

Equalizer EQ/OS 10 設定手順書

Equalizer LX シリーズ
Equalizer OnDemand シリーズ

EQ/OS 10.0.4c 対応版

Ver. 1.2

目次

1	はじめに	5
2	初期設定	6
2.1	機器の設置	6
2.2	Equalizer のポート構成・ネットワーク構成	6
2.3	ターミナルエミュレーターの設定	6
2.4	初期設定 (CLI)	7
2.4.1	シリアルコンソールログイン	7
2.4.2	VLAN の設定	7
2.4.3	VLAN subnet の作成および接続プロトコルの許可設定	7
3	GUI の操作	9
3.1	Equalizer GUI へのアクセス	9
3.2	Equalizer GUI の画面表示について	10
3.2.1	画面構成	10
3.2.2	右クリック操作	10
3.2.3	ドラッグ & ドロップ操作	11
3.2.4	Help ボタンについて	11
3.3	Equalizer GUI からのログアウト	11
4	CLI の操作	12
4.1	Equalizer CLI への SSH によるアクセス	12
4.2	Context およびプロンプト表示	12
4.3	show コマンドによる情報表示	13
4.4	コンテキストのヘルプ表示	14
4.5	設定の反映手順	15
4.5.1	グローバルコンテキストから設定	15
4.5.2	各設定のコンテキストから設定	15
4.6	キュー状態のコマンド	16
4.7	設定の削除・リセット	16
4.8	パラメータの変更	17
4.9	コマンドの補完	17
4.10	Flag の操作	17
5	グローバルパラメータ設定	19
5.1	Global タブ	19
5.1.1	Parameters	19
5.1.2	SNMP	20
5.1.3	Certificates	20

5.1.4	CRL	21
5.2	Logging タブ	22
5.2.1	Event Log	22
5.2.2	Remote Syslog	22
5.3	External Services タブ	23
5.3.1	SMTP Relay	23
5.3.2	VLB Manager	23
5.4	Maintenance タブ	23
5.4.1	Date & Time	23
5.4.2	Backup & Restore	23
5.4.3	Licensing	24
5.4.4	Manage Software	24
5.4.5	Tools	25
5.5	Interfaces タブ	25
5.6	Reporting タブ	26
6	ネットワーク設定	27
6.1	VLAN の追加	27
6.2	subnet の追加	27
6.3	subnet 設定の変更	28
6.3.1	“Configuration”タブ	28
6.3.2	“Failover”タブ	28
6.3.3	“Permitted Subnets”タブ	28
6.3.4	“Static Routes”タブ	29
6.3.5	“Policy Routing”タブ	29
7	サーバー設定	30
7.1	サーバーの新規追加	30
7.2	サーバーの設定変更	30
7.2.1	“Configuration > Required”タブ	30
8	サーバープール設定	32
8.1	サーバープールの新規追加	32
8.2	サーバープールの設定変更	33
8.2.1	“Configuration > LB Policy”タブ	33
8.3	サーバーインスタンスの追加	34
8.3.1	サーバープールから追加する手順	34
8.3.2	サーバープールから追加する手順	35
8.4	サーバーインスタンス設定	35

8.4.1	“Configuration > Required”タブ	35
9	クラスタ設定	37
9.1	クラスタの新規追加	37
9.2	クラスタの設定変更	37
9.2.1	“Configuration > Summary”タブ	37
9.2.2	“Configuration > Settings”タブ	38
9.2.3	“Configuration > Persistence”タブ	39
9.2.4	“Configuration > Timeouts”タブ	41
9.2.5	“Security > Certificate”タブ (https クラスタのみ)	41
9.2.6	“Security > SNI”タブ (https クラスタのみ)	42
9.2.7	“Security > SSL”タブ (https クラスタのみ)	42
9.3	クラスタへのサーバープール追加	42
9.4	クラスタのステータス確認 (Cluster Summary)	42
10	Failover 設定	43
10.1	Failover 動作の基本概念について	43
10.1.1	Primary 役、Backup 役について	43
10.1.2	デフォルト Primary、デフォルト Backup について	43
10.1.3	冗長化の通信 (heartbeat) について	43
10.1.4	Failover ペア同士のコンフィグ同期について	43
10.1.5	Primary への切り替え動作について	44
10.2	Failover 設定の事前準備について	44
10.3	Failover 設定	45
10.3.1	VLAN/Subnet 設定	45
10.3.2	Peer 名設定	46
10.3.3	Signature 情報の取得 (デフォルト Backup)	46
10.3.4	デフォルト Primary 機の Flag 設定	46
10.3.5	Peer の登録 (デフォルト Primary)	47
10.3.6	デフォルト Backup 機の Flag 設定	47
10.3.7	Peer の登録 (デフォルト Backup)	47
10.3.8	Failover 状態の確認	48

1 はじめに

本手順書は、Coyote Point Systems 社 Equalizer 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 Equalizer の設置・設定・運用を行うことができます。本文書は Equalizer をより簡単に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「Equalizer Administration Guide」とは異なる事がありますので予めご了承下さい。

より詳細な説明につきましては「Equalizer Administration Guide」をご参照頂きますようお願い致します。ダウンロードは弊社 Equalizer 製品ページから行うことができます。また、Equalizer 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。

2 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。

2.1 機器の設置

Equalizer のインストールは以下の手順で行います。

1. 同封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。同封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 Equalizer を設置します。
3. 同封されているシリアルケーブルを使用する際に、Equalizer 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. Equalizer に同封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 Equalizer 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スイッチをオンにして、電源を投入します。

