**サービスを開始するときに検索インデックスの再作成をスケジュールします。

このコマンドはデバッグメッセージのみを生成し、エラーメッセージを生成しません。

コンテナホストで、次のコマンドを入力します。

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

# 章 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。

Uyuni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Uyuniにミラーリングし、パッケージ名やその他のデータはUyuni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。

Uyuniには、Uyuniを実行するために必要なすべてのものを提供する、複数のベンダーチャンネルが用意されています。 Uyuni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、ベンダー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。

### プロセッジヤ: チャンネルへのサブスクライバアクセスの制限

1. Uyuni 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ー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

- Uyuni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
```

- チャンネルを削除します。

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

- 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、Uyuni 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

- Uyuni 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。
- [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ーは、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、Uyuni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
```

このコマンドとプロシージャは、一時的なGPGキーの同期専用です。 キーを永続的に保存するには、後述のこのセクションを参照してください。

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] フィールドがオフになっています。 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 Uyuni 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

- Uyuni 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。
- [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。
- [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。
- [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。
- 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。
- [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

- コンテナホストで、キーをキーリングにインポートするコマンドは次のとおりです。

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

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



**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 | <b>deb https://pkg.jenkins.io/debian-stable binary/</b>                                |
| URLマッピング | <b>https://pkg.jenkins.io/debian-stable?uyuni_suite=binary/</b>                        |
|          |  |
| aptソース行  | <b>deb https://deb.debian.org/debian/dists stable main</b>                             |
| URLマッピング | <b>https://deb.debian.org/debian/dists?uyuni_suite=stable&amp;uyuni_component=main</b> |

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. Uyuni 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に、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。

- ・ Uyuni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。
- ・ Uyuni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**

パッチを同期しないでください。

#### **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は同期を停止します。

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。Uyuni 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ます。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. Uyuni 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. Uyuni 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。

- 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

Uyuni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にです。

Web UIを使用してUyuni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

- Uyuni 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。
- [ソフトウェアチャンネルの削除]をクリックします。
- [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。
- [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。

Uyuni 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. サードパーティチャンネル

Uyuniには、オプションのサードパーティリポジトリの内容を、管理可能な製品の一部と同期する機能が含まれています。

一部のサードパーティGPGキーは、Uyuniデータベースにデフォルトで含まれていますが、含まれていないものもあります。 含まれていないサードパーティキーについては、このようなサードパーティリポジトリの同期を選択する際に、関連するキーをインポートする必要があります。

GPGキーをインポートするには、次のコマンド構文を使用し、Uyuniホストサーバでコマンドを実行します。

```
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
```

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

```
mgradm gpg add https://<3rd-party-domain>/path/to/repository/repoadata/repomd.xml.key
```

Uyuni GPGデータベースに現在保持されているキーを一覧表示するには、次のコマンドを実行します。

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



クライアントにパッケージをインストールする際には、クライアント自体でGPGキーを信頼する必要がある場合もあります。このためには、GPGキーがクライアント上でも使用できる必要があります。

詳細については、[Client-configuration › Gpg-keys](#)を参照してください。

# 章 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. Uyuni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。Uyuni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、Uyuni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。
- Uyuni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. Uyuni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。

### プロジェクト: Uyuniのインストール中に認証コンテナを有効にする

- 認証コンテナは、**mgradm install podman**を使用してUyuni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: Uyuni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
```

## プロシージャ: Uyuniのインストール後に認証コンテナを無効にする

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**セキュアポート**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、[こちら](#)を参照してください。

# 章 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きます。

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。

### プロシージャ: コンテンツライフサイクルプロジェクトの作成

1. Uyuni 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受け取るため、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. フィルタタイプ

Uyuni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. フィルタの rule パラメータ

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. フィルタテンプレート

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、Uyuni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. SUSE製品に基づくライブパッチ処理

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

- Uyuni 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。
- 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. Uyuni 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. Uyuni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. [プレフィックス] フィールドに、名前のプレフィックスを入力します。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. コンテンツライフサイクルプロジェクトの構築

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ーチャンネルを使用できます。この場合、Uyuni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。

### プロシージャ: コンテンツライフサイクルプロジェクトの構築

1. Uyuni 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. 環境のプロモート

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。

### プロシージャ: 環境のプロモート

1. Uyuni 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. 環境にクライアントを割り当てる

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、Uyuni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Uyuni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ト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。

#### プロシージャ: By Date (日付別) フィルタの作成

1. Uyuni 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. プロジェクトへのフィルタの追加

##### プロシージャ: プロジェクトへのフィルタの追加

1. Uyuni 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. 新しいプロジェクトビルトへのフィルタの適用

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。

##### プロシージャ: フィルタの使用

1. [ビルト]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、ビルト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、ビルトに時間がかかります。

#### 8.7.1.4. プロジェクトからのパッチの除外

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。

#### プロシージャ: パッチの除外

1. Uyuni 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. プロジェクトにパッチを含める

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。

#### プロシージャ: プロジェクトにパッチを含める

1. Uyuni 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. 既存の月次パッチサイクルの更新

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。

#### プロシージャ: 月次パッチサイクルの更新

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. ライブパッチ処理でプロジェクトを強化

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。

ライブパッチ処理を使用する準備をしている場合には、いくつかの重要な考慮事項があります。

- 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. より新しいカーネルバージョンのパッケージを除外する

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。

#### プロシージャ: より新しいカーネルバージョンのパッケージを除外する

1. Uyuni 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。

[ビルト]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. ライブパッチ処理用の新しいカーネルバージョンに切り替える

特定のカーネルバージョン用のライブパッチ処理は、1年間のみ利用できます。1年後、システムのカーネルを更新する必要があります。以下の環境変更を実行します。

##### プロシージャ: 新しいカーネルバージョンに切り替える

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. 古いカーネルに関連付けられているすべての以前のライブパッチ処理フィルタを取り外します。
4. 新しいカーネルバージョンフィルタを割り当てます。
5. [ビルト]をクリックして、環境を再構築します。



ビルトが完了したら、以下の処理を実行する2つのフィルタを直ちに再度割り当てる必要があります。

- **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

新しい環境には、選択した新しいカーネル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。アップグレードを実行した後で、システムを再起動する必要があります。新しいカーネルは1年間有効です。その年にインストールされたすべてのパッケージは、現在のライブパッチ処理カーネルフィルタと一致します。

## 8.7.5. AppStreamフィルタ

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Uyuniで使用できます。

AppStreamリポジトリはWeb UI全体でネイティブにサポートされています。



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。

### プロシージャ: AppStreamフィルタの使用

1. Uyuni 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。

### プロシージャ: 使用可能なモジュールストリームのブラウズ

1. Uyuni 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。

### プロシージャ: モジュール化の無効化

1. Uyuni 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。

# 章 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텐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。Uyuni 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、Uyuni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텐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。

# 章 10. 切断されたセットアップ

Uyuni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Uyuni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Uyuni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、Uyuni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。



Uyuni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。

Uyuni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

- 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
```

