VMware Identity Manager Connector のアップグレード

VMware Identity Manager 2.8
VMware Identity Manager 2.9.1

vmware®

最新の技術ドキュメントは VMware の Web サイト（https://docs.vmware.com/jp/）にあります
VMware の Web サイトでは最新の製品アップデートも提供されています。
このドキュメントに関するご意見およびご感想がある場合は、docfeedback@vmware.com までお送りください。

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴイエムウェア株式会社
105-0013　東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

目次

VMware Identity Manager Connector のアップグレード

『Upgrading VMware Identity Manager Connector』では、VMware Identity Manager Connector インスタンスのアップグレード方法について説明します。代わりに新規インストールを選択する場合は、『VMware Identity Manager Connector のインストールと構成』を参照してください。新規にインストールすると、既存の構成は保持されないことに注意してください。

次のアップグレード パスがサポートされています。

- 2.3、2.4、2015.10.1 以降のバージョンから、利用可能な最新バージョンへのアップグレード

更新したコネクタ インスタンスの使用方法については、『VMware Identity Manager 管理者ガイド』を参照してください。

対象者

本書は、VMware Identity Manager Connector をインストール、アップグレード、および構成するユーザーを対象としています。また、仮想マシン技術に精通した経験のある Windows または Linux システム管理者を想定しています。

VMware Identity Manager コネクタのアップグレードについて

1

VMware Identity Manager Connector は、オンラインまたはオフラインでアップグレードできます。

デフォルトでコネクタは、VMware の Web サイトを使用してアップグレード手順を実行します。そのため、コネクタ アプライアンスにはインターネット接続が必要です。また、コネクタ アプライアンスのプロキシ サーバ設定を構成する必要があります (該当する場合)。

コネクタ インスタンスにインターネット接続がセットアップされていない場合は、オフラインでアップグレードを実行できます。オフラインでアップグレードするには、アップグレード パッケージをダウンロードして、アップグレード ファイルをホストするようにローカル Web サーバをセットアップします。

次のアップグレード パスがサポートされています。

- バージョン 2.3、2.4、2015.10.1 以降からアップグレード可能な最新バージョン

VMware Identity Manager Connector のアップグレードの準備

2

コネクタ のアップグレードを準備するには、利用可能なアップグレードの確認、アプライアンスのプロキシ サーバ設定の構成 (該当する場合) など、前提条件となる多くのタスクを実行する必要があります。

この章では次のトピックについて説明します。

アップグレードの前提条件

コネクタをアップグレードする前に、前提条件となる次のタスクを実行します。

オンライン アップグレードの前提条件

- コネクタ アプライアンスが、HTTP を介してポート 80 で vapp-updates.vmware.com を解決してアクセスできることを確認します。
- コネクタのアップグレードが存在することを確認します。適切なコマンドを実行して、アップグレードを確認します。「VMware Identity Manager Connector のオンライン アップグレードの利用可能性を確認する (P. 10)」を参照してください。
- アプライアンスのプライマリ ルート パーティションで利用可能なディスク容量が 2 GB 以上あることを確認します。
- コネクタが適切に構成されていることを確認します。
- バックアップのためにコネクタ アプライアンスのスナップショットを取得します。スナップショットの取得方法の詳細については、vSphere のドキュメントを参照してください。
- アウトバウンドの HTTP アクセスのために HTTP プロキシ サーバが必要な場合は、コネクタ アプライアンスのプロキシ サーバ設定を構成します。「VMware Identity Manager Connector アプライアンスのプロキシ サーバ設定を構成する (P. 10)」を参照してください。

オフライン アップグレードの前提条件

- コネクタのアップグレードが存在することを確認します。My VMware Downloads サイト (my.vmware.com) でアップグレードを確認します。
- アプライアンスのプライマリ ルート パーティションで利用可能なディスク容量が 2 GB 以上あることを確認します。
- コネクタが適切に構成されていることを確認します。
- バックアップのためにコネクタ アプライアンスのスナップショットを取得します。スナップショットの取得方法の詳細については、vSphere のドキュメントを参照してください。

- ローカル Web サーバでアップグレード ファイルをホストするようにコネクタ アプライアンスを構成します。第 4 章「VMware Identity Manager Connector のオフライン アップグレードの実行 (P. 13)」を参照してください。

