
EDGE
NEXUS

エッジ ADC

EdgeADC 管理ガイド

ソフトウェア版
5.0.0

内容

ドキュメントのプロパティ	13
免責事項	13
著作権	13
商標	13
サポート	13
はじめに	14
この文書の目的	14
この文書は誰のためのものですか?	14
ロードバランシング入門	15
ロードバランサー、ADC とは?	16
VIP と仮想サービス (VS) の説明	17
ロードバランサー・サービスタイプとは何ですか?	19
旅の始まり	21
EdgeADC のダウンロード	22
インストール	24
EdgeADC のインストール	25
VMware ESXi へのインストール	25
VMXNET3 インターフェースのインストール	26
Microsoft Hyper-V へのインストール	26
Citrix XenServer へのインストール	28
KVM へのインストール	28
必要条件とバージョン	29
Nutanix AHV へのインストール	32
必要条件とバージョン	32
ProxMox へのインストール	33
ProxMox への OVA のアップロード	33
ファーストブート構成	35
ファーストブート - 手動ネットワーク詳細	35
ファーストブート - DHCP 成功	35
初回起動 - DHCP が失敗	35
管理 IP アドレスの変更	36
eth0 のサブネットマスクを変更する	36
デフォルトゲートウェイの割り当て	36

デフォルトゲートウェイ値の確認.....	36
ウェブインターフェースへのアクセス.....	36
コマンド・リファレンス表.....	37
ウェブ・コンソール.....	39
ADC ウェブコンソールの起動.....	40
デフォルトのログイン認証情報.....	40
外部認証サービスの利用.....	40
メイン・ダッシュボード.....	41
サービス.....	42
IP サービス.....	43
バーチャルサービス.....	43
新しい VIP を使用して新しい仮想サービスを作成する.....	43
完成したバーチャルサービスの例.....	45
モニター・エンドポイントの使い方.....	45
サブバーチャルサービスの作成.....	46
仮想サービスの IP アドレスの変更.....	46
コピーサービスを使用して新しい仮想サービスを作成する.....	47
表示データのフィルタリング.....	47
特定の用語を検索する.....	47
列の可視性の選択.....	47
仮想サービスカラムを理解する.....	48
プライマリー/モード.....	48
ビップ.....	48
有効.....	48
IP アドレス.....	48
サブネットマスク/プレフィックス.....	49
ポート.....	49
サービス名.....	49
サービスタイプ.....	49
リアルサーバー.....	50
サーバー.....	50
ベーシック.....	53
上級.....	58
フライトパス.....	64
サーバー直帰に伴うリアルサーバーの変更.....	65

必要なコンテンツサーバーの構成.....	65
一般.....	65
ウィンドウズ.....	65
リナックス.....	66
リアルサーバーの変更 - ゲートウェイモード.....	67
必要なコンテンツサーバーの構成.....	67
シングルアームの例.....	67
デュアルアームの例.....	68
図書館.....	69
アドオン.....	70
アプリ.....	71
フィルター.....	71
ダウンロードされたアプリ.....	71
購入アプリ.....	71
デプロイ.....	72
アプリをダウンロード.....	72
削除.....	72
認証.....	73
認証の設定 - ワークフロー.....	73
認証サーバー.....	73
LDAP、LDAP-MD5、LSAPS、LDAPS-MD5、Radius、SAML 用オプション.....	73
SAML 認証のオプション.....	74
KDC レルム.....	76
認証ルール.....	76
フォーム.....	77
キャッシュ.....	80
グローバルキャッシュ設定.....	80
キャッシュルールの適用.....	81
キャッシュルールの作成.....	81
フライトパス.....	83
詳細.....	83
新しい flightPATH ルールを追加する.....	83
コンディション.....	84
評価.....	88
アクション.....	89

flightPATH ルールのシナリオ	91
flightPATH ルールの適用.....	92
リアル・サーバー・モニター	93
リアルサーバー・モニターの種類.....	93
詳細	97
リアル・サーバー・モニターの例.....	98
SSL 証明書.....	102
ADC は SSL 証明書で何をしますか?.....	102
SSL 設定マネージャー.....	102
証明書リスト・エリア.....	103
アクションボタンと設定エリア.....	104
概要.....	104
リクエストの作成.....	104
名前変更.....	106
削除.....	107
インストール/サイン	107
リニューアル.....	108
証明書の検証.....	108
インターミディエイトを加える.....	109
再注文	110
インポート/エクスポート	111
バックアップ&リストア.....	112
バックアップ.....	112
リストア.....	112
ウィジェット.....	113
設定されたウィジェット.....	113
利用可能なウィジェット.....	113
イベント・ウィジェット	113
システムグラフ・ウィジェット.....	114
インターフェースウィジェット.....	115
ステータスウィジェット	115
トラフィック・グラフィック・ウィジェット	116
表示.....	118
ダッシュボード	119
ダッシュボードの使い方.....	119

ウィジェットメニュー	119
ライブデータの一時的停止ボタン	119
デフォルトのダッシュボードボタン	120
ウィジェットのサイズ変更、最小化、並び替え、削除	120
歴史	121
グラフデータの表示	121
過去ログ	124
W3C ログ	124
システムログ	124
統計	126
圧縮	126
これまでのコンテンツ圧縮	126
これまでの全体的な圧縮	126
総入出力	126
ヒットとコネクション	126
全体ヒット数	127
総接続数	127
ピーク・コネクション	127
キャッシング	127
キャッシュから	127
サーバーより	127
キャッシュの内容	127
アプリケーション・バッファ	128
セッションの永続性	128
現在のセッション数	128
使用率	128
この分の新しいセッション	128
この min を再検証する	128
この分の有効期限切れセッション	128
ハードウェア	129
ディスク使用量	129
メモリ使用量	129
CPU 使用率	129
ステータス	130
バーチャルサービス詳細	130

VIP コラム	130
VS ステータス・コラム	130
名称	131
バーチャルサービス (VIP)	131
ヒット/秒	131
キャッシュ	131
圧縮率	131
RS ステータス (リモートサーバー)	131
リアルサーバー	131
備考	131
コンズ (コネクション)	131
データ	131
Req/Sec (1 秒あたりのリクエスト数)	131
システム	132
クラスタリング	133
役割	133
クラスター	134
マニュアルの役割	135
単独での役割	136
設定	136
フェイルオーバー待ち時間 (ms)	136
フェイルオーバー・メッセージング	136
マネジメント	137
クラスタへの ADC の追加	137
クラスタに ADC を手動で追加する	138
クラスタメンバーの削除	138
ADC の優先順位の変更	139
日時	140
手動日付と時刻	140
タイムゾーン	140
日時の設定	140
日付と時刻の同期 (UTC)	140
タイムサーバー URL	141
hh:mm]で更新	141
更新期間[時間] :	141

NTP タイプ :	141
メールイベント	142
住所	142
イベントを E メールアドレスに送信	142
返信用メールアドレス	142
メールサーバー (SMTP)	142
ホストアドレス	142
ポート	142
送信タイムアウト	143
認証を使用する	143
セキュリティ	143
メインサーバーアカウント名	143
メールサーバーパスワード	143
通知とアラート	143
IP サービスのお知らせ	143
バーチャルサービスのお知らせ	143
リアルサーバーのお知らせ	143
フライトパス	144
グループ通知	144
グループメールの説明	144
グループ送信間隔	144
メールでの警告とイベント説明の有効化	144
ディスク容量	144
空き容量が少ない場合は警告	144
ライセンスの有効期限	144
歴史	145
データ収集	145
有効にする	145
毎回のデータ収集	145
メンテナンス	145
最新のアップデート	145
HP エンタープライズベース ADC	145
バックアップ	146
削除	146
リストア	146

ライセンス	147
ライセンス詳細.....	147
ライセンス ID.....	147
マシン ID.....	147
発行先	147
担当者	147
発行日	148
名称.....	148
設備	148
ライセンスのインストール	148
ライセンスサービス情報	149
ロギング	150
W3C ログの詳細	150
W3C ログレベル.....	150
W3C ログを含める	151
セキュリティ情報を含む	151
シスログ・サーバー.....	151
リモートシスログサーバー	152
リモート・ログ・ストレージ.....	152
フィールド概要.....	153
ログファイルの消去.....	154
ネットワーク	155
仮想環境における仮想ネットワークインターフェースの管理	155
主な検討事項.....	155
ホスト設定の推奨手順.....	155
シナリオ例	156
重要なアプライアンスの頻繁な vMotion の回避.....	156
頻繁な vMotion が推奨されない理由.....	156
クリティカル・アプライアンスの管理に関する推奨事項.....	157
基本設定	157
ALB 名	157
IPv4 ゲートウェイ	157
IPv6 ゲートウェイ	157
DNS サーバー1 & DNS サーバー2.....	158
アダプター詳細.....	158

インターフェイス	158
ボンディング	159
ボンディング・プロフィールの作成.....	160
ボンディング・モード.....	160
静的ルート.....	161
静的ルートの追加.....	161
スタティック・ルートの詳細.....	161
高度なネットワーク設定.....	161
ナグルとは?	161
サーバー・ネーグル.....	162
クライアント・ネーグル.....	162
SNAT.....	162
パワー	164
リスタート.....	164
リブート.....	164
電源オフ.....	164
セキュリティ.....	165
SSH.....	165
認証サービス.....	165
ウェブコンソール.....	166
REST API.....	166
REST API 用ドキュメント.....	166
SNMP.....	168
SNMP 設定.....	168
SNMP MIB.....	168
MIB ダウンロード.....	168
ADC OID.....	168
ヒストリカル・グラフ.....	169
ユーザーと監査ログ.....	171
ユーザー.....	171
ユーザー追加.....	171
ユーザータイプ.....	172
ユーザーの削除.....	173
ユーザーの編集.....	173
監査ログ.....	173

上級	174
構成	175
設定のダウンロード	175
設定のアップロード	175
ジェットパックのアップロード	175
グローバル設定	177
App Store ダウンロードプロキシ	177
HTTP プロキシ URL	177
HTTP プロキシのユーザー名	177
HTTP プロキシパスワード	177
ホストキャッシュタイマー	177
ドレイン	178
SSL	178
認証	179
フェイルオーバー設定	179
プロトコル	180
サーバーがビジー状態	180
転送先	180
フォワード・フォア出力	180
転送用ヘッダー	180
IIS の高度なログ - カスタムログ	181
Apache HTTPd.conf の変更	181
HTTP 圧縮設定	182
グローバル圧縮除外	183
永続性クッキー	183
UDP タイムアウトリセット	184
ソフトウェア	185
ソフトウェア・アップグレードの詳細	185
クラウドからダウンロード	185
ソフトウェアのアップロード	186
アプリのアップロード	186
ソフトウェア/ファームウェアのアップデート	186
ADC に保存されているソフトウェアを適用する	186
トラブルシューティング	188
サポートファイル	188

トレース	188
ピン	189
キャプチャ	190
ヘルプ	191
会社概要	191
参考	191
ジェットパック	192
ジェットパック	193
jetPACK のダウンロード	193
マイクロソフトエクステンション	193
Microsoft Lync 2010/2013	194
ウェブサービス	194
マイクロソフト リモートデスクトップ	195
DICOM - 医学におけるデジタル画像と通信	195
オラクル e ビジネス・スイート	195
VMware Horizon View	195
グローバル設定	195
暗号と暗号ジェットパック	195
強力な暗号	195
アンチ・ビースト	195
SSLv3 なし	196
SSLv3 なし TLSv1 なし RC4 なし	196
NO_TLSv1.1	196
TLS-1.0-1.1 暗号を有効にする	196
暗号例 jetPACK	196
jetPACK の適用	197
jetPACK の作成	197
フライトパス	201
flightPATH の紹介	202
flightPATH とは?	202
flightPATH は何ができるのか?	202
コンディション	202
試合	203
チェック	205
例	205

評価	205
アクション	208
アクション	208
ターゲット	208
データ	208
一般的な用途	210
アプリケーション・ファイアウォールとセキュリティ	210
特徴	210
事前ルール	211
HTML エクステンション	211
インデックス.html	211
フォルダを閉じる	211
CGI-BBIN を隠す:	212
ログ・スパイダー	212
HTTPS を強制する	212
メディア・ストリーム	213
HTTP を HTTPS に切り替える	213
クレジットカードの白紙化	213
コンテンツの有効期限	214
スプーフ・サーバー・タイプ	214
SAML と Entra ID	217
Microsoft Entra での Entra ID 認証アプリケーションのセットアップ	218
テクニカルサポート	221

ドキュメントのプロパティ

文書番号 : 2 .0.3.19.25.12.03

文書作成日 : 19 March 2025

文書の最終編集日 19 March 2025

文書作成者 ジェイ・サヴァール

ドキュメント 最終編集者

ドキュメント EdgeADC - バージョン 5.0.0

免責事項

このマニュアルのスクリーンショットやグラフィックは、製品リリースの違いにより、お使いの製品とは若干異なる場合があります。Edgenexus 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。エドジェネクスはいかなる誤りに対しても責任を負いません。エドジェネクスでは、今後のリリースにおいて、必要に応じて本書の情報を変更、修正することがあります。

著作権

© 2025 無断転載を禁じます。

本書に記載されている情報は、事前の予告なく変更されることがあり、メーカー側の確約を意味するものではありません。本ガイドのいかなる部分も、製造者の書面による明示的な許可なく、その目的を問わず、電子的、機械的を問わず、いかなる形式または手段によっても複製または転送することを禁じます。登録商標は各所有者の財産です。本ガイドは、可能な限り完全かつ正確なものとなるよう最大限の努力を払いますが、その適合性を保証するものではありません。著者および発行者は、本ガイドに含まれ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、いかなる個人または団体に対しても責任や義務を負うものではありません。

商標

Edgenexus のロゴ、Edgenexus、EdgeADC、EdgeWAF、EdgeGSLB、EdgeDNS はすべて Edgenexus Limited の商標または登録商標です。その他すべての商標は、各所有者の財産であり、承認されています。

Edgenexus サポート

本製品に関する技術的なご質問は、support@edgenexus.io までお問い合わせください。

はじめに

このガイドをお読みになっているのは、**Edgenexus EdgeADC** を導入し、サーバーベースのアプリケーションを効率的かつコスト効率よくロードバランスすることをお考えだからです。

EdgeADC は、高い拡張性、セキュリティ、高いパフォーマンス、使いやすい管理インターフェイスを提供する安全性の高いエンジンを中心に構築されています。これらの要素により、導入したシステムは最高の所有コストを実現します。

この文書の目的

本書は、ウェブベースの簡単なインターフェイスを使用して **EdgeADC** を管理できるように作成されています。各機能とその設定について詳しく説明していますので、**EdgeADC** の設定にお役立てください。

この文書は誰のためのものですか？

本書は、ネットワーク、特にプロトコル、アプリケーション、サーバーの知識がある方を対象としています。

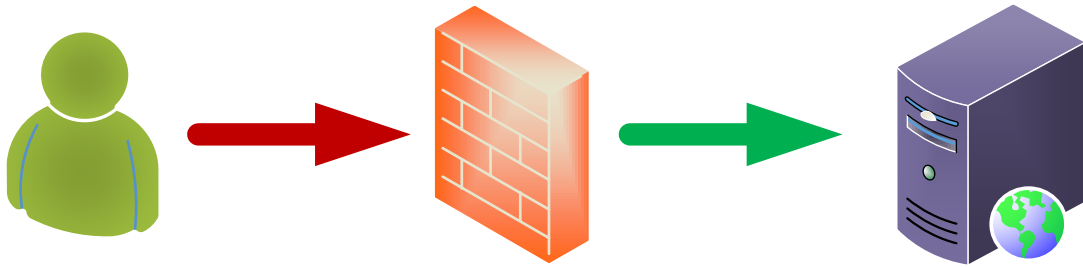
ロードバランシング入門

ロードバランサー、ADCとは？

ロードバランサーは大きく進化し、以前よりもはるかにインテリジェンスがエンジンに組み込まれている。ロードバランサーは今日、アプリケーションデリバリーコントローラーまたは **ADC** と呼ばれることが多い。

