NCD-MWG-1388

Skyhigh Secure Web Gateway
旧 McAfee Web Gateway
アプライアンスアップデート手順書

2024年5月30日
株式会社ディアイティ
テクニカルユニット

目次

1 はじめに

1.1 本書の目的

本手順書は、Skyhigh Secure Web Gateway　旧 McAfee Web Gateway Version7 以降のソフトウェアアップデートを実施するための手順書です。

アップデート開始後、新パッケージのダウンロードが終了するまで Web Gateway サービスは継続しますが、パッケージのダウンロード後自動的に実施されるサービス再起動、およびアプライアンスの再起動中には一時的に使用できなくなりますのでご注意下さい。

また、アップデート実施前には必ず Web Gateway の設定をバックアップしてください。
バックアップ手順については、「Skyhigh Secure Web Gateway 設定バックアップ・リストア手順書」をご確認下さい。

1.2 ブランド名の変更について

2022 年 1 月：McAfee Enterprise は Trellix と Skyhigh Security の二つの組織に分割されました。
2022 年 3 月：McAfee Enterprise のゲートウェイソリューションは Skyhigh Security にリブランディングされました。
旧 McAfee Web Gateway は Skyhigh Secure Web Gateway（SWG）となりました。

1.3 旧ドメイン名の利用停止について

2024 年 9 月 30 日に旧 McAfee Web Gateway がパターンファイルの自動アップデート等に利用している旧ドメイン名の利用停止が予定されています。
ドメイン名はハードコードされているため、設定変更による対応ができません。新ドメインの利用には対応バージョンへのバージョンアップが必要となります。
旧ドメイン名の利用停止以降は自動アップデートが不可能となるため、それまでに新ドメイン名を利用するバージョンにアップデートしてください。

バージョン系統	旧ドメイン利用バージョン	新ドメイン利用バージョン
v10.x	v10.2.26 以前 （EOL:2023/12/31）	v10.2.27 以降 （EOL:2023/12/31）
v11.x	v11.0.0 ～ v11.2.15 (EOL:2024/9/30)	v11.2.16 以降 （EOL:2024/12/31）
v12.x	v12.0.0 ～ v12.1.x （EOL:2024/9/30）	v12.2.0 以降

機能名	旧ドメイン名	新ドメイン名
Update Server domain	tau.mcafee.com	tau.skyhigh.cloud
GTI Lookup domain	tunnel.web.trustedsource.org tunnellist.gti.mcafee.com	swg.repl.gti.trellix.com
SSE list synchronization domain	api.wgcs.mcafee-cloud.com	api.wgcs.skyhigh.cloud.com

2 アップデートパッケージについて

2.1 Web Gateway のアップデートについて

Web Gateway は、ソフトウェアである mwg および OS である Linux に関する新機能や既知の問題の修正が、アップデートの形で不定期にリリースされます。
アップデートは、バージョン番号とビルド番号の組み合わせによりあらわされ、同じバージョンでもビルドが異なる場合には内容が異なります。

また、Web Gateway のソフトウェアバージョンには Main Release と Controlled Release が存在します。

Main Release はパブリックリリースバージョンです。通常の製品利用における運用対象バージョンになります。
Controlled Release は特定の不具合や新機能を実装した、先行リリースバージョンです。該当の不具合修正や新機能をいち早く使用したいお客様が、ご利用するリリースバージョンです。

2024 年 5 月 30 日の Main Release と Controlled Release は以下の通りです。

- Main Release 12.2.8
- Controlled Release 12.2.2

現時点での Main Release と Controlled Release のバージョンは、メーカーの Content & Cloud Security Portal サイトでご確認ください。
※ Content & Cloud Security Portal サイトのご利用には、Web Gateway ご購入時に発行される専用の ID・パスワードが必要です。

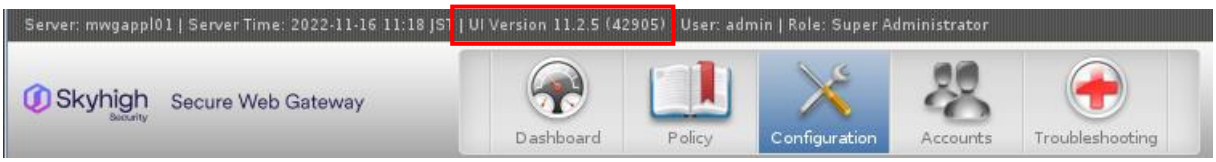
Web Gateway には、一般的なパッチの概念がないため、WebUI にてアプライアンスのアップデートを実施すると、自動的に Main Release の最新版にアップデートされます。

最新版以外のリリースバージョンにアップデートするには、そのバージョンの ISO イメージを Content & Cloud Security Portal よりダウンロードし、アプライアンスの新規インストール後、設定バックアップファイルをリストアします。
ただし、設定バックアップファイルを取得時より前のバージョンにリストアすることはサポートされておりません。
(例： v7.8 の設定バックアップファイルを v7.7 にリストアすることはサポートされていません)

ISO イメージファイルやリリースノートは、メーカーの Content & Cloud Security Portal サイト (旧称:Extranet)よりダウンロード可能です。
ただし、v10.2.16 以前、v11.2.4 以前, v12.0.0 以前の McAfee ロゴを使用したバージョンはダウンロードできません。

2.2 バージョン情報確認方法

バージョン情報は WebUI にログインすることで確認できます。
下記の例では、 11.2.5.0 がバージョンを示し、 (42905)が Build 番号です。



UI Version 11.2.5.0 (42905)

CLI では以下のコマンドを実行します。

```
/opt/mwg/bin/mwg-core -v | head -n 1
```

実行結果例

```
McAfee Web Gateway Core version: 11.2.5 - build: 42905 - git: mwg-11.2-branch c295d7b73d
```

3 アップデート前の注意事項

3.1 設定バックアップの取得

アップデートを行う前には、必ず設定のバックアップを取得してください。
もしも、アップデート後に元のバージョンに戻すことになった場合には、アップデート前の設定バックアップファイルが必要です。

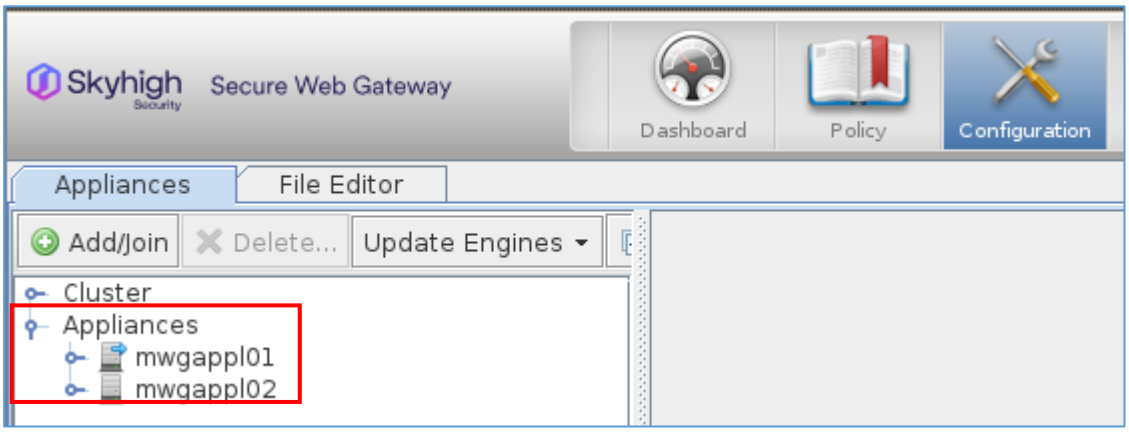
Troubleshooting＞Backup/Restore に移動し、「Backup to file...」をクリックします。

詳細な設定バックアップ取得手順は、「Skyhigh Secure Web Gateway 旧 McAfee WebGateway Version7 以降 設定バックアップ・リストア手順書」をご参照ください。

3.2 Central Management 機能有効時の注意事項

Central Management 機能は、複数の Web Gateway で Policy 設定を同期する機能です。

WebUI で Configuration > Appliances タブを表示したときに、下記の画面のように複数のアプライアンス名が表示されているときは Central Management を有効に設定しています。



■ WebUI へのログイン制限について

Central Management 機能を有効にしている場合には、仕様により、1 台の WebUI にログインしていると、同時に他の Web Gateway の WebUI にログインできません。他の Web Gateway の WebUI にログインする場合は、ログイン中の Web Gateway から一旦ログアウトし、60 秒以上経過したあとに、別 Web Gateway にログインしてください。

■ 同一バージョンの制限について

Central Management 機能を有効にしている場合には、全ての Web Gateway が同一バージョンでなければならないという制限があります。

通常は 1 台ずつアップデートを行いますので、全 Web Gateway のアップデートが完了するまでの期間は異なるバージョンの Web Gateway で同期をとることになり、Central Management 機能に問題が発生する可能性があります。
対策として、メーカーでは一時的に Central Management 機能を無効にして、全 Web Gateway のアップデートが完了した後に、Central Management 機能を有効にする手順を推奨しています。

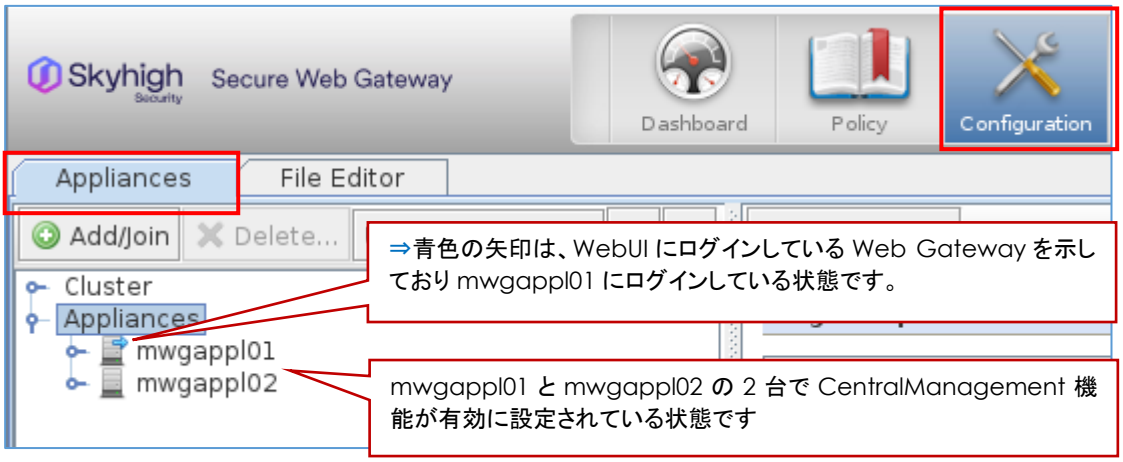
その場合、各アプライアンスを一つずつ削除し、それぞれをアップデートする必要があります。全てのアプライアンスのアップデートに成功したら、再度すべてのアプライアンスを Central Management クラスタに追加します。

1 号機(mwgappl01)と 2 号機(mwgappl02)の 2 台で Central Management 機能を使用している場合を例として、Central Management 機能を無効/有効にする手順を説明します。

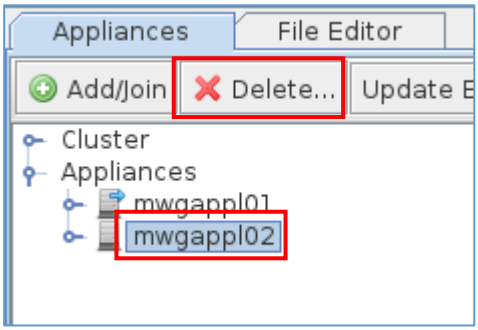
✧ Central Management を無効にする手順

1 号機にログインして 2 号機を削除します。

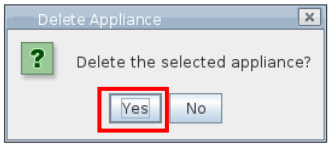
mwgappl01 の WebUI にログインして、 Configuration > Appliances タブを開きます。



