FortiAnalyzer Version.5.0 MR2 Patch4 Information

第 1.0 版

改訂履歴

発行年月	版 数	改版内容
2015/11/9	第 1.0 版	初版発行

目次

1. はじめに

本マニュアルは FortiAnalyzer の OS バージョンを弊社推奨バージョン Version5.0 MR2 Patch4 へアップグレードする際の注意事項について記載しています。
具体的なアップグレード手順については、以下のバージョンアップ手順書を参照ください。

http://gold.nvc.co.jp/supports/fortinet1/verup/faz/
FortiAnalyzer バージョンアップ手順書

2. サポート機種

version5.0 MR2 Patch4 をサポートしている機種は以下の通りです。

FortiAnalyzer	FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400C, FAZ-1000C, FAZ-1000D, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-3900E, and FAZ-4000B
FortiAnalyzer VM	FAZ-VM32, FAZ-VM64, FAZ-VM64-HV, FAZ-VM64-XEN (Citrix XenServer and Open Source Xen), FAZ-VM64-KVM, and FAZ-VM64-AWS.

3. アップグレードパス

現在ご利用の OS バージョンによっては、バージョンアップを段階的に行う必要がございます。下記のアップグレードパスをご参照いただき、ご利用バージョンに合わせたバージョンアップ手順を行ってください。

現在の利用バージョン	→	経由バージョン	→	ターゲットバージョン
version5.0 MR2 patch3 version5.0 MR2 Patch4	→	なし	→	version5.0 MR2 Patch4
version5.0 MR2 patch1	→	version5.0 MR2 Patch2	→	version5.0 MR2 Patch2
version5.0 Patch6 から version5.0 Patch11	→	version5.0 MR2 Patch2 ※注意	→	version5.0 MR2 Patch4

(*表記方法　例 v5.0.5 = version5.0 Patch5 , v4.3.1 = version4.0 MR3 Patch1)

version5.0Patch6 未満のお客様は ver5.0Patch6 以上へ一度バージョンアップを行って頂く必要がございます。バージョンアップ時の注意事項につきましては下記マニュアルをご参照下さい。

FortiAnalyzer Ver.5.0Patch9 Information
http://gold.nvc.co.jp/supports/fortinet/OS/FAZv50p9Informations_v1.pdf

※注意
バージョンアップ後、SQL データベースの再構築が発生致します。
再構築中は下記機能を使用することができませんので御留意下さい。
下記機能は SQL データベースの再構築後、使用が可能になります。

- レポート作成（スケジュールレポート機能も含みます）
- リアルタイムでのログ表示
- FortiView

4. バージョンアップ時の注意事項

下記は version5.0 MR2 patch4 へアップグレードする際の注意事項となります。

リモート SQL データベースのサポート制限

version5.0 Patch7 から version5.0 MR2 で、リモート SQL データベース機能のサポートがリモート MySQL データベースへのログデータ挿入のみとなります。リモート SQL データベースを使用したヒストリカルログの検索や、レポーティング機能はサポートされません。FortiAnalyzer 機能のすべてを使用するには、FortiAnalyzer 上のローカル SQL データベースへログを保管することを推奨致します。ローカルデータベースは FortiAnalyzer 上へすでに保存された raw ログを元にリビルドします。

SQL データベースのリビルド

FortiAnalyzer version5.0 MR2 Patch2 は SQL データベースを再構築している間、新規のログを受信することが可能です。スケジュールレポート機能はすべて無効になります。イベントマネジメント機能は利用可能です。ログビュー、レポートは正しい値が出力されない場合があります。また、レポート作成についてはデータベースのリビルドプロセスが終了してから実施することを推奨します。

デバイスログ設定

version5.0 MR2 Patch1 以降、ローカルデバイスのログ設定を GUI から行うことが可能になりました。

Log Array 再配置

Log Array はタブ「Device Maneger」からタブ「Fortiview」配下の「Log View」へ移動しました。

Log Arrays、 devices および VDOM

FortiAnalyzer version5.0 Patch6 以前のバージョンにおいて devices と VDOM 双方で Log Array を作成する場合、対象の Log Array に付加するための devices と VDOM をそれぞれ選択する必要があります。FortiAnalyzer version5.0 MR2 以降のバージョンにおいて vdom が有効な device を付加する場合、すべての VDOM は自動的に対象の Log Array に付加されます。

