



Equalizer GX シリーズ (E250GX / E350GX / E450GX / E650GX)

Equalizer 設定手順書

Firmware 8.6.0f 対応版 Rev.1.4

[2013/10/10]





本書の内容は予告なく変更することがあります。

本書の内容について(株)ネットワールドは如何なる責任を負うものではありません。

本書の内容の無断転写はできません。

バージョンによって画面イメージが異なります。ご了承下さい。

Copyright 2012 Networld, Corp. All right reserved.

Equalizer™ は米 Coyote Point Systems 社の登録商標です。

— 目次 —

EQUALIZER 設定手順書について.....	10
セクション1 EQUALIZER 設定の準備.....	11
1-1 機器の設置.....	11
1-2 EQUALIZER のポート構成・ネットワーク構成.....	11
1-3 ターミナルエミュレーターの設定.....	12
1-4 初期設定(EQADMIN).....	12
1-4-1 Interfaces (ネットワーク設定).....	14
1-4-2 Time Zone (タイムゾーン設定).....	16
1-4-3 Clock (時刻設定).....	16
1-4-4 Manage users (Web 管理画面アカウント作成).....	17
1-4-5 Console (eqadmin アカウントのパスワード変更).....	18
1-4-6 Commit (設定の適用・再起動).....	18
1-4-7 Shutdown (機器のシャットダウン).....	19
1-4-8 Upgrade (ファームウェアアップグレード).....	19
1-4-9 Manage 'eqsupport' (リモートアカウント接続設定).....	19
1-4-10 Reset VLANs.....	20
1-5 アカウント・パスワード一覧.....	21
1-5-1 ROOT パスワードの変更方法.....	21
セクション2 WEB 管理画面の操作.....	22
2-1 EQUALIZER WEB 管理画面について.....	22
2-1-1 Equalizer Web 管理画面にアクセスする.....	22
2-1-2 Web 管理画面の概要.....	23
2-1-3 機器の詳細情報を表示.....	23
2-1-4 Help メニューの利用.....	25
2-1-5 設定追加・変更の決定ボタンについて.....	26
2-1-6 Web 管理画面のメッセージ表示について.....	26
2-1-7 Web 管理画面からのログアウト.....	26
2-1-8 Equalizer のライセンス表示について.....	27
セクション3 機器のグローバル設定.....	28

3-1 “CLUSTERS” タブ設定	29
3-1-1 “General”	29
3-1-2 “Probes”	30
3-1-3 “VLB”	31
3-1-4 “Networking”	31
3-1-4-1 Send buffer/ Receive buffer について	33
3-1-4-2 Outbound NAT 通信について	33
3-1-4-3 “allow extended chars” 設定について	34
3-2 “STATUS” タブ設定	35
3-2-1 “Cluster Summary”	35
3-2-2 “Statistics”	37
3-2-3 “Event Log”	39
3-2-4 “Plot”	39
3-2-5 “Switch Status”	40
3-3 “MONITORING” タブ設定	41
3-3-1 “Events”	41
3-3-1-1 “logging”	41
3-3-1-2 “handling”	41
3-3-1-3 “email notification”	41
3-3-2 “Export to CSV”	42
3-3-3 “SNMP”	43
3-4 “PERMISSIONS” タブ設定	46
3-4-1 “Users”	46
3-4-1-1 ユーザアカウントの追加	46
3-4-1-2 ユーザアカウント設定の変更	47
3-4-1-3 ユーザアカウントの削除	47
3-5 “MAINTENANCE” タブ設定	48
3-5-1 “General”	48
3-5-1-1 “backup”	48
3-5-1-2 “restore”	49
3-5-1-3 “shutdown”	49
3-5-1-4 “reboot”	50
3-5-1-5 “save state”	51
3-5-1-6 “upgrade”	51
3-5-2 “System Time”	51
3-5-2-1 “timezone setting”	51

3-5-2-2 “date and time”	52
3-5-3 “License Information”	52
3-5-3-1 “license information”	52
3-5-3-2 “Offline License”	53
3-5-3-3 “Online License”	53
3-5-4 “Certificates”	54
3-5-5 “Static Routes (E250GX のみ)”	54
3-6 “NETWORKING” タブ設定 (E250GX を除く)	55
3-6-1 “VLAN Configuration”	55
3-6-1-1 VLAN の新規設定	55
3-6-1-2 VLAN の設定変更	56
3-6-1-3 VLAN の削除	57
3-6-2 “Switch Status”	57
3-6-2-1 スイッチポートのステータス確認	57
3-6-2-2 スイッチポートのステータス変更手順	58
3-6-3 “Static Routes”	59
3-6-3-1 スタティックルートの追加	59
3-6-3-2 スタティックルートの変更	60
3-6-3-3 スタティックルートの削除	60
セクション4 クラスタ・サーバ設定手順	61
4-1 クラスタとサーバの関係	61
4-1-1 クラスタの定義について	61
4-1-2 サーバの定義について	61
4-1-3 サーバに対する Equalizer の監視について	62
4-1-4 Equalizer を通過する通信について	62
4-1-5 サーバのデフォルトゲートウェイについて	62
4-1-6 spoof 設定について(SNAT 設定)	62
4-1-6-1 spoof とは	62
4-1-6-2 SNAT(Source NAT)の動作	63
4-1-6-3 なぜ SNAT を使用するのか	64
4-1-6-4 SNAT のデメリット	65
4-1-6-5 “X-Forwarded-For” ヘッダ追加について	65
4-1-7 ポート変換機能について	65
4-1-8 HTTPS クラスタの動作について	66

4-2 ネットワーク構成について	66
4-3 クラスタ作成	67
4-3-1 クラスタ作成ウィザードの起動.....	67
4-3-2 L4クラスタの作成.....	67
4-3-3 L7クラスタの作成.....	68
4-3-4 クラスタの削除.....	68
4-4 L4 クラスタパラメータ設定	69
4-4-1 “Configuration” タブ.....	69
4-4-1-1 “Required”.....	69
4-4-1-2 “Probes”.....	70
4-4-1-3 “Persistence”.....	71
4-4-1-4 “LB Policy”.....	72
4-4-2 “Servers” タブ.....	72
4-4-3 “Smart Events” タブ.....	73
4-4-4 “Reporting” タブ.....	73
4-4-3-1 “Statistics”.....	73
4-4-3-2 “Plots”.....	74
4-4-5 FTP サービスを提供する場合のクラスタ設定.....	74
4-5 L7/HTTP クラスタパラメータ設定	76
4-5-1 “Configuration” タブ.....	76
4-5-1-1 “Required”.....	76
4-5-1-2 “Probes”.....	77
4-5-1-3 “Persistence”.....	77
4-5-1-4 “LB Policy”.....	78
4-5-1-5 “Networking”.....	78
4-5-2 “Servers” タブ.....	79
4-5-3 “Match Rules” タブ.....	79
4-5-4 “Reporting” タブ.....	79
4-6 L7/HTTPS クラスタパラメータ設定	80
4-6-1 “Security> Certificates”.....	80
4-6-2 “Security > SSL”.....	81
4-7 L4/L7 クラスタ共通パラメータ詳細	83
4-7-1 “Configuration > Require > Policy”.....	83
4-7-2 “Configuration > Require > Responsiveness”.....	85
4-7-3 “Configuration > Probes > ACV probe / response”.....	85
4-7-3-1 “ACV probe”.....	86

4-7-3-2 “ACV response”	86
4-8 サーバ設定	87
4-8-1 サーバ作成	87
4-8-2 サーバ作成ウィザードの入力.....	87
4-8-3 サーバ パラメータ設定変更	87
4-8-4 Configuration タブ設定.....	88
4-8-4-1 “Required”	88
4-8-4-2 “Outbound NAT”	89
4-8-5 “max connection” 設定	91
4-8-6 “hotspare” 設定.....	91
4-8-7 “quiesce” 設定	92
4-8-8 “dont probe” 設定.....	92
4-8-9 “dont persist” 設定	92
4-9 COPY CLUSTER 設定	93
4-9-1 クラスタタイプの違いについて.....	93
4-9-2 サーバ、Smart Events, Match Rules のコピーについて.....	93
4-9-3 Copy Cluster の実施.....	93
セクション5 冗長化設定手順	95
5-1 FAILOVER 動作の基本概念について.....	95
5-2 PRIMARY / BACKUP の関係について	96
5-2-1 Primary”役”、 Backup”役” とは.....	96
5-2-2 切り戻し動作(Failback) について.....	96
5-2-3 冗長化の通信(sibling) について.....	97
5-2-4 Gratuitous ARP について	97
5-2-5 Failover ペア同士のコンフィグ同期について	97
5-2-6 Failover Alias について.....	98
5-2-7 Failover 動作・制限について	98
5-3 FAILOVER 設定.....	99
5-3-1 Failover 設定画面.....	99
5-3-2 “Required” タブ	99
5-3-3 “Synchronization” タブ	101
5-3-4 “Timing” タブ.....	101
セクション6 MATCH RULES 設定手順	103

6-1	MATCH RULES とは.....	103
6-2	MATCH RULES の動作.....	103
6-3	MATCH RULES で精査可能な HTTP ヘッダ情報.....	104
6-4	MATCH RULE 作成手順.....	105
6-4-1	Match Rule 作成ウィザードの起動.....	105
6-4-2	Match Rule 作成ウィザード入力.....	106
6-4-3	Match Rule の順番.....	106
6-4-4	expression の指定.....	107
6-4-5	サーバオプション設定.....	108
6-4-6	Responder 設定.....	109
6-5	MATCH RULES 動作確認方法.....	109
6-6	MATCH RULES 変更・削除方法.....	109
セクション7 RESPONDERS 設定手順.....		110
7-1	RESPONDERS とは.....	110
7-2	RESPONDER 作成ウィザードの起動.....	110
7-3	HTTP リダイレクション作成・設定方法.....	111
7-3-1	Responders 作成ウィザードの使用・パラメータ説明.....	111
7-3-2	Regex を使用したリダイレクション設定について.....	112
7-4	SORRY ページ設定方法.....	113
7-5	MATCH RULES への追加方法.....	114
7-6	RESPONDERS 削除方法.....	114
セクション8 SMART EVENTS 設定手順.....		115
8-1	SMART EVENTS とは.....	115
8-2	SMART EVENTS 作成ウィザードの起動.....	115
8-3	SMART EVENTS 作成・設定方法.....	116
8-3-1	Smart Events 作成ウィザードの使用・新規作成.....	116
8-3-2	Smart Events 作成ウィザードの使用・Trigger / Action 設定.....	116
8-3-3	パラメータ設定.....	117
8-4	TRIGGER のイベントリスト.....	117
8-5	ACTION のイベントリスト.....	119
8-6	SMART EVENTS 時間設定について.....	121
APPENDIX A	セッション維持動作解説.....	122

A-1 セッション維持とは	122
A-2 EQUALIZER が提供するセッション維持方法	122
A-3 STICKY TIME によるセッション維持	123
A-3-1 sticky time の設定.....	123
A-3-2 sticky time の注意点.....	123
A-3-3 inter-cluster sticky 設定について.....	124
A-3-4 sticky network aggregation 設定について.....	124
A-3-5 sticky テーブル情報の同期について.....	124
A-3-6 サーバ単位のセッション維持設定について.....	124
A-4 COOKIE によるセッション維持	125
A-4-1 cookie の設定.....	125
A-4-2 Equalizer の cookie とサーバの cookie の違い.....	125
A-4-3 Equalizer の cookie の詳細解説.....	125
A-4-4 複数クラスタ間の cookie 動作について.....	126
A-4-5 冗長化構成時の cookie 動作について.....	126
A-4-6 once only 使用時の cookie 動作について.....	126
A-4-7 サーバ単位のセッション維持設定について.....	127
 APPENDIX B CSR 作成手順	 128
B-1 EQUALIZER サーバ証明書インストール手順について.....	128
B-2 CSR 作成手順.....	128
B-3 COMPOSITE ファイル 作成手順.....	130
B-4 COMPOSITE ファイル アップロード手順.....	131
B-5 サーバ証明書に関する注意事項.....	132
 改定履歴	 133

Equalizer 設定手順書について

設定手順書を使用することで、Equalizer の設置・設定・運用を行うことができます。頻繁にお問い合わせ頂く機能・設定箇所については、より詳細に解説しています。また、Equalizer をより簡単に設定し運用を行えるように、Equalizer が提供する機能についての個別解説も盛り込まれています(その為、文書構成や記述内容はメーカーから提供されている Equalizer 英文マニュアルとは異なります)。

より詳細な説明につきましては Equalizer 英文マニュアルをご参照頂きます様お願い致します。Equalizer 英文マニュアルは Web 管理画面の上部メニューから “Help > View Guide(PDF)” を選択することでダウンロードが可能です(セクション [2-1-4](#) を参照下さい)。

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、あらかじめご了承下さい。また、改定内容については改定履歴をご確認下さい。

セクション1 Equalizer 設定の準備

1-1 機器の設置

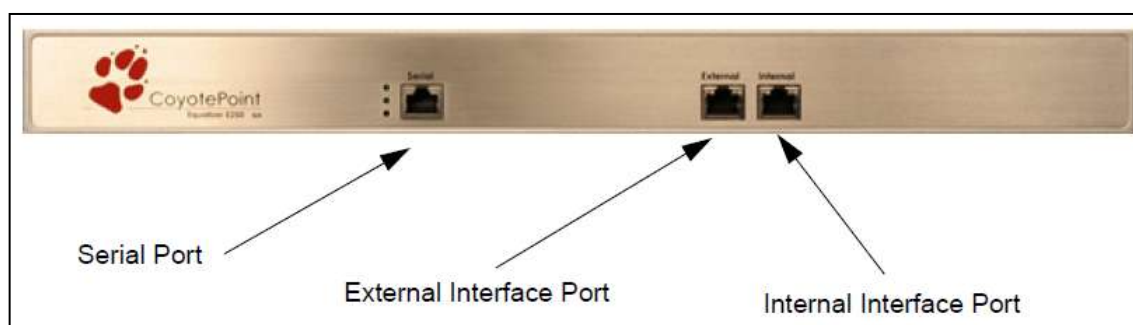
Equalizer のインストールは以下の手順で行います。

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を確認された場合、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。

1-2 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。

E250GX の場合、ポート構成は以下のようになります。



E350GX 以上のモデルではスイッチモジュールが搭載されており、VLAN 機能がサポートされています。Default VLAN を設定するとポート#1および#2 が割り当てられます。

Equalizer をネットワークに設置する場合、以下のネットワーク構成から選択可能です。

■E250GX

デュアルネットワーク構成・シングルネットワーク構成の2パターンから選択可能です。
シングルネットワーク構成の場合、使用するポートは **Internal インターフェースのみ**です。

■E350GX / E450GX / E650GX

シングルネットワーク構成(1VLAN)、デュアルネットワーク構成(2VLAN)、複数 VLAN 構成から選択可能です。

ネットワーク構成のサンプルについては [こちらのサイト](#) をご確認ください。

1-3 ターミナルエミュレーターの設定

Equalizer 機器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 機器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。

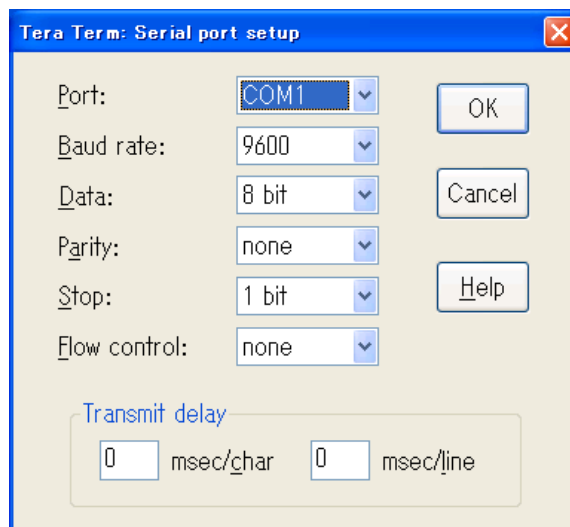
- ・ 9600 baud rate
- ・ 8 data bit
- ・ no parity
- ・ 1 stop bit
- ・ VT100 emulation

(TeraTerm 設定例)

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。



1-4 初期設定(eqadmin)

Equalizer が起動すると、デバイス情報や起動中である旨のメッセージがターミナルに表示され

ます。通常、これらの表示については確認をする必要はありません。しかし、ターミナルエミュレーションソフトウェアでハングアップを無視するように設定していない場合、起動中にターミナルのセッションが2重に存在してしまう可能性があるため、そのような場合はターミナルのセッションを起動し直して下さい。

1. Equalizer の起動処理が終了すると、ログインプロンプトが表示されます。ここで、eqadmin と入力し <Enter> を押します。Equalizer へのログインアカウントとして、root を選択することも可能です(初期パスワードは設定されておりません)。root ユーザとしてログインすると Equalizer 内部システム(FreeBSD ベース)へアクセスすることができます。

※ ファイルを直接編集すると機器不具合の原因にもなりますので、弊社サポートからご依頼させて頂く場合以外の利用はお控え頂きます様お願い致します。

2. パスワードを要求されますので、デフォルトの equalizer を入力します。



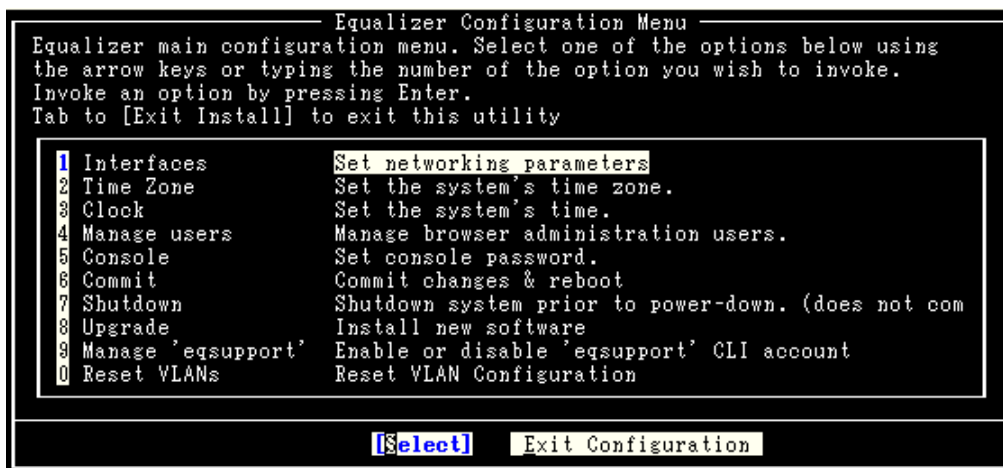
```
COM1 - Tera Term VT
File Edit Setup Control Window Help
FreeBSD/i386 (E450si_121) (ttyd0)
login: eqadmin
Password: [REDACTED]
```

3. Equalizer の基本設定用の CLI 「Equalizer Configuration Utility」が起動します。

4. Configuration Utility でメニューを選ぶ時は矢印キーで上下に設定・変更したいメニュー項目を選びます。選択されたメニューはハイライトで確認する事が出来ます。

使用しているターミナルエミュレーターで矢印キーが使用出来ない場合は <CTRL> + n で次のメニュー項目、<CTRL> + p で前のメニュー項目を選択することが出来ます。矢印キーの左右でモードを選択します。「Select」でメニュー項目を選択出来る状態になります。

「Exit Configuration」を選択すると Configuration Utility が終了し、元のログインプロンプトが表示されます。使用しているターミナルエミュレーターで矢印キーが使用出来ない場合は <Tab> で同様の動作を行う事が出来ます。



```
Equalizer Configuration Menu
Equalizer main configuration menu. Select one of the options below using
the arrow keys or typing the number of the option you wish to invoke.
Invoke an option by pressing Enter.
Tab to [Exit Install] to exit this utility

1 Interfaces          Set networking parameters
2 Time Zone           Set the system's time zone.
3 Clock               Set the system's time.
4 Manage users        Manage browser administration users.
5 Console             Set console password.
6 Commit              Commit changes & reboot
7 Shutdown            Shutdown system prior to power-down. (does not com
8 Upgrade             Install new software
9 Manage 'eqsupport' Enable or disable 'eqsupport' CLI account
10 Reset VLANs        Reset VLAN Configuration

[Select] Exit Configuration
```

項番	項目名	設定内容
1	Interfaces	ネットワークパラメータの設定を行います
2	Time Zone	タイムゾーンの設定を行います
3	Clock	日時の設定を行います
4	Manage users	Web 管理画面のユーザ登録
5	Console	コンソールパスワードを変更します
6	Commit	設定パラメータの変更を決定(再起動が行われます)
7	Shutdown	機器のシャットダウン (設定パラメータの更新は反映されません)
8	Upgrade	ファームウェアのアップグレードを行います
9	Manage 'eqsupport'	SSH によるコンソール画面へのアクセスを設定します
0	Reset VLANs	VLAN 設定を初期化します。 E250GX では使用できません。

1-4-1 Interfaces (ネットワーク設定)

このメニューから、機器のホスト名、ネットワークインターフェース、デフォルトルート、そして DNS サーバなど、ネットワークに関連する設定を行うことができます。E350GX 以上のモデルでは Default VLAN が作成されます。

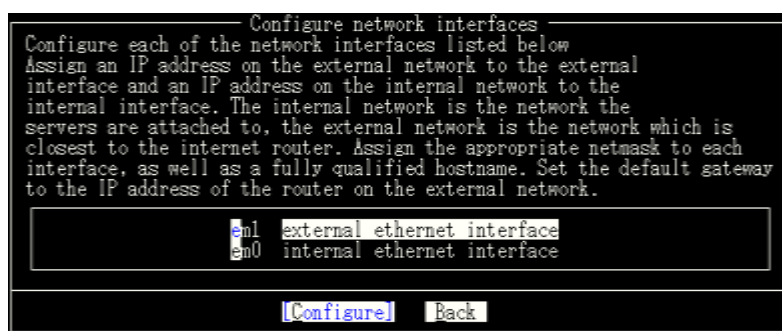
1. E250GX の場合、Configuration Menu ウィンドウの 1 番目のオプション **Interfaces** を選択し <Enter> を押すと「Configuration network interfaces」ウィンドウが表示されます。

External インターフェースを選択すると、ホスト名や DNS サーバなど機器全体の設定と External インターフェースの IP アドレス設定を行うことができます。

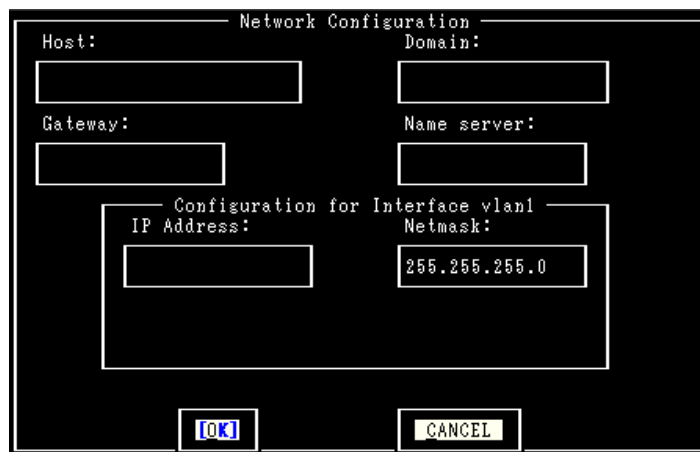
Internal インターフェースを選択すると Internal インターフェース

の IP アドレスの設定を行うことができます。まずは上下の矢印キーで **external ethernet interface** を選択します。

E350GX 以上のモデルでは、Configuration Menu ウィンドウの 1 番目のオプション **Interfaces** を選択し <Enter> を押すと、項目2の画面が表示されます。



2. 下記図の様に「Network Configuration」が表示されます。
機器のグローバル設定として、以下の項目を設定します。



備考：各設定項目の入力後は <Enter> を押し次項目へ移動します。それ以外のキーでは設定が反映されません。

3. Host はお客様ネットワーク環境での Equalizer の名前を入力します。
4. Domain は Equalizer のドメイン名を入力します。
-例えば、FQDN で、equalizer.mydomain.com だとすると、Host の項目には equalizer を入力し、Domain の項目には mydomain.com を入力します。
5. Gateway は Equalizer のデフォルトゲートウェイ IP アドレスを設定します。
6. Name server は Equalizer が使用する DNS サーバの IP アドレスを入力します。DNS サーバが存在しない場合は「0.0.0.0」を入力して下さい。
7. 上記図で「Configuration For Interface em1」と表示されている項目は、E250GX の場合は External ポートの IP アドレス情報を設定し、E350GX 以上の機種の場合はデフォルト VLAN の IP アドレス情報を設定します（「Configuration For Interface vlan1」と表示されます）。
8. 設定が終了したら、OK を選択し <Enter> を押して下さい。
9. E250GX に Internal インターフェースの IP アドレス情報を設定する場合は internal ethernet interface を選択し、<Enter> を押して下さい。



10. IP Address と Netmask を入力します。
11. 設定が終了したら、OK を選択し <Enter> を押して下さい。
12. Back を選択し <Enter> を押すと、メインの Configuration メニュー、Equalizer Configuration Menu に戻ります。
(設定を更新させるには、Equalizer Configuration Menu の 6 番目、Commit を選択します。
その後、Equalizer 機器が再起動します。)

注意: 各インターフェースにある “Extra options to ifconfig” では、ポートの Duplex や Speed を選択することが可能です。デフォルトでは全て Auto で動作していますが、E250GX で固定設定する場合はこちらに記入します。書式については TEC-World の FAQ をご参照下さい。それ以外の GX シリーズでは “Extra options to ifconfig” を使用せず、セクション [3-6-2](#) に従って設定変更を行ってください。

1-4-2 Time Zone (タイムゾーン設定)

現在のタイムゾーンを変更します。この設定は Web 管理画面からも行なうことが可能です。本設定の反映に再起動は必要ありません。

1. Equalizer Configuration Menu ウィンドウで 2 番目の項目、Time Zone を選択して <Enter> を押します。
2. メニューバーから設定したいタイムゾーンを選択します。日本時間の場合は「5 Asia」を選択し「19 Japan」を選択します。
3. 設定が終了したら、OK を選択し <Enter> を押して下さい。

1-4-3 Clock (時刻設定)

現在の日付、時間を設定します。本設定の反映に再起動は必要ありません。

1. Equalizer Configuration Menu ウィンドウで 3 番目の項目、Time を選択して <Enter> を押します。
2. 24 時間での時間を MM/DD/YY HH:MM 表記(月/日/年 時:分)で設定します。設定が終了したら、OK を選択し <Enter> を押して下さい。


```
Equalizer Configuration Menu
Equalizer main configuration menu. Select one of the options below using
the arrow keys or typing the number of the option you wish to invoke.
Invoke an option by pressing Enter.
Tab to [Exit Install] to exit this utility

----- Set current time -----
Please enter the current date and local time using 24-hour style,
in the form MM/DD/YY HH:MM
06/25/07 14:39
[ OK ]      [ Cancel ]

9 Manage 'eqsupport' Enable or disable 'eqsupport' CLI account

[Select]   [Exit Configuration]
```

1-4-4 Manage users (Web 管理画面アカウント作成)

eqadmin で基本設定を行った後は、Web ブラウザから機器へアクセスし設定を行います。この際に使用されるインターフェースは Web 管理画面と呼ばれます。デフォルトで設定されているログインアカウント名は以下の通りです。

touch (設定可能ユーザ。デフォルトパスワード: touch)

look (Read Only ユーザ。デフォルトパスワード: look)

上記以外のユーザ作成を行なう際はこのメニューを使用します。

備考: 同様の作業は Web 管理画面からも行なうことが出来ますが、Web 管理画面へのログインパスワードを紛失した場合などは、ここからユーザを新規作成することで Web 管理画面へのアクセスが必要になります。

touch パスワードはブラウザで Equalizer にアクセスした際に、編集モード(touch)でログインする際のパスワードになります。パスワードに使用出来る文字はスペース以外のプリントが可能な文字列の組み合わせになります。また、文字列の長さは 20 文字までで、大文字小文字は区別されます。パスワード変更を行うには次の手順で行います。

1. Equalizer Configuration Menu ウィンドウで 4 Manage users を選択して <Enter> を押します。
2. 編集可能ユーザ(Full Access) または Read Only ユーザを作成するかを選択します。



3. 以下の項目が表示されますので、入力します。

- Enter username: アカウント名を設定します。
- Enter full name: your user アカウント名の説明を設定します
- Enter password: パスワードを設定します、確認を含め2回入力します

1-4-5 Console (eqadmin アカウントのパスワード変更)

現在設定作業をしている Configuration Utility にアクセスする為にアカウント eqadmin に対するパスワードの変更になります(初期パスワードは equalizer 設定されています)。パスワードに使用出来る文字はスペース以外のプリントが可能な文字列の組み合わせになります。パスワード変更を行うには次の手順で行います。

1. Equalizer Configuration Menu ウィンドウで 5 番目の項目、**Console** を選択して <Enter> を押します。
2. 以下の項目が表示されますので、入力します。パスワードの変更はこの作業後、直ぐに適用されます。
 - Changing local password for eqadmin.
New password:
 - Retype new password:

1-4-6 Commit (設定の適用・再起動)

セクション [1-4-1](#) で行った設定変更を機器に反映させるには、Equalizer を再起動させる必要があります。

1. Equalizer Configuration Menu ウィンドウで 6 番目の項目、**Commit** を選択して <Enter> を押します。
2. 再起動の処理が終了したら設定の更新がされているか、再度確認します。

1-4-7 Shutdown (機器のシャットダウン)

Configuration Utility を使用して Equalizer をシャットダウンさせる事が出来ます。シャットダウンの動作自体は Equalizer の設定更新を行いません。シャットダウンを行うには次の手順で行います。

備考: 機器の電源を落とす場合は、かならずシャットダウンを行なってください(機器が故障する場合があります)。シャットダウンは Web 管理画面から行なうことも可能です。

1. Equalizer Configuration Menu ウィンドウで 7 番目の項目、Shutdown を選択して <Enter> を押します。
2. シャットダウンの処理が終了したら、機器の電源を切って下さい。

1-4-8 Upgrade (ファームウェアアップグレード)

Equalizer のソフトアップグレードを行うには Equalizer Configuration Utility を使用して行います、詳細な手順についてはファームウェア提供時にご案内致します。ファームウェアの提供は弊社より行われます、最新ファームウェアの情報およびファームウェアの申請方法は弊社 TEC-World の FAQ をご確認ください。また最新ファームウェアリリースの提供時に保守契約ユーザー様へメールにて連絡も行っております。

1-4-9 Manage 'eqsupport' (リモートアカウント接続設定)

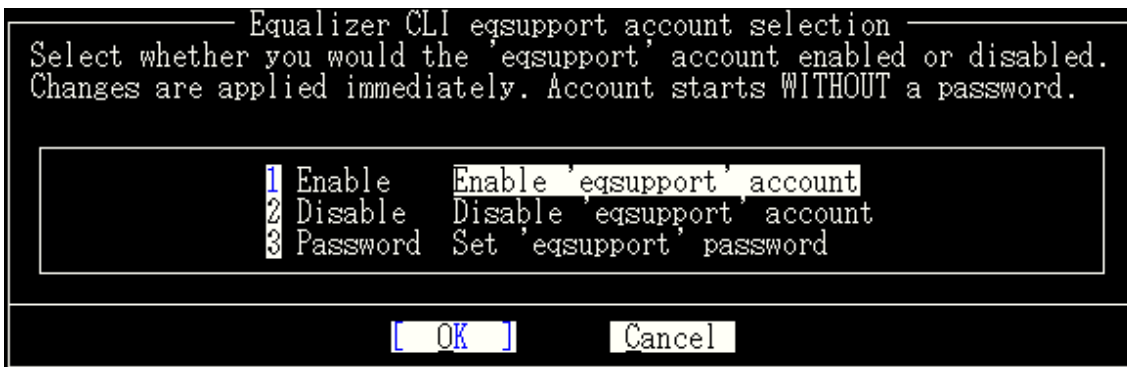
eqsupport アカウントを有効にした場合、SSH を使用して Equalizer へリモートアクセスが可能です(eqsupport アカウントは初期設定では無効になっています)。アカウントは eqsupport のみで追加は出来ません。

