EdgeADC

管理ガイド

コンテンツ

ドキュメントのプロパティ

ドキュメント番号：2.0.5.28.21.09.05

ドキュメント作成日2021年4月30日

ドキュメントの最終更新日May 28, 2021

ドキュメント作成者ジェイ・サヴォア

ドキュメント 最後に編集されたのは

ドキュメントの紹介。 エッジADC- バージョン 4.2.7.1890

ドキュメント免責事項

本書に掲載されているスクリーンショットや画像は、お使いの製品のリリースバージョンの違いにより、お使いの製品とは若干異なる場合があります。Edgenexus社は、本書の情報が完全かつ正確であることを保証するために、あらゆる合理的な努力をしています。Edgenexus は、いかなる誤りに対しても責任を負いません。Edgenexusは、必要に応じて将来のリリースでこの文書の情報を変更および修正します。

著作権について

本資料に記載された情報は、予告なしに変更されることがあり、メーカーの確約を示すものではありません。本ガイドのいかなる部分も、メーカーの書面による許可なしに、電子的または機械的（コピーや記録を含む）に、いかなる目的のためにも複製または送信することはできません。登録商標はそれぞれの所有者に帰属します。本ガイドは、可能な限り完全で正確なものにするよう努力していますが、適合性の保証はありません。本ガイドに掲載されている情報を使用したことにより生じた損失や損害について、著者および出版社はいかなる人や組織に対しても責任を負いません。

Edgenexusサポート

本製品に関する技術的なご質問は、support@edgenexus.io までサポートチケットをご提出ください。

EdgeADCの導入について

EdgeADC（今後はADCと表記）製品は、いくつかの方法でインストールすることができます。各プラットフォームのターゲットにはそれぞれのインストーラーが必要ですが、これらはすべてお客様が利用可能です。

このように、様々な設置モデルが用意されています。

- VMware ESXi
- KVM
- Microsoft Hyper-V
- Oracle VM
- ISO for BareMetal ハードウェア

ADCをホストするために使用する仮想マシンのサイズは、ユースケースのシナリオとデータのスループットに依存します。

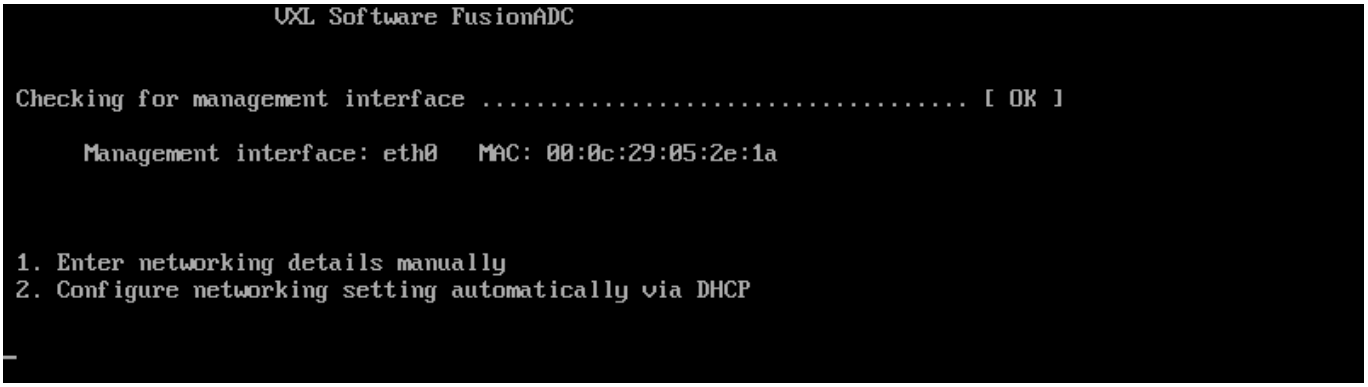
VMware ESXi

ADCは、VMware ESXi are 5.x以上にインストールできます。

- ダウンロードメールに記載されている適切なリンクを使用して、ADCの最新のインストールOVAパッケージをダウンロードします。
- ダウンロードしたら、ESXiホストまたはSAN上の適当なディレクトリに解凍してください。
- vSphere クライアントで、「ファイル：OVA/OVF テンプレートのデプロイ」を選択します。
- ファイルを保存した場所を参照して選択し、OVFファイルを選択して「**NEXT**」をクリックします。
- ESX サーバーがアプライアンス名を要求します。適切な名前を入力し、**NEXT** をクリックします。
- ADCアプライアンスを実行するデータストアを選択します。
- 十分な空き容量のあるデータストアを選択し、**NEXT**をクリックします。
- 製品の情報が表示されますので、「次へ」をクリックします。
- **NEXT**」をクリックします。
- データストアにファイルをコピーしたら、仮想アプライアンスをインストールすることができます。

vSphereクライアントを起動して、新しいADC仮想アプライアンスを確認します。

- VAの上で右クリックし、「電源」→「パワーオン」を選択
- VAが起動し、コンソールにADCの起動画面が表示されます。



初回起動時の設定」を参照してください。

VMXNET3インターフェースのインストール

VMXnet3ドライバーにも対応していますが、まずNICの設定を変更する必要があります。

注：VMware-toolsをアップグレードしないでください。

インポートしたばかりのVA（未起動）でVMXNET3インターフェイスを有効にする

1. VMから両方のNICを削除する
2. VMのハードウェアをアップグレードする--リストのVAを右クリックし、「仮想ハードウェアのアップグレード」を選択する（VMwareツールのインストールやアップデートを開始せず、ハードウェアのアップグレード**のみを**実行する）。
3. 2つのNICを追加し、それらをVMXNET3に選択します。
4. 標準的な方法でVAを起動します。VMXNET3で動作します。

既に稼働しているVAでVMXNET3インターフェイスを有効にする

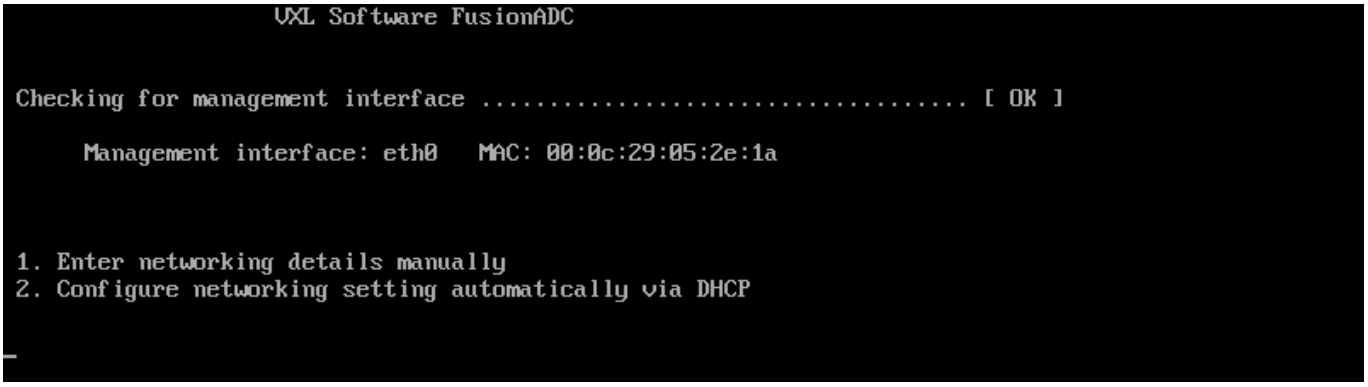
1. VMの停止（CLIのシャットダウンコマンドまたはGUIのパワーオフ
2. 両方のNICのMACアドレスを取得してください（リストのNICの順番を覚えておいてください！）。
3. VMから両方のNICを削除する
4. VMのハードウェアのアップグレード（VMware toolsのインストールやアップデートは行わず、ハードウェアのアップグレード**のみを行う**
5. 2つのNICを追加し、それらをVMXNET3に選択する
6. ステップ2にしたがって、新しいNICのMACアドレスを設定する
7. VAの再起動

本番用プラットフォームとしては、VMware ESXiをサポートしています。 評価用には、VMware WorkstationとPlayerをご利用いただけます。

Microsoft Hyper-V

ADCの仮想アプライアンスは、Microsoft Hyper-Vサーバへのインストールに対応しています。

- Hyper-V ADC VAのzipファイルをローカルマシンまたはサーバーに解凍します。
- Hyper-V Managerを開きます。
- Hyper-V Managerで、サーバーを右クリックして、**"Import Virtual Machine "**を選択します。
- ADCのHyper-Vファイルがあるフォルダを参照します。
- **"仮想マシンのコピー（新しい固有IDの作成）"**をクリックします。
- **"Duplicate all files so the same virtual machine can be again"** のチェックボックスにチェックを入れます。
- **"Import "**をクリック
- マシンは**"ADC ADC VA for Hyper-V "**という名前でインポートされます。
- NICで正しいネットワークを選択しているか
- 複数の仮想アプライアンスをインストールする場合は、各アプライアンスに固有のMACアドレスを設定する必要があります。
- 先ほど作成した仮想マシンを右クリックし、**"接続 "**をクリックします。
- 緑色のスタートボタンをクリックするか、**"ActionStart "**をクリックします。
- VAが起動し、ADCのコンソール画面が表示されます。



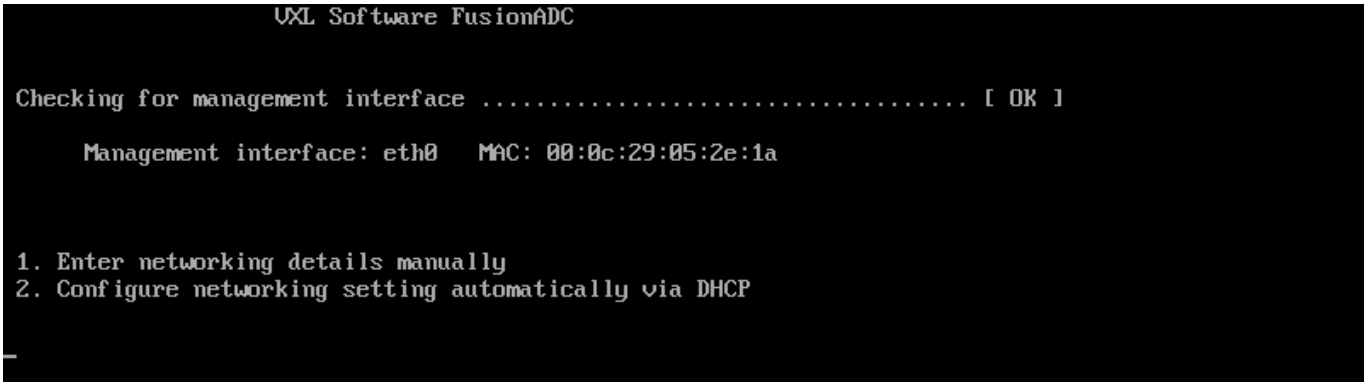
- ネットワークのプロパティを設定すると、VAは再起動し、VAコンソールへのログオンを提示します。

初回起動時の設定」を参照してください。

Citrix XenServer

ADCバーチャルアプライアンスは、Citrix XenServerにインストールできます。

- ADC OVA ALB-VAファイルをローカルマシンまたはサーバーに展開します。
- Citrix XenCenter Clientを開きます。
- XenCenterクライアントで、**"ファイル：インポート "**を選択します。
- **OVA**ファイルをブラウズして選択し、**"Open Next "**をクリックします。
- VMの作成場所を聞かれたら、選択します。
- インストールするXenServerを選択し、**"NEXT "**をクリックします。
- 仮想ディスクを配置するストレージリポジトリ（SR）を聞かれたら選択する。
- 十分なスペースのあるSRを選択し、**"NEXT "**をクリックします。
- 仮想ネットワークインターフェースをマッピングします。両方のインターフェイスにはEth0と表示されますが、一番下のインターフェイスはEth1であることに注意してください。
- 各インターフェースのターゲットネットワークを選択し、「**NEXT**」をクリックします。
- "Use Operating System Fixup "にチェックを入れないでください。
- **"NEXT "**をクリックします。
- 一時的に転送するVMに使用するネットワークインターフェースを選択します。
- 管理インターフェース（通常はネットワーク0）を選択し、ネットワーク設定はDHCPのままにしておきます。転送用のDHCPサーバーがない場合は、静的なIPアドレスを割り当てる必要があることに注意してください。これを行わないと、インポート時に「接続中」と表示され、その後「失敗」となります。**NEXT "**をクリックしてください。
- すべての情報を確認し、正しい設定を確認します。**"FINISH "**をクリックします。
- VMは仮想ディスク "ADC ADC "の転送を開始し、完了するとXenServerの下に表示されます。
- XenCenterクライアント内に、新しい仮想マシンが表示されます。VAを右クリックして、**"START "**をクリックします。
- すると、VMが起動して、ADCの起動画面が表示されます。



- 設定が完了すると、VAへのログオンが提示されます。

初回起動時の設定」を参照してください。

初回起動時の設定

初回起動時には、ADC VAは以下の画面を表示し、本番運用のための設定を要求します。

最初の起動 - 手動ネットワークの詳細

初回起動時に、DHCPによるIP詳細の自動割り当てを10秒で中断することができる

この処理を中断するには、コンソールウィンドウをクリックして、いずれかのキーを押します。その後、以下の詳細を手動で入力することができます。

- IPアドレス
- サブネットマスク
- ゲートウェイ
- DNSサーバー

これらの変更は永続的なもので、再起動後も存続し、VAで再度設定する必要はありません。

最初の起動 - DHCPが成功しました。

ネットワーク割り当てプロセスを中断しない場合、ADCはタイムアウト後にDHCPサーバーに連絡してネットワークの詳細を取得します。連絡が成功した場合、マシンには以下の情報が割り当てられます。

- IPアドレス
- サブネットマスク
- デフォルトゲートウェイ
- DNSサーバー

ADCのVAは、DHCPサーバー内のVAのMACアドレスにIPアドレスが恒久的にリンクしていない限り、DHCPアドレスを使用して操作しないことをお勧めします。VAを使用する際は、固定**IPアドレス**を使用することをお勧めします。ネットワークの設定が完了するまで、**「管理用IPアドレスの変更」**以降の手順に従ってください。

最初の起動 - DHCPが機能しない

DHCPサーバーがない場合や、接続に失敗した場合は、IPアドレス192.168.100.100が割り当てられます。このIP
アドレスは、VAが空きIPアドレスを見つけるまで「1」ずつ増加し
ます。同様に、VAはそのIPアドレスが現在使用されているかどうかを確認し、使用されている場合は、再度増加して再確認します。

管理用IPアドレスの変更

VAのIPアドレスは、以下のように**set greenside=n.n.n.n**というコマンドでいつでも変更することができます。

```
Command:set greenside=192.168.101.1_
```

eth0のサブネットマスクの変更

ネットワークインターフェースには「eth」という接頭語が使われており、ベースとなるネットワークアドレスは「eth0」と呼ばれています。サブネットマスク（ネットマスク）は、**set mask eth0 n.n.n.n.n** というコマンドで変更できます。

```
Command:set mask eth0 255.255.255.0_
```

デフォルトゲートウェイの設定

VAの運用には、デフォルトゲートウェイが必要です。デフォルトゲートウェイを設定するには、以下の例に示すように、**route add default gw n.n.n.n** というコマンドを使用します。

```
Command:route add default gw 192.168.101.254_
```

デフォルトゲートウェイ値の確認

デフォルトゲートウェイが追加され、正しく設定されているかどうかを確認するには、**route**というコマンドを使います。このコマンドを実行すると、ネットワークルートとデフォルトゲートウェイの値が表示されます。以下の例をご覧ください。

```
Command:route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
255.255.255.255 *               255.255.255.255 UH    0      0        0 eth0
192.168.101.0   *               255.255.255.0   U     0      0        0 eth0
default         192.168.101.254 0.0.0.0         UG    0      0        0 eth0
```

グラフィカル・ユーザー・インターフェース（GUI）にアクセスして、生産用または評価用のADCを設定できるようになりました。

ウェブインターフェースへのアクセス

Javascriptを搭載したインターネットブラウザーを使用して、ADCを設定、監視、運用に移すことができます。

ブラウザのURLフィールドに、**「HTTPS://{IP ADDRESS}」または「HTTPS://{FQDN}」**のいずれかを入力します。

ADCは、デフォルトでは、自己署名入りのSSL証明書を使用します。お客様が選択したSSL証明書を使用するように、ADCを変更することができます。

ブラウザがADCに到達すると、ログイン画面が表示されます。ADCの工場出荷時の認証情報は以下の通りです。

デフォルトのユーザー名 = **admin** / デフォルトのパスワード = **jetnexus**

コマンドリファレンス表

コマンド	パラメータ1	パラメータ2	説明	例
デート			現在設定されている日付と時刻を表示	Tue Sept 3 13:00 UTC 2013
デフォルト			工場出荷時の設定をアプライアンスに割り当てる	
出口			コマンドラインインターフェースからのログアウト	
ヘルプ			すべての有効なコマンドを表示	
ifconfig	[空白]		すべてのインターフェイスの設定を見る	ifconfig
	eth0		eth0のみのインターフェース設定を見る	ifconfig eth0
マシンID			このコマンドは、ADC ADCをライセンスするために使用されるマシンIDを提供します。	EF4-3A35-F79
辞める			コマンドラインインターフェースからのログアウト	
リブート			すべての接続を終了し、ADCを再起動する。	リブート
リスタート			ADC ADC仮想サービスの再起動	
ルート	[空白]		ルーティングテーブルの表示	ルート
	追加	デフォルトGW	デフォルトゲートウェイIPアドレスの追加	route add default gw 192.168.100.254
セット	グリーンサイド		ADCの管理用IPアドレスの設定	set greenside=192.168.101.1
	マスク		インターフェイスのサブネットマスクを設定します。インターフェイス名はeth0、eth1....	set mask eth0 255.255.255.0
ショー			グローバルコンフィギュレーション設定を表示	
シャットダウン			すべての接続を終了し、ADCの電源を切る ADC	
ステータス			現在のデータの統計情報を表示	
トップ			CPUやMemoryなどのプロセス情報の表示	

ビューログ	メッセージ	生のsyslogメッセージを表示する	ログメッセージの表示

注意：コマンドは大文字と小文字を区別しません。コマンドの履歴はありません。

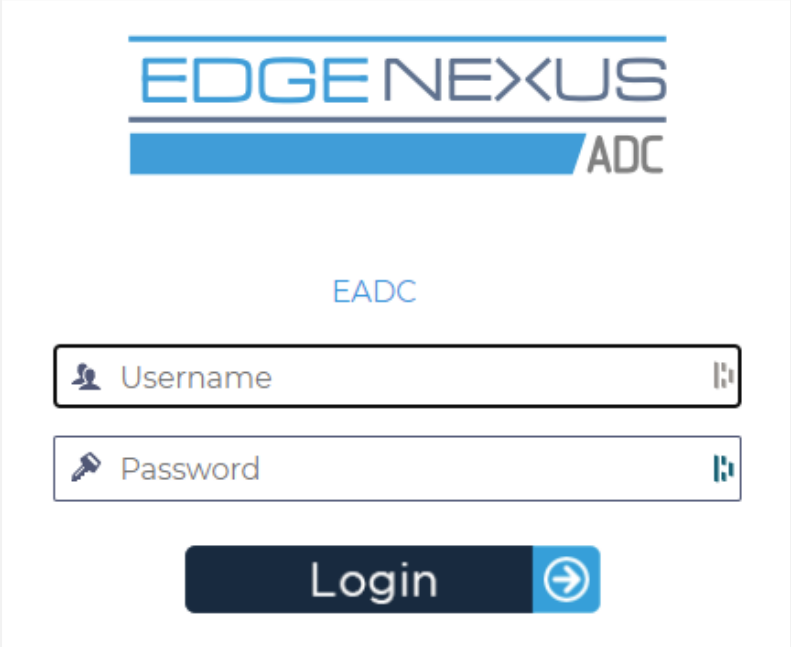
ADCウェブコンソールの起動

ADC（ADCともいう）に関するすべての操作は、ウェブコンソールを使って設定・実行します。Webコンソールは、Javascriptを搭載したブラウザを使ってアクセスします。

ADCのWebコンソールを起動するには、URL欄にADCのURLまたはIPアドレスを入力します。ここでは、adc.company.comを例に説明します。

https://adc.company.com

起動すると、ADCのWebコンソールは以下のようになり、adminユーザーでログインできるようになります。



デフォルトのログイン認証

デフォルトのログイン認証情報は

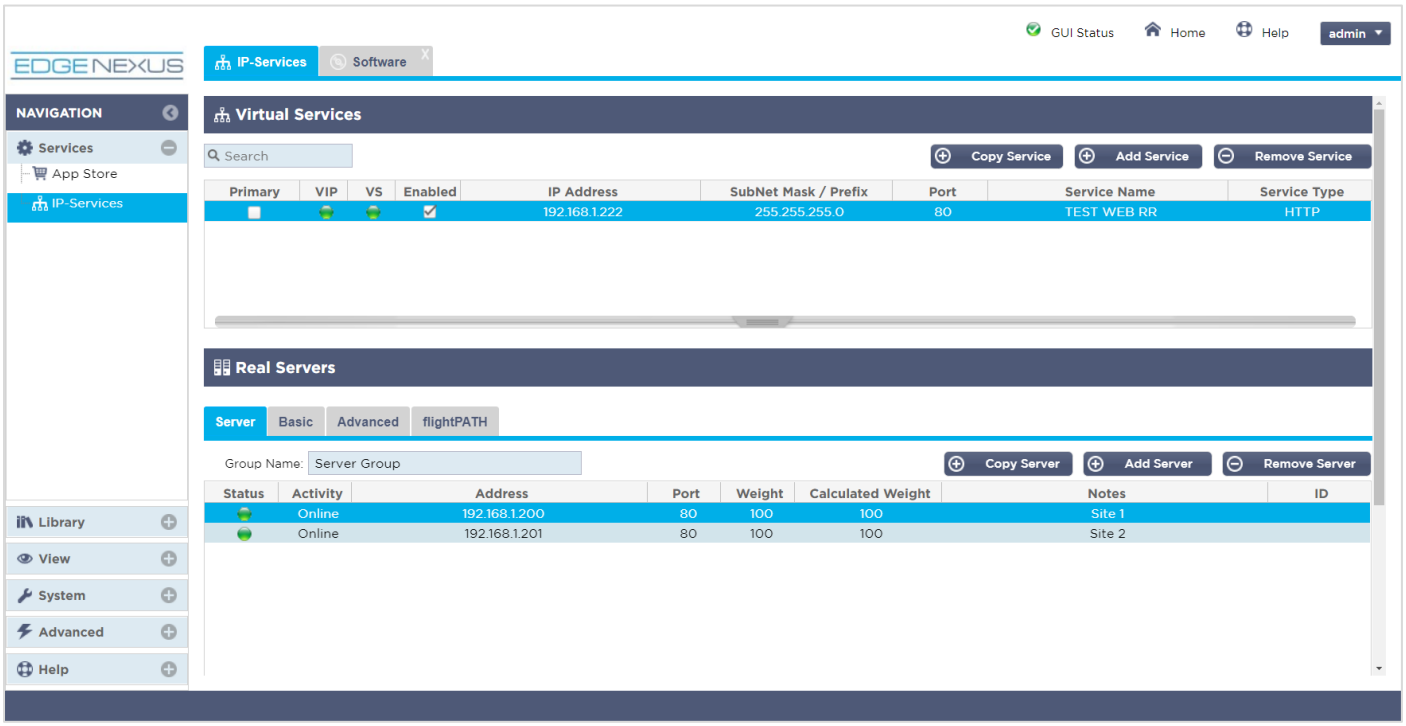
- ユーザーネーム: admin
- パスワード：ジェットネクサス

これは、「*System*」→「*Users*」にあるユーザー設定機能を使って、いつでも変更することができます。

ログインに成功すると、ADCのメインダッシュボードが表示されます。

メインダッシュボード

以下の画像は、ADCのメインダッシュボードまたは「ホームページ」の外観を示しています。改良のために一部変更することがありますが、すべての機能はそのままです。



ここでは、最初に画面の各部を紹介することで、ADCの設定領域の各部を十分に理解していただけるものと考え、できるだけ簡潔に説明するため、詳細な説明はせず、設定要素に焦点を当てて説明します。

左から右に向かって、まず「ナビゲーション」があります。ナビゲーション」は、ADC内のさまざまなエリアで構成されています。ナビゲーションの中の選択肢をクリックすると、対応するセクションが画面の右側に表示されます。また、画面上部の製品ロゴの隣には、選択した設定セクションのタブが表示されています。このタブは、ADCの構成であらかじめ使用されている領域への迅速なナビゲーションを可能にします。

サービス

ADCのサービスセクションには、いくつかの領域があります。サービス」項目をクリックすると、利用可能な選択肢が表示されます。

IPサービス

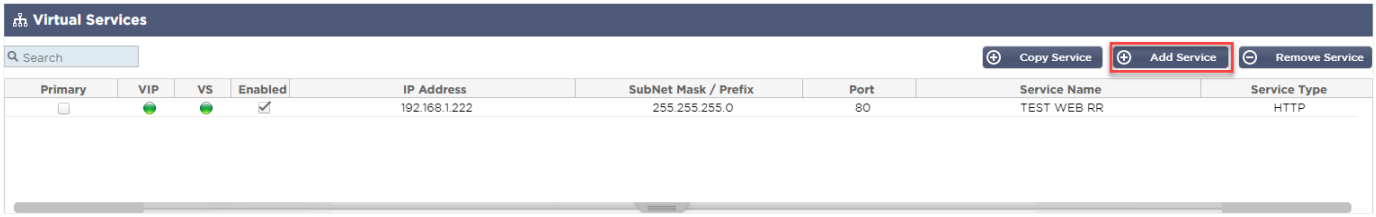
ADCのIPサービスセクションでは、特定のユースケースに必要な様々なバーチャルIPサービスを追加、削除、設定することができます。設定やオプションは以下のセクションに分かれています。これらのセクションは、アプリケーション画面の右側にあります。

バーチャルサービス

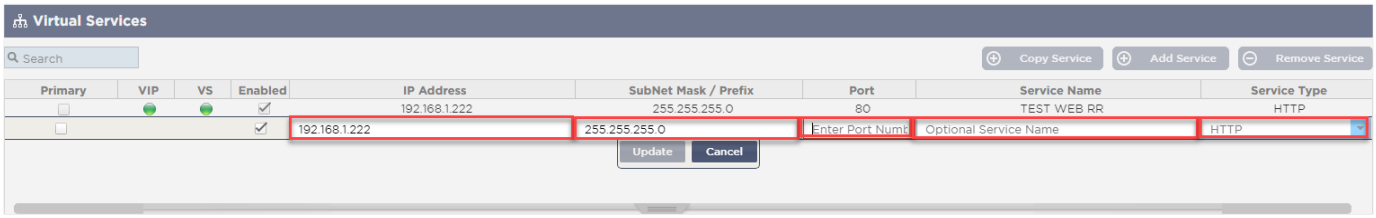
バーチャルサービスは、バーチャルIP（VIP）と、ADCがリッスンするTCP/UDPポートを組み合わせたものです。バーチャルサービスのIPに到着したトラフィックは、そのサービスに関連するリアルサーバーの1つにリダイレクトされます。バーチャルサービスのIPアドレスは、ADCの管理アドレスと同じにすることはできません（例：eth0、eth1など）。

ADCは、「Basic」タブの「Real Servers」セクションで設定されたロードバランシングポリシーに基づいて、トラフィックをサーバーにどのように再分配するかを決定します。

新しいVIPを使った新しいバーチャルサービスの作成



- 上記の「Add Virtual Service」ボタンをクリックします。

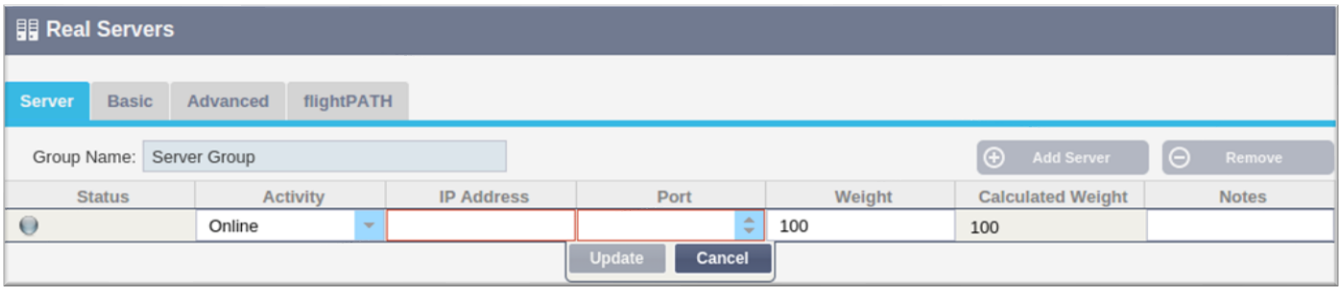


- その後、エディットローモードに入ります。
- ハイライトされた4つのフィールドに必要事項を入力し、更新ボタンをクリックして進みます。

TABキーでフィールドを移動してください。

フィールド	説明
IPアドレス	リアルサーバーにアクセスするためのターゲットエントリーポイントとなる、新しい仮想IPアドレスを入力します。このIPは、ユーザーやアプリケーションが負荷分散されたアプリケーションにアクセスするためのポイントとなります。
サブネットマスク/プレフィックス	このフィールドには、ADCが置かれているネットワークに関連するサブネットマスクを入力します。
ポート	VIPにアクセスする際に使用するエントリーポートです。リバースプロキシを使用している場合、この値は必ずしもリアルサーバーと同じである必要はありません。
サービス名	サービス名は、VIPの目的をテキストで表現したものです。省略可能ですが、わかりやすくするために記入することをお勧めします。
サービスタイプ	サービスタイプには様々なものがあり、お客様が選択することができます。レイヤ4のサービスタイプでは、flightPATH技術は使用できません。

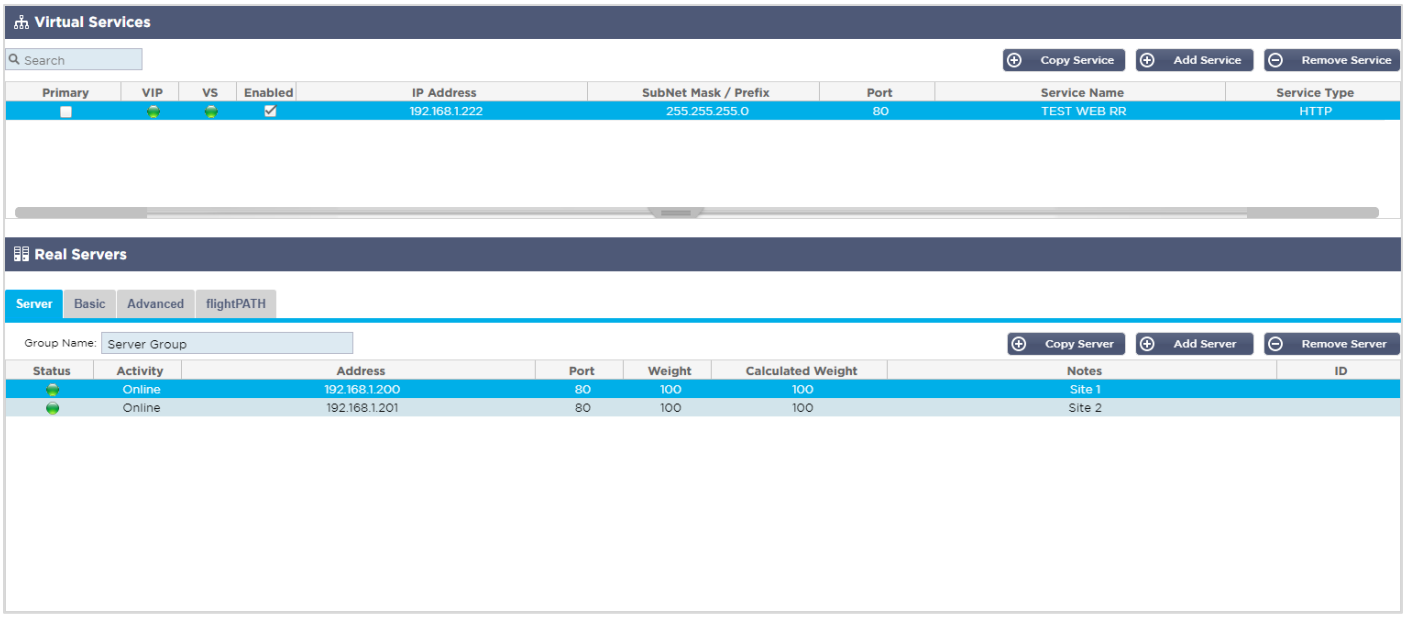
Update」ボタンを押すと、このセクションが保存され、以下の「Real Server」セクションに自動的にジャンプします。



フィールド	説明
アクティビティ	アクティビティ」フィールドでは、負荷分散されたリアルサーバーの状態を表示・変更することができます。 オンライン - サーバーがアクティブで、ロードバランスされたリクエストを受信していることを示す オフライン - サーバーはオフラインで、リクエストを受信していません。 ドレイン - サーバーがドレインモードになり、ユーザーに影響を与えずにパーシステンスをフラッシュし、サーバーをオフライン状態に移行させることができます。 Standby - サーバーがスタンバイ状態になっている。
IPアドレス	この値は、リアルサーバーのIPアドレスです。この値は正確でなければならず、DHCPアドレスであってはなりません。
ポート	リアルサーバーにアクセスする際のターゲットポート。リバースプロキシを使用している場合は、VIPで指定されているエントリーポートとは異なる場合があります。
ウェイトリング	この設定は通常、ADCによって自動的に設定されます。優先順位の重み付けを変更したい場合は、これを変更することができます。

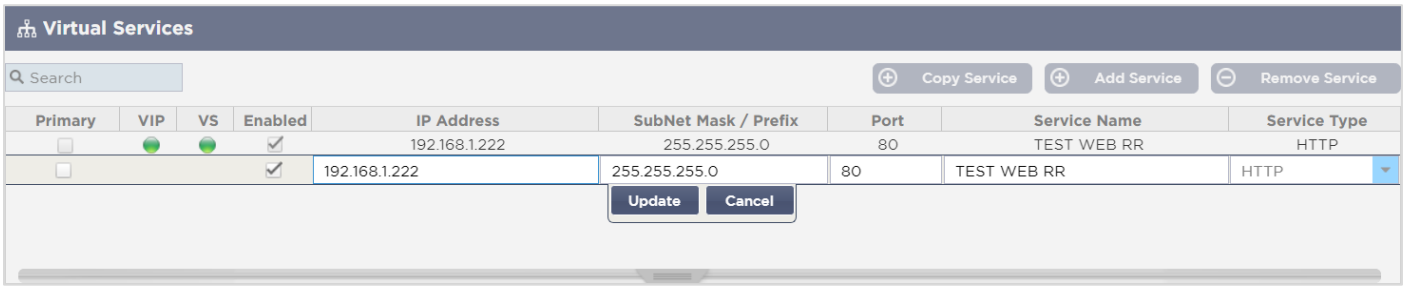
- 更新ボタンをクリックするか、Enterキーを押して変更を保存する
- サーバーヘルスチェックが成功すると、ステータスライトは最初にグレーになり、次にグリーンになります。Real Server Monitorが失敗すると赤になります。
- ステータスランプが赤のサーバーは負荷分散されません。

バーチャルサービスの完成例

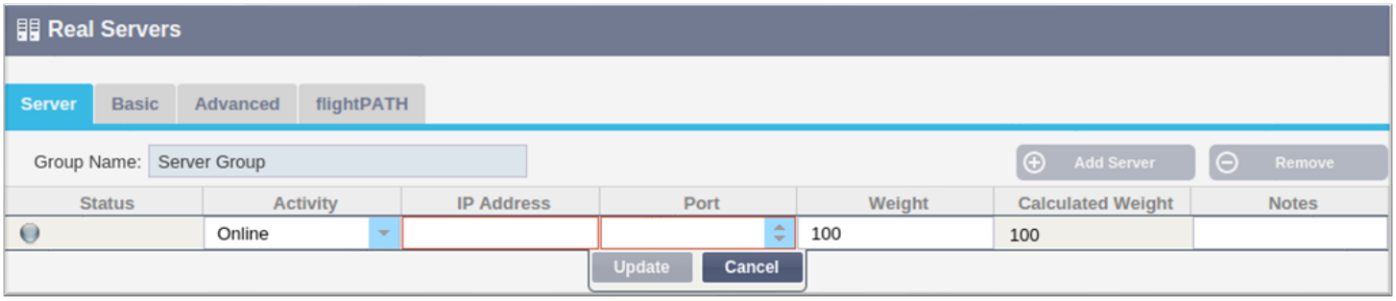


既存のVIPを利用した新しいバーチャルサービスの作成

- コピーしたいバーチャルサービスをハイライト表示する
- バーチャルサービスの追加」をクリックすると、行の編集モードになります。



- IPアドレスとサブネットマスクは自動的にコピーされます。
- ご利用のサービスのポート番号を入力してください。
- サービス名を入力してください。
- サービスタイプの選択
- Update」ボタンを押すと、このセクションが保存され、以下の「Real Server」セクションに自動的にジャンプします。

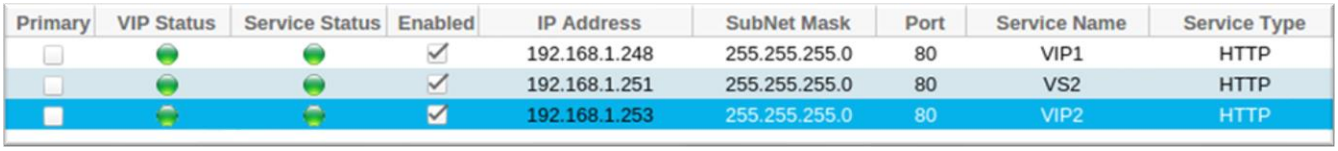


- これは、デフォルトのヘルスモニターであるTCP Connectに合格した場合にロードバランスされることを意味します。この設定は、必要に応じて後で変更できます。
- リアルサーバーのIPアドレスを入力
- リアルサーバーのポート番号を入力してください。
- リアルサーバーの名前を任意で入力
- 更新」をクリックして変更内容を保存する
- サーバーヘルスチェックが成功すると、ステータスライトはまずグレーになり、次にグリーンになります。リアルサーバモニタが失敗すると赤になります。
- ステータスが「赤」のサーバーは負荷分散されません。

バーチャルサービスのIPアドレス変更

既存のバーチャルサービスやVIPのIPアドレスは、いつでも変更することができます。

- IPアドレスを変更したいバーチャルサービスを強調表示します。



- そのサービスのIPアドレス欄をダブルクリック

- IPアドレスを使用したいものに変更する
- 更新ボタンをクリックすると、変更内容が保存されます。

注：バーチャルサービスのIPアドレスを変更すると、そのVIPに関連するすべてのサービスのIPアドレスが変更されます

コピーサービスを利用した新規バーチャルサービスの作成

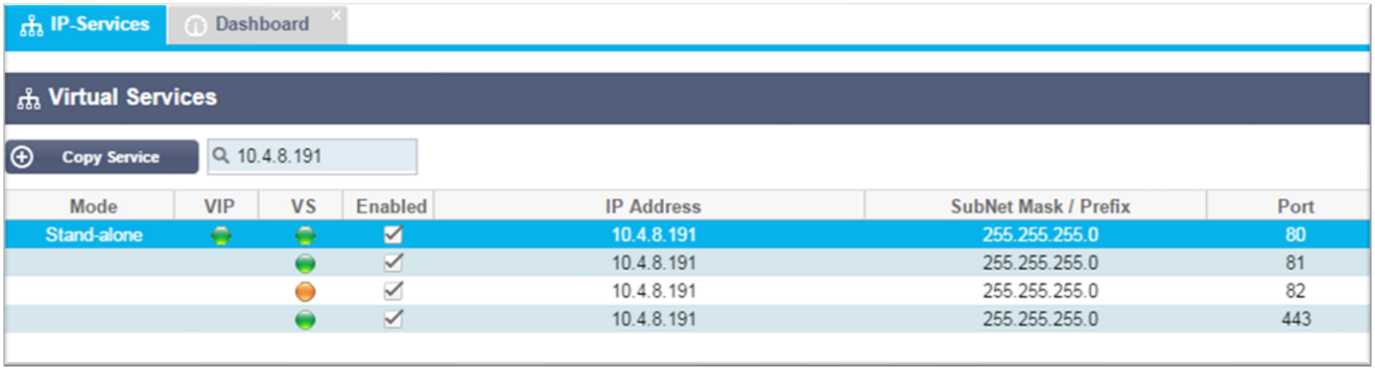
- サービスのコピー」ボタンをクリックすると、サービス全体がコピーされます。このサービスには、関連するすべてのリアルサーバー、基本設定、詳細設定、およびflightPATHルールが含まれます。
- 複製したいサービスを選択し、「サービスのコピー」をクリックします。
- 行エディタが表示され、IPアドレスの列に点滅カーソルが表示されます。
- 固有のIPアドレスに変更するか、IPアドレスを維持する場合は、そのIPアドレスに固有のPortを編集する必要があります。

ロードバランシングポリシーやReal Serverモニターなどの設定を変更したり、flightPATHルールを削除したりした場合は、各タブの編集を忘れないようにしてください。

表示データのフィルタリング

特定の用語を検索する

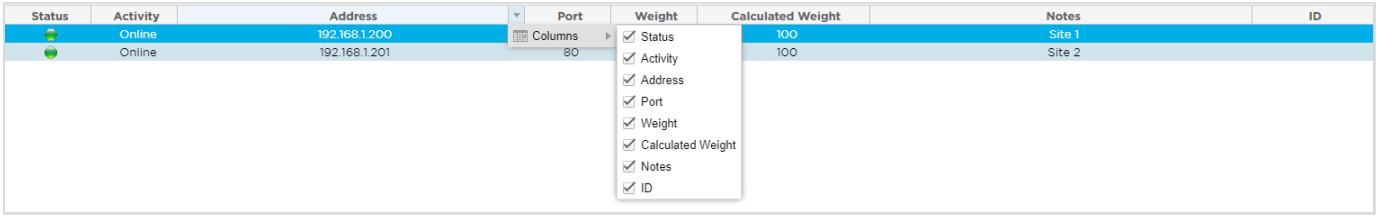
検索ボックスでは、IPアドレスやサービス名のオクテット数など、任意の値を使ってテーブルを検索することができます。



上の例では、10.4.8.191という特定のIPアドレスを検索した結果を示しています。

カラムの可視性を選択する

また、ダッシュボードに表示したい列を選択することもできます。

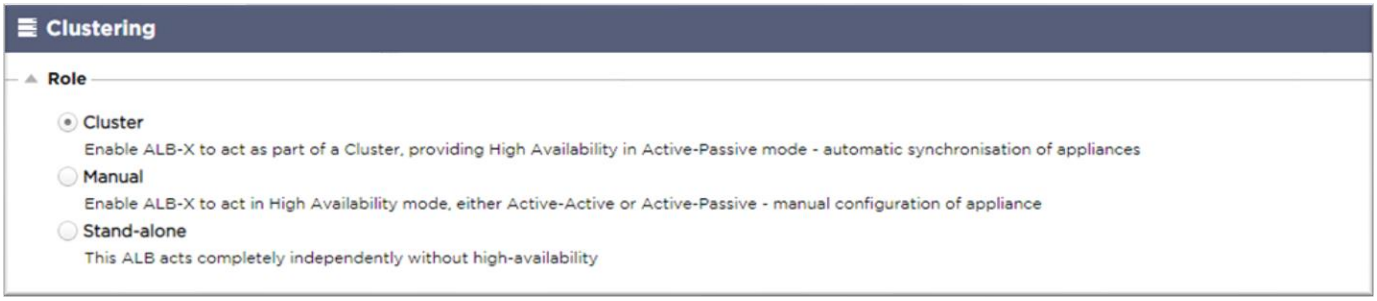


- いずれかの列にマウスを合わせる
- コラムの右端に小さな矢印が表示されます。
- チェックボックスをクリックすると、ダッシュボードに表示させたい列が選択されます。

バーチャルサービスカラムについて

プライマリ/モード

Primary/Mode列は、現在のVIPに選択されている高可用性の役割を示します。このオプションを設定するには、［System］→［Clustering］で利用できるオプションを使用します。



オプション	説明
クラスター	クラスタは、インストール時のADCのデフォルトの役割であり、プライマリ/モードの列は、現在実行されているモードを示します。データセンターにADCアプライアンスのHAペアがある場合、片方がActive、もう片方がPassiveと表示されます。
マニュアル	Manual」ロールは、ADCペアが異なる仮想IPアドレスに対してActive-Activeモードで動作することを可能にします。このような場合、「プライマリ」列には、各固有の仮想IPの横にボックスがあり、「アクティブ」の場合はチェックを入れ、「パッシブ」の場合はチェックを入れないようになっています。
スタンドアローン	ADCはスタンドアロンのデバイスとして動作しており、高可用性モードではありません。そのため、「Primary」欄には「Stand-alone」と表示されます。

VIP

この欄には、各バーチャルサービスのステータスが視覚的に表示されます。指標は色分けされており、以下のようになっています。

LED	意味
●	オンライン
●	フェイルオーバー・スタンバイ。この仮想サービスは、ホットスタンドバイ
●	セカンダリー」が「プライマリー」のために控えていることを示す。

●	サービスに注意が必要です。この表示は、リアルサーバーがヘルスモニターのチェックに失敗した場合や、手動でオフラインに変更された場合に起こります。トラフィックは継続して流れますが、リアルサーバーの容量は減少します。
●	オフラインです。コンテンツサーバに到達できない、またはコンテンツサーバが有効になっていない
●	発見状況
●	ライセンスされていない、またはライセンスされた仮想IPを超える

有効

このオプションのデフォルトは "Enabled "で、チェックボックスにはチェックが入っています。バーチャルサービスを無効にするには、その行をダブルクリックしてチェックボックスのチェックを外し、［更新］ボタンをクリックします。

IPアドレス

IPv4アドレスを10進数のドット表記で、またはIPv6アドレスを追加します。この値は、お客様のサービスの仮想IPアドレス（VIP）となります。例 IPv4「192.168.1.100」。例 Ipv6 "2001:0db8:85a3:0000:0000:8a2e:0370:7334"

サブネットマスク/プレフィックス

サブネットマスクを10進数のドット記法で追加します。例：「255.255.255.0」。また、IPv6の場合は、プレフィックスを追加します。IPv6の詳細については、**HTTPS://EN.WIKIPEDIA.ORG/WIKI/IPV6_ADDRESS**をご覧ください。

ポート

サービスに関連するポート番号を追加します。ポートには、TCPまたはUDPのポート番号を使用できます。例：WebトラフィックにはTCP "80"、Secured WebトラフィックにはTCP "443"。

サービス名

サービスを識別するためのフレンドリーな名前を追加します。例："Production Web Servers."

