

FortiADC E シリーズ設定手順書

FortiADC E シリーズ

FortiADC 4.2 系対応版
(Equalizer 10.3.2 系対応版)

Ver. 1.0

目次

1	改訂履歴	5
2	はじめに	6
3	初期設定	7
3.1	機器の設置	7
3.2	FortiADC のポート構成・ネットワーク構成	7
3.3	ターミナルエミュレーターの設定	8
3.4	初期設定 (CLI)	8
3.4.1	シリアルコンソールログイン	8
3.4.2	VLAN の設定	9
3.4.3	VLAN subnet の作成および接続プロトコルの許可設定	10
4	GUI の操作	11
4.1	FortiADC GUI へのアクセス	11
4.2	FortiADC GUI の画面表示について	12
4.2.1	画面構成	12
4.2.2	右クリック操作	12
4.2.3	ドラッグ&ドロップ操作	13
4.2.4	Help ボタンについて	13
4.3	FortiADC GUI からのログアウト	13
5	CLI の操作	14
5.1	FortiADC CLI への SSH によるアクセス	14
5.2	Context およびプロンプト表示	14
5.3	show コマンドによる情報表示	15
5.4	コンテキストのヘルプ表示	16
5.5	設定の反映手順	17
5.5.1	グローバルコンテキストから設定	17
5.5.2	各設定のコンテキストから設定	17
5.6	キュー状態のコマンド	17
5.7	設定の削除・リセット	18
5.8	パラメータの変更	18
5.9	コマンドの補完	19
5.10	Flag の操作	20
6	System 設定	21
6.1	Global タブ	21
6.1.1	Dashboard	21
6.1.1.1	System Information	21
6.1.1.2	Virtual Server Summary	21
6.1.1.3	CLI Console	21
6.1.1.4	System Resources	22
6.1.1.5	Event log Console	22
6.1.1.6	Virtual Server Network Throughput	22
6.1.2	Alerts Configuration	22
6.1.2.1	Alert の設定	23
6.1.2.2	アラート通知タイプ	24
6.1.2.3	アラートの設定	25
6.1.2.4	SMTP リレーの設定	25
6.1.3	Certificates	26
6.1.3.1	Certificate 作成	27
6.1.3.2	Certificate 更新	28
6.1.3.3	Certificate 削除	28
6.1.4	CRL	28
6.1.5	Parameters	28
6.1.6	Server Side Encryption	29
6.1.7	Smart Controls(保留)	29
6.1.8	SNMP	29
6.2	External Services タブ	29

6.2.1	SMTP Relay	30
6.2.2	VLB Manager	30
6.3	Maintenance タブ	30
6.3.1	Date & Time	30
6.3.2	Backup & Restore	30
6.3.2.1	バックアップ取得手順	31
6.3.2.2	リストア手順	31
6.3.2.3	CLI による復元	33
6.3.3	Manage Software	35
6.3.4	Tools	35
6.4	Network タブ	35
6.4.1	Interfaces タブ	35
6.4.2	Aggregation	36
6.4.3	VLAN の追加	36
6.4.3.1	Subnet の追加・変更	36
6.4.3.2	“Configuration”タブ	37
6.4.3.3	“Failover”タブ	37
6.4.3.4	“Permitted Subnets”タブ	38
6.4.3.5	“Static Routes”タブ	38
6.4.3.6	“NAT”タブ	39
7	サーバー設定	41
7.1	サーバーの新規追加	41
7.2	サーバーの設定変更	41
7.2.1	“Configuration > Settings”タブ	41
8	サーバープール設定	43
8.1	サーバープールの新規追加	43
8.2	サーバープールの設定変更	44
8.2.1	“Configuration > LB Policy”タブ	44
8.3	サーバーインスタンスの追加	44
8.3.1	サーバープールから追加する手順	45
8.3.2	サーバープールから追加する手順	45
8.4	サーバーインスタンス設定	46
8.4.1	“Configuration > Settings”タブ	46
9	クラスタ設定	47
9.1	クラスタの新規追加	47
9.2	クラスタの設定変更	47
9.2.1	“Configuration > Summary”タブ	47
9.2.2	“Configuration > settings”タブ	48
9.2.3	“Configuration > Persistence”タブ	49
9.2.3.1	tcp/udp/l7tcp クラスタの場合	49
9.2.3.2	http/https クラスタの場合	49
9.2.4	“Configuration > Timeouts”タブ	51
9.2.5	“Security > Certificate”タブ (https クラスタのみ)	51
9.2.6	“Security > SNI”タブ (https クラスタのみ)	52
9.2.7	“Security > SSL”タブ (https クラスタのみ)	53
9.3	クラスタへのサーバープール追加	53
9.4	クラスタのステータス確認 (Cluster Summary)	53
10	Health Check 設定	54
10.1	ICMP Health Check	54
10.1.1	ICMP Health Check 追加	54
10.1.2	ICMP Health Check 設定	55
10.1.3	TCP Health Check	56
10.1.3.1	TCP Health Check 追加	56
10.1.3.2	TCP Health Check 設定	56
10.1.3.3	TCP Health Check 計算式について	57
10.1.4	ACV Health Check	58

10.1.4.1	ACV Health Check 追加.....	58
10.1.4.2	ACV Health Check 設定.....	58
10.1.4.3	TCP Health Check 計算式について.....	59
10.1.4.4	ACV のテストについて.....	60
10.1.5	Health Check の登録.....	60
10.1.5.1	Default 登録.....	60
10.1.5.2	手動での登録対象.....	60
10.1.5.3	手動での登録方法.....	61
11	Failover 設定.....	62
11.1	Failover 動作の基本概念について.....	62
11.1.1	Primary 役、Backup 役について.....	62
11.1.2	デフォルト Primary、デフォルト Backup について.....	62
11.1.3	冗長化の通信(heartbeat)について.....	62
11.1.4	Failover ペア同士のコンフィグ同期について.....	62
11.1.5	Primary への切り替え動作について.....	63
11.2	Failover 設定の事前準備について.....	63
11.3	Failover 設定.....	64
11.3.1	VLAN/Subnet 設定.....	64
11.3.2	Peer 名設定.....	65
11.3.3	Signature 情報の取得(デフォルト Backup).....	65
11.3.4	デフォルト Primary 機の Flag 設定.....	65
11.3.5	Peer の登録(デフォルト Primary).....	66
11.3.6	デフォルト Backup 機の Flag 設定.....	66
11.3.7	Peer の登録(デフォルト Backup).....	67
11.3.8	Failover 状態の確認.....	67
11.3.9	Peer のヘルスチェック設定.....	68
12	Log & Report.....	69
12.1	Log & Reports.....	69
12.1.1	Logging タブ.....	69
12.1.1.1	Event Log.....	69
12.1.2	Notification.....	69
12.1.2.1	Notification の通知.....	69
12.1.2.2	通知の表示.....	70
12.1.2.3	Notification の削除.....	71
12.1.2.4	Remote Syslog.....	72
12.1.3	Reporting タブ.....	72
13	その他操作手順.....	73
13.1	touch パスワードのリセット方法.....	73
13.2	FortiADC 初期化方法.....	74

1 改訂履歴

変更履歴

番号	変更年月日	Version	Page	status	変更内容	作成	承認
1	2015/04/15	1.0		O	新規作成	NWD	
2							
3							
4							
5							

status: a(dd), d(elete), r(eplace), o(ther)

2 はじめに

本手順書は、FortiADC E シリーズ製品の日本語設定手順書です。

本設定手順書を使用する事で FortiADC の設置・設定・運用を行うことができます。本文書は FortiADC を設定し運用を行えるように構成されていますので、記述内容はメーカーから提供されている「Handbook for FortiADC E series」とは異なる事がありますので予めご了承下さい。

詳細な説明につきましては「Handbook for FortiADC E series」をご参照頂きます様お願い致します。ダウンロードは弊社 TEC-World FAQ 内から行うことができます。また、FortiADC の GUI にある上部メニューから“Help > Context Help”を選択することで同様の内容を閲覧することができます。

本手順書の GUI 表示については、デフォルトの英語表記での設定手順書とさせていただきます。日本語表示にてご使用されている場合は、言語切り替えなどを必要に応じて実施ください。

また、本手順書以外に TEC-World 内の FAQ にも情報を公開していますので、そちらも参照ください。

本手順書は、予告なしに記載内容に変更がある場合がありますので、予めご了承下さい。

3 初期設定

本章では機器の起動から GUI へのアクセス準備までを説明します。

3.1 機器の設置

FortiADC のインストールは以下の手順で行います。

1. 同梱されているラックマウント用の金具やケーブル等を箱から取り出します。同梱されていたパッケージはそのまま捨てずに保存して下さい。機器初期不良などの理由で機器を返送する際、オリジナルのパッケージが揃っていないと対応出来ない場合が御座いますので、ご了承下さい。（また、ハード機器に変更点の確認された場合、保証対象にならない場合が御座います。）
2. 平らな場所を選んで FortiADC を設置します。
3. 同梱されているシリアルケーブルを使用する際に、FortiADC の前面に「Serial」と書かれている差込み口がありますので、そこに付属のシリアルケーブルを差込みます。TeraTerm Pro 等のターミナル・エミュレータ・ソフトウェア等を使用して設定を行います。
4. FortiADC に同梱されている電源コードを使用して、適切な電源へ接続して下さい。この FortiADC 電源ユニットは 50Hz/60Hz、100~240 VAC 入力に対応しています。
5. 後面パネルにある電源接続すると電源が**自動投入**されます。
※モデルによりスイッチの有無が異なります
※スイッチがある場合はスイッチを ONI にして下さい。

3.2 FortiADC のポート構成・ネットワーク構成

FortiADC はモデルによって筐体前面のポート構成が異なります。

筐体表示	ポート番号
100E	1 - 4
300E	1 - 6
400E	1 - 8
600E/1000E	1 - 8 2 SFP+ 1 管理ポート

3.3 ターミナルエミュレーターの設定

FortiADC を設置し電源を投入した後、ターミナルもしくはターミナルエミュレーターを使用して設定を行います。FortiADC の設定に必要なターミナルもしくはターミナルエミュレーターの設定値は以下の通りです。

項目	設定内容
Baud rate	9600
Data	8 bit
Parity	None
Stop	1 bit
Flow control	None

※Equalizer LX シリーズは Baud rate は **38400** となります。

ターミナルソフトとしては無料で配布されている TeraTerm などを使用することも可能です。

3.4 初期設定 (CLI)

GUI へアクセスするため機器に IP アドレスを設定します。この作業は eqcli と呼ばれる CLI 画面から実施します。機器に同梱されているシリアルケーブルを使用し、機器のシリアルポートに接続します。

3.4.1 シリアルコンソールログイン

デフォルト管理ユーザー名、touch でログインします。パスワードは touch です。

```
Username: touch
Password:
Login successful.

FortiOS v4.2,build0049

eqcli >
```


3.4.2 VLAN の設定

VLAN を作成するコマンドは以下です。

```
vlan [VLAN 名] vid [VID 番号]
vlan [VLAN 名] ifi [interface 名] type [tagged or untagged]
```

項目	設定内容
vlan	作成する VLAN の名前を入力します
vid	作成する VLAN に割り当てる VLAN ID を入力します
ifi	使用インターフェースを指定してポート番号を入力します
type	VLAN に割り当てるタイプを tagged/untagged に指定します

以下の例では Ext という VLAN を VLAN ID 1 で作成し、その後その VLAN に port 1(if01)を untagged で割り当てます。

```
eqcli > vlan Ext vid 1
eqcli > vlan Ext ifi if01 type untagged
```

※スイッチモジュールのないモデルについては、1 ポートに対して、1つの untagged VLAN のみ割当て可能です。

Interface 名については以下の[show interface] コマンドで確認ができます。以下は 300E の出力例で、一番左の項目が各ポート1からの interface 名となります。

※上位モデルの場合表示が異なるため、確認してください。

```
eqcli > show interface

Interface Duplex Mode Speed Status
if01      full          100M Link Up
if02      NA            NA    Link Down
if03      NA            NA    Link Down
if04      NA            NA    Link Down
if05      NA            NA    Link Down
if06      full          100M Link Up
eqcli >
```

3.4.3 VLAN subnet の作成および接続プロトコルの許可設定

VLAN subnet を作成し IP アドレスおよびデフォルトゲートウェイ IP などを設定します。

```
vlan [VLAN 名] subnet [subnet 名] ip [IP アドレス] services [許可プロトコル]
vlan [VLAN 名] subnet [subnet 名] route [ディスティネーション IP アドレス/CIRD] gw [ゲートウェイ IP アドレス]
```

項目	設定内容
vlan	subnet を作成する VLAN の名前を入力します
subnet	作成する subnet 名を入力します
ip	subnet に割り当てる IP アドレスを入力します
route	デフォルトゲートウェイ IP アドレスを入力します。 入力フォーマットは「<dest_cidr>[src <src cidr>] gw <ip_addr> [flags prefer]」で Static Route の設定も同様に行います。
services	この subnet IP へアクセス可能なサービスを入力します。 <ul style="list-style-type: none"> - HTTP - HTTPS - SSH - SNMP - Envoy(ライセンスがある方のみ) - Envoy Agent(ライセンスがある方のみ)

以下の例では「Ext」という VLAN に external という subnet を設定し、IP アドレスは 172.16.0.200/21 を割り当て、デフォルトゲートウェイは 172.16.0.1 にしています。この IP アドレスへのアクセスは SSH/HTTP のみ有効にしています。

```
eqcli > vlan Ext subnet external ip 172.16.0.200/21 services ssh,http
eqcli > vlan Ext subnet external route 0/0 gw 172.16.0.1
```

以上で VLAN および subnet の設定は完了です。VLAN を割り当てたポートにケーブルを挿し周辺機器との接続性を確認します。コマンド ping を CLI から実行することができます。

```
eqcli > ping 172.16.0.1
```

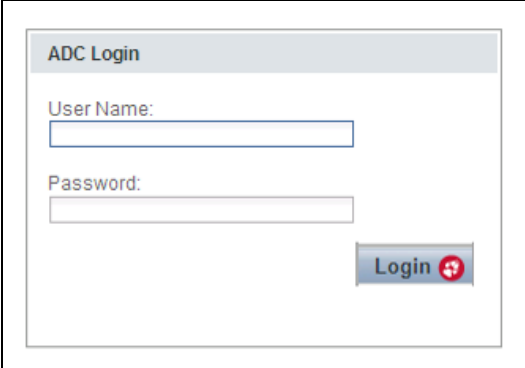
4 GUI の操作

初期設定の完了後は、FortiADC の設定・管理等は GUI から行ないます。サポートされているウェブブラウザは以下の通りです。サポートバージョンは安定バージョンの最新 2 バージョンです。

- Firefox
- Internet Explorer

4.1 FortiADC GUI へのアクセス

ウェブブラウザを使用し、GUI へアクセスします。ブラウザでは JavaScript が有効になっている事を確認下さい。アクセスするとログイン画面が表示されますので、デフォルトで設定されているアカウント touch を使用してログインします。デフォルトパスワードは touch です。

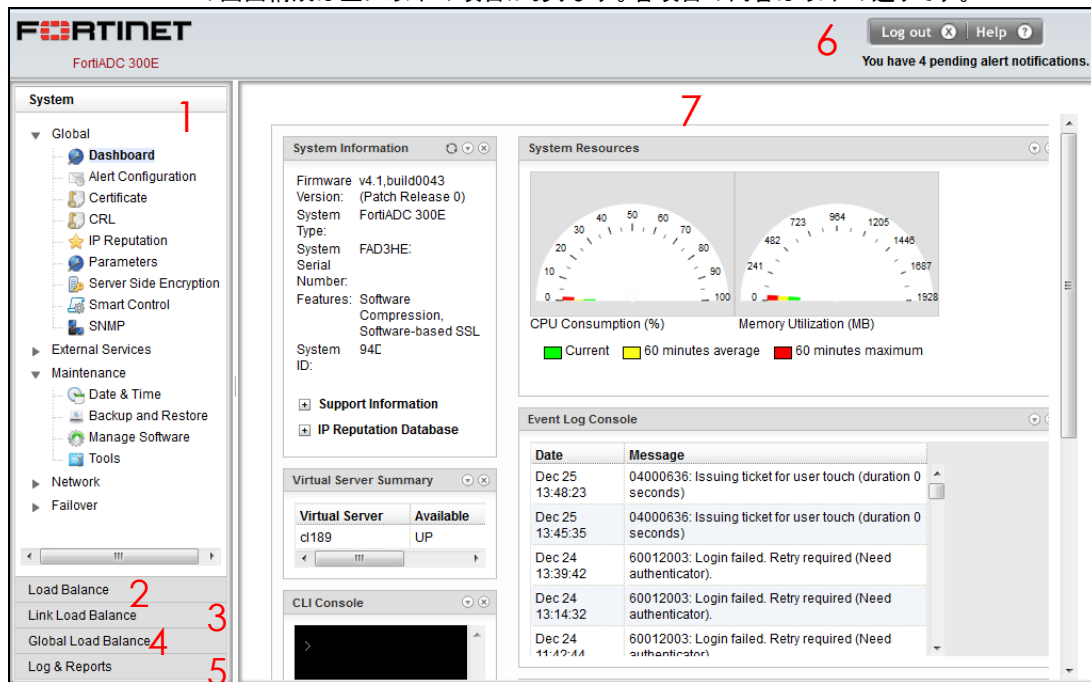


The screenshot shows a web browser window with the title "ADC Login". Inside the window, there is a form with two input fields. The first field is labeled "User Name:" and the second is labeled "Password:". Below the password field is a "Login" button with a red arrow icon pointing to the right.