2.2 Equalizer のポート構成・ネットワーク構成

Equalizer 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
E250GX	1 - 2
E350GX / E450GX	1 - 12
E650GX	1 - 22
E370LX	1 - 6
Equalizer OnDemand	1 - 2 (最大 16 まで拡張可能)

2.3 ターミナルエミュレーターの設定

Equalizer 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。Equalizer 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 (LX シリーズは 38400)
Data	8 bit
Parity	none
Stop	1 bit
Flow control	none

Windows デフォルトのターミナルエミュレーター「HyperTerminal」を使用する場合、keyboard application mode と cursor keypad mode を有効にする必要があります。

もしご利用のターミナルソフトウェアでシリアルラインのハングアップ設定のサポートがある場合、ハングアップを無視するよう設定して下さい。設定する事で、Equalizer が再起動してもシングルターミナルセッションとして使用する事が出来ます。

HyperTerminal のほか、無料で配布されている [TeraTerm](#) を使用することも可能です。

2.4 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。

2.4.1 シリアルコンソールログイン

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

```
EQUALIZER -- EQ/OS 10.0.4c-RELEASE

Username: touch
Password:
Login successful.

      EQ/OS 10.0.4c

      Copyright 2013 Fortinet, Inc.
      Welcome to Equalizer!

eqcli >
```

2.4.2 VLAN の設定

VLAN を作成するコマンドは以下の通りです。

```
vlan [VLAN 名] vid [VID 番号] untagged_ports [untagged ポート番号]
```

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
untagged_ports	VLAN に割り当てる untag ポートの番号を入力します

以下の例では DEFAULT という VLAN を VLAN ID 1 で作成し、port 1 と 2 を割り当てます。

```
eqcli > vlan DEFAULT vid 1 untagged_ports 1,2
```

2.4.3 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]
      default_route [デフォルトゲートウェイ IP アドレス] services [許可プロトコル]
```

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
default_route	デフォルトゲートウェイ IP アドレスを入力します
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 (E650GX のみ) - Envoy Agent (E650GX のみ)

以下の例では「VLAN-1」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 VLAN-1 subnet external ip 172.16.0.200/21
                                default_route 172.16.0.1 services ssh,http