- 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。

- 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
```

- 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
```

- 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。

### プロジェクト: SMTとSCCの同期

- 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
```

- 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

Uyuni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Uyuni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、Uyuni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

Uyuni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。Uyuni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。

### プロジェクト: 切断されたサーバの同期

- Tomcatサービスを再起動します。

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

- ローカルデータを更新します。

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

- 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、UyuniはSUSE Customer Center資格情報が有効かどうかを確認できる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。

# 章 11. ディスク容量管理

ディスク容量が不足すると、Uyuni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。

Uyuni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、Uyuni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
```

ボリュームの詳細については、**Installation-and-upgrade** → **Container-management**を参照してください。

## 11.2. しきい値

デフォルトでは、Uyuni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、Uyuni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。

# 章 12. イメージの構築と管理

## 12.1. イメージの構築の概要

Uyuni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。

### プロセージャ: 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。

Uyuni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。

Kiwiビルドタイプ用のイメージストアは、`srv-www`ボリューム内のファイルシステムディレクトリとして事前定義されています。

イメージファイルは<https://UYUNI-HOST/os-images/ORGANIZATION-ID/FILE-NAME>からダウンロードできます。正確な場所は、イメージ詳細ページで確認できます。

## 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

Uyuni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。

Uyuni 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、Uyuni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

Uyuni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。

## プロセッジヤ: 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

すべての構築されたイメージは、イメージストアにプッシュされます。このセクションでは、イメージストアの作成について説明します。イメージストアは一般的にレジストリと呼ばれます。

## プロセッジヤ: 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、Uyuni 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。
- i** 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Uyuni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**、**ビルト** を選択するか、**イメージ**、**プロファイルリスト** の **ビルト** アイコンをクリックして、プロシージャに従います。

## プロセッジヤ: 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

イメージを取得する2つ目の方法は、任意のイメージを取り込み、検査することです。左側のナビゲーションバーからイメージ、イメージリストを選択します。 [取り込み] ダイアログのテキストボックスに入力します。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] ページに一覧表示されます。

## プロセッジヤ: 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、Uyuni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. 一般的な問題

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イメージ

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できます。

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

Uyuni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。

このプロセッジでは、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トはできません。 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。

#### プロセッジ: Uyuni 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ネルを有効にします。
  - SUSE Linux Enterprise Server 12構築ホストでは、Uyuni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、Uyuni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. Uyuni Webサーバのパブリック証明書RPM

構築ホストのプロビジョニングでは、Uyuni証明書RPMを構築ホストにコピーします。この証明書はUyuni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Uyuni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セッサーの完了後に、**--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 Uyuni 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. OSイメージ用アクティベーションキーの作成

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。



OSイメージを構築するには、**デフォルト**アクティベーションキー以外のチャンネルに関連付けられた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. 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イメージは大量のストレージ容量を必要とする場合があります。 デフォルトでは、イメージストアは**srv-www**ボリュームを使用しています。

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。



イメージファイルは<https://UYUNI-HOST/os-images/ORGANIZATION-ID/FILE-NAME>からダウンロードできます。正確な場所は、イメージ詳細ページで確認できます。

### 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。

#### プロジェクト: 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。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="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

Web UIを使用してイメージを構築または取得する2つの方法があります。 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Uyuni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
- Uyuni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。

# 章 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、Uyuni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UyuniプロキシなどのUyuni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Uyuni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。 Uyuni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、Uyuni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。

### 13.1.1. クライアントツール

サーバを更新する際には、クライアント上の一ツのツールも更新することを検討してください。 クライアント上で `venv-salt-minion`、`zypper`、およびその他の関連する管理パッケージを更新することは厳密な要件ではありませんが、一般的にはベストプラクティスです。 たとえば、サーバの保守更新では、メジャーな新しいSaltバージョンが導入される場合があります。 その後、Saltクライアントは引き続き動作しますが、後で問題が発生する可能性があります。 これを回避するため、SUSEは、`venv-salt-minion`が常に安全に更新されるようにします。

## 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、Uyuni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、Uyuni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、Uyuni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。

# 章 14. Uyuni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、ダウントIME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
```

- spacewalk-manage-channelコマンドにinit引数を指定して、元のベンダー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
```

- 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

- 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。
- Uyuni 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。
- 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。
- 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