4.2 FortiADC GUI の画面表示について

4.2.1 画面構成

GUI の画面構成は主に以下の項目があります。各項目の内容は以下の通りです。



左フレーム

右フレーム

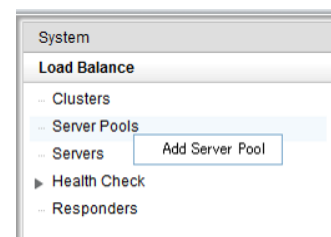
左フレーム: 設定の大項目など項目の表示

右フレーム: 左フレームで選択した内容の詳細情報の表示

1. System: グローバル設定の画面表示
2. Load Balance: バランシング設定の画面表示
3. Link Load Balance: 回線負荷分散設定の画面表示(サポート対象外)
4. Global Load Balance: グローバルロードバランスの設定の画面表示(サポート対象外)
5. Log&Reports: ログ情報の画面の表示
6. ログアウト、画面更新、資料ダウンロードなどの操作を行います
7. 左フレームで選択した項目の詳細が表示されます。タブから大項目・小項目を選択します。

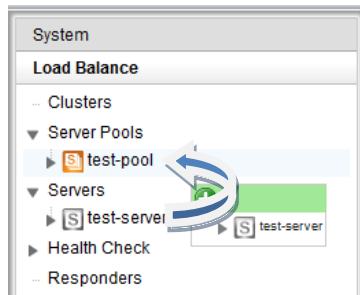
4.2.2 右クリック操作

左フレームの項目を右クリックすることでメニューが表示されます。下の図はサーバープールで右クリックした際の表示です。新規追加(add)や既存設定の削除(delete)、項目の展開・折り畳み(Expand/Collapse)をすることが可能です。



4.2.3 ドラッグ & ドロップ操作

項目によってはドラッグ & ドロップすることで設定することが可能です。下の図は、サーバー「test-server」をドラッグ & ドロップでサーバープール「test-pool」へ追加しています。この他にもサーバープールをクラスタへ追加する、Responders をクラスタへ追加する等が可能です。



4.2.4 Help ボタンについて

Help ボタンをクリックするとメニューが表示されます。「About」を選択するとトップページに戻りファームウェアバージョン等を確認することができます。「Context Help」を選択すると現在右フレームに表示されている設定項目の英文マニュアルを参照することができます。

[Help]→[About]を選択した際には以下の画面へ推移し、機器の情報が確認できます。

項目	設定内容
Firmware Version	ファームウェアバージョンが表示されます
Firmware Tag	ファームウェア追加情報が表示されます(RELEASE、patch 等) ※ EQOS のみ表示
System Type	機器のモデルが表示されます
System Revision	機器のリビジョンが表示されます ※EQOS のみ表示
System Serial Number	機器のシリアル番号が表示されます
System ID	機器の System ID が表示されます
Features	オプション情報が表示されます

4.3 FortiADC GUI からのログアウト

画面右上にある「Logout」ボタンをクリックすることでログアウトします。

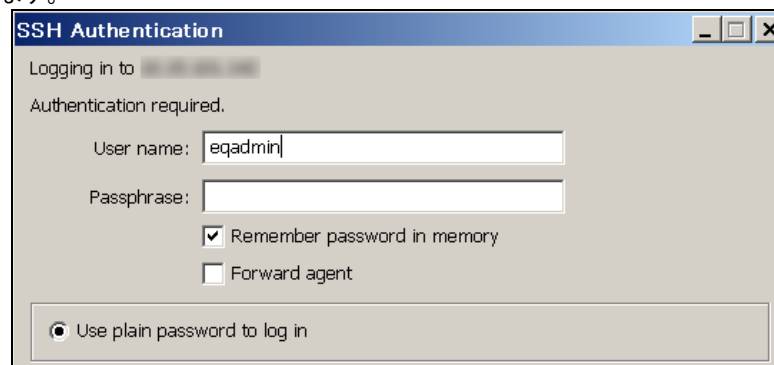
5 CLI の操作

本章では簡単な CLI の操作方法について説明します。CLI は eqcli と呼ばれますが、本書では CLI に統一しています。

5.1 FortiADC CLI への SSH によるアクセス

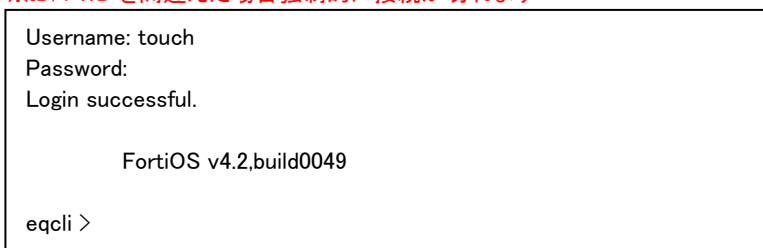
[ターミナルエミュレーターの設定](#)、および[初期設定 \(CLI\)](#) のとおり、CLI へのアクセスはシリアルケーブル経由で行います。サブネットに設定している IP アドレスに対して SSH 通信を行うことで、遠隔からのログインも可能です。SSH 経由でのアクセスを行う場合は、そのサブネットのサービス設定で SSH が有効になっている必要があります。

以下は Tera Term を使用し SSH 経由でログインする手順です。サブネットの IP アドレスへ SSH 接続すると以下のように認証画面が表示されます。ユーザー名は eqadmin と入力し、パスワードは空欄のまま継続します。



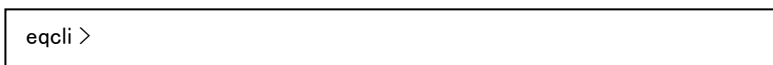
FortiADC の認証画面が表示されますので、設定しているユーザー名とパスワードを入力します。ログインに成功すると以下のような画面になり、プロンプトが「eqcli >」となります。デフォルトでは ID/PWD は touch/touch となっております。

※ID/PWD を間違えた場合強制的に接続が切れます



5.2 Context およびプロンプト表示

CLI はコンテキストの概念をベースに作られており、現在のコンテキストによって使用できるコマンドが変化します。現在のコンテキストはプロンプトに表示されます、以下の図は CLI へログインした直後に表示されるコンテキストです。



これはグローバルコンテキストであることを示しています。すべてのコマンドをこのコンテキストから実行可能で、かつグローバル設定(DNS や NTP など)を実行することも可能です。他のコンテキストに移行することも可能です、以下の例はクラスター「cl-1」のコンテキストに移行しています。

```

eqcli > cluster cl-1
eqcli cl-cl-1>

```

この状態で入力できるコマンドはクラスタ設定に関するのみになり、設定はクラスタ「cl-1」にのみ影響します。コンテキスト名が 4 文字以上の場合は以下のようにアスタリスク(*)によって省略されます。コマンド context を使用するとコンテキストが省略されずに表示されます。

```

eqcli > cluster mycluster
eqcli cl-myc*>

eqcli cl-myc*> context
12000416: The current context is: 'mycluster'
eqcli cl-myc*>

```

5.3 show コマンドによる情報表示

コマンド show を使用することで現在のコンテキストで設定されている情報を表示することができます。グローバルコンテキストで実行すると以下ようになります。

```

eqcli > show

Variable          Value

hostname          XXXXX
~後略~
eqcli >

```

コマンド show に続けてグローバルコンテキスト以外のパラメータを入れると概要の情報が表示されません。

```

eqcli > show cluster

Name          IP Address      Port  Proto

cl-test-tcp  10.15.100.183  80    tcp

eqcli >

```

コンテキストからコマンド show を実行すると、そのコンテキストの情報が表示されます。以下はクラスタ「cl-test-tcp」で実行した際の結果です。

```

eqcli > show cluster cl-test-tcp
This cluster has a problem:
Cluster configuration is incomplete

L4 Cluster Name : cl-test-tcp
Protocol        : tcp
IP Address      : 10.15.100.183
Port           : 80
Port Range     : 0
Preferred Peer  : ADC300E-181
VID            : 1
Server Pool    :
Sticky Timeout : 0
Sticky Netmask : 32
Idle Timeout   : 60
Stale Timeout  : 30
Flags         :
eqcli >

```

5.4 コンテキストのヘルプ表示

各コンテキストで ? を入力することで、使用可能なコマンドとその説明が表示されます。以下の例はグローバルコンテキストで実行した場合です、グローバル設定が表示されます。

```

eqcli >
alerts          : Global Enable/Disable alerts.
agr             : Add or modify an AGR or interface instance.
backup         : Upload a system backup to remote FTP.
~後略~

```

クラスタのコンテキストから実行した場合は、以下のようにクラスタ設定が表示されます。

```

eqcli cl-cl-*>
age            : Set the cookie age for a cluster.
certificate    : Attach a certificate to an HTTPS cluster. Required for HTTPS
                clusters.
cipherspec    : Set the cipherspec for an HTTPS cluster.
~後略~

```

グローバルコンテキストから、クラスタ設定の入力途中に実行した場合でも、同様にクラスタ設定が表示されます。

```

eqcli > cluster cl-test-tcp
age            : Set the cookie age for a cluster.
certificate    : Attach a certificate to an HTTPS cluster. Required for HTTPS
                clusters.
cipherspec    : Set the cipherspec for an HTTPS cluster.
~後略~

```

コマンドの途中で実行した場合は、そのコマンドの説明が表示されます。


```

eqcli > cluster cl-test-tcp stats
stats: Display the statistics for a cluster.

Syntax: cluster <name> stats

```

5.5 設定の反映手順

CLI から設定を行う場合、現在のコンテキストによって手順が異なり、以下 2 つの手順があります。

- ・ グローバルコンテキストから完全なコマンドを実行する。
- ・ 各設定のコンテキストから各コマンドを個別に入力し、commit を実行する。

5.5.1 グローバルコンテキストから設定

各設定には、必須パラメータ(required)が存在します。グローバルコンテキストから必須パラメータを入力することで設定が可能です。以下はサーバー「server-1」を作成するコマンドと表示結果です。「Operation successful」が表示されれば、パラメータに問題はなく、設定が反映されています。

```

eqcli > server server-248 proto tcp ip 10.15.101.248 port 80

eqcli: 12000287: Operation successful
eqcli >

```

上記図では必須パラメータは赤色で記されています。各サーバー設定の内容は以下の通りです。

パラメータ	設定内容
proto	サーバーが使用するプロトコルを指定します。tcp または udp から選択します。
ip	サーバーの IP アドレスを指定します。
port	サーバーのポート番号を指定します。

5.5.2 各設定のコンテキストから設定

各設定のコンテキストへ移行してから、必須パラメータを入力することで設定を行います。設定後にコマンド commit を実行することで、設定が反映されます。以下の例ではサーバー「server-1」を作成しています。

```

eqcli > server server-248
eqcli sv-ser*> proto tcp
eqcli sv-ser*> ip 10.15.101.248
eqcli sv-ser*> port 80
eqcli sv-ser*> commit

eqcli: 12000287: Operation successful
eqcli sv-ser*> exit
eqcli >

```

5.6 キュー状態のコマンド

グローバル以外のコンテキストで入力されたコマンドは、内部でキューされている状態になり、commit を実行することで設定に反映されます。また exit や <ctrl+d> でコンテキストを抜けることでも反映されます。キューされたコマンドを設定に反映しないためには quit を使用します。

以下の例は commit を実行せず、exit でグローバルコンテキストに戻った場合の動作です。メッセージ「Operation successful」が表示され、設定が反映されています。

```
eqcli > server server-248
eqcli sv-ser*> proto tcp
eqcli sv-ser*> ip 10.15.101.248
eqcli sv-ser*> port 80
eqcli sv-ser*> exit

eqcli: 12000287: Operation successful
eqcli >
```

以下の例は quit を使用した場合の動作です、設定は**反映されず**にコンテキストを移動します。

```
eqcli > server server-248
eqcli sv-ser*> proto tcp
eqcli sv-ser*> ip 10.15.101.248
eqcli sv-ser*> port 80
eqcli sv-ser*> quit
eqcli >
```

5.7 設定の削除・リセット

設定の削除や、設定パラメータをデフォルト値に戻すにはコマンドの前に no を入れて実行します。以下の例ではホスト名(hostname)設定をデフォルトの値にし、サーバー「server-1」を削除しています。

```
eqcli > no hostname

eqcli: 12000287: Operation successful
eqcli >
eqcli > no server server-248

eqcli: 12000287: Operation successful
eqcli >
```

クラスタコンテキストの設定を削除する場合は、グローバルコンテキストから行うことが可能です。以下の例ではクラスタ「cl-test-tcp」を削除しています。同じことを各コンテキストに移動してから実行することも可能です。

```
eqcli > no cluster cl-test-tcp

eqcli: 12000287: Operation successful
eqcli >
```

5.8 パラメータの変更

設定変更は、同じコマンドで、変更パラメータの再入力を行います。以下の例では、VLAN 名 VLAN-1 を「VID 10」で作成した後に、「VID 20」に変更しています。変更できないパラメータについては、設定を削除してから再作成する必要があります。

```
eqcli > show vlan

Name  VID

Ext   1
Int   2
eqcli > vlan Int vid 3

eqcli: 12000287: Operation successful
eqcli > show vlan

Name  VID

Ext   1
Int   3
eqcli >
```

5.9 コマンドの補完

スペースキー(<space>) やタブキー(<tab>)をコマンド入力時に使用することで、コマンドの補完が行われます。以下のように、途中で <space> または <tab> を使用すると、

```
eqcli > host<space>
```

host 以降のコマンドが補完されます。

```
eqcli > hostname
```

コマンドの途中で実行した場合はコマンド候補が表示されます、以下の例はグローバルコンテキストで c および con を入力した場合です。

```
eqcli > c<space>
certificate cfg_convert cluster context cri
```

5.10 Flag の操作

殆どのコンテキストには Flag 設定が存在します、これは「有効」または「無効」で設定されるパラメータです。サーバー「server-1」の Flag 設定を変更し、probe_13 を有効にするコマンドは以下の通りです。エクスクラメーションマーク ! をパラメータの前に付与することで、設定を無効にできます。複数の Flag を設定する場合はカンマで区切り入力します。

```
eqcli > show vlan Ext subnet ext
This subnet is enabled.

Subnet Name           : ext
Subnet Flags          : heartbeat, command
Services Flags        : http, https, ssh, fo_http, fo_https, fo_ssh
~後略~
eqcli > vlan Ext subnet ext services !https

eqcli: 12000287: Operation successful
eqcli > show vlan Ext subnet ext
This subnet is enabled.

Subnet Name           : ext
Subnet Flags          : heartbeat, command
Services Flags        : http, ssh, fo_http, fo_https, fo_ssh
~後略~
eqcli >
```

6 System 設定

本章では FortiADC の System 設定について説明します。GUI 左フレームの上部にある[System]内の各タブをクリックすることで表示されます。

6.1 Global タブ

機器全体の設定についてのタブです。

6.1.1 Dashboard

FortiADC の現在の状況を簡易的に表示します。[×]印で項目を削除したり、ブロックの場所を変更しても、[Dashboard]をクリックしますと元に戻ります。

6.1.1.1 System Information

ログインしている機器の基本情報を表示します

パラメータ	設定内容	
Firmware Version	ファームウェアのバージョン表示	
Firmware Tag	ファームウェアのタグ情報表示 ※EQOS のみ表示	
System Type	機器モデルの表示	
System Serial Number	機器のシリアル番号の表示	
Features	ハードウェアオプションの表示	
System ID	機器のシステム ID の表示	
Support Information	Last Refresh Date	情報更新日
	Hardware Support End	ハードウェアサポート終了日
	Hardware Support Level	ハードウェアサポートレベル
	Firmware Support End	ファームウェアサポート終了日
	Firmware Support Level	ファームウェアサポートレベル
	Enhanced Support End	エンハンスサポート終了日
	Enhanced Support Level	エンハンスサポートレベル
IP Reputation Database ※使用には別途契約必要	Last Refresh	最終更新日
	Database Version	取得 DB のバージョン

※サポート終了日がお客様の契約と異なっている場合がございますが、お客様との保守契約とは別となりますので、あらかじめご了承ください。

6.1.1.2 Virtual Server Summary

設定中のクラスタ IP のステータス状況を表示します。

パラメータ	設定内容
Virtual Sever	クラスタ名が表示されます。
Availiable	UP/DOWN ステータスの状況を表示します。
Pool	クラスタに紐付いている Pool 名を表示します。
Current Session	現在のセッション数が表示されます。

6.1.1.3 CLI Console

GUI 経由で簡易的な CLI の操作が可能です。全てのコマンド実行は出来ません。実際のコマンドは SSH など実際に CLI にログインしての操作を推奨します。

6.1.1.4 System Resources

CPU 及びメモリの使用状況を、以下 3 項目を順に緑・黄・赤色で表示します。

- Current (緑色)
- 60 minutes average (黄色)
- 60 minutes maximum (赤色)

6.1.1.5 Event log Console

直近のイベントログが表示されます。

Date	Message
「月 日 時:分:秒」を表示します。 例) Feb 10 13:59:30	エラーコードとメッセージを表示します。 例) 20000180: Server Web01 being marked L3 Down

6.1.1.6 Virtual Server Network Throughput

直近 30 分のトラフィックの状況をクラスタ別に表示します。プルダウンボックスから確認したいクラスタ名を選択します。

Active Connections	アクティブな接続数を赤色で表示します。
Connections/second (CPS)	秒間あたりの接続数を桃色で表示します。
Transactions/second (TPS)	秒間あたりのトランザクション数を緑色で表示します。

6.1.2 Alerts Configuration

アラート・オブジェクトを登録する事で、イベント発生をトリガーとして指定した処理を実行します。例えば、サーバー死活監視によるアップ・ダウン判定やフェイルオーバーのステータス変更が発生した場合にシスログサーバーやメールで通知します。

デフォルトで以下の 5 つのアラートが touch アカウントに設定されております。

- デフォルトアラート設定
 - ・ al_allpeers
 - ・ al_allfogrps
 - ・ al_allservers
 - ・ al_allsis
 - ・ al_allports