ロードバランサーや **ADC** とは何かを理解する前に、IT 担当者やユーザーの問題を認識する必要がある。では、例を挙げてみよう。

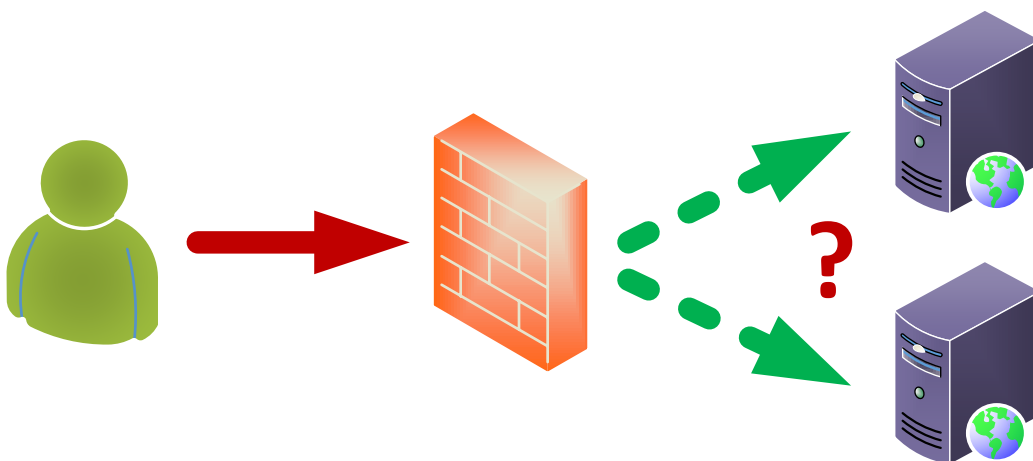
- ある企業が、インターネットに公開するウェブ・アプリケーションを持っています。アプリケーションは1台のウェブサーバでホストされ、データは別のデータベースサーバに保存されます。



User Client

Application Servers

- このサーバーでは、例として **1.2.3.4** の IP アドレスを使用しています。
- アプリケーションにアクセスするクライアントの数は定期的増加しており、アプリケーションのパフォーマンスが低下しているとの指摘もある。
- サーバーを分析したところ、サーバーを襲うトラフィックが大量に増加し、さらに増え続けていることがわかった。
- そこで、アプリケーションをホストするサーバーをもう1台追加することにした。
- 新しいセカンドサーバーは **1.2.3.5** の IP アドレスを使用する。
- 問題は、クライアントを新しいサーバーと現在のサーバーに誘導して負荷を共有し、ユーザーのセッションが最初にログオンしたサーバーで維持されるようにする方法である。



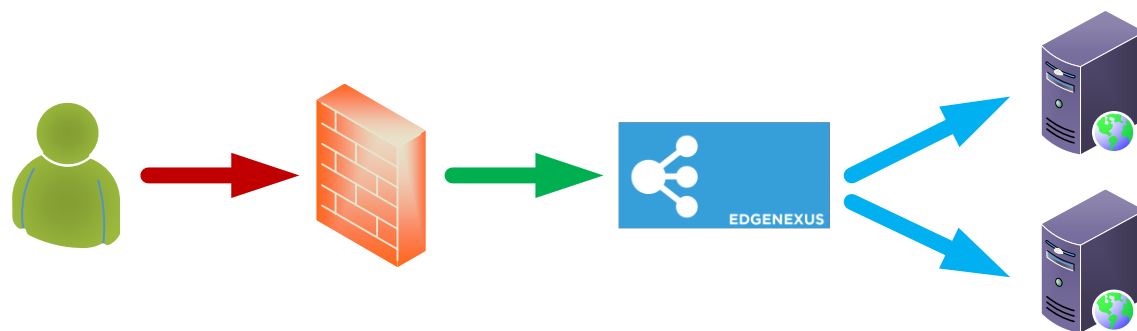
User Client

Application Servers

- その答えはロードバランサーか **ADC** だ。

これで解決だ。

- つのアプリケーションサーバーの前に ADC を配置する。

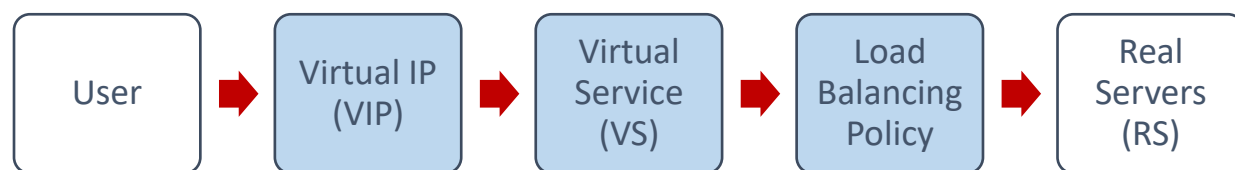


User Client

ADC

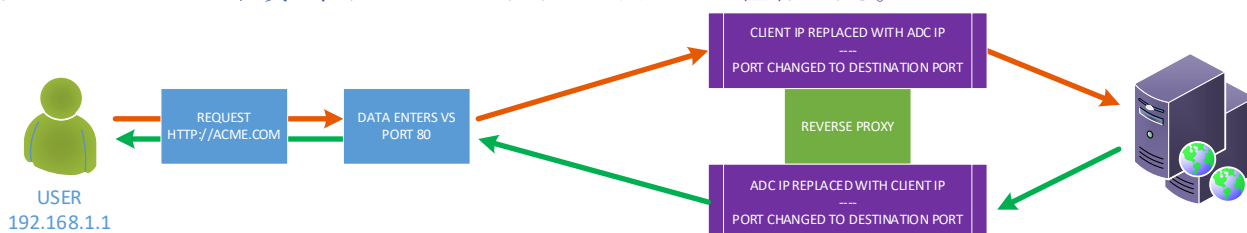
Application Servers

- ADC は 1.2.3.6 という外部に面した IP を持ち、ファイアウォールはリクエストを先の 1.2.3.4 の代わりにこのアドレスに NAT リダイレクトする。
- リクエストを受け取る ADC の IP は VIP と呼ばれ、コンフィギュレーションはバーチャルサービスと呼ばれる。
- ADC はクライアント・ユーザーからのリクエストを受け取り、効率を確保するためにアプリケーション・サーバーの健全性を監視しながら、ロードバランスポリシーを使用して実際のサーバーにリバースプロキシする。



る。

- ADC は、使用中のロードバランシングポリシー、負荷の性質、およびアプリケーションサーバーのステータスに基づいて、サーバーへのトラフィックをバランスする。
- サーバーからのトラフィックは、ADC を通じてクライアントに逆方向に送り返される。
- リバースプロキシの性質上、サーバーとクライアントは互いに匿名である。



- リバースプロキシ技術は、最適なセキュリティレベルを保証します。

VIP と仮想サービス (VS) の説明

VIP とは、要するに、EdgeADC で使用するために定義された IP アドレスのことで、ユーザーはこの IP アドレスに結びついたサービスにアクセスできる。これが VIP の役割だ。EdgeADC の仕組み上、VIP はリアルサーバーと同じサブネットにある必要はなく、このネットワークアドレス変換手法により、内部サーバーにアクセスしようとするハッカーから非常に安全に保護される。

注：VIP の IP アドレスは、管理 IP に使用される IP アドレスと同じにすることはできません。

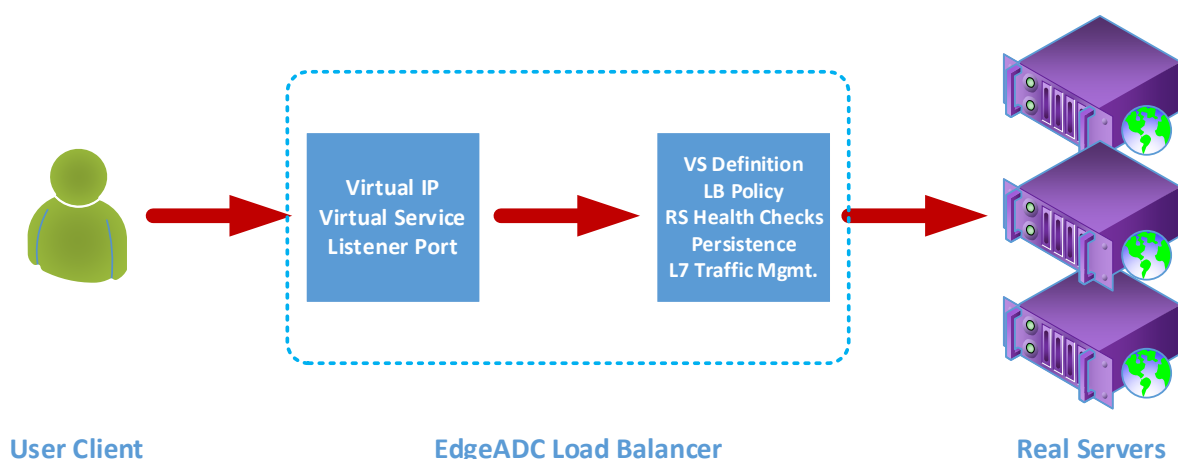
仮想サービスは、EdgeADC のプロキシ技術と負荷分散技術の中核を成す。仮想 IP は、VS がネットワークと世界にアドバタイズされるアドレスであり、VS がサービスするアプリケーションの使用を希望するクライアントからのトラフィックとリクエストを待ち受けます。

クライアントが VS にアクセスすると、VS はトラフィックに対して以下のような多くのアクションを実行するように設定される：

- クライアント接続のプロキシ
- 圧縮、高速化、負荷分散、トラフィック検査など、特定の機能が実行される。
- クライアントのリクエストを、仮想サービスのロードバランシングポリシーで定義されたデスティネーションサーバーに転送する。

VS は、EdgeADC がデータリクエストに備えてリッスンしている IP アドレス (VIP) と結婚していると考えられることもできる。標準的な TCP または HTTP コンフィギュレーションが行われると、クライアントは VIP に接続し、EdgeADC は VS を構成する定義に従ってリクエストを処理する。これが完了すると、EdgeADC は指定されたリアルサーバーにトラフィックを送信します。

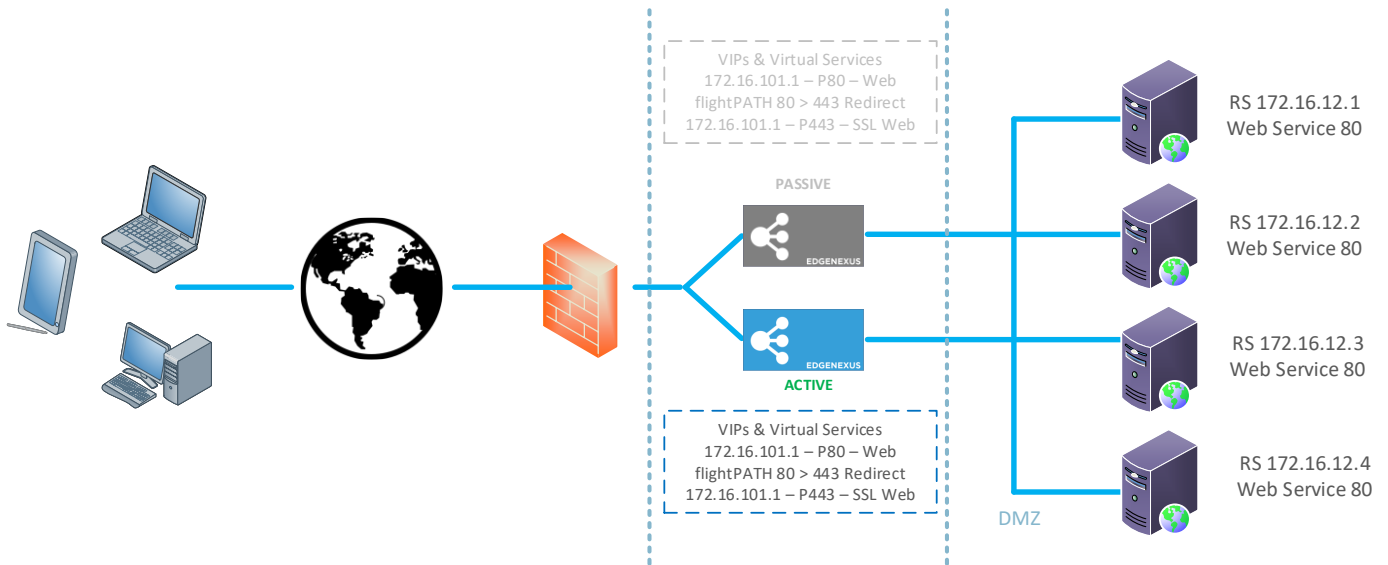
VS は典型的なコンフィギュレーションで接続とデータを受信し、EdgeADC 内のリバース・プロキシ・エンジンを使用して終了またはプロキシする。その後、EdgeADC はリアル・サーバーへの新しいコネクションを開き、データを送信する。リアルサーバーがリクエストに応答すると、EdgeADC は同様のリバースパスを使用してクライアントに応答を送信します。



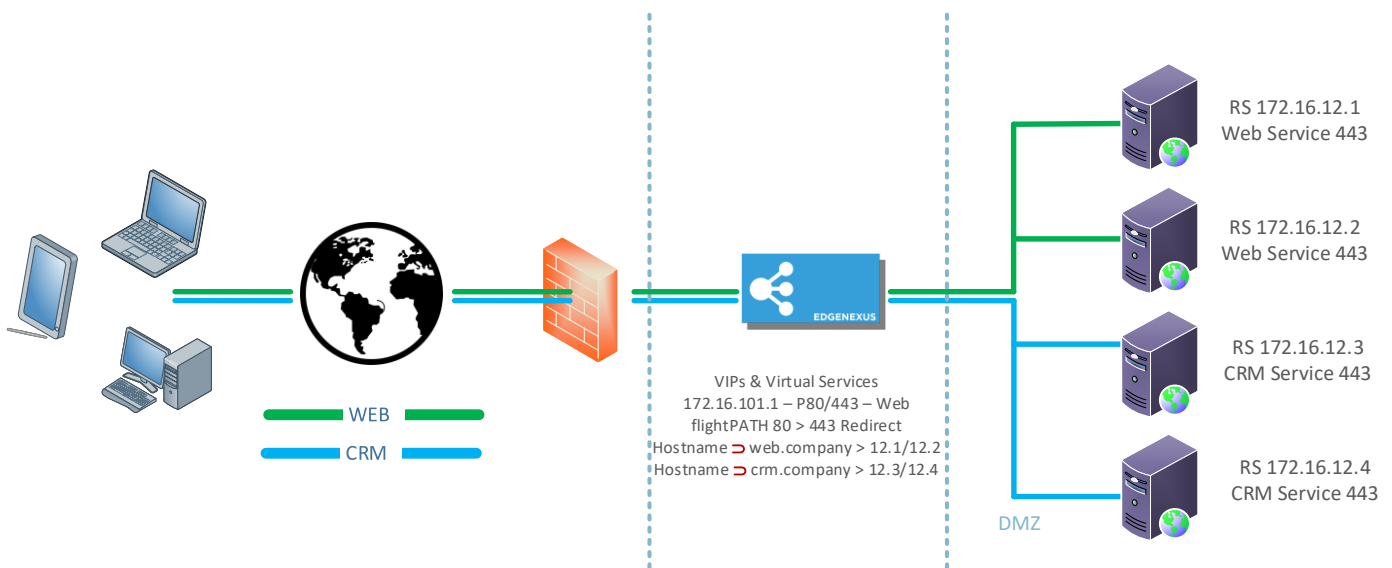
仮想サービス定義は、単一の IP アドレス (VIP) と、さまざまなプロトコルを使用して、さまざまなサービスへのインGRESSポイントとして機能するポートのコレクションで構成されます。

例えば、耐障害性を提供するために、一連のウェブ・サーバーの負荷分散を行う必要があるとします。ここで、これらのシステムには、<https://myweb.company.com> を使って HTTPS で保護された通信でアクセスすると仮定しよう。

このような構成の定義を見ると、1つのVIPに2つのエントリーがあり、1つはポート80用、もう1つはポート443用である。ポート80のVIPには、トラフィックを強制的にHTTPSに変換するflightPATHルールが付加される。ポート443用の2つ目のエントリーは、その下に定義されたリアルサーバーにトラフィックを送信する。同様に、同じVIPの下に他のサービスを置いて、メールサーバーや他のアプリケーションサーバーにトラフィックをロードバランスさせることもできる。



あまり機能的でない ADC では、同じポートを使用するサービスは異なる VIP を必要とするが、ADC とその flightPATH システムでは、同じポートを使用する複数のサービスで単一の VIP を使用することができる。つまり、異なるホスト名で 443 を使用してアクセスする 2 つのアプリケーションを、1 つの VIP で使用することができる。例を以下に示す。



