

GM0 クラウド Private サービス
仮想ロードバランサーオプション
Virtual Traffic Manager 簡易設定手順書

■更新履歴

バージョン	日付	内容
1.0	2018/12/06	初版作成
1.1	2022/01/17	GMO クラウド株式会社 →GMO グローバルサイン・ホールディングス株式会社

はじめに

本書は、GMO クラウド Private で提供している仮想ロードバランサーの設定手順書です。

本書では仮想ロードバランサー（Virtual Traffic Manager）を運用するに当たって必要となる下記オペレーションについて記載しています。

- －Virtual Traffic Manager の概要
- －管理画面の見方
- －一般的な設定方法
 - ・基本的な負荷分散の設定
 - ・SSL 通信の復号化設定
 - ・負荷分散方法の選択
 - ・セッション・パーシステンス（セッション維持）の設定
 - ・ヘルスモニタリング（死活監視設定）
 - ・Sorry サーバーの設定
 - ・クライアント IP アドレス透過設定
- －よくある質問と回答

本書を当社の許諾なく複製 または 第三者へ提供することとはご遠慮下さい。

目次

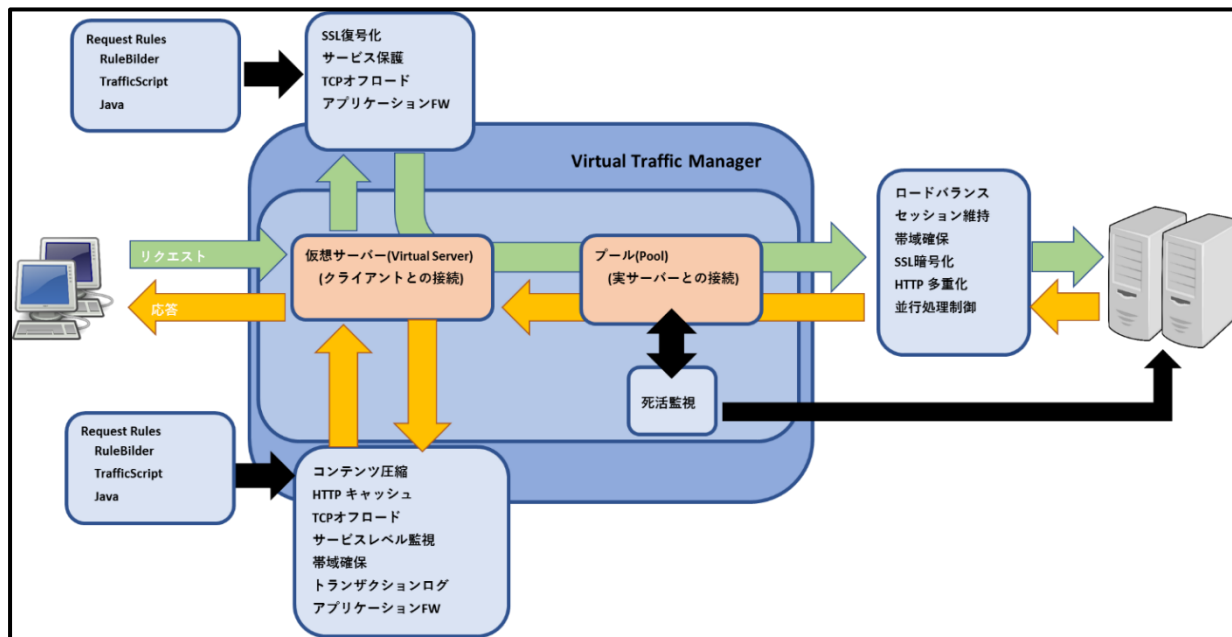
1	Virtual Traffic Manager の概要	6
1.1	主要な構成要素について	6
1.2	管理画面へのログイン	7
2	管理画面の見方	8
2.1	トップメニュー	8
2.2	Services メニュー	10
2.2.1	Traffic IP Groups メニュー [Services]メニュー»[Traffic IP Groups]	10
2.2.2	Virtual Servers メニュー [Services]メニュー»[Virtual Servers]	11
2.2.3	Pools メニュー [Services]メニュー»[Pools]	12
3	一般的な設定方法	13
3.1	基本的な負荷分散の設定	13
3.1.1	Traffic IP Group の作成	13
3.1.2	プール の作成と設定	15
3.1.3	仮想サーバー の作成	16
3.2	SSL 通信の復号化設定	18
3.2.1	ルート証明書のインポート	18
3.2.2	中間証明書のインポート	20
3.2.3	仮想サーバーへの設定	21
3.2.4	待ち受けポート変更	23
3.3	負荷分散方法の選択	24
3.3.1	負荷分散アルゴリズムの種類	24
3.3.2	負荷分散アルゴリズムの設定方法	24
3.4	セッション・パーシステンス(セッション維持)設定	26
3.4.1	セッション・パーシステンスの種類	26
3.4.2	セッション・パーシステンスの設定方法	27
3.5	ヘルスマonitoring(死活監視)設定	29
3.6	Sorry サーバー設定	31
3.6.1	Sorry サーバー・プールの登録	31
3.6.2	プールへ Sorry サーバー・プールを登録	32
3.7	クライアント IP アドレス透過設定	33

4	よくある質問と回答	35
---	-----------------	----

1 Virtual Traffic Manager の概要

本章では、Virtual Traffic Manager (以降、VTM と略します) の概要を示します。

1.1 主要な構成要素について



本製品における主要構成要素は、下記 2 点となります。

① 仮想サーバー (Virtual Server)

クライアントからのリクエストを受信する IP アドレス/ポート番号を管理するグループです。
後述するプールが管理する、バックエンドサーバー群のフロントエンドとして位置付けられます。

仮想サーバーの IP アドレスは、稼働サーバー自身の IP アドレスもしくは Traffic IP Group と呼称する仮想 IP アドレスを使用することができます。

Traffic IP Group は VTM クラスタで共有する仮想 IP アドレスで、Active-Standby もしくは Active-Active のサービスを提供することが可能です。

② プール (Pool)

実際にサービスを提供するバックエンドサーバーの IP アドレス/ポート番号を、論理的に束ねて管理するグループです。

プールは前述の仮想サーバーに割当てるように設定し、仮想サーバーがクライアントから受信したリクエストは、プールに属するバックエンドサーバーに対し（設定した負荷分散方式により）送信されます。

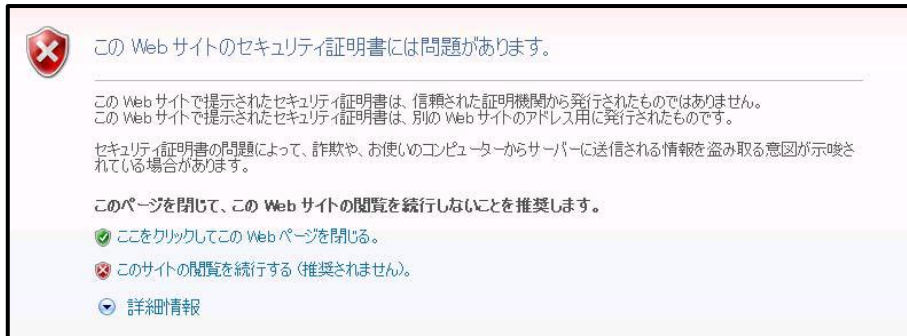
また、プールは負荷分散の他、バックエンドサーバーの死活監視（ヘルスモニタリング）、セッション・パーシステンスなどの設定を行うことが可能です。