サービスタイプ

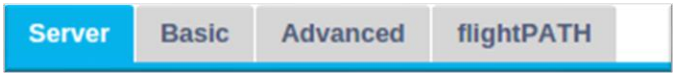
すべての「レイヤー4」サービスタイプでは、ADCはデータストリームの相互作用や変更を行わないため、レイヤー4サービスタイプではflightPATHは利用できないことに注意してください。レイヤ4サービスは、ロードバランシング・ポリシーに従ってトラフィックをロードバランシングするだけです。

サービスタイプ	ポート/プロトコル	サービス層	コメント
レイヤ4 TCP	任意のTCPポート	レイヤー4	ADCは、データストリーム内のいかなる情報も変更せず、ロードバランシングポリシーに基づいてトラフィックの標準的なロードバランシングを行います。
レイヤ4 UDP	任意のUDPポート	レイヤー4	レイヤ4のTCPと同様に、ADCはデータストリーム内のいかなる情報も変更せず、ロードバランシングポリシ

			ーに基づいてトラフィックの標準的なロードバランシングを行います。
レイヤ4 TCP/UDP	任意のTCPまたはUDPポート	レイヤー4	サービスにUDPなどのプライマリプロトコルがあるが、TCPにフォールバックする場合に最適です。ADCは、データストリームの情報を一切変更せず、ロードバランシングポリシーに基づいてトラフィックの標準的なロードバランシングを行います。
HTTP	HTTPまたはHTTPSプロトコル	レイヤー7	ADCは、flightPATHを使ってデータストリームを操作したり、変更したりすることができます。
FTP	ファイル転送プロトコルプロトコル	レイヤー7	クライアントとサーバー間で制御とデータの接続を別々に行う
SMTP	Simple Mail Transfer Protocol	レイヤー4	メールサーバーのロードバランシングに使用
POP3	郵便局のプロトコル	レイヤー4	メールサーバーのロードバランシングに使用
IMAP	インターネットメッセージアクセスプロトコル	レイヤー4	メールサーバーのロードバランシングに使用
RDP	リモートデスクトッププロトコル	レイヤー4	ターミナルサービスサーバーのロードバランシングに使用
RPC	リモートプロシージャコール	レイヤー4	RPCコールを使用してシステムをロードバランシングする場合に使用します。
RPC/ADS	Exchange 2010 アドレスブックサービスの静的RPC	レイヤー4	Exchangeサーバーのロードバランシングに使用
RPC/CA/PF	クライアントアクセスとパブリックフォルダのための Exchange 2010 Static RPC	レイヤー4	Exchangeサーバーのロードバランシングに使用
DICOM	医療におけるデジタルイメージングとコミュニケーション	レイヤー4	DICOMプロトコルを使用するサーバーのロードバランシングに使用

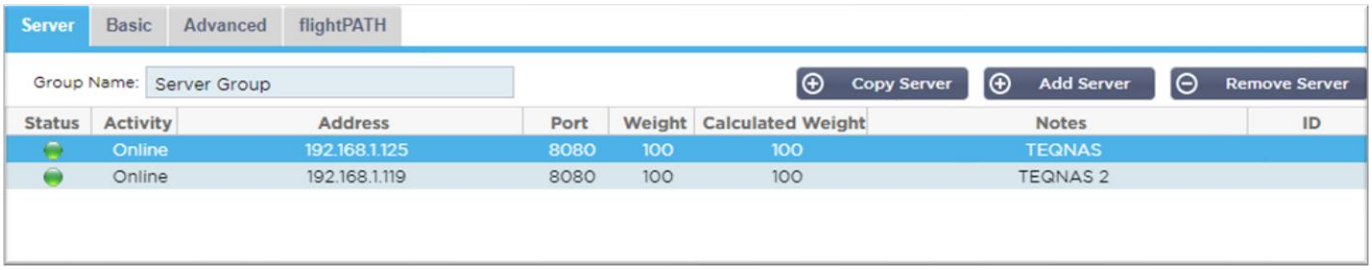
リアルサーバー

ダッシュボードの「Real Servers」セクションにはいくつかのタブがあります。Server」、「Basic」、「Advanced」、「flightPATH」です。



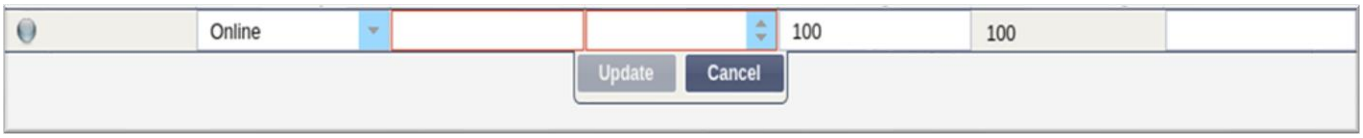
サーバー

サーバー」タブには、現在選択されているバーチャルサービスに対 応するリアルバックエンドサーバーの定義が表示されます。リアルサーバー」セクションには、少なくとも1台のサーバーを追加する必要があります。



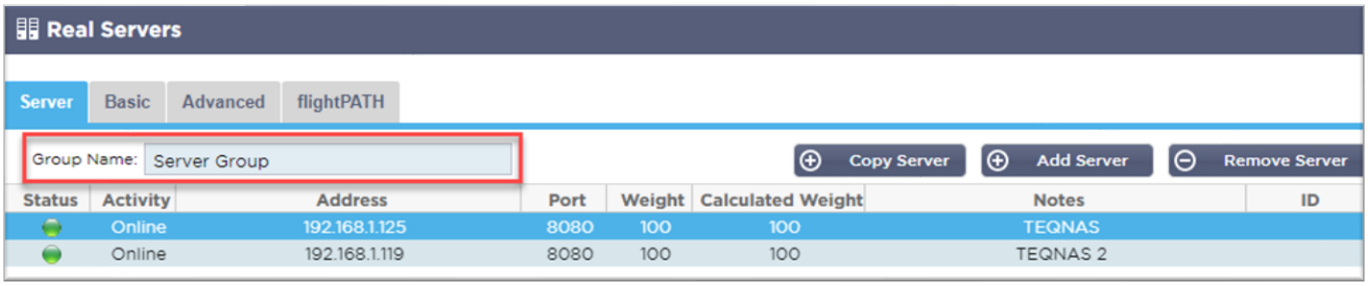
サーバーの追加

- あらかじめ定義しておいた適切なVIPを選択します。
- サーバーの追加」をクリックします。
- 新しい行が表示され、IPアドレスの列にカーソルが点滅します。



- サーバーのIPv4アドレスをドット10進法で入力します。リアルサーバーは、仮想サービスと同じネットワーク上にあっても、直接接続されたローカルネットワーク上にあっても、ADCがルーティングできるネットワーク上にあってもかまいません。例「10.1.1.1」。
- ポート」の欄にタブを移動し、サーバーのTCP/UDPポート番号を入力します。このポート番号は、バーチャルサービスのポート番号と同じでも、リバースプロキシ接続用の別のポート番号でも構いません。ADCは自動的にこの番号に変換します。
- ノートセクションにタブを移動して、サーバーに関連する詳細情報を追加します。例"IISウェブサーバー1"

グループ名



負荷分散セットを構成するサーバーを追加した際に、グループ名を付けることができます。この項目を編集すると、更新ボタンを押さなくても内容が保存されます。

リアルサーバーのステータスライト

リアルサーバーの状態は、「ステータス」欄のランプの色で確認できます。以下をご覧ください。

LED	意味

●	コネクテッド
◎	モニタリングなし
●	排水
●	オフライン
●	スタンバイ
●	接続されていない
●	発見状況
●	ライセンスされていない、またはライセンスされたリアルサーバーを超えた

アクティビティ

リアルサーバーのアクティビティは、ドロップダウンメニューを使っていつでも変更することができます。これを行うには、リアルサーバーの行をダブルクリックして編集モードにします。

オプション	説明
オンライン	オンラインに割り当てられたすべてのリアルサーバーは、「基本」タブ内で設定されたロードバランシングポリシーに従ってトラフィックを受け取ります。
ドレイン	ドレインに設定されたすべてのリアルサーバーは、既存の接続には対応しますが、新規の接続は受け付けません。ドレインが処理されている間、ステータスライトは緑/青に点滅します。既存の接続が自然終了すると、リアルサーバーはオフラインになり、ステータスランプは青一色になります。これらの接続を確認するには、「ナビゲーション」→「モニター」→「ステータス」の順に選択します。
オフライン	オフライン」に設定されたすべてのリアルサーバーは、直ちにオフラインになり、いかなるトラフィックも受け取れなくなります。
スタンバイ	スタンバイに設定されたすべてのリアルサーバーは、オンライングループの**すべての**サーバーがサーバーヘルスモニターのチェックに失敗するまでオフラインのままです。このとき、トラフィックはロードバランシングポリシーに従ってスタンバイグループで受信されます。Onlineグループの1台のサーバーがServer Health Monitorのチェックに合格した場合、この

	Onlineサーバーがすべてのトラフィックを受信し、Standbyグループはトラフィックの受信を停止します。

IPアドレス
このフィールドには、リアルサーバーのIPアドレスを入力します。例「192.168.1.200」。

ポート

リアルサーバーがサービスを受けているTCPまたはUDPのポート番号。例：Webトラフィックの場合は「80」。

重量

この欄は、適切なロードバランシングポリシーが指定されている場合に編集可能になります。

リアルサーバー のデフォルトのウェイトは100ですが、1～100の値を入力することができます。値が100の場合は最大負荷、1の場合は最小負荷を意味します。

3台のサーバーの例は、以下のようになります。

- Server 1 Weight = 100
- Server 2 Weight = 50
- Server 3 Weight = 50

ロードバランシングポリシーが「Least Connections」に設定されていて、クライアントの総接続数が200であるとします。

- サーバー1は100の同時接続を得る
- サーバー2の同時接続数は50
- サーバー3の同時接続数は50

負荷分散の方法としてラウンドロビンを使用した場合、負荷分散されたサーバーセットでリクエストを回転させますが、重みを変更すると、ターゲットとして選ばれるサーバーの頻度に影響します。

最速のロードバランシングポリシーがレスポンスをGETするのにかかった時間の短さを利用していると考えられる場合、ウェイトを調整することで、Least Connectionsと同様にバイアスを変更することができます。

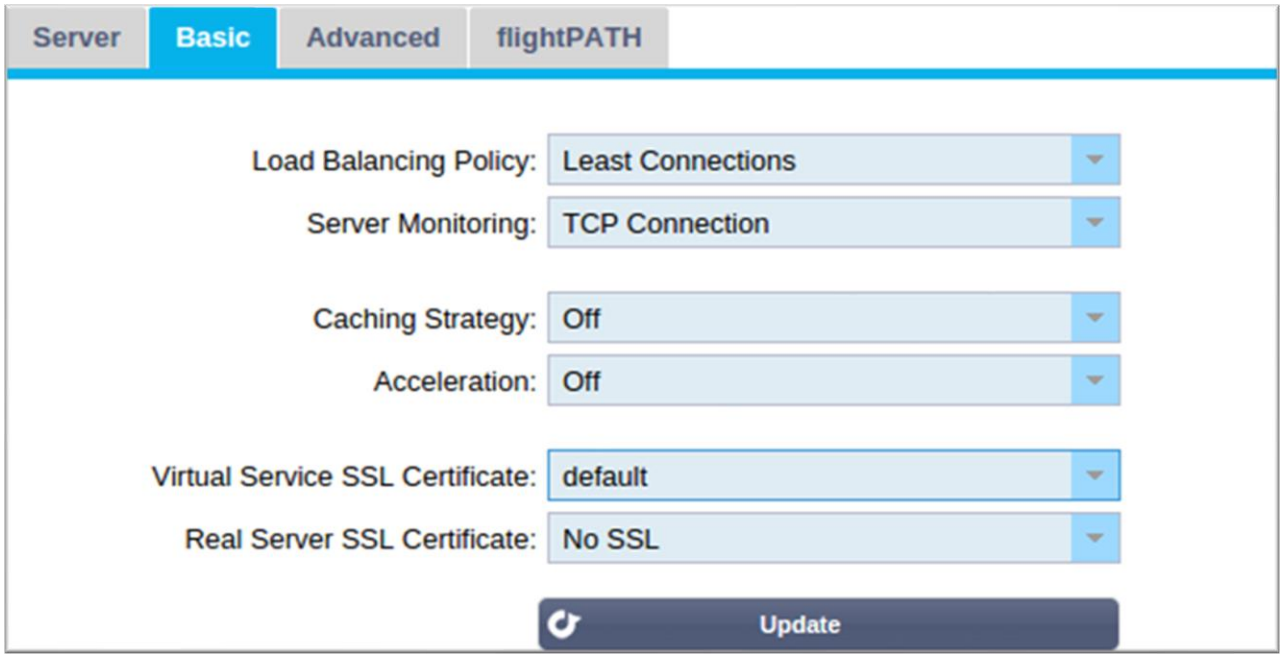
計算された重量

各サーバーの「計算された重み」は、動的に表示することができ、自動的に計算され、編集はできません。このフィールドには、手動での重み付けやロードバランシングポリシーを考慮した場合に、ADCが使用する実際の重み付けが表示されます。

備考

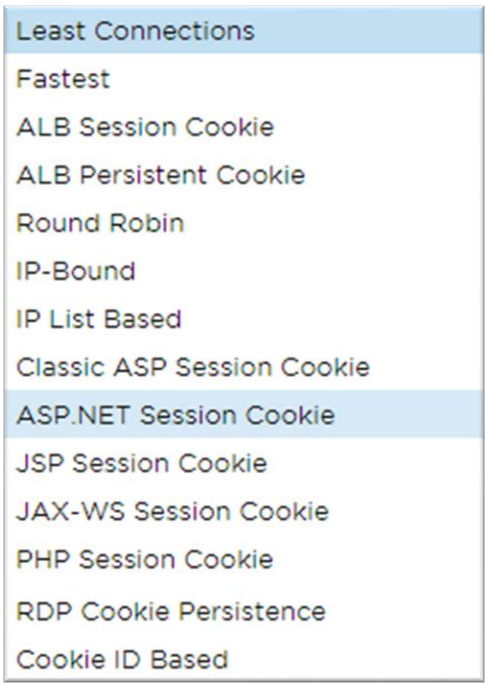
定義されたエントリーを説明するのに役立つ特定のメモを「Notes」フィールドに入力します。例：「IIS Server1 - London DC」。

ベーシック



ロードバランシングポリシー

このドロップダウンリストには、現在サポートされているロードバランシングポリシーが表示されます。ロードバランシングポリシーの一覧とその説明は以下のとおりです。



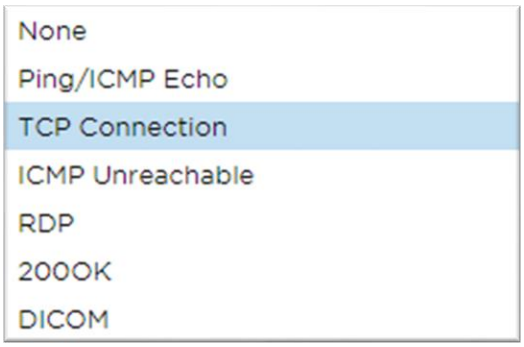
オプション	説明
最速	最速」のロードバランシングポリシーでは、サーバーごとのすべてのリクエストに対する応答時間を時間軸で平滑化して自動的に計算します。計算された重み」欄には、自動的に計算された値が表示されます。手動入力は、このロードバランシングポリシーを使用する場合のみ可能です。

ラウンドロビン	ラウンドロビンは、ファイアウォールや基本的なロードバランサーでよく使われる方法で、最もシンプルな方法です。各リアルサーバーは、新しいリクエストを順番に受け取ります。この方法は、ウェブサーバの検索など、サーバへのリクエストを均等に負荷分散する必要がある場合にのみ適しています。しかし、アプリケーションの負荷やサーバーの負荷に基づいて負荷分散を行う必要がある場合や、セッションで同じサーバーを使用することを保証する必要がある場合には、ラウンドロビン方式は不適切です。
Least Connections	ロードバランサーは、各リアルサーバーへの現在の接続数を記録します。接続数が最も少ないReal Serverが、後続の新しいリクエストを受け取ります。
レイヤー3 セッションアフィニティ/パーシステンス - IPバウンド	このモードでは、クライアントのIPアドレスをもとに、どのリアルサーバーがリクエストを受信するかを選択します。この動作により、持続性が得られます。このモードでは、HTTPとレイヤ4のプロトコルが使用できます。この方法は、ネットワークのトポロジーがわかっていて、上流に「スーパープロキシ」が存在しないことを確信できる内部ネットワークで有効です。レイヤ4やプロキシを使用すると、すべてのリクエストが1つのクライアントから来ているように見えるため、負荷が均一になりません。HTTPでは、プロキシに対応するために、ヘッダ（X-Forwarder-For）情報が存在する場合に使用されます。
レイヤー3 セッションアフィニティ/パーシスタンス - IPリストベース	リアルサーバーへの接続は「最小接続」で開始され、クライアントのIPアドレスに基づいてセッションの親和性が得られます。リストはデフォルトでは2時間保持されますが、jetPACKで変更することができます。
レイヤ7 セッションアフィニティ/パーシスタンス - ALB セッションクッキー	このモードは、HTTP ロードバランシングの最も一般的なパーシステンス方式です。このモードでは、ADCは最初のリクエストごとにIPリストベースのロードバランシングを行います。ADCは最初のHTTPレスポンスのヘッダーにクッキーを挿入します。その後、ADCはクライアントのクッキーを使用して、トラフィックを同じバックエンドサーバーにルーティングします。このクッキーは、クライアントが毎回同じバックエンドサーバーにアクセスする必要がある場合に、永続性のために使用されます。このクッキーは、セッションが終了すると失効します。
レイヤ7 セッションアフィニティ/パーシステンス - ALB パーシステントクッキー	IPリストベースのロードバランシングモードは、最初のリクエストごとに使用されます。ADCは、最初のHTTPレスポンスのヘッダーにクッキーを挿入します。その後、ADCはクライアントのクッキーを使用して、トラフィックを同じバックエンドサーバーにルーティングします。このクッキーは、クライアントが毎回同じバックエンドサーバーに行かなければならない場合に、永続性のために使用されます。クッキーは2時間後に期限切れとなり、接続はIPリストベースのアルゴリズムに従ってロードバランスされます。この有効期限は、jetPACKを使用して設定できます。
セッションクッキー - Classic ASP Session Cookie	Active Server Pages（ASP）は、Microsoft社のサーバーサイド技術です。このオプションを選択すると、ASPクッキーが検出され、既知のクッキーリストに見つかった場合、ADCは同じサーバーへのセッションの永続性を維持します。新しいASPクッキーが検出されると、Least Connectionsアルゴリズムを使用してロードバランスされます。
セッションクッキー - ASP.NETセッションクッキー	このモードは、**ASP.net**に適用されます。このモードを選択すると、ASP.NETのクッキーが検出され、既知のクッキーのリストに見つかった場合、ADCは同じサーバーへのセッションの永続性を維持します。新しい

	ASPクッキーが検出されると、Least Connectionsアルゴリズムを使用して負荷分散されます。
セッションクッキー - JSP セッションクッキー	Java Server Pages (JSP)は、オラクルのサーバーサイド技術です。このモードを選択すると、ADCは、JSPクッキーが検出され、既知のクッキーリストに見つかった場合、同じサーバーへのセッションの永続性を維持します。新しいJSPクッキーが検出されると、Least Connectionsアルゴリズムを使用してロードバランスされます。
セッションクッキー - JAX-WS セッションクッキー	Java Webサービス（JAX-WS）は、オラクルのサーバーサイド技術です。このモードを選択すると、ADCは、JAX-WSクッキーが検出され、既知のクッキーのリストに見つかった場合、同じサーバーへのセッションの永続性を維持します。新しいJAX-WSクッキーが検出されると、Least Connectionsアルゴリズムを使用してロードバランスされます。
セッションクッキー - PHP セッションクッキー	Personal Home Page（PHP）は、オープンソースのサーバーサイド技術です。このモードを選択すると、PHPクッキーが検出された場合、ADCは同じサーバーにセッションの永続性を維持します。
セッションCookie - RDP Cookie Persistence	このロードバランシング方式は、マイクロソフトが作成したユーザー名/ドメイン名に基づくRDPクッキーを使用して、サーバーへの永続性を提供します。この方法の利点は、クライアントのIPアドレスが変更されても、サーバーへの接続を維持できることです。
Cookie-IDベース	PhpCookieBased "や他の負荷分散方法とよく似た新しい方法ですが、CookieIDBasedとcookie RegEx h=[^;]+を使用しています。 この方法では、リアルサーバーのメモ欄に設定されている「ID=X;」という値を、サーバーを識別するためのクッキーの値として使用します。このため、CookieListBasedと同様の手法ですが、異なるCookie名を使用し、スクランブルされたIPではなく、Real ServerからのIDというユニークなCookie値を保存することになります（ロード時に読み込まれます）。 デフォルト値は CookieIDName="h "ですが、バーチャルサーバーの詳細設定でオーバーライド値が設定されている場合は、これを使用してください。**注**：この値が設定されている場合は、上記のクッキー式を上書きして、h=を新しい値に置き換えます。 最後に、未知のクッキー値が到着し、リアルサーバーID のいずれかにマッチした場合は、そのサーバーを選択し、そうでない場合は、次のメソッド（デリゲート）を使用するという ことです。

サーバー監視

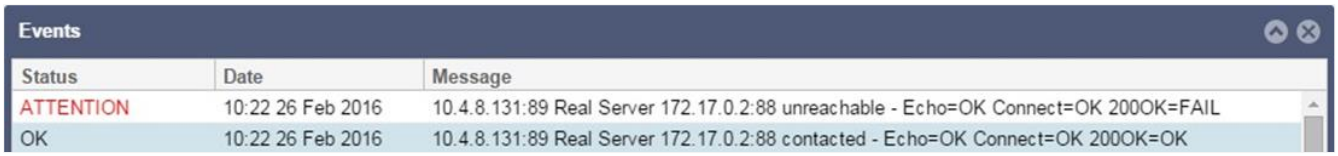
お客様のADCには、以下の6つの標準的なリアルサーバー監視方法があります。



バーチャルサービス（VIP）に適用する監視方法を選択します。

サービスに適したモニターを選択することが不可欠です。例えば、リアルサーバーがRDPサーバーの場合、200OKモニターは関係ありません。どのモニターを選べばよいかわからない場合は、デフォルトのTCPコネクションから始めるのがよいでしょう。

サービスに適用したいモニターを順番にクリックすることで、複数のモニターを選択することができます。選択したモニターは、選択した順に実行されるので、下位層のモニターから順に設定してください。例えば、Ping/ICMP Echo、TCP Connection、200OKのモニターを設定すると、ダッシュボードのイベントに以下の画像のように表示されます。



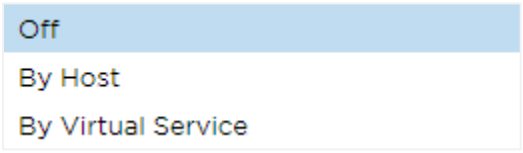
一番上の行を見ると、レイヤー3のPingとレイヤー4のTCP Connectは成功していますが、レイヤー7の200OKは失敗していることがわかります。これらの監視結果は、ルーティングは問題なく、関連するポートでサービスが実行されていることを示すのに十分な情報を提供していますが、ウェブサイトは要求されたページに対して正しく応答していません。ここで、ウェブサーバと「ライブラリ」→「リアルサーバモニタ」セクションを見て、失敗しているモニタの詳細を確認しましょう。

オプション	説明
なし	このモードでは、リアルサーバーは監視されず、常に正常に稼働しています。なし」の設定は、監視によってサーバーが動揺する状況や、ADCのフェイルオーバー動作に加わるべきではないサービスに有効です。これは、H/Aオペレーションにとって主要ではない、信頼性のないシステムやレガシーシステムをホストするためのルートです。この監視方法は、任意のサービスタイプで使用します。
ピン/ICMPエコー	このモードでは、ADCはコンテンツサーバーのIPにICMPエコーリクエストを送信します。有効なエコー応答を受信すると、ADCはリアルサーバーが稼働しているとみなし、サーバーへのトラフィックのスループットが継続されます。また、H/Aペアでのサービス利用も継続されます。この監視方法は、どのようなサービスタイプでも使用できます。
TCP接続	このモードでは、リアルサーバーへのTCP接続が行われ、データを送信せずに直ちに切断されます。接続が成功した場合、ADCはリアルサーバが稼働していると判断します。この監視方法は、どのようなサービスタイプでも使用できます。現在、TCPコネクションの監視に適していないのはUDPサービスだけです。
ICMP Unreachable	ADCはサーバーにUDPヘルスチェックを送信し、ICMPポート到達不能メッセージを受信すると、Real Serverを利用できないとマークします。この方法は、DNS

	ポート53など、サーバーでUDPサービスポートが利用可能かどうかを確認する必要がある場合に役立ちます。
RDP	このモードでは、ICMP Unreachableの方法で説明したように、TCPコネクションが初期化されます。接続が初期化された後、レイヤ7のRDP接続が要求される。接続が確認されると、ADCはリアルサーバーが稼働していると判断します。この監視方法は、どのようなマイクロソフト社製のターミナルサーバーでも使用できます。
200 OK	この方法では、リアルサーバーとのTCP接続が初期化される。接続が成功すると、ADCはReal ServerにHTTPリクエストを送信します。HTTP応答を待ち、"200 OK "応答コードを確認します。200 OK」応答コードを受信した場合、ADCは実在のサーバーが稼働していると判断する。タイムアウトや接続失敗など、何らかの理由で「200 OK」応答コードを受信しなかった場合、ADCはリアルサーバーを利用できないと判断します。この監視方法は、HTTP および Accelerated HTTP サービスタイプでの使用にのみ有効です。HTTP サーバにレイヤ 4 サービスタイプが使用されている場合、Real Server で SSL が使用されていないか、または「コンテンツ SSL」機能で適切に処理されていれば、使用可能です。
DICOM	DICOMモードでリアルサーバへのTCP接続が初期化され、接続時にEchoscuの「Associate Request」がリアルサーバに行われる。コンテンツサーバからの「Associate Accept」、少量のデータの転送、「Release Request」、「Release Response」の順で会話が行われ、モニターが正常に終了する。何らかの理由でモニターが正常に終了しなかった場合、リアルサーバーはダウンしているとみなされる。
ユーザー定義	Real Server Monitoringセクションで設定されたモニターはすべてリストに表示されます。

キャッシング戦略

デフォルトでは、Caching Strategyは無効で、Offに設定されています。サービスタイプがHTTPの場合、2種類のCaching Strategyを適用することができます。



キャッシュの詳細な設定については、「キャッシュの設定」のページを参照してください。なお、Accelerated "HTTP "サービスタイプのVIPにキャッシュを適用した場合、圧縮されたオブジェクトはキャッシュされません。

オプション	説明
ホストによる	ホストごとのキャッシングは、ホスト名ごとのアプリケーションに基づいて行われます。ドメイン/ホスト名ごとに個別のキャッシュが存在します。このモードは、ドメインに応じて複数のWebサイトを提供できるWebサーバーに最適です。
バーチャルサービスによる	このオプションを選択すると、バーチャルサービスごとのキャッシングが可能になります。バーチャルサービスを経由するすべてのドメイン/ホスト名に対して、1つのキャッシュのみが存在します。このオプションは、1つのサイトの複数のクローンで使用するための専門的な設定です。

加速

オプション	説明
オフ	バーチャルサービスの圧縮をオフにする
圧縮	このオプションを選択すると、選択した仮想サービスの圧縮をオンにします。ADCは、要求に応じてクライアントへのデータストリームを動的に圧縮します。この処理は、content-encoding: gzip ヘッダーを含むオブジェクトにのみ適用されます。コンテンツの例としては、HTML、CSS、または Javascript があります。Global Exclusions」セクションを使用して、特定のコンテンツタイプを除外することもできます。

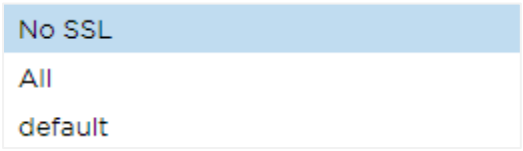
注：オブジェクトがキャッシュ可能な場合、ADCは圧縮されたバージョンを保存し、コンテンツの有効期限が切れて再検証されるまで、これを静的に（メモリから）提供します。

仮想サービスSSL証明書（クライアントとADC間の暗号化

デフォルトでは「No SSL」に設定されています。サービスタイプが「HTTP」または「Layer4 TCP」の場合は、ドロップダウンから証明書を選択してバーチャルサービスに適用できます。作成またはインポートされた証明書は、このリストに表示されます。1 つのサービスに適用する複数の証明書を強調表示することができます。この操作により、SNI拡張機能が自動的に有効になり、クライアントが要求した「ドメイン名」に基づく証明書が許可されます。

サーバー名の表示

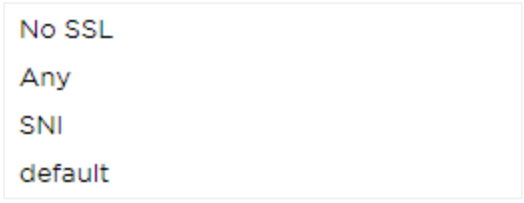
このオプションは、TLSネットワークプロトコルの拡張機能で、ハンドシェイクプロセスの開始時に、クライアントが接続しようとしているホスト名を示します。この設定により、ADCは同じ仮想IPアドレスとTCPポートに複数の証明書を提示することができます。



オプション	説明
SSLなし	ソースからADCへのトラフィックは暗号化されません。
デフォルト	このオプションは、ローカルで作成された「Default」という名前の証明書を、チャネルのブラウザ側に適用する結果となります。SSLが作成またはインポートされていない場合に、このオプションを使用してSSLをテストします。
ユーザーインポートのSSL証明書	ADCにインポートした証明書はすべてここに表示されます。

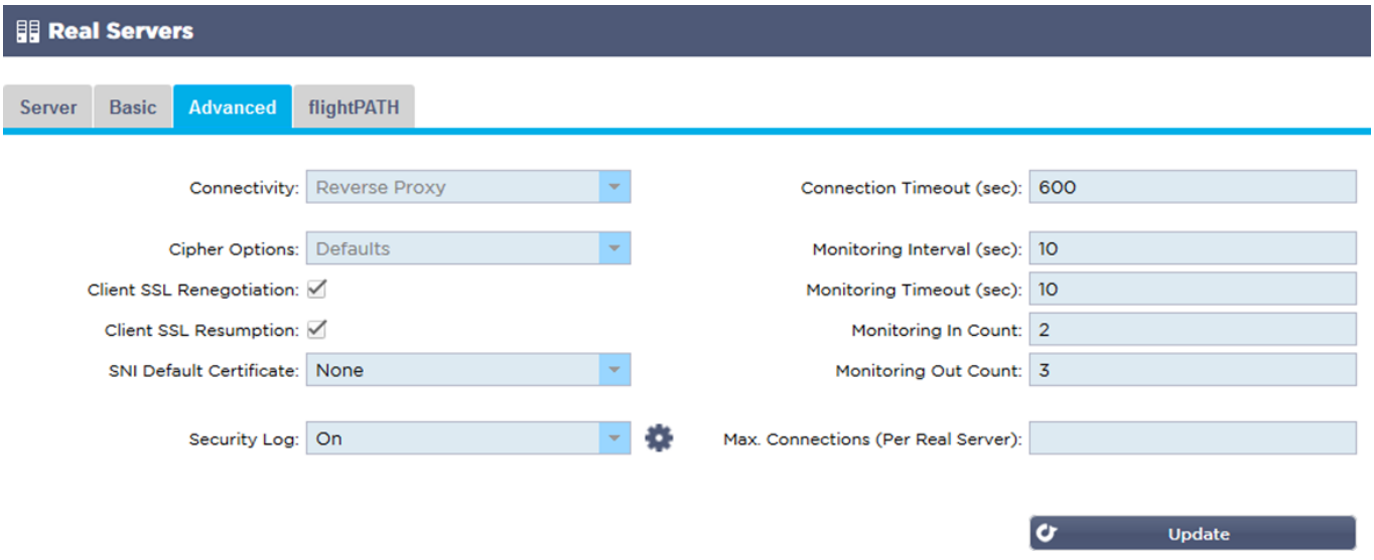
リアルサーバーのSSL証明書（ADCとリアルサーバー間の暗号化

このオプションのデフォルト設定は「No SSL」です。サーバーで暗号化された接続が必要な場合は、この値を［SSLなし］以外の値にする必要があります。作成またはインポートされた証明書は、このリストに表示されます。



オプション	説明
SSLなし	ADCからリアルサーバーへのトラフィックは暗号化されません。ブラウザ側で証明書を選択するということは、"SSLなし "をクライアント側で選択して、"SSLオフロード "と呼ばれる機能を提供することができます。
任意の	ADCはクライアントとして動作し、Real Serverが提示するあらゆる証明書を受け入れます。このオプションを選択すると、ADC からリアルサーバーへのトラフィックが暗号化されます。仮想サービス側で証明書が指定されている場合は、「Any」オプションを使用して、「SSLブリッジング」または「SSL再暗号化」と呼ばれる機能を提供します。
SNI	ADCはクライアントとして動作し、Real Serverが提示するあらゆる証明書を受け入れます。このオプションを選択すると、ADC からリアルサーバーへのトラフィックが暗号化されます。仮想サービス側で証明書が指定されている場合は、「Any」オプションを使用して、「SSLブリッジング」または「SSL再暗号化」として知られているものを提供します。サーバー側のSNIを有効にするには、このオプションを選択します。
ユーザーインポートのSSL証明書	ADCにインポートした証明書はすべてここに表示されます。

アドバンスド



接続性

バーチャルサービスには、4種類の接続方法が設定されています。サービスに適用する接続モードを選択してください。

オプション	説明

リバースプロキシ	リバースプロキシはデフォルト値で、レイヤ7では圧縮とキャッシングで動作します。また、レイヤ4ではキャッシングや圧縮を行いません。このモードでは、ADCがリバースプロキシとして動作し、リアルサーバが見るソースアドレスとなります。
ダイレクトサーバーリターン	Direct Server Return（DSR）は広く知られているが（一部の業界ではDR - Direct Routing）、ロードバランサーの後ろにあるサーバーが、応答時にADCをバイパスしてクライアントに直接応答することができる。DSRは、レイヤー4のロードバランサーでの使用にのみ適しています。したがって、このオプションを選択した場合、キャッシングと圧縮は利用できません。 このDSRでは、レイヤ7のロードバランシングは機能しません。また、IPリストベース以外のパーシステンスサポートはありません。ソースIPパーシステンスのサポートが唯一のタイプであるため、この方法でのSSL/TLSロードバランシングは理想的ではありません。また、DSRでは、Real Serverの変更が必要です。詳しくは「リアルサーバーの変更」をご覧ください。
ゲートウェイ	ゲートウェイモードでは、すべてのトラフィックをADCを介してルーティングすることができ、リアルサーバーからのトラフィックをADCの仮想マシンやハードウェアインターフェースを介して他のネットワークにルーティングすることができます。リアルサーバーのゲートウェイデバイスとして使用することは、マルチインターフェースモードで運用する場合に最適です。 この方法では、IPリストベース以外のパーシステンスがサポートされていないため、レイヤー7のロードバランシングは機能しません。この方法では、リアルサーバーのデフォルトゲートウェイをADCのローカルインターフェースアドレス（eth0、eth1など）に設定する必要があります。詳しくは「リアルサーバーの変更点」をご覧ください。

暗号オプション

暗号はサービスごとに設定でき、SSL/TLSが有効なサービスにのみ関係します。ADCは暗号の自動選択を行いますが、jetPACKSを使って異なる暗号を追加することができます。適切なjetPACKを追加すると、サービスごとにCipherオプションを設定できます。これにより、さまざまなレベルのセキュリティを備えた複数のサービスを作成することができます。古いクライアントは新しい暗号に対応していないので、安全なサービスほどクライアントの数を減らすことに注意してください。

クライアントのSSLリネゴシエーション

クライアント主導のSSL再交渉を許可する場合は、このボックスをチェックします。このオプションをオフにすると、SSLレイヤーに対するDDOS攻撃を防ぐために、クライアントのSSL再ネゴシエーションを無効にします。

クライアントのSSL再開

セッションキャッシュに追加されたSSL再開サーバーセッションを有効にする場合は、このボックスにチェックを入れます。クライアントがセッションの再利用を提案すると、サーバーはそのセッションが見つかった場合に再利用を試みます。Resumptionがチェックされていない場合、クライアントまたはサーバーのセッションキャッシュは行われません。

SNIデフォルト証明書

クライアント側のSNIを有効にしたSSL接続中に、要求されたドメインがサービスに割り当てられた証明書のどれとも一致しない場合、ADCはSNIのデフォルト証明書を提示します。このデフォルト設定は「なし」

で、完全に一致しない場合は事実上、接続を切断します。SSL証明書が完全に一致しなかった場合に提示するために、ドロップダウンからインストールされた証明書を選択します。

セキュリティログ

On」がデフォルト値で、サービスごとに、認証情報をW3Cログに記録するサービスを有効にします。コグのアイコンをクリックすると、「システム」→「ログ」のページが表示され、W3Cログの設定を確認することができます。

接続タイムアウト

デフォルトの接続タイムアウトは600秒（10分）です。この設定は、アクティビティがないときに接続がタイムアウトするまでの時間を調整します。一般的に90秒以下の短命なステートレスWebトラフィックの場合は、この値を減らします。RDPのようなステートフルな接続の場合は、インフラに応じてこの数値を7200秒（2時間）などのように増やします。RDPのタイムアウトの例では、ユーザーが2時間以内に活動しない期間があった場合、接続は開いたままになります。

モニタリング設定

これらの設定は、［基本］タブの［リアルサーバーモニター］に関するものです。この設定には、サーバーのステータスがオンラインまたは故障と判定されるまでに成功または失敗したモニターの数をカウントするグローバルエントリがあります。

インターバル

インターバルは、モニター間の時間を秒単位で指定します。デフォルトの間隔は1秒です。ほとんどの用途では1秒でも問題ありませんが、他の用途やテスト時にはこの値を増やした方が良い場合もあります。

モニタリングタイムアウト

タイムアウト値は、ADCがサーバーからの接続要求に対する応答を待つ時間です。デフォルト値は2sです。忙しいサーバーの場合は、この値を大きくしてください。

モニタリングインカウント

この設定のデフォルト値は2です。2という値は、Real Serverがオンラインになる前にヘルスモニターのチェックに2回合格しなければならないことを示しています。この数値を大きくすると、サーバーがトラフィックを提供できる確率が高くなりますが、間隔によってはサービスを開始するまでに時間がかかります。この値を小さくすると、サーバーが早くサービスを開始できるようになります。

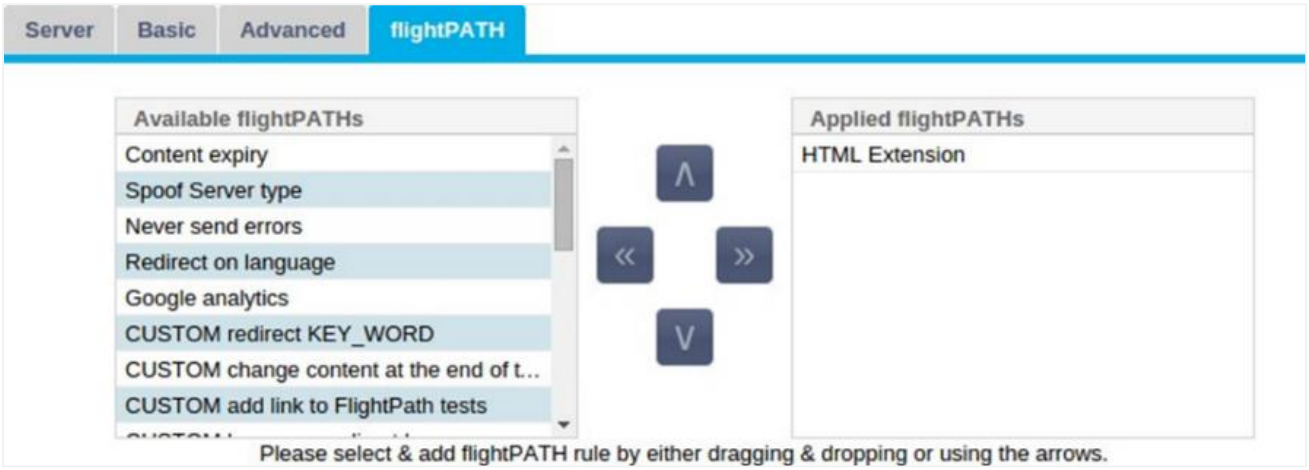
モニタリングアウトカウント

この設定のデフォルト値は3で、ADCがこのサーバーへのトラフィックの送信を停止するまでに、Real Serverモニターが3回失敗しなければならないことを意味し、そのサーバーは「赤」で「到達不能」とマークされます。この数値を大きくすると、ADCがこのサーバーへのトラフィック送信を停止するまでの時間を犠牲にしても、より良い信頼性の高いサービスが得られます。

マックス接続数

Real Server の同時接続数を制限するもので、サービスごとに設定します。例えば、2台のリアルサーバーを使用している場合、ADCは各リアルサーバーの同時接続数を1000に制限します。また、すべてのサーバーでこの制限に達した場合、「サーバーが混雑しています」というページを表示して、応答がなかったり遅延が発生した理由をユーザーに理解してもらうこともできます。無制限に接続したい場合は、この項目を空白にします。ここで設定する値は、お客様のシステムリソースに依存します。

フライトパス



flightPATHは、Edgenexus社が設計したシステムで、ADC内でのみ利用可能です。他のベンダーのルールベースのエンジンとは異なり、flightPATHはコマンドラインやスクリプト入力コンソールを介して操作するものではありません。代わりに、GUIを使用して、必要なものを実現するために実行するさまざまなパラメータ、条件、アクションを選択します。これらの機能により、flightPATH は非常に強力で、ネットワーク管理者は非常に効果的な方法で HTTPS トラフィックを操作することができる。

flightPATHはHTTPS接続でのみ使用可能であり、バーチャルサービスタイプがHTTPでない場合、このセクションは表示されません。

上の画像を見ると、左には利用可能なルールのリストが、右にはバーチャルサービスに適用されたルールが表示されていることがわかります。

利用可能なルールを追加するには、ルールを左側から右側にドラッグ＆ドロップするか、ルールをハイライト表示して右矢印をクリックし、右側に移動させます。

実行の順番は重要で、一番上のルールから順に実行されます。実行順序を変更するには、ルールをハイライトして、矢印を使って上下に動かします。

ルールを削除するには、左のルールインベントリにドラッグ＆ドロップで戻すか、ルールをハイライトして左矢印をクリックします。

flightPATHルールの追加、削除、編集は、このガイドの「flightPATHの設定」セクションで行うことができます。

ライブラリー

アドオン

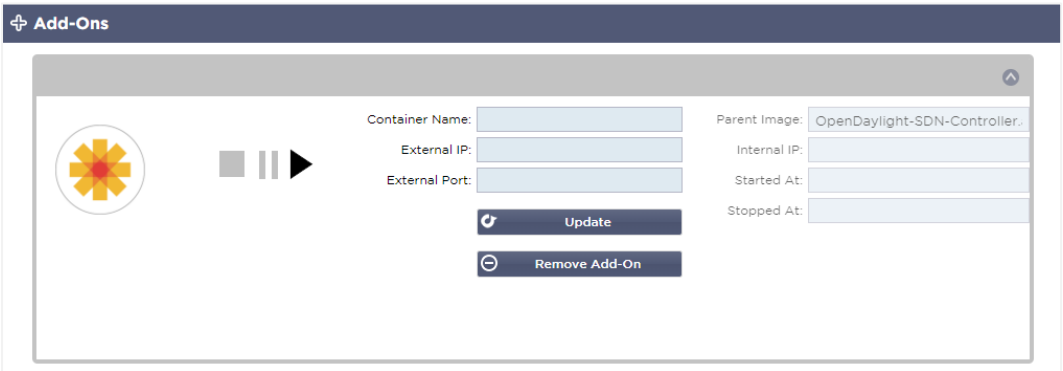
アドオンはDockerベースのコンテナで、ADCの中で隔離されたモードで実行できます。アドオンの例としては、アプリケーションファイアウォールや、ADC自体のマイクロインスタンスなどがあります。

アプリ

Add-Ons内のAppsセクションでは、お客様が購入、ダウンロード、展開したAppsの詳細が表示されます。

アプリが存在しない場合、このセクションには、アプリセクションに進み、アプリをダウンロードして配置することを促すメッセージが表示されます。

アプリを配置すると、アプリエリアに表示されます。



アドオンの購入

Appを購入するには、App Storeへの登録が必要です。購入は、ADC本体を使って行います。あなたは以下を見つけるでしょう。

ADCダッシュボードのLibrary > Appsページに移動します。

ここでは、ダウンロードしたいアプリを選択して、インストールすることができます。

ADCダッシュボードから実行する場合は、1項目のみ選択してください。お客様は複数のADCセットを所有している可能性があり、アプリケーションは展開先のADCに関連付ける必要があります。

デスクトップやブラウザからApp Storeにアクセスした場合は、好きなだけダウンロードすることができます。例えば、WAFやGSLBを4つダウンロードすることができます。ADCの「購入済みアプリ」に表示されますので、ダウンロードしてください。

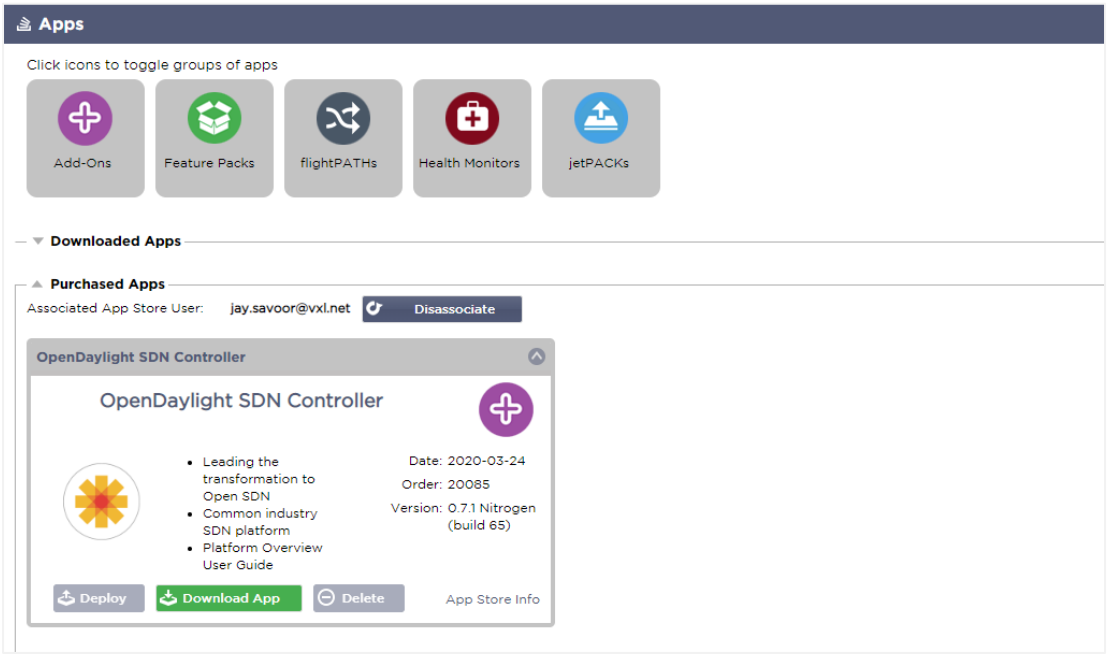
お客様が所有し、登録したADCに関連するアプリです。

お客様がアプリのダウンロードを選択すると、マシンIDの入力を求められます。その後、アプリは暗号化され、ADCのマシンIDにリンクされます。

App Storeへのリンクは

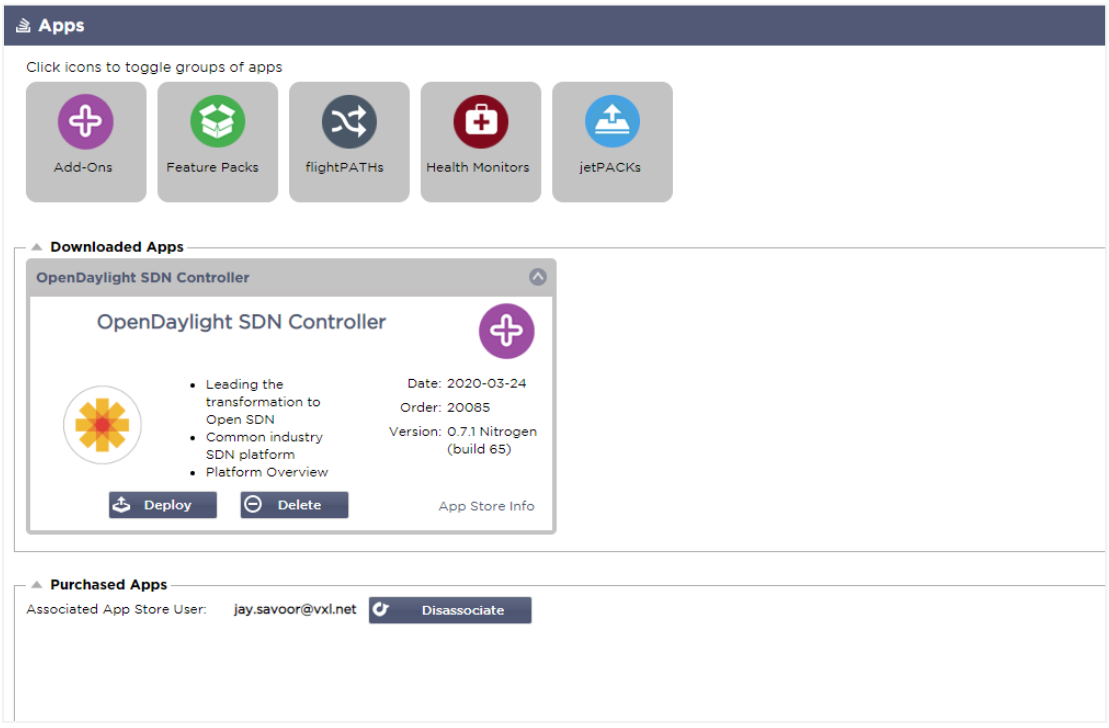
- アドオンです。**HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/ADD-ONS/**
- Health Monitors**HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/SERVER-HEALTH-MONITORS/**
- jetPACKS: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/JETPACKS/**

- フィーチャーパックHTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/EDGENEXUS-FEATURE-PACK/
- flightPATHのルールHTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/FLIGHTPATH/ です。
- ソフトウェア・アップデートHTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/EDGENEXUS-SOFTWAR-UPDATE/



アプリのデプロイ

ADCにダウンロードされたアプリは、「ダウンロードしたアプリ」セクションに移動し、「デプロイ」ボタンを使ってADCにデプロイされます。このプロセスは、ADCの利用可能なリソースに応じて時間がかかります。デプロイされると、「ダウンロードしたアプリ」セクションに表示されます。



認証

ライブラリ」＞「認証」のページでは、認証サーバーを設定し、クライアント側のBasicまたはForms、サーバー側のNTLMまたはBASICのオプションで認証ルールを作成することができます。

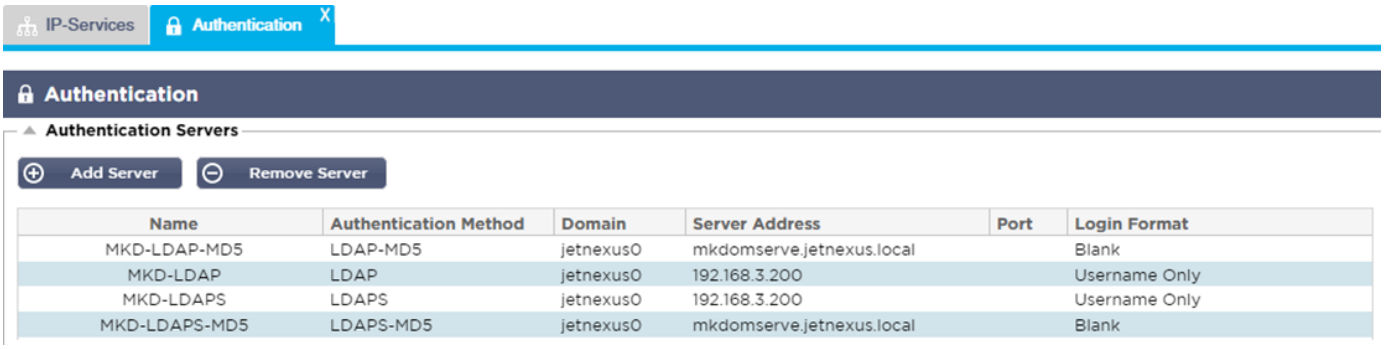
認証の設定 - ワークフロー

お客様のサービスに認証を適用するために、最低限以下の手順を実行してください。

1. Authentication Serverの作成。
2. 認証サーバーを使用する認証ルールを作成します。
3. 認証ルールを使用するflightPATHルールを作成します。
4. flightPATHルールのサービスへの適用

認証サーバー

動く認証方法を設定するには、まず認証サーバーを設定する必要があります。



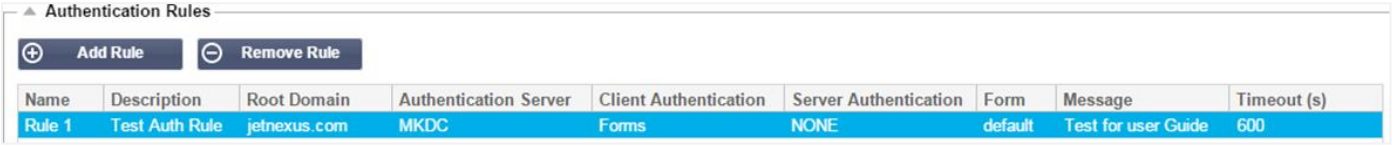
- Add Server "ボタンをクリックします。
- このアクションにより、完成に向けて空白の行が作成されます。

オプション	説明
名前	サーバーを識別するための名前を付けます。この名前はルールで使用されます。
説明	説明文の追加
認証方法	認証方法の選択 LDAP - ユーザー名とパスワードを平文でLDAPサーバーに送信する基本的なLDAP。 LDAP-MD5 - 基本的なLDAPで、ユーザー名は平文、パスワードはMD5でハッシュ化され、セキュリティが強化されています。 LDAPS - LDAP over SSL。ADCとLDAPサーバー間の暗号化トンネル内でパスワードを平文で送信します。 LDAPS-MD5 - LDAP over SSL。ADCとLDAPサーバー間の暗号化されたトンネル内で、パスワードをMD5ハッシュ化してセキュリティを強化します。
ドメイン	LDAPサーバーのドメイン名を入れてください。
サーバーアドレス	認証サーバーのIPアドレスまたはホスト名の追加 LDAP - IPv4アドレスまたはホスト名。 LDAP-MD5 - ホスト名のみ（IPv4アドレスでは動作しません LDAPS - IPv4アドレスまたはホスト名。 LDAPS-MD5 - ホスト名のみ（IPv4アドレスは動作しません）。
ポート	デフォルトでは、LDAPに389番ポート、LDAPSに636番ポートを使用します。LDAPおよびLDAPSのポート番号を追加する必要はありません。他の方法が利用可能になった場合は、ここで設定できるようになります
検索条件	検索条件はRFC4515に準拠する必要があります。例

	(MemberOf=CN=Phone-VPN,CN=Users,DC=mycompany,DC=local)となっています。
検索ベース	この値は、LDAPデータベースでの検索の開始点となります。 例 *dc=mycompany,dc=local*
ログイン形式	必要なログイン形式をご利用ください。 ユーザー名 - このフォーマットを選択すると、ユーザー名のみを入力する必要があります。ユーザーが入力したユーザー情報やドメイン情報はすべて削除され、サーバーのドメイン情報が使用されます。 ユーザー名とドメイン - ユーザーは、ドメインとユーザー名の構文をすべて入力する必要があります。例：*mycompany\gchristie OR someone@mycompany.*サーバーレベルで入力されたドメイン情報は無視されます。 Blank - ADCは、ユーザーが入力したものをすべて受け入れて、認証サーバーに送信します。このオプションは、MD5 を使用する場合に使用します。
パスフレーズ	このオプションは、本バージョンでは使用されていません。
デッドタイム	このバージョンでは使用されていません

認証ルール

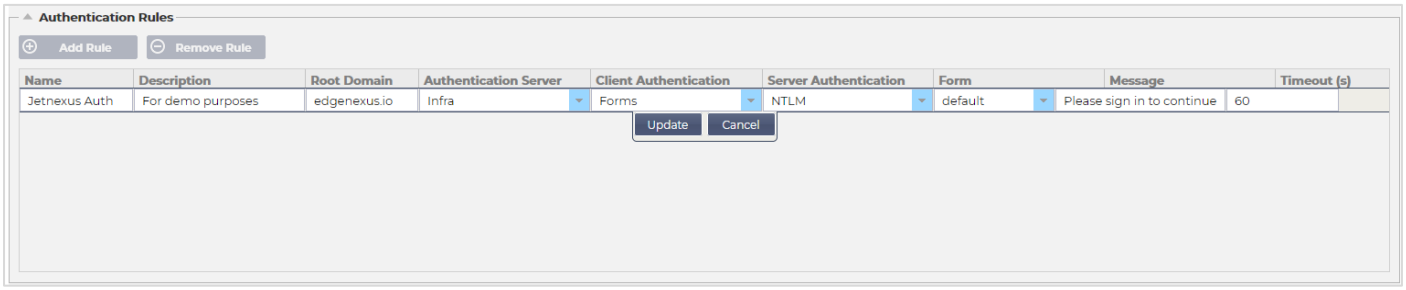
次の段階では、サーバー定義で使用する認証ルールを作成します。



フィールド	説明
名前	認証ルールの適切な名前を追加します。
説明	適切な説明を追加します。
ルートドメイン	サブドメイン間でのシングルサインオンが必要な場合を除き、この項目は空白にしておく必要があります。
認証サーバー	このドロップダウンボックスには、設定済みのサーバーが表示されます。
クライアント認証。	お客様のニーズに合った値をお選びください。 Basic (401) - この方法では、標準の401認証方式を使用します。 Forms - これは、ADCのデフォルトフォームをユーザーに表示します。フォームの中には、メッセージを追加することができます。以下のセクションで、アップロードしたフォームを選択できます。
サーバー認証	適切な値を選択してください。 None - サーバーに既存の認証機能がない場合は、この設定を選択します。この設定は、以前は何もなかったサーバーに、認証機能を追加できることを意味します。 Basic - サーバーで基本認証（401）が有効になっている場合は、「BASIC」を選択します。 NTLM - お使いのサーバーでNTLM認証が有効になっている場合は、「NTLM」を選択します。
フォーム	適切な値を選ぶ Default - このオプションを選択すると、ADCは内蔵のフォームを使用します。 カスタム - 自分でデザインしたフォームを追加して、ここで選択することができます。

メッセージ	フォームに個人的なメッセージを追加します。
タイムアウト	ルールにタイムアウトを追加すると、それ以降はユーザーの再認証が必要になります。タイムアウトの設定は、フォームベースの認証でのみ有効です。

シングルサインオン



ユーザーにシングルサインオンを提供する場合は、Root Domainの欄にドメインを記入します。この例では、edgenexus.ioを使用しています。edgenexus.ioをルートドメインとする複数のサービスを用意すれば、ユーザーは一度だけログインすればよいことになります。以下のようなサービスを考えてみましょう。

- Sharepoint.mycompany.com
- usercentral. mycompany.com
- appstore.mycompany.com

これらのサービスは、1つのVIPに存在することも、3つのVIPに分散して存在することも可能です。usercentral.mycompany.com に初めてアクセスしたユーザーは、使用した認証ルールに応じてログインを求めるフォームが表示されます。同じユーザーがappstore.mycompany.comに接続すると、ADCによって自動的に認証されます。タイムアウトを設定することができ、このタイムアウト時間に達すると、強制的に認証が行われます。

フォーム

このセクションでは、カスタムフォームをアップロードすることができます。

カスタムフォームの作成方法

ADCが提供する基本フォームはほとんどの目的には十分ですが、企業がユーザーに独自のアイデンティティを提示したい場合もあるでしょう。そのような場合にユーザーに入力してもらうためのカスタムフォームを作成することができます。このフォームは、HTM形式またはHTML形式のいずれかでなければなりません。

オプション	説明
名前	フォーム名 = loginform action = %JNURL% です。 メソッド＝POST
ユーザー名	構文: name = "JNUSER"
パスワードです。	name="JNPASS"
任意のメッセージ 1:	%JNMESSAGE%。
任意のメッセージ 2:	%jnauthmessage%。