EdgeADC のシステムは非常に柔軟で、非常に複雑で機能的な構成を定義することができます。

ロードバランサー・サービスタイプとは何ですか？

負荷分散サービスの種類は、サーバーのプール間でトラフィックをインテリジェントに分散または負荷分散するために使用されるアルゴリズムと方法論で構成されます。ADC が利用可能にする方法とアルゴリズムは、負荷分散されるサーバーで使用されるサービスタイプまたはアプリケーションに依存し、使用中のネットワークとサーバーの状態にも依存します。使用するために選択するロードバランシングサービスのタイプは、ADC を介して送信されるトラフィックのレベルにも依存することに注意する必要があります。つまり、トラフィックのスループットや負荷が低い場合、ロードバランシングサービスのタイプはシンプルなものになる。しかし、負荷が大きくなると、バックエンドサーバーへの効率的な負荷分散を達成するために、より複雑なタイプを選択する必要があるかもしれない。

EdgeADC では、以下のロードバランシング・サービス・タイプを利用できます。

EdgeADC - 管理ガイド

ディコム	レイヤー4 UDP	正規化投影座標系
ファイル転送プロトコル	レイヤー4 tcp/udp	RPC/ADS
HTTP(S)	DNS	RPC/CA/PF
アイマップ	ポップスリー	SMTP
レイヤー4 TCP	右派系	GSLB

旅の始まり

EdgeADCのダウンロード

インストールの前に、まずお使いの環境に適した EdgeADC をダウンロードします。

ほとんどの仮想化環境に対応したエディションと、ベアメタルハードウェアに直接インストールするための ISO エディションを提供しています。

ステップ 1 は、エジネクサスのウェブサイト (<https://www.edgenexus.io/products/load-balancer/free-trial/>) にある評価フォームに記入すること。

The screenshot shows the EdgeNexus website's 'Request a Free Trial' form. The form is titled 'Request a Free Trial' and includes the subtext '(Downloaded or cloud provisioned)'. It contains input fields for 'First name', 'Last name', 'Email*', and 'Company name'. Below these fields is a reCAPTCHA widget with a 'protected by reCAPTCHA' label and a 'Submit' button. The website header includes the EdgeNexus logo and navigation links: 'Why Edgenexus?', 'Try', 'Products', 'Solutions', 'Applications', 'Resources', and 'Support'. The main content area features the text 'The Easy choice for Load balancing' and 'Fast, Scalable and Secure Applications'. Below the form, there are logos for Exchange, SharePoint, Microsoft Dynamics, ORACLE, Skype for Business, and VMware Horizon View. At the bottom, it says 'Your Load Balancing Experts' with a chat icon.

手続きは簡単で、フォームに記入して送信すると、ダウンロードページに移動し、そこであなたの環境に合った画像を選択することができます。

EdgeADC は、以下の仮想化システムで利用可能です：

- VMware ESX
- マイクロソフト Hyper-V
- シトリックス XenServer
- ニュータニックス
- KVM

また、Microsoft Azure や Amazon AWS のマーケットプレイス版を使用して、クラウドでテストドライブすることもできます。

オンプレミスインストール用にソフトウェアをダウンロードする場合、14 日間のトライアルライセンスが組み込まれた EdgeADC が届きます。 sales@edgenexus.io、全機能を有効にした 30 日間のライセンス・キーをリクエストすることをお勧めします。

インストール

EdgeADC のインストール

EdgeADC (ADC) はさまざまなプラットフォーム・ターゲットにインストール可能で、それぞれにインストーラーが必要です。

これらは、利用可能なさまざまな設置モデルである。

- VMware ESXi
- KVM
- シトリックス・ゼン
- Nutanix AHV
- マイクロソフト Hyper-V
- オラクルブイエム
- プロックスモックス (OVA 使用)
- ベアメタルハードウェア用 ISO

ADC をホストするために使用する仮想マシンのサイジングは、ユースケースのシナリオとデータスループットに依存する。

VMware ESXi へのインストール

ADC は、VMware ESXi 5.x 以上へのインストールをサポートしています。

- 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する。
- ダウンロードしたら、ESXi ホストまたは SAN 上の適切なディレクトリに解凍してください。
- vSphere クライアントで、[File: Deploy OVA/OVF Template] 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。
- 十分な容量のあるデータストアを選択し、**NEXT** をクリックする。
- 次に、製品に関する情報が表示されます。
- **NEXT** をクリックする。
- 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 を右クリックし、Power > Power-On の順に選択します。
- VA が起動し、コンソールに ADC ブート画面が表示されます。

```
Checking for management interface ..... [ OK ]  
  
Management interface: eth0   MAC: 00:0c:29:05:2e:1a  
  
1. Enter networking details manually  
2. Configure networking setting automatically via DHCP
```

VMXNET3 インターフェースのインストール

VMXnet3 ドライバーはサポートされていますが、最初に NIC の設定を変更する必要があります。

注意 - 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 ハードウェアのアップグレード -- リスト内の VA を右クリックし、Upgrade Virtual Hardware を選択します (VMware ツールのインストールやアップデートは開始せず、ハードウェアのアップグレードのみを実行します)。
3. 2つの NIC を追加し、VMXNET3 とする。
4. 標準的な方法で VA を起動します。VMXNET3 で動作します。

すでに稼働している VA で VMXNET3 インターフェイスを有効にする

1. VM の停止 (CLI シャットダウンコマンドまたは GUI パワーオフ)
2. 両方の NIC の MAC アドレスを取得する (リスト内の 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 のハードウェアをアップグレードする (VMware ツールのインストールやアップデートは開始せず、ハードウェアのアップグレードのみを実行する)。
5. 2つの NIC を追加し、VMXNET3 とする。
6. ステップ 2 に従って、新しい NIC の MAC アドレスを設定する。
7. VA を再起動する

VMware ESXi を本番用プラットフォームとしてサポートしています。 評価目的の場合は、VMware Workstation および Player をご利用いただけます。

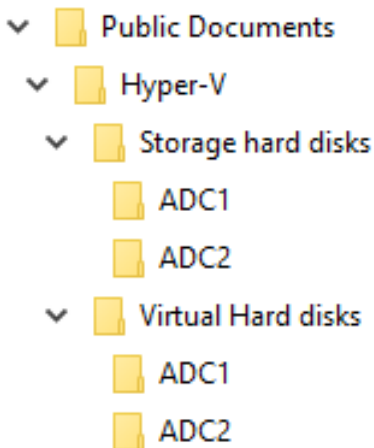
ファーストブート設定のセクションを参照してください。

Microsoft Hyper-V へのインストール

Edgenexus ADC 仮想アプライアンスは、Microsoft Hyper-V 仮想化フレームワーク内に簡単にインストールできます。このガイドでは、ADC とそのロードバランシングアーキテクチャに対応するために、Hyper-V システムとシステムリソースを正しく指定および構成していることを前提としています。

各アプライアンスには固有の MAC アドレスが必要であることを注意すること。

- ダウンロードした Hyper-V 互換 ADC-VA 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 を開く。
- ADC VA 'Virtual hard disk' を入れる新しいフォルダと 'Storage hard disk' を入れる別の新しいフォルダを作成する。例えば、C:\UsersPublic、Public、Documents、Hyper-V、Virtual hard disks、ADC1 と C:\UsersPublic、Public、Documents、Hyper-V、Storage hard disks、ADC1。
- 注：Virtual hard disks と Storage hard disks 用の新しい ADC 固有のサブフォルダは、以下に示すように、各仮想 ADC インスタンス・インストール用に作成する必要があります：



- 解凍した EdgeADC .vhd ファイルを、上記で作成した 'Storage hard disk' フォルダにコピーします。
- Hyper-V Manager クライアントでサーバーを右クリックし、"Import Virtual Machine" を選択します。
- 先にダウンロードした ADC VA イメージファイルを解凍したフォルダを参照する。
- Select Virtual Machine - インポートする仮想マシンをハイライトし、Next をクリックします。
- Select Virtual Machine - インポートする仮想マシンをハイライトし、Next をクリックします。
- インポートの種類を選択し、「仮想マシンをコピーする (新しい一意の ID を作成する)」を選択します。
- 仮想マシンファイルのフォルダを選択します。宛先は Hyper-V のデフォルトのままでも、別の場所を選択することもできます。
- 仮想ハードディスクを探す - 上記で作成した仮想ハードディスク・フォルダを参照して選択し、次へをクリックします。
- Folders to Store Virtual Hard Disk (仮想ハードディスクを保存するフォルダ) を選択し、以前に作成した Storage hard disks フォルダを参照して選択し、next をクリックします。
- Completing Import Wizard Summary (インポートウィザードの完了) ウィンドウの詳細が正しいことを確認し、Finish (完了) をクリックします。
- 新しくインポートした **ADC** 仮想マシンを右クリックし、[Start]を選択します。

注 : [HTTP://SUPPORT.MICROSOFT.COM/KB/2956569](http://support.microsoft.com/kb/2956569) に従って、VA の起動後に以下のように表示される「**DEGRADED (INTEGRATION SERVICES UPGRADE REQUIRED)**」ステータスメッセージは無視してください。何もする必要はなく、サービスはデグレードされていません。

- VM が初期化されている間に、VM エントリを右クリックして Connect... を選択すると、EdgeADC コンソールが表示されます。

```

Checking for management interface ..... [ OK ]

Management interface: eth0  MAC: 00:0c:29:05:2e:1a

1. Enter networking details manually
2. Configure networking setting automatically via DHCP

```

- ネットワークのプロパティを設定すると、VA が再起動し、VA コンソールにログオンします。ファーストブート設定のセクションを参照してください。

Citrix XenServer へのインストール

ADC 仮想アプライアンスは、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、"**File: Import**" を選択します。
- **OVA** ファイルを参照して選択し、"**次を開く**" をクリックします。
- VM の作成場所を尋ねられたら選択する。
- 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) を選択します。
- 十分なスペースのある SR を選択し、"**NEXT**" をクリックする。
- 仮想ネットワークインターフェイスをマッピングします。どちらのインターフェイスも **Eth0** と表示されますが、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。
- 各インターフェイ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" にはチェックを **入れないでください**。
- **NEXT** " をクリックする
- 一時転送 VM に使用するネットワークインターフェイスを選択します。
- 管理インターフェイス (通常はネットワーク 0) を選択し、ネットワーク設定を **DHCP** のままにします。転送用の **DHCP** サーバーがない場合は、静的 IP アドレスの詳細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」と表示され続け、失敗します。**NEXT** " をクリックしてください。
- すべての情報を確認し、正しい設定をチェックする。**FINISH** " をクリックします。
- VM は仮想ディスク「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。
- VM が起動し、ADC のブート画面が表示されます。

```
Checking for management interface ..... [ OK ]  
  
Management interface: eth0  MAC: 00:0c:29:05:2e:1a  
  
1. Enter networking details manually  
2. Configure networking setting automatically via DHCP
```

- 一度設定すると、VA へのログオンが表示される。

ファーストブート設定のセクションを参照してください。

KVM へのインストール

次のセクションでは、KVM プラットフォームに EdgeADC をインストールする方法を示します。この演習で使用した KVM プラットフォームは、Cockpit と仮想化がインストールされた CentOS v8 オペレーティング・システム上で動作します。

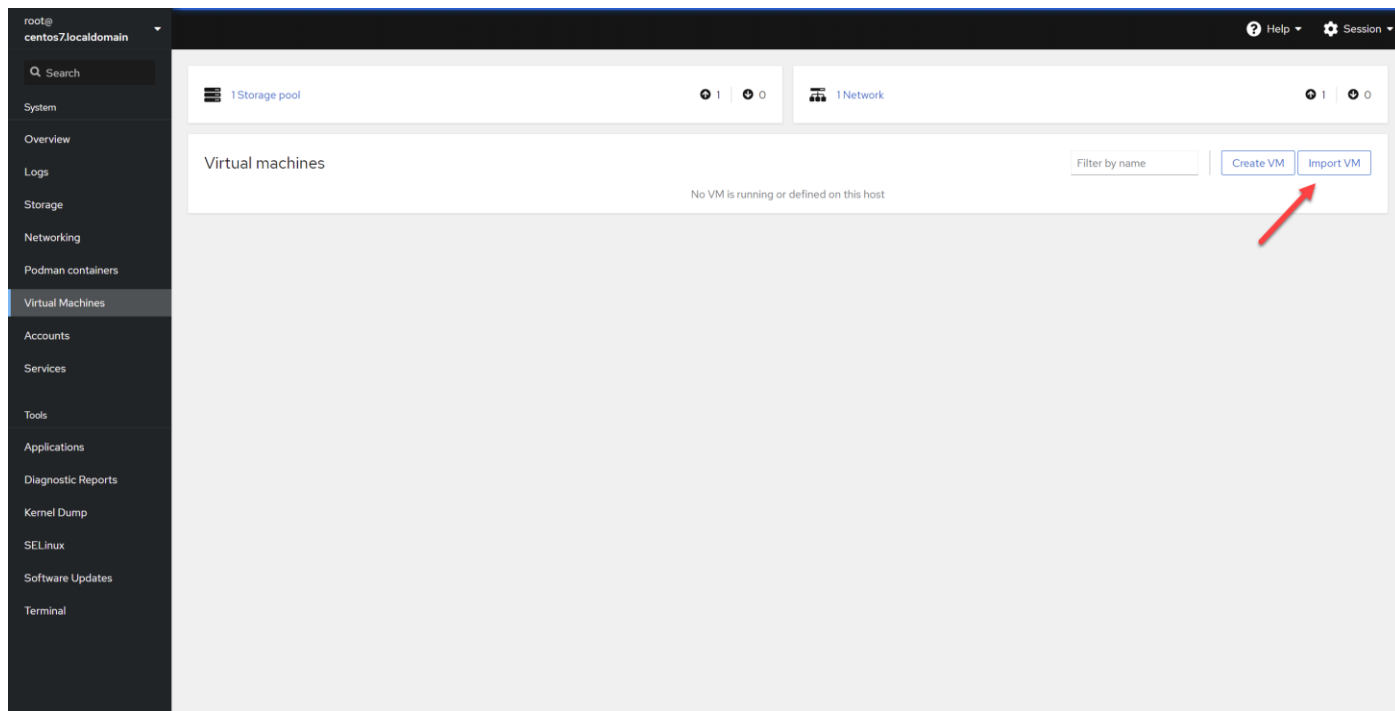
必要条件とバージョン

このガイドは、EdgeADC 4.2.6 以上に対応しています。

以下のガイダンスでは、KVM のインストールやネットワークについては説明しません。

KVM 仮想アプライアンスをダウンロードし、ホスト上のアクセス可能な場所に保存していることを前提としています。

- 最初のステップは、コックピットのコンソールにログインすることです。



- インポート VM をクリック
- 最初のダイアログでは、仮想アプライアンスのインポートの詳細を指定します。フィールドの内容については、以下の画像を参照してください。OS として Red Hat Enterprise 6.0 を指定する必要があります。



Import a virtual machine ×

Name	EdgeADC 🔍
Disk image	/home/Edgenexus-ADC-6.8-64-KVM.1140-1909-7567-bam1727.qcow2 ✕ ▼
Operating system	Red Hat Enterprise Linux 6.0 (Santiago) ✕ ▼
Memory	4 GiB ▼ Up to 7.5 GiB available on the host
Immediately start VM	<input type="checkbox"/>
Import Cancel	

- "Immediately Start VM" のチェックが外れていることを確認してください。
- 詳細を入力したら、インポートボタンをクリックしてください。
- 次の段階では、使用したい vCPU とメモリ割り当てを指定する。

Overview

General

State	Shut off
Memory	4 MiB edit 
vCPUs	1 edit 
CPU type	host edit
Boot order	disk edit
Autostart	<input type="checkbox"/> Run when host boots

Hypervisor details

Emulated machine	pc-i440fx-rhel7.6.0
Firmware	BIOS

- メモリを割り当てるには、以下のようなダイアログが表示されます。

EdgeADC memory adjustment



Current allocation



4

GiB

Maximum allocation



4

GiB

Save

Cancel

- vCPU を割り当てるには、以下のようなダイアログが表示されます。

EdgeADC vCPU details



vCPU count ⓘ

4

Sockets ⓘ

1

vCPU maximum ⓘ

4

Cores per socket

2

Threads per core

2

Apply

Cancel

- ただし、SSL の再暗号化で高スループットを使用する場合は、「表示」>「統計情報」の「ハードウェア」セクションで適宜調整する必要があります。

▲ Hardware

Disk Usage	40%
Memory Usage	11.6% (894.7MB of 7689.6MB)
CPU Usage	16.0%

- これで KVM に ADC がインストールされました。下の画像を参照してください。

Overview

General

State: Running

Memory: 4 GiB [edit](#)

vCPUs: 4 [edit](#)

