Secure Firewall Management CenterおよびSecure Firewall Device ManagerのVDBバージョンのロールバック

内容

[はじめに](#)

[前提条件](#)

- [要件](#)
- [使用するコンポーネント](#)

[設定](#)

- [初期設定](#)
  - [FMCの初期設定](#)
  - [FDMの初期設定](#)
- [FMC v7.3以降のVDBロールバックプロセス](#)
- [FMC v7.2.x以前のVDBロールバックプロセス](#)
- [FMC HAのVDBロールバックプロセス](#)
- [FDMのVDBロールバック・プロセス](#)

[確認](#)

- [FTD CLIから](#)
- [FMCのGUIから](#)
- [制限事項](#)

[関連情報](#)

はじめに

このドキュメントでは、Secure Firewall Management Center(FMC)およびSecure Firewall Device Manager(FDM)の脆弱性データベース(VDB)をロールバックするプロセスについて説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Secure Firewall Management Centerバージョン7.3およびVDB 361+
- Cisco Secure Firewall Management Centerバージョン7.2.1およびVDB 343+

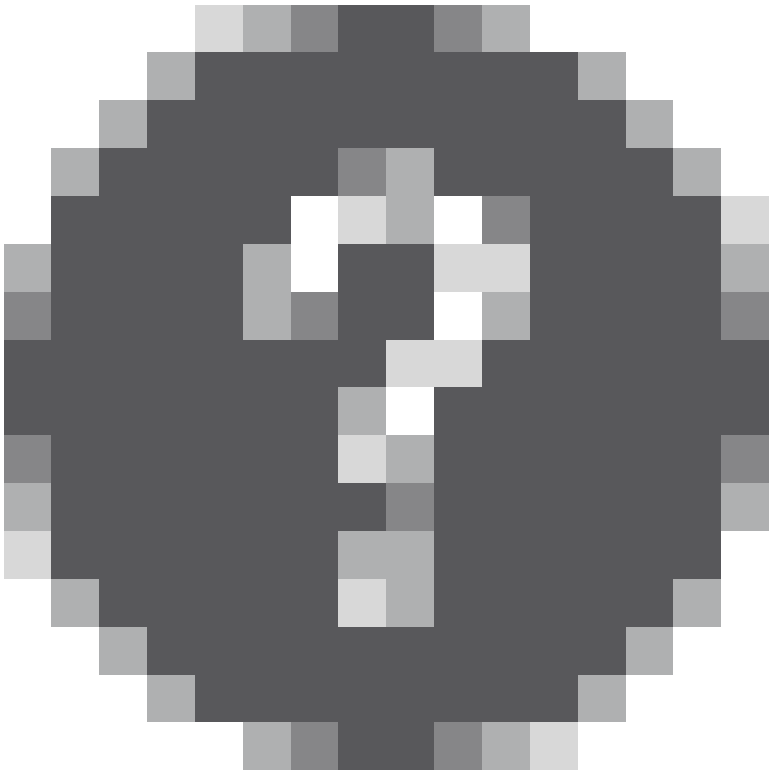
- Cisco Secure Firewall Device Managerバージョン7.0.6およびVDB 395+