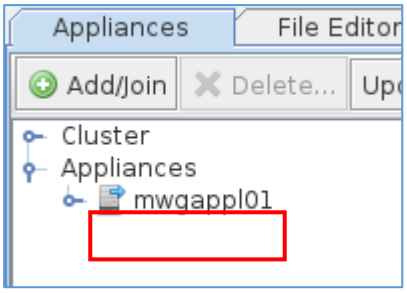
mwgappl02 を選択して、Delete をクリックします。



確認のダイアログウィンドウが表示されますので、Yes をクリックします。



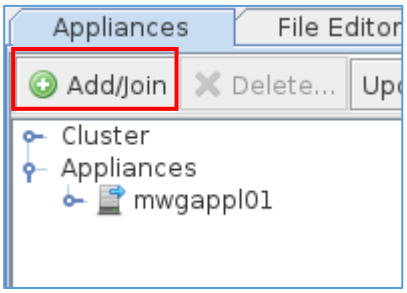
mwgappl02 が削除されます。



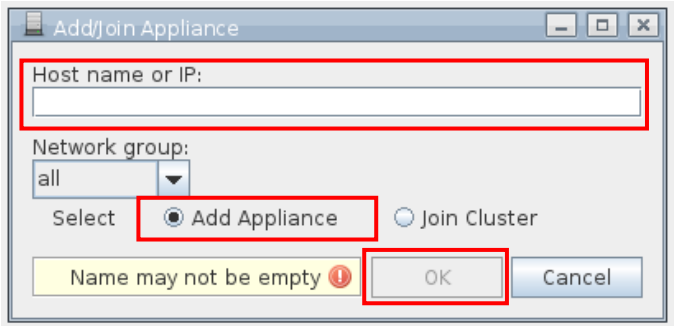
✧ Central Management を有効にする手順

1 号機にログインして、2 号機を追加します。

mwgappl01 の WebUI にログインして、 Configuration > Appliances タブを開きます。
Add/Join をクリックします。

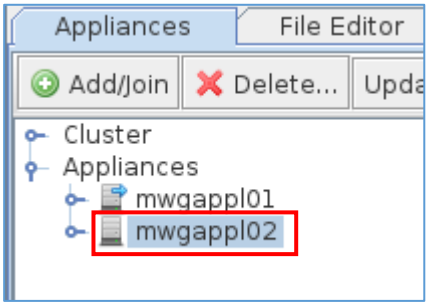


Add/Join Appliance ウィンドウで Host name or IP 欄に、mwgappl02 のホスト名または IP アドレスを入力し OK をクリックします。
ログインしている Web Gateway に別のアプライアンスを追加する場合は Select 欄で Add Appliance を選択します。ログインしているアプライアンスを既存のグループに参加させる場合は Join Cluster を選択します。



削除前に登録していたホスト名または IP アドレスが不明な場合は、2 号機の WebUI にログインして、Configuration > Appliances タブ > Central Management を開き、一番上の
IP addresses and ports of this node used for central management communication 欄で確認できます。

2 号機が追加されます。



3.3 HA 構成時、メンバーのアップデート順序と注意事項

3.3.1 メンバーのアップデート順序

HA 構成の場合は、先に 2 号機をアップデートして、その後 1 号機をアップデートします。

2 号機のアップデートが完了すると、1 号機と 2 号機でバージョンが異なる状態になりますが、HA 機能は稼働します。
ただし、v7.x から v8.2 以降へのアップデート時と v12.2.7 以前から v12.2.8 以降へのアップデート時は除きます。

バージョンが異なる HA 構成で運用を継続することは想定されていないため、なるべく早く 1 号機もアップデートしてください。

3.3.2 HA 構成時の HA サービスと OS バージョンについて

Web Gateway の HA サービスには以下の 3 種類があり、それぞれ設定内容が異なります。

OS バージョン	HA サービス	1 号機 Scanners 設定	2 号機 Scanners 設定
v7.x～v8.1.x	MFEND	Scanners 欄なし	Scanners 欄なし
v8.2.x～v12.2.7	HAProxy 1.8.25	1 号機の IP [Peer/Director] 1 号機の IP [Scanner] 2 号機の IP [Peer/Director] 2 号機の IP [Scanner] **※1**	1 号機の IP [Peer/Director] 1 号機の IP [Scanner] 2 号機の IP [Peer/Director] 2 号機の IP [Scanner]
		1 号機の IP [Scanner] 2 号機の IP [Peer/Director] ※2	**1 号機の IP [Peer/Director] 2 号機の IP [Scanner] ※2**
v12.2.8 以降	HAProxy 2.9.3	**1 号機の IP [Scanner] 2 号機の IP [Peer/Director] ※2**	**1 号機の IP [Peer/Director] 2 号機の IP [Scanner] ※2**

※1は従来の SWG アップデート手順書[NCD-MWG-1382]で説明していた Scanners 欄の設定ですが、HAProxy のバージョンが 1.8.25 から 2.9.3 に変わったときの仕様変更によって Peer/Director, Scanner IP アドレスの厳密な指定が要求されるようになったため、そのまま v12.2.8 以降のバージョンにアップデートすると HAProxy がエラーとなり HA サービスが起動しなくなります。
v12.2.8 以降にアップデートする前に**※2**の設定に変更してください。

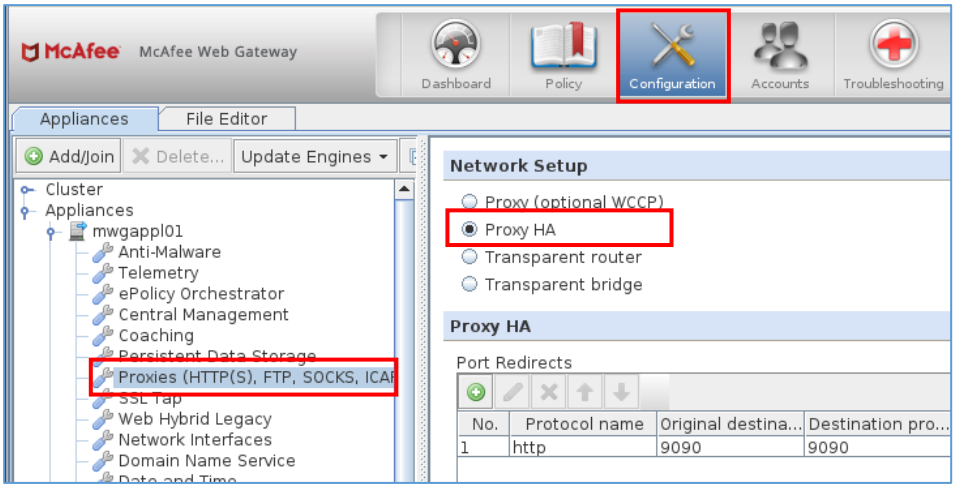
3.3.3　HA 構成時に v7.x から v8.2～v12.2.7 へアップデートしたときの注意事項

v7.x では MFEND(McAfee Network Driver)というカーネルモジュールの機能で HA 構成時の Proxy 機能を実現していましたが、v8.2 以降では HAProxy というテクノロジースタックを使用するように変更されました。
MFEND と HAProxy では設定項目が異なるため、v7.x から v8.2 以降へのアップデート時には ProxyHA の動作に必要な設定変更が必須となりました。

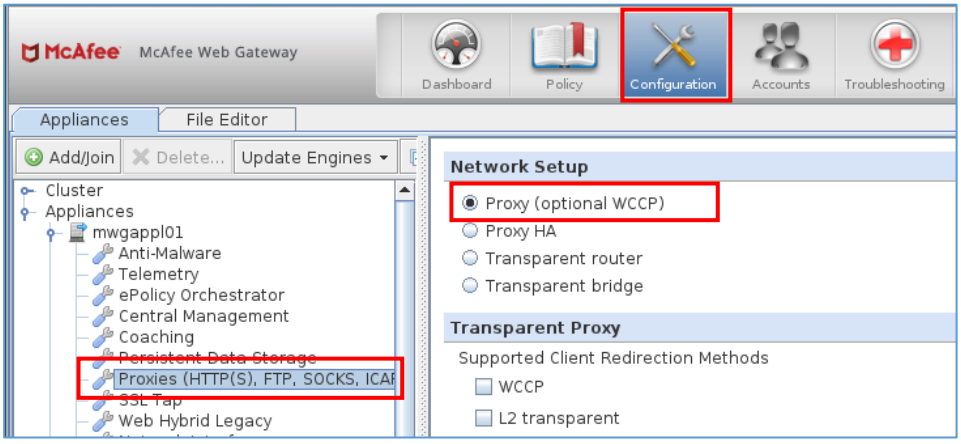
手動で設定変更を行わないときは HA 構成の Proxy 機能は正常に動作しなくなります。そのため、後述の「5.3 HA 構成時に v7.x から v8.2 以降へアップデートする場合の実施手順」を参照の上、設定変更してください。

HA 構成で設定されているかどうかを確認するには、WebUI の Configuration > Appliances タブ > アプライアンス名 > Proxies (HTTP(S), FTP, SOCKS, ICAP..)を開きます。Network Setup で Proxy HA が選択されていれば HA 構成です。(Transparent router/bridge の場合は、弊社サポートにお問い合わせ下さい)

v7.x での HA 構成の場合の設定画面　こちらは v8.2 以降へアップデート後に設定変更が必要です。



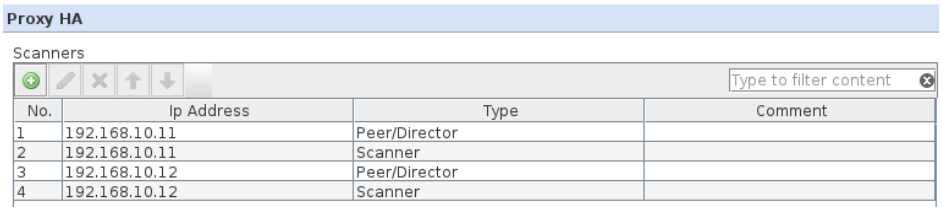
v7.x でのシングル構成の場合の設定画面　こちらは設定変更不要です。



3.3.4 HA 構成時に v8.2.x～v12.2.7 から v12.2.8 以降へのアップデート時の注意事項 1

v8.2.x ～ v12.2.7 までの HA サービスのバージョンと v12.2.8 以降の HA サービスのバージョンが異なります。新バージョンでは仕様変更のためエラーが発生し、HA 機能が動作せず、WebUI で HA 構成の修正が必要となる場合があります。
以下のように 1 号機と 2 号機で Scanners 欄の設定が同じ状態の場合はエラーとなります。

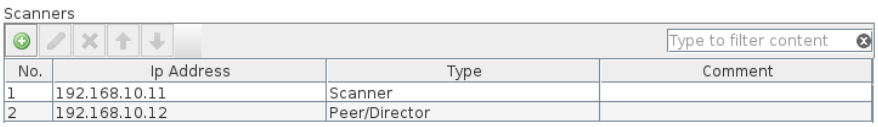
1 号機の IP [Peer/Director]
1 号機の IP [Scanner]
2 号機の IP [Peer/Director]
2 号機の IP [Scanner]



No.	Ip Address	Type	Comment
1	192.168.10.11	Peer/Director	
2	192.168.10.11	Scanner	
3	192.168.10.12	Peer/Director	
4	192.168.10.12	Scanner	

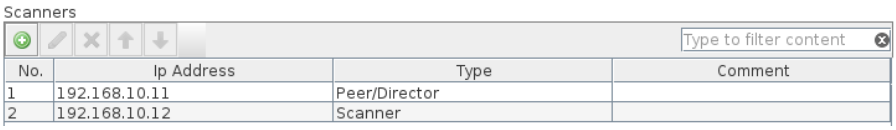
v12.2.8 以降にアップデートする前に HA Scanners の設定を以下のように変更しておくことでエラーの発生は回避できます。

1 号機の Scanners 欄
1 号機の IP [scanner]
2 号機の IP [Peer/Director]



No.	Ip Address	Type	Comment
1	192.168.10.11	Scanner	
2	192.168.10.12	Peer/Director	

