Skyhigh Secure Web Gateway 旧 McAfee WebGateway 設定バックアップ・リストア手順書

2022 年 11 月 16 日 株式会社ディアイティ セキュリティソリューション本部

Η	ケ

1	はじめに		3
	1.1 本書	皆の目的	3
	1.2 ブラ	シンド名の変更について	3
2	設定バッ	ックアップ	4
	2.1 We	·bUI(UserInterface)へのログイン	4
	2.2 バー	-ジョン・ビルドの確認	5
	2.3 バッ	ックアップ手順	6
	2.4 バッ	ックアップに含まれない設定	8
	2.4.1	CLI用 root パスワード	8
	2.4.2	Windows Domain Membership(NTLM 認証)	8
	2.4.3	シリアルポート転送レート設定確認	8
	2.4.4	HA 機能を利用する際の MFEND-LBID 設定 (v7.x のみ、HA 構成のみ)	9
	2.4.5	Cluster CA 情報	9
	2.4.6	HAProxy 情報 (v8.2 以降のみ、HA 構成のみ)	9
3	設定リス	トア	С
	3.1 We	bUI へのログイン)
	3.2 バー	-ジョン適合確認1(C
	3.2.1	バージョン情報が同一の場合	5
	3.2.2	パックアッフ取得した際のパージョンと、Web Gatewayのパージョンに差異がある場合	ŝ
	3.3 1	トプ美施	1
	3.3.1		
	3.3.2	実なる国体の場合(RMA 寺で父授や、機奋リノレースの場合)	3
	3.4 JA	トア対象外の冉設定力法	4
	3.4.1		4
	3.4.Z	Windows Domain Membership(NILM 認証)	4 5
	3.4.3		С /
	3.4.4 2.4.5	□ FA	5
	3.4.3 2.4.4	しいいてして、1月秋	5 7
٨	J.4.0 V B Q O O O	□ ΠΑΓΙΟΧΥ]月報(VO.2 以阵のみ、□Α 悟风のみ)	с о
4	ND0727	2.Central Management 機能で使用する ClusterCA を直さ換える手順	5
5	Cenila		J

1 はじめに

1.1 本書の目的

本書では、McAfee Web Gateway(MWG) Version7 以降の設定バックアップ及びリストア手順を記載します。 なお、設定のリストアは基本的に WebUI より実施します。WebUI 接続に必要な IP アドレスやルーティング等基本的 な設定項目については、紙の資料など設定バックアップファイル以外の方法による記録を実施下さい。

本手順書の画面は基本的に Web Gateway バージョン 11.2.5.0 を使用しています。 旧バージョン固有の説明では旧バージョンを使用しています。

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。

2 設定バックアップ

2.1 WebUI(UserInterface)へのログイン

Web Gateway にブラウザよりログインします。以下 URL を参照します。(ポート 4712 はデフォルト値) https://Web Gateway の IPaddress:4712/

以下3タイプのUIが用意されています。

2022 年現在は、③をご利用ください。①は利用出来ない状況です。②は JRE を別途お持ちのお客様のみご利用 ください。

①ウェブブラウザ上の Java プラグインを使用する UI

表示されている Login 画面に User name、Password を入力してログインします。 使用可能なブラウザは Internet Explorer のみです。Google Chrome、Mozilla Firefox、Edge などのブラウザ は、Java プラグインが無効化されているため Web Gateway の Native UI に対応していません。

②ウェブブラウザではなく専用の Java アプリケーションを使用する UI (v7.6.1 で追加)

[Web Gateway UI as Java-Webstart Download]をクリックします。 「webstart.jnlp」というファイルがダウンロードされます。そのファイルを実行します。 アプリケーションを起動すると別のログイン画面が開きます。Username、Password を入力してログインします。

③Java を使用しない HTML のみで構成された UI (v7.8.0 で追加)

[Web Gateway UI as in-browser HTML]をクリックします。 ブラウザに表示されるログイン画面に Username、Password を入力してログインします。 (日本語入力モードになっていると Username, Password を入力できません)

	McAfee	e We	b Gate	way	Lo x +			_			×
← ·	→ Cª		<u>n</u> ==	htt	os://10.100.0.109:4712/Konfigurator/reg 🚥 👽 🚖 👦	۵	¥	8	Ē	۲	Ξ
				1	McAfee Login User name: Password: Login						
					Modern browsers have commonly stopped supporting Java applets. Please consider one of the following options:						
				2	• Web Gateway UI as Java-Webstart Download						
			- [3	<u>Web Gateway UI as in-browser HTML</u>						
					Please consult the Product Guide for differences.						