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

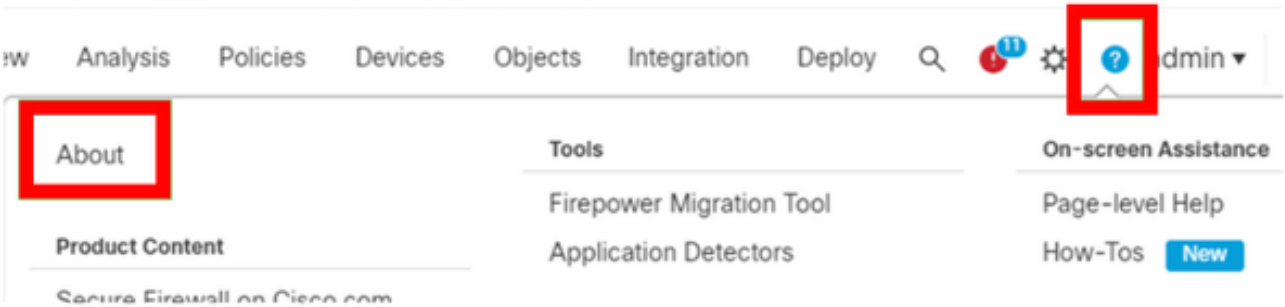
設定

初期設定

FMCの初期設定



FMCのGUIで、Mainメニュー>
> Aboutを選択します。



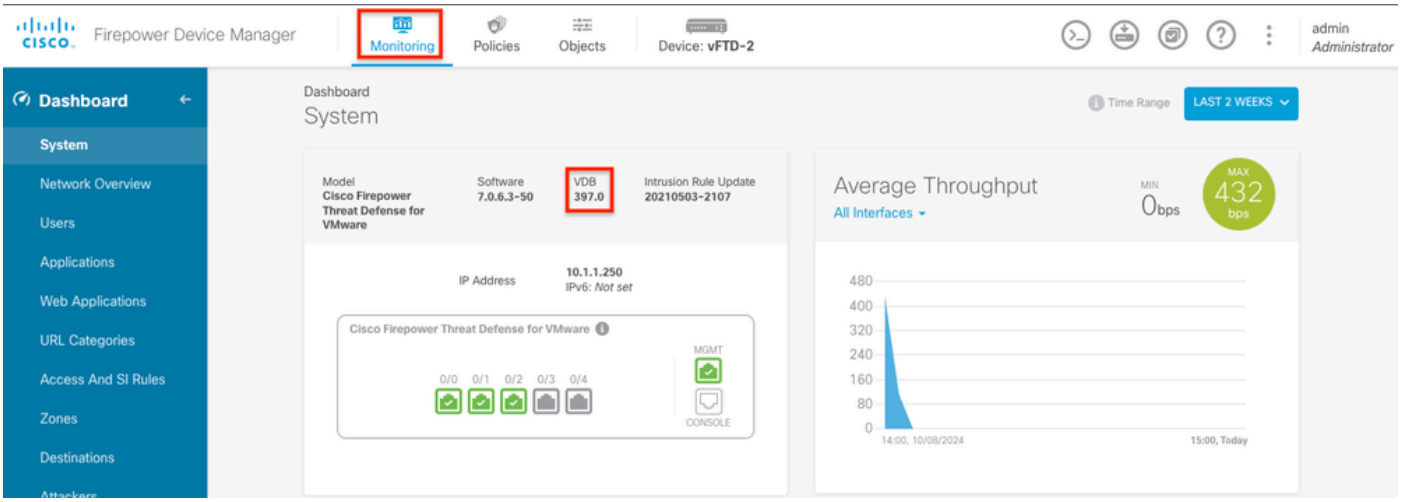
FMCのCLIから、次のコマンドshow versionを使用して、実行されている実際のVDBバージョンを確認できます。

<#root>

```
> show version

-------------------[ firepower ]--------------------
Model : Secure Firewall Management Center for VMware (66) Version 7.3.0 (Build 69)
UUID : e8f4b5de-4da1-11ed-b2ce-4637a3ef82f7
Rules update version : 2023-07-12-002-vrt
LSP version : lsp-rel-20230712-1621

VDB version : 361

----------------------------------------------------
```

