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		3
	1.1	本書	『の目的	3
	1.2	ブラ	シド名の変更について	3
	1.3	旧ド	メイン名の利用停止について	3
2	アッ	ヮ゚゚゚゚゚゚゚゙゙	ートパッケージについて	4
	2.1	We	b Gateway \mathcal{OP} ילדי-רוכסויל	4
	2.2	バー	-ジョン情報確認方法	4
3	アッ	゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚゚ゔゔゔ゚゚゚゚゚゚	ート前の注意事項	5
	3.1	設定	ミバックアップの取得	5
	3.2	Cei	ntral Management 機能有効時の注意事項	5
	3.3	ΗA	構成時、メンバーのアップデート順序と注意事項	7
	3.3	.1	メンバーのアップデート順序	7
	3.3	.2	HA 構成時の HA サービスと OS バージョンについて	8
	3.3	.3	HA 構成時に v7.x から v8.2~v12.2.7 ヘアップデートしたときの注意事項	9
	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 11	0
	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 21	0
	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1	1
	3.4	.1	WebUIでアップデートする場合1	1
	3.4	.2	CLIでアップデートする場合1	1
	3.5	ML	OS 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	2
	3.6	Coi	ntrolled Release へのアップデート1	2
	3.7	v7.8	8 以降へのアップデート1	2
	3.7	.1	仮想アプライアンスにおけるゲスト OS 設定1	2
	3.7	.2	シリアルポート速度設定 1	2
4	アッ	ヮ゚゚゚゚゚゚゙゙゙	一卜実施1	3
	4.1	We	bUIによるアプライアンスのアップデート実施1	3
	4.2	アプ	プライアンスの再起動実施1	4
	4.3	CLI	によるアプライアンスのアップデート実施手順1	5
	4.3	.1	特定バージョンへのアップデート実施手順1	5
	4.3	.2	オフラインによるアップデート実施手順1	8
5	アッ	ヮ゚゚゚゚゚゚゙゙゙	ート実施後の注意事項と作業手順1	9
	5.1	Lan	nguage Pack について1	9
	5.2	v7.8	8 以降へのアップデート1	9
	5.2	.1	仮想アプライアンスにおけるゲスト OS 設定手順1	9
	5.2	.2	シリアルポート転送速度変更手順	0
	5.3	ΗA	構成時に v7.x から v8.2 以降ヘアップデートする場合の実施手順2	2

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、<u>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</u>。 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 <u>Content & Cloud Security Portal</u> <u>サイト</u>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 <u>Content & Cloud Security Portal サイト</u> (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。

Skyhigh Secure Web Gateway	D ashboard	Policy	Configuration				
Appliances File Editor	Appliances File Editor						
Ο Add/Join 🗶 Delete Update Engines 👻 👔							
← Cluster ← Appliances ← mwgappl01 ← mwgappl02							

- 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。

Skyhigh Secure Web G	D ashboard	Policy	Configuration	
Appliances File Edit	tor			
Add/Join X Delete Cluster Appliances	⇒青色の矢印は、V ており mwgappl0	WebUI にログインし 1 にログインしている	ている Web Go る状態です。	ateway を示し
- mwgappl01			· ·	
∽ 🗍 mwgappl02	mwgappl01とm 能が有効に設定され	wgappl02の2台 れている状態です	rで CentralMa	inagement 機

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。

Delete Appliance					
? Delete the selected appliance?					
Yes No					

mwgappl02 が削除されます。

Appliance	s	F	ile E	ditor
🗿 Add/Join	×	Dele	te	Up
⊶ Cluster ⊶ Appliance ⊷ 🖹 mw	gapi	ol01		

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。

📕 Add/Join	Appliance	_ 🗆 🗙				
Host name or IP:						
Network group:						
Select	Select 💿 Add Appliance 🔾 Join Cluster					
Name	may not be empty 🕕	OK Cancel				

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

たたと、(1.2.2.5) (1.2.2.5) (1.4.5) (1.2.2.5) (1.2.2.5) (1.2.2.5) (1.4.5) (1.2.2.5) (1.4.5) (1.2.2.5) (1.4.5) (1.2.2.5) (1.4.5) (1.2.2.5) (1.4.5) (1.2.2.5) (1.4.5) (1.2.2.5) (1.4.5) (1.2.2.5) (1.4.5) (1.2.2.5) (1.4.5) (1.2.2.5) (1.4.5) (1.2.2.5) (1.4.5) (1.4.5) (1.2.2.5) (1.4.5)