```

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

```


3 GUI の操作

初期設定の完了後は、Equalizer 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。

- Chrome
- Firefox
- Safari
- Internet Explorer

3.1 Equalizer 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。パスワードは touch です。

ログインすると画面中央に機器のシステム情報が表示されます。各項目の内容は以下の通りです。

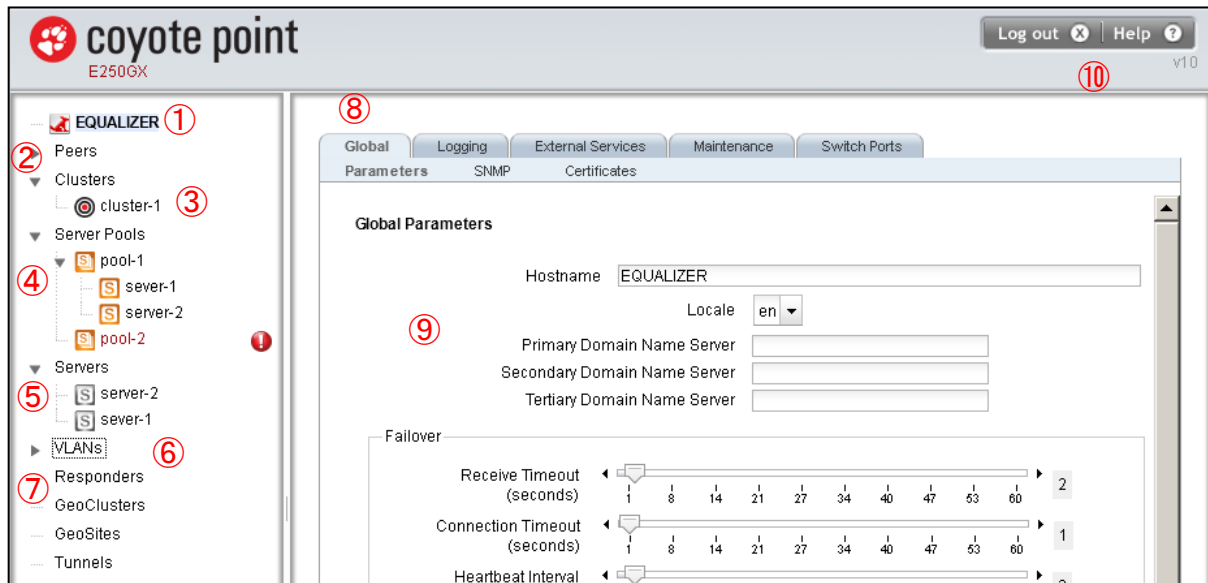
項目	設定内容
System Type	機器のモデルが表示されます
Equalizer O/S Version	ファームウェアバージョンが表示されます
Equalizer Firmware Tag	ファームウェアのタグ情報が表示されます(RELEASE, patch 等)
System Revision	機器のリビジョンが表示されます
System ID	機器の System ID が表示されます
System Serial Number	機器のシリアル番号が表示されます
Hardware Features	ハードウェアのオプション情報が表示されます
Switch Type	スイッチモジュールのタイプが表示されます
Switch Count	スイッチモジュールの数が表示されます
Current Firmware ID	スイッチモジュールの現在の Firmware ID が表示されます
Latest Firmware ID	使用しているファームウェアバージョンの Firmware ID が表示されます

3.2 Equalizer GUI の画面表示について

GUI の画面表示について説明します。

3.2.1 画面構成

GUI の画面構成は主に以下の項目があります。



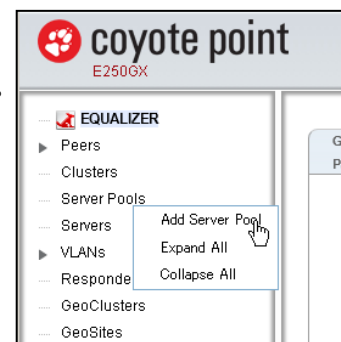
左フレーム

右フレーム

- ① グローバル設定画面を表示します。
- ② Failover 設定画面を表示します。
- ③ 設定されているクラスターが表示されます。
- ④ 設定されているサーバープールが表示されます。
- ⑤ 設定されているサーバーが表示されます。
- ⑥ 設定されている VLAN および subnet が表示されます。
- ⑦ 設定されている Responders が表示されます。
- ⑧ 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。
- ⑨ タブで選択した内容が表示されます。
- ⑩ 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。

3.2.2 右クリック操作

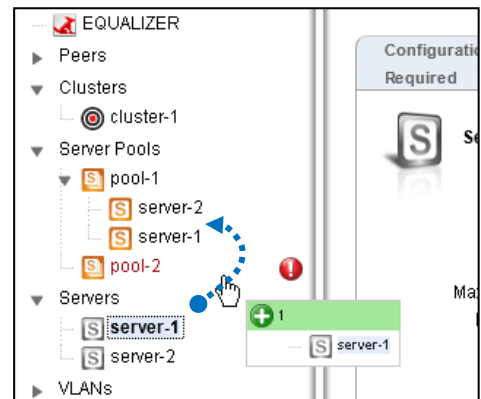
左フレームの項目を右クリックすることでメニューが表示されます。右の図はサーバープールで右クリックした際の表示です。新規追加(add)や既存設定の削除(delete)、項目の展開・折り畳み(Expand/Collapse)をすることが可能です。



3.2.3 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。右の図は、サーバー「server-1」をドラッグ & ドロップでサーバープール「pool-2」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。



3.2.4 Help ボタンについて

ヘルプ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。

3.3 Equalizer 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。

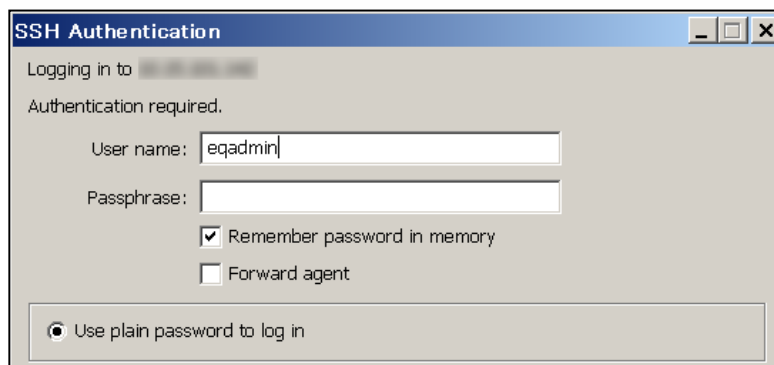
4 CLI の操作

本章では 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。

4.1 Equalizer CLI への SSH によるアクセス

2.3 および 2.4 で前述の通り、CLI へのアクセスはシリアルケーブル経由で行いますが、subnet 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 subnet の service 設定で SSH 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。subnet 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。ユーザ名は eqadmin と入力し、パスワードは空欄のまま継続します。

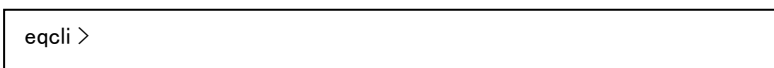


Equalizer の認証画面が表示されますので、設定しているユーザ名・パスワードを入力します。ログインに成功すると以下のような画面になり、プロンプトが eqcli > に変化します。画面スクロールが正常に行われない場合は、ウィンドウの縦を短めに調整下さい。



4.2 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「cl-1」のコンテキストに移行しています。

```
eqcli > cluster cl01
eqcli cl-cl01>
```

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 文字以上の場合に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
The current context is: 'mycluster'
eqcli cl-myc*>
```

4.3 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

recv_timeout  2
conn_timeout  1
probe_interval 2
retry_interval 5
strike_count  3
~後略~
```

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す。

```
eqcli > show cluster

Name      IP Address  Port  Proto
cluster-1 192.168.1.100 25   tcp
cluster-2 192.168.1.200 80   http
eqcli >
```

各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「cluster-1」で実行した際の結果です。

```

eqcli > cluster cluster-1
eqcli cl-clu*> show
This cluster has a problem:
Cluster configuration is incomplete
Cluster is not active on this Equalizer

L4 Cluster Name : cluster-1
Protocol       : tcp
IP Address     : 192.168.1.100
Port          : 25
Port Range    : 0
Preferred Peer :
VID           : 1
Server Pool   :
Sticky Timeout : 0
Sticky Netmask : 0
Idle Timeout  : 60
Stale Timeout  : 30
L4 Flags      :
eqcli cl-clu*>

```

4.4 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 >?

backup       : Upload a system backup to remote FTP.
certificate  : Add or modify an SSL certificate.
cluster      : Add or modify a cluster or a match rule.
~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-cl01>?

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.