FDMの初期設定

FDM GUIで、監視ダッシュボードに移動して、次のように実際に実行されているVDBのバージョンを確認できます：

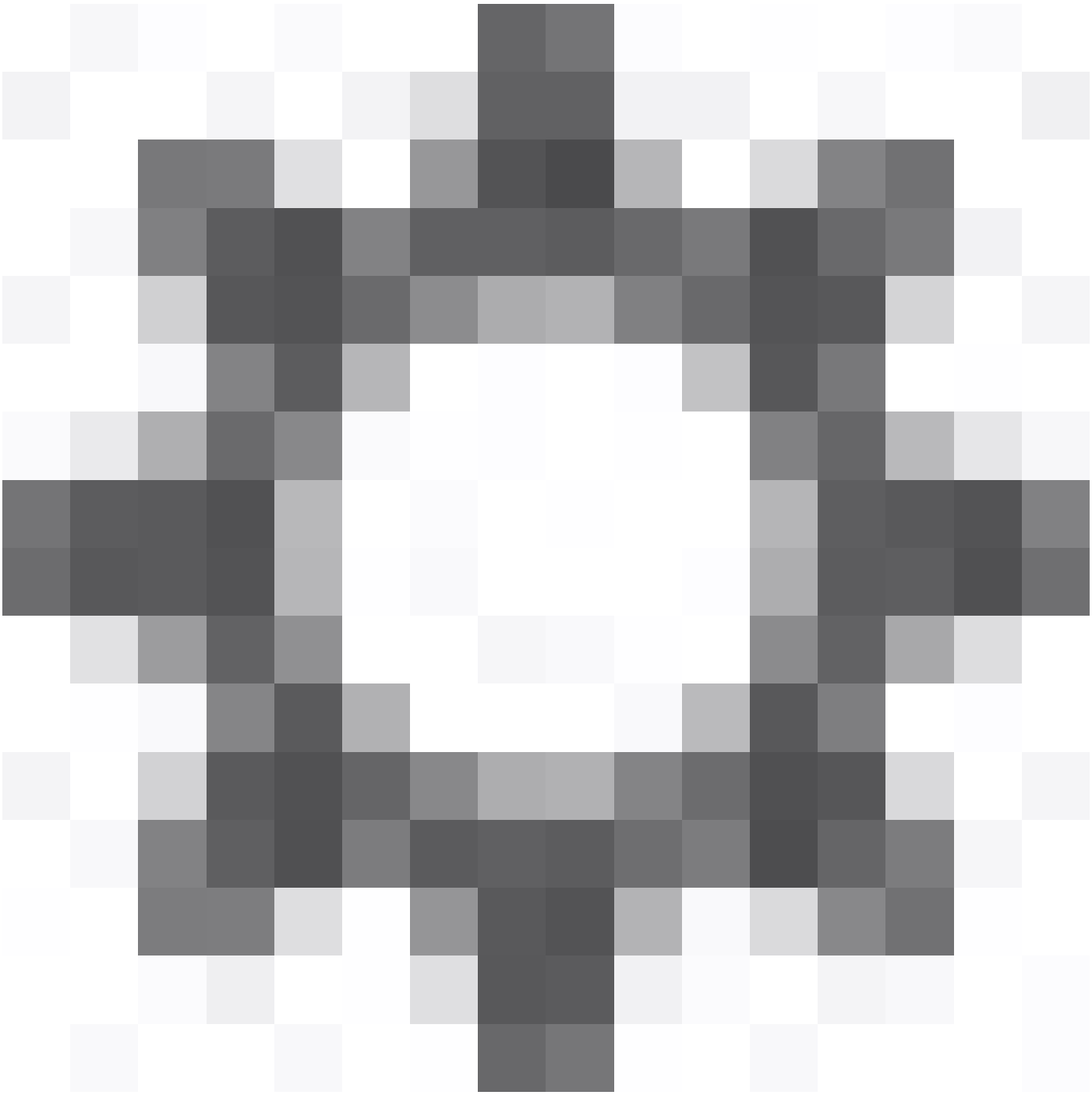


FDM CLIから、次のコマンド「cat /etc/sf/.versiondb/vdb.conf」を使用して、実際に実行されているVDBのバージョンを確認できます。

```
root@vFTD-2:/ngfw/var/cisco/deploy/pkg/var/cisco/packages# cat /etc/sf/.versiondb/vdb.conf
CURRENT_VERSION=4.5.0
CURRENT_BUILD=397
CURRENT_APPID_VER=138
CURRENT_NAVL_VER=158
```

FMC v7.3以降のVDBロールバックプロセス

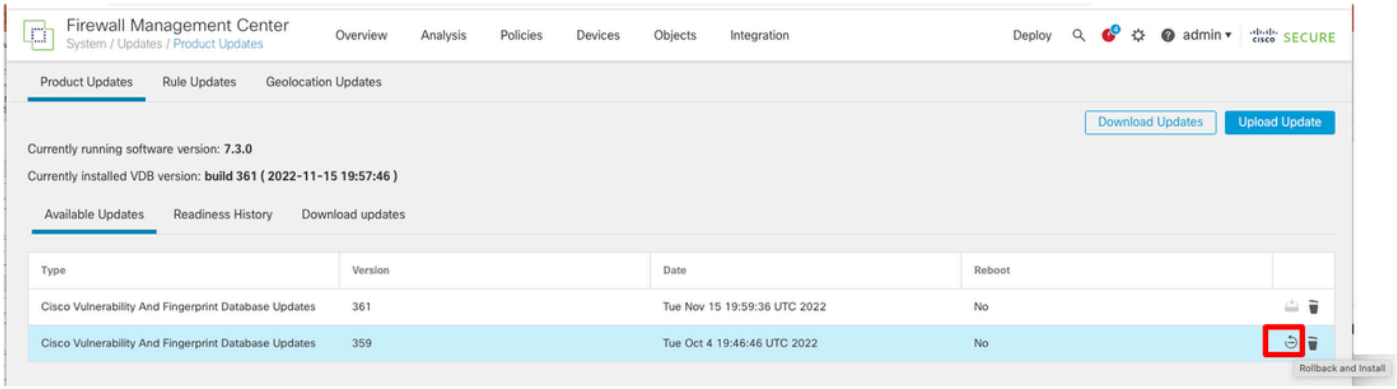
FMC v7.3+のVDBバージョンをロールバックする手順は次のとおりです。次の例では、VDB 361からVDB 359にロールバックします。
1. ロールバック先のVDBファイルがFMCに保存されていない場合は、FMCにファイルをアップロードする必要があります。そのためには、に移動します。 システム(