注意: eqsupport アカウントの無効化やアップグレード処理を遠隔から行うと、SSH にてアクセス出来なくなる場合が御座いますので、編集を伴う処理を行う場合にはシリアル接続にて処理を行って下さい。

リモートアクセスアカウント設定手順は以下の通りになります。

1. 9 番目の「Manage 'eqsupport'」を選んで、<Enter> を押します。
2. オプション1の Enable をハイライトして <Enter> を押します。これで、リモートアカウントが

有効になります。



3. Equalizer CLI eqsupport account selection が下記画面のように表示されるので、オプション3の Password を選択します。

New Password:

Retype New Password:

と表示されますので、従ってパスワードを2回入力します。パスワードが合致し、設定が完了するとメニュー画面に戻ります。

4. リモートアクセスアカウントを無効化する場合は、メニュー画面からオプション2 Disable を選択します。
5. パスワードを変更したい場合は手順1と同様、メインメニューから Manage 'eqsupport' を選択し、パスワードを再度入力します。

※既存のパスワード再入力は求められません。

1-4-10 Reset VLANs

VLAN 機能がサポートされているモデルにおいて、設定をリセットする際に使用します。実行時には root ユーザでコンソールにログインし、コマンド eqadmin を使用してから選択します。このコマンドを使用することで以下の変更が行われます。

1. Default VLAN を除く全 VLAN を削除します。
2. ポート#1および#2 が Default VLAN に割り当てられます。
3. 機器が再起動します。
4. Failover が設定されている場合、無効になります。

またポート間が接続されている場合ループが発生する可能性があるため、作業時には注意が必要です。

1-5 アカウント・パスワード一覧

Equalizer のアカウントおよびパスワードの初期設定一覧は以下の通りです。

アカウント名	CLI(コンソール)	Web 管理画面	初期設定	変更方法
root	○	—	(設定なし)	1-5-1 を参照
eqadmin	○	—	equalizer	1-4-5 を参照
eqsupport	○(SSH)	—	(設定なし)	1-4-9 を参照
touch	—	○	touch	3-4-1-2 を参照
look	—	○	look	3-4-1-2 を参照
カスタム	—	○	(設定なし)	3-4-1-2 を参照

1-5-1 root パスワードの変更方法

1. root アカウントでコンソール画面へログインします。
2. 以下のコマンドを実行します

```
passwd root
```
3. パスワードの入力、および再入力を求められますので、入力し決定します。
4. 設定を反映するには機器の再起動が必要ですので、[1-2-6](#) の Commit changes & reboot を実行し機器の再起動を実施して下さい。

備考: root パスワードを紛失した場合、パスワードのリセットが必要になります。方法は TEC-World の FAQ をご確認ください。この作業には機器の再起動が必要になります。

セクション2 Web 管理画面の操作

2-1 Equalizer Web 管理画面について

セクション1にて初期設定の完了後は、Equalizer のサービスの設定・管理等は Web 管理画面より行ないます。JavaScript が有効なウェブブラウザを使用しログインします。

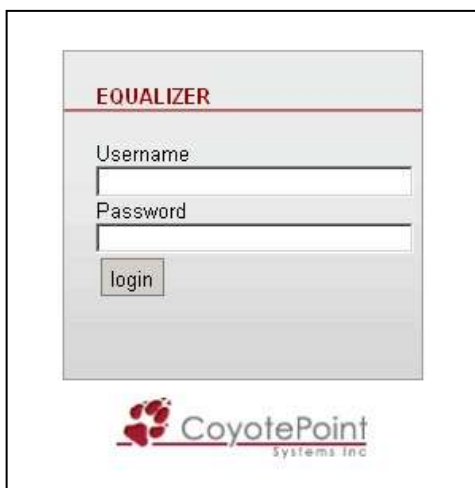
2-1-1 Equalizer Web 管理画面にアクセスする

管理画面で Equalizer にアクセスする為に、ブラウザは JavaScript が有効になっている事を確認下さい。

1. ブラウザ画面に Equalizer の IP アドレスを入力します。 External 側・Internal 側どちらのポートであっても IP アドレスが設定されていればログインが可能です(アクセス制限を行う場合は [3-4-2](#) を参照下さい)。

冗長化構成の場合、2台が共有する Failover Alias の IP アドレスを使用してログインすることも可能です。 この場合、Primary として動作している機器に接続されます。

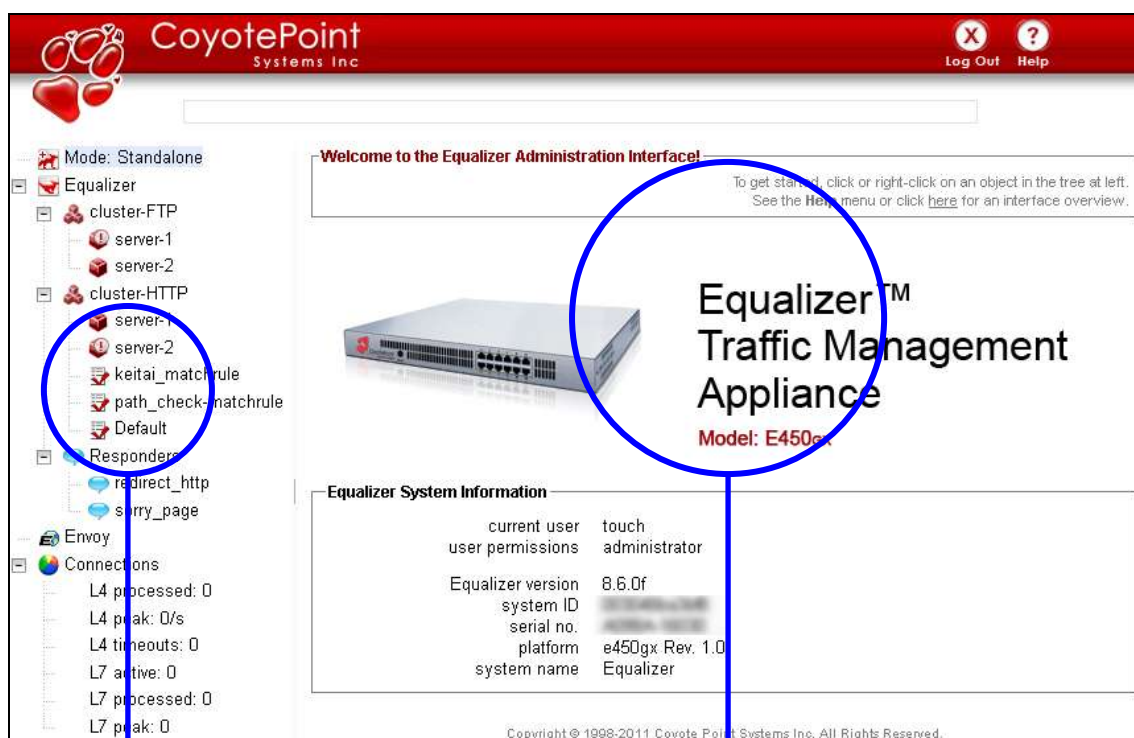
2. ログイン画面が表示されます。 [1-2-4](#) で作成したアカウント、あるいはデフォルトで設定されている touch または look アカウントにてログインを行ないます。



備考: パスワードを忘れてしまった場合は、Equalizer にシリアル接続してアカウントを作成する事が可能です。詳しくは [1-2-4](#) を参照下さい。

2-1-2 Web 管理画面の概要

Web 管理画面へログインすると、以下の画面が表示されます(使用モデルの筐体画像が表示されます)



左フレーム

右フレーム

Web 管理画面は2つのフレームで構成されています。

左フレームは、メインメニュー、設定したクラスター・サーバ・ Match Rules ・ Responder ・ Smart Events などが表示されます(表示される項目は機種・設定によって異なります)。

右フレームは、左フレームで選択した項目の詳細情報が表示されます。右フレーム内に表示されるタブを選択することで、より詳細な項目を設定することが出来ます。

2-1-3 機器の詳細情報を表示

ログイン後、右フレーム下のボックス上にマウスを乗せることで機器の詳細情報を表示することができます。

- current user

- 現在ログインしているユーザ名を表示します。
- user permissions
現在ログインしているユーザの権限を表示します。
- Equalizer version
機器のファームウェアバージョンを確認することができます。
- systemID
機器の SystemID を表示します。この情報はファームウェアアップグレード時などメーカーに機器の登録を行なう際に必要になります。
- serial no.
機器のシリアル番号が表示されます。
- platform
機器のハードウェアプラットフォーム情報が表示されます。
- system Name
1台構成で動作している場合はホスト名(1-4-1 参照)が、冗長化構成の場合は Failover 設定の Equalizer Name(5-3-3-2 参照)が表示されます。

- Default Interface (E250GX: external interface)
Default VLAN に設定されている VLAN ID が表示されます。
E250GX の場合は External Interface と表示されます。
- [VLAN 名] interface (E250GX: internal interface)
複数の VLAN が設定されている場合は、VLAN 名が表示されます。
E250GX の場合は Internal 側のインターフェース名が表示されます。
- Default address (E250GX: external address)
Default VLAN に設定されている IP アドレスが表示されます。
E250GX の場合は External 側 IP アドレスが表示されます。
- [VLAN 名] address (E250GX: internal address)
複数の VLAN が設定されている場合は、その VLAN の IP アドレスが表示されます。
E250GX の場合は Internal 側 IP アドレスが表示されます。

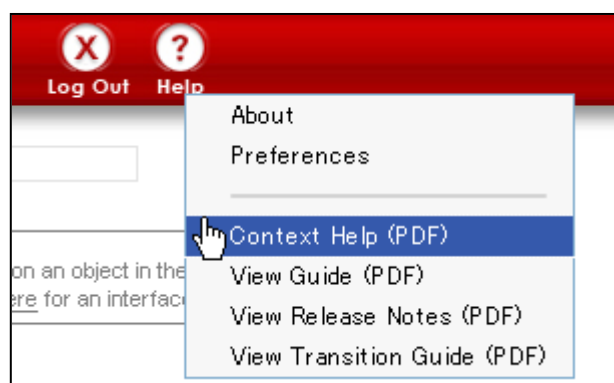
- failover mode
機器のフェイルオーバー状態が表示されます。
 - standalone → 機器は単体で動作しています (Failover 設定がない状態)
 - primary → 機器は Primary 役で動作しています。
 - backup → 機器は Backup 役で動作しています。
 - initializing → Failover Mode を認識中に表示されます (機器起動直後など)。また、ネットワークに問題があり、機器がポージング状態になっている場合でも表示されま

- す。その場合は上位ネットワーク、負荷分散対象サーバの接続を確認して下さい。
- sequence number
機器の sequence 値が表示されます。詳細は[セクション 5-2-5](#)をご参照下さい
 - Envoy geographic load balancing
Envoy 機能の有効・無効を表示します(E650GX)
 - SSL acceleration
Xcel カードの有効・無効を表示します。
 - disabled → Xcel カードが搭載されていません。
 - Xcel I → Xcel I カードが搭載されています。
 - Xcel II → Xcel II カードが搭載されています (E450GX / E650GX)。
 - Hardware GZIP compression
Express カードによる HTTP 圧縮の有効・無効を表示します (E650GX)。
 - Virtualization Load Balancing
 - VLB Basic → VLB Basic 機能が使用可能です。
 - VLB Advanced → VLB Advanced 機能が使用可能です。
 - Default VLAN ports (E250GX を除く GX シリーズのみ)
Default VLAN に所属しているポート番号を表示します。
 - [VLAN 名] VLAN ports (E250GX を除く GX シリーズのみ)
複数 VLAN が設定されている場合は、各 VLAN に所属しているポート番号を表示します。

2-1-4 Help メニューの利用

Web 管理画面右上にある Help メニューから Equalizer に関する情報を確認することが出来ます。確認できるドキュメントは Equalizer 内部からダウンロードしていますので、インターネットへの接続は必要ありません。

- About
ログイン後のトップページへ移動します。
- Preferences
Web 管理画面の自動更新時間を変更します、デフォルトは60秒です。ブラウザの Cookie 情報に保存されますので、使用ブラウザを変更した場合などは設定をやり直してください。
- Context Help(PDF)
Equalizer のマニュアル(英語)をダウンロードし、右フレームに表示されている設定画面に



ついでに説明箇所を表示します。

- View Guide(PDF)
Equalizer のマニュアル(英語)をダウンロードできます。
- View Release Notes(PDF)
インストールされているファームウェアのリリースノートを確認することができます。
- View Transition Guide (PDF)
ファームウェアバージョン7と8の差異について確認することができます。

2-1-5 設定追加・変更の決定ボタンについて

Web 管理画面で設定の追加または変更を行った場合は、必ず決定ボタンを押して反映させる必要があります。この動作を行わない場合、変更内容が失われますのでご注意ください。

決定ボタンは  です。

2-1-6 Web 管理画面のメッセージ表示について

Web 管理画面では、設定画面のステータスメッセージが画面右上に表示されます。現在選択している画面の情報や、設定変更が正常に行われたかなどはメッセージをご確認ください。

右図の例では、クラスタ “Cluster_Web” をクリックした際に表示されるメッセージです、[4-4-1-1](#) で説明されている “required” の設定画面が選択されていることを示しています。



2-1-7 Web 管理画面からのログアウト

Web 管理画面からログアウトするには、画面右上から Log Out を選択します。



2-1-8 Equalizer のライセンス表示について

Equalizer のライセンスは出荷時に有効になっていますが、なんらかの理由でライセンスが無効になった場合には、Web 管理画面のトップページから確認ができます。

下記図のように筐体画像が変化した場合はヘルプデスクへご連絡下さい。



セクション3 機器のグローバル設定

Equalizer のグローバル設定について項目別に設定を行います。全ての設定は Web 管理画面から行います。左フレームから Equalizer を選択すると、右フレームにタブが表示されます。タブを選択することで各設定画面を表示します。

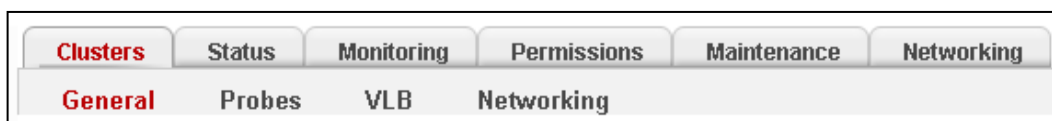
Failover 設定(5-3)を行った場合、
機器に設定した Equalizer Name が表示されます。

表示される右フレームは以下ようになります。

各タブ(Clusters, Status, Monitoring, Permissions, Maintenance, Networking)をクリックするとそれぞれのセクションが表示されます。E250GX では Networking タブは表示されません。




3-1 “Clusters” タブ設定





3-1-1 “General”

+ add						
Name	Type	IP Address	Port	Servers	Actions	
c100-FTP	L4 TCP	10.15.100.145	21	1 1 0		
c100-HTTP	HTTP	10.15.100.145	80	1 1 0		

設定されているクラスタ(4-3 を参照)を一覧表示します、また所属しているサーバの状態も簡易表示することが可能です。

- add
ボタン  を選択することでクラスタ作成ウィザードを起動します。
- Name
クラスタの名称を表示します。
- Type
クラスタタイプ(L4 TCP, L4 UDP, HTTP, HTTPS) を表示します。
- IP Address
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。
- Servers
所属しているサーバの状態が表示されます。
左から Up, Down, dont probe のサーバ数がそれぞれ表示されます。
- Actions
クラスタの削除、変更、新規作成を行うことができます。

項目	内容
	該当クラスタを削除します。
	該当クラスタ設定を変更します。

3-1-2 “Probes”

ヘルスチェック設定を変更します、別途クラスタ個別で設定可能な項目もあります。

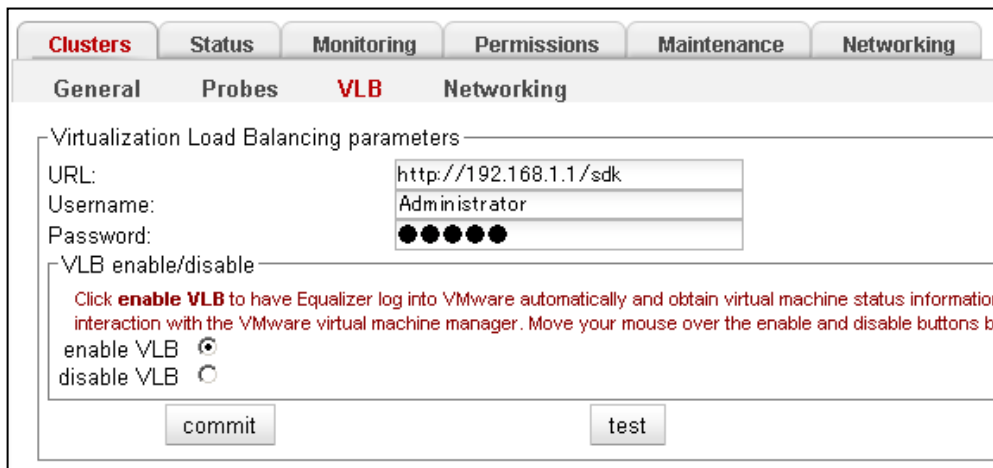
probe parameters

probe interval	<input type="text" value="20.0"/>
probe timeout	<input type="text" value="10.0"/>
strikeout threshold	<input type="text" value="3"/>
event interval	<input type="text" value="15.0"/>
probe delay	<input type="text" value="10.0"/>
agent delay	<input type="text" value="10.0"/>
require agent response	<input type="checkbox"/>
ICMP probe	<input checked="" type="checkbox"/>

項目	設定内容
probe interval	TCP ハンドシェイク(および ACV)が1度失敗した後、2回目以降のヘルスチェックは Probe Interval で設定した間隔(秒)で行われます。 デフォルト 20 秒
probe timeout	TCP ハンドシェイク(および ACV)のタイムアウト時間(秒)を設定します。 デフォルト 10 秒
strikeout threshold	Equalizer がサーバを Down と認識するまでの失敗許容回数です。 単位は回。 デフォルトは 3、設定可能範囲は 1~6 です。
event interval	Smart Events の実行間隔を秒で設定します。 デフォルト15秒。
probe delay	サーバヘルスチェックの間隔(秒)を設定します。 TCP ハンドシェイク(および ACV)はこの間隔行なわれます。 デフォルトは 10 秒です。 設定可能範囲は 0 秒から 60 秒までですが、5 秒以下を設定した場合には自動的に 5 秒間隔になります。
agent delay	VLB や Server Agent を使用したロードバランス時に設定が必要になります。 Equalizer がサーバ上の Agent を確認する間隔(秒)を設定します。 デフォルトは 10 秒、設定可能範囲は 1 ~60 秒です。
require agent response	Server Agent を使用した際にのみ設定します。 設定した場合に Server Agent からの応答がないと、サーバをダウンと判定します。
ICMP probe	ICMP によるヘルスチェックを行いません。 間隔の指定はできません、5 秒間隔で行なわれます。

3-1-3 “VLB”

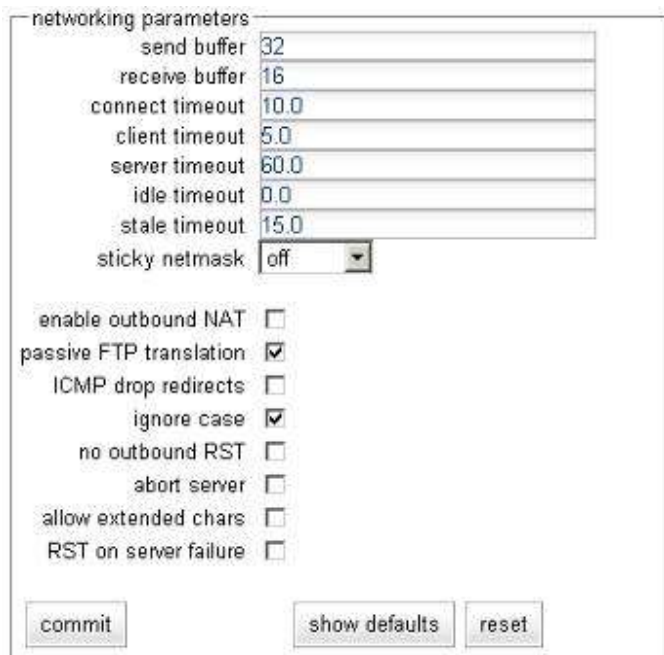
VLB を使用し負荷分散を行なう際に設定を行います。



項目	設定内容
URL	VMware API コネクション用の Virtual Center (または ESX サーバ上) の URL を設定します。デフォルトでは https:// を使用し、/sdk を指定します。サンプルは上図をご参照下さい。
Username	VMware Virtual Center または ESX サーバへログインする際のユーザアカウントを指定します。
Password	VC User のパスワードを入力します。

3-1-4 “Networking”

ネットワークについての設定を行います。



項目	設定内容
send buffer	L7 での送信ソケットバッファサイズです。単位はキロバイト。デフォルトは 32KB です。最大値は 128 です。詳細は 3-1-4-1 を参照して下さい。
receive buffer	L7 での受信ソケットバッファサイズです。単位はキロバイト。デフォルトは 16KB です。最大値は 128 です。詳細は 3-1-4-1 を参照して下さい。
connect timeout	ACV によるヘルスチェックの接続要求に対するサーバ応答タイムアウト値(秒)です。デフォルトは 10 秒です、1~60 秒の範囲で設定が可能です。
client timeout	L7 クラスタのみ反映されます。クライアントのアイドル接続の終了までの時間です。単位は秒で、デフォルトは 5 秒です。設定値は 1.0 秒から設定可能です。
server timeout	L7 クラスタのみ反映されます。サーバのアイドル接続の終了までの時間です。単位は秒。デフォルトは 60 秒です。設定値は 1.0 秒から設定可能です。
idle timeout	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	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。
sticky netmask	Sticky Persistence を使用時のアクセス IP 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。詳細は APPENDIX A を参照して下さい。
enable outbound NAT	Outbound NAT の有効・無効を設定可能です、これはデュアルネットワーク設定でのみ使用可能です。 有効にすると、Equalizer をゲートウェイとして通信する際、端末の送信元 IP アドレスを Equalizer の Default VLAN IP アドレスに NAT します(E250GX の場合は Internal 側から External 側への通信時に、External インターフェース IP アドレスへ NAT)。 無効の状態では送信元 IP アドレスは端末の IP アドレスのまま通信を行いません。詳細は 3-1-4-2 を参照して下さい。
passive FTP translation	passive FTP translation を有効にする場合チェックを入れて下さい。詳細は 4-4-4 を参照して下さい。
ICMP drop redirects	Equalizer を経由する ICMP redirect メッセージを破棄します。
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。各クラスタ・各 Match Rule に対して設定する事も出

	来ます。
no outbound RST	チェックを入れ有効にすると、変換されない TCP RESET パケットを転送させないようにします。
abort server	クローズする際にサーバに対し不意に接続を落とします。
allow extended chars	URI やヘッダ内の ASCII や UTF-8 の透過設定です。デフォルトではチェックが外れて無効の状態です。
RST on server failure	L4 クラスタに適用されます。TCP セッションが確立した後に負荷分散先サーバがダウンした場合、クライアントに対して RST(リセット)パケットを送付します。

3-1-4-1 Send buffer/ Receive buffer について

L7クラスタではディレイドバインディングによるセッション管理が行なわれるため、バッファサイズを使用しデータを一時的に保持します。大きなファイルサイズ(1MB以上など)をやり取りする場合は、バッファサイズがボトルネックになることがありますので、サイズを Send:Receive = 64:32 などのサイズに変更して下さい。

バッファサイズを大きくした場合、セッション毎にメモリが消費されます。セッション数が多い環境においてはメモリ容量が不足する場合があります、ご注意下さい。

3-1-4-2 Outbound NAT 通信について

2つ以上の VLAN を設定している場合、各 VLAN に所属しているノードから通信を行なう際に Equalizer は送信元 IP アドレスの変換は行われず、各ノードは自身の IP アドレスで通信を行います。例えば VLAN の1つがグローバル IP セグメントで、Equalizer がゲートウェイとして動作している場合などは、Equalizer が送信元 IP アドレスを NAT しないと通信が成立しない場合があります。このように Equalizer を経由して行う通信においてルーティングを考慮する必要がある場合は、Outbound NAT 機能を使用可能です。使用した場合、送信元 IP アドレスは Default VLAN の IP ドレスに NAT されて通信が行われます。E250GX の場合、Internal セグメントのノードから External 側(およびその上位)セグメントへ通信を行う場合にのみ NAT されます。

本機能は1VLAN 構成(E250GX では Single Network 構成)では使用できません。

デフォルトで Outbound NAT を有効にした状態では、Equalizer のリアル IP アドレスに NAT 変換されるため、Equalizer を2台使用する冗長化構成の場合、どちらの機器が Primary 役として動作しているかによって、NAT される IP アドレスが変化してしまいます(冗長化については [5-1](#) を参照)。この場合、各サーバで Outbound NAT 設定を行うことで、NAT する IP アドレスを機器のリアル IP アドレスではなく クラスタ IP アドレス や VLAN の Failover Alias IP アドレスにすることが可能です(E250GX の場合は External 側 Failover Alias IP アドレス)。クラスタ IP アドレスは

両機器で共有している IP アドレスであり、どちらの機器が Primary 役であっても外部に通信する際の IP アドレスは共通になります。

通信するアプリケーションやサーバによっては必ず同一 IP アドレスで通信を行なう必要がある場合がありますので、そういった状況では各サーバで Outbound NAT を設定下さい、詳細は [4-8-4-2](#) をご確認下さい。

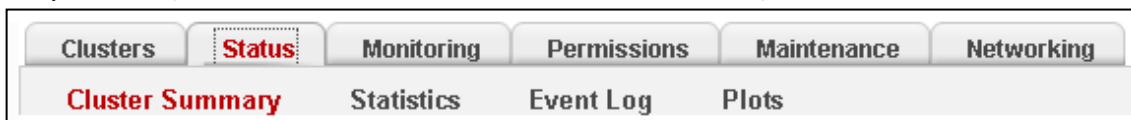
3-1-4-3 “allow extended chars” 設定について

URI や HTTP ヘッダ上に 2 バイト文字が含まれるコンテンツでは、Equalizer 内で正常に処理ができず正常に表示されない場合があります、Equalizer ログに “parameter error” として表示されます。

上記の事象が発生した場合は、“allow extended chars” を有効にし、2 バイト文字を透過的に処理する設定を施すことでこの問題を回避することが可能です。

3-2 “Status” タブ設定

Equalizer の機器情報、クラスタ・サーバ情報、ログ情報などを確認します。









3-2-1 “Cluster Summery”

それぞれのクラスタ・および所属サーバの状況を確認できます。クラスタ名をクリックすると所属するサーバの状況が表示されます。

下図は L4クラスタ “Cluster_Web_2” をクリックした表示です。

Cluster_Web_2							
Servers	Status	Flags	Initial Weight	Current Weight	Processed	Active	Sticky
server_1			Not used	Round Robin	0	0	0
server_2			Not used	Round Robin	0	0	0

項目	内容
Servers	サーバ名を表示します。
Status	サーバ状態がアイコン表示されます。それぞれの意味については下記 Status アイコン表をご確認下さい。
Flags	サーバに設定されたフラグの状態が表示されます。
Initial Weight	サーバに設定された initial weight 値を表示します。Round Robin を負荷分散ポリシーとして選択した場合は Not used と表示されます。Round Robin および Static Weight 以外の、動的負荷分散ポリシーを選択した場合、現在の動的 Weight 値は Current Weight として表示されます。
Current Weight	サーバの動的 weight 値を表示します。Round Robin を負荷分散ポリシーとして選択した場合は Not used と表示されます。動的負荷分散ポリシーを選択している場合、この weight 値によってサーバへの振り分けが行われます。
Processed	完了したセッション数が表示されます。
Active	現在アクティブなセッション数が表示されます。
Sticky	Sticky によるセッション維持が行なわれているユーザ数を表示します。

Status アイコン	内容
	ヘルスチェックに成功し、サーバはアップしています。
	ヘルスチェックに失敗し、サーバはダウンしています。
	ヘルスチェックに成功していますが、サーバの Weight 値が0 に設定されているか、 quiesce 設定 が有効になっています。
	ヘルスチェックに失敗しており、また、サーバの Weight 値が0 に設定されているか、 quiesce 設定 が有効になっています。
	hot spare 設定 が有効になっています。
	該当サーバに対するヘルスチェックが無効に設定され、サーバのステータスを確認することが出来ない状態です。また、クラスタが無効になっている場合にも表示されます。

また、L7クラスタの表示項目は以下のようになります。

c100_143						
Servers	Status	Flags	Initial Weight	Current Weight	Processed	Active
server-1			Not used	Round Robin	13	0
server-2			Not used	Round Robin	0	0
Match rules			Processed	Responder Hits	No Servers	
matchrule-01			13	0	0	
matchrule-02			0	0	0	
Default			0	0	0	

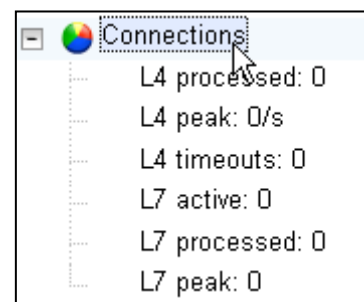
基本的な項目は L4クラスタと同様ですが、Match Rules に関する以下の項目を確認することが可能です。

項目	内容
Match rules	クラスタに設定されている Match Rules の名前を表示します。
Processed	その Match Rules に適合し、処理されたセッション数を表示します。
Responder Hits	その Match Rules に設定された Responders によって処理されたセッション数を表示します。
No Servers	その Match Rules に設定された負荷分散対象サーバが全てダウンしていた際のセッション数を表示します。

3-2-2 “Statistics”

サービス全体の統計情報を確認することが出来ます。

この画面へは左フレームの“Connections”を選択しても移動することが可能です(右図参照)



確認できる情報は Basic Statistics と Advanced Statistics に分けられています。

Basic Statistics	
L4 total connections processed	0
L4 peak connections processed	53 per second
L4 stale connections timed-out	0
L4 idle connections timed-out	0
L7 current active connections	0
L7 total connections processed	13817
L7 peak connections processed	40

項目	内容
L4 total connections processed	L4クラスタで処理された接続数の総数です。
L4 peak connections processed	L4クラスタで1秒間に処理された最大の接続数です。
L4 connections timed-out	L4クラスタでタイムアウトした接続数の数です。
Envoy status	E650GX のみ表示されます。
L7 current active connections	L7クラスタに於いて、現在アクティブな接続数です。
L7 total connections processed	L7クラスタで処理された接続数の総数です。
L7 peak connections processed	L7クラスタで1秒間に処理された最大の接続数です。

Advanced Statistics	
L7 client connections acceptable	0
L7 connections timed out	0
L7 request bytes from clients	0
L7 response bytes to clients	0
L7 complete requests	0
L7 min. usec to complete request	0
L7 max. usec to complete request	0
L7 avg. usec to complete request	0
L7 maximum headers exceeded by client	0
L7 total client connections	0
L7 current client connections	0
L7 requests processed	0
L7 responses processed	0
L7 server conx reused	0
L7 cookies stuffed	0
requests in error	0
L7 responses in error	0
L7 client request timeouts	0
L7 server connect timeouts	0
server response timeouts	0
L7 avg. usec to connect to server	0