VMware Identity Manager Connector のオンライン アップグレードの利用可能性を確認する

コネクタ アプライアンスにインターネット接続がセットアップされている場合は、アプライアンスからオンラインでアップグレードを実行できることを確認します。

手順

1 コネクタ アプライアンスに root ユーザーとしてログインします。

2 次のコマンドを実行します。

```
/usr/local/horizon/update/updatemgr.hzn updateinstaller
```

3 次のコマンドを実行して、オンラインのアップグレードを確認します。

```
/usr/local/horizon/update/updatemgr.hzn check
```

VMware Identity Manager Connector アプライアンスのプロキシ サーバ設定を構成する

コネクタ アプライアンスは、VMware のアップデート サーバにインターネットでアクセスします。HTTP プロキシを使用するインターネット アクセスをネットワーク構成で指定している場合は、アプライアンスのプロキシ設定を調整する必要があります。

インターネット トラフィックのみを処理するプロキシを有効にします。プロキシが正しく設定されていることを確認するために、ドメイン内の内部トラフィック用のパラメータを no-proxy に設定します。

注意　認証が必要なプロキシ サーバはサポートされません。

開始する前に

- コネクタ アプライアンスの root パスワードがあることを確認します。
- プロキシ サーバ情報があることを確認します。

手順

1 コネクタ アプライアンスに root ユーザーとしてログインします。

2 コマンド ラインに YaST と入力して YaST ユーティリティを実行します。

3 左ペインで [ネットワーク サービス] を選択してから、[プロキシ] を選択します。

4 [HTTP プロキシ URL] フィールドと [HTTPS プロキシ URL] フィールドにプロキシ サーバの URL を入力します。

5 [終了] を選択して YaST ユーティリティを終了します。

6 コネクタ仮想アプライアンスで Tomcat サーバを再起動して新しいプロキシ設定を使用します。

```
service horizon-workspace restart
```

コネクタ アプライアンスで VMware のアップデート サーバを利用できるようになりました。

VMware Identity Manager Connector のオンライン アップグレードの実行

3

VMware Identity Manager Connector インスタンスは、オンラインでアップグレードできます。

開始する前に

- 第 2 章「VMware Identity Manager Connector のアップグレードの準備 (P. 9)」に一覧された前提条件を満たしていること。
- コネクタ アプライアンスがパワーオンされていること、そして機能していることを確認すること。

手順

1 コネクタ アプライアンスに root ユーザーとしてログインします。

2 次のコマンドを実行します。

```
/usr/local/horizon/update/updatemgr.hzn updateinstaller
```

3 次のコマンドを実行して、オンラインのアップグレードが存在することを確認します。

```
/usr/local/horizon/update/updatemgr.hzn check
```

4 次のコマンドを実行して、アプライアンスを更新します。

```
/usr/local/horizon/update/updatemgr.hzn update
```

アップグレード中に発生したメッセージは、`update.log` ファイル（`/opt/vmware/var/log/update.log`）に保存されます。

5 もう一度 `updatemgr.hzn check` コマンドを実行して、より新しいアップデートがないことを確認します。

```
/usr/local/horizon/update/updatemgr.hzn check
```

6 アップグレードしたアプライアンスのバージョンを確認します。

```
vamicli version --appliance
```

新しいバージョンが表示されます。

7 コネクタ アプライアンスを再起動します。

```
reboot
```

8 VMware Identity Manager の展開環境の各コネクタ アプライアンスについて、これまでの手順を繰り返します。

コネクタのアップグレードは完了です。

VMware Identity Manager Connector のオフライン アップグレードの実行

4

VMware Identity Manager Connector アプライアンスがアップグレードのためにインターネットに接続できない場合は、オフライン アップグレードを実行できます。ローカル Web サーバにアップグレード リポジトリをセットアップして、コネクタ アプライアンスがローカル Web サーバを使用してアップグレードするように構成する必要があります。

この章では次のトピックについて説明します。

オフライン アップグレード向けにローカル Web サーバを準備する

オフラインでのコネクタのアップグレードを開始する前に、コネクタ アプライアンスのサブディレクトリを含むディレクトリ構造を作成して、ローカルの Web サーバを準備します。