②と③の UI では[Advanced] をクリックすると、Web Gateway の IP アドレスとポートおよび SSL セキュア通信の有無を設定できます。デフォルトポート番号は SSL 有:4712 、 SSL 無:4711 です。

🕖 SWG Login		×
Skyhigh	Secure Web Gateway	
User name		
Password		
▼ Advanced		
IP/hostname	10.100.0.109	
Port	4712	
	☑ Use SSL	
M	issing login (2 problems) 🚇 🛛 Login	

Central Management 機能有効時の注意事項
 Central Management 機能で複数台の Web Gateway で設定を同期している場合には、仕様により1号機にログイン中は、2号機にログインできません。逆に2号機にログイン中は1号機にログインできません。

また、1 号機をログアウトしたあと、続けて2号機にログインするためには、60秒以上経過の後、ログインします。

2.2 バージョン・ビルドの確認

ログイン後、バージョン・ビルド情報を確認します。 以下画面の場合、UI Version 11.2.5 (42905)…の部分がバージョン・ビルド情報です。

🕖 Skyhigh Secure Web Gateway						_ 🗆 🗙
Server: mwgappl Server Time: 2022-11-16 14:31 J	ST UIVersion 11.2.5 (429)	05) User <mark>a</mark> dmin	Role: Super Adm	inistrator		<u>User Preferences</u> <u>Logout</u> ?
Skyhigh Secure Web Gateway	D ashboard	Policy	Configuration	Accounts	Troubleshooting	🔍 Search 📄 Save Changes 💌
Alerts Charts and Tables						
Appliances Status						

2.3 バックアップ手順

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

ブラウザの保存ダイアログが表示されます。ファイルをローカル PC 上に保存します。

デフォルトのファイル名は、日付.backup という名前になるため、対象機器やバージョン情報がわかりません。 バックアップを取得した際の対象機器、バージョン情報、日付が分かるように、ファイル名にホスト名、バージョン 情報を加えて下さい。

(例) ditwg.11.2.5_42905_2022-11-16.backup [ホスト名.バージョン情報_ビルド情報_日付.backup]

バックアップの対象は WebUI より実施の設定のみです。 CLI より実施の設定、編集した設定についてはバックアップ対象ではありません。別途バックアップを行う必要があります。

以上で設定バックアップは完了です。

● v7.4 以降の WebUI

McAfee Web Gateway Server: mwgappl Server Time: 2020-04-22 15:	:38 JST UI Version 8.2.6 (32146) User: admin	Role: Super Administrator <u>User Preferences</u> <u>Loqout</u> ?
McAfee McAfee Web Gateway	Dashboard Policy	Configuration Accounts Troubleshooting
Rule tracing central mwgappl Files Rule tracing files Rule tracing files Rule tracing files Feedback Core files Connection tracing Packet tracing Network tools System tools System tools System tools Rule tracing Rule tracing	Backup/Restore Configurations and Accounts* Policy* SS0 Credentials Configurations and Accounts Policy* SS0 Credentials * Always included	SSO 認証情報(クラウドシングルサイ ンオン機能で使用される認証情報) もバックアップするときにチェックを つけます Back up to file
McAfee Web Gateway Server: mwgappi Server Time: 2020-04-22 16 McAfee McAfee Web Gateway	:19 JST UI Version 8.2.6 (32146) User: admin	Role: Super Administrator <u>User Preferences</u> <u>Lonout</u> ?

Uncaree Michiee web Gateway	Dashboard Policy Configuration Accounts Troubleshooting
Rule tracing central mwgappl - Files - Log files - Rule tracing files - Feedback - Core files - Connection tracing - Packet tracing - Network tools - Synchronization to Cloud Backup/Restore Reset appliance password	Backup/Restore Configurations and Accounts* Policy* SSO Credentials Back up to file Save Backup Exported Backup Location Encryption Password : Select a file location. Ok Cancel

v10.2.x 以降のバージョンでは以下のウインドウがポップアップされます。ファイル名を入力して Save をクリックします。



v7.4~v9.2.x バージョンでは③の[Web Gateway UI as in-browser HTML]では「Back up to file」をクリックしたあと 設定ファイルを保存するときに下記の第三のウインドウを使用します。

💆 McAfee Web Gateway
Server: mwgappi Server Time: 2020-04-2216:20 JST UI Version 8.2.6 (32146) User: admin Role: Super Administrator <u>User Preferences</u> <u>Logout</u> 🕐
Image: McAfee Web Gateway Image: Configuration Image: Configurati
Save X
Save In: CuploadDownload C 目前に 部に 第三のウインドウ
ck up to file
ファイル名を入力して Save をクリック Browse
File Namer 2020 04 22 backup
Files of Type: .backup
Save Cancel
Drag and drop files here
Download selected Upload files Delete selected

McAfee Web Gateway	
McAfee McAfee Web Gateway	Dashboard Policy Configuration Accounts Troubleshooting
Rule tracing central rule tracing central rule tracing files - Log files - Rule tracing files - Rule tracing - Packet tracing - Packet tracing - Network tools - System tools - Syst	Backup/Restore Configurations and Accounts* Policy* SSO Credentials Save Backup Exported Backup Location 294Konfigurator/uploadDownload/2020-04-22.backup Encryption Password : Ok Cancel
Backup successful	

並行してブラウザのファイル保存が実行されます。(Firefox の場合のファイル保存ウインドウ)

OK

2020-04-22.backup を開く X	
次のファイルを開こうとしています:	
2020-04-22.backup	
ファイルの種類: backup File (742 KB)	
ファイルの場所: https://10.100.0.109:4712	
このファイルをどのように処理するか選んでください ○ プログラムで開く(<u>Q</u>): 参照(<u>B</u>) ● ファイルを保存する(<u>S</u>)	
OK キャンセル	

● Central Management 機能有効時の注意事項

Central Management 機能を有効にすると、複数台の Web Gateway で設定が同期されます。1 台にログインする と、すべての Web Gateway の設定も表示されますが、[Backup/Restore]メニューは、ログイン中の Web Gateway のみ表示されます。