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

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

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。

※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 ヘ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 「<u>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</u>」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。



0

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]

Proxy HA

Scanners Type to filter content						
No.	Ip Address	Туре	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]					
Scann	ers				
0	♥ ✓ ★ Type to filter cont				
No.	Ip Address	Туре	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]

Scanners								
0	✓ ★ ↓ Type to filter content							
No.	Ip Address	Туре	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。

Skyhigh Secure Web Gateway	Schoard Policy Policy Accounts Troubleshooting	🔍 Search 🔛 Save Changes 🔻
Appliances File Editor		
🔾 Add/Join 🗶 Delete Update Engines 🗸 🕻	Automatic Engine Updates	
← Cluster	Enable automatic updates	
- A Mobile Cloud Security	Allow to download updates from internet	
UCE Hybrid	Allow to download updates from other nodes	
• Appliances	Update interval (15-360 minutes)	
• ≦ mwgappl01	30	
- Anti-Maiware	15 minutes 6 hours	
Central Management	CRL update interval (3-168 hours) 24	
— 🎤 Persistent Data Storage 👘	3 hours 7 days	
- Join Proxies (HTTP(S), FTP, SOCKS, ICAP - Joint SSL Tap	☑ Enable update proxies	
- Antwork Interfaces	Update proxies (fail over)	
- Pote and Time	$O < X \uparrow \downarrow$	Type to filter content 🛛 🔵 🗕
— 🌽 Bandwidth Control	No. Port User Password	Comment
– 🥜 Network Protection		
- P SNMP		
- A Static Routes		
— 🌽 Port Forwarding 🛛 🛁	+アイコンをクリックして上位プロキシを追加し	
- 🌽 File Server	±+	
– J [®] External Lists	\$ Y 0	
- Jog File Manager		
- 🌽 Windows Domain Membership		
- 🌽 Kerberos Administration	X Advanced Undate Settings	
- Investige - Inve	Mavanceu opuace Settings	

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。

Proxy Address		
Port		
8080		
Proxy Authentication		
User		
Password		
	Set.	
the second second		

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 ヘ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「<u>5.2.2 シリアルポート転</u> 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。

💆 McAfee Web Gateway			X
Server: mwgappl01 Server Time: 2020-06-29 10:50 J			<u>User Preferences</u> <u>Logout</u> 🥑
McAfee Web Gateway	Dashboard Policy Config	Accounts	G Search Save Changes V
Appliances File Editor			
Addijoin X Delete Update Engines Cluster Cluster Cluster Cluster Cluster Telenation Appliances Anti-Maiware Telenetry Repliance Orchestereter	I I Reboot Flush cache	强 Update appliance software	🖀 Shutdown 🚰 Rotate logs 😤 Rotate and push logs

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。

Арр	liance Update Warning	×
?	You need to logout of the use	er interface to update this appliance.
	Logout and start update	Do not logout, cancel update

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。



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。

×

M	Undating	MWG-UI Node	
	oputing	PIWO-OI NOUC	

• • •
when The means 0.75 for least when we represent the set of the
python-iry hoarch 0./s=0.mios3 mios-main-gen_release-base 32 k
pyrton-piy noarch 3,4-11.mioso mios-main-gen_release-base 123 K
pyrion2-pyrisin roarch 0.1.3-7 miles mile-main-gen_release-base 100 k
pyrion2=six noarch 1:00-3 mios miosmain-gen_release-base 31 k
semina-puncy nuarch s.is.i=202.muss mis-main-gen_release-base 432 k
serinux-policy-targeted
noarch 3.13.1-292.mios3 mios-main-gen_release-base / U M
secons-libs x80_04 3.3.8-4.mlos3 mlos-main-gen_release-base 002 k
sga utilis-libs x88.04 1.42-0.mlos3 mlos-main-gen_release-base /0 k
ttmistoir x00_04.3.0.3*42.mios3 mios*main*gen_release*base 47.K
Xalan=c_openssil.i
x80_04 I.I.I.J. mios. mios. mainten release Dase 881 K
xerces-c-s.2 xou_04 s.z.s-1.mius.s.mwg mius-main-gerjelease-base ss/ k
xmm=securitym_perission
xou_u4 2.0.2 fi.miuso.mwg mius-main-geri_release-base 504 k
xmituoining openssii.i
varges 11 factor i the
ves 64 125-21 mion - mion-main-gen release-bace 102 k
vargevillefonter Tural
post i forta rippot
Transaction Summary
Install 6 rackages (**) beperivent packages/
upgraue to ranaes
nemove i rackage
Total download size: 461 M
Inder download size: Yo'r In
14% Hide Log