※デフォルトの設定については FAQ に公開しておりますので、以下のリンクから参照ください。

※ユーザーの追加については FAQ に公開しておりますので、以下のリンクから参照ください。

TEC-World へのアクセスは[こちら](#)

FortiADC を利用の方は以下の FAQ を参照下さい。

※TEC-World へのログインが必要です。

デフォルト設定については[デフォルトの Alert 設定について(FortiADC)]を参照

ユーザー追加については[ユーザ追加/パスワード変更方法(FortiADC)]を参照

Coyote を利用の方は以下の FAQ を参照下さい



※TEC-World へのログインが必要です。

デフォルト設定については[デフォルトの Alert 設定について(EQ/OS 10)]を参照

ユーザー設定については[ユーザ追加/パスワード変更方法(EQ/OS 10)]を参照

6.1.2.1 Alert の設定

アラートの設定画面では以下のような画面となります。
それぞれの項目について案内します。

- ・ アラートを追加する場合
アラートを追加する場合は、 アイコンをクリックする
- ・ アラートを修正する場合
アラートを修正する場合は、修正したいアラートをクリックして、 アイコンをクリックする

内容については、共通項目のため、以下に記載いたします。

パラメータ	設定内容
Disable	有効にすると該当の Alert を無効にします。 デフォルト: 無効
Alert Type	Exception と State Change の二つの項目がございます。ステータスが変った際に通知するかどうかとなります。基本的には両方にチェックを入れていただくことで Alert が検知されます
Alert Target	
Target Object Type	<ul style="list-style-type: none"> ▪ Failover Group: Active/Active 構成の時に使用 デフォルト Alert: al_allfogrps ▪ Interface: フロントパネルのスイッチポートの UP・DOWN 判定や内部基盤ボードのポート DOWN の際に Alert が生成されます デフォルト Alert: al_allports

	<ul style="list-style-type: none"> ▪ Peer: Failover ステータスの変化の際に Alert が生成されます デフォルト Alert: al_allpeers ▪ Server: Server 単体でのステータスの変化で Alert が生成されます デフォルト Alert: al_allservers ▪ Server Instance: Server Pool 内のステータスの変化で Alert が生成されます デフォルト Alert: al_allsis
Target Object Name	設定しているクラスタ名やサーバー名を指定します。ワイルドカードで [*]も使用できます。デフォルトのアラートを参考にしてください。

6.1.2.2 アラート通知タイプ

Email、syslog、snmp、ui の 4 つがアラート通知タイプとしてサポートされています。一つのアラート設定に複数の通知タイプを設定する事が可能です。

1. **email** ー定義された宛先に、設定された SMTP リレーメールサーバーを使ってメールを送信します。
※メールサーバー設定は別途設定が必要です
2. **syslog** ーアラートメッセージをシスログサーバーへ送信します。
※syslog サーバー設定は別途設定が必要です
3. **snmp** ーSNMP トラップメッセージを管理端末に送信します。詳細は後述の SNMP 設定を確認します。
4. **CLI & WebUI** ーui のアラート通知タイプは CLI コンソールにアラートを表示させます。

6.1.2.3 アラートの設定

アラートを設定する為のオブジェクト名指定の際にワイルドカードが利用可能です。これでワイルドカードに適合する全てのオブジェクトを一つのアラートとして設定が可能です。例えば、以下のアラート設定例があります。
※FAQ にデフォルトのアラートの設定については公開していますので参照ください。

```
eqcli> user touch alert al_allports state enable object *:interface alert_type
exception,state_change notify_type ui,syslog
```

上記設定は 300E のスイッチポートのアラート設定例で、ワイルドカードが使用されています。ワイルドカード使用時の制限として、オブジェクト名の唯一の文字か最接尾文字でなければなりません。(例えば、object *sv* というのは許可されません。)

以下はアラート設定の確認コマンドになります。

```
eqcli > show user touch alert al_allports
Alert Name           : al_allports
Alert State          : Enabled
Objects              : *:interface
Alert Type           : exception, state_change
Notify Type          : ui, syslog
From Email Address   :
Email Addresses      :
Subject              :
Smart Controls Objects : None
```

6.1.2.4 SMTP リレーの設定

Email アラート設定で定義するメール受信者に対してメールを送信するには SMTP リレーが必須です。SMTP リレーを設定に必要な情報は以下になります。
GUIでの設定については [SMTP Relay](#) を参照

6.1.2.4.1 SMTP リレーの設定 (CLI)

- SMTP サーバーの IP アドレス、もしくは FQDN 名が必要で、FQDN 設定時には FortiADC に DNS が必須となります。
- インカミングメールの受信ポートの設定が必須となります。(通例、25 番ポートです。)

現在、一つの SMTP リレー設定がサポートされています。CLI コマンドの SMTP リレー設定フォーマットは以下になります。

```
eqcli > ext_services smtp_relay <name> server <IP_or_FQDN> port <number>
```

例えば、postmaster という名前の SMTP リレーサーバーの IP アドレスが 10.0.0.111 で、通常のポート番号を使用している場合の設定は以下です。

```
eqcli > ext_services smtp_relay postmaster server 10.0.0.111 port 25
```

SMTP リレー定義の表示は以下になります。

```

eqcli > show ext_services smtp_relay postmaster
Name : postmaster
Server : 10.0.0.111
Port : 25
eqcli>

```

SMTP リレー定義の削除は以下になります。

```

eqcli > no ext_services smtp_relay postmaster

```

既存の SMTP リレー定義を修正する場合には、修正したい新しい値を定義します。例えば、postmaster の IP アドレスを変更したい場合には以下になります。

```

eqcli > ext_services smtp_relay postmaster server 172.16.0.123

```

6.1.3 Certificates

FortiADC の HTTPS クラスタで使用する証明書情報の管理を行うタブです。サーバー証明書と秘密鍵のファイルを 1 組の Certificate 情報としてアップロードします。(HTTPS クラスタへの適用の仕方は、別途、["Security > Certificate" タブ](#) をご確認ください。

Certificate の登録に必要なものは最大 4 点です。


- CSR 作成時に使用した秘密鍵(※パスワードを設定している場合はパスワードも必要)
- CA によって発行されたサーバー証明書
- 中間証明書(※必要な場合)
- クロスルート証明書(※必要な場合)

FortiADC の証明書管理は秘密鍵ファイルと証明書ファイルの 2 ファイルを管理します。証明書ファイルはサーバー証明書(必須)及び中間証明書/クロスルート証明書(必要であれば)をつなげた証明書ファイルです。

なお、FortiADC4 系(Coyote10 系)では CSR/秘密鍵の**作成はできない**ため、サーバー等で作成を行ってください。

パラメータ	設定内容
Name	アップロードする証明書の名前を設定します。これは FortiADC 管理上、表示される名前です。
Certificate File	証明書ファイルを選択します、これはテキスト形式のファイルです。中間証明書及びクロスルート証明書をご利用の場合は、サーバー証明書に続けて貼り付けて 1 つのファイルにします。
Key File	秘密鍵ファイルを選択します、これはテキスト形式のファイルです。

6.1.3.1 Certificate 作成

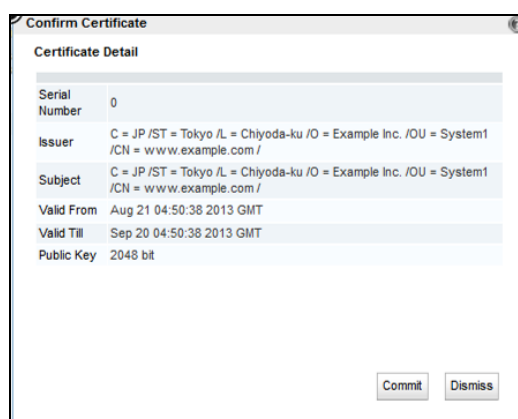
1. 左フレームの System タブから Certificate をクリックします。
2. Certificates タブが表示されましたら、右側の  アイコンをクリックします。




3. Add Certificate が表示されます。

4. Certificate 名 (test) を入力し、証明書インストール準備の②で用意した2つのファイル、secret.key と certificate.pem、を Certificate File と Key ファイルに参照し、Commit をクリックします。
5. 秘密鍵作成時にパスワードを入力した場合、以下のように入力画面が表示されます。パスワードを入力して下さい。

6. 証明書確認の画面が表示されますので、内容に問題がなければ Commit ボタンを押下します。これでサーバー証明書オブジェクトの test の登録が終了です。
※クラスタに実際に紐づける場合は、クラスタ設定を参照ください



6.1.3.2 Certificate 更新

サーバー証明書を更新する場合は、該当の証明書を表示させて  ボタンをクリックし、再度証明書をアップロードします。

証明書については複数作成可能ですので、更新ではなく別証明書をアップしての運用も可能です。

6.1.3.3 Certificate 削除

サーバー証明書を削除する場合は、該当の証明書を選択して  をクリックして削除します。

または、左フレームの Certificate 名を右クリック [Delete Certificate] で削除が可能です。

ただし、HTTPS クラスタにて使用中の場合は、クラスタの紐づけを削除することで削除が可能となります。

6.1.4 CRL

HTTPS クラスタに設定する CRL (Certificate Revocation List / 証明書失効リスト) をアップロードします。CRL を使用することで証明書が現在も有効かどうかを確認することができます。また CRL は複数の HTTPS クラスタで使用することが可能です。

CRL をアップロードするには「Add CRL」ボタンをクリックし、Name を入力し CRL File をアップロードします。

6.1.5 Parameters

各パラメータを設定いたします。

パラメータ	設定内容
Hostname	ホスト名を設定します。
Locale	GUI 表示の言語を変更できます (英語[en]/日本語[ja])
Firewall Rules	Firewall の設定 デフォルト enable のままを推奨
DNS	DNS サーバーを 3 つまで登録可能です。 Primary, Secondary, Tertiary の順に追加してください
Global Service Settings	FortiADC へアクセスするプロトコルの一括設定を行います、デフォルトは全て有効です。 VLAN の Subnet 毎に設定する場合は本設定を有効にして、各 VLAN の Subnet で無効にします。

6.1.6 Server Side Encryption

日本でのサポート対象外となります。
※100E は非対応

6.1.7 Smart Controls

今後記載予定

6.1.8 SNMP

SNMP 設定を行います。

パラメータ	設定内容
System Name	FortiADC の管理者名を入力します。
Community String	コミュニティ名を設定します。SNMP マネージャのコミュニティ名が正しくない場合はポーリングが成功しませんのでご注意ください。
System Contact	FortiADC の責任者名を入力します。
System Location	機器の設置場所を入力します。
System Description	機器情報を入力します、任意の項目です。

FortiADC プライベート MIB をダウンロードするには、GUI にアクセスしているブラウザから以下の URL へアクセスして下さい。


※バージョンにより変更している可能性もあるため、詳細は各 Handbook を参照
<http://<fortiADCのIP>/eqmanual/<mibName>.my>

<mibName>.my の一覧
CPS-EQUALIZER-v10-MIB.my
CPS-REGISTRATIONS-v10-MIB.my
HOST-RESOURCES-MIB.my
HOST-RESOURCES-TYPES.my
IANAifType-MIB.my
IF-MIB.my
INET-ADDRESS-MIB.my
IP-MIB.my
RFC1155-SMI.my
RFC1213-MIB.my
SNMPv2-CONF.my
SNMPv2-MIB.my
SNMPv2-SMI.my
SNMPv2-TC.my
TCP-MIB.my
UDP-MIB.my

6.2 External Services タブ

外部サーバーとの連携時に使用する設定を行います。
CLI で設定する場合は [SMTP リレーの設定 \(CLI\)](#) を参照

6.2.1 SMTP Relay

メール通知による Alert を使用する場合、メールサーバーを SMTP Relay として設定を行います。右上にある  ボタンをクリックすると新規作成画面が表示されます。

パラメータ	設定内容
SMTP Server Name	設定するメールサーバーの名前を入力します。
SMTP Server IP Address	設定するメールサーバーの IP アドレスを入力します。
SMTP Server Port	設定するメールサーバーの TCP ポート番号を入力します。

ユーザーアカウントに紐づける場合は、CLI にログインしていただき、以下のように設定します。ユーザー毎に一つしか紐づけることができません。

```
eqcli > user <ユーザー名> mail_server <SMTP Server Name>
```

例

```
eqcli > user touch mail_server mail
```

6.2.2 VLB Manager

VLB Manager を利用する場合は、設定を行います。

6.3 Maintenance タブ

機器の管理を行う場合に使用します。

6.3.1 Date & Time

機器の時刻設定を行います。各項目にある「Reset」ボタンをクリックすることで、現在の設定を表示することが出来ます。

パラメータ	設定内容
Set Time Zone	機器のタイムゾーンを設定します、デフォルトは UTC です。日本の場合 Asia/TOKYO または Japan に設定
Manually Set Date and Time	手動で時刻設定をおこないます、設定のフォーマットは mm/dd/yyyy hh:mm:ss です。 表示されている時間は、この画面へアクセスしたときの時間 例) 2015 年 1 月 2 日 14 時 55 分 00 秒の場合 01/02/2015 14:55:00
Automatically Set Date and Time	「NTP Server」に使用する NTP サーバーを指定します。IP アドレスまたは FQDN で設定が可能です。その後「Enable NTP Synchronization」のチェックを有効にすることで、NTP サーバーとの同期が有効になります。 デフォルト: pool.ntp.org

6.3.2 Backup & Restore

FortiADC のバックアップファイルの取得や、取得したバックアップファイルで FortiADC をリストアさせる手順の説明です。設定ファイルのバックアップ先やリストア元は、それぞれ、FTP サーバーへアップロードを行うか、GUI を操作するローカル端末を指定する事が可能です。

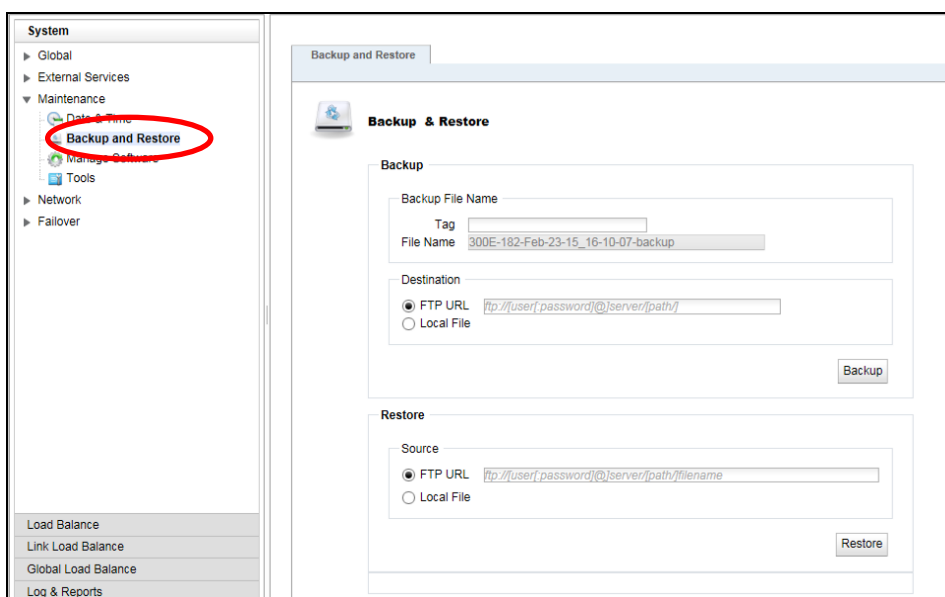
リストア時には、GUI よりリストア出来ない旨表示される場合があります。その際には「[CLI によるリ](#)

ストア」を参照します。

パラメータ	設定内容
Backup	機器からバックアップファイル(コンフィグファイル)を取得します。 ・Tag: バックアップファイルに個別で判別用の tag を付与します。 ・File Name: バックアップファイルの名前が表示されます。 ・Destination FTP URL: FTP サーバーにファイルを保存します。 ・Local File: ローカル PC にファイルをダウンロードします。 ※バックアップファイルに SSL 証明書/秘密鍵は保存されません
Restore	機器へバックアップファイルのリストアを行います。 ・Source FTP URL: FTP からリストアファイルをダウンロードします Local File: ローカル PC からファイルをアップロードします

6.3.2.1 バックアップ取得手順

1. System > Maintenance > Backup and Restore をクリックすると、画面中央に「Backup & Restore」が表示されます。



2. バックアップ内の宛先から Local File を選択してバックアップボタンをクリックします。
3. 保存先を選択して終了です。デフォルトのバックアップファイル名は「<FortiADC ホスト名>-<月>-<日>-<年>-<時>-<分>-<秒>-backup.cps」になります。
備考: タグ空欄に文字を入力すると FortiADC ホスト名と月の間に該当文字列が入力されます。バックアップ名は以下のフォーマットになります。
 <FortiADC Host 名>-<タグ入力文字>-<月>-<日>-<年>-<時>-<分>-<秒>-backup.cps
 また、宛先に FTP URL を入力する事も可能です。