レポートグルーピング

類似したレポートを大量に生成する場合、レポートをグルーピングすることによってレポートの生成時間を改善することが可能です。

データベース再構築中のレポート生成

FortiAnalyzer のアップグレード後、スキーマ変更に伴ってデータベースを再構築する必要がある場合がございます。データベースの再構築が完了するまでは正確なレポート生成に影響を及ぼすことがございますのでご注意ください。

レポート名における特殊文字に関して

FortiAnalyzer version5.0 MR2 ではレポート名に下記特殊文字を使用することができません。
¥ / ‘ “ > < & , |

レポートをインポートする際は上記の特殊文字を使用なさらないようにご注意ください。適切にレポート名が表示されない場合がございます。

データセットへの必要な変更

version5.0 MR2 におけるデータベースのスキーマ変更によって、すべての既存データセットもしくは新規のデータセットは以下の規定に従わなければなりません。

・データセットが srcip や dstip のような IP 関連のデータを参照する場合、適切に表示するために IP アドレスに変換する ipstr('…')機能をご使用ください。(例) ipstr('srcip') は送信元 IP を返します。
・カラムである,status は action に変更されましたので適切な status 表示のために、データセットクエリの status を action に置換してください。

FortiAnalyzer VM に関して

VM 環境において、FortiAnalyzer VM のインストールやアップグレード前に VM サーバーを最新の状態にアップグレードしていただき VM ホストサーバープロバイダーから配布されるパッチを適用してください。

ebtime の前処理ロジック

下記の条件に合ったログは推定ブラウジング時間の計算に用いることができます。

・Logid13 や 2 のトラフィックログ
　※logid=13 のときはホストネームをつける必要があります
・The service field が HTTP, 80/TCP もしくは 443/TCP のどちらか

上記の条件をすべて満たす場合、devid, vdom, user (srcip ユーザーが空欄の場合)はユーザーを特定するためのキーとして結びつけられています。時間推定のため、duration の現在値はセッション開始、終了時間の履歴に対して計算され、オーバーラップされていない箇所のみ現在ログの ebtime として用いられます。
FortiAnalyzer v5.0.5 以降のバージョンにおいて、推定ブラウジング時間の計算時に Explicit Proxy logs (logid=10)がチェックされます。

FortiAnalyzer VM ライセンスチェック

ライセンス認証過程の一環として FortiAnalyzer VM は自身の IP アドレスとライセンスファイルの IP 情報を比較します。IP アドレスが合わない場合、FortiAnalyzer VM は CLI コマンド「get system status」の出力に「IP does not much」 というエラーを返します。新しいライセンスがインポートされたり、FortiAnalyzer VM の IP アドレスが変更されたりする場合、変更の確認と有効なライセンスを作動させるために FortiAnalyzer VM を手動で再起動する必要がございます。

アプリケーションコントロールのための拡張 UTM ログ

FortiAnalyzer version5.0 MR2 Patch4 にアップグレードする場合、FortiOS CLI において拡張 UTM ログを許可するまではアプリケーションコントロールログを見ることができません。
拡張 UTM ログを有効にするため、下記の CLI コマンドを使用してください。

```
config application list
edit <name>
set extended-utm-log enable
end
```

ConnectWise Management Services Platform (MSP)サポート

ConnectWise Management Services Platform (MSP)は FortiAnalyzer version5.0 MR2 をサポートしておりません

配布アップグレード

コレクター/アナライザ　アーキテクチャのアップグレードに関して、先にアナライザをアップグレードすることを推奨しています。
先にコレクターをアップグレードするとアナライザのパフォーマンスに影響を及ぼす可能性があります。

5. v5.0.6 以上からバージョンアップする際の注意事項

FortiAnalyzer version5.0 Patch6～Patch9のOSをアップグレードする際の注意事項は以下の通りです。

パーテションのリサイズについて

FortiAnalyzer v5.0.7以降のバージョンではシステムファームウェアを格納しているフラッシュのパーテションがリサイズされます。このパーテションに収容されているセカンダリのファームウェアやシステム設定はアップグレード後に失われます。必要に応じてシステム設定の再設定を行って下さい。