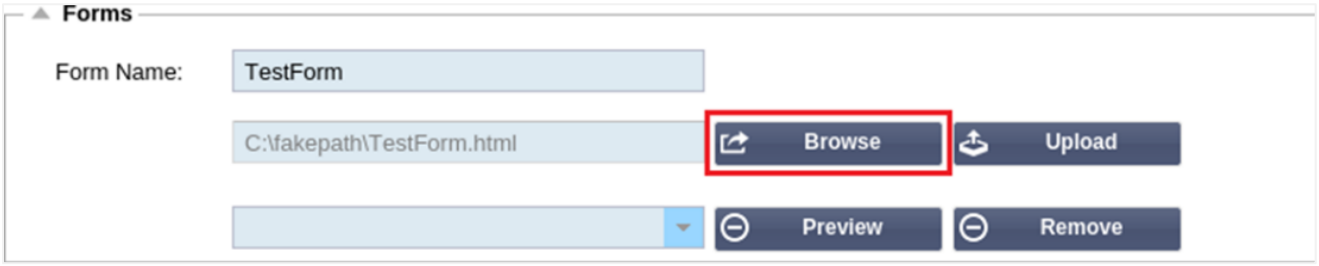
イメージ	画像を追加したい場合は、Base64エンコーディングを使用してインラインで追加してください。

非常に基本的でシンプルなフォームのhtmlコード例

```
<HTML>
<HEAD
<title>sample auth form</title>
</HEAD>。
<BODY>
%JNMESSAGE%<br>。
<form name="loginform" action="%JNURL%" method="post"> USER: <input type="text" name="JNUSER" size="20" value=""></br>。
PASS：<input type="password" name="JNPASS" size="20" value=""></br>。
<input type="submit" name="submit" value="OK">。
</form>。
</b> </b> </b> </b
</HTML>
```

カスタムフォームの追加

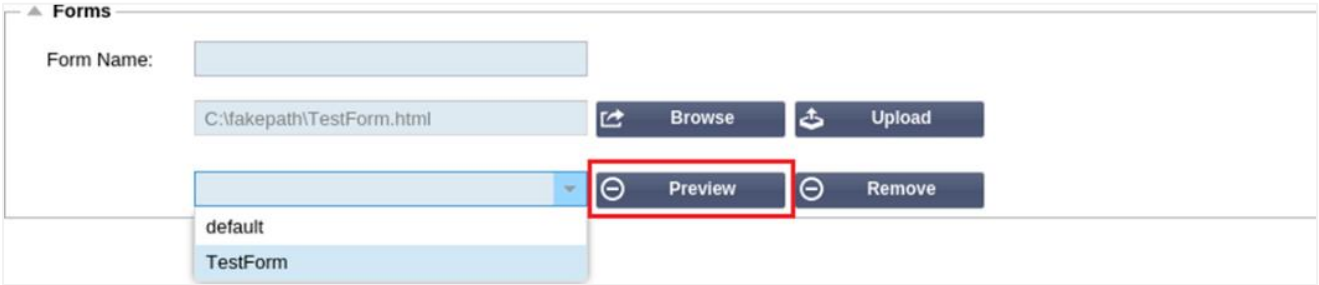
カスタムフォームを作成したら、「フォーム」セクションを使って追加することができます。



1. フォームの名前を決める
2. あなたのフォームをローカルにブラウズする
3. アップロードをクリック

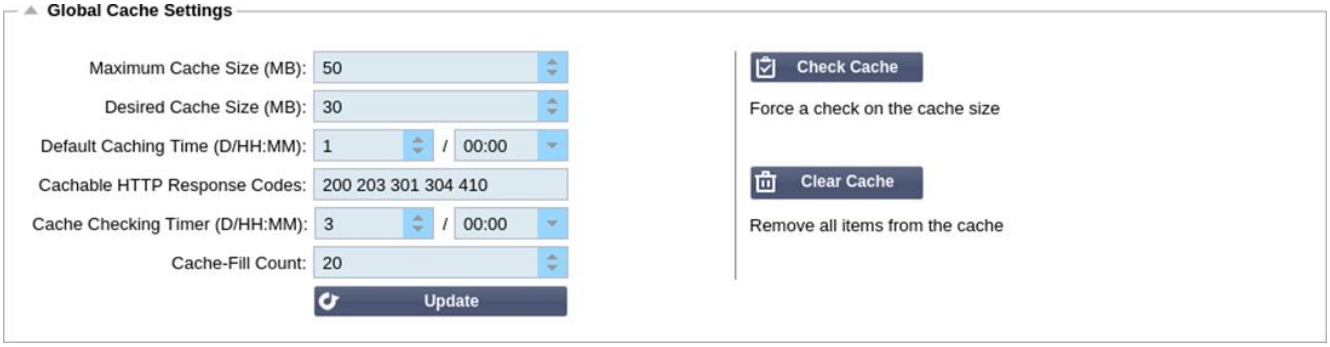
カスタムフォームのプレビュー

アップロードしたばかりのカスタムフォームを表示するには、フォームを選択して「プレビュー」をクリックします。このセクションでは、不要になったフォームを削除することもできます。



キャッシュ

ADCは、内部メモリ内にデータをキャッシュすることができ、このキャッシュを定期的にADCの内部ストレージにフラッシュします。この機能を管理するための設定をこのセクションで説明します。



グローバルキャッシュの設定

最大キャッシュサイズ(MB)

この値は、Cache が消費する最大の RAM を決定します。ADC キャッシュはメモリ内キャッシュであり、再起動、リブート、およびシャットダウン操作後もキャッシュの永続性を維持するために定期的にストレージ媒体にフラッシュされます。この機能は、最大キャッシュサイズがアプライアンスのメモリーフットプリント（ディスクスペースではなく）内に収まる必要があり、利用可能なメモリーの半分以下であることを意味します。

希望のキャッシュサイズ（MB

この値は、キャッシュを切り詰めるための最適な RAM を示します。最大キャッシュサイズは、キャッシュの絶対的な上限を示しますが、希望キャッシュサイズは、キャッシュサイズの自動または手動によるチェックが行われたときに、キャッシュが達成しようとする最適なサイズを意図しています。最大キャッシュサイズと希望キャッシュサイズの間のギャップは、キャッシュサイズを定期的にチェックして期限切れのコンテンツを切り詰める間に、新しいコンテンツが到着したり重なったりすることに対応するために存在します。繰り返しになりますが、デフォルト値（30MB）を受け入れて、「モニター」→「統計」でキャッシュのサイズを定期的に確認し、適切なサイズにすることがより効果的です。

デフォルトのキャッシュタイム (D/HH:MM)

ここで入力された値は、明示的な有効期限のないコンテンツの寿命を表しています。デフォルトのキャッシング時間は、"no-store "ディレクティブやトラフィックヘッダーに明示的な有効期限がないコンテンツが保存される期間です。

つまり、"1/01:01"（デフォルトは1/00:00）と入力すると、ADCは1日分のコンテンツを保持し、"01:00 "は1時間分、"00:01 "は1分分のコンテンツを保持することになります。

キャッシング可能なHTTP レスポンスコード

キャッシュされるデータセットの一つにHTTPレスポンスがあります。キャッシュされるHTTPレスポンスコードは

- 200 - 正常なHTTPリクエストに対する標準的な応答
- 203 - ヘッダーは確定したものではなく、ローカルまたはサードパーティのコピーから収集したものです。
- 301 - リクエストされたリソースに新しいパーマネントURLが割り当てられました。

- 304 - 最後のリクエストから変更されていないため、ローカルにキャッシュされたコピーを使用する必要があります。
- 410 - リソースがサーバーで利用できなくなり、転送先のアドレスがわからない。

このフィールドは、最も一般的なキャッシュ可能なレスポンスコードがすでにリストアップされているため、注意して編集する必要があります。

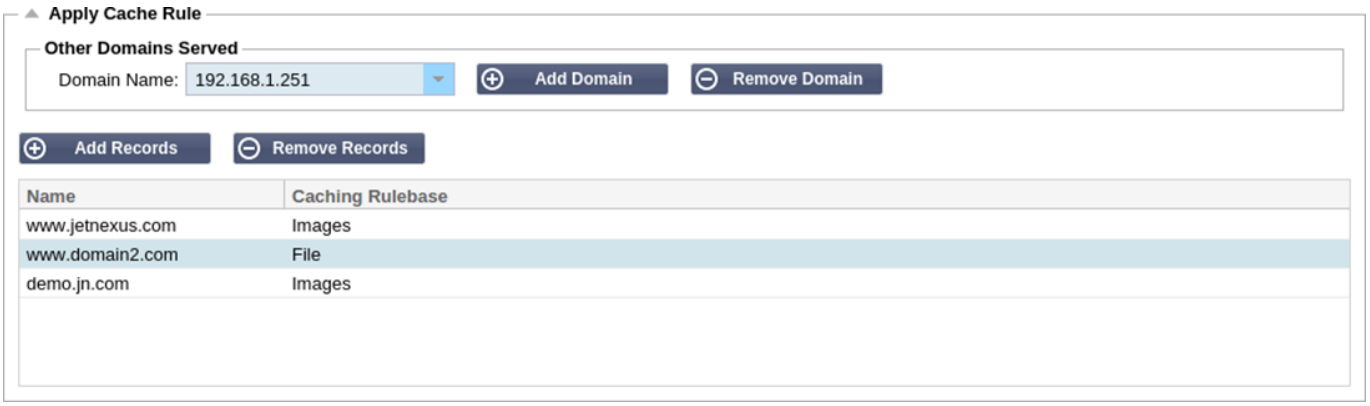
キャッシュチェック時間 (D/HH:MM)

この設定は、キャッシュトリム操作の時間間隔を決定します。

キャッシュ・フィル・カウント

この設定は、一定の数の304が検出された場合に、キャッシュを埋めるための補助機能です。

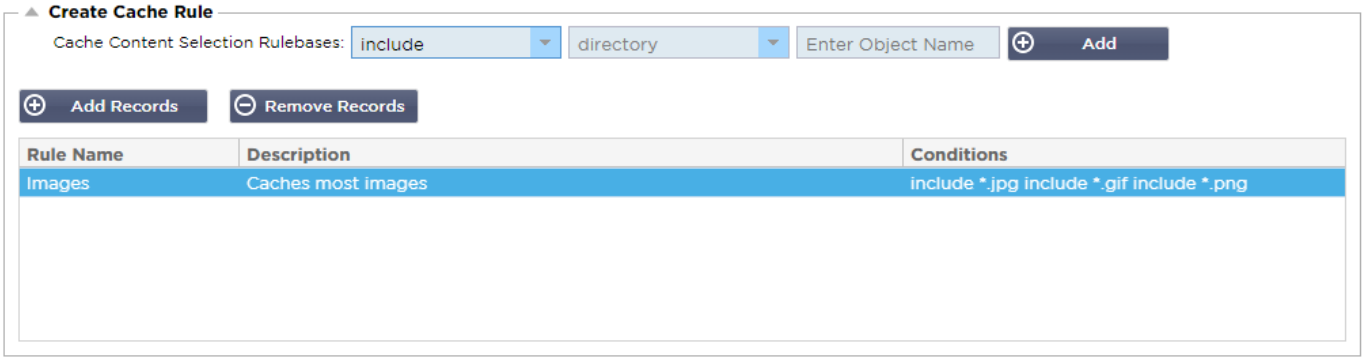
キャッシュルールの適用



ここでは、キャッシュルールをドメインに適用することができます。

- レコードの追加」ボタンでドメインを手動で追加します。その際、完全修飾ドメイン名またはIPアドレスをドットデシマル表記で入力してください。例 www. mycompany.com または 192.168.3.1:80
- ドロップダウン矢印をクリックし、リストからドメインを選択する
- トラフィックが仮想サービスを通過し、仮想サービスにキャッシュ戦略が適用されている限り、このリストは入力されます。
- Caching Rulebase列をダブルクリックして、リストからキャッシュルールを選択します。

キャッシュルールの作成



このセクションでは、いくつかの異なるキャッシングルールを作成して、ドメインに適用することができます。

- レコードの追加」をクリックし、ルールの名前と説明を入力します。
- 条件を手動で入力するか、「条件の追加」を使って

選択ルールベースを使って条件を追加するには

- 含める」または「除外する」を選択
- すべてのJPEG画像を選択
- 追加マークをクリック
- 条件に「include *.jpg」が追加されていることがわかります。
- さらに条件を追加することができます。手動で追加する場合は、各条件を新しい行に追加する必要があります。条件」ボックスをクリックするまでは、ルールは同じ行に表示され、その後は別の行に表示されますのでご注意ください。

フライトパス

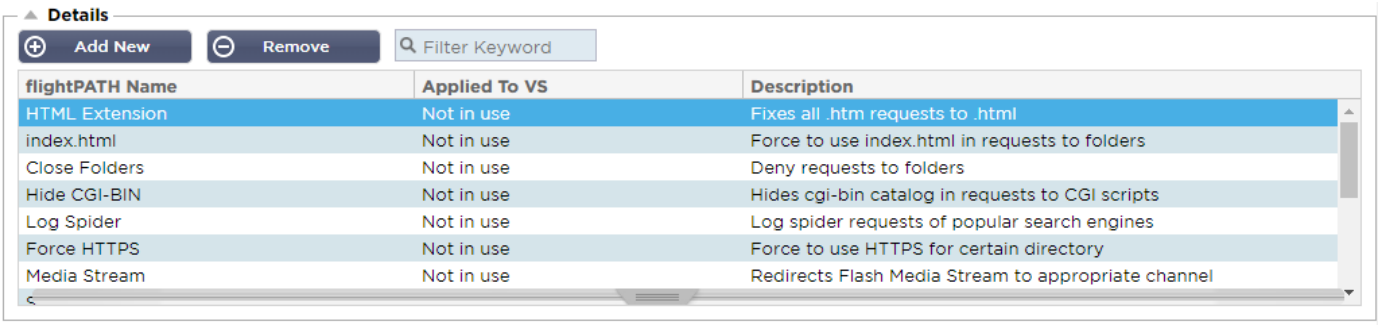
flightPATH」は、ADCに搭載されたトラフィック管理技術です。「flightPATH」は、HTTPやHTTPSのトラフィックをリアルタイムに検査し、条件に応じてアクションを実行することができます。

IPオブジェクトをルール内で使用する場合、flightPATHルールをVIPに適用する必要があります。

フライトパスルールは4つの要素で構成されています。

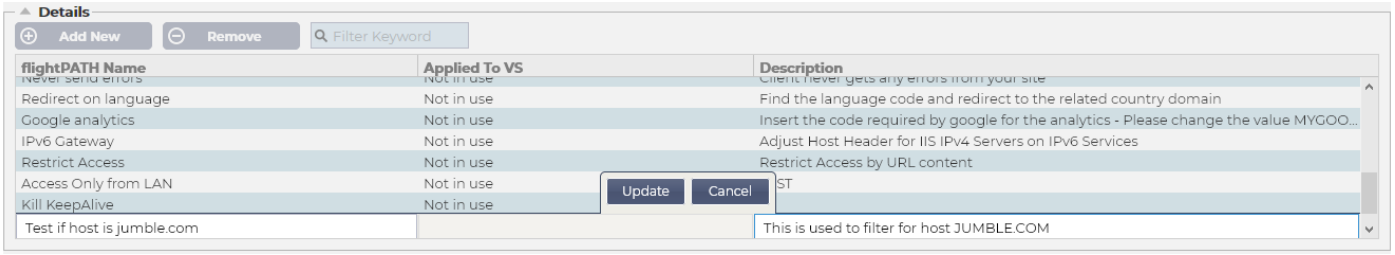
1. Details（詳細）では、flightPATH Name（フライトパス名）とアタッチ先のService（サービス）を定義します。
2. ルールのトリガーとなる条件を定義することができます。
3. アクションの中で使用できる変数を定義することができる評価
4. 条件が満たされたときに起こるべきことを管理するために使用されるアクション

詳細



詳細セクションには、利用可能なflightPATHルールが表示されます。このセクションでは、新しいflightPATHルールを追加したり、定義済みのルールを削除することができます。

新しいflightPATHルールの追加



フィールド	説明

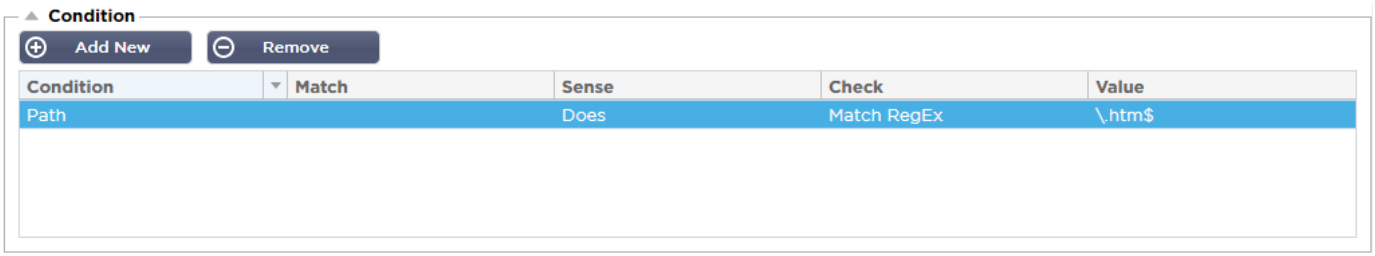
フライトパス名	このフィールドは、flightPATHルールの名前です。ここで指定した名前は、ADCの他の部分に表示され、参照されます。
VSに適用	この列は読み取り専用で、flightPATHルールが適用されるVIPを示します。
説明	読みやすさのために用意された説明文を表す値。

flightPATHルールを追加する手順

1. まず、"Details "セクションにある "Add New "ボタンをクリックします。
2. ルールの名前を入力します。例 Auth2
3. ルールの説明を入力する
4. ルールがサービスに適用されると、[Applied To]列にIPアドレスとポートの値が自動入力されます。
5. 更新ボタンを押して変更内容を保存するのを忘れないでください。間違った場合は、キャンセルボタンを押して以前の状態に戻してください。

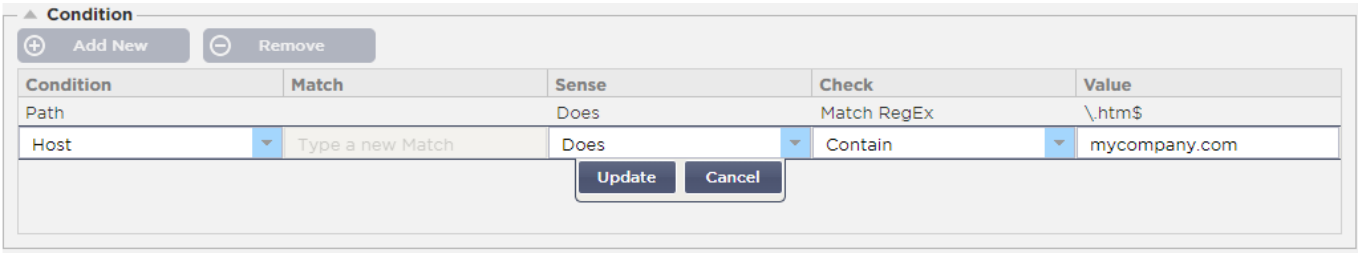
状態

flightPATH ルールは任意の数の条件を持つことができます。条件は AND で動作するため、アクションがトリガーされる条件を設定できます。OR条件を使用したい場合は、追加のflightPATHルールを作成し、正しい順序でVIPに適用します。



また、[Check] フィールドで [Match RegEx] を、[Value] フィールドで [RegEx] の値を選択して RegEx を使用することもできます。RegEx の評価が含まれることで、flightPATH の機能が大幅に拡張されます。

flightPATH条件の新規作成



状態

私たちは、ドロップダウン内にあらかじめ定義されたいくつかの条件を提供し、想定されるすべてのシナリオをカバーしています。新しい条件が追加された場合は、Jetpackのアップデートにより利用可能になります。

選択肢は以下の通りです。

コンディション	説明	例題
<form>（英語	HTMLフォームはサーバーにデータを渡すために使われる	例 "form doesn't have length 0"

GEO ロケーション	送信元IPアドレスとISO3166の国コードとの比較	GEO ロケーションが GB に該当する場合、または GEO ロケーションが Germany に該当する場合
ホスト	URLから抽出したホスト	www.mywebsite.com または 192.168.1.1
言語	language HTTPヘッダから抽出した言語	この条件では、Languagesのリストを含むドロップダウンが生成されます。
方法	HTTPメソッドのドロップダウン	GET、POSTなどを含むドロップダウン
オリジンIP	上流のプロキシがX-Forwarded-For（XFF）をサポートしている場合、真のOriginアドレスを使用します。	クライアントIPです。また、複数のIPやサブネットを使用することもできます。 10.1.2.0 /24 subnet 10\.1.2.3|10\.1.2.4 Use | for multiple IP's
パス	ウェブサイトのパス	/mywebsite/index.asp
POST	POSTリクエストメソッド	Webサイトにアップロードされるデータのチェック
問い合わせ	クエリの名前と値で、クエリ名か値も受け付けることができる	"Best=jetNEXUS" マッチはBest、バリューはedgeNEXUSの場合
問い合わせ文字列	? "文字以降のクエリ文字列全体	
リクエストクッキー	クライアントから要求されたクッキーの名前	MS-WSMAN=afYfn1CDqqCDqUD::
リクエストヘッダー	Any HTTP Header	リファラー、ユーザーエージェント、From、Date
リクエストバージョン	HTTPバージョン	http/1.0またはhttp/1.1
レスポンスボディ	レスポンスボディに含まれるユーザー定義の文字列	サーバーアップ
応答コード	応答のHTTPコード	200 OK, 304 Not Modified
レスポンスクッキー	サーバーから送られてきたクッキーの名前	MS-WSMAN=afYfn1CDqqCDqUD::
レスポンスヘッダー	Any HTTP Header	リファラー、ユーザーエージェント、From、Date
レスポンスバージョン	サーバーから送られてきたHTTPバージョン	http/1.0またはhttp/1.1
ソースIP	オリジンIP、プロキシサーバーIP、またはその他の集約されたIPアドレスのいずれか	ClientIP、ProxyIP、FirewallIP。複数のIPや

	サブネットを使用することもできます。ドットはRegEXなので必ずエスケープしてください。例 10\\.1\.2\.3 は 10.1.2.3 です。

マッチ

一致」フィールドは、ドロップダウンまたはテキスト値のいずれかで、「条件」フィールドの値に応じて定義できます。例えば、ConditionがHostに設定されている場合、Matchフィールドは利用できません。Conditionが<form>に設定されている場合、Matchフィールドはテキストフィールドとして表示され、ConditionがPOSTに設定されている場合、Matchフィールドは適切な値を含むドロップダウンとして表示されます。

選択肢は以下の通りです。

MATCH	説明	例題
受け入れ	許容されるコンテンツタイプ	Accept: text/plain
Accept-Encoding	使用可能なエンコーディング	Accept-Encoding: <compress | gzip | deflate | sdch | identity>。
アクセプト・ランゲージ	回答に使用できる言語	Accept-Language: en-US
受け入れ範囲	このサーバーがサポートしているパーシャルコンテンツの範囲タイプ	Accept-Ranges: bytes
オーソライズ	HTTP認証用の認証情報	オーソライズされています。基本 QWxhZGRpbjpvcGVuIHNlc2FtZQ==。
チャージ・トゥー	要求された方法の適用にかかるコストの勘定情報を含む	
Content-Encoding	使用されているエンコーディングの種類	Content-Encoding: gzip
Content-Length	レスポンスボディの長さをオクテット（8ビットバイト）で表したもの	Content-Length: 348
コンテンツタイプ	リクエストの本文のmimeタイプ（POSTおよびPUTリクエストで使用されます	Content-Type: application/x-www-form-urlencoded
クッキー	Set-Cookie（下記）でサーバーから送られてきたHTTPクッキー	Cookie: $Version=1; Skin=new;
日付	メッセージが発信された日付と時間	Date = "日付" ":" HTTP-date
ETag	リソースの特定のバージョンを示す識別子で、多くはメッセージダイジェストです。	ETag:"aed6bdb8e090cd1:0"
より	リクエストを行ったユーザーのEメールアドレス	From: user@example.com
If-Modified-Since	コンテンツが変更されていない場合に、304 Not Modifiedを返すことができる。	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT

Last-Modified	リクエストされたオブジェクトの最終更新日（RFC2822形式）。	Last-Modified:Tue, 15 Nov 1994 12:45:26 GMT
Pragma	実装。リクエスト-レスポンスの連鎖のどこかで様々な効果をもたらす可能性のある特定のヘッダー。	Pragma: no-cache
リファラー	現在要求されているページへのリンクを辿った前のWebページのアドレス	リファラー：HTTP://www.edgenexus.io
サーバー	サーバーの名前	サーバーです。Apache/2.4.1 (Unix)
セット-クーキー	HTTPクッキー	セット-クーキーUserID=JohnDoe; Max-Age=3600; Version=1
User-Agent	ユーザーエージェントの文字列	User-AgentMozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Vary	下流のプロキシに対して、将来のリクエストヘッダーをどのように照合し、オリジンサーバーから新たなレスポンスをリクエストするのではなく、キャッシュされたレスポンスを使用できるかどうかを判断する方法を指示します。	Vary:User-Agent
X-Powered-By	Webアプリケーションを支える技術（ASP.NET、PHP、JBossなど）を指定します。	X-Powered-By:PHP/5.4.0

センス

Senseフィールドはドロップダウン式のブール型フィールドで、DoesまたはDoesn'tの選択肢があります。

チェック

チェックフィールドでは、条件に対するチェック値を設定することができます。

選択できる項目は以下の通りです。Contain、End、Equal、Exist、Have Length、Match RegEx、Match List、Start、Exceed Length

CHECK	説明	例題
存在する	これは、条件の詳細を気にせず、存在するかしないかだけを気にするものです。	ホストが存在する
スタート	文字列は、Valueで始まります。	パス - Does - Start - /secure
終了	文字列の最後には、Value	パス - Does - End - .jpg
収録内容	この文字列には、以下の値が含まれています。	リクエストヘッダー - アクセプト - Does - Contain - image
イコール	文字列は「値」に等しい	ホスト - Does - Equal - www.jetnexus.com
長さ	文字列は、値の長さを持っています。	ホスト - Does - Have Length - 16 www.jetnexus.com = TRUE www.jetnexus.co.uk = FALSE

Match RegEx	完全なPerl互換の正規表現を入力することができます。	Origin IP - Does - Match Regex - 10\...* | 11\...*

条件を追加する手順

新しい flightPATH 条件の追加はとても簡単です。その例を上に示します。

1. 条件エリア内の「新規追加」ボタンをクリックします。
2. ドロップダウンボックスから条件を選択します。ここではHostを例に説明します。フィールドに入力することもでき、ADCはドロップダウンで値を表示します。
3. Senseを選ぶ。例えば、Does
4. チェックを選びます。例えば、「Contain
5. 値を選択します。例えば、mycompany.com

上記の例では、ルールが完了するためには、両方ともTRUEでなければならない2つの条件があることを示しています。

- 1つ目は、要求されたオブジェクトが画像であるかどうかを確認することです。
- 2つ目は、URLのホストがwww.imagepool.com であるかどうかをチェックします。

評価

定義可能な変数を追加できるのは魅力的な機能です。通常のADCでは、スクリプトやコマンドラインのオプションを使ってこの機能を提供していますが、これは誰にとっても理想的ではありません。ADCでは、以下に示すように、使いやすいGUIを使って任意の数の変数を定義することができます。

flightPATH変数の定義には、4つのエントリーが必要です。

- Variable - これは変数の名前です。
- Source - ドロップダウンリストに表示されるソースポイント。
- 詳細 - ドロップダウンから値を選択するか、手動で入力します。
- Value - 変数が保持する値で、英数字または微調整用のRegExが使用できます。

内蔵変数。

組み込み変数はすでにハードコードされているので、これらのために評価エントリを作成する必要はありません。

アクション "セクションでは、以下のような変数が使用できます。

各変数の説明は、上の「条件」の表にあります。

- メソッド = $method$
- パス = $path$
- クエリストリング = $querystring$
- Sourceip = $sourceip$
- レスポンスコード（テキストには "200 OK "も含まれる） = $resp$

- ホスト = $host$
- バージョン = $version$
- クライアントポート = $clientport$
- Clientip = $clientip$
- ジオロケーション = $geolocation$"

ACTION	TARGET
アクション = リダイレクト 302	ターゲット = HTTPs://$host$/404.html
アクション＝ログ	ターゲット = $sourceip$:$sourceport$のクライアントが$path$ページをリクエストしました。

説明します。

- 存在しないページにアクセスすると、通常はブラウザの404エラーページが表示されます。
- 代わりに、ユーザーが使用した元のホスト名にリダイレクトされますが、不正なパスは404.htmlに置き換えられます。
- Syslogに "A client from 154.3.22.14:3454 has just requested the wrong.html page "というエントリが追加されます。

アクション

プロセスの次の段階では、flightPATHルールと条件に関連するアクションを追加します。

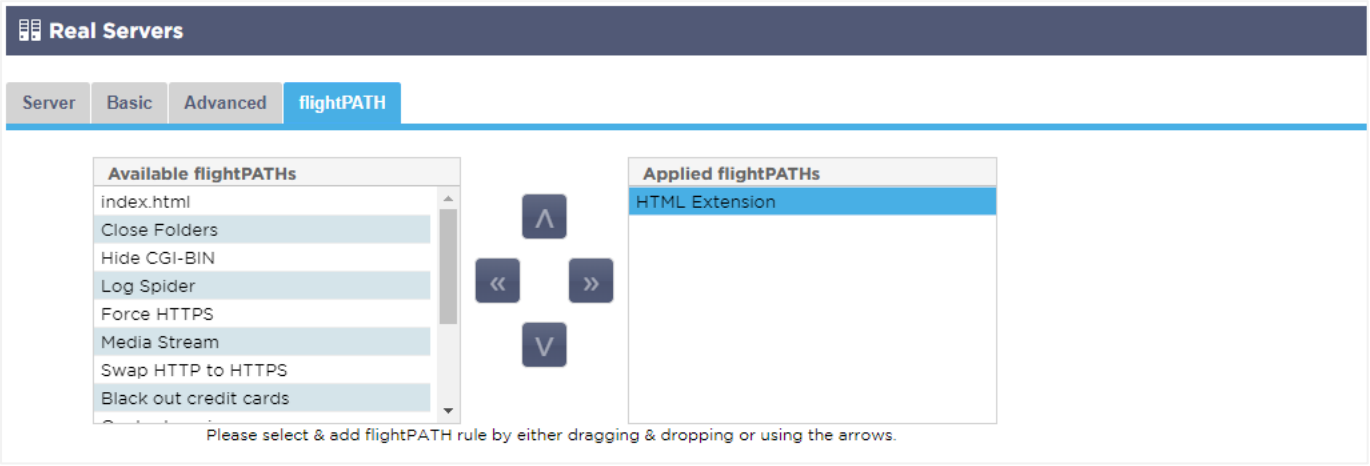
この例では、ユーザーが入力したURLを反映させるために、URLのパス部分を書き換えます。

- 新規追加」をクリックします。
- アクション」ドロップダウンメニューから「パスの書き換え」を選択します。
- ターゲット」欄に「$path$/myimages」と入力します。
- アップデートをクリック

このアクションでは、パスに/myimagesが追加されるので、最終的なURLは www.imagepool.com/myimages となります。

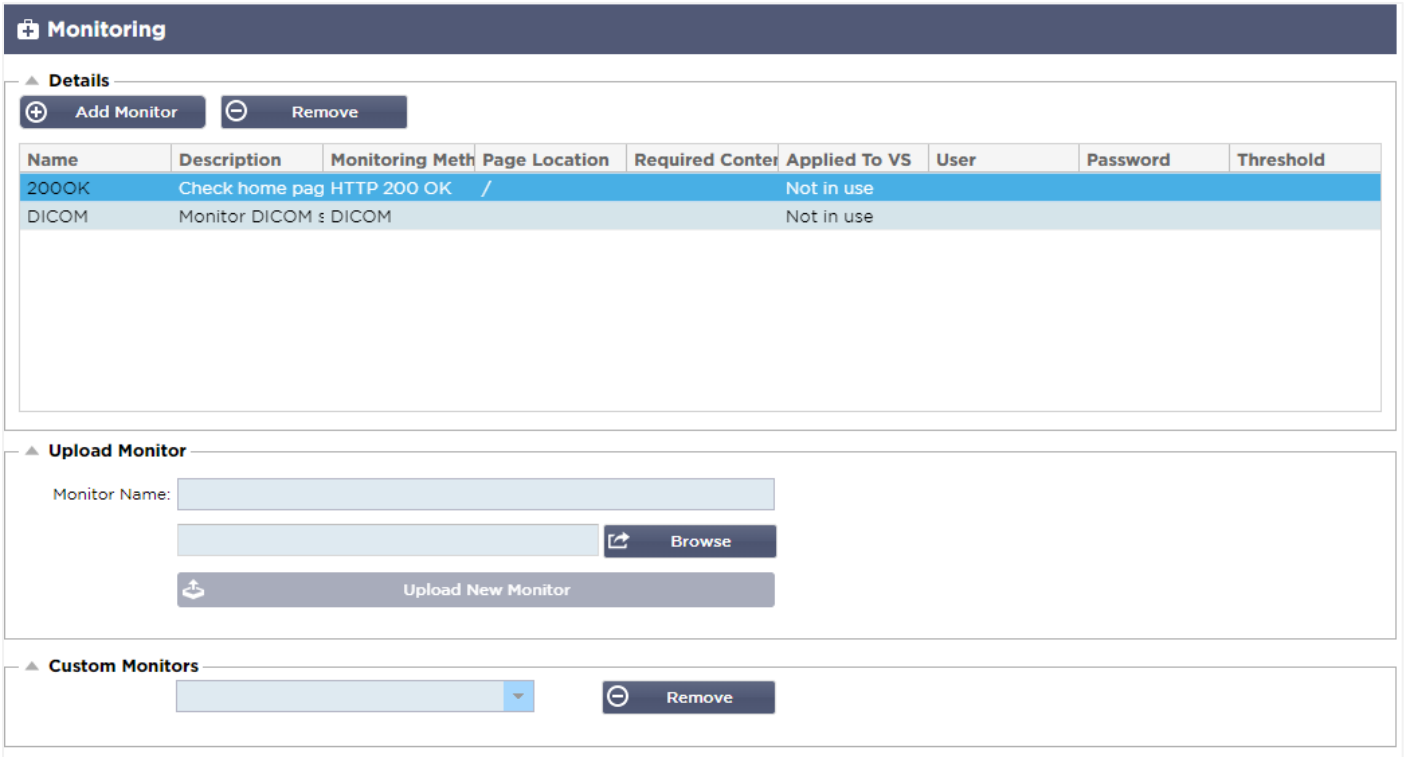
flightPATHルールの適用

flightPATHルールの適用は、各VIP/VSのflightPATHタブ内で行われます。



- サービス」→「IPサービス」を選択し、flightPATHルールを割り当てるVIPを選択します。
- 以下のようなReal Serverのリストが表示されます。
- flightPATHタブをクリックします。
- 設定したflightPATHルール、またはサポートされている事前構築済みのルールのいずれかを選択します。必要に応じて複数のflightPATHルールを選択できます。
- 選択したセットを「Applied flightPATHs」セクションにドラッグ＆ドロップするか、>>矢印ボタンをクリックします。
- ルールは右側に移動し、自動的に適用されます。

リアルサーバーモニター



ロードバランシングが設定されている場合、実際のサーバーとその上で動作しているアプリケーションの健全性を監視することが有用です。例えば、Webサーバーでは、状態を監視するための特定のページを設定したり、ADCが持つ他の監視システムを利用したりすることができます。

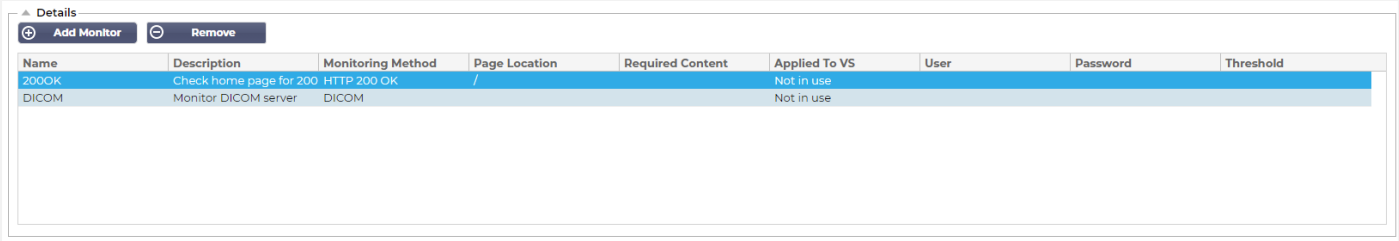
ライブラリ］＞［リアルサーバモニタ］ページでは、カスタムモニタを追加、表示、編集することができます。これらはレイヤ7サーバーの「ヘルスチェック」であり、定義した仮想サービスの「基本」タブ内の「サーバー監視」フィールドから選択します。

リアルサーバーモニター」のページは、3つのセクションに分かれています。

- 詳細
- アップロード
- カスタムモニター

詳細

詳細セクションでは、新しいモニターを追加したり、不要なモニターを削除したりします。また、既存のモニターをダブルクリックして編集することもできます。



名前

モニターのご希望の名前

説明

このモニターのテキストの説明です。できるだけ説明的なものにすることをお勧めします。

モニタリング方法

ドロップダウンリストから監視方法を選択します。選択できるのは

モニタリング方法	説明	例
HTTP 200 OK	リアルサーバへのTCP接続が行われる。接続が完了すると、簡単なHTTPリクエストがリアルサーバに送信されます。サーバーからのHTTPレスポンスを待って、「200 OK」レスポンスコードを確認します。200 OK」の応答コードを受信した場合、リアルサーバーは稼働していると判断されます。タイムアウトや接続の失敗など、何らかの理由で「200 OK」レスポンスコードが受信されない場合、そのReal Server はダウンしていて利用できないとみなされます。この監視方法は、HTTPとAccelerated HTTPのサービスタイプでのみ使用することができます。ただし、HTTPサーバにレイヤ4サービスタイプが使用されている場合、リアルサーバでSSLが使用されていないか、「コンテンツSSL」機能で適切に処理されていれば、使用することができます。	名前200OK 説明します。チェックプロダクションのWebサイト モニタリング方法です。HTTP 200 OK ページの位置/main/index.html OR HTTP://www.edgenexus.io/main/index.html 必須コンテンツです。該当なし

HTTPレスポンス	リアルサーバーへの接続とHTTPリクエスト／レスポンスが行われ、先ほどの例で説明したようにチェックされます。ただし、レスポンスコードが「200 OK」であるかどうかではなく、HTTPレスポンスのヘッダーにカスタムテキストが含まれているかどうかをチェックします。テキストは、ヘッダー全体、ヘッダーの一部、ページの一部の行、または1つの単語であることができます。このテキストが見つかった場合、Real Server は稼働していると判断されます。この監視方法は、実際にはHTTPとAccelerated HTTPのサービスタイプにしか使用できません。ただし、HTTPサーバでレイヤ4サービスタイプが使用されている場合、リアルサーバでSSLが使用されていないか、「コンテンツSSL」機能で適切に処理されていれば、使用することができます。	名前サーバーアップ 説明します。Server Up」のページの内容を確認します。" モニタリング方法です。HTTPレスポンス ページの位置/main/index.html OR HTTP://www.edgenexus.io/main/index.html 必須コンテンツです。サーバーアップ
DICOM	必要なコンテンツ欄に「Source Calling」AE Titleの値を使用してDICOMエコーを送信します。また、「Destination Called」AE Titleの値は、各サーバーのNotes欄に設定することができます。Notes欄は、IP Services-の中にあります。 -バーチャルサービス--サーバーページ。	名前DICOM 説明します。DICOMサービスのL7ヘルスチェック モニタリング方法。DICOM ページの位置。N/A 必要なコンテンツAET値
TCP アウトオブバンド	TCP Out of Band方式は、必要なコンテンツの欄に監視したいポートを指定できること以外は、TCP Connectと同じです。このポートは通常、トラフィックポートとは異なり、サービスを結びつけたい場合に使用します	名前を教えてください。TCP アウトオブバンド 説明アウトオブバンド/トラフィックポートの監視 ページの位置。N/A 必須コンテンツです。555
マルチポートのTCPモニタ	この方法は、複数の異なるポートを持つことができるという点を除いて、上記の方法と同様です。必須コンテンツセクションで指定されたすべてのポートが正しく応答した場合のみ、モニターは成功したとみなされます。	名称マルチポートモニター 説明複数のポートを監視して成功させる ページの位置。N/A 必要なコンテンツ135,59534,59535

ページの位置

URL HTTPモニターのページ位置。この値は、/folder1/folder2/page1.htmlのような相対リンクにすることができます。また、ウェブサイトがホスト名にバインドされる絶対リンクも使用できます。

必須コンテンツ

この値には、モニターが検出して利用する必要のあるコンテンツが含まれています。ここに表示される値は、選択されたモニタリング方法によって変わります。

VSに適用

このフィールドには、モニターが適用されているバーチャルサービスのIP/ポートが自動的に入力されます。バーチャルサービスで使用されているモニターは削除できません。

ユーザー

カスタムモニターの中には、この値をパスワードフィールドと一緒に使用して、Real Serverにログインできるものがあります。

パスワード

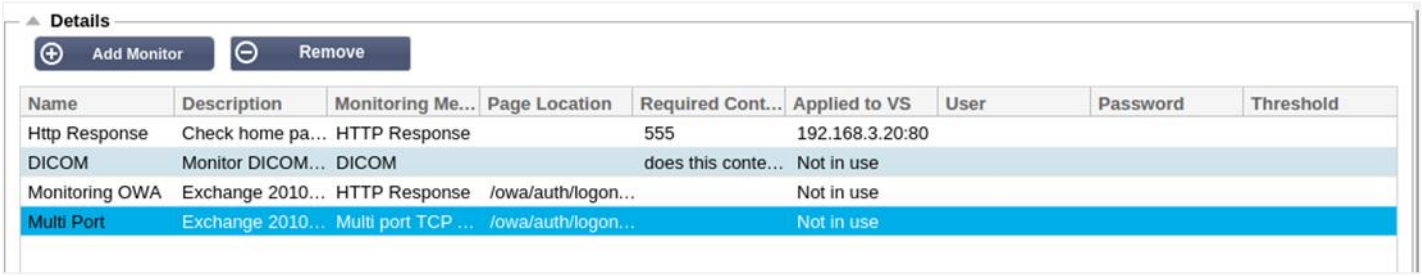
カスタムモニターの中には、この値をUserフィールドとともに使用して、Real Serverにログインできるものがあります。

しきい値

Thresholdフィールドは、CPUレベルなどのしきい値が必要なカスタムモニターで使用される一般的な整数です。

注：アプリケーションサーバーからのレスポンスが"Chunked"レスポンスでないことを確認してください。

リアルサーバーモニターの例



アップロードモニター

ユーザーが独自のカスタムモニターを作成することも多いと思いますが、このセクションではそのモニターをADCにアップロードすることができます。

カスタムモニターは、PERLスクリプトを使って書かれており、ファイルの拡張子は.plです。

- モニタリング方法のリストで識別できるように、モニタに名前を付けます。
- .plファイルを探す
- 新規モニターのアップロードをクリック
- 作成したファイルは正しい場所にアップロードされ、新しいモニタリング方法として表示されます。

カスタムモニター

このセクションでは、アップロードされたカスタムモニターを確認し、不要になった場合は削除することができます。

- ドロップダウンボックスをクリック
- カスタムモニターの名前を選択
- 削除」をクリックします。
- カスタムモニターは、モニタリング方法のリストに表示されなくなります。

カスタムモニター用Perlスクリプトの作成

注意：このセクションは、Perlでの使用および記述の経験がある方を対象としています。

このセクションでは、Perlスクリプト内で使用できるコマンドを紹介します。

Monitor-Name: コマンドは、ADCに保存されているPerlスクリプトに使用される名前です。この行を入れないと、スクリプトが検索されません。

以下は必須項目です。

- #モニター名
- use strict;
- 使用上の注意

Perl スクリプトは CHROOTED 環境で実行されます。WGETやCURLなどの別のアプリケーションを呼び出すことが多い。SNIのような特定の機能のために、これらのアプリケーションを更新する必要がある場合もあります。

ダイナミックバリュー

- my $host = $_[0]; - IP Services--Real Serverセクションの "Address "を使用しています。
- my $port = $_[1]; - IP Services--Real Serverセクションの "Port "を使用しています。
- my $content = $_[2]; - これは、「ライブラリ--リアル・サーバー・モニタリング」セクションの「Required Content」の値を使用します。
- my $notes = $_[3]; - これは、IP ServicesのReal Serverセクションにある「Notes」列を使用します。
- my $page = $_[4]; - これは、Library--Real Server Monitorセクションの "Page Location "の値を使用しています。
- my $user = $_[5]; - これは、Library--Real Server Monitorセクションの "User "値を使用しています。
- my $password = $_[6]; - これは、「ライブラリ--リアル・サーバー・モニター」セクションの「パスワード」の値を使用します。

カスタムヘルスチェックには2つの結果があります。

- 成功
  戻り値1

成功メッセージをSyslogに出力する
リアルサーバーをオンラインにする（IN COUNTが一致する場合）。

- 失敗した
戻り値2
Syslogに「Unsuccessful」というメッセージを出力
リアルサーバーをオフラインにする（OUT Countが一致した場合）。

カスタムヘルスモニターの例

```
#モニター名 HTTPS_SNI
use strict:
使用上の注意
# 利用可能なヘルスチェックのドロップダウンに上記のモニター名が表示される
# このスクリプトには6つの値が渡されています(下記参照)
# このスクリプトは以下の値を返します。
# 1 はテストが成功した場合
# 2 テストが失敗した場合 サブモニター
{
my Shost      = $_[0]; ### ホストのIPまたは名前
my Sport      = $_[1]; ### Host Port
my Scontent   = $_[2]; ### 探したいコンテンツ（WebページやHTTPヘッダーの中から
my Snotes     = $_[3]; ### バーチャルホスト名
my Spage      = $_[4]; ### URLのホストアドレス以降の部分
私のSuser     = $_[5]:### ドメイン/ユーザー名 (オプション)
my Spassword  = $_[6]; ### パスワード (オプション)
私の$resolve;
私の$auth     =;
if ($port)
{
        $resolve = "$notes:$port:$host "となります。
}
else {
        $resolve = "$notes:$host";
}
if ($user && $password) {...
        $auth = "-u $user:$password :
}
my @lines = 'curl -s -i -retry 1 -max-time 1 -k -H "Host:$notes --resolve $auth HTTPs://${notes}${page}.2>&1'; if(join(""@lines)=~/$content/)
        {
        print "HTTPs://$notes}${page} looking for - $content - Health check successful.\n";
        return(1)です。
        }
その他
```

```
        {
        print "HTTPs://${notes}${page} looking for - $content - Health check failed.\n";
        戻る(2)
        }
}
```

モニター(@ARGV)になります。

注：カスタムモニタリング - グローバル変数の使用はできません。ローカル変数のみの使用 - 関数内で定義された変数

SSL証明書

SSLで暗号化された接続を使用しているサーバーでレイヤー7の負荷分散を成功させるためには、ADCはターゲットサーバーで使用されているSSL証明書を備えている必要があります。これは、データストリームを復号し、検査し、管理し、ターゲットサーバーに送信する前に再度暗号化するためです。

SSL証明書には、ADCが生成する自己署名証明書から、信頼できるプロバイダーが提供する従来の証明書（ワイルドカードを含む）まであります。また、Active Directoryから生成されるドメイン署名付き証明書を使用することもできます。

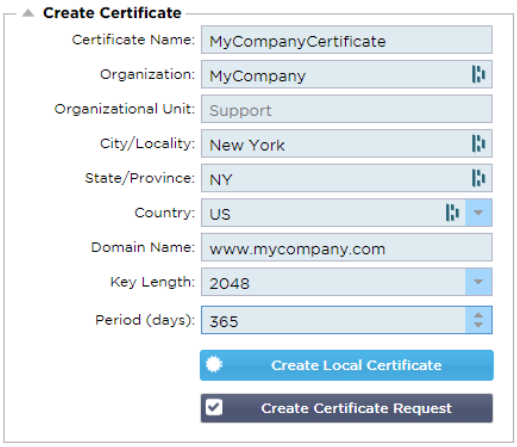
ADCはSSL証明書を使って何をするのですか？

ADCは、データに含まれる内容に応じて、トラフィック管理ルール（flightPATH）を実行できます。この管理は、SSL暗号化されたデータに対しては実行できません。ADCがデータを検査する際には、まずデータを復号化する必要があり、そのためにはサーバーが使用しているSSL証明書が必要となります。復号化されると、ADCはflightPATHルールを検査・実行できるようになります。その後、データはSSL証明書を使って再度暗号化され、最終的にReal Serverに送信されます。

証明書の作成

ADCはグローバルに信頼されたSSL証明書を使用することができますが、自己署名付きSSL証明書を生成することもできます。自己署名入りSSLは、内部のロードバランシングの要件に最適です。ただし、お客様のITポリシーによっては、信頼できるCA証明書やドメインCA証明書が必要になる場合があります。

ローカルSSL証明書の作成方法



- 上記の例のように、すべての詳細を記入してください。
- ローカル証明書の作成」をクリックします。
- これをクリックすると、証明書をバーチャルサービスに適用することができます。

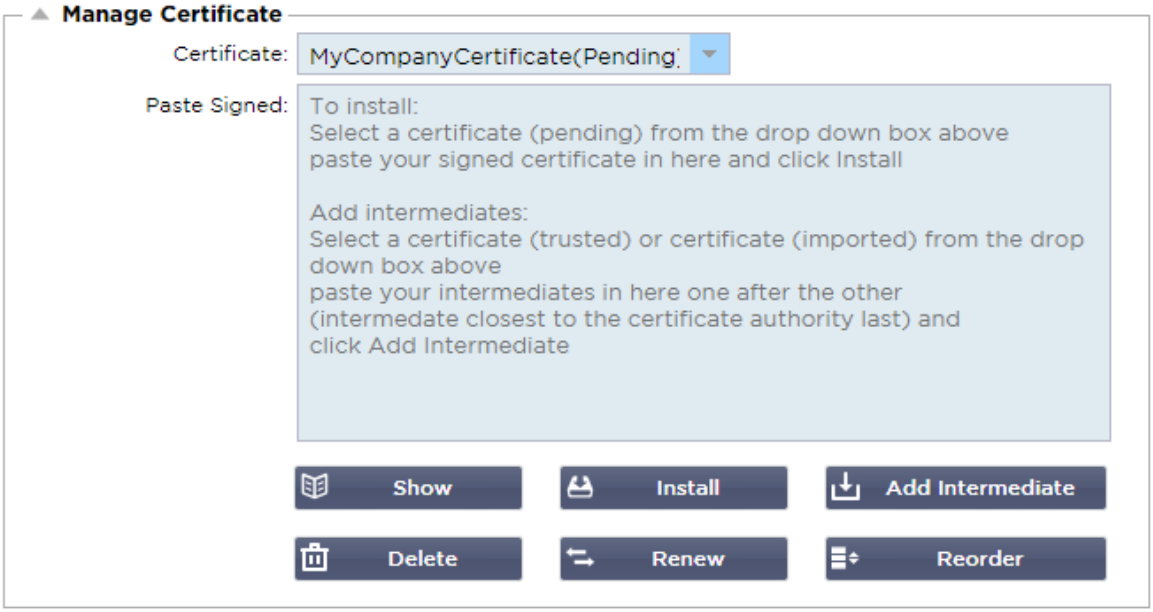
証明書要求（CSR）の作成

グローバルに信頼されるSSLを外部のプロバイダーから取得する必要がある場合、SSL証明書を生成するためのCSRを生成する必要があります。

上記のフォームに必要な情報を入力し、「証明書発行依頼」ボタンをクリックします。あなたが提供したデータに対応するポップアップが表示されます。

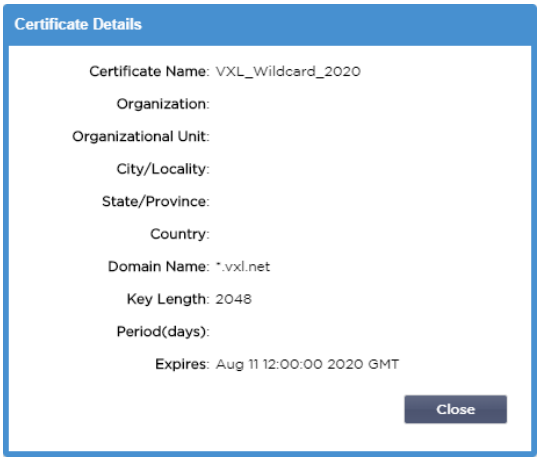
その内容をテキストファイルにカット&ペーストし、CSRファイルの拡張子をつけてください。このCSRファイルを認証局に提出して、SSL証明書を作成してもらう必要があります。