CPU type: custom (Cooperlake) [edit](#)

Boot order: disk [edit](#)

Autostart: Run when host boots

Hypervisor details

Emulated machine: pc-i440fx-rhel7.6.0

Firmware: BIOS

Usage

Memory: 583.4 / 4096 MiB

CPU: 6% of 4 vCPUs

Console

VNC console [Expand](#)

[Send key](#) [Disconnect](#)

```

Welcome to Edgenexus ADC
Copyright (C) 2002-2021 Edgenexus Ltd. All Rights Reserved.

Using Intel AES Hardware Acceleration

GUI address is https://192.168.159.100:443
After login, type "Help" for a list of commands.

jetnexus login:

```

Disks

[Add disk](#)

Device	Used	Capacity	Bus	Access	Source	
disk	1.4 GiB	25 GiB	virtio	Writeable	File /home/Edgenexus-ADC-6.8-64-KVM.1140-1909-7567-bam1727qcow2	Remove Edit

Networks

[Add network interface](#)

Type	Model type	MAC address	IP address	Source	State	
network	virtio	52:54:00:60:83:65	Unknown	default	up	Delete Unplug Edit

Nutanix AHV へのインストール

次のセクションでは、EdgeADC を Nutanix AHV プラットフォームにインストールする方法を示します。

必要条件とバージョン

このガイドは、EdgeADC 4.2.6 以上に対応しています。

Nutanix ハイパーバイザーのすべてのバージョンに互換性があるが、認証は Nutanix バージョン 5.10.9 で実施された。

- 最初のステップは、Nutanix Prism Central にログインすることです。

EdgeADC イメージのアップロード

- 仮想インフラストラクチャ > イメージ
- 画像の追加ボタンをクリックします。
- ダウンロードした EdgeADC 画像ファイルを選択し、[開く]ボタンをクリックして画像をアップロードします。
- 画像の説明フィールドに画像の名前を入力します。
- 適切なカテゴリーを選択する
- 画像を選択し、右矢印キーをクリックします。
- すべての画像]を選択し、[保存]をクリックします。

VM の作成

- 仮想インフラ > VMs に移動する
- VM の作成ボタンをクリックします。
- VM の名前、CPU の数、VM に割り当てるコアの数を入力します。
- 次にダイアログを下にスクロールし、VM に割り当てたいメモリ量を入力する。最初は 4GB から始め、使用状況に応じて増やすことができる。

ディスクの追加

- 次に、**Add New Disk** リンクをクリックします。
- 操作]ドロップダウンから[イメージサービスからクローン]オプションを選択します。
- 追加した **EdgeADC** イメージを選択し、**[Add]** ボタンをクリックします。
- ブータブルディスクとなるディスクを選択します。

NIC、ネットワーク、アフィニティの追加

- 次に、「**Add New NIC**」ボタンをクリックします。2つの **NICS** が必要です。
- ネットワークを選択し、追加ボタンをクリックします。
- **Set Affinity** ボタンをクリックします。
- VM の実行を許可する **Nutanix** ホストを選択し、**[Save]** ボタンをクリックします。
- 設定を確認し、「保存」ボタンをクリックします。

VM のパワーオン

- VM のリストから、先ほど作成した VM 名をクリックする。
- VM の **Power On** ボタンをクリックする。
- VM の電源が入ったら、**Launch Console** ボタンをクリックします。

EdgeADC ネットワークの設定

- 最初の起動環境」のセクションの指示に従ってください。
- ブラウザと管理 IP アドレスを使用して、EdgeADC の GUI にアクセスできます。

ProxMox へのインストール

ProxMox へのインストールは簡単ですが、いくつかの追加ステップが必要です。

VMWare OVA バージョンのインストールを使用します。これは複数ステップのプロセスで、ProxMox のシェルコマンドの知識が必要です。しかし、できるだけ簡単に説明できるようにしました。ProxMox に精通していることを前提としているため、ProxMox の機能については深く触れません。

ProxMox への OVA のアップロード

OVA バージョンを使用するので、まず OVA を ProxMox にアップロードする必要があります。

- ProxMox コンソールにログイン
- **OVA_Import** というフォルダを作成する。
- WinSCP (Windows) や CyberDuck (Mac) などの SFTP クライアントを使用して、OVA ファイルを転送する必要があります。
- ファイルが転送されると、作成したフォルダにファイルが表示されます。
- 以下のコマンドを入力し、OVA ファイルの内容を展開する。
- `tar xvf {ファイル名}`.以下の例を参照のこと。

```
tar xvf Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.ova
```

- 抽出されると、以下の例のように表示されるはずです。

```
root@proxmox:~/OVA_Import# ls
```

```
Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.ova
```

```
root@proxmox:~/OVA_Import# tar xvf Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.ova
```

```
Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.ovf
```

```
Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.mf
```

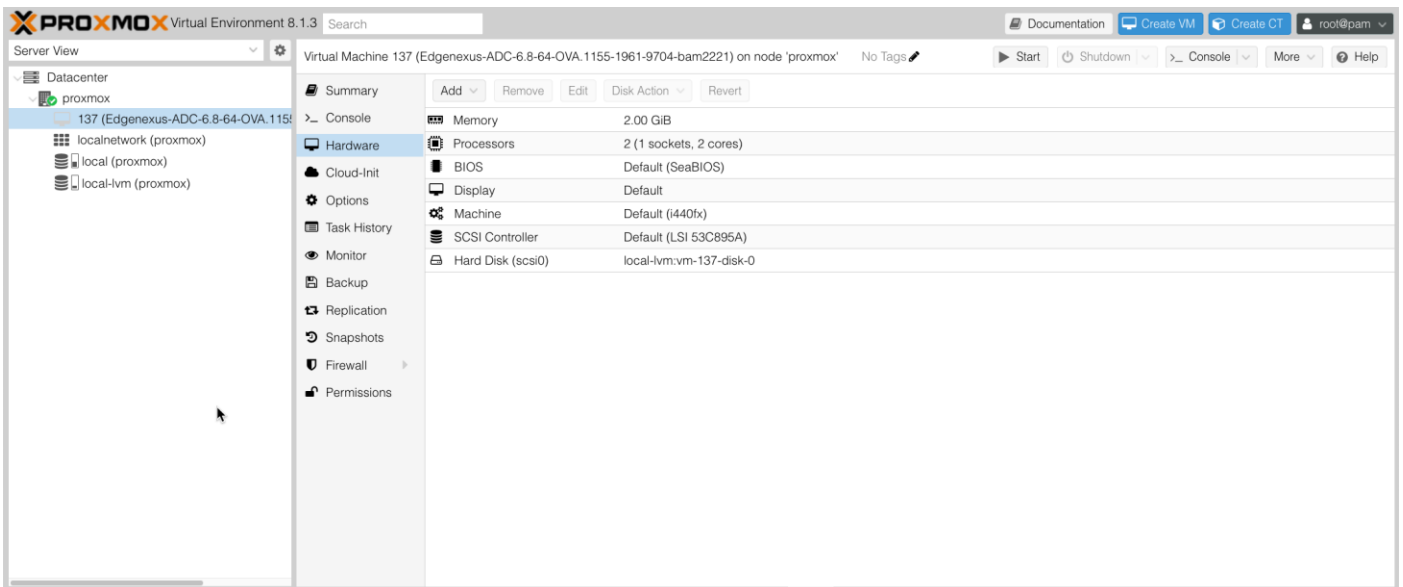
```
Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221-disk1.vmdk
```

```
root@proxmox:~/OVA_Import#
```

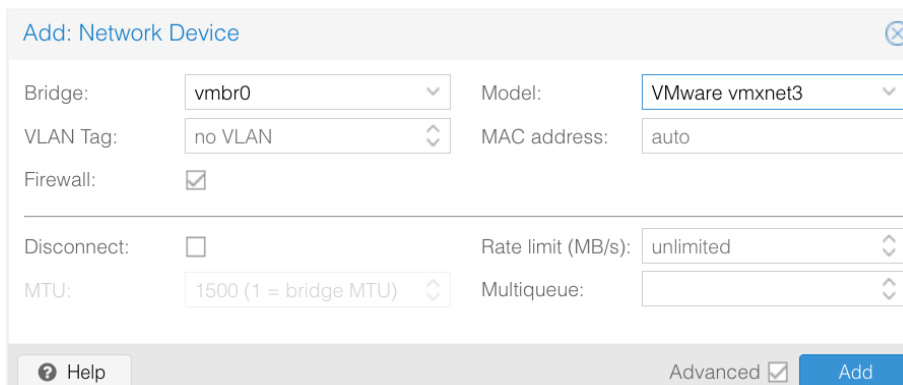
- 3つのファイルがある。`.ovf`と`.mf`はコンフィギュレーション。`.vmdk`はADCを保持する仮想ディスクである。
- 次のステップは、VMDKをProxMoxにインポートし、仮想マシンを作成することです。
- 以下のコマンドを入力し、設定ファイルを使用して仮想マシンを作成します。

```
qm importovf 137 ./[ファイル名.ovf] local-lvm --format qcow2
```

- この例では、IDを100としましたが、ProxMoxで既に仮想マシンを作成している場合は、インストールによって異なる場合があります。ProxMoxでVMの作成プロセスを開始するか、100より大きい数字で手の届かない安全な数字を選択することで、次のIDを決定することができます。
- これでVMが作成された。



- 次のステップは、VMにネットワーク・インターフェイスを追加することだ。
- 右パネルの「ハードウェア」をクリックする。
- **Add** をクリックし、ネットワークインターフェイスを選択します。



- 上の画像のように設定する。モデルをVMware vmxnet3にすることが重要だ。
- 設定したら **Add** をクリックする。
- 必要に応じてネットワークアダプターを追加することができる。
- これでVMを起動し、ファースト・ブート設定の章にある手順を使用することができます。

ファーストブート設定

最初の起動時に、ADC（以下、VA ともいう）は、本番運用のための設定を要求する以下の画面を表示する。

```
Checking for management interface ..... [ OK ]

Management interface: eth0  MAC: 00:0c:29:05:2e:1a

1. Enter networking details manually
2. Configure networking setting automatically via DHCP
```

ファーストブート - 手動ネットワーク詳細

最初の起動時に、DHCP による IP 詳細の自動割り当てを中断するための 10 秒間が与えられます。

このプロセスを中断するには、コンソールウィンドウをクリックし、いずれかのキーを押す。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で、再起動後も有効であり、VA 上で再度設定する必要はない。

ファーストブート - DHCP 成功

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。コンタクトが成功すると、マシンに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

その IP アドレスが DHCP サーバー内の ADC の MAC アドレスに恒久的にリンクしている場合のみ、DHCP アドレスを使用して ADC を操作することをお勧めします。仮想アプライアンスを使用する場合は、常に**固定 IP アドレス**を使用することをお勧めします。ネットワーク設定が完了するまで、**管理 IP アドレスの変更**および以降のセクションの手順に従います。

初回起動 - DHCP が失敗

DHCP サーバーがない場合、または接続に失敗した場合、IP アドレス 192.168.100.100 が割り当てられません。

VA が空いている IP アドレスを見つけるまで、IP アドレスは「1」ずつ増加します。同様に、VA は IP アドレスが現在使用中かどうかを確認し、使用中であれば、再度インクリメントして再確認します。

管理 IP アドレスの変更

VA の IP アドレスは、**set greenside=n.n.n.n** コマンドを使っていつでも変更できます。

```
greenside={IPアドレス}に設定
```

eth0 のサブネットマスクを変更する

ネットワークインターフェイスは接頭辞「eth」を使用し、基本ネットワークアドレスは **eth0** と呼ばれる。サブネットマスクまたはネットマスクは、**set mask [NIC] [MASK]** コマンドを使って変更できる。以下に例を示す。

```
set mask eth0 {mask}
```

デフォルトゲートウェイの割り当て

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 [GATEWAY IP]** というコマンドを使用します。

```
route add default gw {IPアドレス}。
```