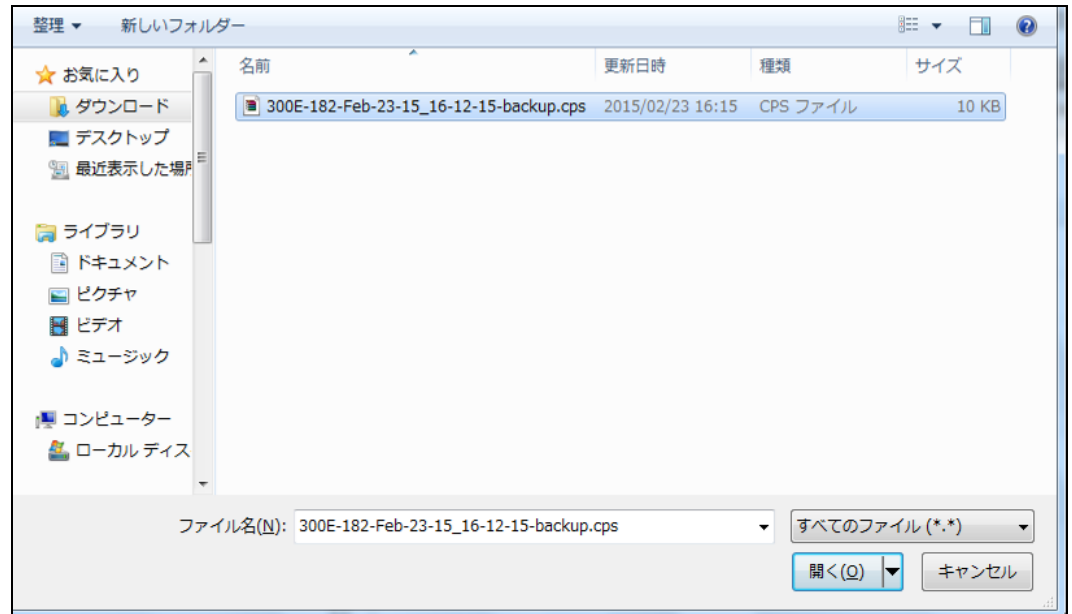
6.3.2.2 リストア手順

6.3.2.2.1 設定のリストア

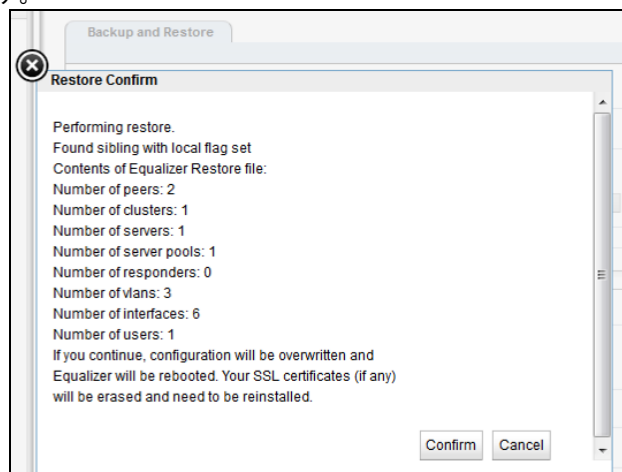
リストアする為に、事前に FortiADC のウェブ管理インターフェースにアクセスが出来るようにしておきます。機器のインターフェース設定が無い場合には、Network タブの章と

VLAN の追加を参照してインターフェースにアクセスできるように準備します。

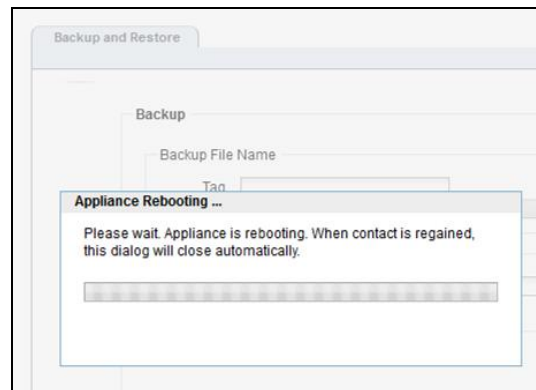
1. System > Maintenance > Backup and Restore をクリックすると、画面中央に「Backup and Restore」が表示されます。
2. Restore 内の Source から Local File を選択したら、復旧したい Backup File を選択して、開くをクリックします。



3. リストアの確認画面が表示されますので、問題が無ければ Confirm をクリックして続きます。



4. 機器が再起動します。起動すると、IP の変更がない場合は通常のログイン画面になります。IP アドレスはリストアファイルに合わせて対応してください。



5. **(必要な場合)**証明書を使用している場合は、再度証明書/鍵ファイルをアップロードしてください

6.3.2.3 CLI による復元

V4.2 以降では、ローカルの意味を持つフラグがバックアップファイルに付加されています。また、冗長化構成時のバックアップファイルには Peer 情報を含む為、どの設定で復旧させるのかを選択する事が可能です。

GUI による復旧時に「Cannot use GUI to restore this backup. You must use the CLI. Please select 'Cancel'」のエラー表示が出力される場合には、ここで説明する手順で復旧を行ってください。

CLI で復旧を行う場合には、バックアップファイルを流し込む為、FTP サーバーとバックアップファイルを用意します。バックアップファイルはルートディレクトリに保存しておきます。

1. CLI で eqcli にログインを行います。

```
Username: touch
Password:
Login successful.

FortiOS v4.2,build0049

eqcli >
```

2. restore url <url> name <Backup_FileName> を実行します。
FTP にID/PWD を設定されている場合は <ftp://ID:PWD@IP/> と定義します。

```
※restore コマンドのヘルプ
eqcli > restore
restore: Restore a system backup from remote FTP.

Syntax:  restore url <url> name <name>

        <url> := location to upload backup image

        for example: ftp://10.0.0.121/

        <name> := the full file name of the restore image

eqcli >
※restore の実施
eqcli > restore url ftp://ID:PWD@IP/ name ADC100E-backup.cps
Performing restore.
Downloading ftp://ID:PWD@IP/ADC100E-backup.cps
```

```

Connected to xxx.xxx.xxx.xxx.
~中略~
local: ADC100E-backup.cps remote: ADC100E-backup.cps
229 Entering Extended Passive Mode (|||52839|)
150 Opening data channel for file download from server of "/ADC100E-backup.cps"
100% |*****| 9842 105.76 KiB/s 00:00 ETA
226 Successfully transferred "/ADC100E-backup.cps"
9842 bytes received in 00:00 (105.54 KiB/s)
221 Goodbye

```

備考: 上記出力は xxx.xxx.xxx.xxx で設定された FTP サーバーのルートディレクトリに保存されている 100E-backup.cps のバックアップファイルで FortiADC を復旧するシナリオです。

3. バックアップファイルが展開され、バックアップファイルの内容が表示されます。復旧を継続する場合、「y」を選択して FortiADC 設定を復旧させます。

```

Contents of Equalizer Restore file:
Number of peers:          1
Number of clusters:      2
Number of servers:       2
Number of server pools:  1
Number of responders:    1
Number of vlans:         2
Number of interfaces:    4
Number of users:         1

If you continue, configuration will be overwritten and
Equalizer will be rebooted. Your SSL certificates (if any)
will be erased and need to be reinstalled.

Are you sure you want to continue with the restore? [y/N]:
y

```

4. バックアップファイルから設定が展開され、機器が再起動します。復元作業は終了です。

```

Are you sure you want to continue with the restore? [y/N]:
y
Removing SSL data:
Restoring files:
etc/eq/responders
etc/eq/responders/test.html
etc/eq/smart_control
etc/eq/snmp
etc/eq/snmp/snmpd.cnf
etc/eq/logo_custom.png
etc/eq/eq.conf
tar: ustar vol 1, 10 files, 32768 bytes read, 0 bytes written in 1 secs (32768 bytes/sec)
Restore completed. Rebooting.
Shutdown NOW!
shutdown: [pid 13145]
~中略~
syncing disks... done
rebooting...

```

再起動後リストアした設定で起動してきます。

6.3.3 Manage Software

FortiADC ファームウェアの情報を表示します。

パラメータ	設定内容
Current Boot Image	現在起動している Partition が表示されます (A または B)。また、現在の Partition で動作している FortiADC のバージョン情報が表示されます。
Upgrade	ファームウェアのアップグレードを実施します。ファームウェアを FortiADC へアップロードする方法を選択します。 ※アップグレードのファイル等は FAQ に公開しています。

6.3.4 Tools

機器シャットダウンや再起動などのオペレーションを行います。

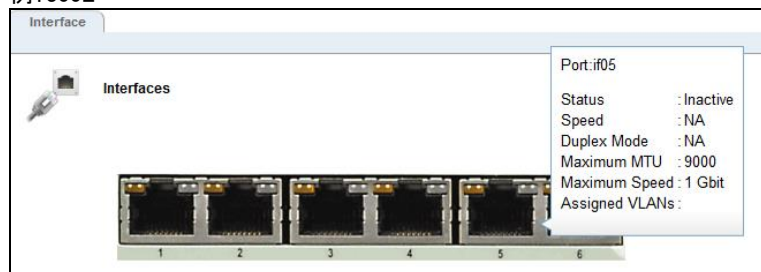
パラメータ	設定内容
Halt/Shutdown System	機器の【シャットダウン】を実行します。「Halt」ボタンをクリックすると確認が表示されますので「Continue」ボタンをクリックし確定します。
Reboot System	機器の【再起動】を実行します。「Reboot」ボタンをクリックすると確認が表示されますので「Continue」ボタンをクリックし確定します。
Save System State	FortiADC の機器情報をダウンロードすることができます。ヘルプデスク等にご連絡頂いた場合などではこちらのファイルを取得するご依頼をさせて頂く事がございます。 <ul style="list-style-type: none"> • Save State File Name: Save State のファイルに Tag を付与します。 • File Name には Save State ファイルの名前が表示されます。 • Destination Local: ローカル PC に Save State ファイルをダウンロードします FTP URL: FTP サーバーにファイルを保存します。

6.4 Network タブ

本章では Network タブについて説明します。Network タブでは FortiADC の VLAN インターフェースや物理ポートを割り当てます作成された VLAN に Subnet を設定することで、基本的な設定が終了し通信を行えるようになります。

6.4.1 Interfaces タブ

機器のネットワークインターフェース設定および状態確認を行います。表示されている画像のポートにカーソルを合わせるとステータスが表示されます。
例: 300E



パラメータ	設定内容
Port	ポート番号とインターフェース名が表示されます。
Status	リンクアップ状態が Active/Inactive で表示されます。

Speed	現在のポートスピードが 1000Mbit/100Mbit/10Mbit で表示されます。
Duplex Mode	現在のポート Duplex が Full/Half で表示されます。
Maximum MTU	現在の MTU 設定が表示されます。
Maximum Speed	最大速度が表示されます。
Assigned VLANs	ポートが所属している VLAN の情報が表示されます。

画像のポートをクリック(選択)することで、ポートに対する設定変更を行うことが可能です。設定項目は以下のようになっています。

パラメータ	設定内容
Speed	ポートの速度設定を 1000Mbit/100Mbit/10Mbit から選択します。
Duplex Mode	ポートの Duplex 設定を Full/Half から選択します。

6.4.2 Aggregation

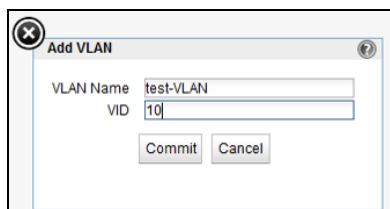
Link Aggregation を使用する場合は、この画面で設定を行います。

6.4.3 VLAN の追加

VLAN 設定の追加は以下の通りに行います。設定項パラメータの内容は以下の通りです。
 なお、HA 構築をする場合は、VLAN の設定は **HA 間で機器 IP アドレス以外(VLAN 名や Subnet 名)は全て統一**する必要があります。

パラメータ	設定内容
tagged	ポートを tag で VLAN に割り当てます。
untagged	ポートを untag で VLAN に割り当てます。
VID	VLAN の ID 番号を設定します、1~4094 の間で設定します(必須)。

GUIの左フレームの「VLANs」タブ上で右クリックし「Add VLAN」を選択します。以下のウィンドウが表示されますので、VLAN 名と VID 番号を入力し Commit をクリックします。



画面が更新されポート設定が表示されますので、ポートの割り当て設定を行います。

パラメータ	設定内容
Port	筐体の物理ポート番号です。
Status	VLAN を割り当てるポートで「assigned」にチェックを入れます。
Type	tagged ポート、untagged ポートの選択を行います。

1VLANに複数ポート設定したい場合は、CLIより該当のVLANにポートを割り当てる必要があります。
 ※[スイッチモデル](#)のみ対応(E350GX/E450GX/E650GX)

6.4.3.1 Subnet の追加・変更

設定した VLAN に subnet を作成することで IP 通信を行うことが可能になります。Subnet 単位でデフォルトゲートウェイやアクセスプロトコルの設定を行います。作成された Subnet がある場合、左フレームから該当の Subnet をクリックし、右フレームに表示されるタブから設定変更が可能です。

左フレームから subnet を追加したい VLAN を右クリックし、「Add Subnet」をクリックします。以下のダイアログが表示されますので、Subnet 名と IP アドレスを入力します。

(VLAN Name は VLAN インターフェースを追加した際の名前です。上記の例では「default」となっています。)

パラメータ	設定内容
Name	subnet の名前を設定します。
IP Address	subnet の IP アドレスを入力します。
Services on IP Address	有効にしたサービスプロトコルを使用して、subnet の IP アドレスへアクセスが可能になります。SNMP は 1 つの subnet のみ有効にすることができます。

6.4.3.2 “Configuration”タブ

設定した Subnet を選択すると以下画面が表示されます。

6.4.3.3 “Failover”タブ

Failover に関連する設定を行います、パラメータは以下の通りです。

Failover を設定する場合は両機器でこの項目を統一する必要があります。
その他に、[VLAN 名] [subnet 名] [VLAN 設定 interface] も同じである必要があります。

パラメータ	設定内容
Failover IP Address	両機器で共有する仮想 IP アドレスを設定します、これは サーバーのゲートウェイ IP アドレスとして主に使用されます。
System Services on the Failover IP Address	有効にしたサービスプロトコルを使用して、Failover IP Address へアクセスが可能になります。SNMP は機器で 1 つの subnet のみ有効にすることができます。
Heartbeat	subnet 上で Failover を有効にします。
Heartbeat Interval	冗長化している Peer 間で行う Heartbeat の間隔を秒数でしています(デフォルト 2 秒)。
Failed Probe Count	Peer がダウン判定されるまでに Heartbeat が失敗する回数を指定します(デフォルト 3)。

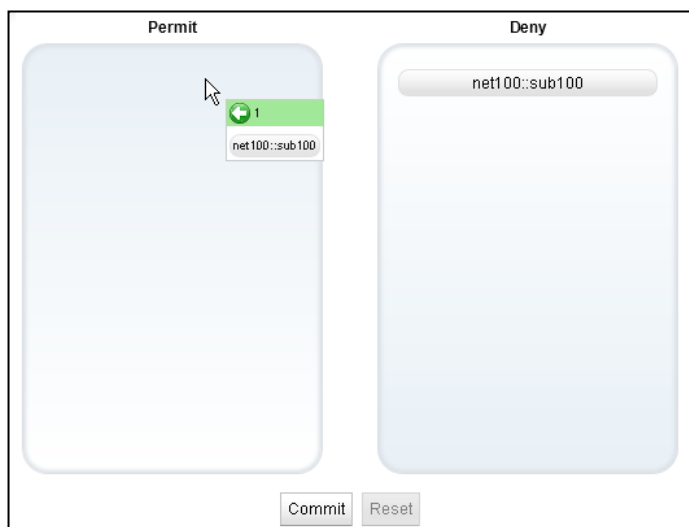
6.4.3.4 “Permitted Subnets”タブ

subnet 間の通信許可設定を行います。デフォルトでは subnet への通信はすべて拒否(Deny)設定になっていますが、subnet を「Deny」リストから「Permit」リストへドラッグ&ドロップすることで該当 subnet からの通信を許可します。


図では、VLAN「net100」に所属する subnet「sub100」からの通信を許可させるためドラッグ&ドロップしています。双方向で通信を行うためには、もう片側の subnet でも同様に許可する必要があります。

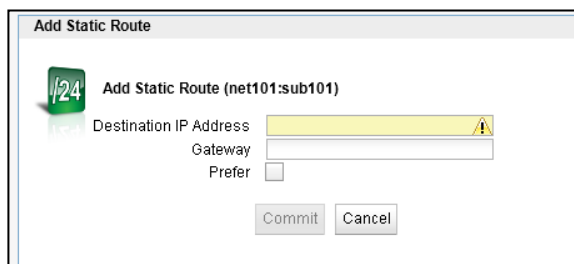
設定後、画面下部の commit ボタンをクリックし決定します。

HA の場合は同期対象ではないため、両機器で実施する必要があります。



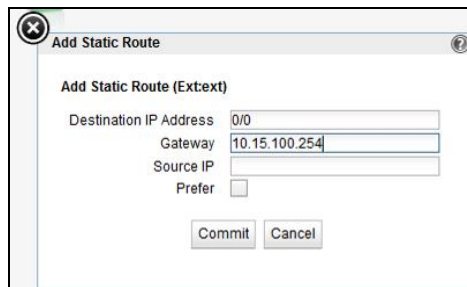
6.4.3.5 “Static Routes”タブ



宛先による静的ルーティングを設定します。ボタン  をクリックすることで、以下のようなルーティング追加ウィンドウが表示されます。



パラメータ	設定内容
Destination IP Address	宛先 IP アドレスを設定します、CIDR 表記で記載します。 例) 192.168.100.1/32
Gateway	ゲートウェイとして使用する宛先 IP アドレスを指定します。
Prefer	この設定を有効にすることで、FortiADC に接続されている subnet であっても優先的にルーティングさせることができます。

デフォルトゲートウェイは以下の例のように【0/0】で設定を行います。



ルーティングを追加するとリストとして表示されます。設定の変更を行うにはリストから該当ルーティングを選択し、 からボタンをクリックします。削除を行うには選 択してボタンをクリックします。