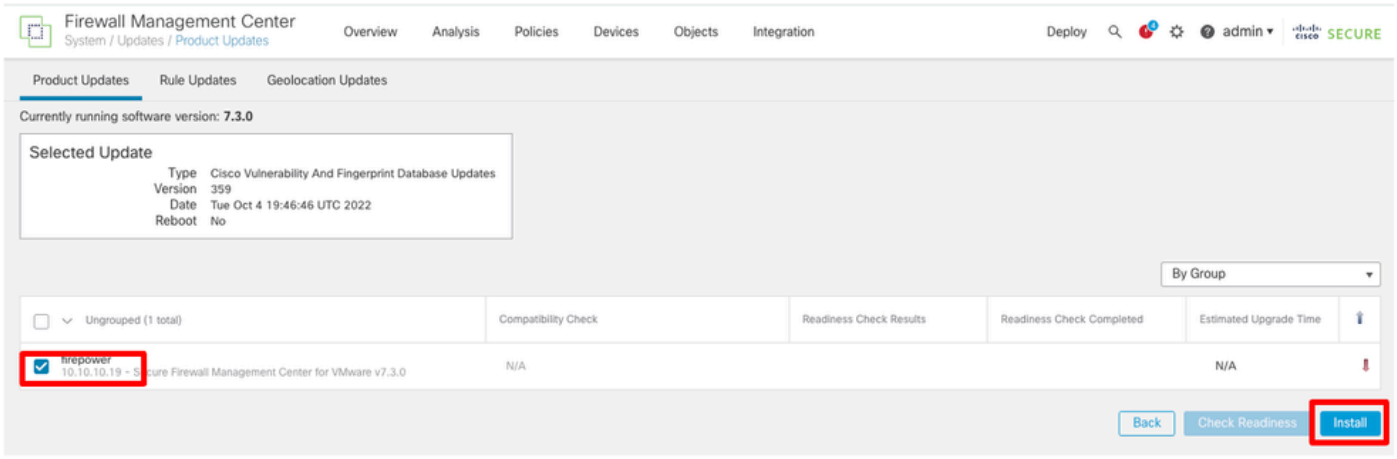
) > アップデート > 製品アップデート > Available Updates> Upload Updatesの順に選択し、ローカルコンピュータからVDBファイルを選択して、Uploadをクリックします。

2. VDBファイルがFMCにアップロードされると、古いバージョンのVDB (この例ではバージョン359) ではInstallアイコンの代わりにRollbackアイコンが表示されます。

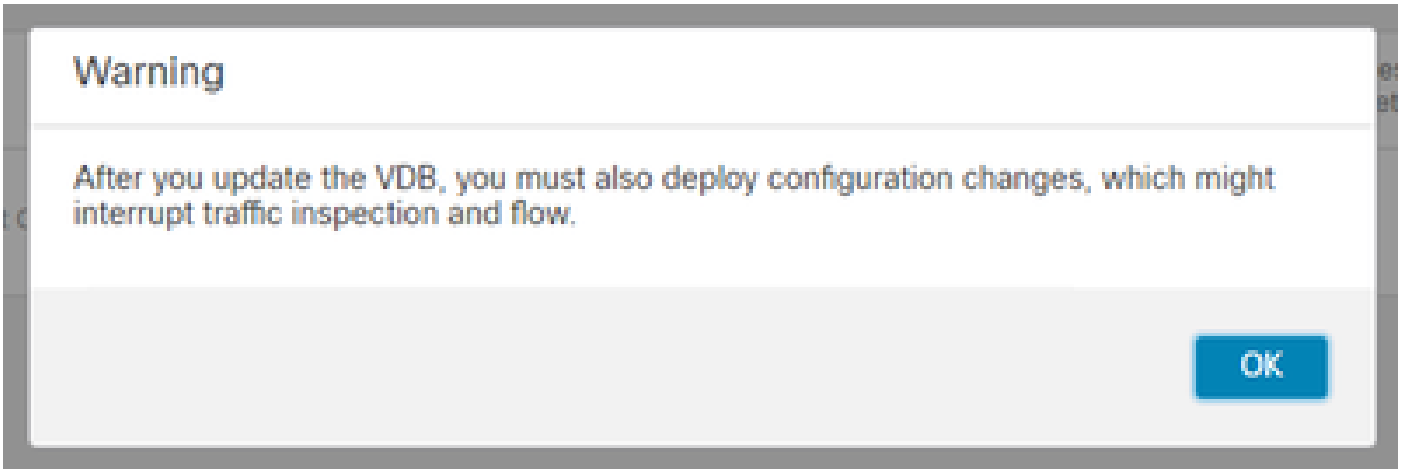
3. VDB 361からVDB 359へのロールバックに進むには、「ロールバック」ボタンをクリックします。



4. 次に、FMCのチェックボックスをオンにして、Installをクリックします。



5. VDBロールバック後に管理対象デバイスに変更を展開した場合に、トラフィックが中断される可能性があることを示す警告プロンプトが表示されます。



FMC v7.2.x以前のVDBロールバックプロセス

FMC v7.2.x以前のVDBバージョンをロールバックするには、次の手順を実行します。

1. FMC CLIにSSHで接続します。

2. エキスパートモードに切り替え、rootにして、次のようにロールバック変数を'1'に設定します。

<#root>

>expert

$sudo su
#export ROLLBACK_VDB=1

3. ロールバック先のVDBパッケージが次のFMCディレクトリ/var/sf/updatesにあることを確認します。VDBファイルがこのパスにない場合は、必要なVDBファイルをFMCにアップロードします。