Central Management 環境で取得した1つの Backup ファイルには、すべての管理ノードの設定が含まれているので、どのノードにおいても設定が復元(リストア)可能です。しかし、筐体交換等でハードウェアが変更された場合は、UUID が変わってしまうので、Backup ファイルをリストアするためには下記メーカーFAQ の手順にて、機器固有の ID(UUID)を指定しコマンドラインからリストアする必要があります。

<KB80762: コマンドラインから backup ファイルをフルリストアする方法> https://kcm.trellix.com/corporate/index?page=content&id=KB80762

2.4 バックアップに含まれない設定

現在確認されている内容として、下記項目はバックアップファイルに含まれないため、リストア後に手動で設定実施の必要があります。

そのため、設定内容を事前に紙面等で控えリストアに備えご準備下さい。

2.4.1 CLI 用 root パスワード

CLI 用に準備されている root パスワードはインストール時に設定されています。 バックアップファイル中には root パスワードは含まれないため、構築時等に別途記録を残して下さい。

2.4.2 Windows Domain Membership(NTLM 認証)

NTLM 認証利用時、Web Gateway は WebUI の [Configuration] > [Appliances] > ホスト名 > [Windows Domain Membership] にてドメイン参加の設定を実施されていますが、Administrator name および Password は Web Gateway に保存されません。 従って、Windows Domain Membership に参加していないアプライアンスに設定バックアップをリストアして

も Windows Domain Membership に参加していない状態のままとなります。 Windows Domain Membership に参加する手順は、「3.4.2 Windows Domain Membership(NTLM 認 証)」を参照してください。

2.4.3 シリアルポート転送レート設定確認

ー部の環境でシリアルポートの設定値を変更されるケースがあります。 (ほぼ UPS 利用のための設定変更です) 設定変更手順については「3.4.3 シリアルポートの転送レート設定変更」を参照下さい。

- 2.4.3.1 v7.7.x 以前の場合
 - 1. Web Gateway の CLI にログインし、/etc/init に移動します。
 - 2. ttyS0.conf ファイルを開き、ファイル中の以下の記載を確認します。
 (デフォルトでは 19200 となっております)

exec /sbin/agetty /dev/ttyS0 9600 vt100

2.4.3.2 v7.8.x 以降の場合

- 1. Web Gateway の CLI にログインし、/etc/default に移動します。
- 2. grub ファイルを開き、ファイル中の以下の 2 か所の記載を確認します。 (デフォルトでは 19200 となっております)

一箇所目:

GRUB_CMDLINE_LINUX="\$GRUB_CMDLINE_LINUX console=ttyS0,9600n8 console=tty0"

二箇所目:

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

2.4.4 HA 機能を利用する際の MFEND-LBID 設定 (v7.x のみ、HA 構成のみ)

/etc/sysconfig/mfend ファイルの最下行に MFEND-LBID=数値 の設定を実施している場合に、対象行を手動で記録しておいて下さい。

なお、本設定は同ーネットワーク内に複数の Web Gateway HA システムを構築する際に利用するため、 通常設定されていないケースがほとんどです。

v8.2 以降では MFEND は使用されていないため/etc/sysconfig/mfend ファイルの手動記録は不要です。

2.4.5 Cluster CA 情報

Central Management 機能を使用するときに必要となる Cluster CA データは設定バックアップファイルに 含まれていません。筐体交換等で新規インストール後には、既存の Central Management メンバーで使用 されている証明書をインポートする必要があります。

<KB89292: The Central Management Currently uses the default CA (How to replace the default Web Gateway cluster CA)> https://kcm.trellix.com/corporate/index?page=content&id=KB89292

詳細は「4 KB89292:Central Management 機能で使用する ClusterCA を置き換える手順」をご参照ください。

2.4.6 HAProxy 情報 (v8.2 以降のみ、HA 構成のみ)

v8.2 以降では MFEND ドライバの代わりに HAProxy 負荷分散が使用されています。 HA 構成機器において v8.1 以前の設定バックアップファイルには v8.2 以降で使用する HAProxy 負荷分 散用の設定が含まれていません。v7.x のバックアップファイルを v8.2 以降の機器にリストアする場合は手 動で HA 設定を変更する必要があります。

<KB91848:McAfee ネットワークドライバー (MFEND) から McAfee Web Gateway (MWG) 8.2.x の HAProxy への移行>

https://kcm.trellix.com/corporate/index?page=content&id=KB91848&actp=null&viewlocale=ja_JP& locale=ja_JP

同一バージョンのバックアップファイルをリストアする場合は HA 構成データが含まれていますので手動での設定変更は必要ありません。

3 設定リストア

3.1 WebUI へのログイン

設定バックアップの際と同様、「2.1WebUI(UserInterface)へのログイン」の手順にてログインを実施します。

3.2 バージョン適合確認

リストアを実行する前に、バックアップを取得した際の Web Gateway のバージョンと、これよりリストア対 象機器のバージョンをご確認下さい。バックアップファイルのバージョン情報については、バックアップファ イル名をご確認下さい。

以下画面の場合、UI Version 11.2.5 (42905)…の 11.2.5 の部分が同一であることをご確認下さい。 build に差異がある場合でも、問題なくリストアすることが可能です。下記の例では、42905 が build 番号 です。

