ニフクラ環境

Ivanti Virtual Traffic Manager セットアップ手順書

図研ネットウエイブ株式会社
2025 年 6 月 ver7.7.1

変更履歴

Ver7.0	[2021 年 4 月] ・ver20.1r1 の説明に変更
Ver7.1	[2021 年 5 月] ・P14 の記載を以下のように変更 (変更前) CentOS では、vTM ver18.2 系は CentOS 7.x、ver20.1 系は CentOS 8.x がシステム要件のカーネルバージョンになります。 (変更後) CentOS では、vTM ver18.2 系は CentOS 7.x、ver20.1 系は CentOS 7.x、CentOS 8.x がシステム要件のカーネルバージョンになります。
Ver7.2	[2022 年 5 月] ・P42 flipper!frontend_check_addrs の項目に「複数の宛先アドレスを追加頂くことを強く推奨します。」という文言及び設定例を追記
Ver7.3	[2022 年 11 月] ・ver22.2 の説明に変更
Ver7.4	[2024 年 1 月] ・P10 トランスペアレント動作に関する記載を修正 ・P11 NAT 設定に関する記載を修正 ・P18 弊社サポートサイトにログインする際の ID とパスワード情報を修正 ・P61 IP トランスペアレントの設定に関する記載を修正
Ver7.5	[2024 年 5 月] ・P100 軽微な誤りを修正
Ver7.6	[2024 年 7 月] ・P14、P15「パブリックイメージ」の表記を「スタンダードイメージ」に修正 ・P87「アップグレード手順」の章を追加

Ver7.7	[2024 年 11 月] ・P27「管理 UI へのアクセス制限」に関する記載を追加 ・バージョン「22.2」の表記を「22.2r1」に変更 ・P63 RuleBuilder を使用した設定の説明を一部修正
Ver7.7.1	[2025 年 6 月] ・P119 現行 LTS バージョンのサポート期間を更新

目　次

1. 本書の目的

本書はニフクラ環境において Ivanti Virtual Traffic Manager （以下：vTM） の構築を行うためのファーストステップガイドです。

配布及び内容の一部または全体の複製、ニフクラ環境でレイヤー7（L7）ロードバランサーのサービスをご使用中以外のお客様のご利用は固くお断りしております。

本書の内容とメーカー提供のマニュアル、ソフトウェア内のヘルプの説明が異なる場合、メーカー提供のマニュアル、ソフトウェア内のヘルプの内容が優先されます。

図研ネットウエイブがサポートを提供する範囲は vTM の部分のみとなります。

図研ネットウエイブではニフクラ環境に関連する機能の設定、対応、Google 等の検索エンジンで検索可能な一般的な Linux コマンド操作、設定プロトコルの仕様、動作についてのサポート、対応は行っておりません。

仮想サーバー基盤、オペレーティングシステム(OS)等のニフクラ側での対応範囲、また、ニフクラ環境の設定につきましてはニフクラ様の FAQ をご確認いただき、ご質問はニフクラ問合せ窓口までお問合せください。

負荷分散サービスの詳細な設定方法、本書に掲載のない情報につきましては

・弊社サポートサイト

・メーカー提供のマニュアル

・管理画面（以下：管理 UI）から参照可能なヘルプでご確認ください。

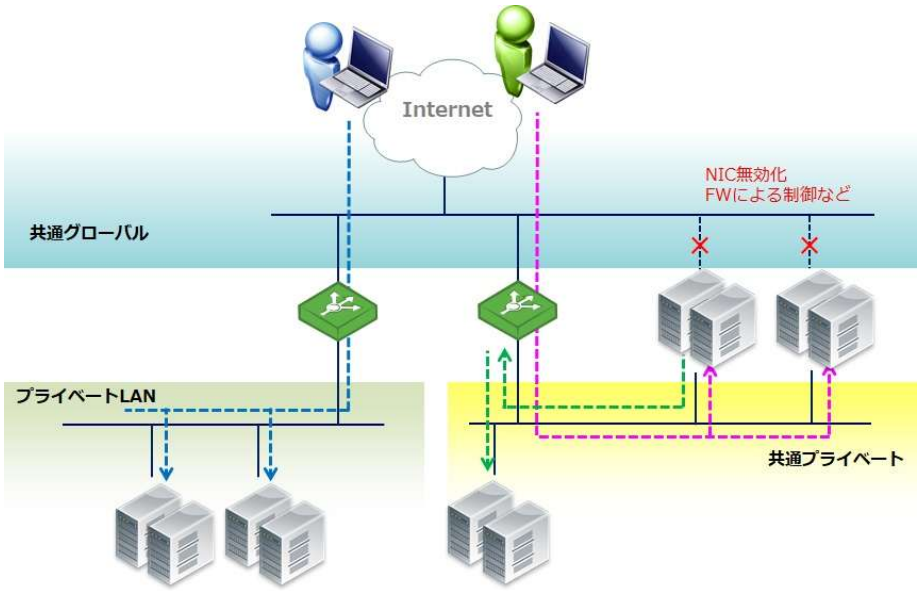
vTM の設定の説明、対応は有償サービスメニューになっております。

設定に関して詳細なご説明をお求めの場合は有償サービスメニューをご利用ください。

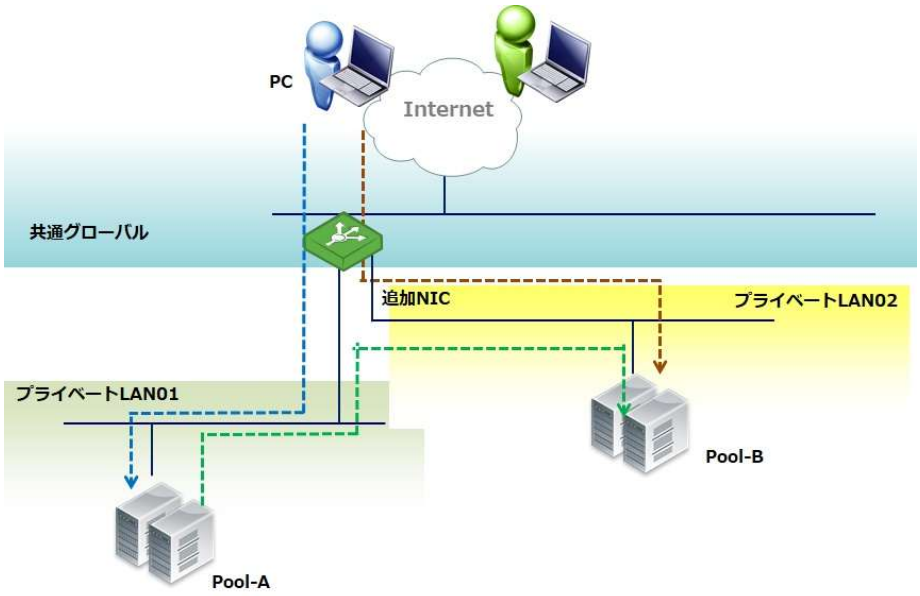
2. ニフクラ環境での動作

1) ニフクラ環境での動作

vTM の負荷分散機能は全てのリージョン、ゾーンで、通常構成（共通グローバル、共通プライベート）、プライベート LAN に設定いただくことができます。



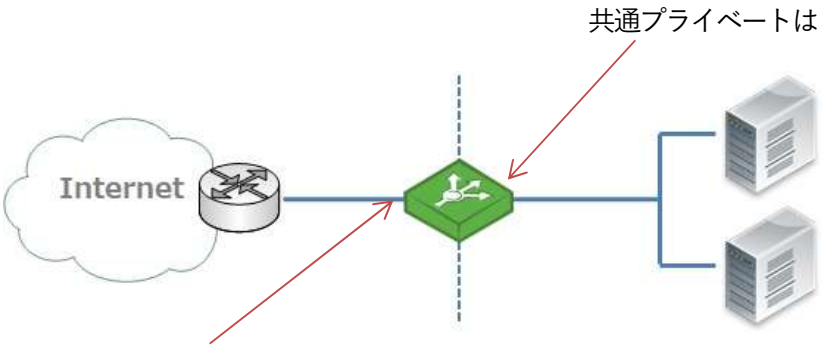
vTM で NIC を追加する場合（実際は OS への追加）



2) 1 台構成の動作

共通グローバル、共通プライベートの IP アドレスは DHCP で割り当てられます。

グローバル側に複数の IP アドレスを設定する場合はマルチ IP アドレス環境への申し込みとなります。



マルチ IP 環境では OS のインターフェース設定で IP アドレスを設定します。
負荷分散用バーチャル IP アドレス(TIP)は vTM の WebUI で設定します。

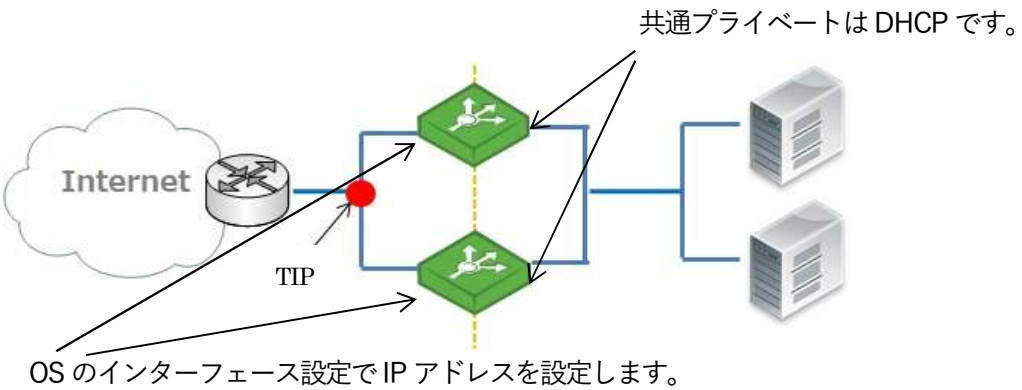
※設定されたバーチャル IP アドレスのことを、vTM システム上では Traffic IP Address（以下：TIP）と呼びます。

3) 2 台構成(冗長構成)の動作

共通グローバルを利用した冗長構成では固定 IP アドレスを設定します。ニフクラ環境のマルチ IP アドレスへの申し込みを行います。

マルチ IP アドレス環境ではグローバル側の IP アドレスを OS のインターフェースに手動で設定します。

クライアントからのアクセスを受付する TIP は、vTM の WebUI で設定します。



TIP は vTM の WebUI で設定します。

4) ワンアーム構成

共通グローバルまたは共通プライベートのどちらか一方のネットワークインターフェースを使用した構成にも対応できます。

5) トランスペアレント動作

ニフクラ環境の基本構成では、接続元からのアクセスを vTM が Proxy し、ノードに設定するバックエンドサーバー（以下：バックエンドノード）にアクセスを渡します。

デフォルトの設定ではバックエンドノードに記録されるアクセス元 IP アドレスは vTM の IP アドレスとなります。

vTM をトランスペアレントで動作させることで、vTM の IP アドレスではなく、接続元の IP アドレスに変わります。（トランスペアレント動作でも MAC アドレスは vTM の MAC アドレスでのアクセスとなります）

トランスペアレントの動作では、バックエンドノードのデフォルトゲートウェイを vTM のプライベート側のネットワークインターフェースに向けていただく必要があります。

ニフクラ環境では、共通グローバルまたは共通プライベートと、プライベート LAN(※1)との 2 つのネットワーク間に vTM を構成することで、vTM をトランスペアレントで動作させることができます。

（※1）vTM の IP アドレス及びバックエンドノードの IP アドレスはともに、プライベート LAN をご利用ください。ニフクラのプライベート LAN のご利用には別途料金が必要です。

6) 追加 NIC の設定

ニフクラ環境ではプライベート LAN のネットワークセグメントに対して NIC を追加することができます。

追加 NIC はニフクラ環境メニュー、OS 側のインターフェース設定で行います。

vTM は OS 側で設定されたインターフェースを利用するため、追加された NIC についても認識しますの

で、利用することができます。

利用できる NIC 数はニフクラ環境の制約や、OS によって制約があります。

7） NAT 設定

ニフクラ環境では、バックエンドノードからの外部への通信を vTM 経由で行う際には、vTM が動作している OS 側の機能による NAT の設定(※1)を行い、バックエンドノード vTM の IP アドレスで発信元 NAT を行う必要があります。

(※1) NAT の設定を利用する場合には、vTM、バックエンドノードともにプライベート LAN をご利用ください。ニフクラのプライベート LAN のご利用には別途料金が必要です。

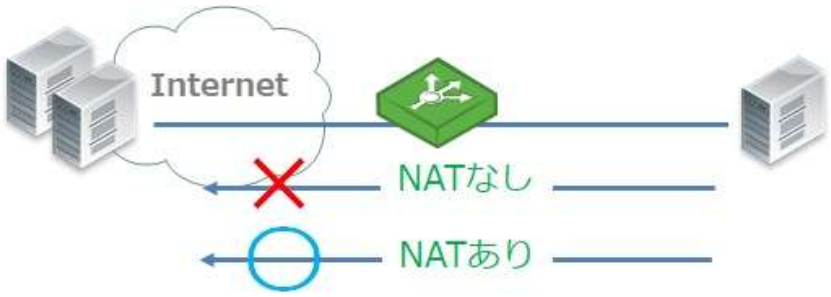
NAT が動作することで vTM を経由してバックエンドノードから外部への通信が行われます。

NAT 動作ではバックエンドノードのデフォルトゲートウェイに、vTM のプライベート側のネットワークインターフェースの IP アドレスを設定します。

NAT 設定ではご利用状況が過多の場合に通信障害が発生することがあります。

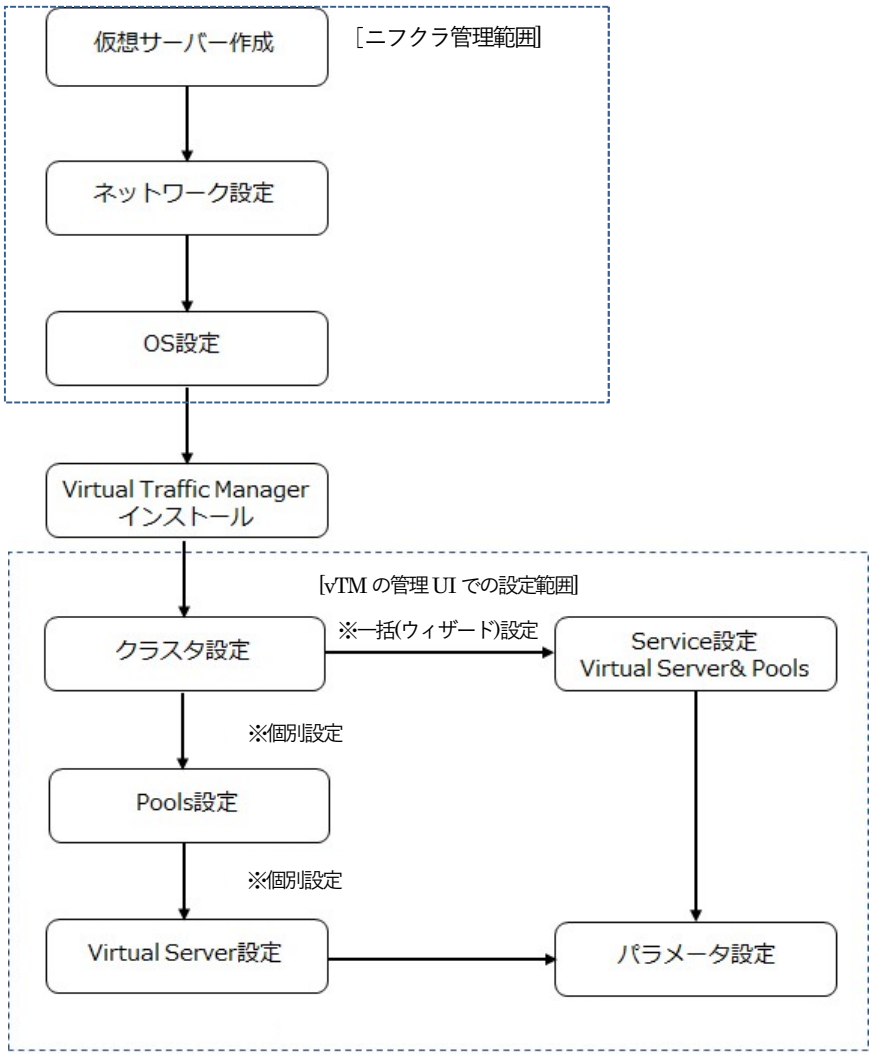
事前にお客様側でカーネルの TCP パラメータについて検討し、必要に応じてパフォーマンスチューニングを実施してください。

※通常の負荷分散設定(クライアントからバックエンドノードへの通信を vTM で負荷分散させる設定)には、NAT 設定は不要です。バックエンドノード発の通信をさせたい場合に NAT 設定を行います。



3. 仮想サーバー作成、vTM 設定の流れ

ニフクラ環境での仮想サーバー作成から vTM 設定までの流れは以下になります。



2 台以上でクラスタを構成する場合、vTM への設定はクラスタ構成後の設定を推奨しています。

Virtual Server、Pool のパラメータ設定、vTM 自身の設定はバックエンドノードで提供するアプリケーションの動作や接続元からのアクセスを考慮しながら実施しなければならないことがあります。

1) ライセンス申し込み

ニフクラ様に vTM のライセンスを申し込みします。

ライセンスにはご利用の IP アドレス情報が必要となります。

ライセンスの申し込みはご利用の IP アドレスの情報を確認したうえで行ってください。

申し込み方法はニフクラ問合せ窓口にお問合せください。

2) マルチ IP アドレス申し込み

2 台以上（冗長）構成において共通グローバル側でのご利用時にはニフクラ マルチ IP アドレス環境への申し込みを行ってください。

ニフクラ マルチ IP アドレス環境に申し込み後、ニフクラ様からお客様へネットワーク設定に関する情報がメールで通知されます。

メールに記載されている情報を基に、vTM が動作することになる仮想サーバー(OS)のネットワークインターフェースにスタティックの IP アドレスの設定を行います。

申し込み方法はニフクラ問合せ窓口にお問合せください。

4. ニフクラ仮想サーバーの作成、設定

※ニフクラ コントロールパネル上の表記は「サーバー」です。この「サーバー」上で OS、vTM が動作することになります。

ニフクラ コントロールパネルのサーバーメニューからサーバー作成を行います。

ニフクラで公開しているスタンダードイメージから Linux 系の OS を選択し、サーバーを作成します。

vTM のシステム要件にはカーネルと glibc のバージョンが指定されています。

各バージョンとも Java のセッション維持などを利用される場合は別途 Java のインストールが必要となります。

CentOS では、vTM ver19.2 系、ver20.1 系、ver22.2 系は CentOS 7.x がシステム要件のカーネルバージョンになります。

※ver19.2 系、ver20.1 系は CentOS 6.x にも対応しておりますが、ver22.2 系は CentOS 7.x のみ対応となりますので、ご注意ください。

	カーネルバージョン	glibc バージョン
ver.19.2 系	2.6.32 - 4.15	2.12 以上
ver20.1 系	2.6.32 - 5.2	2.12 以上
ver22.2 系	3.10－5.13	2.17 以上

vTM に求められるスペック要件は vCPU:1 以上、メモリ 2GB 以上です。

SSL 処理性能を求める場合、トラフィック量が多い場合は vCPU、メモリ量が多いタイプを選択します。

推奨スペックにつきましては、ニフクラ環境の L7 ロードバランサー（vTM）仕様・機能の説明ページに推奨サーバーの参考資料が掲載されております。

また、必要なスペックに関するご質問はニフクラ問合せ窓口までお問合せください。

■サーバータイプ(CPU 数)の変更

vTM が動作する仮想サーバーのサーバータイプ(CPU 数)を変更する場合、vTM が稼働中ですと管理 UI にエラーや警告が表示されることがあります。

そのため、vTM のサービスを停止してから、サーバータイプ(CPU 数)を変更してください。

仮想サーバーのサーバータイプ(CPU 数)変更方法に関するご質問はニフクラ問合せ窓口までお問合せください。

※vTM のサービスを停止する場合は、本ドキュメントの［補足 1 コマンド］ページの「vTM サービス 停止」コマンドをご参照ください。

1) 仮想サーバーの作成

ニフクラ コントロールパネルから、OS、vTM が動作することになる仮想サーバーを作成します。

2) OS 側の設定

作成した仮想サーバーに OS の設定を行います。

① 必要なモジュール

システム要件以外に以下のモジュールをインストールすることを推奨しています。

ニフクラで公開しているスタンダードイメージの利用時に含まれてない場合はインストールをお勧めします。

net-tools	netstat コマンド利用のために必要となります。
gdb	デバッグによるエラー発生時、解析に必要となります。
Java	Java Extensions の利用 デフォルトで有効（Yes）となっております。 不要な場合は、vTM 稼働後、System＞Global settings＞Java Extension Settings の java!enabled の設定を No（無効）に変更してください。

② 設定

vTM ソフトウェアをインストールする前に、以下の仮想サーバー(OS)の設定を行います。

・ホスト名の指定

・DNS 参照または名前解決の指定

・時刻修正、同期

・余分なサービスの停止

vTM の負荷分散サービスにおいて利用するポート番号が競合するサービスを停止させます。

iptables6 は有効にします。

3) ネットワーク設定

作成された仮想サーバー(OS)に IP アドレスやスタティックルートなどのネットワークを設定します。

vTM ソフトウェアインストール後に IP アドレスやスタティックルートを設定する場合は、vTM のサービスを停止したうえで実施してください。

4) OS 側のチューニング設定

パフォーマンスチューニングを実施される場合は、お客様側で、カーネルの TCP パラメータを検討、チューニング設定してください。

以下は参考となりますが、Virtual Appliance 版（vTM に OS も含めて提供）の値になります。

※ニフクラ環境に弊社が提供しているのはソフトウェア版（vTM ソフトウェアのみ提供）となります。

項　　目	VA 版　値
/proc/sys/fs/file-max	2097152
/proc/sys/net/ipv4/ip_local_port_range	1024-65535
/proc/sys/net/ipv4/tcp_fin_timeout	60

/proc/sys/net/ipv4/tcp_syncookies	1
/proc/sys/net/core/somaxconn	1024
/proc/sys/net/ipv4/tcp_max_tw_buckets	1800000
/proc/sys/net/ipv4/tcp_slow_start_after_idle	0
/proc/sys/net/ipv4/tcp_timestamps	1
/proc/sys/net/ipv4/tcp_window_scaling	1
/proc/sys/net/netfilter/nf_contrack_max	10485752

nf_contrack_max の設定がない場合は、/etc/modules.conf　または　/etc/modprobe.d/<任意のファイル名>　に以下を記述します。

　options ip_conntrack hashsize=　任意の値

　options nf_conntrack hashsize=　任意の値

詳しくは以下のメーカーサイトをご確認ください。

https://community.pulsesecure.net/t5/Pulse-Secure-vADC/Routing-and-Performance-tuning-for-Stingray-Traffic-Manager-on/ta-p/28504

また、チューニング設定については以下のメーカーサイトの内容についてもご確認ください。

https://community.pulsesecure.net/t5/Pulse-Secure-vADC/Tuning-the-Linux-operating-system-for-Stingray-Traffic-Manager/ta-p/28501

5. Virtual Traffic Manager (vTM)ソフトウェア

1) vTM ソフトウェアのインストール

弊社サポートサイトからソフトウェアをダウンロードします。

弊社 URL（https://www.znw.co.jp/support）にアクセスいただき、「Virtual Traffic Manager サポートサイト」をクリックします。

以下の ID とパスワードでログインします。

ID: **steelapp-limit**

Password: **sa*8USpuY8dR**

サポート情報＞ファームウェア DL からソフトウェア版のファイルをダウンロードします。

Ver. 22.2r1 のインストール用ファイルは　ZeusTM_222r1_Linux-x86_64.tgz（※）になります。

（※）222r1 は ver22.2r1 を示します。他のバージョンを利用する際には異なる番号となります。

ダウンロードしたファイルをファイル転送ソフト（WinSCP 等）で仮想サーバーにアップロードします。

アップロード完了後、以下のコマンドを実行します。

 # tar zxvf ZeusTM_222r1_Linux-x86_64.tgz

ファイルが解凍されます。

解凍後、以下のコマンドを実行し、該当バージョン名のフォルダに移動してインストールを開始します。

＃cd ZeusTM_222r1_Linux-x86_64

 # ./zinstall

表示メッセージに合わせて以下のように入力します。

```
# ./zinstall

You are installing a package built for Linux-x86_64
Pulse Secure Virtual Traffic Manager Installation Program
Copyright (C) 2022, Pulse Secure, LLC. All rights reserved.

Checking distribution ... all packages match checksums
-----------------------------------------------------------------------
```

Use of this software is subject to the Pulse Secure Terms and Conditions
of Sale.

Please review these terms, published at
https://www.pulsesecure.net/support/eula before proceeding.

Enter `accept' to accept this license, or press return to abort:
“accept”を入力し、Enter キーを押します

Where should the product be installed? [/usr/local/zeus]: **Enter キーを押します**

Installing zxtm-22.2r1...
Installing admin-22.2r1...
Installing updater-22.2r1...
Installing zxtmadmin-22.2r1...
Installing stingrayafm-22.2r1...
Installing zxtmadmin_lang_en_gb-22.2r1...
Installing zxtmadmin_lang_en_us-22.2r1...

Pulse Secure Virtual Traffic Manager is now installed in /usr/local/zeus.

Are you ready to perform the initial configuration now ? (Y/N) [Y]: **Enter キーを押します**

Running /usr/local/zeus/zxtm/configure

Pulse Secure Configuration Program
Copyright (C) 2022, Pulse Secure, LLC. All rights reserved.

This program will perform the initial configuration of the
Pulse Secure Virtual Traffic Manager.

Each traffic manager in your cluster must have a unique name,
resolvable by each member of the cluster.

This traffic manager is currently called 'localhost.localdomain'.
Would you like to

1. Keep the current traffic manager name (default)
2. Specify a new resolvable hostname
3. Use an IP address instead of a hostname

Choose option [1]: **Enter キーを押します**

Generating SSL key for control communications... done
Control SSL fingerprint:
C8:08:C7:04:6E:64:C2:79:8F:3E:12:B0:64:F9:96:42:7E:F8:44:67

Different product features are enabled depending on the license key provided.
If a license key isn't provided now, this product will run
as the Community Edition until a license key is installed.

Enter the license key filename, or leave blank for the Community Edition: **Enter キーを押します**

When using the Community Edition, most of the software functionality is
present, however outgoing bandwidth is restricted to 10 Mb/s and
the maximum cluster size is restricted to 4.
See the user guide for more information about the Community Edition.

Do you wish to use it? Y/N [N]: **“y” を入力し、Enter キーを押します**

Choose a UNIX user for the zxtm process to run as [nobody]: **Enter キーを押します**

Choose a UNIX group for the zxtm process to run as [nobody]: **Enter キーを押します**

Pulse Secure Virtual Traffic Manager can be configured to only allow management
on one specific IP address. This restricts all admin server access, SOAP
management, REST API access and other control information to this IP. This
setup is useful if you want to completely separate your public and private
networks.

Would you like to restrict management to one IP? Y/N [N]: **Enter キーを押します**

Installing SSL key for Admin Server... done

Pulse Secure Virtual Traffic Manager can be installed so that it
automatically runs when this computer boots.