- 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
```
- Uyuni 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。
  - 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。
  - [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。

- Uyuni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Uyuni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

- 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。

| Package Name                                                 | Architecture |
|--------------------------------------------------------------|--------------|
| <code>kernel-livepatch-4_12_14-195-default-4-10.1</code>     | x86_64       |
| <code>kernel-livepatch-4_12_14-197_10-default-1-3.3.1</code> | x86_64       |
| <code>kernel-livepatch-4_12_14-197_4-default-3-2.1</code>    | x86_64       |
| <code>kernel-livepatch-4_12_14-197_7-default-2-2.1</code>    | x86_64       |
| <code>kernel-livepatch-tools-1.1-9.5</code>                  | x86_64       |
| <code>kernel-livepatch-tools-devel-1.1-9.5</code>            | x86_64       |

- 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。
- 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。
- 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. Uyuni 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

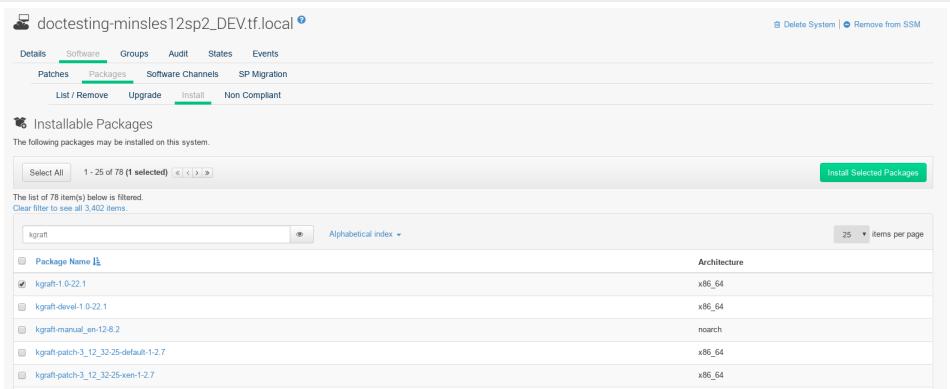
SLES 12システムでは、ライブパッチ処理はkGraftで管理されます。kGraftの使用に関する詳細については、<https://documentation.suse.com/sles/12-SP5/html/SLES-all/cha-kgraft.html>を参照してください。

開始する前に、以下を確認します。

- Uyuni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Uyuni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. Uyuni 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。



# 章 15. メンテナスウィンドウ

Uyuniのメンテナ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、Uyuni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アプリケーション

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: 新しいメンテナスカレンダーのアップロード

1. Uyuni Web UIで、スケジュール、メンテナスウィンドウ、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. Uyuni 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. Uyuni 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、メンテナススケジュールを割り当てます。



新しいメンテナススケジュールをクライアントに割り当てるとき、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。

メンテナスウィンドウを作成したら、メンテナ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. Uyuni 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

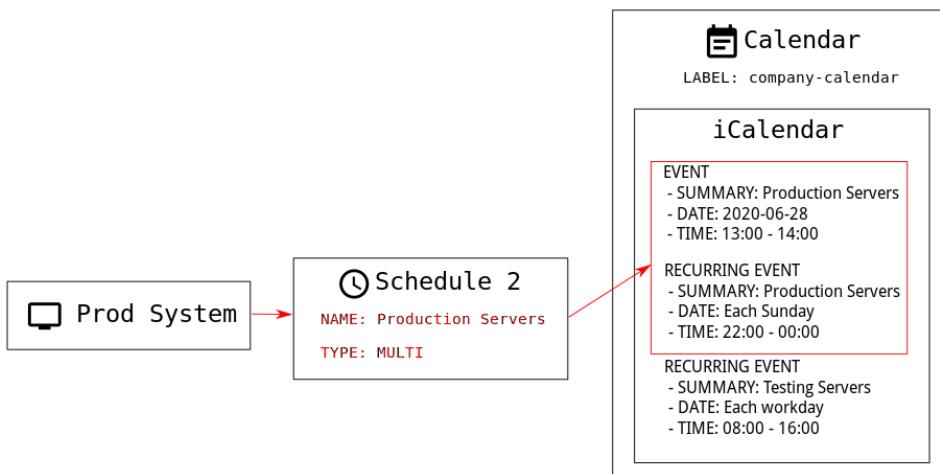
ンスウィンドウを選択します。

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. Uyuni 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
- highstateの適用
- 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



**Salt** › リモートコマンドに移動することで、いつでもリモートコマンドを直接実行できます。これは、クライアントがメンテナスウィンドウ中であるかどうかに関係なく適用されます。リモートコマンドの詳細については、Administration › Actionsを参照してください。

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。

# 章 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Uyuni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、Uyuni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         | <b>mgr-sync list channels</b>                     |
| add     | チャンネル、組織の資格情報、または製品を追加する           | <b>mgr-sync add channel &lt;channel_name&gt;</b>  |
| 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 | <b>mgr-sync refresh</b>                           |
| 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       | <b>mgr-sync delete credentials</b>                |
| 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      | <b>mgr-sync sync channel &lt;channel_name&gt;</b> |

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                      | <b>mgr-sync --help</b>    |
| version | N/A     | 現在インストールされているバージョンの <b>mgr-sync</b> を表示する | <b>mgr-sync --version</b> |

| 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                                            | <b>mgr-sync --verbose refresh</b>                  |
| store-credentials | s       | 資格情報をローカルの隠しファイルに保存する                                 | <b>mgr-sync --store-credentials</b>                |
| 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。 | <b>mgr-sync -d 3 refresh</b>                       |
| no-sync           | N/A     | <b>add</b> 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       | <b>mgr-sync --no-sync add &lt;channel_name&gt;</b> |

**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

# 章 17. PrometheusとGrafanaを使用したモニタリング

PrometheusとGrafanaを使用して、Uyuni環境を監視できます。Uyuni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Uyuni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。

Uyuni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。

## 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。

| メトリック名                                          | ラベル | タイムスタンプ         | 値     |
|-------------------------------------------------|-----|-----------------|-------|
| http_requests_total{status="200", method="GET"} |     | @1557331801.111 | 42236 |

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. モニタリングサーバの設定

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、Uyuni 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、UyuniプロキシおよびUyuni for Retailプランチサーバでも使用できます。



- Uyuni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`を実行するか、1つのコマンドを実行するには `mgrctl exec <options> --<command>`を実行します。
- コンテナ内からコンテナホストにファイルをコピーするには、`mgrctl cp`を使用します。



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。

### プロシージャ: Web UIを使用したPrometheusのインストール

- Uyuni 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. [Uyuni サーバ] セクションに、有効なUyuni 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インター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。

## プロシージャ: Prometheusを手動でインストールおよび設定する

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. Prometheusインター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>)。
4. `/etc/prometheus/prometheus.yml`にある設定ファイルを開き、この設定情報を追加します。`server.url`をUyuniサーバのURIで置き換え、Uyuni資格情報に一致するように [ユーザ名] および [パスワード] フィールドを調整します。
 

```
# {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Uyuniで管理されているクライアントの場合は、Uyuni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Uyuniプロキシでは使用できません。

## プロシージャ: Web UIを使用したGrafanaのインストール

1. Uyuni 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インター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>)。
  - Grafanaに正常にアクセスするには、ファイアウォールでポート3000が開いていることを確認します