4. 次に、次のコマンドを入力して、VDBロールバックのインストールを続行します。

<#root>

install_update.pl --detach /var/sf/updates/

例：

```
root@FMC:/var/sf/updates# install_update.pl --detach /var/sf/updates/Cisco_VDB_Fingerprint_Database-4.5
ARGV[0] = --detach
ARGV[1] = /var/sf/updates/Cisco_VDB_Fingerprint_Database-4.5.0-394.sh.REL.tar
bundle_filepath: /var/sf/updates/Cisco_VDB_Fingerprint_Database-4.5.0-394.sh.REL.tar
install_update.pl begins. bundle_filepath: /var/sf/updates/Cisco_VDB_Fingerprint_Database-4.5.0-394.sh.
Makeself GetUpdate Info params FILEPATH : /var/tmp/upgrade-patch/Cisco_VDB_Fingerprint_Database-4.5.0-3
FILEPATH directory name /var/tmp/upgrade-patch at /usr/local/sf/lib/perl/5.24.4/SF/Update/Makeself.pm l
Inside GetInfo FILEPATH :/var/tmp/upgrade-patch/Cisco_VDB_Fingerprint_Database-4.5.0-394.sh at /usr/loc
Use of uninitialized value in string ne at /usr/local/sf/lib/perl/5.24.4/SF/Update/Makeself.pm line 125
```

4. 次のディレクトリの場所/var/log/sf/<VDB Package file>でvdbインストールログを監視し、status.logファイルからVDBインストールの進捗状況を確認します。

```
root@FMC:/var/log/sf/vdb-4.5.0-394# tail -f status.log
state:running
ui:The install has begun.
ui:[ 0%] Running script pre/000_start.sh...
ui:[ 4%] Running script pre/001_check_required_upgrade.pl...
ui:[ 8%] Running script pre/005_check_low_end.pl...
ui:[12%] Running script pre/010_check_versions.sh...
ui:[15%] Running script pre/011_check_versions.pl...
ui:[19%] Running script pre/020_check_space.sh...
```

```
ui:[23%] Running script pre/500_stop_rna.pl...
ui:[27%] Running script pre/999_finish.sh...
ui:[31%] Running script installer/000_start.sh...
ui:[35%] Running script installer/100_install_files.pl...
ui:[38%] Running script installer/200_install_fingerprints.sh...
ui:[42%] Running script installer/300_install_vdb.sh...
ui:[46%] Running script installer/400_install_rdps.pl...
ui:[50%] Running script installer/420_delete_obsolete_ids.pl...
ui:[54%] Running script installer/430_change_dupe_custom_app_names.pl...
ui:[58%] Running script installer/450_resave_detectors.pl...
ui:[62%] Running script installer/480_update_dynamic_config_with_csds.pl...
ui:[65%] Running script installer/525_export_compliance_policies.pl...
ui:[69%] Running script installer/900_update_version.sh...
ui:[73%] Running script installer/901_update_db_version.pl...
ui:[77%] Running script installer/950_reapply_to_sensor.pl...
ui:[81%] Running script installer/975_export_data.pl...
ui:[85%] Running script installer/999_finish.sh...
ui:[88%] Running script post/000_start.sh...
ui:[92%] Running script post/500_start_rna.pl...
ui:[96%] Running script post/999_finish.sh...
ui:[100%] The install completed successfully.
ui:The install has completed.
state:finished
```

5. VDBのインストールが完了したら、管理対象デバイスへのポリシー導入を実行します（ポリシー導入を実行するには、設定で最小限の変更を行う必要があります）。

6. FMCのCLIから、show versionコマンドを実行して、実行中の実際のVDBバージョンを確認します。

```
> show version
----------------[ FMC ]-----------------
Model                     : Secure Firewall Management Center for VMware (66) Version 7.2.1 (Build 40)
UUID                      : 597fda3e-386e-11ed-95e2-dbc141b3e897
Rules update version      : 2022-09-14-001-vrt
LSP version               : lsp-rel-20220511-1540
VDB version               : 394
----------------------------------------------------
```

FMC HAのVDBロールバックプロセス

1. FMC HAの同期を一時停止し、各FMCのVDBをロールバックします。

2. 各FMCに対してVDBロールバックプロセスが完了したら、FMC HAを再開します。

- HAページで、VDBバージョンの不一致により「vdb not in sync」が表示される場合があります。このメッセージは無視してかまいません。

3. FMCに対してVDBのロールバックプロセスを実行した後で、これが機能せず、最新のVDBアップデートが自動的に再インストールされる場合は、最新のVDBファイルを見つけて、両方の

FMC用に以下のディレクトリから削除します。

```
/var/sf/updates (.sh file)
/var/cisco/pacakges/ (.tgz file)
```

4. 次に、上記のステップ1および2を繰り返して、FMC HAのVDBをロールバックします。

FDMのVDBロールバック・プロセス

FDMのVDBバージョンをロールバックするには、Cisco TACケースをオープンし、TACエンジニアにこのシスコのドキュメントを示してサポートを依頼してください。