HA の場合は同期対象ではないため、両機器で実施する必要があります。

6.4.3.6 “NAT”タブ

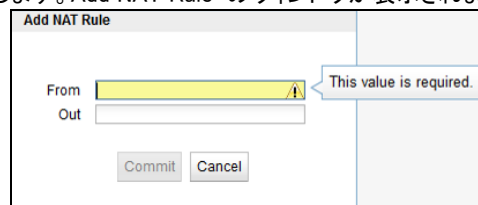
FortiADC のサブネットインターフェースを経由する通信に対して Outbound NAT IP アドレスを設定出来ます。デフォルトでは無効設定で、何もリストには存在していない状態です。Internal セグメントのルート設定が無い場合のサーバー群が External ネットワークに NAT をする事で通信が行えるようになる場合に、この設定を有効にすると FortiADC がサブネットを経由する全てのパケットを変換して通信を成立させます。該当する全てのパケットを変換しますので、パフォーマンスに影響がある可能性があります。

HA の場合は同期対象ではないため、両機器で実施する必要があります。

サーバーIP アドレス群は Outbound NAT の IP にそのサブネットに存在する FortiADC 実 IP、フェイルオーバーゲートウェイ IP、そしてクラスター IP を指定する事が可能です。設定が必要なサブネットを左フレームから選択し、サブネットの NAT タブを選択して下さい。

Outbound NAT 設定手順は以下になります。

1. + ボタンをクリックします。Add NAT Rule のウィンドウが表示されます。



2. 「From」に IP アドレスを入力します。個々の IP アドレスでも、CIDR 形式で入力する事も可能です。
(例) 192.168.0.1 もしくは 192.168.0.0/24 の入力フォーマットです。)
3. 「Out」に Outbound NAT IP アドレスとして指定したい IP アドレスを入力します。FortiADC 実 IP アドレス、フェイルオーバーゲートウェイ IP アドレス、クラスター IP アドレスを指定して下さい。**この3種類以外の設定についてはサポート対象外となります。**

eqcli で設定する場合には以下のフォーマットで入力します。

```
vlan <vlan-name> subnet <subnet-name> nat from [<ip>,<ip_cidr>] [upto
<ip>] out <outbound_nat_ip>

eqcli >vlan SAMPLE_EXT subnet test_subnet nat from 192.168.1.0/24 out
10.15.0.254

eqcli: 12000287: Operation successful
```

備考: NAT 設定では編集ボタンがありません。設定の間違いがあった場合には、一旦削除して、NAT の再設定を行って下さい。

7 サーバー設定

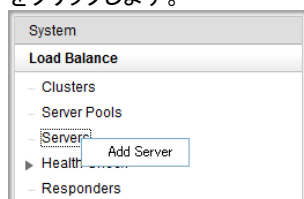
本章では FortiADC のサーバー設定について説明します。

サーバーの基本的な設定として対応プロトコル、IP アドレス、ポート番号です。この設定を行うと L3 レベル (ICMP)によるヘルスチェックがデフォルトで追加されます。サーバーをサーバープールに所属させることで、クライアントからのリクエストを負荷分散させることが可能になります。

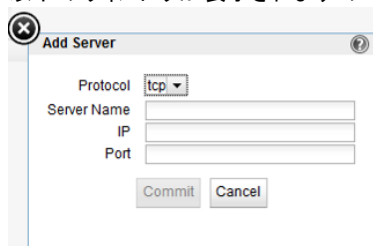
ヘルスチェックについては [Health Check 設定](#) を参照

7.1 サーバーの新規追加

GUI からサーバーの追加を行うには、左フレーム「Servers」を右クリックし、表示される「Add Server」をクリックします。



以下のウィンドウが表示されますので入力し、Commit ボタンをクリックします。



パラメータ	設定内容
Protocol	サーバーが受け付けるプロトコルを TCP/UDP から指定します。
Server Name	サーバーの名称を任意で指定します。
IP	サーバーの IP アドレスを指定します。
Port	サーバーのポート番号を指定します。

7.2 サーバーの設定変更

左フレームからサーバーを選択すると、右フレームに詳細設定画面が表示されます。

7.2.1 “Configuration > Settings”タブ

サーバーの基本設定を行います。サーバー名とプロトコル以外の設定を変更することができます。

パラメータ	設定内容
VID	サーバーが所属する VLAN の ID が表示されます(変更不可)。
Protocol	サーバーが受け付けるプロトコルです(変更不可)。
IP	サーバーの IP アドレスを指定します。
Port	サーバーのポート番号を指定します。
Maximum Reused	HTTP Multiplexing 有効時に、再利用される接続プー

Connections	ルの最大数を設定します(1~65535)。デフォルトは0で再利用されるコネクション数に制限はありません。
Reused Connections Timeout	再利用可能接続プールのエントリーがアイドル状態になった場合に、クローズするまでの時間を秒数で指定します。デフォルトは0で、再利用可能接続プールのエントリーはタイムアウトしません。

8 サーバプール設定

本章では FortiADC のサーバプール設定について説明します。

前章で設定したサーバーを所属させることで、クラスタ(次章参照)への通信を負分散させることが可能になります。負分散ポリシーやヘルスチェックプローブ設定、また各サーバーの詳細設定もサーバプールから行います。

8.1 サーバプールの新規追加

GUI からサーバプールの追加を行うには、左フレームの「Server Pool」を右クリックし、表示される「Add Server Pool」を選択します。

ウィンドウが表示されますので、必要な項目を設定し commit ボタンをクリックします。



パラメータ	設定内容
Server Pool Name	サーバプールの名称を任意で設定します。
Policy	サーバプールに所属するサーバーへの負分散ポリシーを設定します。各パラメータの説明は以下の通りです。
round-robin	デフォルトの負分散アルゴリズムです。設定ファイルの該当クラスタ所属サーバーの登録順に上から順に振り分けが行われ、最後のサーバーまで振り分けが行われると最初の登録サーバーに戻って通信を処理します。サーバーが Down した場合にはそのサーバーを負分散サーバーのリストから除外して負分散処理を継続します。 round robin はサーバーの Initial Weight/Current Weight 値には影響されず負分散を行なう静的なアルゴリズムです。サーバーのレスポンス時間やコネクション数に関わらず動作します。
Static	各サーバー個別に設定された weight 値を基に負分散を行います。高い weight 値が設定されたサーバーに対しては高い割合でリクエストが振り分けられます。設定された Initial Weight 値を考慮しランダムに振り分けを行なうイメージです。
Adaptive	FortiADC 独自のアルゴリズムになり、以下3つの要素を基に最適な振り分け先サーバーを判断します。 <ul style="list-style-type: none"> Server response time サーバーからの応答時間です。 Active connection count サーバーに振られているアクティブ接続数です。 Server agent value サーバーで起動しているサーバーエージェントデーモンによって返される数値です

Response	サーバーのレスポンス時間をもっとも短いサーバーに対して高い確率で負荷分散されます。ただし、仮に FortiADC が一度にそのリクエストを対象サーバーに振ってしまうと、そのサーバーの負荷が一度に上がってサーバーのレスポンス時間が遅くなる結果を招く可能性があります。このことから FortiADC はクラスタ単位でこのレスポンス時間を最適化します。 この負荷分散アルゴリズムでは FortiADC はアクティブ接続数と（設定がされていれば）サーバーエージェント値を確認します。しかし両数値が adaptive で運用するよりも小さな影響になります。あるサーバーのレスポンス時間がそのクラスタ内で一番早かったとしてもアクティブ接続数が大きい場合やサーバーエージェント値が高い数値の場合には FortiADC は新規セッションをそのサーバーに振らない事があります。
least-cxns	サーバーのアクティブ接続数をもっとも少ないサーバーに対して高い確率で負荷分散されます。ただし、fastest response の様に FortiADC は該当するサーバーがこの振り分けによってレスポンスを落とさない様にサーバーのアクティブ接続数やサーバーエージェント値を確認しています。Least connection もクラスタワイドでサーバーへの接続振り分けを最適化しています。
server-agent	サーバーエージェント値のもっとも低いサーバーに対して高い確率で負荷分散されます。fastest response と同様にアクティブ接続数とレスポンス時間を確認しています。server agent はサーバーエージェント機能が有効になっている時のみ動作します（日本でのサポートは現状ございません）。
Custom	サーバーのレスポンス時間、サーバーのアクティブ接続数、サーバーエージェント値の3点をカスタマイズ設定することが可能です。

8.2 サーバールールの設定変更

左フレームからサーバールールを選択すると、右フレームに詳細設定画面が表示されます。ヘルスチェックについては [Health Check 設定](#) を参照。

8.2.1 “Configuration > LB Policy”タブ

サーバールールの負荷分散ポリシーやヘルスチェックプローブ設定を行います。

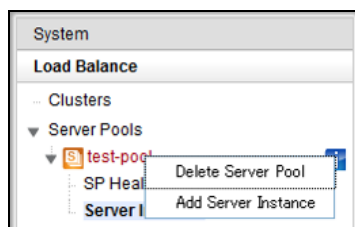
パラメータ	設定内容
Disable	設定しているサーバールールを無効にします。 (デフォルト無効)
Policy	サーバールール作成時に設定した負荷分散ポリシーを変更します。
Responsiveness	responsiveness の設定は FortiADC がサーバーの動的 weight 値をどのくらい頻繁に調整するかの設定になります。slowest、slow、medium、fast、fastest の 5 つから選択します。このレスポンス設定は adaptive、response、least-cxns を使用する際に影響を与えます。

8.3 サーバースタンスの追加

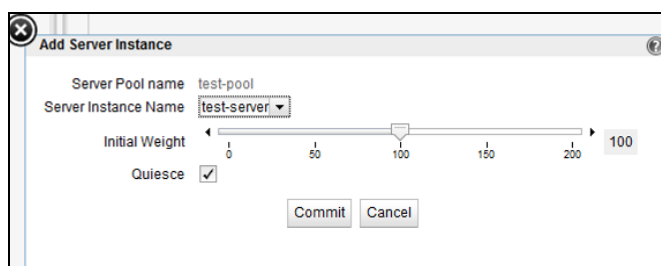
サーバーをサーバールールへ追加します。サーバールール内のサーバーに対して負荷分散通信が行われます。

8.3.1 サーバプールから追加する手順

図のように、サーバーを追加するサーバプールを左フレーム上で右クリックし、メニューを表示させます。



「Add Server Instance」をクリックすると以下サーバー追加画面が表示されます。必要な項目を設定し、Commit ボタンをクリックします。

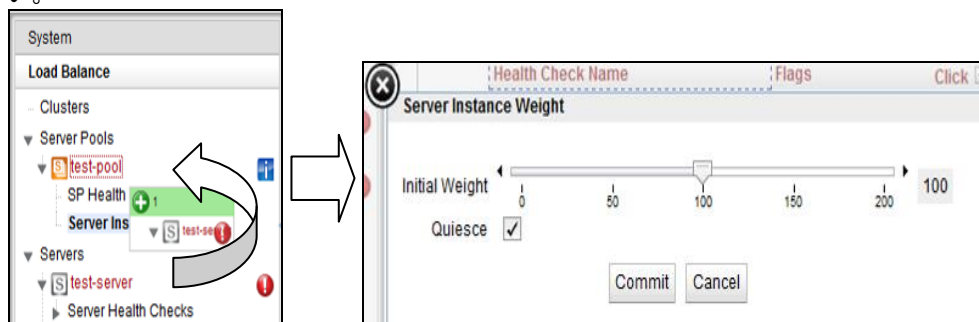


パラメータ	設定内容
Server Instance Name	設定されているサーバー一覧をボックスから選択します。
Initial Weight	サーバーの Initial Weight 値を設定します(デフォルト 100)。
Quiesce	チェックを有効にすることで、Quiesce 状態にすることができます。サーバーへ通常の負荷分散を行う場合は無効にします。詳細は 8.4.1 を参照 (デフォルト有効)

8.3.2 サーバプールから追加する手順

GUI の左フレームから、追加したいサーバーを選択し、サーバプール上にドラッグ&ドロップします。右図ではサーバー「test-server」を、サーバプール「test-pool」に追加しています。

正常に追加されると以下サーバー追加画面が表示されます。設定項目内容は 8.3.1 を照下さい。



8.4 サーバーインスタンス設定

サーバープールへ追加されたサーバーに対して個別設定を行うことが可能です。

8.4.1 “Configuration > Settings”タブ

The screenshot shows the 'Server Instance (test-server)' configuration page. It includes a 'Server Pool name' field set to 'test-pool' and a 'Current Weight' field set to '100'. Below these is a slider for 'Initial Weight' ranging from 0 to 200, with the current value set to 100. There are also input fields for 'Maximum Connections' (0), 'Hot Spare' (unchecked), 'Strict Max Cx' (checked), 'Override Persistence' (unchecked), and 'Quiesce' (checked). At the bottom, there are 'Commit' and 'Reset' buttons.

パラメータ	設定内容
Server Pool name	所属するサーバープールの名称が表示されます(変更不可)
Current Weight	現在の Weight 値が表示されます。
Initial Weight	サーバーの Initial Weight 値を設定します(デフォルト 100)。値を0にするとこのサーバーの Up/Down 関係なしに割り振りをしなくなります。
Maximum Connections	サーバーへ振り分けを行う最大同時コネクション数を設定します。デフォルトは 0 で制限を行いません。
Hot Spare	サーバーをバックアップとして動作させます。サーバープール内でアップ状態のサーバーが1台のみになった場合に、Hot Spareに指定したサーバーへ振り分けを行います。(デフォルト無効)
Override Persistence	Sticky や Cookie によるセッション維持を行わない場合は有効にします。(デフォルト無効)
Quiesce	メンテナンス時などサーバーを使用停止する際に、既存コネクションを維持しながら、緩やかに新規コネクションを減少させる際に使用します。quiesce に設定されたサーバーに対しては既存で確立しているセッションは振り分けられますが、新規リクエストは振り分けられません。コネクションが減少した後、サーバーメンテナンスを行なうことでサービスへの影響を最小限に抑えることが可能になります。 クラスタ内で quiesce 設定されたサーバーのみがアップ状態である状況では、FortiADC は 例外的 に新規リクエストを quiesce サーバーに振り分けます。 セッション維持された通信については quiesce サーバーに対して振り分けを行いません。(デフォルト有効)
Strict Max Cx	max connection 設定の動作を変更します(デフォルト有効)。有効の場合、max connection 値が常に使用され、設定値を越えた通信は振り分けられません。無効の場合は以下の状況で max connection 値に達した後も通信が振り分けられます。 <ul style="list-style-type: none"> Hotspare 設定がされたサーバーへの通信が行われた場合 クライアントが L7 クラスタへ通信し、Cookie によってセッション維持されている場合 クライアントが L4 クラスタへ通信し、Sticky Time によってセッション維持されている場合

9 クラスタ設定

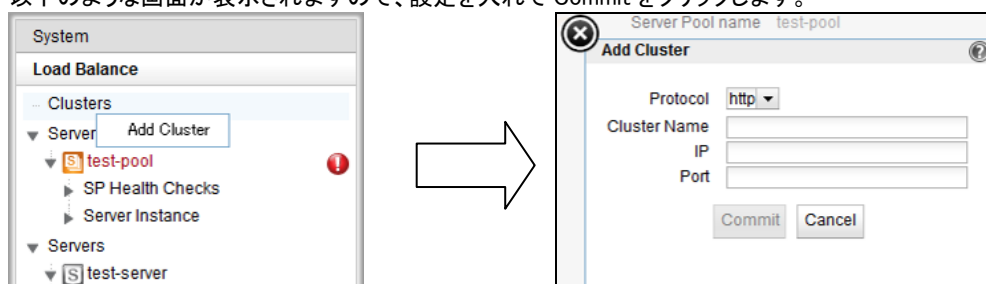
本章では FortiADC のクラスタ設定について説明します。

クラスタは仮想 IP を持ちクライアントからの通信を受け付ける動作をします。サーバープールと紐づけ通信をサーバーへ振り分けます。また接続の管理やセッション維持設定、Match Rule や Responder の紐づけもクラスタから行います。

9.1 クラスタの新規追加

GUI からクラスタの追加を行うには、左フレームの「Clusters」を右クリックし、表示される「Add Cluster」を選択します。

以下のような画面が表示されますので、設定を入れて Commit をクリックします。



パラメータ	設定内容
Protocol	クラスタのプロトコルを選択します、以下から選択します。 <ul style="list-style-type: none"> •http : HTTP 通信を L7 レベルで処理する際に選択します (IPv4/IPv6) •https : HTTPS 通信を SSL オフロードし、L7 レベルで処理する際に選択します (IPv4/IPv6) •tcp : TCP 通信を L4 レベルで処理する際に選択します (IPv4) •udp : UDP 通信を L4 レベルで処理する際に選択します (IPv4) •l7tcp : IPv6 を使用し TCP を L4 レベルで処理する際に選択します (IPv4/IPv6)
Cluster Name	クラスタの名称を任意で指定します。
IP	クラスタの IP アドレスを指定します。
Port	クラスタのポート番号を指定します。

9.2 クラスタの設定変更

左フレームからクラスタを選択すると、右フレームに詳細設定画面が表示されます。

9.2.1 “Configuration > Summary”タブ

クラスタ設定の概要が表示されます。

項目	内容
Active Connections	クラスタにアクセスしているアクティブな接続数が表示されます。
Connections/second(GPS)	秒間の接続数が表示されます。
Transactions/second(TPS)	秒間のトランザクション数が表示されます(L7 クラスタのみ)
Protocol	クラスタ作成時に指定したプロトコルが表示されます。
VID	クラスタが所属している VID(VLAN ID)が表示されます。
IP	クラスタの IP アドレスが表示されます。

Port	クラスタのポート番号が表示されます。
Server Pool	設定されている Server Pool が表示されます。
Disable	クラスタを無効にします。 IP アドレスはリリースされ、クライアントからの接続はできなくなります。 チェックを入れ commit ボタンをクリックし設定します。
Performance History: Last 30 Minutes	直近 30 分間の接続情報を表示します。