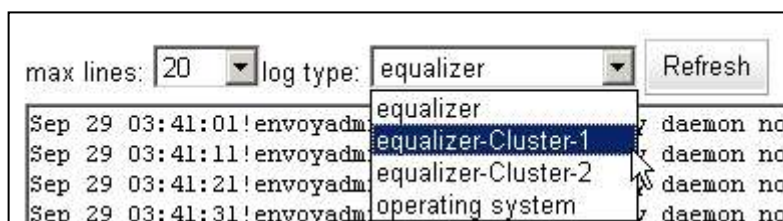
項目	内容
L7 client connections acceptable	開始された L7 コネクション数です。
L7 connections timed out	Client timeout 値、Connect timeout 値、Server timeout 値等を過ぎたことでタイムアウトした L7 コネクション数です。
L7 request bytes from client	クライアントから受け取ったデータをバイト数で表示します。
L7 response bytes to client	サーバから受け取ったデータをバイト数で表示します。
L7 complete requests	L7 クラスタで完了したクライアントリクエスト数を表示します (Client timeout 値に達する前に処理したリクエスト)
L7 min. usec to complete request	クライアントリクエストの受付完了までにかかった最小時間をマイクロ秒で表示します。
L7 max. usec to complete request	クライアントリクエストの受付完了までにかかった最大時間をマイクロ秒で表示します。
L7 avg. usec to complete request	クライアントリクエストの受付完了までにかかった平均時間をマイクロ秒で表示します。
L7 maximum headers exceeded by client	Equalizer がサポートする最大 64 ヘッダを超えた L7 クライアントリクエスト数を表示します (Equalizer は 64 ヘッダを超えたクライアントリクエストはドロップします)
L7 total client connections	受け付けた L7 クライアントコネクション数を表示します (必ずしも完了した (Processed) コネクションではありません)
L7 current client connections	現在のアクティブな L7 コネクション総数を表示します。
L7 request processed	完了した L7 クライアントリクエスト総数を表示します。
L7 response processed	完了した L7 サーバレスポンス総数を表示します。
L7 server conx refused	クローズせず、再度 Equalizer で利用されたサーバコネクション数を表示します。
L7 cookies stuffed	Equalizer が L7 パケットにセッション維持用 Cookie を付与した回数を表示します。
requests in error	エラーが発生した L7 リクエストの総数を表示します。
L7 responses in error	エラーが発生した L7 レスポンスの総数を表示します。
L7 client requests timeouts	Client timeout 値に達したためドロップされた L7 リクエスト総数を表示します。
L7 server connect timeouts	Connect timeout 値に達したためドロップされた L7 リクエスト総数を表示します。
server response timeouts	Server timeout 値に達したためドロップされた L7 リクエスト総数を表示します。

L7 avg. used to connect to server	Equalizer がサーバへのコネクション確立に要する平均時間 (秒)
-----------------------------------	--------------------------------------

3-2-3 “Event Log”

Equalizer のログ情報を確認することができます、ログは3種類に分かれています。

- equalizer
負荷分散、ヘルスチェック、Failover 等、サービスに関するログが表示されます。
- operating system
Equalizer の内部 OS ログ、NTP、ポート状態などのログが表示されます。
- クラスタ別ログ
Equalizer Log から、指定したクラスタのログを抜粋して表示します。

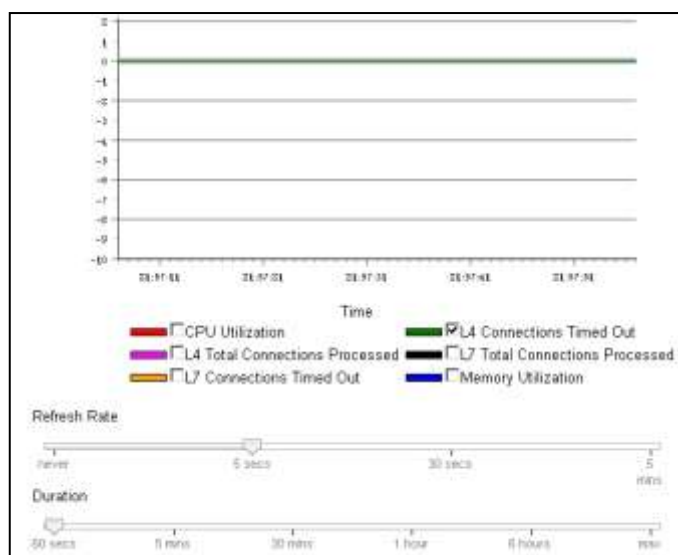


項目	内容
max lines	ボックス内に表示するログの行数を指定します。 デフォルト20行、最大1000行まで指定が可能。
log type	equalizer, operating system, クラスタ別ログから種類を指定します。
Refresh	ログを最新の状態に更新します。

ボックス内に表示されたログは、テキストとしてコピーすることが可能です。 サポートなどでログ採取を行なう場合には、こちらから行って下さい。

3-2-4 “Plot”

Equalizer の状態をグラフ表示します。



項目	内容
CPU Utilization	CPU 使用率を表示します。
L4 Connections Timed Out	タイムアウトした L4コネクション数を表示します。
L4 Total Connections Processed	処理された L4コネクション数を表示します(全 L4 クラスタ合計)
L7 Total Connections Processed	処理された L7コネクション数を表示します(全 L7クラスタ合計)
L7 Connections Timed Out	タイムアウトした L7コネクション数を表示します。
Memory Utilization	メモリ使用率を表示します。
Refresh Rate	更新する間隔を設定します。
Duration	表示する時間の範囲を選択します。

3-2-5 “Switch Status”

E250GX で表示されますが、使用することはできません。E350GX 以上のモデルをご利用の場合はセクション [3-6-2](#) をご参照下さい。

3-3 “Monitoring” タブ設定

Equalizer による監視・トラップ設定を行います。

Clusters	Status	Monitoring	Permissions	Maintenance	Networking
Events	Export to CSV	SNMP			

3-3-1 “Events”

3-3-1-1 “logging”

logging

Enter the hostname or IP address of a system running a syslogd daemon on the standard syslog UDP port (514).
Enable the check box to send all events logged by Equalizer to the remote system.

use remote syslog

syslog host

Logging 設定では、Equalizer のログを syslog サーバへ出力する場合に設定します。Syslog サーバへの通信は UDP/514 ポートにて行なわれます。“use remote syslog” にチェックを入れ、“syslog host” に Syslog サーバの IP アドレスを入力し、commit ボタンで決定します。

注意： ファシリティ設定、メッセージレベル設定は行うことができません。

3-3-1-2 “handling”

handling

Enter the full pathname of a command or script to run on any server event (server up/down, server agent up/down, failover).

command to run on server event

Handling 設定は、イベント発生時に入力されたコマンドやシェルを実行します。サポート外項目になりますので、詳細は英文マニュアルをご参照下さい。

3-3-1-3 “email notification”

email notification

Enter from and to addresses in "user@example.com" or "<user@example.com>" format. The SMTP server can be specified as an IP address or hostname. Enable the check box to send email on any server event.

enable email notification

from

to

SMTP server

Email Notification は、イベント発生時にアラートメールを送付します。

項目	内容
enable email notification	メール送付設定を有効にします。
from	メールを送付の際に使用する From アドレスを指定します。SMTP サーバのセキュリティなどに問題がなければ特に制限なく指定可能です。
to	メールの送付先アドレスです、複数の宛て先を指定する場合はメールアドレスを “<” “>” で囲み、メールアドレスの間にスペースを入れて下さい。 例： <first@email.com> <second@email.com>
SMTP server	使用する SMTP サーバを指定します。Equalizer に DNS 設定がある場合はドメインによる指定も可能です。

メールが送付されるイベントは大きく分けて以下の 2 種類です

- サーバのヘルスチェックがアップ・ダウンを検知した時
- Failover が発生した時

3-3-2 “Export to CSV”

export to csv

Create a comma separated value (CSV) file containing the data used by Equalizer to plot cluster and server histories.
Note: Exported file size may be large when a long time period is selected.

time period:

クラスタの統計データおよびサーバヒストリを含む稼働統計、また機器の統計を5秒間隔で出力することができます。出力する時間は Time Period から指定することが出来、直近5分間から保存している全てのデータまで範囲の指定が可能です。

クラスタ・サーバ統計

項目	内容
Delay	サーバの平均サービスタイム。 サービスタイムとはクライアントリクエストをうけてから、サーバがリプライパケットを送信開始するのにかかる時間です。
Agent	サーバから返すサーバエージェント値の平均 (※負荷分散 Policy として Server Agent を使用していない場合は関係ございません)
Connections	サーバのアクティブコネクションの平均数
Load	サーバ負荷。
Total	サーバにより処理されたコネクション総数
Time	サーバのアップタイム
Weight	サーバの Weight 値

機器情報統計

項目	内容
Total Connections Processed	処理されたコネクションの総数
Peak Connections Processed	1 秒あたりに処理された最大のコネクション数
Connections over last sec	最後の 1 秒間に処理されたコネクション数
Connections Timed Out	コネクションタイムアウト値を超え、ドロップされたコネクション数
CPU Utilization	使用されている CPU 容量のパーセンテージ

3-3-3 “SNMP”

SNMP agent configuration

Set values below to be used by the SNMP agent, and enable the check box to run the agent. There are two MIB files to import into your MIB browser: the [Registrations](#) MIB and the [Equalizer](#) MIB.

Enable SNMP Agent	<input checked="" type="checkbox"/>
system description	<input type="text" value="Equalizer"/>
system location	<input type="text" value="location"/>
system contact	<input type="text" value="contact"/>
system name	<input type="text" value="equalizer"/>
community string	<input type="text" value="public"/>
agent IP address	<input type="text"/>

SNMP の設定を行います。E250GX では SNMP 機能はサポートされていません。

SNMP エージェントを有効にし、Equalizer へのポーリングを行なうには以下を設定します。

- Enable SNMP Agent
SNMP 機能を有効にするため、チェックを入れます。
- system description
機器情報を入力します、ユーザ様任意の項目です。
- system location
機器の設置場所を入力します。
- system contact
Equalizer の責任者名を入力します。
- 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。
- agent IP address
デフォルトでは、SNMP エージェントは各 VLAN の VLAN IP アドレスで待ち受けを行います。それ以外の IP アドレスを使用する場合は設定します。多くの場合では VLAN の Failover IP アドレスを入力します。

Equalizer プライベート MIB をダウンロードするには、表示されているリンクをクリックして下さい。

Enable SNMP traps by setting an IP address and optional port (default 162) to receive the traps. Enable the check boxes next to the events that will generate traps.

trap IP address:port	<input type="text"/>
Enable server up/down events	<input checked="" type="checkbox"/>
Enable peer events	<input checked="" type="checkbox"/>
Enable failover events	<input checked="" type="checkbox"/>
Enable partition events	<input checked="" type="checkbox"/>

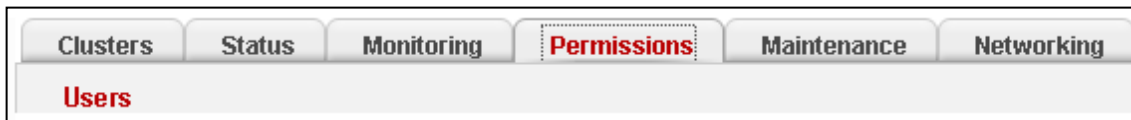
イベント発生時に SNMP によるトラップを送付する場合は以下の設定を行ってください。

- trap IP address: port
トラップを送付する IP アドレスおよびポート番号を指定します。デフォルトのポート番号は 162 番です。
- Enable server up/down events
サーバヘルスチェックの結果、サーバがダウン、またはアップと判定された際にトラップ送付します。

- Enable peer events
冗長化構成の際に、Peer との通信が途絶えた場合や再度通信疎通が取れた場合にトラップ送付します。
- Enable failover events
冗長化構成の際に、Equalizer が Primary として動作宣言をした場合にトラップ送付します。
- Enable partition events
冗長化構成の際に、両方の Equalizer が Primary として動作していることを検知した場合にトラップ送付します。

設定後画面下部の Commit ボタンを押して設定を反映させます。

3-4 “Permissions” タブ設定



3-4-1 “Users”

Web 管理画面へのログインアカウントを管理します。 [1-4-4](#) で作成したアカウントはこちらで表示され管理することが可能です。

管理できる内容は以下のようになっております

- ・ アカウントの作成・削除
- ・ パスワードの変更
- ・ 権限(グローバル・各クラスタ)の変更

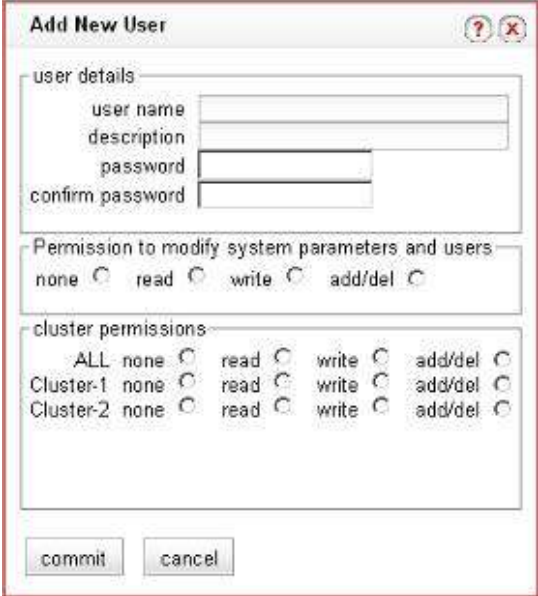
3-4-1-1 ユーザアカウントの追加

ユーザテーブルの上部にある  ボタンを押すと、以下のようなアカウント登録ウィザードが表示されます。

「user details」では作成するアカウント情報を入力します。

- ・ user name
アカウント名を入力します。
- ・ description
[1-4-4](#) の enter fullname と同一項目です、アカウントの詳細を入力します。
- ・ password / confirm password
アカウントのパスワードを入力します。

「Permission to modify system parameters and users」ではグローバル設定画面に対しての権限設定を行います。



「cluster permissions」では全体クラスタ(ALL) または 各クラスタ設定(各クラスタ名)に対する権限の設定を行います。

権限の内容は以下をご参照下さい。

権限	内容
none	アクセスする権限がありません。グローバル設定を確認することは出来なくなり、各クラスタが Web 管理画面上に表示されなくなります。
read	グローバル設定・各クラスタ設定を読み取ることが可能です、変更する権限はありません。
write	グローバル設定・各クラスタ設定を読み取り・変更することが可能です。新規作成（クラスタなど）を行なうことは出来ません。
add/del	グローバル設定・各クラスタ設定に対し、全ての権限を保持します。

クラスタ権限の設定例

```

cluster permissions
  ALL none  read  write  add/del 
  Cluster-1 none  read  write  add/del 
  Cluster-2 none  read  write  add/del 
  
```

左の例では、Cluster-1 に対しては全ての権限がありますが、それ以外のクラスタについては ALL の設定が有効ですので、読み取り専用となります。

3-4-1-2 ユーザアカウント設定の変更

ユーザアカウントのパスワードや権限を変更する為には、write 以上の権限を持ったユーザによってのみ行なうことが可能です。

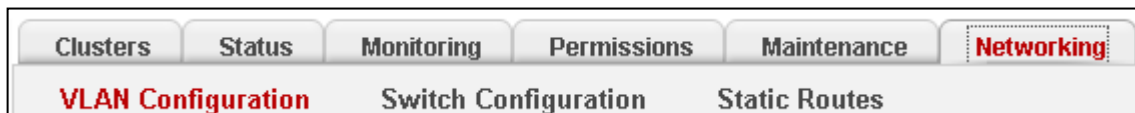
ユーザテーブルの Action の欄から  ボタンを選択すると変更ウィンドウが表示されますので、変更を行って下さい。

3-4-1-3 ユーザアカウントの削除

ユーザアカウントを削除する場合は、グローバル設定に add/del の権限を持ったユーザが削除を行なうことが可能です。

ユーザテーブルの Action の欄から  ボタンを選択すると変更ウィンドウが表示されますので、変更を行って下さい。

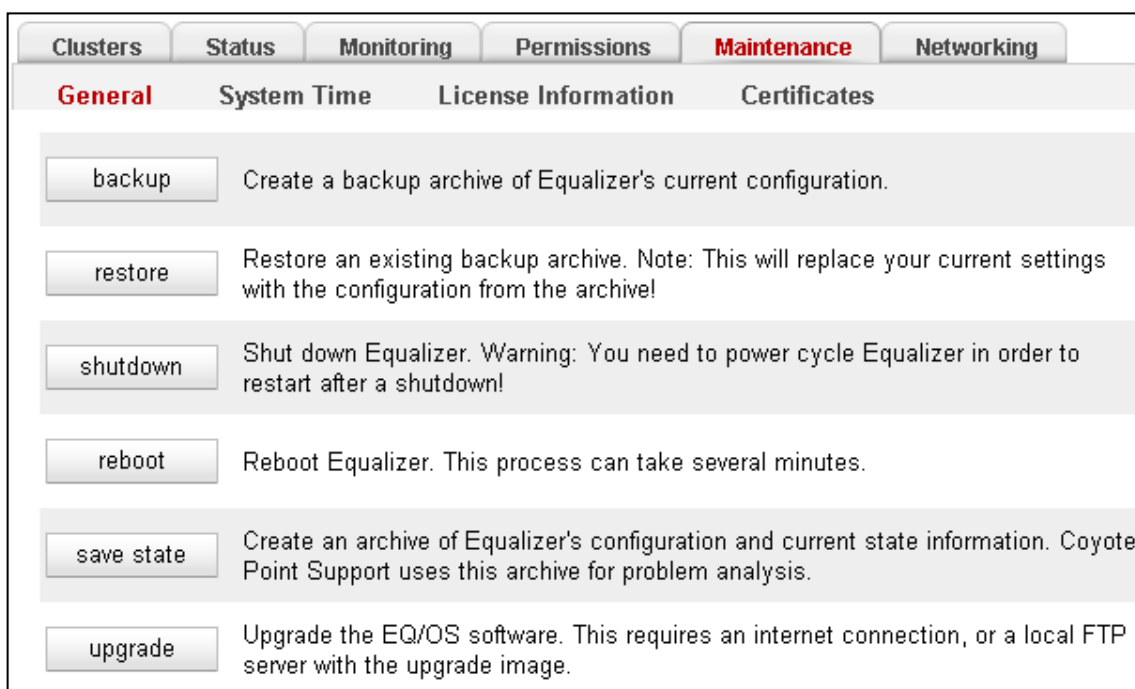
3-5 “Maintenance” タブ設定



このタブでは機器の設定・管理について設定を行います。

3-5-1 “General”

General のセクションでは、機器のシャットダウン・リブートやコンフィグに関する運用管理を行ないます。



3-5-1-1 “backup”

Equalizer の設定コンフィグ(バックアップファイル)を保存します。 ボタンを押すとブラウザのダウンロードウィンドウが表示されますので、アクセス端末上に保存して下さい。ファイル拡張子は .bkp です。

ファイル名はお客様の設定や取得した日時により異なります。

形式は [Hostname]-[MM].[DD].[YYYY]-[HH].[MM].bkp となります。

例) Equalizer1-09.20.2008-10.50.bkp

上記はホスト名(1-4-1を参照) "Equalizer1" の機器上で

2008年9月20日 10時50分に取得されたバックアップファイルです。

注意: 設定を変更した場合は必ずバックアップファイルを新規で保存して下さい。機器故障により交換した場合は、バックアップファイルがないと復旧させることが出来なくなります。

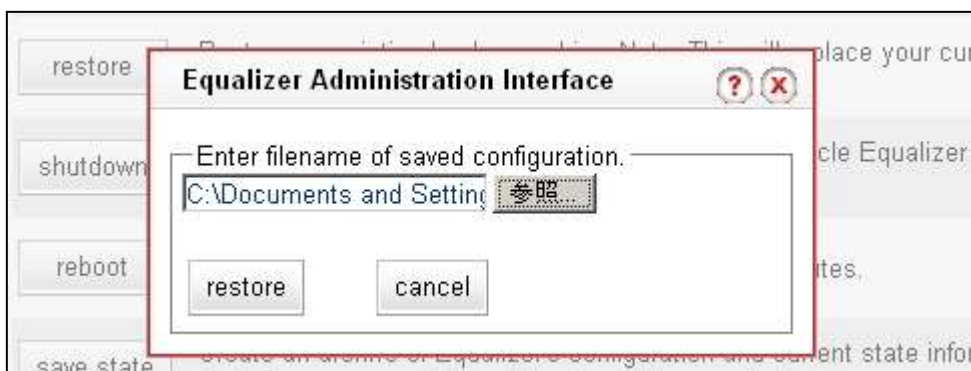
注意: 冗長化構成の場合は、両機器からバックアップファイルを取得して下さい。IPアドレスなどの情報も含まれるため、冗長構成であったとしても両機器には差異があります。

3-5-1-2 "restore"

Equalizer に対して、3-5-1-1 で取得したバックアップファイルをリストアする際に使用します。リストアすると機器は再起動し、リストアしたコンフィグにて起動します。

ボタンを選択すると下図のウィンドウが表示されますので、ファイルを端末から選択して下さい。

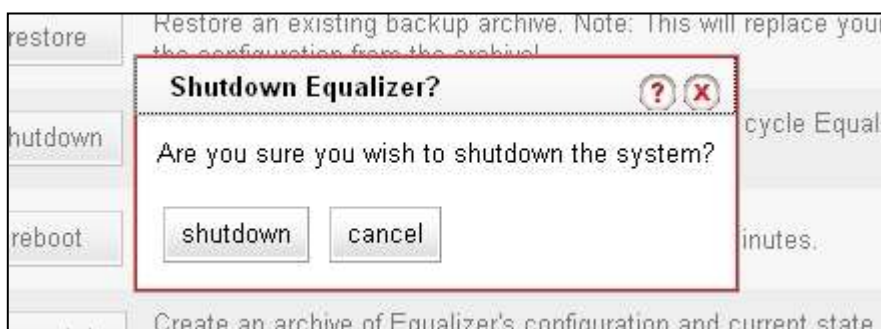
ハードウェア交換などで、MAC アドレスが異なる機器にリストアを行う場合には、リストア後に手動でコンフィグを修正する必要があります。詳細は TEC-World の FAQ をご確認ください。



3-5-1-3 "shutdown"

Equalizer の電源を切る際は、Shutdown をまず行なう必要があります。ボタンを選択すると、下図の確認メッセージが表示されますので、shutdown を再度選択すると実行されます。Shutdown が行われると画面が切り替わり「Equalizer is shutting down. Please wait one minute before cycling power.」と表示されますので、1分程度待ち、機器背面の電源をオフにします。

注意: 画面が切り替わった状態でブラウザ画面を更新すると、再度 shutdown 処理が行われます。再度機器へアクセスする場合はブラウザの更新を行わないで下さい。



3-5-1-4 “reboot”

Equalizer を再起動させる場合はこちらから行ないます。 ボタンを選択すると下図のメッセージが表示されますので、reboot を再度選択すると reboot を行ないます。



決定すると、再起動が完了するまで下記のウィンドウが表示されます。完了するとウィンドウは自動的に閉じられます。



3-5-1-5 “save state”

Equalizer の機器の状態を一括で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。このボタンを押すと以下のようなウィンドウ(ブラウザの種類により異なります)が表示されますので、アクセス端末に保存して下さい(ファイル名は “Collect_[機器の SystemID].tgz”)。



取得できるデータにはコンフィグやログなどのデータが含まれておりますが、リストア時に使用することは出来ません。コンフィグの保存は 3-5-1-1 に沿って行なって下さい。

注意： ファイル取得時には、一時的ではありますが CPU 使用率が上昇します。可能であれば、サービスへのアクセスが少ない時間に行なって頂くことが推奨されております。

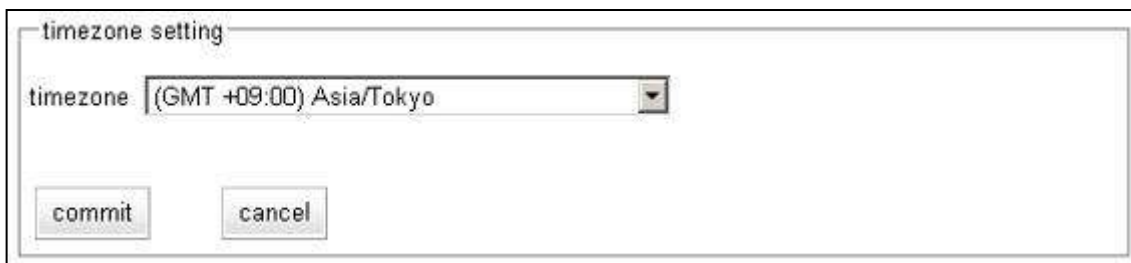
3-5-1-6 “upgrade”

セクション [1-4-8](#) と同じく、機器ファームウェアのアップグレードを行います。手順についてはファームウェア提供時にご案内致します。

3-5-2 “System Time”

機器の現在時刻、タイムゾーン、および NTP サーバの設定を行います。

3-5-2-1 “timezone setting”



「timezone setting」のセクションでは、機器のタイムゾーン設定が可能です。

3-5-2-2 “date and time”

「date and time」のセクションでは日時設定 および NTP 設定を行うことができます。NTP は 3つまで登録が可能です。commit ボタンを押すとrebootの実行を求められますので、実行します。再起動後、時刻の設定および NTP 設定は有効になります。

date and time

current date

current time :

To automatically set system time using a Network Time Protocol (NTP) server, set at least a primary server and enable the check box below. For a list of NTP pool servers, select **Help > Context Help**.

enable NTP synchronization

primary server

secondary server

tertiary server

追記：時刻の設定のみであれば、再起動せずに行うことが可能です。時刻を設定変更後、commit ボタンを押します。reboot 実行の確認メッセージが表示されますが、ここで cancel を選択すると、時刻の設定は変更されます。

3-5-3 “License Information”

Equalizer の負荷分散機能を使用するためにはライセンスを取得する必要があります。弊社から出荷された Equalizer はライセンスが取得された状態になっており、再度ライセンスを取得頂く必要は通常ございません(ファームウェアのアップグレード時など、ライセンスを再度確認する必要が発生する場合がございます)。

ライセンスの取得・確認はインターネット経由でメーカーのライセンスサーバへ通信することで行なわれます、使用するポート番号は TCP/80 番になります。

3-5-3-1 “license information”

license information

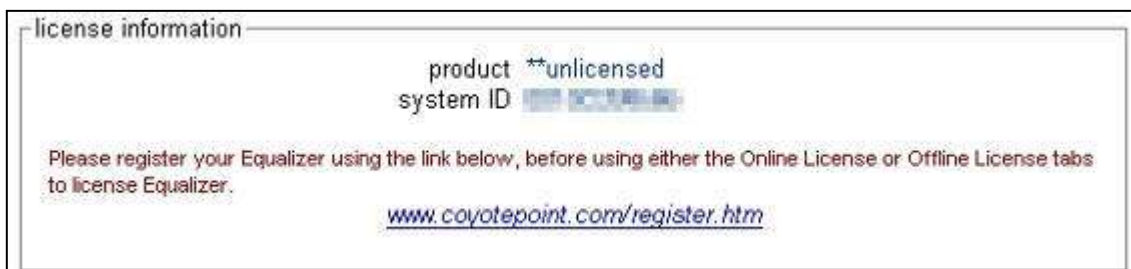
product e350
feature Envoy
servers per cluster 32
serial no. CP0608-0021
system ID XXXXXXXXXX

Please register your Equalizer using the link below, before using either the Online License or Offline License tabs to license Equalizer.

www.coyotepoint.com/register.htm

ライセンスが正常に取得・認識されている機器では、上記のようにシリアル番号などの情報が表示されます。ライセンスが正常に取得または認識されていない場合は、下記のように ”

“unlicensed” と表示されます。



注意：ライセンスが取得・認識できていない Equalizer では負荷分散の機能を使用することが出来ません。製品を正常に使用するには、ライセンスが必要になります。

3-5-3-2 “Offline License”

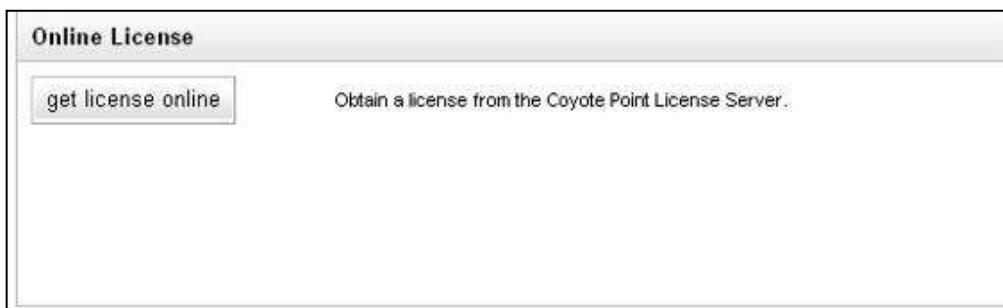


ライセンスを取得するには、通常インターネット経由でライセンスサーバにアクセスする必要がありますが(3-5-3-3 参照)、オフライン環境の場合は、Offline License 申請を行なうことでライセンス申請を行なう事が可能です。

上図の“create license request file”を選択すると、申請ファイルを端末に保存することができます。こちらのファイルを弊社 TEC-World 宛にご送付下さい(インシデント消費はございません)。

メーカーより発行されたライセンスファイルをインストールするには、上図の“install signed license file”を選択し、ライセンスファイルを選択します。機器の再起動を行う旨メッセージが表示されますので、決定します。再起動後、ライセンスファイルが正常に取得できたかを 3-5-3-1 からご確認下さい。

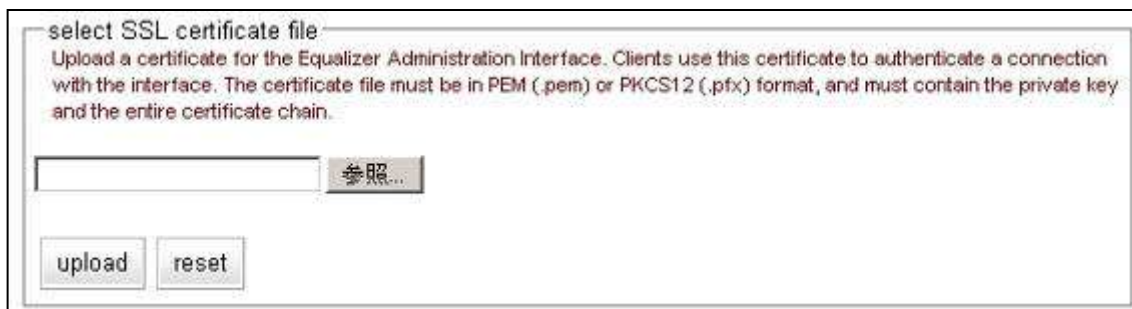
3-5-3-3 “Online License”



インターネット経由でライセンスを取得する際には、上図“get license online”を選択します。Equalizer はポート 80 番を使用しライセンスサーバへアクセスを行いません。正常に取得できた場合は、再起動を行う旨メッセージが表示されますので、決定します。再起動後、ライセンスファイルが正常に取得できたかを 3-5-3-1 からご確認下さい。

3-5-4 “Certificates”

Equalizer の Web 管理画面へアクセスする際に SSL サーバ証明書を使用する場合、こちらから証明書のアップロードを行なうことができます。サーバ証明書を申請するための CSR の作成方法などの手順については[こちらの資料](#)をご参照下さい。



注意： サービス用のサーバ証明書とは別になります。 SSL でサービスを行なう際は、別途クラスタ毎にサーバ証明書のインストールが必要になります。詳細につきましては [4-6-1](#) をご参照下さい。





3-5-5 “Static Routes (E250GX のみ)”





E250GX ではこちらに表示されます。設定内容はセクション [3-6-3](#) と同様ですので、そちらをご参照下さい。

3-6 “Networking” タブ設定 (E250GX を除く)


3-6-1 “VLAN Configuration”

Equalizer の VLAN 設定を行います。VLAN テーブル各項目の内容は以下の通りです。

+ add					
Name	VID	Contents	Tagged Ports	Untagged Ports	Actions
Default	1		None	1, 2	
vlan2	2		None	3, 4, 5, 6, 7, 8, 9, 10, 11, 12	 

項目	内容
Name	VLAN 名を設定します。
VID	VLAN ID を設定します。1～4095 までの数値が入力できます。
Contents	VLAN にクラスタ・サーバが含まれている場合、該当のアイコンが表示されます。クリックするとリストが表示されます。  はクラスタ、  はサーバを意味します。
Tagged Ports	タグポートとして登録されているポート番号を表示します。
Untagged Ports	アンタグポートとして登録されているポート番号を表示します。
Actions	 を選択すると該当 VLAN の設定変更画面を表示します。  を選択すると確認メッセージを表示後に VLAN を削除することができます。