🕖 Skyhigh Se	cure Web Gateway		_				_ — ×
Server: mwgappl	Server Time: 2022-11-16 14:31 JST	UI Version 11.2.5 (4290	5) User: admin	Role: Super Adm	inistrator		<u>User Preferences</u> <u>Logout</u> ?
Skyhigh	Secure Web Gateway	Dashboard	Policy	Configuration	Accounts	Troubleshooting	🔾 Search 📄 Save Changes 🔻
Alerts	Charts and Tables						
Appliances St	atus						

3.2.1 バージョン情報が同一の場合

「3.3リストア実施」の手順に従ってリストアを実施下さい。

3.2.2 バックアップ取得した際のバージョンと、Web Gateway のバージョンに差異がある場合

過去のバージョンでバックアップ取得したファイルを、それよりも新しいバージョンにリストアすること は可能ですが、新しいバージョンでバックアップ取得したファイルをそれより過去のバージョンにリス トアすることはできません。

例:

v7.7.2.14 でバックアップ取得したファイルを v7.8.2.6 にリストアすることができます。 v7.8.2.4 でバックアップ取得したファイルを v7.7.2.5 にリストアすることができません。

特定バージョンの Web Gateway を構築するためには、下記の Content & Cloud Security Portal サイト(旧称:Extranet)より、構築したいバージョンのインストール用 ISO イメージファイルをダウンロー ドして、新規インストールを行う必要があります。

<Content & Cloud Security Portal> <u>https://contentsecurity.skyhigh.cloud/software_mwg7_download</u> ログインに必要な ID とパスワードは保守契約サポート証書をご確認下さい。サポート証書に記載ない場 合は、お客様にてパスワードを設定されておられます。

インストールは CD より起動することで自動的に行われます。 詳細は、以下のメーカードキュメントをご確認下さい。

<セキュア Web Gateway の初回インストールについて> https://success.myshn.net/Skyhigh_Secure_Web_Gateway_(On_Prem)/Secure_Web_Gateway_Install ation/Install_for_the_First_Time/About_Installing_Secure_Web_Gateway_for_the_First_Time?mtlanguage=JA

不明点は弊社保守サポート窓口までお問い合わせ下さい。

3.3 リストア実施

3.3.1 同一筐体の場合

ここでの「筐体」とは WG4000 等の機種ではなく個体を意味します。

IP アドレスやルーティング等 Policy メニュー以外の設定項目のリストアを WebUI で行う場合はバックアップ 取得を行った筐体と同一の筐体に対してのみ可能です。異なる筐体に対して Policy メニュー以外の設定を リストアする場合には、次項「3.3.2 異なる筐体の場合(RMA 等で交換や、機器リプレースの場合)」を参照 下さい。

[Troubleshooting] > [Backup/Restore] に移動し、[Restore from file]をクリックしてリストアしたいファイル を選択します。

Policy のみをリストアしたい場合には、[Configurations and Accounts] のチェックを外します。 Configuration や Account の項目も全てリストアしたい場合には、[Configurations and Accounts] にチェッ クを付けます。

v7.4 以降の WebUI

💆 McAfee Web Gateway	
Server: mwgappi Server Time: 2020-04-22 17	:10 JST UI Version 8.2.6 (32146) User: admin Role: Super Administrator <u>User Preferences</u> <u>Loqout</u> 💽
McAfee McAfee Web Gateway	Dashboard Policy Policy Configuration Accounts
œ e	Backup/Restore
Rule tracing central	✓ Configurations and Accounts* 其本設定とアカウント情報もUIストアオス
- Files	☑ Policy* ときにチェックをつけます
 Rule tracing files Eachback 	SSO Credentials
- Core files	Back up to file
 Packet tracing Network tracing 	Configurations and Accounts SSO 認証情報(クラウドシングルサインオ
- System tools	☑ Policy* ン機能で使用される認証情報)もリストア するときにチェックをつけます
 Synchronization to Claud Backup/Restore 	SS0 Credentials
– Reset appliance password	Restore from file
	* Always included



[Continue with restore] をクリックしリストアを進めます。

v10.2.x 以降のバージョンでは以下のウインドウがポップアップされます。Browse をクリックしてバックアップファイルを選択します。

OPEN FILE					
Please select a file to impo					
Browse	Cancel				

v7.4~v9.2.x バージョンでは③の[Web Gateway UI as in-browser HTML]では「Restore from file」をクリックしたあ と設定ファイルをアップロードするときに第三のウインドウを使用しますので、その部分を補足します。