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

	Updating MWG-UI Node	×
	vim-common:x8b_64_27.4.160+6.mlos3 vim-enhanced:x86_64_27.4.160+6.mlos3 vim-minal:x86_64_27.4.160+6.mlos3 vim-minal:x86_64_27.4.160+6.mlos3 weet:x86_64_02.1.14+19.mlos3 xinetd:x86_64_22.3.15+132.mlos3.mwg xkeyboard-coorfig:noarch_02.24+1.mlos3.mwg xorg=x11-server-common:x86_64_01.20.4+7.mlos3.mwg xorg=x11-server-common:x86_64_01.20.4+7.mlos3.mwg xorg=x11-server-common:x86_64_01.20.4+7.mlos3.mwg xorg=x11-server-common:x86_64_01.20.4+7.mlos3.mwg xorg=x11-server-common:x86_64_01.20.4+7.mlos3.mwg xorg=x11-server-common:x86_64_01.20.4+7.mlos3.mwg xorg=x11-server-common:x86_64_01.20.4+7.mlos3.mwg yum-plugin-chaseledignoarch_01.1.31+50.mlos3 yum-plugin-chasetsmirror.noarch_01.1.31+50.mlos3 yum-utils.noarch_01.1.31+50.mlos3 yum-utils.noarch_01.1.31+50.mlos3 yum-utils.noarch_01.1.31+50.mlos3 yum-utils.noarch_01.1.31+50.mlos3 xalance:x86_64_02.6.1+1.mlos3.mwg xarces=c:x86_64_03.1.1+8.mlos3 xml=security=c:x86_64_01.7.3+1.mlos3.mwg xmltooling:x86_64_01.7.4+1.mlos3.mwg	^
XI	Complete!	
	**************************************	~
		>
	100% Hide Log Lo	gout

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<mark>※1</mark>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。

NCD-MWG-1388

🔽 McAfee Web Gateway Server: mwgappl01 Server Time: 2020-06-29 10:50 JST UJ Version 7.8.2.6.0 (27882) User Admin 19Alex Ginese Administrator <u>User Preferences</u> <u>Logout</u> 🕑
McAfee Web Gateway Dashboard Policy Dashboard Policy Configuration Troubleshooting
Appliances File Editor
Add/join X Delete Update Engines Fush cache Plush cache

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。

Rebo	ot Appliance 📃 🎴	K
?	Do you really want to reboot?	
	Yes No	

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。

	poot Appliance
?	You are connected to the appliance you want to reboot and will be logged out. Do you really want to reboot this appliance?
	Yes No

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

	9 0	
		oot Appliance 🛛 🗙
	i	The reboot message has been sent to the appliance 'mwgappl02'.
l		

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 ヘ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@mwgapp101 ~]# mwg-switch-repo -l
Current Configuration: Non-sticky MWG main (release)

```
[root@mwgapp101 ~]# mwg-switch-repo -1
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@mwgapp101 ~]# mwg-switch-repo -1
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@mwgapp101 ~]# 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@mwgapp101~]#
C) yum upgrade コマンドでアップデートを開始します。
[root@mwgapp101 ~]# 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
                                          | 1.3 kB
mlos-7.8.2.17-gen_release-base/x86_64/signature
                                                    00:00
涂中省略
           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@mwgapp101 ~]#
    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。
D)
[root@mwgapp101 ~]# reboot
再起動が終了すると 7.8.1.6 で起動します。
    再起動後に SSH でログインし、もう一度 yum upgrade を実行します。
E)
[root@mwgapp101 ~]# 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 <code>/var/cache/yum/x86_64/3.5</code> ... (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@mwgapp101 ~]# 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@mwgapp101 ~]#

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。

```
mwgapp1-7.8.2.17.0-31544.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 mwgapp1-7.8.2.17.0-31544.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@mwgapp101 tmp]# cd /tmp
[root@mwgapp101 tmp]# mwg-update -o mwgapp1-7.8.2.17.0-31544.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
 mwgapp1-7.8.2.17.0-31544.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@mwgapp101 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@mwgapp101 tmp]# reboot
再起動後に iso ファイルを削除します。
[root@mwgapp101 ~] # rm /tmp/mwgapp1-7.8.2.17.0-31544.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