3-6-1-1 VLAN の新規設定

VLAN テーブル上部にある  を選択すると VLAN 作成画面が表示されます。

Add New vlan

Name: VLAN IP:

VID: Netmask:

Permissions:

GUI http GUI Failover http

GUI https GUI Failover https

ssh Failover ssh

Failover IP:

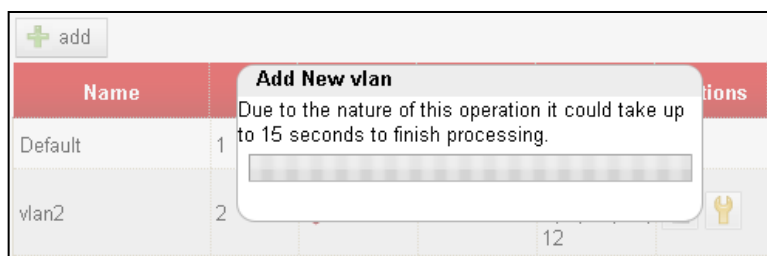
Failover Netmask:

Use IP for Failover Heartbeat

port	status		type	
1	<input type="radio"/> assigned	<input checked="" type="radio"/> unassigned	<input type="radio"/> tagged	<input type="radio"/> untagged
2	<input type="radio"/> assigned	<input checked="" type="radio"/> unassigned	<input type="radio"/> tagged	<input type="radio"/> untagged
3	<input type="radio"/> assigned	<input checked="" type="radio"/> unassigned	<input type="radio"/> tagged	<input type="radio"/> untagged
4	<input type="radio"/> assigned	<input checked="" type="radio"/> unassigned	<input type="radio"/> tagged	<input type="radio"/> untagged
5	<input type="radio"/> assigned	<input checked="" type="radio"/> unassigned	<input type="radio"/> tagged	<input type="radio"/> untagged
6	<input type="radio"/> assigned	<input checked="" type="radio"/> unassigned	<input type="radio"/> tagged	<input type="radio"/> untagged

項目	内容	
Name	VLAN 名を設定します。	
VID	VLAN ID を設定します。 1~4095 までの数値が入力できます。	
VLAN IP	VLAN に設定するリアル IP アドレスを設定します。	
Netmask	リアル IP アドレスのネットマスクを設定します。	
Failover IP	冗長化構成時に VLAN に設定する Failover Alias IP アドレスを設定します。	
Failover Netmask	Failover Alias IP アドレスのネットマスクを設定します。	
Use IP for Failover Heartbeat	冗長化構成時に該当 VLAN で冗長化用通信を行うかを設定します。 無効の場合は VLAN でネットワーク障害が発生した場合でも Failover が行われません。	
Permissions	GUI http	リアル IP アドレスへの HTTP アクセスを許可します。
	GUI https	リアル IP アドレスへの HTTPS アクセスを許可します。
	ssh	リアル IP アドレスへの SSH アクセスを許可します。
	GUI Failover http	Failover Alias IP アドレスへの HTTP アクセスを許可します。
	GUI Failover https	Failover Alias IP アドレスへの HTTPS アクセスを許可します。
	Failover ssh	Failover Alias IP アドレスへの SSH アクセスを許可します。
ポート番号リスト	port	前面スイッチのポート番号を表示します。
	status	assigned を選択することで該当ポートを VLAN に所属されます。所属させない場合は unassigned を選択します。
	type	tagged または untagged を選択します。 tagged に設定する場合はポートが所属している全ての VLAN で tagged に設定する必要があります。

各設定を入力後、 ボタンで決定することで設定が反映されます。 その際に以下メッセージが表示されます、設定追加が完了するとメッセージは自動的に消えます(メッセージが表示されるまで数秒かかることがあります)。




3-6-1-2 VLAN の設定変更

該当 VLAN の Action から  を選択することで設定変更を行うことができます。 機器が冗長化構成されている場合は Use IP for Failover Heartbeat のチェックを外してから変更を行います。

また Default VLAN の IP アドレスを変更した場合は機器の再起動が必要になりますので、表示されるメッセージに従って commit & reboot を実施してください。

3-6-1-3 VLAN の削除

VLAN を削除する場合は、該当 VLAN の Action から  を選択することで可能です。選択後に確認メッセージが表示されますので delete を選択します。冗長化構成時は Use IP for Failover Heartbeat のチェックを外してから削除します。

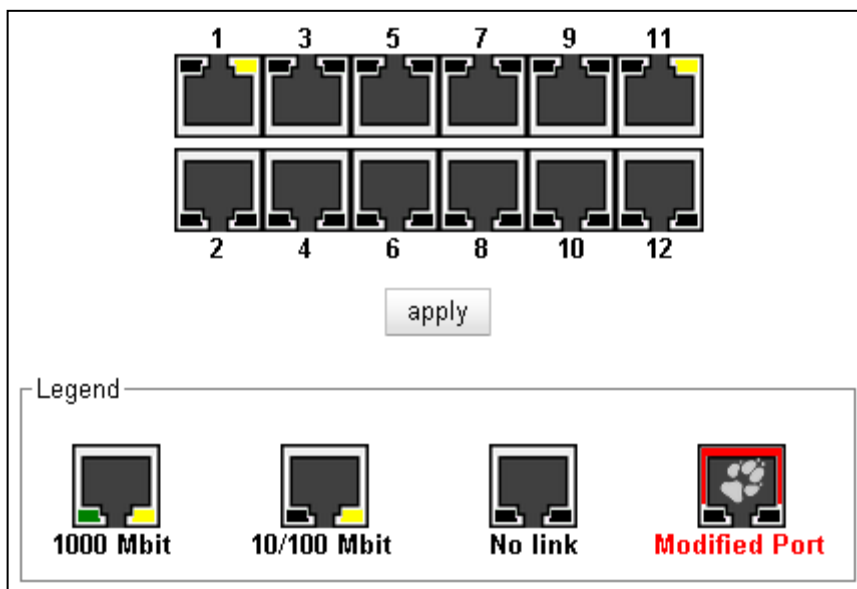
補足: VLAN 設定の注意点については TEC-World 内の FAQ でまとめているのでご確認下さい。


3-6-2 “Switch Status”




Equalizer 筐体前面のスイッチポート設定を行います、E250GX では使用できません。

3-6-2-1 スイッチポートのステータス確認

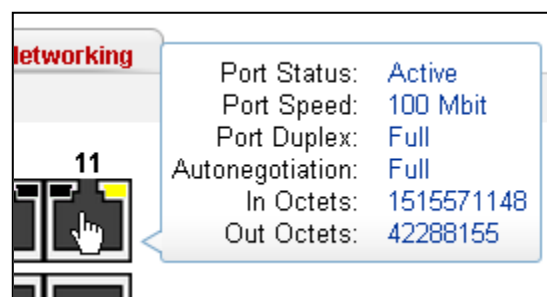
表示される下記ポート図で、機器スイッチポートステータス確認が出来ます。



解説図	内容
 1000 Mbit	緑・黄色の両 LED 表示が点灯している場合、そのポートは 1000Mbps でリンクアップしています。

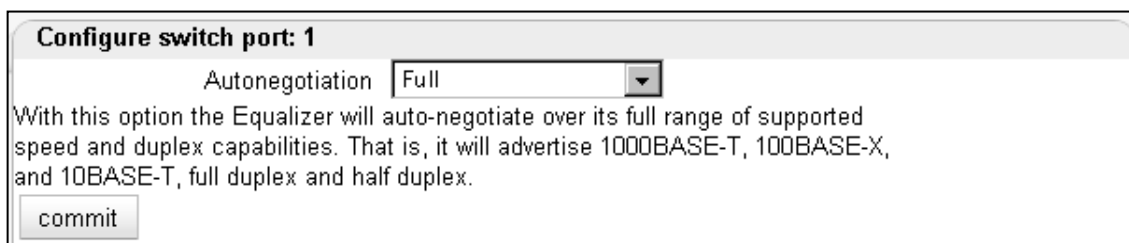
 10/100 Mbit	黄色の LED 表示のみ点灯している場合、そのポートは 10Mbps または 100Mbps でリンクアップしています。
 No link	LED 表示がなにもない場合、そのポートはリンクダウンしていません。
 Modified Port	ポート設定を変更した場合、枠線が赤くなり Coyote 足跡マークが表示されます。この状態ではまだ変更は確定しておらず、Commit を押して変更を決定する必要があります。

また、右図のようにポートの上にマウスカursorを合わせることで、そのポートの設定や、リンクアップしている場合は現在のリンク状態を確認することが可能です。



3-6-2-2 スイッチポートのステータス変更手順

スイッチポートのステータス変更を行うには、変更したいポートをポート図でクリックし、選択します。変更可能なパラメータが下記のように表示されます。






項目	選択肢	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/Duplex	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。
commit	設定を完了し、ポート図に戻ります。	

ポートの設定を更新後、ポート図上で当該ポートが“Modified Port”として表示されていることを確認して下さい。確認後、ポート図下部の apply ボタンを選択し、変更内容を決定します。“Modified Port”の表示が消えれば設定変更は完了です。

3-6-3 “Static Routes”

スタティックルートの設定・変更・削除を行います。

Use this table to define static routes on Equalizer. This is usually necessary only when a client or server is not on the same subnet as Equalizer's external or internal interfaces.

Name	Type	Network/Host	Gateway	Actions
192segment	-net	192.168.1/24	10.15.100.5	 
				

3-6-3-1 スタティックルートの追加

Add New Route ? X


new route settings

name

route type host ▼

network/host

gateway

スタティックルートを追加するにはルートテーブル画面から  を選択します。上記のウィンドウが表示されますので、パラメータを記載します。


- ・ name
作成するルートに名称を設定します。
例)route1 route2
- ・ route type
ネットワークを設定するには network、ホストを設定するには host を選択します。
- ・ network/host
あて先ネットワーク/ホストを指定します。
例)192.168.1/24, 10.10/16, 192.168.1.100/32

- gateway


宛先のゲートウェイアドレスを指定します。

例)172.16.100.1, 10.10.50.1

3-6-3-2 スタティックルートの変更

作成したスタティックルート情報を変更するにはルートテーブル画面から  を選択します。
3-5-5-1 と同様のウィンドウが表示されますので、設定を変更し、決定します。

3-6-3-3 スタティックルートの削除

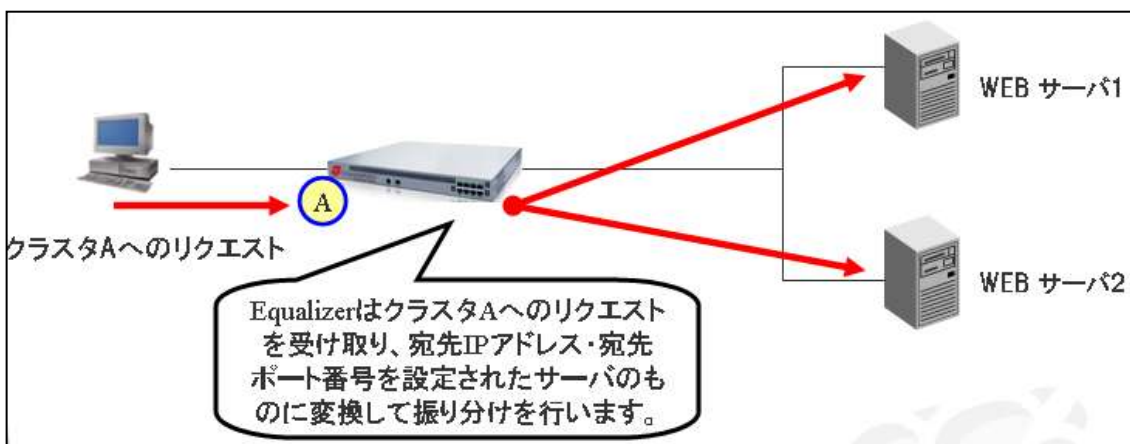
作成したスタティックルート情報を削除するにはルートテーブル画面から  を選択します。
確認のウィンドウが表示されますので、決定を選択するとルート情報は削除されます。

セクション4 クラスタ・サーバ設定手順

4-1 クラスタとサーバの関係

このセクションでは、サービスを提供するために必要なクラスタ、およびクラスタに所属するサーバについて、その設定手順を説明致します。

4-1-1 クラスタの定義について



Equalizer で実際のサービスを行なう IP アドレスは、Equalizer のリアル IP アドレスではなく別途作成される仮想 IP アドレスです。この仮想 IP アドレス (Virtual IP, VIP) に受け付けるポート番号を組み合わせたものがクラスタと呼ばれます (上図参照)。

注意: クラスタ IP アドレスに到達した通信でも、クラスタのポート番号とリクエストのポート番号が違う場合 Equalizer は通信を受け付けません。

4-1-2 サーバの定義について

クラスタの IP アドレス・ポート番号に到達した通信は、実際にサービスを提供するサーバに割り振られます。Equalizer ではサーバは各クラスタに所属していますので、各クラスタに対してサーバ追加を行う設定になります。

注意: 別クラスタで受け付けた通信を同一サーバに振り分ける場合は、クラスタを複数作成し、各クラスタに同じサーバを設定します。

4-1-3 サーバに対する Equalizer の監視について

Equalizer はサービスを継続して行なう為、サーバにヘルスチェック(死活監視)を行ないます。ヘルスチェックに失敗したサーバは「ダウン」となり、リクエストの振り分けが停止します。

4-1-4 Equalizer を通過する通信について

4-1-1 で、クラスタに到達した通信は所属するサーバに割り振られるという説明がありましたが、クラスタ IP アドレス、Equalizer のリアル IP アドレス、Failover Alias IP アドレス以外に対する通信については、Equalizer はルーティング処理を行ない処理します。従って、2つ以上の VLAN がある構成(E250GX ではデュアルネットワーク構成)においても Equalizer をまたぐ通信が可能になります(Equalizer のリアル IP アドレスまたは Failover Alias IP アドレスをゲートウェイとして指定します)。

4-1-5 サーバのデフォルトゲートウェイについて

Equalizer を使用する際、通常は負荷分散対象サーバのデフォルトゲートウェイは Equalizer のリアル IP アドレスを指定します。これは、Equalizer が負荷分散通信を行なう際に IP アドレスを NAT している為です、この NAT された IP アドレスを再変換するためにサーバからの応答通信は Equalizer へ戻される必要があります(4-1-6 も併せてご確認ください)。

冗長化構成の場合は、2台の Equalizer が共有する Failover Alias をゲートウェイとして設定します(5-2-6)。

4-1-6 spoof 設定について(SNAT 設定)

4-1-5 のように負荷分散サーバのデフォルトゲートウェイは通常 Equalizer に向ける必要がありますが、spoof の設定を変更することで別の機器をデフォルトゲートウェイとして設定し、かつ負荷分散通信も行なうことが可能になります。

4-1-6-1 spoof とは

spoof は各クラスタに個別で行なう設定で、機器全体に対する設定ではありません。デフォルトは有効になっていますが、無効にすることで Equalizer は SNAT(Source NAT) の動作をしません。設定箇所については [4-4-1-1](#)、[4-5-1-1](#) をご参照ください。

SNAT 動作を行なうと、クライアントからの通信を Equalizer がサーバに振り分ける際に、クライアントの送信元 IP アドレスを Equalizer のリアル IP アドレスに NAT 変換します。

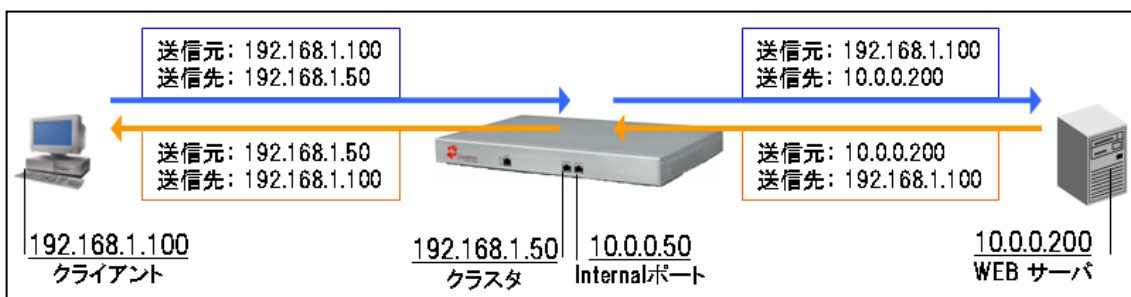
spoof 設定と SNAT 動作の関係については以下の表をご参照下さい。

spoof 設定	SNAT 動作
有効(デフォルト)	しない
無効	する

4-1-6-2 SNAT(Source NAT)の動作

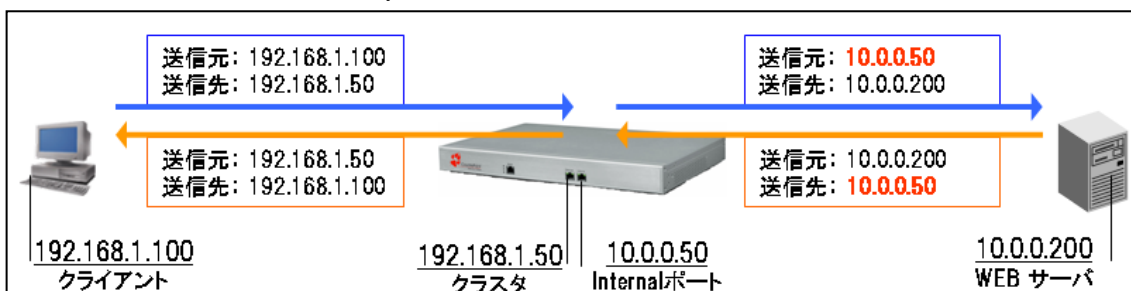
デュアル・シングル両ネットワーク構成において、SNAT の動作がどのように行なわれるのか、以下の図で解説します。

■デュアルネットワーク構成、spoof 有効(SNAT 無効)の状態



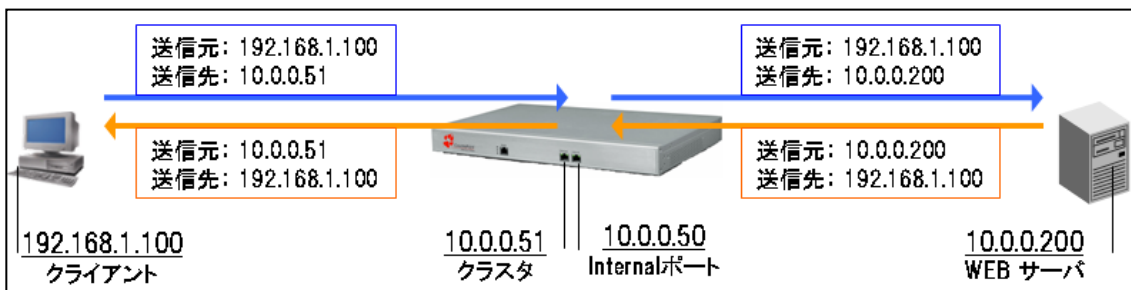
Equalizer はクライアントのリクエストを受け付け、送信先 IP アドレスをサーバの IP アドレスに変換し通信をおこないます。しかし送信元 IP アドレスは変換せず、クライアントの IP アドレスがそのままサーバへ到達しています。

■デュアルネットワーク構成、spoof 無効(SNAT 有効)の状態

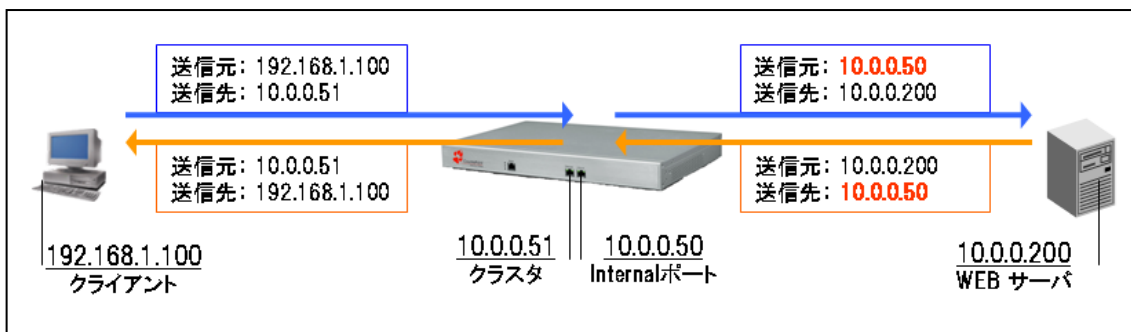


Equalizer がサーバへ通信を行なう際、送信元 IP アドレスを Equalizer のリアル IP アドレスへ変換 (NAT)していることが分かります。

■シングルネットワーク構成、spoof 有効(SNAT 無効)の状態



■シングルネットワーク構成、spooF 無効(SNAT 有効)の状態



上記例のように、spooF を無効にして SNAT 動作を行なうことで、サーバへのアクセスは全て Equalizer のリアル IP アドレスから行なわれるようになります。

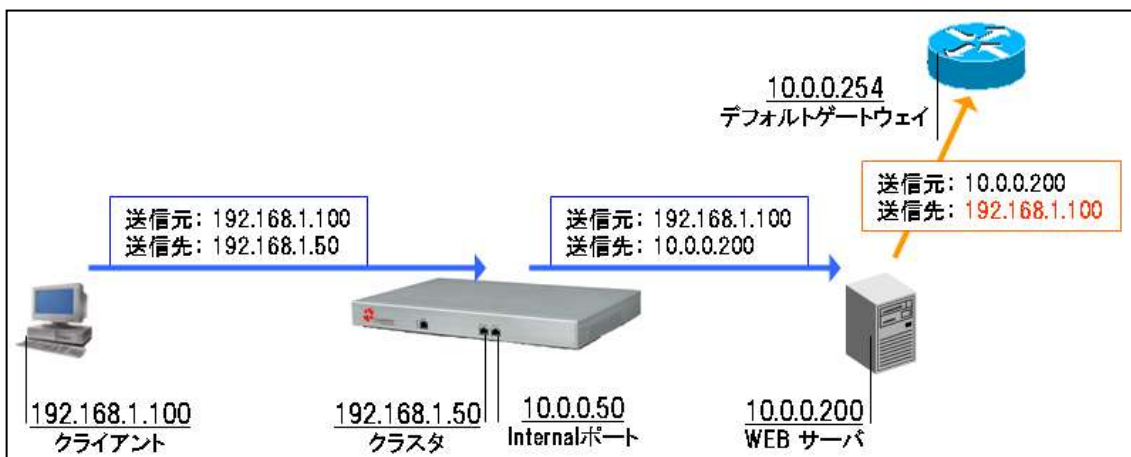
ファームウェア 8.6.0f で VLAN 機能を使用した場合(E350GX 以上)、SNAT される IP アドレスはサーバが所属する VLAN の IP アドレスになります。E250GX で L4 クラスタを使用した場合、必ず Internal ポートの IP アドレスに SNAT されます。

4-1-6-3 なぜ SNAT を使用するのか

4-1-5 の通り、通常サーバのデフォルトゲートウェイは Equalizer へ指定し、Equalizer へ通信を戻しますが、ネットワーク環境などによってはサーバのデフォルトゲートウェイを Equalizer 以外の機器に向ける必要がある場合があります。

このようなケースでは spooF を無効(SNAT を使用)にし、サーバへのアクセスは必ず同一セグメントである Equalizer から行なうようにします。同一セグメント内の通信になるため、サーバはデフォルトゲートウェイを使用せずに応答通信を Equalizer へ戻すことが可能になり、負荷分散の通信が確立します。

下記図では、サーバのデフォルトゲートウェイが Equalizer 以外に向いているため、他セグメントである 192.168.1.100 から到達したリクエストはデフォルトゲートウェイに向かって送信されています。このような状況では SNAT を使用することで、通信を正常に行うことが可能になります。



4-1-6-4 SNAT のデメリット

4-1-6-3 のように、SNAT を使用することでサーバのデフォルトゲートウェイを意識せずに通信を行なうことが可能ですが、全アクセスの送信元 IP アドレスが Equalizer のリアル IP アドレスになります。サーバで送信元 IP のログ収集を行なうことが出来なくなりますので注意が必要です。この問題を解決するため、Equalizer は X-Forwarded-For ヘッダを追加する機能を備えています。詳細は 4-1-6-5 をご確認ください。

また Equalizer を冗長化構成で使用している場合は、Primary 役として処理を行なっている Equalizer の IP アドレスが送信元 IP アドレスになります。

4-1-6-5 “X-Forwarded-For” ヘッダ追加について

L7/HTTP、L7/HTTPS クラスタを使用した場合、Equalizer がクライアントリクエストをサーバへ振り分ける際にクライアントの送信元 IP アドレスを X-Forwarded-For ヘッダとして追加することが可能です。サーバで X-Forwarded-For ヘッダを確認することで、クライアントの送信元 IP アドレスを取得することが可能になります。設定方法は [4-5-1-5](#) をご確認ください。

4-1-7 ポート変換機能について

通常では、クラスタが受け付けるポート番号とサーバが受け付けるポート番号は同じです。例えば、TCP/80 番でサービスを提供しているクラスタに所属するサーバのポート番号は、同じく TCP/80 番になっています。

Equalizer ではポートリダイレクション機能が提供されていて、サーバのポート番号をクラスタとは別に設定することが可能です。以下の設定ではサービスの提供は TCP/80 番で行なっていますが、Equalizer とサーバ間の通信は TCP/8080 番で行なっています。

- クラスタ “Cluster_Web” (ポート: TCP/80)
- サーバ1:192.168.1.10 (ポート:TCP/8080)

サーバ2:192.168.1.11 (ポート:TCP/8080)

Equalizer は自動的にポートを変換しています。この設定はサーバを作成する際に(4-8 参照)ポート番号を指定するだけで行なうことができます。サーバ作成後は、サーバのポート番号に対して TCP ヘルスチェックが開始されます。

サーバのポート番号とは別のポート番号を使用してヘルスチェックを行ないたい場合は、[4-8-3](#) の probe port 設定を行ってください。

4-1-8 HTTPS クラスタの動作について

HTTPS クラスタを使用した場合、SSL 通信をクラスタで受け付け処理することが可能になります。HTTPS クラスタには SSL サーバ証明書がインストールされており([4-6-1](#)を参照) SSL の複号処理を行なった後、サーバに対しては HTTP 通信を行ないます。

サーバからの戻り通信は、Equalizer まで HTTP 通信で行なわれた後、Equalizer が再度 SSL 暗号処理を行い、クライアントに対して通信を行ないます。この動作によって、クライアントと Equalizer の間はセキュアなコネクションが保たれます。



補足: HTTPS クラスタ作成時のデフォルトポート番号は 443、HTTPS クラスタのサーバデフォルトポート番号は 80 に設定されています。

4-2 ネットワーク構成について

Equalizer で実現可能なネットワーク構成について、また構成によるクラスタ・サーバの IP アドレス体系などにつきましては、[弊社サポートページ](#) をご確認ください。

4-3 クラスタ作成

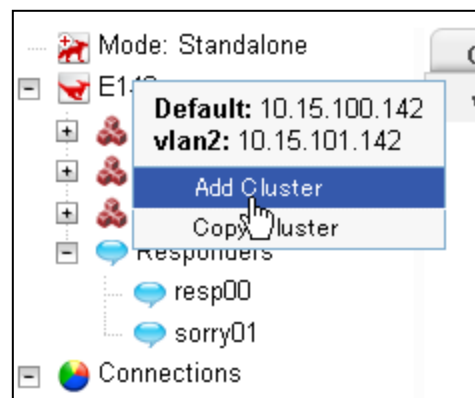
Equalizer で作成できるクラスタは、以下の4種類になります。

モデル	L4/TCP	L4/UDP	L7/HTTP	L7/HTTPS
E250si	○	○	×	×
E350si / E450si E550si	○	○	○	○
全 GX シリーズ	○	○	○	○


アドバイス：冗長化構成では、まず冗長化設定(セクション5参照)を行うことを推奨しています。これは、冗長化構成の Equalizer はデフォルトではクラスタ・サーバの設定は同期するので、同期させることで片側機器のみ設定を行うともう一方の機器に設定が自動でコピーされるからです。

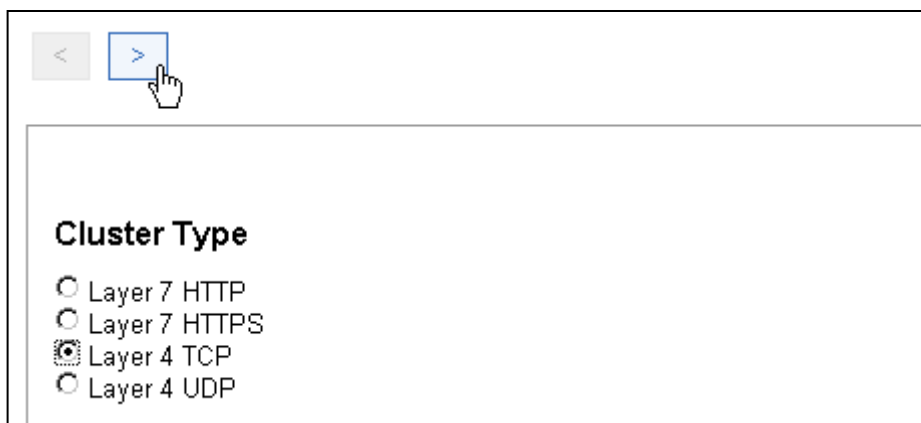
4-3-1 クラスタ作成ウィザードの起動

クラスタの作成は、クラスタ作成ウィザードから行ないます。左フレームを右クリックすると、メニューが表示されます(下図)。メニューから“Add Cluster”を選択し、ウィザードを起動します。

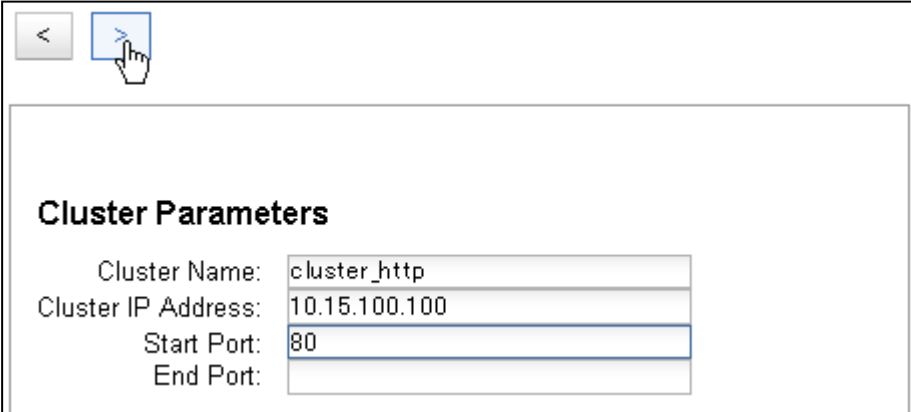


4-3-2 L4クラスタの作成

L4クラスタを作成する場合は、ウィザードで“Layer 4 TCP”または“Layer 4 UDP”を選択し  ボタンを押して次に進みます。



次画面にて作成するクラスタの詳細情報を入力します。




Cluster Parameters	
Cluster Name:	cluster_http
Cluster IP Address:	10.15.100.100
Start Port:	80
End Port:	

- Cluster Name
クラスタの名称設定です、アルファベットから始まる必要があります。
- Cluster IP Address
クラスタの IP アドレスを入力します。
- Start Port
受付ポートの開始ポートを設定します。
- End Port
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。単一ポートのみの設定であれば空欄にします。

次画面で設定内容を確認し commit すると新規 L4クラスタが追加されます。

4-3-3 L7クラスタの作成

L7クラスタを作成する場合は、ウィザードで“Layer 7 HTTP”または“Layer 7 HTTPS”を選択し  ボタンを押して次に進みます。

次画面では 4-3-2 と同じくクラスタ情報を入力します。L4クラスタと違い、設定するポート番号は1つです。設定内容を確認し commit すると新規 L7クラスタが左メニューに追加されます。