McAfee Web Gateway Server: mwgappl Server Time: 2020-04-3	T 🔀
McAfee Web Gatew	ay 😪 🛄 💥 🤽 🔶 🔍 Save Changes 🗸
Rule tracing central	Look In: DuploadDownload
 P-	第三のウインドウ
 Feedback Core files Connection tracing 	
 Packet tracing Network tools System tools Synchronization to Cloud 	Upload files をクリックして別途表示される
 Backup/Restore Reset appliance passwore 	File Name: エクスクロークで設定クアイルを選択します。 Files of Type: .backup または、[Drag and drop files here]欄に
	設定ファイルをドラッグ&ドロップします。
	Drag and drop files he Download selected Upload files Delete selected
 ● ファイルのアップロード ← → < ↑ < OS (C:) > testfolder 	× v む の testfolderの 検索
整理 ▼ 新しいフォルダー MacroLog へ 名前 MinGW	
PerfLogs Perl Program Files	Windows のエクスプローラ
Program Files SWSETUP Tenable	でリティル名を入力して 開くをクリック
testfolder ファイル名(N): 2020-04-22.8	ackup
	(O) 第(O) 年代又有化
McAfee Web Gateway Server: mwgappi Server Time: 2020-04-	2 17:25 JST UI Version 8.2.6 (32146) User: admin Role: Super Administrator <u>User Preferences</u> <u>Loqout</u> ?
McAfee McAfee Web Gatew	ay 😪 🛄 🗙 🤽 <table-cell-rows> 🖓 🖓 Save Changes 🗸</table-cell-rows>
Rule tracing central	
Files Log files Rule tracing files	2020-04-22.backup アップロードしたファイルが 表示されない場合は、
 Feedback Core files Connection tracing Packet tracing 	View Refresh を選択します。
 Network tools System tools Synchronization to Cloud 	Sile Name: 2020.04-22 backup
Reset appliance passwor	Files of Type: backup
	ファイル名を人力して Open をクリック
	Download selected Upload files Delete selected
Restore successful	X
Restore successful.	

リストア実施後、自動的にログアウトされます。再度ログインしてアプライアンスを再起動します。 再起動後、設定反映をご確認下さい。 以上で設定リストアは完了です。

ОК

3.3.2 異なる筐体の場合(RMA 等で交換や、機器リプレースの場合)

バックアップを取得した筐体とリストア先筐体が別個体である場合、リストアはコマンドラインより実施しま す。詳細は、以下のメーカーナレッジセンターをご確認下さい。

<KB80762: コマンドラインより backup ファイルをフルリストアする方法>
<u>https://kcm.trellix.com/corporate/index?page=content&id=KB80762&actp=null&viewlocale=ja_JP&showDr</u>
aft=false&platinum_status=false&locale=ja_JP

コマンドラインから backup ファイルをフルリストアする方法 技術的な記事 ID: KB80762 最終更新: 2014/02/13

問題の詳細

GUIの「Troubleshooting」-「Backup/Restore」から同一の機器の backup ファイルの場合はフルリストアすることができますが、異なる機器の場合はフルリストアすることができません。 異なる機器の場合も下記コマンドラインの手順にて backup ファイルをフルリストすることができます。

- 1. GUI ヘログインしている場合は事前にログオフします。
- 2. コンソールへアクセスし、保存した backup ファイルを、フルリストアしたい Web Gateway の/tmp へ 保存します。

※USB Stick、SCP、LFTP などで適宜 backup ファイルを Web Gateway へ保存してください。 3. 保存した backup ファイルのパーミッションを変更します。

- chmod 777 保存した backup ファイル名*
- UUID を設定しフルリストアのコマンドを実行します。 /opt/mwg/bin/mwg-coordinator -R 'file:in=PATHTOBACKUPFILE;options:uuid=UUID' ※上記の PATHTOBACKUPFILE へ backup ファイルのパスを入力します。 ※上記の UUID へ backup ファイルをテキストエディタで開いた中にある、(<co_node id="xxxx">)の xxxx 部分を入力します。

※v7.3 以降でバックアップ時にパスワードを指定して設定ファイルを暗号化した場合には以下のよう にしてパスワードを指定してください。

options:uuid=UUID,password=PASSWORD

保存した backup ファイルが「config.backup」、UUID が「44454C4C-4A00-1039-8047-B9C04F355031」の場合の実行例は下記です。

/opt/mwg/bin/mwg-coordinator -R 'file:in=config.backup;options:uuid=44454C4C-4A00-1039-8047-B9C04F355031'

5. 下記のような結果が返ってきたことを確認し、設定を反映させるために再起動を行います。

/opt/mwg/bin/mwg-coordinator -R 'file:in=config.backup;options:uuid=44454C4C-4A00-1039-8047-B9C04F355031'

successfully sent restore request "file:in=config.backup;options:uuid=44454C4C-4A00-1039-8047-B9C04F355031" to running Coordinator process.

Job queued with id: 1160 Job progress: . Job finished. Coordinator responded: OK

6. GUI ヘログインし、設定がフルリストアされていることを確認します。

7. /tmp へ保存した backup ファイルを削除します。

注意点

ご利用バージョンの backup ファイルをそれより前のバージョンに復元することはサポートしておりません。

3.4 リストア対象外の再設定方法

現在確認されている一部の設定についてはバックアップに含まれないため、リストア後に手動で再設定を行います。

3.4.1 CLI 用 root パスワード

```
リストア対象の機器は Web Gateway インストール時に設定された root パスワードを保持しています。
パスワードを変更する場合は、passwd コマンドを利用し、下記の通り変更します。
(CAPS Lock 等により、想定外パスワードとなることを回避するため、複数 root にて CLI を接続しておき、
パスワード変更後、想定パスワードでログイン可能なことを確認する手順を推奨します。)
```

```
# passwd
Changing password for user root.
New password: <-- 1回目の新しいパスワードを入力
Retype new password: <-- 2回目の新しいパスワードを入力(1回目と同内容を確認)
passwd: all authentication tokens updated successfully.
[root@mwg ~]#
```