2 号機の Scanners 欄
1 号機の IP [Peer/Director]
2 号機の IP [scanner]



No.	Ip Address	Type	Comment
1	192.168.10.11	Peer/Director	
2	192.168.10.12	Scanner	

3.3.5 HA 構成時に v8.2.x～v12.2.7 から v12.2.8 以降へのアップデート時の注意事項 2

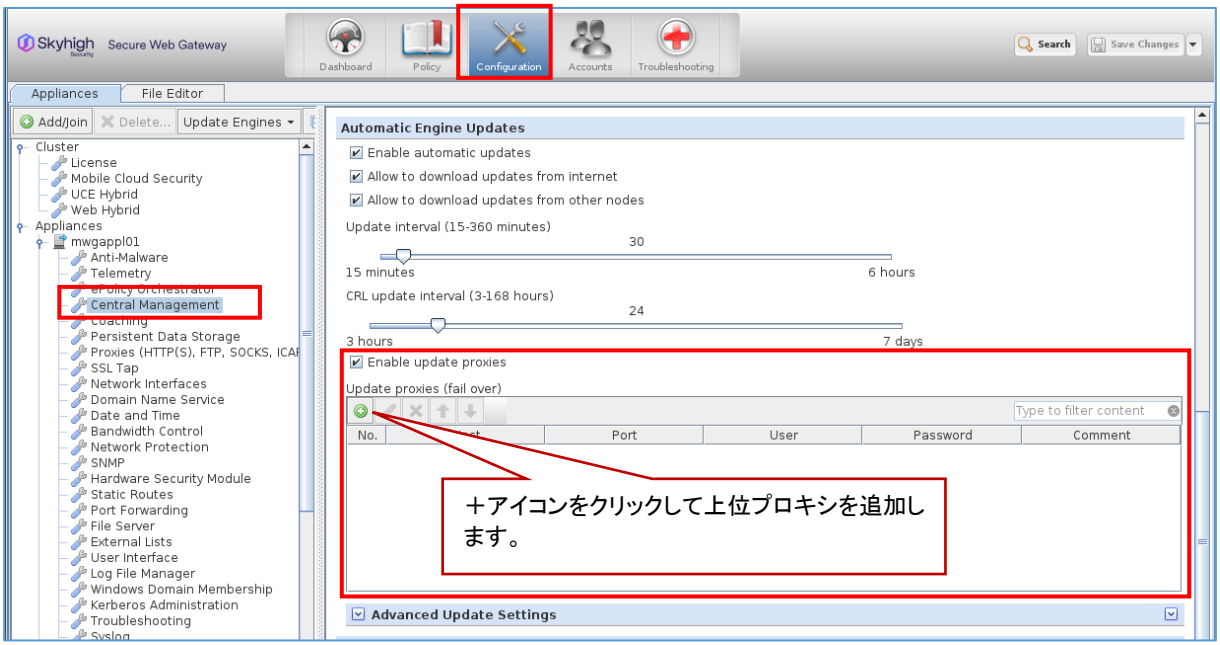
v8.2.x ～ v12.2.7 までの HA サービスのバージョンと v12.2.8 以降の HA サービスのバージョンが異なることにより 1 台目のアップデート完了後から 2 台目のアップデートが完了するまでの期間中は HA サービスが動作しなくなるため、ユーザがプロキシを利用できない時間帯が長く発生します。
運用に影響のない時間帯にアップデートを実施することを推奨します。

3.4 アップデート時のインターネット接続を上位プロキシ経由で実施する場合の注意事項

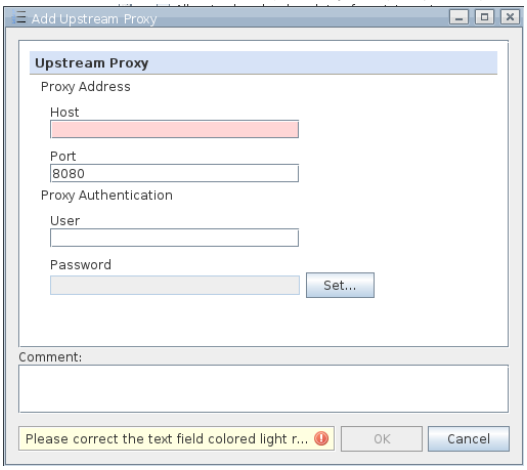
3.4.1 WebUI でアップデートする場合

v7.6.x までのバージョンでは、WebUI でアップデートする場合でも/etc/yum.conf ファイルを手動で修正する必要がありましたが、v7.7.0 以降は以下の WebUI で指定した上位プロキシを使用するように変更されました。

Configuration > Appliances タブ > Central Management を開き Automatic Engine Updates 欄を展開し Enable Update Proxies にチェックをつけて上位プロキシを登録します。



ホスト名または IP アドレス、Port 番号、必要であれば認証情報を入力して OK をクリックします。



3.4.2 CLI でアップデートする場合

CLI でのアップデートを行う場合に上位プロキシを経由する場合は、/etc/yum.conf に上位プロキシサーバの情報を追記する必要があります。

vi /etc/yum.conf でファイルを編集し下記の proxy 行を追加します。

```
proxy = http://proxy.example.com:xxxx
```

ユーザ認証が必要な場合は以下の認証情報も追加します。

```
proxy_username = username
proxy_password = password
```

3.5 MLOS のアップデートを含むバージョンへのアップデートは 2 段階

Web Gateway は OS として、McAfee Linux Operating System (MLOS)を使用しています。これまで MLOS1、MLOS2、MLOS3 とアップデートされています。v7.7 からv7.8 にアップデートするときのように MLOS2 から MLOS3 にアップデートされる場合は、2 段階のアップデートが実行されます。第 1 段階のアップデート終了時に再起動が実行されますが、バックグラウンドで第 2 段階のアップデートが継続して実行されます。

Web Gateway バージョンと MLOS バージョンの対応表

Web Gateway バージョン	MLOS バージョン	第 1 段階アップデート後のバージョン
v7.2 以前	MLOS1	-
v7.3 ～ v7.7	MLOS2	v7.3.2.8
v7.8 以降	MLOS3	v7.8.1.6

3.6 Controlled Release へのアップデート

Main Release から Controlled Release へアップデートする場合には、WebUI によるアップデートを実施する前に、コマンドラインによるリポジトリの更新作業が必要です。

アップデート手順は、アップデート前バージョンとアップデート後バージョンの組み合わせで異なりますので、必ずアップデート後のリリースノートで **Installation instructions** 項をご確認ください。

3.7 v7.8 以降へのアップデート

3.7.1 仮想アプライアンスにおけるゲスト OS 設定

仮想マシンで Web Gateway を利用する場合、v7.8 から仮想マシンのゲスト OS の要件が変更となりました。

・7.7.2.x 以前: **Linux (64 ビット)、バージョン 2.6**
・7.8.2.x 以降: **CentOS (64 ビット)、バージョン 7**

仮想基盤でゲスト OS の対応が可能であるかをご確認ください。ゲスト OS とバージョンを変更する手順は「5.2.1 仮想アプライアンスにおけるゲスト OS 設定」をご参照ください。

3.7.2 シリアルポート速度設定

シリアルポート速度は Web Gateway ではデフォルト値 19200 となっており、UPS(9600)の制限に合わせるためシリアルポート速度を 9600 へ変更しているケースがあります。
v7.7 以前のシリアルポート速度設定は引き継がれません。そのため、後述の通り「5.2.2 シリアルポート転送速度変更」を参照の上、シリアルポート速度を変更して下さい。

4 アップデート実施

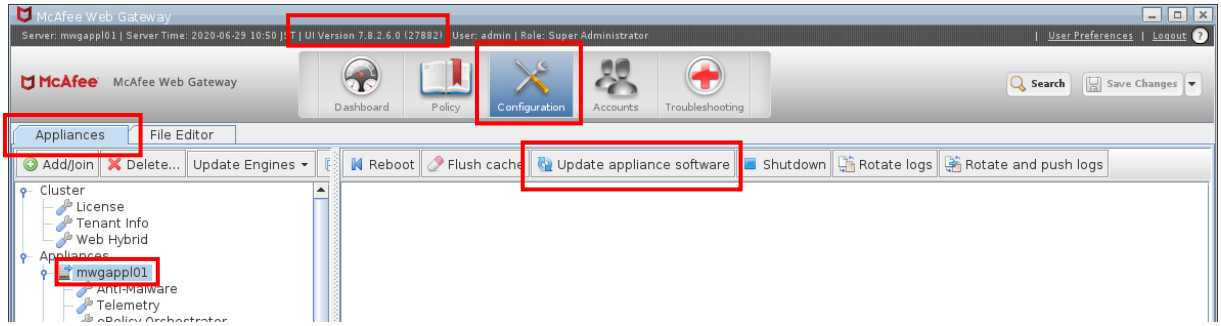
4.1 WebUI によるアプライアンスのアップデート実施

Web ブラウザで以下の URL にアクセスしてログインします。

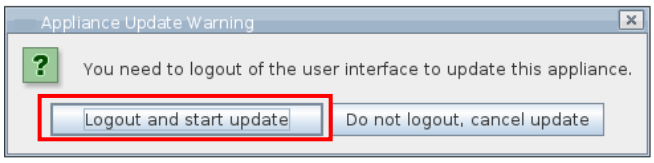
https://Web Gateway の IP アドレス:4712/

トップレベルメニューバーの Configuration をクリックし、 Appliances タブを選択して、対象の Web Gateway 名(下記の例では mwgappl01)をクリックします。

次に、右側に表示されるアプライアンスツールバーの Update appliance software をクリックします。最新バージョンへのアップデートが開始されます。

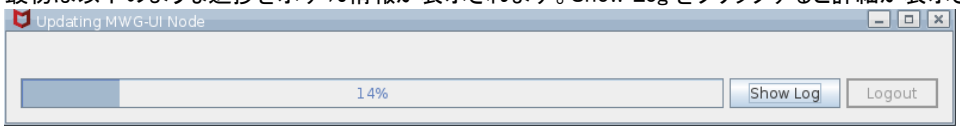


以下のように、アプライアンスをアップデートするためにはログアウトする必要がある旨のメッセージが表示されますので、Logout and start update をクリックします。アップデートを中止する場合は、Do not logout, cancel update をクリックします。

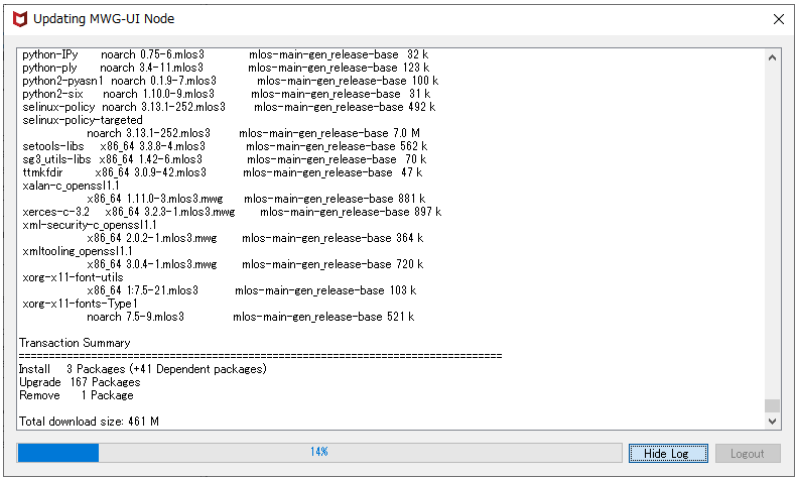


ログアウトが行われ、アップデートの進捗状況を示す画面に切替ります。

最初は以下のような進捗を示す%情報が表示されます。Show Log をクリックすると詳細が表示されます。



下記画面のように、14%等一定のパーセンテージの状態が数十分続く場合がありますが、バックグラウンドでダウンロードを実施中であり停止しているわけではありません。バージョンのアップデート幅が大きいほどダウンロードするパッケージのサイズが大きくなるため時間がかかる傾向があります。