```

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 cl01 ?

age          : Set the cookie age for a cluster.
certificate  : Attach a certificate to an HTTPS cluster. Required for
HTTPS clusters.
~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 mycluster stats ?

stats: Display the statistics for a cluster.

Syntax: cluster <name> stats

```

4.5 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

4.5.1 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-1 proto tcp ip 192.168.1.1 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。

4.5.2 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-1
eqcli sv-ser*> proto tcp
eqcli sv-ser*> ip 192.168.1.1
eqcli sv-ser*> port 80
eqcli sv-ser*> commit

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

```

4.6 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-1
eqcli sv-ser*> proto tcp
eqcli sv-ser*> ip 192.168.1.1
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-1
eqcli sv-ser*> proto tcp
eqcli sv-ser*> ip 192.168.1.1
eqcli sv-ser*> port 80
eqcli sv-ser*> quit
eqcli >
```

4.7 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 > no server server-1

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「mycluster」に設定されている Match Rules「match-1」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 mycluster match match-1

eqcli: 12000287: Operation successful
eqcli >
```


4.8 パラメータの変更

設定の変更を行うには、同じコマンドを実行し設定変更したいパラメータを再度入力します。以下の例では、VLAN「VLAN-1」を VID 10 で作成した後に、VID を 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 > vlan VLAN-1vid 10
eqcli: 12000287: Operation successful

eqcli > vlan VLAN-1vid 20
eqcli: 12000287: Operation successful
eqcli >

```

4.9 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 cluster conn_timeout context crl

eqcli > con<space>
conn_timeout context

```

4.10 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。

```

eqcli > server server-1 flags probe_13

eqcli: 12000287: Operation successful
eqcli >

```

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。

```

eqcli > server server-1 flags !probe_13

eqcli: 12000287: Operation successful
eqcli >

```

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 > srvpool pool-1 si server-1 flags quiesce,probe_14  
  