以上でパスワードの変更完了です。

v7.7.1 以降では WebUI でも設定可能になりました。 [Troubleshooting] > [Appliance] > [Reset appliance]

3.4.2 Windows Domain Membership(NTLM 認証)

NTLM 認証を行っている場合、リストア後に再度 Web Gateway をドメインに参加する必要があります。 Configuration > Windows Domain Membership を開き Join をクリックします。

Skyhigh Secure Web Gateway	Image: Save Changes Dashboard Policy Configuration Accounts Troubleshooting
Appliances File Editor	
 Add/Join × Delete Update Engines ▼ Cluster Mobile Cloud Security UCE Hybrid Web Hybrid Web Hybrid Anti-Malware Telemetry ePolicy Orchestrator Coaching Persistent Data Storage Proxies (HTTP(S), FTP, SOCKS, ICAP SSL Tap Network Interfaces Domain Name Service Date and Time Bandwidth Control Network Protection SIMP Hardware Security Module Static Routes Port Forwarding File Server External Lists User Interface Log-Itte Manager Windows Domain Membership Kerberos Administration Troubleshooting Suna 	Windows Domain Membership Appliance is joined to the following Windows Domains ③ Join Modify Leave Type to filter domain Refresh Domain Account Domain NTLM V Timeout Reconn Active D Skyhigh Secure Web Gateway account name: Import the existing account Import the existing account Import the existing account W Use NTLM version 2 Use DC name from NTLM handshake Import the for requests to this NTLM domain: Is Seconds (Format: 1-99) Wait time for reconnect to Domain Controller: Iso Seconds (Format: 5-300) Configured Domain Controller(s), comma separated: Win2008r2-adlab.nsec.co.jp Mumber of active Domain Controller(s), comma separated: Muniper of active Domain Controller(s), Import the domain. These credentials will be used once to create the machine account for Skyhiah Secure Web Administrator name および Password la MWG I= CR存さ h ast the o.
	OK Cancel

Copyright©2022 dit Co., Ltd . All rights reserved.

ドメインへの参加に成功すると以下のようになります。

Appliance is joined to the following Windows Domains

Join	Modify	🗶 Leave Type to filter doma	🗟 🍓 Refr	esh				_	
Domain	Account	Domain Controller(s)	NTLM V	Timeout	Recon	Active	Status	Г	
nsec.co.jp	MWG	win2008r2-adlab.nsec.co.jp	2	15	180	1	•	_	ADと連携中は称色です
								Ľ	

3.4.3 シリアルポートの転送レート設定変更

ー部の環境でシリアルポートの設定値を変更されるケースがあります。 (ほぼ UPS 利用のための設定変更です)

ファイルの編集は viコマンド等をご利用下さい。 設定変更を行う前に変更対象のファイルをコピーするなどしてバックアップ後、実施下さい。

3.4.3.1 v7.7.x 以前の場合

- 8. Web Gateway の CLI にログインし、/etc/init に移動します。
- 9. ttyS0.conf ファイルを編集し、19200 を 9600 に変更します。 (デフォルトでは 19200 となっております)

exec /sbin/agetty /dev/ttyS0 19200 vt100

exec /sbin/agetty /dev/ttyS0 9600 vt100

10. 機器を再起動し変更を反映させます。

3.4.3.2 v7.8.x 以降の場合

1

- 1. Web Gateway の CLI にログインし、/etc/default に移動します。
 - # cd /etc/default
- 2. 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
- 3. 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

- 4. grub ファイルを編集し、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"
- 5. 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
- 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 linux16 /boot/vmlinuz-3.18.118-1.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

7. 機器を再起動し変更を反映させます。

8. 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)

console=ttv0

[0.00000] 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] [ffffea000000000-ffffea00061fffff] PMD -> [ffff8801b9600000ffff8801be9fffff] 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

3.4.4 HA 機能を利用する際の MFEND-LBID 設定 (v7.x のみ、HA 構成のみ)

/etc/sysconfig/mfend ファイルを編集してファイルの最後にパラメータを追加し、Web Gateway をリブートします。

なお、HA 対向装置(リストア対象でない)にて MFEND-LBID=の記述がない場合は編集不要です。

HAの2台に対して、同時に復旧する場合は、同一ネットワーク内に Web Gateway(HA 構成)がなければ 不要。あれば、重複しない ID を指定しリストア下さい。

MFEND-LBID=10			MFEND-	LBID=20
MWG1	MWG2		MWG3	MWG4
		J		

3.4.5 Cluster CA 情報

Central Management 機能で使用するときに必要となる Cluster CA データは設定バックアップファイルに 含まれていません。筐体交換等で新規インストール後には、既存の Central Management メンバーで使用 されている証明書をインポートする必要があります。

詳細は「4 KB89292:Central Management 機能で使用する ClusterCA を置き換える手順」をご参照ください。

新規インストール後に Cluster CA データをインポートする前に、Central Management が有効となっている ときに取得した設定バックアップファイルをフルリストアしてしまうと、Cluster CA データを変更することがで きなくなりますので、一旦 Central Management を無効にした状態で Cluster CA データをインポートして から Central Management を有効にしてください。