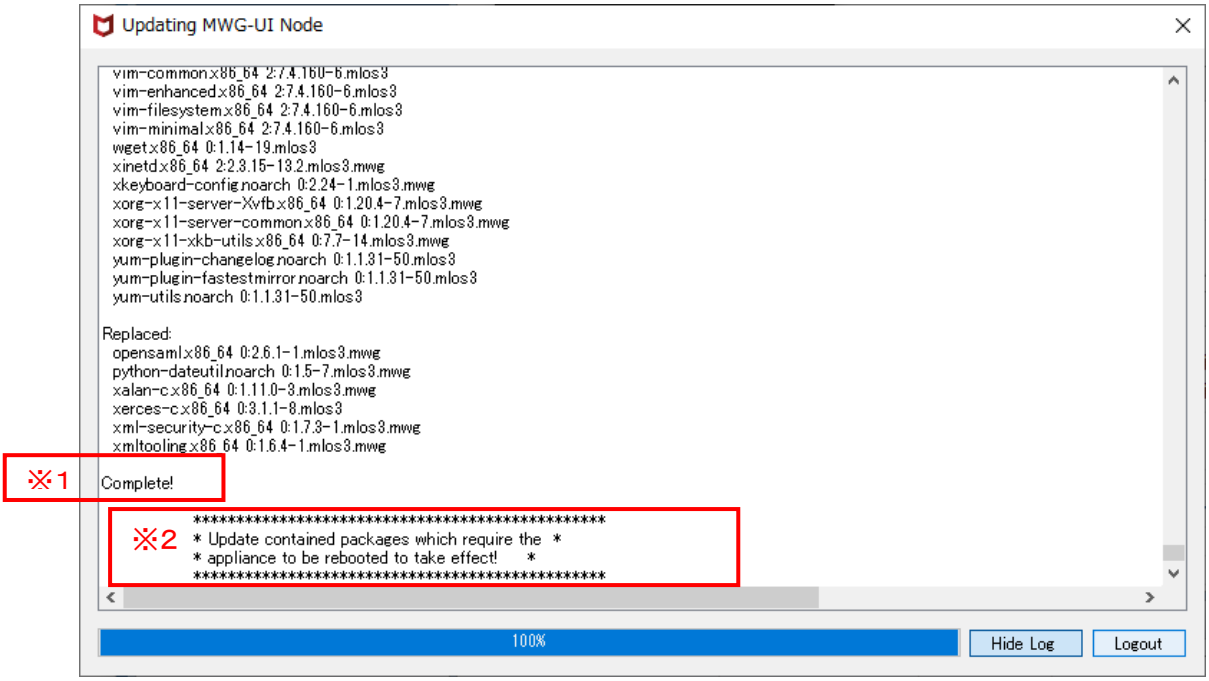


アップデート中も可能な限りサービスを継続しますが、ダウンロード終了後に各サービスの再起動が行われる期間はサービスが停止します。
WebUI サービスが再起動されるときは下記のように一時的に WebUI への表示ができないというメッセージが表示されます。

```
Please wait. The UI service is temporarily unavailable. Connection Status: invalid status code:500
```

WebUI サービスが起動されるとアップデート状態表示が復旧します。もしも、WebUI が復旧しない場合は CLI で/opt/mwg/log/update/sysconfd.update.log ファイルを参照してください。
tail -f コマンドでファイルの末尾に書き込まれた情報をリアルタイム表示します。

```
tail -f /opt/mwg/log/update/sysconfd.update.log
```



進捗表示が 100%になったらログアウト後に再度ログインしてバージョンが最新となっていることを確認してください。

上記画面※1のように Complete! が表示されていない場合は、バックグラウンドでアップデートが継続している場合があります。そのときは、ローカルコンソールまたは、SSH でアプライアンスにログインして、以下のログファイルに、Compete! と記録されるまで待ってください。

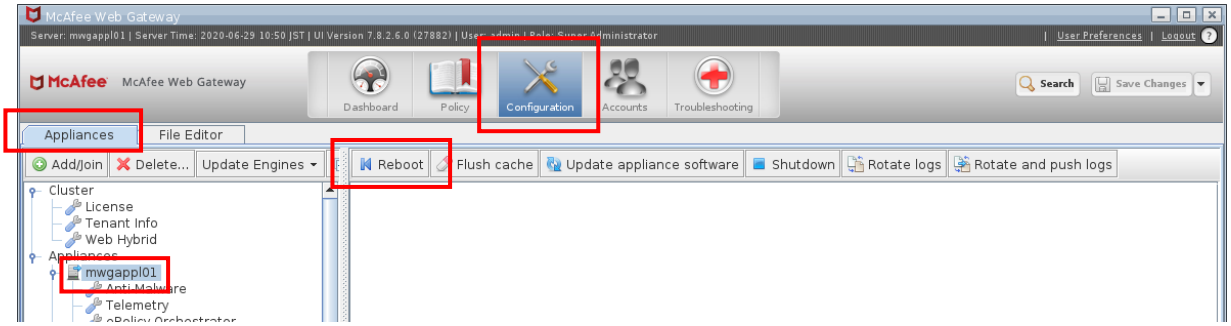
```
/opt/mwg/log/update/sysconfd.update.log
```

※2「Update contained packages which require the appliance to be rebooted to take effect!」メッセージが表示された場合には、アプライアンスの再起動が必要なパッケージが含まれていますので、再度ログイン後、「4.2 アプライアンスの再起動実施」の手順に従って、アプライアンスの再起動を実施してください。

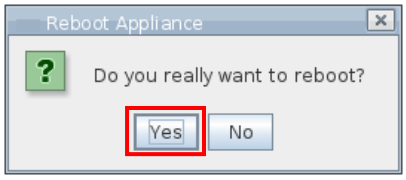
ただし、Controlled Release へのアップデートの場合は、「Update contained packages which require the appliance to be rebooted to take effect!」メッセージが表示されない場合でもアプライアンスを再起動する必要があります。

4.2 アプライアンスの再起動実施

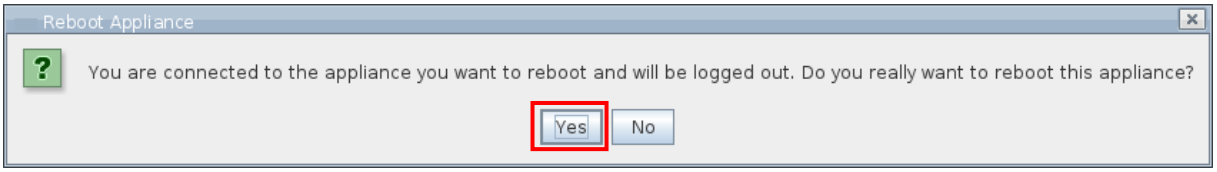
WebUI でアプライアンスを再起動するには、トップレベルメニューバーの Configuration をクリックし、Appliances タブを選択して、対象の Web Gateway 名(下記の例では mwgappl01)をクリックします。
次に、右側に表示されるアプライアンスツールバーの Reboot をクリックします。



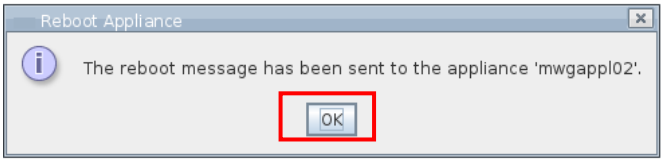
リブート実施の確認画面が表示されます。Yes をクリックします。



WebUI にログイン中のアプライアンスを再起動しようとしている場合は、確認の画面が表示されます。Yes をクリックします。



Central Management 機能を有効にしており、WebUI にログイン中のアプライアンス以外を再起動した場合は上記の確認画面は表示されず、以下のリブートメッセージが通知された画面が表示されます。OK をクリックします。



以上でアップデートは完了です。

4.3 CLI によるアプライアンスのアップデート実施手順

Main Release の最新版以外の特定バージョンにアップデートするときやオフラインアップデートを行うときには CLI のコマンドを使用します。

4.3.1 特定バージョンへのアップデート実施手順

Main Release の最新バージョン以外へのアップデートを行うときには CLI コマンドの mwg-switch-repo -sticky〈特定バージョン〉を実行後に、yum upgrade を実行します。

v7.7.2.15 から v7.8.2.17 へアップデートするときの実行例で説明します。MLOS2 から MLOS3 へのアップデートも含まれるため 2 段階アップデートとなります。

A) mwg-switch-repo -l コマンドで現在の設定を確認します。

```
mwg-switch-repo -l
```

現在の Main Release 最新版にアップデートされる場合は、Non-sticky のあとに main や現在のバージョン情報が表示されます。

```
[root@mwgappl01 ~]# mwg-switch-repo -l
Current Configuration: Non-sticky MWG main (release)
```

```
[root@mwgappl01 ~]# mwg-switch-repo -l
Current Configuration: Non-sticky MWG 7.7.2.15 (release)
```

特定バージョンに固定されている場合は Sticky のあとにバージョンが表示されます。

```
[root@mwgappl01 ~]# mwg-switch-repo -l
Current Configuration: Sticky MWG 7.8.2.17 (release)
```

B)　mwg-switch-repo --sticky <バージョン>コマンドでアップデート後のバージョンを指定します。

```
[root@mwgappl01 ~]# mwg-switch-repo --sticky 7.8.2.17
Creating repository configuration for Sticky MWG 7.8.2.17 (release)
Testing connectivity to repository. This may take a while.
Repository configuration has been updated.
Now run "yum upgrade yum && yum upgrade" to perform the actual upgrade.
[root@mwgappl01 ~]#
```

C)　yum upgrade コマンドでアップデートを開始します。

```
[root@mwgappl01 ~]# yum upgrade
Loaded plugins: changelog, fastestmirror
Loading mirror speeds from cached hostfile
 * mlos-7.8.2.17-gen_release-base: appliance2.webwasher.com
mlos-7.8.2.17-gen_release-base/x86_64/signature          |  833 B     00:00
mlos-7.8.2.17-gen_release-base/x86_64/signature          | 1.3 kB     00:00

途中省略

               x86_64 7.7-12.mlos2.mwg     mlos-7.8.2.17-gen_release-base  97 k

Transaction Summary
================================================================================
Install      33 Package(s)
Upgrade      25 Package(s)

Total download size: 277 M
Is this ok [y/N]:
```

ダウンロード可否確認では y [Enter]を入力します。
このあとインターネット上のメーカーサーバよりアップデートファイルをダウンロードします。

```
Downloading Packages:
(1/58): daemonize-1.7.3-1.mlos2.x86_64.rpm               |  18 kB     00:00
(2/58): dejavu-fonts-common-2.33-1.mlos2.mwg.noarch.rpm  |  62 kB     00:00

途中省略

  python-urlgrabber.noarch 0:3.9.1-11.mlos2
  xinetd.x86_64 2:2.3.14-41.mlos2

Replaced:
  yum-plugin-downloadonly.noarch 0:1.1.30-10.mlos2

Complete!
[root@mwgappl01 ~]#
```

D)　Complete! の表示後、コマンドプロンプトに戻ったあとに reboot を実行します。

```
[root@mwgappl01 ~]# reboot
```

再起動が終了すると 7.8.1.6 で起動します。

E)　再起動後に SSH でログインし、もう一度 yum upgrade を実行します。

```
[root@mwgappl01 ~]# yum upgrade
**************************************
        Starting MLOS3 Upgrade
```

```
Installed package versions:
'mlos3-upgrade': 1.2.3-1.mlos2.mwg
'mwg':           7.8.1.6.0-26087.mlos2.mwg

Commencing major appliance OS upgrade.
Service will be unavailable for the
duration of the upgrade. Appliance will
reboot automatically after upgrade is
complete. Upgrade process will create
a configuration backup at
  /opt/mwg-mlos3upgrade.backup

During upgrade UI update progress will
be unavailable for some time. If UI
does not reconnect after 60 Minutes
please login to appliance via console
or ssh and inspect upgrade log at
  /opt/mwg/log/update/mlos3.upgrade.log

Will update to
sticky 7.8.2.17 version (release)

Do you want to proceed? ([y]es/[n]o)
**************************************
```