確認

FTD CLIから

FTDでVDBのインストール履歴を確認するには、次のディレクトリの内容を確認する方法があります。

<#root>

root@firepower:/ngfw/var/cisco/deploy/pkg/var/cisco/packages#

ls -al

```
total 72912
drwxr-xr-x 5 root root 130 Sep 1 08:49 .
drwxr-xr-x 4 root root 34 Aug 16 14:40 ..
drwxr-xr-x 3 root root 18 Aug 16 14:40 exporter-7.2.4-169
-rw-r--r-- 1 root root 2371661 Jul 27 15:34 exporter-7.2.4-169.tgz
drwxr-xr-x 3 root root 21 Aug 16 14:40
```

vdb-368

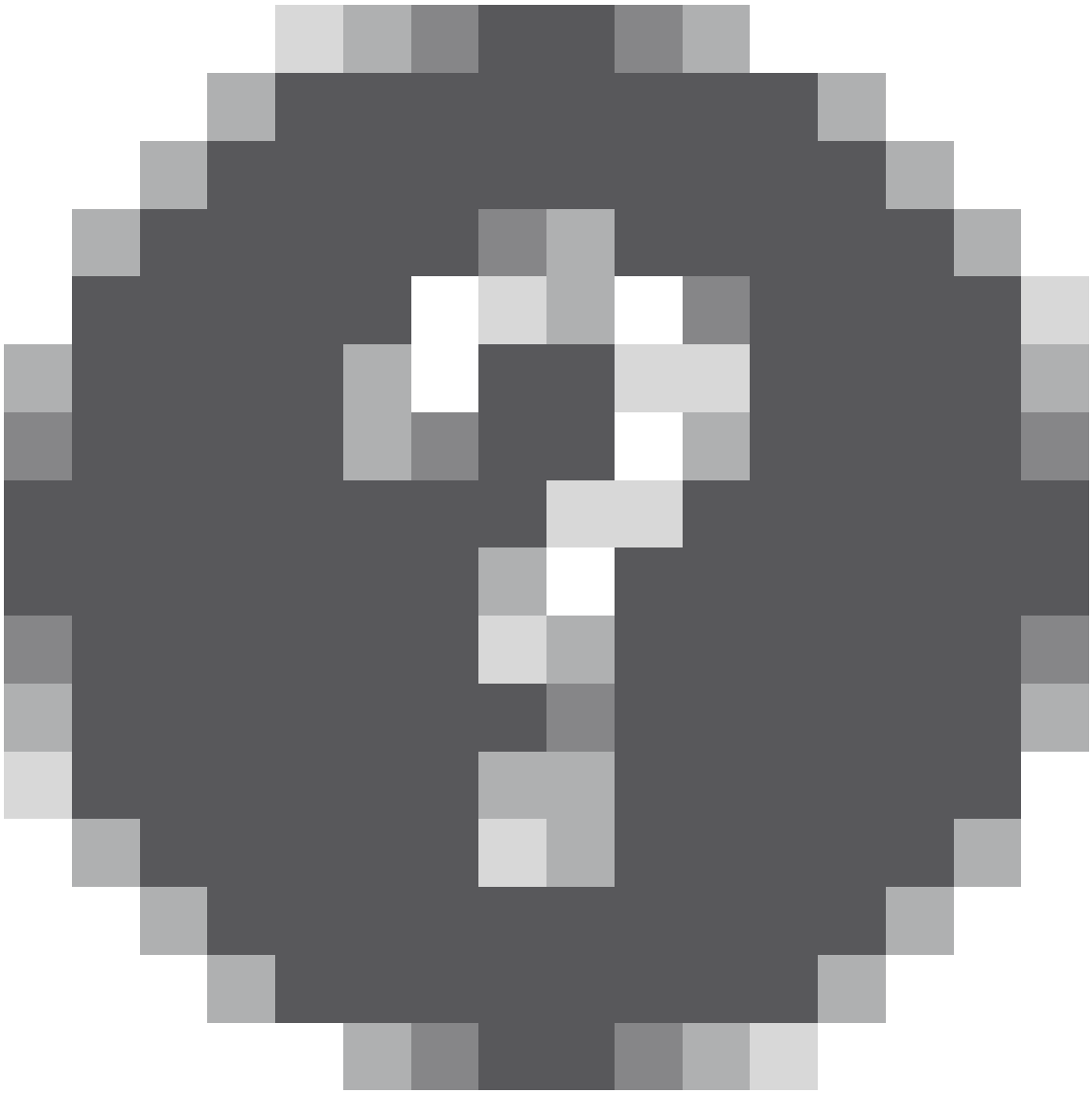
```
-rw-r--r-- 1 root root 36374219 Jul 27 15:34 vdb-368.tgz
drwxr-xr-x 3 root root 21 Sep 1 08:49
```