 $\underline{https://contentsecurity.skyhigh.cloud/software_mwg7_language}$

※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。

Rule Sets Lists	Settings	Templates	
Templates			
Import Export		Œ	
 ➡ Default Schema ➡ ➡ Single Sign On Sch ➡ ➡ SAML Request Sch 	iema ema		

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。

仮想ハードウェア 仮想マシンオプシ	
▼ 一般オプション	
仮想マシン名:	mwg7823
仮想マシン構成ファイル	[datastore1] mwg7823/mwg7823.vmx
仮想マシンの動作場所	[datastore1] mwg7823
ゲスト 0S	Linux
ゲスト 0S のバージョン	CentOS 7 (64 ビット)
▶ VMware Remote Consoleのオプ ション	□ 最後のリモート ユーザーの切断時にゲスト OS をロック

(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"

 $d(d)_{3}(d)_{3$

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

 $[\ 0.\ 000000]$ [ffffea00000000-ffffea00061ffff] PMD \rightarrow [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。

McAfee McAfee Web Gateway	ſ	(And And And And And And And And And And	Policy	Config	X juration	Accounts	Troubleshootin	g	
Appliances File Editor									
📀 Add/Join 🗙 Delete Update Engines	- [📕 Reboo	ot 🧷 Flush	cache	🔂 Up	date appliar	nce software	🔳 Shutdowr	1
Cluster License Protect Info Web Hybrid Appliances Protect Info Immogapp102									

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。

McAfee Web Gateway	D	ashboard	Policy	Configure	ation Acc	Bounts	Troubleshooting	
Appliances File Editor			•					
🗿 Add/Join 🗙 Delete Update Engines	•	📕 Reboot	🧷 Flush	cache 🎙	🎍 Update a	applian	ce software	Shutdown
Cluster License Protection for the former of			_					

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。

◆ <u>2</u>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。

🗸 McAfee Web Gateway							
		<u>User Preferences</u> <u>Loqout</u> ?					
McAfee McAfee Web Gateway	Policy Configuration Accounts	Save Changes 💌					
Appliances File Editor							
Addjoin Piete Update Engines • • • Cluster Mobile Cloud Security • Web Hybrid • Appliances • Anti-Malware • Policy Orchestrator • Central Management • Caching • Persistent Data Storage • Provises (HTTP(S), FTP, SOCKS, ICAP) • Storage • Domain Name Service • Dota and Time • Bandwidth Control • Network Protection • SNMP • Hardware Security Module • Static Routes • Port Forwarding </td <td>Network Setup Proxy (optional WCCP) Proxy HA Transparent router Transparent bridge Proxy HA Scanners No. Ip Address Director priority 5 Low Relay Port 9200 Scanner Probe Interval(in milli seconds) Z000 Virtual IPs No. Virtual IP (Format: IP in CIDR nota 1 192.168.10.13/24</td> <td>Type to filter content Type Comment</td>	Network Setup Proxy (optional WCCP) Proxy HA Transparent router Transparent bridge Proxy HA Scanners No. Ip Address Director priority 5 Low Relay Port 9200 Scanner Probe Interval(in milli seconds) Z000 Virtual IPs No. Virtual IP (Format: IP in CIDR nota 1 192.168.10.13/24	Type to filter content Type Comment					
Scanners		Type to filter content					
No. In Address	Comment						
1 192.168.10.11	Peer/Director	comment					
2 192.168.10.11	scanner						
3 192.168.10.12	Peer/Director						
4 192.168.10.12 scapper							

この画面は従来の 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。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。

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。

Scanners Image: Scanners Image: Type to filter content							
No.	Ip Address	Туре	Comment				
1	192.168.10.11	Peer/Director					
2	192.168.10.12	Scanner					