Would you like Pulse Secure Virtual Traffic Manager to start at boot time?
Y/N [Y]: **Enter キーを押します**

Start script linked into /etc/rc2.d/S85zeus
Start script linked into /etc/rc3.d/S85zeus

Generating a unique identifier for this traffic manager... done

Searching for Pulse Secure Virtual Traffic Manager clusters... done

No existing Pulse Secure Virtual Traffic Manager clusters could be found

You may choose to manually specify a different machine to contact
or create a new cluster

C) Create a new cluster
S) Specify another machine to contact

```
Select option [C]: Enter キーを押します

Please choose a password for the admin server: admin アカウントに設定するパスワードを入力します
Re-enter: admin アカウントに設定するパスワードを再度入力します

Would you like to register this vTM with a Services Director? Y/N [N]: Enter キーを押します

Configuration successful

Starting Pulse Secure Virtual Traffic Manager Software... OK

**
** The SHA-1 fingerprint of the admin server's SSL certificate:
**     9A:F2:D7:F2:7E:4C:70:96:0A:C8:AD:A2:B1:34:41:8A:07:60:E8:C1
** Keep a record of this for security verification when connecting
** to the admin server with a web browser and when clustering other
** Pulse Secure Virtual Traffic Manager installations with this one.
**
** To configure the Pulse Secure Virtual Traffic Manager, connect to the admin
** server at:
**     https://localhost.localdomain:9090/
** and login as the 'admin' user with your admin password.
**

Please read the release notes (/usr/local/zeus/zxtm/RELEASE_NOTES)
```

vTM インストール完了後、ブラウザで https://ホスト名（または IP アドレス）:9090 を入力することで、

管理 UI へアクセスすることができます。

2) ログローテート設定

vTM のログファイルは 配下に格納されます。

/usr/local/zeus/zxtm/log/errors	イベントログ
/usr/local/zeus/zxtm/log/audit	認証、操作ログ
/usr/local/zeus/admin/log/access	vTM へのアクセスログ
/usr/local/zeus/admin/log/errors	vTM の起動、停止ログ

vTM をインストールしただけでは、ログファイルはローテートされません。

仮想サーバー(OS)側の/etc/logrotate.d 配下にログのローテートを設定します。

vTM のログをローテートする場合は、以下のシグナルを vTM プロセスに送信する設定を追加します。

```
/bin/kill -USR2 `cat /usr/local/zeus/zxtm/internal/pid | awk '{print$1}'`
```

Virtual Server のロギングはデフォルトで無効です。

クラウド環境ではロギングによる DISK の I/O の負荷となりやすいため、ご利用しないように弊社ではご案内しております。

もしご利用される場合はリソース不足の発生、サービスダウンにつながる要因となることをご理解のうえ、ご利用ください。

Virtual Server を設定する前はロギング用のログファイルは存在しません。Virtual Server の設定を実施したのち、リクエストロギングを有効にすることでログファイルが作成されます。

Virtual Server のログの保管先は Virtual Server の Request Logging の log!filename: の設定項目で指定します。

保管先及びファイル名はデフォルトで %zeushome%/zxtm/log/%v.log の指定になります。

%zeushome%/zxtm/log/ ＝ /usr/local/zeus/zxtm/log と読み替えてください。

ログファイルが肥大化し、空き容量が不足しないよう Request Logging で設定されたログファイルもローテートの設定が必要となります。

vTM は空き容量が不足した場合に、動作や処理に影響が出ることがあります。

3) サーバーコピー、イメージからの仮想サーバー作成

vTM をインストールした仮想サーバー作成後のニフクラ環境のサーバーコピーやイメージからの仮想サー

バー作成については弊社ではサポートしておりませんので、ニフクラ問合せ窓口にお問合せください。

サーバーコピーやイメージからの仮想サーバー作成後、vTM では以下の操作が必要になります。

・ホスト名、IP アドレス変更した場合、vTM の再インストール

・vTM の UUID の変更

なお、本番環境のインスタンスを検証環境にコピーしてライセンスをそのまま使用することは、ライセンス違反にあたります。

検証環境には、新たな評価ライセンスが必要となりますので、ご注意ください。

■vTM の UUID の変更

System＞Traffic Managers メニューの Manage **** の UUID の項目で Regenerate ボタンをクリックします。

Cluster を構成する vTM で同じ UUID が設定されていると Cluster の構成エラーとなります。Cluster を構成する前に UUID を変更してください。

4) 管理 UI へのログイン

管理 UI へのアクセスは https://＜vTM アドレス＞:9090 でアクセスすることができます。

デフォルトの ID は admin、パスワードはインストール時に設定いただいたパスワードになります。

5) Hotfix の適用

Hotfix がリリースされた場合、管理 UI へログイン後、Hostfix を適用します。

Hostfix は弊社サポートサイトの「サポート情報 ＞ ファームウェア DL」からダウンロードすることがで

きます。

■Hotfix 適用方法

① Hotfix が適用できるバージョンであることを確認します。

② 管理 UI にログインします。

③ ログイン後、System>Traffic Manager メニューの Software Upgrade で Upgrade ボタンをクリックします。

④ Software Package で ファイルを選択 ボタンをクリックし、Hotfix ファイルを選択します。

Upload ボタンをクリックし、Upload したファイルの内容を確認します。

環境のバージョンが同じであることを確認します。

⑤ Select the desired upgrade scope and click Upgrade to begin the upgrade.という項目が表示した場合、Upgrade specified traffic managers.を選択し Hotfix を適用する Traffic Manager を指定します。

Hotfix は一度に複数の Traffic Manager へ適用することができません。

⑥ Install this upgrade ボタンをクリックします。

⑦ アップグレード後、プロセスがリスタートします。

この時、通信断が発生します。

⑧ 管理 UI にログインします。

⑨ System>Traffic Managers メニューの Hotfixes の項目を参照します。

⑩ Hotfix が適用されていることを確認します。

以下は適用時の表示例です。

6） 外部への通信

ver.18.2 以降 Telemetry の設定により外部への通信が発生します。（デフォルト設定 Yes のため）

Telemetry の設定では vTM 内部で収集した設定や基板情報を深夜 0 時～3 時の間に telemetry.zeus.com に送信します。

ユーザ情報などは匿名化されます。

No（無効）にした場合、telemetry.zeus.com への通信は行われません。また既存サービスへの影響はありません。

設定は　System>Global Settings＞Telemetry メニューの telemetry!enabled の設定で行います。

7） オープンポート

vTM を起動させると必要な通信ポートはオープンした状態となります。

必要な通信ポートへのアクセスが出来ない場合、vTM 自身のエラー、フェイルオーバーなどが発生し、動作に支障をきたすことがあります。

TCP/22	SSH
TCP/53、UDP/53	DNS
TCP/443	
TCP/9060、UDP/9060	Java　※利用時
TCP/9070	REST API　※17.2 以降有効
TCP/9080、UDP/9080	Cluster 監視用、コンフィグ同期
TCP/9090	管理 UI アクセス、zcli（コマンドラインモード）
UDP/9090	ハートビート
UDP ランダムポート	コンフィグ同期
ICMP	

このほかに負荷分散サービスを設定するポートがオープンした状態となります。

デフォルトでは vTM が持つ全てのインターフェースで上記の通信が必要となります。

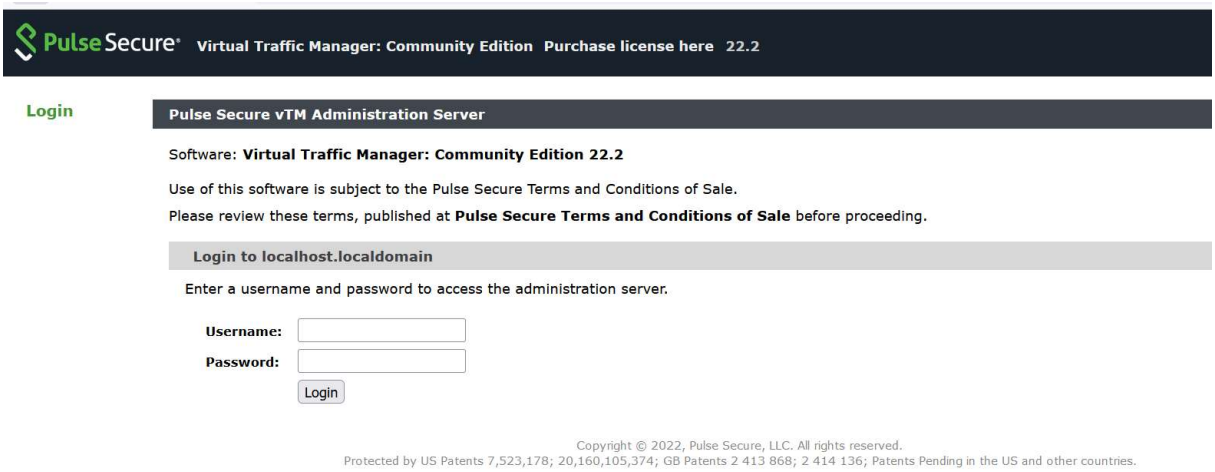
ニフクラ環境では OS 上の設定等により上記以外のポート番号がオープンした状態となることがあります。

6. Virtual Traffic Manager (vTM)の設定

1) 管理 UI へのアクセス方法

管理 UI へのアクセスは　**https://<vTM アドレス>:9090**　を使用してアクセスすることができます。

デフォルトの ID が admin、パスワードはインストール時に設定いただいたパスワードになります。



2) 管理 UI へのアクセス制限

■ニフクラのファイアウォール機能でアクセス元を制限する方法

ニフクラのファイアウォール機能(ルール追加)を使用して、vTM 管理 UI へのアクセス元を制限することができます。

不正なアクセス元からの侵入を防ぐために、こちらの方法で管理 UI へのアクセス元を制限することを強く推奨します。

詳細は下記のページの「IN ルールの追加」の説明をご参照ください。

https://docs.nifcloud.com/cp/help/fw/rule_new.htm

［補足］

※ 操作方法についてのご質問は、ニフクラ問合せ窓口までお問合せください。

■vTM の Restricting Access 機能でアクセス元を制限する方法

vTM の Restricting Access 機能を使用して、vTM 管理 UI へのアクセス元を制限することができます。

不正なアクセス元からの侵入を防ぐために、こちらの方法で管理 UI へのアクセス元を制限することを強く推奨します。

※上記「■ニフクラのファイアウォール機能でアクセス元を制限する方法」との併用が望ましいです。

※設定を間違えますと管理 UI にアクセスできなくなりますので、作業の際には十分にご注意ください。

・事前準備

設定前に、ニフクラ環境でバックアップのためにスナップショットを取得します。

2 台以上構成（冗長構成）の場合は、1 台ずつ取得します。

※ ニフクラのスナップショットのご利用には別途料金が必要です。

※ 操作方法についてのご質問は、ニフクラ問合せ窓口までお問合せください。

・設定方法

① 管理 UI（https://< vTM アドレス >:9090）に管理用ユーザでログインします。

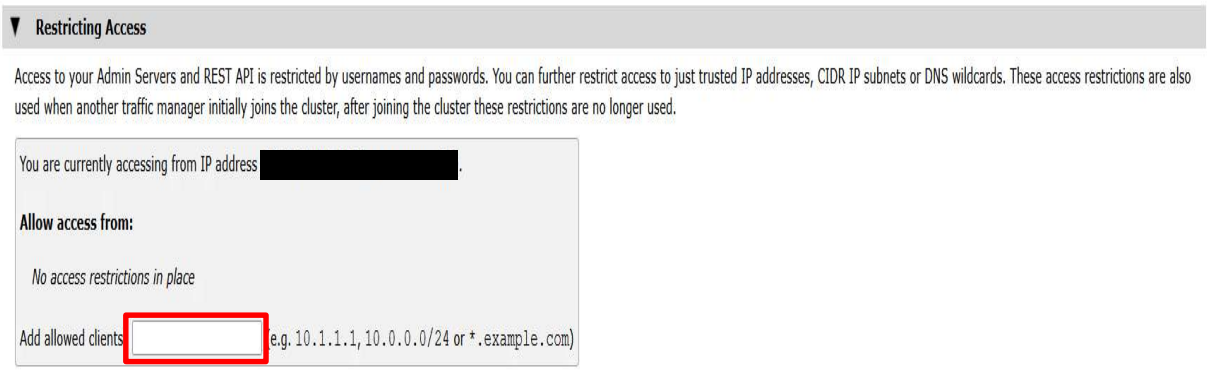
② [System] > [Security] に移動します。

③ [Restricting Access]で[Add allowed clients:]に IP アドレスまたはネットワークを設定します。

［補足］

[Restricting Access]で、クライアント IP アドレスを複数設定することが可能です。

（例：10.1.1.1,10.1.1.2,10.1.1.3 ・・）



④　画面下部の[Update]を押下して適用します。

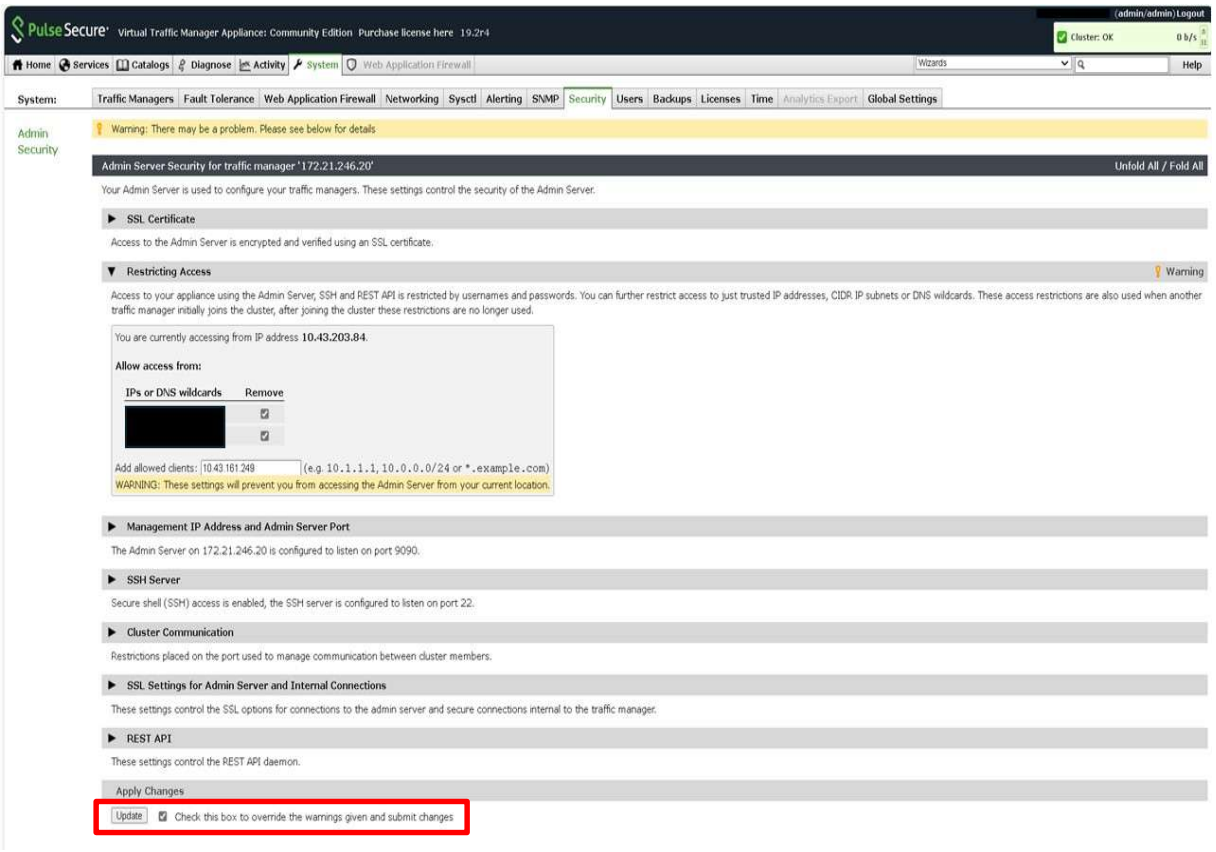
［補足］

現在のアクセス元(管理 UI にアクセスしているクライアント IP アドレス)以外を Restricting Access で設定しようとすると、[Update]実行後に以下の警告文（図の赤枠）が表示されます。

警告文：[Check this box to override the warnings given and submit changes]

※仕様上、誤り防止のために警告文へのチェックが必要になります。

警告文に確認のチェックをした後に再度[Update]すると、現在のアクセス元から管理 UI へのアクセスができなくなります。

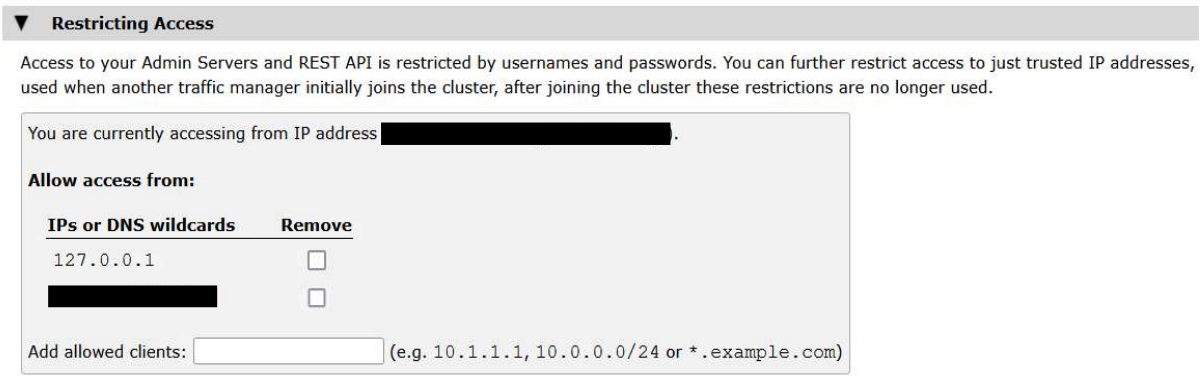


・設定確認

① 管理 UI（https://< vTM アドレス>:9090）に管理用ユーザでログインします。

② [System] > [Security] に移動します。

③ [Restricting Access]に希望の設定が反映されているかを確認します。



・復旧方法

もしも誤った設定を行い、管理 UI にアクセスができなくなった場合は、設定前にニフクラ環境で取得したスナップショットから復旧します。

3) ライセンス設定

vTM の動作には 1 台毎にライセンスファイルが必要となります。

ライセンスには稼働する vTM の IP アドレス情報が必要です。ライセンス申込時に申請された IP アドレスは vTM 機器以外から通信が出来るインターフェースに設定されていなければなりません。

vTM の IP アドレスが変わると利用中のライセンスは無効になります。

ご利用の仮想サーバーの IP アドレスの変更が生じた場合はライセンスの変更をニフクラ問合せ窓口にご連絡ください。Cluster 構成ではマルチ IP アドレスでのご利用となります。

マルチ IP アドレス環境では仮想サーバー作成直後の IP アドレスから変更された IP アドレスとなります。

ライセンス申し込み時にはニフクラ様から通知されたマルチ設定環境の内容をご確認のうえ、お申込みください。

■ライセンスインポート方法

System＞License メニューにアクセスします。

Install new License Key の項目で Key File の ファイルを選択 ボタンをクリックし、ライセンスファイルを選択します。ライセンスファイル選択後、 Install key ボタンをクリックします。

ライセンスは動的に切替わります。

ライセンスインポートによる vTM の再起動、サービスのリスタートは発生いたしません。

Cluster を構成している場合はいずれかの vTM 上で全てのライセンスをインポートすることができます。

ライセンスをインポートしない場合、帯域 10Mbps に制限された Community Edition で動作します。

Community Edition での動作はサポート提供外となります。必ずライセンスをインポートしてご利用し

てください。

Cluster を構成する全ての vTM に同じライセンスタイプをインポートしてください。異なるライセンスタイプで Cluster を構成することは推奨されていません。

■ライセンス更新

ニフクラ環境では年 1 回、毎年 2～3 月頃にライセンスを更新する必要があります。

ライセンスを更新しない場合、3 月 31 日でご利用帯域のライセンスが使用できなくなります。

ライセンスの期限が切れますと、Community Edition での運用（帯域 10Mbps）に切り替わります。

新しいライセンスは毎年 2 月を目途にニフクラ様からご利用中のお客様に対して送付されます。

新しいライセンスは自動適用されませんのでお客様ご自身で適用いただく必要があります。

デフォルトの設定ではライセンス更新期限の 90 日前、60 日前、30 日前、15 日前、7 日前にメッセージがイベントログに出力されます。

新しいライセンスはライセンスインポート方法と同じ方法でインポートすることができます。

新しいライセンスが有効になりますと古いライセンスが残っていることでエラーが出力されます。

エラー解除には古いライセンスを削除していただく必要があります。

■ライセンスの切替え

ご利用途中に帯域変更などでライセンス変更を希望された場合、上位帯域のライセンスをインポートすることで、自動で上位の帯域のライセンスが有効となり、下位帯域のライセンスは無効となります。

逆に下位帯域のライセンスをインポートした場合、上位帯域のライセンスを手動で削除いただかないと下位帯域のライセンスは有効となりません。

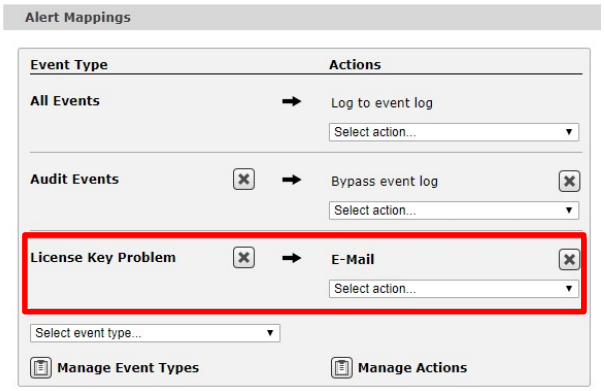
不要となった上位帯域のライセンスを削除せず、そのまま利用しますとライセンス違反となります。

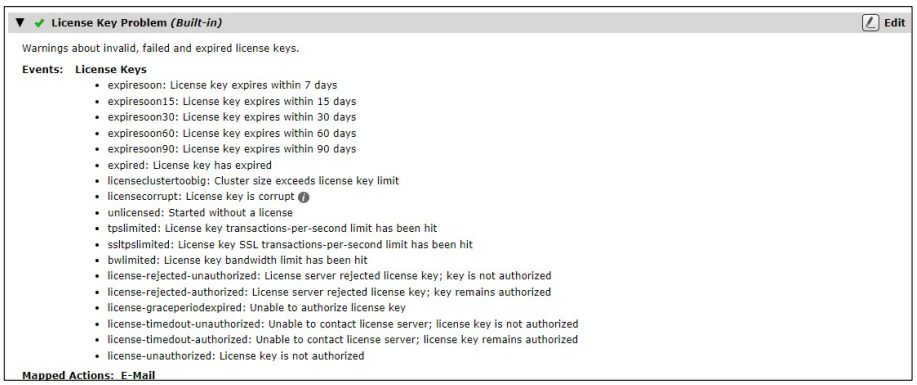
必ず不要となったライセンスを削除してください。不要となったライセンスを削除すると残っているライ

センス(下位帯域のライセンス)に自動で切り替わります。

■ライセンス更新期限のアラート設定

Alerting の Event Type で License Key Problem を設定し、メール通知や SNMP Trap を設定いただきますと、期限切れの 90 日前、60 日前、30 日前、15 日前、7 日前にアラートを送信することができます。



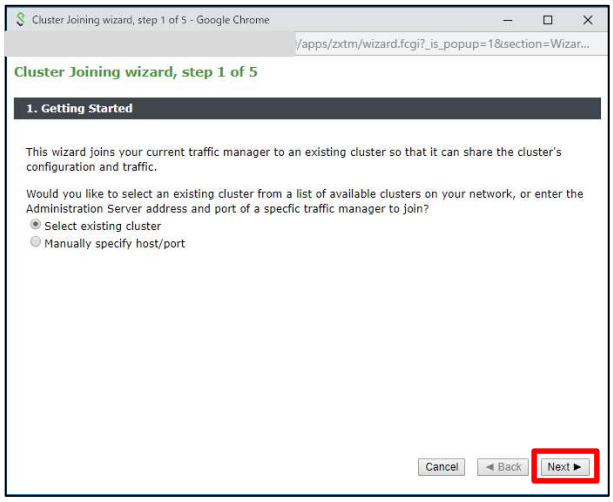


4) Cluster（冗長）設定

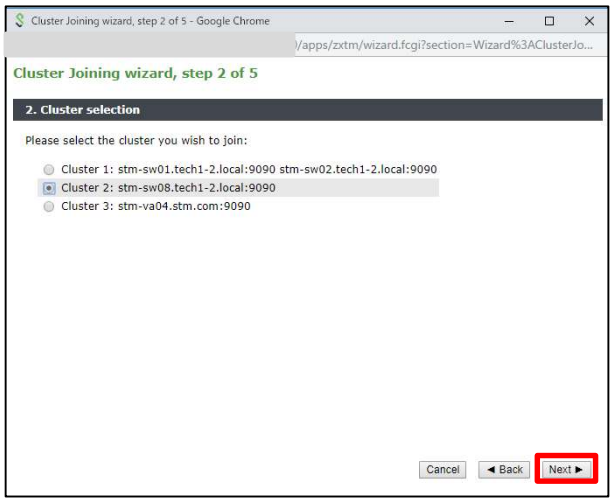
ホスト名、DNS 設定、マルチ IP アドレス環境の設定のほかに NTP に関する設定をすることで、Cluster 構成を行う準備が完了となります。

管理 UI 右上の Wizards メニューから　Join a Cluster　を選択します。

“Join a Cluster” のデフォルト操作では Cluster 構成を行うと操作側マシンの設定が相手側によって上書きされます。Service 等の設定は Cluster を構成後に実施してください。

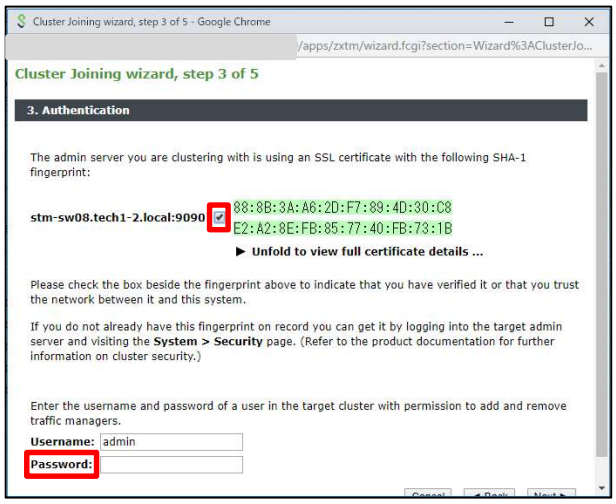


1. Getting Started で Select existing cluster を選択し Next ボタンをクリックします。



2. Cluster selection

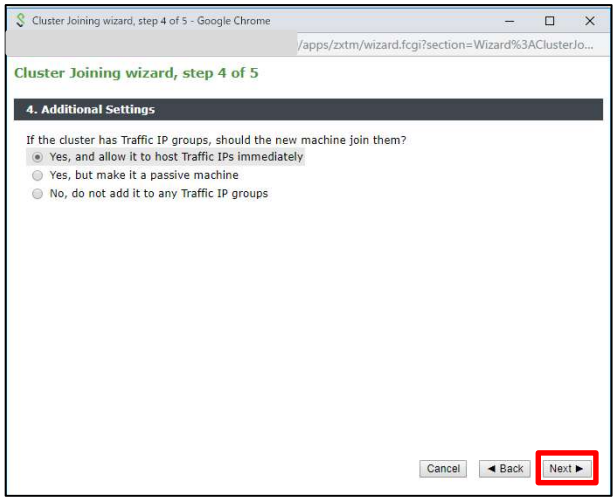
Cluster を構成する相手を選択し、Next ボタンをクリックします。



3. Authentication

既存 Traffic Manager の Fingerprint にチェックを入れ、相手の admin パスワードを設定します。

設定後 Next ボタンをクリックします。



4. Additional Settings

接続方法を選択します。

Yes, and allow it to host Traffic IPs immediately

※　Active として接続します。

この設定を選択した場合に、Passive（Standby）側のコンフィグが上書きされます。

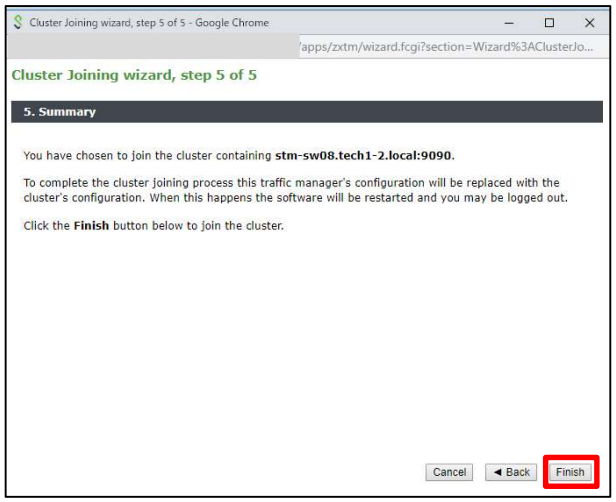
Yes, but make it a passive machine

※　Passive（Standby)として接続します。

No, do not add it to any Traffic IP groups

※　管理 UI への統合はできますが TIP に対する Active-Standby の構成にはなりません。

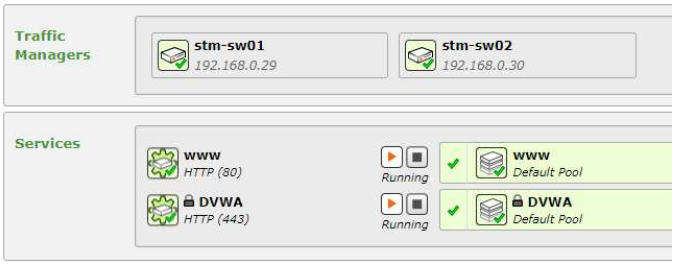
選択後、Next ボタンをクリックします。



5. Summary で、Finish ボタンをクリックします。

管理 UI 上に Cluster 構成された vTM の構成台数分のアイコンが表示されます。

Cluster 構成では、負荷分散設定など、サービスに関する設定はアクティブ側、 スタンバイ（Passive）側のどちらから設定しても相手側に反映されます。



続いて、Traffic IP Networks を設定します。

インターフェースの IP アドレスと同じネットワークセグメントで TIP を利用する場合は Traffic IP network の設定は不要です。

インターフェースの IP アドレスと異なるネットワークセグメントで TIP を利用する場合は Traffic IP network の設定を行います。

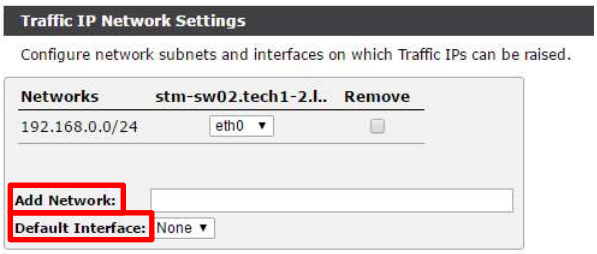
設定は Services＞Traffic IP Groups＞Traffic IP networks＞Network Settings をクリックします。

