

2025 年 09 月 16 日
株式会社ネットワーク

FortiManager がインストール中にポリシーを誤って消去する問題について

Fortinet 社より、重大な問題が発生する可能性があるとのアナウンスがございました。ご利用の構成や製品（バージョン）をご確認いただき、該当する場合は、速やかにメーカー推奨の対策をご実施いただきますようお願いいたします。記述されていない製品およびバージョンにつきましては非該当となります。

説明:

2 台以上の FortiGate ユニットが高可用性（HA）クラスタに構成されている場合、クラスタの通常の動作の一部として、すべてのメンバー間で設定が同期されます。ただし、クラスタ内のすべての設定がメンバー間で同期されるわけではありません。

FortiGate クラスタでは、次のコマンドでこの動作を確認します。

```
#diag sys ha nonhaconf <FortiGate serial>
```

FortiManager ユニットでは、次のコマンドでこの動作を確認します。

```
#exe fmpolicy print-device-nonsync-config <adom-oid> <dev-oid> <FortiGate serial>
```

HA クラスタ内のプライマリ FortiGate が、FortiManager に無効な nonhaconf 設定を返すという問題が発生する場合があります。その後、FortiManager からデバイス設定のみをインストールすると、FortiManager によって FortiGate HA クラスタからすべてのポリシーが削除される可能性があります。

影響が生じる可能性のある製品:

FortiManager 7.2.5 - 7.2.10

FortiManager 7.4.6

FortiOS 7.2 all patches

FortiOS 7.4 all patches

FortiManager を用いたワークアラウンド:

- 1) デバイスレベルの設定のみを適用する場合でも、ポリシーパッケージとデバイス設定を毎回インストールしてください。
- 2) グローバル設定「set force-remote-diff enable」はインストールプレビューに問題のある変更を表示しますが、問題の発生を防ぐことはできません。

対策:

Fortinet 社は下記バージョンにて修正を提供しています。

FortiOS 7.4.9 or later(※)

FortiOS 7.6.4 or later

FortiManager 7.2.11 or later

FortiManager 7.4.7 or later

FortiManager 7.6.3 or later

FortiManager の修正による副作用として、無効な nonhaconf のエラー処理が強化されたため、FortiManager GUI で手動で取得を実行した際に取得に失敗する可能性があります。この問題は Bug ID : 1167436 として管理されており、FortiManager 7.2.11、7.4.8、および 7.6.4 で修正される予定です。

下記 CLI コマンドを用いた情報の再取得(retrieve)の実行がワークアラウンドとされております。

```
#diagnose test deploymanager reloadconfig <devid>
```

2025 年 9 月 16 日段階で公開されている内容は以上となります。

※FOS 7.4.9 は、近日中にリリースを予定しております。但し、予定が変更となる場合も御座います事を、悪しからずご承知置きくださいますと幸いです。

以上