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、正しいかどうかを確認するには、**route** コマンドを使う。このコマンドはネットワークルートとデフォルトゲートウェイの値を表示します。以下の例を参照してください。

```
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・インターフェイス（GUI）にアクセスして、ADC を本番用または評価用に設定することができます。

ウェブインターフェースへのアクセス

JavaScript を搭載した任意のインターネット・ブラウザを使用して、ADC を設定、監視、運用開始することができます。

ブラウザの URL フィールドに、**HTTPS://{IP アドレス}** または **HTTPS://{FQDN}** のいずれかを入力する。

ADC はデフォルトで、自己署名 SSL 証明書を使用します。任意の SSL 証明書を使用するように ADC を変更できます。

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 の工場出荷時のデフォルト認証情報は以下のとおりです：

Username: admin / Pwd: 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
日付			現在設定されている日付と時刻を表示します。	2013年9月3日火曜日 13:00 UTC
デフォルト			アプライアンスの工場出荷時のデフォルト設定を割り当てる	
出口			コマンドラインインターフェイスからログアウトする	
ヘルプ			有効なコマンドをすべて表示	
イフコンフィグ	空白		すべてのインターフェイスのインターフェイス・コンフィグレーションを表示する	イフコンフィグ
	エスゼロ		eth0 のインターフェイス設定のみを表示する	ifconfig eth0
マシン ID			このコマンドは、ADC ADC のライセンスに使用されるマシン ID を提供します。	EF4-3A35-F79
やめる			コマンドラインインターフェイスからログアウトする	
再起動			すべての接続を終了し、ADC を再起動する。	再起動
リスタート			ADC の仮想サービスを再起動する	
ルート	空白		ルーティングテーブルを見る	ルート
	追加	デフォルト GW	デフォルトゲートウェイの IP アドレスを追加する	route add default gw 192.168.100.254
セット	グリーンサイド		ADC の管理 IP アドレスを設定する	set グリーンサイド =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する。インターフェイス名は eth0 、 eth1... です。	マスク 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します。	
シャットダウン			すべての接続を終了し、ADC の電源を切ります。	
ステータス			現在のデータ統計を表示	
トップ			CPU やメモリなどのプロセス情報を見る	
ビューログ	メッセージ		生の syslog メッセージを表示する	ログメッセージを見る

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。

ウェブ・コンソール

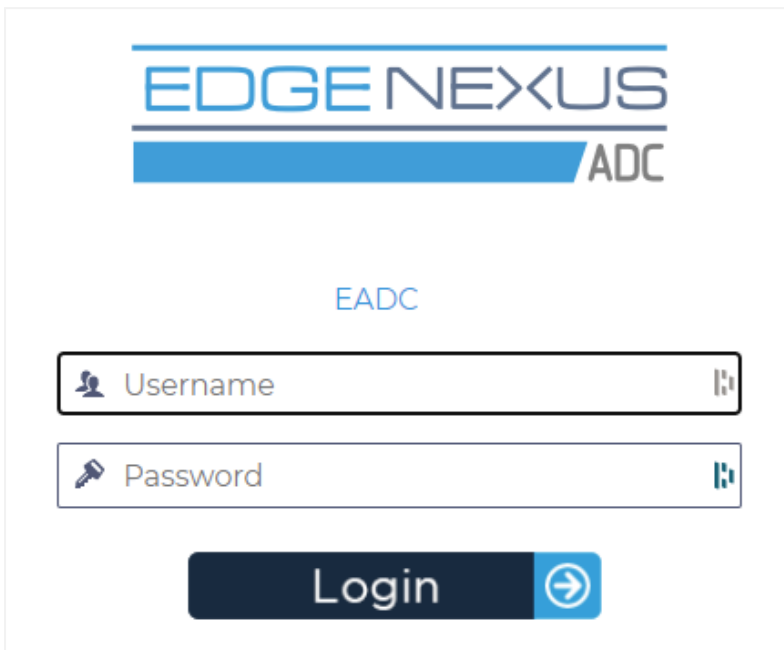
ADCウェブコンソールの起動

ADCのすべての操作は、ウェブ・コンソールを使用して設定および実行される。ウェブ・コンソールには、JavaScriptを搭載したブラウザでアクセスできます。

ADCのWebコンソールを起動するには、URLフィールドにADCのURLまたはIPアドレスを入力します。ここでは例として `adc.company.com` を使用します：

`https://adc.company.com`

起動すると、ADCのウェブ・コンソールは以下のようになり、adminユーザーとしてログインできる。



デフォルトのログイン認証情報

デフォルトのログイン認証情報は以下の通り：

Username: admin / Pwd: jetnexus

この設定は、[システム]>[ユーザー]にあるユーザー設定を使っていつでも変更できます。

ログインに成功すると、ADCのメイン・ダッシュボードが画面に表示されます。

外部認証サービスの利用

外部の認証サービスを使用したい場合は、認証サーバーと認証サービスを設定することで、使用することができます。

これに関する情報は、[認証](#) および [認証サービス](#) を参照されたい。

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」がどのように見えるかを示しています。時折、改良のために変更することがありますが、すべての機能は残ります。

The screenshot displays the EdgeADC main dashboard. At the top, there is a navigation bar with 'EDGE NEXUS' on the left and 'GUI Status', 'Home', 'Help', and 'admin' on the right. Below this, a 'NAVIGATION' sidebar on the left contains 'Services', 'App Store', and 'IP-Services'. The main content area is titled 'Virtual Services' and includes a search bar and buttons for 'Copy Service', 'Add Service', and 'Remove Service'. A table lists a single virtual service with the following data:

Mode	VIP	VS	Enab...	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active			<input checked="" type="checkbox"/>	10.0.0.130	255.255.255.0	80	Web Sites	HTTP(S)

Below the 'Virtual Services' section is the 'Real Servers' section, which has tabs for 'Server', 'Basic', 'Advanced', and 'flightPATH'. It features a search bar for 'Group Name' (set to 'Server Group') and buttons for 'Copy Server', 'Add Server', and 'Remove Server'. A table lists three real servers with the following data:

Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
	Online	10.0.0.20	80	100	50		
	Online	10.0.0.21	80	100	100		
	Online	10.0.0.22	80	100	100		

At the bottom of the dashboard, there is a footer indicating '[Timed licence 14 days left]'.

左側のナビゲーション・セクションでは、ADCの様々な機能をナビゲートすることができます。デフォルトでは、"Services"セクションが選択され、"Virtual Services"セクションの上にあるタブで示される"IP Services"サブセクションが開きます。このタブは固定されており、常に表示されます。

ナビゲーション内のセクションをクリックすると、そのセクションが展開され、内容が表示されます。セクション内のオプションをクリックすると、右側にセクションの内容が表示され、上部にタブが配置されるため、素早く切り替えることができます。

それぞれのナビゲーション・セクションについては、後の章で詳しく説明する。

サービス

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さまざまな仮想IPサービスを追加、削除、設定できます。設定と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

仮想サービスは、仮想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。仮想IPに到着したトラフィックは、そのサービスに関連付けられたリアルサーバーの1つにリダイレクトされます。仮想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。

ADCは、Real ServersセクションのBasicタブ内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再分配する方法を決定します。

新しいVIPを使用して新しい仮想サービスを作成する

Mode	VIP	VS	Enab...	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active			<input checked="" type="checkbox"/>	10.0.0.130	255.255.255.0	80	Web Sites	HTTP(S)

- 上記のように [Add Virtual Service] ボタンをクリックします。

Mode	VIP	VS	Enab...	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active			<input checked="" type="checkbox"/>	10.0.0.130	255.255.255.0	80	Web Sites	HTTP(S)

すると、行の編集モードに入る。

- ハイライトされた4つのフィールドに入力し、更新ボタンをクリックします。

TABキーを使用して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트리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、ユーザーまたはアプリケーションがロードバラン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になります。
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用である。
ポート	VIPにアクセスするとき使用するエントリポート。リバースプロキシを使用している場合は、この値をリアルサーバーと同じにす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したものです。省略可能ですが、わかりやすくするために入力することをお勧めします。このフィールドはGSLBを使用するとき他の特定の目的で使用されることに注意してください。
サービスタイプ	さまざまなサービスタイプをお選びいただけます。レイヤー4のサービスタイプはflightPATHテクノロジーを使用できません。

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：

Real Servers									
Server Basic Advanced flightPATH									
Group Name: Server Group						Copy Server		Add Server	Remove Server
Status	Activity	Address	Port	Weight	Cal. Weight	Monitor End Point	Notes	ID	
●	Online	10.0.0.20	80	100	100	Self		WEB1	
●	Online	10.0.0.21	80	100	100	Self		WEB1	
●	Online	10.0.0.22	80	100	100	Self		WEB1	

フィールド	説明
アクティビティ	<p>Activity フィールドは、負荷分散されたリアルサーバーのステータスを表示したり変更したりするのに使用できる。</p> <p>オンライン - サーバーがアクティブで、負荷分散されたリクエストを受信していることを示す。</p> <p>Offline - サーバーがオフラインで、リクエストを受信していない。</p> <p>ドレイン - サーバーがドレインモードになったため、パーシステンスがフラッシュされ、ユーザーに影響を与えることなくサーバーがオフライン状態に移行しました。</p> <p>スタンバイ - サーバーがスタンバイ状態になりました。</p>
IP アドレス	この値はリアルサーバーの IP アドレスである。正確でなければならず、DHCP アドレスであってはならない。
ポート	リアルサーバーのアクセス対象ポート。リバースプロキシを使用する場合は、VIP で指定したエントリポートと異なる可能性があります。
ウェイト	この設定は通常、ADC によって自動的に設定される。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る。
Cal.重量	重み付けをデフォルト値のままにしておくと、ADC は応答時間に基づいて重み付けを自動的に計算する。
モニター終了点	デフォルト値は「Self」である。ただし、ポート値または IP アドレス:ポートに変更できます。このフィールドは別のエンドポイントを監視し、トラフィックを仮想サービスに渡すかどうかを決定するのに使用します。以下の「モニター・エンドポイントの使い方」を参照してください。

- 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します。
- ステータスランプは、まず灰色に点灯し、サーバーの健全性チェックが成功すると緑色に点灯します。リアル・サーバー・モニターが失敗すると、赤色に変わります。
- ステータスランプが赤のサーバーはロードバランスされません。

完成したバーチャルサービスの例

Virtual Services									
Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type	
Active			<input checked="" type="checkbox"/>	10.0.0.142	255.255.255.0	443		HTTP(S)	
			<input checked="" type="checkbox"/>	10.0.0.142	255.255.255.0	80		HTTP(S)	
Active			<input checked="" type="checkbox"/>	10.0.0.143	255.255.255.0	443		HTTP(S)	

Real Servers										
Server	Basic	Advanced	flightPATH							
Status	Activity	Address	Port	Weight	Cal. Weight	Monitor End Point	Notes	ID		
	Online	10.0.0.20	80	100	100	Self	Web1	web1		
	Online	10.0.0.21	80	100	100	Self	Web2	web2		
	Online	10.0.0.22	80	100	100	Self	Web3	web3		

モニター・エンドポイントの使い方

例 1

エンドユーザーにウェブ・アプリケーションを提供する、負荷分散された 2 台のウェブ・サーバーからなるインフラを例にとってみよう。ウェブアプリケーションはバックエンドのデータベースサーバーに接続されています。データベースサーバーへのアクセスがダウンしても、ウェブアプリケーションサーバーは稼動したままです。ユーザーはウェブアプリケーションを使おうとしてエラーを受け取ります。

解決策は、モニター・エンド・ポイントを使うことである。

Virtual Services									
Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type	
Active			<input checked="" type="checkbox"/>	10.0.0.142	255.255.255.0	443		HTTP(S)	
			<input checked="" type="checkbox"/>	10.0.0.142	255.255.255.0	80		HTTP(S)	
Active			<input checked="" type="checkbox"/>	10.0.0.143	255.255.255.0	443		HTTP(S)	

Real Servers										
Server	Basic	Advanced	flightPATH							
Status	Activity	Address	Port	Weight	Cal. Weight	Monitor End Point	Notes	ID		
	Online	10.0.0.20	80	100	100	10.0.0.111:4033	Web1	web1		
	Online	10.0.0.21	80	100	100	10.0.0.111:4033	Web2	web2		
	Standby	10.0.0.22	80	100	100	Self	Web3	web3		

- この例では、10.0.0.20 と 10.0.0.21 という 2 台のウェブサーバーと、10.0.0.22 という 3 台目のウェブサーバーを示しています。10.0.0.22 サーバーはスタンバイ・モードになっています。
- 2 つのアクティブなウェブサーバは、データベースサーバ接続 IP アドレスとポートである 10.0.0.111:4033 の監視エンドポイント値で構成されています。
- データベース・サーバーの接続が切断された場合、2 台のアクティブ・サーバーはオフライン・モードになり、スタンバイ・サーバーはオンラインになり、顧客にシステムがメンテナンス中であることを知らせるウェブ・ページを提供します。

例 2

Monitor End Point のもう 1 つの使用例は、Always-On-VPN などの UDP プロトコルのサーバーをロードバランシングする場合である。ご存知のように、UDP ポートは確実に監視できないため、TCP ポートを監視する必要があります。

Monitor End Point を使用すると、そのようなことが可能になります。常時接続 VPN サーバが使用するメインポートは 53/udp ですが、8433/tcp を監視することになります。このような場合は、Monitor End Point フィールドにポート値を入力するだけでよい。

サブバーチャルサービスの作成

また、同じ VIP で異なるポートを使用してロードバランスを行う必要がある場合は、サブ仮想サービスを作成することもできます。たとえば、同じ仮想 IP を使用してポート 80、8088、443 でアクセスするサーバーがある場合、これに対応するためにサブ仮想サービスを作成する必要があります。

- コピーする仮想サービスをハイライトします。
- [Add Virtual Service] をクリックして行編集モードに入ります。

Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active	●	●	<input checked="" type="checkbox"/>	10.0.0.130	255.255.255.0	80	Web Sites	HTTP(S)
	●	●	<input checked="" type="checkbox"/>	10.0.0.130	255.255.255.0	443	Web Sites 443	HTTP(S)

- 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。
- サービスのポート番号を入力してください。
- 任意のサービス名を入力
- サービスタイプを選択してください。
- 更新ボタンを押すと、このセクションが保存され、以下のリアルサーバーのセクションに自動的にジャンプします。

Status	Activity	IP Address	Port	Weight	Calculated Weight	Notes
●	Online			100	100	

- サーバーの [アクティビティ] オプションを [オンライン] のままにします。これは、TCP コネクトのデフォルトのヘルスマニターをパスすれば、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することができます。
- 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
- Notes フィールドに Real Server の任意の名前を入力します。このメモ欄は flightPATH 変数など、他の特定の目的で使用されることを覚えておいてください。
- 更新をクリックして変更を保存します。
- リアルサーバーモニターが成功すると、ステータスランプはまずグレーに点灯し、次に緑に点灯します。リアルサーバーモニターが失敗すると赤に変わります。
- 赤のステータスランプが点灯しているサーバーは、負荷分散されません。

仮想サービスの IP アドレスの変更

既存の仮想サービスまたは VIP の IP アドレスはいつでも変更できます。

- IP アドレスを変更する仮想サービスをハイライトします。
- そのサービスの IP アドレスフィールドをクリックして、編集可能な状態に変更します。

Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active	●	●	<input checked="" type="checkbox"/>	10.0.0.130		80	Web Sites	HTTP(S)
Passive		●	<input checked="" type="checkbox"/>	10.0.0.131	255.255.255.0	443	Web Sites 443	HTTP(S)

- 使用したい IP アドレスに変更する。
- **Update** ボタンをクリックして変更を保存します。

注：仮想サービスの IP アドレスを変更すると、VIP に関連付けられたすべてのサービスの IP アドレスが変更されます。

コピーサービスを使用して新しい仮想サービスを作成する

- サービスのコピー ボタンをクリックすると、リアルサーバー、基本設定、詳細設定、flightPATH ルールなど、サービス全体がコピーされます。
- 複製したいサービスをハイライトし、「サービスをコピー」をクリックします。
- 行エディターが表示され、IP アドレス列に点滅するカーソルが表示されます。
- IP アドレスを一意になるように変更するか、IP アドレスを維持したい場合は、その IP アドレスに一意になるように 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、リアルサーバーモニター、flightPATH ルールの削除などの設定を変更した場合は、各タブを編集することを忘れないでください。

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 アドレスのオクテットやサービス名など、任意の値を使用してテーブルを検索することができます。

列の可視性の選択

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。

Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
●	Online	192.168.1.200	80	<input checked="" type="checkbox"/>	100	Site 1	
●	Online	192.168.1.201	80	<input checked="" type="checkbox"/>	100	Site 2	

- いずれかの列の上にマウスを移動させる。
- 列の右側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したい列が選択されます。

仮想サービスカラムを理解する








プライマリー/モード

モード]列には、現在のVIPで選択されている高可用性の役割が表示されます。モードについては、システム > クラスタリング > ロールを参照してください。

オプション	説明
アクティブ	クラスタモードでは、このフィールドの値は Active です。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、一方は Active 、もう一方は Passive と表示されます。現在のアプライアンス
パッシブ	ADC がクラスタのセカンダリ・メンバとして動作している場合、"Passive" が "Mode" 列に表示されます。
マニュアル	Manual の役割は、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、Primary 列には、各仮想 IP の横に、Active の場合は選択可能、Passive の場合はチェックなしのボックスが表示されます。
スタンドアロン	ADC はスタンドアロン・デバイスとして動作しており、High Availability モードではありません。そのため、Primary 欄には Stand-alone と表示される。

ビップ

この列は各仮想サービスのステータスを視覚的に表示します。インジケータは次のように色分けされています：

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バイ
	「セカンダリ」が「プライマリー」のために控えていることを示す。