Central Management の有効化と無効化の手順は「5Central Management 機能の有効化と無効化」をご 参照ください。

3.4.6 HAProxy 情報 (v8.2 以降のみ、HA 構成のみ)

v8.2 以降では MFEND ドライバの代わりに HAProxy 負荷分散が使用されています。 HA 構成機器において v8.1 以前の設定バックアップファイルには v8.2 以降で使用する HAProxy 負荷分 散用の設定が含まれていません。v8.1 以前のバックアップファイルを v8.2 以降の機器にリストアする場合 は手動で HA 設定を変更する必要があります。

<KB91848:McAfee ネットワークドライバー (MFEND) から McAfee Web Gateway (MWG) 8.2.x の HAProxy への移行>

https://kcm.trellix.com/corporate/index?page=content&id=KB91848&actp=null&viewlocale=ja_JP& locale=ja_JP

同一バージョンのバックアップファイルをリストアする場合は HA 構成データが含まれていますので手動での設定変更は必要ありません。

バックアップファイルバージョン	リストアシステムバージョン	手動変更の要否
v7.x	v7.x	不要
v7.x	v8.2 以降	必要
v8.2	v8.2	不要

v7 から v8.2 以降へのアップデートについては別紙「McAfee Web Gateway Version7 以降 アプライアン スアップデート手順書」をご参照ください。

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。

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。





4 KB89292:Central Management 機能で使用する ClusterCA を置き換える手順

以下のメーカー情報を基に手順を説明します。

The Central Management Currently uses the default CA (How to replace the default Web Gateway cluster CA) <u>https://kcm.trellix.com/corporate/index?page=content&id=KB89292</u>

環境

McAfee Web Gateway (MWG) 7.7.1.4 and later McAfee Web Gateway (MWG) 7.8.x, 8.x

問題

v7.7.1.4 以降のバージョンで、デフォルトの Cluster CA を使用しているとダッシュボードにエラーが表示されるようになります。

それより過去のバージョンでは Central Management にてデフォルトの Cluster CA が使用されています。

Dashboard > Alerts

(intel) s	Security 🤠	Web Gateway	Dashboard	Policy Cor	higuration Accounts	Troubleshootin	9	Q Se	arch 🛛 🖓 Save C	hanges 🔻
Alerts	Charts and	Tables	\sim							
Appliances S	Status									
Appliance Name	Performane Alert peaks,	c e last 7 days Reques	ts per second	McAfee Anti-M Last update	Talware Versions Gateway Engine	Gateway DATs	Engine	DATs	URL Filter Last update	Version
mwg 1				0 44 minutes ago	7001.2015.2058	6329	5900.7845	8957	12 minutes ago	76512
Alerts										Reset Filters
Appliance	Filter 👻	Date Filter 👻	Message Filter	: 🔽 Error 🔽 Warn	ning 🔲 Information Ty	pe to filter alerts	0			
All		mi	Error, Warning							
mwg 1		18-Jul-2018 09:08:18 JST	📕 The Central N	lanagement currently	uses the default CA. Go	to Configuration > Ap	pliances to repla	ce it (Origin:	Centralized Manageme	ent, ID: 3020)
mwg 1		17-Jul-2018 18:09:38 JST	The Central N	Anagement currently	uses the default CA. Go	to Configuration > Ap	pliances to repla	ce it (Origin:	Centralized Manageme	ent, ID: 3020)

default CA 使用時のエラーアラート表示

原因

v7.7.1.4 以降のバージョンでは Cluster CA をチェックしており、デフォルトの Cluster CA を使用していると ダッシュボードにエラーが表示されるようになりました。

これはセキュリティ警告ですが、ダッシュボードにエラーが表示されるだけであり機能的な問題はありません。

解決策

ユニークな SSL 証明書を新規に作成し、それを全 Cluster ノードにインポートすることで解決します。

Cluster CA に使用するためのユニークな SSL 証明書の作成手順

- 1. ひとつのノードの WebUI にログインして、Policy > Settings タブを開く
- 2. Engines > SSL Client Context with CA を展開
- 3. 新規証明書の設定を作成
 - A) ツールバーの Add をクリック
 - B) Name 欄に名前を入力 (例: Own Cluster Certificate)
 - C) OK をクリック
 - D) 新規作成の設定が表示されます

Policy > Settings > Engines > SSL Client Context with CA を選択し右クリック > Add をクリック



4. 新規設定を確認

新規に作成された設定を選択すると Define SSL Client Context (Certificate Authority) 欄の各パラ メータがデフォルト状態で設定されていることを確認できます。

- 5. 専用の証明書を生成します
 - A) Generate をクリック
 - B) 各種パラメータに値を入力して OK をクリック
 - C) 証明書とキーが生成されてエクスポート可能になります

Generate をクリックし新 CA を作成します



- A) Export Key をクリック.
- B) Browse.をクリック
- C) File Name 欄で名前を付けて保存します(拡張子は .pem を指定).
- D) 保存するディレクトリを確認します
- E) オプションでパスワードをつけることができます
- F) OK をクリックし選択したディレクトリにエクスポートされます