証明書の管理



このサブセクションには、ADC内で使用するSSL証明書を管理するためのさまざまなツールが含まれています。

ショー

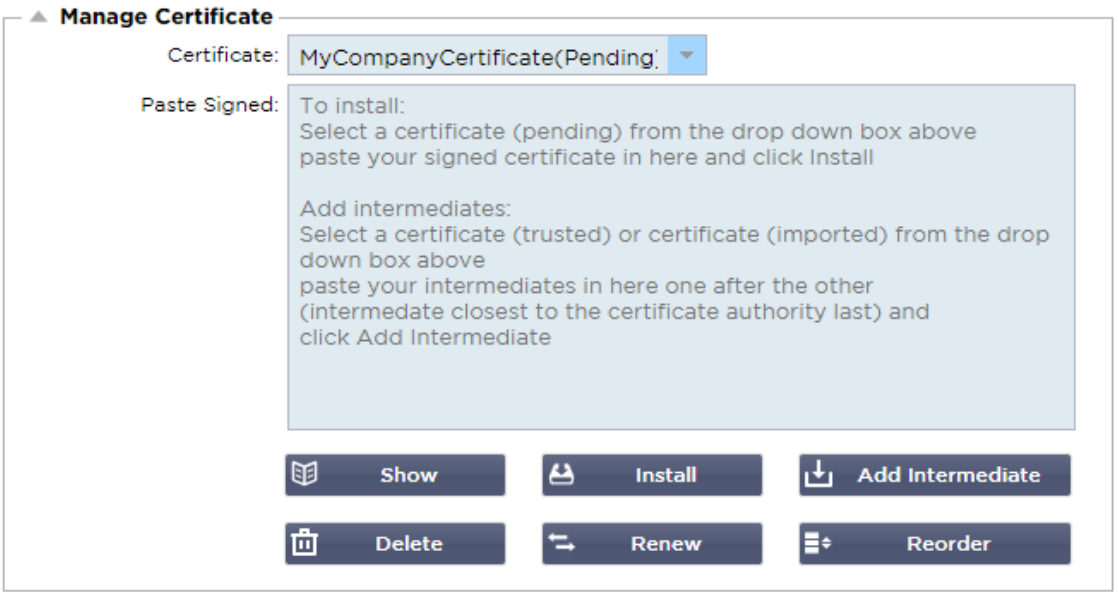


インストールされているSSL証明書の詳細を確認したい場合があります。

- ドロップダウンメニューから証明書を選択する
- 表示ボタンをクリック
- 以下のようなポップアップが表示され、証明書の詳細が表示されます。

証明書のインストール

信頼できる認証局から証明書を入手したら、生成されたCSRと照合し、ADC内にインストールする必要があります。



- 上記の手順で生成した証明書を選択します。ラインアイテムに（Pending）のステータスが固定されています。この例では、MyCompanyCertificateが上の画像のように表示されます。
- テキストエディタで証明書ファイルを開く
- ファイルの内容をすべてクリップボードにコピーする
- 信頼できる機関から受け取った署名入りSSL証明書の内容を、「Paste Signed」と書かれた欄に貼り付けます。
- また、その下の「インターメディエイト」にも、順番に気をつけて貼り付けてください。
    1. (TOP)　　サイン入り証明書
    2. (上から2番目)　　中級編
    3. (上から3番目)　　中級編
    4. (下)　　中級3
    5. ルート認証局　　クライアントマシンに存在しているので、追加する必要はありません。
       (ADCは、Real Serverのクライアントとして動作する再暗号化のためのルートバンドルも含んでいます)
- インストールをクリック
- 証明書のインストールが完了すると、証明書の横にステータス（Trusted）が表示されます。

中間順序を間違えて入力した場合は、「証明書（信頼済み）」を選択し、正しい順序で証明書（署名済み証明書を含む）を再度追加し、「インストール」をクリックする

中級者向け

場合によっては、中間証明書を別途追加する必要があります。例えば、中間証明書を持たない証明書をインポートした場合などです。

- 証明書（信頼済み）または証明書（インポート）をハイライト表示する
- 認証局に最も近い中間体が最後に貼り付けられるように注意しながら、中間体を下から順に貼り付けます。
- Add Intermediate」をクリックします。

注文を間違えてしまった場合は、プロセスを繰り返し、再度中間体を追加することができます。この操作では、前の中間体が上書きされるだけです。

証明書の削除

削除ボタンを使って、証明書を削除することができます。削除すると、証明書はADCから完全に削除されますので、証明書を交換し、必要に応じてバーチャルサービスに再適用する必要があります。

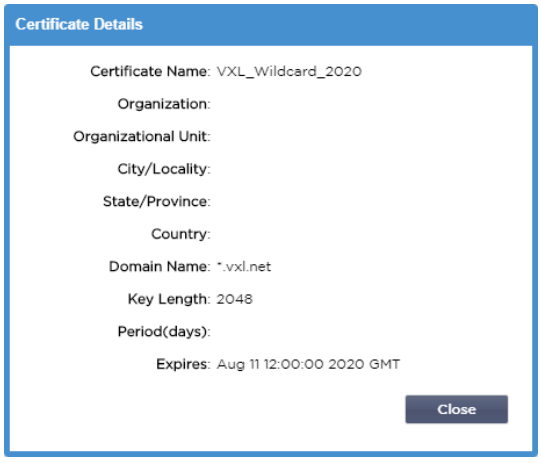
注：証明書を削除する前に、その証明書が運用中のVIPに添付されていないことを確認してください。

証明書の更新

Renew」ボタンをクリックすると、新しい Certificate Signing Request を取得することができます。この操作は、証明書の有効期限が切れて更新する必要がある場合に必要です。

- ドロップダウンリストから証明書を選択してください。
- 更新をクリック
- 新しいCSRの詳細をコピーして、新しい証明書を取得できるようにする。

- 新しい証明書を取得する際には、以下の手順を踏んでください。



- インストールされているSSL証明書の詳細を確認したい場合があります。
- ドロップダウンメニューから証明書を選択する
- 表示ボタンをクリック
- 以下のようなポップアップが表示され、証明書の詳細が表示されます。
- 証明書のインストール
- これで、新しく更新された証明書がADCにインストールされます。

証明書のインポート

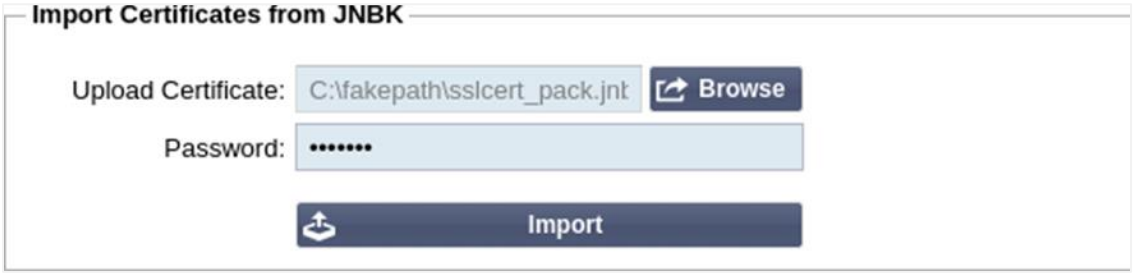
多くの場合、企業は、内部のセキュリティ体制の一部として、ドメイン署名された証明書を使用する必要がある。証明書はPKCS#12形式でなければならず、パスワードは常にこのような証明書を保護している。

下の図は、1つのSSL証明書をインポートするためのサブセクションを示しています。

- 証明書に親しみやすい名前を付けます。この名前は、ADC で使用されるドロップダウンリストで証明書を識別します。証明書のドメイン名と同じである必要はありませんが、空白を含まない英数字である必要があります。_と-以外の特殊文字は使用できません。
- PKCS#12証明書の作成に使用したパスワードを入力します。
- 証明書名}.pfxを参照します。
- Import」をクリックします。
- ADC内のSSLドロップダウンメニューに証明書が表示されます。

複数の証明書のインポート

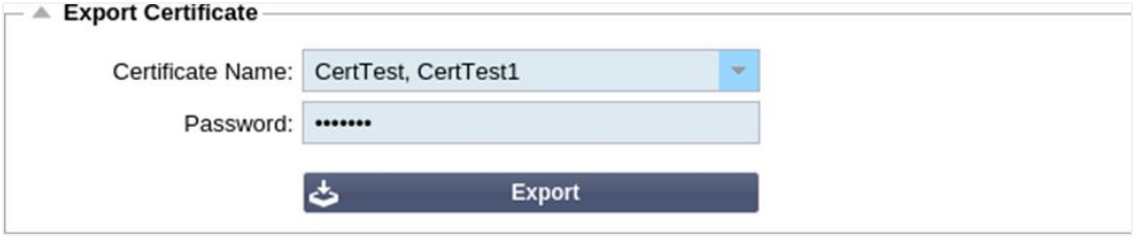
ここでは、複数の証明書を含むJNBKファイルのインポートを行います。JNBKファイルは、複数の証明書をエクスポートする際に、ADCが暗号化して作成します。



- JNBK ファイルを参照します。複数の証明書をエクスポートすることで、これらのファイルを作成することができます。
- JNBKファイルの作成時に使用したパスワードを入力してください。
- Import」をクリックします。
- 証明書は、ADC内の関連するSSLドロップダウンメニューに表示されます。

証明書のエクスポート

時折、ADC内に保持されている証明書の一つをエクスポートしたいと思うことがあります。ADCはこれを行う機能を備えています。



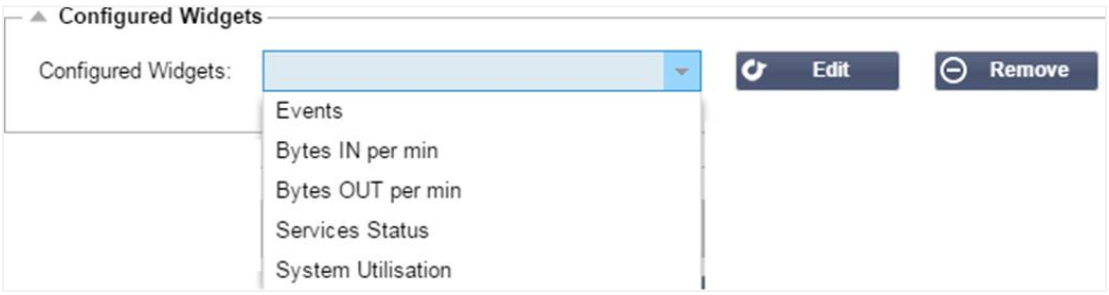
- インストールする証明書をクリックします。リストにあるすべての証明書を選択するには、［すべて］オプションをクリックします。
- エクスポートされたファイルを保護するためのパスワードを入力します。パスワードの長さは6文字以上でなければなりません。使用できる文字は、アルファベット、数字、一部の記号です。< > " ' ( ) ; „ ^ ʷ ^ „ % & &
- エクスポート」をクリックします。
- 単一の証明書をエクスポートする場合は、生成されるファイルは sslcert_{certname}.pfx という名前になります。たとえば、sslcert_Test1Cert.pfx のようになります。
- 複数の証明書をエクスポートする場合、生成されるファイルは JNBK ファイルになります。ファイル名は sslcert__pack.jnbk となります。

注）JNBKファイルは、ADCが作成する暗号化されたコンテナファイルで、ADCへのインポート時のみ有効です。

ウィジェット

ライブラリ」＞「ウィジェット」ページでは、カスタムダッシュボードに表示される様々な軽量のビジュアルコンポーネントを設定することができます。

設定済みウィジェット

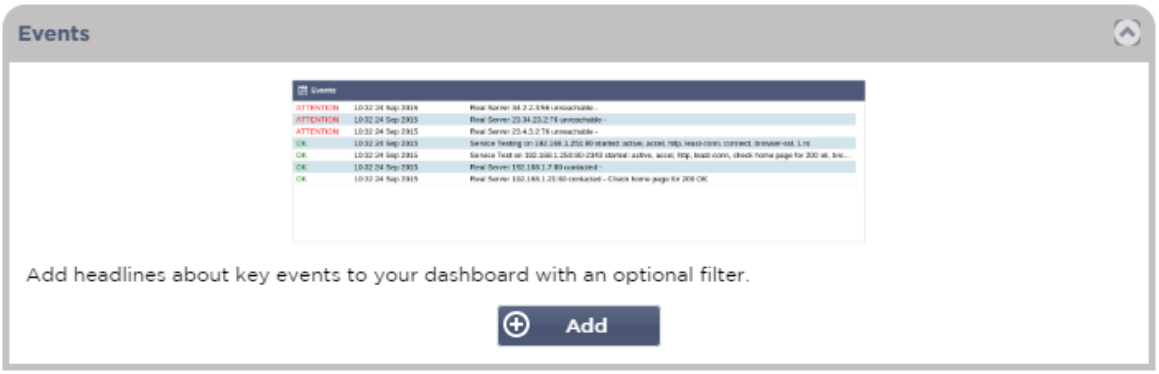


Configured Widgets」セクションでは、「available widgets」セクションから作成されたウィジェットの表示、編集、削除を行うことができます。

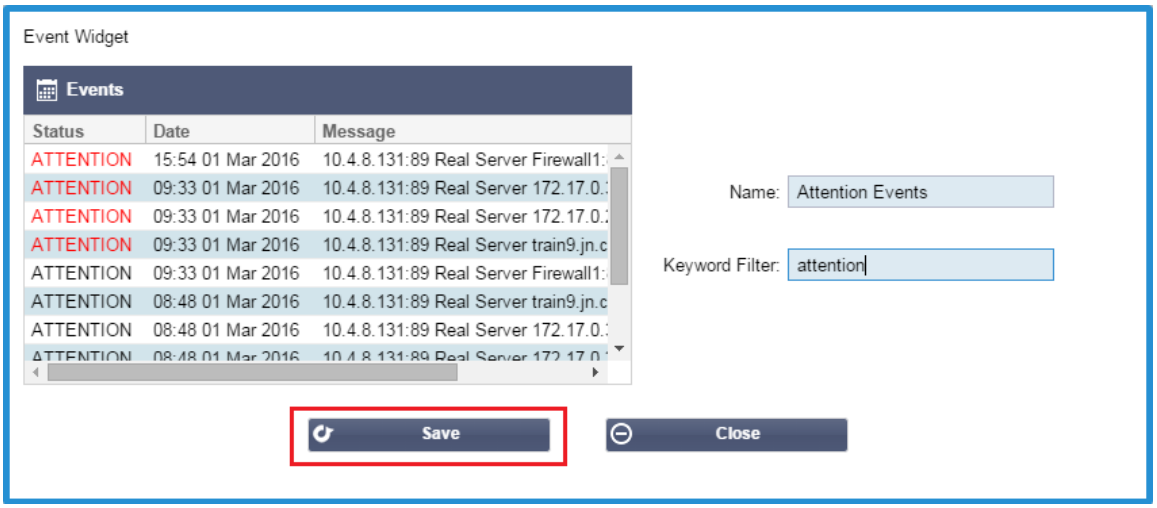
利用可能なウィジェット

ADC内には5種類のウィジェットが用意されており、必要に応じてそれらを設定することができます。

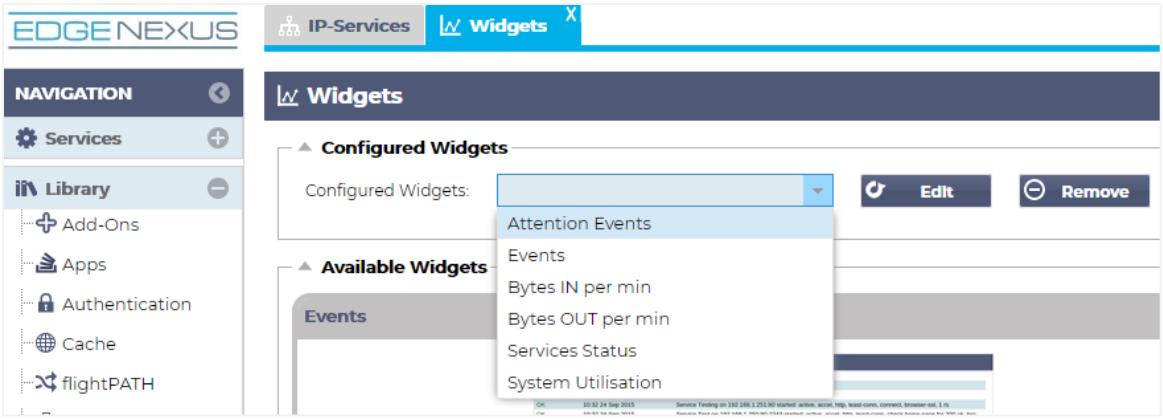
イベントウィジェット



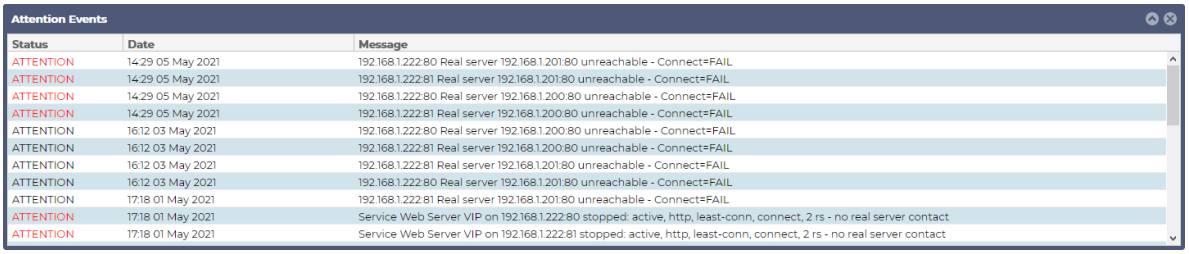
- Events "ウィジェットにイベントを追加するには、"Add "ボタンをクリックします。
- イベントの名前を記入します。この例では、イベント名として「Attention Events」を追加しています。
- キーワードフィルターを追加しました。また、Attentionのフィルター値を追加しています。



- 保存」をクリックし、「閉じる」をクリックします。
- Configured Widgets」のドロップダウンに「Attention Events」というウィジェットが追加されています。

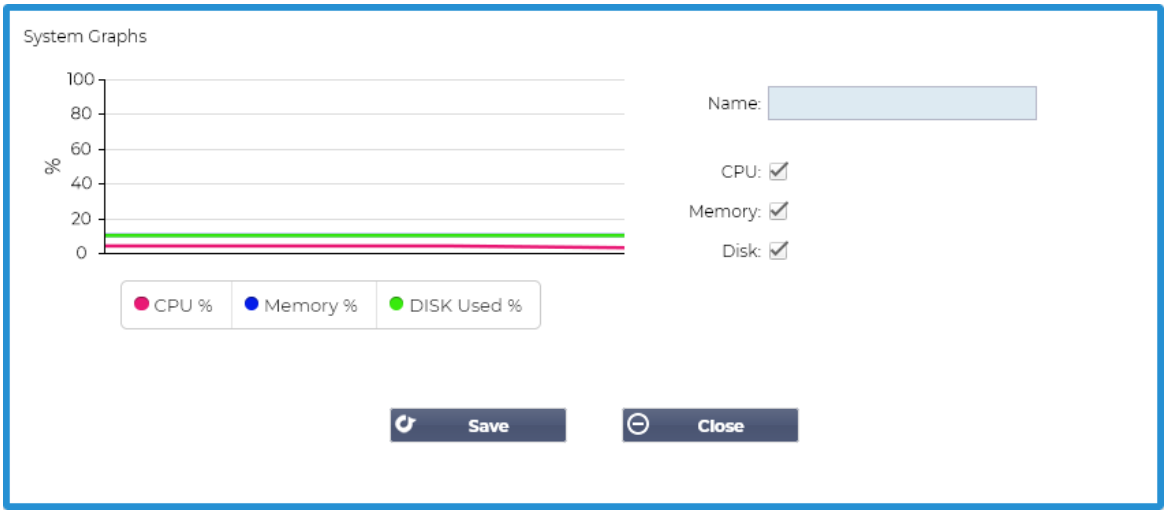


- これで、「表示」→「ダッシュボード」セクションにこのウィジェットが追加されたことがわかります。
- Attention Events」ウィジェットを選択すると、ダッシュボード内に表示されます。以下を参照してください。



また、「Pause Live Data」ボタンをクリックすると、ライブデータの配信を一時停止したり、再開したりすることができます。また、「Default Dashboard」ボタンをクリックすれば、いつでもデフォルトのダッシュボードに戻すことができます。

システム・グラフ・ウィジェット

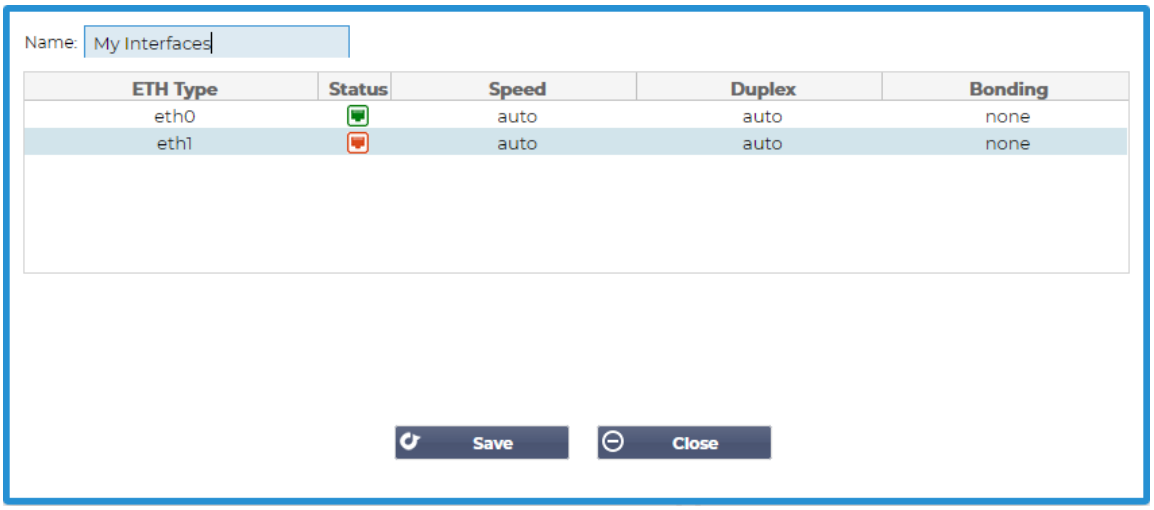


ADCには、設定可能な「System Graph」ウィジェットがあります。ウィジェットの「Add」ボタンをクリックすると、以下の監視グラフを追加して表示することができます。

- CPU
- MEMORY
- DISK

追加した後は、ダッシュボードのウィジェットメニューで個別に利用できるようになります。

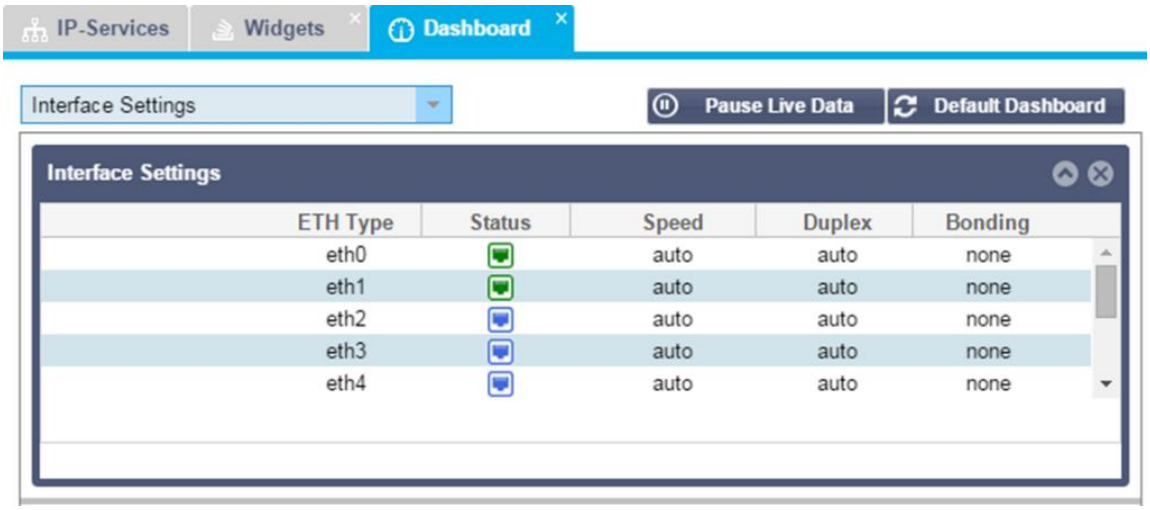
インターフェース・ウィジェット



インターフェース」ウィジェットでは、ETH0、ETH1など、選択したネットワーク・インターフェースのデータを表示することができます。追加可能なインターフェイスの数は、仮想アプライアンスに定義した、またはハードウェアアプライアンス内でプロビジョニングしたネットワークインターフェイスの数によって異なります。

完了したら、「Save」ボタン、「Close」ボタンの順にクリックします。

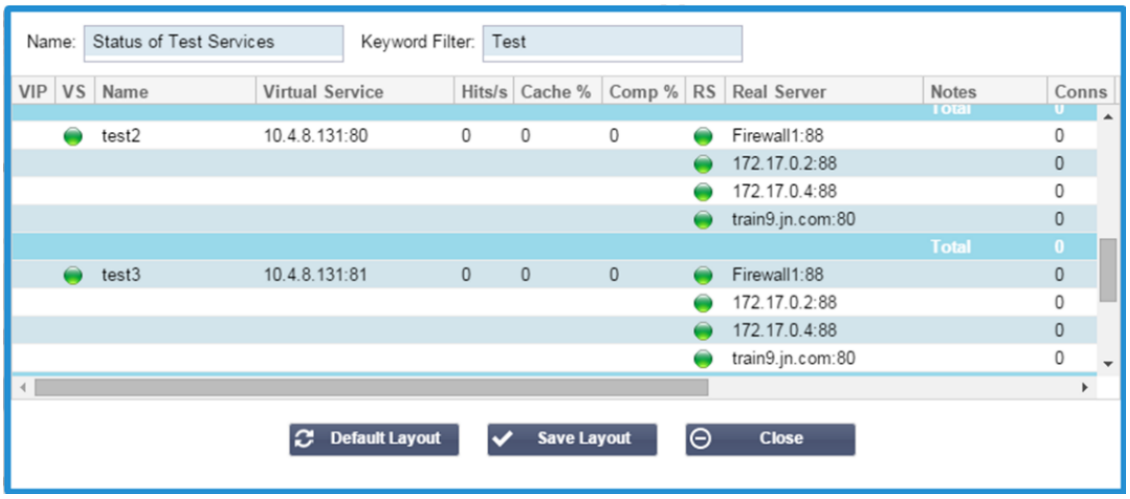
ダッシュボード内のウィジェットのドロップダウンメニューから、先ほどカスタマイズしたウィジェットを選択します。すると、以下のような画面が表示されます。



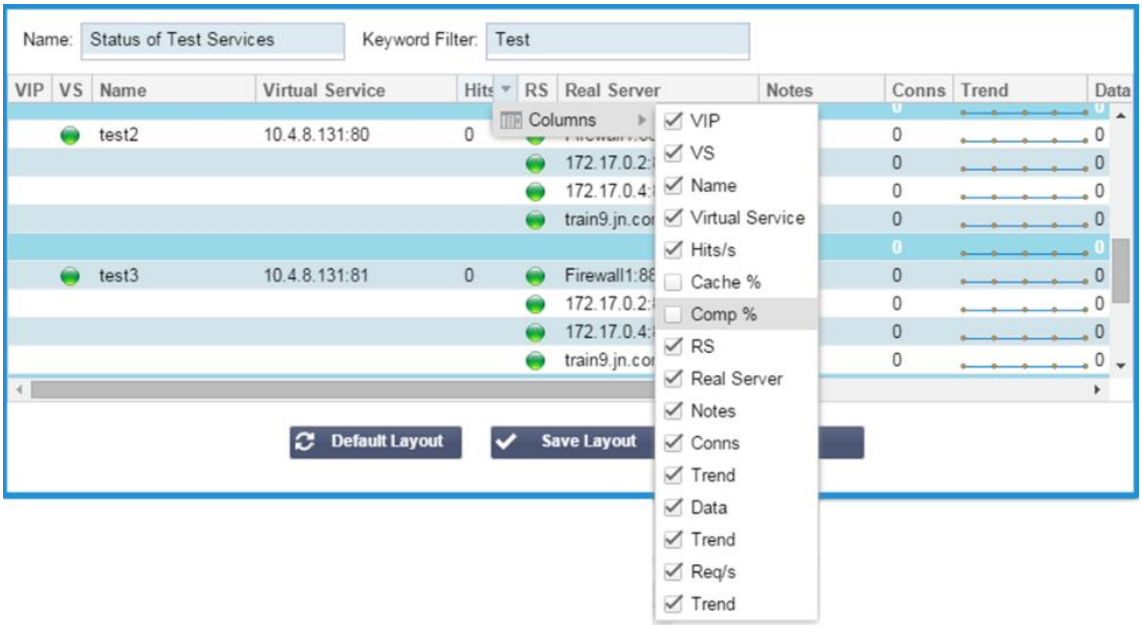
ステータスウィジェット

Statusウィジェットでは、ロードバランシングの動作を確認することができます。また、表示をフィルタリングして特定の情報を表示することもできます。

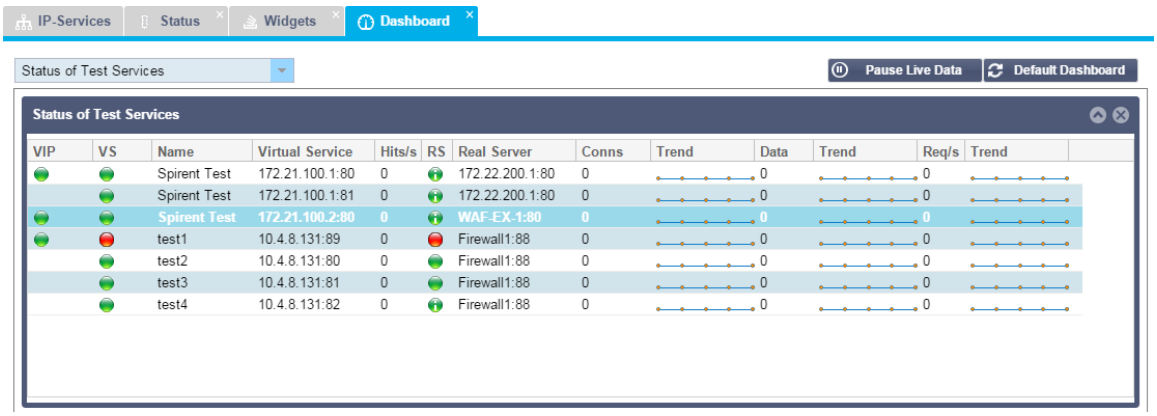
- Add」をクリックします。



- 監視したいサービスの名前を入力する
- また、ウィジェットに表示する列を選択することもできます。

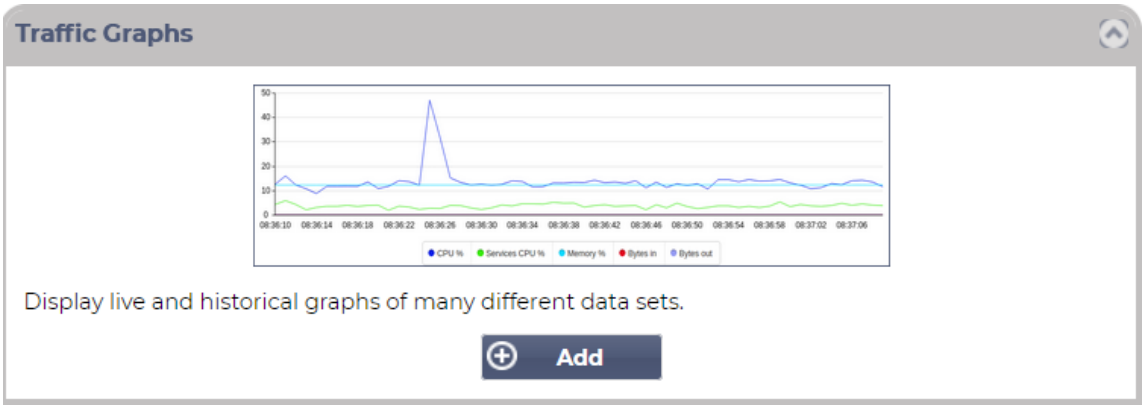


- 問題がなければ、「Save」をクリックし、「Close」をクリックします。
- 選択されたステータスウィジェットは、ダッシュボードセクションで利用可能になります。



トラフィック・グラフィックス・ウィジェット

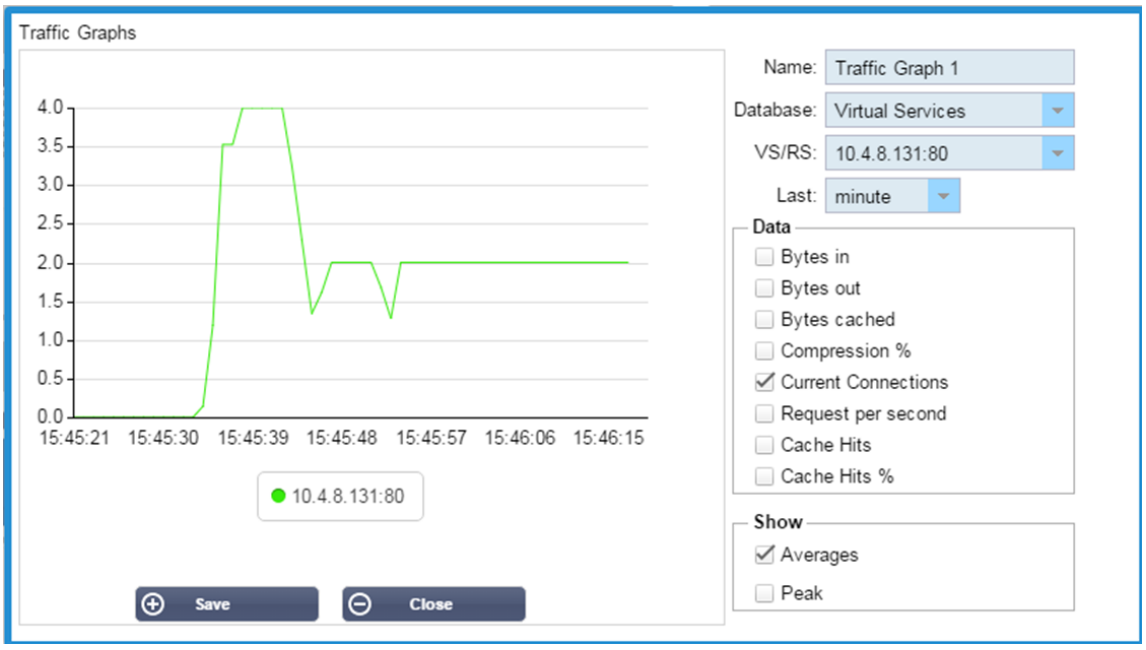
このウィジェットは、仮想サービスやリアルサーバーごとの現在および過去のトラフィックデータを表示するように設定できます。さらに、グローバルトラフィックの全体的な現在および過去のデータを表示することもできます。



- 追加ボタンをクリック
- ウィジェットに名前をつけてください。

- Virtual Services」、「Real Servers」、「System」からデータベースを選択します。
- Virtual Services」を選択した場合は、「VS/RS」ドロップダウンから仮想サービスを選択できます。
- Last」のドロップダウンから期間を選択します。
    - 分-最後の60秒
    - Hour - 過去60分間の各分のデータを集約したもの
    - Day - 過去24時間の各時間帯のデータを集約したもの
    - 週 - 過去7日間の各日のデータを集計
    - 月 - 過去7日間の各週のデータを集約したもの
    - 年 - 過去12ヶ月間の各月のデータを集計
- 選択したデータベースに応じて、利用可能なデータを選択します。
    - バーチャルサービスデータベース
    - のバイト数
    - バイトアウト
    - キャッシュされたバイト数
    - 圧縮率
    - 現在の接続
    - 1秒あたりのリクエスト数
    - キャッシュヒット
    - キャッシュヒット率
- リアルサーバー
    - のバイト数
    - バイトアウト
    - 現在の接続
    - リクエスト・パー・セカンド
    - 応答時間
- システム
    - CPUの割合
    - サービス CPU
    - メモリ容量
    - ディスクの空き容量
    - のバイト数
    - バイトアウト
- 平均値とピーク値のどちらを表示するかを選択
- すべてのオプションを選択したら、「保存して閉じる」をクリックします。

トラフィックグラフの例



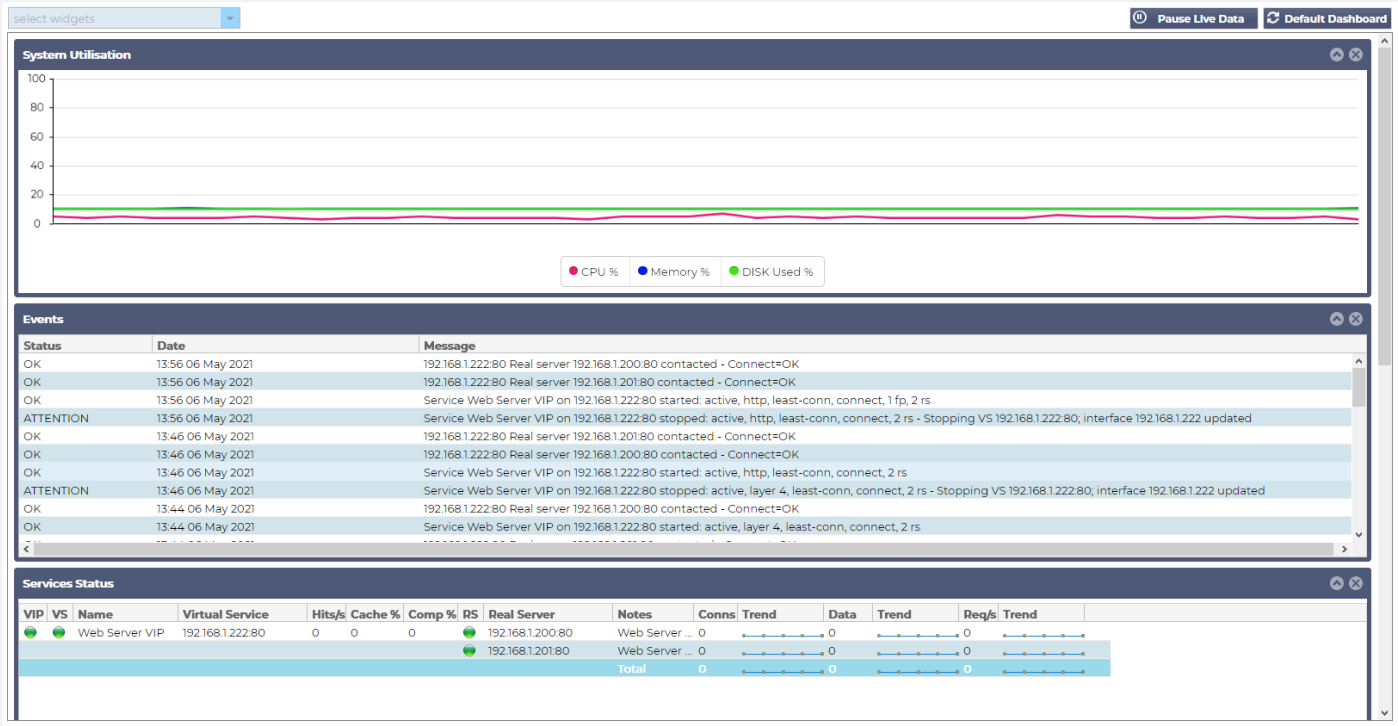
トラフィックグラフのウィジェットを「表示」→「ダッシュボード」に追加できるようになりました。

ビュー

ダッシュボード

他のITシステム管理インターフェースと同様に、ADCが扱っているパフォーマンス指標やデータを見る必要がある場合が多々あります。私たちはカスタマイズ可能なダッシュボードを提供し、簡単かつ有意義な方法でこれを行うことができます。

ダッシュボードは、ナビゲーターパネルの「表示」セグメントを使ってアクセスできます。選択すると、いくつかのデフォルトのウィジェットが表示され、自分で定義したカスタマイズしたウィジェットを選択することができます。



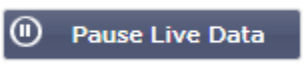
ダッシュボードの使用状況

ダッシュボードUIには、「ウィジェットメニュー」、「一時停止/再生ボタン」、「デフォルトダッシュボードボタン」の4つの要素があります。

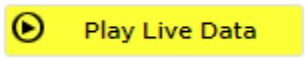
ウィジェットメニュー

ダッシュボードの左上にある「ウィジェット」メニューでは、あなたが定義した標準またはカスタマイズされたウィジェットを選択して追加することができます。これを使用するには、ドロップダウンからウィジェットを選択します。

ライブデータ一時停止ボタン



このボタンは、ADCがダッシュボードをリアルタイムで更新するかどうかを選択することができます。一時停止すると、ダッシュボード・ウィジェットは更新されないので、自由にコンテンツを検討することができます。一時停止が開始されると、ボタンの状態はPlay Live Dataの表示に変わります。



終わったら、Play Live Dataボタンをクリックするだけで、データ収集が再開され、ダッシュボードが更新されます。

デフォルトのダッシュボードボタン

ダッシュボードのレイアウトをデフォルトに戻したいことがあるかもしれません。そのような場合には、「Default Dashboard」ボタンを押してください。一度クリックすると、ダッシュボードに加えた変更はすべて失われます。

ウィジェットのサイズ変更、最小化、並び替え、削除

ウィジェットのサイズ変更

ウィジェットのサイズ変更はとても簡単です。ウィジェットのタイトルバーをクリックしたまま、ダッシュボードエリアの左右にドラッグしてください。すると、新しいウィジェットのサイズを表す点線の長方形が表示されます。矩形内にウィジェットをドロップし、マウスボタンを離します。サイズ変更したウィジェットを以前にサイズ変更したウィジェットの横にドロップしたい場合は、横にドロップしたいウィジェットの隣に矩形が表示されます。

ウィジェットの最小化

ウィジェットのタイトルバーをクリックすると、いつでもウィジェットを最小化することができます。この操作により、ウィジェットが最小化され、タイトルバーのみが表示されます。

ウィジェットの移動順序

ウィジェットを移動させるには、タイトルバーをクリックしたままマウスを動かすことで、ドラッグ＆ドロップが可能です。

ウィジェットの削除

ウィジェットのタイトルバーのアイコン⊗をクリックすると、削除することができます。

歴史

ナビゲーターから選択可能な「履歴」オプションにより、管理者はADCの過去のパフォーマンスを調べることができます。履歴の表示は、仮想サービス、リアルサーバー、およびシステムについて作成できます。

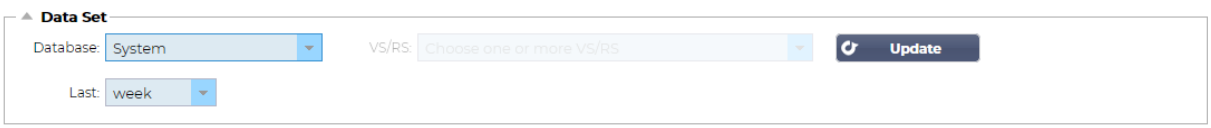
また、ロードバランシングの動作を確認することができ、調査が必要なエラーやパターンの発見に役立ちます。なお、この機能を利用するには、「システム」→「履歴」で履歴ログを有効にする必要があります。

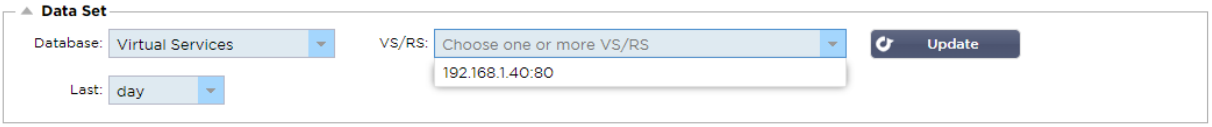
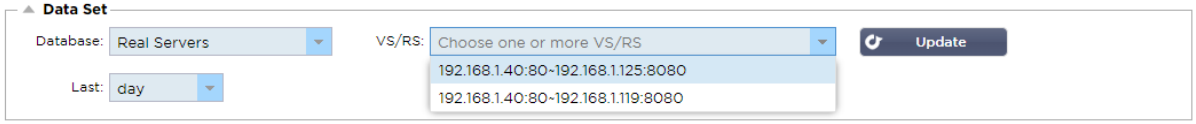
グラフィカルなデータの表示

データセット

過去のデータをグラフィカルに表示するには、以下の手順で行います。

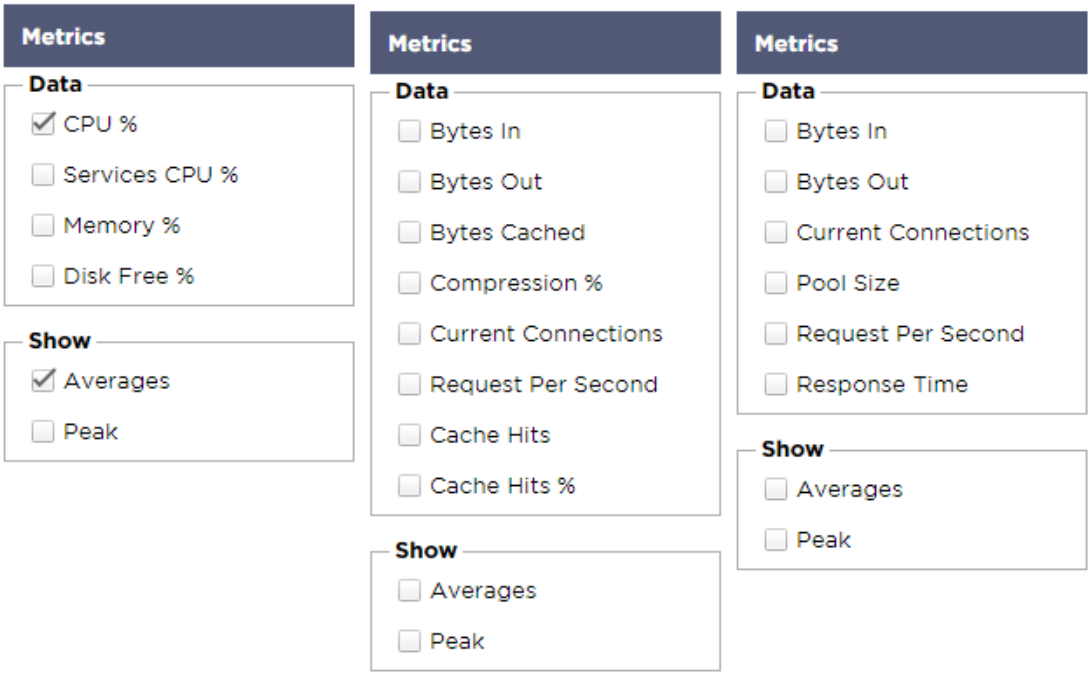
最初のステップは、表示したい情報に関連するデータベースと期間を選択することです。最後」のドロップダウンから選択できる期間は、「分」「時間」「日」「週」「月」「年」です。

データベース	説明
システム	このデータベースを選択すると、CPU、メモリ、ディスクドライブの容量を時系列で確認することができます。 

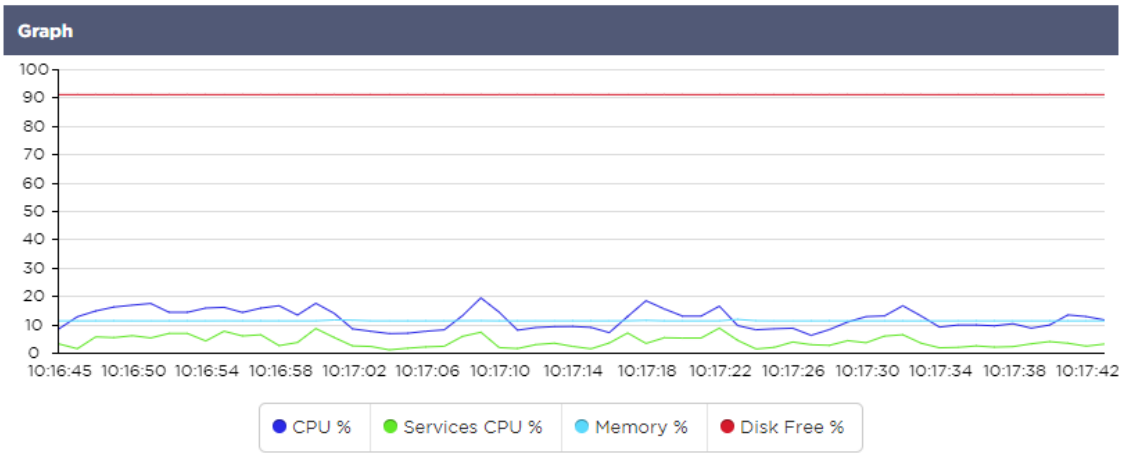
バーチャルサービス	このデータベースを選択すると、データのロギングを開始したときからデータベース内のすべてのバーチャルサービスを選択することができます。バーチャルサービスの一覧が表示されますので、そこから選択してください。 
リアルサービス	このデータベースを選択すると、データのロギングを開始した時点からデータベース内のすべてのリアルサーバーを選択することができます。リアルサーバーの一覧が表示されますので、そこから選択してください。 

メトリクス

使用するデータセットを選択したら、次は表示するメトリクスを選択します。下の図は、管理者が選択できるメトリクスを示しています。これらの選択は、左からSystem、Virtual services、Real Serversに対応しています。



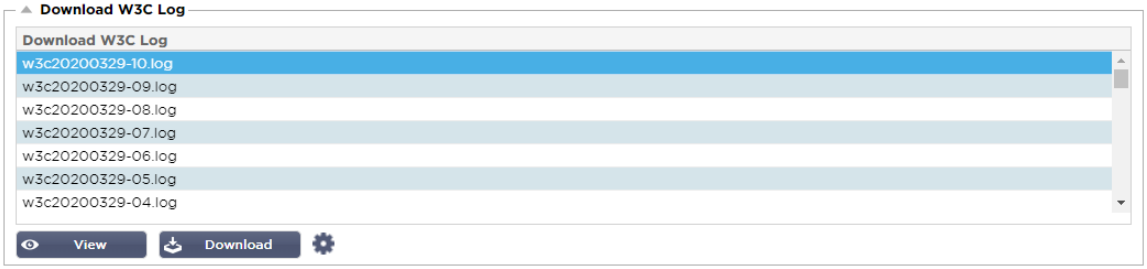
サンプルグラフ



ログ

View」セクションの「Logs」ページでは、W3CおよびSystemのログをプレビューおよびダウンロードすることができます。このページは、以下の2つのセクションで構成されています。

W3Cログのダウンロード



W3Cログは、「システム」→「ロギング」セクションで有効になります。W3Cログとは、Webサーバーのアクセスログのことで、アクセスリクエストごとに、送信元のIPアドレス、HTTPバージョン、ブラウザの種類、参照元ページ、タイムスタンプなどのデータをテキストファイルとして生成するものです。W3Cのログは、記録されるデータ量やログの種類によって、非常に大きなサイズになることがあります。

W3Cのセクションから、必要なログを選択して、表示またはダウンロードすることができます。

ボタンを見る

表示」ボタンをクリックすると、選択したログをメモ帳などのテキストエディターウィンドウで表示することができます。

ダウンロードボタン

このボタンを押すと、ログをローカルストレージにダウンロードして後で見ることができます。

コグアイコン

このアイコンをクリックすると、「システム」→「ロギング」にある「W3Cログ設定」セクションに移動します。この設定については、本ガイドの「ログ」の項で詳しく説明します。

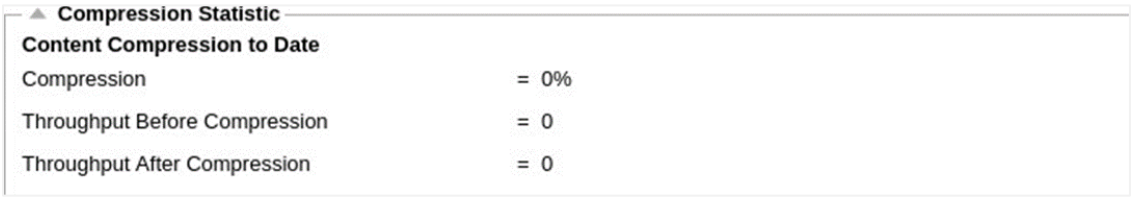
統計情報

ADCのStatisticsセクションは、ADCのパフォーマンスが期待通りであることを確認したいシステム管理者が多く利用するエリアです。

圧縮

ADCの目的は、データを監視し、データを受信するように設定されたリアルサーバーにデータを送ることです。圧縮機能は、ADCのパフォーマンスを向上させるためにADCに搭載されています。管理者は、ADCのデータ圧縮情報をテストして確認したい場合があります。このデータは、「統計」の「圧縮」パネルで提供されます。

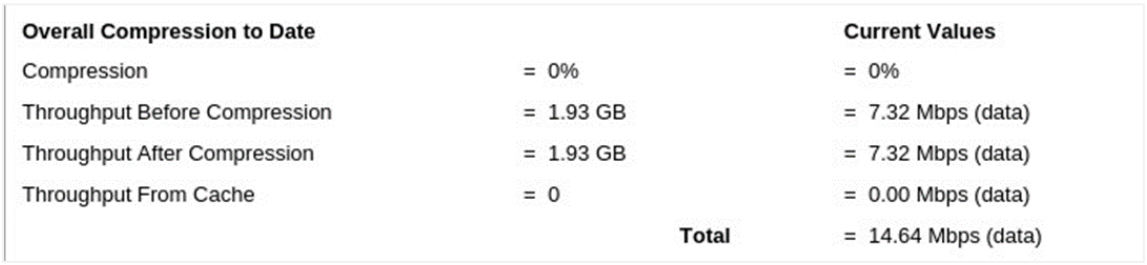
これまでのコンテンツ圧縮



Compression Statistic	
Content Compression to Date	
Compression	= 0%
Throughput Before Compression	= 0
Throughput After Compression	= 0

このセクションのデータは、圧縮可能なコンテンツに対してADCが達成した圧縮レベルの詳細を示している。60〜80%の値は、一般的な圧縮率と考えられます。

これまでの総合的な圧縮



Overall Compression to Date			Current Values
Compression	= 0%		= 0%
Throughput Before Compression	= 1.93 GB		= 7.32 Mbps (data)
Throughput After Compression	= 1.93 GB		= 7.32 Mbps (data)
Throughput From Cache	= 0		= 0.00 Mbps (data)
		Total	= 14.64 Mbps (data)

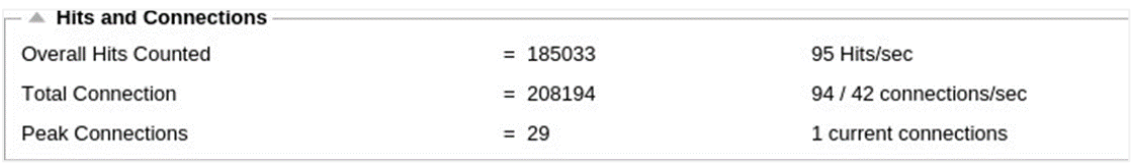
このセクションで提供される値は、ADCがすべてのコンテンツでどれだけの圧縮を達成したかを報告します。一般的な圧縮率は、サービスに含まれる事前に圧縮された画像の数に依存します。画像の数が多ければ多いほど、全体の圧縮率は小さくなる可能性があります。