開始する前に

- My VMware から `identity-manager-connector-<versionNumber>-<buildNumber>-updaterepo.zip` ファイルをダウンロードします。my.vmware.com にアクセスして、[VMware Identity Manager Download] ページに移動し、[VMware Identity Manager コネクト オフライン アップグレード パッケージ] に表示されているファイルをダウンロードします。
- IIS Web サーバを使用する場合は、ファイル名に特殊文字を利用できるよう Web サーバを構成します。これを構成するには、[フィルタリングを要求] セクションで [ダブル エスケープを許可] オプションを選択します。

手順

1 Web サーバの http://<YourWebServer>/<VM>/ にディレクトリを作成して、ダウンロードした zip ファイルをコピーします。

2 Web サーバに `.sig` (text/plain) および `.sha256` (text/plain) の MIME タイプが含まれていることを確認します。

これらの MIME タイプが含まれない場合、Web サーバの更新確認は失敗します。

3 zip ファイルを展開します。

zip ファイルから抽出された内容は、http://<YourWebServer>/<VM>/ に配置されます。

ファイルから抽出された内容には、サブディレクトリの `/manifest` と `/package-pool` が含まれます。

4 次の `updatelocal.hzn` コマンドを実行して、URL に有効なアップデート コンテンツが含まれていることを確認します。

```
/usr/local/horizon/update/updatelocal.hzn checkurl http://<YourWebServer>/<VM>
```

コネクタを構成してオフライン アップグレードを実行する

オフライン アップグレードを実行するには、ローカルの Web サーバを参照するようにコネクタ アプライアンスを構成します。その後にアプライアンスをアップグレードします。

開始する前に

「オフライン アップグレード向けにローカル Web サーバを準備する (P. 13)」。

手順

1 コネクタ アプライアンスに root ユーザーとしてログインします。

2 次のコマンドを実行して、ローカルの Web サーバを使用するアップグレード リポジトリを構成します。

```
/usr/local/horizon/update/updatelocal.hzn seturl http://<YourWebServer>/<VM>/
```

注意　構成を元に戻してオンライン アップグレードの機能を回復するには、次のコマンドを実行します。

```
/usr/local/horizon/update/updatelocal.hzn setdefault
```

---

3 アップグレードを実行します。

a 次のコマンドを実行します。

```
/usr/local/horizon/update/updatemgr.hzn updateinstaller
```

b 次のコマンドを実行して、利用可能なアップグレードのバージョンを確認します。

```
/usr/local/horizon/update/updatemgr.hzn check
```

c 次のコマンドを実行して、コネクタを更新します。

```
/usr/local/horizon/update/updatemgr.hzn update
```

アップグレード中に発生したメッセージは、`update.log` ファイル（`/opt/vmware/var/log/update.log`）に保存されます。

d `updatemgr.hzn check` コマンドを再実行します。

```
/usr/local/horizon/update/updatemgr.hzn check
```

e アップグレードしたアプライアンスのバージョンを確認します。

```
vamicli version --appliance
```

このコマンドは新しいバージョンを表示します。

f コネクタ アプライアンスを再起動します。

たとえば、コマンド ラインで次のコマンドを実行します。

```
reboot
```

4 VMware Identity Manager の展開環境の各コネクタ アプライアンスについて、これまでの手順を繰り返します。

コネクタのアップグレードは完了です。

コネクタをアップグレードした後の設定の構成

5

コネクタ 2016.3.1.0 以降にアップグレードした後は、次の設定を構成します。

- ThinApps、Kerberos 認証、または Active Directory（統合 Windows 認証）ディレクトリを使用する場合は、ドメインへの参加を解除して、再びドメインに参加させる必要があります。この操作は、環境内のすべてのコネクタ仮想アプライアンスに必要です。
  a [ID とアクセス管理] タブをクリックします。
  b [セットアップ] をクリックします。
  c [コネクタ] ページで、ThinApps の統合、Kerberos 認証、または Active Directory（統合 Windows 認証）ディレクトリに使用されている各コネクタに対し、[ドメイン参加を解除] をクリックします。
  d [ドメインに参加] をクリックして、再びドメインに参加させます。