1.2 管理画面へのログイン

- ① WEB ブラウザを起動し、下記 URL にアクセスします。

https://<VTM の IP アドレス>:9090/

※初回ログイン時は下記のセキュリティ警告が表示されるため、「このサイトの閲覧を続ける（推奨されません）」を押下します。

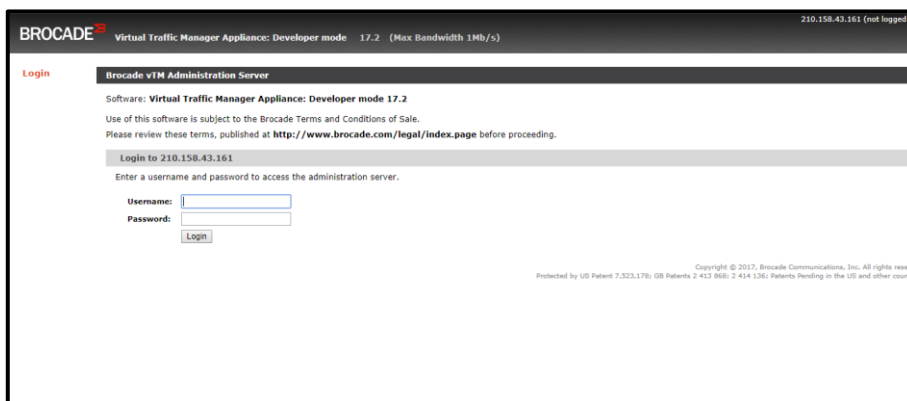


- ② 認証画面が表示されますので、必要な値を入力して[Login]ボタンを押下します。

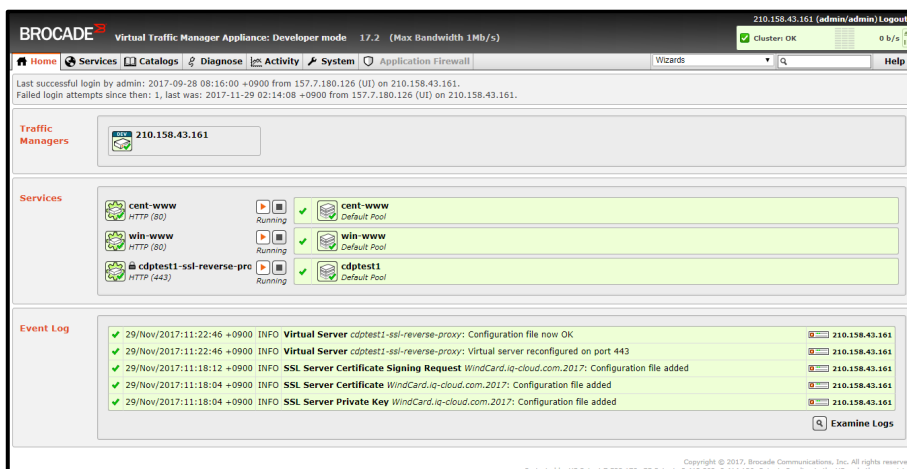
● [Username] にログインユーザー名を入力（初期値：admin）。

● [Password] にパスワードを入力。

※ユーザー名/パスワードは設定完了通知書をご参照下さい。



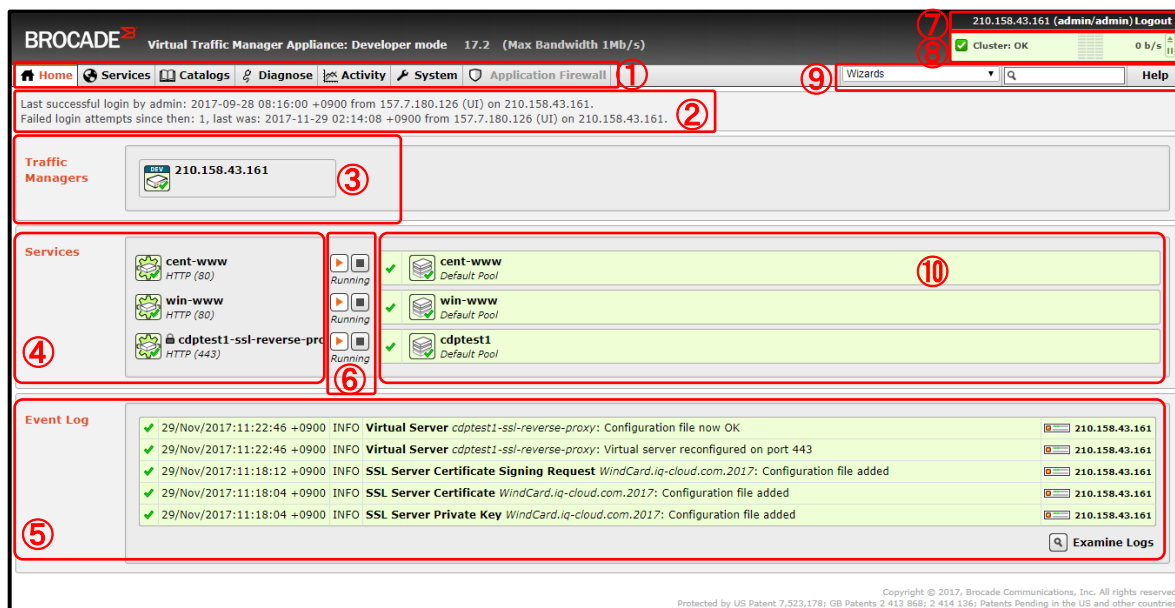
- ③ ログインに成功すると管理 WebUI のトップ画面が表示されます。



2 管理画面の見方

2.1 トップメニュー

このページでは、クラスタを構成する VTM の状態、仮想サーバーおよびプールの状態、イベントログなどを確認することができます。



① セクションボタン

VTM の管理操作を行うための各セクションページへ移動します。
セクションページ毎の詳細説明はメーカー提供のユーザーマニュアルを参照下さい。

② ログイン・インフォメーション・バナー

最後にログインに成功した時刻および失敗した時刻が表示されます。

③ トラフィックマネージャー

管理対象の VTM が表示されます。
VTM にエラーが発生した場合にアイコンが変化してメッセージが表示されます。
アイコンを押下しますと、[System]メニュー≫[Traffic Managers]タブへ移動し、VTM の状態を確認することができます。

④ 仮想サーバー

設定された仮想サーバーが表示されます。
仮想サーバーにエラーが発生した場合、アイコンが変化し、メッセージが表示されます。
アイコンを押下しますと[仮想サーバー]ページへ移動し、仮想サーバーの状態を確認することができます。

⑤ ログ

VTM が検出したエラー、警告、情報メッセージが表示されます。
[Examine Logs]を押下しますと、[Event Log]タブへ移動し、詳細にログを確認することができます。

⑥ スタート／ストップボタン

④に表示されている各仮想サーバーを手動で停止または起動することができます。

【ボタンの説明】

停止	
起動	

⑦ ログアウトボタン

ボタンを押下することにより、VTM の管理 WebUI からログアウトできます。

⑧ ステータス・アプレット

クラスタの状態や、現在のトラフィック量を表示します。

クラスタにエラーが発生した場合、下記のようにアイコンが変化してメッセージが各エリアに表示されます。

アイコンを押下しますと、[Diagnose] メニュー » [Cluster Diagnostic] タブへ移動し、クラスタの状態を確認できます。

【アイコン表示の例】

正常時	 Cluster OK
警告的エラー時	 Cluster Warning
致命的エラー時	 Cluster Error

⑨ ウィザード、サーチ、HELP

ウィザードは VTM の管理者が行う一般的な操作を対話形式にしたものです。

サーチは指定した文字にヒットする管理 WebUI 内の情報を表示します。

HELP は開いているページに関するオンラインヘルプを表示します。

⑩ プール

仮想サーバーに割当てたプールの状態を表示します。

プールにエラーが発生した場合、アイコンが変化し、メッセージが表示されます。

アイコンを押下しますと [プール] ページへ移動し、プールの状態を確認することができます。

2.2 Services メニュー

本章では、VTM 管理 WebUI の[Services]メニューの表示内容について示します。

2.2.1 Traffic IP Groups メニュー [Services]メニュー≫[Traffic IP Groups]

クラスター間で共有する TrafficIP アドレス（仮想 IP アドレス）の一覧（初期状態では無し）が表示されます。また、新しい Traffic IP Groups を作成することができます。

The screenshot displays the Brocade Virtual Traffic Manager (VTM) web interface. The top navigation bar shows 'Home', 'Services', 'Catalogs', 'Diagnose', 'Activity', and 'System'. The 'Services' menu is selected. Below the navigation bar, the 'Traffic IP Groups' section is active. A red box labeled '1' highlights the list of existing Traffic IP Groups, which includes 'Cent6test', 'Cent7test', 'Win2012test', 'Win2016test', 'cdptest1-ssl.lq-cloud.com', 'hatest1', 'hatest2', 'lbtest1c', and 'lbtest1w'. Below the list, there is a 'Create a new Traffic IP Group' section, which is highlighted by a red box labeled '2'. This section contains fields for 'Name', 'Traffic Managers' (with a dropdown and a 'Passive Add' checkbox), 'IP Addresses', and 'IP Mode' (with radio buttons for 'Single-Hosted mode', 'Multi-Hosted mode', and 'Use route health injection').

① Traffic IP Group 一覧

設定された Traffic IP Group が表示されます。
 または[Unfold All]を【▶】押下しますと、一つもしくは全ての Traffic IP Group の設定サマリーを表示できます。
 Traffic IP Group 名、または【Edit】を押下しますと、Traffic IP Group の詳細設定が開きます。

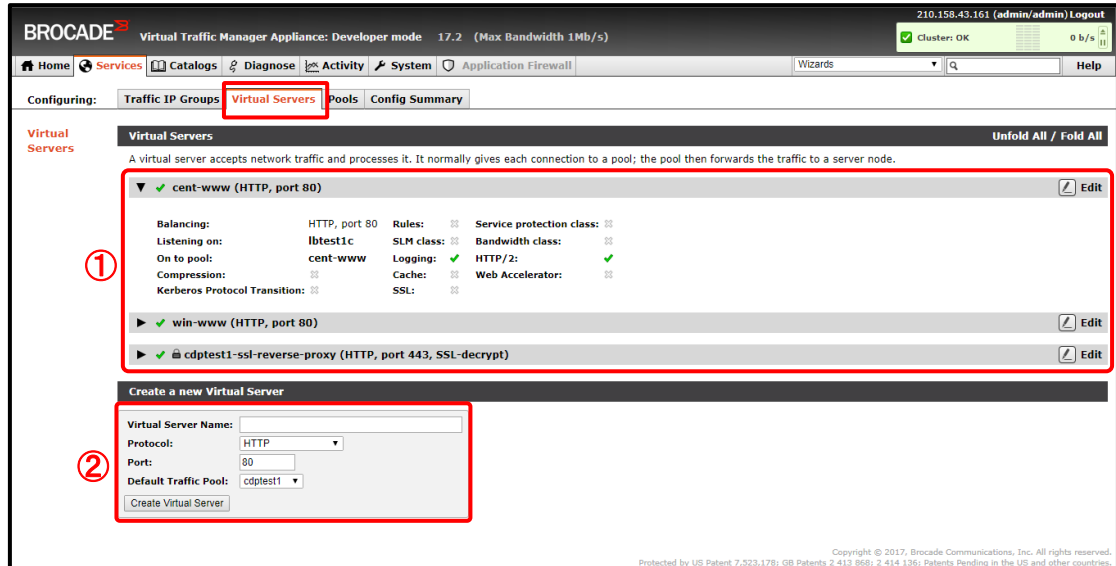
② Traffic IP Group の作成

新しい Traffic IP Group を作成することができます。

2.2.2 Virtual Servers メニュー [Services]メニュー≫[Virtual Servers]

本項目では、VTM 管理 WebUI の [Virtual Servers] タブの表示内容について示します。

VTM 管理 WebUI の [Services] メニューを押下しますと、設定された仮想サーバーの一覧（初期状態では無し）が表示されます。また、新しい仮想サーバーを作成することができます。