eqcli: 12000287: Operation successful  
eqcli >
```

5 グローバルパラメータ設定

本章では Equalizer のグローバルパラメータ設定について説明します。

GUI 左フレームの上部にあるホスト名(デフォルト「EQUALIZER」)をクリックすることで表示されます。各タブで Commit ボタンを押下することで設定が反映されます。

5.1 Global タブ

機器全体の設定を行います。

5.1.1 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/日本語)
Primary Domain Name Server	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

- ・ Failover

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

パラメータ	設定内容
ICMP Probe Maximum Tries	「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。デフォルトでは 15 秒の間に 3 回 ICMP によるチェックを行います。 (デフォルト: 3 回)
ICMP 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)

- ・ Global Service Settings

パラメータ	設定内容
Global Service Settings	Equalizer 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。

5.1.2 SNMP

SNMP 設定を行います。

パラメータ	設定内容
System Name	Equalizer 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	Equalizer 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、ユーザ様任意の項目です。

Equalizer 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。

<http://<equalizer 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

5.1.3 Certificates

HTTPS クラスタに設定するサーバー証明書をアップロードすることができます。

サーバー証明書のアップロードを行うには「Add Certificate」ボタンをクリックします。以下のような画面が表示されます。

Add Certificate

Certificate

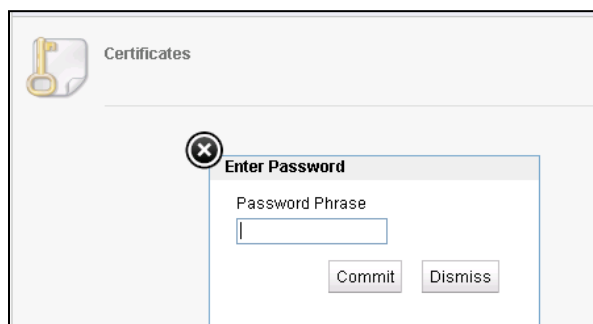
Name

Certificate File

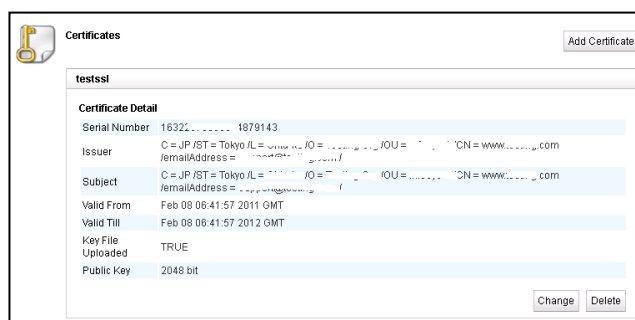
Key File

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 Equalizer 内部でのみ使用される名前です。
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。

Commit をクリックし決定します。秘密鍵にパスワードが設定されている場合は、以下のようにパスワード入力画面になります。パスワードを入力してください。



サーバー証明書のアップロードが完了しますと、以下のような形で内容が表示されます。



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か「Change」ボタンをクリックし、再度証明書をアップロードします。

サーバー証明書を削除する場合は、Delete をクリックして削除します。

5.1.4 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である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。

5.2 Logging タブ

ログに関する設定/確認を行います。

5.2.1 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。

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	Sever 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

Filter Parameters

Start Time - 15/02/2013 14:05:00 End Time - 21/02/2013 17:40:27

Start Time End Time

Error Warning Info

5.2.2 Remote Syslog

Equalizer 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

5.3 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。

5.3.1 SMTP Relay

SMTP Relay を使用する場合は、設定を行います

5.3.2 VLB Manager

VLB Manager を利用する場合は、設定を行います。

5.4 Maintenance タブ

機器の管理を行う場合に使用します。

5.4.1 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。
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。 例) 2013 年 5 月 1 日 14 時 55 分 00 秒の場合 05/01/2013 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。

5.4.2 Backup & Restore

Equalizer のコンフィグをバックアップ・リストアします。コンフィグファイルのバックアップ先やリストア元は、それぞれ FTP サーバーまたはローカル端末を指定することが可能です。

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 <ul style="list-style-type: none"> ・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 にはバックアップファイルの名前が表示されます。 ・Destination <ul style="list-style-type: none"> 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
Restore	機器へバックアップファイルのリストア(復元)を行います。

	*Source FTP URL: FTP からリストアップ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
--	--

5.4.3 Licensing

ライセンスの管理を行います。

パラメータ	設定内容
Retrieve Online License	オンラインでライセンスを取得します
Request Offline License	オフラインライセンスを発行するための情報を取得します。これはローカル PC に保存することが可能です。
Upload Offline License	オフラインライセンスをアップロードします。弊社から提供したオフラインライセンスを選択し、アップロードします。

ライセンスファイルは以下のように表示されます。ValidがYESになっていればライセンスは有効な状態で機器に保存されています。ライセンスを削除する場合は各ライセンスの右下に表示される「Delete」をクリックします。

04-23-2013.12-38-08.1 (E370LX)	
License Name	: 04-23-2013.12-38-08.1
Version	:
Comment	:
Product	: E370LX
Key	:
System ID	:
Serial	:
Valid	: YES
Start Date	: 03-01-2013
End Date	: none
Delete	

5.4.4 Manage Software

Equalizer 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 EQ/OS バージョン情報が表示されます。
EQ/OS Release Status	現在のファームウェアのバージョンと、最新ファームウェアのバージョンが表示されます。最新ファームウェアの情

	報は Manage Software 画面を開いた際にインターネットから情報を取得します。
Upgrade	EQ/OS 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 Equalizer へアップロードする方法を選択します。

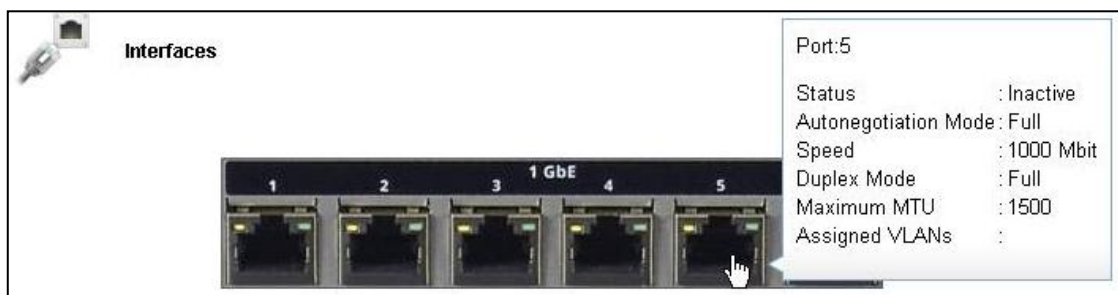
5.4.5 Tools

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
Configuration Converter	バージョン 8.6 のコンフィグをアップロードし、EQ/OS 10 コンフィグへコンバートします。
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メッセージ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メッセージ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	Equalizer 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。

5.5 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。



パラメータ	設定内容
Port	ポート番号が表示されます。
Status	リンクアップ状態が Active/Inactive で表示されます。
Autonegotiation Mode	オートネゴシエーション設定が Full/Select/Force 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。
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