VM環境においてFortiAnalyzer VMを稼動させるためにはハードディスクに513MB以上の空き容量が必要です。

6. ダウングレードについて

FortiAnalyzerはすべてのダウングレードパスを提供しておりません。Web-based ManagerもしくはCLIから以前のバージョンにダウングレード可能ですが、設定が失われてしまいます。ダウングレード完了後、システムのリセットとdiskのフォーマットを行う必要がございます。リセットとdiskのフォーマットを行う場合は、コンソール接続をして以下のCLIコマンドを入力して下さい。

```
execute reset all-settings
execute format {disk | disk-ext4}
```

※コマンド実行後、機器の再起動が発生致します。

7. VM 版の環境について

FortinetはVMware ESX/ESXi およびMicrosoftHyper-V Server virtualization environmentsのための FortiAnalyzer仮想ファームウェアイメージを提供しております。
以下は提供しているファームウェアイメージの説明となります。

Citrix XenServer and Open Source XenServer

・ .outファイル
既存のFortiAnalyzer VMインストーラをアップグレードするためのファームウェアです。

・ .out.OpenXen.zipファイル
新規のFortiAnalyzer VMインストーラのためのパッケージとなります。
Open Source Xen Server のために、QCOW2ファイルが含まれています。

・ .out.CitrixXen.zipファイル
新規のFortiAnalyzer VMインストーラのためのパッケージとなります。
このパッケージにはCitrix XenServer Disk (VHD)やOVF filesが含まれています。

Linux KVM

・ .outファイル
既存のFortiAnalyzer VMインストーラをアップグレードするためのファームウェアです。

・ .out.kvm.zipファイル
新規のFortiAnalyzer VMインストーラのためのパッケージとなります。
qemu. のために、QCOW2ファイルが含まれています。

Microsoft Hyper-V Server

・.outファイル
既存のFortiAnalyzer VM インストーラをアップグレードするためのファームウェアです。

・.hyperv.zip
新しいFortiAnalyzer VM インストーラのためのパッケージをダウンロード。このパッケージは Microsoft Hyper-V Server向けのVirtual Hard Disk (VHD) ファイルを内蔵しております。

VMware ESX/ESXi

・.out
既存のFortiAnalyzer VM インストーラをアップグレードするためのファームウェアです。32bitもしくは64bit のファームウェアイメージをダウンロードします。

・.ovf.zip
新しいFortiAnalyzer VM インストーラのためのファームウェアです。32bitもしくは64bitのパッケージをダウンロードします。このパッケージはVMware向けのOpen Virtualization Format (OVF)とデプロイ中にOVFファイルによって使用される二つのVirtual Machine Disk Format (VMDK)ファイルを内蔵しております。

詳しくは以下のURLをご参照下さい。
http://www.fortinet.com/products/fortianalyzer/index.html.

8. サポート機種

FortiAnalyzer Version5.0 MR2 Patch4 は以下の機種をサポートします。

FortiOS FortiOS Carrier	version5.0 MR2 以降、version5.0 以降、version4.0 MR3 Patch2 以降
FortiMail	version5.0 MR2 Patch4、version5.0 MR1 Patch5、version5.0 Patch8
FortiWeb	version5.0 MR3 Patch7、version5.0 MR2 Patch4、 version 5.0 MR1 Patch4、version 5.0Patch6
FortiClient	version5.0 MR2 以降、version5.0 Patch4 以降
FortiManager	version5.0 MR2 以降、version5.0 以降
FortiSandbox	version 1.0 MR4 以降

9. サポート仮想環境

FortiAnalyzer-VM は下記の仮想環境をサポートしております。

- Citrix XenServer 6.2
- Linux KVM Redhat 6.5
- Microsoft Hyper-V Server 2008 R2, 2012, and 2012 R2
- OpenSource XenServer 4.2.5
- VMware
  - ESX versions 4.0 and 4.1
  - ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, and 6.0

10. 推奨 Web ブラウザ

FortiAnalyzer Version5.0 Patch9 での推奨 Web ブラウザは下記の通りです。

・Microsoft Internet Explorer versions 11
・Mozilla Firefox version 40
・Google Chrome version 45

上記以外のブラウザを利用する場合、動作は保障致しかねます。

以上