Add network:　TIP のネットワークアドレス

Default Interface:　TIP を設定するインターフェース

を設定します。

設定後、Apply Changes の Update ボタンをクリックします。



Traffic IP Networks の設定は、TIP を利用する各セグメント、インターフェース毎に設定してください。

スタティックルートなど OS 側のルーティング設定を行う場合、vTM サービスを停止したうえで実施してください。

最後に Traffic IP Groups を設定します。

Services＞Traffic IP Groups メニューの Create a new Traffic IP Group で以下を設定します。

Name	設定名称
Traffic Managers　Passive add	Passive(スタンバイマシン)を指定
IP Addresses	クライアントからのアクセスを受付する負荷分散用バーチャル IP

	アドレス(TIP)を指定
IP Mode ※ライセンスを適用すると、この設定項目は表示されなくなります。	Raise each address on a single machine (Single-Hosted mode) を選択

Create Traffic IP Group ボタンをクリックします。Traffic IP Groups の一覧に追加されます。

Traffic IP Groups 設定画面

Traffic IP Groups で設定した IP Address が、クライアントからのアクセスを受付する負荷分散用バーチャル IP アドレス(TIP)となります。

冗長構成の vTM のどちらかに通信を片寄せしたい場合は、設定した全ての Traffic IP Groups にて、上記 Traffic IP Groups 設定画面のスタンバイ機にしたい Traffic Manager(vTM)の［Passive］にチェックを入れてください。

Passive にチェックの入った vTM がスタンバイ機となります。

グローバル側、プライベート側にそれぞれ Traffic IP Groups を構成する場合も、Passive に設定する vTM が同じになるように設定してください。

どちらの vTM にも Passive にチェックが入っていない場合、どちらの vTM がアクティブ、スタンバイ(Passive)になるかは自動で決定されます。

アクティブの確認方法は、下記「■アクティブの確認方法」をご参照ください。

■アクティブ−アクティブ時の制約

Cluster 構成ではアクティブースタンバイ構成となります。アクティブーアクティブの構成には以下の制約があります。

・Cluster を構成する vTM が 4 台以上

・HTTPS（SSL オフロードまたは HTTPS の負荷分散）のみ

・バックエンドノード側の設定追加

これらが必要となるため、日本国内では通常サポート外となっています。

■アクティブの確認方法

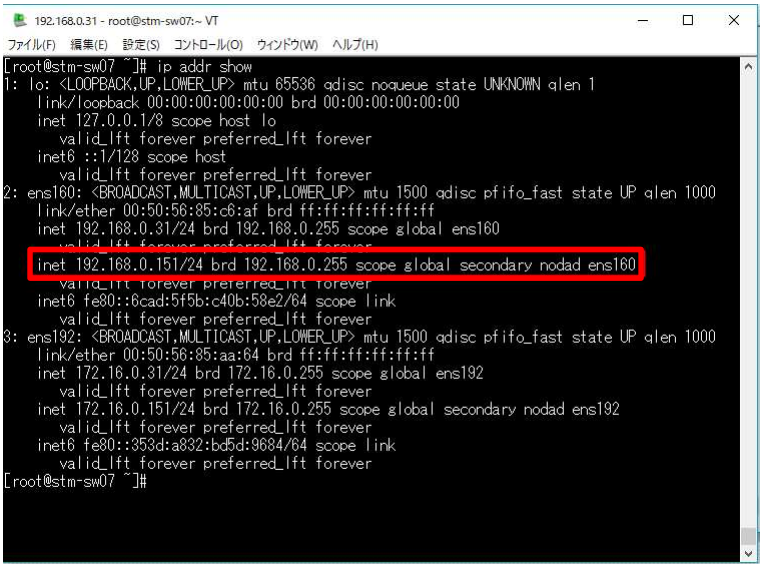
Cluster 構成では以下の方法でアクティブ側の vTM を確認することができます。

管理 UI での確認	Services > Traffic IP Groups の Traffic IP Groups セクションの 右側(画面右上)に表示されている「Unfold All/Fold All」の「Unfold All」をクリックします。 各 Traffic IP Groups セクションの各 vTM 名 の下に、現在その vTM にホストされている IP アドレス(TIP)が表示されます。 ホストされている TIP を持つ vTM がアクティブ側の vTM となります。
OS での確認	“ip addr show” コマンドで確認できます。 このコマンド結果で、「secondary」が表示されている TIP が、

	“ip addr show” コマンドを実行した vTM にホストされていることを示します。 ホストされている TIP を持つ vTM がアクティブ側の vTM となります。 「secondary」が表示されていない TIP については、別の vTM がホストしており、そちらがアクティブになっています。 下記「＜例. アクティブ側 vTM の確認方法(OS での確認)＞」参照
zcli （vTM コマンドラインモード)での確認	zcli モードでの ”show trafficip” コマンドで確認できます。 このコマンド結果で、「IPs Raised」に表示されている TIP が、 zcli モードを実行した vTM にホストされていることを示します。 ホストされている IP アドレスを持つ vTM がアクティブ側の vTM となります。 ※zcli コマンドモードを使用するには、[/usr/local/zeus/zxtm/bin/zcli] コマンドを入力してください。zcli モードになるとプロンプトが[admin@127.0.0.1 >]となります。

＜例. アクティブ側 vTM の確認方法(OS での確認)＞

以下の画面で、 TIP(192.168.0.151/24)に「secondary」の表記がある(赤枠)ので、その TIP については、“ip addr show” コマンドを入力した vTM がアクティブになります。

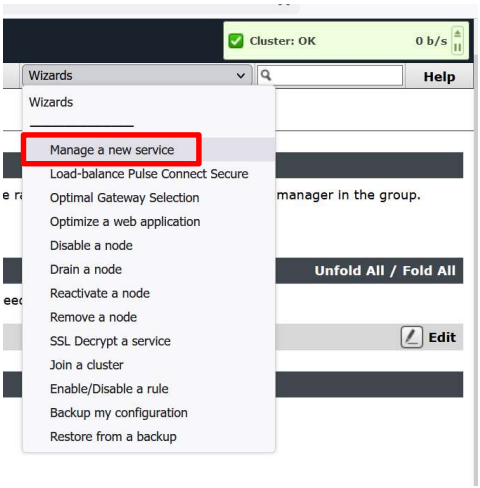


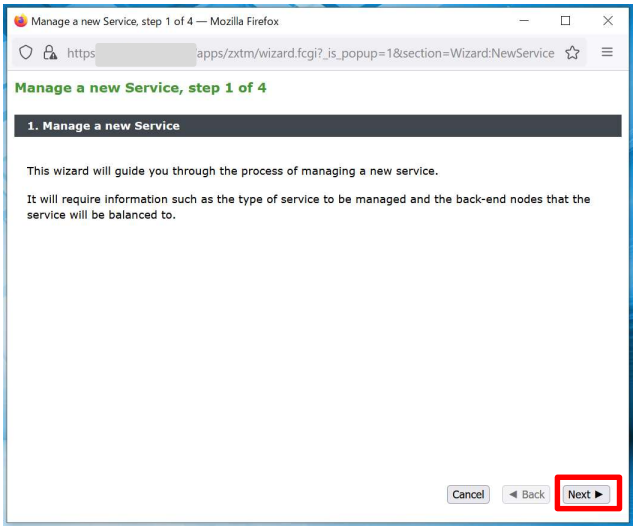
5) ウィザードによる負荷分散サービスの設定

Service 作成とは負荷分散サービスの作成を意味します。

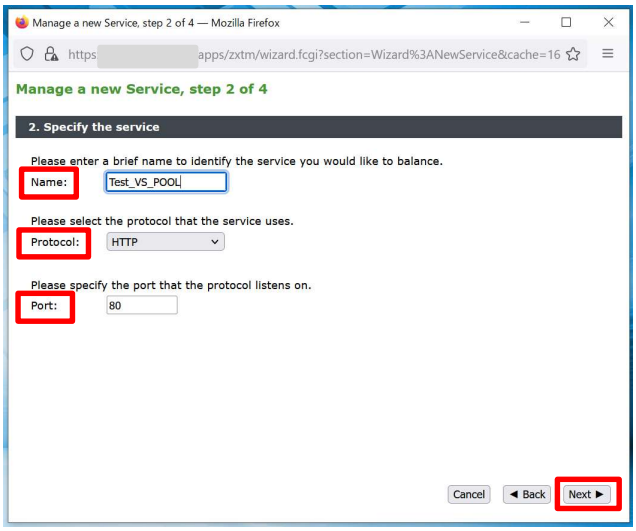
負荷分散サービスには、ウィザードで設定する方法と手動で設定する方法とがあります。

ウィザードでの設定方法は、管理 UI 右上の Wizards（ウィザード）から Manage a new Service を選択します。





1. Manage a new Service で Next をクリックします。



2. Specify the service

① Name（名前）、②Protocol（プロトコル）、③Port（ポート番号）を入力します。

設定された Name は Virtual Server、Pool の共通のオブジェクト名となります。

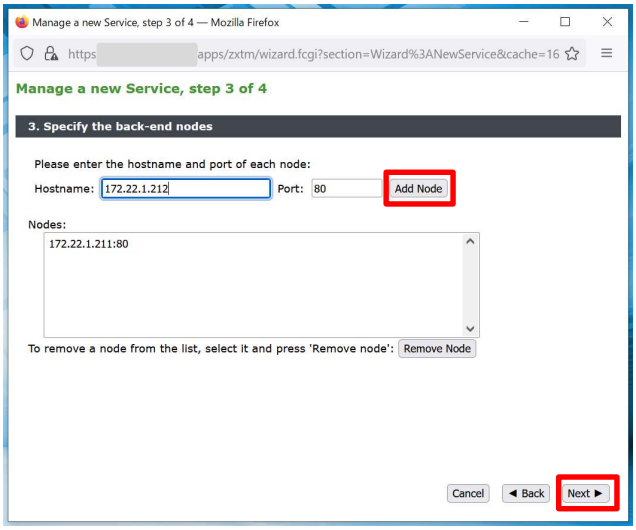
完了後、Next ボタンをクリックします。

ここで入力した名前は管理 UI 上の Services で表示する名称になります。

Name に 2 バイト文字、括弧を使用することは推奨しておりません。

これらのご利用は障害時の調査に支障をきたすことがあります。

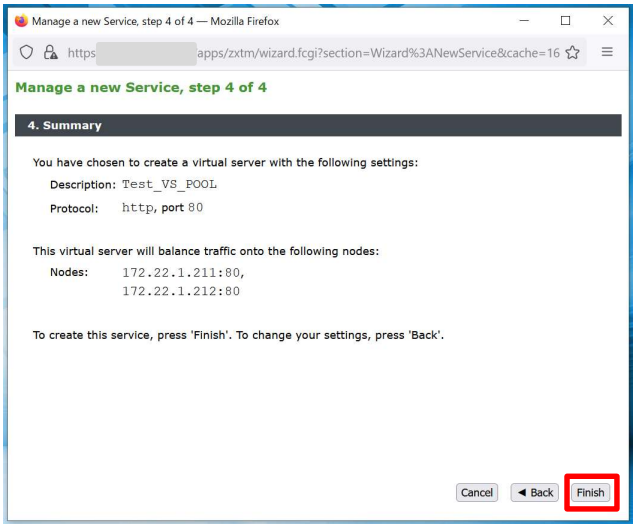
日本語で設定を分かりやすく管理されたい場合は Virtual Server、Pools の各設定の Notes の項目に記載してください。



3. Specify the back-end nodes

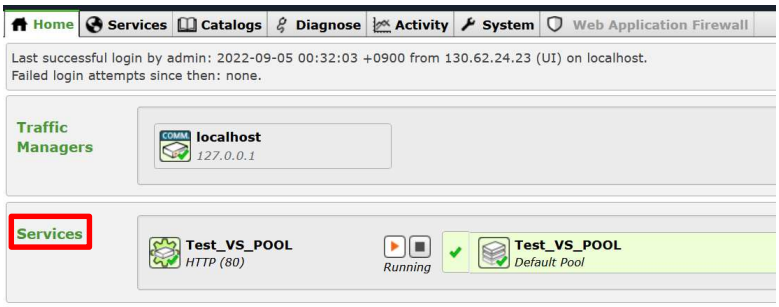
バックエンドノード(分散対象サーバ)の ① Hostname（ホスト名または IP アドレス)、② Port（ポート番号）を入力し、Add Node ボタンをクリックします。

Nodes の項目に入力したノードが追加されます。全てのノードを設定後、Next ボタンをクリックします。



4.Summary

設定内容を確認します。問題がなければ Finish ボタンをクリックします。



Home タブの Services の項目に追加されます。

ここまでの設定で負荷分散の基本動作を確認することができます。

クライアントから Traffic Manager のインターフェースに設定した IP アドレスや Traffic IP Groups に設定した IP アドレスにアクセスしてノードにトラフィックが渡ることを確認します。

［補足］

Virtual Server の設定では同じ IP アドレスに同じポート番号を割り当てるとエラーになります。

vTM 内で OS 上の FTP や postfix など、他のサーバー機能を設定している場合は、Virtual Server で同一の Service（ポート番号）が設定できません。

ニフクラ環境ではサポートするプロトコルが指定されています。サポート外のプトロコルを利用されたい場合は事前にご相談ください。

SSH や Proxy サーバーなどの Virtual Server を設定する場合は Protocol に　Generic Server First　や　Generic Client First　を選択します。

詳しくはユーザマニュアルや弊社サポートサイトの「技術情報」を参照してください。

6)　手動による負荷分散サービスの設定

ウィザードを使用せずに手動で作成するには、Pools、Virtual Servers の順番で作成します。

■Pools の作成

Serveices＞Pools＞Create a new Pool メニューで設定します。

Pool Name	Pool オブジェクトの名前を設定します。
Nodes	バックエンドノードを指定します。 IP アドレス:ポート番号　または　ホスト名:ポート番号　で指定します。 複数のノードを指定する場合はカンマで区切ります。
Monitor	プルダウンからモニタを設定します。

入力後　Create Pool　のボタンをクリックします。

■Virtual Server の作成

Services＞Virtual Server＞Create a new Virtual Server メニューで作成します。

Virtual Server Name	Virtual Server オブジェクトの名前を設定します。
Protocol	通信プロトコルをプルダウンから指定します。 ニフクラ環境ではサポートするプトロコルが指定されております。 サポート対象外のプトロコルについてはご利用前にご相談ください。
Port	ポート番号を指定します。
Default Traffic Pool	Virtual Server に組合せする Pool を選択します。

入力後　Create Virtual Server　のボタンをクリックします。

既に他の Virtual Server で同じポート番号が利用されている場合はエラーとなり、作成することができません。

7） Listen の設定

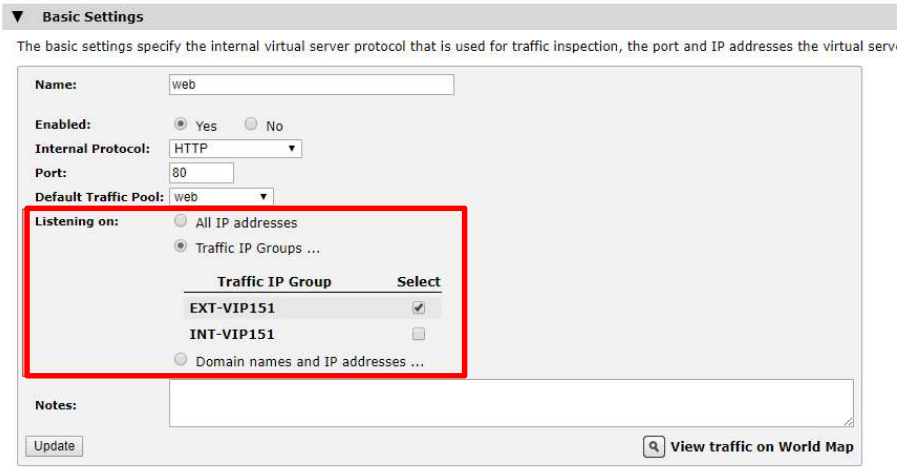
ウィザードまたは手動で Virtual Server を設定した場合に、Virtual Server の Listen の設定はデフォルトの All IP Address となります。

All IP Address の設定では vTM で利用可能な全ての IP アドレスで Virtual Server にアクセスすることができます。

Listen の設定を変更するには Services＞Virtual Servers＞Virtual Server 名をクリックし、Basic Settings の項目を変更します。

以下のいずれかを選択します。

All IP Address	Traffic Manger に設定されている全ての IP アドレスでアクセスすることができます。
Traffic IP Groups	Traffic IP Groups に設定された IP アドレス（TIP）でのみアクセスすることができます。
Domain names and IP Address…	特定のインターフェースに設定されている複数の IP アドレスから１つを指定してアクセスする場合に選択します。



Virtual Server へのアクセスは IP アドレス＋ポート番号の考えかたになります。

他の Virtual Server で利用している IP アドレス＋ポート番号と競合した場合、Virtual Server の設定はエラーとなります。

例えば、

Traffic IP Groups-A　に Traffic IP Address：192.168.0.201

Traffic IP Groups-B　に Traffic IP Address：192.168.0.202

が設定されている場合、192.168.0.201 用の Virtual Server で All IP Address を選択していると 192.168.0.202 用の Virtual Server を作成するとエラーとなります。

その場合は 192.168.0.201 用の Virtual Server の設定で Listen on を Traffic IP Groups に変更し　Traffic IP Groups-A を選択し、192.168.0.202 用 Virtual Server の設定では Listen on に Traffic IP Groups-B を指定します。

8)　フォルトトレーランス

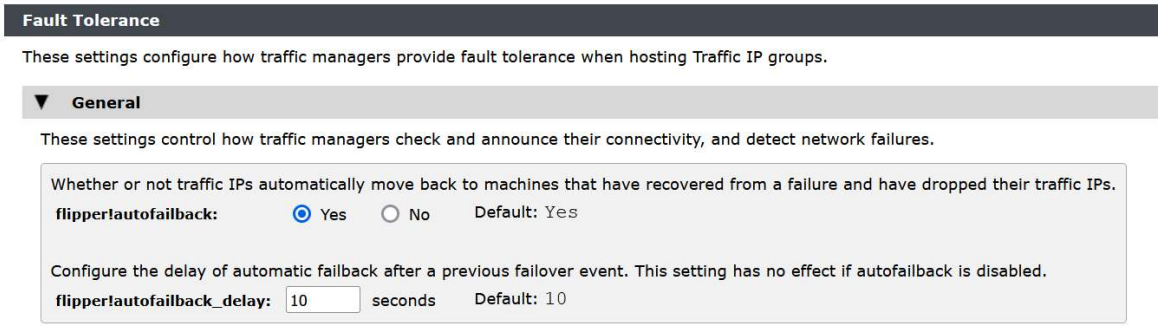
フォルトトレーランス（Fault Tolerance）のメニューではフェイルオーバーに関する項目を設定します。

vTM は 1 台構成でもゲートウェイ側、バックエンドノード側への Ping 送信による自身の死活監視を行っています。

Cluster を構成している vTM 間において、相互にチェック(ハートビート)を行います。

また 2 台以上の vTM で Cluster を構成した場合、フェイルオーバーからの復帰後、自動でフェイルオーバー発生前にアクティブだったマシンに戻すフェイルバックが設定されています。

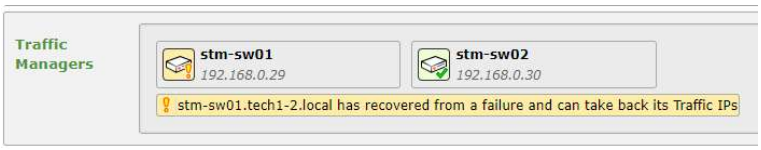
フォルトトレーランスの設定は System＞Fault Tolerance＞General のメニューで設定します。



flipper!autofailback	フェイルオーバー後の自動切り戻しを設定します。
flipper!autofailback_delay	自動切り戻しの時間を設定します。0(ゼロ)を設定すると vTM 復帰後、すぐに切り戻しが行われます。

flipper!autofailback の設定が No のときは手動による切り戻しが可能です。

手動操作による切り戻しがされるまで、管理 UI 上には警告メッセージが表示されます。



警告メッセージは

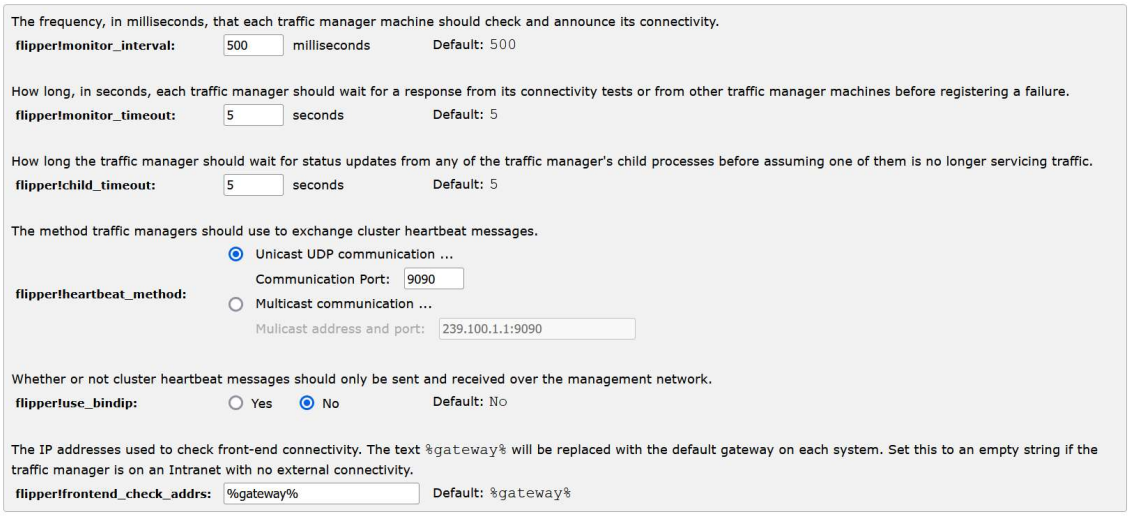
<ホスト名> has recovered from a failure and can take back its Traffic IPs

というメッセージになります。

この警告は Diagnose＞Cluster Diagnosis のメニューにも表示されます。

（右上の Cluster Error をクリックすると Cluster Diagnosis のメニューにジャンプします。）

画面内の Reactivate this traffic manager　をクリックすると Active だった側のマシンに切り戻すことができます。



flipper!monitor_interval	・flipper!frontend_check_addrs (フロントエンド)への Ping ・バックエンドノードへの Ping ・vTM ハートビートの送信 のタイミング（間隔）を設定します。単位は“ミリ秒”です。
flipper!monitor_timeout	vTM のフェイルを検知するタイムアウト時間を設定します。 単位は“秒”です。 この設定時間内に Cluster を構成する他の vTM から通知が送られてこない場合、vTM はフェイルオーバーします。
flipper!frontend_check_addrs	フロントエンドノード(バックエンドノード以外)への死活監視先を設定しま

	す。 デフォルトの設定は %gateway%(デフォルトゲートウェイ)となりますが、 複数の宛先アドレスを追加頂くことを強く推奨します。 設定した全ての宛先に対する死活監視が出来なくなると、フェイルオーバーが発生します。一つでも死活監視出来れば、フェイルオーバーは発生しません。 複数の宛先を指定する場合はカンマ区切りで追加します。 設定例 ：%gateway%,10.1.1.1,10.1.1.2

flipper!child_timeout の設定はメーカーから指示があった際に変更します。

通常は設定値を変更しません。

flipper!monitor_interval の設定で Ping が送信されるバックエンドノードは、全ての Pools に設定されているバックエンドノードから vTM がランダムに決めます。

Ping 送信先のバックエンドノードがダウンしている場合は、他のバックエンドノードに送信先を切り替えます。

全てのバックエンドノードがダウンし、タイムアウト時間が経過すると vTM はフェイル検知され、フェイルオーバーされます。

Health Monitor ではない、vTM からバックエンドノードへの死活監視の Ping は停止させることができません。

vTM 間のハートビートは相互に行われます。デフォルト設定では vTM は認識している全インターフェースを使い、ハートビート通信を行います。

ハートビートを行うインターフェースを制限したい場合、System＞Security＞Cluster Communication メ

ニューの controlallow で設定します。（デフォルト：all）

インターフェースを制限する場合、ライセンス申し込み時の IP アドレスが設定されているインターフェースでハートビート通信ができないと Traffic Manager 自身がエラーとなり、フェイル判定されます。

■フェイルオーバー条件

フェイルオーバーは、以下の場合に発生します。

① flipper!frontend_check_addrs に設定された全ての宛先への Ping 応答が得られない場合

② Pool に設定された全てのバックエンドノードへの Ping 応答が得られない場合

③ Cluster を構成する vTM で以下の事象が発生した場合

－対向の vTM から「I have failed」を受信した時

－対向の vTM から、flipper!monitor_timeout 以内に何のメッセージも受信しなかった時（ハートビートエラー）

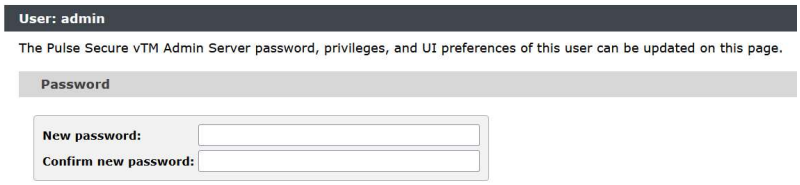
－対向の vTM から、子プロセス(負荷分散処理プロセス)が flipper!child_timeout 以内にレスポンスを返さず、トラフィック処理がされなくなったとの通知があった時

9） パスワード変更、ユーザ追加

■admin パスワードの変更

インストール時に設定した admin パスワードの変更は、System＞Users＞Local Users メニューで admin をクリックします。

password の項目で新しいパスワード入力します。



■パスワードセキュリティの設定

設定するパスワード自体のセキュリティ強化を行いたい場合は、System＞Users＞Local Users＞Password Policy Settings＞Password Security Settings で設定します。

password_security で Default restrictions を選択した場合、以下の内容で強化されます。

・8 文字以上

・2 文字以上の英字が含まれていること

・1 つ以上の大文字が含まれていること

・1 つ以上の数字が含まれていること。

・1 つ以上の英数字以外の特殊文字が含まれていること

・連続した文字を繰り返し使用することはできません

password_reuse_after の設定で過去に設定したパスワードの再利用について設定することができます。

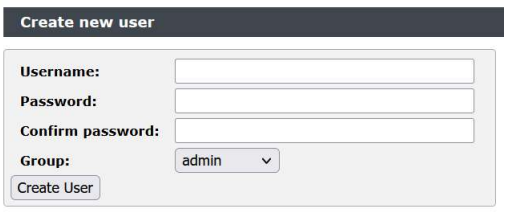
0（ゼロ）を選択した場合に、ユーザは過去に設定したパスワードを制限なく再利用できます。

password_changes_per_day を設定することで、24 時間以内にパスワード変更可能な回数を指定することができます。

0（ゼロ）の設定はこの機能の無効を意味します。

■ユーザ追加

System＞Users＞Local Users メニューの Create new user の項目で新しいユーザを追加することができます。



■root パスワード

OS 側の root パスワードは vTM 上から変更することはできません。

■vTM 上のユーザアカウントについて

vTM で設定された admin アカウントなどのユーザアカウントは OS 側の設定とリンクしません。

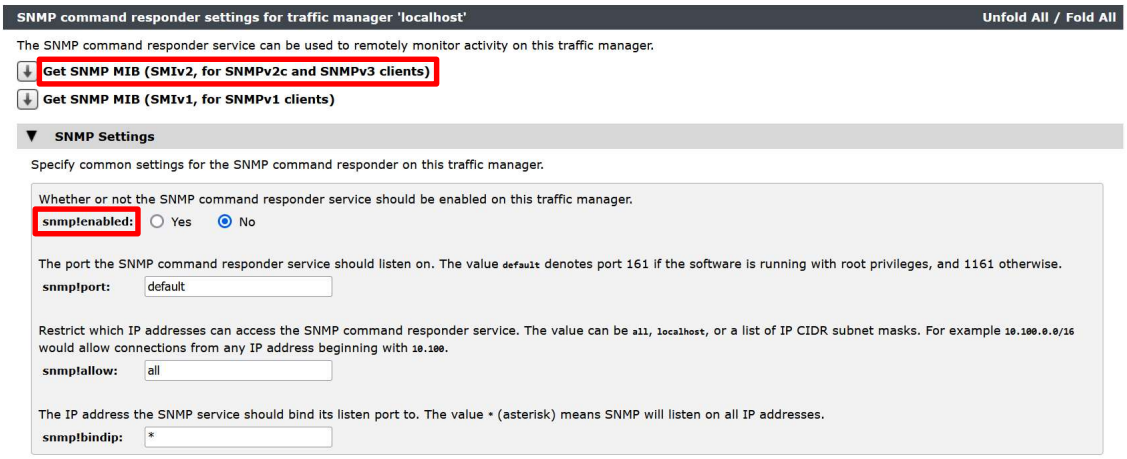
10) SNMP 設定

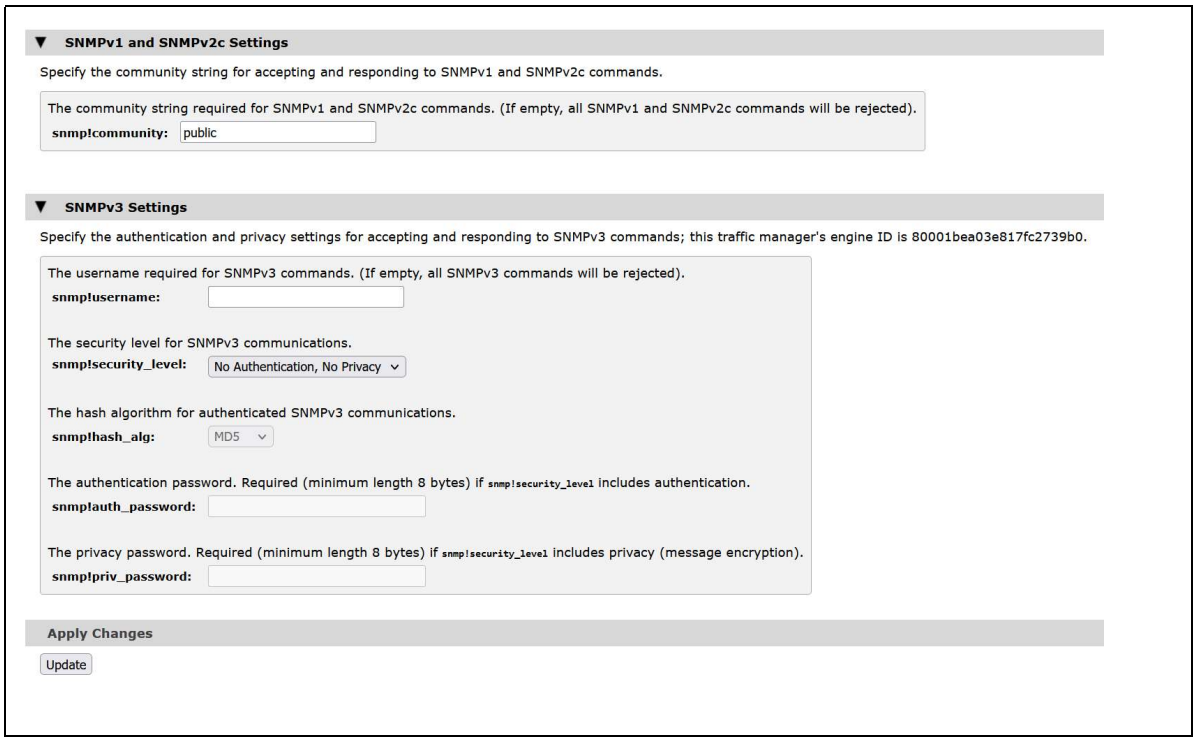
snmp の設定は System＞SNMP メニューで設定します。

この設定は SNMP Trap の設定とは異なります。

SNMP Settings で　snmp!enabled を Yes に設定することで外部から vTM の OID を GET することができます。

vTM のプライベート MIB ファイルは SNMP のメニュー内にある「Get SNMP MIB (SMIv2, for SNMPv2c and SNMPv3 clients)」から取得することができます。





vTM の SNMP 設定は OS 上の SNMP の設定や OID の取得を行いません。

vTM 側の SNMP 設定を無効にしている場合は OS 上の SNMP の設定、Zabbix 等のエージェントで vTM の OID は取得できないことがあります。