	サービスには注意が必要です。この表示は、リアルサーバーがヘルスマニターチェックに失敗したか、手動でオフラインに変更されたために表示されます。トラフィックは流れ続けますが、リアルサーバーの容量は減少します。
	オフラインです。コンテンツサーバーに到達できない、またはコンテンツサーバーが有効になっていない
	調査状況
	ライセンスを取得していない、またはライセンスを超えた仮想 IP

有効

このオプションのデフォルトは [有効] で、チェックボックスはオンになっています。仮想サービスを無効にするには、行をダブルクリックしてチェックボックスをオフにしてから、[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 進ドット表記で、または IPv6 アドレスを追加します。この値は、サービスの仮想 IP アドレス (VIP) になります。例 IPv4 「192.168.1.100」。IPv6 の例 "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 進ドット表記で追加します。例「255.255.255.0」。また、/24 のようなサブネット値や、IPv6 の場合はプレフィックスを追加することもできます。IPv6 の詳細については、[HTTPS://JA.WIKIPEDIA.ORG/WIKI/IPV6_ADDRESS](https://ja.wikipedia.org/wiki/IPv6_address) を参照してください。

ポート

サービスに関連するポート番号を追加します。ポート番号には TCP または UDP を指定します。例：Web トラフィックには TCP「80」、セキュア Web トラフィックには TCP「443」。80～87 のように範囲を指定することもできます。

現在のところ、カンマ区切りの値を使用して、連続しないポート値を指定することはできません。

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"。このフィールドは GSLB を使用する場合にも使用されます。

サービスタイプ

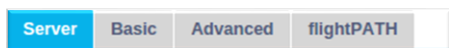
すべての "レイヤー4" サービスタイプでは、ADC はデータストリームを相互作用させたり変更したりしないため、flightPATH はレイヤー4 サービスタイプでは利用できないことに注意してください。レイヤー4 サービスは、ロードバランシングポリシーに従ってトラフィックをロードバランスするだけです：

サービスタイプ	ポート/プロトコル	サービス層	コメント
レイヤー4 TCP	任意の TCP ポート	レイヤー4	ADC はデータストリーム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従ってトラフィックの標準的なロードバランシングを実行する。
レイヤー4 UDP	任意の UDP ポート	レイヤー4	レイヤ 4 TCP と同様に、ADC はデータストリーム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従ってトラフィックの標準的なロードバランシングを実行する。
レイヤー4 TCP/UDP	任意の TCP または UDP ポート	レイヤー4	サービスが UDP などのプライマリ・プロトコルを持ちながら、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変更せず、ロードバランシングポリシーに従ってトラフィックの標準的なロードバランシングを実行します。
DNS	TCP/UDP	レイヤー4	DNS サーバーのロードバランスに使用される。
HTTP(S)	HTTP または HTTPS プロトコル	レイヤー7	ADC は、flightPATH を使用して、データストリームを操作し、変更することができます。
ファイル転送プロトコル	ファイル転送プロトコル	レイヤー7	クライアントとサーバー間で、制御とデータ接続を別々に使用する。
SMTP	簡易メール転送プロトコル	レイヤー4	メールサーバーの負荷分散に使用

ポップスリー	郵便局の手順	レイヤー4	メールサーバーの負荷分散に使用
アイマップ	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	メールサーバーの負荷分散に使用
右派系	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負荷分散に使用
正規化投影座標系	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の負荷分散を行う場合に使用する。
RPC/ADS	Exchange 2010 アドレス帳サービスの静的 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	Exchange 2010 クライアントアクセスとパブリックフォルダの静的 RPC	レイヤー4	Exchange サーバーのロードバランシングに使用
ディコム	医療におけるデジタル画像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を負荷分散する場合に使用します。

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る : **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仮想サービスとペアになっている実際のバックエンドサーバーの定義が表示されます。実サーバー] セクションに少なくとも 1 つのサーバーを追加する必要があります。

Status	Activity	Address	Port	Weight	Calculated Weight	Monitor End Point	Notes	ID
Online	Online	10.0.0.20	80	100	100	Self		
Online	Online	10.0.0.21	80	100	100	Self		
Online	Online	10.0.0.22	80	100	100	Self		

サーバーの追加

- 以前に定義した適切な **VIP** を選択します。
- サーバーの追加
- 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**をドット付き **10 進表記**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、直接接続されたローカルネットワーク、または **ADC** がルーティングできるネットワーク上にあることができます。例「**10.1.1.1**」。
- **Port]** 列にタブして、サーバーの **TCP/UDP** ポート番号を入力します。ポート番号は、仮想サービスポート番号と同じか、リバースプロキシ接続用の別のポート番号にすることができます。**ADC** は自動的にこの番号に変換します。
- **Notes** セクションに移動し、サーバーに関連する詳細を追加します。例"**IIS** ウェブサーバー1"

グループ名

Server		Basic	Advanced	flightPATH						
Group Name: <input type="text" value="Server Group"/>					Copy Server		Add Server		Remove Server	
Status	Activity	Address	Port	Weight	Calculated Weight	Monitor End Point	Notes	ID		
	Online	10.0.020	80	100	100	Self				
	Online	10.0.021	80	100	100	Self				
	Online	10.0.022	80	100	100	Self				

負荷分散セットを構成するサーバーを追加したら、グループ名を追加することもできます。このフィールドを編集すると、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・ステータス・ライト

リアルサーバーのステータスは、「ステータス」カラムの光の色で確認できます。下記をご覧ください：

LED	意味
	接続済み
	モニターなし
	水抜き
	オフライン
	スタンバイ
	未接続
	発見状況
	ライセンスを取得していない、またはライセンスを取得したリアルサーバーを超える

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	ドレインとして割り当てられたすべてのリアルサーバーは、既存の接続へのサービスは継続しますが、新しい接続は受け付けません。ドレイン処理中は Status ランプが緑/青に点滅します。既存の接続が自然に閉じられると、リアルサーバーはオフラインになり、 Status ライトは青で点灯します。ナビゲーション」>「モニター」>「ステータス」セクションに移動して、これらの接続を表示することもできます。 Drain Behaviour は Advanced setting タブで変更できます。

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、トラフィックを受信しなくなります。
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サーバーがすべてサーバーヘルスマニターのチェックに失敗するまでオフラインのままになります。この場合、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つのサーバーがサーバーヘルスマニターチェックに合格すると、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

このフィールドはリアルサーバーの IP アドレスです。例「192.168.1.200」。

ポート

リアルサーバーがサービスのためにリッスンしている TCP または UDP ポート番号。例：ウェブトラフィックの場合は「80」。

重量

この列は、適切なロードバランシングポリシーが指定されると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、1~100 の値を入力できます。100 は最大負荷、1 は最小負荷を意味します。

サーバーが 3 台の場合の例は次のようになります：

- サーバー1 ウェイト = 100
- サーバー2 ウェイト = 50
- サーバー3 ウェイト = 50

ロードバランシングポリシーが **Least Connections** に設定され、クライアント接続の合計が 200 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 は 50 の同時接続を得る
- サーバー3 の同時接続数は 50

負荷分散されたサーバーセットでリクエストをローテーションさせるラウンドロビンを負荷分散方法として使用する場合、重みを変更することは、サーバーがターゲットとして選択される頻度に影響します。

Fastest ロードバランシングポリシーがレスポンスの **GET** にかかる最短時間を使用すると考える場合、重みを調整することで、**Least Connections** と同様にバイアスが変化します。

計算重量

各サーバーの **Calculated Weight** は動的に表示され、自動的に計算されます。このフィールドは、ADC が手動重み付けとロードバランシングポリシーを考慮する際に使用している実際の重み付けを示します。

モニター終了点

この機能により、監視する特定のエンドポイントを指定して、リアルサーバーエントリの健康状態を判断することができます。デフォルト値の「自己」のままにすると、仮想サービスに指定されたリアルサーバーモニターに依存します。また、IP アドレス、ポート、または IP アドレス:ポートを指定して、ネットワーク上の別のエンドポイントを監視することもできます。この例としては、サービスが依存しているデータベースサーバーなどがあります。

備考

「Notes」フィールドに、定義されたエントリーの説明に役立つ特定のメモを入力します。例「IIS Server1 - London DC」。このフィールドは、flightPATH ルールと GSLB 内の特定のニーズに使用できます。

身分証明書

このセッティングには多くの用途がある。


永続性

この値は、クッキーID ベースの永続化メソッドと組み合わせて使用することができます。これは PHP のセッションベースの永続化とよく似ていますが、Cookie ID Based と Cookie RegEx `h=[^;]+` という新しいテクニックを使います。クッキーID ベースの永続化ベースのメソッドは、ID フィールドの値を使用してクッキーを生成します。

flightPATH の使用法

また、このフィールドの値を使用して、トラフィックなどを誘導することもできます。

ベーシック

Server	Basic	Advanced	flightPATH
Load Balancing Policy:	Least Connections		
Server Monitoring:	TCP Connection		
Caching Strategy:	Off		
Acceleration:	Compression		
Virtual Service SSL Certificate:	No SSL		
Real Server SSL Certificate:	No SSL		
 Update			

ロードバランシングポリシー

ドロップダウンリストには、現在サポートされている使用可能な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説明は以下の通りです。

- Least Connections
- Fastest
- Persistent Cookie
- Round Robin
- IP-Bound
- IP List Based
- Shared IP List Based
- Classic ASP Session Cookie
- ASP.NET Session Cookie
- JSP Session Cookie
- JAX-WS Session Cookie
- PHP Session Cookie
- RDP Cookie Persistence
- Cookie ID Based

オプション

説明

最も少ないコネクション	ロードバランサは各リアルサーバへの現在の接続数を記録します。コネクション数が最も少ないリアルサーバが、その後の新しいリクエストを受け取ります。
最速	最速ロードバランシングポリシーでは、サーバーごとの全リクエストの応答時間を自動的に計算し、時間を平滑化します。計算された重み]列には、自動的に計算された値が含まれます。手動入力、このロードバランシングポリシーを使用する場合にのみ可能です。
永続的クッキー	レイヤ7セッション・アフィニティ/パーシステンス 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る。ADC は最初の HTTP レスポンスのヘッダーに Cookie を挿入する。その後、ADC はクライアント・クッキーを使用して、同じバックエンド・サーバーにトラフィックを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時間後に失効し、接続はIP リストベースのアルゴリズムに従って負荷分散されます。この有効期限は jetPACK を使って設定できます。
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、最も単純な方法である。各リアルサーバは新しいリクエストを順番に受け取ります。この方法は、サーバへのリクエストを均等にロードバランスする必要がある場合にのみ適切です。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したり、セッションに同じサーバーを使うようにしたりする必要があるときは、ラウンドロビン方式は不適切です。
IP バウンド	レイヤ3セッションアフィニティ/パーシステンスクッキー。 このモードでは、クライアントの IP アドレスが、どの Real Server がリクエストを受け取るかを選択する基準になる。この動作は永続性を提供する。HTTP とレイヤ4プロトコルはこのモードを使うことができる。この方法は、ネットワークポロジがわかかっていて、上流に「スーパープロキシ」がないと確信できる内部ネットワークに役立ちます。レイヤ4とプロキシでは、すべてのリクエストがあたかも1つのクライアントから来ているように見え、負荷が均等にならない。HTTP では、ヘッダー(X-Forwarder-For)情報はプロキシに対処するために存在するときに使われます。
IP リストベース	リアルサーバーへの接続は「最小接続数」を使用して開始され、セッションの親和性はクライアントの IP アドレスに基づいて達成されます。リストはデフォルトで2時間維持されますが、jetPACK を使用して変更できます。
共有 IP リストベース	このサービスタイプは、接続モードが Direct Server Return に設定されている場合にのみ利用可能です。主に VMware のロードバランシングをサポートするために追加されました。
永続的クッキー	レイヤ7セッション・アフィニティ/パーシステンス IP リストベースのロードバランシングモードは、それぞれの最初のリクエストに使用される。ADC は最初の HTTP レスポンスのヘッダーに Cookie を挿入する。その後、ADC はクライアント・クッキーを使用して、同じバックエンド・サーバーにトラフィックを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時間後に失効し、接続はIP リストベースのアルゴリズムに従って負荷分散されます。この有効期限は jetPACK を使って設定できます。
クラシック ASP セッションクッキー	Active Server Pages (ASP) は Microsoft 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、ADC は、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、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 アルゴリズムを使って負荷分散が行われます。
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。このモードが選択されると、ADC は、ASP.NET クッキーが検出され、既知のクッキーのリストで見つかった場合、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 ASP クッキーが検出されると、Least Connections アルゴリズムを使って負荷分散されます。
JSP セッションクッキー	Java Server Pages (JSP)は Oracle 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、その既知のクッキー・リストで見つかった場合、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 アルゴリズムを使って負荷分散が行われます。
JAX-WS セッションクッキー	Java Web サービス (JAX-WS) は、Oracle 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で見つかった場合、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 アルゴリズムを使って負荷分散が行われます。
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とき、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。
RDP クッキーの永続性	このロードバランシング方式では、ユーザー名/ドメインに基づいてマイクロソフトが作成した RDP クッキーを使用して、サーバーへの永続性を提供する。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。
クッキーID ベース	<p>PhpCookieBased」や他の負荷分散メソッドによく似た新しいメソッドですが、CookieIDBased とクッキーの RegEx <code>h=[^;]+</code> を使います。</p> <p>このメソッドは、サーバを識別するクッキーの値として、リアルサーバのノートフィールド「ID=X;」に設定された値を使用します。したがって、これは CookieListBased と同じような方法論ですが、異なるクッキー名を使い、スクランブルされた IP ではなく、Real Server からの ID(ロード時に読み込まれます。)というユニークなクッキー値を保存することを意味します。</p> <p>デフォルト値は CookieIDName="h" ですが、仮想サーバの詳細設定にオーバーライド値がある場合は、代わりにこれを使用してください。注意: この値が設定されている場合、h= を新しい値に置き換えるために、上記のクッキー式を上書きします。</p> <p>そうでなければ、次のメソッド(delegate.)を使ってください。</p>

サーバー監視

ADC には、あらかじめ定義されたリアルサーバー監視方法がいくつかあります。

仮想サービス (VIP) に適用する監視方法を選択

サービスに適したモニターを選択することが不可欠である。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。同様に、TCP 接続と 200OK を選択しても、200OK を動作させるには TCP 接続が必要なので、意味がありません。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 Connection 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番に実行されます。したがって、最初に低レイヤーのモニターから開始します。例えば、Ping/ICMP エコー、TCP コネクション、200OK のモニターを設定すると、下図のようにダッシュボードのイベントに表示されます：

Status	Date	Message
ATTENTION	10:22 26 Feb 2016	10.4.8.131:89 Real Server 172.17.0.2:88 unreachable - Echo=OK Connect=OK 200OK=FAIL
OK	10:22 26 Feb 2016	10.4.8.131:89 Real Server 172.17.0.2:88 contacted - Echo=OK Connect=OK 200OK=OK

一番上の行を見ると、レイヤー3のPingとレイヤー4のTCPコネクトは成功しているが、レイヤー7の200OKは失敗していることがわかる。これらのモニタリング結果は、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ますが、ウェブサイトは要求されたページに正しく応答していません。次に、ウェブサーバーと「ライブラリ > リアルサーバーモニター」セクションを見て、失敗したモニターの詳細を確認します。

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、常に正常に稼働します。なし]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参加すべきでないサービスに役立ちます。これは、H/A運用のプライマリではない、信頼性の低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。どのサービスタイプでも、このモニタリング方法を使用してください。
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エコー要求を送信する。有効なエコー応答を受信した場合、ADCはReal Serverを稼働中とみなし、サーバーへのトラフィック・スルーputを継続する。また、H/Aペアでサービスを利用可能な状態に保つ。このモニタリング方法は、どのサービス・タイプでも使用可能です。
TCP コネクション	このモードでは、リアル・サーバーにTCP接続が確立され、データを送信することなく直ちに切断される。接続が成功した場合、ADCはReal Serverが稼働中であるとみなす。この監視方法はどのサービスタイプでも使用可能で、UDPサービスは現在のところTCPコネクション監視には適していません。
ICMP 到達不能	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した場合、リアルサーバーを使用不可としてマークします。この方法は、DNSポート53など、UDPサービスポートがサーバーで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。
右派系	このモードでは、ICMP Unreachableの説明に従ってTCP接続が初期化されます。接続が初期化された後、レイヤ7RDP接続が要求されます。リンクが確認されると、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Microsoft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、TCP接続がReal Serverに対して初期化される。接続が成功すると、ADCはReal Serverに対してHTTPリクエストを送信する。HTTPレスポンスが待機され、「200 OK」レスポンスコードがチェックされる。「200 OK」レスポンスコードを受信した場合、ADCはReal Serverが稼働していると判断します。タイムアウトや接続失敗など、何らかの理由で「200 OK」レスポンス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不可と判断します。この監視方法は、HTTPおよびaccelerated HTTPサービスタイプでのみ有効です。HTTPサーバーにレイヤー4サービスタイプが使用されている場合、リアルサーバーでSSLが使用されていないか、または「コンテンツSSL」機能によって適切に処理されていれば使用可能です。