トータルインプット/アウトプット

Total Input	= 2.13 GB	Input/s	= 9.10 Mbps
Total Output	= 2.18 GB	Output/s	= 9.24 Mbps

合計入出力の数値は、ADCに出入りする生データの量を表しています。kbps、Mbps、Gbpsとサイズが大きくなるにつれ、測定単位も変わってきます。

ヒットとつながり



Hits and Connections		
Overall Hits Counted	= 185033	95 Hits/sec
Total Connection	= 208194	94 / 42 connections/sec
Peak Connections	= 29	1 current connections

ヒット数と接続数」には、ADCを通過したヒット数とトランザクション数の全体的な統計情報が含まれています。では、ヒット数と接続数は何を意味するのでしょうか？

- ヒットとは、レイヤー7のトランザクションとして定義されます。一般的にはウェブサーバーで使用され、画像などのオブジェクトに対するGETリクエストです。
- コネクションとは、レイヤ4のTCPコネクションのことです。1つのTCPコネクションで多くのトランザクションが発生します。

全体のヒット数

このセクション内の数字は、前回のリセット以降のキャッシュされていないヒット数の累積を示しています。右側には、現在の1秒あたりのヒット数が表示されます。

総接続数

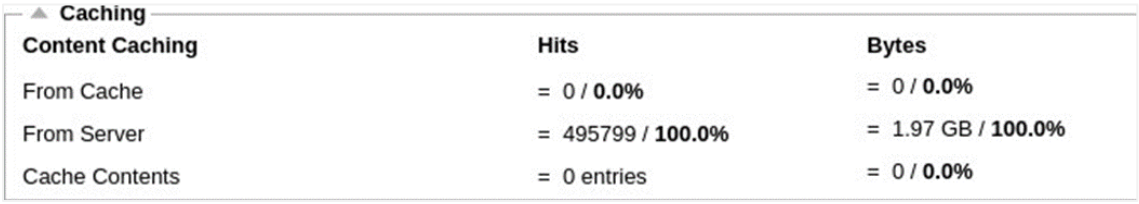
合計接続数」の数値は、前回のリセット以降のTCP接続の累積数を表しています。2列目の数字は、ADCへの1秒あたりのTCP接続数を示しています。右側の列の数値は、リアルサーバーに対して1秒あたりに行われるTCP接続数です。例 6/8 コネクション/秒。図の例では、Virtual Serviceへの1秒あたりのTCP接続数が6本、Real Serversへの1秒あたりのTCP接続数が6本です。

ピーク時の接続

Connectionsのピーク値は、ADCに対して行われたTCP接続の最大数を示します。右端の列の数字は、現在のアクティブなTCPコネクションの数を示します。

キャッシング

ご存知のように、ADCは圧縮とキャッシングの両方を備えています。このセクションでは、チャネルにキャッシングが適用されている場合の、キャッシングに関連する全体的な統計を示します。キャッシングがチャンネルに適用されておらず、正しく設定されていない場合は、キャッシュコンテンツが0と表示されます。



キャッシュから

ヒット数です。最初の列には、前回のリセット以降にADCキャッシュから提供されたトランザクションの総数が表示されます。総トランザクション数に対する割合も表示されます。

バイトです。2列目は、ADCキャッシュから提供されたデータの総量をキロバイト単位で示しています。また、総データ量に対する割合も表示されます。

サーバから

ヒット数です。1列目は、前回のリセット以降にリアルサーバーから提供されたトランザクションの総数を示しています。総トランザクション数に対する割合も表示されます。

バイトです。2列目は、リアルサーバーから提供されたデータの総量をキロバイト単位で示しています。また、総データ量に対する割合も表示されます。

キャッシュの内容

ヒット数です。この数字は、ADCキャッシュに含まれるオブジェクトの総数を示しています。

バイトです。最初の数字は、ADCのキャッシュオブジェクトの全体的なサイズをメガバイトで表しています。また、最大キャッシュサイズに対する割合も表示されます。

ハードウェア

ADCを仮想環境で使用している場合でも、ハードウェア内で使用している場合でも、このセクションでは、アプライアンスのパフォーマンスに関する貴重な情報を提供します。

Hardware

Disk Usage	= 22%
Memory Usage	= 18.9%(277.5MB of 1465.1MB)
CPU Usage	= 11.0%

ディスク使用量

2列目に記載されている値は、現在使用されているディスク容量の割合を示しており、ストレージに定期的に保存されるログファイルやキャッシュデータの情報も含まれています。

メモリ使用量

2列目は、現在使用されているメモリの割合を示しています。括弧内のより重要な数字は、ADCに割り当てられているメモリの合計量です。ADCには、最低2GBのRAMを割り当てることを推奨します。

CPU使用率

提供される重要な値の1つは、ADCが現在使用しているCPUの割合です。この値が変動するのは当然のことです。

ステータス

表示」→「ステータス」ページでは、定義した仮想サービスのADCを通過するライブトラフィックを表示します。また、各リアルサーバーへの接続数やデータも表示されるので、リアルタイムでロードバランシングを体験することができます。

バーチャルサービスの詳細

Virtual Service Details

VIP	VS	Name	Virtual Service	Hits/s	Cache %	Comp %	RS	Real Server	Notes	Conns	Data	Req/s	Pool
●	●	VIP1	192.168.1.248:80	23	0	0	●	192.168.1.7:80		2	4.19Mb	23	0
●	●	VS2	192.168.1.251:80	40	0	0	●	192.168.1.21:80	VS2 Serv...	0	7.40Mb	40	200
●	●	VIP2	192.168.1.254:80	0	0	0	●	192.168.1.21:80	VIP2 Serv...	0	0	0	0
			ALB-X Total	63	0	0				0	11.60Mb	63	200

VIPコラム

ライトの色は、1つまたは複数の仮想サービスに関連付けられた仮想IPアドレスの状態を示しています。

ステータス	説明
●	オンライン
●	フェイルオーバー・スタンバイ。この仮想サービスは、ホットスタンドバイ

●	"パッシブ "が "アクティブ "のために我慢していることを示す。
●	オフラインです。リアルサーバに到達できない、またはリアルサーバが有効になっていない
●	発見状況
●	ライセンスされていない、またはライセンスされた仮想IPを超える

VSステータス欄

ライトの色は、バーチャルサービスの状態を示します。

ステータス	説明
●	オンライン
●	フェイルオーバー・スタンバイ。この仮想サービスは、ホットスタンドバイ
●	"パッシブ "が "アクティブ "のために我慢していることを示す。
●	サービスに注意が必要です。このステータス表示は、リアルサーバーがヘルスモニターに失敗した場合や、手動で「オフライン」に変更された場合に発生します。トラフィックは継続して流れますが、リアルサーバーの容量は減少します。
●	オフラインです。リアルサーバに到達できない、またはリアルサーバが有効になっていない
●	発見状況
●	ライセンスされていない、またはライセンスされた仮想IPを超える

名前

バーチャルサービスの名前

バーチャルサービス（VIP

サービスの仮想IPアドレスとポート、ユーザーやアプリケーションが使用するアドレス。

Hit/Sec

クライアント側では1秒間に7回のトランザクションが発生します。

キャッシュ

ここでは、ADCのRAMキャッシュから提供されたオブジェクトの割合を示しています。

圧縮率

この数値は、クライアントとADCの間で圧縮されたオブジェクトの割合を表しています。

RSステータス（リモートサーバー

以下の表は、VIPに接続されているリアルサーバーのステータスの意味をまとめたものです。

ステータス	説明
●	コネクテッド
●	モニターなし
●	ドレインまたはオフライン
●	スタンバイ
●	接続されていない
●	発見状況
●	ライセンスされていない、またはライセンスされた仮想IPを超える

リアルサーバー

リアルサーバーのIPアドレスとポートです。

備考

この値には、エントリーの目的を他の人に理解してもらうための役立つメモを入れることができます。

Conns（コネクション

各 Real Server への接続数を表すことで、ロードバランシングの動作を確認することができます。ロードバランシングのポリシーが正しく機能しているかどうかを確認するのに非常に役立ちます。

データ

この欄の値は、各リアルサーバーに送信されているデータ量を示しています。

Req/Sec (1秒あたりのリクエスト数)

各リアルサーバーに送られる1秒あたりのリクエスト数。

システム

ADC のユーザー・インターフェースの System セグメントでは、ADC のシステム全体にアクセスして制御することができます。

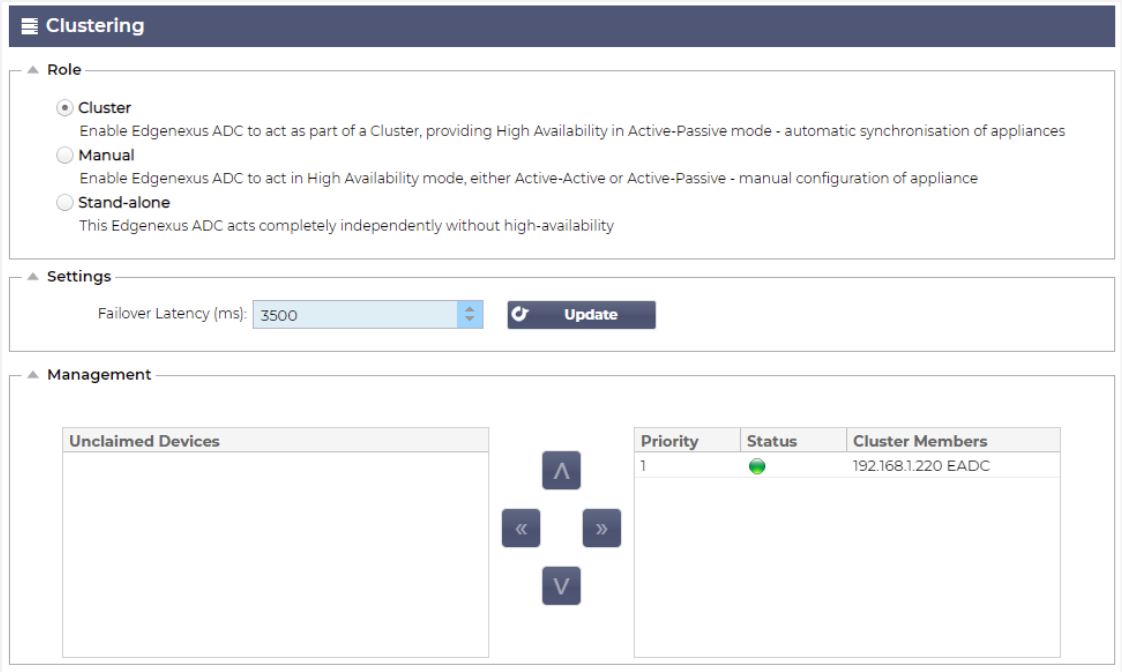
クラスタリング

ADCは単独で使用することもできますし、それはそれで問題ありません。しかし、ADCの目的がサーバー群の負荷分散であることを考えると、ADC自体をクラスター化する必要性が見えてくる。ADCの簡単に操作できるUIデザインにより、クラスタリングシステムの設定が簡単にできます。

System > Clustering ページでは、ADC アプライアンスの高可用性を設定します。このセクションはいくつかのセクションに分かれています。

重要なお知らせ

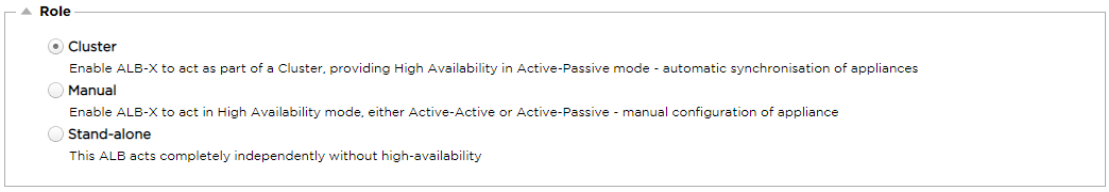
- 高稼働率のハートビートを維持するために、ADCペアの間に専用ケーブルを敷設する必要はありません。
- ハートビートは、高可用性を必要とする仮想サービスと同じネットワーク上で行われます。
- ADCアプライアンス間のステートフルなフェイルオーバーはありません。
- 2台以上のADCでハイアベイラビリティーを有効にすると、各ボックスは提供するように設定された仮想サービスをUDP経由でブロードキャストします。
- 高可用性フェイルオーバーでは、ユニキャストメッセージングとGratuitous ARPを使用して、新しいActive Load Balancerスイッチに通知します。



役割

ADCを高可用に設定する場合、3つのクラスターの役割があります。

クラスター



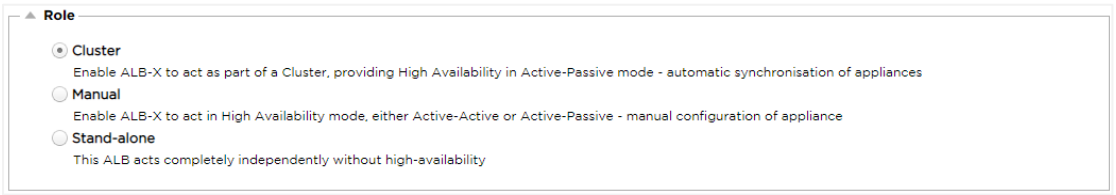
- デフォルトでは、新しいADCはClusterロールを使用して電源を入れます。この役割では、各クラスター・メンバーは同じ「作業構成」を持ち、その結果、クラスター内の1つのADCのみが常にアクティブになります。
- 作業用コンフィグレーション」とは、管理用IPアドレス、ALB Name、ネットワーク設定、インターフェースの詳細など、一意に設定する必要がある項目を除く、すべてのコンフィグレーションパラメータを意味します。
- Cluster Members」ボックスの「Priority 1」（最上位）にあるADCは、クラスタオーナーであり、アクティブなロードバランサーであり、他のADCはすべてパッシブメンバーです。
- クラスター内の任意のADCを編集することができ、変更内容はすべてのクラスターメンバーに同期されます。
- ADCをクラスタから削除すると、そのADCからすべての仮想サービスが削除されます。
- クラスタの最後のメンバーを「未使用のデバイス」に削除することはできません。最後のメンバーを削除するには、ロールをManualまたはStand-aloneに変更してください。
- 以下のオブジェクトは同期されていません。
    - マニュアル日付と時刻のセクション - (NTPセクションが同期されます)
    - フェイルオーバー・レイテンシー（ms
    - ハードウェアセクション
    - アプライアンスセクション
    - ネットワーク部門

クラスターオーナーの故障

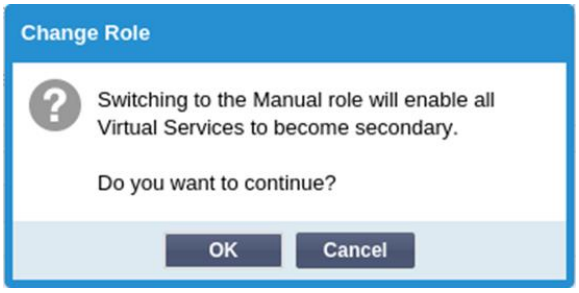
- クラスターのオーナーに障害が発生した場合、残りのメンバーの1つが自動的に引き継いで、トラフィックの負荷分散を行います。
- クラスタのオーナーが戻ってくると、トラフィックのロードバランシングを再開し、オーナーの役割を引き継ぎます。
- オーナーが失敗して、メンバーがロードバランシングを引き継いだとします。ロードバランシングのトラフィックを引き継いだメンバーを新しいオーナーにしたい場合は、そのメンバーをハイライトして上矢印をクリックし、優先順位1の位置に移動させます。
- 残りのクラスターメンバーの1つを編集し、オーナーがダウンした場合、編集されたメンバーは、トラフィックを失うことなく自動的にオーナーに昇格します

クラスターロールからマニュアルロールへの変更

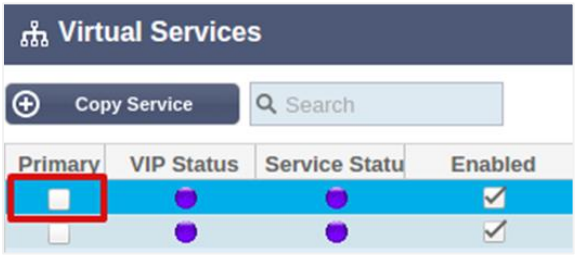
- 役割をClusterからManualに変更したい場合は、Manual roleオプションの横にあるラジオボタンをクリックします



- ラジオボタンをクリックすると、次のようなメッセージが表示されます。



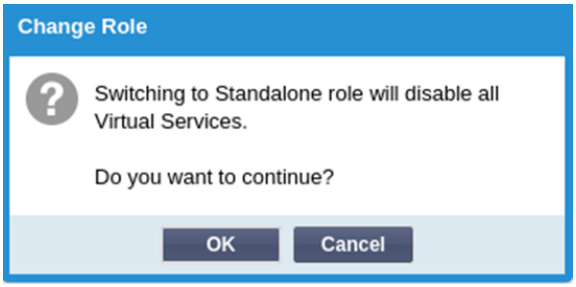
- OKボタンをクリック
- Virtual Services "セクションを確認します。プライマリ」の欄にチェックの入っていないボックスが表示されているのがわかります。



- これは安全機能であり、同じ仮想サービスを持つ別のADCがあったとしても、トラフィックフローが中断されることはありません。

クラスターからスタンドアローンへの役割変更

- クラスターからスタンドアロンに変更したい場合は、「スタンドアロン」オプションの横にあるラジオボタンをクリックしてください。
- 次のようなメッセージが表示されます。



- OK」をクリックすると、ロールが変更されます。
- バーチャルサービスを確認します。プライマリカラムの名前がスタンドアロンに変更されているのがわかります。
- また、安全上の理由から、すべての仮想サービスが無効になっている（チェックが入っていない）ことも確認できます。
- 同じネットワーク上の他のADCに重複した仮想サービスがないことが確認できたら、それぞれの仮想サービスを順番に有効にします。

マニュアルの役割

ManualロールのADCは、Manualロールの他のADCと連携して高可用性を実現します。クラスタ役割に対する主な利点は、仮想IPに対してどのADCをアクティブにするかを設定できることです。不利な点は、ADC間で設定の同期が行われないことです。すべての変更は、GUIを介して各ボックスに手動で複製する必要

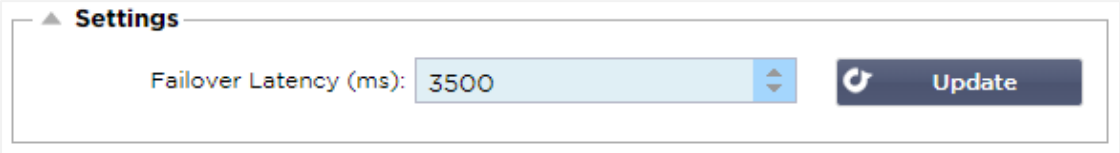
があります。また、多くの変更を行う場合は、一方のADCからjetPACKを作成し、これをもう一方のADCに送信することができます。

- バーチャルIPアドレスを "アクティブ "にするには、プライマリカラムのチェックボックスにチェックを入れます（「IPサービス」ページ）。
- バーチャルIPアドレスを "パッシブ "にするには、プライマリカラムのチェックボックスを空白にします（IPサービスページ）。
- イベントでは、ActiveサービスがPassiveにフェイルオーバーします。
    - プライマリー欄が両方ともチェックされている場合は、選択プロセスが行われ、最も低いMACアドレスがアクティブになります。
    - 両方ともチェックされていない場合は、同じ選挙プロセスが行われます。また、両方ともチェックされていない場合、元のActive ADCに自動的にフォールバックすることはありません。

単体での役割

スタンドアロン」のADCは、そのサービスに関して他のADCと通信しないため、すべてのバーチャルサービスは「グリーン」の状態で接続されたままとなります。すべての仮想サービスに固有のIPアドレスを持たせないと、ネットワーク上で衝突が発生します。

設定

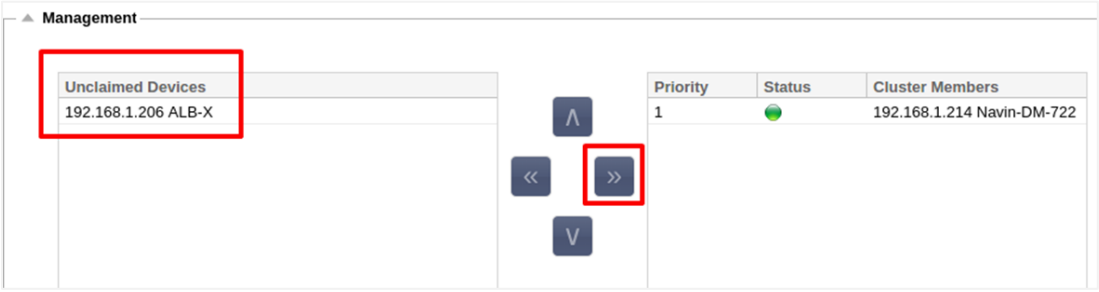


設定」セクションでは、「フェイルオーバー・レイテンシー」をミリ秒単位で設定できます。これは、「アクティブADC」が故障した後、「パッシブADC」が仮想サービスを引き継ぐまでに待つ時間です。

10000msまたは10秒に設定することをお勧めしますが、お客様のネットワークや要件に合わせて、この値を減らしたり増やしたりすることができます。許容できる値は1500msから20000msの間です。低いレイテンシーでクラスターが不安定になる場合は、この値を大きくしてください。

マネジメント

このセクションでは、クラスターメンバーの追加と削除、およびクラスター内のADCの優先順位の変更を行います。このセクションは2つのパネルと、その間にある矢印キーで構成されています。左側のエリアがUnclaimed Devicesで、右端のエリアがCluster自体です。

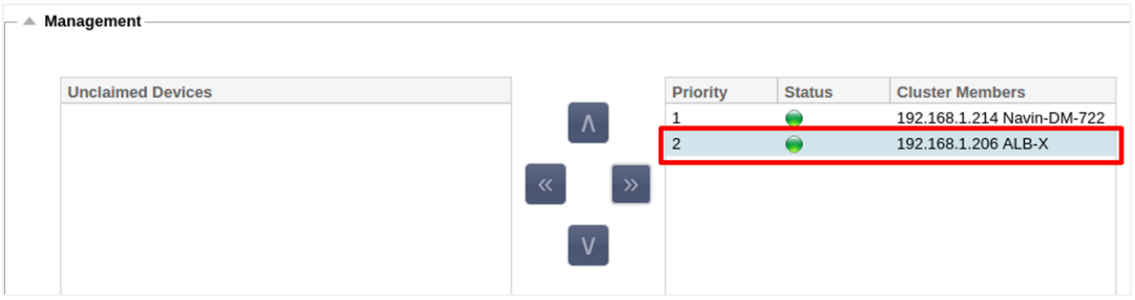


クラスターへのADCの追加

- ADCをクラスターに追加する前に、すべてのADCアプライアンスに、「System」>「Network」セクションで固有の名前セットが提供されていることを確認する必要があります。

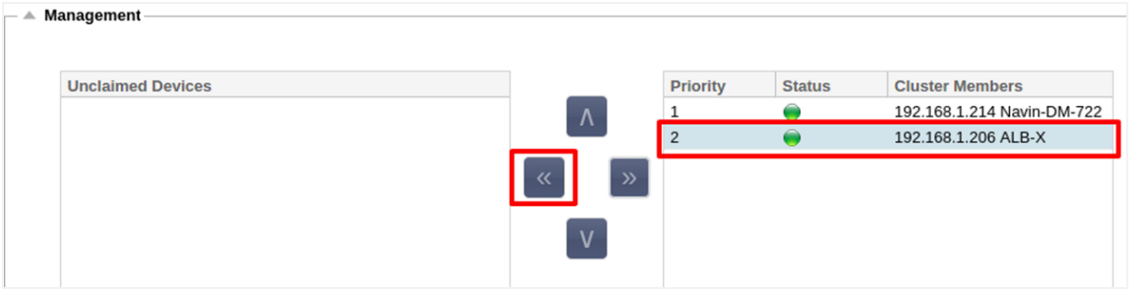
- 管理セクションの［Cluster Members］列に、優先度1でステータスが緑色のADCとその名前が表示されているはずです。このADCは、デフォルトのプライマリアプライアンスです。
- 他のすべての利用可能なADCは、管理セクションの［Unclaimed Devices］ウィンドウに表示されます。要求されていないデバイス」とは、クラスタロールに割り当てられているものの、仮想サービスが設定されていないADCのことです。
- Unclaimed Devices "ウィンドウでADCをハイライト表示し、右矢印ボタンをクリックします。
- 以下のメッセージが表示されます。

- OK」をクリックすると、ADCがクラスターに昇格します。
- これで、ADCがクラスタ・メンバー・リストにPriority 2として表示されるはずです。



クラスターメンバーの削除

- クラスタから削除するクラスタ・メンバをハイライト表示します。
- 左矢印ボタンをクリックします。



- 確認リクエストが表示されます。
- OK」をクリックして確認します。
- あなたのADCは削除され、「未請求のデバイス」側に表示されます。

ADCの優先順位変更

メンバーリスト内のADCの優先順位を変更したい場合があります。

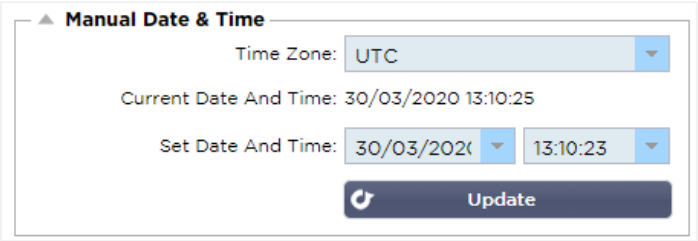
- クラスタ・メンバ・リストの最上位にあるADCには優先度1が与えられ、すべての仮想サービスのActive ADCとなります。
- リストの2番目に位置するADCには優先度2が与えられ、すべての仮想サービスのパッシブADCとなる

- どのADCをアクティブにするかを変更するには、ADCをハイライトし、リストの一番上に表示されるまで上矢印をクリックします。

日付と時刻

日付と時刻のセクションでは、ADCが置かれているタイムゾーンを含む、ADCの日付/時刻の特性を設定することができます。日付と時刻は、タイムゾーンとともに、SSL暗号化に関連する暗号化処理に重要な役割を果たします。

マニュアル 日付と時刻



タイムゾーン

このフィールドに設定した値は、ADCが設置されているタイムゾーンを表します。

- タイムゾーンのドロップダウンボックスをクリックして、位置情報を入力します。
  例えば、ロンドン
- 入力を始めると、ADCは自動的にLの文字を含む場所を表示します。
- 引き続き「Lon」と入力していくと、「Lon」を含む場所が絞り込まれていきます。'
- あなたが例えばロンドンにいるなら、「ヨーロッパ/ロンドン」を選択して位置情報を設定します。

上記の変更を行っても日付と時刻が正しくない場合は、手動で日付を変更してください。

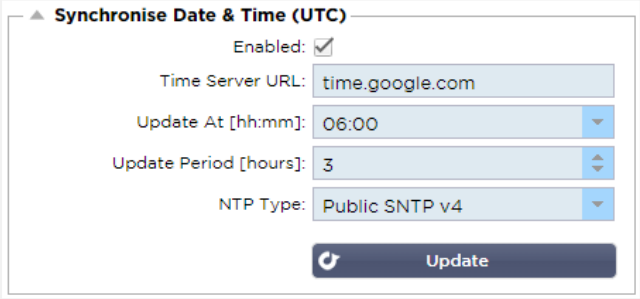
日付と時刻の設定

この設定は、実際の日付と時刻を表しています。

- 最初のドロップダウンから正しい日付を選択します。
  または、以下の形式で日付を入力することもできます。 DD/MM/YYYY
- 例えば、午前6時10秒の場合は06:00:10のように、hh: mm: ssの形式で時間を入れます。
- 正しく入力したら、「更新」をクリックして応募してください。
- そうすると、新しい日付と時刻が太字で表示されます。

日付と時刻の同期（UTC

NTPサーバーを使って、日付と時刻を正確に同期させることができます。NTPサーバーは世界中に設置されていますが、インフラで外部からのアクセスに制限がある場合は、独自の内部NTPサーバーを持つこともできます。



タイムサーバーのURL

NTPサーバーの有効なIPアドレスまたは完全修飾ドメイン名（FQDN）を入力してください。サーバーがインターネット上のグローバルに配置されたサーバーである場合は、FQDNの使用を推奨します。

hh:mm]で更新

ADCをNTPサーバーと同期させるスケジュール時間を選択します。

更新期間[時間]。

同期を取る頻度を選択します。

NTPタイプ。

- パブリックSNTP V4 - NTPサーバーと同期する際には、この方法が現在の優先的な方法です。**RFC 5905**
- NTP v1 Over TCP - TCP上のレガシーNTPバージョン。**RFC 1059**
- NTP v1 Over UDP - レガシーの NTP バージョンを UDP で提供します。**RFC 1059**

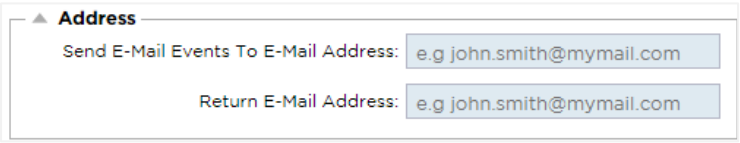
注：同期はUTCのみですのでご注意ください。ローカルタイムを設定したい場合は、手動でのみ行うことができます。この制限は、後のバージョンでタイムゾーンを選択できるように変更される予定です。

イベントメール

ADCは重要な機器であり、他の重要なシステムと同様に、注意が必要な問題をシステム管理者に通知する機能を備えています。

System > Email Events」ページでは、メールサーバーの接続を設定し、システム管理者に通知を送信することができます。このページは以下のセクションに分かれています。

アドレス



Eメールへの送信 イベントをEメールアドレスに送信

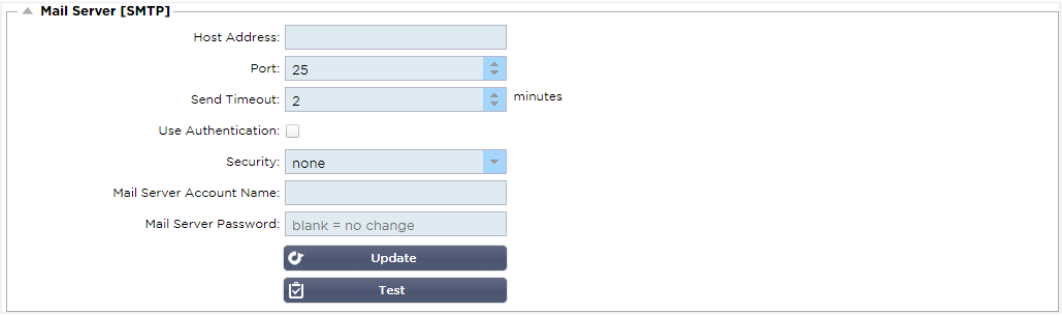
アラート、通知、イベントの送信先となる有効なEメールアドレスを追加します。例 **SUPPORT@DOMAIN.COM**。

返信用Eメールアドレス。

受信箱に表示されるメールアドレスを入れてください。例 **ADC@DOMAIN.COM**。

メールサーバー（SMTP

このセクションでは、電子メールの送信に使用するSMTPサーバーの詳細を入力する必要があります。送信に使用するメールアドレスが許可されていることを確認してください。



ホストアドレス

SMTPサーバーのIPアドレスを入れてください。

ポート

SMTPサーバーのPortを入力してください。SMTPのデフォルトのポートは25で、SSLを使用する場合は587です。

送信タイムアウト

SMTPタイムアウトを追加します。デフォルトでは2分に設定されています。

認証の使用

お使いのSMTPサーバーで認証が必要な場合は、チェックを入れてください。

セキュリティ

- なし
- 初期設定は「なし」です。
- SSL - SMTPサーバーがSecure Sockets Layer認証を必要とする場合、この設定を使用します。
- TLS - SMTPサーバーがTransport Layer Security認証を必要とする場合、この設定を使用します。

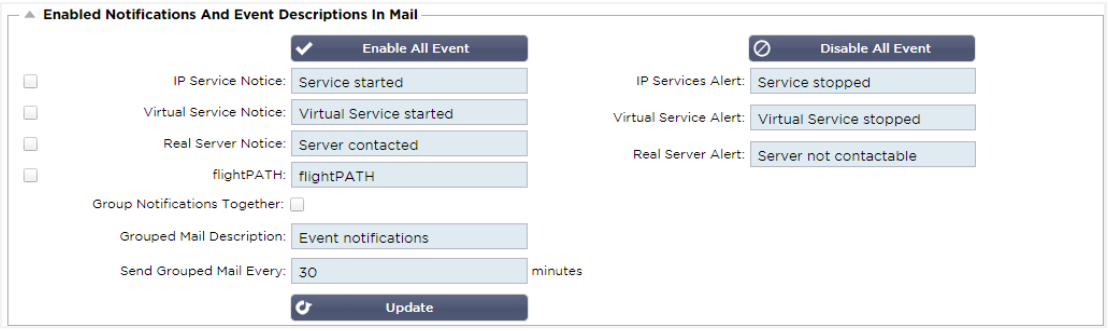
メインサーバーのアカウント名

認証に必要なユーザー名を入れます。

メールサーバーのパスワード

認証に必要なパスワードを入れてください。

通知とアラート



ADCが受信設定された人に送信するイベント通知には、いくつかの種類があります。送信すべき通知やアラートにチェックを入れて有効にすることができます。通知は、Realサーバーに接続されたときやチャンネルが開始されたときに発生します。アラートは、Realサーバーに接続できなかったり、チャンネルが停止したりしたときに発生します。

IPサービス

IPサービス通知は、任意のバーチャルIPアドレスがオンラインになったとき、または動作が停止したときに通知します。この動作は、VIPに属するすべてのバーチャルサービスに対して実行されます。

バーチャルサービス

受信者に、バーチャルサービスがオンラインになったこと、または動作が停止したことを通知します。

リアルサーバー

Real SeverとPortが接続されている場合、または連絡が取れない場合、ADCはReal Server通知を送信する。

フライトパス

この通知は、ある条件を満たしたときに送られるメールで、ADCにイベントのメールを指示するアクションが設定されています。

グループ通知

通知をグループ化するためにチェックを入れます。これにチェックを入れると、すべての通知やアラートが1つのメールに集約されます。

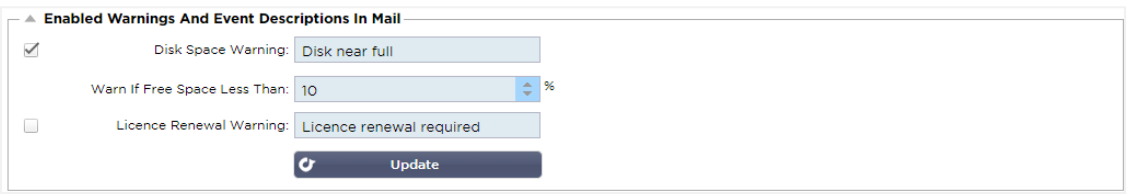
グループメールの説明

グループ通知メールの件名を指定します。

グループ送信間隔

グループ通知メールを送信するまでの待ち時間を指定します。最小時間は2分です。

注意事項



警告メールには2種類ありますが、どちらも無視してはいけません。

ディスク容量

警告を送信する前に、ディスクの空き容量の割合を設定します。これに達すると、メールが送信されます。

ライセンスの有効期限

この設定では、システム管理者に送信されるライセンス期限切れ警告メールを有効または無効にすることができます。これに達すると、メールが送信されます。

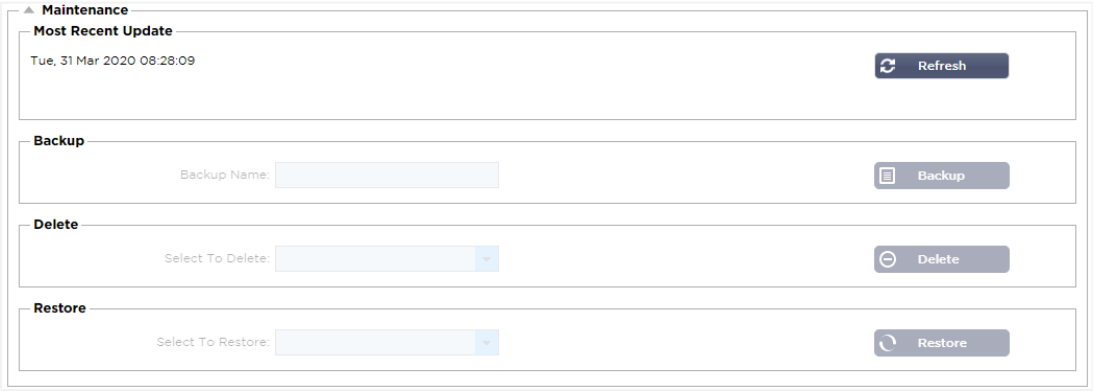
システム履歴

システム」セクションには、「システム履歴」オプションがあり、CPU、メモリー、1秒あたりのリクエスト数などの履歴データを配信することができます。このオプションを有効にすると、[表示] > [履歴] ページで結果をグラフィカルに表示できます。このページでは、履歴ファイルをローカルのADCにバックアップまたはリストアすることもできます。

データの収集

- データの収集を有効にする場合は、チェックボックスにチェックを入れてください。
- 次に、ADCにデータを収集させたい時間間隔を設定します。この時間値は、1～60秒の範囲で設定できます。

メンテナンス



履歴ログを有効にしている場合、このセクションはグレーアウトされます。Collect Data "セクションの "Enabled "チェックボックスをオフにして、"Update "をクリックすると、履歴ログのメンテナンスが可能になります。

バックアップ

バックアップにはわかりやすい名前をつけます。バックアップをクリックすると、すべてのファイルがADCにバックアップされます。

削除

ドロップダウンリストからバックアップファイルを選択します。ADCからバックアップファイルを削除するには、［削除］をクリックします。

リストア

以前に保存したバックアップファイルを選択します。復元」をクリックすると、このバックアップファイルからデータが入力されます。

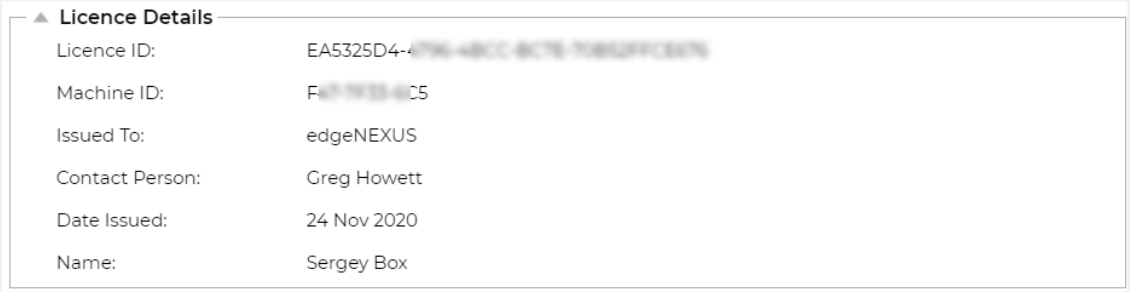
ライセンス

ADCは、お客様の購入条件やお客様のタイプに応じて、以下のいずれかのモデルを使用してライセンスされます。

ライセンスタイプ	説明
パーペチュアル	お客様は、ADCおよびその他のソフトウェアを永続的に使用する権利を有しています。また、サポートやアップデートを受けるために、サポートを購入することを妨げるものではありません。
SaaS	SaaS（Software-as-a-Service）とは、基本的にソフトウェアを継続的または従量制でレンタルすることを意味します。このモデルでは、ソフトウェアの年間レンタル料を支払います。ソフトウェアを使用する永久的な権利はありません。
MSP	マネージド・サービス・プロバイダーは、ADCをサービスとして提供し、VIP単位でライセンスを購入し、毎年課金・支払いを行うことができます。

ライセンスの詳細

各ライセンスには、購入する個人または組織に関連した特定の詳細が含まれています。



ライセンスID

このライセンスIDは、お客様が購入したADCに固有のマシンIDなどと直接リンクしています。この情報は必須で、App Storeからアップデートなどを取得する際に必要となります。

マシンID

マシン ID は、仮想 ADC アプライアンスの eth0 IP アドレスと、ハードウェアベースの ADC の MAC ID を使って生成されます。仮想ADCアプライアンスのIPアドレスを変更した場合、ライセンスは無効になります。その場合は、サポートにお問い合わせください。仮想ADCアプライアンスのIPアドレスは固定し、変更しないように指示することをお勧めします。テクニカルサポートは、HTTPs://edgenexus.ioでチケットを発行してご利用いただけます。

注：ADCアプライアンスのIPアドレスやMAC IDを変更してはいけません。仮想化されたフレームワークを使用している場合は、MAC IDとIPアドレスを修正してください。

発行先

この値は、ADCのマシンIDに関連付けられた購入者の名前を含みます。

コンタクトパーソン

この値には、マシンIDに関連付けられているお客様の会社の連絡先が含まれます。

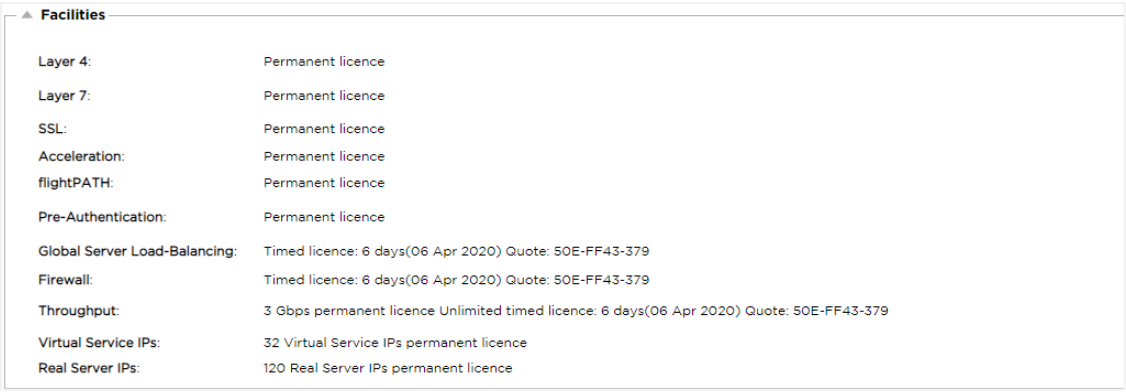
日付の問題

ライセンスが発行された日

名前

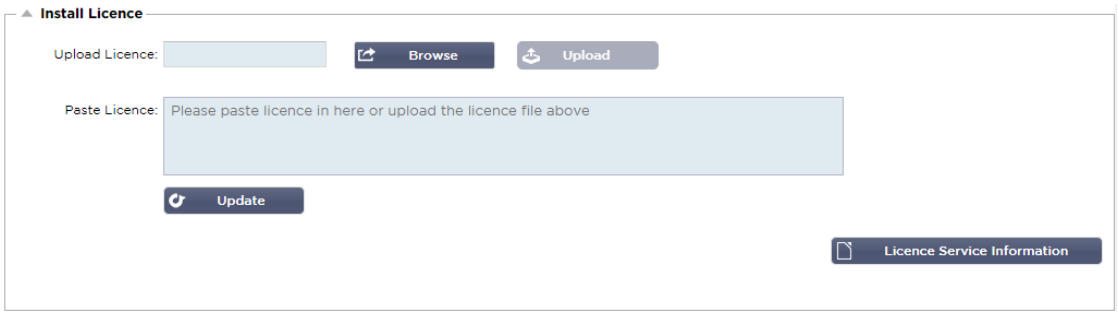
この値は、あなたが提供したADCアプライアンスの記述的な名前を示しています。

設備紹介



設備セクションでは、ADC内のどの機能が使用許諾されているか、またライセンスの有効性についての情報を提供します。また、ADCにライセンスされているスループットと、リアルサーバーの数も表示されます。この情報は、お客様が購入されたライセンスによって異なります。

ライセンスのインストール



- 新しいライセンスのインストールはとても簡単です。Edgenexusから新規または交換用のライセンスが届くと、テキストファイルの形で送られてきます。そのファイルを開き、内容をコピーして「Paste License」フィールドに貼り付けることができます。
- コピー・ペーストができない場合は、ADCにアップロードすることもできます。
- 更新ボタンをクリックしてください。
- これでライセンスがインストールされました。

ライセンスサービス情報

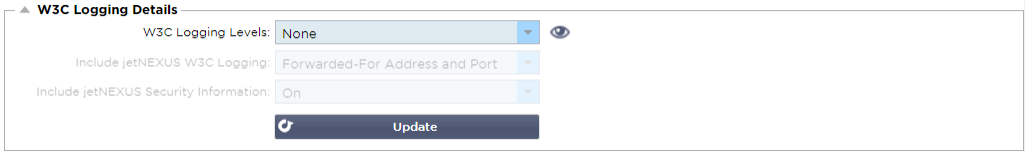
ライセンスサービス情報」ボタンをクリックすると、ライセンスに関するすべての情報が表示されます。この機能は、サポート担当者に詳細を送信するために使用することができます。

ロギング

System > Logging」ページでは、W3Cのログレベルを設定したり、ログが自動的にエクスポートされるリモートサーバーを指定することができます。このページは以下の4つのセクションで構成されています。

W3Cのロギング詳細

W3Cログを有効にすると、ADCはW3C互換のログファイルの記録を開始します。W3Cログは、Webサーバーのアクセスログで、各アクセスリクエストに関するデータ（送信元IPアドレス、HTTPバージョン、ブラウザータイプ、参照元ページ、タイムスタンプなど）を含むテキストファイルが生成されます。このフォーマットは、Webの進化のための標準化を推進する団体であるW3C（World Wide Web Consortium）によって開発されました。ファイルはASCIIテキストで、列はスペースで区切られています。このファイルには、#で始まるコメント行が含まれています。このコメント行の1つは、データをマイニングできるようにフィールドを示す（列名を指定する）行である。HTTPプロトコルとFTPプロトコルのファイルがあります。



W3Cのロギングレベル

ロギングレベルが異なるため、サービスの種類によって提供されるデータが異なります。

以下の表は、W3C HTTPのログレベルについて説明したものです。

価値	説明
なし	W3Cのロギングはオフです。
ブリーフ	存在するフィールドは以下の通りです。#Fields: time c-ip c-port s-ip method uri x-c-version x-r-version sc-status cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x- round-trip-time cs(User-Agent) x-sc(Content-Type).
フル	これは、日付と時刻のフィールドが分かれている、よりプロセッサに適合したフォーマットです。各フィールドの意味については、以下のフィールド概要を参照してください。現在のフィールドは以下の通りです。#Fields: date time c-ip c-port cs-username s-ip s-port cs-method cs-uri-stem cs-ur- -query sc-status cs(User-Agent) referer x-c-version x-r-version cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x-roun-trip-time x-sc(Content-Type).
サイト	このフォーマットは「Full」とよく似ていますが、フィールドが追加されています。各フィールドの意味については、以下のフィールドの概要をご覧ください。存在するフィールドは以下の通りです。#Fields: date time x-mil c-ip c-port cs-username s-ip s-port cs-host cs-method cs-uri-stem cs-ur--query sc-status cs(User-Agent) referer x-c-version x-r-version cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x-round--trip-time x-sc(Content-Type).
診断	このフォーマットには、開発スタッフやサポートスタッフに関連する様々な情報が含まれています。各フィールドの意味については、以下のフィールド概要をご覧ください。現在あるフィールドは以下の通りです。#フィールドdate time c-ip c-port cs-username s-ip s-port x-xff x-xffcustom cs-host x-r-ip x-r-port cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent) referer x-c-version x-r-version cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x-round-trip-time x-trip-times(new,rcon,rqf,rql,tqf,tql,rsf,rsl,tsf,tsl,dis,log) x-closed-by x-compress-action x-sc(Content-Type) x-cache-action X-finish

以下の表は、W3C FTPのロギングレベルを示しています。

価値	説明
ブリーフ	#Fields: date time c-ip c-port s-ip s-port r-ip r-port cs-method cs-param sc-status sc-param sr-method sr-param rs-status rs-param
フル	#Fields: date time c-ip c-port s-ip s-port r-ip r-port cs-method cs-param cs-bytes sc-status sc-param sc-bytes sr-method sr-param sr-bytes rs-status rs-param rs-bytes
診断	#Fields: date time c-ip c-port s-ip s-port r-ip r-port cs-method cs-param cs-bytes sc-status sc-param sc-bytes sr-method sr-param sr-bytes rs-status rs-param rs-bytes

W3Cロギングを含む

このオプションでは、どのようなADC情報をW3Cログに含めるかを設定できます。

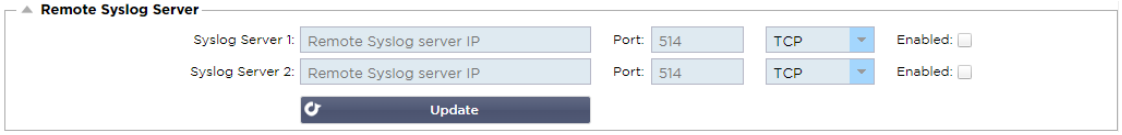
価値	説明
お客様のネットワークアドレスとポート	ここで表示される値は、実際のクライアントのIPアドレスをポートとともに表示しています。
クライアントのネットワークアドレス	このオプションは、実際のクライアントのIPアドレスを含み、それのみを表示します。
転送先のアドレスとポート	このオプションは、アドレスやポートなど、XFFヘッダーに保持されている詳細を表示します。
転送先のアドレス	このオプションは、アドレスのみを含む、XFFヘッダーに保持されている詳細を表示します。

セキュリティ情報の記載

このメニューは2つのオプションで構成されています。

価値	説明
オン	この設定はグローバルです。オンに設定すると、認証を使用している仮想サービスで W3C ログが有効になっている場合、ユーザー名が W3C ログに追加されます。
オフ	これにより、グローバルレベルでユーザー名をW3Cログに記録する機能がオフになります。

リモートSyslogサーバ



このセクションでは、すべてのシステムログを送信する2つの外部Syslogサーバーを設定することができます。

- SyslogサーバーのIPアドレスの追加
- ポートの追加
- TCPまたはUDPを選択
- ボックスにチェックを入れる
- アップデートをクリック

リモートログストレージ

W3Cのすべてのログは、1時間ごとに圧縮されてADCに保存されます。ディスクの残り容量が30%になると、最も古いファイルが削除されます。これらのファイルをリモートサーバーにエクスポートして保管したい場合は、SMB共有を使用して設定することができます。なお、W3Cのログは、ファイルが完成して圧縮されるまでリモートに転送されません。ログは1時間ごとに書き込まれるため、仮想マシンアプライアンスでは最大2時間、ハードウェアアプライアンスでは5時間かかることがあります。

今後のリリースでは、設定が正しいかどうかのフィードバックを提供するために、テストボタンを設ける予定です。

Col1	Col2
リモートログストレージ	リモートログストレージを有効にする場合はチェックを入れてください
IPアドレス	SMBサーバーのIPアドレスを指定します。ドット付き10進法で指定してください。例：10.1.1.23
シェア名	SMBサーバーの共有名を指定します。例：w3c.
ディレクトリ	SMBサーバー上のディレクトリを指定します。例/logを指定します。
ユーザー名	SMBシェアのユーザー名を指定する。
パスワード	SMB共有のパスワードを指定する

フィールドの概要

状態	説明
日付	ローカライズされていない = 常に YYYY-MM-DD (GMT/UTC)
時間	Not localised = HH:MM:SS or HH:MM:SS.ZZZ (GMT/UTC) * Not-unfortunately, this is two formats (Site
	は0.ZZZミリ秒もありません。)
X-MIL	サイト形式のみ＝タイムスタンプのミリ秒単位
C-IP	ネットワークまたはX-Forwarded-Forヘッダーから得られる可能な限りのクライアントIP
Cポート	ネットワークまたはX-Forwarded-Forヘッダーから得られる可能な限りのクライアントポート
cs-username	クライアントのユーザー名のリクエストフィールド
S-IP	ALBのリスニングポート
s-port	ALBの試聴VIP
x-xff	X-Forwarded-Forヘッダーの値

x-xffcustom	Configuration-namedのX-Forwarded-Forタイプのリクエストヘッダの値
cs-host	リクエストのホスト名
x-r-ip	使用するリアルサーバーのIPアドレス
エックスアールポート	使用するリアルサーバーのポート
cs-method	HTTPリクエストメソッド * Brief形式を除く
メソッド	* cs-methodにこの名前を使うのは、ブリーフフォーマットだけです。
cs-uri-stem	リクエストされたリソースのパス * Brief形式を除く
cs-uri-query	リクエストされたリソースへの問い合わせ * Brief形式を除く
ウリ	* パスとクエリ文字列を組み合わせた短いフォーマットのログ
sc-status	HTTPレスポンスコード
cs(User-Agent)	ブラウザのUser-Agent文字列（クライアントから送られてきたもの
レフェリー	参照元ページ（クライアントから送られてきたもの
x-c-version	クライアントのリクエスト HTTPバージョン
x-r-version	Content-Server's response HTTP version
cs-bytes	リクエストに含まれる、クライアントからのバイト数
sr-bytes	リアルサーバーに転送されるバイト数、リクエストの
rs-bytes	レスポンスに含まれるリアルサーバーからのバイト数
sc-by-tes	レスポンスの中で、クライアントに送信されたバイト数
x-percent	圧縮率 * = 100 * (1 - 出力 / 入力) ヘッダを含む
時間をかけて	リアルサーバーにかかった時間（秒
X-TRIP-TIMES NEW pcon	接続してから "初心者リスト "に掲載されるまでのミリ秒 接続してからリアルサーバーへの接続が完了するまでのミリ秒
acon	接続してからリアルサーバーへの接続が完了するまでのミリ秒
rcon	接続してからリアルサーバーの接続を確立するまでのミリ秒
rqf	接続してからクライアントからの最初のバイトのリクエストを受信するまでのミリ秒
rql	接続してからクライアントからのリクエストの最後のバイトを受信するまでのミリ秒
tqf	接続してからリアルサーバーにリクエストの最初のバイトを送信するまでのミリ秒
tql	接続してからリアルサーバーにリクエストの最後のバイトを送信するまでのミリ秒
rsf	接続してからリアルサーバーからの最初のバイトのレスポンスを受信するまでのミリ秒
RSL	接続してからリアルサーバーからの最後のバイトのレスポンスを受信するまでのミリ秒
tsf	接続からクライアントへのレスポンスの最初のバイトを送信するまでのミリ秒
tsl	接続からクライアントへの応答の最後のバイトを送信するまでのミリ秒