    ドメインに参加させるには、ドメインへの参加権限を含む Active Directory 証明書が必要です。ドメインへの参加の詳細については、『VMware Identity Manager のインストールと構成』の「Active Directory との連携」を参照してください。
  e Kerberos 認証を使用している場合、Kerberos 認証アダプタを再度有効にします。[認証アダプタ] ページにアクセスするには、[コネクタ] ページの [ワーカー] 列で適切なリンクをクリックし、[認証アダプタ] タブを選択します。
  f 使用している他の認証アダプタが有効になっていることを確認します。
- Active Directory（統合 Windows 認証）を使用している場合、または LDAP 経由の Active Directory で [このディレクトリ は DNS サービス ロケーションをサポートします] オプションを有効にしている場合は、ディレクトリの [ドメイン] ページを更新します。
  a [ID とアクセス管理] タブをクリックします。
  b [ディレクトリ] ページで、ディレクトリをクリックします。
  c バインド DN ユーザーのパスワードを入力して、[保存] をクリックします。
  d ページの左側で [同期設定] をクリックして、[ドメイン] タブを選択します。
  e [保存] をクリックします。

注意　コネクタ 2016.3.1.0 以降では、DNS サービス ロケーションを有効にしたディレクトリを作成するときに、`domain_krb.properties` ファイルが自動的に作成され、ドメイン コントローラが自動的に入力されます。元の環境に `domain_krb.properties` ファイルが含まれていた場合、アップグレード後に [ドメイン] ページを保存し直すと、このファイルが更新され、後から追加したドメインがファイルに追加されます。元の環境に `domain_krb.properties` ファイルが含まれていない場合は、ファイルが作成され、ドメイン コントローラが自動的に入力されます。`domain_krb.properties` ファイルの詳細については、『VMware Identity Manager のインストールと構成』の「Active Directory との連携」を参照してください。

アップグレード エラーのトラブルシューティング 6

アップグレードで発生する問題をトラブルシューティングするには、エラー ログを調べます。アップグレード後にコネクタが起動しない場合は、スナップショットにロールバックして前のインスタンスに戻ることができます。

この章では次のトピックについて説明します。

アップグレード エラー ログの確認

アップグレード時に発生したエラーを解決するには、エラー ログを確認します。アップグレード ログ ファイルは、`/opt/vmware/var/log` ディレクトリ内にあります。

問題

アップグレードの終了後に、コネクタが起動せず、エラー ログにエラーが表示される。

原因

アップグレード時にエラーが発生しました。

解決方法

1. コネクタ アプライアンスにログインします。
2. `/opt/vmware/var/log` ディレクトリに移動します。
3. `update.log` ファイルを開いてエラー メッセージを調べます。
4. エラーを解決して、もう一度アップグレード コマンドを実行します。アップグレード コマンドは、停止した場所から再開します。

注意　または、スナップショットにロールバックしてもう一度アップデートを実行します。

コネクタのスナップショットへのロールバック

アップグレード後にコネクタが適切に起動しない場合は、前のインスタンスにロールバックできます。

問題

コネクタ インスタンスのアップグレード後に、インスタンスが正しく起動しない。アップグレード エラー ログを確認してもう一度アップグレード コマンドを実行したが、問題が解決しない。

原因

アップグレード プロセス中にエラーが発生しました。

解決方法

- 元のコネクタ インスタンスのバックアップとして取得したスナップショットのいずれかにロールバックします。詳細については、vSphere のドキュメントを参照してください。

ログ ファイル バンドルの収集

VMware サポートに送信するログ ファイルのバンドルを収集できます。バンドルはコネクタの構成ページから取得します。

次のログ ファイルがバンドルに収集されます。

表 6-1. ログ ファイル

コンポーネント	ログ ファイルの場所	説明
Apache Tomcat ログ (catalina.log)	`/opt/vmware/horizon/workspace/logs/catalina.log`	Apache Tomcat は他のログ ファイルに記録されないメッセージを記録します。
Configurator ログ (configurator.log)	`/opt/vmware/horizon/workspace/logs/configurator.log`	Configurator が REST クライアントと Web インターフェイスから受け取る要求。
コネクタ ログ (connector.log)	`/opt/vmware/horizon/workspace/logs/connector.log`	Web インターフェイスから受信された各要求の記録。各ログ エントリには要求 URL、タイムスタンプ、例外が含まれています。同期アクションは記録されません。

手順

1 コネクタの構成ページ (https://<connectorURL>:8443/cfg/logs) にログインします。

2 [ログ バンドルの準備] をクリックします。

3 バンドルをダウンロードして、これを VMware サポートに送信します。

インデックス