9.2.2 “Configuration > settings”タブ

クラスタの設定変更を行います。

パラメータ	設定内容
各クラスタ共通	
Protocol	クラスタ作成時に指定したプロトコルが表示されます(変更不可)。
VID	クラスタが所属している VID(VLAN ID)が表示されます(変更不可)。
IP	クラスタの IP アドレスを設定します。
Port	クラスタのポート番号を設定します。
Preferred Peer	クラスタが所属する Peer を設定します。
Server Pool	負荷分散対象のサーバープールを選択します。
Spoof	無効の状態では SNAT が有効になり、サーバーへ行われる通信の送信元 IP アドレスは FortiADC の subnet IP アドレスになります(デフォルト無効)。
tcp/udp クラスタ共通	
Range	受付ポート番号の範囲指定を行なう場合は終点ポートの設定をします。 Port で設定されているポート番号が始点ポートになります。
Direct Server Return	DSR 構成を行なう際、有効にします。
l7tcp クラスタ共通	
Delayed Binding	設定を有効にすることで、新規の接続に対してサーバーが最初のバイト情報を送るように要求します。
http/https クラスタ共通	
Responder	クラスタに紐づける Responder を指定します。
Custom Header	FortiADC で受け付けるリクエストに対して、サーバーへの負荷分散時にカスタムの HTTP ヘッダを挿入します。
Abort Server (l7tcp にも同設定あり)	デフォルト(無効)の状態では、クライアントが TCP 接続を切断した場合に FortiADC はサーバーとの接続を切断せず応答を待ちます。 有効に設定すると、FortiADC はサーバーからの応答を待たずに TCP RST を送信し接続を切断します(デフォルト無効)。
Allow Multibyte Characters	URI やヘッダ内の ASCII や UTF-8 の透過設定です(デフォルト有効)。
Ignore Case	チェックを入れ有効にすると、Match Rules での大文字・小文字の区別をしません(デフォルト無効)。
Insert Client IP	有効にした場合、クライアントリクエストをサーバーへ送付する際に、HTTP ヘッダ “X-Forwarded-For” を FortiADC が付与します。 このヘッダにはクライアント IP アドレスが記載されています(デフォルト[http 無効][https 有効])。
Once Only	1つの TCP セッションに対して複数のリクエスト投げるようなクライアント通信で最初のリクエストのみ FortiADC cookie を確認してセッション維持を行います。 また、HTTP/1.1 でのプロ

	キシサーバー経由通信がmultiplexingで動作する場合には無効にする必要がある場合があります(デフォルト無効)。
TCP Multiplexing	有効にすると TCP Multiplexing がクラスタで有効になります(デフォルト無効)。
https クラスタのみ	
Ignore Critical Extensions	クライアント証明書の CRL 配布点(CRL Distribution Point)を処理するかどうか設定します。
Rewrite Redirects	L7 HTTPS クラスタの設定を行うと、その所属サーバーの待ち受けポートは HTTP で処理されます。サーバーが Location: header を使用し HTTP リダイレクトを送信すると、この URL は http: として行われますが、FortiADC が https: に自動で書き換えます(デフォルトの場合)書き換えない場合は無効にします(デフォルト有効)。

9.2.3 “Configuration > Persistence”タブ

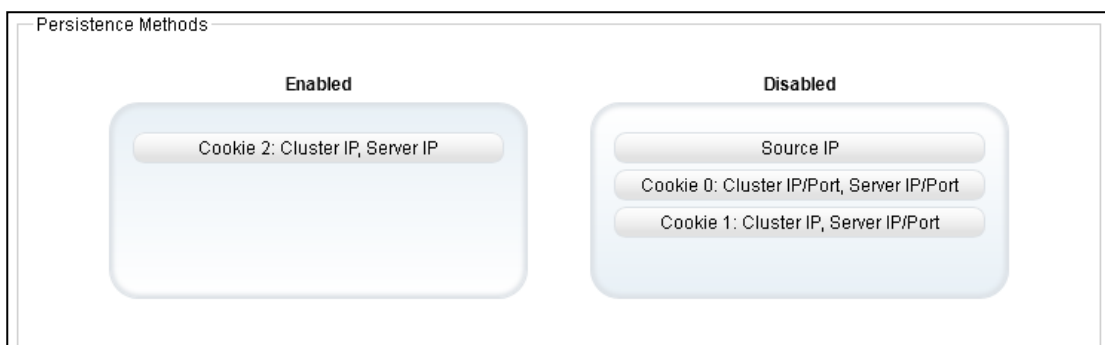
サーバーセッション維持に関する設定を行います。

9.2.3.1 tcp/udp/l7tcp クラスタの場合

パラメータ	設定内容
Sticky Netmask	Sticky Timeout が 0 秒以外の場合に送信元 IP アドレスに対するネットマスクの設定になります。デフォルトは off です。クラスフルな設定になります。
Sticky Timeout (seconds)	クライアントの送信元 IP アドレスを利用してセッションを維持させる為の時間設定(秒)です。アクセスがあった送信元 IP は Sticky レコードに記録され、時間設定以内に再度通信が行なわれた場合は同じサーバーに対して振り分けが行なわれます。セッション維持が必要ではない場合 0 秒を設定して下さい。 設定可能値: 0-1073741823 (デフォルト 0 秒)。
Inter Cluster Sticky	L4 クラスタを使用し、同じ IP を持つ複数のクラスタが同一のサーバー構成で設定されている状況で、そのクラスタをまたがった通信でセッション維持を行ないたい場合にはチェックを入れます。(デフォルト無効)

9.2.3.2 http/https クラスタの場合

「Persistence Methods」で Enabled 枠に入っている設定が有効になっているセッション維持方法です、以下のようにデフォルトでは「Cookie 2: Cluster IP, Server IP」が有効になっています。その他のセッション維持方法を有効にするには Disabled 枠にある項目をドラッグ & ドロップで Enabled 枠に移動させます。



パラメータ	設定内容
Cookie 2: Cluster IP, Server IP (クッキー2: クラスタ IP, サーバー IP)	FortiADC が付与する Cookie によってセッション維持を行います。クライアントがアクセスするクラスタ IP と振り分けられたサーバーIP を判別して動作します。クラスタとサーバーのポート番号については無視されます。
Cookie 1: Cluster IP, Server IP/Port (クッキー1: クラスタ IP, サーバー IP/ポート)	FortiADC が付与する Cookie によってセッション維持を行います。クライアントがアクセスするクラスタ IP と振り分けられたサーバーIP/ポート番号を判別して動作します。クラスタのポート番号については無視されます。
Cookie 0: Cluster IP/Port, Server IP/Port (クッキー0: クラスタ IP/ポート, サーバー IP/ポート)	FortiADC が付与する Cookie によってセッション維持を行います。クライアントがアクセスするクラスタ IP/ポート番号と振り分けられたサーバーIP/ポート番号を判別して動作します。
Source IP (ソース IP)	クライアントの送信元 IP アドレスを利用してセッションを維持させます。アクセスがあった送信元 IP は Sticky レコードに記録され、時間設定以内に再度通信が行なわれた場合は同じサーバーに対して振り分けが行なわれます。

Cookie の詳細パラメータは以下の通りです。

パラメータ	設定内容
Cookie Path (クッキーパス)	リクエスト URI 内に設定されたパスが存在する場合に cookie をブラウザに付与します。 (例えば、/store/ と設定し、 http://www.hogehoge.com/store/mypage.html にアクセスした場合には cookie がブラウザに保存されます。 http://www.hogehoge.com/goods/information.html では cookie はブラウザに保存されません)
Cookie Domain (クッキードメイン)	設定されたドメイン名でアクセスするクライアントのブラウザにのみ cookie の付与を行ないます。 (例えば www.coyotepoint.com や my.coyotepoint.com)。
Cookie Age (クッキーエイジ)	Cookie の有効期限を秒で指定します。有効時間を過ぎた Cookie を持って通信が行なわれた場合は、FortiADC はセッション維持動作を行ないません。 設定する場合は、クライアント・FortiADC・サーバーが同じ時刻に設定されていることを確認して下さい。時刻設定に差異がある場合、正常に動作しないことがあります。
Cookie Generation (クッキー生成)	cookie scheme が 2 もしくはそれ以上の場合に追加します。適切な cookie として認識させる為に cookie generation 値はブラウザに保存されるその数値と一致しなければなりません。逆に古い cookie を適用させたくない場合にはこの数値

	を加算します。
Always (常にセッション維持)	無効時:クライアントが新規接続である場合や、クライアントの Cookie を認識できない場合に Cookie を付与します。 有効時:サーバーの応答に必ず Cookie を付与します。 (デフォルト無効)

9.2.4 “Configuration > Timeouts”タブ

クラスタのタイムアウト設定を行います。

パラメータ	設定内容
tcp/udp クラスタ共通	
Idle Timeout (seconds)	L4 クラスタへの設定値で、アイドル状態にある TCP コネクションを FotiADC が切断するまでのタイムアウト時間を設定します。 設定可能値: 1-65535 (デフォルト 60 秒)(0 秒は非推奨)
Stale Timeout (seconds)	L4 クラスタへの設定値で、ハーフオープン接続として存在している L4 接続をタイムアウトさせる設定時間(秒)になります。 設定可能値: 1-120(デフォルト 30 秒)
http/https/l7top クラスタ共通	
Client Timeout	FotiADC がクライアントリクエストの終了を待つまでのタイムアウト設定値になります。 設定可能値: 1-65535(デフォルト 10 秒)。
Server Timeout	FotiADC がサーバーヘリクエストを投げてから次のリクエストを受け取るまでの接続をタイムアウトとして判定するまでの設定値になります。 設定可能値: 1-65535 (デフォルト 60 秒)。
Connect Timeout	接続要求に対してサーバーがレスポンスを返すまでの FotiADC のタイムアウト値になります(デフォルト 10 秒)。

9.2.5 “Security > Certificate”タブ (https クラスタのみ)

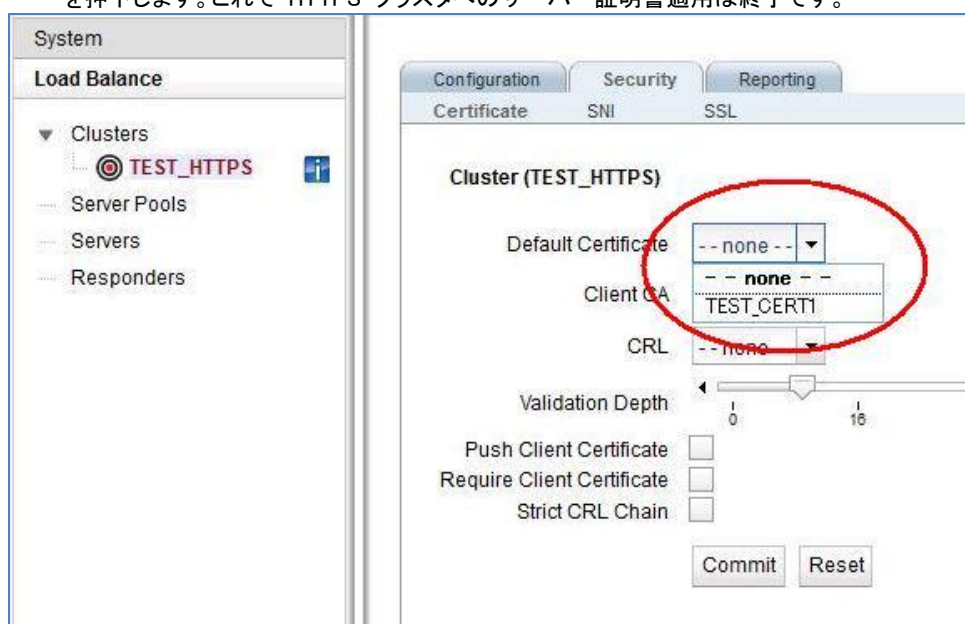
Certificate で登録した Certificate 情報を HTTPS クラスタに適用します。

パラメータ	設定内容
Default Certificate	https クラスタで標準使用するサーバー証明書を選択します。証明書のアップロード手順は 5.1.3 Certificates を参照して下さい。
Client CA	https クラスタで使用するクライアント証明書を選択します。
CRL	https クラスタで使用する CRL を選択します。
Validation Depth	クライアント証明書に対して行うチェックの階層を指定します。デフォルトの 9 ではクライアント証明 (Level 0) と 9 階層上を確認し、それより上位の階層は無視されます。
Push Client Certificate	有効にするとクライアント証明書をバックエンドサーバーへ送信します。サーバーが SSL リネゴシエーション無しでクライアントの接続を認証することができます。
Require Client Certificate	有効にすると接続するクライアントに対してクライアント証明書の提示を要求します。
Strict CRL Chain	有効にすると証明書チェーンの証明書をクラスタに設定された CRL と確認し、有効性を確認します。チェーン内の証明書どれかの有効性が確認できない場合はエラーが表示されます。無効(デフォルト)の場合、最後の証明書のみ有効性が確認されます。

1. 左フレームの Load Balance を選択し、Cluster の△をクリックして展開します。



2. サーバー証明書を適用する HTTPS クラスタをクリックします。(上記の図では「test-cluster-https」となっています。)
3. 中央の HTTPS クラスタの画面の Security タブから Certificate を選択します。Default Certificate のプルダウンボックスから登録した証明書オブジェクト名を選択し、Commit を押下します。これで HTTPS クラスタへのサーバー証明書適用は終了です。



9.2.6 “Security > SNI”タブ (https クラスタのみ)

1 つの HTTPS クラスタで複数ドメイン名を扱う際には、この設定を追加します。適切な証明書情報を合わせて紐付けます。

1. (Temporary underconstruction)

https クラスタで SNI 機能を使用する場合は、この画面から SNI Certificate を追加します。画面右上のアイコン  をクリックすることで SNI Certificate 追加画面が表示されます。

パラメータ	設定内容
SNI Certificate Name	SNI Certificate の名前を指定します。47 文字以下で ASCII 文字とピリオド(.)、ダッシュ(-)、アンダースコア(_)を使用できます。
Server Name	SNI Certificate を使用するウェブサイト名を指定します。
Certificate	使用するサーバー証明書を選択します。

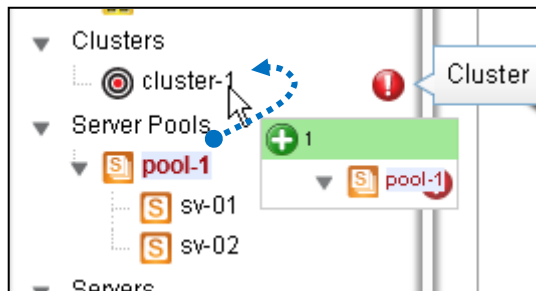
9.2.7 “Security > SSL”タブ (https クラスタのみ)

Cipher Suite 設定などに関する設定を行います。
Cipher Suites については Handbook や FAQ を参照ください。

パラメータ	設定内容
Cipher Suites	クラスタへの HTTPS リクエストに対して使用する Cipher Suite を設定します。
Allow SSLv2	SSLv2 による接続を有効にします。 (無効推奨)
Allow SSLv3	SSLv3 による接続を有効にします。 (無効推奨)
Allow TLSv1.0	TLSv1.0 による接続を有効にします。
Allow TLSv1.1	TLSv1.1 による接続を有効にします。
Allow TLSv1.2	TLSv1.2 による接続を有効にします。
Software SSL Only	SSL ハードウェアアクセラレーションを使用せず、ソフトウェア処理で暗号化・復合を行います。

9.3 クラスタへのサーバープール追加

クラスタへサーバープールを追加する場合、サーバープールをドラッグ&ドロップすることでも操作が可能です。以下の図ではサーバープール「」をクラスタ「」へ追加しています。



9.4 クラスタのステータス確認 (Cluster Summary)

GUI 左メニューから「Clusters」をクリックすると、クラスタのサマリー情報が表示されます。各サーバーへの通信状態などを確認することが出来ます。

10 Health Check 設定

本章では FortiADC の Health Check 設定について説明します。

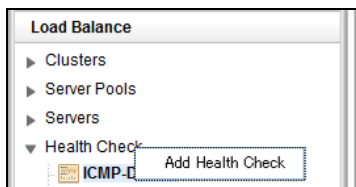
4.2 系より Health Check の設定項目が Pool ごとに個別設定から、Global 項目として設定を行うようになりました。HealthCheck の種類は大きく6種類ございます。本手順書では主に使用する3種類を記載させていただきます。その他の項目については Handbook を参照ください。

10.1 ICMP Health Check

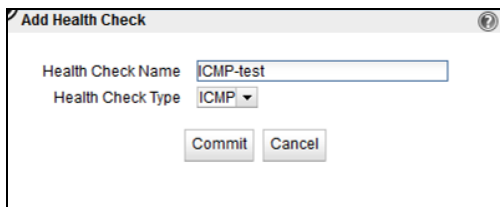
ICMP の Health check について記載します。

10.1.1 ICMP Health Check 追加

ICMP の Health Check を追加する場合は、左フレームの「Health Check」を右クリックし、[Add Health Check]を選択



[Health Check Type]を[ICMP]に変更し、[Health Check Name]を定義し、[commit]で作成します



10.1.2 ICMP Health Check 設定

参考として、デフォルトで登録されている[ICMP-Default]をもとに記載します。

The screenshot shows the configuration page for 'ICMP Health Check (ICMP-Default)'. It includes the following settings:

- Disable:**
- Target Object Parameters:**
 - Use Parent Parameters:
 - Target Object IP: [Redacted]
- ICMP Parameters:**
 - Relaxed:
- Health Check Timers:**
 - Probe Interval (seconds): 15
 - Max Tries Per Interval: 3

Buttons for 'Commit' and 'Reset' are visible at the bottom.