Uyuni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。

## プロシージャ: Grafanaの手動インストール

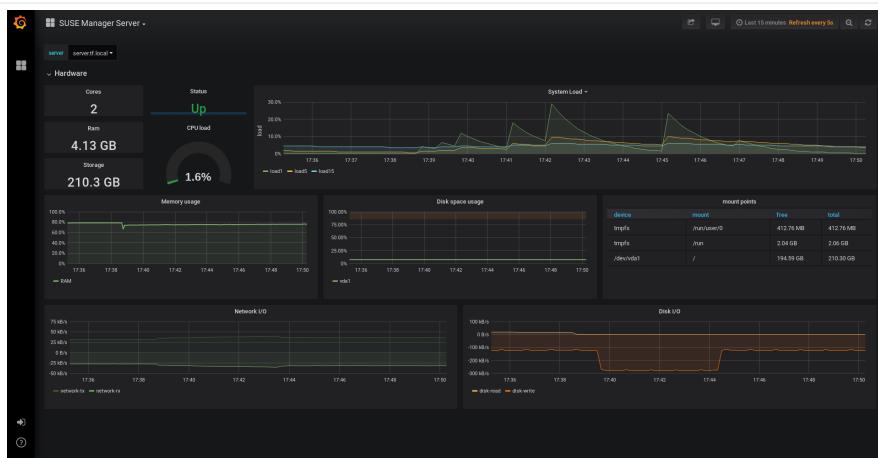
1. grafanaパッケージをインストールします。

```
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>)。
  - Grafanaに正常にアクセスするには、ファイアウォールでポート3000が開いていることを確認します。
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. [ログイン]をクリックします。 ログインに成功すると、パスワードを変更するプロンプトが表示されます。
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. Uyuni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. Uyuni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. Uyuniのモニタリングの設定

Uyuni 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. サーバ自己監視

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Uyuni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Uyuni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](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](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](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Uyuni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](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Uyuni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サービスはデフォルトで無効になっています。

## プロシージャ: 自己監視の有効化

1. Uyuni 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Uyuni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Uyuni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 |

| メトリック                         | タイプ  | 説明               |
|-------------------------------|------|------------------|
| 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_count | 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. 管理対象システムの監視

Prometheus metrics exportersは、式を使用してSaltクライアントにインストールおよび設定できます。 パッケージはUyuniクライアントツールチャンネルから入手でき、Uyuni Web UIで直接有効化および設定できます。

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](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](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](https://github.com/Lusitaniae/apache_exporter)を参照してください。



SL Microでは、Node exporterとBlackbox exporterのみが利用できます。

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。

## プロシージャ: クライアントでのPrometheus Exportersの設定

1. Uyuni 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。

以下のポートが有効になっており、ファイアウォールでブロックされないようにする必要があります。



- 監視側: 9090/tcp
- 監視対象システム側: 9100/tcp、9117/tcp、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. Grafanaパスワードの変更

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. ネットワーク境界

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ができます。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. リバースプロキシのセットアップ

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。

### プロシージャ: リバースプロキシを使用したPrometheus Exportersのインストール

- Uyuni 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。
- [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。
- 上部メニューの [Prometheus Exporters] タブに移動します。
- [Enable reverse proxy] (リバースプロキシを有効にする) オプションをオンにして、有効なリバースプロキシポート番号を入力します。例: 9999。
  - ファイアウォールでポート9999/tcpが開いていることを確認します。

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。 Uyuni 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。 Uyuni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、Uyuni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、Uyuni 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. Uyuni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実行します。
  - a. 証明書ファイルを生成するには、次のコマンドを実行します。

**set-cname**パラメータが、Saltクライアントの完全修飾ドメイン名(FQDN)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、**set-cname**パラメータを複数回使用できます。

```
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
```

結果:

```
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. `server.crt`および`server.key`ファイルをサーバコンテナからホストにコピーします。

```
mgrctl cp server:/root/ssl-build/minion/server.key server.key
mgrctl cp server:/root/ssl-build/minion/server.crt server.crt
```