Autonegotiation	Full: サポートされる Speed および Duplex を全て使用し、オートネゴシエーションを行います(デフォルト設定) Select: Speed および Duplex を指定し、その設定でのみオートネゴシエーションを行います。 Force: Speed および Duplex を指定し、オートネゴシエーションせずに固定接続を行います。
Speed	Autonegotiation を Select または Force に設定した場合、ポートの速度設定を 1000Mbit/100Mbit/10Mbit から選択します。
Duplex Mode	Autonegotiation を Select または Force に設定した場合、ポートの Duplex 設定を Full/Half から選択します。

5.6 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)

6 ネットワーク設定

本章では Equalizer のネットワーク設定について説明します。
ネットワークの設定はまず VLAN を作成しポートを割り当てます。各 VLAN に subnet を設定することで通信を行えるようになります。

6.1 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。

パラメータ	設定内容
tagged_ports	ポートを tag で VLAN に割り当てます。
untagged_ports	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、1～4096 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。

6.2 subnet の追加

設定した VLAN 上で 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。

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(Default Route はオプション項目です)。

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。

6.3 subnet 設定の変更

左フレームから subnet 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。

6.3.1 “Configuration”タブ

subnet の基本設定を行います、パラメータは以下の通りです。

パラメータ	設定内容
IP Address	IP アドレスを設定します。
Default Route	subnet のデフォルトゲートウェイを設定します。
Outbound NAT Address	outbound NAT 機能で使用する IP アドレスを設定します。
Default Source Address	有効にする事で outbound NAT 使用時に subnet の送信元 IP が使用されます。1 つの subnet のみ設定可能です。
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。

6.3.2 “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。

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。
Command Transfer	有効になっている subnet でコンフィグ同期が行われます。機器で 1 つの subnet のみ設定可能です。
Heartbeat	subnet 上で Failover を有効にします。
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 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)。

6.3.3 “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。

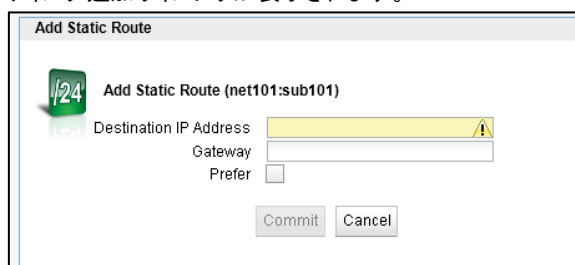
図では、VLAN「net100」に所属する subnet「sub100」からの通信を許可させるためドラッグ&ドロップしています。双方向で通信を行うためには、もう片側の subnet でも同様に許可する必要があります。

設定後、画面下部の commit ボタンをクリックし決定します。





6.3.4 “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、Equalizer 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。

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てから  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。

6.3.5 “Policy Routing”タブ

宛先と送信元 IP を指定してルーティングを設定します。

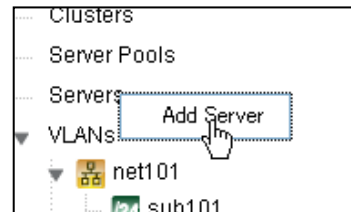
7 サーバー設定

本章では Equalizer 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行われます。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。

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。

 A screenshot of the 'Add Server' dialog box. It has a title bar 'Add Server' and a server icon. The 'Protocol' dropdown is set to 'tcp'. There are input fields for 'Server Name', 'IP', and 'Port'. At the bottom are 'Commit' and 'Cancel' buttons.

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 > Required”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 Connections	HTTP Multiplexing 有効時に、再利用されるコネクションプー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。
Probe Layer 3	ICMP プロープの有効・無効を設定します。

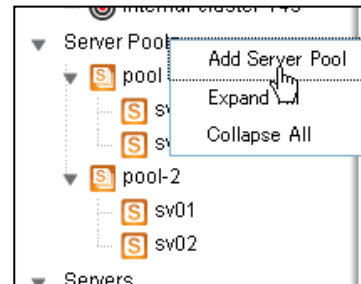
8 サーバプール設定

本章では Equalizer 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)への通信を負荷分散させることが可能になります。負荷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。



以下の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。

 A screenshot of the 'Add Server Pool' dialog box. It has a title bar 'Add Server Pool' and a server icon. Below the icon, there is a 'Server Pool Name' text box containing 'server-pool' and a 'Policy' dropdown menu set to 'round-robin'. At the bottom, there are 'Commit' and 'Cancel' buttons.

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荷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	デフォルトの負荷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荷分散サーバーのリストから除外して負荷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荷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 値を基に負荷分散を行います。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	Equalizer 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。

	<ul style="list-style-type: none"> 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	<p>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 Equalizer 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 Equalizer はクラスタ単位でこのレスポンス時間を最適化します。</p> <p>この負荷分散アルゴリズムでは Equalizer 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 Equalizer は新規セッションをそのサーバーに振らないことがあります。</p>
least-cxns	<p>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 Equalizer 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。</p>
server-agent	<p>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）。</p>
custom	<p>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。</p>

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。

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	サーバールールを無効にします、負荷分散の振り分けは行われなくなります。