① 仮想サーバー一覧

設定された仮想サーバーが表示されます。

【▶】または[Unfold All]を押下しますと、一つもしくは全ての仮想サーバーの設定サマリーを表示できます。仮想サーバー名を押下しますと、仮想サーバーの詳細設定が開きます。

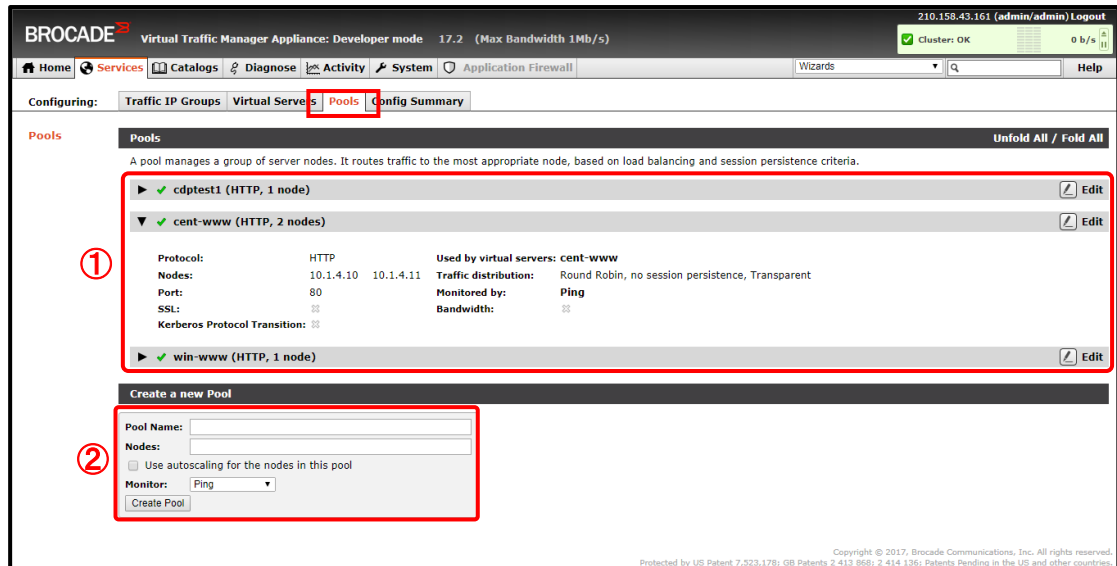
② 仮想サーバーの作成

新しい仮想サーバーを作成することができます。

2.2.3 Pools メニュー [Services]メニュー≫[Pools]

本項目では、VTM 管理 WebUI の [Pools] タブの表示内容について示します。

VTM 管理 WebUI の [Services] メニュー≫ [Pools] タブを押下しますと、設定されたプールの一覧（初期状態は無し）が表示されます。また、新しいプールを作成することができます。



① プール一覧

設定されたプールが表示されます。

【▶】または [Unfold All] を押下しますと、一つもしくは全てのプールの設定サマリーを表示できます。プール名、または【Edit】を押下しますと、プールの詳細設定が開きます。

② プールの作成

新しいプールを作成することができます。

3 一般的な設定方法

本章では、VTM の一般的な設定例を紹介します。

3.1 基本的な負荷分散の設定

本節では、基本的な負荷分散を行うための「Traffic IP Group」「仮想サーバー」「プール」を追加する方法を示します。

例として、下記の条件について設定します。

- HTTP 用の Traffic IP Group : [web]を作成し、仮想 IP アドレスを割り振る。
- 仮想サーバーに紐付くプール名 : [web]を作成し、バックエンドサーバー情報とポート番号を登録する。
- HTTP をサービスする仮想サーバー名 : [web]を作成する。

名称	IP アドレス	名称	プロトコル名: ポート	名称	振り先サーバー アドレス:ポート	監視方式
web	210.158.43.183	web	HTTP:80	WEB	210.158.43.185:80	Simple
					210.158.43.186:80	HTTP

3.1.1 Traffic IP Group の作成



- ① [Services]メニュー ≫ [Traffic IP Groups]タブを開きます。



- ② [Traffic IP Groups] 画面の [Create a new Traffic IP Group] セクションに下記設定を行い、[Create Traffic IP Group] ボタンを押下します。

Name:	web
IP Addresses:	210.158.43.183

Create a new Traffic IP Group

Name:

Traffic Managers:

Traffic Manager	Passive Add
210.158.43.187	☒

IP Addresses:

IP Mode:

- ☒ Raise each address on a single machine (Single-Hosted mode)
- ☐ Raise each address on every machine in the group (Multi-Hosted mode) - IPv4 only ...
- ☐ Use route health injection to route traffic to the active machine - IPv4 only

- ③ 「Your configuration has been updated.」と表示され、「web」が作成されたことを確認します。

Home Services Catalogs Diagnose Activity System Application

Configuring: **Traffic IP Groups** Virtual Servers Pools Config Summary

Traffic IP Groups

✓ Your configuration has been updated.

A Traffic IP group contains a selection of traffic managers and a set of one or

▼ ✓ **web (1 IP address, 1 traffic manager, Single-Hosted IPs)**

Traffic Manager - 210.158.43.187

210.158.43.183/27 eth0

3.1.2 プールの作成と設定



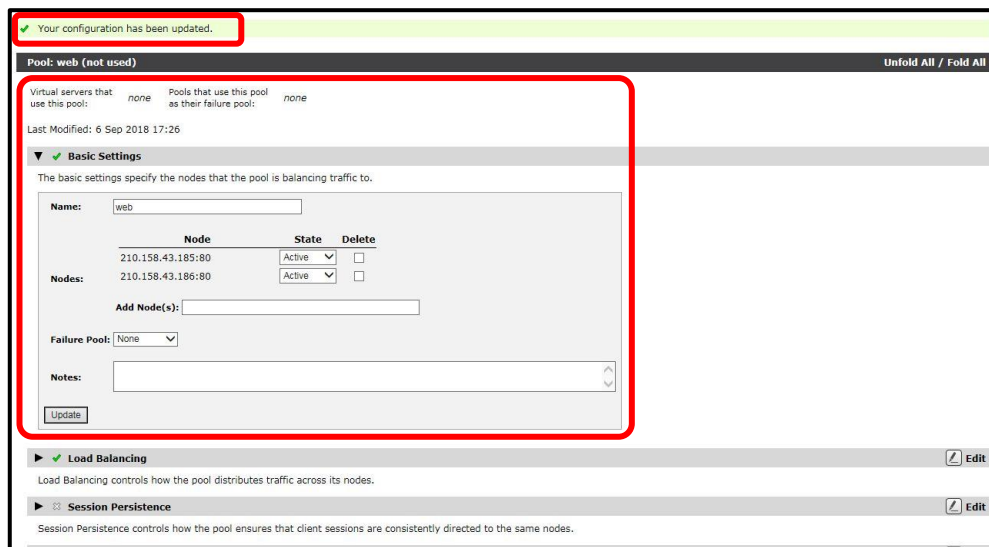
- ① [Services]メニュー ≫ [Pools]タブを開きます。



- ② [Create a new Pool]セクションに下記設定を行い、[Create Pool]ボタンを押下します。
※[Nodes]は、カンマを使って複数同時に登録する事が出来ます。

Pool Name:	web
Nodes:	210.158.43.185:80, 210.158.43.186:80
Monitor:	Simple HTTP

- ③ 「Your configuration has been updated.」と表示され、プール名:「web」の詳細画面が表示される事を確認します。



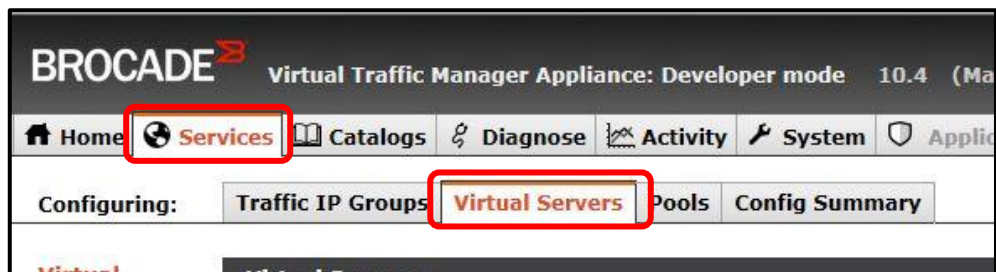
3.1.3 仮想サーバー の作成

Traffic IP Group の作成

プールの作成

仮想サーバーの作成

- ① [Services]メニュー ≫ [Virtual Servers]タブを開きます。



- ② [Virtual Servers] 画面の [Create a new Virtual Server] セクションに下記設定を行い、[Create Virtual Server] ボタンを押下します。

Virtual Server Name:	web
Protocol:	HTTP
Port:	該当プロトコルのウェルノウンポート番号に自動設定される為、必要な場合は変更する。(80→8080 など)
Default Traffic Pool:	web

- ③ 「Your configuration has been updated.」と表示され、仮想サーバー名:「web」の詳細画面が表示されるので、[Basic Settings]のセクションで以下の項目を設定し、[Upload]をクリックします。

Listening on: ●[Traffic IP Groups ...]→[web]にチェックを入れる

▼ **Basic Settings**

The basic settings specify the internal virtual server protocol that is used for traffic inspection, the port and IP addresses the virtual server listens on.