SSL 証明書とプライベートキーファイルのエクスポート



Save Changes をクリックして設定を保存します

CAfee Web Gateway	Dashboard	Configuration Accounts Troubleshooting
Rule Sets Lists Settings 1	lemplates	
🔇 Add 🥒 Edit 🗙 Delete 🕒 📄	Define SSL Client Conte	xt (Certificate Authority)
Type to filter settings Image: Comparison of the setting of the s	Subject Common Name (CN) Organizational Unit (OU) Issuer Common Name (CN) Organization (O) Organizational Unit (OU) Validity Not Before	McAfee Web Gateway McAfee, Inc. NSBU McAfee Web Gateway McAfee, Inc. NSBU Jul 10, 2020 3:42:04 PM
 Cloud Storage Encryption Cloud Storage Encryption Support Coaching Composite Opener Data Loss Prevention (Classificatio) Data Trickling Email Notification 	Not After Extensions Comment Fingerprint Private key	Jul 8, 2030 3:42:04 PM This is the default McAfee Web Gateway root CA. It will be delivered with each web gateway installation. We recommend to generate and use your own CA c2 b0 6d 00 65 5c 49 37 42 52 73 7d 47 46 eb 1b 2e b2 12 a6 present
 External Lists File System Logging HTML Opener ICAP Client 	Certificate Authority	Import Import Import Import Import
 Mobile Device Certification Next Hop Proxy Persistent Data Storage Progress Page Protocol Detector Proxy Control SafeSearch Enforcer SAML Request SAML Response Secure Reverse Proxy Filter 	Send certificate chain Certificate chain	uired for self-signed certificates)
 Secure Token Single Sign On SSL Client Certificate Handling SSL Client Context with CA Default CA Own Cluster Certificate SSL Client Context without CA 	Use custom server key Custom server key < RSA server key size	not set>

SSL 証明書とプライベートキーファイルを Cluster CA としてインポートします

- 1. Configuration > Appliances タブを開きます
- 2. Appliances ツリーの Appliances をクリック > Cluster CA をクリックします



3. Change CA をクリックします

既存の Cluster CA が存在する場合の画面

🔤 Cluster CA	🐸 Cluster C A 📃 🗖 🛛
Common Name (CN): McAfee Web Gateway Cluster CA Change CACancel	Common Name (CN): Cluster CA SHA256 Hash : 0504be7f79b64dbead530ada578f1487a6a502f3c8f435b3793cad254a48d250 Generate Change CA Cancel
既存の Cluster CA が存在しない場合の画面 Cluster CA Certificate Not Defined Cluster CA not defined Please Generate/Import Cluster CA Certificate OK	v7.7.x 以降 のクリーンインストール直後で Cluster CA が登録されていないときに Cluster CA not defined と表示されます
Cluster CA	
Common Name (CN): SHA256 Hash :	Cluster CA が登録されていない場合は Hash 値が表示されません
Generate CA	nge CA Cancel

4. SSL 証明書ファイルをインポートします

A) Certificate: Browse をクリックします

윢 Import Certificate Authority for Cluster	_ 🗆 🗙
Certificate:	
	Browse
Private Key:	
	Browse
Password:	
Please select a file 🕕 Import	Cancel

B) 証明書ファイルを選択します

Look <u>I</u> n:	uploadDownload
🗋 OwnC	ClusterCA-key.pem
🗋 OwnC	ClusterCA.pem
_	
(OwnClusterCA.pem を選択します
File <u>N</u> am	e: OwnClusterCA.pem
Files of <u>T</u>	ype: Certificate (*.cer, *.crt, *.pem)

5. プライベートキーファイルをインポートします A) Private Key: Browse をクリック

T INALE NEY. DIOWSE 2 7777	
瀺 Import Certificate Authority for Cluster	_ 🗆 🗙
Certificate:	
≥1dc2cKonfigurator/uploadDownload/OwnClusterCA.pem	Browse
Private Key:	
	Browse
Password:	
	Cancel
	Carleer

B) プライベートキーファイルを選択

Open				
Look <u>I</u> n:	uploadDownload			
OwnClusterCA-key.pem				
OwnClusterCA.pem				
OwnClusterCA-key.pem を選択します				
File <u>N</u> ame:	OwnClusterCA-key.pem			
Files of <u>T</u> ype:	Private Key (*.key, *.pem)			
	Open Cancel			

C) エクスポート時にパスワードを入力したときは Password に入力し Import をクリック

🔓 Import Certificate Authority for Cluster 📃 🗖 💌	
Certificate: 11dc2cKonfigurator/uploadDownload/OwnClusterCA.pem Browse	
Private Key:	
2cKonfigurator/uploadDownload/OwnClusterCA-key.pem Browse	
Password:	エクスポート時に Password を入力 したときのみ、同じ Password を入
Import Cancel	力します。

インポートに成功すると successfully changed と表示されます

Changing CA 🛛 🗙			
i	Cluster CA successfully changed		
	OK		

5 Central Management 機能の有効化と無効化

◆ <u>Central Management を無効にする手順</u>
 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 Gateway	Dashboard	Policy	Configuration
Appliances File Editor			
③ Add/Join × Delete ⇒青色の矢印は、	⇒青色の矢印は、WebUIにログインしている MWG を示しており mwgappl01 にログインしている状態です。		
- Appliance			
←	nwgappl02 の 2 台 れている状態です	で CentralMar	nagement 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イ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。



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

A	Add/Join.をクリックします。			
	Appliances		File E	ditor
	🔾 Add/Join 🗙		Delete	Up
	⊶ Cluster • Appliances • 📄 mwgappl01			

Add/Join Appliance ウインドウで 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:				
all	-			
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。



Copyright©2022 dit Co., Ltd . All rights reserved.