Load Balancing Policy	
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 Equalizer 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。
Layer 4 Handshake Probes	
Probe Interval (seconds)	この時間内に TCP/UDP のプローブは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。 Probe Interval が 3 に設定され Max Tries Per Interval が 3 の場合、Probe Interval の時間内で最大で 3 回プローブを実施します(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)。
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 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。
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。
Probe 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。

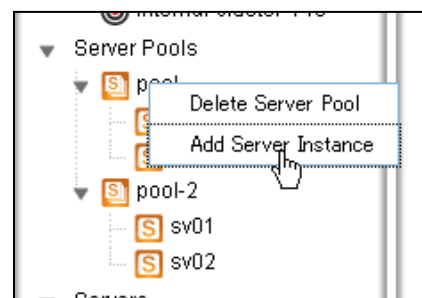
8.3 サーバーインスタンスの追加

サーバーをサーバープールへ追加します。 サーバープ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 サーバープールから追加する手順

右図のように、サーバーを追加するサーバー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。



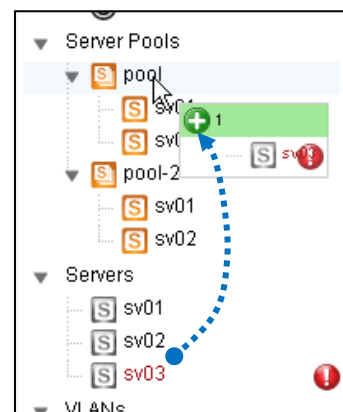
必要な項目を設定し、Commit ボタンをクリックします。

パラメータ	設定内容
Server Instance Name	設定されているサーバーが表示されるので、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。詳細な説明は 7.3.3 を参照下さい。(デフォルト有効)

8.3.2 サーバー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、サーバープール上にドラッグ & ドロップします。右図ではサーバー「sw03」を、サーバープール「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 7.3.1 の説明を参照下さい。



Server Instance Weight

Initial Weight 100

Quiesce

Commit Cancel

8.4 サーバースタンス設定

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 > Required”タブ

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ず(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)。
Maximum Connections	サーバーへ振り分けを行う最大同時接続数を設定します。デフォルトは 0 で制限を行いません。

Probe Port	ヘルスチェックに使用するポート番号を、サーバーポートとは別にする場合に使用します。デフォルトは0でサーバーに指定しているポート番号を使用します。
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。デフォルトは無効です。
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	<p>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。</p> <p>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、Equalizer 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。</p> <p>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。</p>
Probe Layer 4	有効にすることでサーバーに対し L4 によるヘルスチェックおよび ACV(オプション)を行います。デフォルト無効。
Strict Max Cx	<p>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。</p> <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

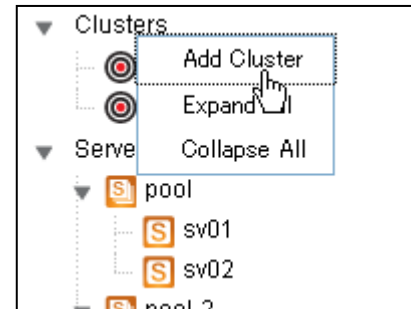
本章では Equalizer のクラスタ設定について説明します。

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。またコネクション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コネクション数が表示されます。
Connections/second(CPS)	秒間のコネクション数が表示されます。

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 分間のコネクション情報を表示します。

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 Equalizer 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、新規のコネクション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	Equalizer 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 コネクションを切断した場合に Equalizer はサーバーとのコネクションを切断せず応答を待ちます。 有効に設定すると、Equalizer はサーバーからの応答を待たずに TCP RST を送信しコネクションを切断します(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(デフォルト無効)。
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 Equalizer 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(デフォルト無効)。
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 Equalizer 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を設定します。
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、Equalizer が https: に自動で書き換えます(デフォルトの場合)書き換え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。

tcp/udp/l7tcp クラスタでは以下の設定になります。

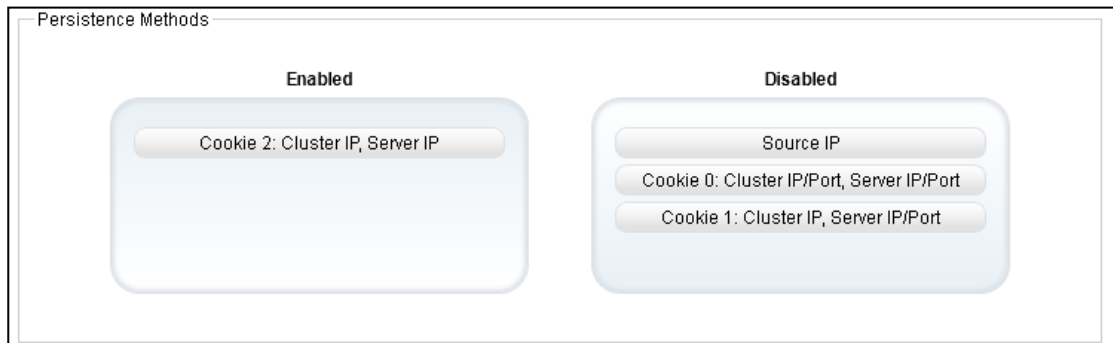
The screenshot shows the 'Persistence' configuration page. At the top, there is a 'Sticky Netmask' slider ranging from 0 to 32, with the current value set to 32. Below it, 'Sticky Timeout (seconds)' is a text input field containing '0'. 'Inter Cluster Sticky' is a checkbox that is currently unchecked. At the bottom, there are 'Commit' and 'Reset' buttons.

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(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。

http/https クラスタでは以下の設定になります。

「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	Equalizer 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ー IP と振り分けられたサーバーIP を判別して動作します。クラスター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	Equalizer 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ー 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。クラスター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	Equalizer 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ー 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	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	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	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 の付与を行いません。 (例えば www.coyotepoint.com や my.coyotepoint.com)。