実行確認では y を入力します。

```
Upgrade in progress, please wait ...

########################################
#                                      #
#     The download and installation    #
#     of the packages may take a       #
#     considerable length of time.     #
#                                      #
#  !!!  DO NOT CANCEL THIS PROCESS  !!! #
#                                      #
########################################

Installing intermediate packages ...

Downloading MLOS3 packages list to /var/cache/yum/x86_64/3.5 ... (551 MiB)
  - Download DONE.
Installing MLOS3 packages ...
Upgrading to sticky 7.8.2.17 version (release) ...

----------------------------------
MLOS3-Upgrade successfully done.

Backupfile: /opt/mwg-mlos3upgrade.backup
Logfile:    /opt/mwg/log/update/mlos3.upgrade.log
**********************************************
        MLOS3 Upgrade is rebooting your machine now!

        If machine does not reboot automatically
        within the next few minutes try to login
        on console and execute 'reboot -f'.

        If you cannot access command line
        perform a power cycle.

        * Trigger automatic reboot *
**********************************************
Rebooting system after 30 seconds. (Abort with [ctrl-c])
```

アップデート終了の 30 秒後に自動的に再起動が実行されます。

F) 次回のアップデート時に Main Release の最新版にアップデートするように設定を戻す場合は、mwg-switch-repo main コマンドを実行します。

```
[root@mwgappl01 ~]# mwg-switch-repo main
Creating repository configuration for Non-sticky MWG main (release)
Testing connectivity to repository. This may take a while.
Repository configuration has been updated.
Now run "yum upgrade yum && yum upgrade" to perform the actual upgrade.
[root@mwgappl01 ~]#
```

4.3.2 オフラインによるアップデート実施手順

v7.7.2 からの新機能として、iso ファイルからのオフラインアップデートが行えるようになりました。

注意事項

v7.7 から v7.8 以降へのアップデートのように MLOS のアップデートを含むバージョンへのアップデートではオフラインアップデートは実行できません。

A) 適用したいバージョンの ISO ファイルを SCP などで Web Gateway に転送します。
B) iso ファイルを保存したディレクトリに移動し、mwg-update -o <ファイル名>コマンドを実行します。

v7.8.2.6 から v7.8.2.17 にアップデートしたときの実行例を示します。

```
mwgappl-7.8.2.17.0-31544.x86_64.iso ファイルを McAfee 社サイトからダウンロードして
SCP でアプライアンスにコピーします。
SSH でログイン後、/tmp 以下に mwgappl-7.8.2.17.0-31544.x86_64.iso をコピーしておき
mwg-update -o <iso ファイル名>を実行します。

[root@mwgappl01 tmp]# cd /tmp
[root@mwgappl01 tmp]# mwg-update -o mwgappl-7.8.2.17.0-31544.x86_64.iso
  Preparing files...

  Creating repository...
  ************************************************
  Ready to update the current version
  mwg-7.8.2.6.0-27882.mlos3.mwg.x86_64 using the file
  mwgappl-7.8.2.17.0-31544.x86_64.iso
  ************************************************
Do you want to proceed? ([y]es/[n]o)

[y]を入力

アップデートが開始されるので、完了するまで待ちます。
※進行状況も表示されます

  途中省略
  yum-plugin-fastestmirror.noarch 0:1.1.31-50.mlos3
  yum-utils.noarch 0:1.1.31-50.mlos3

Complete!

Current version: mwg-7.8.2.17.0-31544.mlos3.mwg.x86_64
[root@mwgappl01 tmp]#

Complete!と表示されればバージョンアップ完了です。

Web Gateway を再起動し、GUI にログインしてバージョンアップされていることを確認します。
[root@mwgappl01 tmp]# reboot

再起動後に iso ファイルを削除します。
[root@mwgappl01 ~]# rm /tmp/mwgappl-7.8.2.17.0-31544.x86_64.iso
```

5 アップデート実施後の注意事項と作業手順

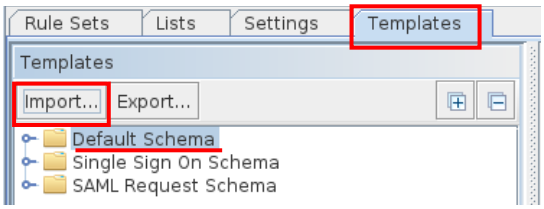
5.1 Language Pack について

過去バージョンの Language Pack でアラートのテンプレートを日本語化している場合は、過去バージョンで使用していたテンプレートは日本語化されますが、新バージョンで新規に追加された機能のテンプレートは英語となります。必要であれば新バージョン用の Language Pack を Content & Cloud Security Portal サイトよりダウンロードして適用してください。

Web Gateway 7 Language Packs download サイト
https://contentsecurity.skyhigh.cloud/software_mwg7_language
※Content & Cloud Security Portal サイトのご利用には、Web Gateway ご購入時に発行される専用の ID・パスワードが必要です。

適用手順は以下の通りです。

Policy > Templates > Default Schema を選択し、Import ボタンをクリックします。



Browse ボタンを押して、事前にダウンロードしておいた Language Pack の Zip ファイルを選択し、Import ボタンを押します。
Import が完了すると Import Successfully finished. メッセージが表示されます。
Save Changes をクリックして保存します。

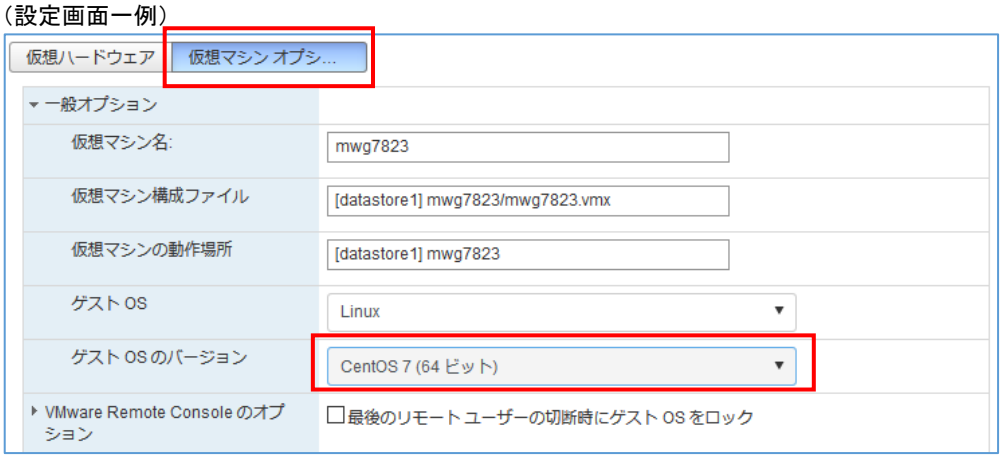
5.2 v7.8 以降へのアップデート

5.2.1 仮想アプライアンスにおけるゲスト OS 設定手順

仮想マシンで Web Gateway を利用する場合、v7.8 から仮想マシンのゲスト OS の要件が変更されました。
・7.7.2.x 以前: **Linux (64 ビット)、バージョン 2.6**
・7.8.2.x 以降: **CentOS (64 ビット)、バージョン 7**
アップデート後は、リリースノートにある「Upgrade from the interface」の通り、ESXi 等仮想の管理画面より、ゲスト OS を変更した後仮想マシンの再起動を実施して下さい。

仮想基盤に合わせて変更して下さい。下記は ESXi 6.5 における設定変更画面の一例です。なお、仮想マシン稼働中は、グレーアウトで変更出来ません。Web Gateway アップデート完了後、Web Gateway をシャットダウンしてから変更して下さい。

（設定画面一例）



5.2.2　シリアルポート転送速度変更手順

v7.7 以前の場合

A) Web Gateway の CLI にログインし、/etc/init に移動します。
B) ttyS0.conf を開き、ファイル中の 19200 を 9600 に変更します。
（デフォルトでは 19200 となっています）

```
exec /sbin/agetty /dev/ttyS0 19200 vt100
↓
exec /sbin/agetty /dev/ttyS0 9600 vt100
```

C) 機器を再起動し変更を反映させます。

v7.8 以降の場合

A) Web Gateway の CLI にログインし、/etc/default に移動します。

```
# cd /etc/default
```

B) ファイル編集前に、ディレクトリ内にある grub を cp コマンド等でコピーし、バックアップを作成します。

```
# cp grub grub.backup20181121
```

C) 下記コマンドにて生成したバックアップファイルが表示されることを確認します。

```
# ls -la
```

D) grub を開き、ファイル中 2 か所ある 19200 を 9600 に変更します。

一箇所目:

```
GRUB_CMDLINE_LINUX="$GRUB_CMDLINE_LINUX console=ttyS0,19200n8 console=tty0"
↓
GRUB_CMDLINE_LINUX="$GRUB_CMDLINE_LINUX console=ttyS0,9600n8 console=tty0"
```

二箇所目:

```
GRUB_SERIAL_COMMAND="serial --speed=19200 --word=8 --parity=no --stop=1"
↓
GRUB_SERIAL_COMMAND="serial --speed=9600 --word=8 --parity=no --stop=1"
```

E) CLI 上で以下のコマンドを実行し、変更を適用します。

```
# /usr/sbin/grub2-mkconfig -o /boot/grub2/grub.cfg
```

F) 下記コマンドを実行し、grub.cfg に設定が適用されていることを確認します。
(適用出来ていない場合は、実行結果が戻りません)

```
# cd /boot/grub2
# grep 9600 grub.cfg
実行例）
serial --speed=9600 --word=8 --parity=no --stop=1
linux16 /boot/vmlinuz-3.18.118-2.mlos2.mwg.x86_64 root=UUID=e2445e0b-ea01-49ce-b62b-
6882230d6de0 ro acpi=on rootfstype=ext4 net.ifnames=0 biosdevname=0 quiet selinux=0
crashkernel=128M elevator=deadline console=ttyS0,9600n8 console=tty0
linux16 /boot/vmlinuz-3.18.118-2.mlos2.mwg.x86_64 root=UUID=e2445e0b-ea01-49ce-b62b-
6882230d6de0 ro acpi=on rootfstype=ext4 net.ifnames=0 biosdevname=0 quiet selinux=0
crashkernel=128M elevator=deadline console=ttyS0,9600n8 console=tty0
```

G) 機器を再起動し変更を反映させます。

H) 再起動後、CLI にて下記コマンドを実行し、9600 への変更を確認します。
(変更出来ていない場合は、実行結果が戻りません)

```
# dmesg | grep 9600
```

実行例）

```
 [ 0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-3.18.118-2.mlos2.mwg.x86_64
root=UUID=e2445e0b-ea01-49ce-b62b-6882230d6de0 ro acpi=on rootfstype=ext4 net.ifnames=0
biosdevname=0 quiet selinux=0 crashkernel=128M elevator=deadline console=ttyS0,9600n8
console=tty0
[ 0.000000] [ffffea0000000000-ffffea00061fffff] PMD -> [ffff8801b9600000-ffff8801be9fffff] on
node 0
[ 0.000000] Kernel command line: BOOT_IMAGE=/boot/vmlinuz-3.18.118-2.mlos2.mwg.x86_64
root=UUID=e2445e0b-ea01-49ce-b62b-6882230d6de0 ro acpi=on rootfstype=ext4 net.ifnames=0
biosdevname=0 quiet selinux=0 crashkernel=128M elevator=deadline console=ttyS0,9600n8
console=tty0
```