Name: web

Enabled: ☐ Yes ☒ No

Internal Protocol: HTTP

Port: 80

Default Traffic Pool: web

Listening on: ☐ All IP addresses ☒ Traffic IP Groups ...

Traffic IP Group	Select
web	☒
☐ Domain names and IP addresses ...	

Notes:

- ④ 再度「Your configuration has been updated.」と表示された事を確認します。

✔ Your configuration has been updated.

3.2 SSL 通信の復号化設定

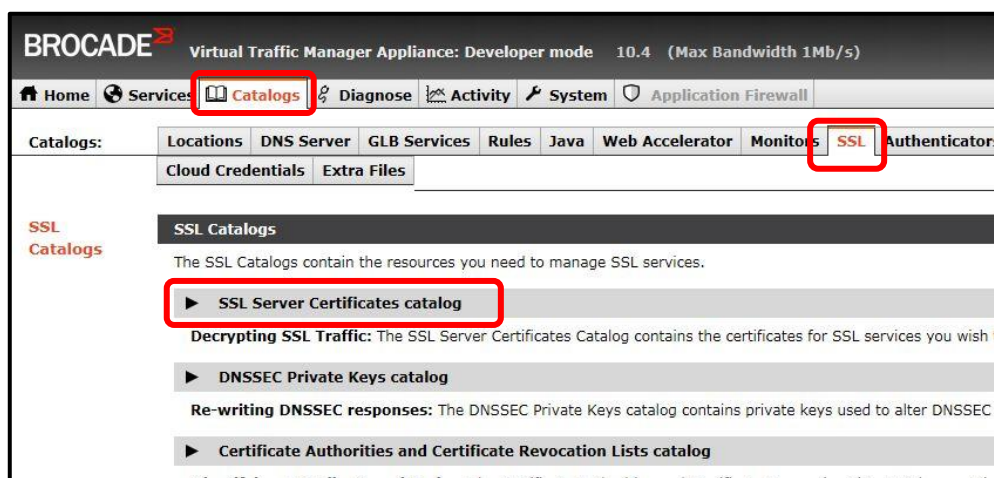
本節では、VTM の仮想サーバーに SSL 復号化 (SSL オフロード) を行う設定方法を示します。

なお、本設定を行うには事前に SSL 証明書 (ルート証明書, 中間証明書, 秘密鍵) をご準備いただく必要がございます。

3.2.1 ルート証明書のインポート



- ① [Catalogs] メニュー ≫ [SSL] タブで [SSL Certificate catalog] をクリックします。



- ② [SSL Server Certificates Catalog] 画面で [Import Certificate] を押下します。



- ③ [Import SSL Certificate] 画面で下記設定を行い、[Import Certificate] を押下します。

[Name]:	任意の証明書名を入力
[Certificate file]:	インポートする証明書ファイルを指定
[Private key file]:	インポートする秘密鍵ファイルを指定

Import SSL Certificate

This form lets you import an SSL certificate and private key.

Enter a short name to identify your certificate:

Name:

Enter the location of your certificate file:

Certificate file: 参照...

Enter the location of your private key file:

Private key file: 参照...

Import certificate

- ④ 「Your configuration has been updated.」と表示され、証明書が登録された事を確認します。

✓ Your configuration has been updated.

SSL Server Certificates Catalog

Decrypting SSL Traffic: The SSL server certificates catalog contains the certificates for the SSL se

▶ domain.cert

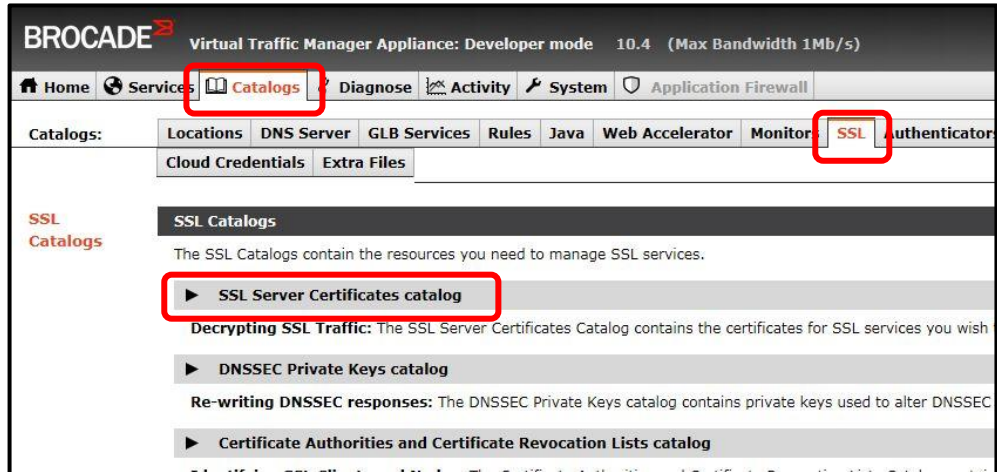
Create new SSL certificate

SSL certificates are used to identify the SSL services you are running, and they are needed to de