ディコム	DICOMモードでReal ServerへのTCP接続が初期化され、接続時にEchoscuからReal Serverへ"Associate Request"が行われる。コンテンツサーバーからの"Associate Accept"、少量のデータ転送、"Release Request"、"Release Response"の会話でモニターは正常に終了する。モニターが正常に終了しなかった場合、リアルサーバーは何らかの理由でダウンしたとみなされる。
ユーザー定義	リアルサーバーモニタリングセクションで設定されたモニターがリストに表示されます。

キャッシュ戦略

デフォルトでは、キャッシュ・ストラテジーは無効で **Off** に設定されています。サービスタイプが **HTTP** の場合、2種類のキャッシュ戦略を適用できます。

キャッシュの詳細設定については、キャッシュの構成ページを参照してください。アクセラレーテッド **"HTTP"** サービスタイプの **VIP** にキャッシュが適用されている場合、圧縮オブジェクトはキャッシュされないことに注意してください。

オプション	説明
ホスト	ホストごとのキャッシュは、ホスト名ごとのアプリケーションに基づいています。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、ドメインによって複数のウェブサイトを提供できるウェブサーバーに最適です。
バーチャル・サービス	このオプションを選択すると、仮想サービスごとにキャッシュを利用できます。仮想サービスを通じてすべてのドメイン/ホスト名に対して、キャッシュは1つだけ存在します。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	仮想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がオンになります。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。コンテンツの例には、 HTML 、 CSS 、または JavaScript が含まれます。 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）提供する。

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、設定は **[SSL なし]** です。サービスタイプが「**HTTP**」の場合、ドロップダウンから証明書を選択して仮想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。

また、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もできます。この操作により、クライアントが要求した「ドメイン名」に基づく証明書を許可する **SNI** エクステンションが自動的に有効になります。

Virtual Service SSL Certificate:

No SSL

All

default

AnyUseCert

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ない。
すべて	使用可能なすべての証明書をロードする

デフォルト	このオプションを使用すると、ローカルで作成された "Default " という証明書がブラウザ側のチャンネルに適用されます。このオプションは、 SSL が作成またはインポートされていない場合に SSL をテストするために使用します。
-------	--

リアルサーバー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。サーバーが暗号化された接続を必要とする場合、この値は **SSL** なし以外でなければなりません。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。

No SSL
Any
SNI
default

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、クライアント側で "SSL なし" を選択し、いわゆる "SSL オフロード" を提供できることを意味する。
どんなものでも	ADC はクライアントとして動作し、 Real Server が提示するどの証明書も受け入れる。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は暗号化されます。仮想サービス側で証明書が指定されている場合は、「 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する「 Any 」オプションを使用します。
エスエヌアイ	SNI (Server Name Indication) は、TLS ネットワーク・プロトコルの拡張機能で、ハンドシェッキング・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す。この設定により、ADC は同じ仮想 IP アドレスと TCP ポートで複数の証明書を提示できるようになります。
デフォルト	生成した自己署名証明書はすべてここに表示される。

上級

Real Servers

Server
Basic
Advanced
flightPATH

Connectivity: Reverse Proxy

Cipher Options: Defaults

Client SSL Renegotiation:

Client SSL Resumption:

SNI Default Certificate: None

Client Proxy Header: None

Server Proxy Header: None

Real Server Source Address: Base IP

Security Log: On

Max. Connections (Per Real Server):

Connection Timeout (sec): 600

Persistence Timeout (sec):

Monitoring Interval (sec): 10

Monitoring Timeout (sec): 2

Monitoring In Count: 2

Monitoring Out Count: 3

Monitoring KCD Realm: None

Drain Behaviour: Persistence Driven

Switch To Offline On Failure:

Update

コネクティビティ

仮想サービスはさまざまなタイプの接続を設定できます。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	<p>リバースプロキシはデフォルトの値で、レイヤー7で使用する場合は圧縮とキャッシュを使用します。レイヤ4では、リバースプロキシはキャッシュや圧縮なしで動作します。このモードでは、ADCがリバースプロキシとして動作し、リアルサーバから見えるソースアドレスになります。</p>
サーバー直行便	<p>ダイレクト・サーバー・リターン (DSR) は DR (ダイレクト・ルーティング) と呼ばれ、ロードバランサーの背後にあるサーバが、レスポンスの ADC をバイパスしてクライアントに直接レスポンスすることを可能にします。DSR はレイヤー4 のロードバランシング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、キャッシュと圧縮は利用できません。</p> <p>このモードは、TCP、UDP、および TCP/UDP サービス・タイプでのみ使用できる。ロードバランシングの永続化ポリシーも、Least Connections、Shared IP List Based、Round Robin、IP List Based に制限されている。</p> <div data-bbox="395 860 754 992" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Least Connection</p> <p>Shared IP List Based</p> <p style="background-color: #e0f0ff;">Round Robin</p> <p>IP List Based</p> </div> <p>DSR を使用するには、リアルサーバの変更も必要です。リアルサーバの変更のセクションを参照してください。</p>
ナット	<p>デフォルトでは、ADC はソース IP アドレスとして ADC の IP アドレスを使用し、リアルサーバはクライアントに応答を返すために ADC に応答を送り返します。これはほとんどすべての状況で問題ありませんが、リアルサーバが ADC ではなくクライアントのソース IP アドレスを見る必要があるシナリオがあります。</p> <p>NAT モードが適用されると、ADC は受信要求を受け取り、ソース IP アドレスを仮想サービスのもの (VIP アドレス) に戻した後、それをリアルサーバに送信します。</p> <p>このモードは、以下のロードバランシングポリシーでのみ使用できます：</p> <div data-bbox="395 1352 810 1462" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Least Connection</p> <p style="background-color: #e0f0ff;">Round Robin</p> <p>IP List Based</p> </div>
ゲートウェイ	<p>ゲートウェイモードでは、ADC を介してすべてのトラフィックをルーティングすることができ、リアルサーバを ADC の仮想サービスまたはハードウェアインターフェイ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。リアルサーバのゲートウェイデバイスとしてデバイスを使用することは、マルチインターフェースモードで実行する場合に最適です。</p> <p>ロードバランシング・パーシステンス・ポリシーも、Least Connections、Shared IP List Based、Round Robin、IP List Based に制限されている。</p> <div data-bbox="395 1756 754 1888" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Least Connection</p> <p>Shared IP List Based</p> <p style="background-color: #e0f0ff;">Round Robin</p> <p>IP List Based</p> </div> <p>この方法では、Real Server が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。リアルサーバの変更のセクションを参照してください。</p>

ゲートウェイモードはクラスタ環境でのフェイルオーバーをサポートしないことに注意してください。

暗号オプション

暗号は **SSL** 暗号の基礎を形成し、安全なウェブコンテンツとアプリケーションの配信を成功させるために非常に重要です。

ADC には、使用可能な最新の安全なものからなるデフォルトの暗号セットが組み込まれています。

ユーザが特定の一連の暗号の利用可能性を発表することを望む場合があり、**ADC** はユーザが作成した **jetPACK** を通じてそのような暗号を作成することができます。ユーザが作成した **jetPACK** は、「設定」>「ソフトウェア」を通じて **ADC** にインポートすることができ、その後、「暗号オプション」メニューを使用して選択できるようになります。

暗号化オプションは各 **VIP** に特化し、高い柔軟性とセキュリティを提供します。

サイファーオプションの詳細については、こちらをご覧ください：[サイファー](#)

クライアント **SSL** 再ネゴシエーション

クライアント主導の **SSL** 再ネゴシエーションを許可する場合は、このボックスにチェックを入れます。クライアントの **SSL** 再ネゴシエーションを無効にして、**SSL** レイヤーに対する **DDOS** 攻撃の可能性を防ぎます。

クライアント **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した場合、サーバーはセッションが見つければ再利用を試みます。再開] をオフにすると、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 **SNI** が有効な **SSL** 接続中、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いずれとも一致しない場合、**ADC** は **SNI** デフォルト証明書を提示する。デフォルトの設定は「None」であり、完全に一致しない場合、接続は事実上切断される。**SSL** 証明書の完全一致に失敗した場合、ドロップダウンからインストールされている証明書のいずれかを選択して提示します。

プロキシ・プロトコル

Proxy プロトコルは、ネットワークプロキシがクライアントの接続情報(発信元 **IP** アドレスやポート番号など)を受信サーバに転送できるように設計されている。このプロトコルは、トラフィックがロードバランサーやリバースプロキシを通してルーティングされる間、実際のエンドユーザー **IP** アドレスを保持する必要があるシナリオで特に有用です。これは、ロギング、統計、またはセキュリティの目的で元のクライアントのソース **IP** を維持するのに役立ち、トラフィックの真のソースに基づいて情報に基づいた意思決定を行う機能を強化します。

クライアントプロキシヘッダ

Client Proxy Header は、**ADC** がクライアントのリクエストに追加するヘッダーを指し、元の接続情報(クライアントの **IP** アドレスやポートなど)をカプセル化する。これは、**ADC** がプロキシとして動作し、サーバがロギング、セキュリティ評価、クライアント固有の動作の維持などの目的のために元のクライアント

トの詳細を知る必要がある環境では極めて重要です。Client Proxy Header は、ADC の仲介の役割にもかかわらず、サーバがクライアントの元の接続の詳細を正確に識別し、対話できることを保証します。

オプションは以下の通り：

オプション	説明
なし	Proxy ヘッダーがないか、現在のサービスタイプでサポートされていない場合。
削除	TCP パケットから Proxy ヘッダを削除する。
フォワード	Proxy ヘッダーをサーバーに転送

サーバー・プロキシ・ヘッダー

Server Proxy Headers には 2 つのバージョンがある：バージョン 1 とバージョン 2 です。

オプション	説明
バージョン 1	<ul style="list-style-type: none"> テキストベースのフォーマットで、実装とデバッグが容易。 ソース IP、宛先 IP、ソースポート、宛先ポートなど、クライアントの接続に関する基本情報を提供します。 プロトコル行は TCP コネクションの先頭に追加されるため、人間が読むことは可能だが、バイナリ・フォーマットと比較するとパフォーマンス面で若干劣る。
バージョン 2	<ul style="list-style-type: none"> パフォーマンスと効率を高めるために設計されたバイナリ形式。 アドレス・ファミリーやプロトコル固有情報などの追加データをサポートし、接続について中継できる情報を拡張する。 IPv6 や TCP 以外のトランスポート・プロトコルのサポートなど、最新のネットワーク・プロトコルや機能との互換性が向上しています。

Client Proxy Header オプションと Server Proxy ヘッダーオプションは、レイヤ 4 とレイヤ 7 の HTTP サービスタイプでのみ使用できます。

リアル・サーバー・ソース・アドレス

この設定はリバースプロキシとレイヤー4 TCP、レイヤー4 UDP、HTTP(S)サービスのいずれかと連動します。この設定には 3 つのオプションがあります。

オプション	説明
ベース IP (デフォルト)	リクエストのソース IP として、ADC の eth0、またはベース IP アドレスを使用する。
バーチャル IP	サービスの仮想 IP を使用する。
<IP アドレス	ADC の一部である IP アドレスを指定できます。これは、別のネットワークインターフェイスまたは別の VIP である可能性があります。

セキュリティログ

On」はデフォルト値で、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。ログアイコンをクリックすると、「システム」>「ログ」ページに移動し、W3C ログの設定を確認できます。

マックス最大接続数

リアルサーバーの同時接続数を制限し、サービスごとに設定します。たとえば、この値を 1000 に設定し、2 台のリアルサーバーを使用する場合、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すると、「サーバーが混み合っています」ページを表示することもできます。無制限に接続する場合は、ここを空白のままにします。ここで設定する値は、システムリソースによって異なります。

接続タイムアウト

デフォルトの接続タイムアウトは 600 秒または 10 分です。この設定は、アクティビティがない場合に接続がタイムアウトするまでの時間を調整します。短時間のステートレス Web トラフィック（通常は 90 秒以下）の場合は、この値を小さくします。RDP のようなステートフル接続の場合は、インフラストラクチャに応じて、この数値を 7200 秒（2 時間）以上に増やします。RDP のタイムアウトの例は、ユーザーが 2 時間以下の非アクティブ時間がある場合、接続はオープンのままであることを意味します。

永続タイムアウト

ロードバランサの永続タイムアウト設定は、ロードバランサがクライアントのセッション情報を保持する期間を指定します。これにより、同じクライアントからのそれ以降のリクエストが同じバックエンドサーバーに向けられ、セッションの一貫性とステートフルな通信が保証されます。指定されたタイムアウト時間が過ぎてクライアントの動きがなくなると、セッション情報は破棄され、新しいリクエストは別のサーバーに送られます。

モニタリング間隔

間隔はモニター間の時間を秒単位で指定する。デフォルトの間隔は 1 秒である。ほとんどの用途では 1 秒が許容範囲ですが、他の用途やテスト時には間隔を広げた方がよいでしょう。

監視タイムアウト

タイムアウト値は、ADC が接続要求に対してサーバーが応答するまで待機する時間である。デフォルト値は 2 秒である。ビジー状態のサーバーでは、この値を増やします。

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マニターチェックに 2 回合格する必要がある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に対応できる確率が高くなりますが、間隔によってはサービス開始までに時間がかかります。この値を小さくすると、サーバーのサービス開始が早くなります。

監視アウト回数

この設定のデフォルト値は 3 です。これは、ADC がサーバーへのトラフィック送信を停止するまでに、リアル・サーバー・モニターが 3 回失敗しなければならず、そのサーバーは RED で到達不能とマークされることを意味します。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、より優れた信頼性の高いサービスが提供されます。

KCD 領域のモニタリング

この設定により、Kerberos 定義で設定した Kerberos Constrained Delegation Realm の監視を有効にできます。認証] > [Kerberos] を参照してください。

ドレインの挙動

リアルサーバをドレインモードにするときは常に、送信されるトラフィックの動作を制御できる方がよいでしょう。Drain Behaviour メニューでは仮想サービスごとにトラフィックの動作を選択できます。オプションは以下の通りです：

オプション	説明
パーシステンス・ドリブン	これはデフォルトの選択である。 ユーザーが永続セッションを使用して訪問するたびに、永続セッションは拡張される。 24 時間使用すれば、ドレインが発生しない可能性もある。 しかし、実サーバーへの接続数が 0 になった場合、ドレインは終了し、永続セッションは削除され、すべての訪問者は次の接続でバランスを取り直す。
訪問者の移行	再接続時に永続セッションが無視される - (2022 年以前のレガシーな動作) 新しい TCP 接続は（既存のセッションの一部であるかどうかにかかわらず）、常にオンラインのリアルサーバーに対して行われる。 永続化セッションが消耗している実サーバーに対するものであった場合、それは上書きされる。 仮想サービスは新しい接続の永続性を実質的に無視し、新しいサーバーに負荷分散されます。
引退セッション	永続的なセッションは延長されない。 着信したユーザー接続は、希望するサーバーに割り当てられるが、持続セッションは延長されない。そのため、永続セッション時間を超えると、新しい接続として扱われ、別のサーバーに移動します。

失敗時にオフラインに切り替える

これをチェックすると、ヘルスチェックに失敗したリアルサーバーはオフラインになり、手動でのみオンラインに設定できます。

フライトパス

flightPATH は Edgenexus によって設計されたトラフィック管理テクノロジーで、ADC 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動作しない。その代わりに、**GUI** を使用して、必要なものを達成するために実行するさまざまなパラメータ、条件、アクションを選択する。これらの機能により、**flightPATH** は非常に強力になり、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できるようになる。

flightPATH は **HTTPS** 接続でのみ使用可能で、仮想サービスタイプが **HTTP** でない場合はこのセクションは表示されません。

左側に利用可能なルールの一覧があり、右側にバーチャルサービスに適用されるルールがある。

利用可能なルールを適用するには、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して右矢印をクリックして右側に移動します。

実行順序は必須であり、一番上のルールが最初に実行される。実行順序を変更するには、ルールをハイライトし、矢印を使って上下に移動する。

ADC のこのセクションの **flightPATH** ルールはブール値の **OR** ベースで動作するのに対し、**flightPATH** 定義エリア内の条件とアクションは **AND** ベースで動作することを理解することが重要である。

ルールを削除するには、左側のルール・インベントリにドラッグ・アンド・ドロップするか、ルールをハイライトして左矢印をクリックします。

このガイドの **Configure flightPATH** セクションで **flightPATH** ルールを追加、削除、編集することができます。

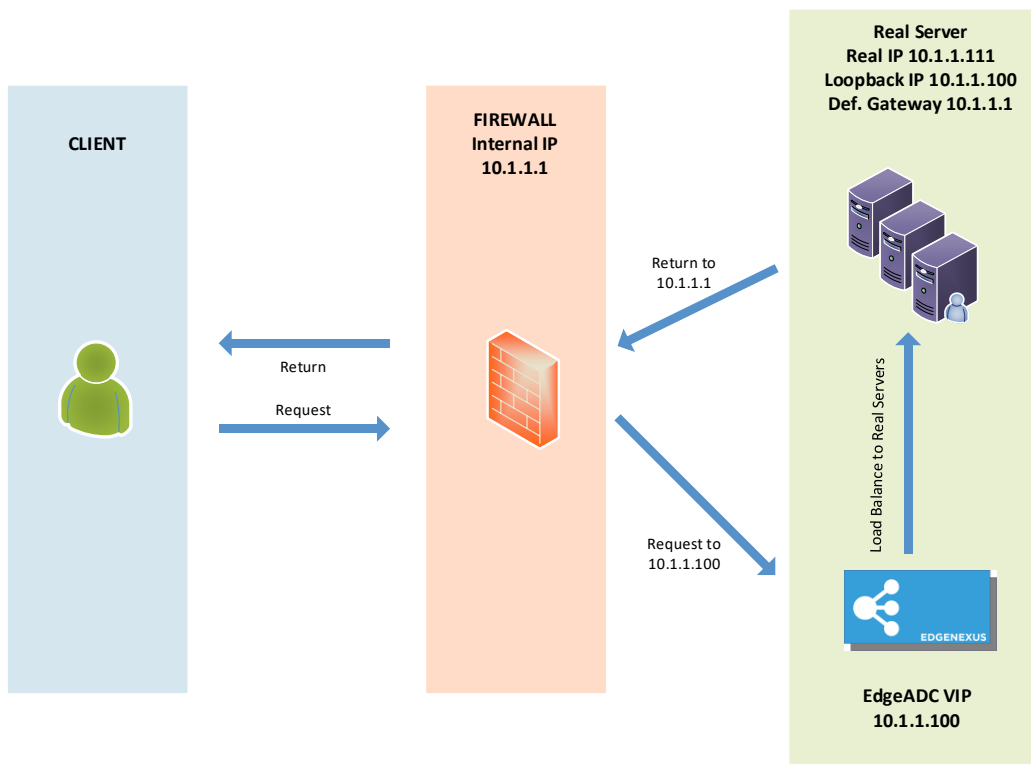
サーバー直帰に伴うリアルサーバーの変更

ダイレクト・サーバー・リターンまたは **DSR**（広く知られているように **DR - ダイレクト・ルーティング**）は、**ADC** の背後にあるサーバーがクライアントに直接応答し、応答時に **ADC** をバイパスすることを可能にします。**DSR** はレイヤー4 のロードバランシングにのみ適している。キャッシングと圧縮は、有効にすると利用できません。

この方法によるレイヤー7 ロードバランシングは、ソース IP 以外のパーシステンスサポートがないため、機能しません。この方法による **SSL/TLS** ロードバランシングは、ソース IP のパーシステンスサポートしかないため、理想的ではありません。

仕組み

- クライアントは **EdgeADC VIP** にリクエストを送信する。
- **EdgeADC** がリクエストを受信
- コンテンツ・サーバーへのリクエスト
- **EdgeADC** を経由せずにクライアントに直接送信されるレスポンス



必要なコンテンツサーバーの構成

一般

- コンテンツサーバーのデフォルトゲートウェイは通常通り設定する。(ADC 経由ではない)
- コンテンツサーバーとロードバランサーは同じサブネットになければならない。

ウィンドウズ

- コンテンツサーバーは、チャンネルまたは **VIP** の IP アドレスでループバックまたはエイリアスをチャンネルまたは **VIP** の IP アドレスで設定する必要があります。

- ARP リクエストに応答しないようにするには、ネットワークのメトリックを 254 にする必要がある。
- Windows Server 2012 でループバックアダプターを追加する - [ここをクリック](#)
- Windows Server 2003/2008 でループバックアダプターを追加する - [ここをクリック](#)
- Windows リアルサーバーに設定した各ネットワークインターフェイスについて、コマンドプロンプトで以下を実行します。