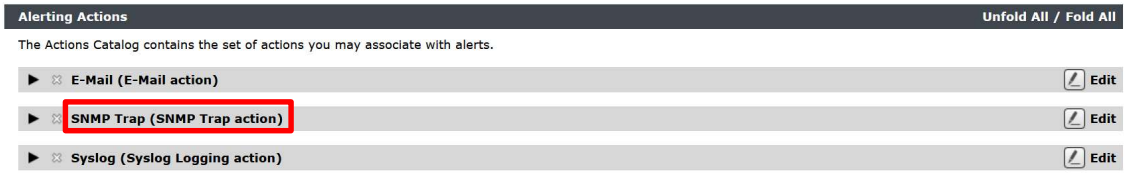
vTM の OID には CPU やメモリの値を取得するものが含まれています。

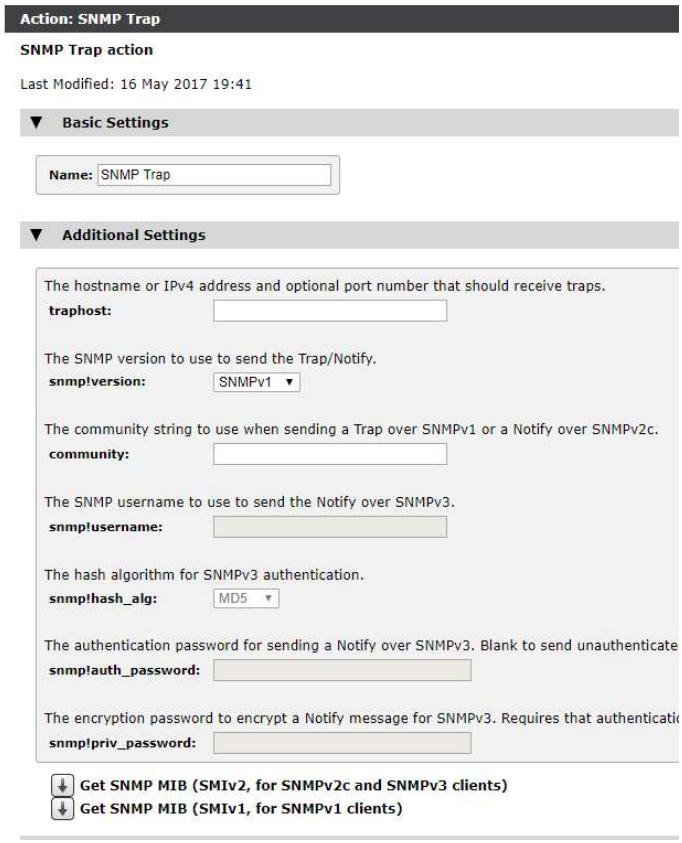
弊社では vTM 側の SNMP のご利用を推奨しており、OS 側の SNMP の設定、Zabbix 等のエージェントでの vTM の OID 取得に関するサポート対応は実施しておりません。

OS 側の SNMP の設定や Zabbix 等のエージェントを設定された場合、お問合せ内容によっては停止、削除いただいたうえでの動作をご確認いただくような回答を提示させていただくことがあります。

SNMP Trap の設定は　System＞Alerting メニューの Manage Actions で設定します。

SNMP Trap (SNMP Trap action)　を Edit して、設定します。

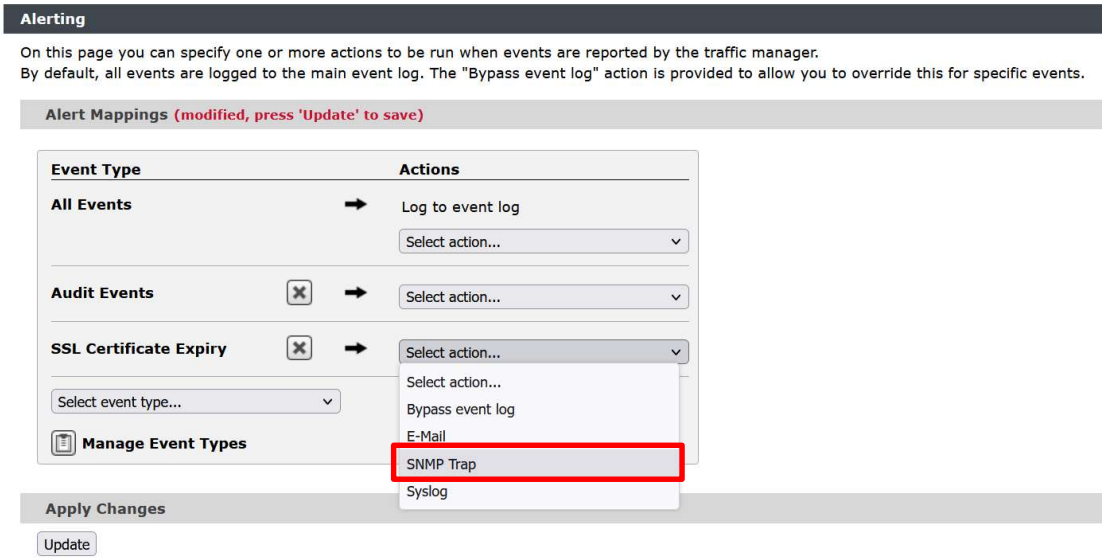


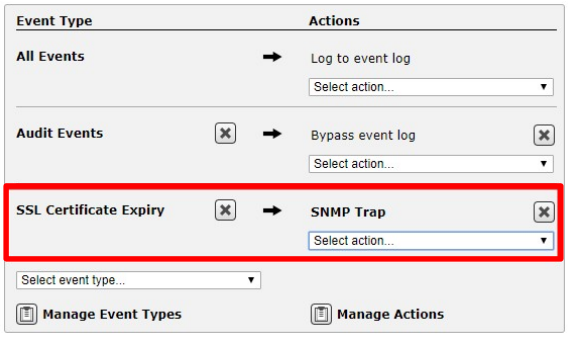


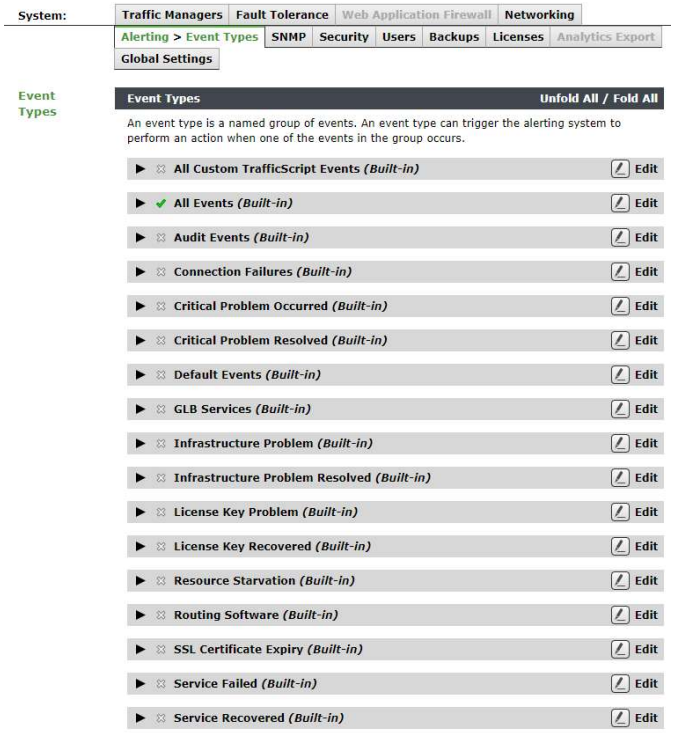
SNMP Trap を送信する項目は System＞Alerting メニューの Event Type で設定します。

選択された Event Type に Actions として SNMP Trap を割当てることで SNMP Trap が送信されます。

デフォルトで設定されている Event Type ではなく、新規に Event Type を作成した際に、フェイル検知と復帰の通知はセットでないため、フェイル検知の通知と復帰の通知を個別に選択することが必要となる場合があります。







7. Virtual Server の設定の調整

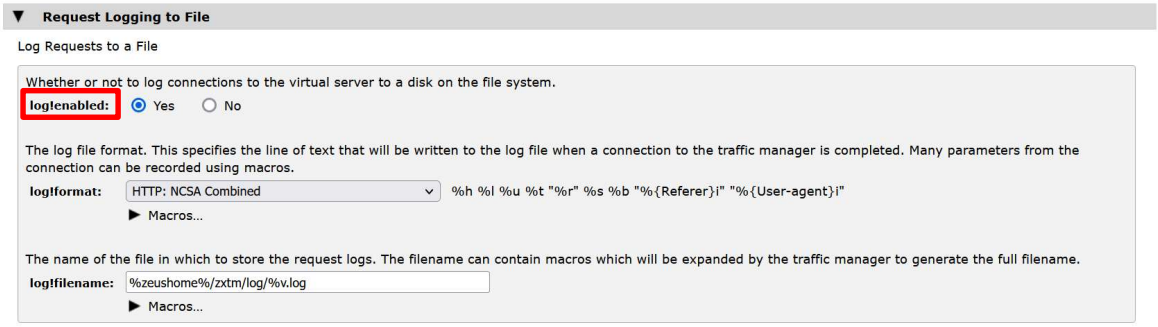
1) Request Logging の設定

Request Logging のメニューで Virtual Server へのアクセスを vTM の内部にロギングすることができます。

クラウド環境では負荷となりやすいため、弊社では本設定をご利用しないよう案内しております。

もしご利用される場合はリソース不足の発生、サービスダウンにつながる要因となることをご理解のうえ、ご利用ください。

Services＞Virtual Server＞Virtual Server 名＞Request Logging のメニューで Request Logging to File の log!enabled を Yes に設定します。



この設定により Traffic Manager 内には Virtual Server のアクセスログが保存されますが、ログファイルのローテート、アーカイブは行われません。

ログファイルはお客様自身でローテート、アーカイブを設定いただく必要があります。

ログローテート、アーカイブ設定は OS 側の設定となります。

※log!format の設定でカスタムマクロを設定した場合に、毎日ログファイルを作成するローテートを設定することができますが、アーカイブは実施されません。

2) ソーリーページの設定

vTM では対象の Pools に設定されているすべてのバックエンドノードがフェイルした場合や Draining 設定によって受けつけない新規接続に対してソーリーページを表示させることができます。

ソーリーページの設定は Services＞Virtual Servers＞Virtual Server 名＞Protocol Settings＞Error Handling メニューの error_file の項目で設定します。

Protocol Default	Traffic Manager 内に持つデフォルトのページ（Service Unavailable）を表示させます。
ファイル名	Catalogs＞Extra Files でアップロードされたカスタマイズページを表示させます。
Protocol Default （Headers Only）	内部サーバーエラー、HTTP ERROR 500 を表示させます。
Close Connection	・このページは表示できません ・ERR_EMPTY_RESPONSE ・接続がリセットされました などが表示します。

ソーリーページによるメッセージは HTTP 以外でも表示させることができます。

カスタマイズページのファイルを Catalogs＞Extra Files＞Miscellaneous Files　メニューからファイルを

アップロードします。

カスタマイズページには JPG 等のファイルを設定することができますが、ページファイル内に画像ファイルを Base64 フォーマットで記述しなければなりません。

例）<img src=********>

ソーリーページの HTTP 応答コードは 500 番となります。異なる応答コードとしたい場合は、ソーリーページのファイル内に応答コード、HTTP/1.1 200 OK　や　HTTP/1.1 503 Service Unavailable　を記述します。

以下の場合、ソーリーページは表示されません。

・Virtual Server が停止している場合

・vTM 自身がフェイル、停止している場合

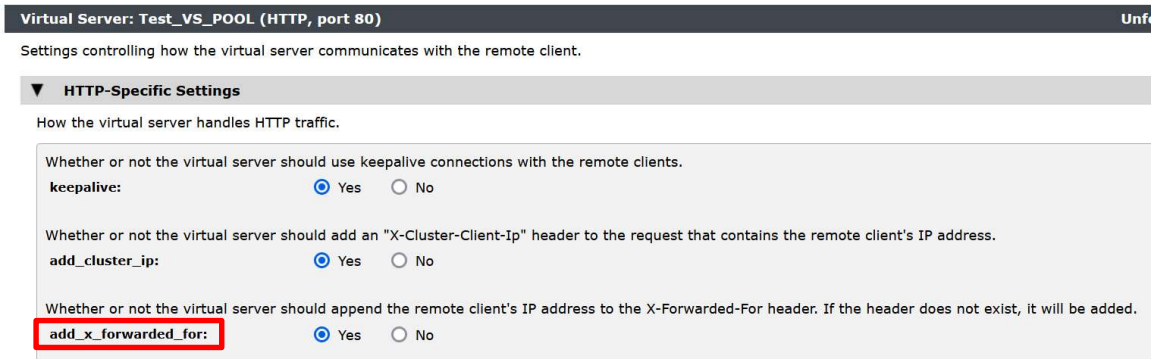
・Failure Pools が設定され、Failure Pools で設定された Pool のバックエンドノードへのアクセスが可能な場合

3)　X-Forwarded-For の設定

X-Forwarded-For をヘッダーに挿入するには、Services＞Virtual Server＞Virtual Server 名＞Protocol

Settings＞HTTP-Specific Settings にアクセスします。

add_x_forwarded_for　の設定を Yes にします。

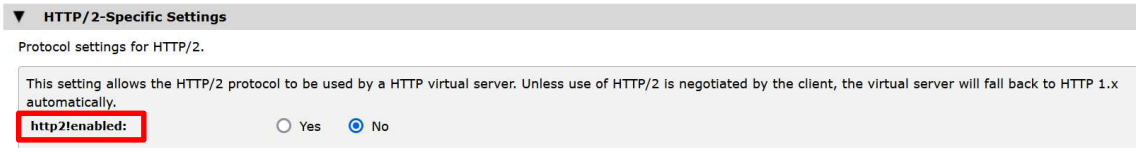


4)　HTTP/2 の設定

Services＞Virtual Server＞Virtual Server 名＞Protocol Settings＞HTTP/2-Specific Settings にアクセスします。

HTTP/2 を利用させたくない場合は、http2!enabled の設定を No に変更します。

TLS1.2 を無効にした場合、HTTP/2 の利用はできません。TLS1.2 を無効にした場合も http2!enabled 設定を No に変更します。

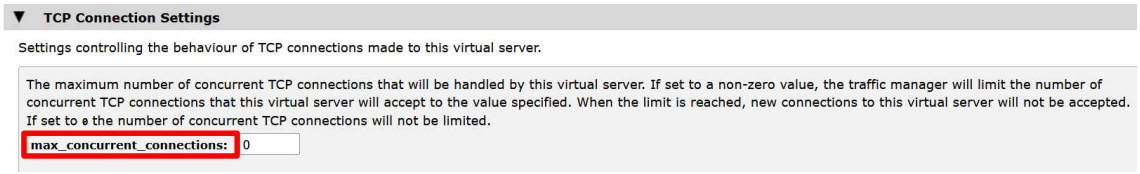


5)　アクセス上限の設定

ver.17.2 以降 Virtual Server へのアクセス数の上限を設定できるようになりました。

設定は Services＞Virtual Servers＞Virtual Server 名＞Protocol Settings＞TCP Connection Settings メニューの max_concurrent_connections の項目で設定します。

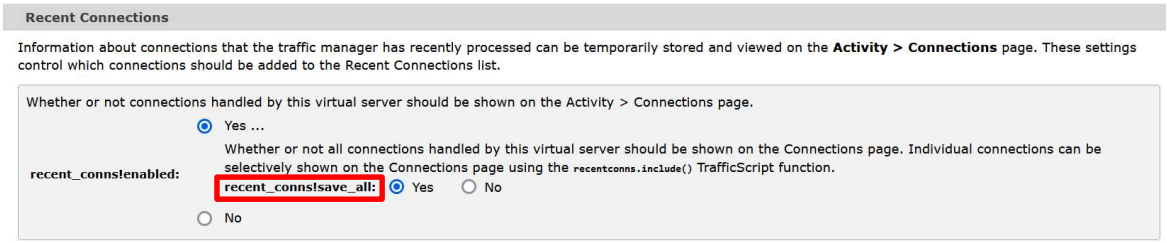
0（ゼロ）以外の値を設定することで接続数の上限を設定することができます。



6) Connection Analytics の設定

vTM を通過するコネクションの情報は Connection Analytics 機能で詳細を確認することができます。

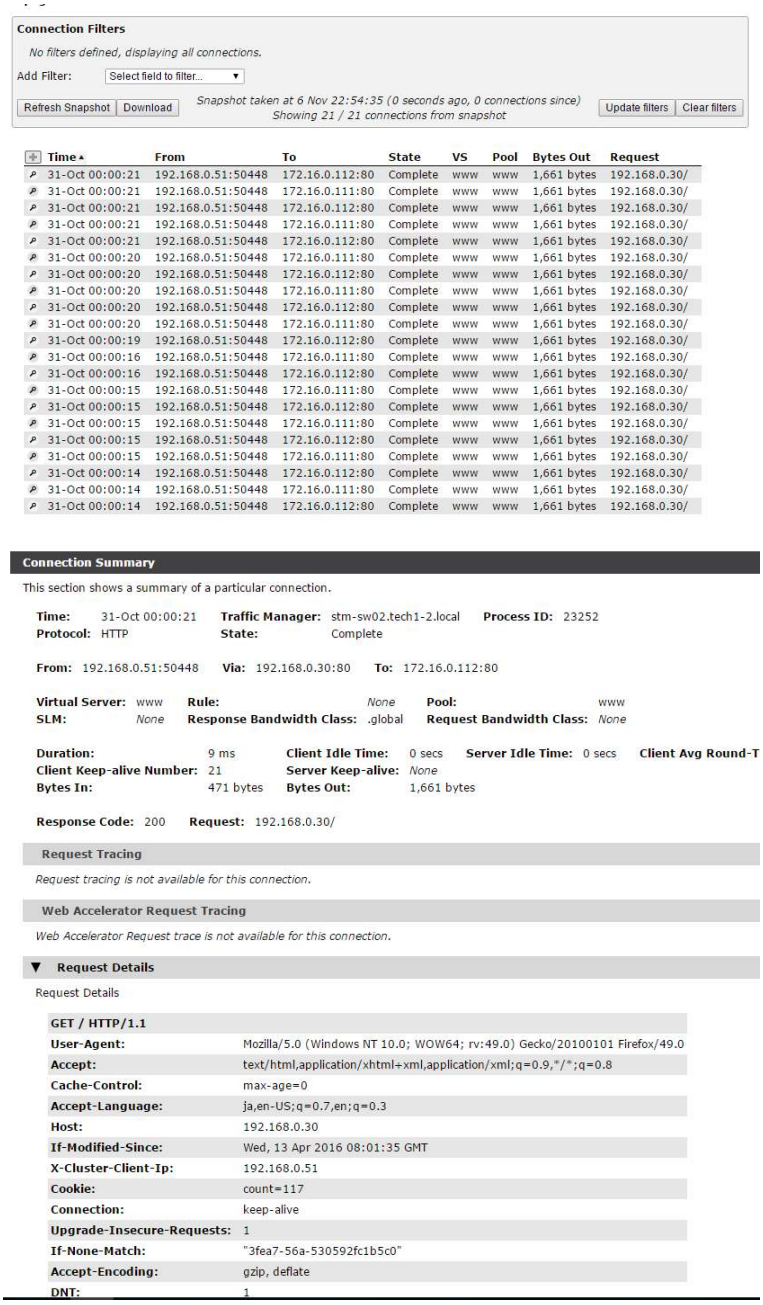
Services＞Virtual Servers＞Virtual Server 名＞Connection Analytics メニューで recent_conns!save_all の設定を Yes にします。



vTM を通過するコネクションが記録され、Activity＞Connections メニューで確認することができます。

Ivanti vTM 600 シリーズ(以下、vTM600 シリーズ)のライセンスでは Connections メニューにはコネクションの一覧が表示されます。

Ivanti vTM 1000 シリーズ(以下、vTM1000 シリーズ)以上のライセンスでは個々のコネクションの詳細を確認することができます



Connection Filters

No filters defined, displaying all connections.

Add Filter: Select field to filter...

Refresh Snapshot | Download

Snapshot taken at 6 Nov 22:54:35 (0 seconds ago, 0 connections since)
Showing 21 / 21 connections from snapshot

Update filters | Clear filters

Time	From	To	State	VS	Pool	Bytes Out	Request
31-Oct 00:00:21	192.168.0.51:50448	172.16.0.112:80	Complete	www	www	1,661 bytes	192.168.0.30/
31-Oct 00:00:21	192.168.0.51:50448	172.16.0.111:80	Complete	www	www	1,661 bytes	192.168.0.30/
31-Oct 00:00:21	192.168.0.51:50448	172.16.0.112:80	Complete	www	www	1,661 bytes	192.168.0.30/
31-Oct 00:00:21	192.168.0.51:50448	172.16.0.111:80	Complete	www	www	1,661 bytes	192.168.0.30/
31-Oct 00:00:21	192.168.0.51:50448	172.16.0.112:80	Complete	www	www	1,661 bytes	192.168.0.30/
31-Oct 00:00:20	192.168.0.51:50448	172.16.0.111:80	Complete	www	www	1,661 bytes	192.168.0.30/
31-Oct 00:00:20	192.168.0.51:50448	172.16.0.112:80	Complete	www	www	1,661 bytes	192.168.0.30/
31-Oct 00:00:20	192.168.0.51:50448	172.16.0.111:80	Complete	www	www	1,661 bytes	192.168.0.30/
31-Oct 00:00:20	192.168.0.51:50448	172.16.0.112:80	Complete	www	www	1,661 bytes	192.168.0.30/
31-Oct 00:00:20	192.168.0.51:50448	172.16.0.111:80	Complete	www	www	1,661 bytes	192.168.0.30/
31-Oct 00:00:19	192.168.0.51:50448	172.16.0.112:80	Complete	www	www	1,661 bytes	192.168.0.30/
31-Oct 00:00:16	192.168.0.51:50448	172.16.0.111:80	Complete	www	www	1,661 bytes	192.168.0.30/
31-Oct 00:00:16	192.168.0.51:50448	172.16.0.112:80	Complete	www	www	1,661 bytes	192.168.0.30/
31-Oct 00:00:15	192.168.0.51:50448	172.16.0.111:80	Complete	www	www	1,661 bytes	192.168.0.30/
31-Oct 00:00:15	192.168.0.51:50448	172.16.0.112:80	Complete	www	www	1,661 bytes	192.168.0.30/
31-Oct 00:00:15	192.168.0.51:50448	172.16.0.111:80	Complete	www	www	1,661 bytes	192.168.0.30/
31-Oct 00:00:15	192.168.0.51:50448	172.16.0.112:80	Complete	www	www	1,661 bytes	192.168.0.30/
31-Oct 00:00:15	192.168.0.51:50448	172.16.0.111:80	Complete	www	www	1,661 bytes	192.168.0.30/
31-Oct 00:00:14	192.168.0.51:50448	172.16.0.112:80	Complete	www	www	1,661 bytes	192.168.0.30/
31-Oct 00:00:14	192.168.0.51:50448	172.16.0.111:80	Complete	www	www	1,661 bytes	192.168.0.30/
31-Oct 00:00:14	192.168.0.51:50448	172.16.0.112:80	Complete	www	www	1,661 bytes	192.168.0.30/

Connection Summary

This section shows a summary of a particular connection.

Time: 31-Oct 00:00:21 **Traffic Manager:** stm-sw02.tech1-2.local **Process ID:** 23252
Protocol: HTTP **State:** Complete

From: 192.168.0.51:50448 **Via:** 192.168.0.30:80 **To:** 172.16.0.112:80

Virtual Server: www **Rule:** *None* **Pool:** www
SLM: *None* **Response Bandwidth Class:** .global **Request Bandwidth Class:** *None*

Duration: 9 ms **Client Idle Time:** 0 secs **Server Idle Time:** 0 secs **Client Avg Round-T**
Client Keep-alive Number: 21 **Server Keep-alive:** *None*
Bytes In: 471 bytes **Bytes Out:** 1,661 bytes

Response Code: 200 **Request:** 192.168.0.30/

Request Tracing

Request tracing is not available for this connection.

Web Accelerator Request Tracing

Web Accelerator Request trace is not available for this connection.