Cookie Age	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、Equalizer はセッション維持動作を行いません。 設定する場合は、クライアント・Equalizer・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	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	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。

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 Equalizer が切断するまでのタイムアウト時間を設定します。
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。
http/https/l7tcp クラスタ共通	
Client Timeout (seconds)	Equalizer 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(デフォルト 10 秒)。
Server Timeout (seconds)	Equalizer がサーバーへリクエストを投げてから次のリクエストを受け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(デフォルト 60 秒)。
Connect Timeout (seconds)	接続要求に対してサーバーがレスポンスを返すまでの Equalizer 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)

https クラスタでは SSL 通信のオフロードに関する設定があります。

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。

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

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。

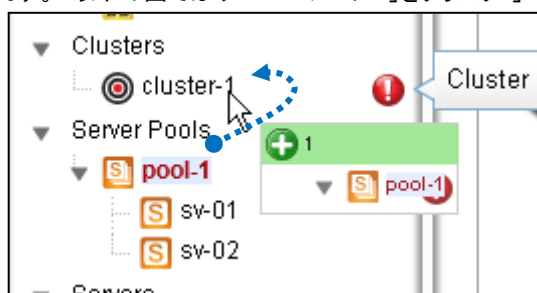
9.2.7 “Security > SSL”タブ (https クラスタのみ)

Cipher Suite 設定などに関する設定を行います。

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。
Allow SSLv3	SSLv3 による接続を有効にします。
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。

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 Failover 設定

本章では 2 台の Equalizer を冗長化する設定について説明します。

10.1 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。

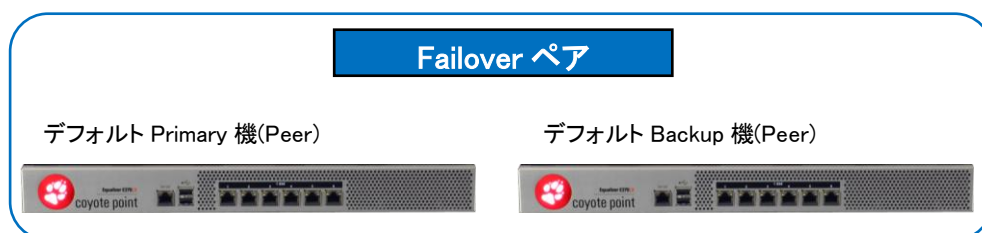
10.1.1 Primary 役、Backup 役について

Failover 設定が行われた 2 台の Equalizer 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 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 に切り替え、通信を継続します。

Failover 設定された 2 台の Equalizer 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。

10.1.2 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。



10.1.3 冗長化の通信(heartbeat)について

冗長化された Equalizer 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。

10.1.4 Failover ペア同士のコンフィグ同期について

Failover ペアを組む Equalizer 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
Servers	Subnets
Responders	Tunnels
SSL Certificates	Users
CRLs	Licenses
GeoClusters	
GeoSite	
GeoSite Instances	
Global Parameters: Syslog server NTP server Name servers	
Health Checks	
Health Check Instances	
SMTP Relays	
VLB Managers	

10.1.5 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。

10.2 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、以下は異なっても問題ありません。
・VLAN のポート番号割り当て
・Subnet の IP アドレス
2. Equalizer 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 Equalizer 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 Equalizer 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 VLAN subnet では Failover IP Address が設定されている必要があります。
4. Equalizer 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 Equalizer から Ping が成功することを確認して下さい。
- ・Equalizer のデフォルトゲートウェイ
 - ・負荷分散対象サーバー

10.3 Failover 設定

Failover の設定を実施します、必ず 10.2 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	EQ-Unit-1	EQ-Unit-2
VLAN/Subnet IP address	192.168.10.11	192.168.10.12
Failover IP address	192.168.10.10	
Default Gateway Address	192.168.10.254	
Preferred Primary	有効 (デフォルト Primary)	無効 (デフォルト Backup)

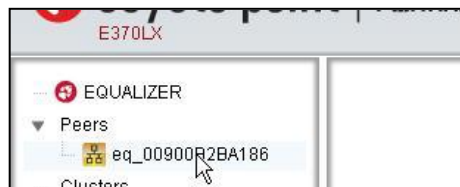
10.3.1 VLAN/Subnet 設定

両機器の Subnet に Failover 設定を行います。左フレームから VLAN > Subnet > 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。

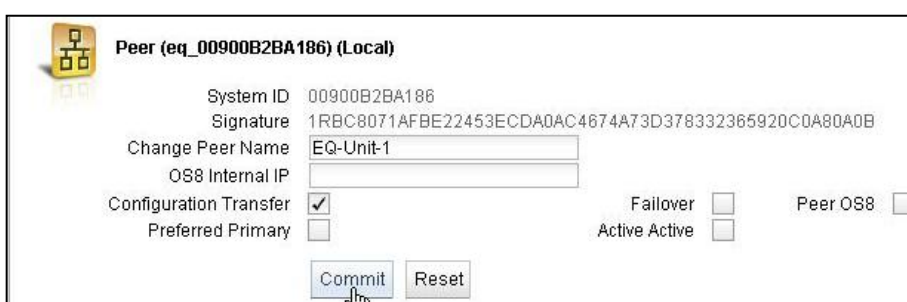
パラメータ	設定内容
Failover IP Address	Primary 役の機器が保持する仮想 IP アドレスです。クラスタ IP アドレスとは異なる IP アドレスを設定する必要があります。サーバーのゲートウェイなどとして使用されます。
Command Failover	Subnet 上でコンフィグ同期を行います。
Heartbeat	Subnet 上で heartbeat 通信を行います。
System Services on Failover IP Address	Failover IP Address で設定した IP アドレスへ通信が行われた際のプロトコル許可設定を行います。許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。

10.3.2 Peer 名設定

両機器の Peer 名を変更します。左フレームの Peers 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。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。



10.3.3 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。



10.3.4 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。

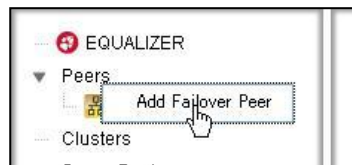


続いてデフォルト Primary 機からも Signature 情報をコピーし、テキスト等に保存します。



10.3.5 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 Peers 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 10.3.3 でコピーしたものです。



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。

10.3.6 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。



10.3.7 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。10.3.5 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 10.3.4 でコピーしたものです。

以上で Failover 設定は完了です。

10.3.8 Failover 状態の確認

左フレームの Peers 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。

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
EQ-Unit-1	Local	OS/10	Failover, Preferred Primary, Configuration Transfer	Primary	None
EQ-Unit-2	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
EQ-Unit-2	Local	OS/10	Failover, Configuration Transfer	Backup	None
EQ-Unit-1	Remote	OS/10	Failover, Preferred Primary, Configuration Transfer	Primary	None