vdb-369

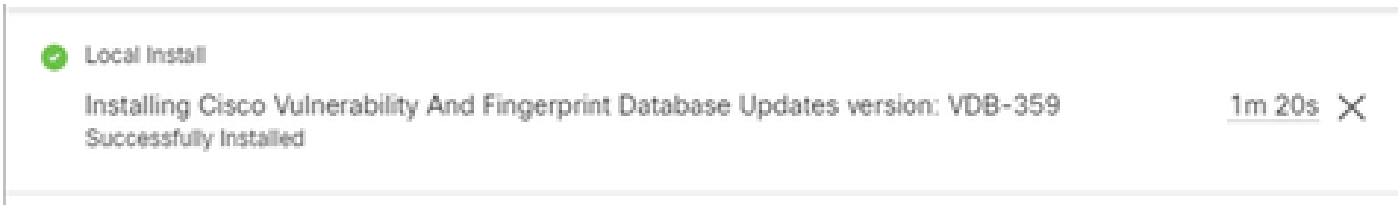
```
-rw-r--r-- 1 root root 35908455 Sep 1 08:48 vdb-369.tgz
```

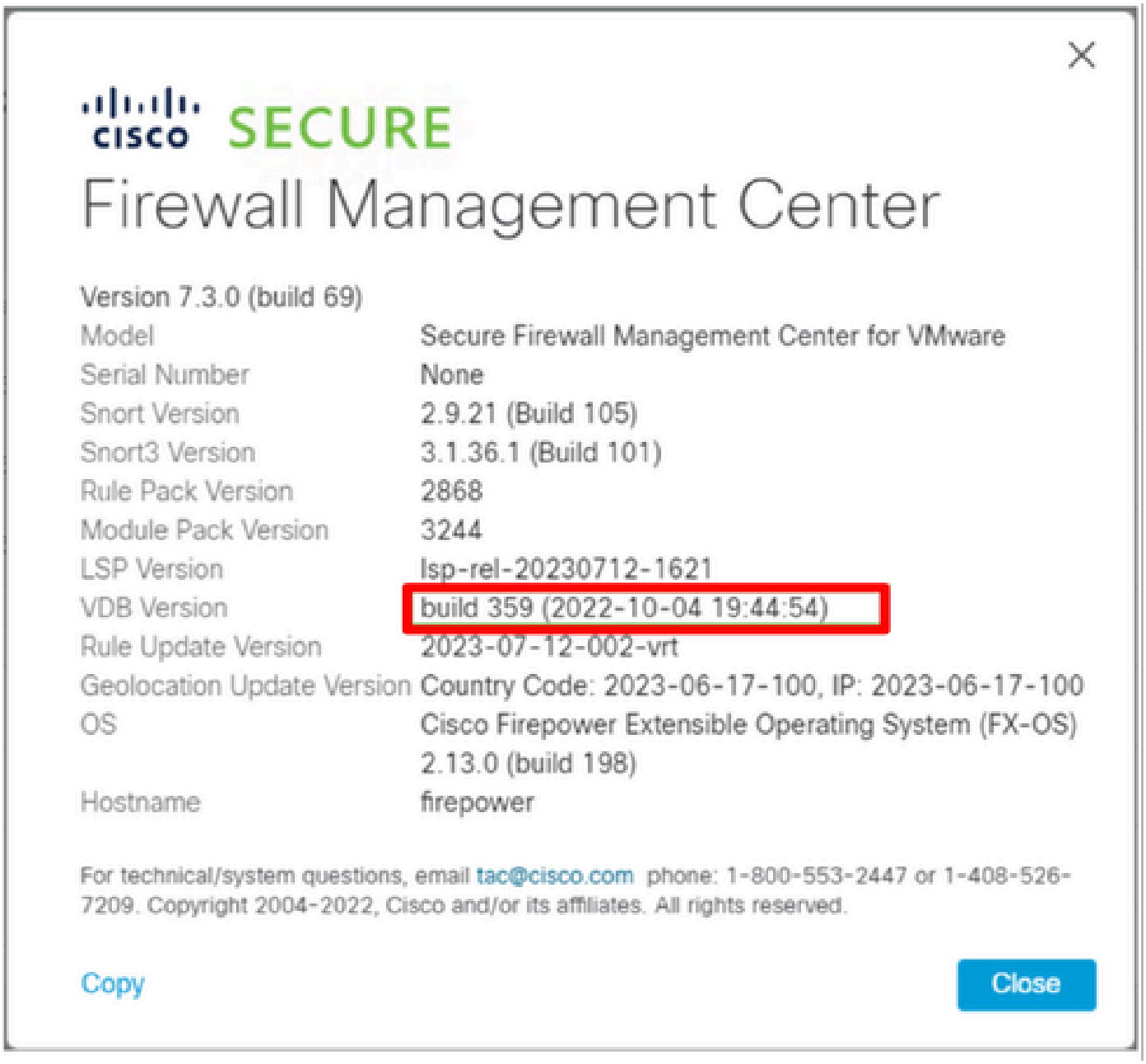
FMCのGUIから

ロールバックタスクが完了すると、VDBのバージョンをメインメニュー>

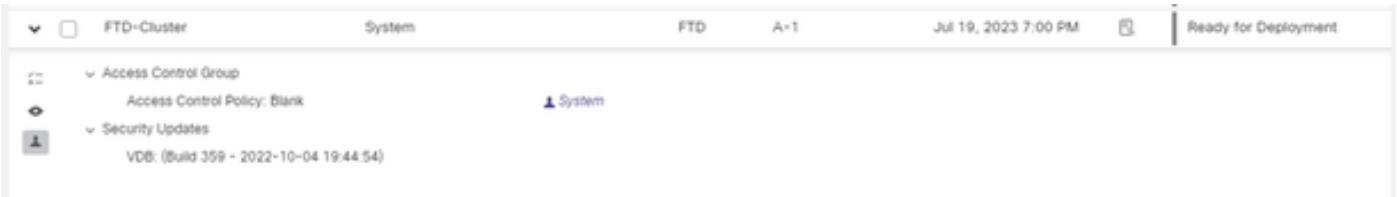


> バージョン情報。


Local Install
Installing Cisco Vulnerability And Fingerprint Database Updates version: VDB-359
Successfully Installed
1m 20s

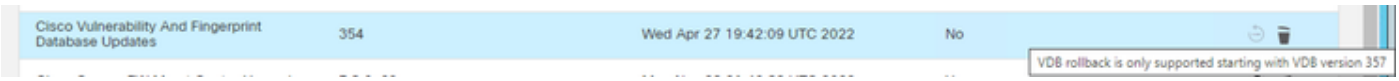


最後に、VDBがロールバックされた後、ポリシーを展開して、新しいVDB設定をFMC管理対象ファイアウォールにプッシュする必要があります。

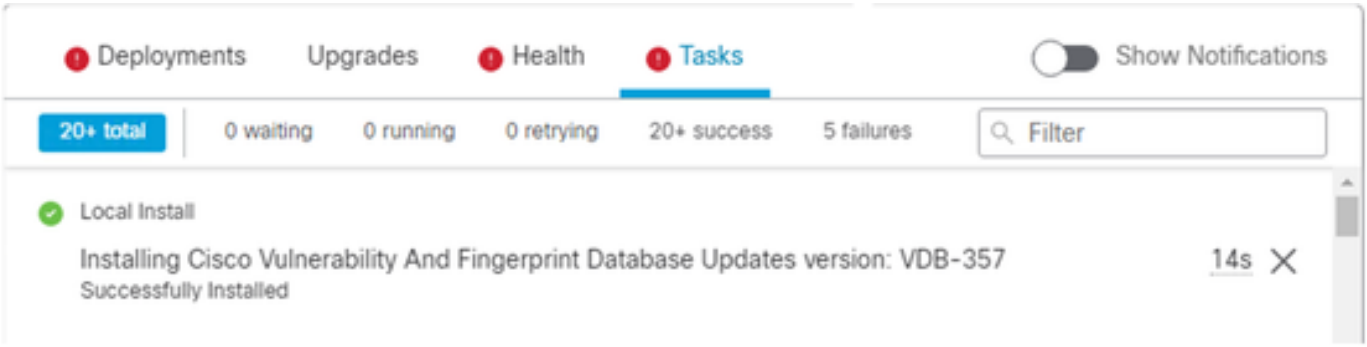


制限事項

- VDBロールバックボタンは、7.3より前のFMCバージョンでは使用できません。
- VDBを357より古いバージョンにロールバックすることはできません。357より古いVDBバージョンがFMCにアップロードされると、ロールバックボタンはグレー表示になります。



- VDBのバージョンがFMCのベースVDBのバージョンよりも低い場合、完了したロールバックタスクが表示されますが、表示されるVDBのバージョンは引き続きロールバックの試行の前と同じです。



FMCのCLIから、ロールバックのターゲットバージョンがベースFMCのバージョンよりも低いためにこの状況が発生したことを確認できます。これは、FMC CLIのstatus.logファイルで確認できます。

```
> expert
sudo su
cd /var/log/sf/vdb-4.5.0-<vdb number>/
cat status.log

root@firepower:/var/log/sf/vdb-4.5.0-357# cat status.log
state:running
ui:The install has begun.
ui:[ 0%] Running script pre/000_start.sh...
ui:[ 4%] Running script pre/010_check_versions.sh...
ui:[ 4%] Non-Fatal error: Non-Fatal error: Cannot rollback to version(357) lower than default VDB 358
ui:[ 4%] The install completed successfully.
ui:The install has completed.
state:finished

-----------------------------------------------------
```

関連情報

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。