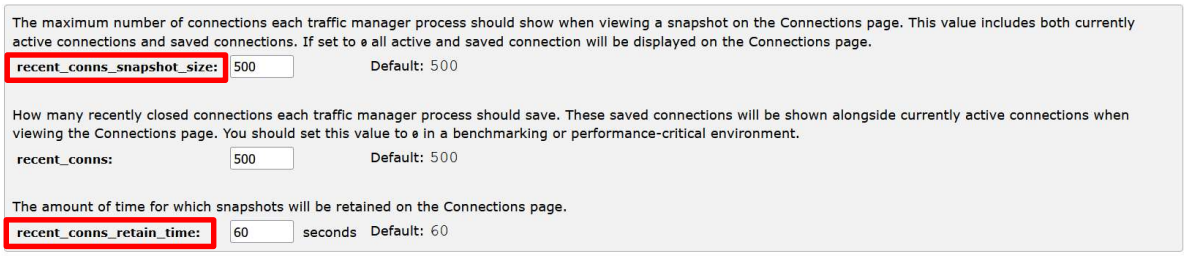
▼ Request Details

Request Details

GET / HTTP/1.1	
User-Agent:	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept:	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Cache-Control:	max-age=0
Accept-Language:	ja,en-US;q=0.7,en;q=0.3
Host:	192.168.0.30
If-Modified-Since:	Wed, 13 Apr 2016 08:01:35 GMT
X-Cluster-Client-Ip:	192.168.0.51
Cookie:	count=117
Connection:	keep-alive
Upgrade-Insecure-Requests:	1
If-None-Match:	"3fea7-56a-530592fc1b5c0"
Accept-Encoding:	gzip, deflate
DNT:	1

保存されるデータ数は System>Global Settings>Logging メニューの recent_conns_snapshot_size の項目で設定します。デフォルトは 500 です。

recent_conns_retain_time の設定(デフォルト 60 秒)で保存時間を設定します。



7） Rule の作成と適用

Rule はトラフィック処理ルールを設定するメニューです。

機能としては RuleBuilder、TrafficScript があります。

RuleBuilder、TrafficScript で作成した Rule の Virtual Server への適用タイミングは 3 種類あります。

Request Rules	リクエストが Pools に送信される前にルールを適用
Response Rules	バックエンドノードがリクエストに応答した後、ルールを適用
Transaction Completion Rules	トランザクションの完了時にルールを適用

1 つの Virtual Server に設定された Rule が複数ある場合、上から順番にチェックを行い、ルールを適用します。

但し、以下の Rule が適用された場合は、以降の Rule 適用を行いません。

・Drop Connections

・HTTP redirect

・Change HTTP site

・Choose Pool

7-1 RuleBuilder

■RuleBuilder の設定方法

RuleBuilder では、管理 UI を使用して、簡単にルールを設定することができます。

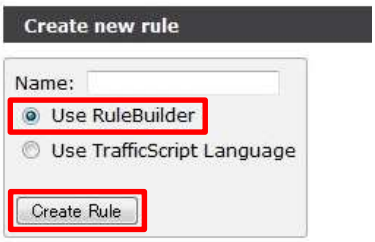
※RuleBuilder はvTM600 シリーズから使用可能

設定方法は以下となります。

Catalogs＞Rules catalog メニューの Create new rule で Name:に任意の名前を入力します。

Use RuleBuilder を選択し、Create Rule をクリックします。

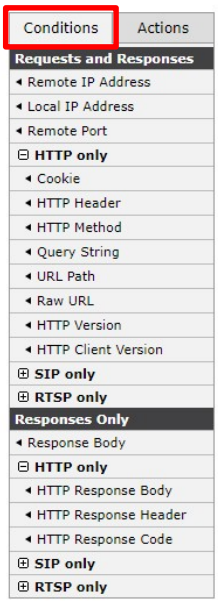
※以下のような選択肢が表示されるのは、vTM1000 シリーズ以降となります。

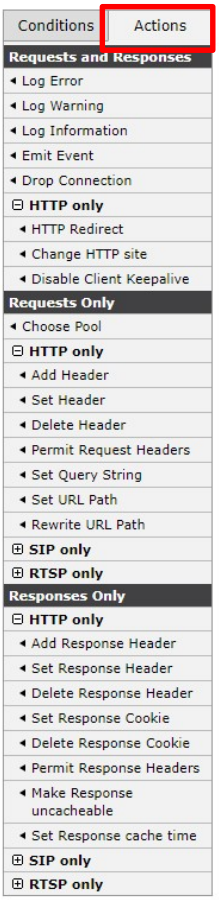


Rule は Condition（条件）と Action（実行）で構成されます。

Conditions、Actions ともに右側のメニューから項目を選択します。

選択した項目に対して、値を設定します。





設定された Rule の順番は、Rule 名称の左側をドラッグすることで上下に移動させ適用順番を変更することができます。

Rule 設定のサンプルは弊社サポートサイトに掲載しています。

「【Rule】」というキーワードで検索することができます。

また本ドキュメントの［補足 2 Rule 設定サンプル］ページにサンプルを掲載しています。

7-2 TrafficScript

TrafficScript では、スクリプトを記述することで、条件分岐などの複雑なルールを設定することができます。

※TrafficScript は vTM1000 シリーズから使用可能

TrafficScript で利用可能なパラメータ（項目）は Traffic Script ガイド（弊社サポートサイト参照）に記載されています。

ただし、条件文等の記述方法はサポート対象外となっています。

参考までに、TrafficScript 設定のサンプルを弊社サポートサイトに掲載しています。

「【TrafficScript】」というキーワードで検索することができます。

8. Pools の設定の調整

1) IP トランスペアレントの設定

トランスペアレントの設定は Services＞Pools＞Pool 名＞IP Transparency メニューで設定します。

トランスペアレント設定は初期値が No になっています。トランスペアレントを Yes に変更した場合、Pool に設定されているバックエンドノードのデフォルトゲートウェイを vTM のインターフェースの IP アドレスを指定してください。

Cluster 構成では Traffic IP Groups を作成し、Traffic IP Groups に設定した Traffic IP Address をバックエンドノードのゲートウェイに指定します。

また　Services＞Traffic IP Groups＞Basic Settings で keeptogether の設定を Yes に設定します。

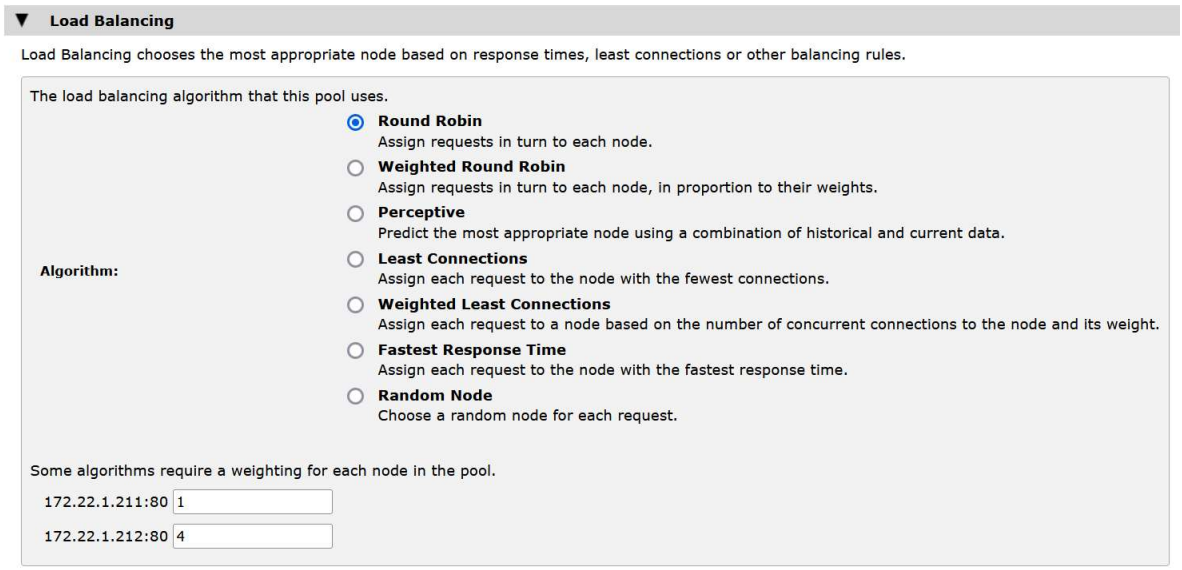
FTP はトランスペアレントで動作しません。

ウィザードで FTP 負荷分散サービスを作成した場合、FTP の Pool では Transparent を設定することはできませんが、手動で FTP の Pool を作成した場合は Transparent を設定できてしまうため、注意が必要です。

2) Load Balancing の設定

Load Balancing の設定はデフォルトでラウンドロビンに設定されます。

設定は Services＞Pools＞Pools 名＞Load Balancing の項目になります。



Weighted Round Robin を選択された場合、Some algorithms require a weighting for each node in the pool. の項目で重み付けを設定することができます。

例えば、1 対 4 で設定された場合、172.16.0.111 が 1 回リクエストを受けることに対して、172.16.0.112 が 4 回リクエストを受けるという設定になります。

Session Persistence を設定されている場合、Round Robin を設定されても、リクエストを処理するバックエンドノードは Session Persistence の設定、処理に基づき選択されます。

Round Robin	交互にバックエンドノードにトラフィックを渡します。
Weighted Round Robin	重み付けに従ってバックエンドノードにトラフィックを渡します。
Perceptive	現在のコネクション数とレスポンス時間を組み合わせ、トラフィックの最適な分布を予測します。
Least Connections	最小セッション数を持つバックエンドノードにトラフィックを渡します。
Weighted Least Connections	現在接続中のセッション数を重み付けで割り算し、一番小さい値を持つバックエンドノードにトラフィックを渡します。

Fastest Response Time	直近の数リクエストの応答時間が早いバックエンドノードを選択しトラフィックを渡します。
Random Node	ランダムにバックエンドノードを選択しトラフィックを渡します。

■Priority List の設定

本書ではファーストステップを目的としているため、Priority List の設定に関する記載は省略させていただきます。

Priority List の動作、設定につきましては弊社サポートサイトの「技術情報」を参照してください。

3) Session Persistence の設定

vTM の Session Persistence 機能は Cookie で接続元側から管理する方法と vTM 側から管理する方法があります。

vTM 側で管理する場合、アクセス数で保持量を管理します。

保持時間によるセッション管理ではございませんのでご注意ください。

保持期間によるセッション管理を行いたい場合は TrafficScript と Cookie を用いた方法となり、Univarsal Session Persistence を利用します。

TrafficScript 機能を利用するため、vTM600 シリーズのライセンスではご利用いただけません。

vTM600 シリーズでは保持したい時間内のおおよそのアクセス数をもとに保持量を設定するかたちとなります。

設定された保持量を超える古いセッション情報から順に上書きされます。

Cookie ベースの Session Persistence は Traffic Manager 内にセッション維持情報を保持しません。

保持されたセッション情報は Traffic Manager のリスタート、再起動などで消去されます。

Session Persistence の保持量はキャッシュ設定で設定します。

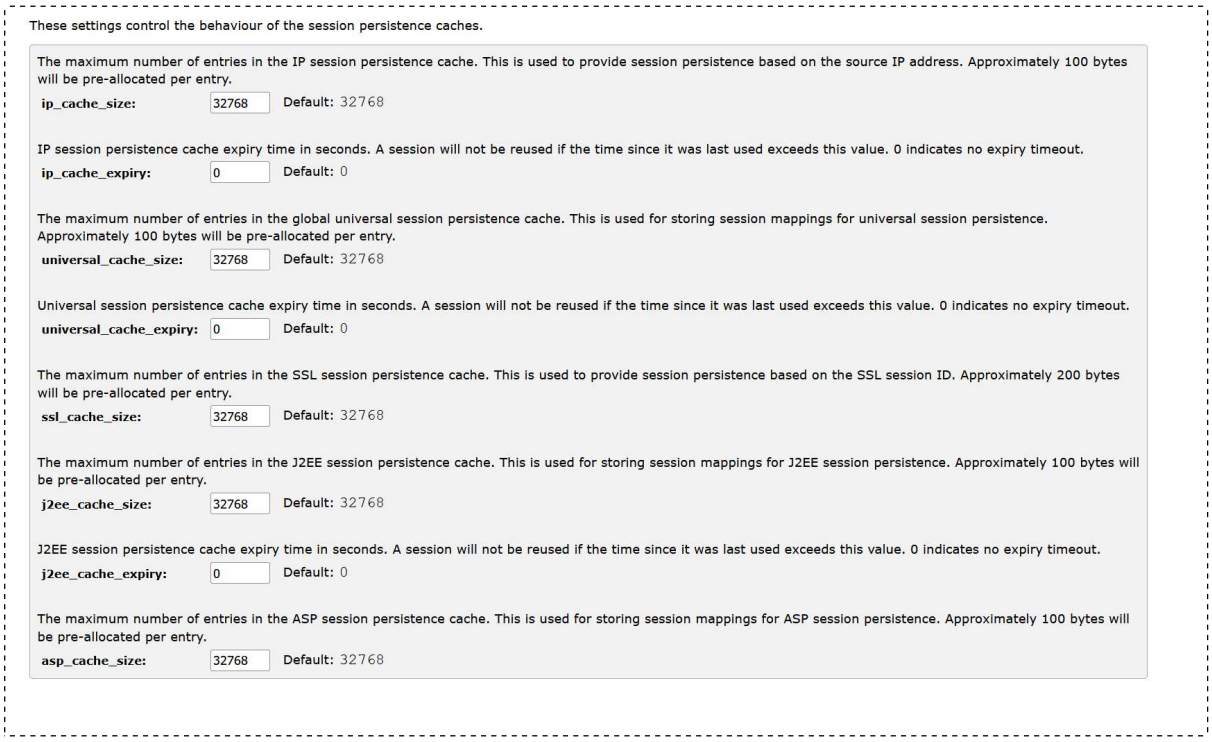
設定は System＞Global settings＞Cache Settings の項目になります。

Cache Settings の設定を変更するとリスタートを求められます。

vTM600 シリーズのライセンスでは、選択できる Type が少なくなりますのでご注意ください。

Univarsal Session Persistence は vTM600 シリーズではご利用することができません。TrafficScript が利用できる vTM1000 シリーズ以上のライセンスでのご利用となります。

■Cache Settings



Cache Settings で設定可能な最大値はメモリサイズに依存します。

値　“1”に対して、2 バイトのメモリが消費されます。

Cache Settings で設定できる項目の値を変更する際に、vTM のリスタートを求められます。

Cluster が構成されている場合は、全ての Traffic Manager をリスタートしなければなりません。

Cluster 構成では vTM をリスタートすることによってフェイルオーバーが発生します。

■Persistence タイプ

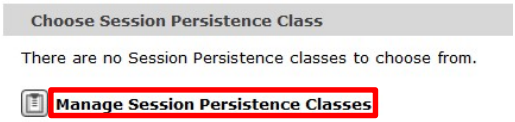
IP-based persistence	同じ送信元アドレスから同じ実サーバーにリクエストします。 subnet prefix length を設定することでセッション維持情報を保持する IP アドレスを制限させることができます。
Universal session persistence （vTM1000 以上）	Traffic Script の設定で提供されるデータを使ってセッションを識別します。
Named Node session persistence （vTM1000 以上）	Traffic Script の設定で提供されるノードでセッションを識別します。
Transparent session affinity	クッキー情報を使ってセッションを識別します。 vTM 側には情報を保持しません。 Cookie としてクライアント側で保持します。
Monitor application cookies ...	アプリケーションクッキーを監視しセッションを識別します。 vTM 側には情報を保持しません。 Cookie としてクライアント側で保持します。
J2EE session persistence	Java の JSESSIONID cookie と URL を使用してセッションを識別します。
ASP and ASP.NET session persistence	cookie、もしくは URL に埋め込まれている asp の識別子を使用してセッションを識別します。
X-Zeus-Backend cookies	X-Zeus-Backend クッキー情報とノード名でセッションを識別します。
SSL Session ID persistence	SSL パススルーで選択可能です。 SSL 時は IP-based Persistence と Transparent session affinity を選択できます。

vTM のリスタートを実施しますと既に保持されている Session Persistence の情報がクリアされます。

vTM 内に保存されているセッション保持情報を完全にクリア（削除）するには Traffic Manager の停止が伴います。

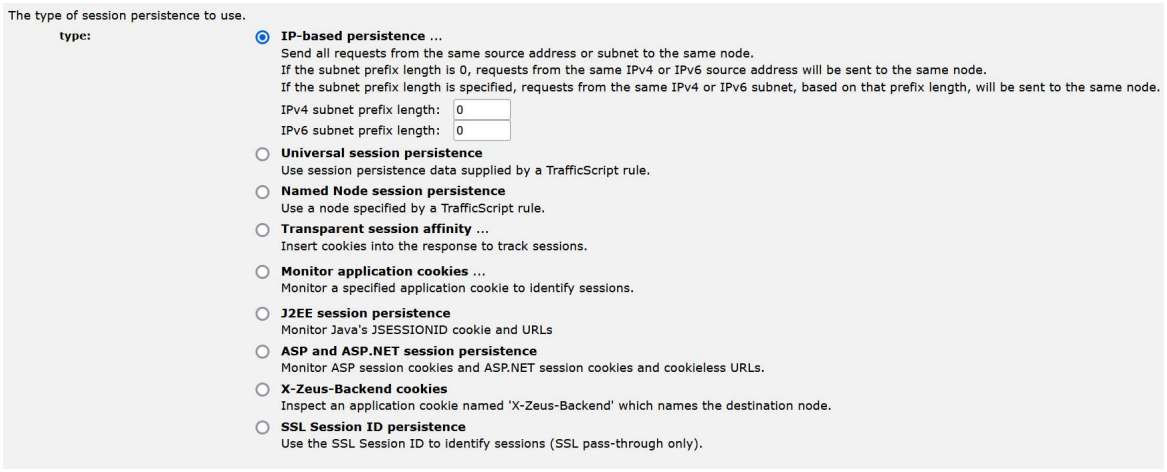
Session Persistence を設定するには、Services＞Pools＞Pool 名＞Session Persistence のメニューで設定します

新規に設定する場合、Choose Session Persistence Class の項目で、Manage Session Persistence Classes をクリックします。



Create new Session Persistence class メニューで Name を設定し、Create Class ボタンをクリックます。

Type から設定する Persistence を選択します。



Cache Settings の対象となる Session Persistence では Pool 毎に個別の設定を行うことはできません。共通の設定となります。

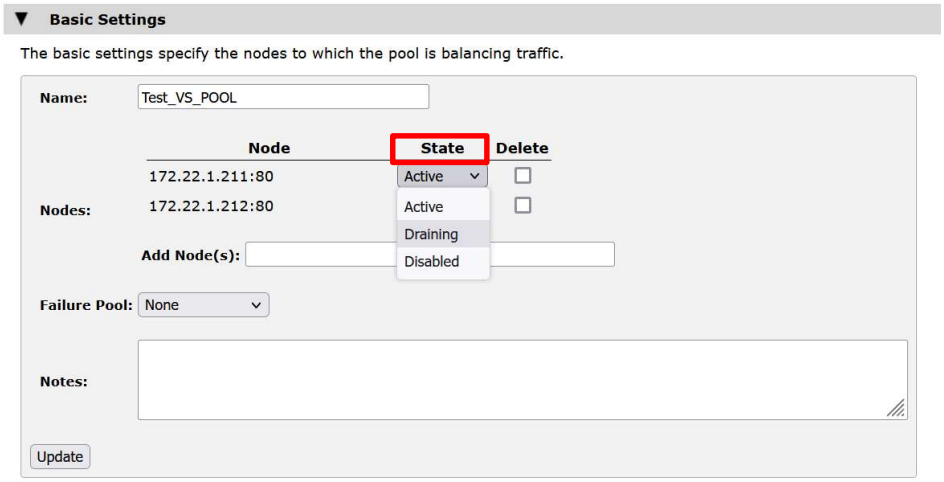
■Draining と Session Persistence の動作

バックエンドノードへの新規接続を行わないように設定する方法が Draining になります。

Draining の設定は Services＞Pools＞Pool 名の Basic Settings でノードの State を変更する設定となります。

Session Persistence を設定している場合、既に保持された情報と同じアクセス元からのアクセスは新規接続ではなく、既知の接続として扱われます。

Session Persistence で保持された接続は Draining 動作の対象外となります。



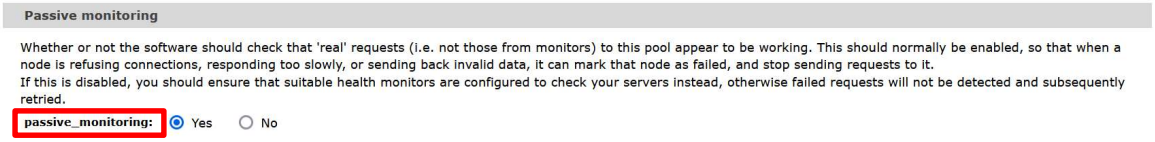
4) Health Monitoring の設定

Health monitoring には Passive Monitoring と Active Monitoring の 2 つがあります。

Health monitoring の設定は Services＞Pools＞Pool 名＞Health Monitoring に項目があります。

Passive Monitoring は Health Monitoring に設定されている Monitor でのチェックに加えてリクエストをバックエンドノードに送信するたびにヘルスチェックを実行します。

Passive Monitoring のデフォルト設定は有効（Yes）です。



Passive Monitoring が有効（Yes）の時

・バックエンドノードとのコネクションが確立されない

・データ書き込みが完了する前にコネクション断となる

・max_reply_time の設定時間内にバックエンドノードからのレスポンスの最初のデータが受信されない

といった状況でバックエンドノードへのチェックはタイムアウトとなり、vTM は Pools に設定されている

他のバックエンドノードへのチェックを再試行したのちノードフェイルを判断します。

Passive Monitoring が無効（No）の設定のときに Active Monitoring で動作します。

Active Monitoring では Health Monitoring で設定された Monitor の内容で一定時間毎にヘルスチェックを実行します。

Monitors には以下の設定項目があります。

delay （sec）	ヘルスチェックの実施間隔を設定します。
timeout （sec）	応答を待つ時間のタイムアウトを設定します。
failures （回）	フェイルを検知するヘルスチェックの失敗回数を設定します。

これらの値を調整することで Monitors の設定によるノードフェイルの検知のタイミングが変わります。

例えば、

delay を【5】秒、timeout を【10】秒、failures を【3】回と設定した場合、

TCP Connect の Monitor では　バックエンドノードとして設定されているポート番号に対して接続が確立できない場合にノードフェイルを判断します。

TCP ポートに接続が出来ない場合、すぐに結果が得られますので timeout の時間を待つことはありません。

よって、Monitors によるチェック開始から 10 秒でノードフェイルを検知します。

【TCP Connect】	【Simple HTTP】
1 回目のチェック／接続 NG	1 回目のチェック／応答待ちタイムアウト　10sec
↓　Delay　5sec	↓　Delay　5sec
2 回目のチェック／接続 NG	2 回目のチェック／応答待ちタイムアウト　10sec

↓ Delay 5sec 3 回目のチェック／接続 NG ↓ ノードフェイル検知	↓ Delay 5sec 3 回目のチェック／応答待ちタイムアウト 10sec ↓ ノードフェイル検知

max_reply_time の設定時間よりも Monitors のタイムアウト値が小さい場合、Health Monitor がノードをフェイルと判断してしまうことがあります。

max_reply_time の設定は Services＞Pools＞Pool 名＞Protocol Settings＞TCP Pool Settings に項目があります。

システムの構成によっては max_reply_time と Monitors の Delay、Timeout 設定の調整が必要となります。

Health Monitoring の設定では少なくとも Monitor の設定を実施してください。

Monitor の設定を無効にし、Passive Monitoring のみを有効にしますとノードフェイルから復帰した場合でも復帰状態を検知できず、ステータスがフェイルのままとなってしまうことがあります。

■複数の Pool にまたがるバックエンドノードに対する Health Monitor の設定について

Monitor 対象のポート番号は Pool に設定されたバックエンドノードのポート番号に対して実施されます。

バックエンドノードに指定していないポート番号に対してのチェックは行われません。

例えば、以下の Pool 設定でポートに TCP Connect monitor を設定している場合

Pool_A： SV01：80、SV02：80

Pool_B： SV01：25、SV02：25

SV01：80 の TCP Connect がエラーとなり、Monitor がエラーを検知した際に、Pool_B では SV01：25 は 25 番ポートに TCP Connect の接続ができると SV01：25 はフェイルを検知しません。

そのため、Pool_A がフェイルとなっても、Pool_B はフェイルとなりません。

vTM の基本機能では SV01：80 のフェイルを検知した際に SV01：25 をフェイルとさせることはできません。

バックエンドノードに設定していないポート番号に対してチェックを行いたい場合は、対象のポート番号をチェックする Monitor プログラムを作成し設定します。

作成した Monitor プログラムを vTM にアップロードし Pool の Monitor として設定します。

■よく利用される Monitor 設定

Connect	バックエンドノードへの TCP 接続をチェックします。 接続ポートはバックエンドノードに設定されたポート番号になります。
Simple HTTP（HTTPS）	バックエンドノード上のドキュメントルートへの応答コードをチェックします。 2xx、3xx、4xx の応答コードが得られると Monitor は成功となります。
Full HTTP（HTTPS）	ホストヘッダーや URL をチェック対象として設定することができます。応答コードは正規表現で指定します。
POP	POP バナーが応答することをチェックします。
SMTP	SMTP バナーが応答することをチェックします。

■ノードの復帰判断

何かしらの理由でバックエンドノードのサービスがダウンするなどでフェイルと検知されたノードに対して、vTM は復帰を確認するためのヘルスチェックを定期的に実施します。

バックエンドノードの復帰が確認されると vTM はノードのステータスをフェイルから WORK（復帰）に変更します。

バックエンドノードの復帰の確認は Passive Monitoring と Active Monitoring で異なる動作をします。

Passive_Monitoring：Yes（有効）時

Pool に 2 つのバックエンドノードが設定されている場合、アクセスが生じると

・1 台目はすぐにチェックされ、WORK（復帰）します。

・2 台目へのチェックは node_fail_time の設定時間経過後となります。

node_fail_time の設定は Services＞Pools＞Pool 名＞Protocol Settings＞TCP Pool Settings に項目があります。

Active Monitoring（Monitor）の設定ではアクセスが生じなくとも定期的にチェックされるため、1 台目、2 台目ともにすぐに WORK（復帰）となります。

ノードの復帰を自動ではなく手動で行いたい場合、vTM のデフォルトの機能、設定はできません。

CLI コマンドと組み合わせた Monitor プログラムを作成いただく必要があります。

9. SSL オフロードの設定

SSL オフロードの負荷分散を設定する場合は、SSL サーバー証明書を設定したのち、Wizards 機能を使わずに負荷分散の設定を行います。

SSL サーバー証明書は

・vTM 内部で CSR を作成し、外部の SSL サーバー証明書発行機関で発行し内容を vTM に反映

・既存または外部で発行済みの SSL サーバー証明書を vTM にインポート

という 2 つの方法で vTM に設定することができます。

vTM で実施可能なのは SSL オフロードになります。SSL インスペクションの動作は行いません。

1) サーバー証明書の対応

テスト済みの SSL サーバー証明書　※2018 年 12 月時点

・サイバートラスト Sure Server/Sure Server EV

・GMO Global Sign 企業認証 SSL

・デジサート（旧シマンテック）　セキュア・サーバーID

・GeoTrust　トゥルービジネス ID

・Let's Encrypt

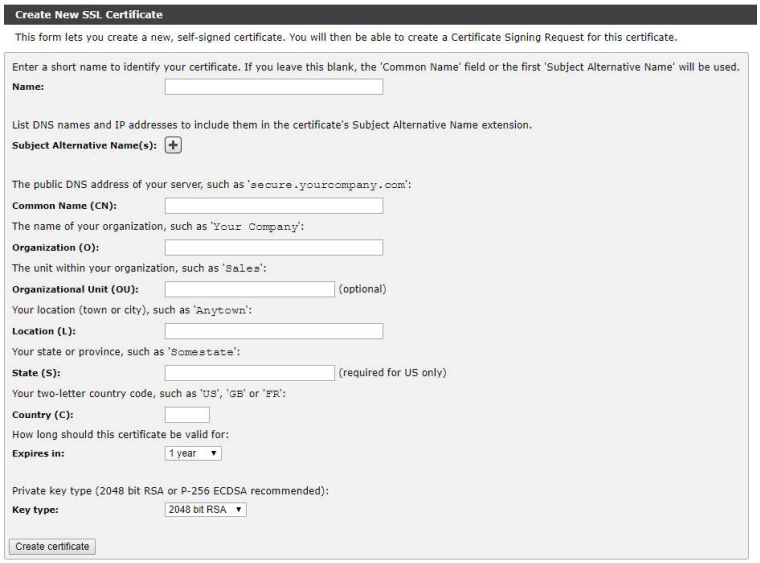
マルチドメイン、ワイルドカード証明書の利用も可能です。

他の発行機関が提供するサーバー証明書については弊社では動作確認を実施しておりません。

テスト用サーバー証明書などを利用し、事前に確認いただくことをお勧めしています。

2) CSR 作成

Catalogs＞SSL＞ SSL Server Certificates catalog メニューの Create new SSL certificate で Create Self-Signed Certificate / Certificate Signing Request をクリックします。



項目に情報を設定します。

Subject Alternative Name(s) についてはサーバー証明書発行機関にお問合せください。

Organizational Unit (OU)は“(optional)”となっていますが登録いただくことをお勧めします。

State は“(required for US only)”となっていますが都道府県名を入力してください。

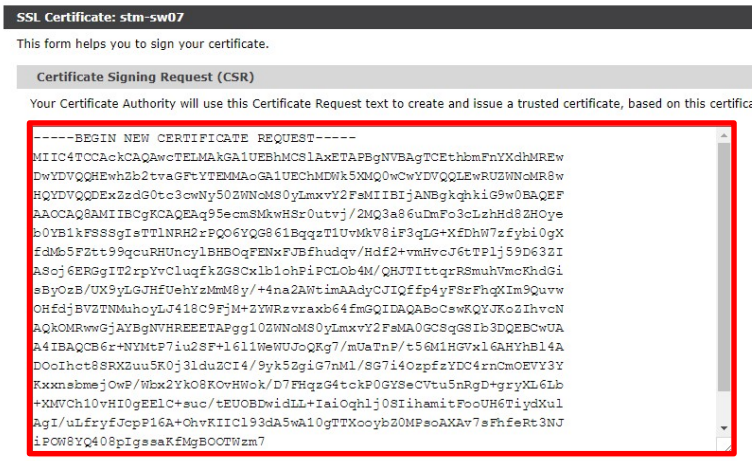
入力がされていないと SSL サーバー証明書発行機関において受付されないことがあります。

Key Type は 2048bitRSA または P-256 ECDSA が推奨されています。(ver.17.2 以降)