◆ <u>2 号機の変更箇所② HTTP Proxy の Listener address を修正します。</u>

McAfee Web Gateway	
Server: mwgappl02 Server Time: 2020-08-20 11:12 JST UI Version 9.2.2	(33635) User: admin Role: Super Administrator <u>User Preferences</u> <u>Logout</u> 🕥
HCAfee McAfee Web Gateway	Policy Policy Configuration Accounts Troubleshooting
Appliances File Editor	
Cluster Cluster Cluster Mobile Cloud Security Web Hybrid Appliances Appliances Anti-Malware	Virtual router id 51 VRRP interface eth0 HTTP Proxy
letemetry evoluty Orchestrator Central Management Coaching Persistent Data Storage Prosises (HTTP(S), FTP, SOCKS, ICAP) SSL Tap Web Hybrid Legacy Web Hybrid Legacy Detrork Interfaces Domain Name Service Date and Time Bandwidth Control Network Protection Network Protection StMP Hardware Security Module Static Routes Port Forwarding	Enable H11P proxy HTTP port definition list No. Listener add Serve transp Ports treate Transparent McAfee Web Accept PROX Comment 1 0.0.0.0:9090 true 443 false true 1 0.0.0.0:9090 をダブルクリックして実 IP アドレスに変更します 複数のインターフェイス使用時は + アイコンをクリックして 2 番目以降の実 IP アドレスを追加します Anonymous login for FTP over HTTP
File Server File Server User Interface Jug File Manager Windows Domain Membership Kerberos Administration Troubleshooting Syslog	anonymous Password for anonymous login for FTP over HTTP anon@localhost Add Via HTTP header Adjust content-type header for requests to archives (depending on the content-encoding) FTP Proxy Enable FTP proxy FTP port definition list Type to filter content No. Listener a Data port Port rangePort rangeAllow clientMcAfee We Comment

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。

🚍 Edit HTTP Proxy Port 📃 🗖 🗙	= Edit	HTTP Proxy Port	_ 🗆 🗙
HTTP Proxy Port	HT	TP Proxy Port	
Listener address (Format: IP:port) 0.0.0.0:9090 Serve transparent SSL connections Ports treated as SSL (Format: port[, port]* or *) 443 Transparent common name handling for proxy requests McAfee Web Gateway uses passive FTP over HTTP connections Accept PROXY Protocol header		tener address (Format: IP:port) 2.168.10.12:9090 Serve transparent SSL connections Ports treated as SSL (Format: port[, port]* or *) 443 Transparent common name handling for proxy requests McAfee Web Gateway uses passive FTP over HTTP connect Accept PR0XY Protocol header	ions
Maximum segment size (MSS)	Ma	aximum segment size (MSS)	
comment:	Comm	ient:	
OK Cancel		ОК	Cancel

そ そ 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。

FT	P Pro	ху							
	Enable FTP proxy								
	FTP po	ort definition list							
	0	/ X 🕇 🕂						Type to filter	content 🔞
	No.	Listener addr	Data port	Port range fo	Port range fo	Allow clients	McAfee Web	McAfee Web	Comment
	1	0.0.0.0:2121	2020	15000-20000	20001-25000	true	false	true	
		0.0.0.0.2121	2020	13000-20000	20001-23000	true	laise	true	

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。
			<u>User F</u>	Preferences Logout ?	
			Q Search	Save Changes	

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。





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。

McAfee McAfee Web Gateway	ſ	(An and a shboard a shboar	Policy	Configuration	Accounts	Troubleshooting
Appliances File Editor						
🔇 Add/Join 🗙 Delete Update Engines 🕶		📕 Reboo	ot 🧷 Flush	cache 强 Up	date appliar	nce software 🛛
Cluster License Tenant Info Web Hybrid Appliances Second Statement Appliances						

- I) 1 号機の HA 構成の設定を変更します。
 - ◆ <u>1</u>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。

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。

Kanger Server: mwgapp101 Server Time: 2020-08-20 11:47 JST UI Versi	on 9.2.2 (33635) User: admin Role: Super Administrator	User Preferences Logout ?
McAfee Web Gateway	ashboard Policy Configuration Accounts Troubleshooting	Save Changes V
Appliances File Editor		
🔾 Add/Join 🗶 Delete Update Engines 👻 🖡	Network Setup	<u>^</u>
	Proxy (optional WCCP) Proxy HA Transparent router Transparent bridge Proxy HA Scanners A content of the second sec	Type to filter content @ Comment
Port Forwarding File Server External Lists User Interface Windows Domain Membership Kerberos Administration Troubleshooting Syslog	10 Low Relay Port 9200 Scanner Probe Interval(in milli seconds) 2000 Virtual IPs No. Virtual IP (Format: IP in CIDR notation) 1 192.168.10.13/24	gh Type to filter content Ø Comment
		_
Scanners	Type to filter	content 📾

0	/ × 🕇 +		Type to filter content 🛛 😣	
No.	Ip Address	Туре	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		
	この画面は従来の 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。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。			

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。

Scann	ers		
0	/ X 1 +		Type to filter content 🛛 🛽 🛽
No.	Ip Address	Туре	Comment
1	192.168.10.11	Scanner	
2	192.168.10.12	Peer/Director	