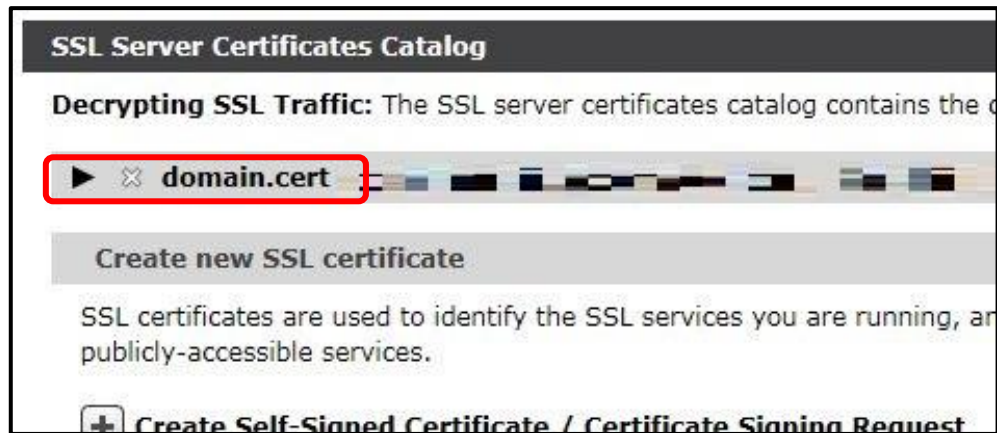
3.2.2 中間証明書のインポート



- ① [Catalogs]メニュー ≫ [SSL]タブで[SSL Certificate catalog] をクリックします。



- ② [SSL Server Certificates Catalog] 画面で[作成した証明書名] をクリックします。

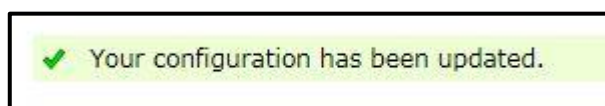


- ③ [SSL Certificates Catalog]画面で[Update/Add Intermediate Certificate]を押下します。



- ④ [Certificate file]に中間証明書ファイルを指定し、[Upload intermediate certificate]ボタンを押下します。

- ⑤ 「Your configuration has been updated.」と表示された事を確認します。



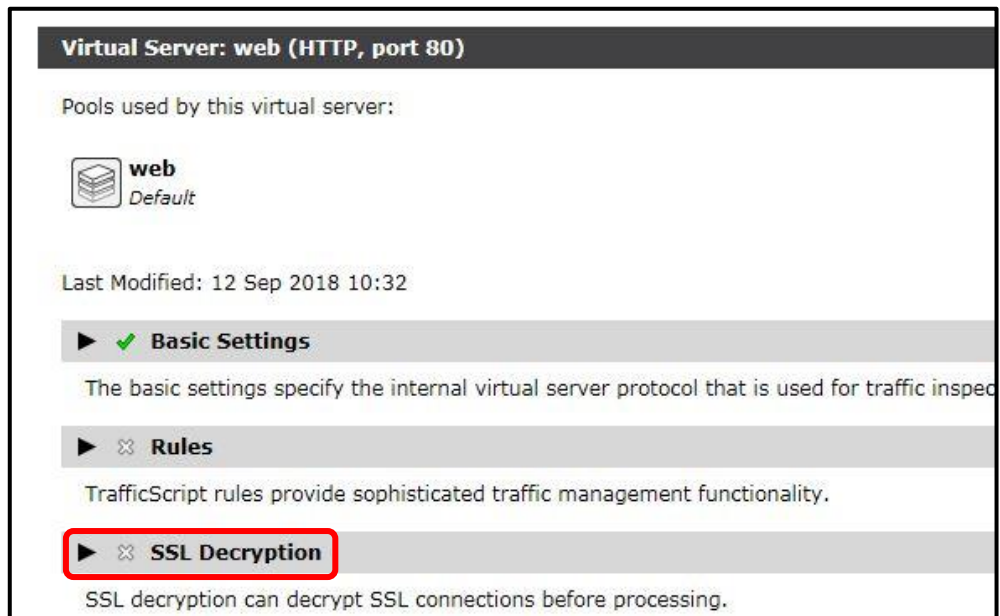
3.2.3 仮想サーバーへの設定



- ① [Services]メニュー ≫ [Virtual Servers]タブ ≫ [作成した仮想サーバー名]を開きます。

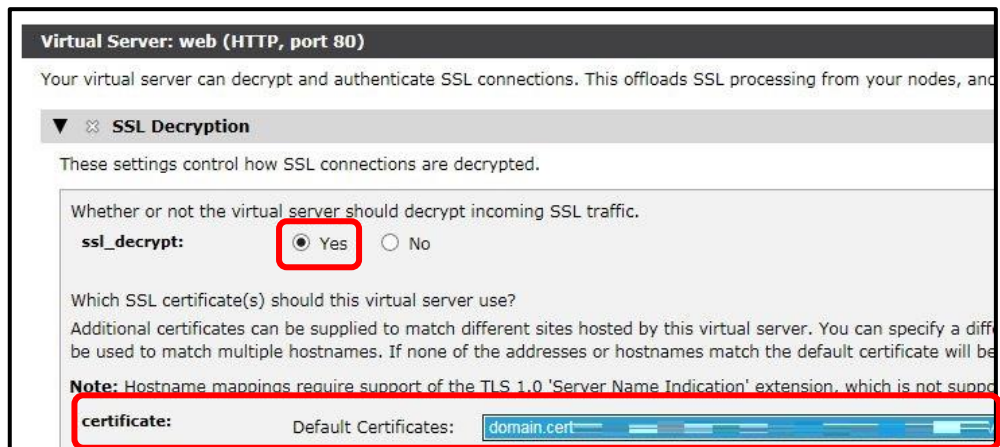


- ② [Virtual Servers] 画面で[SSL Decryption] を押下します。



- ③ [SSL Decryption] 画面で下記設定を行い、ページ最下段の[Update] を押下します。

[ssl_decrypt]:	[Yes]に変更
[certificate]:	[作成した証明書名] に変更



3.2.4 待ち受けポート変更

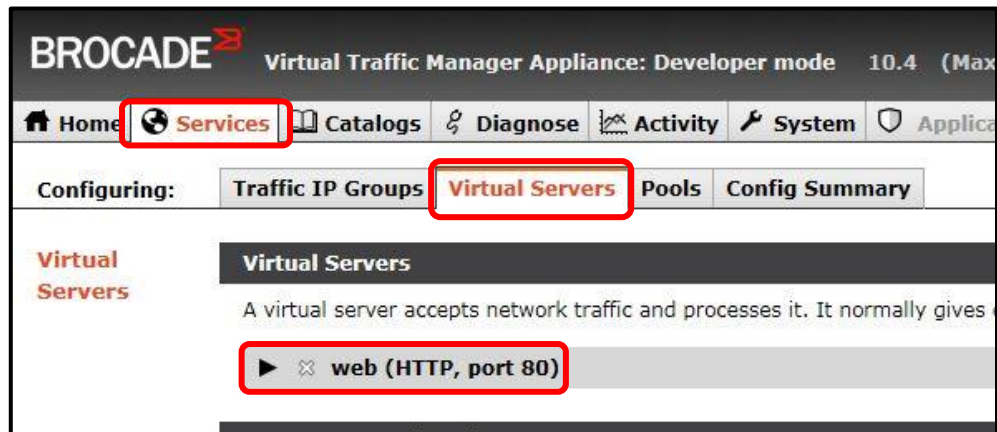
ルート証明書のインポート

中間証明書のインポート

仮想サーバーへの設定

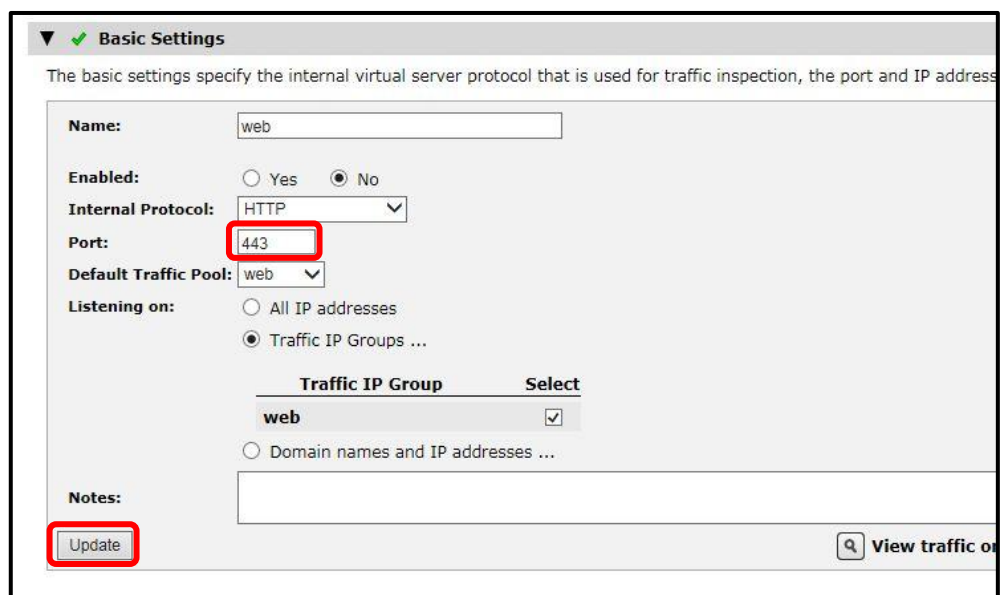
待ち受けポート変更

- ① [Services]メニュー ≫ [Virtual Servers]タブ ≫ [作成した仮想サーバー名]を開きます。



- ② [Virtual Servers] 画面で下記設定を行い、[Update] を押下します。

[Port]: [443] に変更



3.3 負荷分散方法の選択

本項目では、負荷分散アルゴリズムの種類とその設定方法について示します。

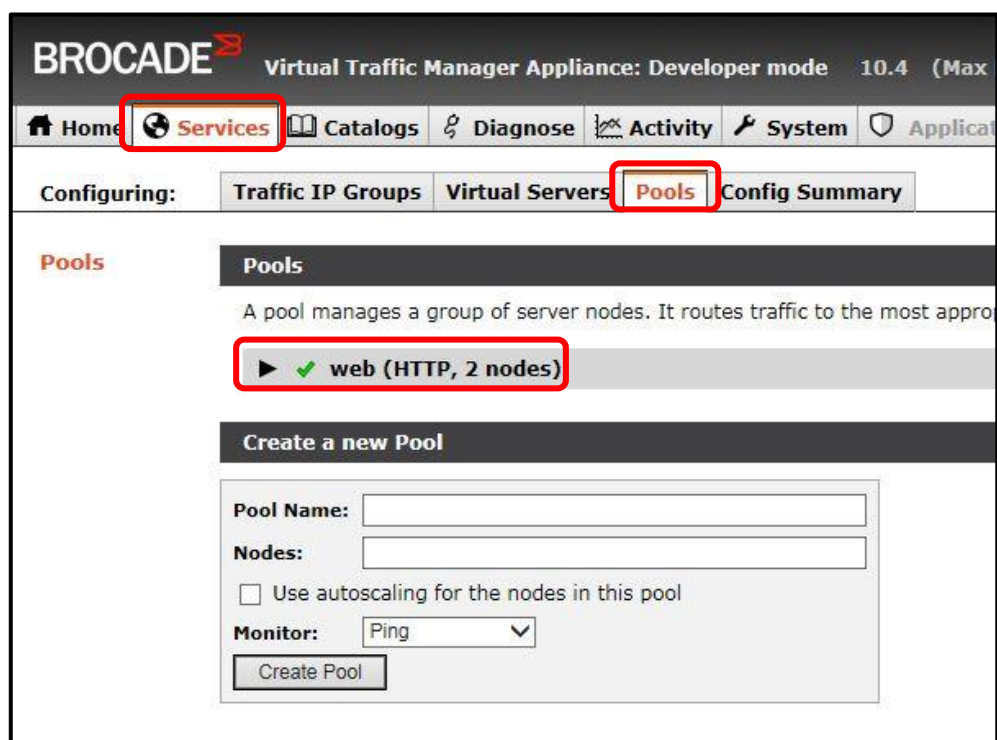
3.3.1 負荷分散アルゴリズムの種類

名称	動作
Round Robin	バックエンドサーバーに順番にリクエストを送信します。 ※デフォルト
Weighted Round Robin	バックエンドサーバーに割当てた重み付けに応じて、リクエストを送信します。
Perceptive	コネクションとデータのレスポンス時間の組合せにより、リクエストを送信するバックエンドサーバーを調整します。
Least Connections	実行中のコネクションが最も少ないバックエンドサーバーへ優先的にリクエストを送信します。
Weighted Least Connections	バックエンドサーバーに割当てた重み付けに応じて、実行中のコネクションが最も少ないバックエンドサーバーへ優先的にリクエストを送信します。
Fastest Response Time	コネクションの応答時間を監視し、最も応答時間の早いバックエンドサーバーへ優先的にリクエストを送信します。
Random Node	ランダムにバックエンドサーバーを選択して、リクエストを送信します。

3.3.2 負荷分散アルゴリズムの設定方法

プール名 : web の負荷分散方式を [Weighted Round Robin] に設定します。

- ① [Services]メニュー ≫ [Pools]タブ ≫ [対象のプール名]を開きます。



- ② [Pools] 画面で[Load Balancing] を押下します。

Pool: web (HTTP)

Virtual servers that use this pool:  **web** Pools that use this pool as their failure pool: *none*

Last Modified: 6 Sep 2018 17:26

▶ **Basic Settings**

The basic settings specify the nodes that the pool is balancing traffic to.

▶ **Load Balancing**

Load Balancing controls how the pool distributes traffic across its nodes.