項目への入力後、Create Certificate をクリックします。

次画面で Certificate signing の Export CSR / Update Certificate をクリックします。

Certificate Signing Request（CSR）の内容を全てコピーし、SSL サーバー証明書発行機関に証明書発行を申し込みします。



-----BEGIN NEW CERTIFICATE REQUEST-----　から

-----END NEW CERTIFICATE REQUEST-----　まで

が CSR の内容となります。

3)　CSR から作成されたサーバー証明書の適用

Catalogs＞SSL＞ SSL Server Certificates catalog メニューで CSR を作成した際の設定を Edit します。

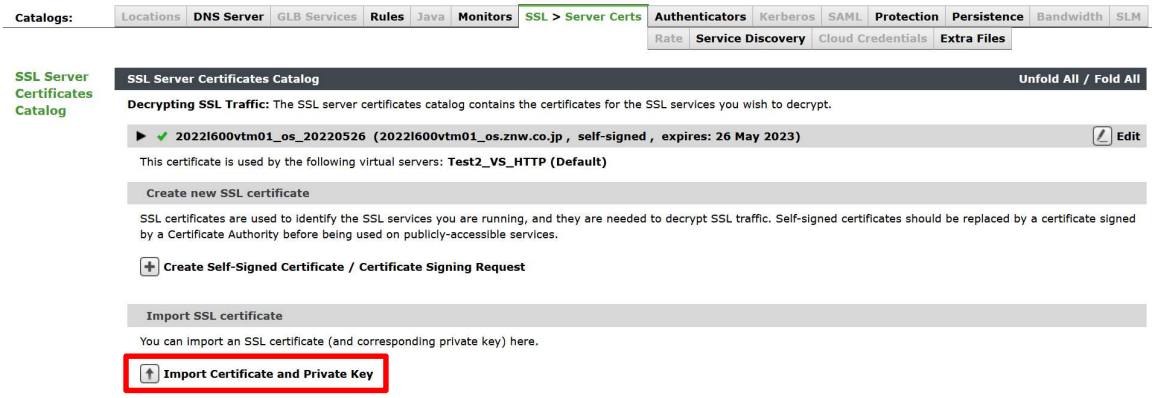
Certificate signing の項目の Export CSR / Update Certificate をクリックします。

Replace certificate の項目に証明書発行機関から発行された SSL サーバー証明書をテキストエディタ等で開き、内容をコピー&ペーストし、Update Certificate ボタンをクリックします。

4)　SSL サーバー証明書のインポート

Catalogs＞SSL＞ SSL Server Certificates catalog メニューの Import SSL certificate で Import Certificate

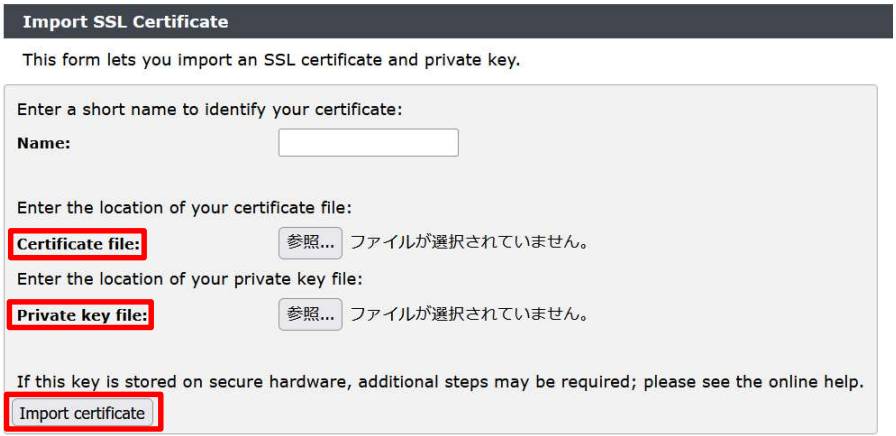
and Private Key をクリックします。



Certificate file に証明書ファイル

Private key file に秘密鍵ファイル

を選択し、Name を設定して、Import Certificate ボタンをクリックします。



Name は vTM に既に設定されている SSL サーバー証明書と異なる名称を設定してください。

SSL Server Certificates catalog にインポートされた証明書の設定が追加されます。

PCKS#12 形式でのインポートはできません。PEM フォーマットファイルでインポートしてください。

■インポート用秘密鍵ファイルの変換方法

既存または外部の SSL サーバー証明書をインポートするには SSL サーバー証明書のほかに秘密鍵が必要です。

サーバー証明書に対応する秘密鍵がない場合、インポートはできません。

また秘密鍵はそのままインポートできない場合があります。その場合は openssl コマンドを利用し秘密鍵をインポートできる形式に変換します。

vTM では openssl コマンドを利用することができますので、vTM 内に秘密鍵をアップロードし、以下のコマンド操作で変換することができます。

openssl rsa -in <秘密鍵ファイル> -out <出力ファイル>

を実施し、出力されたファイルを取り出します。

または

openssl rsa -in <秘密鍵ファイル>

を実施し、表示された内容のうち、

-----BEGIN RSA PRIVATE KEY----- から

-----END RSA PRIVATE KEY----- までを

コピーしテキストファイル等に保存します。

5) 中間 CA 証明書のインポート

Catalogs＞SSL＞ SSL Server Certificates catalog メニューにて、作成済みの SSL サーバー証明書の設定を Edit します。

Certificate signing の項目で Update / Add Intermediate Certificate をクリックします。

Certificate file でインポートする中間 CA 証明書のファイルを選択します。

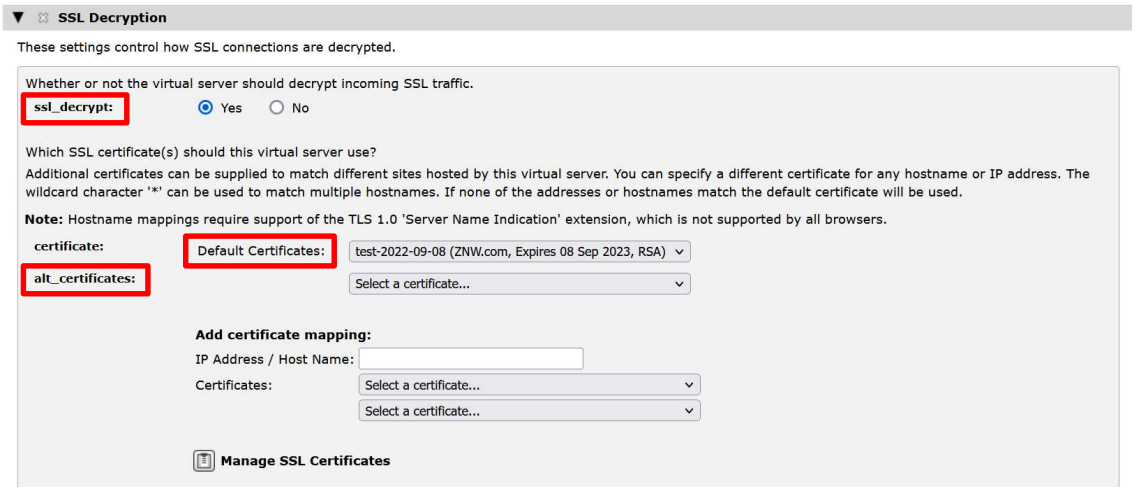
upload Intermediate Certificate をクリックします。

中間 CA 証明書の設定は SSL サーバー証明書の設定に追加されます。インポートした SSL サーバー証明書以外には適用されません。複数のサーバー証明書をインポート設定している場合はサーバー証明書の設定毎に中間 CA 証明書を設定してください。

サーバー証明書の期限更新などでサーバー証明書を更新されますと更新処理で中間 CA 証明書の設定が消失します。サーバー証明書更新処理の際には中間 CA 証明書をインポートし直してください。

6) Virtual Server への適用

Services>Virtual Servers＞Virtual Server 名＞SSL Decryption のメニューで設定します。



certificate の Default Certificates で作成済みの SSL サーバー証明書を選択します。

alt_certificates の項目で、異なる鍵タイプのサーバー証明書を追加設定することもできます。

例）Default Certificates：【RSA】、alt_certificates：【ECDSA】

証明書の選択後、ssl_decrypt を Yes に変更し、Apply Changes の Update をクリックし設定を保存します。

続いて Virtual Servers＞Virtual Server 名＞Basic Settings メニューの Internal Protocol と Port を変更します。

例えば Virtual Server で HTTPS を構成し、HTTP 用のノードに対して SSL オフロードを行う場合は、

Internal Protocol：HTTP

Port：443

を選択、設定します。

変更後、Update ボタンをクリックします。

7） サーバー証明書の更新

サーバー証明書の更新には、

・既存のサーバー証明書の更新

・新たにサーバー証明書をインポートし、Virtual Server に適用するサーバー証明書を切替え

の 2 つの方法があります。

「既存のサーバー証明書の更新」では有効期間の更新時に選択する方法となります。

Catalogs＞SSL＞ SSL Server Certificates catalog メニューで更新するサーバー証明書名を Edit します。

Export CSR / Sign Certificate をクリックし、Replace certificate に新しいサーバー証明書の内容をコピー＆ペーストし、Update Certificate ボタンをクリックします。サーバー証明書の Expire が更新されます。

この操作では中間 CA 証明書が消失しますので、再度中間 CA 証明書をインポートしてください。

「新たにサーバー証明書をインポートし、Virtual Server に適用するサーバー証明書を切替え」はサーバー証明書の内容変更、証明書のタイプ変更など、そのままサーバー証明書を更新できない場合に選択する方法です(サーバー証明書の有効期間の更新時にも選択できます)。

「4 サーバー証明書のインポート」の方法で新しいサーバー証明書を作成し、「6 Virtual Server への適用」の方法で、Virtual Server の SSL Decryption 設定で使用する Default Certificates を新しいサーバー証明書に変更します。

8) 日本語 JP ドメイン用のサーバー証明書

日本語 JP ドメインの設定はドメインを Punycode 表記で設定します。

外部で作成した日本語 JP ドメインのサーバー証明書を利用する際には UTF-8 形式ではなく、Punycode 表記で作成された CSR をもとにしたサーバー証明書をご利用ください。

Punycode 表記でない場合、SNI 設定を行っても正しく名前解決できないことがあります。

9) クライアント証明書の利用

SSL オフロードには SSL クライアント証明書を使った認証を設定することができます。

TrafficScript を利用することで、特定の URL パスへアクセスした際にクライアント証明書を要求する設定が可能となります。

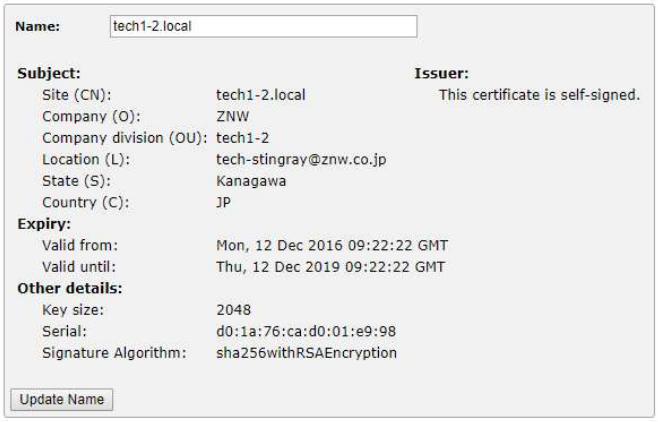
弊社で確認しているクライアント証明は

・サイバートラスト　デバイス ID

・自己証明書

でテストを行っております。

Catalogs＞SSL＞Certificate Authorities and Certificate Revocation Lists Catalog メニューで、外部機器にて作成した CA ファイルと CRL ファイルをインポートします。



クライアント証明書による認証設定は、Services＞Virtual Servers＞Virtual Server 名＞SSL Decryption の設定で行います。

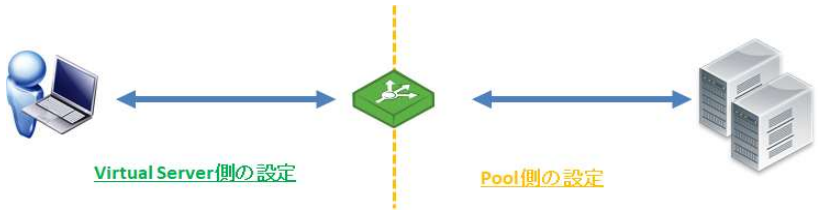
アクセスが発生した際にクライアント証明書を要求するために、request_client_cert を Require a client certificate に変更し、認証対象のドメインを指定するために client_cas でインポートしている CA の設定を選択します。

Certificate Authority でCA 設定にチェックがない場合、クライアント証明書の有無しかチェックしません。クライアント証明書が vTM で設定するサイトと異なるコモンネームのものであっても認証が OK となり SSL サイトへの認証、アクセスができてしまいます。

また、複数の CA の設定がインポートされている場合、チェックされている CA のドメインのみが認証 OK となります。

10. タイムアウト設定の調整

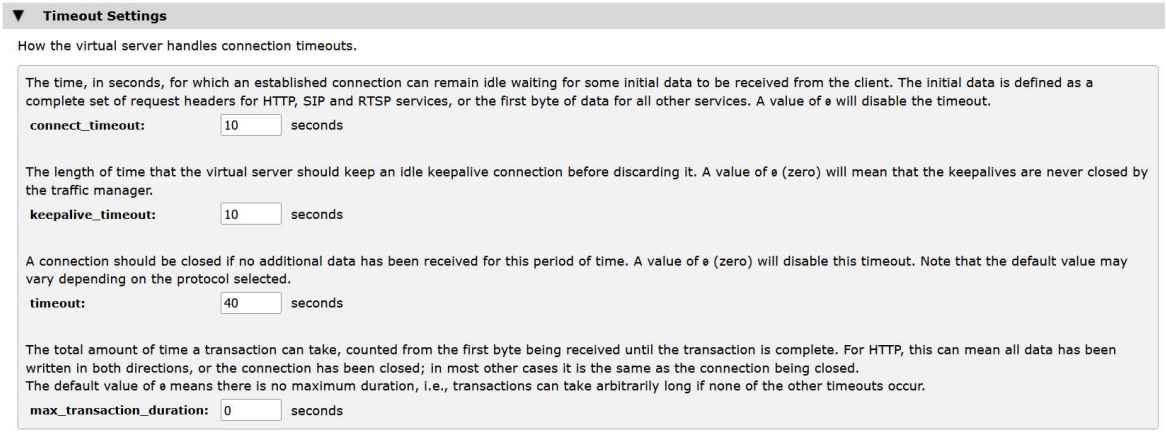
タイムアウトの設定は２つに分かれます。



接続端末ーvTM 間	Virtual Server の設定 Services>Virtual Servers＞Virtual Server 名＞Protocol Settings＞Timeout Settings
vTM－バックエンドノード間	Pools の設定 Services>Pools＞Pool 名＞Protocol Settings

1) Virtual Sever 側の設定

接続端末－vTM 間の設定は Services>Virtual Servers＞Virtual Server 名＞Protocol Settings>Timeout settings メニューで設定します。



Connect_timeout	新しいコネクションからのデータを待つ時間を設定します。
Keepalive_timeout	HTTP の場合に表示します。 アイドル状態の keepalive のタイムアウトを設定します。
timeout	既存コネクションがデータを受信しない場合に接続を閉じる時間を設定します。

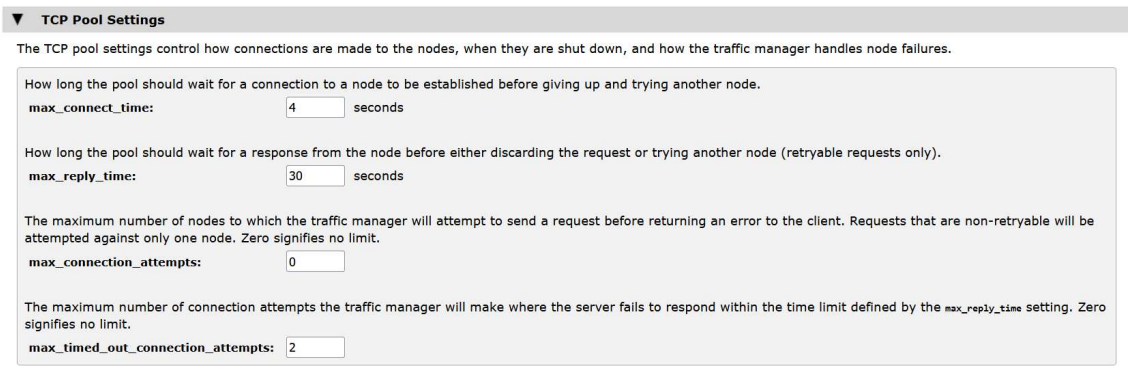
これらの値はバックエンドノードで動作するアプリケーション、接続元などシステム設計等を踏まえて調整を実施します。

デフォルト設定では HTTP/2 のタイムアウトは Timeout settings メニューで共通の設定となります。

HTTP/2 のタイムアウトを個別に設定する場合は、Services＞Virtual Server＞Virtual Server 名＞Protocol Settings＞HTTP/2-Specific Settings で設定します。

2) Pools 側の設定

vTM－バックエンドノード間の設定は Services＞Pools＞Pool 名＞Protocol Settings>TCP Pool Settings のメニューと TCP Connection Limits and Queueing のメニューで設定します。



■max_reply_time の設定

max_reply_time の設定は Health Monitoring の設定と関連します。

Health Monitoring の設定値より max_reply_time の値が大きい時、バックエンドノードからの応答を待っている間に、Health Monitoring のタイムアウトによってノードがフェイルと判断されてしまうことがあります。

そのため、Monitors で検知される時間のほうが遅い設定とするか Monitors で検知される時間と同じくらいに max_reply_time の値を設定します。

3) ノードへの再試行

■再試行の設定

再試行の設定項目におけるノード数等の設定には初回分が含まれます。

例えば max_timed_out_connection_attempts の設定が 2 の場合、最初にエラーとなったバックエンドノード+他のバックエンドノードというカウントになります。

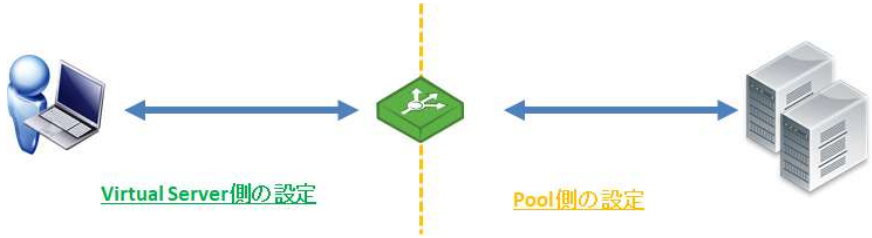
最初のバックエンドノードがエラーとなったのち、再試行するバックエンドノードが 2 台という設定にはなりません。

■応答コードによる再試行

Passive_Monitoring:Yes の際の再試行動作では応答コード 503 の場合のみ、設定条件によって再試行されますが、他の 5xx の応答コードにつきましては、応答コードによって再試行の判断はされません。

コネクション、リクエストのタイムアウトで判定されます。

4) Timeout の計算方法



タイムアウトを設定するにあたっては

接続元－vTM 間のタイムアウト（Virtual Server 側の設定）は vTM―バックエンドノード間のタイムアウト（Pool 側の設定）より大きい値を設定します。

これにより、vTM―バックエンドノード間よりも接続元－vTM 間の方があとにタイムアウトすることになります。

vTM―バックエンドノード間のタイムアウト（Pool 側の設定）は Passive Monitoring の有効／無効により変わります。

Passive Monitoring の設定は Services＞Pools＞Pool 名＞Health Monitoring に項目があります。

■vTM－バックエンドノード間のタイムアウト最大値の計算

Passive_monitoring：No の設定時

max_reply_time　x　max_timed_out_connection_attempts

Passive_monitoring：Yes の設定時

（max_connect_time　＋　max_reply_time）　x　max_timed_out_connection_attempts

■接続元－vTM 間のタイムアウト最大値の計算

上記 vTM－バックエンドノード間のタイムアウト最大値の計算値に 5～10 を加算した値が Virtual Sever 側の timeout　の最大値となります。

11. アップグレード手順

ここでは、ver22.2 系（ソフトウェア版）をベースにアップグレード手順を紹介します。

基本的にアップグレード前の設定は、アップグレード後も引き継がれます。

その他のバージョンをご利用の場合、表現が一部異なる場合がありますが、手順に大きな差異はないため適宜読み替えをお願いします。

1） バージョンアップ要件

バージョンアップを行うにあたり、実施前にディスク空き容量が 2GB 以上を満たしている必要があります。

ver10.4 系、ver17.2 系のバージョンから ver22.2 系には直接アップグレードができません。この場合、一度メジャーバージョン(ver20.1)を経由する必要があります。ver18.2 系以降のバージョンは直接アップグレードが可能です。

2） バージョンアップ前の正常稼働の確認

vTM がエラー/警告状態でないことを確認します。管理 UI 右上ステータス表示が ”Cluster: OK” であれば、正常な状態です。

［補足］

1 台構成（シングル構成）と 2 台以上構成（冗長構成）のどちらの場合も、ステータス表示は ”Cluster: OK” が正常な状態になります。

3） スナップショットの取得

ニフクラ環境でバックアップのためにスナップショットを取得します。2 台以上構成（冗長構成）の場合は、1 台ずつ取得します。

アップグレードに不具合のあった場合は、スナップショットから現状復帰します。

［補足］

ニフクラのスナップショットのご利用には別途料金が必要です。なお、スナップショットの取得についてのご質問は、ニフクラ問合せ窓口までお問合せください。

4) 1 台構成（シングル構成）におけるアップグレード

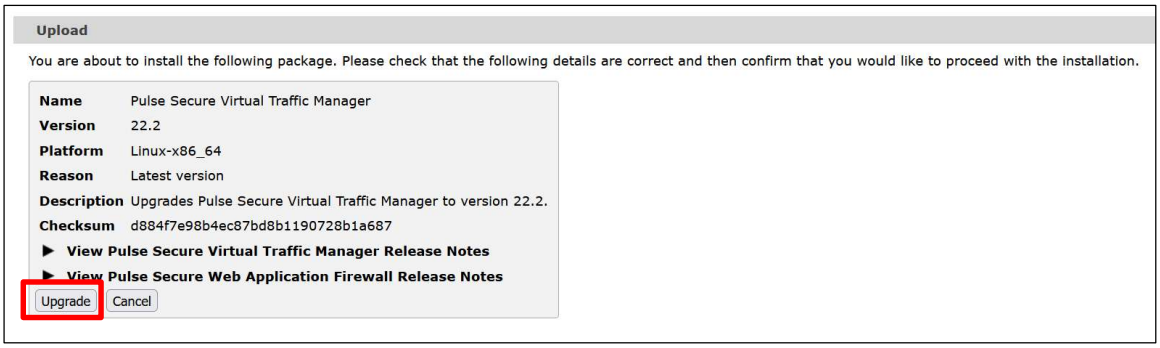
ここでは、vTM のパッケージファイルを用いたアップグレードの方法を紹介します。

※アップグレード作業前に、前述の［バージョンアップ前の正常稼働の確認］と［スナップショットの取得］の作業を実施してください。

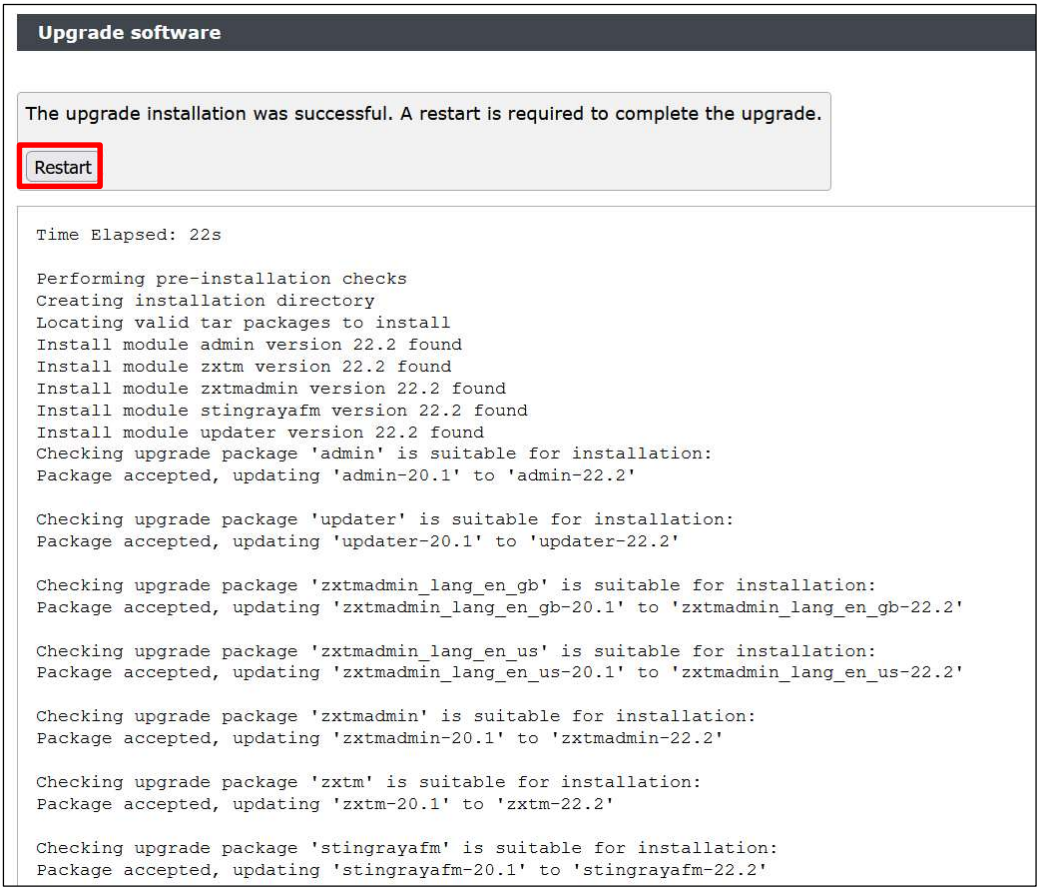
1．System＞Traffic Managers メニューの Software Upgrade セクションで Upgrade ボタンを押下します。

2．Software package セクションで参照･･･ボタンを押下し、パッケージファイルを選択後に Upgrade ボタンを押下し、ファイルをアップロードします。

3．パッケージファイルの情報が表示されたら、内容を確認し Upgrade ボタンを押下します。



4．アップグレードプロセスが完了したら、Restart ボタンを押下します。

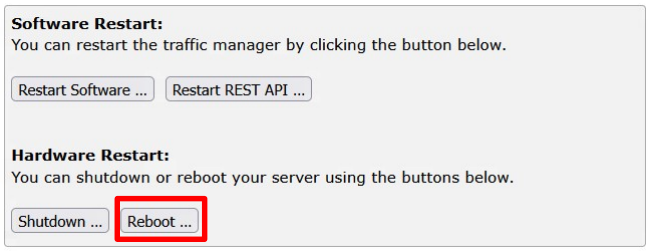


5．アップグレードが完了した後は、vTM を再起動します。

System＞Traffic Managers メニューの Hardware Restart セクションで Reboot ボタンを押下します。

確認画面が表示されるので、再度 Reboot ボタンを押下します。

※再起動により、ダウンタイムが発生します。



6．System＞Traffic Managers メニューでバージョンがアップグレードされていることを確認します。

5） 2 台以上構成（冗長構成）におけるアップグレード

前述の 1 台構成（シングル構成）の手順と同様に vTM のパッケージファイルを用いて、1 台ずつアップグレードを実施してください。

※アップグレード作業前に、前述の［バージョンアップ前の正常稼働の確認］と［スナップショットの取得］の作業を実施してください。

［補足］

アップグレードの過程で、管理 UI 右上ステータス表示が ”Cluster: Conflict” と表示されることがあります。これは異なるバージョンのクラスタ構成になっていることが原因です。異なるバージョンのクラスタ構成では、クラスタ間で設定を同期することができませんので、ご注意ください。（異なるバージョンのクラスタ構成では、各種パラメータを変更することができません。）そのまま運用することはせずに全て同じ

バージョンにアップグレードを行ってください。アップグレード完了後にステータス表示は正常状態に戻ります。

6） 新しい OS サーバー（vTM 用）を作成する必要がある場合のアップグレード

ここでは、サーバーの OS のサポート終了などが理由で、新しくサーバーを作成して vTM の移行が必要になる場合のアップグレード方法を紹介します。

この手順では、新しく作成するクラスタ構成のサーバー2 台の IP アドレスが移行前の環境と異なっております。移行前と同じ IP アドレスでサーバーを作成した場合も手順に大きな差異はございません。