◆ <u>1 号機の変更箇所② HTTP Proxy の Listener address を修正します。</u>

Preck medgessell streamline: 222224222 (1152) [12024000 2223 (1152) [12024000 2223 (1152) [12024000 2223 (1152) [1202400 2223 (1152) [120240 2223 (1152) [120240 2233 (115240 2233 (1152	McAfee Web Gateway		
Processor Provessor	Server: mwgappl01 Server Time: 2020-08-20 11:50 JST UI Vers	on 9.2.2 (33635) User: admin Role: Super Administrator	User Preferences Logout ?
Appliances File Editor Appliances File Editor Cluster Update Engines ▼ Cluster Virtual router Id Standard Standard Papilances Papilances Papilances Papilances Papilances Papilances Papilances Papilances <th>McAfee McAfee Web Gateway</th> <th>ashboard Poicy Configuration</th> <th>🔍 Search 🛛 🙀 Save Changes 💌</th>	McAfee McAfee Web Gateway	ashboard Poicy Configuration	🔍 Search 🛛 🙀 Save Changes 💌
Addjoin DeleteUpdate Engines ▼ Wirtual router id Supervised additional additin additional additionadditi	Appliances File Editor		
A Ne Listenson Data and Data and Destrongen Allow slight Michael V. Community	Add/join × Delete Update Engines • Cluster Cluster Cluster Cluster Cluster Cluster Cluster Coching Appliances Coching Anti-Malware Telemetry Central Management Cocching Persistent Data Storage Port Portection Network Protection Voutes Port Portection Voutes Voutes Voutes	Virtual router id S1 VRRP interface eth0 HTTP proxy ✓ Enable HTTP proxy HTTP port definition list No. Listener addr Serve transp Ports treated Transparen 1. 0.0.0.0:9090 をダブルクリックし実 IP アドレ 複数のインターフェイス使用時は+アイコン ドレスを追加します Anonymous login for FTP over HTTP anon@localhost Add Via HTTP header ✓ Adjust content-type header for requests to archives (dependir FTP Proxy ✓ Enable FTP proxy FTP port definition list ✓ Listener add Data and Data and Data and Data and To data and	Type to filter content @ Int McAfee Web Accept PROXY Comment true false レスに変更します なクリックして 2番目以降の実 IP ア ng on the content-encoding)

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。

🚍 Edit HTTP Proxy Port	Edit HTTP Proxy Port	
HTTP Proxy Port Ustener address (Format: IP:port) 0.0.0.0990 Serve transparent SSL connections Ports treated as SSL (Format: port[, port]* or *) 443 Transparent common name handling for proxy requests McAfee Web Gateway uses passive FTP over HTTP connections Accept PROXY Protocol header Maximum segment size (MSS) C Comment: O Comment: O Comment: O Comment: Comm	HTTP Proxy Port Listener address (Format: IP:port) 192.168.10.11:9090 Ø Serve transparent SSL connections Ports treated as SSL (Format: port[, port]* or *) 443 Transparent common name handling for proxy requests Ø McAfee Web Gateway uses passive FTP over HTTP connections Accept PROXY Protocol header Maximum segment size (MSS) Ø Comment: Ø OK	el

 ◆ <u>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</u> 号機の実 IP アドレスに変更します。

FT	P Pro	xy							
	Enab	ole FTP proxy							
	TP po	rt definition list							
	0	/ X 🕇 🕂						Type to filter	content 🛛 🛞
	No.	Listener addr	Data port	Port range fo	Port range fo	Allow clients	McAfee Web	McAfee Web	Comment
	1	0.0.0.0:2121	2020	15000-20000	20001-25000	true	false	true	
	•		2020	10000 20000	20001 20000	trac	laise	ride	

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。

\diamond	最後に画面右上の	Save Changes	をクリックして	<u>こ設定を保存します。</u>
			<u>User</u>	Preferences Logout ?
oublesho	oting		Q Search	Save Changes 🔻

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。

McAfee Web Gateway	Dashboard	Policy	Configuration
Appliances File Editor			
 Add/Join X Delete Update Engines Cluster Appliances 			

2 号機の IP アドレスを入力して OK をクリックします。

📕 Add/Join Appliance 📃 🗖				
Host name or IP:				
Network group:				
Select 💿 Add Appliance	🔾 Join Cluster			
Name may not be empty 🕖	OK Cancel			

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。