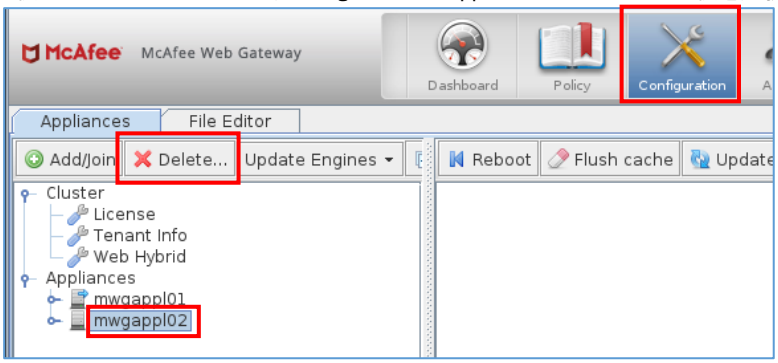
5.3 HA 構成時に v7.x から v8.2 以降へアップデートする場合の実施手順

v8.2 では、HA 構成時の Peer/Director, Scanner IP アドレスの厳密な指定が要求されるよう仕様変更が行われました。
Peer/Director, Scanner IP アドレスが正しく設定されていない場合、v7.x から v8.2 以降へアップデート後、設定を正しく修正するまで Proxy 経由の通信が停止します。復旧のための修正実施手順を以下に示します。

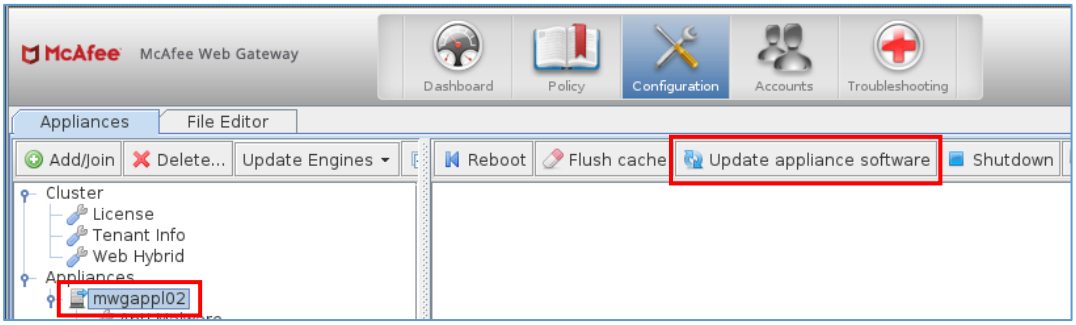
※v7.8.2.6 から v9.2.2 へのアップデートを例に説明します。

A) アップデートを実行する前に設定バックアップを取得します。

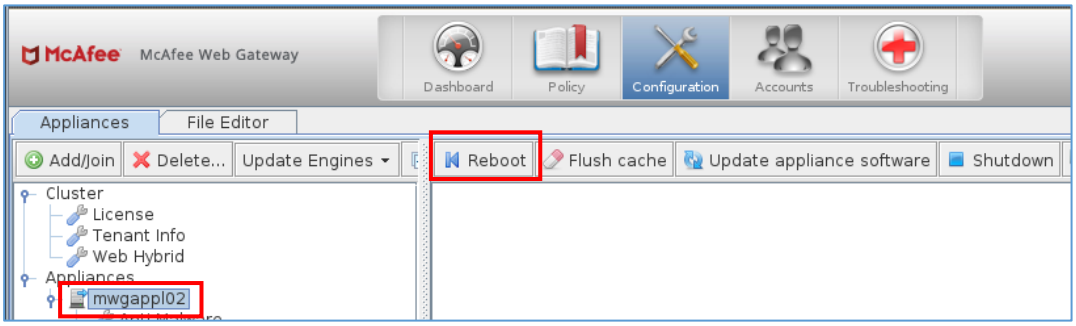
B) Central Management を有効にしている場合は、一旦無効にします。
1 号機の WebUI にログイン後、Configuration > Appliances タブから 2 号機を選択し、Delete をクリックします。



C) 先に 2 号機をアップデートします。
2 号機の WebUI にログインして、2 号機をアップデートします。
Configuration > Appliances タブで、2 号機を選択して、Update appliance software をクリックします。



D) 2 号機のアップデート後は 2 号機を手動で再起動する必要があります。
WebUI の場合は、Configuration > Appliances タブで、2 号機を選択して、Reboot をクリックします。

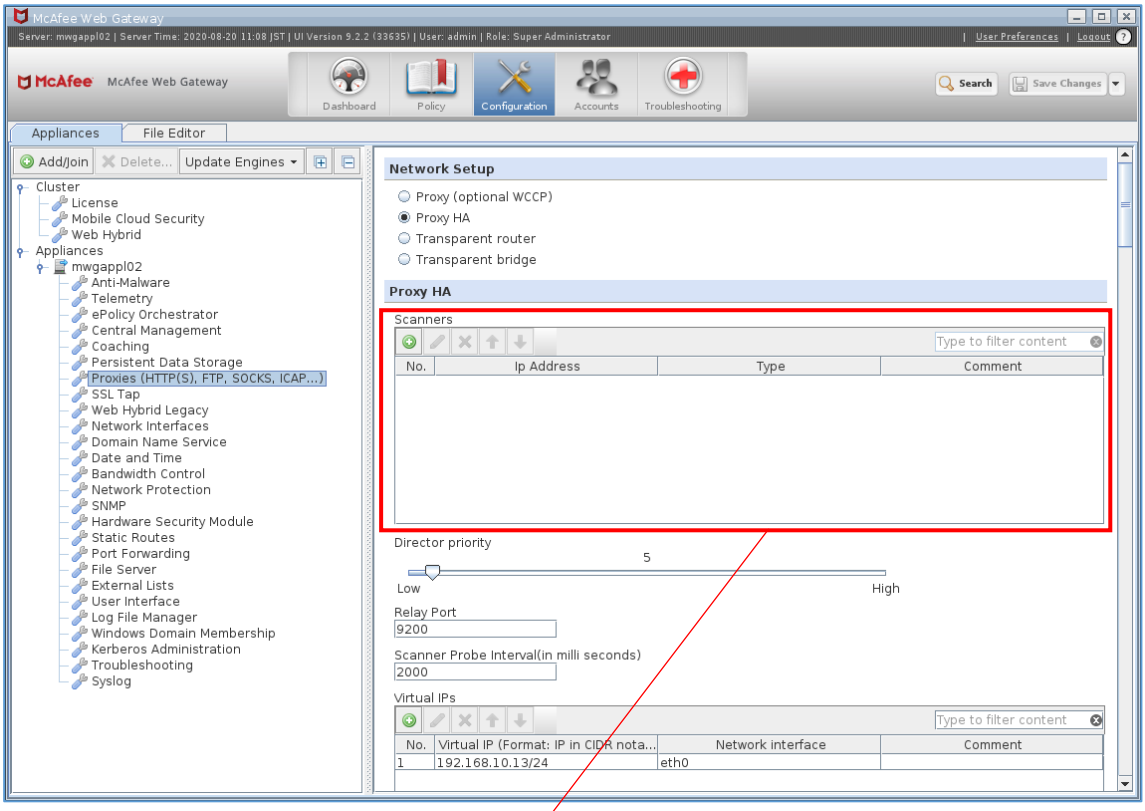


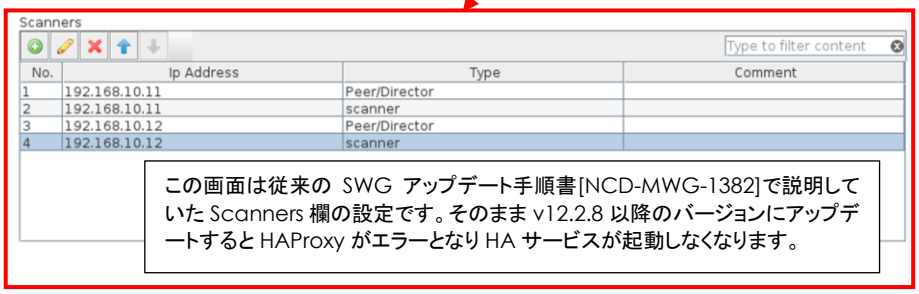
2 号機が起動しても HA 構成に必要な設定が行われていない状態です。この時点では VIP への Proxy 通信は 1 号機側で処理されるため通信断は発生しません。

E)　2 号機の HA 構成の設定を変更します。
2 号機の WebUI にログインし Configuration > 2 号機 > Proxies (HTTP(S), FTP, SOCKS, ICAP..)を開きます。

✧　2 号機の変更箇所① Scanners に Peer/Director と Scanner ノードを追加します。

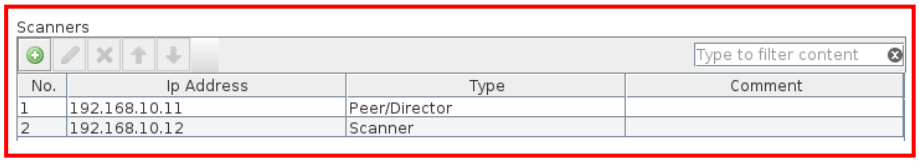
Proxy HA 欄の Scanners のプラスアイコンをクリックし、1 号機の IP アドレスを Peer/Director とし、2 号機の IP アドレスを Scanner として追加します。



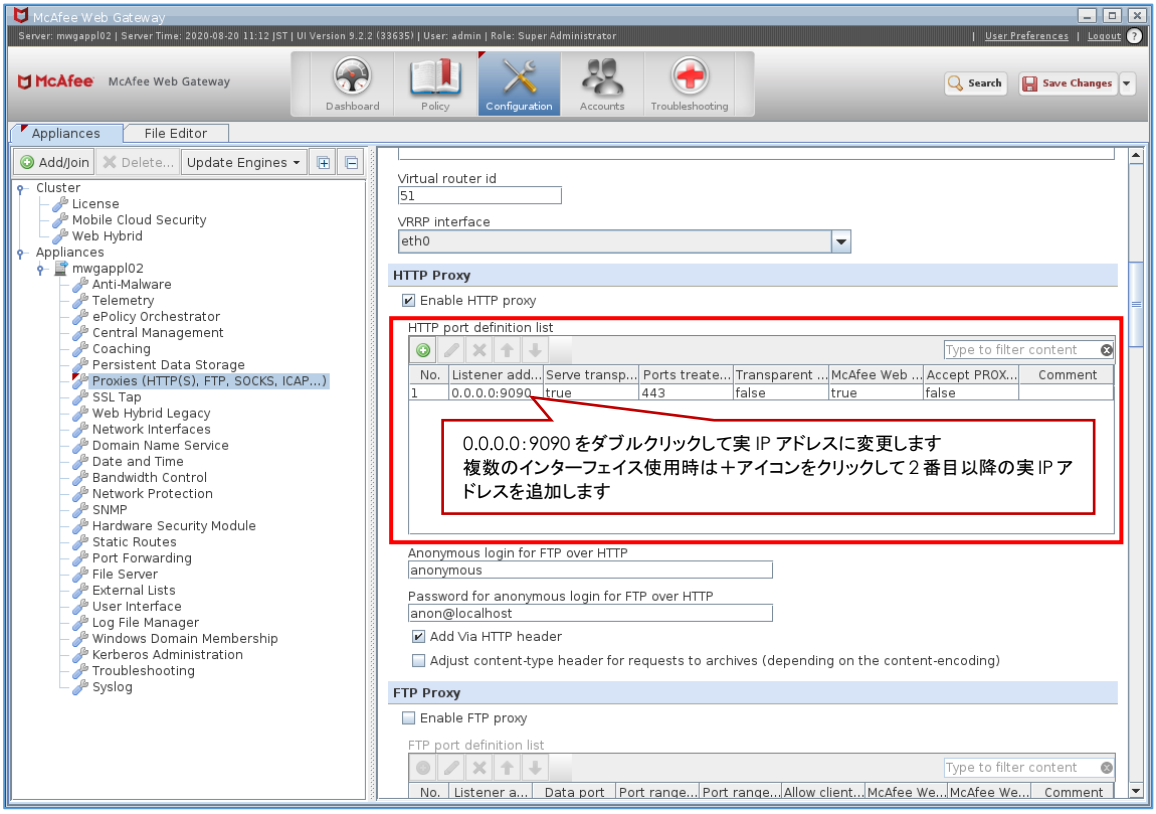


上記は eth0 インターフェイスで下記の実 IP アドレスを使用している場合です。
　1 号機の実 IP アドレス: 192.168.10.11
　2 号機の実 IP アドレス: 192.168.10.12
　仮想 IP アドレス: 192.168.10.13
複数のインターフェイスを使用している場合は、その実 IP アドレスも追加します。