1. 新しいアクティブマシンとスタンバイマシンとして、vTM をインストール後に新しいライセンスが投入された状態のサーバーを 2 台用意します。

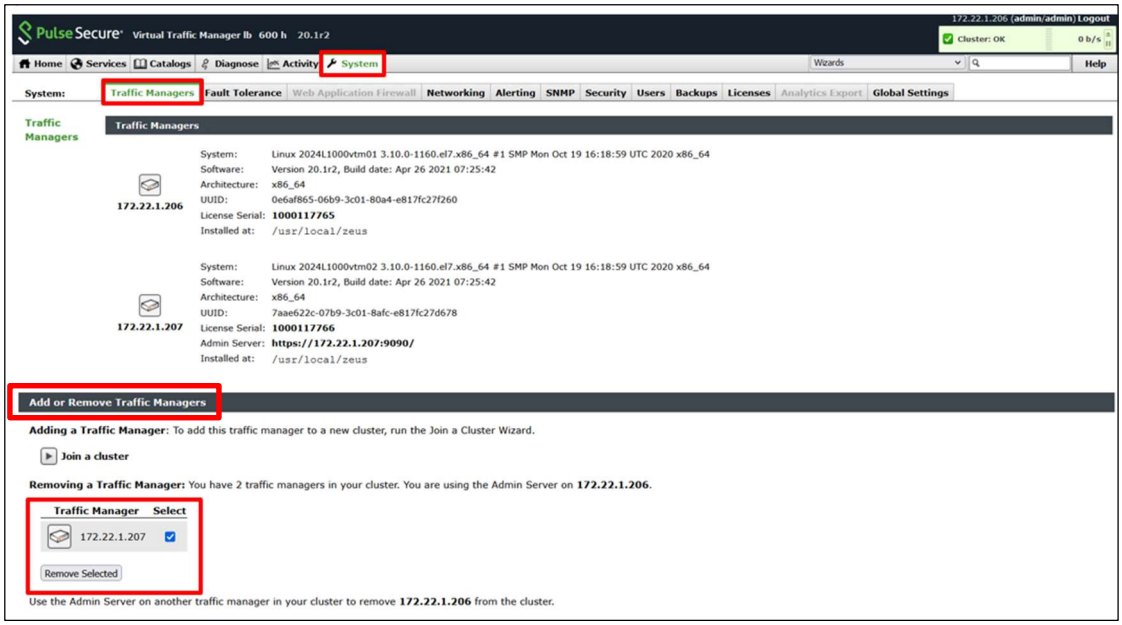
［補足］

新しく作成するクラスタ構成のサーバー2 台の IP アドレスが移行前と同じ場合は、既存のライセンスが引き継がれますので、ライセンス投入は不要です。

※アップグレード作業前に、前述の［バージョンアップ前の正常稼働の確認］と［スナップショットの取得］の作業を実施してください。

2．現行アクティブマシンの管理 UI にログインし、現行スタンバイマシンのクラスタ切り離しを行います。

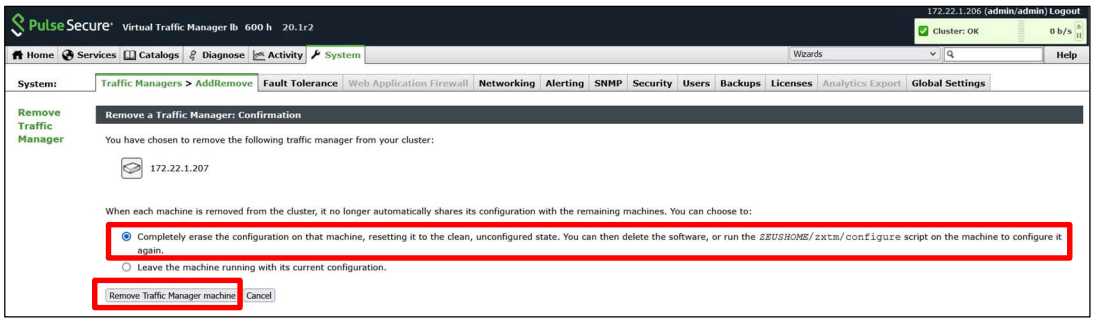
System＞Traffic Managers メニューの Add or Remove Traffic Managers セクションで、現行スタンバイマシンを選択し、Remove Selected ボタンを押下します。



“Completely erase the～” を選択し、Remove Traffic Manager machine ボタンを押下します。

［補足］

現行スタンバイマシンの管理 UI には、クラスタ切り離し後アクセスできなくなります。



3．現行スタンバイマシンをシャットダウンし、新しいスタンバイマシンを起動します。

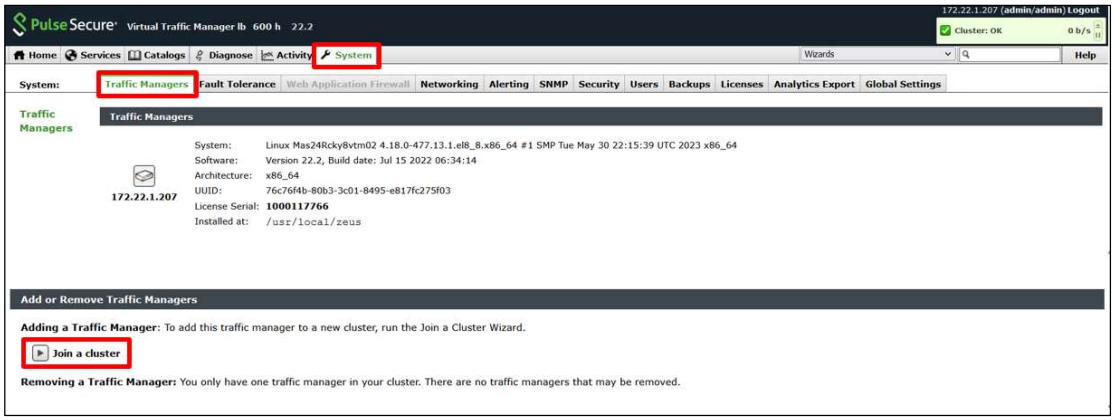
［補足］

マシンのシャットダウンは、ニフクラ環境でサーバー停止をします。（停止オプションは不要です。）

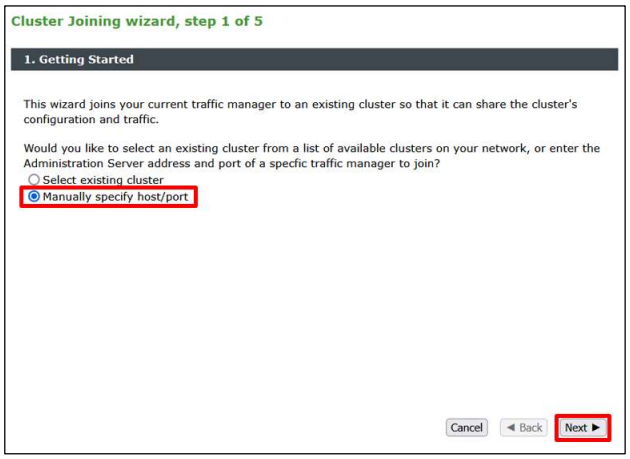
なお、ニフクラ環境での操作についてのご質問は、ニフクラ問合せ窓口までお問合せください。

4．新しいスタンバイマシンの管理 UI にログインし、クラスタ参加設定を行います。

System＞Traffic Managers メニューの Join a cluster を押下します。



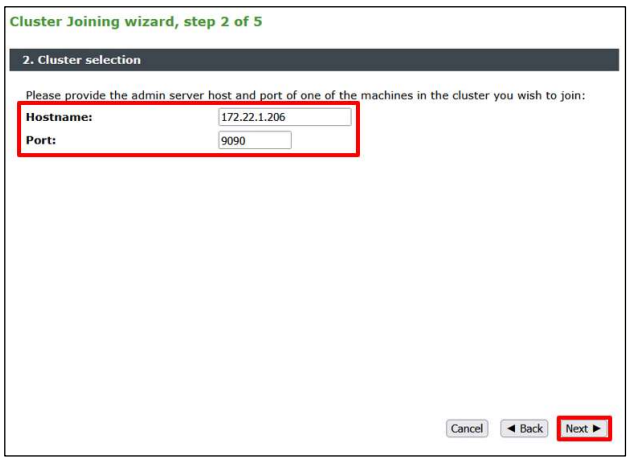
「1.Getting Started」画面の ”Manually specify host/port” を選択し、Next ボタンを押下します。



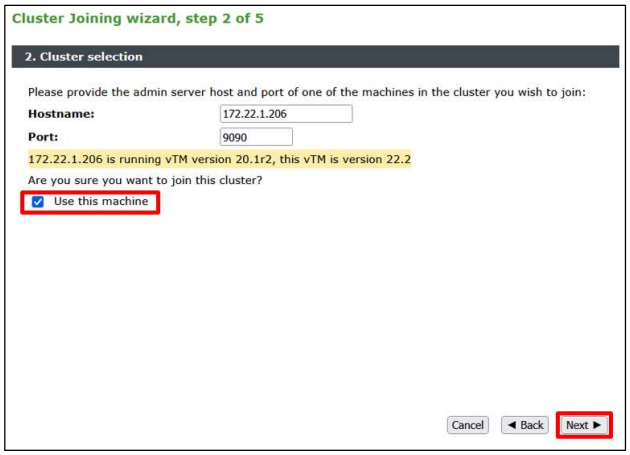
「2.Cluster selection」画面で現行アクティブマシンの Hostname（IP アドレス または ホスト名）、Port（ポート番号）を入力して、Next ボタンを押下します。

［補足］

ポート番号は、現行アクティブマシンの管理 UI にアクセスするために必要な通信ポート（デフォルトは 9090）の情報です。



“Use this machine” にチェックを入れ、Next ボタンを押下します。

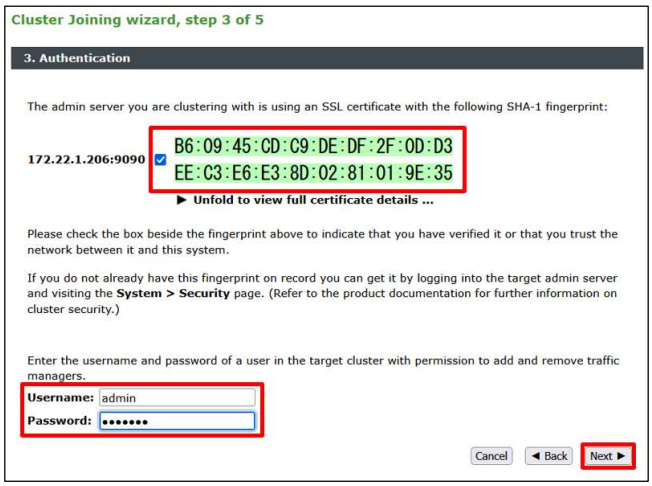


「3.Authentication」画面で下記を設定し、Next ボタンを押下します。

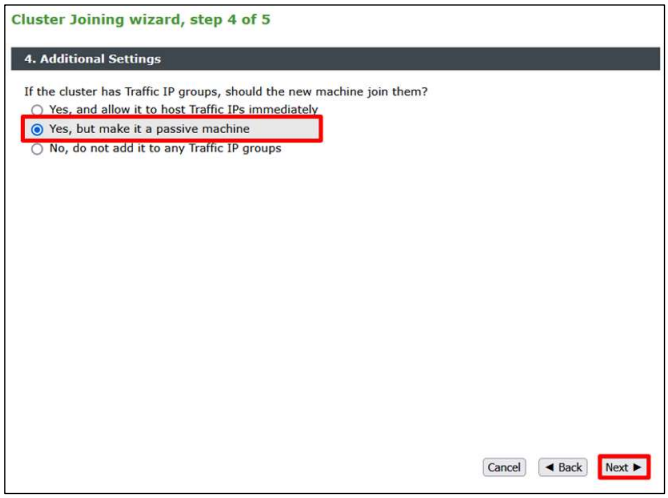
［補足］

ここで入力する情報は、現行アクティブマシンの情報になります。

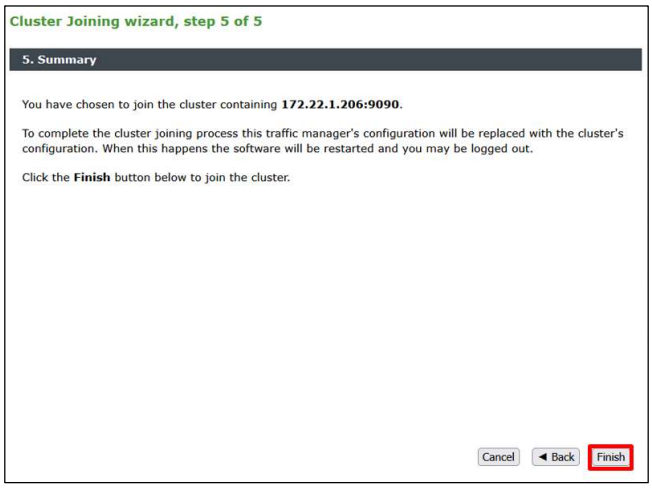
Fingerprint	チェックボックスにチェックを入れる
Username	現行アクティブマシンの管理ユーザー名を入力
Password	管理ユーザーに対応するパスワードを入力



「4.Additional Settings」画面で ”Yes, but make it a passive machine” を選択して、Next ボタンを押下します。

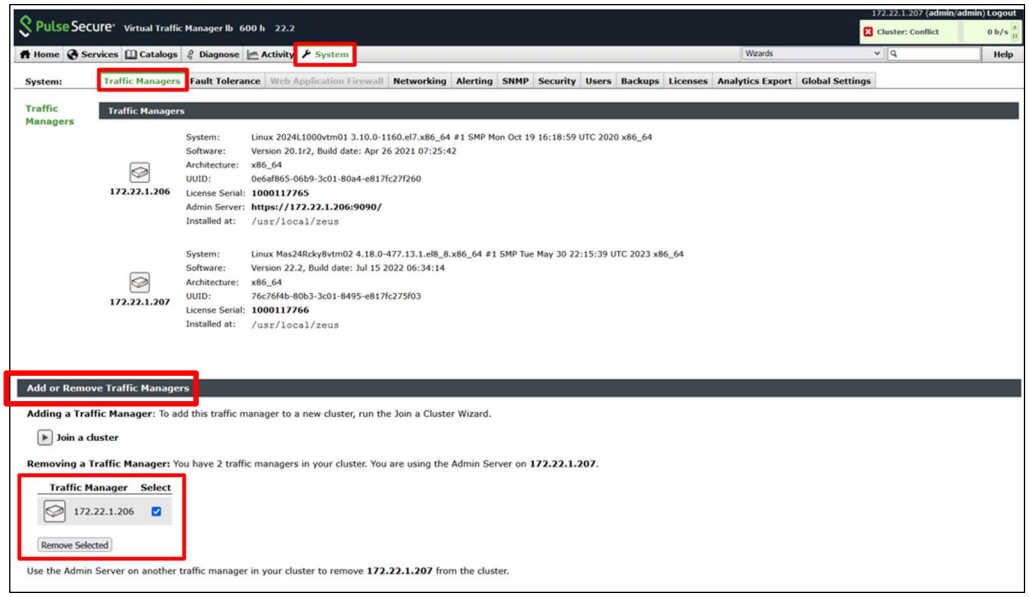


「5.Summary」画面で Finish ボタンを押下します。



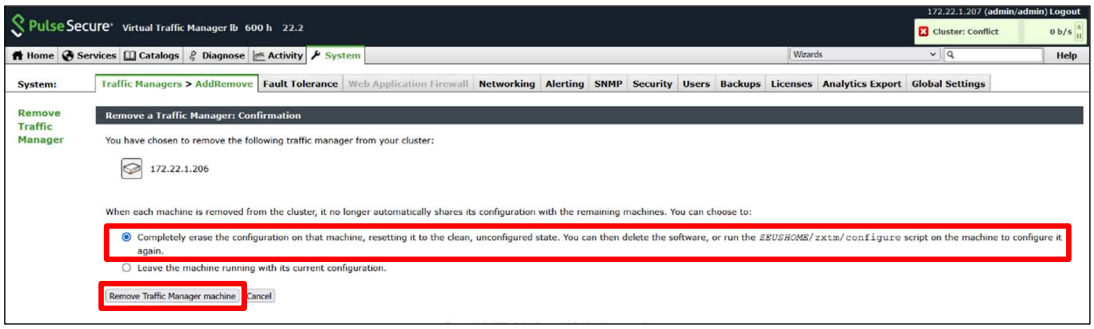
5．引き続き新しいスタンバイマシンの管理 UI で、現行アクティブマシンのクラスタ切り離しを行います。

System＞Traffic managers メニューの Add or Remove Traffic Managers セクションで、現行アクティブマシンを選択し、Remove Selected ボタンを押下します。



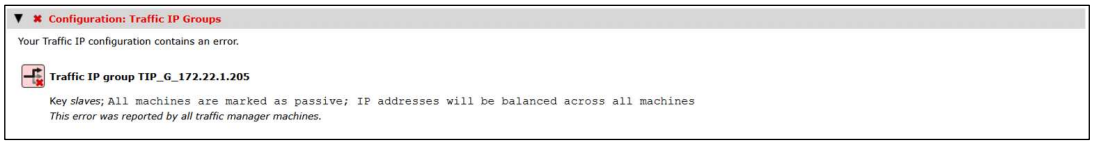
“Completely erase the～”を選択し、Remove Traffic Manager machine ボタンを押下します。

※Traffic IP がフェールオーバーするため、ダウンタイムが発生します。



［補足］

現行アクティブマシンのクラスタ切り離しをすることで、Passive の Traffic Manager のみとなるために、管理 UI 右上ステータス表示が ”Cluster: Warning” となり、一時的に［Configuration: Traffic IP Groups］に以下のエラーメッセージが表示されます。アップグレード完了後にエラーメッセージは解消されます。



6．現行アクティブマシンをシャットダウンし、新しいアクティブマシンを起動します。

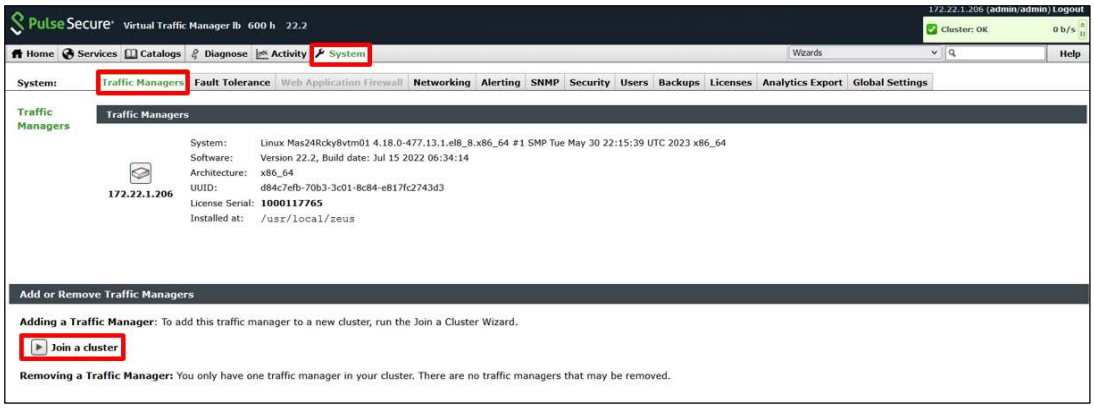
［補足］

マシンのシャットダウンは、ニフクラ環境でサーバー停止をします。（停止オプションは不要です。）

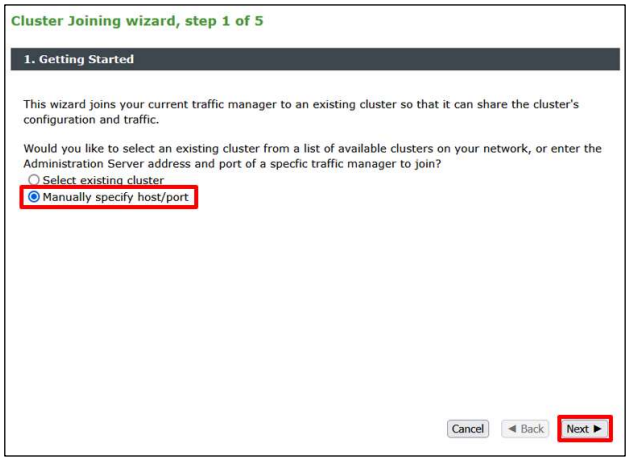
なお、ニフクラ環境での操作についてのご質問は、ニフクラ問合せ窓口までお問合せください。

7．新しいアクティブマシンの管理 UI にログインし、クラスタ参加設定を行います。

System＞Traffic Managers メニューの Join a cluster を押下します。



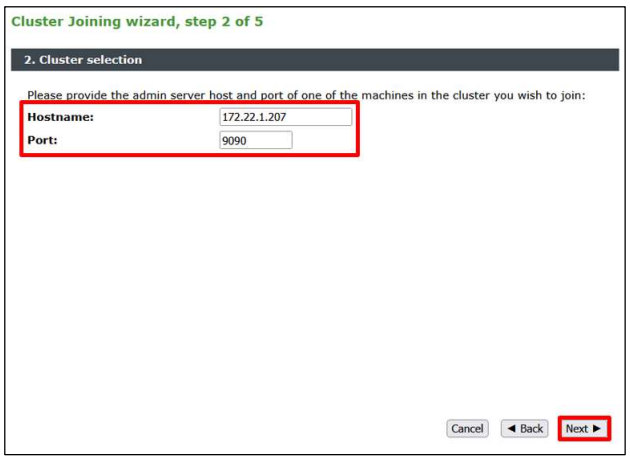
「1.Getting Started」画面の ”Manually specify host/port” を選択し、Next ボタンを押下します。



「2.Cluster selection」画面で新しいスタンバイマシンの Hostname（IP アドレス または ホスト名）、Port（ポート番号）を入力して、Next ボタンを押下します。

［補足］

ポート番号は、新しいスタンバイマシンの管理 UI にアクセスするために必要な通信ポート（デフォルトは 9090）の情報です。

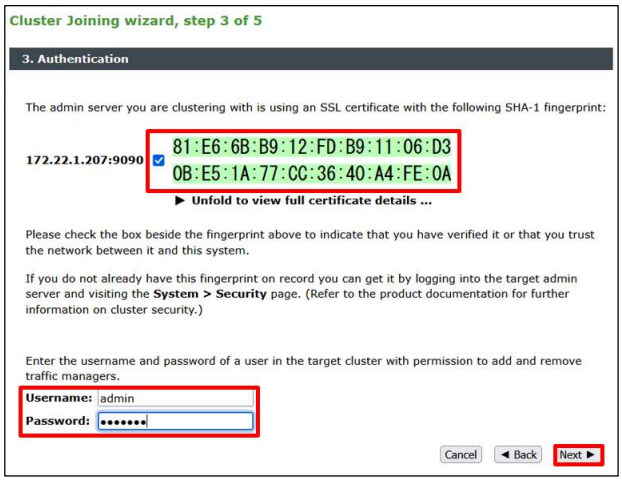


「3.Authentication」画面で下記を設定し、Next ボタンを押下します。

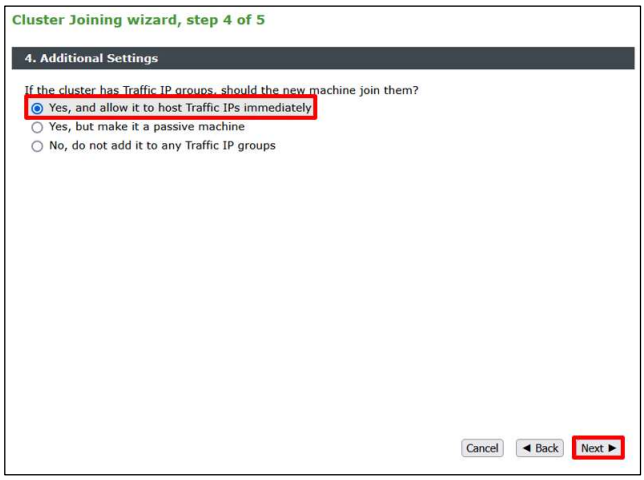
［補足］

ここで入力する情報は、新しいスタンバイマシンの情報になります。

Fingerprint	チェックボックスにチェックを入れる
Username	新しいスタンバイマシンの管理ユーザー名を入力
Password	管理ユーザーに対応するパスワードを入力

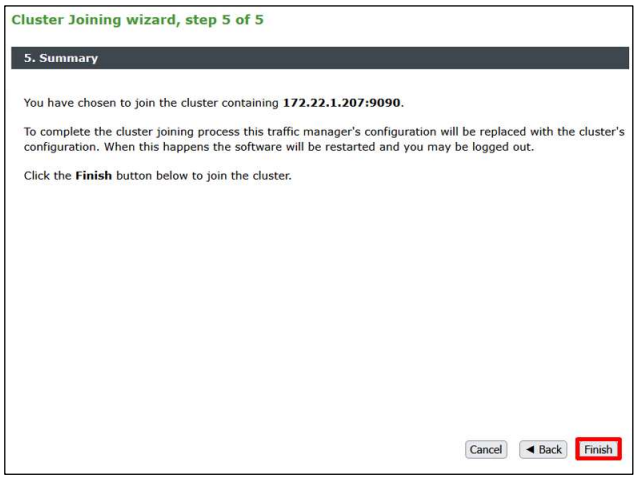


「4.Additional Settings」画面で、”Yes, and allow it to host Traffic IPs immediately” を選択して、Next ボタンを押下します。



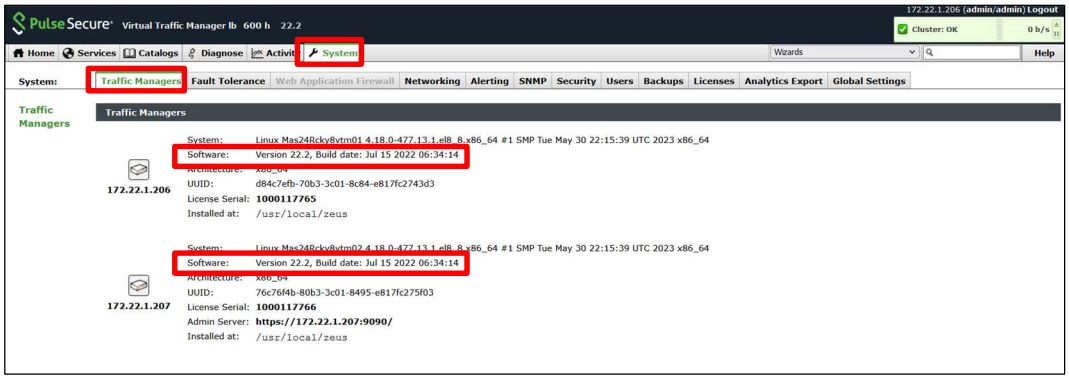
「5.Summary」画面で Finish ボタンを押下します。

※Traffic IP がフェールオーバーするため、ダウンタイムが発生します。



8．バージョンがアップグレードされていることを確認します。

System＞Traffic Managers メニューでバージョンがアップグレードされていることを確認します。



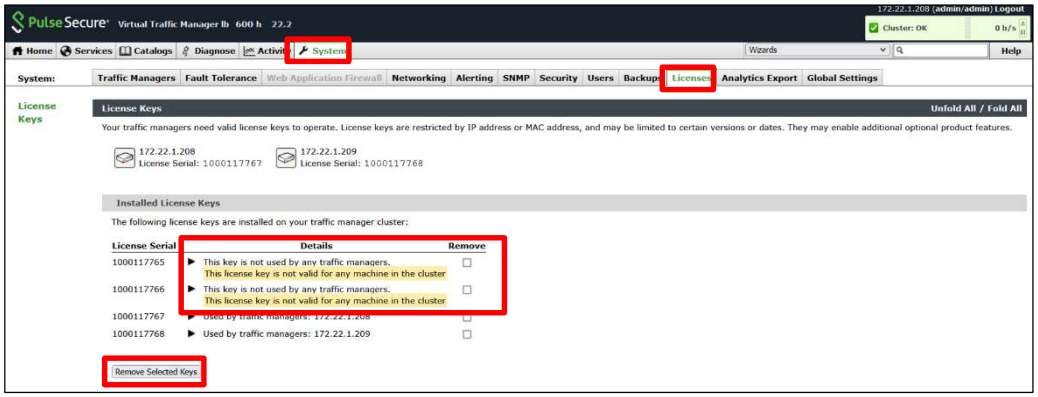
9. クラスタから切り離したマシンの不要なライセンスを削除します。

System> Licenses メニューの Installed License Keys セクションにて、Details に［This key is not used by any traffic managers. This license key is not valid for any machine in the cluster.］のメッセージが表示されているライセンスシリアルの Remove にチェックをし、Remove Selected Keys ボタンを押下します。

ライセンスの削除はクラスタ間で同期されるため、新しいアクティブマシンもしくはスタンバイマシンのどちらか一方の管理 UI で実施をいただければ問題ございません。

［補足］

新しく作成するクラスタ構成のサーバー2 台の IP アドレスが移行前と同じ場合は、既存のライセンスが引き継がれますので、この手順は不要です。



7） Rollback について

System＞Traffic Managers メニューの Switch Versions の項目で、表示されている元のバージョン（アップグレード前のバージョン）に Rollback できます。

元のバージョン選択後、Confirm のチェックをクリックし、Rollback ボタンをクリックします。

Rollback で該当バージョンへ切り替りが完了した後は、vTM を再起動してください。

■Rollback 後のアップグレードについて

既に上位バージョンを適用している環境で Rollback を行っている場合、ファームウェアのアップロードがエラーとなることがあります。

System＞Traffic Managers メニューの Switch Versions　の項目にてバージョンが表示されている場合、Rollback の動作で該当バージョンに戻すことができます。

バージョン選択後、Confirm のチェックをクリックし、Rollback ボタンをクリックします。

Rollback にて該当バージョンへ切り替りが完了した後は、vTM を再起動してください。

Software Upgrade メニューを利用したダウングレードはできません。

Rollback 操作にて旧バージョンが表示されない場合は、vTM をアンインストールし、残ったファイルを削除したのち、希望されるバージョンにて再度インストールする方法となります。