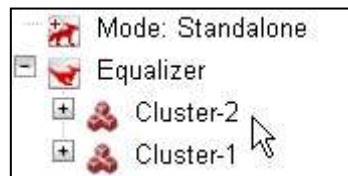
4-3-4 クラスタの削除

作成したクラスタを削除するには、左フレームで削除したいクラスタを選択し右クリックします。表示されるメニューから Delete Cluster を選択すると、確認画面が表示されますので、決定を押すと削除完了です。

または、[3-1-1](#) で削除ボタンを使用することでも行なうことが可能です。

4-4 L4 クラスタパラメータ設定

クラスタのパラメータを設定します。作成したクラスタを左メニューから選択することでパラメータ設定画面へ移行することができます(右図)。



注意: 一部のパラメータは [3-1](#) と同様のものです。3-1 の設定内容はグローバル設定として、すべてのクラスタに適用されます。3-1 と同様のパラメータを各クラスタに個別設定した場合はグローバル設定よりも優先されます。

4-4-1 “Configuration” タブ



クラスタ動作に必要な設定を行うタブです。以下3つに分類されています。

4-4-1-1 “Required”

cluster parameters

protocol: Layer 4 TCP

ip: 192.168.100.10

start port: 80

end port: 80

idle timeout: 0.0

VLAN: 1: Default

disable:

spooof:

direct server return:

commit show defaults reset

項目	内容
protocol	4-3-2 で作成したクラスタ種類が表示されます (変更は出来ません)
ip	4-3-2 で作成した IP アドレスが表示されます (変更可能です)
start port	4-3-2 で作成したポート番号が表示されます (変更可能です)
end port	同上
idle timeout	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。 デフォルトは0秒でタイムアウト時間はありません。
VLAN	クラスタに設定された IP アドレスから、所属する VLAN を判別し表示します。 リストからVLANを選択し手動で変更することも可能です。 E250GX では表示されません。
disable	クラスタサービス無効にする設定です。 試験的にクラスタ導入を行い、検証時間外にリクエストを受け付けたくない場合等に、有効にします。
spooof	有効の場合、アクセスするクライアントの送信元 IP アドレスをクラスタ所属サーバにそのまま振り分けます。 無効の場合、アクセスするクライアントの送信元 IP アドレスは Equalizer のインターフェースに NAT されサーバに振り分けが行なわれます。 詳細は 4-1-6 を参照して下さい。
direct server return	DSR 構成を行なう際、有効にします。

4-4-1-2 “Probes”

cluster parameters

probe port	<input type="text" value="0"/>
ACV probe	<input type="text"/>
ACV response	<input type="text"/>
probe delay	<input type="text" value="10.0"/>
server agent port	<input type="text" value="1510"/>
agent probe	<input type="text"/>
probe ssl	<input type="checkbox"/>

agent type

Server agent requires custom agent running on each server. Virtualization Load Balancing (VLB) agent uses Virtual Center configuration to monitor servers.

server agent

VLB

none

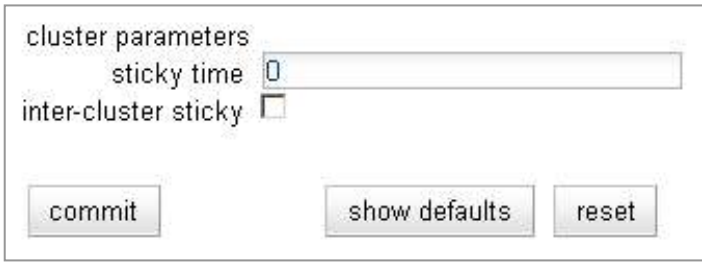
commit
show defaults
reset

項目	内容
probe port	サーバヘルスチェックのポート番号を指定します。 デフォルトでは0と表示され、クラスタの受付ポートが使用されます。
ACV probe	ACV によるサーバヘルスチェックを行なう際に使用します、詳細は 4-7-3 をご確認ください。
ACV response	ACV によるサーバヘルスチェックを行なう際に使用します、詳細は 4-7-3 をご確認ください。
probe delay	3-1-2 と同様の設定になります。

server agent port	Server agent を使用するとサーバからパフォーマンス統計を収集し、その情報に基づき負荷分散を行ないませんが、サーバ上でエージェントデーモンを走らせる必要があります(日本国内サポート対象外の機能です)。agent type の設定を server agent を選択するとこのパラメータは有効になります。
agent probe	サーバ側の agent に対して通信を行なう際のポート番号を指定します。デフォルトでは 1510 を使用します。
probe ssl	SSL 通信を提供しているクラスタで ACV の設定がされている場合に有効にします。
agent type	server agent や VLB を使用した負荷分散を行なう場合に、該当する箇所を有効にします。

4-4-1-3 “Persistence”

セッション維持の動作設定を行います。L4 クラスタに於けるセッション維持動作については [APPENDIX A](#) をご参照下さい。



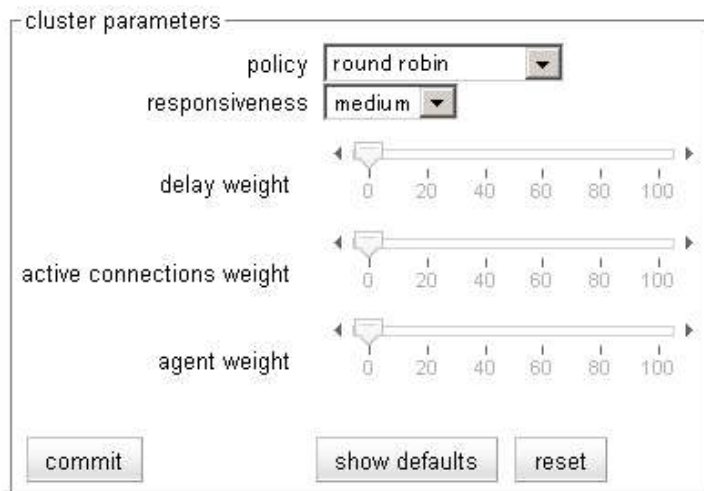
項目	内容
sticky time	クライアントの送信元 IP アドレスを利用してセッションを維持させる為の時間設定(秒)です。アクセスがあった送信元 IP は Sticky レコードに記録され、時間設定以内に再度通信が行なわれた場合は同じサーバに対して振り分けが行なわれます。セッション維持が必要ではない場合、0 秒を設定して下さい。
inter-cluster sticky	L4 クラスタを使用し、同じ IP を持つ複数のクラスタが同一のサーバ構成で設定されている状況で、そのクラスタをまたがった通信でセッション維持を行ないたい場合にはチェックを入れます。

注意: Sticky レコードを保持するためにはメモリを使用します。アクセスが多い環境などで Sticky 設定時間が長すぎる場合には機器メモリがひっ迫する可能性がありますので、ご注意下さい。600秒程度がメーカーの推奨値となっております。

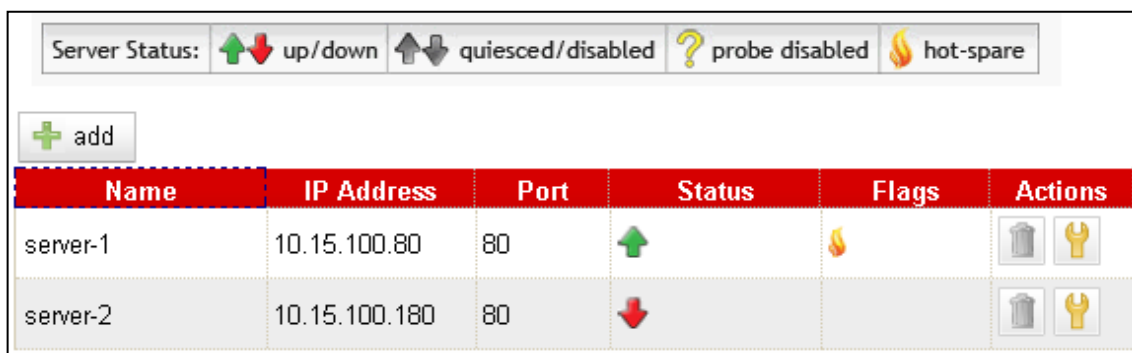
4-4-1-4 “LB Policy”

このクラスタ内で使用される負荷分散ポリシーを選択します。各ポリシーの詳細は [4-7-1](#) を参照下さい

動的負荷分散の反応速度もこの画面から設定します、詳細は [4-7-2](#) を参照下さい






4-4-2 “Servers” タブ







Name	IP Address	Port	Status	Flags	Actions
server-1	10.15.100.80	80	↑	🔥	🗑️ 🛠️
server-2	10.15.100.180	80	↓		🗑️ 🛠️

クラスタ所属のサーバー一覧が表示されます。

項目	内容
Name	設定したクラスタ名が表示されます。
IP Address	設定した IP アドレスが表示されます。
Port	設定したポート番号が表示されます。
Status	サーバの状態がアイコンで表示されます。各アイコンの意味については、 3-2-1 を参照して下さい。
Flags	サーバが Hotspare 設定されているとアイコンが表示されます。
Actions	該当するサーバの削除  変更  を行うことができます。サーバ新規作成を行なう場合には  を選択します。

4-4-3 “Smart Events” タブ

クラスタに設定されている Smart Events の一覧を表示し、作成・削除などの管理を行うことができます。 Smart Events についての詳細は、[セクション8](#) をご確認ください。

+ add		
Name	Status	Actions
event-1	ready	 
event-2	ready	 

項目	内容
Name	Smart Events 名が表示されます。
Status	各 Smart Events の状態が表示されます。「ready」と表示されている場合はその Smart Events は動作可能な状態です。「blocked」と表示されている場合は、Smart Events はアクション “event_wait” によってブロックされている状態です。
Actions	各ボタンを選択することで、削除・設定変更が可能です。

4-4-4 “Reporting” タブ

Configuration	Servers	Smart Events	Reporting
Statistics Plots			

クラスタに対する通信の状況などを確認することができます。

4-4-3-1 “Statistics”

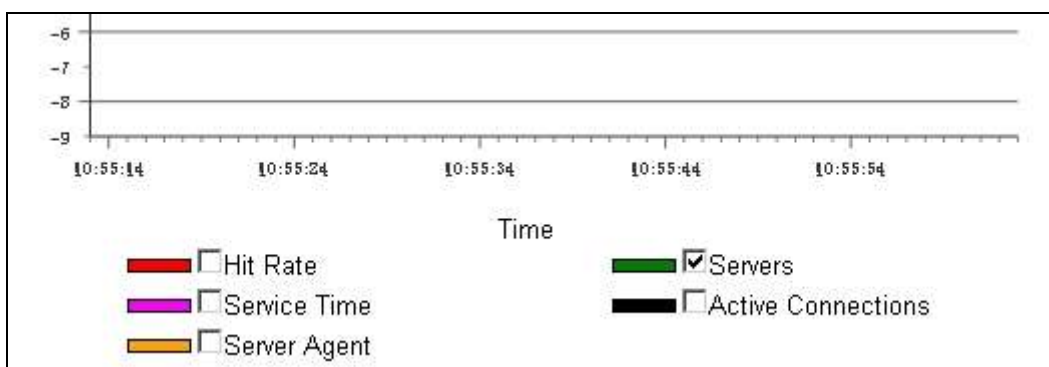
クラスタに対する通信の統計を簡単に確認することが可能です(右図)。各パラメータについては以下をご参照下さい。

Cluster Statistics
total number of servers: 2
server active connections: 0
total connections served: 754
active sticky records: 0

項目	内容
total number of servers	クラスタに設定されているサーバ数が表示されます。
server active connections	3-2-1 で確認できる Active の項目と同様です。現在アクティブなセッション数を表示します。

total connections served	3-2-1 で確認できる Processed の項目と同様です。処理されたセッション数を表示します。
active sticky records	3-2-1 で確認できる Sticky の項目と同様です。クラスタが保持している Sticky 数を表示します。

4-4-3-2 “Plots”



クラスタ・サーバについての統計をグラフ表示することが出来ます。

4-4-5 FTP サービスを提供する場合のクラスタ設定

Equalizer でFTP サービスを提供する場合は、以下の設定を参照して下さい。FTP は複数のポートを使用し、かつFTP が行なう NAT 動作を正常に処理するため、Equalizer は特別な仕様になっています。

クラスタの作成方法などは通常と同じですが、FTP クラスタ用の設定については以下の表を参照して下さい。

設定項目	使用するパラメータ
クラスタ	L4/TCP クラスタ
ポート番号	21
spooof	有効

外部からアクセス出来ないネットワークセグメントにサーバ群が設定されている場合 passive FTP translation のオプションを有効にすることが必要な場合があります(3-1-4を参照)。有効にした場合、Equalizer はサーバの IP アドレスではなくクラスタ IP アドレスを含めるようにサーバから外部への FTP PASV コントロールメッセージを書き直します。

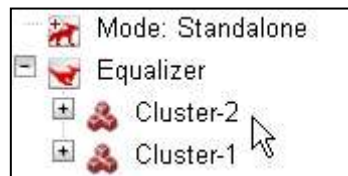
FTP クラスタを使用する際には、以下の点にも留意して下さい。

- Equalizer のポート変換機能は使用できません。クラスタで設定されたポート番号と、サー

- バで設定されたポート番号は同じでなければなりません。
- FTP クラスタは前述の通りポート21番で設定する必要があります。ポートの範囲指定機能を使用し、例えばポート19番～50番を設定したとしても Equalizer は FTP クラスタとは認識しません。
 - FTP のデータコネクションは Equalizer の内部動作として sticky time は1秒として処理されています。これは、多くの Web ブラウザで使用されている Passive モードのデータコネクションをサポートするためです。
 - FTP クラスタは Web 管理画面には1つのクラスタのみ表示されますが、内部動作としては2つのクラスタスロットを使用しています。こうすることでサーバからの FTP データコネクションを正常に NAT し外部へ通信させることができます。

4-5 L7/HTTP クラスタパラメータ設定

クラスタのパラメータを設定します。作成したクラスタを左メニューから選択することでパラメータ設定画面へ移行することができます(右図)。



4-5-1 “Configuration” タブ



クラスタ動作に必要な基本設定を行うタブです。以下5つのセクションに分かれています。

4-5-1-1 “Required”

cluster parameters

protocol	Layer 7 HTTP
ip	192.168.100.200
port	80
netmask	0xffffffff
VLAN	1: Default
disable	<input type="checkbox"/>
ignore case	<input checked="" type="checkbox"/> (inherit from global: <input checked="" type="checkbox"/>)
spoof	<input type="checkbox"/>

commit show defaults reset

項目	内容
protocol	4-3-2 で作成したクラスタ種類が表示されます (変更は出来ません)
ip	4-3-2 で作成した IP アドレスが表示されます (変更可能です)
responsiveness	動的負荷分散の反応速度を設定します、詳細は 4-7-2 を参照下さい
netmask	External ポートで定義されているサブネットマスクとは異なるサブネットがクラスタ IP のサブネットに適用されている場合のネットマスクの値になります。これはお客様が適切なルーティングをクラスタが複数 IP サブネットにアクセス出来るように設定されている事が条件になります。
VLAN	クラスタに設定された IP アドレスから、所属する VLAN を判別し表示します。リストから VLAN を選択し手動で変更することも可能です。E250GX では表示されません。

disable	クラスタサービス無効にする設定です。 試験的にクラスタ導入を行い、検証時間外にリクエストを受け付けたくない場合等に、有効にします。
ignore case	有効な場合 Match Rules で精査する内容で大文字・小文字の判別を行いません。
spooof	有効の場合、アクセスするクライアントの送信元 IP アドレスをクラスタ所属サーバにそのまま振り分けます。 無効の場合、アクセスするクライアントの送信元 IP アドレスは Equalizer のインターフェースに NAT されサーバに振り分けが行なわれます。 詳細は 4-1-6 を参照して下さい。

4-5-1-2 “Probes”

[4-4-1-2](#) と同様の設定になります、そちらのセクションをご参照下さい。

4-5-1-3 “Persistence”

セッション維持の動作設定を行います。 L7クラスタに於けるセッション維持動作については APPENDIX A をご参照下さい。

cluster parameters

cookie age

cookie scheme

cookie generation

cookie domain

cookie path

persist

always

項目	内容
cookie age	Equalizer のセッション維持用 Cookie の有効期限を秒で指定します。 有効時間を過ぎたセッション維持用 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 scheme	cookie scheme は 0~2 の値で設定し、クラスタで使用されるセッション維持用 cookie のフォーマットを指定します(通常はデフォルトの 2 で問題ありません)。

	<p>0 = cookie にはクラスタの IP アドレスおよびポート番号、またサーバの IP アドレスおよびポート番号が保存されます。</p> <p>1 = cookie にはクラスタの IP アドレス、またサーバの IP アドレスおよびポート番号が保存されます。</p> <p>2 = cookie にはクラスタの IP アドレス、またサーバの IP アドレスが保存されます。</p>
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。
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 セッション維持用 cookie の付与を行いません。 (例えば www.coyotepoint.com や my.coyotepoint.com)。
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 セッション維持用 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セッション維持用 cookie がブラウザに保存されます。http://www.hogehoge.com/goods/information.html ではセッション維持用 cookie はブラウザに保存されません)
persist	Cookie を使用したサーバセッション維持を行なう際に有効にします。
always	無効の場合、サーバが set cookie を行ったかを確認し、行っていればセッション維持用 Cookie を Equalizer も付与し、行っていないければ Equalizer はセッション維持用 Cookie を付与しません。 有効の場合は、必ずセッション維持用 Cookie を付与します。

4-5-1-4 “LB Policy”

[4-4-1-4](#)と同様の設定になります、そちらのセクションをご参照下さい。

4-5-1-5 “Networking”

L7クラスタ固有のタイムアウト値などの設定を行います。

cluster parameters

send buffer	<input type="text" value="32"/>
receive buffer	<input type="text" value="16"/>
request max	<input type="text" value="32"/>
response max	<input type="text" value="32"/>
custom header	<input type="text"/>
connect timeout	<input type="text" value="10.0"/>
client timeout	<input type="text" value="5.0"/>
server timeout	<input type="text" value="60.0"/>
abort server	<input type="checkbox"/> (inherit from global: <input checked="" type="checkbox"/>)
once only	<input type="checkbox"/>
insert client IP	<input type="checkbox"/>

項目	内容
send buffer	ネットワークインターフェースから送信される直前のデータが L7プロキシ処理を行う為に確保するメモリ領域をキロバイトで設定する値になります。
receive buffer	ネットワークインターフェースに受信されているデータを L7プロキシ処理する為に確保するメモリ領域をキロバイトで設定する値になります。
request max	キロバイトでの最大 HTTP リクエストヘッダの取得サイズになります。
response max	キロバイトでの最大 HTTP レスポンスヘッダの取得サイズになります。
custom header	Equalizer で受け付けるリクエストに対して、カスタムの HTTP ヘッダを挿入します。
connect timeout	接続要求に対してサーバ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。
client timeout	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。
server timeout	Equalizer がサーバ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。
abort server	クローズする際にサーバに対し不意に接続を落とします。
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。
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。詳細については 4-1-6-5 を参照して下さい。

4-5-2 “Servers” タブ

4-4-2 と同様の設定になりますので、そちらのセクションをご参照下さい。

4-5-3 “Match Rules” タブ

L7ヘッダを確認し振り分けを行なう Match Rules を使用する際にはこちらから設定します。詳細は [セクション6](#) をご確認ください。

4-5-4 “Reporting” タブ

[4-4-4](#) と同様の設定になります。Statistics にある time since last activity は最後にクラスタへ通信が行われてからの秒数が表示されます。

4-6 L7/HTTPS クラスタパラメータ設定

Configuration	Security	Servers	Match Rules	Smart Events	Reporting
Required	Probes	Persistence	LB Policy	Networking	

SSL 通信を Equalizer で終端させる場合は、L7/HTTPS クラスタを作成します。作成手順については 4-3-3 をご参照下さい。また、基本的な設定内容は L7/HTTP クラスタと同じですので、このセクションでは L7/HTTPS にのみ存在するパラメータについて説明します。

L7/HTTPS クラスタ作成後は、下記のようなエラーが表示されます。

SSL certificate warning
This HTTPS cluster will not function until a certificate is installed. Please select the Security tab to install a certificate.

これは L7/HTTPS クラスタはサーバ証明書をインストールしないと使用できないため、4-6-1 の手順でサーバ証明書をインストールすることで表示されなくなります。

4-6-1 “Security> Certificates”

SSL サーバ(クライアント)証明書のインストール・更新を行い、インストールした証明書の内容を確認することが出来ます。CSR 作成手順につきましては [APPENDIX B](#) をご参照下さい。

- store private key material in XCEL hardware
 XCEL- I カードを使用している場合、証明書情報をカード内部に格納することが出来ます。こうすることで Equalizer のコンソールからも証明書の情報を確認することが出来なくなり、セキュリティレベルが向上します。

この設定は XCEL カードを搭載した SI シリーズにのみ表示されます。

- select client or cluster certificate
 インストールする証明書がサーバ証明書であれば cluster、クライアント証明書であれば client を選択します。
- select SSL certificate file
 インストールする証明書を選択し、決定します。

upload を選択し決定すると、選択された証明書の内容が表示されます。サーバ証明書にパスワードが設定されている場合には、右図のよ



うにパスフレーズ入力画面が表示されます。

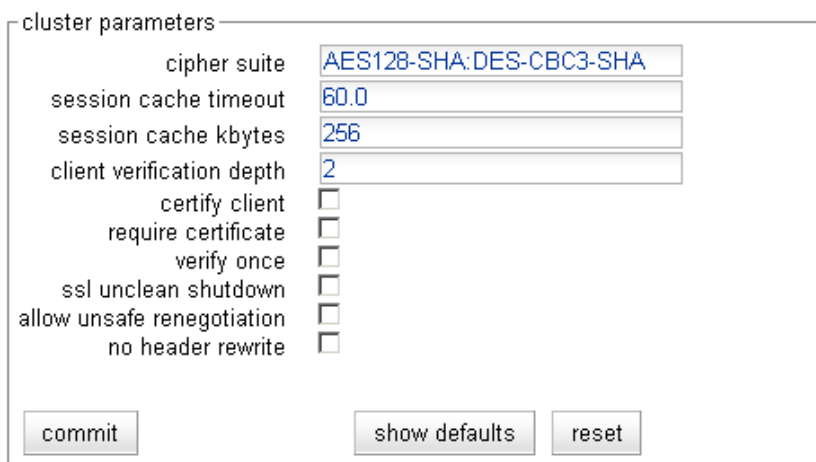
サーバ証明書の内容は下記のように表示されます。下の例ではサーバ証明書と中間証明書が組み込まれた Composite ファイルなので、2つの証明書情報が記載されております。選択したいサーバ証明書であると確認後、 **continue** を押して決定します。



画面が更新され、サーバ証明書の内容が表示されることを確認します。

4-6-2 “Security > SSL”

SSL 関連の設定はこちらから行います。各パラメータの詳細については下記をご確認ください。



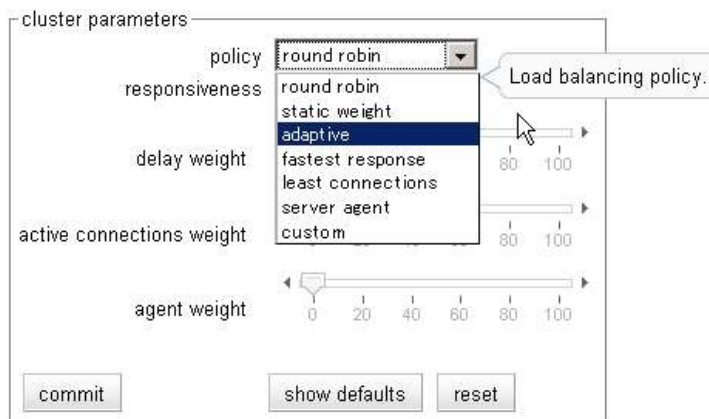
項目	内容
cipher suite	L7 HTTPS クラスタの設定値で、サーバによって提供される cipher suite を制限します。XCEL カードが認識された時、XCEL カードで

	アクセラレートされるデフォルトの cipher suite が設定されます。
session cache timeout	SSL セッションキャッシュで確保された領域を破棄する設定秒数になります。
session cache kbyte	SSL セッションキャッシュで領域確保されるキロバイトでの最大値になります。
client verification depth	L7 HTTPS クラスタの設定値で、例えば、デフォルトの 2 という数値はクライアント証明(Level 0)と2階層上(Level 1、Level 2)を確認します。Level 2 より大きい証明パスは無視されます。
certify client	クライアントのリクエストを Equalizer が受けた際にクライアント証明書をサーバに代わって確認するか否かの設定項目になります
require certificate	クライアントのリクエストを Equalizer が受けた際にクライアント証明書を Equalizer が要求するか否かの設定になります。
verify once	たとえ SSL で再認証されたとしても、Equalizer はクライアントの最初のリクエストのみ証明確認します。
ssl unclean shutdown	L7 HTTPS クラスタの設定値で、HTTP/1.1 での HTTPS 接続維持を行う際にエラーが表示される場合にはチェックを付けてお試し下さい。この問題は Internet Explore と Apache サーバとの接続時に依存する問題で、通常断続的に起きるようです。
allow unsafe renegotiation	HTTPS クラスタでは SSL renegotiation 機能はデフォルトで無効になっています。この設定を有効にすることで、SSL renegotiation を行うことが可能になります(セキュリティの観点から無効にしておくことが推奨されています)。
no header rewrite	サーバからクライアントへのレスポンスをそのまま通す設定になります。通例 Equalizer の L7 HTTPS クラスタの設定を行うと、その所属サーバの待ち受けポートは HTTP として処理されます。Equalizer はクライアントと SSL で通信していますので、仮にサーバが Location: header を使用し HTTP リダイレクトを送信すると、この URL は https: が含まれないプロトコルとなります。Equalizer はそれが HTTPS になるようにサーバからのレスポンドを自動で書き換えますが、この書き換えを Equalizer に行わせたくない場合に、この項目にチェックを付けて有効にします。

4-7 L4/L7 クラスタ共通パラメータ詳細

4-7-1 “Configuration > Require > Policy”

クラスタ負荷分散アルゴリズムの設定を行います。ポリシー設定は各クラスタ個別で行ないます。各アルゴリズムの内容は下記をご確認下さい。



項目	内容
round robin	Equalizer 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の登録順に上から順に振り分けが行われ、最後のサーバまで振り分けが行われると最初の登録サーバに戻って通信を処理します。サーバが Down した場合にはそのサーバを負荷分散サーバのリストから除外して負荷分散処理を継続します。 round robin はサーバの 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 weight	各サーバ個別に設定された 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 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を判断します。 <ul style="list-style-type: none"> Server response time サーバからの応答時間です。 Active connection count サーバに振られているアクティブ接続数です。 Server agent value サーバで起動しているサーバエージェントデーモンによって返される数値です
fastest response	サーバのレスポンス時間がもっとも短いサーバに対して高い確率で負荷分

	<p>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に振ってしまうと、そのサーバの負荷が一度に上がってサーバ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に振らない事があります。</p>
least connections	<p>サーバのアクティブ接続数がもっとも少ないサーバ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のアクティブ接続数やサーバ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への接続振り分けを最適化しています。</p>
server agent	<p>サーバエージェント値のもっとも低いサーバ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>サーバのレスポンス時間、サーバのアクティブ接続数、サーバエージェント値の3点をカスタマイズ設定することが可能です。</p>

サーバエージェントの利用について

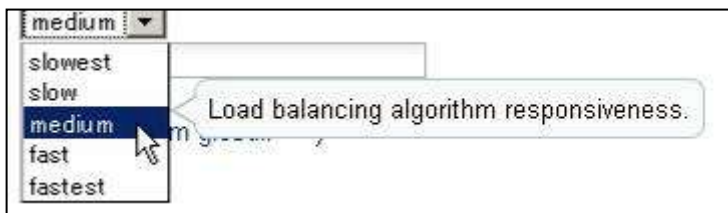
サーバエージェントはサーバのパフォーマンスの統計情報を収集します。サーバエージェントを使用する設定をクラスタに行った場合、Equalizer は定期的にサーバエージェントデーモンが起動しているクラスタ所属サーバにアクセスしてパフォーマンス統計情報を収集します。

また、サーバエージェントをカスタマイズしてサーバリソースをサーバエージェントへ通知させる仕組みを作ることで、Equalizer はデータベースやその他のサーバリソースが提供状況にない場合にサーバに対してリクエストを振り分けしなくなります。

備考：負荷分散アルゴリズムを server agent に設定した場合には、各クラスタ所属サーバはサーバエージェントデーモンがパフォーマンス統計情報を収集する為、起動している必要があります。もし負荷分散アルゴリズムを server agent に設定し、クラスタ所属サーバにサーバエージェントデーモンが起動していない場合でクラスタパラメータの pedantic agent が無効の状態であれば、Equalizer はサーバエージェントデーモンが返す数値無しで負荷分散を行います。pedantic

agent が有効の場合で、サーバエージェントデーモンがサーバで起動していない場合にはそのサーバは DOWN 判定を受けます。

4-7-2 “Configuration > Require > Responsiveness”



responsiveness の設定は Equalizer がサーバの動的 weight 値をどのくらい頻繁に調整するかの設定になります。Equalizer は slowest、slow、medium、fast、fastest の 5 つのレスポンス設定を提供しています。このレスポンス設定は adaptive、least connections、fastest response 負荷分散アルゴリズムを使用する際に影響を与えます。

動的 weight 値による負荷分散

クラスタ内の各サーバの静的 weight 値を適切に設定した後に Equalizer が各サーバの動的 weight 値を調整していない事があります。つまり負荷が高いのにも関わらず動的 weight 値に変化が無い場合ですが、このような場合にはクラスタのレスポンスのパラメータを fast へ変更します。Equalizer はサーバのパフォーマンスを最適化します。これにより、クラスタワイドのパフォーマンスの改善が図られるでしょう。

Dynamic Weight Oscillations

特定サーバの動的 weight 値が振幅している場合(例えば、動的 weight 値が 100[デフォルトの静的 weight 値]を基準にした時に時間軸に対して振幅が上下に激しい場合など)には、クラスタのレスポンスを slow へ変更します。同時にサーバのアプリケーションが不適切な動作をしていないか確認を行います。

4-7-3 “Configuration > Probes > ACV probe / response”

コンテンツレベルでサーバのヘルスチェックを行なう場合に設定を行います。

probe port	443
ACV probe	GET /equalizer/check.html HTTP
ACV response	Server OK
probe delay	10.0

ACV は各クラスタ個別で設定されます。ACV が設定された状態では、HTTP リクエストをサーバ

に対して行い、応答される文字列によってサーバ状態を確認しています。

テキストベースでのリクエスト/レスポンスに対応するプロトコルで ACV 設定が可能です。ただし L4/UDP クラスタでは ACV の設定は出来ません。

設定項目は2箇所です。

4-7-3-1 “ACV probe”

■L4 クラスタの場合： GET /<URL Path> HTTP/1.0(1.1)¥r¥nHost: <hostname>¥r¥n¥r¥n と設定します。

例) GET /index.htm HTTP/1.1¥r¥nHost: www.coyotepoint.com¥r¥n¥r¥n

L4 クラスタでは設定されるサービスが HTTP とは限らない為、改行コードが必要になります。また、サーバによってこの改行コードが当てはまらない場合がありますので、サーバ側の設定をご確認下さい。

■L7 クラスタの場合： GET /<URL path> HTTP/1.0(1.1)¥r¥nHost: <hostname> と設定します。

例) GET /index.html HTTP/1.1¥r¥nHost: www.networld.co.jp

(最後の「¥r¥n¥r¥n」のような改行コードは必要ありません。自動で入力されます。ただし、サーバによって自動で付加される改行コードが当てはまらない場合がありますので、サーバ側の設定をご確認下さい。)

4-7-3-2 “ACV response”

サーバからあるべき応答の文字列を指定します。ACV string で取得するファイルの先頭 1024 バイト目までを確認しますので、ACV response で指定する文字列は必ずこの 1024 バイトに含まれている必要があります。