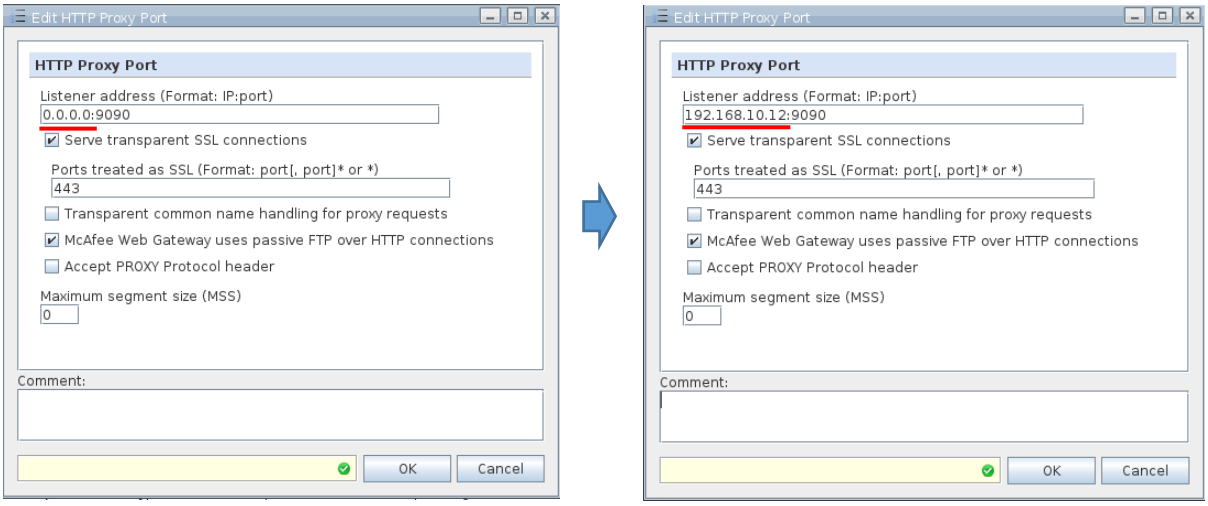
2024/5/30 追加情報
v12.2.8 以降のバージョンでは、HAproxy の仕様変更により上記のように1号機と 2 号機の Scanners が同じ設定の場合はエラーが発生し HA サービスが起動しなくなります。
2 号機の Scanners 欄では以下のように 1 号機の IP アドレスを Peer/Director で登録し、2 号機の IP アドレスを Scanner で登録します。



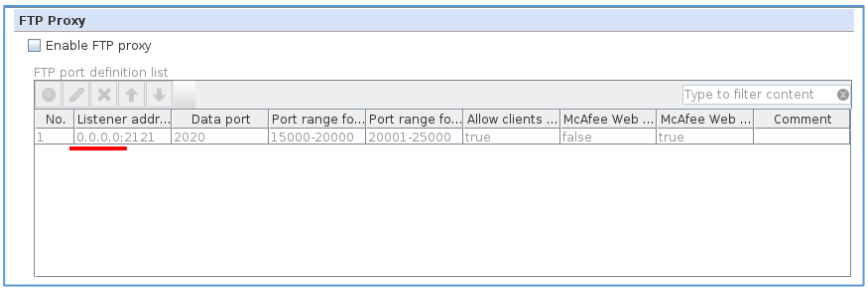
✧ 2 号機の変更箇所② HTTP Proxy の Listener address を修正します。



HTTP Proxy 欄の HTTP port definition list の中で 0.0.0.0 と登録されている Listener address を 2 号機の実 IP アドレスに変更します。

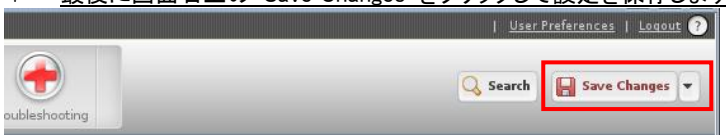


✧ 2 号機の変更箇所③ FTP Proxy を有効にしている場合は、その Listener address を 0.0.0.0 から 2 号機の実 IP アドレスに変更します。



その他、 ICAP Server, SOCKS Proxy, TCP Proxy などを使用している場合は Listener address を実 IP アドレスに変更します。

✧ 最後に画面右上の Save Changes をクリックして設定を保存します。

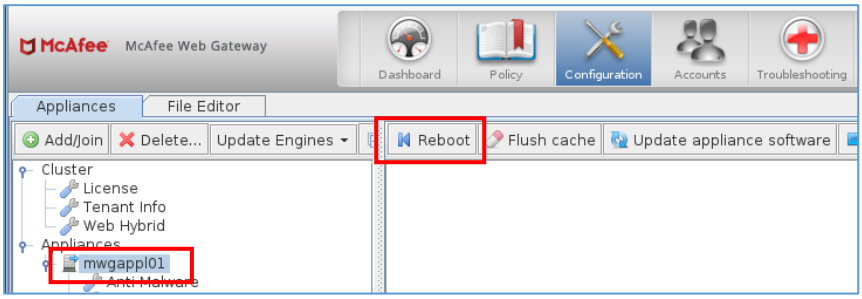


変更箇所①、②、③以外は v7.x の設定を引き継ぐため設定を変更する必要はありません。

以上で 2 号機の HA 構成設定は完了しています。

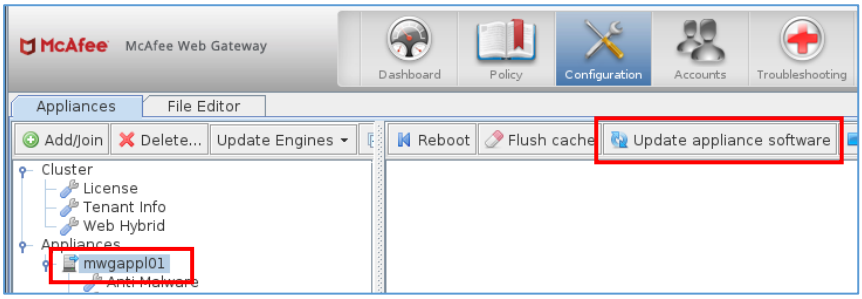
この時点では 1 号機のみで Proxy 処理を行っていますが、このまま 1 号機をアップデートすると 1 号機のアップデート途中でサービス停止→再開時に少し長めの Proxy 通信断が発生するため、1 号機のアップデートを開始する前のタイミングで 1 号機をリブートして 2 号機に Proxy 処理を切り替えておきます。

F) 1 号機の WebUI にログインして、1 号機をリブートします。
Configuration > Appliances タブで、1 号機を選択して、Reboot をクリックします。

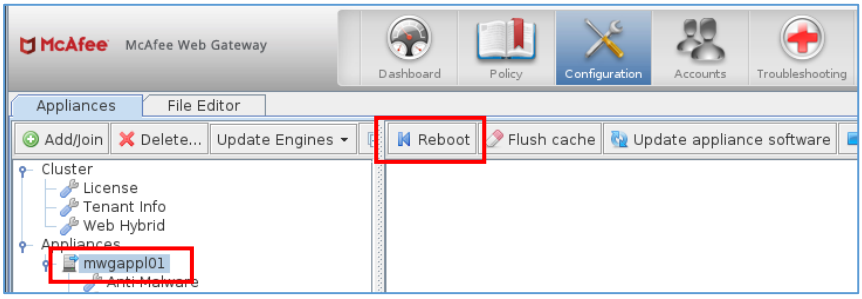


2 号機の下記アクセスログを参照して 2 号機が Proxy 処理を行っていることを確認します。
/opt/mwg/log/user-defined-logs/access.log/access.log

G) 1 号機のアップデートを実施します。
1 号機の WebUI にログインして、1 号機をアップデートします。
Configuration > Appliances タブで、1 号機を選択して、Update appliance software をクリックします。



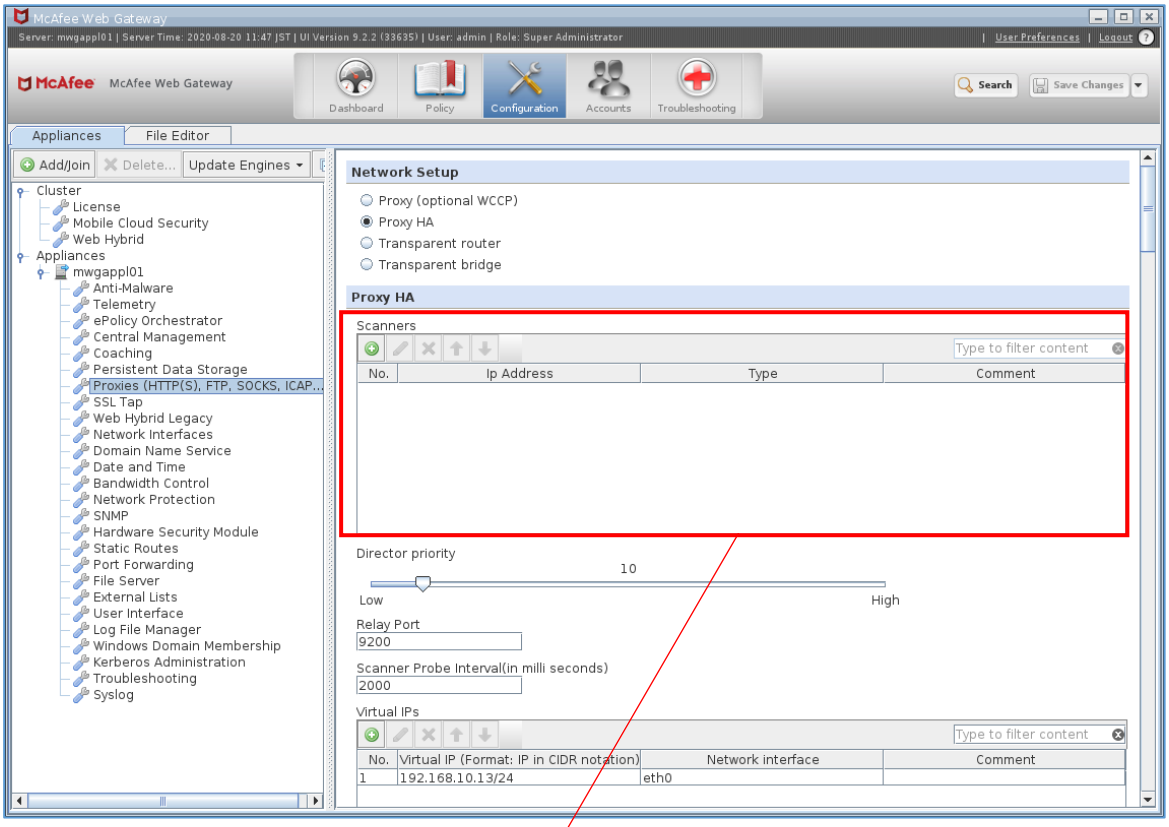
H) 1 号機のアップデート後は 1 号機を手動で再起動する必要があります。
WebUI の場合は、Configuration > Appliances タブで、1 号機を選択して、Reboot をクリックします。

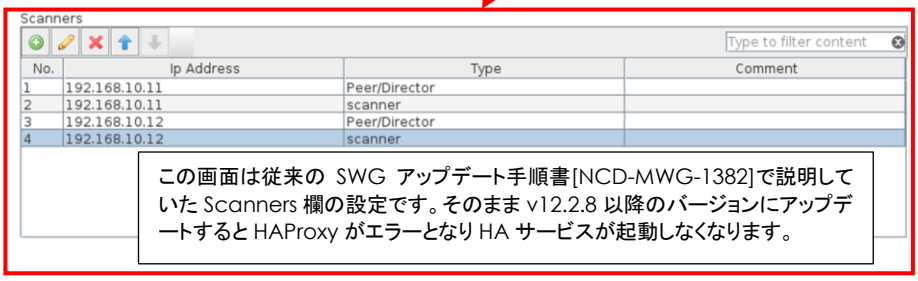


I)　1 号機の HA 構成の設定を変更します。

✧　<u>1 号機の設定変更箇所①　Scanners　に Peer/Director と Scanner ノードを追加します。</u>

Proxy HA 欄の　Scanners のプラスアイコンをクリックし、1 号機の IP アドレスを Scanner とし、2 号機の IP アドレスを　Peer/Director として追加します。