▶ **Session Persistence**

Session Persistence controls how the pool ensures that client sessions are consistently directed to

- ③ [Load Balancing] セクションに下記設定を行い、[Update] ボタンを押下します。

[Algorithm]:	[Weighted Round Robin] を選択
[Some algorithms require a weighting for each node in the pool.]:	[任意の重み付け] を設定

Pool: web (HTTP, 2 nodes)

Load Balancing controls how the pool selects the destination node for each new request.

▼ **Load Balancing**

Load Balancing chooses the most appropriate node based on response times, least connections or other balancing rules.

The load balancing algorithm that this pool uses.

☐ **Round Robin**
Assign requests in turn to each node.
 ☒ **Weighted Round Robin**
Assign requests in turn to each node, in proportion to their weights.
 ☐ **Perceptive**
Predict the most appropriate node using a combination of historical and current data.

Algorithm:
☐ **Least Connections**
Assign each request to the node with the fewest connections.
 ☐ **Weighted Least Connections**
Assign each request to a node based on the number of concurrent connections to the node and its weight.
 ☐ **Fastest Response Time**
Assign each request to the node with the fastest response time.
 ☐ **Random Node**
Choose a random node for each request.

Some algorithms require a weighting for each node in the pool.

210.158.43.186:80

210.158.43.185:80

- ④ 画面上部に[Your configuration has been updated] が表示されることを確認します。

✔ Your configuration has been updated.

3.4 セッション・パーシステンス(セッション維持)設定

本項目では、VTM のセッション・パーシステンス(スティッキーセッション)の種類とその設定手順について示します。

3.4.1 セッション・パーシステンスの種類

【サポートするセッション・パーシステンス・クラス】

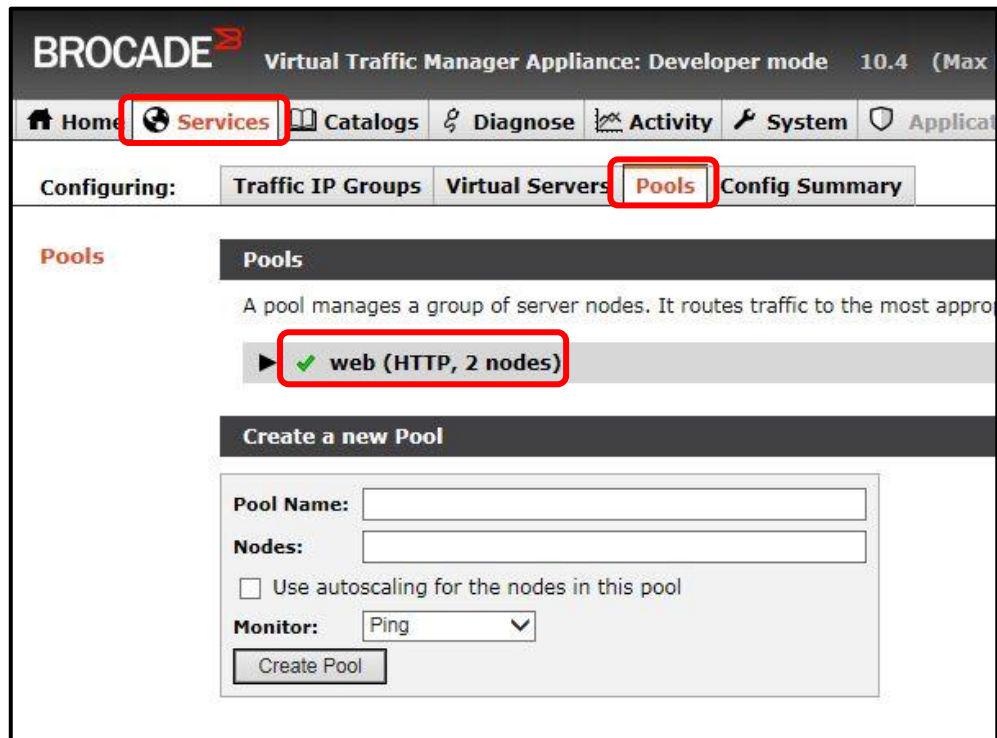
手法	対応プロトコル	内容
IP-based Persistence	全プロトコル	同じソースアドレスからのすべてのリクエストを同じノードに送信します。
Universal session persistence	全プロトコル	このクラスでは、Traffic Script ルールで独自のパーシステンスキーを設定して、リクエストのあらゆる情報に基づいてセッション・パーシステンスを設定することができます。
Named Node persistence	全プロトコル	この手法では、Traffic Script ルールで接続を特定のノードに振り向けることができます。
Transparent session affinity	HTTP, HTTPS	レスポンスにクッキーを挿入して、セッションをトラッキングします。
Monitor application cookies	HTTP, HTTPS	指定アプリケーションクッキーをモニタリングして、セッションを識別します。
J2EE	HTTP, HTTPS	Java の JSESSIONID クッキーとその URL-Rewriting フォールバックをモニタリングします。
ASP および ASP.net	HTTP, HTTPS	この手法を使うと、セッション・パーシステンスを使って、両方のタイプの ASP セッションを処理できます。
X-Zeus-Backend cookies	HTTP, HTTPS	宛先ノードを指定する X-Zeus-Backend という名前のアプリケーションクッキーを検査します。
SSL Session ID persistence	SSL プロトコル	SSL セッション ID を使ってセッションを識別します。

3.4.2 セッション・パーシステンスの設定方法

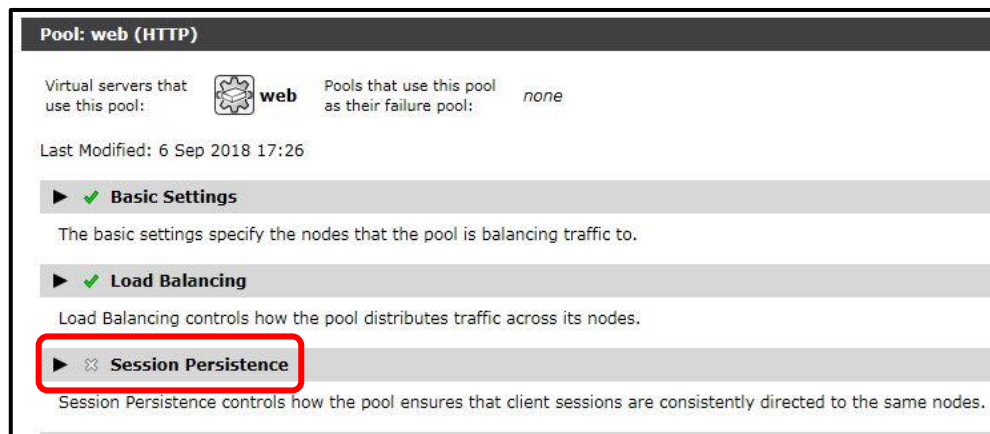
例として、下記の条件について設定します。

- プール名：web のセッション・パーシステンス・カタログを作成し、任意の方式に設定します。

- ① [Services]メニュー ≫ [Pools]タブ ≫ [対象のプール名]を開きます。



- ② [Pools] 画面で [Session Persistence] を押下します。



- ③ [Edit Session Persistence]画面で[Manage Session Persistence Classes]を押下します。

Pool: web (HTTP, 2 nodes)

Session Persistence ensures that all requests from a client will always get sent to the same node.

Choose Session Persistence Class

There are no Session Persistence classes to choose from.

 **Manage Session Persistence Classes**

- ④ [Session Persistence Catalog]画面に下記設定を行い[Create Class]ボタンを押下します。

[Name]:

Session Persistence Catalog

The Session Persistence Catalog contains a set of classes which control session persistence.

Your Session Persistence catalog is empty.

Create new Session Persistence class

Name:

Create Class ☒ and associate it with pool **web**

- ⑤ [Basic Settings]画面に下記設定を行い、ページ最下段の[Update]ボタンを押下します。

[type]:

Class: web

Rules using this: none

Pools using this:  web

Last Modified: 12 Sep 2018 16:43

Basic Settings

Each Session Persistence class controls two main issues: How to identify requests from the same session, and what action to take if the required

Name:

The type of session persistence to use.

type:

- ☒ **IP-based persistence**
Send all requests from the same source address to the same node.
- ☐ **Universal session persistence**
Use session persistence data supplied by a TrafficScript rule.
- ☐ **Named Node session persistence**
Use a node specified by a TrafficScript rule.
- ☐ **Transparent session affinity**
Insert cookies into the response to track sessions.
- ☐ **Monitor application cookies ...**
Monitor a specified application cookie to identify sessions.
- ☐ **J2EE session persistence**
Monitor Java's JSESSIONID cookie and URLs
- ☐ **ASP and ASP.NET session persistence**
Monitor ASP session cookies and ASP.NET session cookies and cookieless URLs.
- ☐ **X-Zeus-Backend cookies**
Inspect an application cookie named 'X-Zeus-Backend' which names the destination node.
- ☐ **SSL Session ID persistence**
Use the SSL Session ID to identify sessions (SSL pass-through only).