12. よくある質問

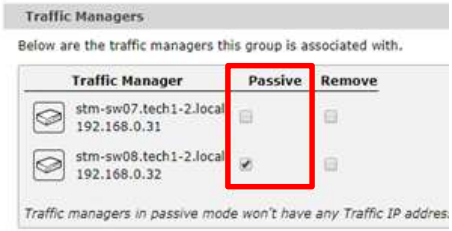
1) アクティブースタンバイの切替え

冗長構成された vTM のアクティブースタンバイを手動で切り替えるには、Traffic IP Groups のメニューで設定します。

管理 UI から Services＞Traffic IP Groups＞Traffic IP Groups 名の Edit をクリックします。

Traffic Managers の項目で、Standby 側に設定したい Traffic Manager の Passive の項目にチェックを入れます。

Active 側に設定したい Traffic Manager には Passive にチェックをしません。



Apply Changes の Update ボタンをクリックし設定を反映させます。

Passive にチェックがついているマシンが Standby マシンとして動作します。

［補足］

冗長構成の vTM のどちらかに通信を片寄せしたい場合は、全ての Traffic IP Groups 名で、上記設定を行ってください。

フェイルオーバー時を含め、アクティブースタンバイが切り替わる際にコネクション、セッションは引き継がれません。通信断が発生します。

vTM 内にキャッシュされている Session Persistence の情報は Cluster を構成する vTM 間で同期しているため、切り替わり後も同じノードに接続することができます。

2) 通信断

フェイルオーバー発生時、コネクション、セッションは引き継がれません。

また異なる鍵タイプ、暗号化スィートへの切替え時など SSL 設定を変更された場合も通信断は発生します。

Service Protection 等の Classes 設定ではキャパシティが関連するため、縮小する設定に変更された場合、通信への影響は発生します。

Pools へのノードの追加設定では通信断は発生しません。

3) DNS 解決エラー

vTM では DNS 参照による名前解決が必要となります。

名前解決ができない場合、Cluster Error となり、エラーが記録されます。

/etc/resolv.conf に名前解決ができる DNS サーバーが設定されていない場合、Join a Cluster 実施時にエラーとなります。

また vTM 自身のホスト名が解決できない場合、イベントログに

*Hostname ***** dose not resolve to any of our specified IP Address*

と記録されます。

vTM1000 シリーズ以上で利用可能な DNS-derived autoscaling の機能を設定される場合、名前解決ができないことによって期待される動作とならず、ノードのエラーが記録されることがあります。

4) Cluster Error

管理 UI 右上に表示する Cluster Error、Cluster Warning は vTM の設定・動作に問題が発生した際に表示します。

文字をクリックするとエラー詳細を確認することができます。

この Cluster　という表示は冗長構成での Cluster という意味ではありません。

構成するマシンという意味になり、vTM が 1 台でも Cluster で表示になります。

5)　ノードフェイル

vTM がノードフェイルを検知すると、イベントログに　nodefail が記録されます。

ノードフェイルは Pool に設定された Health Monitoring の設定、vTM の死活監視で検知されます。

vTM のイベントログにはノードのフェイルを検知したことだけが記録されます。

メッセージ例
Monitor Full HTTP: Monitor has detected a failure in node '172.16.0.127:80': Read failed: Connection refused
Pool default-web, Node 172.16.0.127:80: Node 172.16.0.127 has failed - A monitor has detected a failure

ノードフェイルの原因の多くは

・時間内にコネクション確立ができない

・バックエンドノードのアプリケーションからの応答が得られない

などのタイムアウトといったものです。

vTM 側ではなく、基盤上の負荷の影響、ネットワーク疎通の問題やバックエンドノード側の応答遅延といった場合、バックエンドノード側の状態をご確認いただくこととなります。

弊社サポートセンターに原因の質問をいただいても、vTM のイベントログからはバックエンドノード側の原因を調べることはできません。

6） Traffic Manager 自身のダウン

vTM はゲートウェイ、バックエンドノードへの Ping 疎通ができない場合、自身をフェイルと判断します。

自身をフェイルと判断した場合に、設定されている Traffic IP Address の関連が解除されます。

Cluster 構成ではアクティブ側として動作していた vTM が自身をフェイルと判断することによって、Traffic IP Address の関連をスタンバイしていた vTM 側に移動します。

フェイルオーバー動作となり、スタンバイがアクティブに昇格し、Traffic IP Address への通信が可能となります。

Cluster を構成する全ての vTM が自身をフェイルと判断した場合に、Traffic IP Address の関連は解除され、 TIP への通信はできなくなります。

デフォルトではハートビート通信は vTM で認識している全インターフェースを利用します。

ライセンスを申し込んだ IP アドレスが設定されているインターフェースでハートビート通信ができないと vTM はフェイル判断をします。

ハートビート通信を制限する設定は System＞Security＞Cluster Communication メニューの controlallow の設定で行います。

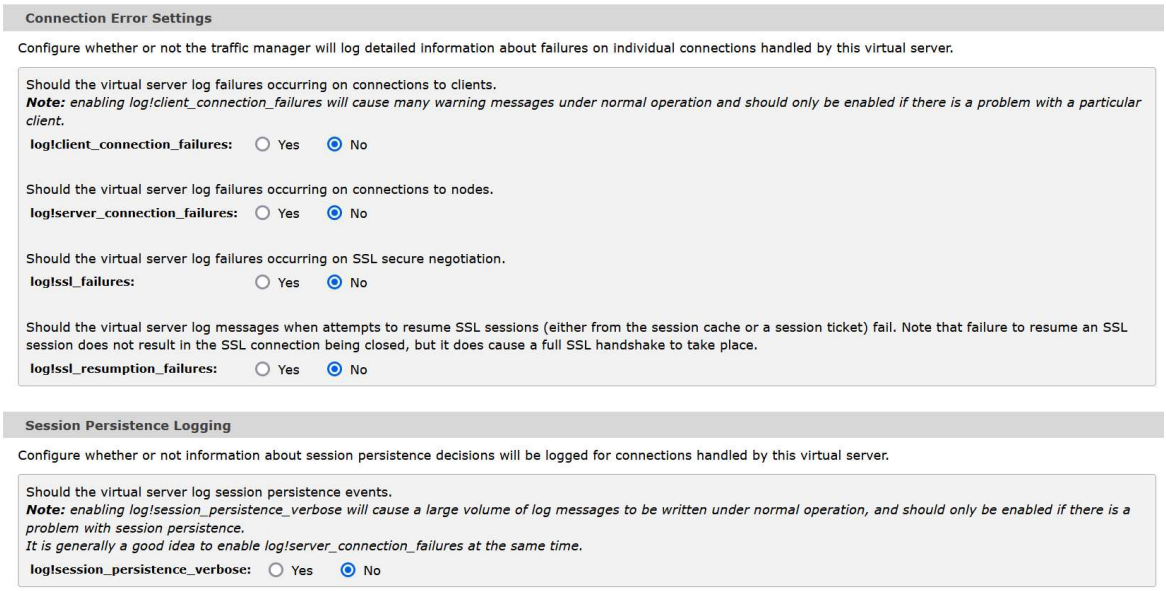
本設定でハートビート通信を行うネットワークを制限する場合はライセンスを申し込んだ IP アドレスのネットワークが含まれるように設定してください。

また OS 側の iptables 等で制限しないようにご注意ください。

7） コネクションエラーの出力

コネクションエラーはログに出力させることができます。

Services＞Virtual Servers＞Virtual Server 名＞Error Logging のメニューで設定します。



log!client_connection_failures	接続元－Virtual Server 間の接続で発生したエラーをログに出力します。 ログ量が多量となるため、接続元に問題がある場合のみ有効（Yes）にしてください。
log!server_connection_failures	ノードへの接続で発生したエラーをログに出力します。
log!ssl_failures	接続元－Virtual Server 間の SSL 接続で発生したエラーをログに出力します。
log!ssl_resumption_failures	接続元－Virtual Server 間においてセッションキャッシュ、セッションチケットによる SSL 再接続のログを出力します。
log!session_persistence_verbose	Session Persistence による接続をログに出力します。 合わせて log!server_connection_failures を有効にすることが推奨されます。 本設定を有効（Yes）にすることで、多量のログが出力されます。

設定を有効（Yes）にすることにより、ログが多量となり、DISK 領域を圧迫する結果となることがあります。

障害解析以外の目的では設定を無効（No）にし、運用してください。

8） SSL 暗号化スィートの設定

vTM では vTM 全体または Virtual Server 毎に利用する SSL 暗号化スィートを指定することができます。

vTM 全体で設定する場合は

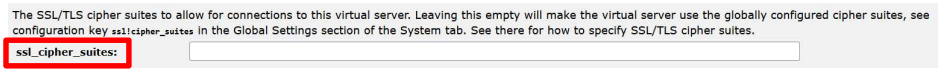
System＞Global Settings＞SSL Configuration メニュー

Virtual Server 毎に設定する場合は

Services＞Virtual Servers＞Virtual Server 名＞SSL Decryption メニュー

で設定します。

vTM 全体の設定よりも Virtual server 個別の設定が優先されます。

vTM 全体の設定 *System＞Global Settings＞SSL Configuration* 	ssl!cipher_suites
Virtual Server 毎の設定 *Services＞Virtual Servers＞Virtual Server 名＞SSL Decryption* 	ssl_cipher_suites

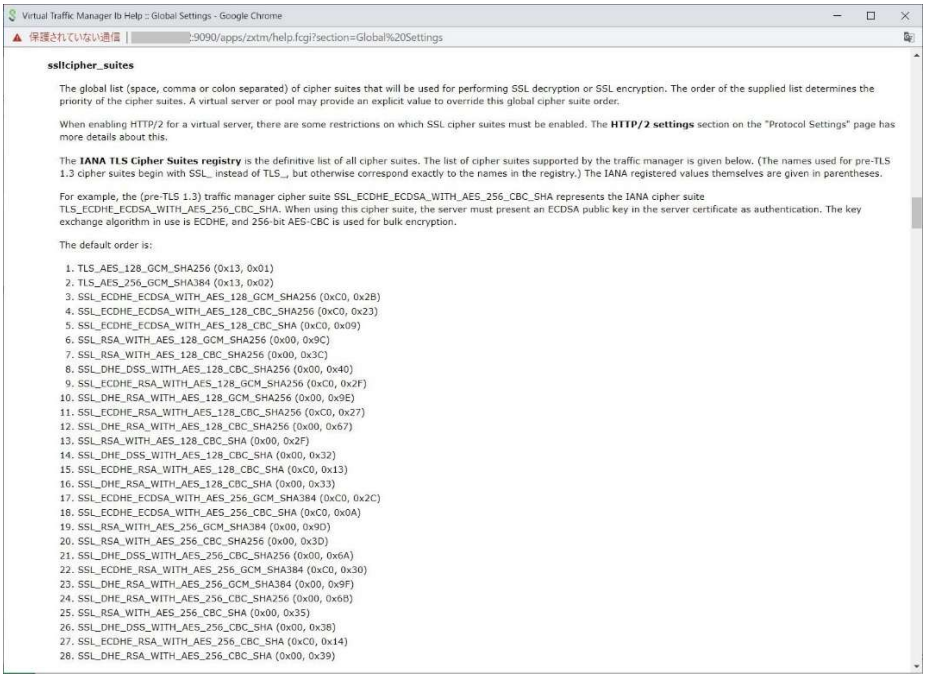
項目はデフォルトで空欄です。空欄の状態ではデフォルトで有効となる暗号化スィート全てが利用可能です。

デフォルトで有効となる暗号化スィートは HELP から確認することができます。

管理 UI から System＞Global Settings＞SSL Configuration メニューを開き、右上の HELP をクリックします。

別ウィンドウが開き、ssl!cipher_suites の項目で対応する暗号化スィートを確認することができます。

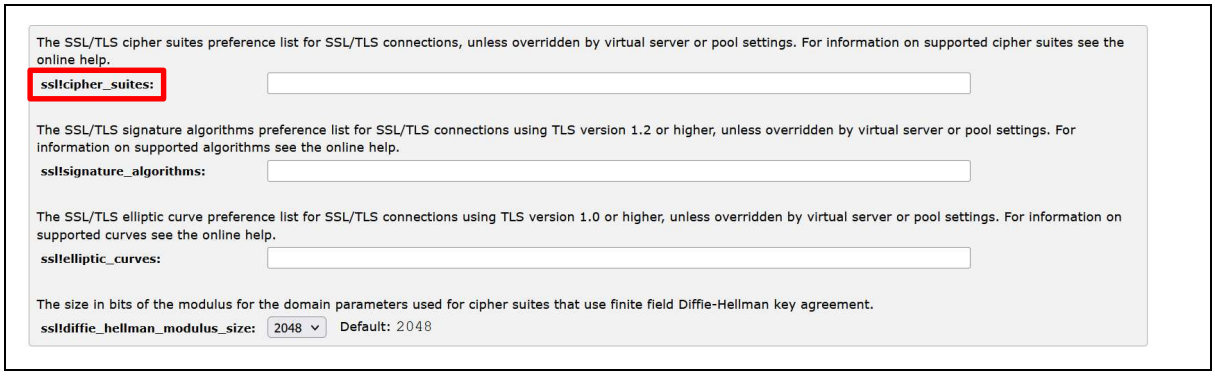
暗号化スィートはリストの上位から順番に優先利用されます。



SSL オフロードで利用する特定の暗号化スィートを指定するには ssl!cipher_suites の項目に設定します。

複数の暗号化スィートはカンマ区切りで指定します。

優先される順番は先頭からの順になります。



暗号化スィートは SSL/TLS バージョン毎に指定することはできませんが、指定する暗号化スィートによって利用できる SSL/TSL バージョンが異なります。

暗号化スィート毎に対応する SSL/TLS バージョンに関する情報は弊社サポートサイトの「技術情報」に掲載しております。

9) SSL コネクションエラー

SSL コネクションエラーは SSL/TLS バージョン、ネゴシエーションに利用する暗号化スィートのミスマッチで発生します。

vTM は設定された通りの SSL 接続となります。

SSL コネクションエラー発生時には必ず汎用的なツールである、IE、Firefox、Chrome 等の複数のウェブブラウザ、openssl コマンドで再現性をご確認ください。

（ブラウザ毎に挙動が異なる場合があります。必ず複数のブラウザでご確認ください。）

汎用的なツールで SSL コネクションエラーが発生しない場合、vTM の SSL 設定が接続元の設定とミスマッチしているか、接続元のアプリケーションに起因する問題が考えられます。

汎用的なツールで SSL コネクションエラーが発生しない場合の解析へのご協力ができません。システムの構築担当、開発担当の各会社様にてご対応ください。

ver.18.2 以降 SSLv2 の設定は無く、SSLv2 の Client Hello を受け入れることができません。

13. サポート

1) サポート窓口

ニフクラ環境でご利用の vTM に関する問合せは、原則ニフクラ問合せ窓口にお問合せください。

弊社に直接ご連絡いただく場合には　E-mail support-tm@znw.co.jp 宛にメールでお問合せください。

弊社でご提供する直接対応ではサポート範囲内の対応となります。また以下の点にもご注意ください。

・原則お電話でのお問合せは対応しておりません。

・受付対応時間　弊社営業日　10：00～17：00　にて対応させていただいております。

・ご質問に対する回答期限のご要望には応じておりません。

2) サポート範囲

弊社が提供するサポートはシステムが稼働開始された後の POST サポートです。

導入前のお問合せはニフクラ問合せ窓口にご質問をお送りください。導入時の設定に関するご質問は有償でのご提供となる場合があります。

弊社が対応する範囲は vTM のソフトウェア部分となります。

弊社では以下のご質問に対してのサポート対応は実施しておりません。

・OS に関する操作、設定、エラー

・OS 側の脆弱性情報

・プロトコル動作、仕様

・ニフクラ環境の機能、サービス

・基盤側が関連する事象の説明

・vTM の設計、設定の詳細解説などコンサルティングや構築作業にかかわる点（別途有償対応）

・vTM の設定確認、設定の正当性確認（別途有償対応）

・お客様側にて作成された手順書の確認（別途有償対応）

・弊社提供外のモジュール、機能

・システムのネットワーク設定

・バックエンドノード側の設定、動作

vTM が動作している仮想サーバー内に、他のアプリケーションをインストール・設定されている場合、アプリケーションとの切り分けはお客様ご自身で実施してください。

vTM 設定方法の説明、コンフィグの正当性確認などは全て有償での対応をさせていただいております。
初めて構築されるお客様に対しては、弊社において導入前のご相談への対応、勉強会、レクチャを実施しております。
詳しくはニフクラ担当営業様までお尋ねください。

3） お問合せに必要な情報

お問合せ時には以下の情報をお送りください。

	障害	設定エラー	メッセージ	仕様
発生時刻	◎		◎	
問題の切り分けの実施状況 ※vTMの問題と確定していない場合	◎	○		
対象設定 Virtual Server/Poolなど	◎	◎	○	○
設定内容(設定項目名)		◎		○
動作結果 設定した結果の動作など		◎		△
Technical Support Report	◎	△	○	
コンフィグ	◎ ※SSL時	◎	○	△
構成図／処理フロー図	○	○		△

◎ … 必須情報

○ … なるべく提供いただきたい情報

△ … あるとよい情報

特に事象発生時間、対象の設定をご連絡いただきませんとスムーズな対応ができない場合があります。

■Technical Support Report（TSR）取得方法

Diagnose＞Technical Support ＞Querying Technical Support メニューで Manage Technical Support Reports をクリックします。

TSR Options で全ての項目にチェックを入れ、Generate TSR ボタンをクリックします。

Technical Support Report の生成がスタートし、準備ができますと操作を行っている PC 上にダウンロードされます。

■コンフィグ取得方法

System＞Backups＞Create a Backup メニューで Save ボタンをクリックします。

Save したバックアップが Backups stored on Traffic Manager に表示されます。

バックアップされた名称をクリックします。

Export Backup archive メニューから Export Configuration をクリックします。

操作 PC 上にコンフィグがダウンロードされます。

4） サポート終了

提供中の vTM の各バージョンにはメーカーのサポート提供に期日があります。

ver.22.2 系	2026 年 1 月 19 日

上記バージョン以外の古いバージョンは既にメーカーサポートが終了しています。

サポート終了後のバージョンに対してメーカーの解析は実施されません。

サポート終了後は弊社のノウハウ、ナレッジの範囲内で対応させていただきますが、全てのご質問に対して回答を提示できるとは限りません。

ご利用のバージョンがサポート終了となる前に上位バージョンへのアップグレードをご検討ください。

■メーカーリリースのバージョンとご案内バージョンの差異について

日本国内においてご案内するバージョンはメーカーがリリースした全てのバージョンではございません。

LTS（Long-Term Support）の対象となっているバージョンのみ日本ではご案内しております。

LTS バージョンはリリースから 3 年のメーカーサポート期間が設定されています。

ご案内しているバージョンではない、メーカーリリースバージョンをご利用されますとサポートを提供することができません。

5） サポートサイト

弊社では vTM を正規ライセンスでご利用されているお客様向けにサポートサイトを開設しております。

正規ライセンスお申し込み前のご利用は利用規約違反となります。

サポートサイト　http://www.znw.co.jp/support

「Virtual Traffic Manager サポートサイト」をクリックします。

ログイン画面が表示します。

サポートサイトへのログインには ID とパスワードが必要となります。

（評価を予定されているお客様、評価中のお客様は前述の steelapp-limit の ID とパスワードでログインしてご利用ください。）

ID とパスワードは以下の URL またはメールでお問合せください。

メールでの問合わせ宛先　info@znw.co.jp

URL　https://www.znw.co.jp/contact

お問合せ内容/ご依頼内容の欄にニフクラ ID をご記入してください。

サポートサイトへのログイン ID、パスワードをご要望ください。

サポートサイトのパスワードは定期的に変更しております。上記 URL でお申し込みいただきましたお客様に対しては変更前の事前通知を行っております。

右上の「検索はこちらに入力」に検索キーワードを入力することで、掲載内容を検索することができます。

複数のキーワードをスペースで区切って入力しますと AND 条件で検索することができます。

【設定】、【Rule】、【zcli】、【TrafficScript】などタイトルの先頭に区別する文字を設定しています。

こちらの文字列で検索いただくことも可能です。

サポートサイトはニフクラ環境で弊社が提供するソリューションサービスをご利用いただいているお客様向けのサイトです。

正規ライセンスをご利用中でないお客様に対しては内容の開示、掲載ドキュメントの提供は行っておりません。

補足１ コマンド

vTM はコマンド操作でサービスの起動、停止といった操作が可能です。

また zcli というコマンドモードがあり、設定の実施、情報を取得することができます。

■コマンド操作例

vTM サービス　停止	/usr/local/zeus/stop-zeus
vTM サービス　スタート	/usr/local/zeus/start-zeus
vTM サービス　再起動	/usr/local/zeus/restart-zeus
vTM コマンドラインモードへの切替え	/usr/local/zeus/zxtm/bin/zcli
vTM コマンドラインモードの終了	Exit
Admin パスワードのリセット	/usr/local/zeus/zxtm/bin/reset-admin-password
ロールバック	/usr/local/zeus/zxtm/bin/rollback

■zcli（コマンドライン）モード例

上記コマンド操作を参照し、vTM コマンドラインモードへの切替えを実行します。

show info	Uptime や Virtual Server、Pool のオブジェクト、IP アドレスなどが表示します。
show trafficip	Traffic IP Groups の設定が表示します。
show pool	Pool の設定情報が表示します。
show virtualserver	Virtual Server の設定情報が表示します。
stats pool	pool へのデータ量、Queue 時間などが確認できます。
stats virtualserver	virtual server へのリクエスト数、コネクション数などが確認できます。
stats session	session persistence のエントリ数（保持量）を確認できます。

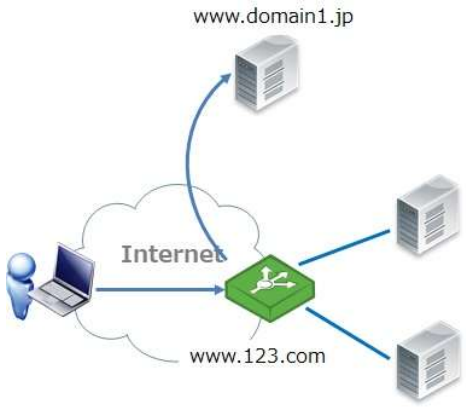
補足 2　Rule 設定サンプル

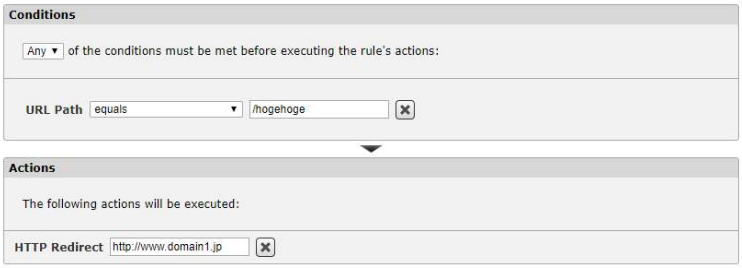
RuleBuilder の設定方法の情報です。

例 1：Redirect

Redirect は　vTM へのアクセスを自動的に他のサイトに転送します。

この例では　http://www.123.com/hogehoge へのアクセスを　http://www.domain1.jp へ転送します

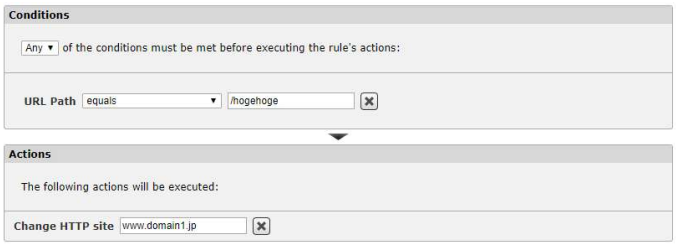




例 2：Change HTTP

Change HTTP の設定では、パスを変えずに、ドメイン部分を変更します。

この設定では　http://www.123.com/hogehoge　にアクセスがあると　http://www.domain1.jp/hogehoge に転送されます。転送先指定にパス部分の　/hogehoge を指定しません。



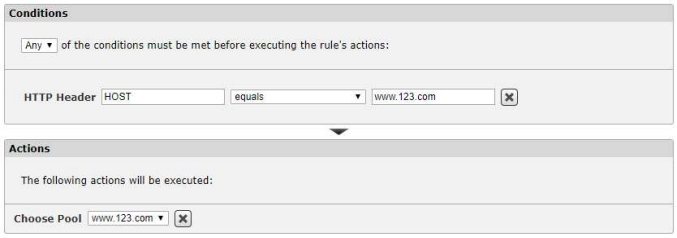
例３：Choose Pool

Choose Pool の設定は動作において、Pool の選択を行います。

Rule 設定において Pool を選択することで Virtual Server に設定された Pool 設定を変更することができます。

この設定は 1 つの IP アドレス、1 つの Virtual Server 設定で複数の FQDN の指定を処理する場合に利用します。

HOST ヘッダーの条件毎にアクセス先ノードを設定した Pool を切り替えることができます。

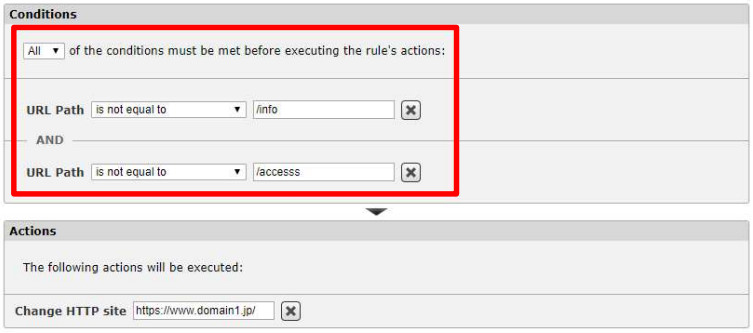


Choose Pool は HOST ヘッダーとの組合せ以外にも利用することができます。

URL Path と組合せた場合、Choose Pool で指定された Pool のバックエンドノード上の URL Path にアクセスします。

例４：URL パスの否定条件

URL Path が　/info、/faq　/access　/support　/registration /products /member と構成され、/info、/access 以外へのアクセス時には HTTPS サイトに切替えします。



Conditions の設定は　Any ではなく、All に設定します。

is not equal to　で/info とイコールでない、/access とイコールでないという 2 つの条件を全て満たす場合にアクションを実行させます。

例 5：URL Path と Raw URL の違い

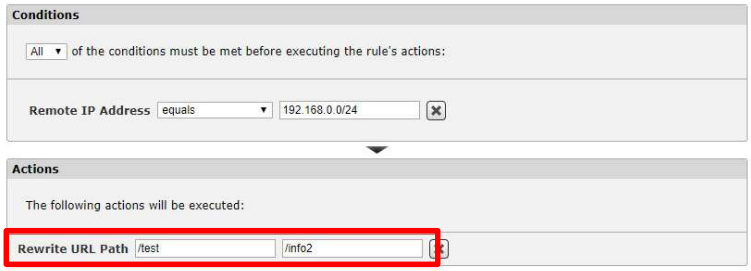
URL Path の設定では　/hogehoge　や　/hogehoge/index.php　と設定します。

Raw URL では　/hogehoge/board.cgi?action=guestbook　と設定します。

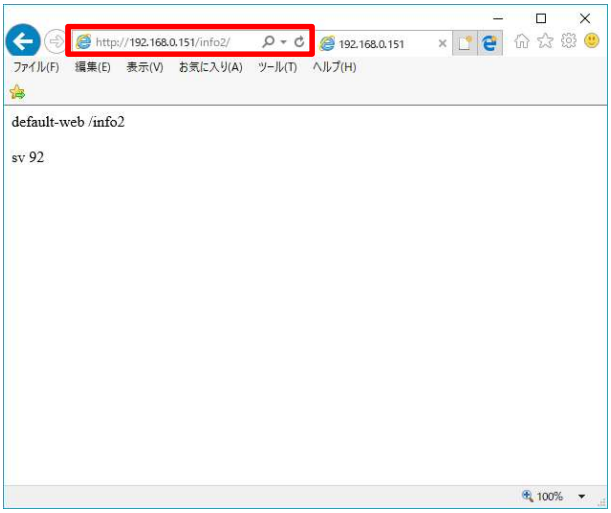
URL 上のパラメータまで設定するには Raw URL を利用します。

例 6：リライト

Rewrite URL Path の設定ではパスの指定の仕方によって表示が変わります。

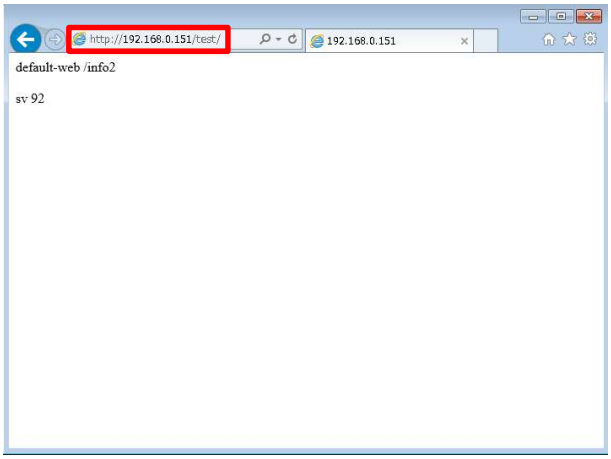


Actions 設定に Rewrite URL Path を設定する際に pattern を　/test　とし、Replacement を　/info2 とした場合



ブラウザからの http://*****/test　にアクセスした場合に、http://*****/info2　に変わります。

Actions 設定に Rewrite URL Path を設定する際に pattern を　/test/　とし、Replacement を　/info2 とした場合



ブラウザからの http://*****/test/　にアクセスした場合に、URL 表記は変わらずに　/info2　の内容が表示します。