ディス	接続から切断までのミリ秒（両サイド-最後に切断した側
ログ	接続からこのログレコードまでのミリ秒は、通常、次のように続きます。
x-round trip-time	ALBにかかった時間（秒
x-closed-by	どのようなアクションによって接続が閉じられたか（または開いたままになったか
x-compress-action	圧縮がどのように行われたか、または防止されたか
x-sc(Content-Type)	応答のContent-Type
x-cache-action	キャッシングがどのように反応したか、あるいは防止されたか
X-FINISH	このログ行の原因となったトリガー

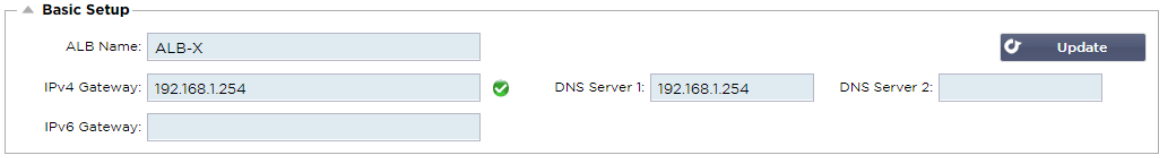
ログファイルの消去

この機能では、ADC のログファイルを消去することができます。ドロップダウンメニューから削除したいログの種類を選択して、「Clear」ボタンをクリックします。

ネットワーク

ライブラリ内の「ネットワーク」セクションでは、ADCのネットワーク・インターフェースとその動作を設定することができます。

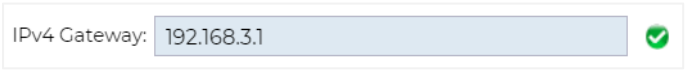
基本設定



ALB名

ADCアプライアンスの名前を指定します。クラスター内に複数のメンバーがいる場合は変更できませんのでご注意ください。クラスタリングの項をご参照ください。

IPv4ゲートウェイ



IPv4ゲートウェイアドレスを指定します。このアドレスは、既存のアダプターと同じサブネット内にある必要があります。ゲートウェイを誤って追加した場合、赤丸の中に白十字が表示されます。正しいゲートウェイを追加すると、ページの下部に緑色の成功バナーが表示され、IPアドレスの横に緑色の円の中に白いチェックマークが表示されます。

IPv6ゲートウェイ

IPv6ゲートウェイアドレスを指定します。このアドレスは、既存のアダプターと同じサブネット内にある必要があります。ゲートウェイを誤って追加した場合、赤丸の中に白十字が表示されます。正しいゲート

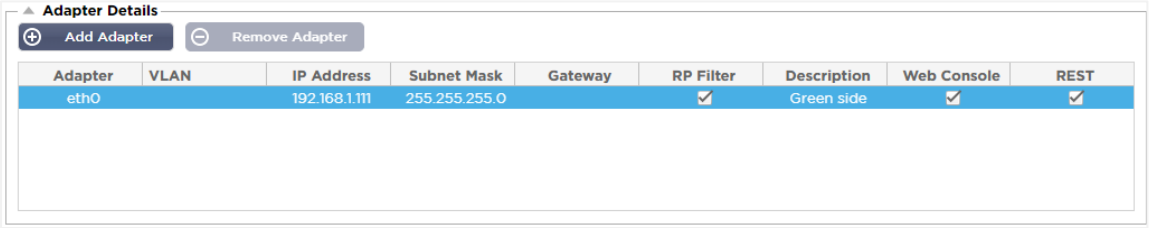
ウェイを追加すると、ページの下部に緑色の成功バナーが表示され、IPアドレスの横に緑色の円の中に白いチェックマークが表示されます。

DNSサーバー1とDNSサーバー2

1台目と2台目（オプション）のDNSサーバーのIPv4アドレスを入れます。

アダプターの詳細

ネットワークパネルのこのセクションには、ADCアプライアンスにインストールされているネットワークインターフェースが表示されます。必要に応じてアダプタを追加・削除することができます。

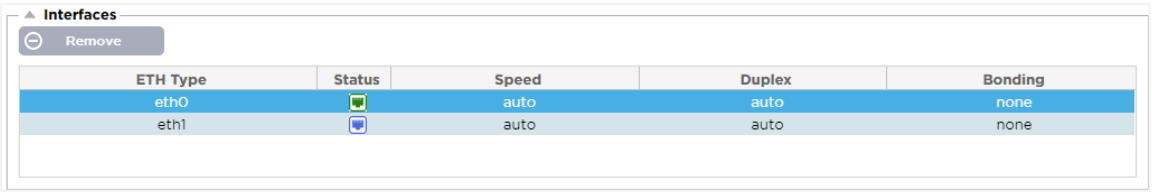


コラム	説明
アダプター	この列には、アプライアンスにインストールされている物理アダプタが表示されます。利用可能なアダプタのリストからアダプタをクリックして選択します。ダブルクリックすると、リストの行が編集モードになります。
VLAN	ダブルクリックして、アダプターのVLAN IDを追加します。VLANとは、仮想ローカルエリアネットワークのことで、個別のブロードキャストドメインを作ります。VLANは物理的なLANと同じ属性を持っていますが、同じネットワークスイッチを使用していないエンドステーションをより簡単にグループ化することができます。
IPアドレス	ダブルクリックして、アダプターのインターフェイスに関連するIPアドレスを追加します。同一のインターフェースに複数のIPアドレスを追加することができます。IPアドレスは、IPv4の32ビットの四則演算による10進数で指定します。例 192.168.101.2
サブネットマスク	ダブルクリックして、アダプター・インターフェースに割り当てられているサブネットマスクを追加します。これには、IPv4の32ビットの数値を、4つの点線付き10進法で記述します。例 255.255.255.0
ゲートウェイ	インターフェイスのゲートウェイを追加します。これを追加すると、ADCは、このインターフェイスから開始された接続が、このインターフェイスを経由して指定されたゲートウェイルーターに戻されることを許可する単純なポリシーを設定します。これにより、複雑なポリシーベースのルーティングを手動で設定することなく、より複雑なネットワーク環境にADCをインストールすることができます。
説明	ダブルクリックして、アダプターの説明を追加します。パブリックインターフェースの例。 注：ADCは、最初のインターフェースをGreen Side、2番目のインターフェースをRed Side、3番目のインターフェースをSide 3などと自動的に命名します。 これらの命名規則は、ご自由に変更してください。
ウェブコンソール	列をダブルクリックし、ボックスにチェックを入れて、グラフィカルユーザーインターフェースのWebコンソールの管理アドレスとしてインターフェースを割り当てます。Webコンソールがリッスンするインターフェイスを変更する場合は、十分に注意してください。変更後の Web コンソールに到達するためには、正しいルーティ

	ングを設定するか、新しいインターフェイスと同じサブネットにいる必要があります。これを元に戻すには、コマンドラインにアクセスしてset greensideコマンドを発行するしかありません。これにより、eth0以外のすべてのインターフェースが削除されます。

インターフェイス

ネットワークパネル内の「Interfaces」セクションでは、ネットワークインターフェースに関する特定の要素を設定することができます。また、[Remove]ボタンをクリックすると、リストからネットワークインターフェースを削除することができます。仮想アプライアンスを使用している場合、ここに表示されるインターフェースは、基盤となる仮想化フレームワークによって制限されます。



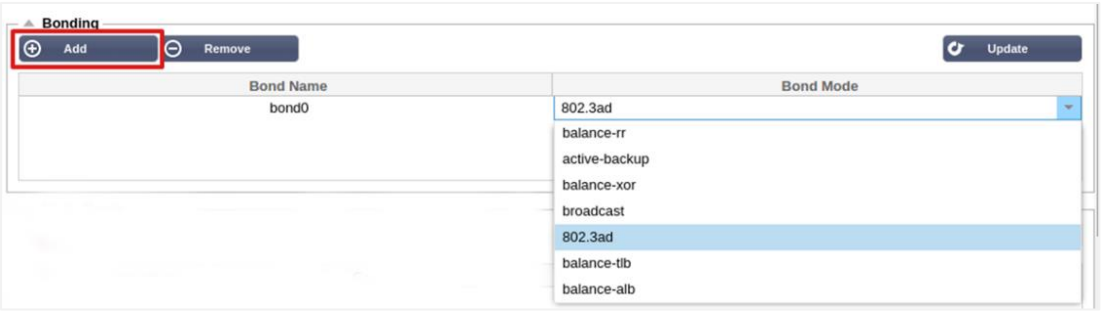
コラム	説明
ETHタイプ	この値は、ネットワークインターフェースに対するOS内部の参照を示します。このフィールドはカスタマイズできません。値はETH0から始まり、ネットワークインターフェースの数に応じて順番に続きます。
ステータス	このグラフィック表示は、ネットワークインターフェースの現在のステータスを示します。緑色のステータスは、インターフェイスが接続され、稼働していることを示します。その他のステータス表示は以下のとおりです。  **アダプターUP**  アダプターダウン  アダプターの抜き差し  アダプター欠品
スピード	デフォルトでは、この値は速度を自動ネゴシエーションするように設定されています。しかし、インターフェイスのネットワーク速度を、ドロップダウンで利用可能な任意の値に変更することができます（10/100/1000/AUTO）。
デュプレックス	このフィールドの値はカスタマイズ可能で、Auto（デフォルト）、Full-Duplex、Half-Duplexの中から選択できます。
ボンディング	定義したボンディングタイプの中から1つを選ぶことができます。詳しくは、「ボンディング」の項をご覧ください。

ボンディング

ネットワークインターフェイスボンディングのタイトルには多くの名称が使われている。ポートトランキング、チャネルボンディング、リンクアグリゲーション、NICチーミングなど。ボンディングは、複数のネットワーク接続を1つのチャネルボンディングされたインターフェースに結合または集約する。ボンディングすることで、2つ以上のネットワークインターフェースを1つのものとして動作させ、スループットを向上させ、冗長性やフェイルオーバーを実現します。

ADCのカーネルには、複数の物理的なネットワーク・インターフェースを単一の論理的なインターフェースに集約するためのボンディング・ドライバーが組み込まれています（例えば、eth0とeth1をbond0に集約するなど）。ボンディングされたインターフェースごとに、モードとリンクモニタリングのオプションを定義することができます。モードには7つのオプションがあり、それぞれ負荷分散とフォールトトレランスの特性が異なります。下の図はその例です。

注：ボンディングは、ハードウェアベースのADCアプライアンスにのみ設定できます。

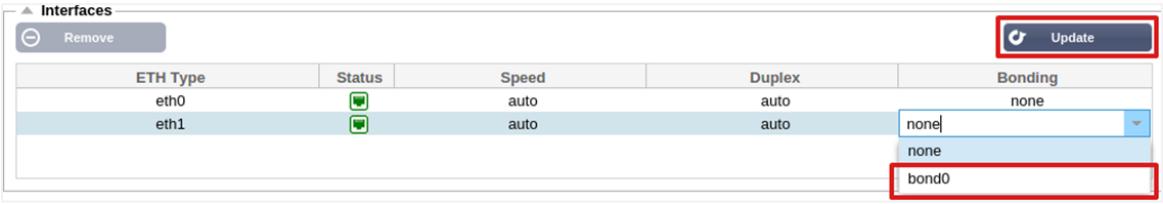


ボンディング・プロファイルの作成

- 追加ボタンをクリックすると、新しいボンドが追加されます。
- ボンディング設定の名前をつける
- どのボンディングモードを使用するかを選択

次に、「Interfaces」セクションで、ネットワーク・インターフェースの「Bond」ドロップダウン・フィールドから使用するボンディング・モードを選択します。

以下の例では、eth0、eth1、eth2がbond0の一部になりました。一方、eth0は管理インターフェースとして単独で残っています。



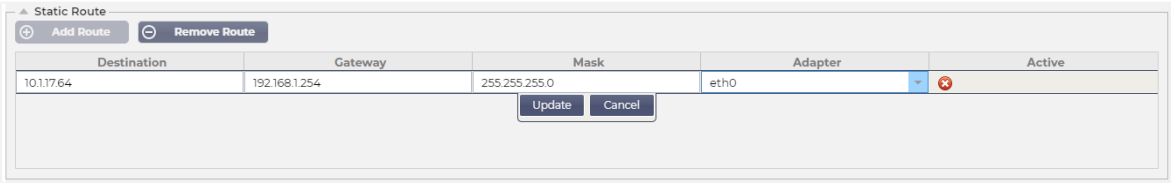
ボンディング・モード

ボンディングモード	説明
balance-rr:	パケットは、各インターフェイスを1つずつ順番に送受信します。
アクティブ・バックアップ。	このモードでは、1つのインターフェースがアクティブになり、2つ目のインターフェースはスタンバイ状態になります。このセカンダリーインターフェースは、1つ目のインターフェースのアクティブな接続が失敗した場合にのみアクティブになります。
balance-xor。	送信元のMACアドレスと送信先のMACアドレスをXORして送信します。このオプションでは、各宛先MACアドレスに対して同じスレーブが選択されます。
を放送しました。	このモードでは、すべてのスレーブインターフェースですべてのデータを送信します。

802.3adです。	802.3ad仕様に基づき、アクティブアグリゲーター内のすべてのスレーブを利用し、同じ速度とデュプレックス設定を共有するアグリゲーショングループを作成します。
balance-tlb:	アダプティブ・トランスミッション・ロードバランシング・ボンディング・モード。特別なスイッチのサポートを必要としないチャネルボンディングを提供します。発信トラフィックは、各スレーブの現在の負荷（速度に対して計算される）に応じて分配されます。現在のスレーブが着信トラフィックを受信します。受信スレーブが故障した場合は、別のスレーブが故障した受信スレーブのMACアドレスを引き継ぎます。
balance-alb:	アダプティブロードバランシングボンディングモード：balance-tlbに加え、IPV4トラフィックのための受信ロードバランシング（RLB）も含まれており、特別なスイッチのサポートは必要ありません。受信負荷分散はARPネゴシエーションによって実現されます。ボンディングドライバーは、ローカルシステムから送信されるARP Repliesを途中でインターセプトし、ソースハードウェアアドレスをボンド内のスレーブの1つのユニークなハードウェアアドレスで上書きすることで、異なるピアがサーバーに異なるハードウェアアドレスを使用するようにします。

静的ルート

ネットワーク内の特定のサブネットに対してスタティック・ルートを作成する必要がある場合があります。ADCでは、Static Routesモジュールを使ってこれを行うことができます。



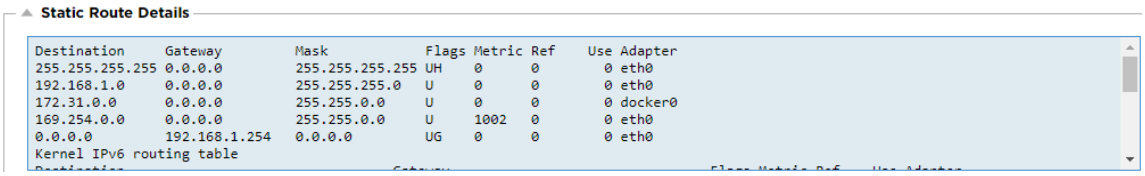
スタティックルートの追加

- Add Route」ボタンをクリックします。
- 下表の内容を参考にして記入してください。
- アップデート」ボタンをクリックしてください。

フィールド	説明
目的地	送信先のネットワークアドレスを10進数のドット表記で入力します。例 123.123.123.5
ゲートウェイ	ゲートウェイのIPv4アドレスを10進数のドット表記で入力します。例 10.4.8.1
マスク	送信先のサブネットマスクを10進数のドット記法で入力します。例 255.255.255.0
アダプター	ゲートウェイに到達できるアダプターを入力します。例 eth1.
アクティブ	緑のチェックボックスは、ゲートウェイに到達できることを示します。赤色の十字は、そのインターフェイスではゲートウェイに到達できないことを示します。ゲートウェイと同じネットワーク上にインターフェースとIPアドレスが設定されていることを確認してください。

スタティック・ルートの詳細

このセクションでは、ADCに設定されているすべてのルートについての情報を提供します。



高度なネットワーク設定

ナグルとは？

Nagleのアルゴリズムは、ネットワーク上で送信する必要のあるパケットの数を減らすことで、TCP/IPネットワークの効率を向上させるものである。**NAGLEに関するウィキペディアの記事**を見る

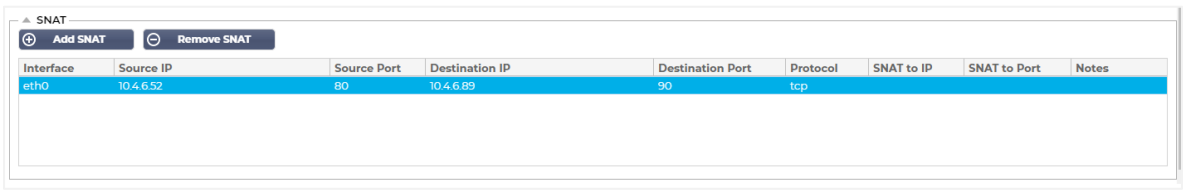
サーバーNagle

このボックスにチェックを入れると、Server Nagleの設定が有効になります。Server Nagleは、ネットワーク上で送信する必要のあるパケットの数を減らすことで、TCP/IPネットワークの効率を向上させる手段です。この設定はサーバー側のトランザクションに適用されます。NagleやACKの遅延はパフォーマンスに重大な影響を与えるため、サーバーの設定には注意が必要です。

クライアントNagle

Client Nagle の設定を有効にするには、このボックスにチェックを入れます。上記と同様ですが、クライアント側のトランザクションに適用されます。

SNAT



SNATとはSource Network Address Translationの略で、ベンダーによってSNATの実装に若干の違いがあります。EdgeADCのSNATを簡単に説明すると以下のようになります。

通常の場合、インバウンドのリクエストは、リクエストのソースIPを見ることができるVIPに向けられます。例えば、ブラウザのエンドポイントのIPアドレスが81.71.61.51であった場合、これがVIPに表示されます。

SNATが有効な場合、リクエストの元のソースIPはVIPから隠され、代わりにSNATルールで指定されたIPアドレスが表示されます。SNATは、レイヤ4およびレイヤ7のロードバランシングモードで使用できます。

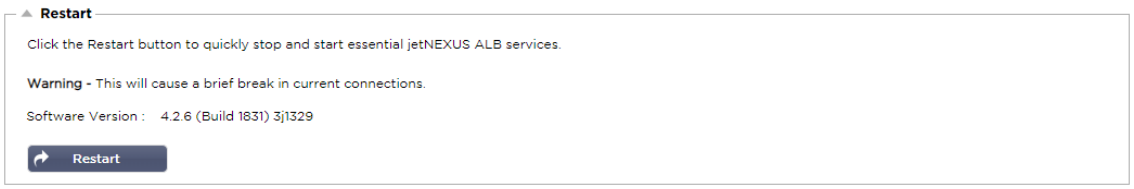
フィールド	説明
ソースIP	送信元IPアドレスはオプションで、ネットワークIPアドレス（/mask付き）またはプレーンIPアドレスのいずれかを指定できます。マスクには、ネットワークマスク、またはネットワークマスクの左端にある1の数を指定するプレーンな数字を指定できます。したがって、/24のマスクは、255.255.255.0に相当します。

送信先IP	宛先IPアドレスは任意で、ネットワークIPアドレス（/mask付き）またはプレーンIPアドレスのいずれかを指定します。マスクは、ネットワークマスク、またはネットワークマスクの左端にある1の数を指定するプレーンな数字のいずれかです。したがって、/24のマスクは、255.255.255.0に相当します。
ソースポート	ソースポートはオプションで、1つの数字で、そのポートだけを指定することもできますし、コロンを含めて、ポートの範囲を指定することもできます。例を挙げます。80 または 5900:5905。
デスティネーションポート	デスティネーションポートは任意であり、1つの数字で、そのポートのみを指定することも、コロンを含んでポートの範囲を指定することもできます。例を挙げます。80 または 5900:5905。
プロトコル	SNATを単一のプロトコルで使用するか、すべてのプロトコルで使用するかを選択できます。より正確にするためには、特定することをお勧めします。
SNATからIPへ	SNAT to IPには、必須のIPアドレスまたはIPアドレスの範囲を指定します。例を示します。10.0.0.1または10.0.0.1-10.0.0.3。
SNAT→ポート	SNAT to Portはオプションで、1つの数字で、そのポートのみを指定することも、ダッシュを含んでポートの範囲を指定することもできます。例80」または「5900～5905」。
備考	ルールが存在する理由を思い出すために、親しみやすい名前を付けるために使用します ;-)。これはSyslogでのデバッグにも役立ちます。

パワー

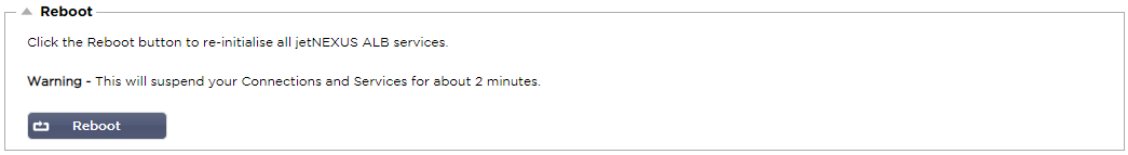
また、このADCシステムの機能により、ADC上でいくつかの電源関連の作業を行うことができます。

再起動



この設定は、すべてのサービスのグローバルな再起動を開始し、その結果、現在アクティブな接続がすべて切断されます。すべてのサービスはしばらくすると自動的に再開されますが、そのタイミングは、設定されているサービスの数によって異なります。再起動の確認を求めるポップアップが表示されます。

再起動



Reboot ボタンをクリックすると、ADC の電源を切り、自動的にアクティブな状態に戻ります。再起動操作の確認を求めるポップアップが表示されます。

電源オフ

Power Off」ボタンをクリックすると、ADCがシャットダウンされます。ハードウェアアプライアンスの場合、電源を入れるにはデバイスへの物理的なアクセスが必要です。シャットダウン操作の確認を求めるポップアップが表示されます。

セキュリティ

このセクションでは、ウェブコンソールのパスワードを変更したり、Secure Shellアクセスを有効または無効にすることができます。また、REST API機能を有効にすることもできます。

SSH

オプション	説明
Secure Shell Remote Conn	SSH を使って ADC にアクセスしたい場合は、チェックボックスにチェックを入れてください。"Putty "は、このための優れたアプリケーションです。

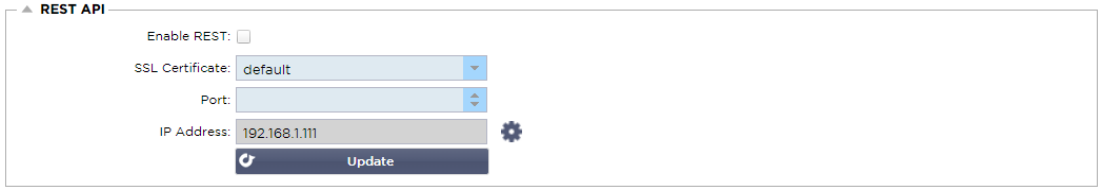
ウェブコンソール

SSL Certificate ドロップダウンリストから証明書を選択します。選択した証明書は、ADC の Web ユーザーインターフェースへの接続を保護するために使用されます。ADC内で自己署名証明書を作成するか、**SSL証明書**セクションから証明書をインポートすることができます。

オプション	説明
セキュアポート	Webコンソールのデフォルトのポートは443です。セキュリティ上の理由で別のポートを使用したい場合は、ここで変更することができます。

REST API

REST API（RESTful APIとも呼ばれます）は、RESTアーキテクチャスタイルに準拠したアプリケーションプログラミングインターフェースで、ADCの設定やADCからのデータ抽出を可能にします。RESTという言葉は、representational state transferの略で、コンピュータ科学者のRoy Fielding氏によって作られました。



オプション	説明

RESTの有効化	REST APIによるアクセスを有効にするには、このボックスにチェックを入れます。なお、どのアダプタでRESTを有効にするかを設定する必要があります。以下のCogのリンク先の注意事項を参照してください。
SSL証明書	RESTサービス用の証明書を選択します。ドロップダウンには、ADCにインストールされているすべての証明書が表示されます。
ポート	RESTサービスのPortを設定します。443以外のポートを使用することをお勧めします。
IPアドレス	これにより、RESTサービスが接続されているIPアドレスが表示されます。RESTサービスが有効になっているアダプタを変更するには、「歯車」のリンクをクリックして「ネットワーク」ページにアクセスします。
コグリンク	このリンクをクリックすると、REST用のアダプターを設定できる「ネットワーク」ページが表示されます。

REST APIのドキュメント

REST APIの使用方法に関するドキュメントは、**jetAPI | 4.2.3 | jetNEXUS | SwaggerHubです。**

注：Swaggerのページでエラーが発生する場合は、クエリ文字列のサポートに問題があるためです。エラーをスクロールして、jetNEXUS REST APIに進んでください。

例

CURLを使ったGUIDです。

- コマンド

```
curl -k HTTPs://<rest ip>/POST/32 -H "Content-Type: application/json" -X POST -d '{"<rest username>":"<password>"}'
```

- を返します。

```
{"Loginstatus": "OK", "Username":"<rest username>", "GUID":"<guid>"}。
```

- 妥当性
  - GUIDの有効期限は24時間です。

ライセンスの詳細

- コマンド

```
curl -k HTTPs://<レストip>/GET/39 -GET -b 'GUID=<guid;>'
```

SNMP

SNMPセクションでは、ADC内に存在するSNMP MIBの設定を行います。このMIBは、SNMPを搭載した機器と通信可能なサードパーティのソフトウェアによって照会することができます。

SNMP設定

オプション	説明
SNMP v1 / V2C	V1/V2C MIBを有効にする場合は、チェックボックスにチェックを入れます。SNMP v1 は、RFC-1157 に準拠しています。SNMP V2cはRFC-1901-1908に準拠しています。
SNMP v3	チェックボックスにチェックを入れて、V3 MIBを有効にします。RFC-3411-3418に準拠しています。 v3のユーザー名はadminです。 例： - snmpwalk -v3 -u admin -A jetnexus -l authNoPriv 192.168.1.11 1.3.6.1.4.1.38370
コミュニティ・ストリング	エージェントに設定され、マネージャーがSNMP情報を取得する際に使用される読み取り専用の文字列です。デフォルトのコミュニティ文字列はjetnexus
PassPhrase	これは、SNMP v3を有効にする際に必要なパスワードで、8文字以上で、Aa-Zzの文字と0-9の数字のみを含む必要があります。デフォルトのパスフレーズは**jetnexus**です。

SNMP MIB

SNMPで表示可能な情報は、MIB（Management Information Base）によって定義されます。MIBは、管理データの構造を記述し、階層的なオブジェクト識別子（OID）を使用します。各OIDは、SNMP管理アプリケーションを介して読み取ることができます。

MIBダウンロード

MIBはこちらからダウンロードできます。

ADC OID

ルートOID

iso.org.dod.internet.private.enterprise = .1.3.6.1.4.1

当社のOID

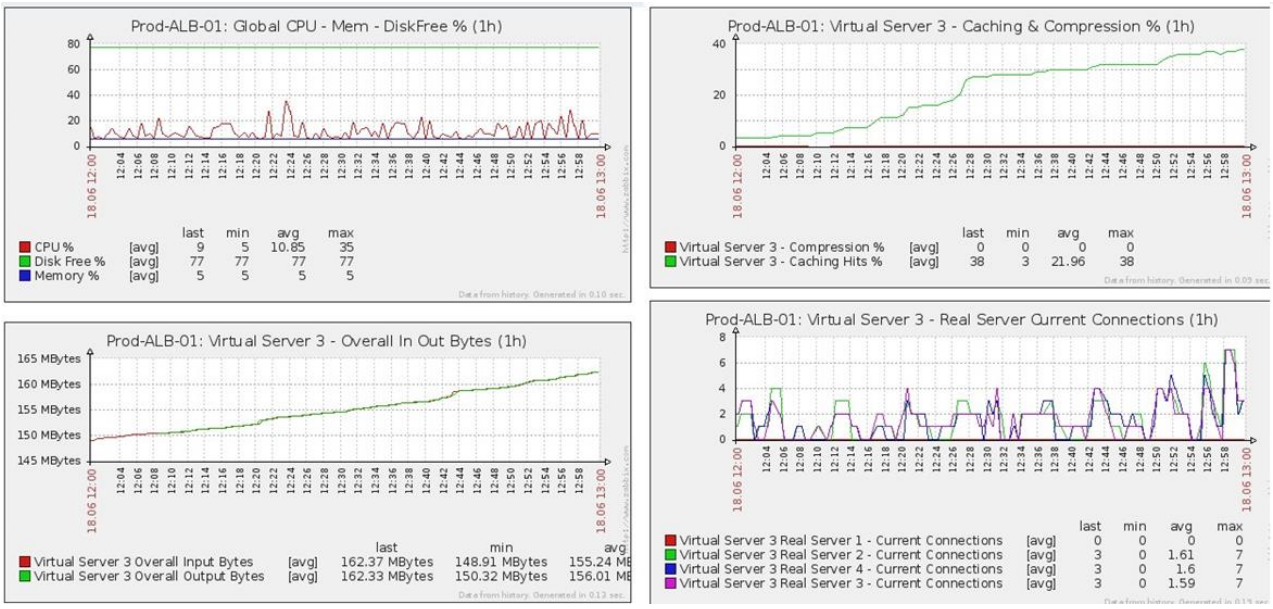
.38370 ジェットネクサスMIB
- .1 **jetnexusData** (1.3.6.1.4.1.38370.1)
  - .1 jetnexusGlobal (1.3.6.1.4.1.38370.1.1)
  - .2 **jetnexusVirtualServices** (1.3.6.1.4.1.38370.1.2)
  - .3 **jetnexusServers** (1.3.6.1.4.1.38370.1.3)
    - .1 **jetnexusGlobal** (1.3.6.1.4.1.38370.1.1)
      - .1 **jetnexusOverallInputBytes** (1.3.6.1.4.1.38370.1.1.1.0)
      - .2 **jetnexusOverallOutputBytes** (1.3.6.1.4.1.38370.1.1.2.0)
      - .3 **jetnexusCompressedInputBytes** (1.3.6.1.4.1.38370.1.1.3.0)
      - .4 **jetnexusCompressedOutputBytes** (1.3.6.1.4.1.38370.1.1.4.0)
      - .5 **jetnexusVersionInfo** (1.3.6.1.4.1.38370.1.1.5.0)
      - .6 **jetnexusTotalClientConnections** (1.3.6.1.4.1.38370.1.1.6.0)
      - .7 **jetnexusCpuPercent** (1.3.6.1.4.1.38370.1.1.7.0)
      - .8 **jetnexusDiskFreePercent** (1.3.6.1.4.1.38370.1.1.8.0)
      - .9 **jetnexusMemoryPercent** (1.3.6.1.4.1.38370.1.1.9.0)
      - .10 **jetnexusCurrentConnections** (1.3.6.1.4.1.38370.1.1.10.0)
    - .2 **jetnexusVirtualServices** (1.3.6.1.4.1.38370.1.2)
      - .1 **jnvirtualserviceEntry** (1.3.6.1.4.1.38370.1.2.1)
        - .1 **jnvirtualserviceIndexvirtualservice** (1.3.6.1.4.1.38370.1.2.1.**1**)
        - .2 **jnvirtualserviceVSAddrPort** (1.3.6.1.4.1.38370.1.2.1.**2**)
        - .3 **jnvirtualserviceOverallInputBytes** (1.3.6.1.4.1.38370.1.2.1.**3**)
        - .4 **jnvirtualserviceOverallOutputBytes** (1.3.6.1.4.1.38370.1.2.1.**4**)

.5 jnvirtualserviceCacheBytes (1.3.6.1.4.1.38370.1.2.1.5)
.6 jnvirtualserviceCompressionPercent (1.3.6.1.4.1.38370.1.2.1.6)
.7 jnvirtualservicePresentClientConnections (1.3.6.1.4.1.38370.1.2.1.7)
.8 jnvirtualserviceHitCount (1.3.6.1.4.1.38370.1.2.1.8)
.9 jnvirtualserviceCacheHits (1.3.6.1.4.1.38370.1.2.1.9)
.10 jnvirtualserviceCacheHitsPercent (1.3.6.1.4.1.38370.1.2.1.10)
.11 jnvirtualserviceVSStatus (1.3.6.1.4.1.38370.1.2.1.11)

.3 jetnexusRealServers (1.3.6.1.4.1.38370.1.3)
.1 jnrealserverEntry (1.3.6.1.4.1.38370.1.3.1)
.1 jnrealserverIndexVirtualService (1.3.6.1.4.1.38370.1.3.1.1)
.2 jnrealserverIndexRealServer (1.3.6.1.4.1.38370.1.3.1.2)
.3 jnrealserverChAddrPort (1.3.6.1.4.1.38370.1.3.1.3)
.4 jnrealserverCSAddrPort (1.3.6.1.4.1.38370.1.3.1.4)
.5 jnrealserverOverallInputBytes (1.3.6.1.4.1.38370.1.3.1.5)
.6 jnrealserverOverallOutputBytes (1.3.6.1.4.1.38370.1.3.1.6)
.7 jnrealserverCompressionPercent (1.3.6.1.4.1.38370.1.3.1.7)
.8 jnrealserverPresentClientConnections (1.3.6.1.4.1.38370.1.3.1.8)
.9 jnrealserverPoolUsage (1.3.6.1.4.1.38370.1.3.1.9)
.10 jnrealserverHitCount (1.3.6.1.4.1.38370.1.3.1.10)
.11 jnrealserverRSStatus (1.3.6.1.4.1.38370.1.3.1.11)

ヒストリカルグラフ

ADCのカスタムSNMP MIBの最も良い使い方は、履歴グラフを任意の管理コンソールにオフロードすることです。以下は、上記の様々なOID値に対してADCをポーリングするZabbixの例です。



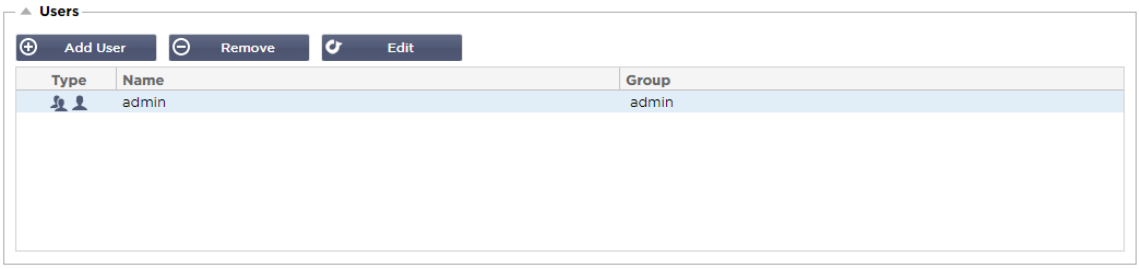
ユーザーと監査ログ

ADCは、ADCが何をするかを設定・定義するためのユーザーを内部に持つ機能を提供しています。ADC内で定義されたユーザーは、そのユーザーに割り当てられた役割に応じて、様々な操作を行うことができます。

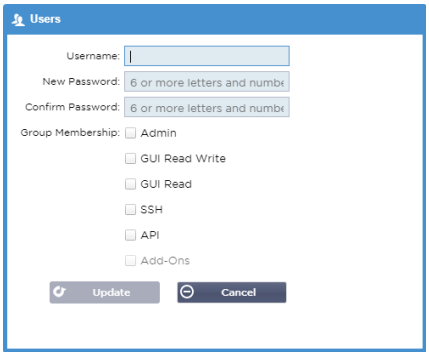
ADCを最初に設定するときに使用する**admin**というデフォルトユーザーがあります。adminのデフォルトのパスワードは**jetnexus**です。

ユーザー

ユーザー」セクションでは、ADCからユーザーを作成、編集、削除することができます。



ユーザーの追加



上の図の「Add User」ボタンをクリックすると、「Add User」ダイアログが表示されます。

パラメータ	説明・用途
ユーザー名	任意のユーザー名を入力 ユーザーネームは、以下に準拠する必要があります。 • 最小文字数 1 • 最大文字数 32 • 文字は大文字でも小文字でもOK • 数字が使われることもあります。 • シンボルマークの使用は不可
パスワード	以下の条件に適合した**強力な**パスワードを入力してください。 • 最小文字数 6 • 最大文字数 32 • 少なくともアルファベットと数字の組み合わせを使用する必要があります。 • 文字は大文字でも小文字でもOK • 以下の例にあるものを除き、記号の使用が認められています。 **£, %, & , < , >**
パスワードの確認	パスワードが正しいかどうか、もう一度確認する
グループメンバー	ユーザーを所属させたいグループにチェックを入れます。 • Admin - このグループはすべてのことができます • GUI Read Write - このグループのユーザーは、GUIにアクセスし、GUIを介して変更を行うことができます。 • GUI Read - このグループのユーザーは、GUIにアクセスして情報を閲覧することのみ可能です。変更はできません • SSH - このグループのユーザーは、Secure Shell で ADC にアクセスできます。この方法では、最低限のコマンドを備えたコマンドラインにアクセスできます。 • API - このグループのユーザーは、SOAPおよびRESTのプログラム可能なインターフェイスにアクセスできます。RESTはソフトウェアバージョン4.2.1から利用可能です。

ユーザータイプ

ローカルユーザー
Stand-AloneまたはManual H/AロールのADCは、Local Usersのみを作成します。
デフォルトでは、"admin "というローカルユーザーが*adminグループのメンバーになっています。後方互換性のため、このユーザーは決して削除できません。
このユーザーのパスワードを変更したり、削除したりすることはできますが、最後のローカル admin

クラスターユーザー
クラスタ・ロールのADCは、クラスタ・ユーザのみを作成します。
クラスタ・ユーザは、クラスタ内のすべてのADCで同期されます。
クラスタ・ユーザを変更すると、クラスタのすべてのメンバーで変更される
クラスタユーザーとしてログオンしている場合、クラスタからマニュアルまたはスタンドアロンへのロールの切り替えはできません。

クラスターとローカルユーザー
Stand-AloneまたはManualロールで作成されたユーザーはすべてクラスタにコピーされます。
ADCがクラスターから離脱した場合、ローカルユーザーのみが残る
ユーザーに最後に設定されたパスワードが有効になる

ユーザーの削除

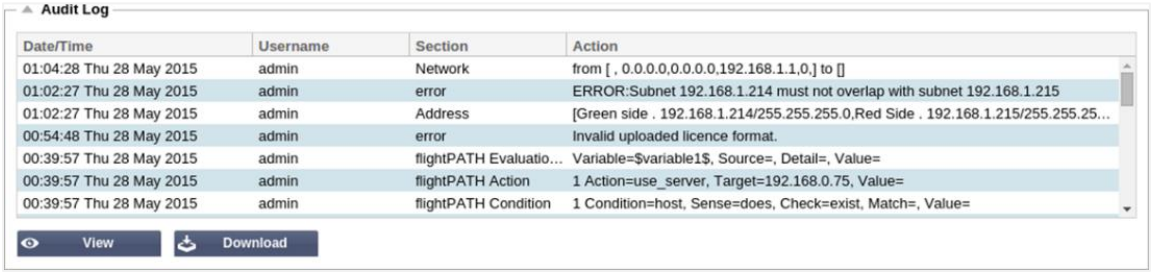
- 既存ユーザーの強調表示
- 削除」をクリックします。
- 現在、サインインしているユーザーを削除することはできません。
- adminグループの最後のローカルユーザーを削除することはできません。
- 管理者グループに最後まで残っているクラスターユーザーを削除することはできません
- 後方互換性のため、adminユーザーを削除することはできません。
- ADCをクラスターから削除すると、ローカルユーザーを除くすべてのユーザーが削除されます

ユーザーの編集

- 既存ユーザーの強調表示
- 編集」をクリックします。
- ユーザーのグループメンバーシップを変更するには、適切なボックスにチェックを入れ、更新します。
- また、管理者権限があれば、ユーザーのパスワードを変更することもできます。

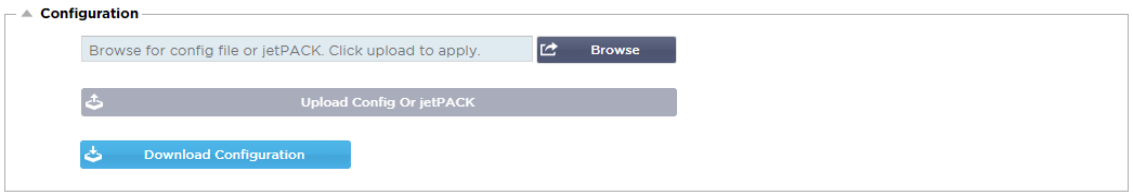
監査ログ

ADCは、個々のユーザーがADCの設定に加えた変更をログに記録します。監査ログには、すべてのユーザーが実行した最後の50のアクションが表示されます。また、[Logs]セクションにALLエントリが表示されることもあります。例えば、以下のようになります。



アドバンスド

構成



ADCが完全にセットアップされ、必要に応じて動作するようになったら、ADCのコンフィギュレーションをダウンロードして保存するのが常に最善の方法です。Configurationモジュールを使って、設定のダウンロードとアップロードの両方を行うことができます。

ジェットパックは、標準的なアプリケーションのための設定ファイルで、作業を簡単にするためにEdgenexusが提供しています。これらもConfigurationモジュールを使ってADCにアップロードすることができます。

設定ファイルは基本的にテキストベースのファイルであり、メモ帳やVIなどのテキストエディターで編集することができます。必要に応じて編集した後、設定ファイルをADCにアップロードすることができます。

コンフィグレーションのダウンロード

- ADCの現在の設定をダウンロードするには、「Download Configuration」ボタンを押します。
- ポップアップが表示され、.confファイルを開くか保存するかを尋ねられます。
- 便利な場所に保存します。
- Notepad++などのテキストエディターで開くことができます。

コンフィグレーションのアップロード

- 保存した設定ファイルをアップロードするには、保存した.confファイルを参照してください。
- Upload Config or Jetpack」ボタンをクリックします。
- ADCは設定をアップロードして適用した後、ブラウザを更新します。自動的に更新されない場合は、ブラウザの更新をクリックしてください。
- 完了すると、Dashboardページにリダイレクトされます。

jetPACKのアップロード

- jetPACKとは、既存の設定にアップデートを加えた設定のセットです。
- jetPACKは、TCPタイムアウトの値を変更する程度の小さなものから、Microsoft ExchangeやMicrosoft Lyncなどのアプリケーションに特化した完全な設定を行うものまであります。
    - jetPACKは、本ガイドの最後に掲載されているサポートポータルから入手できます。
- jetPACK.txtのファイルを参照します。
- アップロード」をクリックします。
- アップロード後はブラウザが自動的に更新されます。
- 完了すると、Dashboardページにリダイレクトされます。
- Microsoft Lyncなどの複雑なデプロイメントでは、インポートに時間がかかる場合があります。

グローバル設定

Global settings "セクションでは、SSL暗号化ライブラリを含む様々な要素を変更できます。

ホストキャッシュタイマ

ホストキャッシュタイマーは、IPアドレスの代わりにドメイン名を使用している場合に、一定期間リアルサーバーのIPアドレスを保存する設定です。このキャッシュは、リアルサーバーの障害時にフラッシュされます。この値を0に設定すると、キャッシュのフラッシュが行われません。この設定の最大値はありません。

ドレイン

ドレイン機能は、仮想サービスにリンクされた各リアルサーバーに対して設定できます。デフォルトでは、［Drain Clears Persistence］設定が有効になっており、Drainモードに設定されたサーバーは、メンテナンスのためにオフラインにすることができるように、潔くセッションを終了することができます。

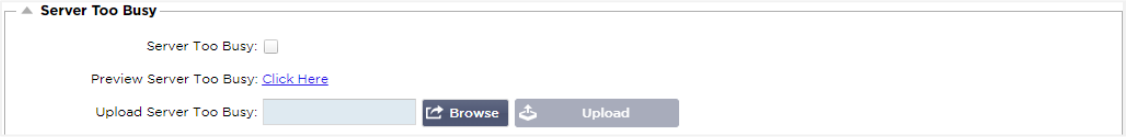
SSL

このグローバル設定では、必要に応じてSSLライブラリを変更することができます。ADCが使用するデフォルトのSSL暗号化ライブラリはOpenSSLです。別の暗号化ライブラリを使用したい場合は、ここで変更できます。

プロトコル

プロトコル」セクションでは、HTTPプロトコルに関するさまざまな詳細設定を行います。

サーバーが忙しすぎる



例えば、リアルサーバーへの最大接続数を制限していたとします。この制限に達した場合、フレンドリーなWebページを表示するように選択できます。

- あなたのメッセージを掲載した簡単なWebページを作成してください。他のウェブサーバーやサイトにあるオブジェクトへの外部リンクを含めることができます。また、Webページに画像を掲載したい場合は、インラインでBase64エンコードされた画像を使用することもできます。
- 新しく作成したWebページのHTM(L)ファイルを参照する
- アップロードをクリック
- ページのプレビューをご希望の場合は、「Click Here」のリンクをクリックしてください。

転送先

Forwarded Forは、レイヤー7のロードバランサーやプロキシサーバーを経由してウェブサーバーに接続するクライアントの発信元IPアドレスを特定するためのデファクトスタンダードです。

フォワード・フォア・アウトプット

オプション	説明
オフ	ADC は Forwarded-For ヘッダを変更しません。
アドレスとポートの追加	この選択は、ADCに接続されている機器またはクライアントのIPアドレスとポートをForwarded-Forヘッダーに追加します。
アドレスの追加	この選択は、ADCに接続された機器またはクライアントのIPアドレスをForwarded-Forヘッダーに追加します。
アドレスとポートの交換	この選択は、Forward-Forヘッダーの値を、ADCに接続された機器またはクライアントのIPアドレスとポートに置き換えます。
アドレスの置き換え	この選択により、Forwarded-Forヘッダーの値が、ADCに接続されている機器またはクライアントのIPアドレスに置き換えられます。

Forwarded-For Header

このフィールドでは、Forwarded-Forヘッダーに付ける名前を指定します。通常は「X-Forwarded-For」ですが、環境によっては変更される場合があります。

IISの高度なロギング - カスタムロギング

X-Forwarded-Forの情報は、IIS Advanced logging 64-bit appをインストールすることで取得できます。ダウンロードしたら、以下の設定で「X-Forwarded-For」というカスタムロギングフィールドを作成します。

Source Type "リストの "Category "リストから "Default "を選択し、"Request Header "を選択します。
Source Name "ボックスで、"X-Forwarded-For "と入力します。

HTTP://www.iis.net/learn/extensions/advanced-logging-module/advanced-logging-for-iis-custom-logging

Apache HTTPd.confの変更

X-Forwarded-ForクライアントのIPアドレス、またはX-Forwarded-Forヘッダーが存在しない場合は実際のクライアントのIPアドレスをログに記録するために、デフォルトのフォーマットにいくつかの変更を加える必要があります。

その変更点は以下の通りです。

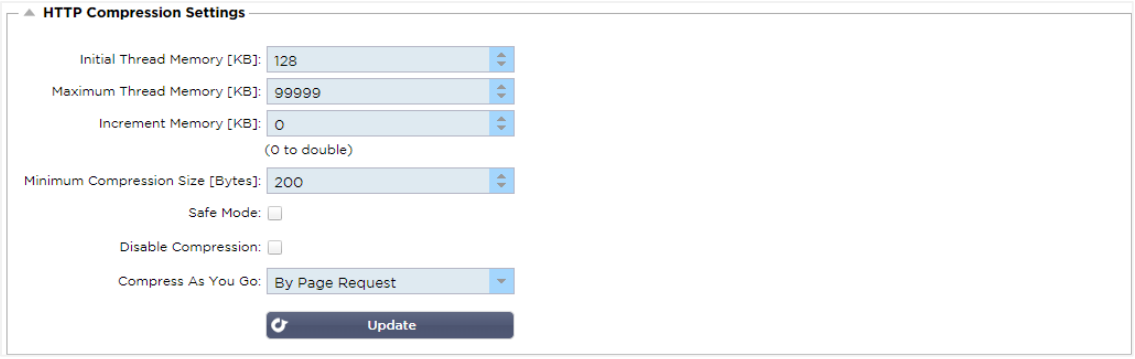
タイプ	価値
LogFormatです。	"%h %l %u %t ⋈⋈⋈◍＞ ◡*)"%{User-Agent}i\" combined
LogFormatです。	"%{X-Forwarded-For}i %l %u %t \"%>s %b \"%{Referer}i\""proxy SetEnvIf X- Forwarded-For "^.*\\...*\...*" forwarded
カスタムログ。	"logs/access_log" 結合env=!forwarded
カスタムログ。	"logs/access_log" プロキシ env=forwarded

このフォーマットは、環境変数に基づく条件付きロギングをサポートする Apache の組み込み機能を利用しています。

- 1行目は、デフォルトからの標準的な複合ログのフォーマットされた文字列です。
- 2行目では、%h（リモートホスト）フィールドをX-Forwarded-Forヘッダーから取り出した値で置き換え、このログファイルパターンの名前を「proxy」に設定します。
- 3行目は環境変数「forwarded」の設定で、IPアドレスにマッチする緩やかな正規表現が含まれていますが、今回はX-Forwarded-ForヘッダーにIPアドレスが存在するかどうかの方が重要なので、これでOKです。
- また、3行目は次のようにも読めます。"X-Forwarded-Forの値があれば、それを使用する。"
- 4 行目と 5 行目は Apache にどのログパターンを使用するかを伝えます。X-Forwarded-For の値が存在する場合は "proxy" パターンを使用し、そうでない場合はリクエストに対して "combined" パターンを使用します。読みやすくするために、4 行目と 5 行目は Apache の rotate logs (piped) ロギング機能を利用していませんが、ほとんどの人が利用していると思われます。

この変更により、すべてのリクエストに対してIPアドレスが記録されるようになります。

HTTP圧縮の設定



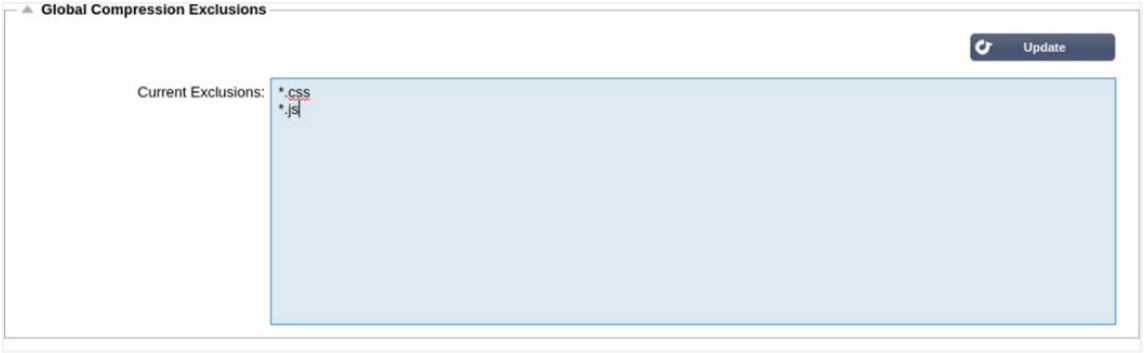
圧縮は高速化のための機能で、「IPサービス」ページでサービスごとに有効にします。

警告：不適切な設定をすると、ADCの性能に悪影響を及ぼす可能性があるため、これらの設定を行う際には十分な注意が必要です。

オプション	説明

初期スレッドメモリ[KB]	この値は、ADCが受信した各リクエストが最初に割り当てるメモリの量です。最も効率的なパフォーマンスを得るために、この値は、ウェブサーバーが送信する可能性のある最大の圧縮されていないHTMLファイルをちょうど超える値に設定する必要があります。
最大スレッドメモリ[KB]	この値は、ADCが1回のリクエストで割り当てるメモリの最大量です。最大のパフォーマンスを得るために、ADCは通常、すべてのコンテンツをメモリーに保存し、圧縮します。この値を超える例外的に大きなコンテンツファイルを処理する場合、ADCはディスクに書き込み、そこでデータを圧縮します。
インクリメントメモリ[KB]	この値は、Initial Thread Memory Allocationにさらにメモリが必要な場合に追加されるメモリの量を設定します。デフォルトの設定はゼロです。これは、データが現在の割り当てを超えた場合（128Kb、256Kb、512Kbなど）、「スレッドごとの最大メモリ使用量」で設定された上限まで、ADCが割り当てを2倍にすることを意味します。これは、大部分のページが一定のサイズで、たまに大きなファイルがある場合に有効です。(例：大部分のページは128Kb以下だが、たまに1Mbのサイズのレスポンスがある場合など)大規模な可変サイズのファイルがある場合には、重要なサイズの線形増分を設定する方が効率的です（例：応答のサイズが2Mb～10Mbの場合、初期設定を1Mbにして1Mbずつ増分する方が効率的）。
最小圧縮サイズ バイト数	この値は、ADCが圧縮を試みないサイズをバイト単位で指定します。200バイト以下では圧縮がうまくいかず、圧縮ヘッダーのオーバーヘッドのためにサイズが大きくなる可能性があるため、これは便利です。
セーフモード	ADCがスタイルシートやJavaScriptに圧縮を適用しないようにするには、このオプションにチェックを入れます。この理由は、ADCが個々のブラウザで圧縮コンテンツを処理できることを認識していても、他のプロキシサーバーの中には、HTTP/1.1に準拠していると主張していても、圧縮されたスタイルシートやJavaScriptを正しく伝送できないものがあるためです。プロキシサーバーを経由したスタイルシートやJavaScriptで問題が発生する場合は、このオプションを使用してこれらのタイプの圧縮を無効にしてください。ただし、この場合、コンテンツの全体的な圧縮量は減少します。
圧縮を無効にする	ADCがレスポンスを圧縮しないようにするには、これにチェックを入れます。
随時圧縮	ON - このページで「Compress as You Go」を使用します。これは、サーバーから受信したデータの各ブロックを、完全に圧縮解除可能な個別のチャンクとして圧縮します。 OFF - このページで Compress as you Go を使用しません。 By Page Request - ページの要求に応じて Compress as You Go を使用します。