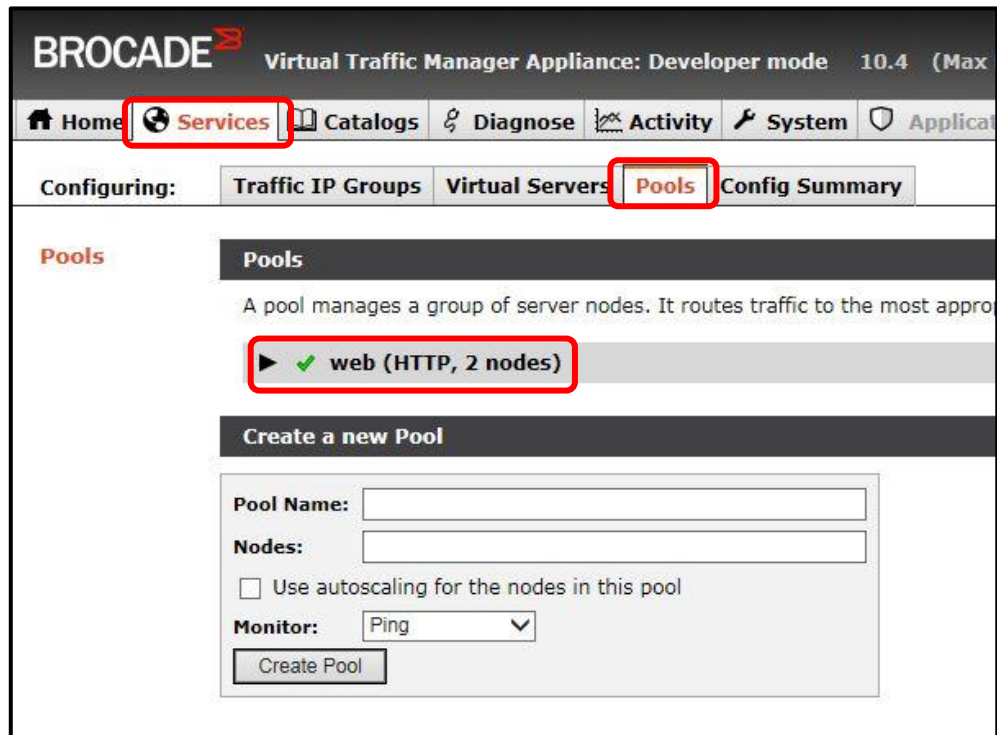
3.5 ヘルスモニタリング(死活監視)設定

本項目では、VTM が振り分け先サーバーに対してヘルスモニタリングを行う設定の手順を示します。

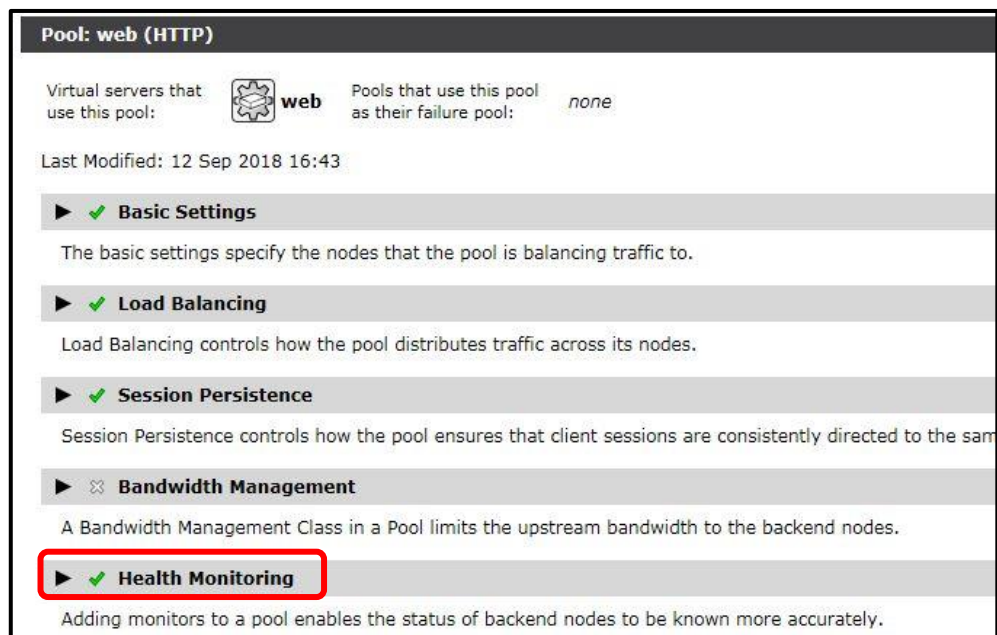
例として、下記の条件について設定します。

- プール名 : web のヘルスモニタリングを HTTP のポート監視を行う [Simple HTTP] に設定します。

- ① [Services] メニュー ≫ [Pools] タブ ≫ [対象のプール名] を開きます。



- ② [Pools] 画面で [Health Monitoring] セクションを押下します。



- ③ [Add Monitor]に[Simple HTTP]を選択し、[Add Monitor]ボタンを押下します。

Pool: web (HTTP, 2 nodes)

Monitors

Monitors watch the nodes in a pool, and inform the traffic manager if the nodes are functioning correctly.

► Ping

Add monitor: Simple HTTP Add Monitor Manage Monitors in Catalog

- ④ デフォルトで設定されている[Ping]設定を削除するため、[× Remove]ボタンを押下します。

Pool: web (HTTP, 2 nodes) Unfold All / Fold All

Monitors

Monitors watch the nodes in a pool, and inform the traffic manager if the nodes are functioning correctly.

► Ping × Remove Edit

► Simple HTTP × Remove Edit

Add monitor: Client First Add Monitor Manage Monitors in Catalog

- ⑤ [Update] ボタンを押下します。

Pool: web (HTTP, 2 nodes)

Monitors

Monitors watch the nodes in a pool, and inform the traffic manager if the nodes are functioning correctly.

► Simple HTTP

Add monitor: Client First Add Monitor Manage Monitors in Catalog

Passive monitoring

Whether or not the software should check that 'real' requests (i.e. not those from monitors) to this pool application normally be enabled, so that when a node is refusing connections, responding too slowly, or sending back invalid responses, it can be detected as failed, and stop sending requests to it. If this is disabled, you should ensure that suitable health monitors are configured to check your servers instead of the traffic manager, so that failures can be detected and subsequently retried.

passive_monitoring: ☒ Yes ☐ No

Apply Changes

Update

- ⑥ 画面上部に[Your configuration has been updated] が表示されることを確認します。

3.6 Sorry サーバー設定

本項目では、プールに属するすべてのサーバーが、リクエストに対するレスポンスができない状態に陥った際にアクセスする Sorry サーバーの設定方法について示します。

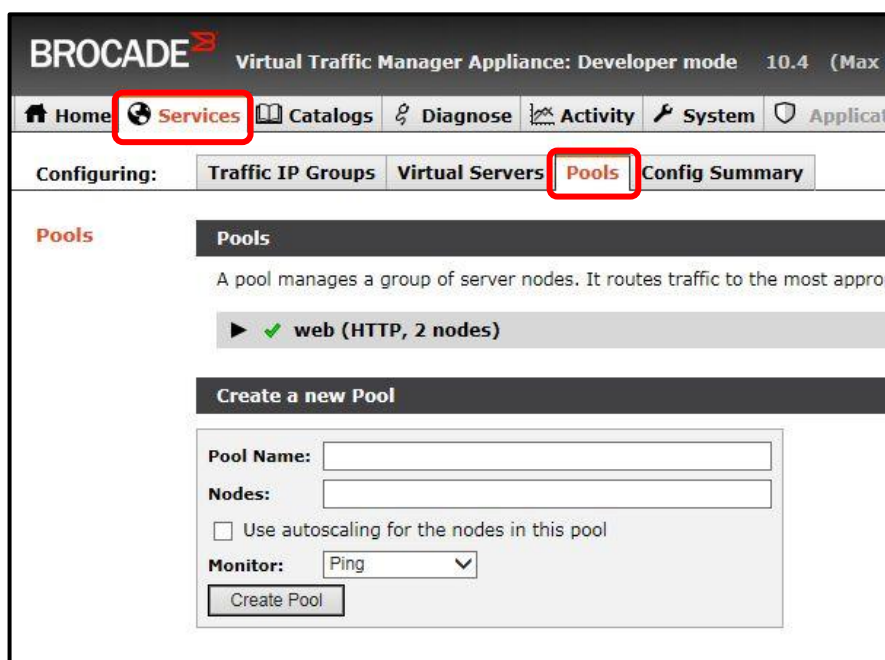
例として、下記の条件について設定します。

Sorry サーバー・プール名	Sorry サーバー : ポート番号	監視方式
sorry_pool	210.158.43.182:80	Simple HTTP

- すべてのサーバーがダウンしている場合、リクエストを 210.158.43.182:80 へ送信します。

3.6.1 Sorry サーバー・プールの登録

- ① [Services]メニュー ≫ [Pools]タブを開きます。



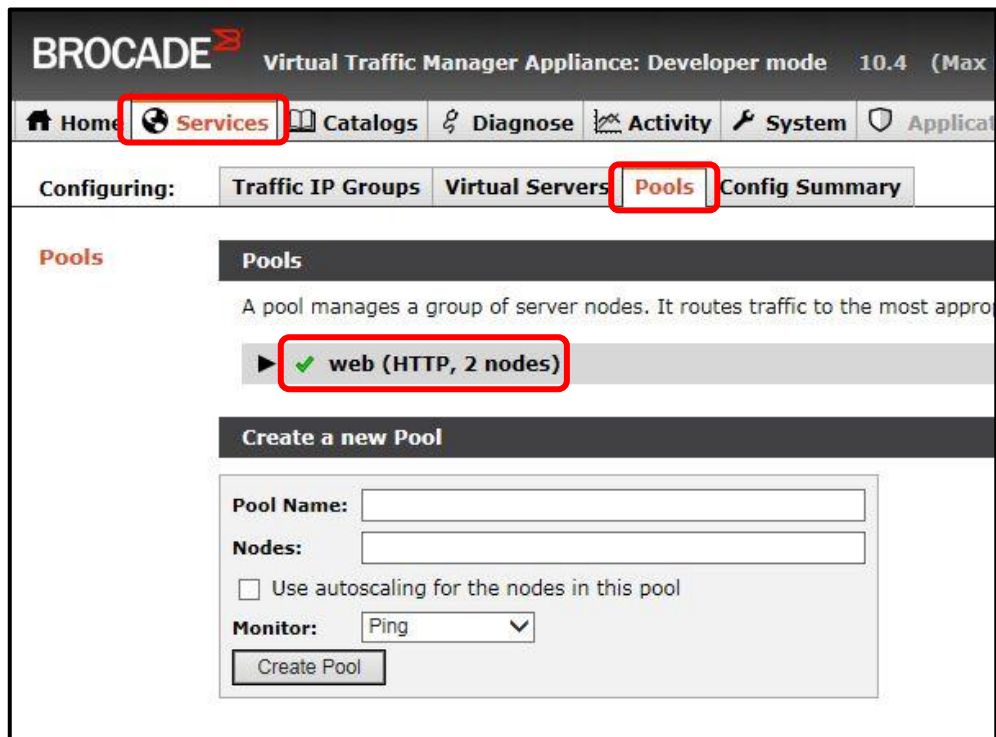
- ② [Create a new Pool] 画面で下記設定を行い、[Create Pool] を押下します。