- c. `server.crt`および`server.key`ファイルをホストからモニタリングクライアントにコピーします。

```
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. Saltフォーミュラを設定するには、前のステップで指定されたディレクトリ名を入力します。

フォーミュラサーバ証明書`/etc/ssl/mlm-server-certs/server.crt` サーバキー`/etc/ssl/mlm-server-certs/server.key`

- a. フォーミュラminion

# 章 18. 組織

組織は、Uyuni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することができます。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、Uyuni管理者としてログインする必要があります。

## プロセージャ: 新しい組織の作成

1. Uyuni 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

Uyuni 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. 組織の作成

[**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、Uyuni Web UIで**設定** > **チャンネル**に移動して作成できます。Uyuni 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. Uyuni 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。

# 章 19. パッチ管理

この章では、パッチ管理に関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つ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、Uyuni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、Uyuni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。Uyuni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、Uyuni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Uyuni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。

# 章 20. Uyuni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、Uyuni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。



Uyuniを介してPTFチャンネルにアクセスするには、L3サポートから要求する必要があります。

### 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

- コンソールで、**mgr-sync refresh**と入力します。
- 「**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**。
- 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。Uyuni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: UyuniのWeb UIを使用したPTFリポジトリの有効化および同期

1. Uyuni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. Uyuni 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. Uyuni 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。

# 章 21. レポートの生成

Uyuni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、Uyuni 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、Uyuni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

Uyuni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。
- すべての布尔値は、**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         | <b>actions</b>         | All actions.                                                                                                                   | Yes                     | The column <b>id</b> is now called <b>action_id</b> |
| Activation Keys | <b>activation-keys</b> | 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      | <b>activation-keys-channels</b> | All activation keys and the entities associated with each key.                                                    | No                      |                      |
| Activation Keys: Configuration | <b>activation-keys-config</b>   | All activation keys and the configuration channels associated with each key.                                      | No                      |                      |
| Activation Keys: Server Groups | <b>activation-keys-groups</b>   | All activation keys and the system groups associated with each key.                                               | No                      |                      |
| Activation Keys: Packages      | <b>activation-keys-packages</b> | All activation keys and the packages each key can deploy.                                                         | No                      |                      |
| Channel Packages               | <b>channel-packages</b>         | All packages in a channel.                                                                                        | Yes                     |                      |
| Channel Report                 | <b>channels</b>                 | Detailed report of a given channel.                                                                               | Yes                     |                      |
| Cloned Channel Report          | <b>cloned-channels</b>          | Detailed report of cloned channels.                                                                               | Yes                     |                      |
| Configuration Files            | <b>config-files</b>             | All configuration file revisions for all organizations, including file contents and file information.             | No                      |                      |
| Latest Configuration Files     | <b>config-files-latest</b>      | 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           | <b>custom-channels</b>         | Channel metadata for all channels owned by specific organizations.                 | Yes                     | The column <b>id</b> is now called <b>channel_id</b>     |
| Custom Info               | <b>custom-info</b>             | Client custom information.                                                         | Yes                     |                                                          |
| Patches in Channels       | <b>errata-channels</b>         | All patches in channels.                                                           | Yes                     |                                                          |
| Patches Details           | <b>errata-list</b>             | All patches that affect registered clients.                                        | Yes                     |                                                          |
| All patches               | <b>errata-list-all</b>         | All patches.                                                                       | No                      |                                                          |
| Patches for Clients       | <b>errata-systems</b>          | Applicable patches and any registered clients that are affected.                   | Yes                     |                                                          |
| Host Guests               | <b>host-guests</b>             | Host and guests mapping.                                                           | Yes                     |                                                          |
| Inactive Clients          | <b>inactive-systems</b>        | Inactive clients.                                                                  | Yes                     | The mandatory parameter is now called <b>threshold</b> . |
| System Inventory          | <b>inventory</b>               | Clients registered to the server, together with hardware and software information. | Yes                     | The column <b>osad_status</b> has been removed.          |
| Kickstart Scripts         | <b>kickstart-scripts</b>       | All kickstart scripts, with details.                                               | No                      |                                                          |
| Kickstart Trees           | <b>kickstartable-trees</b>     | Kickstartable trees.                                                               | No                      | "                                                        |
| All Upgradable Versions   | <b>packages-updates-all</b>    | All newer package versions that can be upgraded.                                   | Yes                     |                                                          |
| Newest Upgradable Version | <b>packages-updates-newest</b> | Newest package versions that can be upgraded.                                      | Yes                     |                                                          |

| Report                            | Invoked as                   | Description                                                                                             | Uses reporting database | Specific differences |
|-----------------------------------|------------------------------|---------------------------------------------------------------------------------------------------------|-------------------------|----------------------|
| Proxy Overview                    | <b>proxies-overview</b>      | All proxies and the clients registered to each.                                                         | Yes                     |                      |
| Repositories                      | <b>repositories</b>          | All repositories, with their associated SSL details, and any filters.                                   | No                      |                      |
| Result of SCAP                    | <b>scap-scan</b>             | Result of OpenSCAP <b>sccdf</b> evaluations.                                                            | Yes                     |                      |
| Result of SCAP                    | <b>scap-scan-results</b>     | Result of OpenSCAP <b>sccdf</b> evaluations, in a different format.                                     | Yes                     |                      |
| System Data                       | <b>splice-export</b>         | Client data needed for splice integration.                                                              | No                      |                      |
| System Currency                   | <b>system-currency</b>       | Number of available patches for each registered client.                                                 | No                      |                      |
| System Extra Packages             | <b>system-extra-packages</b> | All packages installed on all clients that are not available from channels the client is subscribed to. | Yes                     |                      |
| System Groups                     | <b>system-groups</b>         | System groups.                                                                                          | Yes                     |                      |
| Activation Keys for System Groups | <b>system-groups-keys</b>    | Activation keys for system groups.                                                                      | No                      |                      |
| Systems in System Groups          | <b>system-groups-systems</b> | Clients in system groups.                                                                               | Yes                     |                      |
| System Groups Users               | <b>system-groups-users</b>   | System groups and users that have permissions on them.                                                  | No                      |                      |
| System Hardware                   | <b>system-hardware</b>       | System hardware information.                                                                            | No                      |                      |

| Report                 | Invoked as                          | Description                                                                       | Uses reporting database | Specific differences                                |
|------------------------|-------------------------------------|-----------------------------------------------------------------------------------|-------------------------|-----------------------------------------------------|
| History: System        | <b>system-history</b>               | Event history for each client.                                                    | Yes                     |                                                     |
| History: Channels      | <b>system-history-channels</b>      | Channel event history.                                                            | Yes                     |                                                     |
| History: Configuration | <b>system-history-configuration</b> | Configuration event history.                                                      | Yes                     | The column <b>created_date</b> has been removed.    |
| History: Entitlements  | <b>system-history-entitlements</b>  | System entitlement event history.                                                 | Yes                     |                                                     |
| History: Errata        | <b>system-history-errata</b>        | Errata event history.                                                             | Yes                     | The column <b>created_date</b> has been removed.    |
| History: Kickstart     | <b>system-history-kickstart</b>     | Kickstart event history.                                                          | Yes                     | The column <b>created_date</b> has been removed.    |
| History: Packages      | <b>system-history-packages</b>      | Package event history.                                                            | Yes                     | The column <b>created_date</b> has been removed.    |
| History: SCAP          | <b>system-history-scap</b>          | OpenSCAP event history.                                                           | Yes                     | The column <b>created_date</b> has been removed.    |
| MD5 Certificates       | <b>system-md5-certificates</b>      | All registered clients using certificates with an MD5 checksum.                   | No                      |                                                     |
| Installed Packages     | <b>system-packages-installed</b>    | Packages installed on clients.                                                    | Yes                     |                                                     |
| System Profiles        | <b>system-profiles</b>              | All clients registered to the server, with software and system group information. | No                      |                                                     |
| Users                  | <b>users</b>                        | All users registered to Uyuni.                                                    | Yes                     | The column <b>organization_id</b> has been removed. |

| Report               | Invoked as           | Description                                                                                  | Uses reporting database | Specific differences                                |
|----------------------|----------------------|----------------------------------------------------------------------------------------------|-------------------------|-----------------------------------------------------|
| MD5 Users            | <b>users-md5</b>     | All users for all organizations using MD5 encrypted passwords, with their details and roles. | Yes                     | The column <b>organization_id</b> has been removed. |
| Systems administered | <b>users-systems</b> | Clients that individual users can administer.                                                | Yes                     | The column <b>organization_id</b> 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。

# 章 22. セキュリティ

## 22.1. 監査

Uyuni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。

Uyuni 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。

Uyuni 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. Uyuni 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. Uyuni 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。さらにパ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。

Uyuni 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、『Uyuni 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、Uyuni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、ゼロディ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. コンテナ内のファイル/etc/rhn/rhn.confで次の設定を追加または編集します。

```
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. Uyuni 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. Uyuni 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、Uyuni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                 |                                                                                                               |
| openSUSE Leap Micro           |                                                                                                               |
| SUSE Linux Enterprise Server  | <a href="https://ftp.suse.com/pub/projects/security/oval">https://ftp.suse.com/pub/projects/security/oval</a> |
| SUSE Linux Enterprise Desktop |                                                                                                               |
| SUSE Linux Enterprise Micro   |                                                                                                               |
| RedHat Enterprise Linux       | <a href="https://www.redhat.com/security/data/oval/v2">https://www.redhat.com/security/data/oval/v2</a>       |
| Debian                        | <a href="https://www.debian.org/security/oval">https://www.debian.org/security/oval</a>                       |
| Ubuntu                        | <a href="https://security-metadata.canonical.com/oval">https://security-metadata.canonical.com/oval</a>       |



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、Uyuniで使用できる情報にのみ基づいています。

Uyuni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Uyuni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Uyuni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。



Uyuni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

- 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'
```

- 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
```

- 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、Uyuni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

- /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
```

- 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Uyuni 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

Uyuni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は、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>

Uyuni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. SCAPスキャンのためのクライアントの準備

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Uyuni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。Uyuni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 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



Other profiles, such as the CIS profile, are community supplied and not officially supported by SUSE.

- CIS profile for SUSE Linux Enterprise Server 12 and 15 (unsupported)

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コンテンツファイル

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。

Uyuni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-scapi_datastream_from_xccdf_ssg-sle15-xccdf-1.2.xml
Generated: (null)
Version: 1.2
Checklists:
    Ref-Id: scap_org.open-scapi_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
```

```

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. 監査スキャンの実行

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、Uyuni Web UIを使用してトリガできます。 Uyuni 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。

### プロシージャ: Web UIからの監査スキャンの実行

1. Uyuni 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/oscrap 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

**i** **--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。

## プロシージャ: APIからの監査スキャンの実行

- 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。
- 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 xmlrpclib
client = xmlrpclib.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>は、クライアント上のコンテンツファイルの場所へのパスです。たとえば、`/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。
- 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. スキャン結果

実行したスキャンに関する情報は、Uyuni 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。Uyuni 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
```