グローバル・コンプレッションの除外項目



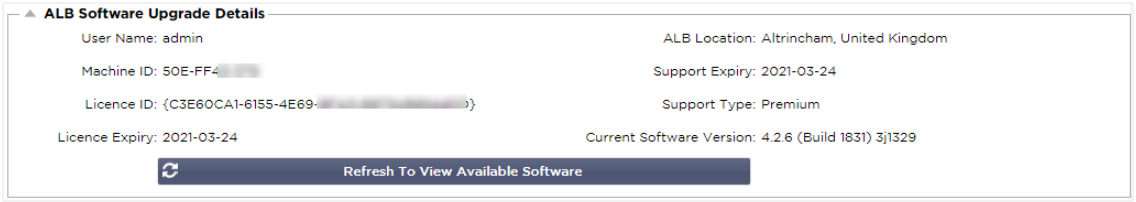
追加された拡張子が除外リストにあるページは、圧縮されません。

- 個別のファイル名を入力します。
- アップデートをクリックします。
- ファイルタイプを追加したい場合は、「*.css」と入力するだけで、すべてのカスケードスタイルシートを除外することができます。
- 各ファイルやファイルタイプは、新しい行に追加する必要があります。

ソフトウェア

ソフトウェア」セクションでは、ADCの構成やファームウェアをアップデートすることができます。

ソフトウェアアップグレードの詳細



このセクションの情報は、お客様がインターネットに接続している場合に入力されます。お使いのブラウザがインターネットに接続されていない場合は、このセクションは空白になります。インターネットに接続されると、以下のバナーメッセージが表示されます。

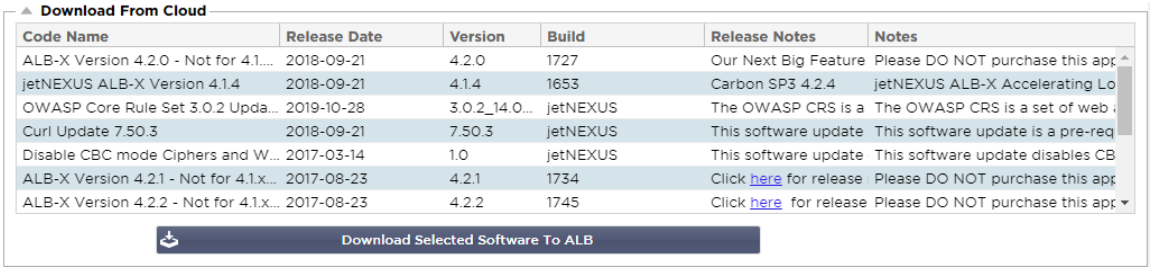
以下の「クラウドからのダウンロード」セクションには、お客様のサポートプランで利用可能なアップデート情報が表示されます。サポートタイプとサポート有効期限に注意してください。

注：Edgenexus Cloudから利用可能なものを表示するために、お客様のブラウザのインターネット接続を使用します。ADCがインターネットに接続されている場合のみ、ソフトウェア・アップデートをダウンロードすることができます。

これを確認するために

- Advanced--Troubleshooting--Ping
- IPアドレス - appstore.edgenexus.io
- Ping」をクリックします。
- ping: unknown host appstore.edgenexus.io. "と表示された場合。"
- ADCは、クラウドから何かをダウンロードすることはできません。

クラウドからのダウンロード



ブラウザがインターネットに接続されていれば、クラウドで利用できるソフトウェアの詳細が表示されます。

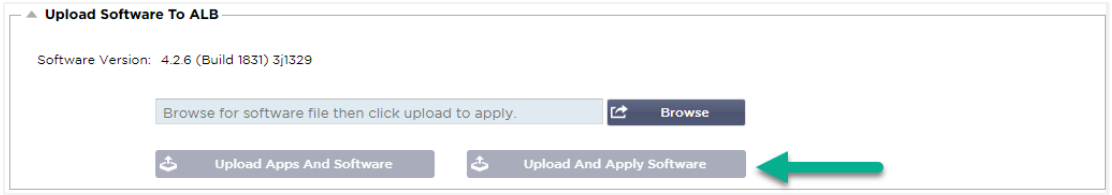
- 興味のある行をハイライトして、「選択したソフトウェアをALBにダウンロード」をクリックします。"ボタン
- 選択されたソフトウェアは、クリックするとALBにダウンロードされ、後述の「ALBに保存されているソフトウェアの適用」で適用することができます。

注）ADCが直接インターネットに接続されていない場合は、下記のようなエラーが表示されます。

ダウンロードエラー、ALB not able to access ADC Cloud Services for file build1734-3236-v4.2.1-Sprint2-update-64.software.alb

ALBへのソフトウェアのアップロード

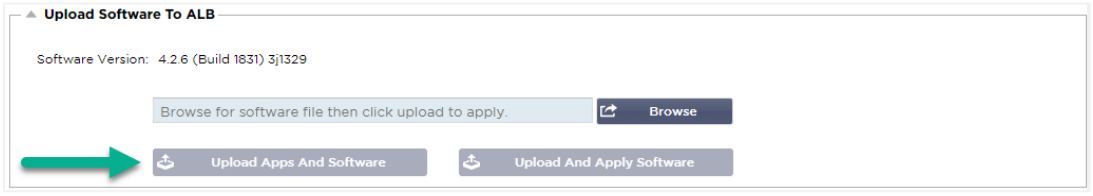
アプリのアップロード



<apptype>.albで終わるアプリファイルがあれば、この方法でアップロードすることができます。

- Appには5つのタイプがあります。
  - <アプリ名>flightpath.alb
  - <アプリ名>.monitor.alb
  - <アプリ名>.jetpack.alb
  - <アプリ名>.addsons.alb
  - <アプリ名>.featurepack.alb
- アップロードされた各アプリは、「ライブラリ」の「アプリ」セクションに表示されます。
- その後、そのセクションの各Appを個別にデプロイする必要があります。

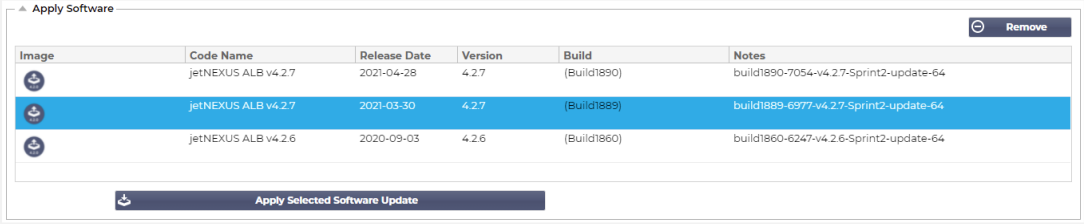
ソフトウェア



- ソフトウェアを適用せずにアップロードする場合は、強調表示されたボタンを使用してください。

- ソフトウェアファイルは「<softwarename>.software.alb」です。
- すると、「ALBに保存されているソフトウェア」に表示され、そこから好きな時に適用することができます。

ALBに格納されているソフトウェアの適用



このセクションでは、ALB に保存されている、デプロイ可能な全てのソフトウェアファイルが表示されます。このリストには、更新された Web Application Firewall (WAF)のシグネチャが含まれます。

- 使用したい「ソフトウェア」の行を選択してください。
- 選択されたソフトウェアの適用 "をクリック
- ALBソフトウェアアップデートの場合、アップロード後にALBを再起動して適用することになりますので、ご注意ください。
- 適用するアップデートがOWASPシグネチャアップデートの場合は、再起動することなく自動的に適用されます。

トラブルシューティング

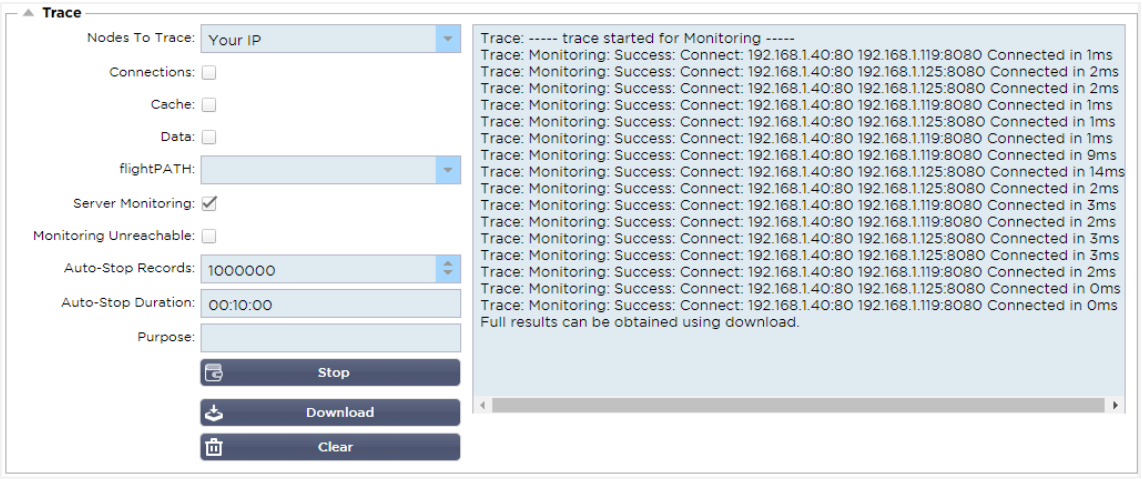
根本的な原因と解決策を導き出すために、トラブルシューティングが必要な問題は常にあります。このセクションでは、それを可能にします。

サポートファイル

ADCに問題が発生し、サポート・チケットを作成する必要がある場合、テクニカル・サポートはしばしばADCアプライアンスから複数の異なるファイルを要求します。これらのファイルは現在、1つの.datファイルにまとめられており、このセクションからダウンロードできます。

- ドロップダウンから時間帯を選択します。3日、7日、14日、全日の中からお選びいただけます。
- サポートファイルのダウンロード "をクリック
- Support-jetNEXUS-yyymmddhh-NAME.datという形式のファイルがダウンロードされます。
- サポートポータルでサポートチケットを発行してください。サポートポータルの詳細はこのドキュメントの最後にあります。
- 問題点をしっかりと説明し、.datファイルをチケットに添付してください。

トレース



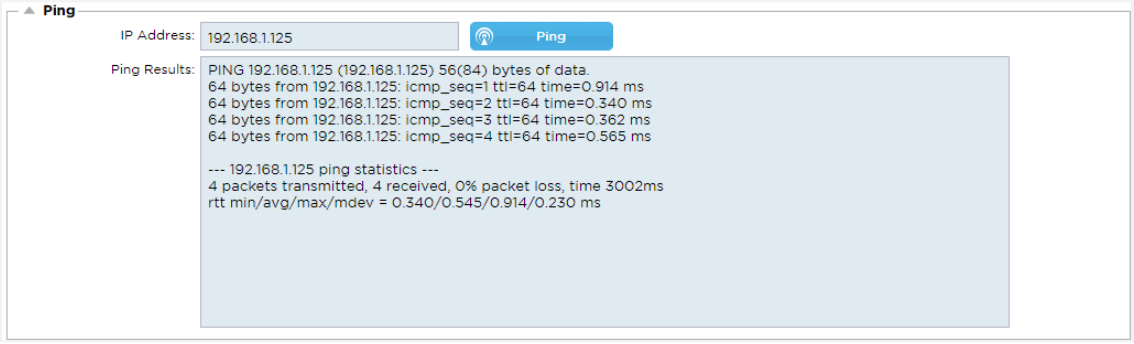
トレース」セクションでは、問題のデバッグに必要な情報を確認できます。配信される情報は、ドロップダウンやチェックボックスから選択したオプションによって異なります。

オプション	説明
トレースするノード	**Your IP**: GUIにアクセスしているIPアドレスを使用して出力をフィルタリングします（モニタリングではADCのインターフェースアドレスを使用するので、このオプションを選択しないでください）。 **All IP**：フィルターは適用されません。忙しいボックスでは、これはパフォーマンスに悪影響を与えることに注意してください。
コネクション	このチェックボックスをオンにすると、クライアント側とサーバー側の接続に関する情報が表示されます。
キャッシュ	このチェックボックスをオンにすると、キャッシュされたオブジェクトに関する情報が表示されます。
データ	このチェックボックスをオンにすると、ADCで入出力される生データのバイトが含まれます。
フライトパス	flightPATH」メニューでは、モニターする特定のflightPATHルール、または「すべてのflightPATHルール」を選択できます。
サーバー監視	このチェックボックスをオンにすると、ADCでアクティブなサーバーヘルスモニターとその結果が表示されます。
モニタリング 到達不能	このチェックを入れると、失敗したモニターのみを表示し、これらのメッセージのみを対象としたフィルターのような役割を果たすことを除いては、上記と同様です。
オートストップの記録	初期値は 1,000,000 レコードで、これを超えるとトレース機能は自動的に停止します。これは、トレース機能を誤ってオンにしたままにして、ADCの性能に影響を与えないようにするための安全対策です。
自動停止時間	デフォルトの時間は 10 分に設定されており、これを過ぎるとトレース機能は自動的に停止します。これは、誤ってトレース機能をオンにしたままにして、ADC の性能に影響を与えないようにするための安全対策です。
スタート	手動でトレース機能を開始する場合はクリックします。

ストップ	自動記録や時間に達する前に手動でトレース機能を停止する場合は、クリックします。
ダウンロード	右側にはライブビューワが表示されますが、情報の表示が早すぎる場合があります。Trace.logをダウンロードすると、その日の様々なトレースで集められた全ての情報を見ることができます。これは基本的に、トレース情報のフィルタリングされたリストです。前日のトレース情報を表示したい場合は、その日のシスログをダウンロードすることができますが、手動でフィルタリングする必要があります。
クリア	トレースログのクリア

ピン

Pingツールを使用して、インフラストラクチャ内のサーバーやその他のネットワークオブジェクトへのネットワーク接続を確認することができます。



テストしたいホストのIPアドレスを入力します。例えば、ドット10進法によるデフォルトゲートウェイや、IPv6アドレスなどです。Ping」ボタンを押した後、結果がフィードバックされるまで数秒待つ必要があるかもしれません。

DNSサーバーを設定している場合は、完全修飾ドメイン名を入力することができます。DNSサーバーの設定は、「**DNSサーバー1**」と「**DNSサーバー2**」のセクションで行います。Ping」ボタンを押した後、結果がフィードバックされるまで数秒待つ必要があるかもしれません。

キャプチャー

ネットワークトラフィックをキャプチャするには、以下の簡単な手順に従ってください。

- フォーム内のオプションを入力してください。
- 生成」をクリックします。
- キャプチャが実行されると、ブラウザがポップアップしてファイルの保存先を尋ねてきます。jetNEXUS.cap.gz "という形式になります。
- サポートポータルでサポートチケットを発行してください。サポートポータルの詳細はこのドキュメントの最後にあります。
- 問題点をしっかりと説明し、そのファイルをチケットに添付してください。

- Wiresharkを使ってコンテンツを見ることもできます。

オプション	説明
アダプター	ドロップダウンからアダプターを選択してください。すべてのインターフェースを"any "でキャプチャすることもできます。
パケット	この値は、キャプチャーするパケットの最大数です。通常は、99999
期間	キャプチャーが実行される最大時間を選択します。トラフィックの多いサイトでは15秒が一般的です。キャプチャー期間中は、GUIにアクセスできません。
アドレス	この値は、ボックスに入力されたすべてのIPアドレスをフィルタリングします。空白にするとフィルタリングされません。

パフォーマンスを維持するために、ダウンロードファイルの容量を10MBに制限しています。もし、これでは必要なデータをすべて取り込むことができないということであれば、この数値を増やすことも可能です。

注：ライブサイトのパフォーマンスに影響を与えます。利用可能なキャプチャーサイズを増やすには、グローバル設定のjetPACKを適用してください。

jetPACKとは

jetPACKsは、特定のアプリケーションのためにADCを即座に設定するユニークな方法です。これらの使いやすいテンプレートは、ADCから最適化されたサービス提供を楽しむために必要な、すべてのアプリケーション固有の設定が事前に設定され、完全に調整されています。jetPACKの中にはflightPATHを使用してトラフィックを操作するものがあり、この要素を動作させるにはflightPATHのライセンスが必要です。flightPATHのライセンスをお持ちかどうかを確認するには、「ライセンス」のページを参照してください。

jetPACKのダウンロード

- 下記の各jetPACKは、jetPACKのタイトルに含まれるユニークなバーチャルIPアドレスで作成されています。例えば、以下の最初のjetPACKは、1.1.1.1のバーチャルIPアドレスを持っています。
- jetPACKをそのままアップロードして、GUIでIPアドレスを変更するか、jetPACKをメモ帳などのテキストエディターで編集して、1.1.1.1を仮想IPアドレスに置き換えて検索してください。
- また、それぞれのjetPACKには、127.1.1.1と127.2.2.2のIPアドレスを持つ2つのReal Serverが作成されています。これらはアップロード後にGUIで変更することもできますし、事前にNotepad++で変更することもできます。
- 以下のjetPACKのリンクをクリックして、リンクをjetPACK-VIP-Application.txtファイルとして任意の場所に保存してください。

Microsoft Exchange

アプリケーション	ダウンロードリンク	何をするのか？	何が含まれていますか？
Exchange 2010	jetPACK-1.1.1.1-Exchange-2010	このjetPACKは、Microsoft Exchange 2010をロードバランスするための基本的な設定を追加します。HTTPサービスのトラフィックをHTTPSにリダイレクトするflightPATHルールが含まれていますが、これはオプションです。flightPATHのライセンスをお持ちでない場合でも、このjetPACKは動作します。	グローバル設定サービスタイムアウト 2時間 モニターです。Outlook Webアプリ用のレイヤ7モニター、クライアントアクセスサービス用のレイヤ4アウトオブバンドモニター バーチャルサービスIP：1.1.1.1 バーチャルサービスのポート80, 443, 135, 59534, 59535 リアルサーバー127.1.1.1 127.2.2.2 flightPATH：HTTPからHTTPSへのリダイレクトを追加します。
	jetPACK-1.1.1.2-Exchange-2010-SMTP-RP	上記と同じですが、リバースプロキシ接続でポート25にSMTPサービスを追加します。SMTPサーバはALB-Xのインターフェースアドレスをソースとして認識します。	グローバル設定サービスタイムアウト 2時間 モニターです。Outlook Webアプリ用のレイヤ7モニター。クライアント・アクセス・サービス用のレイヤ4アウトオブバンド・モニター

			バーチャルサービスIP：1.1.1.1 バーチャルサービスのポート80, 443, 135, 59534, 59535, 25 (リバースプロキシ) リアルサーバー127.1.1.1 127.2.2.2 flightPATH：HTTPからHTTPSへのリダイレクトを追加します。
	jetPACK-1.1.1.3-Exchange-2010-SMTP-DSR	上記と同じですが、このjetPACKはSMTPサービスがDirect Server Return接続を使用するように設定します。このjetPACKは、SMTPサーバーがクライアントの実際のIPアドレスを確認する必要がある場合に必要です。	グローバル設定サービスタイムアウト 2時間 モニターです。Outlook Webアプリ用のレイヤ7モニター。クライアント・アクセス・サービス用のレイヤ4アウトオブバンド・モニター バーチャルサービスIP：1.1.1.1 バーチャルサービスのポート80, 443, 135, 59534, 59535, 25 (direct server return) リアルサーバー127.1.1.1 127.2.2.2 flightPATH: HTTPからHTTPへのリダイレクトを追加しました。
Exchange 2013	jetPACK-2.2.2.1-Exchange-2013-Low-Resource	この設定では、1つのVIPとHTTPおよびHTTPSトラフィック用の2つのサービスが追加され、必要なCPUが最も少なくなります。VIPに複数のヘルスチェックを追加して、個々のサービスが稼働しているかどうかを確認することが可能です。	グローバル設定。 モニターです。OWA、EWS、OA、EAS、ECP、OAB、ADSのレイヤー7モニター バーチャルサービスIP：2.2.2.1 バーチャルサービスのポート80, 443 リアルサーバー127.1.1.1 127.2.2.2 flightPATH：HTTPからHTTPSへのリダイレクトを追加します。
	jetPACK-2.2.3.1-Exchange-2013-Med-Resource	この設定では、各サービスに固有のIPアドレスを使用するため、上記よりも多くのリソースを使用します。各サービスを個別のDNSエントリとして設定する必要があります 例： owa.jetnexus.com、ews.jetnexus.comなど。各サービスのモニターが追加され、関連するサービスに適用されます。	グローバル設定。 モニターします。OWA、EWS、OA、EAS、ECP、OAB、ADS、MAPI、PowerShellのレイヤー7モニター 仮想サービスIP：2.2.3.1、2.2.3.2、2.2.3.3、2.2.3.4、2.2.3.5、2.2.3.6、2.2.3.7、2.2.3.8、2.2.3.9、2.2.3.10

			バーチャルサービスのポート 80, 443 リアルサーバー127.1.1.1 127.2.2.2 flightPATH: HTTPからHTTPへのリダイレクトを追加しました。
	jetPACK-2.2.2.3Exchange2013-HIgh-Resource	このjetPACKは、1つのユニークなIPアドレスと、異なるポート上の複数のバーチャルサービスを追加します。 flightPATHは、正しいバーチャルサービスへの宛先パスに基づいてコンテキストスイッチを行います。このjetPACKは、コンテキストスイッチを実行するために最も多くのCPUを必要とします。	グローバル設定。 モニターします。OWA、EWS、OA、EAS、ECP、OAB、ADS、MAPI、PowerShellのレイヤー7モニター バーチャルサービスIP：2.2.2.3 バーチャルサービスのポート 80, 443, 1, 2, 3, 4, 5, 6, 7 リアルサーバー127.1.1.1 127.2.2.2 flightPATH：HTTPからHTTPSへのリダイレクトを追加します。

Microsoft Lync 2010/2013

リバースプロキシ	フロントエンド	エッジ内部	エッジ・エクスターナル
jetPACK-3.3.3.1-Lync-Reverse-Proxy	jetPACK-3.3.3.2-Lync-Front -End	jetPACK-3.3.3-Lync-Edge-Internal	jetPACK-3.3.3.4-Lync-Edge-External（ジェットパック-3.3.3.4-Lync-Edge-External

ウェブサービス

通常のHTTP	SSLオフロード	SSL再暗号化	SSL Passthrough
jetPACK-4.4.4.1-Web-HTTP	jetPACK-4.4.4.2-Web-SSL Offload	jetPACK-4.4.4.3-Web-SSL-Re-Encryption	jetPACK-4.4.4.4-Web-SSL Passthrough

マイクロソフト・リモート・デスクトップ

jetPACK-5.5.5.1-Remote-Desktop

DICOM - Digital Imaging and Communication in Medicine

jetPACK-6.6.6.1-DICOM

オラクルe-ビジネススイート

SSLオフロード
jetPACK-7.7.7...1-Oracle-EBS

VMware Horizon View

接続サーバー - SSL オフロード	セキュリティサーバ - SSL再暗号化
jetPACK-8.8.8.1-View-SSL-Offload	jetPACK-8.8.8.2-View-SSL-Re-encryption

グローバル設定

- GUIセキュアポート443 - このjetPACKは、セキュアなGUIポートを27376から443に変更します。HTTPs://x.x.x.x
- GUIタイムアウト1日 - GUIは20分ごとにパスワードの入力を要求します。この設定では、その要求を1日に増やします

- ARP Refresh 10 - HAアプライアンス間のフェイルオーバー時に、この設定は移行中のスイッチを支援するために**Gratuitous ARP**の数を増やします。
- キャプチャーサイズ 16MB - デフォルトのキャプチャーサイズは2MBです。この値を設定すると、サイズが最大16MBになります。

暗号オプション

- Strong Ciphers - 暗号オプションのリストから「Strong Ciphers」を選択できる機能が追加されます。
    - 暗号 = ALL:RC4+RSA:+RC4:+HIGH::DES-CBC3-SHA::SSLv2::ADH::EXP::ADHexport::MD5
- Anti-Beast - 暗号オプションのリストから「Anti Beast」を選択できるようになります。
    - 暗号 = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4:HIGH::MD5::aNULL::EDH
- No SSLv3 - 「暗号オプション」リストから「No SSLv3」を選択できるようになります。
    - 暗号 = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH::MD5::aNULL::EDH::RC4
- No SSLv3 no TLSv1 No RC4 - 「暗号オプション」リストから「No-TLSv1 No-SSLv3 No-RC4」を選択できる機能が追加されます。
    - 暗号 = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH::MD5::aNULL::EDH::RC4
- NO_TLSv1.1 -「暗号オプション」リストから「NO_TLSv1.1」を選択する機能が追加されます。
    - 暗号= ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:RSA+AESGCM:RSA+AES:HIGH:!3DES:!aNULL:!MD5::DSS::MD5::aNULL::EDH::RC4

flightPATHs

- X-Content-Type-Options - このヘッダーが存在しない場合は追加し、"nosniff "に設定することで、ブラウザが自動的に "MIME-Sniffing "を行うことを防ぎます。
- X-Frame-Options - このヘッダが存在しない場合は追加し、"SAMEORIGIN "に設定します。あなたのウェブサイトのページをフレームに含めることができますが、同じウェブサイト内の他のページにのみ含めることができます。
- X-XSS-Protection - このヘッダーが存在しない場合は追加し、「1; mode=block」に設定します - ブラウザのクロスサイトスクリプティング保護機能を有効にします。
- Strict-Transport-Security - ヘッダーが存在しない場合は追加し、"max-age=31536000 ; includeSubdomains "に設定します - クライアントが、max-ageの間、すべてのリンクがHTTPs://であることを尊重するようにします。

jetPACKの装着

任意のjetPACKを任意の順番で適用できますが、同じ仮想IPアドレスのjetPACKを使用しないように注意してください。この行為により、コンフィグレーション内でIPアドレスが重複してしまいます。誤ってこのような操作をしてしまった場合は、GUIで変更することができます。

- 詳細設定」→「ソフトウェアの更新」を選択する
- 設定セクション
- 新しい設定ファイルまたはjetPACKのアップロード
- jetPACKを見る
- アップロードをクリック
- ブラウザの画面が白くなったら、更新をクリックして、ダッシュボードのページが表示されるのを待ってください。

jetPACKの作成

jetPACKの優れた点のひとつは、自分で作成できることです。あるアプリケーションのために完璧なコンフィグを作成し、これを他のいくつかのボックスに独立して使用したいと思うかもしれません。

- まず、既存のALB-Xから現在の構成をコピーします。
  - アドバンスド
  - ソフトウェアの更新
  - 現在の設定のダウンロード
- このファイルをNotepad++で編集する
- 新しいtxtドキュメントを開き、名前を "yourname-jetPACK1.txt "とします。
- 設定ファイルから関連する部分をすべて "yourname-jetPACK1.txt "にコピーします。
- 完成したら保存

重要：各jetPACKはそれぞれ分割されていますが、すべてのjetPACKはページの先頭に#!jetpackを付ける必要があります。

編集・コピーを推奨する箇所は以下の通りです。

セクション0:

#!ジェットパック

この行はjetPACKの一番上にある必要があります。そうしないと、現在の設定が上書きされてしまいます。

セクション1:

[jetnexusdaemon]

このセクションには、一度変更するとすべてのサービスに適用されるグローバル設定が含まれています。これらの設定の中には、ウェブコンソールから変更できるものもありますが、ここでしか利用できないものもあります。

例

ConnectionTimeout=600000

この例では、TCPのタイムアウト値をミリ秒単位で指定しています。この設定は、10分間活動しないと、TCP接続が閉じられることを意味します

ContentServerCustomTimer=20000

この例では、DICOMなどのカスタムモニターのコンテンツサーバーのヘルスチェックの間の遅延をミリ秒単位で表しています。

jnCookieHeader="MS-WSMAN"

この例では、永続的なロードバランシングで使用されるCookieヘッダーの名前を、デフォルトの「jnAccel」から「MS-WSMAN」に変更します。この特別な変更は、Lync 2010/2013のリバースプロキシに必要です。

Section 2:

[jetnexusdaemon-Csm-Rules] です。

このセクションでは、通常ここのウェブコンソールから設定されるカスタムサーバー監視ルールが含まれています。

例

[jetnexusdaemon-Csm-Rules-0] です。

Content="サーバーアップ"

Desc="Monitor 1

Method="CheckResponse"

Name="Health Check- Is Server Up"

Url="HTTP://demo.jetneus.com/healthcheck/healthcheck.html"

Section 3:

[jetnexusdaemon-LocalInterface]を使用しています。

このセクションには、「IPサービス」セクションのすべての詳細が含まれています。各インターフェースには番号が振られており、各チャンネルのサブインターフェースも含まれています。チャンネルにflightPATHルールが適用されている場合は、Pathセクションも含まれます。

例

[jetnexusdaemon-LocalInterface1] です。

1.1=”443″

1.2=”104″

1.3=”80″

1.4=”81″

Enabled=1

Netmask="255.255.255.0″

PrimaryV2="{A28B2C99-1FFC-4A7C-AAD9-A55C32A9E913}"

[jetnexusdaemon-LocalInterface1.1]を参照してください。

1=">,""セキュアグループ"",2000,""

2="192.168.101.11:80,Y,""IIS WWW Server 1″""

3="192.168.101.12:80,Y,""IIS WWW Server 2″""

AddressResolution=0

CachePort=0

CertificateName="default"

ClientCertificateName="SSLなし"

Compress=1

ConnectionLimiting=0

DSR=0

DSRProto="tcp"

Enabled=1

LoadBalancePolicy="CookieBased"

MaxConnections=10000

MonitoringPolicy="1

PassThrough=0

Protocol="Accelerate HTTP"

ServiceDesc="Secure Servers VIP"

SNAT=0

SSL=1

SSLClient=0

SSLInternalPort=27400

[jetnexusdaemon-LocalInterface1.1-Path]を参照してください。

1=”6″

Section 4:

[jetnexusdaemon-Path]を参照してください。

このセクションには、すべてのflightPATHルールが含まれています。番号は、インターフェイスに適用されたものと一致しなければなりません。上の例では、flightPATHルール「6」がチャンネルに適用されていることがわかり、これを含めて以下の例のようになります。

例

[jetnexusdaemon-Path-6]を参照してください。

Desc="特定のディレクトリにHTTPSを強制的に使用する"

Name="Gary - Force HTTPS"

[jetnexusdaemon-Path-6-Condition-1]を参照してください。

Check="contain"

条件="パス"

Match=

センス="does"

Value="/secure/"

[jetnexusdaemon-Path-6-Evaluate-1]を参照してください。

Detail=

ソース="ホスト"

値=

Variable="$host$"[jetnexusdaemon-Path-6-Function-1]とします。

Action="redirect"

Target="HTTPs://$host$$path$$querystring$"

値=

flightPATHの紹介

flightPATHとは何ですか？

flightPATHは、Edgenexus社が開発した、HTTPおよびHTTPSトラフィックを操作・ルーティングするためのインテリジェントなルールエンジンです。高度な設定が可能で、非常にパワフルでありながら、非常に簡単に使用することができます。

flightPATHの一部のコンポーネントはソースIPなどのIPオブジェクトですが、flightPATHはHTTPに等しい**サービスタイプ**にのみ適用することができます。これ以外のサービスタイプを選択した場合、「IPサービス」の「flightPATH」タブは空白になります。

flightPATHルールには3つの要素があります。

オプション	説明
状態	flightPATHルールのトリガーとなる複数の基準を設定します。
評価	アクションエリアで使用可能な変数の使用を許可します。
アクション	ルールがトリガーされた後の動作。

flightPATHは何ができるのでしょうか？

flightPATHは、受信および送信するHTTP(s)のコンテンツやリクエストの変更に使用できます。

Starts with "や "Ends With "などの単純な文字列マッチだけでなく、Perl互換の強力な正規表現（RegEx）を使った完全な制御が可能です。

RegExの詳細については、こちらの参考サイト https://www.regexbuddy.com/regex.html をご覧ください。

また、**アクション**エリアでは、カスタム変数を作成して使用することができ、さまざまな可能性を秘めています。

状態

状態	説明	例
<form>（英語	HTMLフォームはサーバーにデータを渡すために使われる	例 "form doesn't have length 0"
GEO ロケーション	これは、送信元IPアドレスとISO 3166の国コードを比較するものです。	GEO ロケーションが GB に該当する場合または GEO ロケーションが Germany に該当する場合
ホスト	これは、URLから抽出したホスト	www.mywebsite.com または 192.168.1.1
言語	これは、言語の HTTP ヘッダーから抽出された言語です。	この条件では、言語のリストを含むドロップダウンが生成されます。
方法	これは、HTTPメソッドのドロップダウンです。	これは、GET、POSTなどを含むドロップダウンです。

オリジンIP	上流のプロキシがX-Forwarded-For（XFF）をサポートしている場合、真のOriginアドレスを使用します。	クライアントIP。複数のIPやサブネットを使用することも可能。 10.1.2.0 /24 subnet 10\.1.2.3|10\.1.2.4 Use | for multiple IP's
パス	これは、ウェブサイトのパス	/mywebsite/index.asp
POST	POSTリクエストメソッド	Webサイトにアップロードされるデータのチェック
問い合わせ	これは、クエリの名前と値であり、クエリの名前または値を受け入れることができます。	"Best=jetNEXUS" マッチはBest、バリューはedgeNEXUSの場合
問い合わせ文字列	? "文字以降のクエリ文字列全体	
リクエストクッキー	これは、クライアントから要求されたクッキーの名前です。	MS-WSMAN=afYfn1CDqqCDqUD::
リクエストヘッダー	これは、任意のHTTPヘッダ	リファラー、ユーザーエージェント、From、Date
リクエストバージョン	これがHTTPバージョン	http/1.0またはhttp/1.1
レスポンスボディ	レスポンスボディに含まれるユーザー定義の文字列	サーバーアップ
応答コード	レスポンスのHTTPコード	200 OK, 304 Not Modified
レスポンスクッキー	これは、サーバーが送信したクッキーの名前です	MS-WSMAN=afYfn1CDqqCDqUD::
レスポンスヘッダー	これは、任意のHTTPヘッダ	リファラー、ユーザーエージェント、From、Date
レスポンスバージョン	サーバーから送られてきたHTTPバージョン	http/1.0またはhttp/1.1
ソースIP	オリジンIP、プロキシサーバーIP、またはその他の集約されたIPアドレスのいずれかです。	ClientIP、ProxyIP、FirewallIP。複数のIPやサブネットを使用することもできます。 ドットはRegEXなので必ずエスケープしてください。 例 10\\.1\.2\.3 は 10.1.2.3 です。

マッチ	説明	例
受け入れ	許容されるコンテンツタイプ	Accept: text/plain
Accept-Encoding	使用可能なエンコーディング	Accept-Encoding: <compress | gzip | deflate | sdch | identity>。
アクセプト・ランゲージ	回答に使用できる言語	Accept-Language: en-US

受け入れ範囲	このサーバーがサポートしているパーシャルコンテンツの範囲タイプ	Accept-Ranges: bytes
オーソライズ	HTTP認証用の認証情報	オーソライズされています。基本 QWxhZGRpbjpvcGVuIHNlc2FtZQ==。
チャージ・トゥー	要求された方法の適用に必要なコストのアカウント情報を含む	
Content-Encoding	データに使用されているエンコーディングの種類。	Content-Encoding: gzip
Content-Length	レスポンスボディの長さをオクテット（8ビットバイト）で表したもの	Content-Length: 348
コンテンツタイプ	リクエストの本文のmimeタイプ（POSTおよびPUTリクエストで使用されます	Content-Type: application/x-www-form-urlencoded
クッキー	Set-Cookie（下記）でサーバーから送られてきたHTTPクッキー	Cookie: $Version=1; Skin=new;
日付	メッセージが発信された日付と時間	Date = "日付" ":" HTTP-date
ETag	リソースの特定のバージョンを示す識別子で、多くはメッセージダイジェストです。	ETag:"aed6bdb8e090cd1:0"
より	リクエストを行ったユーザーのEメールアドレス	From: user@example.com
If-Modified-Since	コンテンツが変更されていない場合に、304 Not Modifiedを返すことを許可する	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Last-Modified	リクエストされたオブジェクトの最終更新日（RFC2822形式）。	Last-Modified:Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Implementation-specific headersは、リクエスト・レスポンスの連鎖のどこかで様々な影響を与える可能性があります。	Pragma: no-cache
リファラー	これは、現在要求されているページへのリンクを辿った前のウェブページのアドレスです。	リファラー：HTTP://www.edgenexus.io
サーバー	サーバーの名前	サーバーです。Apache/2.4.1 (Unix)
セット-クーキー	HTTPクッキー	セット-クーキーUserID=JohnDoe; Max-Age=3600; Version=1
User-Agent	ユーザーエージェントの文字列	User-AgentMozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Vary	下流のプロキシに対して、将来のリクエストヘッダーをどのように照合し、 オリジンサーバーから 新たなレスポンスをリクエストするのではなく、キャッシュされたレスポンスを使用できるかどうかを判断する方法を指示します。	Vary:User-Agent

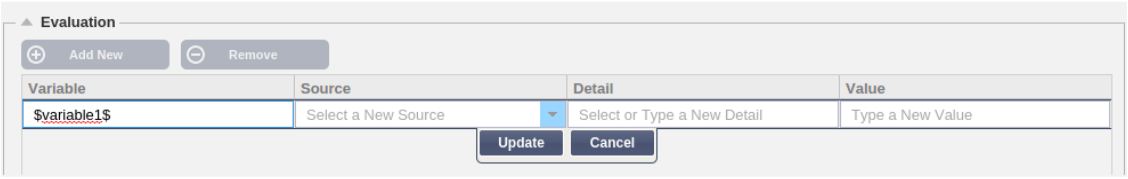
X-Powered-By	Webアプリケーションを支える技術（ASP.NET、PHP、JBossなど）を指定します。	X-Powered-By:PHP/5.4.0

チェック	説明	例
存在する	これは、条件の詳細を気にせず、存在するかしないかだけを気にするものです。	ホストが存在する
スタート	文字列は、Valueで始まります。	パス - Does - Start - /secure
終了	文字列の最後には、Value	パス - Does - End - .jpg
収録内容	この文字列には、以下の値が含まれています。	リクエストヘッダー - アクセプト - Does - Contain - image
イコール	文字列は「値」に等しい	ホスト - Does - Equal - www.jetnexus.com
長さ	文字列は値の長さを持っています。	ホスト - Does - Have Length - 16 www.jetnexus.com = TRUE www.jetnexus.co.uk = FALSE
Match RegEx	これにより、Perl互換の完全な正規表現を入力することができます。	Origin IP - Does - Match Regex - 10\...* | 11\...*

例

- この例では、2つの条件があり、アクションを実行するには**両方を**満たす必要があります。
- 1つ目は、要求されたオブジェクトが画像であるかどうかを確認することです。
- 2つ目は、特定のホストネームをチェックすること

評価



Variableの追加は、リクエストからデータを抽出してActionsで活用できるようになる魅力的な機能です。例えば、ユーザのユーザ名を記録したり、セキュリティ上の問題があった場合にメールを送信したりすることができます。

- 変数です。変数の最初と最後は$記号でなければなりません。例えば、 $variable1$
- ソースドロップダウンボックスから変数のソースを選択する
- 詳細関連する場合はリストから選択します。Source=Request Headerの場合、DetailはUser-Agentになります。
- 値を入力します。変数を微調整するためのテキストまたは正規表現を入力します。

内蔵変数。

- 組み込み変数はすでにハードコーディングされているので、これらのために評価エントリを作成する必要はありません。
- アクションには、以下のいずれかの変数を使用できます。
- 各変数の説明は、上の「条件」の表にあります。
    - メソッド = $method$
    - パス = $path$
    - クエリストリング = $querystring$
    - Sourceip = $sourceip$
    - レスポンスコード（テキストには "200 OK "も含まれる） = $resp$
    - ホスト = $host$
    - バージョン = $version$
    - クライアントポート = $clientport$
    - Clientip = $clientip$
    - ジオロケーション = $geolocation$"

アクション例

- アクション = リダイレクト 302
    - ターゲット = HTTPs://$host$/404.html
- アクション＝ログ
    - ターゲット = $sourceip$:$sourceport$のクライアントが$path$ページをリクエストしました。

説明します。

- 存在しないページにアクセスしたクライアントには、通常、ブラウザの404ページが表示されます。
- この例では、ユーザーが使用した元のホスト名にリダイレクトされますが、間違ったパスは404.htmlに置き換えられます。
- syslogに "A client from 154.3.22.14:3454 has just made request to wrong.html page "というエントリが追加されます。

ソース	説明	例
クッキー	これは、クッキーヘッダーの名前と値です。	MS-WSMAN=afYfn1CDqqCDqUD::ここで、名前はMS-WSMAN、値はafYfn1CDqqCDqUD:.となります。
ホスト	これは、URLから抽出したホスト名	www.mywebsite.com または 192.168.1.1
言語	以下は、Language HTTPヘッダーから抽出された言語です。	この条件では、言語のリストを含むドロップダウンが生成されます。
方法	これは、HTTPメソッドのドロップダウンです。	ドロップダウンには、GET、POST
パス	これは、ウェブサイトのパス	/mywebsite/index.html
POST	POSTリクエストメソッド	Webサイトにアップロードされるデータのチェック

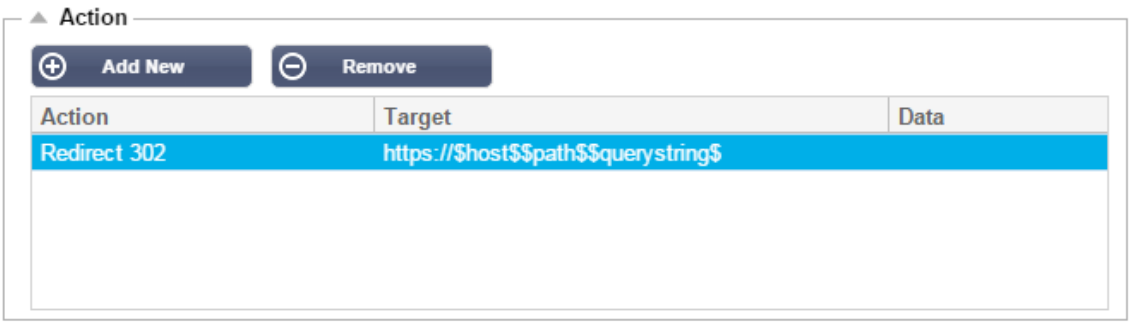
問い合わせ項目	これは、クエリの名前と値です。そのため、クエリー名または値も受け入れることができます。	"Best=jetNEXUS" マッチはBest、バリューはedgeNEXUSの場合
問い合わせ文字列	? "の後の文字列全体です。	HTTP://server/path/program?query_string
リクエストヘッダー	これは、クライアントが送信した任意のヘッダーであることができます	Referrer、User-Agent、From、Date...。
レスポンスヘッダー	これは、サーバーから送信された任意のヘッダーであることができます	Referrer、User-Agent、From、Date...。
バージョン	これがHTTPバージョン	HTTP/1.0またはHTTP/1.1

詳細	説明	例
受け入れ	許容されるコンテンツタイプ	Accept: text/plain
Accept-Encoding	使用可能なエンコーディング	Accept-Encoding: <compress | gzip | deflate | sdch | identity>。
アクセプト・ランゲージ	回答に使用できる言語	Accept-Language: en-US
受け入れ範囲	このサーバーがサポートしているパーシャルコンテンツの範囲タイプ	Accept-Ranges: bytes
オーソライズ	HTTP認証用の認証情報	オーソライズされています。基本QWxhZGRpbjpvcGVuIHNlc2FtZQ==。
チャージ・トゥー	要求された方法の適用に必要なコストのアカウント情報を含む	
Content-Encoding	データに使用されているエンコーディングの種類。	Content-Encoding: gzip
Content-Length	レスポンスボディの長さをオクテット（8ビットバイト）で表したもの	Content-Length: 348
コンテンツタイプ	リクエストの本文のmimeタイプ（POSTおよびPUTリクエストで使用されます	Content-Type: application/x-www-form-urlencoded
クッキー	Set-Cookie（下記）を用いてサーバーから送信されたHTTPクッキー	Cookie: $Version=1; Skin=new;
日付	メッセージが発信された日付と時間	Date = "日付" ":" HTTP-date
ETag	リソースの特定のバージョンを示す識別子で、多くはメッセージダイジェストです。	ETag:"aed6bdb8e090cd1:0"
より	リクエストを行ったユーザーのEメールアドレス	From: user@example.com
If-Modified-Since	コンテンツが変更されていない場合は、304 Not Modifiedを返すことができます。	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT

Last-Modified	リクエストされたオブジェクトの最終更新日（RFC2822形式）。	Last-Modified:Tue, 15 Nov 1994 12:45:26 GMT
Pragma	実装に特化したヘッダーで、リクエスト・レスポンスの連鎖のどこかで様々な影響を与える可能性があります。	Pragma: no-cache
リファラー	これは、現在要求されているページへのリンクを辿った前のウェブページのアドレスです。	リファラー：HTTP://www.edgenexus.io
サーバー	サーバーの名前	サーバーです。Apache/2.4.1 (Unix)
セット-クーキー	HTTPクッキー	セット-クーキーUserID=JohnDoe; Max-Age=3600; Version=1
User-Agent	ユーザーエージェントの文字列	User-AgentMozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Vary	ダウンストリームプロキシに対して、将来のリクエストヘッダーをどのように照合し、 オリジンサーバーから 新たなレスポンスをリクエストするのではなく、キャッシュされたレスポンスを使用できるかどうかを 判断する方法を伝えます。	Vary:User-Agent
X-Powered-By	Webアプリケーションを支える技術（ASP.NET、PHP、JBossなど）を指定します。	X-Powered-By:PHP/5.4.0

アクション

アクションとは、条件が満たされたときに有効になるタスクのことです。



アクション

Action "列をダブルクリックすると、ドロップダウンリストが表示されます。

ターゲット

Target列をダブルクリックすると、ドロップダウンリストが表示されます。リストはActionに応じて変化します。

いくつかのアクションでは、手動で入力することもできます。

データ

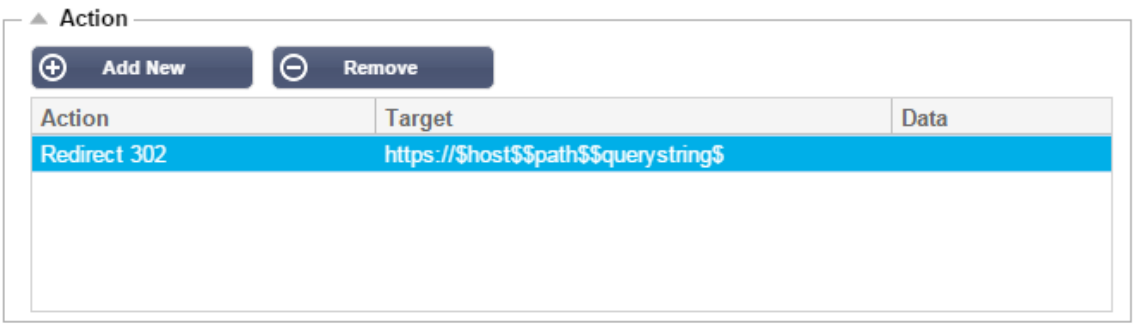
データ欄をダブルクリックして、追加・置換したいデータを手動で追加します。

すべてのアクションのリストは以下の通りです。

アクション	説明	例
追加リクエストクッキー	ターゲット」に記載されているリクエスト・クッキーを「データ」に記載されている値で追加します。	ターゲット＝クッキー データ= MS-WSMAN=afYfn1CDqqCDqCVii
リクエストヘッダーの追加	Dataセクションの値を持つTargetタイプのリクエストヘッダを追加する	ターゲット＝アクセプト データ=画像/png
レスポンスクッキーの追加	データセクションの値で、ターゲットセクションに詳述されたレスポンスクッキーを追加する	ターゲット＝クッキー データ= MS-WSMAN=afYfn1CDqqCDqCVii
レスポンスヘッダーの追加	Dataセクションの値でTargetセクションに詳細なリクエストヘッダーを追加する	Target= Cache-Control データ＝max-age=8888888
ボディはすべて交換	レスポンスボディを検索し、すべてのインスタンスを置き換える	Target= HTTP:// (検索文字列) Data= HTTPs:// (置換文字列)
ボディーリプレイスファースト	レスポンスボディを検索し、ファーストインスタンスのみを置き換える	Target= HTTP:// (検索文字列) Data= HTTPs:// (置換文字列)
ボディー・リプレイス・ラスト	レスポンスボディを検索し、最後のインスタンスのみを置き換える	Target= HTTP:// (検索文字列) Data= HTTPs:// (置換文字列)
ドロップ	これで接続が切れる	目標＝不詳 データ= N/A
電子メール	メールイベント」で設定したアドレスにメールを送信します。アドレスやメッセージには、変数を使用できます。	Target= "flightPATHはこのイベントにメールを送りました" データ= N/A
ログイベント	これにより、イベントがシステムログに記録されます	Target= "flightPATH has log this in syslog" データ= N/A
リダイレクト301	これにより、永久的なリダイレクトが行われます。	ターゲット= HTTP ://www.edgenexus.ioData= N/A
リダイレクト302	これにより、一時的なリダイレクトが行われます。	ターゲット= HTTP ://www.edgenexus.ioData= N/A
リクエストクッキーの削除	ターゲット」に記載されたリクエストクッキーの削除	ターゲット＝クッキー データ= MS-WSMAN=afYfn1CDqqCDqCVii
リクエストヘッダーの削除	ターゲット」に記載されたリクエストヘッダーを削除	Target= ServerData=N/A
レスポンスクッキーの削除	ターゲット」に記載されているレスポンスクッキーの削除	ターゲット=jnAccel

レスポンスヘッダーの削除	対象セクションに記載されているレスポンスヘッダーを削除	ターゲット= Etag データ= N/A
リクエストクッキーの交換	Targetセクションで指定されたリクエストクッキーをDataセクションの値で置き換える	ターゲット＝クッキー データ= MS-WSMAN=afYfn1CDqqCDqCVii
Replace Request Header	ターゲットのリクエストヘッダをDataの値で置き換える	対象＝接続 データ＝キープアライブ
レスポンスクッキーの交換	Targetセクションに記載されているレスポンスクッキーをDataセクションの値に置き換える	Target=jnAccel=afYfn1 CDqqCDqCViiDate=MS-WSMAN=afYfn1CDqqCDqCVii
応答ヘッダーの置き換え	Targetセクションに記載されているレスポンスヘッダーをDataセクションの値で置き換える	対象＝サーバー データ=セキュリティのため非公開
リライトパス	これにより、条件に応じてリクエストを新しいURLにリダイレクトすることができます。	ターゲット= /test/path/index.html$querystring$ データ= N/A
セキュアサーバーの使用	使用するセキュアサーバーや仮想サービスの選択	Target=192.168.101:443 Data=N/A
使用するサーバー	使用するサーバーや仮想サービスの選択	Target= 192.168.101:80 Data= N/A
クッキーの暗号化	これは、クッキーを3DES暗号化した後、base64エンコードします。	Target= 暗号化するクッキー名を入力、最後にワイルドカードとして*を使用してもよい Data= 暗号化のためのパスフレーズを入力

例



以下のアクションは、セキュアなHTTPSバーチャルサービスへの一時的なリダイレクトをブラウザに発行します。リクエストと同じホスト名、パス、クエリーストリングを使用します。

一般的な使い方

アプリケーションファイアウォールとセキュリティ

- 不要なIPをブロック
- 特定の（またはすべての）コンテンツに対してユーザーにHTTPSを強制する
- スパイダーをブロックまたはリダイレクトする
- クロスサイトスクリプティングの防止と警告

- SQLインジェクションの防止と警告
- 内部のディレクトリ構造を隠す
- リライトクッキー
- 特定のユーザーのためのセキュアなディレクトリ

特徴

- パスに基づいてユーザーをリダイレクト
- 複数のシステムへのシングルサインオンの提供
- ユーザーIDやクッキーをもとにしたユーザーのセグメント化
- SSLオフロード用ヘッダーの追加
- 言語検出
- ユーザーリクエストの書き換え
- 壊れたURLの修正
- ログとメールアラート 404レスポンスコード
- ディレクトリアクセス/ブラウジングの防止
- スパイダーに異なるコンテンツを送る

構築済みのルール

HTML拡張

すべての.htmリクエストを.htmlに変更

状態です。

- 条件＝パス
- センス＝ドーズ
- チェック＝マッチ RegEx
- Value = „^ᵚ^„)

評価

- ブランク

アクション

- アクション = Rewrite Path
- ターゲット = $path$I

Index.html

フォルダーへのリクエストでindex.htmlを強制的に使用する。

条件：この条件は、ほとんどのオブジェクトにマッチする一般的な条件です

- 条件＝ホスト
- センス＝ドーズ
- チェック＝存在する

評価

- ブランク

アクション

- アクション = リダイレクト 302
- ターゲット = HTTP://$host$$path$index.html$querystring$

フォルダーを閉じる

フォルダーへのリクエストを拒否する。

条件：この条件は、ほとんどのオブジェクトにマッチする一般的な条件です

- 条件＝これはちゃんと考えないと
- 感覚＝。
- チェック =

評価

- ブランク

アクション

- アクション =
- ターゲット =

CGI-BBINを隠す。

CGI スクリプトへのリクエストに cgi-bin カタログを隠します。

条件：この条件は、ほとんどのオブジェクトにマッチする一般的な条件です

- 条件＝ホスト
- センス＝ドーズ
- チェック＝マッチ RegEX
- Value = urchin.cgi$

評価

- ブランク

アクション

- アクション = Rewrite Path
- ターゲット = /cgi-bin$path$

ログスパイダー

人気のある検索エンジンのスパイダー・リクエストを記録する。

条件：この条件は、ほとんどのオブジェクトにマッチする一般的な条件です

- 条件＝リクエストヘッダー
- マッチ＝ユーザー・エージェント
- センス＝ドーズ
- チェック＝マッチ RegEX
- 値 = Googlebot|Slurp|bingbot|ia_archiver

評価

- 変数 = $crawler$
- ソース＝リクエストヘッダー
- 詳細＝ユーザー・エージェント

アクション

- アクション＝イベントのログ
- ターゲット = [$crawler$] $host$$path$$querystring$

強制的にHTTPSにする

特定のディレクトリに強制的にHTTPSを使用します。この場合、クライアントが /secure/ ディレクトリを含むものにアクセスすると、要求された URL の HTTP バージョンにリダイレクトされます。

状態です。

- 条件＝パス
- センス＝ドーズ
- チェック＝コンテイナー
- 値 = /secure/

評価

- ブランク

アクション

- アクション = リダイレクト 302
- ターゲット = HTTPs://$host$$path$$querystring$

メディアストリーム。

Flash Media Streamを適切なサービスにリダイレクトします。

状態です。

- 条件＝パス
- センス＝ドーズ
- チェック＝終了
- 値 = .flv

評価

- ブランク

アクション

- アクション = リダイレクト 302
- ターゲット = HTTP://$host$:8080/$path$

HTTPからHTTPSへの切り替え

ハードコードされているHTTP://をHTTPS://に変更する。

状態です。

- 条件＝レスポンスコード
- センス＝ドーズ
- チェック＝イコール
- 値＝200 OK

評価

- ブランク

アクション

- アクション＝ボディ・リプレイス・オール
- ターゲット = HTTP://
- データ = HTTPs://

クレジットカードの白紙化

回答の中にクレジットカードが入っていないことを確認し、入っていた場合は空白にします。

状態です。

- 条件＝レスポンスコード
- センス＝ドーズ
- チェック＝イコール
- 値＝200 OK

評価

- ブランク

アクション

- アクション＝ボディ・リプレイス・オール
- Target = [0-9]+[0-9]+[0-9]+[0-9]+-[0-9]+[0-9]+[0-9]+[0-9]+-[0-9]+[0-9]+[0-9]+[0-9]+-[0-9]+[0-9]+[0-9]+[0-9]+
- データ = xxxx-xxxx-xxxx-xxxx

コンテンツの有効期限

リクエストや304の数を減らすために、ページに賢明なコンテンツの有効期限を追加します。

条件：これはキャッチオールとしての一般的な条件です。この条件を重視することは、あなたの

- 条件＝レスポンスコード
- センス＝ドーズ
- チェック＝イコール
- 値＝200 OK

評価

- ブランク

アクション

- Action = 応答ヘッダーの追加
- 対象＝Cache-Control
- データ = max-age=3600

スプーフィング・サーバー・タイプ

サーバータイプを取得して、別のものに変更します。

条件：これはキャッチオールとしての一般的な条件です。この条件を重視することは、あなたの

- 条件＝レスポンスコード
- センス＝ドーズ
- チェック＝イコール
- 値＝200 OK

評価

- ブランク

アクション

- Action = Replace Response Header
- 対象＝サーバー
- データ＝シークレット

エラーを出さない

クライアントは、あなたのサイトからエラーが出ることはありません。

状態

- 条件＝レスポンスコード
- センス＝ドーズ
- チェック＝コンテイナー
- 値＝404

評価

- ブランク

アクション

- アクション = リダイレクト 302
- ターゲット = HTTP//$host$/

言語に関するリダイレクト

言語コードを検索して、関連する国のドメインにリダイレクトします。

状態

- 条件＝言語
- センス＝ドーズ
- チェック＝コンテイナー
- 値＝ドイツ語（標準

評価

- 変数 = $host_template$
- ソース＝ホスト
- Value €.