[例] welcome

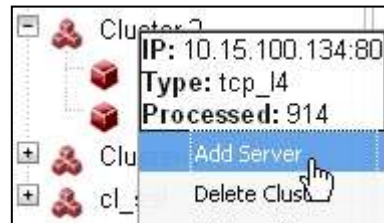
4-8 サーバ設定

クラスタ設定後、サーバを追加します。

4-8-1 サーバ作成

左メニューから新規サーバを所属させるクラスタ上で右クリックすると、メニューが表示されますので“Add Server”を選択するとサーバ作成ウィザードが表示されます。

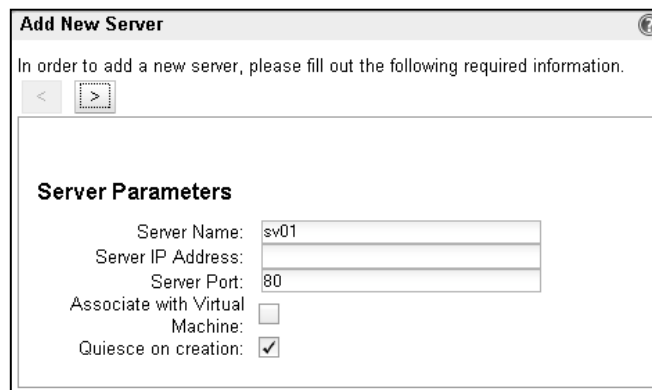
同様のことを [4-4-3](#) のサーバー一覧画面から行なうことができます。サーバテーブルから  を選択します。



4-8-2 サーバ作成ウィザードの入力

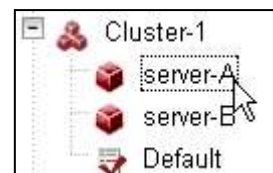
サーバ作成ウィザードにサーバ情報を入力します。

- Server Name
 - サーバの名称設定です、アルファベットから始まる必要があります。
- Server IP Address
 - サーバの IP アドレスを入力します。
- Server Port
 - サーバのサービス受付ポート設定です。デフォルトではクラスタのポート番号が自動で設定されますが、クラスタの受け付けポートとは別に任意の番号へ変更することが可能です([4-1-7](#)を参照下さい)。
- Associate with Virtual Machine:
 - VLB 機能を有効にしたクラスタに、仮想サーバを追加する場合チェックを入れます。
- Quiesce on creation
 - サーバ作成後すぐに負荷分散が行われることを防ぐため、サーバ作成時には Quiesce が有効になっています。必要ない場合はチェックをはずし無効にします。



4-8-3 サーバ パラメータ設定変更

左フレームのリストからサーバを選択することで、詳細情報を確認することができます(右図)。



4-8-4 Configuration タブ設定

Configuration	Reporting
Required	Outbound NAT

4-8-4-1 “Required”

Server parameters

VLAN	1: Default
ip	10.15.100.60
port	80
probe port	0
max connections	0
initial weight	100
strict max cx	<input checked="" type="checkbox"/>
hot spare	<input type="checkbox"/>
quiesce	<input type="checkbox"/>
dont probe	<input type="checkbox"/>
dont persist	<input type="checkbox"/>

commit show defaults reset

サーバの基本パラメータ設定を行います。

注意： Server Name については変更することが出来ません

項目	内容
VLAN	サーバに設定された IP アドレスから、所属する VLAN を判別し表示します。リストから VLAN を選択し手動で変更することも可能です。E250GX では表示されません。
ip	サーバの IP アドレスを入力します。
port	サーバのポート番号を入力します。
probe port	ヘルスチェックを行なうポート番号を別途指定する場合は設定します。デフォルトは 0 と表示され、この場合はサーバのポート番号を使用します。
max connections	サーバに振り分ける最大同時接続数を設定します。詳細は 4-8-5 を参照下さい。
Initial weight	サーバの初期 Weight 値を設定します。設定範囲は 20 ~ 200 です。例えば、サーバ2台を 50:100 の割合にした場合はおよそ 1:2 の割合でリクエストが割り振られます。

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
hotspare	<p>バックアップサーバや Sorry サーバとして使用する際に有効にします。詳細は 4-8-6 を参照下さい。</p>
quiesce	<p>メンテナンス時などサーバを使用停止する際に、クライアントからのコネクションを維持しながら行なう際に使用します。詳細については 4-8-7 を参照下さい。</p>
dont probe	<p>サーバに対して TCP ハンドシェイク(および ACV)によるヘルスチェックを行わない場合は、この設定を有効にします。詳細は 4-8-8 を参照下さい。</p>
dont persist	<p>サーバ個別に対してセッション維持を無効にする場合は、この設定を有効にします。詳細は 4-8-9 を参照下さい。</p>

4-8-4-2 “Outbound NAT”

Configuration	Reporting
Required	Outbound NAT

Outbound NAT 機能([3-1-4-2](#) を参照)の詳細設定を行います。デフォルトでは Equalizer の Default VLAN IP アドレスに NAT されますが(E250GX の場合は External 側リアル IP アドレス)、本設定を行うことで NAT する IP アドレスをクラスタ IP アドレスなどに設定が可能になります。本設定を使用するには、事前にグローバル設定で Outbound NAT が有効になっている必要があります。設定方法は [3-1-4](#) をご参照下さい。

本設定を行う理由として、以下のようなケースがあります。

- ・ 冗長化構成時に、Equalizer の Failover が発生すると Outbound NAT 時に使用される IP アドレスも併せて変更されるため、一意の IP アドレスに NAT することが出来ない。Failover Alias に NAT させることで、どちらの機器が Primary 役であっても同一 IP アドレスで外部へアクセスすることが出来る。

- ・ アプリケーションの仕様上、サーバからクライアントへ通信を行う必要があるが、通常の Outbound NAT ではクラスタ IP アドレスとは異なってしまいうため、クライアントと正常に通信ができない。クラスタ IP アドレスに NAT させることで、サーバからクライアントへの通信を、サービスとして提供している IP アドレスから行うことができる。

参考： 同一 IP アドレスのサーバが、複数クラスタに所属している場合は、最後に変更された設定が適用されます（最後に更新された時点で、別クラスタに所属する同一 IP アドレスのサーバが自動的に Default address に変更されます）。

Default address
This option will set the outbound NAT address to the Default setting. This means that if this server's outbound NAT option is not set explicitly in another cluster, the Equalizer's address will be used. If it is set explicitly in another cluster, that address (either Failover or Cluster) will be used.

Equalizer address
This option will set the outbound NAT address for this server (in this and all other clusters) to use the Equalizer's administrative IP address as the source address for outbound traffic.

Failover address
This option will set the outbound NAT address for this server (in this and all other clusters) to use the Failover IP address as the source address for outbound traffic.

Cluster c100-144's address
This option will set the outbound NAT address for this server (in this and all other clusters) to use the IP address of this cluster. This means that if this server (a server with the same IP address) exists in another cluster, that server's Outbound NAT option will be reset to use this address.

項目	内容
Default address	<p>通常の Outbound NAT と同様、Equalizer の External 側 IP アドレスに NAT します。冗長化している環境では、Primary 役として動作している機器の IP アドレスに NAT されます。</p> <p>同一 IP アドレスのサーバが別クラスタに存在し、Default address 以外の設定であった場合は、その設定が優先されます。（デフォルトでこの設定が有効になっています）</p>
Equalizer address	<p>動作としては Default address と同様です。一度 Default address から設定変更を行い、それから再度 Default address の状態に戻すために使用します。そのサーバが1クラスタにのみ設定されている場合は Default address に設定し直せば問題ありませんが、サーバが複数のクラスタにまたがっている場合は明示的に Equalizer address を指定する必要があります。</p>
Failover address	External 側の Failover Alias として設定されている IP アドレスを使用

	<p>します。設定方法については 5-3-4-1 をご参照下さい。この設定は冗長化構成の時のみ設定可能です。</p>
Cluster [クラスタ名]'s address	<p>サーバが所属するクラスタ IP アドレスを使用します。</p> <p>L4クラスタ使用時に受付ポート番号の範囲指定を行なった場合は、サーバが使用する送信元ポート番号がクラスタの受付ポート番号の範囲外である必要があります。ポート番号が重複した場合、正常に通信ができなくなります。</p>

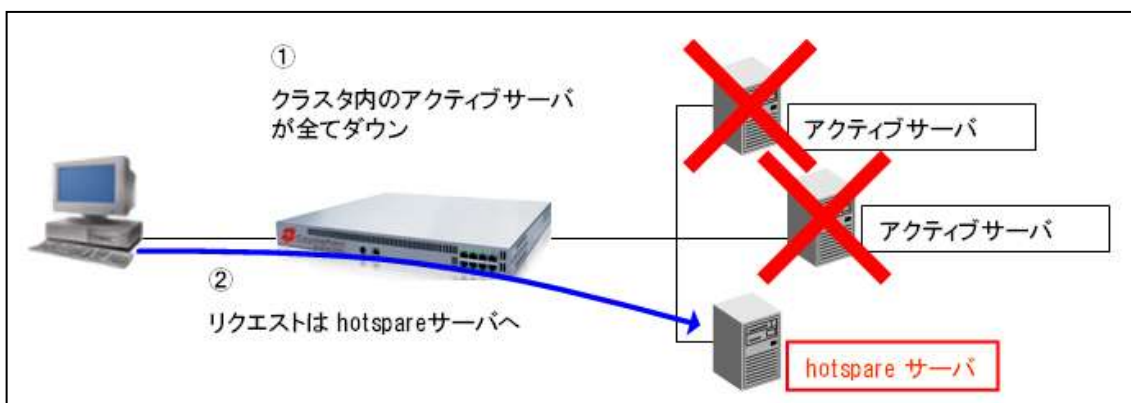
4-8-5 “max connection” 設定

各サーバが同時に受け付けることが出来るアクティブコネクション数の上限を設定します、これは L4/ L7 クラスタに設定可能なパラメータです。上限を超えたコネクションリクエストが行なわれた場合、そのサーバへの振り分けは行なわれず、クラスタ内の他サーバに割り振られます。

クラスタに hotspare サーバを設定、または Match Rules 内に Responders を設定することで、振り分け先サーバ全てが max connection に達した場合に、リクエストを hotspare サーバや Responders に処理させる事が可能です。例えば「現在混み合っております」などの HTML ページを表示することが可能になります。

4-8-6 “hotspare” 設定

バックアップサーバや sorry サーバを設定する際に使用します。hotspare に設定したサーバに対しては通常リクエストが振り分けられることはありませんが、クラスタ内のアクティブなサーバが全てダウンと判定された場合に hotspare サーバへの振り分けが開始されます。



セッション維持された通信は hotspare サーバに対しても優先的に振り分けが行なわれます。例えば、アクティブサーバがダウンし hotspare へ振り分けられたクライアントは hotspare サーバとセッション維持を行ないます。この場合、アクティブサーバが復旧したとしてもセッション維持されたクライアントは hotspare サーバへ振り分けられてしまいます。この状況はサーバ個別にセッション維持を無効にすることで回避が可能です、詳細は 4-8-8 を参照下さい。

4-8-7 “quiesce” 設定

メンテナンス時などサーバを使用停止する際に、クライアントからの接続を維持しながら、緩やかにサーバへの接続を減少させる際に使用します。quiesce に設定されたサーバ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。接続が減少した後、サーバ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 設定されたサーバのみが存在し、その他アクティブなサーバが全てダウンしている状況に於いては、サービスの継続を優先させるため Equalizer は例外的に新規リクエストも quiesce サーバに振り分けを行いません。

セッション維持された通信については、Equalizer は quiesce サーバに対して振り分けを行いません。

4-8-8 “dont probe” 設定

サーバに対する Equalizer のヘルスチェックはデフォルトでクラスタ内の全サーバに対して行なわれています。クラスタ内特定サーバへのヘルスチェックを無効にする場合にこの設定を行います。この設定を有効にしても ICMP によるヘルスチェック(3-1-2 参照)は行なわれませんが、L4 レベル以上のヘルスチェック(ACV を含む)は行なわれません。

注意： ICMP によるヘルスチェックを無効にしている場合、サーバへのヘルスチェックが全て無効になってしまい、サーバのダウンを検知できなくなりますのでご注意ください。

4-8-9 “dont persist” 設定

セッション維持の設定はクラスタ単位で行なわれ、クラスタ所属のサーバ全てに対して有効になりますが、この設定を有効にすることでサーバ単位のセッション維持を無効にすることが可能です。

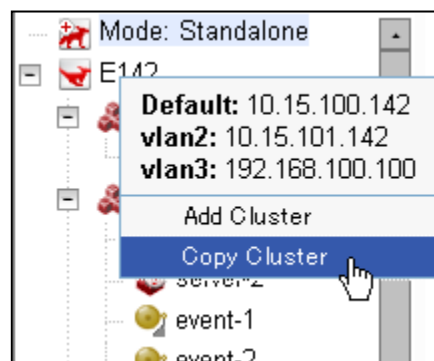
hot spare サーバを設定している場合にこの設定を使用することで、望まれないセッション維持を回避することが可能になります。

4-9 Copy Cluster 設定

既に設定されたクラスタをコピーすることで、より簡単にクラスタ追加を行うことが可能になります

Copy Cluster には以下の内容を設定する必要があります。

- ・ 新規作成するクラスタ名
- ・ クラスタの IP アドレス
- ・ クラスタのポート番号



4-9-1 クラスタタイプの違いについて

Copy Cluster を行うには、コピー元のクラスタとコピーされるクラスタの「クラスタタイプ」は同じである必要があります。「クラスタタイプ」はクラスタ作成時に選択するクラスタの種類です。例えば、L4/TCP クラスタをコピー元として Copy Cluster する場合には、新規作成するクラスタも L4/TCP である必要があります。仮に L4/TCP クラスタをコピー元として L7/HTTP クラスタを作成するなど、「クラスタタイプ」が異なる場合は、クラスタ設定値がすべてデフォルトに戻ります (Copy Cluster 時に設定した、クラスタ名・クラスタ IP アドレス・クラスタポート番号は反映されません)。

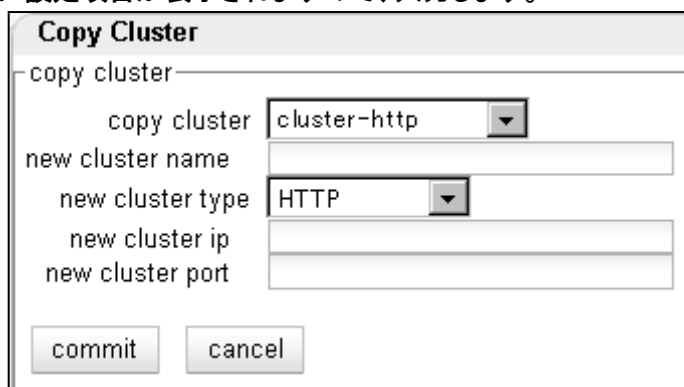
4-9-2 サーバ、Smart Events, Match Rules のコピーについて

Copy Cluster を行うと、コピー元クラスタに所属しているサーバ、Smart Events, Match Rules も同時にコピーされます。L7 クラスタから L4 クラスタにコピーした場合には、Match Rules 設定は削除されます。

4-9-3 Copy Cluster の実施

上図のように左メニューから Equalizer(冗長化構成時は機器の Equalizer Name)を右クリックするとメニューが表示されますので “Copy Cluster” をクリックします。

以下のように設定項目が表示されますので、入力します。



設定項目	内容
new cluster name	新規作成クラスタ名を設定します。
new cluster IP	新規作成クラスタの IP アドレスを設定します。
new cluster port	新規作成クラスタのポート番号を設定します。

セクション5 冗長化設定手順

Equalizer は全てのモデルにおいて冗長化(または Failover と呼ばれます)することが可能です。冗長化を行なうことでどちらかの機器に障害が発生した場合に於いてもサービスを継続させることが可能になります。

5-1 Failover 動作の基本概念について

Failover を組んでいる2台の Equalizer は Failover ペアと呼ばれ、役割としては以下の2種類どちらかになります。

- ・ デフォルト Primary 機
- ・ デフォルト Backup 機



上記のように Equalizer は Primary と呼ばれる機器がアクティブ機器として動作しサービスを行ないます。デフォルト Primary 機に障害が発生した場合は、デフォルト Backup 機が検知し、サービス提供を引き継ぎます。

補足: Failover 設定の注意点については TEC-World 内の FAQ でまとめていますのでご確認下さい。

5-2 Primary / Backup の関係について

Primary / Backup の関係について、以下の点にご注意頂く必要があります。

5-2-1 Primary”役”、 Backup”役” とは

5-1 のように、Failover ペアを組む2台の Equalizer は「デフォルト Primary 機」「デフォルト Backup 機」と設定されます。デフォルト Primary 機に障害が発生した場合、デフォルト Backup 機が Primary として動作しますが、この場合『デフォルト Backup 機が「Primary 役」として動作する』と表現します。

このようにデフォルト設定に関わらず Primary/Backup として動作している事は「役」と呼ばれます。運用中に**どちらの機器が実際の Primary として動作しているのか**については、各機器の「役」を確認する必要があります。下記表のような組み合わせになります。

■デフォルトの Primary/Backup 設定と、Primary/Backup 役の組み合わせ

パターン	デフォルト設定	Primary 役	Backup 役
1	デフォルト Primary	○	
	デフォルト Backup		○
2	デフォルト Primary		○
	デフォルト Backup	○	

5-2-2 切り戻し動作(Failback) について

Primary 役として動作している機器に障害が発生すると、Backup 役であった機器が Primary 役に切り替わり(Failover)、サービス提供を開始します。その後、Primary 役として動作していた機器が復旧した場合は、Primary 役としてではなく Backup 役として動作を開始します。

このように、一度切り替わり動作(Failover)が発生すると、Primary 役の機器が入れ替わり、その状態のまま引き続き運用が行われます。Equalizer では基本的に切り戻し動作(Failback)は行われませんが、障害パターンによっては切り戻りが発生します。詳細についてはヘルプデスクサポート TEC-World にある FAQ「Equalizer GX シリーズの Failover 動作について」をご確認下さい。

補足: Primary 役/Backup 役を意図的に入れ替えたい場合は、Primary 役として動作している機器を再起動させることで可能です。相手機器がないことを検知した Backup 役の Equalizer は Primary 役へ移行します。

5-2-3 冗長化の通信(sibling) について

Failover ペアの Equalizer 間では互いの生存確認を行う sibling と呼ばれる通信をネットワーク経由で行なっています。この通信によってペア同士は切り替わりなど Failover の状態確認を行います。

この通信は TCP/501 によって行なわれ、VLAN 単位で無効にしない限りは設定されている全ての VLAN 上で通信が発生します。ただし最初に設定される2つの VLAN では必ず Sibling が行われます。

注意: Equalizer の周辺ネットワークは sibling 通信が正常に行えるように設計する必要があります。Equalizer 上位・下位のスイッチは STP 機能をポート単位で OFF にするなど、必ず sibling 通信を妨げないようにして下さい。Equalizer がファイアウォールに直接接続されている場合なども、問題になるケースがございますので、十分にご注意下さい。

5-2-4 Gratuitous ARP について

Failover 動作が発生すると、Primary 役として動作を開始した Equalizer は以下の IP アドレスを自分の MAC アドレスを紐付けるために Gratuitous ARP を送出します。

- ・ クラスタ IP アドレス
- ・ 各 VLAN の Failover Alias IP アドレス
(E250GX の場合は External/Internal の Failover Alias IP アドレス)

Equalizer 同士、および周辺ネットワーク機器は上記の Gratuitous ARP を正常に受け取ることが出来る環境である必要があります。

5-2-5 Failover ペア同士のコンフィグ同期について

Failover ペアを組む Equalizer はコンフィグの同期を行ないません。

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・デフォルト Backup 機のどちらの設定を更新してもコンフィグ同期が実施されます。sequence 値の確認はセクション [2-1-3](#) を参照下さい。

同期対象となる設定項目については以下の通りです。

- ・ グローバル設定(Probe、Networking)
- ・ クラスタ設定
- ・ サーバ設定
- ・ Match Rules、Responders、Smart Events 設定
- ・ メール送付設定([3-3-1-3](#))

- ・ Handing 設定([3-3-1-2](#))
- ・ Logging 設定([3-3-1-1](#)) ※オプション設定で有効にする必要があります。
- ・ DNS サーバ設定 ※オプション設定で有効にする必要があります。
- ・ SSL サーバ証明書 ※オプション設定で有効にする必要があります。

同期対象ではないコンフィグは以下の通りです。

設定については Failover ペアを組んでいたとしても必ず両機器に設定する必要があります。

- ・ SNMP 設定
- ・ ログ情報
- ・ Sticky テーブル情報
- ・ Host 名
- ・ Domain 名
- ・ Default Gateway 設定
- ・ Equalizer IP アドレス
- ・ Time Zone/時刻/NTP サーバ設定

補足: コンフィグの同期はデフォルトで有効になっています、無効にするには [5-3-3](#) をご参照下さい。

5-2-6 Failover Alias について

Failover ペアを組む Equalizer は Failover Alias と呼ばれる IP アドレスを共有します。これは冗長構成にのみ使用する IP アドレスで、VLAN やインターフェースに設定されたリアル IP アドレスとは異なる IP アドレスを設定します。セクション [3-6-1](#) の VLAN configuration から行います。

通常、負荷分散対象サーバのデフォルトゲートウェイは Equalizer のリアル IP に設定しますが ([4-1-5](#))、冗長化構成の場合は Equalizer 2台それぞれにリアル IP アドレスが存在するため、2台の Equalizer が共有する Failover Alias IP アドレスに設定します。

Failover Alias IP アドレスは各 VLAN に設定し (E250GX では External/Internal に設定します)、リアル IP アドレスと同様に各 VLAN 間の通信を行なうゲートウェイアドレスとして動作します。

5-2-7 Failover 動作・制限について

Failover の動作や制限については、TEC-World FAQ(リンク)にて別途資料を掲載しています。検索ワード「failover」でダウンロードできます。

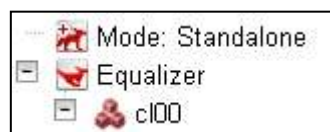
5-3 Failover 設定

Failover 設定は、2 台の機器情報を互い設定することで進めていきます。設定手順はいくつかありますが、本手順書ではウィザードを使用しない手順で説明します。

事前準備として、両機器には同じ数の VLAN を設定します。またその VLAN ID を同じ値に設定します。次に同じ VLAN 設定画面から、Failover Alias IP アドレス(画面上表示は "Failover IP")を設定します(Failover Alias IP アドレスは両機器で同じです)。

5-3-1 Failover 設定画面

左フレームの最上部に "Mode: Standalone" と表示されているアイコンがあります。Failover ペアとしてではなく、単体で動作している機器はこのように Standalone と表示されます。このアイコンを選択し、Failover 設定画面を表示します。



ペア登録される Equalizer は **Peer** と呼称され、各 Peer に対して Equalizer Name を設定します(管理上、機器ホスト名を Equalizer Name にすることを推奨します)。

5-3-2 "Required" タブ

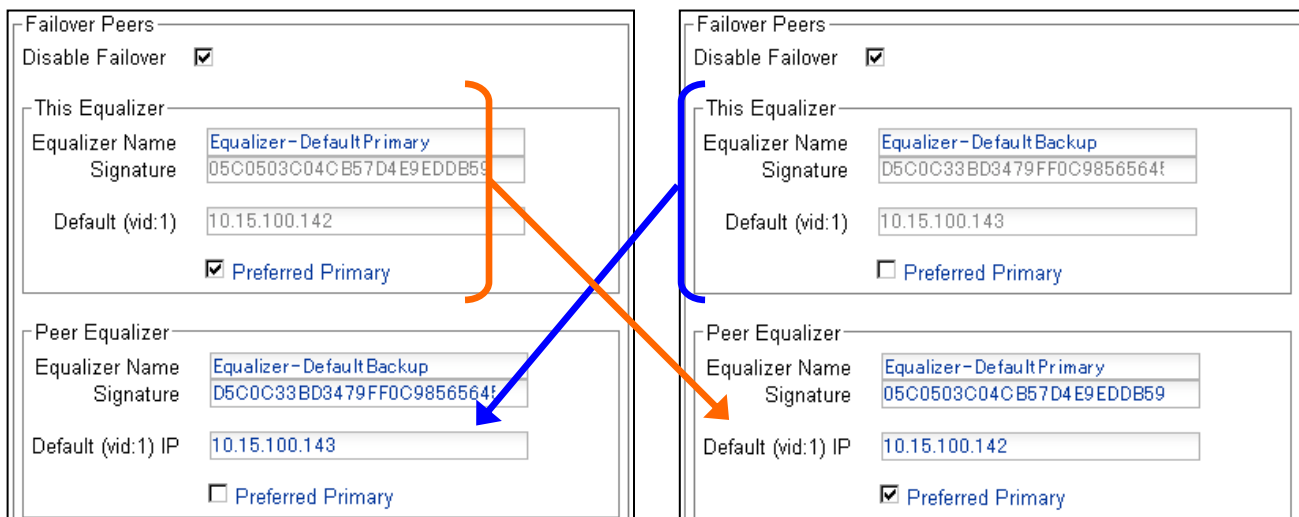
右図のように Peers タブが表示されます。このタブにペアとなる Equalizer 2 台を登録します。まず、両機器の Equalizer Name 設定、Signature 情報、VLAN IP アドレスをコピーします。併せて、デフォルト Primary として設定する側の設定で "Preferred Primary" のチェックを有効にします。Failover Alias IP アドレスは、VLAN 設定で記載されていれば自動的に反映されます。

<初期状態>

Required	Synchronization	Timing
<p>The failover configuration is currently disabled. To enable failover, you can either use the wizard or fill out the required information below on <i>both</i> Equalizers. Click Help for instructions.</p>		
<p>Failover Peers</p> <p>Disable Failover <input checked="" type="checkbox"/></p>		
<p>This Equalizer</p> <p>Equalizer Name <input type="text" value="eq_10.15.100.142"/></p> <p>Signature <input type="text" value="05C0503C04CB57D4E9EDDB59"/></p> <p>Default (vid:1) <input type="text" value="10.15.100.142"/></p> <p><input type="checkbox"/> Preferred Primary</p>		
<p>Peer Equalizer</p> <p>Equalizer Name <input type="text"/></p> <p>Signature <input type="text"/></p> <p>Default (vid:1) IP <input type="text"/></p> <p><input type="checkbox"/> Preferred Primary</p>		

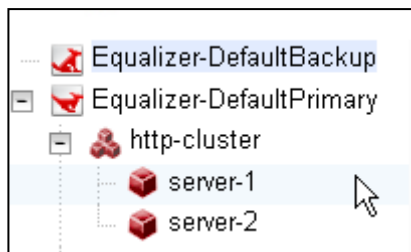
Required	Synchronization	Timing
<p>The failover configuration is currently disabled. To enable failover, you can either use the wizard or fill out the required information below on <i>both</i> Equalizers. Click Help for instructions.</p>		
<p>Failover Peers</p> <p>Disable Failover <input checked="" type="checkbox"/></p>		
<p>This Equalizer</p> <p>Equalizer Name <input type="text" value="eq_10.15.100.143"/></p> <p>Signature <input type="text" value="D5C0C33BD3479FF0C9856564f"/></p> <p>Default (vid:1) <input type="text" value="10.15.100.143"/></p> <p><input type="checkbox"/> Preferred Primary</p>		
<p>Peer Equalizer</p> <p>Equalizer Name <input type="text"/></p> <p>Signature <input type="text"/></p> <p>Default (vid:1) IP <input type="text"/></p> <p><input type="checkbox"/> Preferred Primary</p>		

<Peer 情報設定後>

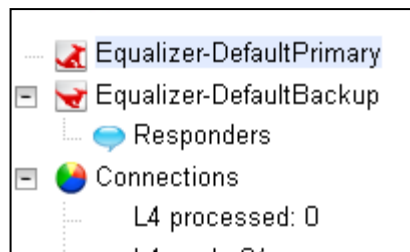


設定を入力後、画面下部の **Commit** ボタンを選択し設定反映を行ないます。この時点で以下のように左メニューの表示が変更され、設定した Equalizer Name が表示されるようになります。この時点ではコンフィグ同期は行なわれないため、コンフィグには差異があります。

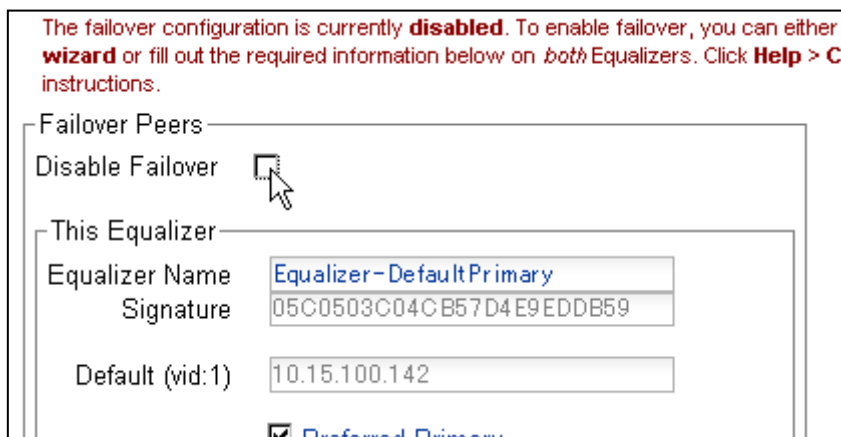
<デフォルト Primary 機器>



<デフォルト Backup 機器>



続いて Failover 設定画面で “Disable Failover” のチェックを外します。両機器でチェックを外してから、画面下部の **Commit** ボタンを選択します。



このタイミングで両機器間の冗長化が行なわれます。画面左上から Help > About を選択し表示される “Equalizer System Information” から failover mode を確認します。片側が Primary、もう 1 方が Backup になっていることを確認します。

<デフォルト Primary 機器>

failover mode	primary
sequence number	74
Envoy geographic load balancing	disabled
SSL acceleration	Xcel II
hardware GZIP compression	disabled
Virtualization Load Balancing	VLB Advanced

<デフォルト Backup 機器>

failover mode	backup
sequence number	74
Envoy geographic load balancing	disabled
SSL acceleration	Xcel II
hardware GZIP compression	disabled
Virtualization Load Balancing	VLB Advanced

上図のように Primary と Backup の状態であることを確認します。またコンフィグ同期で使用される sequence number が同一であることを確認します。

5-3-3 “Synchronization” タブ

冗長化された機器のコンフィグ同期設定を行なうことができます。

項目	内容
dont transfer	コンフィグ同期の有効・無効を設定します。チェックを入れるとコンフィグ同期が無効になります。
Transfer envoy configuration	Envoy 設定を同期します(E650GX のみ)
Transfer Certificates	L7/HTTPS クラスタのサーバ証明書情報を同期する場合には有効にします。
Transfer DNS Configuration	DNS 設定(eqadmin 上の Name Server 設定)を同期する場合には有効にします。
Transfer Syslog Configuration	Syslog 設定を同期する場合には有効にします。
Use SSL only	有効にするとコンフィグ同期の通信は SSL で暗号化されます。

5-3-4 “Timing” タブ

Sibling 通信のタイムアウト時間などを設定します。

項目	内容
receive timeout	sibling 通信に対する相手 Peer からの応答を待つタイムアウト時間です(秒)
connection timeout	ペアの sibling 通信に対するタイムアウト時間です(秒)。
probe interval	sibling 通信を行なう間隔です(秒)。

Backup 役**の機器**で、receive timeout または connection timeout のどちらかが発生した場合、1 回目の Strikeout として計算されます。この Strikeout が3回に達すると Backup 役は Primary 役へと切り替わり動作を行ないます。

※ E250si
E250GX
非対応

セクション6 Match Rules 設定手順

6-1 Match Rules とは

Match Rules を使用すると、L7/HTTP クラスタ ・ L7/HTTPS クラスタを使用した際にクライアントリクエストの HTTP ヘッダ情報を精査し、あらかじめ指定した条件にしたがってそのリクエストを特定のサーバに振り分けることが可能になります(振り分け先サーバは Match Rules 毎に設定することが可能です)。

HTTP ヘッダ情報まで確認を行いリクエストの振り分けを行うことで、より詳細な通信制御を行うことが可能になります。 また、条件にマッチした通信を特定のサーバに振り分けることで、セッション維持と同じ動作を実現させることも可能です。