Uyuni 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
rvh4-script-pci-dss.sh
rvh4-script-rvh-stig.sh
rvh4-script-rvh-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。

```
PGPPASS="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. Uyuni 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。

# 章 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。Uyuni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 Uyuni.
-  ロールはユーザに割り当てられ、ユーザに集約された許可を付与します。
- **許可:** Uyuni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。Uyuni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:** Uyuni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. Uyuniでのユーザロール

Uyuni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                                 |
|---------------------------------|---------|------------------------------------|
| <code>cm.build</code>           | 変更      | コンテナまたはKiwiイメージを構築します              |
| <code>cm.image.import</code>    | 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       |
| <code>cm.image.list</code>      | 表示      | すべてのイメージを一覧表示します                   |
| <code>cm.image.list</code>      | 変更      | イメージを削除します                         |
| <code>cm.image.overview</code>  | 表示      | イメージの詳細、パッチ、パッケージ、構築ログ、クラスタ情報表示します |
| <code>cm.image.overview</code>  | 変更      | イメージを検査、再構築、削除します                  |
| <code>cm.profile.details</code> | 表示      | イメージプロファイルの詳細を表示します                |
| <code>cm.profile.details</code> | 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     |
| <code>cm.profile.list</code>    | 表示      | すべてのイメージプロファイルを一覧表示します             |
| <code>cm.profile.list</code>    | 変更      | イメージプロファイルを削除します                   |
| <code>cm.store.details</code>   | 表示      | イメージストアの詳細を表示します                   |
| <code>cm.store.details</code>   | 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           |
| <code>cm.store.list</code>      | 表示      | すべてのイメージストアを一覧表示します                |
| <code>cm.store.list</code>      | 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、Uyuni 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

Uyuni 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:** Uyuni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:** Uyuni内に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、Uyuni 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。

# 章 24. SSL証明書

Uyuni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Uyuni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を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、Uyuniで自己署名証明書を使用することです。この場合、Uyuni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Uyuni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、Uyuni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、Uyuni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. Uyuniツールを使用して自己署名証明書を作成する方法
2. Uyuni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. Uyuni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、Uyuniは自己署名証明書を使用します。 この場合、証明書はUyuni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

- Uyuni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Uyuni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と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

- Uyuni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
```

- 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"
```

- 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Uyuni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Uyuni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も利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。

サードパーティの機関は通常、中間CAを使用して、要求されたサーバ証明書に署名します。この場合、チェーン内のすべてのCAが使用できる必要があります。**mgrdadm**コマンドは証明書の順序付けを行います。理想的には、ルートCAを独自のファイルに格納する必要があります。サーバ証明書ファイルには、まずサーバ証明書、次にすべての中間CA証明書が順番に含まれている必要があります。

### 24.3.1. 新しいインストール用証明書のインポート

By default, Uyuni uses a self-signed certificate. Certificates can be imported with third-party certificates at the installation time.

## Procedure: Importing certificates on a new Uyuni server

1. Installation-and-upgrade › Install-server の手順に従って Uyuni 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。

|                              |                    |
|------------------------------|--------------------|
| カードパーティ 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 Uyuni Proxy

1. Installation-and-upgrade › Install-proxy の手順に従って、Uyuni 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 Uyuni 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 Uyuni 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/uyuni/proxy-deployment-uyuni.pdf](#)を参照してください。 proxy-deployment-uyuni.adoc

If the Root CA was changed, it needs to get deployed to all the clients connected to Uyuni. This is ideally done in advance to minimize the disruption.

CA証明書が更新された場合、Kiwi証明書を含むRPMファイルを再パッケージ化する必要があります。

Uyuniサーバのコンテナホストで、次のコマンドを実行します。



```
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. Uyuni 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。

Uyuniでは、HSTSはデフォルトで有効になっています。 サーバ上で無効にする必要がある場合は、次のプロセージャに従います。

### プロセージャ: サーバでHSTSを無効にする

1. サーバコンテナホストで、rootとして次のコマンドを実行し、設定max-age=0を含む新しい設定ファイルを作成します。

```
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
```

プロキシ上で無効にする必要がある場合は、次のプロシージャに従います。

## プロシージャ: プロキシでHSTSを無効にする

1. サーバコンテナホストで、rootとして次のコマンドを実行し、設定max-age=0を含む新しい設定ファイルを作成します。

```
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。

 Uyuni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。Uyuni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。

# 章 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。 Uyuni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、Uyuni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Uyuni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。

# 章 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。

SUSE Manager Schedules 

Below is a list of defined schedules. A schedule defines frequency, how often a predefined bunch shall be triggered.

1 - 23 of 23

25 items per page

| Schedule name                 | Frequency    | Active From              | Bunch                       |
|-------------------------------|--------------|--------------------------|-----------------------------|
| auto-errata-default           | 0 5/10 * * ? | 2018-06-05 11:40:50 CEST | auto-errata-bunch           |
| channel-repo-data-default     | 0 * * * ?    | 2018-06-05 11:40:50 CEST | channel-repo-data-bunch     |
| cleanup-data-default          | 0 0 23 ? * * | 2018-06-05 11:40:50 CEST | cleanup-data-bunch          |
| clear-tasklogs-default        | 0 0 23 ? * * | 2018-06-05 11:40:50 CEST | clear-tasklogs-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          |

**Uyuni Schedules (Uyuni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。



- Uyuni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。 **Uyuni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-repo-data-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-tasklogs-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**

Uyuni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/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、Uyuni、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インター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Uyuni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、Uyuni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Uyuniサーバからすべてのレポーティングデータを収集し、ハブレポート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。

# 章 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Uyuni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
```

# 章 28. ユーザー

Uyuni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、Uyuni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。

Uyuniユーザを管理するには、ユーザ[ユーザー一覧 >すべて]に移動し、Uyuni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

Uyuni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、Uyuni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 Occurrences (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 Occurrences (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。

Uyuni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Uyuni 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Uyuni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Uyuni管理者が必要です。

Uyuni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**、**ユーザー一覧**、**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Uyuni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、**[Uyuni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                                                                   |
|----------------|----------------------------------------------------------------------|
| Uyuni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

Uyuni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](#)、[ユーザー一覧](#)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](#)、[ユーザー一覧](#)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](#)、[ユーザー一覧](#)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。