アクション

- アクション = リダイレクト 302
- ターゲット = HTTP//$host_template$de$path$$querystring$

Google Analytics

アナリティクス用にGoogleが要求するコードを挿入してください - 値MYGOOGLECODEをあなたのGoogle UA IDに変更してください。

状態

- 条件＝レスポンスコード
- センス＝ドーズ
- チェック＝イコール
- 値＝200 OK

評価

- ブランク

アクション

- アクション＝ボディ・リプレイス・ラスト
- ターゲット = </body>
- Data = <
  scripttype='text/javascript'> var _gaq = _gaq || []; _gaq.push(['_setAccount', 'MY GOOGLE CODE']); _gaq.push(['_trackPageview']); (function() { var ga = document.createElement('script'); ga.type = 'text/javascript'; ga.async = true; ga.src = ('HTTPs' == document.location.protocol ?'HTTPs//ssl' 'HTTP//www') + '.google-analytics.com/ga.js'; var s = document.getElementsByTagName('script')[0];s.parentNode.insertBefore(ga, s); }.)(); </script> </body> </divine

IPv6ゲートウェイ

IPv6サービス上のIIS IPv4サーバーのホストヘッダーを調整する。IIS IPv4サーバーは、ホストクライアントの要求にIPV6アドレスが含まれることを好まないため、このルールではこれを一般的な名前に置き換えます。

状態

- ブランク

評価

- ブランク

アクション

- Action = Replace Request Header

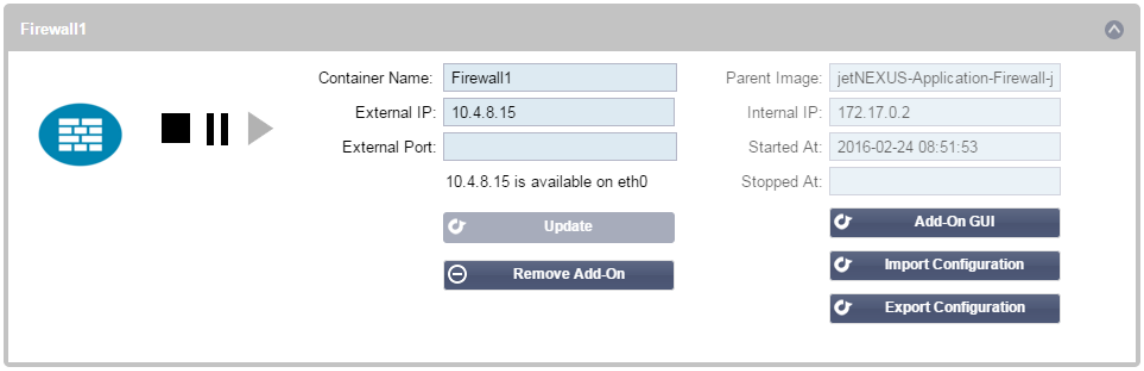
- ターゲット＝ホスト
- データ =ipv4.host.header

Webアプリケーション・ファイアウォール（edgeWAF

Web Application Firewall (WAF) はご要望に応じて利用でき、年間課金ベースでライセンスされます。WAFのインストールは、ADCに内蔵されているAppsセクションを使って行います。

WAFの運用

Dockerコンテナ内で動作するWAFは、起動前にいくつかのネットワークパラメータを設定する必要があります。

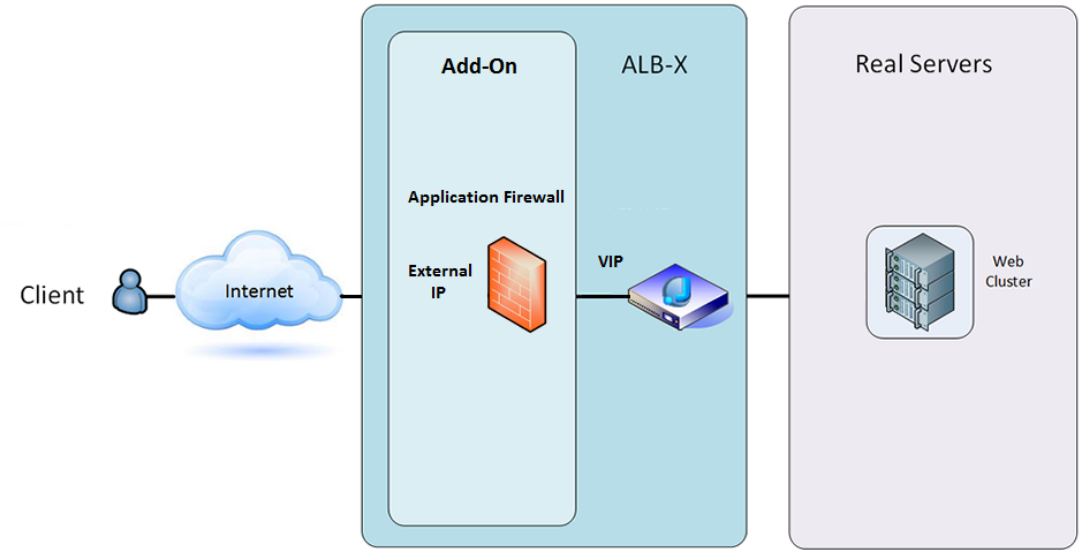


オプション	説明
ストップ	Add-Onインスタンスが開始されるまではグレーアウトしています。このボタンを押すと、Dockerインスタンスが停止します。
ポーズ	このボタンは、Add-Onを一時停止します。
プレイ	現在の設定でAdd-Onを起動します。
コンテナ名	自分のコンテナには、他のコンテナと区別するための名前を付けてください。これは一意でなければなりません。この名前をリアルサーバの名前として使用すると、インスタンスの内部IPアドレスに自動的に解決されます。
外部IP	ここでは、アドオンにアクセスするための外部IPを設定できます。これは、アドオンのGUIや、アドオンを介して実行されるサービスにアクセスするためのものです。ファイアウォールアドオンの場合、これはHTTPサービスのIPアドレスです。ファイアウォールは、ロードバランシングのために複数のサーバを含むサーバや ALB-X VIP にアクセスするように設定することができます。
外部ポート	この項目を空白にしておくと、すべてのポートがファイアウォールに転送されます。これを制限するには、カンマで区切られたポートリストを追加します。例 80, 443, 88.ファイアウォールのGUIアドレスは**HTTP//[外部IP]88/waf**になることに注意してください。したがって、外部ポートの設定を空白にするか、ポートリストを制限する場合はGUIにアクセスするためのポート88を追加してください。
アップデート	アドオンの設定を更新できるのは、インスタンスが停止してからです。インスタンスが停止した後は、コンテナ名、外部IP、外部ポートの設定を変更することができます。
アドオンの削除	Add-OnページからAdd-Onを完全に削除します。再びアドオンを展開するには、Library-Appsページに移動する必要があります。
親のイメージ	Add-OnがビルドされたDockerイメージを示します。Firewallや他のタイプのAdd-Onには複数のバージョンが存在する可能性があるため、これはそれらを区別するのに

	役立ちます。このセクションは情報提供のみを目的としているため、グレーアウトされています。
内部IP	Dockerは内部IPアドレスを自動的に作成するため、編集することはできません。また、Dockerインスタンスを停止して再起動すると、新しい内部IPアドレスが発行されます。このような理由から、サービスに外部IPアドレスを使用するか、サービスのリアルサーバーアドレスにコンテナ名を使用する必要があります。
開始日	これは、Add-Onが開始された日時を記載します。例 2016-02-16 155721
Stopped At	Add-Onが停止した日時が記載されます。例 2016-02-24 095839

アーキテクチャ例

外部IPアドレスを使用するWAF

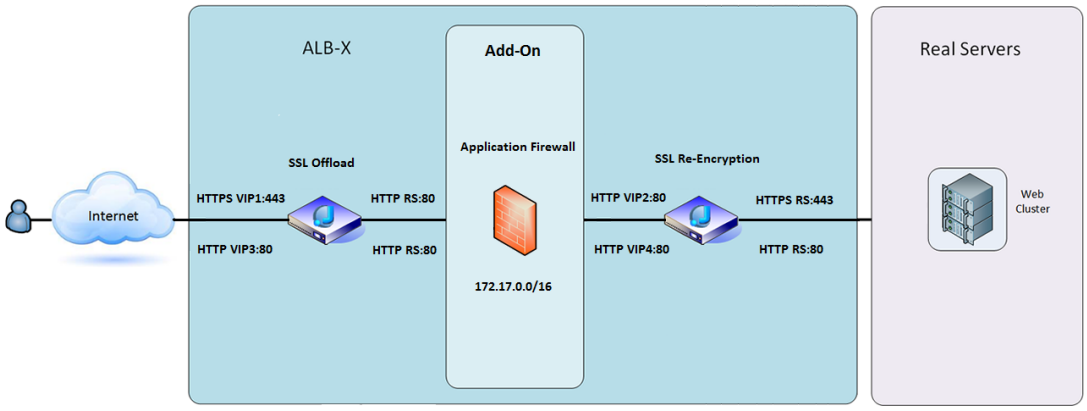


このアーキテクチャでは、Firewall が HTTPS トラフィックを検査できないため、サービスには HTTP しか使用できません。

また、ALB-X VIP にトラフィックを送るように Firewall を設定する必要があります。

ALB-X VIPは、Webクラスタへのトラフィックをロードバランスするように設定されています。

内部IPアドレスを使用するWAF



このアーキテクチャでは、HTTPとHTTPSを指定することができます。

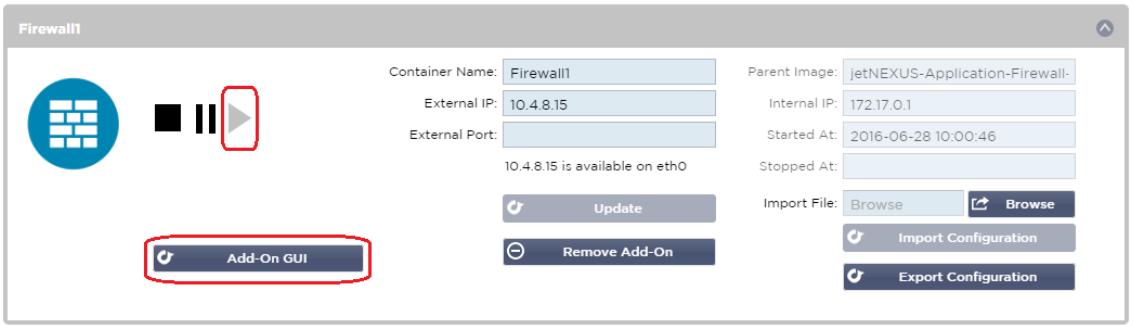
HTTPSは、クライアントからALB-Xへの接続と、ALB-Xからリアルサーバへの接続を暗号化するエンド・ツー・エンドにすることができます。

ALB-Xからファイアウォールの内部IPアドレスへのトラフィックは、検査できるように暗号化を解除する必要があります。

トラフィックがファイアウォールを通過すると、別のVIPに転送され、VIPはトラフィックを再暗号化して安全なサーバーにロードバランスするか、単にHTTPで安全でないサーバーにロードバランスすることができます。

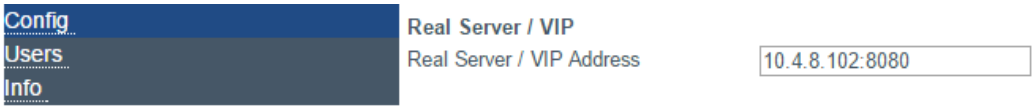
WAFアドオンへのアクセス

- ファイアウォールの詳細を入力する
- ポートを必要なものだけに制限することも、空白にしてすべてのポートを許可することもできます。
- 再生ボタンをクリック
- Add-On GUIボタンが表示されます。

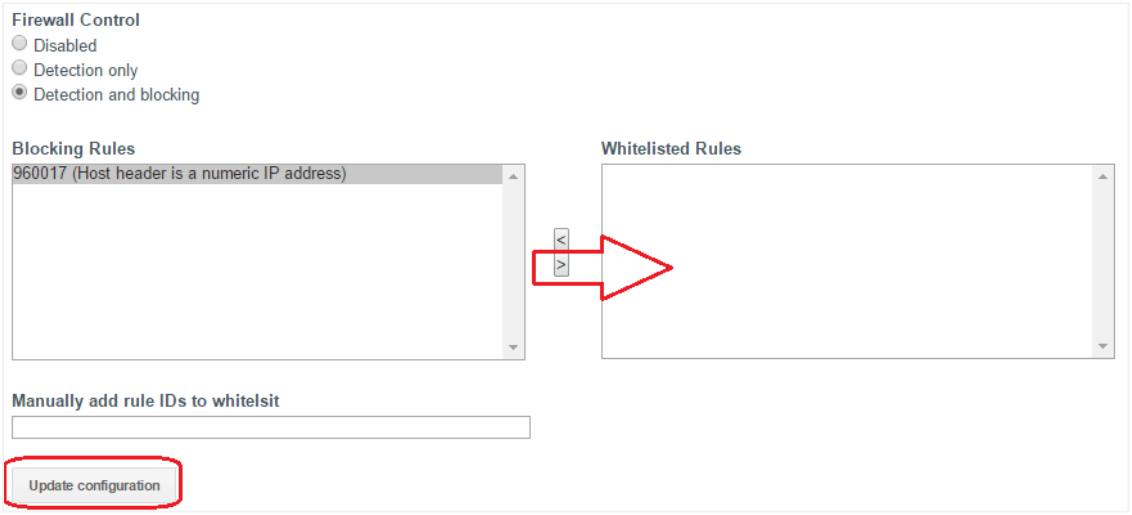


- このボタンをクリックすると、HTTP://[外部IP]:88/wafのブラウザが起動します。
- この例では、HTTP://10.4.8.15:88/wafとなります。
- ログインダイアログが表示されます。
- ADCの認証情報を入力します。
- ログインが完了すると、WAFのホームページが表示されます。

- ホーム画面では、アプリケーションファイアウォールが実行したフィルタリングアクションであるイベントの概要がグラフィカルに表示されます。
- 最初にページを開いたときは、ファイアウォールを介したアクセスがないため、グラフが空白になっていることがほとんどです。
- ファイアウォールがトラフィックをフィルタリングした後に、トラフィックを送信するIPアドレスまたはウェブサイトのドメイン名を設定することができます。
- これはManagement > Configセクションで変更できます。



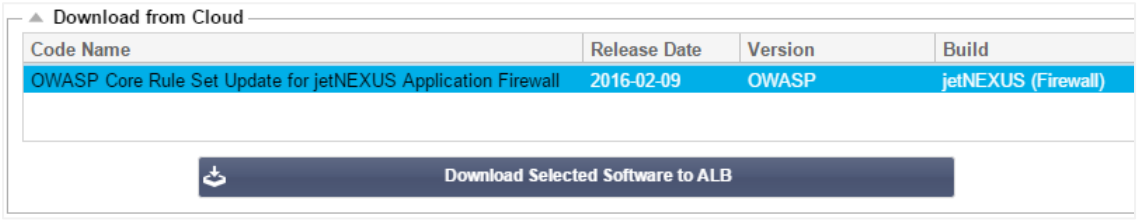
- ファイアウォールは、トラフィックを検査してから、ここにあるリアルセブルIPまたはVIPアドレスに送信します。IPアドレスと一緒にポートを入力することもできます。IPアドレスを単独で入力した場合、そのポートは80番ポートとみなされます。設定の更新」ボタンをクリックすると、この新しい設定が保存されます。
- ファイアウォールがアプリケーションリソースをブロックすると、トラフィックをブロックしているルールが「ホワイトリスト」ページの「ブロックルール」リストに表示されます。
- ファイアウォールが有効なアプリケーションリソースをブロックしないようにするには、ブロックルールをホワイトリストルールのセクションに移動してください。



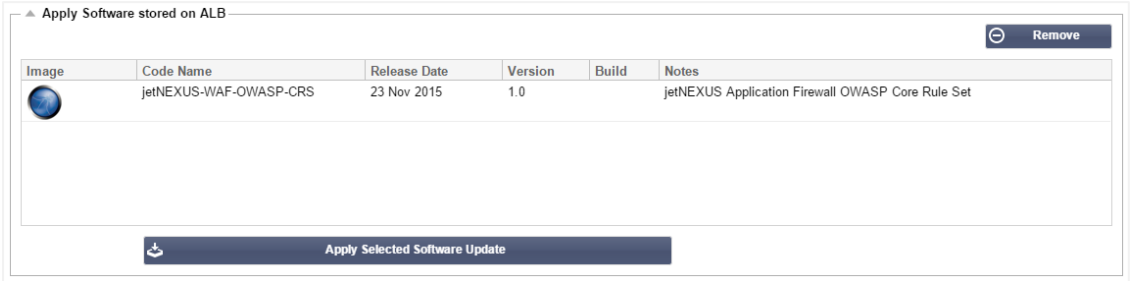
- BlockingセクションからWhitelistセクションにすべてのルールを転送したら、Update Configuration を押します。

ルールの更新

- アプリケーションファイアウォールのルールを更新するには、「Advanced - Software」セクションにアクセスします。
- Refresh "をクリックすると、"Software Upgrade Details "セクションに利用可能なソフトウェアボタンが表示されます。
- クラウドからのダウンロード」という追加のボックスが表示されるようになりました。
- OWASPコア・ルール・セットが利用できるかどうかを確認する。

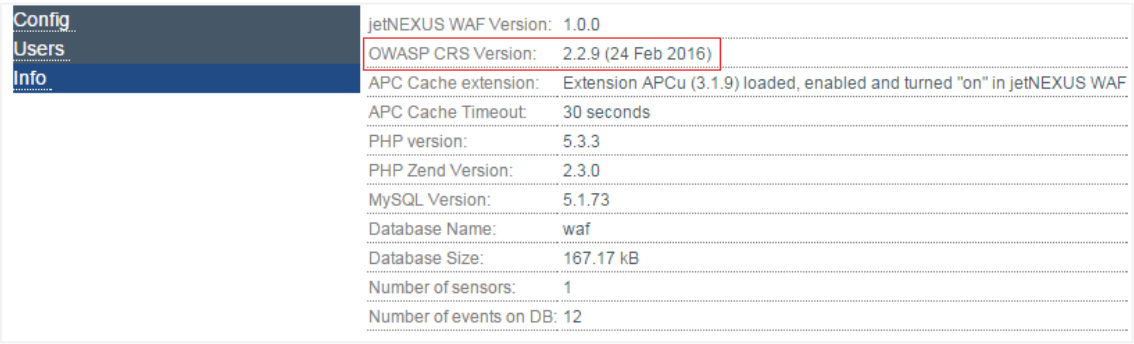


- その場合は、ハイライトして「選択したソフトウェアをALB-Xにダウンロード」をクリックします。
- これにより、ALB に格納されている Apply Software にスマートファイルがダウンロードされます。



- jetNEXUS-WAF-OWASP-CRSをハイライト表示し、「Apply Selected Software Update」をクリックし、「Apply」をクリックします。
- ファイアウォールは、更新されたルールセットを自動的に検出し、ロードして適用します。
- ホワイトリストに登録されているルールのIDは維持されます。ただし、新しいルールが有効なアプリケーションリソースをブロックするようになる可能性があります。

- この場合は、ホワイトリストページの「ブロックルール」リストを確認してください。
- また、ファイアウォール GUI の「管理情報」セクションで OWASP CRS のバージョンを確認することができます。



グローバルサーバーロードバランシング（edgeGSLB

はじめに

グローバルサーバーロードバランシング（GSLB）とは、インターネット上でネットワークトラフィックを分散させる手法を指す言葉です。GSLBはサーバーロードバランシング（SLB）やアプリケーションロードバランシング（ALB）とは異なり、従来のADC/SLBが単一のデータセンター内でトラフィックを分散させるのに対し、GSLBは複数のデータセンター間でトラフィックを分散させるために使用されるのが一般的である。

GSLBは通常、以下のような状況で使用されます。

レジリエンシーとディザスタリカバリ

複数のデータセンターがあり、それらをActive-Passiveで運用し、一方のデータセンターに障害が発生しても、もう一方のデータセンターにトラフィックが送られるようにしたいと考えています。

ロードバランシングとジオロケーション

データセンターのパフォーマンス、データセンターの能力、データセンターのヘルスチェック、クライアントの物理的な位置（最も近いデータセンターに送信できるように）などの特定の基準に基づいて、Active-Activeの状況でデータセンター間のトラフィックを分配したいと考えています。

商用面での配慮

特定の地域のユーザーが特定のデータセンターに送られるようにする。クライアントがいる国、リクエストしているリソース、言語などのいくつかの条件に応じて、他のユーザーに異なるコンテンツを提供（またはブロック）するようにする。

ドメインネームシステムの概要

GSLBは複雑なので、不思議なドメインネームサーバー（DNS）システムの仕組みを理解するために時間をかける価値があります。

DNSは3つの重要な要素で構成されています。

- DNSリゾルバ、すなわちクライアント：リゾルバは、最終的に必要なリソースの完全な解決につながるクエリを開始する責任があります。
- ネームサーバー：クライアントがDNSの解決を行うために最初に接続するネームサーバーのことです。
- 権威あるネームサーバー。トップレベルドメイン（TLD）のネームサーバーとルートネームサーバーを含む。

典型的なDNSトランザクションを以下に説明します。

- ユーザーがWebブラウザに「example.com」と入力すると、そのクエリがインターネット上に伝わり、DNSの再帰的リゾルバに受信されます。
- その後、リゾルバはDNSルートネームサーバ（...）に問い合わせます。
- そして、ルートサーバーは、トップレベルドメイン（TLD）のDNSサーバー（.comや.netなど）のアドレスをレゾルバに応答し、そのドメインの情報を保存します。example.comを検索する場合、私たちのリクエストは.com TLDに向けられます。

- そしてリゾルバは、.com TLDをリクエストします。
- そして、TLDサーバは、ドメインのネームサーバであるexample.comのIPアドレスを応答します。
- 最後に、再帰的リゾルバは、ドメインのネームサーバにクエリを送信します。
- そして、ネームサーバーから、example.comのようなIPアドレスがリゾルバに返されます。
- DNSリゾルバは、最初に要求されたドメインのIPアドレスをWebブラウザに応答します。
- DNS検索の8つのステップでIPアドレス（example.com）が返されると、ブラウザはWebページを要求できるようになります。
- ブラウザは、IPアドレスに対して**HTTP**リクエストを行います。
- そのIPのサーバーは、ブラウザでレンダリングされるべきウェブページを返します。

このプロセスはさらに複雑になります。

キャッシング

リゾルバがレスポンスをキャッシュすることで、多くのクライアントに同じレスポンスを送ることができます。クライアント側のリゾルバとアプリケーションは、異なるキャッシュポリシーを持つことがあります。

注：テストのために、オペレーティングシステムのサービスセクション内のWindows DNSクライアントを停止して無効にします。 DNS名は引き続き解決されますが、結果のキャッシュやコンピュータ名の登録は行われません。他のサービスに影響を与える可能性がありますので、システム管理者は、この方法がお客様の環境に最適なオプションであるかどうかを判断する必要があります。

Time To Live

解決側のネームサーバーは、TTL（Time To Live）、つまりレスポンスのキャッシュタイムを無視することがあります。

GSLBの概要

GSLBはDNSをベースにしており、上述したような非常に似た仕組みを採用しています。

ADCは、このガイドで後述するいくつかの要因に基づいて応答を変更することができます。ADCは、リソース自体にアクセスしてリモートリソースの可用性をチェックするモニターを利用しています。しかし、何らかのロジックを適用するには、システムがまずDNSリクエストを受信する必要があります。

いくつかのデザインがこれを可能にします。1つ目は、GSLBが権威あるネームサーバーとして機能する場合です。

2つ目のデザインは最も一般的な実装で、権威的なネームサーバーの構成と似ていますが、サブドメインを使用します。プライマリの権威DNSサーバーはGSLBに置き換えられず、サブドメインに解決を委任します。名前を直接委譲するか、CNAMEを使用するかで、GSLBで処理するものとしないものをコントロールすることができます。この場合、GSLBを必要としないシステムでは、すべてのDNSトラフィックをGSLBにルーティングする必要はありません。

冗長性を持たせることで、1つのネームサーバー（GSLB）に障害が発生しても、リモートネームサーバーが自動的に別のGSLBに別のリクエストを発行し、ウェブサイトのダウンを防ぐことができます。

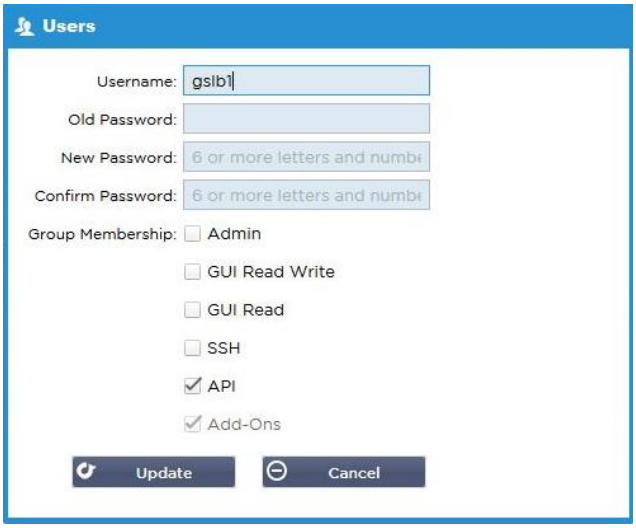
GSLBの構成

GSLBアドオンをダウンロードした後、ADC GUIのLibrary > Appsページにアクセスし、以下のように「Deploy」ボタンをクリックして、GSLBアドオンをデプロイしてください。

インストール後、ADC GUIのLibrary > Add-Onsページで、下図のようにGSLBアドオンの詳細（コンテナ名、外部IP、外部ポートなど）を設定してください。

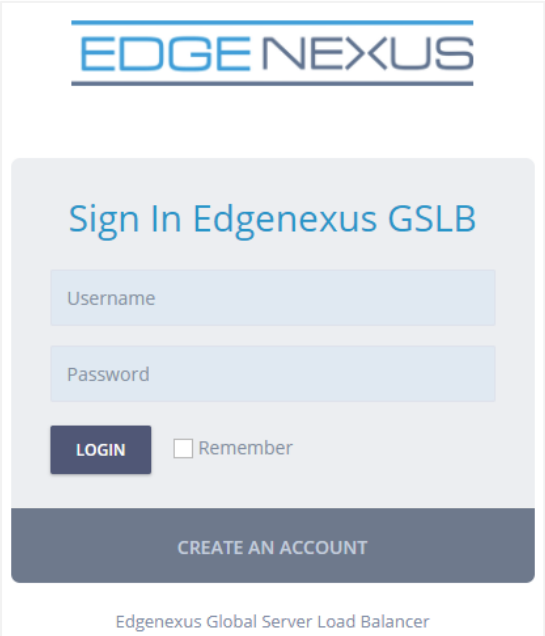
- コンテナ名は、ADC がホストする実行中のアドオンインスタンスの一意の名前で、同じ種類の複数のアドオンを区別するために使用されます。
- 外部IPは、GSLBに割り当てられるネットワーク上のIPです。
- GEOベースの決定を行う場合は、GSLBに外部IPアドレスを設定する必要があります。これにより、GSLBはクライアントの実際のIPアドレスを見ることができます。
- 外部ポートは、他のネットワークホストからアクセス可能なGSLBのTCPおよびUDPポートのリストです。
- 外部ポートの入力欄に「53/UDP, 53/TCP, 9393/TCP」と入れて、DNS（53/UDP, 53/TCP）とedgeNEXUS GSLBのGUI通信（9393/TCP）を許可してください。
- アドオンの詳細を設定した後、「更新」ボタンをクリックしてください。
- 実行ボタンをクリックしてGSLB Add-Onを起動します。

- 次のステップは、edgeNEXUS GSLB Add-OnがADCの設定を読み込んで変更できるようにすることです。
- ADC GUIのSystem > Usersページにアクセスし、下図のように、導入したGSLB Add-Onと同じ名前のユーザーを編集してください。
- gslb1」ユーザーを編集して「API」にチェックを入れ、「更新」をクリックします。ただし、最近のバージョンでは、デフォルトでチェックが入っている場合があります。



- 次のステップは、テストや評価目的でGSLBを構成し、インターネット上のDNSゾーンデータを変更したくない場合にのみ必要です。
- この場合、下図のようにADCのGUIの「システム」→「ネットワーク」ページの「DNSサーバー1」を変更して、GSLB Add-Onをプライマリ DNSリゾルブサーバーとして使用するように指示してください。
- DNSサーバー2は、一般的にローカルのDNSサーバー、またはGoogle 8.8.8.8などのインターネット上のDNSサーバーを設定することができます。

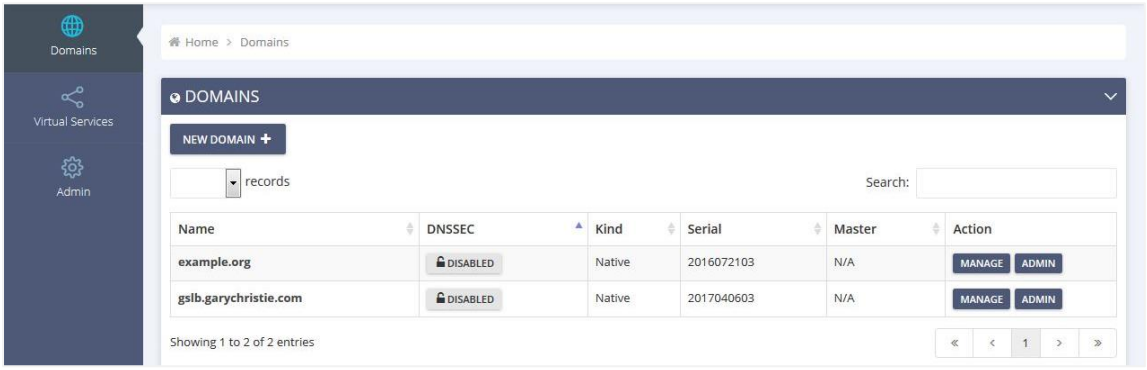
- ここで、GSLBのGUIにログインします。
- ADC GUIのLibrary > Add-Onsページに移動し、Add-On GUIボタンをクリックしてください。
- クリックすると、以下のようなGSLB GUIのログイン画面が表示されます。



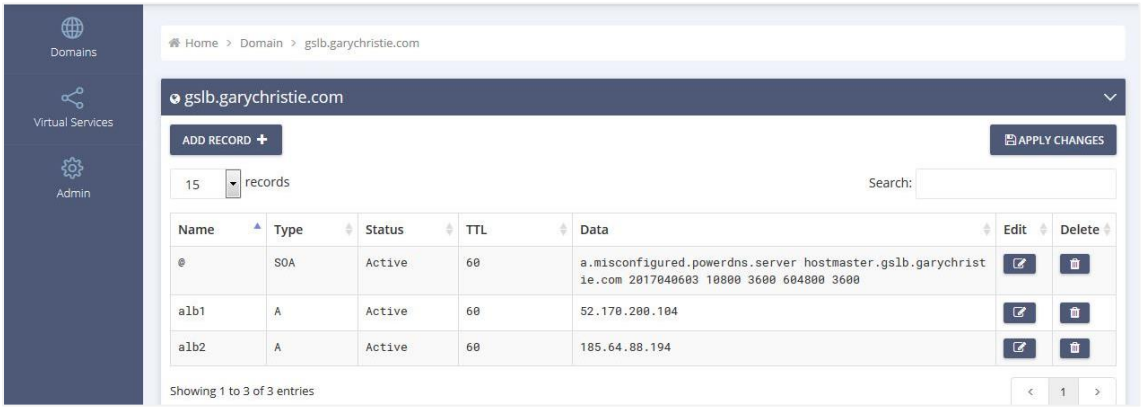
- デフォルトのユーザー名はadmin、デフォルトのパスワードはjetnexusです。GSLB GUIのAdministrator > My Profileページでパスワードの変更を忘れずに行ってください。

- 設定手順の次のステップは、GSLBの一部であるPowerDNSネームサーバーにDNSゾーンを作成し、「example.org」ゾーンの権威ネームサーバーか、前述の「DNSベースのGSLBの概要」の項で述べた「geo.example.org」サブドメインのようなサブドメインゾーンにします。
- DNSゾーン構成の詳細については、**PowerDNS Nameserverのドキュメント**を参照してください。図6にゾーンの例を示します。

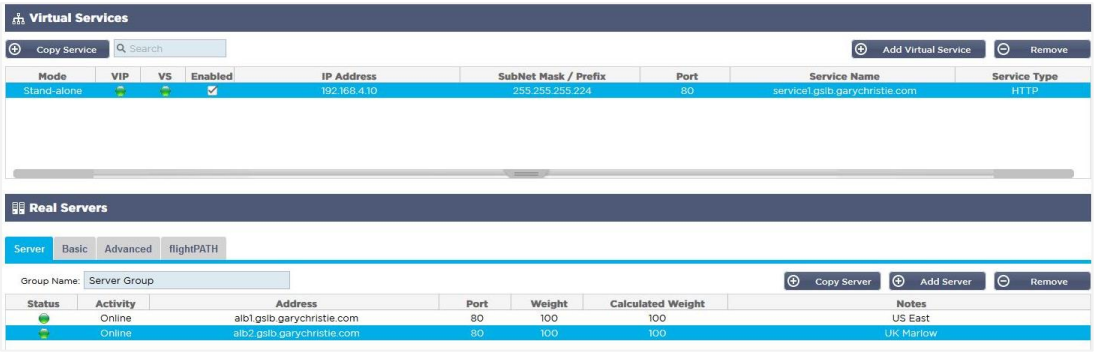
edgeNEXUS GSLBのGUIは、オープンソースプロジェクトであるPowerDNS-Adminをベースにしています。



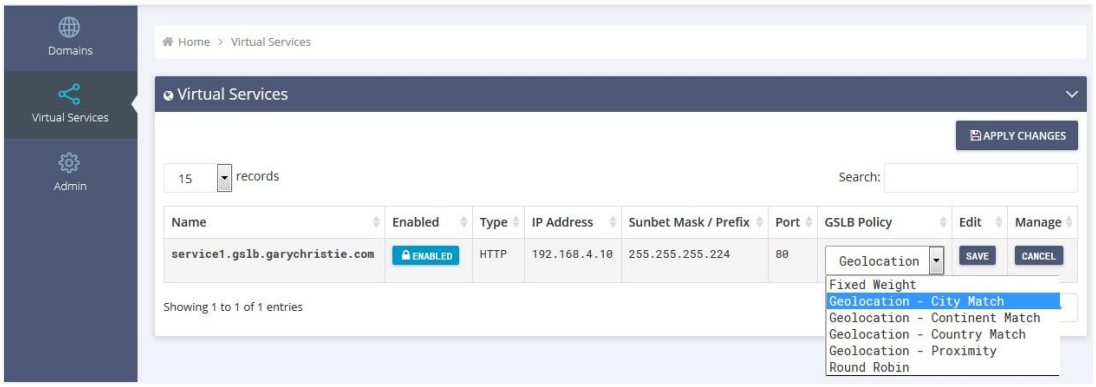
- DNSゾーンの作成後、管理ボタンをクリックし、下図のようにホスト名をドメインに追加してください。
- GSLBのGUIで既存のレコードを編集した後、Saveボタンを押してください。
- ホスト名レコードの作成が完了したら、「Apply Changes」ボタンをクリックしてください。Apply」をクリックせずにページを修正すると、変更内容が失われてしまいます。
- 以下では、IPv4アドレスのレコードを作成しています。
- IPv6アドレスのAAAAレコードを含め、解決したいすべてのレコードのレコードを作成してください。



- では、ADCのGUIに戻って、先ほど作成したDNSゾーンに対応するバーチャルサービスを定義してみましょう。



- このバーチャルサービスは、GSLBドメイン内のサーバーのヘルスチェックに使用されます。
- GSLBは、カスタムモニターを含む、ADCのヘルスチェックメカニズムを活用しています。GSLBは、ADCがサポートしているすべてのサービスタイプで使用することができます。
- 下図のように、ADC GUIの「サービス」>「IP-サービス」ページに移動し、バーチャルサービスを作成してください。
- サービス名」には、GSLBで使用したい正しいドメイン名を設定してください。GSLBはAPIを介してこの情報を読み取り、GSLB GUIのバーチャルサービスセクションに自動的に入力します。
- 上の画像の「リアルサーバー」の下に、GSLBドメインのすべてのサーバーを追加してください。
- サーバーは、ドメイン名またはIPアドレスで指定することができます。
- ドメイン名を指定した場合は、GSLBに作成されたレコードが使用されます。
- 基本」タブと「詳細」タブでは、異なるサーバーヘルス監視方法とパラメーターを選択できます。
- Active-Passiveシナリオでは、一部のサーバーのアクティビティをStandbyに設定することができます。
- この場合、「Online」サーバーがヘルスチェックに失敗し、健全な「Standby」サーバーがある場合、Edgenexus EdgeGSLBはドメイン名をStandbyサーバーのアドレスに解決します。
- バーチャルサービスの設定については、「バーチャルサービス」の項を参照してください。
- では、GSLBのGUIに移りましょう。
- 仮想サービス」ページに移動し、ADC仮想サービスセクションから取得したAPIのドメインのGSLBポリシーを選択します。
- 下図のようになります。



- GSLBは以下の方針を支持します。

ポリシー	説明
固定ウェイト	GSLBは、最も高いウェイトを持つサーバーを選択する（サーバーのウェイトは、ユーザーが割り当てることができる）。複数のサーバーが最も高いウェイト

	を持っている場合、GSLBはその中からランダムに1つのサーバーを選択します。
ウェイト付きラウンドロビン	サーバーを1台ずつ順番に選んでいきます。ウェイトの高いサーバーは、ウェイトの低いサーバーよりも多く選択されます。
ジオロケーション	近接性 - 地理的な緯度と経度のデータを使用して、クライアントの所在地に最も近い場所にあるサーバーを選択します。お客様と同じ国にあるサーバーが優先されますが、近隣の国のサーバーよりも遠くても構いません。
ジオロケーション	都市の一致 - クライアントと同じ都市にあるサーバーを選択します。クライアントの都市にサーバーがない場合は、クライアントの国のサーバーを選択します。クライアントの国にサーバーがない場合は、同じ大陸にあるサーバーを選択します。それができない場合は、地理的な緯度と経度のデータを使って、お客様の所在地に最も近い場所にあるサーバーを選択します。
ジオロケーション	国合わせ - クライアントと同じ国のサーバーを選択します。同じ国にサーバーがない場合は、同じ大陸を試し、次に最も近い場所を試します。
ジオロケーション	大陸一致 - クライアントと同じ大陸にあるサーバーを選択します。同じ大陸にサーバーがない場合は、最も近い場所を探します。

- GSLBポリシーを選択した後、「変更の適用」ボタンを忘れずにクリックしてください。
- ここで「管理」ボタンをクリックすると、バーチャルサービスの詳細を確認・調整することができます。
- 以下のようなページが表示されます。
- ウェイトベースのポリシーを選択している場合は、サーバーのGSLBウェイトを調整する必要があります。
- ジオロケーションベースのGSLBポリシーを選択した場合、サーバーの地理的データを指定する必要があります。
- サーバの地理的データを何も指定しない場合、GSLBはMaxMindのGeoLite2データベースが提供するデータを使用します。
- また、このページでは、サーバー名、ポート、アクティビティを変更することもできます。
- これらの変更は、"Apply Changes "ボタンをクリックすると、ADCと同期します。

- GSLBがどのような答えをクライアントに送り返すかを確認するには、NSLOOKUPを使うのが良いでしょう。
- Windowsをお使いの方は、以下のコマンドをご利用ください。

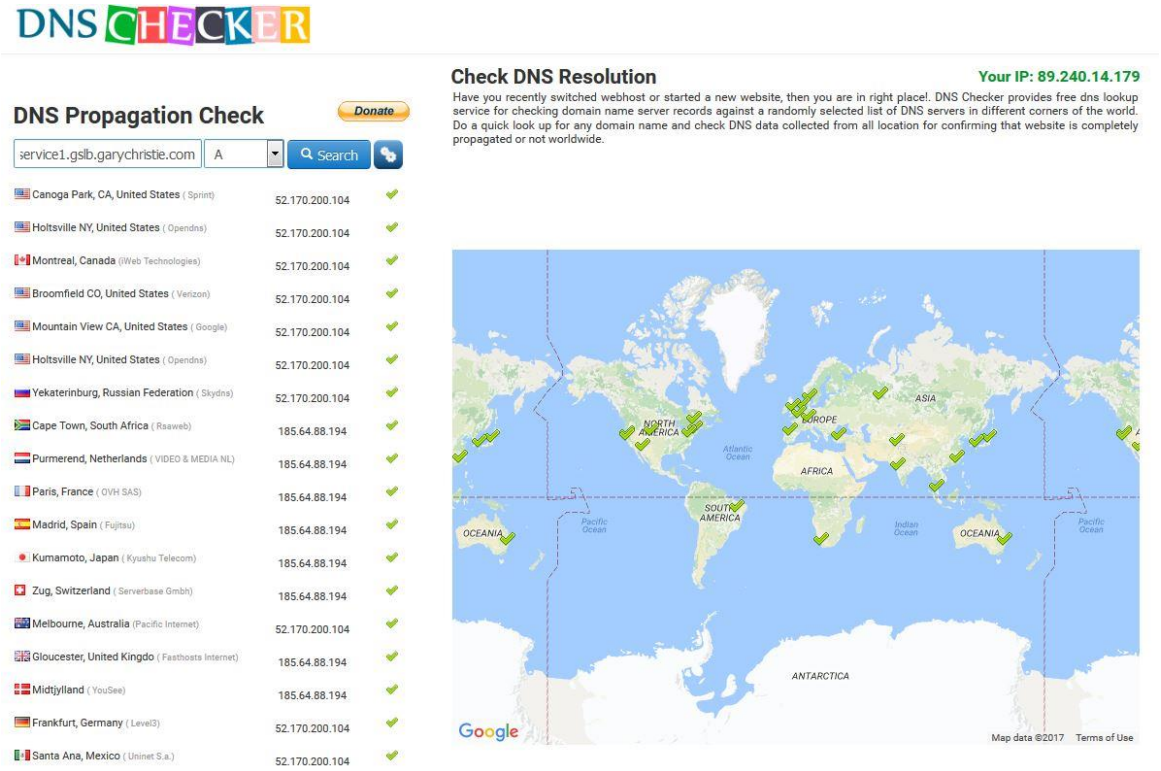
```
NSLOOKUP service1.gslb.garychristie.com 192.168.4.10
```

- service1.gslb.garychristie.comは、解決したいドメイン名です。

- 192.168.4.10は、GSLBの外部IPアドレスです。
- インターネット上でどのようなIPアドレスが返ってくるかを確認するには、googleのDNSサーバーである8.8.8.8を利用するとよいでしょう。

  Nslookup service1.gslb.garychristie.com 8.8.8.8.

- 代わりに、HTTPs://dnschecker.orgのようなものを使用することもできます。
  例 HTTPs://dnschecker.org/#A/service1.gslb.garychristie.com.
- 結果の一例は以下の通りです。



カスタムロケーション

プライベートネットワーク

また、GSLBは、カスタムロケーションを使用するように設定することができるので、内部の「プライベート」ネットワークで使用することができます。上記のシナリオでは、GSLBは、クライアントのパブリックIPアドレスをデータベースと照合してクライアントの位置を決定します。また、同じデータベースからサービスIPアドレスの位置を割り出し、ロードバランシングポリシーがGEOポリシーに設定されている場合は、最も近いIPアドレスを返します。この方法はパブリックIPアドレスに対しては完璧に機能しますが、IPv4アドレスがRFC1918、IPv6アドレスがRFC4193に準拠している内部のプライベートアドレスに対してはそのようなデータベースはありません。

プライベートアドレスについては、ウィキペディアのページを参照してください
HTTPS://EN.WIKIPEDIA.ORG/WIKI/PRIVATE_NETWORK

その仕組み

一般的に、GSLBを内部ネットワークに使用するのは、特定のアドレスのユーザーが、どのネットワークにいるかによって、サービスに対する異なる回答を受け取るようにするためです。例えば、NorthとSouthという2つのデータセンターが、それぞれnorth.service1.gslb.comとsouth.service1.gslb.comというサービスを提供しているとしましょう。北側のデータセンターからGSLBに問い合わせがあった場合、サービスが正

常に動作していれば、GSLBはnorth.service1.gslb.comに関連付けられたIPアドレスで応答するようにします。一方、南側のデータセンターからGSLBに問い合わせがあった場合、サービスが正常に動作していれば、GSLBは再びsouth.service1.gslb.comに関連するIPアドレスで応答することが望まれます。

では、上記のシナリオを実現するためにはどうすればいいのでしょうか。

- 少なくとも2つのCustom Locationsが必要で、各データセンターに1つずつ必要です。
- 様々なプライベートネットワークをこれらの場所に割り当てる
- 各サービスをそれぞれのロケーションに割り当てる

GSLBでこの外観を設定するには？

北部データセンターの場所を追加

- 左側の「カスタムロケーション」をクリック
- Add Location」をクリックします。
- 名前
  - 北
- 北部ネットワークのプライベートIPアドレスとサブネットマスクを追加します。この演習では、サービスとクライアントのIPアドレスが同じプライベートネットワーク内にあると仮定します。
  - 10.1.1.0/24
- 大陸コードの追加
  - EU
- 国コードの追加
  - イギリス
- 都市の追加
  - エンフィールド
- 緯度の追加 - googleから取得
  - 51.6523
- 経度の追加 - googleから取得
  - 0.0807

なお、正しいコードはこちらから入手できます。

南部データセンターの場所を追加

- 左側の「カスタムロケーション」をクリック
- Add Location」をクリックします。
- 名前
  - 南
- 南部ネットワークのプライベートIPアドレスとサブネットマスクを追加します。この演習では、サービスとクライアントのIPアドレスが同じプライベートネットワーク内にあることを前提としています。
  - 192.168.1.0/24
- 大陸コードの追加
  - EU
- 国コードの追加
  - イギリス
- 都市の追加
  - クロイドン
- 緯度の追加 - googleから取得

    - 51.3762
- 経度の追加 - googleから取得
    - 0.0982

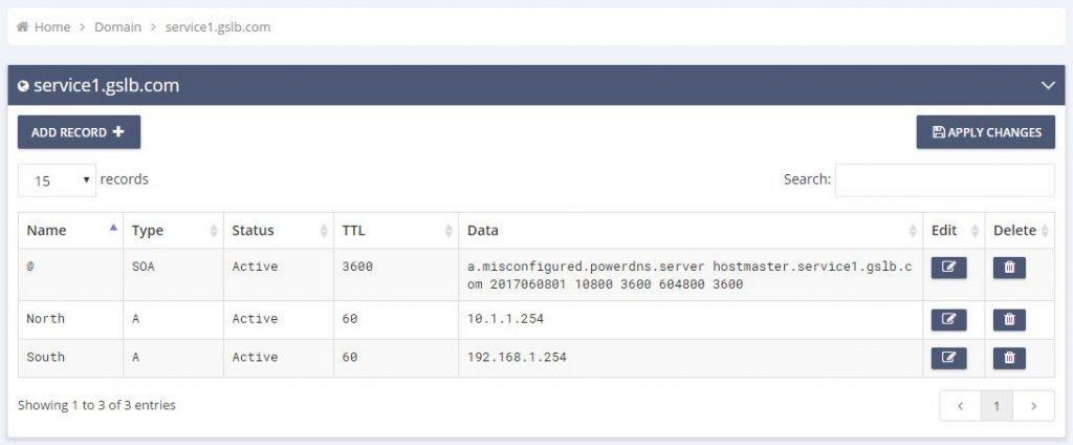
なお、正しいコードはこちらから入手できます。

north.service1.gslb.comのAレコードの追加

- ドメインservice1.gslb.comをクリックします。
- レコードの追加」をクリックします。
- 名前の追加
    - 北
- タイプ
    - A
- ステータス
    - アクティブ
- TTL
    - 1分
- IPアドレス
    - 10.1.1.254（Enfieldの所在地と同じネットワーク内にあることに注意してください。

south.service1.gslb.comのAレコードの追加

- ドメインservice1.gslb.comをクリックします。
- レコードの追加」をクリックします。
- 名前の追加
    - 南
- タイプ
    - A
- ステータス
    - アクティブ
- TTL
    - 1分
- IPアドレス
    - 192.168.1.254（ここはCroydonの所在地と同じネットワーク内です。



トラフィックフロー

例1 - 北部データセンターのクライアント

- クライアントIP 10.1.1.23は、service1.gslb.comのGSLBを問い合わせます。
- GSLBは、IPアドレス10.1.1.23を調べて、カスタムロケーションEnfield 10.1.1.0/24と照合します。
- GSLBは、service1.gslb.comのAレコードを確認し、ネットワーク10.1.1.0/24に含まれるnorth.service1.gslb.comにマッチします。
- GSLBは10.1.1.23に対して、service1.gslb.comのIPアドレス10.1.1.254を応答します。

例2 - 南部データセンターのクライアント

- クライアントIP 192.168.1.23 service1.gslb.comのGSLBへの問い合わせ
- GSLBは、IPアドレス192.168.1.23を調べ、カスタムロケーションCroydon 192.168.1.0/24と照合します。
- GSLBは、service1.gslb.comのAレコードを見て、south.service1.gslb.comが192.168.1.0/24のネットワークにも含まれていることを確認します。
- GSLBは、192.168.1.23に対して、service1.gslb.comのIPアドレス192.168.1.254を応答します。

テクニカルサポート

当社は、すべてのユーザーに対して、当社の標準的な利用規約に基づいて技術サポートを提供します。

edgeADC、edgeWAF、edgeGSLBのサポート＆メンテナンス契約が有効であれば、テクニカルサポートですべてのサポートを行います。

サポートチケットの発行をご希望の方は、こちらをご覧ください。

https://www.edgenexus.io/support/