ICMP Health Checks

パラメータ	設定内容
Disable	表示している HealthCheck を無効にします(デフォルト:無効)
Max Tries Per Interval	「ICMP Probe Interval」で設定され時間内に送信するICMPの回数を指定します。(デフォルト:3回)
Probe Interval	ここで設定された時間内に最低 1 回は ICMP に成功する必要がある、成功しない場合はサーバーがダウン判定されます。(デフォルト:15秒)

基本的には上記の設定のみの変更となります。

ヘルスチェックの間隔についてですが、デフォルトでは 15 秒の間に 3 回 ICMP によるチェックを行います。

計算式としては $\text{Probe Interval} / \text{Max Tries Per Interval}$ という計算式になります。

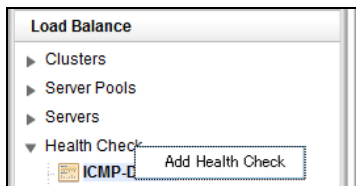
そのため、デフォルトでは $15 \text{ 秒} \div 3 \text{ 回} = 5 \text{ 秒毎}$ という計算となります。

10.1.3 TCP Health Check

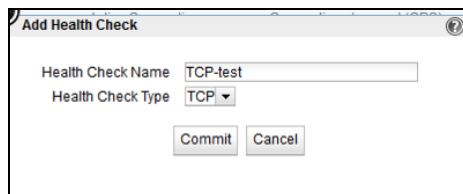
TCP Health Check について記載します。

10.1.3.1 TCP Health Check 追加

TCP の Health Check を追加する場合は、左フレームの「Health Check」を右クリックし、[Add Health Check]を選択

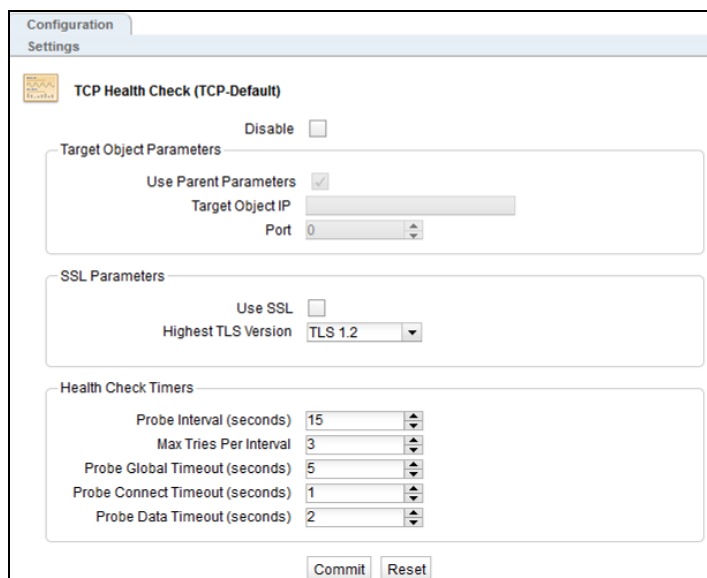


[Health Check Type]を[TCP]に変更し、[Health Check Name]を定義し、[commit]で作成します



10.1.3.2 TCP Health Check 設定

参考として、デフォルトで登録されている[ICMP-Default]をもとに記載します。



TCP Handshake Probes	
Disable	表示している HealthCheck を無効にします(デフォルト:無効)
Probe Interval (seconds)	この時間内に TCP/UDP の Health Check が成功しなくては いけません(デフォルト 15 秒)。 1 回またはそれ以上のプローブが成功するとサーバーはア ップと判定され、タイマーはリセットされます。 プローブが成功 しなかった場合サーバーはダウンと判定され、タイマーはリセ ットされます。
Max Tries Per Interval	Probe Interval の時間内でサーバーに対して行う TCP/UDP のプローブ最大回数を指定します。(デフォルト 3 回)。
Probe Global Timeout (seconds)	サーバーに対する TCP/UDP のプローブが行われ、コネクショ ンが確立されるか応答があるまでの最大時間を指定します。 Probe Interval よりも長い時間を設定した場合、Probe Interval が Probe Global Timeout として動作します(デフォルト 5 秒)。
Probe Connect Timeout (seconds)	サーバーに対する TCP プローブのコネクションが確立するま での最大時間を指定します(デフォルト 1 秒)。 ACV のヘルスチェックやTCPの3ハンドシェイクに時間がか かるサーバーの場合は 2 または 3 に変更を推奨します。
Probe Data Timeout (seconds)	サーバーに対する TCP プローブに対して、最初のデータが返 ってくるまでの最大時間を指定します(デフォルト 2 秒)。
Use SSL	有効にすると L4 プローブは SSL で暗号化された状態で実行 されます。

10.1.3.3 TCP Health Check 計算式について

ヘルスチェックの間隔についてですが、デフォルトでは 15 秒の間に 3 回 TCP によるチェックを行います。計算式としては $\text{Probe Interval} / \text{Probe Maximum Tries}$ という計算式になります。そのため、デフォルトでは $15 \text{ 秒} \div 3 \text{ 回} = 5 \text{ 秒毎}$ という計算となります。

また、3種類のTimeoutの設定については以下の制限がございます。
設定の際には確認して設定ください。

$(\text{Probe Interval} / \text{Probe Maximum Tries}) \geq \text{Probe Global Timeout}$

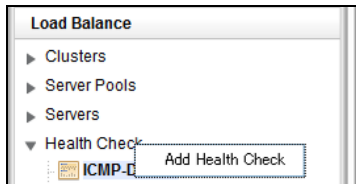
$\text{Probe Global Timeout} \geq (\text{Probe Connect Timeout} + \text{Probe Data Timeout})$

10.1.4 ACV Health Check

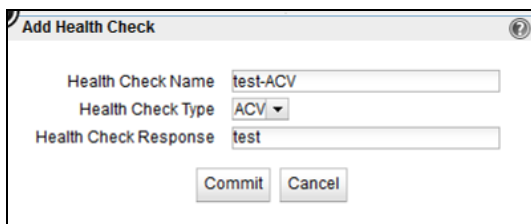
ACV Health Check について記載します。

10.1.4.1 ACV Health Check 追加

TCP の Health Check を追加する場合は、
左フレームの「Health Check」を右クリックし、[Add Health Check]を選択

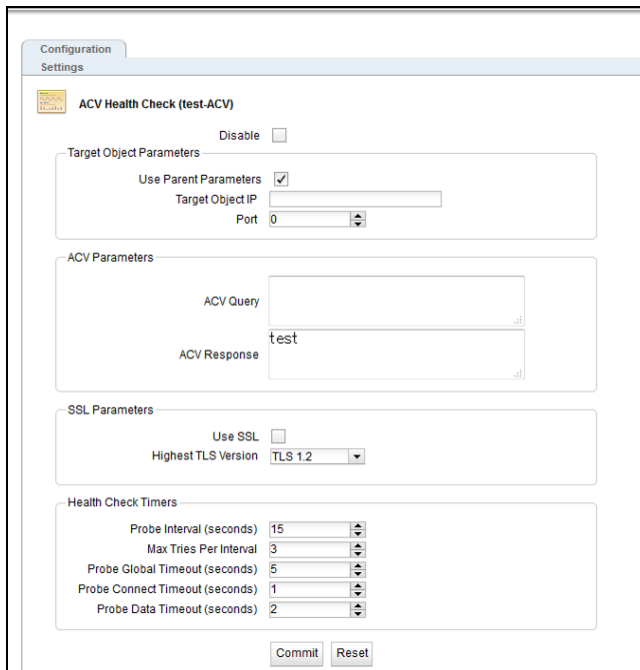


[Health Check Type]を[ACV]に変更し、[Health Check Name]を定義し、
[Health Check Response]は仮でなにかしら文字列を入力し、[commit]で作成します



10.1.4.2 ACV Health Check 設定

画像は 10.1.4.1 で設定したばかりの内容の画像です。



TCP Handshake Probes	
Disable	表示している HealthCheck を無効にします(デフォルト:無効)
ACV Query	TCP プローブ時のオプションとしてサーバーへ文字列を送付します。 設定例: GET /index.html HTTP/1.1¥r¥nHost: FotiADC ¥r¥n¥r¥n
ACV Response	ACV Query によってサーバーから送付される文字列を指定します。この値と同じである場合にサーバーはアップと判定されます。Query のコンテンツにアクセスした際に含まれる文字列がない場合は、ダウン判定となります。 設定例: 200
Use SSL	有効にすると L4 プローブは SSL で暗号化された状態で実行されます。
Probe Interval (seconds)	この時間内に TCP/UDP の Health Check が成功しなくてはなりません(デフォルト 15 秒)。 1 回またはそれ以上のプローブが成功するとサーバーはアップと判定され、タイマーはリセットされます。プローブが成功しなかった場合サーバーはダウンと判定され、タイマーはリセットされません。
Max Tries Per Interval	Probe Interval の時間内でサーバーに対して行う TCP/UDP のプローブ最大回数を指定します。(デフォルト 3 回)。
Probe Global Timeout (seconds)	サーバーに対する TCP/UDP のプローブが行われ、コネクションが確立されるか応答があるまでの最大時間を指定します。Probe Interval よりも長い時間を設定した場合、Probe Interval が Probe Global Timeout として動作します(デフォルト 5 秒)。
Probe Connect Timeout (seconds)	サーバーに対する TCP プローブのコネクションが確立するまでの最大時間を指定します(デフォルト 1 秒)。 ACV のヘルスチェックやTCPのハンドシェイクに時間がかかるサーバーの場合は 2 または 3 に変更を推奨します。
Probe Data Timeout (seconds)	サーバーに対する TCP プローブに対して、最初のデータが返ってくるまでの最大時間を指定します(デフォルト 2 秒)。

※ACVの Health Check については、テストを行うためには、該当項目に一度紐づける必要があります。
そのため、紐づけの前には[Disable]にした状態でまずは紐づけていただくことを推奨します。

10.1.4.3 TCP Health Check 計算式について

TCP Health Check と内容は同じとなります。
前項の [TCP Health Check 計算式について](#) を参照。

10.1.4.4 ACV のテストについて

ACV の Health Check については、テストすることが可能です。
 次項目の「Health Check の登録」を参照していただき、ACV を動作させたい Server Pool または Server Pool 内の Server へ紐づけを行ってください。
 紐づけた Health Check が以下ようになります。

まず、こちらの画面で、[Disable] を有効にしてください。
 その後、元の Health Check を [Disable] にしていた場合は、そちらの [Disable] を無効にしてください。

次に、Pool 内のサーバーへのテストですが、画面上の [ACV Test] の項目の [Test This Server] 横にあります、[Choose a server] を選択すると、設定している Server Pool に設定してある Server を選ぶことができます。テストしたいサーバーを選択し、その左にある [Test] を選択すると該当サーバーへの ACV を実施します。正常にいかない場合は、サーバー側の設定または Health Check の値の調整を行ってください。設定に問題がなくなりましたら、任意のタイミングで、[Disable] を解除してください。

10.1.5 Health Check の登録

設定した Health Check の紐づけを案内します。

10.1.5.1 Default 登録

- ・ ICMP-Default は Servers の項目にサーバーを登録した段階でデフォルトで紐づけされます
- ・ TCP-Default は Server Pool に一つでもサーバーを紐づけた段階でデフォルトで紐づけされます。

10.1.5.2 手動での登録対象

Default 以外に、ACV の Health Check などの個別の Health Check については手動での紐づけが必要です。

紐づけできるのは以下の3か所になります。
 なお、どこかのヘルスチェックでダウンした段階で、ダウン判定となりますので、紐づける場所については確認して設定を行ってください。

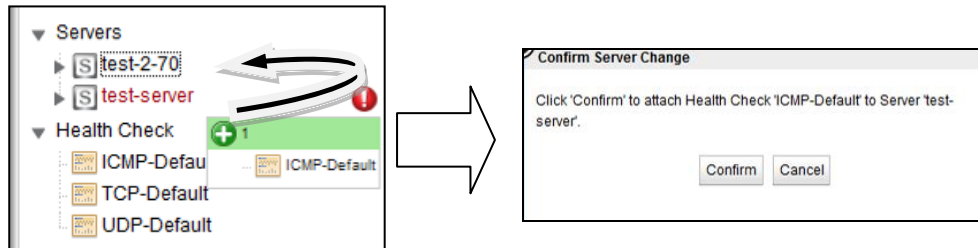
- ・ Servers 内の Server 毎
- ・ Server Pools の Server Pool 毎
- ・ Server Pool 内の Server 毎

Health Check については、紐づけた段階で動作しますので、紐づけだけ行いたい場合は、対象設定を [Disable] にしてから紐づけてください。紐づけた段階で、NG の場合は Down 判定となります。

10.1.5.3 手動での登録方法

ACVのHealth Check やデフォルト以外を定義したものについては、手動での登録が必要です。登録方法は Sever Pool に Server を紐づけるのと同じで、GUI上で作業可能です。

下の図は[ICMP Default] を [test-server]に紐づけています。その後、紐づけの確認が表示されるので[Confirm]で登録となります。



※紐づける Health Check をDisable にしないまま、紐づけた場合、紐づけた段階で、Health Check が動作します。Health Check が正常に回答しない場合 Down 判定となります。必要に応じて登録する Health Check は事前に[Disable]にして対応してください。設定完了後に Disable を解除してください。

11 Failover 設定

本章では 2 台の FortiADC を冗長化する設定について説明します。

11.1 Failover 動作の基本概念について

Failover 動作の概要は以下の通りです。

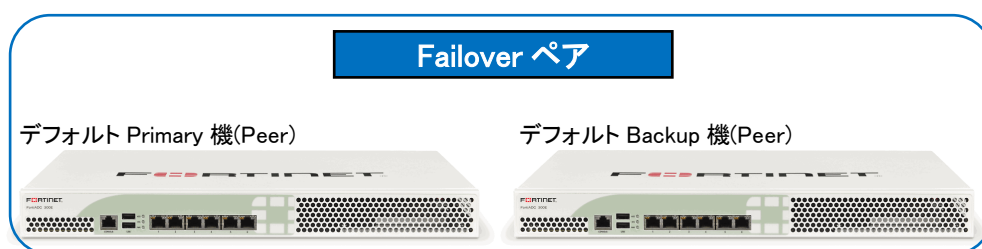
11.1.1 Primary 役、Backup 役について

Failover 設定が行われた 2 台の FortiADC はそれぞれ Primary 役 (Primary role)、Backup 役 (Backup role) として動作を行います。Primary 役の機器がクラスター IP や Failover IP アドレスを保持し通信を行います。Primary 役の機器に障害が発生した場合、Backup 役の機器が Primary に切り替わり、通信を継続します。

Failover 設定された 2 台の FortiADC は「Failover ペア」と呼ばれ、それぞれの機器は Peer (ピア) と呼ばれます。

11.1.2 デフォルト Primary、デフォルト Backup について

Failover 設定を行う際は、片方の機器を「デフォルト Primary」として設定します。デフォルト Primary として設定された機器は、両機器が同時に起動した場合などに優先して Primary として動作します。



11.1.3 冗長化の通信 (heartbeat) について

冗長化された FortiADC はネットワーク経由で互いに死活監視を行います、この通信を heartbeat と呼びます。heartbeat 通信に問題が発生した場合、Failover が行われます。この通信は TCP で行われます。

11.1.4 Failover ペア同士のコンフィグ同期について

Failover ペアを組む FortiADC 間ではコンフィグ同期を行なうことが可能です。

機器設定の追加/変更/削除を実施すると、機器の sequence 値が増加します。Failover ペアを組んでいる機器間で sequence 値を比較し、値が大きい機器のコンフィグを最新と判断し、もう一方の機器に同期させます。従って、デフォルト Primary 機・Backup 機のどちらかで設定を更新してもコンフィグ同期が実施されます。

コンフィグの同期は Command Transfer フラグが有効になっている VLAN/Subnet を経由して行われます。どの VLAN/Subnet でも有効になっていない場合は、最初の VLAN が使用されます。

コンフィグ同期の対象になる設定、対象ではない設定の一覧は以下の通りになります。

コンフィグ同期に含まれる設定	コンフィグ同期に含まれない設定
Alerts	Interfaces (Switch Port Configuration)
Clusters	Peers
Server Pools	VLANs
SSL Certificates	Subnets
CRLs	Tunnels
Servers	
Responders	
GeoClusters	
GeoSite	
GeoSite Instances	
Global Parameters: Syslog server NTP server Name servers	
Health Checks	
Health Check Instances	
SMTP Relays	
VLB Managers	
Users	

11.1.5 Primary への切り替え動作について

Heartbeat 設定を有効にしている subnet からは、Heartbeat Interval で設定された時間ごとに heartbeat が行われます。heartbeat を受け取らない場合は失敗として Failed Probe Count が増加します。Failed Probe Count の上限に達すると、Backup 役の機器が Primary へ移行します。

Primary 移行の際は以下の動作をします。

1. 設定されているクラスタ IP や Failover IP Address がネットワークに存在するかを ICMP で確認します。
2. 自機のネットワーク接続状況と、heartbeat から得られた対向機器のネットワーク接続状況を比較します。
3. 他の機器がクラスタ IP や Failover IP Address を持たず、また、自機が対向機器よりも良いネットワーク接続状況であった場合、Primary 役に移行します。それ以外の場合は Backup 役として動作をします。

11.2 Failover 設定の事前準備について

Failover 設定を行う前に以下の点を確認して下さい。

1. VLAN 設定は両機器の間で完全に同じである必要があります。
これはすべての VLAN と Subnet 設定を含みますが、以下は異なっていても問題ありません。
•Subnet の IP アドレス(機器IP)
2. FotiADC が接続されるスイッチ上で STP が有効になっている場合、両方の FotiADC が Primary になってしまう状況が発生します。この状況を防ぐためにはスイッチの STP は無効にする、あるいは FotiADC 接続ポートの Portfast 設定を有効にします。
3. VLAN Subnet は以下の通りに設定されている必要があります。
a) Heartbeat 設定がどこか 1 つの VLAN で有効になっている必要があります