Match Rules は E250si および E250GX を除く Equalizer の全モデルで使用することが可能です。

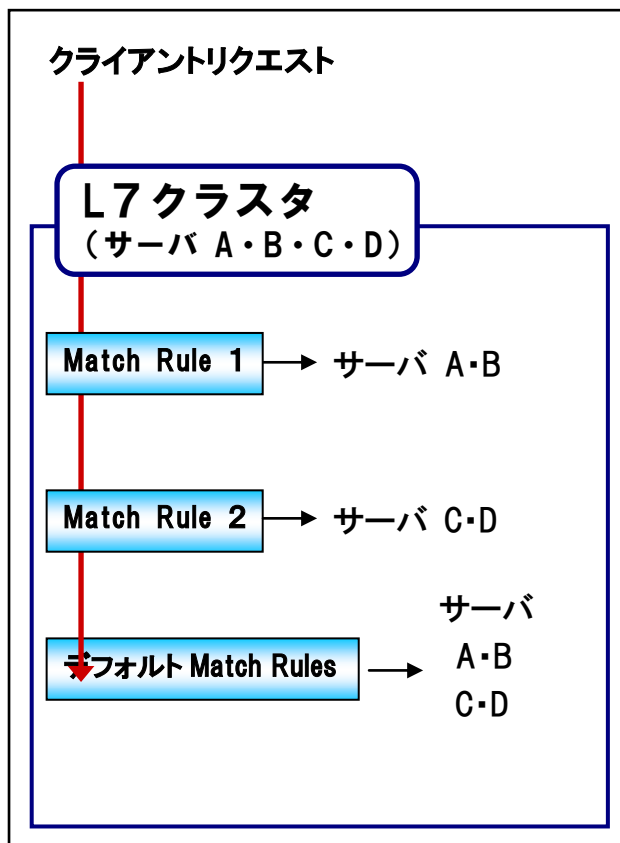
補足: HTTPS クラスタ使用時は、SSL 通信を復号化後に Match Rules の確認を行います。

6-2 Match Rules の動作

L7クラスタへのリクエストは、設定された全ての Match Rules に上位から順番に照合されます。 Match Rules の条件に適合した場合、リクエストは指定された振り分け先サーバに振り分けられます。

Match Rules は L7クラスタ毎に複数作成することが可能ですが、リクエストが設定した Match Rules に適合しなかった場合は、L7クラスタ作成時に自動的に生成される「デフォルト Match Rules」に適合します。 デフォルト Match Rules にはクラスタに所属している全てのサーバが振り分け先として設定されています。

Match Rules の設定可能数に上限は



ありませんが、Match Rules 動作には Equalizer の機器リソースを使用するため、可能な限りシンプルに設定することが推奨されています（CPU やメモリ消費が問題になる程の多量・複雑な Match Rules の作成はパフォーマンス低下を招く恐れがあります）。

振り分け先サーバを複数設定した場合、Match Rules 内部の負荷分散ポリシーに従って振り分けが行われます。セッション維持用 Cookie を保持したリクエストは、Match Rules 内でその Cookie に従って振り分けられます。

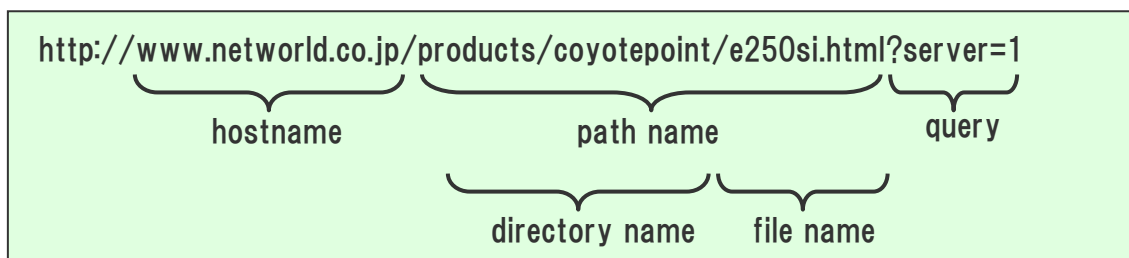
注意： Match Rules の振り分け先サーバが1つのみ設定されている場合、振り分け先サーバがダウンしても、条件に適合したリクエストはそのサーバに振り分けられます。

Match Rules に Responders を設定することで、振り分け先サーバが全てダウンしている場合に、Sorry ページ表示や HTTP リダイレクションを行うことが可能になります(Responders 設定は [6-4-6](#) ご参照下さい)。

6-3 Match Rules で精査可能な HTTP ヘッダ情報

Match Rules を使用し、大きく分けて以下の情報を精査することが可能です。

- URI 上に含まれる情報



- その他 HTTP ヘッダ情報

サポートされる HTTP ヘッダー一覧

Accept	From	Referer
Accept-Charset	Host	TE
Accept-Encoding	If-Match	Trailer
Accept-Language	If-Modified-Since	Transfer-Encoding

Authorization	If-None-Match	Upgrade
Cache-Control	If-Range	User-Agent
Connection	If-Unmodified-Since	Via
Content-Length	Max-Forwards	Warning
Cookie	Pragma	X-Forwarded-For
Date	Proxy-Authorization	
Expect	Range	

・ クライアントの送信元 IP アドレス

ホストアドレスやネットワーク範囲を指定することが可能です。

例) 10.10.2.245/32 , 10.10.2.0/24 など

・ SSL/TLS バージョン情報

HTTPS クラスタ使用時のみ使用可能になります。SSL や TLS のバージョンを確認することが可能です。


6-4 Match Rule 作成手順

6-4-1 Match Rule 作成ウィザードの起動

新規に Match Rule を作成するには作成ウィザードを起動します。作成ウィザードは以下2つの手順から起動できます。

1. 左フレームのクラスタアイコンから作成
Match Rule を作成するクラスタ上で右クリックし、メニューを表示します。メニューから "Add Match Rule" を選択します(右図)。



2. クラスタ内の Match Rules リストから作成
左フレームからクラスタを選択し、右フレームに表示されるタブから Match Rules を選択します。クラスタに設定されている Match Rules の一覧が表示されますので  ボタンを押します。



6-4-2 Match Rule 作成ウィザード入力

ウィザードが起動すると右図の画面が表示されます。以下パラメータを入力し、commit ボタンを押し決定します。

Match Name:

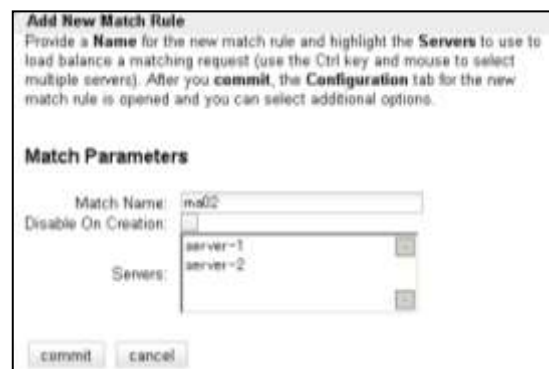
Match Rule の名称を入力します。
(後から変更することは出来ません)

Disable On Creation:

作成後すぐに動作することを防ぐためには、チェックを入れ Match Rule を無効にします。

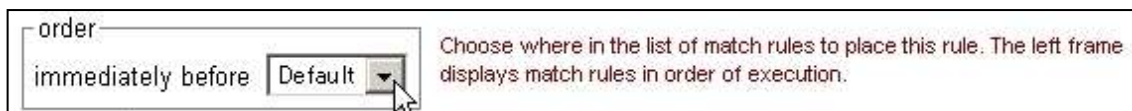
Servers:

作成する Match Rule に適合したリクエストの振り分け先サーバを選択します。複数サーバを選択するには、CTRL キー や SHIFT キーを同時に押しサーバを選択して下さい。サーバ名の色がハイライトされれば選択されています。(後から変更することが可能です)



作成が完了すると、新規 Match Rule の設定画面に自動的に移動します。

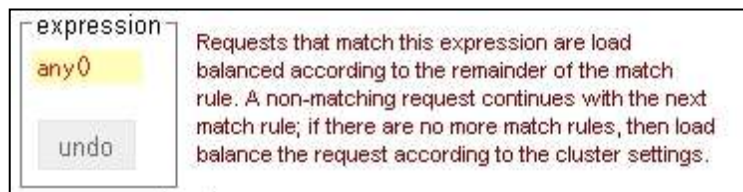
6-4-3 Match Rule の順番



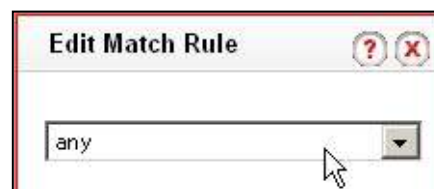
クラスタ内で Match Rule が照合される順番を指定します。“order” 枠内に表示されるタブから Match Rule を選択すると、選択した Match Rule の直前に配置されます。デフォルト Match Rule よりも後に配置することは出来ません。

6-4-4 expression の指定

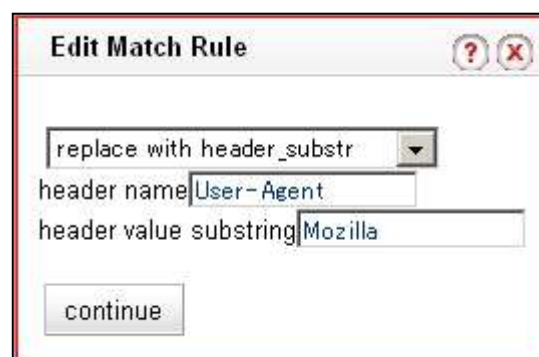
精査する HTTP ヘッダを指定します。デフォルトでは any() が設定されており、これは全てのリクエストに適合する事を意味します(デフォルト Match Rule と同様です)。



expression をクリックし、Edit Match Rule の画面を表示します(右図)。プルダウンメニューから精査するヘッダ情報を選択します。



選択したヘッダ情報に従って、照合する文字列を入力します。“replace with header_substr”を選択すると空欄が2つ表示されますので、1つ目にHTTPヘッダ名、2つ目に照合する文字列を入力します(右図)。



選択後、continue を選択します。

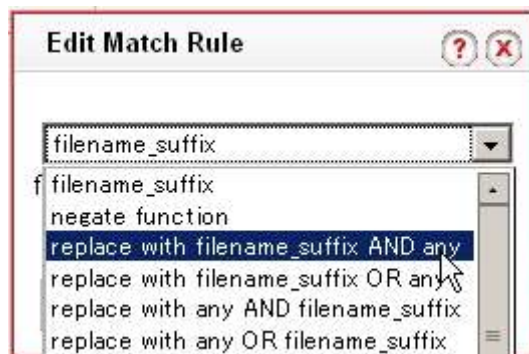
AND / OR 構文を使用し、1つの Match Rule 内で複数の情報を精査する場合は、以下の手順で行ってください。以下の例では、filename_suffix を選択後、User-Agent も確認し 2 つが同時に適合した場合に動作する Match Rule となります。

まず、先ほどの手順で expression を指定します。この例では、右図のように filename_suffix を使用し、ファイル名の後半部分が jpg である場合に適合する Match Rule を作成します。



次に expression をクリックし、再度 Edit Match Rule 画面を表示させます。

“replace with filename_suffix AND any” を選択し、continue を選択します。



再度 Match Rule 設定画面に戻り、右図のように2つの条件が AND によって連結されていること

を確認します。ここで any() をクリックし Edit Match Rule 画面を表示し、精査するヘッダ情報を選択します。

設定後、以下のように expression に2つの条件が記載されていることを確認します。

```
expression
( filename_suffix("jpg")
  AND header_substr("User-Agent", "Mozilla")
)
```

undo

```
expression
( filename_suffix("jpg")
  AND any()
)
```

undo

6-4-5 サーバオプション設定

servers and options

servers: server-1 (selected), server-2

policy: round robin

cookie age: 0

cookie domain:

cookie path:

disable:

spooof: (inherit from cluster:)

once only: (inherit from cluster:)

abort server: (inherit from cluster:)

persist: (inherit from cluster:)

insert client IP: (inherit from cluster:)

persist always: (inherit from cluster:)

項目	内容
servers	サーバ名をハイライトし、振り分けられるサーバを選択します。
policy	Match Rule 内で使用される負荷分散ポリシーを選択します。
cookie age cookie domain cookie path	セッション維持に使用する cookie のパラメータを、クラスタ設定とは別途設定する場合に入力します。空欄の場合はクラスタ設定が使用されます。
disable	Match Rule を無効にする(使用しない)場合に有効にします。Match Rule 設定時の動作テストなどにご利用下さい。
spooof once only abort server persist insert client IP persist always	各パラメータをクラスタ設定とは別途設定する場合に入力します。 “inherit from cluster” が有効になっている場合は、クラスタ設定が使用されます。

6-4-6 Responder 設定

responder response <input type="text" value="none"/>	Choose an existing Responder to handle matching requests when no servers are available. Click Responders in the left frame to add one.
---	--

振り分け先として設定されたサーバが全てダウンしていた場合、responder を設定することでクライアントのリクエストに対して Sorry ページ表示や HTTP リダイレクションを行うことができます。Responder 設定は [セクション7](#) を参照下さい。

上記設定を行い、画面最下部にある ボタンを押して Match Rule 作成は完了です。

6-5 Match Rules 動作確認方法

Match rules	Processed	Responder Hits	No Servers
ma01	0	0	0
Default	90	0	10

Match Rules に適合したセッション数は、Cluster Summary から確認できます。クラスタを選択し、表示される Match rules 名の “Processed” を確認して下さい。Match Rules 内の Responder 設定が使用された場合は “Responders Hits” がカウントされます。振り分けるサーバが存在しない場合は “No Servers” がカウントされます。

6-6 Match Rules 変更・削除方法

Match Rules の設定変更を行うには、左フレームから Match Rule を選択し、設定画面を表示します。設定変更後、画面最下部の ボタンを押して設定を更新します。

Match Rules を削除するには、左フレームから Match Rule を右クリックで選択し “Delete Match Rule” を選択するか、クラスタの Match Rules リストから該当 Match Rule に表示される ボタンをクリックします。

※ E250si
E250GX
非対応

セクション7 Responders 設定手順

7-1 Responders とは


Responders によって、以下2つの機能が提供されます。

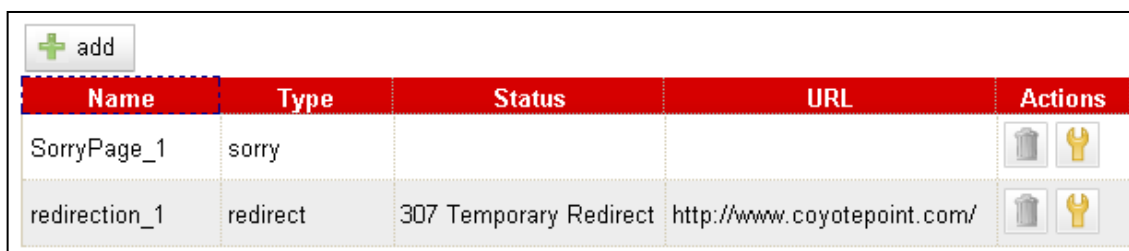
機能	内容
HTTP リダイレクト	アクセスするクライアントに対して HTTP のリダイレクトを行い、指定した URL へ通信を転送します。
Sorry ページ	Equalizer 上で Sorry ページを作成し、クライアントのリクエストに対して Sorry ページを表示します。ソースコードは 4096 バイト以下である必要があります。





Responders は Equalizer 上でグローバルに作成し、クラスタに所属する Match Rules に対して関連付けを行うことで設定します。通常 Match Rules に適用された通信は、所属するサーバに振り分けが行われますが、サーバが全てダウンしていた場合にのみ、設定された Responders が動作します。

各 Match Rules 個別に異なった Responders を設定可能なため、Match Rules の条件に合わせた Responders 設定が可能です。Responders は E250si および E250GX を除く Equalizer の全モデルで使用することが可能です。

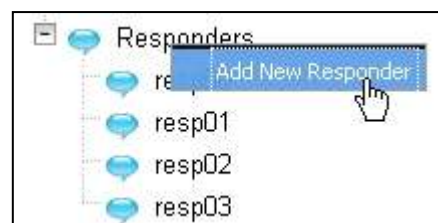
7-2 Responder 作成ウィザードの起動

Web 管理画面の左フレームから Responders をクリックすると、設定している Responders が一覧表示されます(下図)。  を押すと作成ウィザードが起動します。



Name	Type	Status	URL	Actions
SorryPage_1	sorry			 
redirection_1	redirect	307 Temporary Redirect	http://www.coyotepoint.com/	 

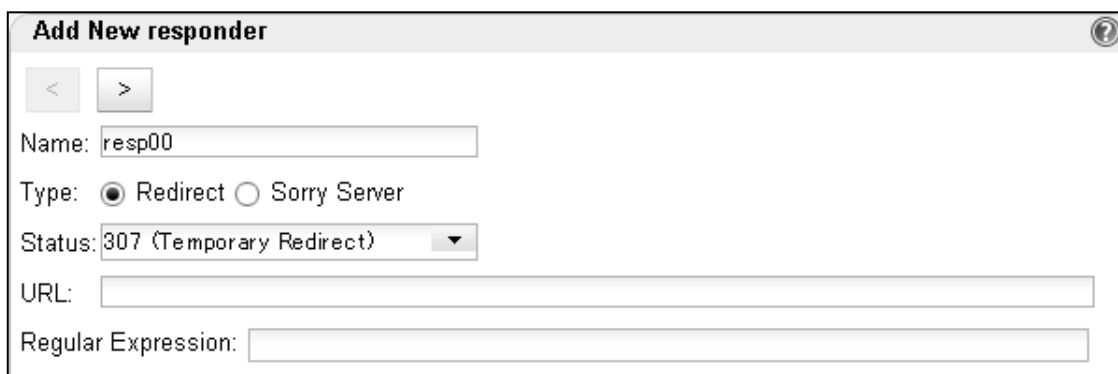
また、左フレームの Responders 上で右クリックすると Add New Responder が表示されますので、選択することでもウィザードを起動できます。



7-3 HTTP リダイレクション作成・設定方法




7-3-1 Responders 作成ウィザードの使用・パラメータ説明

Responder 作成ウィザードで Type から Redirect を選択します。



設定するパラメータは以下の通りです。

項目	内容
Name	Responders の名前を決定します。後から設定変更することは出来ません。
Type	“Redirect” または “Sorry Server” のどちらかを選択します。HTTP リダイレクション機能の場合は “Redirect” を選択します。
Status	HTTP リダイレクションを行う際に、Equalizer がクライアントに返す HTTP ステータスコードを選択します。以下の4つから選択可能です。 <ul style="list-style-type: none"> ・ 307 (Temporary Redirect) ※デフォルト ・ 301 (Moved Permanently) ・ 302 (Found) ・ 303 (See Other)
URL	クライアントのリクエストを転送する URL 先を指定します。 例) http://www.coyotepoint.com/
Regex	クライアントのリクエスト URL をいくつかの要素に分解し、指定した要素のみを変更し、転送する場合に使用します。
Test	上記 Regex 設定の設定を確認する際に使用します。テスト用の URL を入力し、画面下部の test ボタンを押すことで、その URL を要素に分解し表示します。

パラメータを入力後、画面下の  ボタンを選択し、次画面に進みます。 ボタンを使用すると指定 URL へのアクセスが可能です。ウィザード最後の画面で  ボタンを押し決定することで作成完了です。

7-3-2 Regex を使用したリダイレクション設定について

Regex 設定を行うことで、以下のような動作が可能になります。

- ・ ホスト名を変更しつつ、リクエスト URL のパラメータ(パス名など)は変更せず引き継ぎ、リダイレクションを行う。
- ・ リクエスト URL のホスト名や URL パラメータは変更せず引継ぎ、プロトコルのみを変更させる。
(例: <http://www.example.com> を <https://www.example.com> へリダイレクトする)
- ・ リクエスト URL のパラメータを部分的に変更し、リダイレクションを行う。
(例: www.example.com へのアクセスを www.example.co.jp へリダイレクトする)

上記設定を行うには、Regex 設定によって URL を各要素に分解することで行います。Regex の詳細な設定方法は別途英文マニュアルをご参照下さい。ここでは、リクエスト URL のパラメータを引き継ぎリダイレクションする設定を説明します。

リクエスト URL	http://www.example.com/product/loadbalancer/index.html
リダイレクト URL	http://www.networld.co.jp/product/loadbalancer/index.html

Regex 設定として、以下の文字列を入力します。

```
^(([^ :/?#]+):)?//(?:([^\r/?#.]+)?\.[^\r/?#.]+)?\.[^\r/?#.]+(?:/[^\r]+)?
```

同じ画面で をクリックし、以下の URL を設定します。

```
http://www.example.com/product/loadbalancer/index.html
```

Test ボタンを押すと、以下のようなメッセージがブラウザに表示されます。

Add New responder

< >

Redirect URL: <http://www.example.com/product/loadbalancer/index.html>

Regular Expression: `^(([^ :/?#]+):)?//(?:([^\r/?#.]+)?\.[^\r/?#.]+)?\.[^\r/?#.]+(?:/[^\r]+)?`

Test Expression: <http://www.example.com/index.html>

Match Components:

- \$0: "http://www.example.com/index.html"
- \$1: "http:"
- \$2: "http"
- \$3: "www"
- \$4: "example"
- \$5: "com"
- \$6: "/index.html"

Resulting redirect: <http://www.example.com/product/loadbalancer/index.html>

Test 設定として入力した URL が \$1、\$2 といった要素に分解されていることが確認できます。これらの要素を使用し、リダイレクト URL を入力します。

\$1//\$3.networld.co.jp\$6

実際の Responder 設定は以下のようになります。



7-4 Sorry ページ設定方法

Responders の Sorry ページ設定機能を使用することで、Equalizer が簡易的な Sorry ページを表示させることが可能になり、例えば Match Rules に設定されたサーバが全てダウンした場合、「サービスが一時的に停止しています」等のアナウンスを行うことが可能です。


Responder 作成ウィザード上で HTML コンテンツを入力することで、Sorry ページの作成が可能です。ウィザードを起動し、Type を “Sorry Server” に設定すると以下のような HTML 入力画面が表示されます。入力後、画面下部の test ボタンを押すことで、事前に HTML コンテンツを確認することが出来ます。



7-5 Match Rules への追加方法

作成した Responders を Match Rules へ登録する方法は [6-4-6](#) を参照下さい。

7-6 Responders 削除方法

Web 管理画面の左フレームから Responders をクリックし一覧表示されます。削除したい Responder の右に表示された  ボタンを押し、削除することが可能です。

また、左メニューから削除したい Responders を右クリックし Delete Responder をクリックします。



※ SIシリーズ
 ※ E250GX
 非対応

セクション8 Smart Events 設定手順

8-1 Smart Events とは

Smart Events は、L4/L7クラスタで使用できる機能で、Trigger と Action の組み合わせによって設定されます。Trigger で設定する条件が満たされた場合に、Action で設定された動作を行なうことで、その状況に対応することができます。


設定項目	内容
Trigger	Action を動作させる条件を設定します。例えば「アクティブサーバの台数が3台以下になった場合」などです。
Action	Trigger によって設定された条件が満たされた場合に、動作する内容を設定します。例えば「“Number of active servers are under 3” とログを出力する」などです。

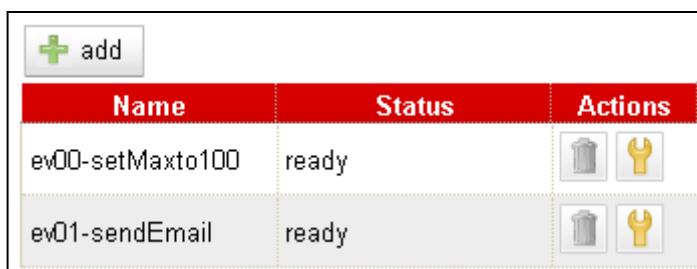
例えば、以下のような使用方法があります。





- ・ クラスタに所属するサーバ台数が残り1台になった場合、メールや Syslog トラップで管理者に通知を行なう。
- ・ アクティブコネクション数が一定数に達すると、サーバに設定された Quiesce を無効にする。

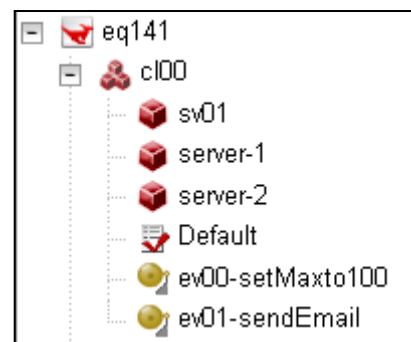
注意： Smart Events で設定可能な Trigger/Action には、VLB Advanced 機能と紐づいたものがあり、この Trigger/Action は VLB Advanced 機能がライセンスされている機器でのみ表示されます。

8-2 Smart Events 作成ウィザードの起動

該当クラスタを左メニューから選択し、表示されるタブから “Smart Events” をクリックするとクラスタに設定されている Smart Event が一覧表示されます(下図)。  を押すと作成ウィザードが起動します。



+ add		
Name	Status	Actions
ev00-setMaxto100	ready	 
ev01-sendEmail	ready	 

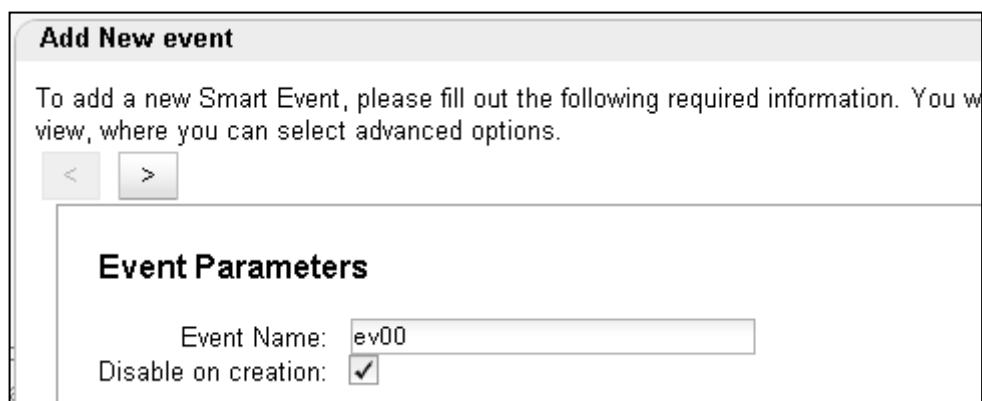


右図のように該当クラスタを右クリックし、表示されるメニューから “Add Event” を選択することも可能です。

8-3 Smart Events 作成・設定方法

8-3-1 Smart Events 作成ウィザードの使用・新規作成

Smart Events 作成ウィザードを起動すると以下の画面が表示されます。



Add New event

To add a new Smart Event, please fill out the following required information. You will then be taken to a detailed event view, where you can select advanced options.

< >

Event Parameters

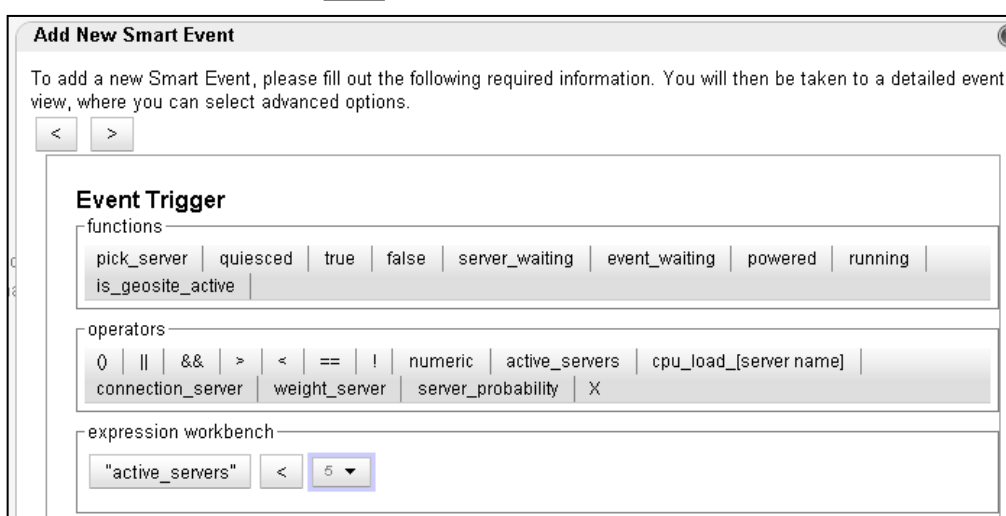
Event Name:

Disable on creation:

項目	内容
Event Name	Smart Event の名前を決定します。後から設定変更することは出来ません。
Disable on creation	新規作成後に Disable 状態にする場合はチェックします。設定後、すぐに通信に影響させない場合に使用します。

8-3-2 Smart Events 作成ウィザードの使用・Trigger / Action 設定

次の画面では Trigger を設定し、 を押すことで Action 設定画面に進みます。



Add New Smart Event

To add a new Smart Event, please fill out the following required information. You will then be taken to a detailed event view, where you can select advanced options.