リスト内的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。

Uyuni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 |
|--------------|--------|--------|
| <b>bn_IN</b> | バングラ語  | インド    |
| <b>ca</b>    | カタロニア語 |        |

| 言語コード | 言語      | ダイアレクト |
|-------|---------|--------|
| de    | ドイツ語    |        |
| en_US | 英語      | 米国     |
| es    | スペイン語   |        |
| fr    | フランス語   |        |
| gu    | グジャラート語 |        |
| hi    | ヒンディー語  |        |
| it    | イタリア語   |        |
| ja    | 日本語     |        |
| ko    | 韓国語     |        |
| pa    | パンジャブ語  |        |
| pt    | ポルトガル語  |        |
| pt_BR | ポルトガル語  | ブラジル   |
| ru    | ロシア語    |        |
| ta    | タミル語    |        |
| zh_CN | 中国語     | 本土、簡体字 |
| zh_TW | 中国語     | 台湾、繁体字 |



Uyuniの翻訳はコミュニティによって提供されており、不正確または不完全である可能性があります。 翻訳が利用できない場合、Web UIはデフォルトで英語(en\_US)になります。

## 28.7.1. ユーザデフォルトのインターフェーステーマ

デフォルトでは、Uyuni 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。

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。

デフォルトのテーマを変更するに

```
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  |

# 章 29. サポート

Uyuniでシステムを管理し、SUSEからサポートを受ける資格がある場合、**supportconfig**や **sosreport**などのサポートデータを取得できます。 管理対象クライアントからデータを取得し、SUSEグローバルテクニカルサポートに直接アップロードします。

## 29.1. サービスリクエスト番号の作成

グローバルテクニカルサポートにサポートデータを渡す前に、まずサービスリクエスト番号を生成する必要があります。

サービスリクエストを作成するには、<https://scc.suse.com/support/requests>に移動して、画面の指示に従います。 サービスリクエスト番号を書き留めます。

### プライバシーステートメント



SUSEはシステムレポートを機密データとして扱います。 SUSEのプライバシーに関する取り組みの詳細については、<https://www.suse.com/company/policies/privacy/>を参照してください。

## 29.2. UyuniからSUSEにサポートデータを収集してアップロードする

### プロジェクト: Uyuni Web UIでのサポートデータの収集とアップロード

1. Uyuni Web UIで、**システム**、**システム一覧**、すべてに移動して、サポートデータをケースに追加する必要があるクライアントを選択します。
2. [詳細] タブに移動し、 [サポート] サブタブを選択します。
3. [サポートケース番号] フィールドに、上記で作成したサービスリクエスト番号を入力します。
4. [アップロードドリージョン] フィールドで、データをアップロードするサーバに応じて、 [EU] または [us] オプションを選択します。
5. [コマンドラインの引数] フィールドには、ターゲットシステムからデータを収集するために使用するツールのオプションを入力できます。 使用するツールは、このフィールドの下にあるヒントで確認できます。
6. 指定時刻以降にスケジュールで、このアクションの実行時刻を選択します。
7. [スケジュール] ボタンをクリックします。 アクションがスケジュールされ、指定された時間に実行されます。 クライアントからデータを収集し、アップロードサーバに直接アップロードします。

サポートデータを収集可能なサポート対象製品:

- Uyuniプロキシ
- ハブシナリオで周辺機器サーバとして登録されているUyuniサーバ
- すべてのSUSE Linux EnterpriseおよびopenSUSEクライアント
- SUSE Libertyおよび互換クライアント
- Ubuntuクライアント
- Debianクライアント



サポートデータをメインのUyuniサーバからアップロードするには、コンテナホストから引き続き **mgradm support config** を使用してください。



# 章 30. トラブルシューティング

このセクションには、Uyuni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。

## 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Uyuni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Uyuni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を確認します。

## 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、Uyuni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. Uyuni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とすると、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。

### プロジェクト: 破損したリポジトリデータの解決

1. `/var/cache/rhn/repoadata/<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、Uyuni 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。
  - Uyuni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。

## 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。

Uyuni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 utilmgr_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、Uyuni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。 Uyuni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。

未使用的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

- 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。
- 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。 Uyuni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、Uyuni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Uyuni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Uyuni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、UyuniサーバからUyuni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/tftboot**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。

Uyuni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/1i000000lI5B/B2AmvIJN2\\_JsAyjTQzCVP\\_x5ioVgd0bYN9X9NpMugS8](https://suse.my.salesforce.com/sfc/p/1i000000gLOd/a/1i000000lI5B/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。

- UyuniプロキシシステムがWAN接続を介して接続されている。
- **/srv/tftboot**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、Uyuni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. Uyuni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。

- Uyuniサーバの場合:

```
tcpdump -i ethX -s 200 host <ip-address-of-susemanagerproxy> and not ssh
```

- Uyuni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Uyuniが使用する各ネットワークインターフェースにethX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
```

- cobbler sync**が終了したら、TCPdumpsを停止します。
- 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。
- TCPタブに切り替えます。 このタブに表示される数は、UyuniサーバとUyuni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。
- [**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、Uyuni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Uyuni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いる。
- クライアントが誤って設定されたプロキシの背後にいる。
- クライアントが異なるUyuni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Uyuni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Uyuni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、キャッシングを使用してISSマスターとスレーブを管理します。これらのキャッシングには、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、キャッシング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、すべてのキャッシングをクリアして、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。

キャッシングエラーにより、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ングを削除して、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キャッシングエラーの解決

- 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ングファイルを削除します。

```
rm -rf /var/cache/rhn/xml-*
```

- サービスを再起動します。

```
rcaapache2 restart
```

- 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ング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、Uyuni 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. 大量のMachine\_idの重複

Uyuni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。

1方が他方のクローンである2つのマシンを登録しようとする場合、おそらく、Uyuni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、Uyuniは両方のクライアントを1つのシステムとして登録し、2台目のマシンが登録されると、データが上書きされます。

これは、Uyuni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。 マシンIDの変更方法の詳細と手順については、Administration > Troubleshootingを参照してください。

ただし、状況によっては、既存のマシンIDに依存する他のアプリケーションを妨害する可能性があるため、すべてのシステムでマシンIDを変更することは実行可能でも、実用的ではありません。このような場合、Uyuniのコンテキストで使用するための偽のマシンIDを生成するオプションを利用できます。

### プロシージャ: 登録時におけるUyuniのマシンIDの生成

1. ブートストラップスクリプトを作成します(すでにある場合はこのステップをスキップしてください)。 詳細については、Client-configuration >

Registration-bootstrapを参照してください。

2. ファイルを開き、パラメータを変更します。

```
GENERATE_OWN_MACHINEID=1
```

3. 厳密なブートストラップの使用を開始すると、マシンIDが競合しなくなります。

## 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/pgsql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,\n    ChannelSyncFinished,CreateBootstrapRepoFailed,StateApplyFailed,\n    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. 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、Uyuni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。

- SUSE Linux EnterpriseおよびopenSUSEでは、`zypper locks`コマンドを使用します。

## 30.22. 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Uyuniに渡します。Uyuni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、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。

Uyuni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
```

## 30.23. 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、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、Uyuni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
```