- b) Command Transfer 設定が 1 つの VLAN で有効になっている必要があります。
 ※有効になっていない場合、最初の VLAN が使用されます。
- c) heartbeat 設定 または Command Transfer 設定が有効になっている
4. VLAN subnet では Failover IP Address が設定されている必要があります。
 FortiADC は Failover 時にネットワークの疎通確認を行います。
 疎通が取れない場合、正常に Failover は動作しないため、以下どちらかへ FortiADC から Ping が成功することを確認して下さい。
- ・FortiADC のデフォルトゲートウェイ
 - ・負荷分散対象サーバー

11.3 Failover 設定

Failover の設定を実施します、必ず 11.2 の条件を満たしていることを事前に確認して下さい。
 本例で使用する機器の設定は以下の通りです。

設定/Peer 名	ADC300E-181	ADC300E-182
VLAN/Subnet IP address	10.15.100.181	10.15.100.182
Failover IP address	10.15.100.180	
Default Gateway Address	10.15.100.254	
Preferred Primary	有効 (デフォルト Primary)	無効 (デフォルト Backup)

11.3.1 VLAN/Subnet 設定

両機器の Subnet に Failover 設定を行います。

左フレームから System > Network > VLANs > 対象 VLAN > 対象 Subnet

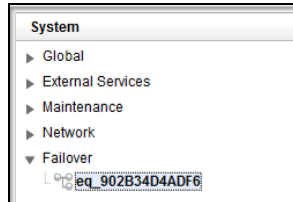
>右フレーム > Failover を選択すると以下の画面が表示されます。両機器で**同じ設定**を行います。

※Subnet が複数ある場合は**すべてで実施**します。

パラメータ	設定内容
Failover IP Address	Primary 役の機器が保持する仮想 IP アドレスです。クラスタ IP アドレスとは異なる IP アドレスを設定する必要があります。サーバーのゲートウェイなどとして使用されます。
Command Failover	Subnet 上でコンフィグ同期を行います。
Heartbeat	Subnet 上で heartbeat 通信を行います。
System Services on Failover IP Address	Failover IP Address で設定した IP アドレスへ通信が行われた際のプロトコル許可設定を行います。許可したいプロトコルにチェックを入れます。
Heartbeat Interval (seconds)	Peer 間で行われる heartbeat 通信の間隔を設定します。(デフォルト:2 秒)
Failed Probe Count	Peer がダウン判定される heartbeat 通信の失敗回数を設定します。

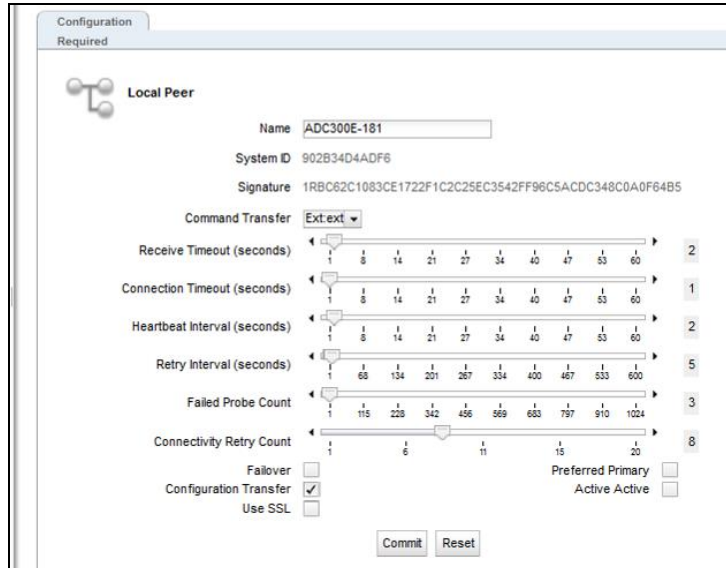
11.3.2 Peer 名設定

両機器の Peer 名を変更します。左フレームの System > Failover にある、Peer アイコンをクリックします。デフォルトの名前は「eq_<systemID>」になっています。



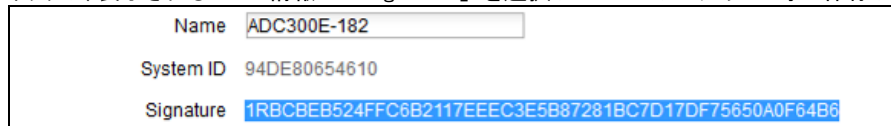
Peer 情報が表示されますので「Change Peer Name」に設定する Peer 名を入れ、Commit ボタンをクリックします。その他の設定は次の項目で実施するため、まずは名前のみ変更します。左フレームが更新され、Peer 名が変更されたことを確認します。

両機器で変更を行います。更新されない場合は、画面リロードまたはログアウトをして下さい。その後、**念のため更新された左フレームの Peer 名を選択しておいてください。**



11.3.3 Signature 情報の取得(デフォルト Backup)

デフォルト Backup 機にログインし、Signature 情報を取得します。左フレームの Peer アイコンをクリックし、表示される Peer 情報の「Signature」を選択してコピーしてテキスト等に保存します。



11.3.4 デフォルト Primary 機の Flag 設定

デフォルト Primary 機にログインし、左フレームから Peer アイコンをクリックします。表示される Peer 情報から、Failover と Preferred Primary にチェックを入れて Commit ボタンをクリックします。

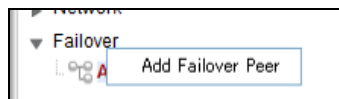
Failover	<input checked="" type="checkbox"/>	Preferred Primary	<input checked="" type="checkbox"/>
Configuration Transfer	<input checked="" type="checkbox"/>	Active Active	<input type="checkbox"/>
Use SSL	<input type="checkbox"/>		
<input type="button" value="Commit"/> <input type="button" value="Reset"/>			

続いてデフォルト Primary 機からも Signature 情報をコピーし、テキスト等に保存します。

Name	ADC300E-181
System ID	902B34D4ADF6
Signature	1RBC62C1083CE1722F1C2C25EC3542FF96C5ACDC348C0A0F64B5

11.3.5 Peer の登録(デフォルト Primary)

デフォルト Primary 機で Peer の登録を行います。登録する Peer はデフォルト Backup 機です。左フレームの Failover を右クリックすると「Add Failover Peer」と表示されるので、クリックします。



Peer 登録画面が表示されるので、デフォルト Backup 機の Peer 名と Signature を入力して Commit ボタンをクリックします。Signature は 11.3.3 でコピーしたものです。

Add Failover Peer	
Peer Name	ADC300E-182
Signature	1RBCBEB524FFC6B2117EEEC3E5B87281BC7D17DF75650A0F64B6
<input type="button" value="Commit"/> <input type="button" value="Cancel"/>	

左フレームの Peers に、Peer アイコンが 2 つ表示されることを確認します。

11.3.6 デフォルト Backup 機の Flag 設定

デフォルト Backup 機にログインし、左フレームから Peer アイコンをクリックします。表示される Peer 情報から、Failover にチェックを入れて Commit ボタンをクリックします。

※Preferred Primary にはチェックを入れないこと

Failover	<input checked="" type="checkbox"/>	Preferred Primary	<input type="checkbox"/>
Configuration Transfer	<input checked="" type="checkbox"/>	Active Active	<input type="checkbox"/>
Use SSL	<input type="checkbox"/>		
<input type="button" value="Commit"/> <input type="button" value="Reset"/>			

11.3.7 Peer の登録(デフォルト Backup)

デフォルト Backup 機で Peer の登録を行います、登録する Peer はデフォルト Primary 機です。11.3.5 と同じように「Add Failover Peer」と表示させ、クリックします。Peer 登録画面が表示されるので、デフォルト Primary 機の Peer 名と Signature を入力して Commit ボタンをクリックします。Signature は 11.3.4 でコピーしたものです。

以上で Failover 設定は完了です。

11.3.8 Failover 状態の確認

左フレームの Failover をクリックすると、Peer Summary 画面が表示され状態確認ができます。Failover Status ウィンドウに「No Errors Detected」とある場合、エラーなく Failover 構成になっていることを示します。また、右上の[Configuration Sequence Number]の値が両機器で同値であることも確認して下さい。

下部には Peer の状態が表示されます。Failover Mode がそれぞれ Primary と Backup になっていることを確認します。下はデフォルト Primary 機の Peer Summary です。

Peer Name	L/R	Type	Flags	Failover Mode	Messages
ADC300E-181	Local	OS/10	Failover, Preferred Primary, Configuration Transfer	Primary	None
ADC300E-182	Remote	OS/10	Failover, Configuration Transfer	Backup	None

下はデフォルト Backup 機の Peer Summary です、Failover Mode は表示が逆になります。

Peer Name	L/R	Type	Flags	Failover Mode	Messages
ADC300E-182	Local	OS/10	Failover, Configuration Transfer	Backup	None
ADC300E-181	Remote	OS/10	Failover, Preferred Primary, Configuration Transfer	Primary	None

11.3.9 Peer のヘルスチェック設定

下記の各項目にて、Peer のヘルスチェックの設定を行います。設定変更は Peer 名の後ろに (Local)とついている機器自身のみ変更可能です。

パラメータ	設定内容
Receive Timeout	Failover peer への接続確立後のレスポンス待機時間 デフォルト: 2 秒
Connection Timeout	Failover peer への接続確立の待ち時間 デフォルト: 1 秒
Heartbeat Interval	Heartbeat 正常時のヘルスチェックの間隔 デフォルト: 2 秒
Retry Interval	Heartbeat 失敗時のヘルスチェックの間隔 デフォルト: 5 秒
Failed Probe Count	Failover peer がダウンと判定するまでの判定回数 デフォルト: 3 回

複数 ISP 接続は提供サービスの冗長性を確立するのに重要です。回線負荷分散 (Link Load Balance、LLB) 機能は ADC アプライアンスがインフラにおいて複数上流リンクをサポートする事が可能になります。

プライマリの ISP リンクが切れてしまった場合に、回線負荷分散はシームレスに通信をバックアップ回線へ切り替え致します。広域負荷分散 (Global Server Load Balance、GSLB) と同様に、Inbound LLB (ILLB) はゲートウェイの代わりに DNS ベースの負荷分散によって、Border Gateway Protocol (BGP) での冗長化の必要性を排除します。また、LLB は複数経路でクライアントの到達性を、Outbound と Inbound の両通信について設定を行う事で、確保します。

12 Log & Report

本章では、ログ情報と機器の負荷状況を表示される項目についての内容を記載いたします。

12.1 Log & Reports

12.1.1 Logging タブ

ログに関する設定/確認を行います。

12.1.1.1 Event Log

各種イベントログを表示します。左側にあるパラメータをクリックすることで、関連するログを表示することが可能です。

なお、すべてのログについては、サポートでも使用します、save state を取得していただければ、その中に本ログを確認することが可能です。

パラメータ	内容
Hostname	全てのログを表示します
Clusters	クラスタ毎のログを表示します
Server Pools	Server Pool 毎のログを表示します
Servers	Server 毎のログを表示します
Responders	Responder 毎のログを表示します
Syslog	Syslog を表示します
Upgrade Log	アップグレード時のログを表示します

右上のボタンは以下の通りに動作します。

パラメータ	内容
Export CSV	表示されているログを CSV 形式で出力します。
Refresh	現在の表示を更新して最新の情報を表示します
Click To Filter Date	ログの表示期間を任意の範囲を変更して表示します

12.1.2 Notification

12.1.2.1 Notification の通知

Configuration で設定されたアラートで ui が設定された場合に、Notification の一覧が表示されます。通知されるアラートは ID 管理され、機器の起動時から 1 番号を振り、200 まで増加し、1 に戻り上書きされます。

ID	Notification ID です。番号1から始まる整数を表示します。
Time Stamp	アラート通知された時間を表示します。
Alert Type	アラートタイプです。アラートのオブジェクト名を参照して下さい。
Object Type	アラートタイプです。

Object Name	アラート対象となったオブジェクト名です。
Alert Name	設定されるアラート名です。

以下に説明する例では CLI にログイン時に **ハイライト**2つのペンディングアラートが確認出来ます。

```
12000004: You have 2 pending alert notifications.
eqcli >
```

alert_interval パラメーターの設定によって、ペンディングメッセージの確認インターバルを変更する事が可能です。また、ペンディング通知がある場合にはコンソール上にメッセージが表示されます。

1. ペンディング通知の数に変更が生じた時
2. コマンドプロンプトでデータを入力しない状態が継続した際には、ペンディング通知は Enter キーが押された時点で表示されます。

12.1.2.2 通知の表示

全てのペンディング通知リストを表示するには show notification を実行します。

```
eqcli > show notification
```

生成されるアラート順にアラート通知がリストされます。

```
eqcli > show notification

ID   Time Stamp      Type           Obj Type  Obj Name  Alert Name
1    Jan  1 00:00:00 state_change  server   server1_80 al_test1
2    Jan  1 00:00:00 state_change  server   server2     al_test2
3    Jan  1 00:00:00 state_change  si       server2     al_test2
4    Jan  1 00:00:00 state_change  si       server2     al_test2
5    Jan  1 00:00:00 state_change  si       svever1_80 al_test1
eqcli>
```

最初の通知を表示したい場合には show notification first を入力します。以下は表示例になります。

```
eqcli > show notification first

fiest
Notification ID : 1
Alert Type : state_change
Alert Subtype : Up
Alert Name : al_switch
Object Type : interface
Object Name : swport01
Message : 50000197: Port 1 has become ACTIVE
eqcli>
```

フィルタリング表示する事で 1 つ、もしくは複数の適合する通知を表示させる事も可能です。

```
eqcli> show notification first alert_type alerttype object_type objecttype object_name
objectname
```

オブジェクト名が明確な場合、object_type も明記する必要があります。以下は swport01 の表示例です。

```
eqcli > show notification first alert_type state_change object_type interface object_name
swport01

Notification ID : 1
Alert Type : state_change
Alert Subtype : Up
Alert Name : al_switch
Object Type : interface
Object Name : swport01
Message : 50000197: Port 1 has become ACTIVE
eqcli >
```

12.1.2.3 Notification の削除

通知された Notification は連番でリスト化されます。通知され、確認が済んだ Notification を削除します。

表示される Notification リストの ID の左ボックスにチェックを入れゴミ箱をクリックすると、指定した Notification が削除されます。表示される全ての Notification を選択したい場合には、Alert Name の左ボックスにチェックを入れると全選択になります。

CLI での削除は no notification all で削除します。

```
eqcli > no notification all
```

個別のアラート通知を削除する場合には no notification <id-number> で ID 番号を入力します。

```
eqcli > no notification <id-number>
```

以下表示と削除の実行例です。

```
eqcli > show notification

ID   Time Stamp      Type           Obj Type  Obj Name      Alert Name
---   -
1    Feb 23 16:41:08 state_change  interface  if01          UI, syslog
2    Feb 23 16:41:08 state_change  interface  if06          UI, syslog
3    Feb 23 16:41:08 state_change  fogrp      Unassigned    al_allpeers
eqcli >
```

12.1.2.4 Remote Syslog

FortiADC のログを Syslog サーバーへ出力する場合に設定します。

パラメータ	設定内容
Syslog Server	syslog サーバーの IP アドレスの設定
Enable Remote Logging	Remote Syslog の有効・無効の変更

12.1.3 Reporting タブ

機器の CPU とメモリの利用状況を表示します。

各項目に3つの目盛りがあり、それぞれ現在の値、直近 60 分の平均、直近 60 分の最大値を指しています。

パラメータ	設定内容
CPU Consumption (%)	CPU 使用率(%)
Memory Utilization (MB)	メモリ使用量(MB)

13 その他操作手順

13.1 touch パスワードのリセット方法

ユーザ touch のパスワード初期化は、コンソールの debug モードから行うことができます。パスワード初期化を行っても、ユーザ touch に紐づくそれ以外の設定は初期化されません。

- 1 以下のようにログイン画面を表示します。

```
ADC300E-181 login: eqadmin on tty tty00
Username:
```

- 2 キーボードのコントロールキー(Ctrl) と C キー(c) を同時に入力すると以下のように表示され debug モードに入ります。

```
Username: ^CCaught interrupt.  Exiting to debug mode
(type 'help' and press enter for help).
debug >
```

- 3 コマンド reset passwd を入力すると、パスワードがリセットされます。

```
debug > reset passwd
Reset password successful.
debug >
```

- 4 コマンド exit を入力し、debug モードを抜けると通常のログインプロンプトが表示されますので、デフォルトのパスワード touch を入力し、ログインします。

```
ADC300E-181 login: eqadmin on tty tty00
Username: touch
Password:
Login successful.
      FortiOS v4.0,build0012
eqcli >
```

13.2 FortiADC 初期化方法

FortiADC を工場出荷状態へ戻すには、CLI から以下のコマンドを実行します。コマンドを実行すると以下のように確認メッセージが表示されます。「Y」を入力することで実行されます。実行後、機器は自動的に再起動します。

```
eqcli > hidden reset keep-license
```

```
WARNING! This command resets the Equalizer configuration to a
factory installed condition. All VLANs, subnets, clusters, servers,
SSL certificates, and other user-supplied objects and settings will
be removed. After the configuration has been reset, the system will
be rebooted. Do you want to continue (Y/N)?
```

注意点:

コマンドを実行すると、機器の両方の Boot パーティションが初期化されます。

Boot パーティション A でコマンドを実行した場合は、Boot パーティション A, B の両方が初期化されます。