フリービットクラウド VDC
FortiGateログ可視化テンプレート
ご利用マニュアル

Ver.1.02

フリービット株式会社

Confidential

本マニュアルでは、フリービットクラウド VDC FortiGate 可視化テンプレートで提供される仮想マシンについて、お客様側で以下の設定を行うための手順をご案内します。

OS テンプレート名　：　FortigateAnalyzer (kibana)
推奨スペック　　：　Disk 50GB, CPU：1 コア, メモリ：2GB

1　Docker コンテナの再起動

仮想マシンの起動時に、Docker コンテナが自動的に起動されますので、基本的には、起動・停止の操作は不要です。データ保存期間を変更した場合には、Docker を手動で再起動してください。

```
sudo service docker-compose start # 起動

sudo service docker-compose stop # 停止

sudo service docker-compose restart # 再起動
```

2　データの保存期間を変更

データの保存期間を変更したい場合には、/opt/FortiAnalyzer/docker/docker-compose.yml 内の RETENTION_DAYS の設定値を変更してください。(デフォルトは 31 日間保存)

```
cron:

  build: docker_build/delete_cron

  links:

    - esmaster:es

  volumes:

    - /etc/localtime:/etc/localtime:ro

  environment:

    - RETENTION_DAYS=31  # ここを修正
```

変更後に

```
cd /opt/FortiAnalyzer/docker

sudo /usr/local/bin/docker-compose up -d cron
```

を実行してください。

3　SSL 証明書のインストール

SSL 証明書を利用される場合には、証明書を作成し、

/opt/FortiAnalyzer/docker/conf/nginx/conf.d/に置いてください。

```
$ cd /opt/FortiAnalyzer/

$ openssl req -new -days 365 -x509 -nodes -keyout cert.key -out cert.crt

$ mv cert.key cert.crt docker/conf/nginx/conf.d/
```

4　BASIC 認証(HTPASSWD 作成)

初期設定で BASIC 認証を有効にしており、以下のユーザ ID とパスワードが設定されています。

ユーザ ID：FA

パスワード：password

変更される場合には、htpasswd を作成し、/opt/FortiAnalyzer/docker/conf/nginx/conf.d/に置いてください。

```
$ htpasswd -c htpasswd user_name

$ mv htpasswd docker/conf/nginx/conf.d/
```

－ FortiGate 可視化テンプレートのサポート範囲につきまして －

FortiGate 可視化テンプレートは、FortiGate の syslog を可視化するために必要な、kibana をはじめとする各種ミドルウェアがインストールされた状態でご提供いたします。

インストールされている kibana には予め、汎用的にご利用いただくことのできるグラフ表示のための visualization 設定が、登録されています。登録済みの visualization は、Web ブラウザで kibana にアクセスし、visualize 画面で Load Saved visualization(フォルダの形をしたアイコン)をクリックしていただくことで表示できます。全般的なマニュアルも visualization から参照いただけます。

なお、お客様側で新規に visualization 設定を作成していただくこともできますが、具体的な手順についてはサポート外とさせていただきますので、ご了承ください。

kibana はオープンソースですので、、インターネット上からも各種情報の入手が可能です。