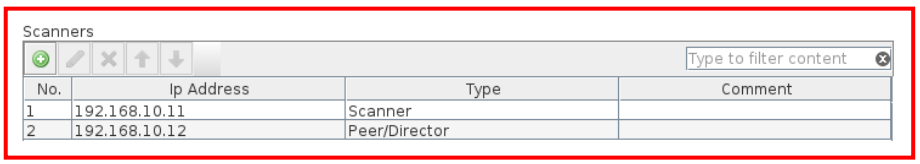
~~Scanners 欄は 2 号機と同じ設定となります~~。

複数のインターフェイスを使用している場合は、その実 IP アドレスも追加します。

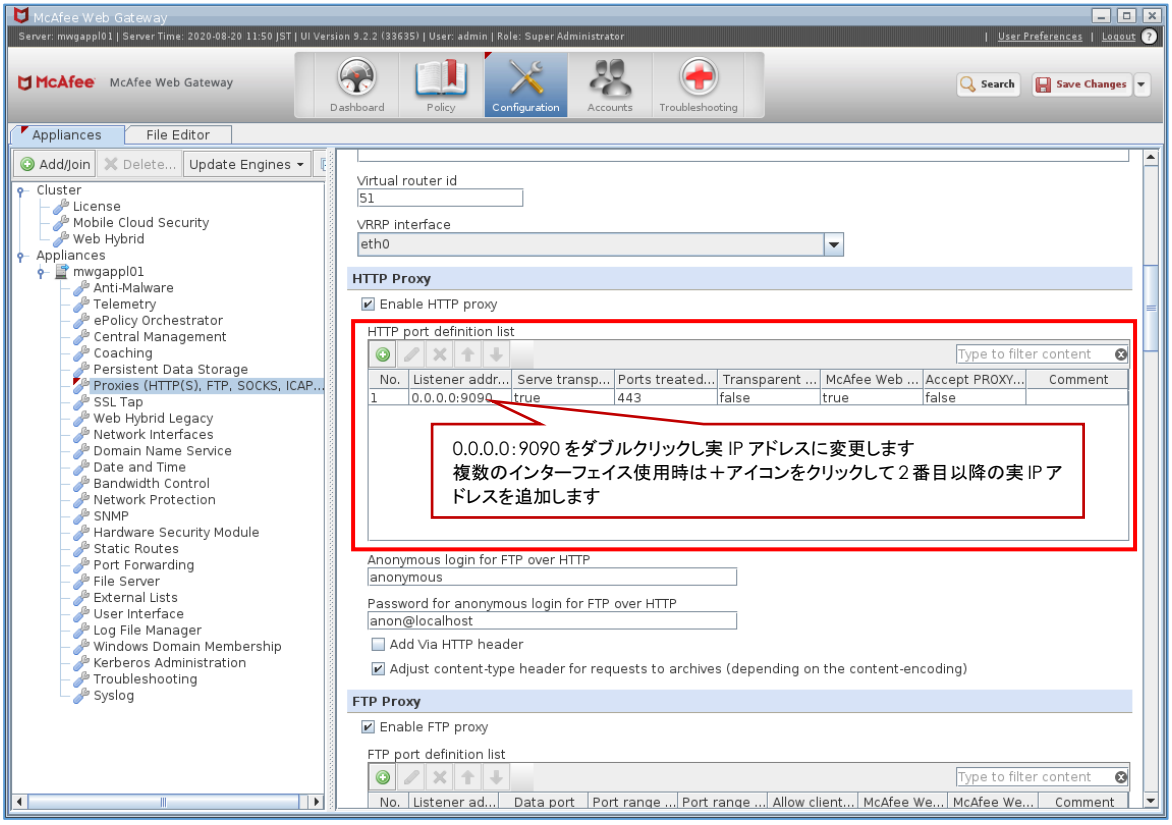
2024/5/27 追加情報

v12.2.8　以降のバージョンでは、HAproxy の仕様変更により上記のように1号機と 2 号機の Scanners が同じ設定の場合はエラーが発生し HA サービスが起動しなくなります。

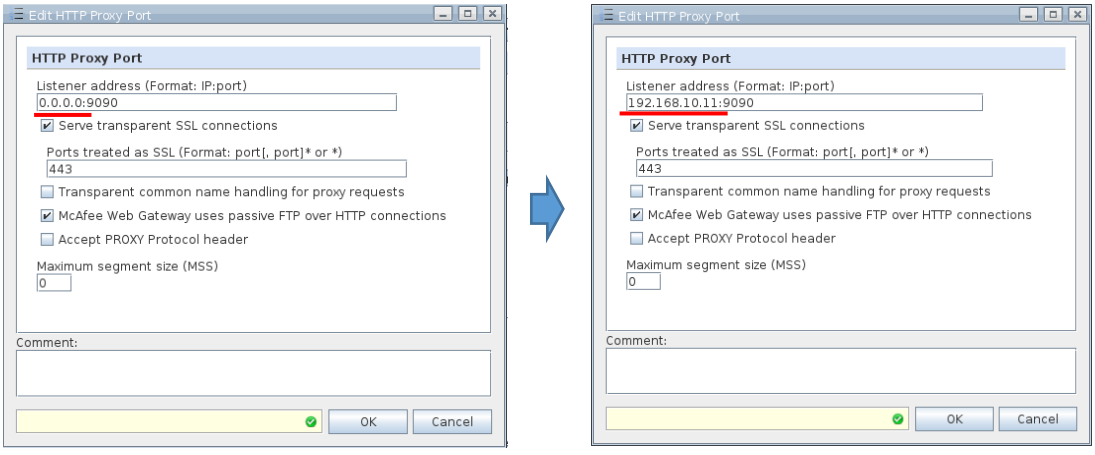
1 号機の Scanners 欄では以下のように　1 号機の IP アドレスを　Scanner　で登録し、2 号機の IP アドレスを　Peer/Director　で登録します。



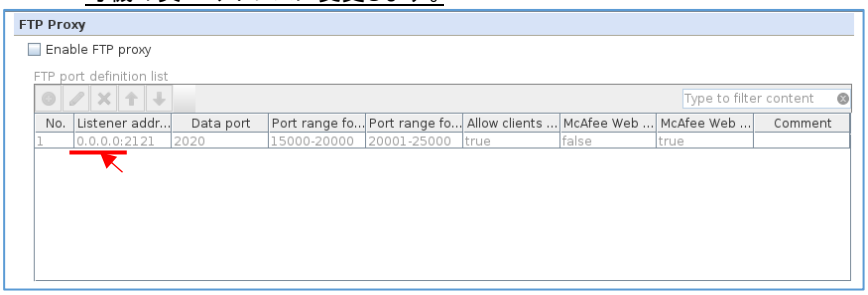
✧ 1 号機の変更箇所② HTTP Proxy の Listener address を修正します。



HTTP Proxy 欄の HTTP port definition list の中で 0.0.0.0 と登録されている Listener address を 1 号機の実 IP アドレスに変更します。

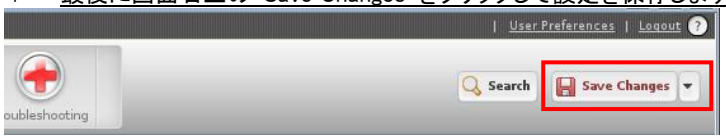


✧ 1 号機の変更箇所③ FTP Proxy を有効にしている場合は、その Listener address を 0.0.0.0 から 1 号機の実 IP アドレスに変更します。



その他、 ICAP Server, SOCKS Proxy, TCP Proxy などを使用している場合は Listener address を実 IP アドレスに変更します。

✧ 最後に画面右上の Save Changes をクリックして設定を保存します。



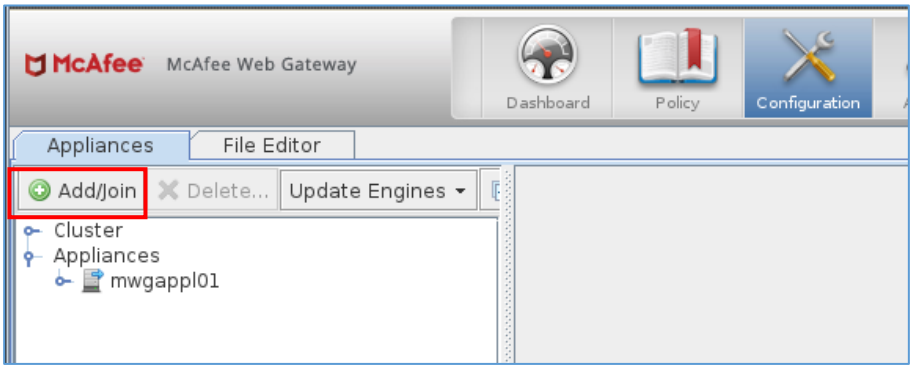
変更箇所①、②、③以外は v7.x の設定を引き継ぐため設定を変更する必要はありません。

J) Central Management を使用する場合は有効にします。

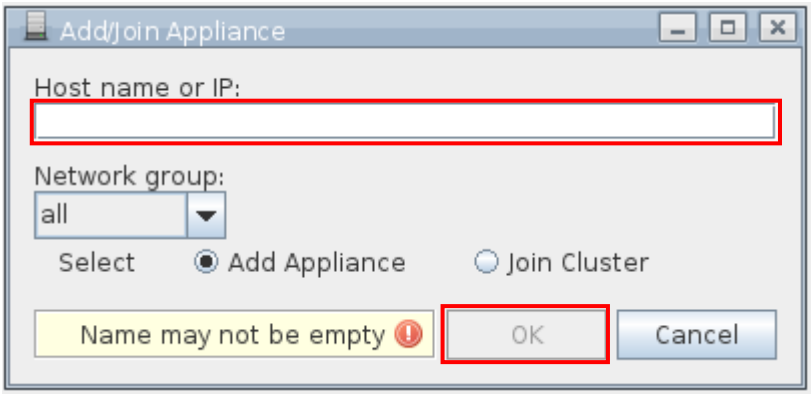
✧ Central Management を有効に戻す場合は、2 号機を追加します。

2 号機の WebUI にログインしている場合はログアウトしておきます。

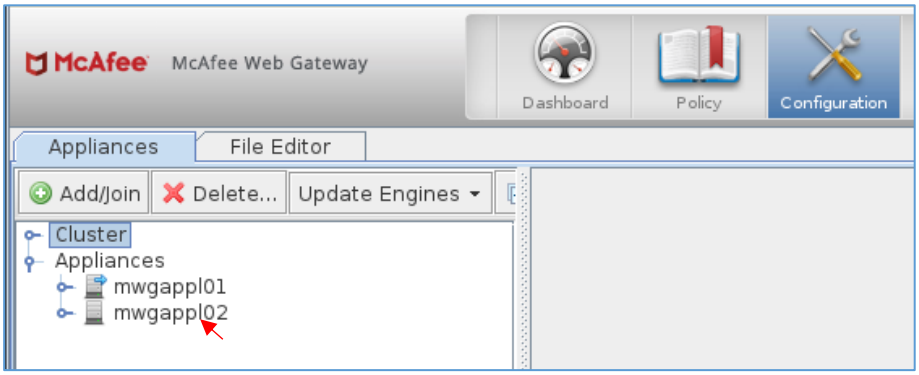
1 号機の WebUI にログインして Configuration > Appliances タブで、Add/join をクリックします。



2 号機の IP アドレスを入力して OK をクリックします。



2 号機が表示されます。



以上で HA 構成のアップデートは終了です。

K) アップデート完了後の設定バックアップを取得します。