[Pool Name] :	sorry_pool
[Nodes] :	210.158.43.182:80
[Monitor]	[ヘルスモニタリング方法]



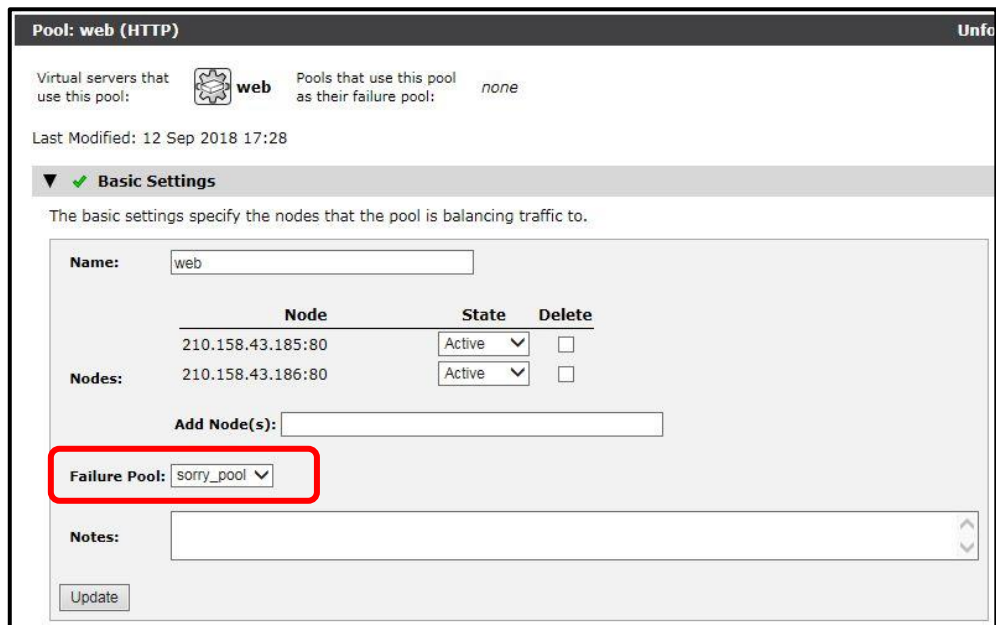
3.6.2 プールへ Sorry サーバー・プールを登録

- ① [Services]メニュー ≫ [Pools]タブ ≫ [対象のプール名]を開きます。



- ② [Pools] 画面の [Basic Settings] に下記設定を行い、[Update] を押下します。

[Failure Pool]:	sorry_pool
-------------------	------------

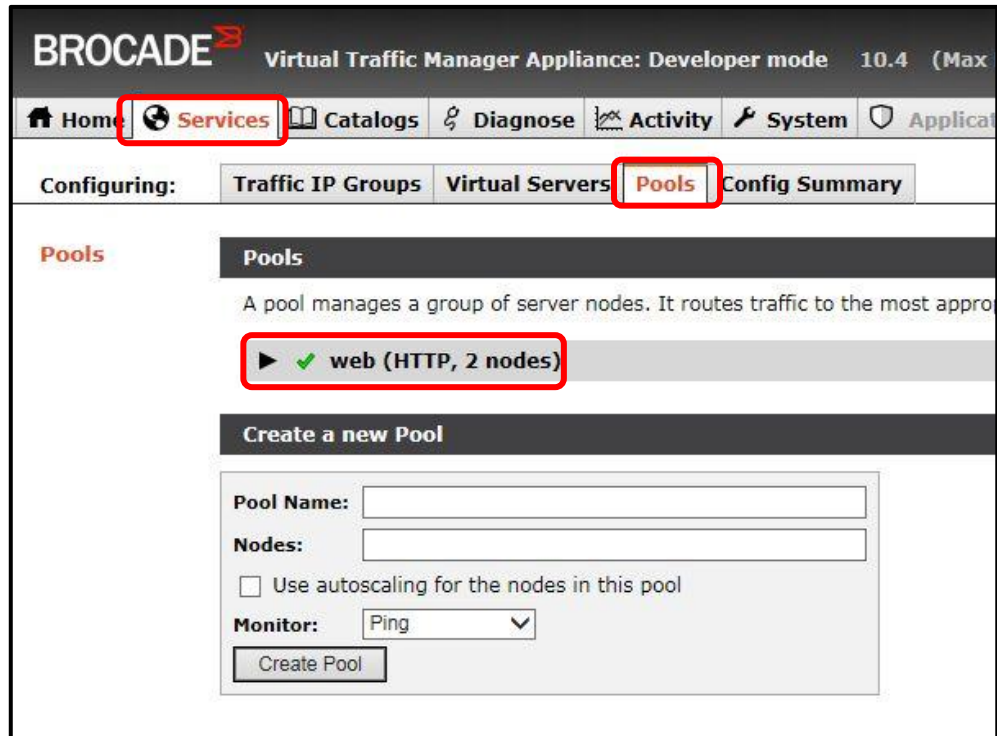


3.7 クライアント IP アドレス透過設定

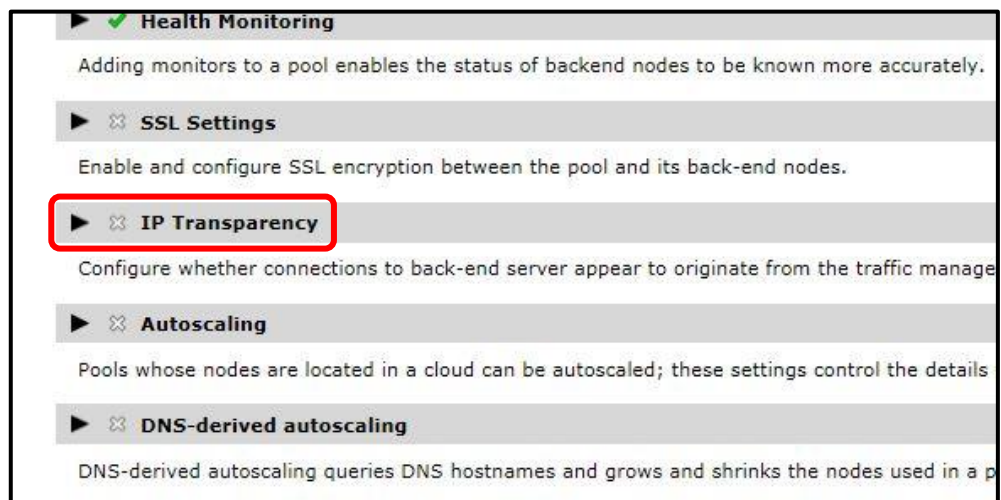
本項目では、クライアントの IP アドレスをバックエンドサーバーに透過する設定について示します。

デフォルト設定では、VTM がバックエンドサーバーにリクエストを送信する際のソース IP アドレスは VTM 自身のアドレスとなります。

- ① [Services]メニュー >> [Pools]タブ >> [対象のプール名]を開きます。



- ② [Pools] 画面で、[IP Transparency] セクションを押下します。



- ③ [IP Transparency] 画面に下記設定を行い、[Update] ボタンを押下します。
- [transparent] を [Yes] に変更します。

Pool: cent-www (HTTP, 2 nodes).

Configure whether connections to the back-end server should appear to originate from the traffic manager or the source client IP address.

▼ IP Transparency

The IP transparency settings allow you to configure whether or not the traffic manager should preserve the source IP address and support and correctly configured routing tables on the back-end nodes. Refer to the User's Guide for more information.

Whether or not connections to the back-ends appear to originate from the source client IP address.

transparent: ☒ Yes ☐ No

Where possible, the traffic manager will use the system's packet filter rules tables to implement IP transparency. Managing how the traffic manager uses iptables are available on the *System > Networking* page.

▶ Modify global IP transparency settings

Apply Changes

Update

4 よくある質問と回答

Q: 送信元の IP を変換されたくない、IP を透過した接続を実施したい。

A: 『3.7 クライアント IP アドレス透過設定』を参照ください

Q: ロードバランサー上で SSL 処理をしたい

A: 『3.2 SSL 通信の復号化設定』を参照ください

Q: ロードバランサーに接続するトラフィック量を増やしたい

A: 弊社の営業までご相談ください、