## 30.24. 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

Uyuni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、Uyuni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、Uyuni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、Uyuni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。



このプロセ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。このプロセージャではUyuni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. 初期システム設定

- 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. 重複するマシンIDを解決する

- systemdをサポートするディストリビューションの場合:

- マシンに同じマシンIDがある場合は、rootとして、複製された各クライアントのファイルを削除し、再作成します。

```
rm /etc/machine-id
rm /var/lib/dbus/machine-id
rm /var/lib/zypp/AnonymousUniqueId
dbus-uuidgen --ensure
systemd-machine-id-setup
```

- 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)
```

- \_systemdをサポートしないディストリビューションの場合:\_

- rootとして、dbusからマシンIDを生成します。

```
rm /var/lib/dbus/machine-id
rm /var/lib/zypp/AnonymousUniqueId
dbus-uuidgen --ensure
```

- 後でSUSE Liberty Linuxに解放されるRed Hat Enterprise Linux 8.10サーバのクローンを作成する場合は、カーネル設定ファイルを修正するための追加のステップを実行する必要があります。



Red Hat Enterprise LinuxはマシンIDを使用して`/boot/loader/entries`にカーネルエントリを生成します。これらのステップを実行しないと、解放後に古いカーネルエ

ントリと新しいカーネルエントリが混在する結果となります。これはSUSE Liberty Linuxカーネルが古いエントリを置き換えるのではなく新しいエントリを作成するためです。

- マシンIDの変更後、および解放前に、次のコマンドを実行します。

```
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
```

- Red Hat Enterprise Linux 8.10サーバの解放に関する詳細と例については、[Client-configuration](#) > [Contact-methods-intro](#)を参照してください。

### 3. Saltクライアントの再設定

- 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 Uyuni, 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。

## 30.25. 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](https://www.suse.com/releasenotes/x86_64/SL-Micro/6.1/index.html#jsc-SMO-405)).

UyuniプロキシなどのUyuni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

SSHルートログインは2つの異なる方法で有効化できます。どちらの方法でも機能します。セットアップに最適な方法を選択してください。

#### オプションA: 事前設定されたパッケージを使用する

1. クライアントのUI/APIからパッケージ**openssh-server-config-rootlogin**をインストールします。
2. UIまたは端末からコンテナホストを再起動して新しい設定を有効化します。

#### オプションB: SSH設定を手動で編集する

1. 次の内容を含むドロップイン設定/etc/ssh/sshd\_config.d/permit\_root.confファイルを追加します。

```
PermitRootLogin yes
```

2. SSHサーバ設定の再ロード

```
systemctl reload sshd
```

3. SSHを使用して接続している場合、サーバから切断する前に、新しいSSH接続を開いてSSHサーバが正しく機能していることを確認します。

**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。

## 30.26. 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、Uyuni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
```

## 30.27. 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。

## 30.28. 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できますが、Uyuni Web UIは単一の証明書しかインポートできません。 CDNがUyuni 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。)
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、Uyuni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单一の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单一の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Uyuniサーバにインポートできます。

# 30.29. Uyuniサーバの名前変更のトラブルシューティング

Uyuniサーバのホスト名をローカルで変更する場合は、Uyuni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。

## 30.29.1. Rename server

Uyuniサーバのホスト名を変更する必要がある場合は、mgradm server renameコマンドを使用して変更できます。このコマンドはPostgreSQLデータベースの設定とUyuniの内部構造を更新します。

### 30.29.1.1. Server configuration

コマンドは必須パラメータを取りませんが、コンテナホストのホスト名とは異なる場合は、新しいホスト名を受け取ることができます。

新しいホスト名に一致するようにSSL証明書を生成する必要がある場合は、SSL CA/パスワードを提供する必要があります。これは、設定ファイルを使用して安全に実行されます

## プロシージャ: SSL CAパスワード用の設定ファイルの準備

1. config.yamlファイルを次のような内容で作成します。

```
ssl:
  password: "<CA PASSWORD>"
```

This file will be used in the next procedure.

## プロシージャ: Uyuni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があります。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. Uyuni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. 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ます。SSL CAパスワードを保存するファイルを作成した場合は、-c config.yamlを追加します。

```
mgradm server rename
```

新しいホスト名が解決できない場合、コマンドは失敗します。

名前変更のプロシージャは、サーバコンテナの再起動中にも実行されます。次のコマンドを実行して、ログを確認できます。

```
mgrctl exec -ti -- journalctl -u uyuni-update-config
```

サーバコンテナを再起動する際に、このコマンドがすべてのSaltクライアントのpillarデータの更新をトリガすることに注意してください。実行にかかる時間は登録済みクライアントの数によって異なります。

### 30.29.1.2. Directly managed clients reconfiguration

クライアントがUyuni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。

## Procedure: Reconfiguring directly managed clients

- 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(Uyuni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>
```

- 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
```

### 30.29.1.3. Client Connection with applying high state

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。

## 30.29.2. 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Uyuni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
```

## 30.30. 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

- Uyuni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'
```

Uyuniプロキシで、`/etc/uyuni/proxy/config.yaml`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。変更を有効にするには、プロキシコンテナを再起動する必要があります。

```
timeout: 'number'
```

- 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
```

- 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。

## 30.31. 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。Uyuni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、Uyuni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、Uyuni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、Uyuni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Uyuniサーバが確認するのに時間がかかり、Uyuni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。

## 30.32. 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。

## 30.33. 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

Uyuni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、Uyuni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
326a904c2fb7a0e20033c87fc84ebba6b24d937 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):
```

## 30.34. 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。

## プロジェクト: Taskomaticの問題の解決

- Uyuni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。
- taskomaticを再起動します。

```
service taskomatic restart
```

- 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.repodm.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.repodm.RepositoryWriter - Repository metadata
generation for 'cloned-2018-q1-sles12-sp3-updates-x86_64' finished in 4 seconds
```

## 30.35. 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。

# 章 31. GNU Free Documentation License

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

## 0. PREAMBLE

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

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

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

## 1. APPLICABILITY AND DEFINITIONS

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

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

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

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

---

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

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

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

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

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

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

## 2. VERBATIM COPYING

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

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

### **3. COPYING IN QUANTITY**

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

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

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

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

### **4. MODIFICATIONS**

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

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

---

below.

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

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

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

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

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

## **5. COMBINING DOCUMENTS**

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

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

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

## **6. COLLECTIONS OF DOCUMENTS**

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

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

## **7. AGGREGATION WITH INDEPENDENT WORKS**

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

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

## **8. TRANSLATION**

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this

---

License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

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

## 9. TERMINATION

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

## 10. FUTURE REVISIONS OF THIS LICENSE

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

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

## ADDENDUM: How to use this License for your documents

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