< >

Event Trigger

functions

pick_server | quiesced | true | false | server_waiting | event_waiting | powered | running | is_geosite_active

operators

() | || | && | > | < | == | ! | numeric | active_servers | cpu_load_[server name] | connection_server | weight_server | server_probability | X

expression workbench

"active_servers" < 5

“functions” および “operators” から使用する項目を “expression workbench” へドラッグします。上記例では「アクティブサーバ数が5を下回った場合」の設定です。

operator で使用するパラメータは以下の通りです。

項目	内容
=, >, <	数値の等号、大なり、小なり をそれぞれ表します。
, &&, !	論理 OR、AND、NOT をそれぞれ表します。
()	複数の function や operator をグループ化します。
x	選択した function や operator を削除します。

設定後、確認画面で commit を押すと左メニューに Event が表示されます。

8-3-3 パラメータ設定

作成した Smart Event を左メニューから選択し、表示されるタブから Configuration > Required を選択することでパラメータ設定を行うことが可能です。

項目	内容
window time	この値はトリガー weight_server() によってのみ使用され、CPU 負荷の計算に使用されるサンプル数を設定します。 デフォルト値は5で、これは weight_server() がサーバ統計情報にある直近5つの動的 Weight 値を平均化した値を確認しています。 この値がトリガーによって算出される動的 Weight 値になります。
event timer	指定した Smart Event が実行される頻度を設定します(単位:秒)。デフォルト値は15秒で、これはグローバル設定の event interval(3-1-2 参照)と同様です。 この event timer と event interval 値をデフォルトに設定した場合、Smart Events は15秒間隔で実行されます。 event timer 値は event interval よりも高い値に設定されない限り実行頻度には影響ありません。 詳細は 8-6 を確認下さい。
event priority	作成した Smart Events を実行する優先順位を設定することができます。デフォルト値は0で、これは最も優先される設定です。 event priority 値が0で作成されると画面左フレームにある event priority 値0の Smart Events リストの最後に付け加えられ、表示されている順番で実行されます。event priority 値を変更することで左フレームの順番も変更されます。
disable	チェックを入れることで Smart Event を無効にします。

8-4 Trigger のイベントリスト

Trigger として設定可能な Event は以下の通りです。

Trigger 項目(変数)	内容
active_servers	クラスタに所属しているサーバの、アクティブ状態のサーバ数を返します。
connection_server(server)	ドロップダウンメニューから選択したサーバの、アクティブコネクション数を返します。
event_waiting(event)	ドロップダウンメニューから選択した Event が event_wait によって Blocked 状態になっているか確認します。Blocked 状態であれば値 “true”を返し、Blocked 状態でなければ値 “false”を返します。
false()	常に値 “false”を返します。
is_geosite_active(geocluster, geosite)	ジオサイトおよびジオクラスタが、アップ状態であれば値 “true”を返し、それ以外の状態であれば値 “false”を返します。ジオクラスタ名とジオサイト名はテキストボックスに入力する必要があります。
numeric(value)	数値を入力する際に使用します。
pick_server(1,2,3,4)	入力する数値(1~4)によって選択されるサーバが異なります。以下の4パターンがサポートされています。 1 = current weight が最も低いサーバ 2 = current weight が最も高いサーバ 3 = unquiesced されている current weight が最も低いサーバ 4 = unquiesced されている current weight が最も高いサーバ
quiesced(server)	ドロップダウンメニューから選択したサーバが quiesced になっているか確認します。quiesced であれば値 “true”を返し、quiesced でなければ値 “false”を返します。
server_probability(server)	ドロップダウンメニューから選択されたサーバに振り分けられているクラスタ通信の割合を返します。例えば、クラスタにサーバ4台が所属している構成において Round Robin により均等に負荷が振り分けられている場合には値 25 が返されます。
server_waiting(server)	ドロップダウンメニューから選択したサーバが server_wait によって Blocked 状態になっているか確認します。Blocked 状態であれば値 “true”を返し、Blocked 状態でなければ値 “false”を返します。
true()	常に値 “true”を返します。
weight_server(server)	ドロップダウンメニューから選択されたサーバの current weight を返します、この値は 0~200 になります。0の場合は新規リクエストが振り分けられないダウン状態となります。
cpu_load_server	選択した VMware のバーチャルマシンサーバが使用している CPU の割合を返します。この Trigger は VLB Advanced ライセンスがある場合にのみ使用できます。

powered(server)	選択した VMware のバーチャルマシンサーバがパワーオン状態である場合に値 “true” を返します。パワーオン状態でない場合は値 “false” を返します。
running(server)	選択した VMware のバーチャルマシンサーバがランニング状態である場合に値 “true” を返します。ランニング状態でない場合は値 “false” を返します。例えば、VMware が起動しているけれども BIOS 設定画面である場合はトリガー powered() は True を返しますがトリガー running() は False になります。

8-5 Action のイベントリスト

Action として設定可能な Event は以下の通りです。

Trigger 項目(変数)	内容
email (address, message)	指定メールアドレスにメッセージを送信します。メールアドレスのフォーマットは <i>user@domain</i> である必要があります(例: <i>joe@example.com</i>)。メール送信設定が有効になっている必要があります、詳細は 3-3-1-3 を参照下さい。
event_wait (event, seconds)	指定した Event を一定時間(秒)使用されないようにブロックするタイマーをセットします。常に値 “true” を返します。
false ()	常に値 “false” を返します。
ipmi_poweroff (BMC IP, BMC username, BMC password, lan)	Baseboard Management Controller (BMC) と Intelligent Platform Management Interface (IPMI) ドライバーが備わり設定が行われているサーバに対して、パワーオフの命令を送信します。詳細はメーカマニュアル P169 のセクション “Using IPMI to Power Servers On/Off” を参照下さい。
ipmi_poweron (BMC IP, BMC username, BMC password, lan)	Baseboard Management Controller (BMC) と Intelligent Platform Management Interface (IPMI) ドライバーが備わり設定が行われているサーバに対して、パワーオンの命令を送信します。詳細はメーカマニュアル P169 のセクション “Using IPMI to Power Servers On/Off” を参照下さい。
log (“message”)	指定されたメッセージをログに記載します。常に値 “true” を返します。
max_connection (server,max)	値 <i>server</i> で指定したサーバに対し、値 <i>max</i> で指定した最大同時接続数(max connection) を動的に設定します。この動作はサーバに設定されている max connection 値には影響しません。この動的な最大同時接続数の設定は、サーバ設定が変更されるとサーバ設定にリセットされます。
numeric (value)	数値の変数を設定します。矢印をクリックすることで数値を入力します。
pick_server (heuristic)	指定した値(数値)によってクラスタからサーバを指定します。 値:

	<p>1 = 最もcurrent weightが小さいサーバ</p> <p>2 = 最もhighest currentが大きいサーバ</p> <p>3 = quiesceが無効、かつ最もcurrent weightが小さいサーバ</p> <p>4 = quiesceが無効、かつ最もcurrent weightが大きいサーバ</p>
quiesce (server)	指定したサーバの quiesce 設定を有効にします。このEventによって quiesce が設定された場合は値 “true” を返します。設定されなかった場合は値 “false” を返します (例えば既に設定されていた場合など)
reboot_equalizer()	この reboot_equalizer() は 2 台の Equalizer が異なるゲートウェイを保持している状況における Failover 動作をサポートします。これはゲートウェイ IP アドレスに対してヘルスチェックやアクティブ状態のサーバ数を確認し、失敗した場合に機器を再起動する Event と併用されることを想定されています。再起動した機器が Failover ペアの Primary 役である場合、Backup 役の Equalizer(別のゲートウェイ IP を使用)が Primary 役になります。
server_wait (server, seconds)	指定したサーバで Event による影響から一定時間(秒)ブロックするタイマーをセットします。常に値 “true” を返します。ブロックされているサーバを使用した Event は “false”を返します。
set_weight (server, weight)	指定したサーバの動的 Weight 値(Current Weight)に Weight 値(0-200)を設定します。これは、サーバに設定する Initial Weight 値(セクション 4-8-4)に影響しません。この動的な Weight 値の設定は、サーバ設定が変更されると Initial Weight 値にリセットされます。
true ()	常に値 “true”を返します。
unquiesce (server)	指定したサーバの quiesce 設定を無効にします。このEventによって quiesce が無効化された場合は値 “true” を返します。無効化されなかった場合は値 “false” を返します。
power_off (server)	VMware の仮想マシンをパワーオフします(事前にシャットダウンは実施しない)。通常は quiesce_server と event_wait を前もって実施しアクティブなコネクションが無い状態でシャットダウンが行われるようにします。仮想マシンがパワーオフされた場合は値 “true” を返します、それ以外では値 “false” を返します。
power_on (server)	VMware の仮想マシンをパワーオンします。仮想マシンがパワーオンされた場合は値 “true” を返します、それ以外では値 “false” を返します。
shutdown (server)	Equalizer VLB が VMware に仮想マシンをシャットダウンさせるように動作します。通常は quiesce_server を前もって実施しアクティブなコネクションが無い状態でシャットダウンが行われるようにします。仮想マシンがシャットダウンされた場合は値 “true” を返します、それ以外では値 “false” を返します。

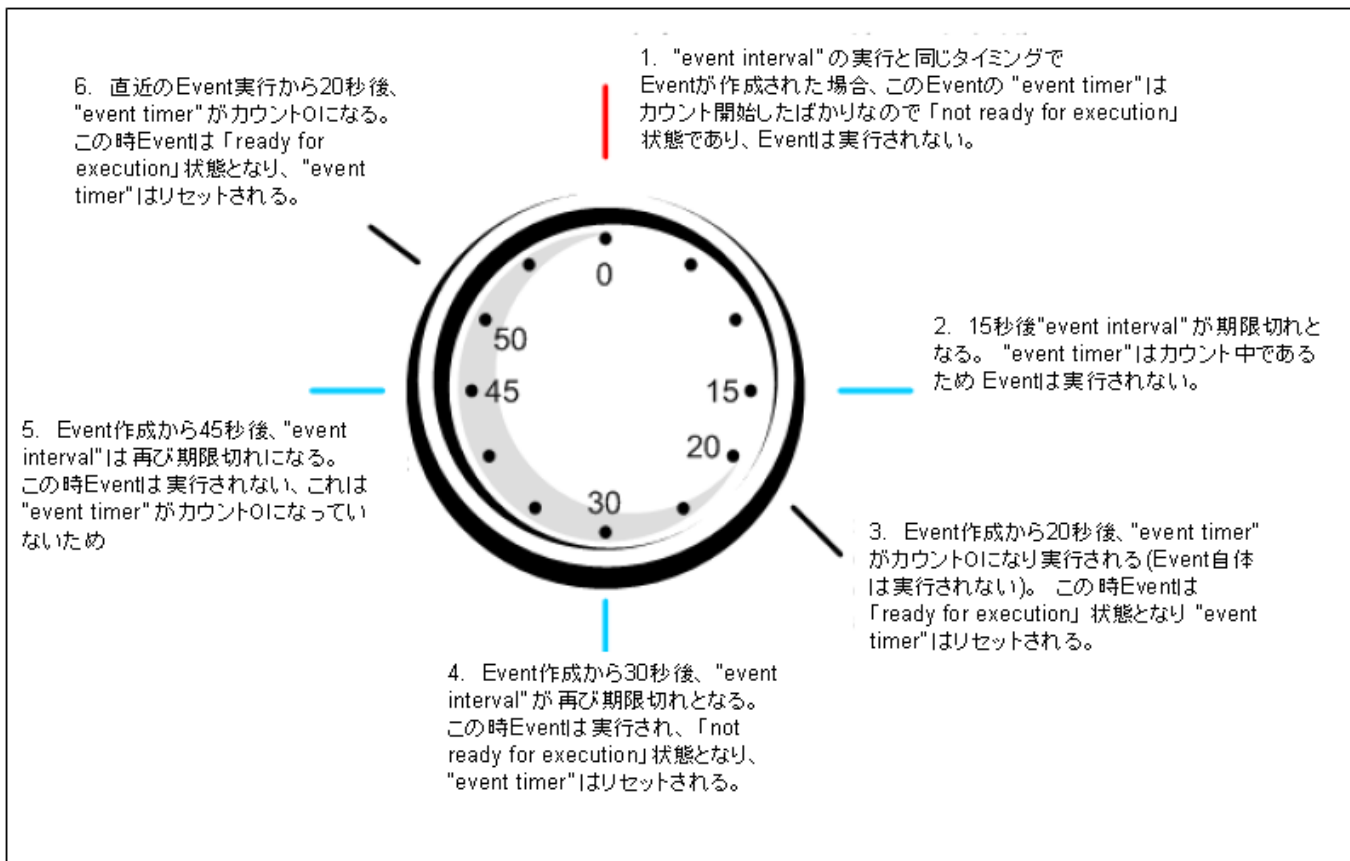
8-6 Smart Events 時間設定について

Smart Events で使用する時間設定は、グローバルで設定する event interval(3-1-2 参照)と各 Event で設定する event timer(8-3-3)の2つがあります。

Event 単位で指定される event timer によって、Event が実行されるかどうか決定されます。作成後は「not ready for execution」状態ですが event timer 時間が経過すると、この Event は「ready for execution」状態になります。event timer の時間は event timer または event interval 時間を経過するとリセットされます。

Smart Event の実行は event interval で指定した時間ごとに行われます。実行される Event は「ready for execution」状態である必要があります。

以下の例では event interval が 15 秒(デフォルト)、作成された Smart Event の event timer は 20 秒で設定された場合の動作について解説しています。



APPENDIX A セッション維持動作解説

A-1 セッション維持とは

Equalizer は負荷分散を行なうため、クラスタへ到達したクライアントのリクエストをクラスタ所属のサーバに対して振り分けます。 [4-7-1](#)にある負荷分散ポリシーによって、振り分け先サーバはアクセスした瞬間に決定されます。

しかし各サーバが、以前に行なった通信のユーザ情報を個別に参照しなくてはいけないケースがあります。例えばショッピングサイトで買い物を行なっている場合など、ユーザのログイン情報やユーザがどの品物をショッピングカートに入れたかという情報は、サーバとクライアントが共有しなくてはなりません。

このようにサーバが固有情報を保持し、あるクライアントは常に同一サーバにアクセスする必要がある場合、負荷分散ポリシーによってランダムにサーバを選択することは出来ません。この、以前にアクセスしたサーバに次回以降も引き続いてアクセスを行なわせる動作を**セッション維持**といいます。

注意: Equalizer はユーザのログイン情報や、ショッピングカートの情報などのセッション情報を認識することはありません。Equalizer が提供する「セッション維持」とはアクセスするクライアントと振り分けられるサーバとの紐付けです。

これは、同一ユーザが前回のアクセス時とは別の TCP セッションを使用しクラスタにアクセスした場合でも、そのユーザが特定のサーバに振り分けられる必要があると IP レベル・HTTP レベルで判断するということです。

A-2 Equalizer が提供するセッション維持方法

Equalizer が提供するセッション維持機能は、クラスタによって異なります。

クラスタ	セッション維持方法	セッション維持動作	解説
L4/TCP L4/UDP	sticky time	クライアントの送信元 IP アドレスを判別しセッション維持を行なう	A-3
L7/HTTP L7/HTTPS	cookie	Equalizer がセッション維持用 Cookie をクライアントに付与することでセッション維持を行なう	A-4

sticky time や cookie によるセッション維持は、Hot Spare や Quiesce として設定したサーバに対しては優先して適用されます。例えば、クライアントがサーバへセッション維持されている状態で該当サーバを Hot Spare に設定変更した場合、通常(他にアクティブなサーバがクラスタ内に存在する場合)では Hot Spare サーバへは通信が振り分けられませんが、セッション維持されたクライアントは Hot Spare サーバへ振り分けられます。

A-3 sticky time によるセッション維持

L4クラスタの動作では、Equalizer はリクエストしてくるクライアントの送信元 IP アドレスを Sticky テーブル情報として記録します。次回以降のリクエスト送信元 IP アドレスがこの Sticky テーブルに記載されている場合は、前回振り分けたサーバに再度振り分けを行なうことでセッション維持動作を実現します。

A-3-1 sticky time の設定

設定は各クラスタ個別に行ないます、設定箇所は [4-4-1-3](#) を参照して下さい。

sticky time は秒数で指定しますが、これは初回のアクセス時からの秒数ではありません。最終的に行なわれたアクセスからの秒数になります。さらに厳密には TCP セッションが終了してから秒数のカウントダウンが開始しますので、HTTP/1.1 の KeepAlive などにより TCP セッションが KeepAlive タイムアウト時間内でクローズされずに残っている場合はカウントが開始されず、TCP セッションが終了してからカウントが行なわれます。

A-3-2 sticky time の注意点

クライアントの送信元 IP アドレスを判別しセッション維持を行なうことから、クライアントの IP アドレスが同一になってしまう環境などに於いては sticky によるセッション維持を行なうことは難しくなります。以下の例を参照して頂き、該当する場合は L7 クラスタを使用するなど、別途セッション維持の方法をご検討下さい。

- ・ クライアントと Equalizer の間にリバース Proxy 等が存在し、クラスタへアクセスする IP アドレスが特定の IP アドレスに NAT 変換されてしまう場合。
- ・ 携帯電話からのアクセスは、通信キャリアのゲートウェイアドレスに変換されてしまうため、送信元 IP アドレスが偏る可能性があります。
- ・ 移動している携帯電話などは、通信する基地局が切り替わった際に送信元 IP アドレスが切り替わる場合があります。このように送信元 IP アドレスが途中で変わる状況においては、sticky によるセッション維持に問題が出る可能性があります。

A-3-3 inter-cluster sticky 設定について

複数のクラスタで同一の IP アドレスを使用し、個別のポート番号でサービスを行なっている場合にクラスタ間で sticky テーブル情報を共有することが可能です。sticky time によるセッション維持を設定している場合にのみ設定可能になります。以下の例では 80 番(HTTP)および 443(HTTPS)のサービスを行なっている2つのクラスタがあります。

■クラスタ “WebHTTP” (192.168.200.1 :80)

サーバ1:192.168.1.10

サーバ2:192.168.1.11

■クラスタ “WebHTTPS” (192.168.200.1 :443)

サーバ1:192.168.1.10

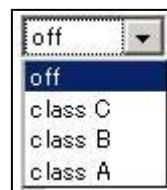
サーバ2:192.168.1.11

上記例に於いて inter-cluster sticky を有効にすることで、“WebHTTP” に対して80番でアクセスしたクライアントが、その後 “WebHTTPS” に443番でアクセスした場合に同じサーバへ割り振ることが可能になります。

A-3-4 sticky network aggregation 設定について

クライアントの送信元 IP アドレスをネットワークセグメント単位で判断し、同一のサーバへ割り振る際に使用します。例えば複数の Proxy サーバが存在し送信元 IP アドレスが固定されない場合などに使用します。

クラス A, B, C から選択します。設定箇所は [3-1-4](#) を参照して下さい。



A-3-5 sticky テーブル情報の同期について

冗長化構成時、2台の Equalizer 間では Sticky テーブル情報は同期されません([5-2-5](#) も併せて参照下さい)。Equalizer が Failover すると、既存で行なわれていた通信も新規リクエストとして処理されます。

A-3-6 サーバ単位のセッション維持設定について

通常、セッション維持はクラスタ単位で設定しますが、サーバ単位でセッション維持動作の有効・無効を選択することが可能です。詳細は [4-8-8](#) の dont persist 解説をご参照下さい。

A-4 cookieによるセッション維持

L7/HTTP・HTTPS クラスタでは、セッション維持方法として cookie を付与します。初回のリクエストで Equalizer が付与した cookie を次回リクエストの HTTP ヘッダに埋め込んで通信が行なわれるため、Equalizer は cookie 情報を確認し同じサーバへ振り分けることが実現できます。

L7/HTTPS クラスタの場合は、SSL 複合処理を行ってから cookie 情報を確認し、クライアントへ通信を戻す際には cookie を付与してから SSL 暗号処理を行いません。従って L7/HTTP クラスタと同様に cookie によるセッション維持動作を行なうことが可能です。

A-4-1 cookie の設定

設定箇所およびパラメータについては [4-5-1-3](#) を参照下さい。デフォルトでは cookie によるセッション維持は有効になっています。

A-4-2 Equalizer の cookie とサーバの cookie の違い

Equalizer が付与する cookie はセッション維持に使用する cookie ですので、サーバが発行する cookie とは使用目的が違います。Equalizer はサーバの cookie に対しては書き換え・削除等の動作は一切行わず、自身が付与した cookie のみ確認を行います。

注意： Match Rules 機能を使用した場合、サーバが発行した cookie の情報を精査し、振り分け先サーバを選択する事も可能になります。

サーバが set-cookie をした場合にのみ、Equalizer が cookie を付与する設定は [4-5-1-3](#) の always 設定をご確認下さい。

A-4-3 Equalizer の cookie の詳細解説

Equalizer が付与する cookie にはクラスタ・サーバの情報が記載されていますので、クライアントが cookie を保持した状態でリクエストをすることで、Equalizer は振り分け先サーバを判別することが可能です。実際に付与される Equalizer の cookie は例えば以下のようになります。

`coyote-2-a0f648f=a0f65d2`

cookie が付与される際の通信フローについては以下の図を参照して下さい。



A-4-4 複数クラスタ間の cookie 動作について

A-4-3 の解説の通り、cookie にはクラスタ・サーバの情報が記載されていますが、ポート番号については認識していません。従って、同一 IP アドレスの L7/HTTP・HTTPS クラスタが複数ポート番号にまたがってサービスを提供している場合は同じ cookie を使用することができます(サーバ IP アドレスが同一である必要があります)。A-3-3 と同じ例ですが、下記のように2つのクラスタが同一サーバを所属させてサービスをしている場合、クラスタ “WebHTTP” で発行された cookie は、クラスタ “WebHTTPS” でも認識することができます。

■クラスタ “WebHTTP” (192.168.200.1 :80)

サーバ1:192.168.1.10

サーバ2:192.168.1.11

■クラスタ “WebHTTPS” (192.168.200.1 :443)

サーバ1:192.168.1.10

サーバ2:192.168.1.11

A-4-5 冗長化構成時の cookie 動作について

cookie にはクラスタ・サーバ情報が含まれている為、冗長化構成時に Equalizer が Failover したとしてもクライアントが cookie を HTTP リクエストヘッダ内に挿入していれば問題なく Equalizer は判断し同じサーバへ振り分けることができます。

L4クラスタの sticky の設定では、sticky テーブル情報を Failover ペアが共有しないために Failover 後はセッション維持を行なうことが出来ませんが、L7クラスタの cookie を使用することで実現が可能です。

A-4-6 once only 使用時の cookie 動作について

L7HTTP/HTTPS クラスタでは once only と呼ばれる設定パラメータがあります([4-5-1-5 参照](#))。once only を有効にした状態で、1つの TCP セッション内で複数の HTTP リクエストが行なわれた場合、Equalizer は先頭リクエストのヘッダ情報のみ確認します。また、先頭リクエストに対してのみ cookie を付与します。

複数クライアントの HTTP リクエストが1つの TCP セッション内にまとめられてしまう環境などでは、正常にセッション維持を行なう為に once only の設定を無効にする必要があります。

また先頭リクエストに対してのみ cookie 付与が行われる為、cookie age 設定で有効期限を設定している場合に、1つの TCP セッションで通信を行なっている最中に cookie 有効期限が過ぎてしまうことがあります。ブラウザは有効期限が過ぎた cookie をリクエストヘッダに挿入しない

ため、同一のクラスタに対して新規に TCP セッションを開いた場合にセッション維持が行なえなくなります。

once only 設定を無効にする、あるいは cookie age 設定を 0 秒にすることで、このようなケースを防ぐことが可能です。

A-4-7 サーバ単位のセッション維持設定について

通常、セッション維持はクラスタ単位で設定しますが、サーバ単位でセッション維持動作の有効・無効を選択することが可能です。詳細は [4-8-8](#) の dont persist 解説をご参照下さい。

APPENDIX B CSR 作成手順

B-1 Equalizer サーバ証明書インストール手順について

HTTPS クラスタへサーバ証明書をインストールする手順について説明します。
作成する CSR(Certificate Server Request) は RSA 3DES 2048bit で暗号化することを前提としています。CSR を提出する CA(認証局) がこの暗号化をサポートしていない場合は、暗号化の鍵長や暗号化アルゴリズムを変更する必要がありますので、Equalizer 上で Openssl のオンラインマニュアル等を参照し、手順内容を変更して下さい。

B-2 CSR 作成手順

サーバ証明書を発行するには CSR を作成し CA へ提出する必要があります。CSR 作成は Equalizer 上で行うことができます。CA が提示している作成手順と異なる場合は、その手順にて作成してください。

1. シリアルコンソール画面へシリアルケーブル または SSH にてログインします、ログインは root にて行って下さい。(SSH の場合はログイン後に su にて root 権限に切り替えます)。
2. ディレクトリを移動します。
cd /tmp
3. 秘密鍵作成のための擬似乱数を作成します。
openssl md5 * > rand.dat
※ rand.dat = 出力する擬似乱数。任意のファイル名)
※下記エラーが表示されますがrand.dat が作成されていれば作業に問題はございません。
snmpctl: Operation not supported
switchc_server.sock: Operation not supported
switchd_server.sock: Operation not supported
4. 2048bit 3DES により秘密鍵を生成します
openssl genrsa -rand rand.dat -des3 2048 > key.pem
※ パスフレーズの入力を求められます。任意の文字列を入力します。
※ 鍵長を 1024bit で作成する場合は以下のように入力します
openssl genrsa -rand rand.dat -des3 1024 > key.pem
※ XCEL カードが搭載された SI シリーズ筐体で 2048bit 鍵長の秘密鍵を使用する場合は、Composite ファイルをアップロードする際 “use secure key storage”を無効化して下さい。

- ※ key.pem = パスフレーズの必要な秘密鍵。任意のファイル名)
5. パスフレーズを無効にする場合は下記を実行します。
(パスフレーズを無効にしない場合は 6 へ進みます。)
openssl rsa -in key.pem -out keyout.pem
※ パスフレーズの入力を求められます、先ほどの文字列を入力して下さい。
※ keyout.pem = 無効化して出力する秘密鍵。任意のファイル名。
 6. 生成した秘密鍵によって CSR を作成します。
 - 5 でパスフレーズを無効にした場合：
openssl req -new -key keyout.pem -out csr.pem
※ csr.pem = 出力する CSR。任意のファイル名
 - 5 でパスフレーズを無効にしない場合：
openssl req -new -key key.pem -out csr.pem
※ csr.pem = 出力する CSR。任意のファイル名
Enter pass phrase for key.pem
 7. 4 で入力したパスフレーズを入力します
証明書情報(ディスティンゲイッシュネーム)を入力します。
CA に申請する情報を入力します。

参考例

表示される項目	日本語訳	入力例
Country Name(2 letter code)	<国>	JP
State or Province Name	<都道府県名>	Tokyo
Locality Name	<市区町村名>	Chiyoda-ku
Organization Name (eg, company)	<正式英語組織名>	Example Inc.,
Organizational Unit Name (eg, section)	<部門名>	System 1
Common Name (eg, YOUR name)	<URL<FQDN>>	www.example.com
Email Address	<管理者のメール<省略可>>	
A challenge password	<省略>	
An optional company name	<省略>	

※A challenge password、An optional company name の入力は省略します。

何も入力せず Enter キーを押し決定します。

Equalizer 上から FTP コマンドを使用し、作成した CSR および 秘密鍵 を外部へ転送します上記 CSR を元に、CA へサーバ証明書の発行を申請します。

また 次のコマンドにて表示されるテキストをコピー&ペーストしていただくことでも可能です。

```
# cat key.pem
# cat csr.pem
```

必要な証明書の枚数などは CA により異なりますので、申請先 CA へ直接お問い合わせ下さい。

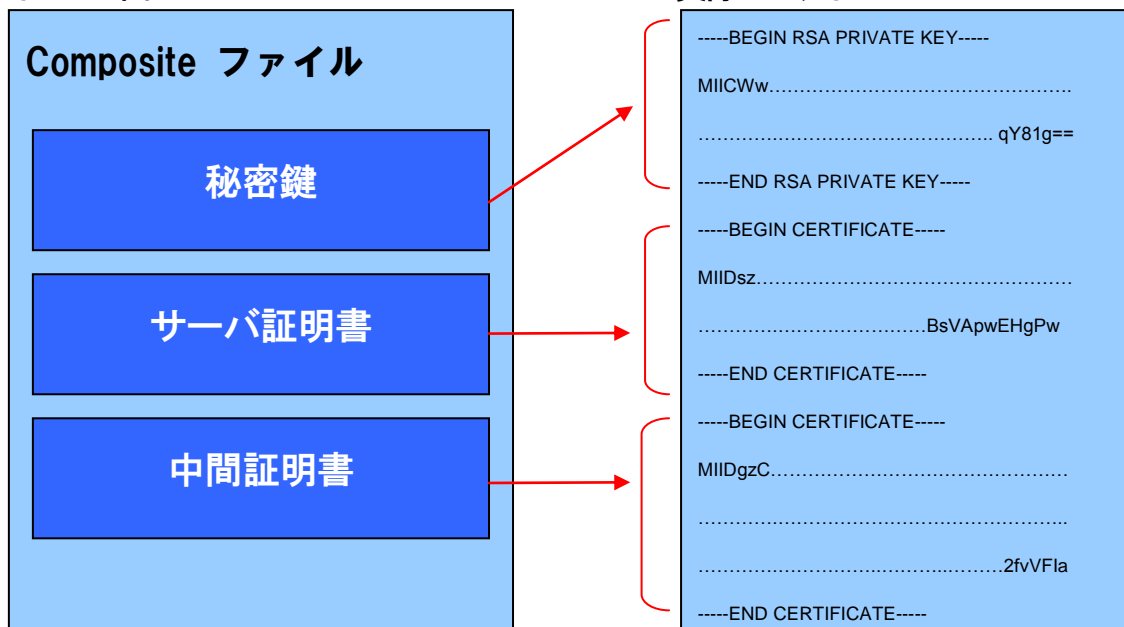
B-3 Composite ファイル 作成手順

Equalizer へアップロードするファイルは Composite ファイル と呼ばれます。

これは次の3点をあわせたテキスト形式ファイルです。拡張子 “.pem” にて保存します。

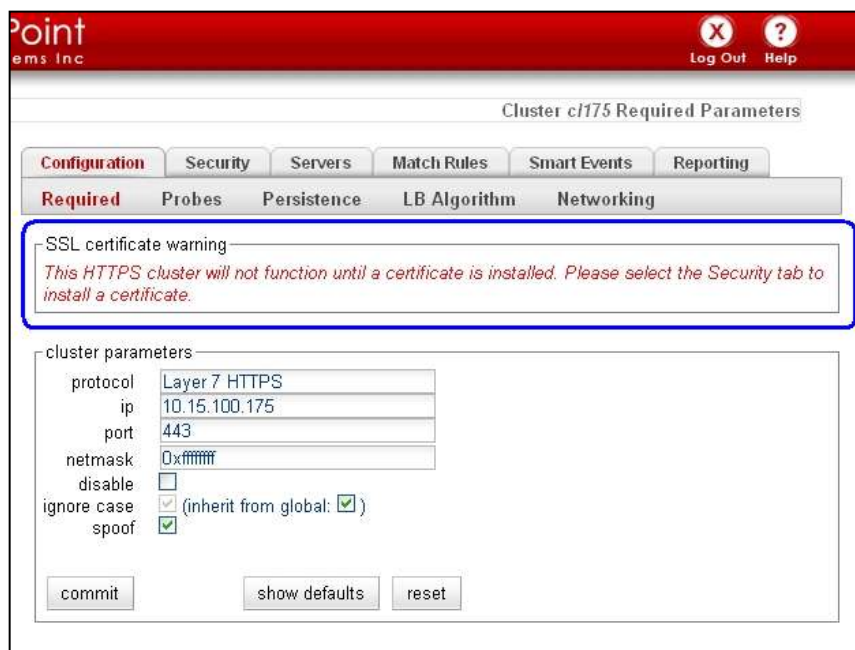
- ・ 秘密鍵
- ・ CA より発行されたサーバ証明書
- ・ 中間証明書

イメージ図



B-4 Composite ファイル アップロード手順

Composite ファイル は Equalizer の Web 管理画面からアップロードします。ブラウザから ユーザ touch または編集ユーザ にて Equalizer へログインして下さい。左フレームから、該当 HTTPS クラスタを選択します。SSL サーバ証明書が無い状態では、SSL certificate warning が表示されます。

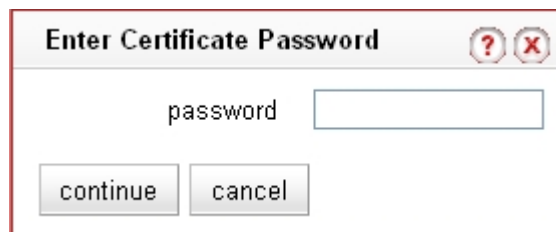


表示された画面から Security タブから Certificates を選択すると、下記のように“参照”ボタンが表示されますので、ローカル PC 上から Composite ファイルを選択し、“upload”ボタンを押します。XCEL カードが搭載された SI シリーズ筐体では“use secure key storage”オプションが表示されます(デフォルト:有効)。有効の場合、秘密鍵が XCEL カードのメモリ内部に格納され外部からアクセスが出来なくなりますので、セキュリティを向上させることが可能になります。



CSR 作成時にパスフレーズを有効にした場合は、アップロード時にパスフレーズ入力画面が表示されます(右図)。

continue をクリックすると、インストールする証明書の内容が表示されますので、確認します。



continue を押して決定することで、サーバ証明書のアップロードは完了です。

クラスタ内のサーバ証明書情報を確認すると Certificate が反映されています。certificate 1 がサーバ証明書、certificate 2 が中間証明書 となります。 証明書の内容や、有効期限なども確認可能です。

サーバ証明書をアップロード後、該当クラスタに SSL certificate warning が表示されなくなったことを確認します。 また Failover 設定で Transfer Certificates が有効になっている場合はサーバ証明書が同期されることを確認します。



B-5 サーバ証明書に関する注意事項

- ・ 機器のコンフィグ情報である「バックアップファイル」にはアップロードしたサーバ証明書の情報はセキュリティの観点から含まれません。
- ・ SI シリーズで Xcel カードを使用している場合は、デフォルト設定で秘密鍵は Xcel カード内に格納されます。 このため、Web 管理画面・コンソール画面から秘密鍵情報を参照することは出来ません。 GX シリーズでは Equalizer の内部に保存されます。
- ・ ハードウェア故障などで、機器交換を行った場合は「バックアップファイル」にて設定をリストアした後、サーバ証明書を再度アップロードする必要があります。

改定履歴

改定番号	改定内容	改定日
1.0	新規作成し、8.6.0dに対応しました。	2011/09/13
1.1	ファームウェア 8.6.0f に対応しました。	2012/02/29
1.2	3-5-1-3 の記載内容を修正しました	2012/04/04
1.3	B-4 の記載内容を修正しました。	2012/11/27
1.4	4-4-4-5 の一部記載内容を削除しました。	2013/10/10