```
netsh interface ipv4 set interface "Windows network interface name" weakhostreceive=enable
```

```
netsh interface ipv4 set interface "Windows loopback interface name"  
weakhostreceive=enable
```

```
netsh interface ipv4 set interface "Windows loopback interface name" weakhostsend=enable
```

リナックス

- 永久ループバックインターフェイスを追加する
- etc/sysconfig/network-scripts" を編集する。

```
ifcfg-lo:1
```

```
DEVICE=lo:1
```

```
IPADDR=x.x.x.x
```

```
NETMASK=255.255.255.255
```

```
BROADCAST=x.x.x.x
```

```
ONBOOT=はい
```

- etc/sysctl.conf" を編集する。

```
net.ipv4.conf.all.arp_ignore = 1
```

```
net.ipv4.conf.eth0.arp_ignore = 1
```

```
net.ipv4.conf.eht1.arp_ignore = 1
```

```
net.ipv4.conf.all.arp_announce = 2
```

```
net.ipv4.conf.eth0.arp_announce = 2
```

```
net.ipv4.conf.eth1.arp_announce = 2
```

- sysctl - p" を実行する。

リアルサーバーの変更 - ゲートウェイモード

ゲートウェイモードでは、すべてのトラフィックを ADC 経由でルーティングすることができます。これにより、コンテンツサーバーから発信されたトラフィックは、ADC ユニットのインターフェイスを介して他のネットワークにルーティングされます。デバイスをコンテンツサーバーのゲートウェイデバイスとして使用するには、マルチインターフェースモードで実行する必要があります。

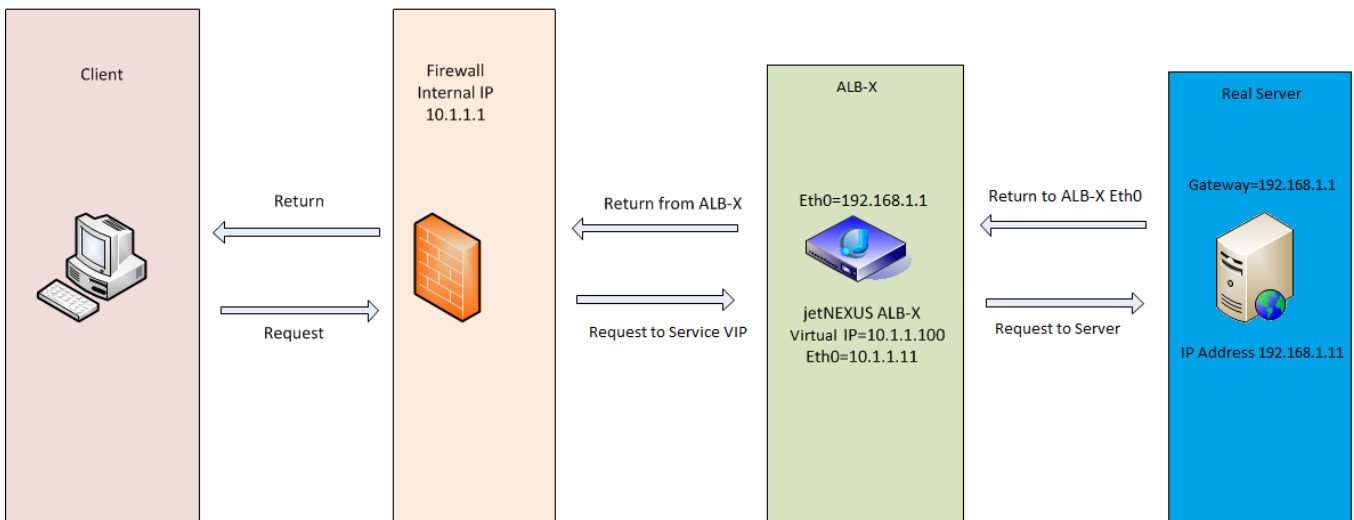
仕組み

- クライアントは EdgeADC にリクエストを送信する。
- EdgeADC がリクエストを受信
- コンテンツサーバーへのリクエスト送信
- EdgeADC に返信
- ADC はレスポンスをクライアントにルーティングする

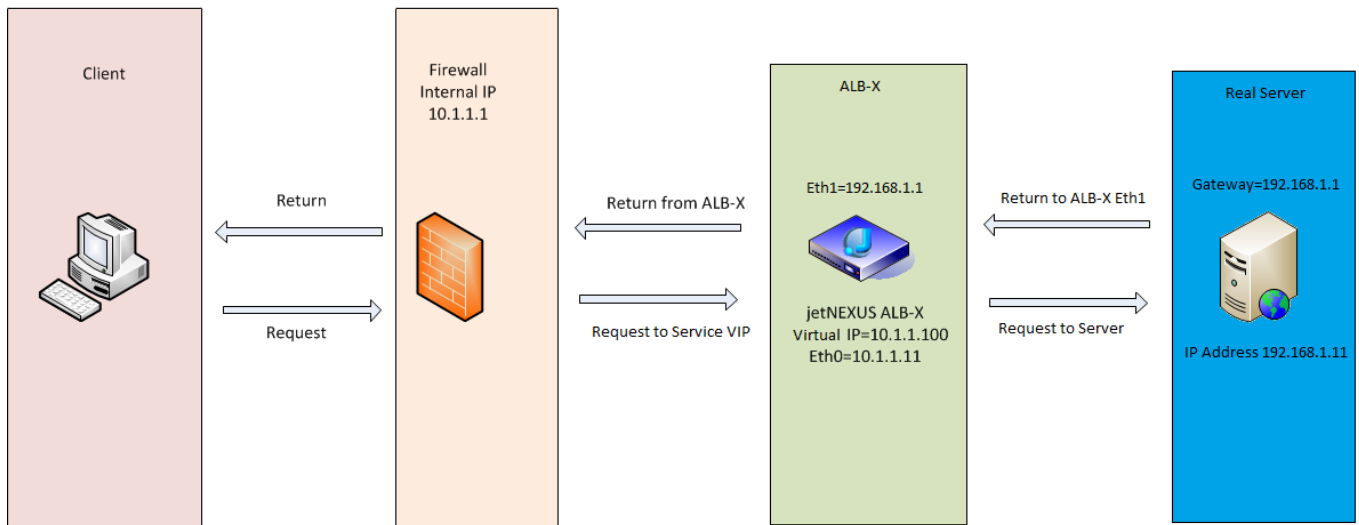
必要なコンテンツサーバーの構成

- シングルアームモード - 1つのインターフェイスを使用しますが、サービス VIP とリアルサーバーは異なるサブネット上にある必要があります。
- デュアルアームモード - 2つのインターフェイスを使用しますが、サービス VIP と実サーバーは異なるサブネット上にある必要があります。
- シングルアームとデュアルアームのそれぞれのケースで、リアルサーバーは、関連するサブネット上の ADC インターフェイスアドレスにデフォルトゲートウェイを設定する必要があります。

シングルアームの例



デュアルアームの例

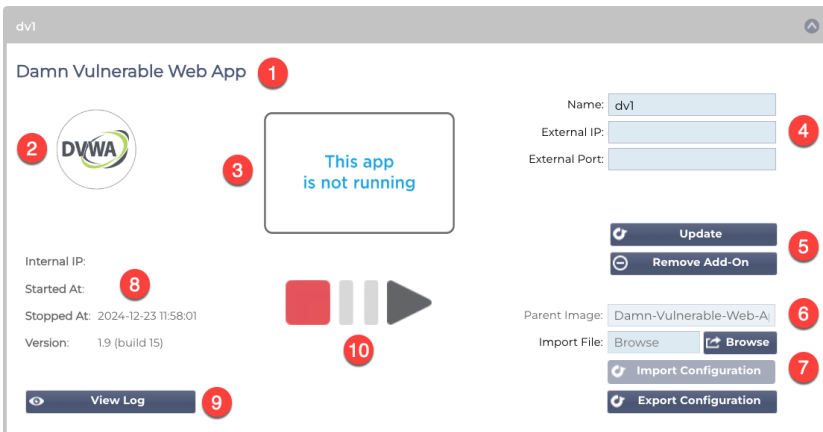


図書館

アドオン

アドオンは、コンテナとしてロードされ、ADC 内で隔離されたモードで実行されるアプリケーションである。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る。

アプリは、このガイドで説明されているように、Apps ページを使用して Add-Ons セクションにデプロイされます。デプロイされると、App はこのように表示されます。



上の画像からわかるように、ハイライトされている要素がいくつかある。

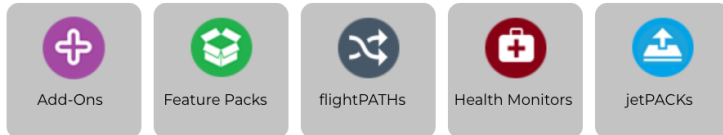
項目	説明
1	アプリ名
2	アプリのアイコン
3	アプリ実行中の表示。アプリが実行中の場合、画面のミニチュアが表示されます。
4	アクセスの詳細 名前 ：これは仮想サービスセクション内からアプリを参照するために使用する内部名です。IP アドレスを使用してアプリを参照することはできません。英数字のみで、スペースは使用できません。 External IP (外部 IP) ：アプリに提供する必要がある IP アドレスです。これはネットワークサブネットの一部になります。 External Port (外部ポート) ：これは重要なフィールドです。アプリへのアクセスに使用するポートを指定する必要があります。アプリの外部のトラフィックがアクセスする場合、以下の表記で指定する必要があります：53/tcp または 53/udp。これに加えて、アプリの UI ポートを指定する必要があります。これらは各アプリのフィールドツールチップに表示される。
5	更新ボタン：5 で指定した詳細を入力したら、このボタンをクリックして入力を確認し、アプリを設定します。 Remove Add-On (アドオンの削除) ボタンは、Apps (アプリ) セクションから削除するために使用します。アプリを削除するには、削除を試みる前に、アプリへのすべての参照も削除されていることを確認してください。
6	親画像は情報フィールドであり、ユーザーの観点からは使用されない。
7	設定のインポートとエクスポートは、設定のバックアップを保持するために重要です。インポートおよびエクスポート機能を実行するには、これを使用します。
8	Run Details は、Internal API IP アドレス、開始・停止時間、アプリのバージョン番号に関する情報を提供する。
9	このボタンをクリックすると、ログをダウンロードして表示することができます。これは主にサポートチケットを開く必要がある場合に使用されます。
10	アプリの操作はこれらのボタンで行う。赤=停止、金=一時停止、緑=走行中です。

アプリ

Apps（アプリ）セクションには、ADC で使用可能なアプリを扱ういくつかのサブセクションがあります。これらは、フィルター、ダウンロード済みアプリ、購入済みアプリです。

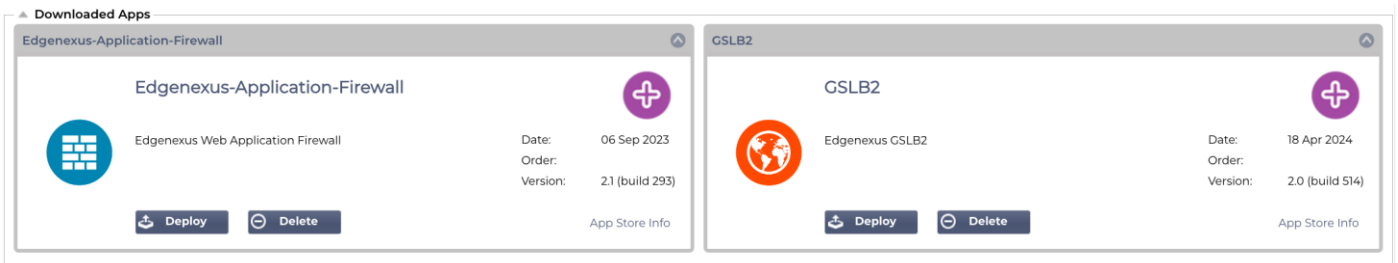
フィルター

Click icons to toggle groups of apps



フィルターでは、アプリ/ツールをタイプ別に絞り込むことができます。

ダウンロードされたアプリ

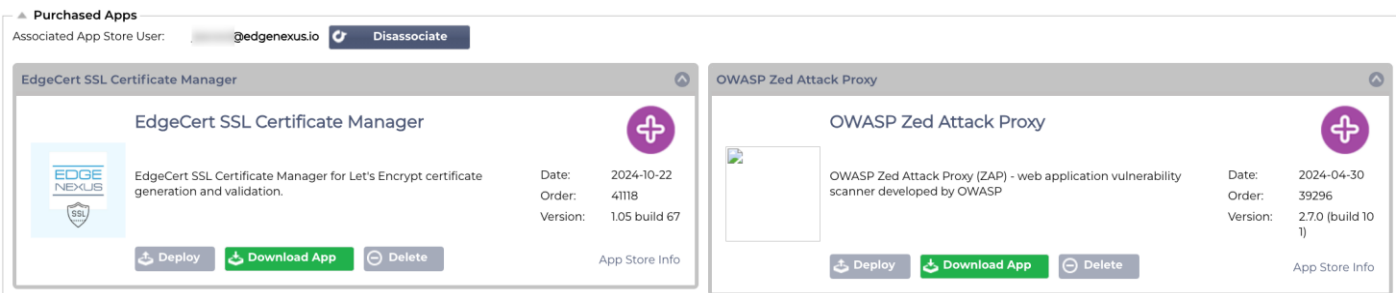


このセクションには、ADC にダウンロードされたアプリが含まれます。ローカルデスクトップにダウンロードし、その後 ADC にアップロードした場合も、内蔵の App Store ポータル経由でダウンロードした場合もあります。

各アプリには、2つのボタンと、バージョン番号とリリース日を示すデータが備わっている。

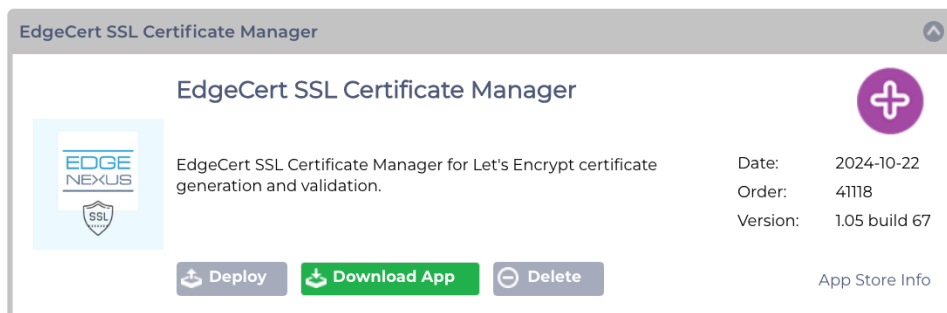
Deploy ボタンはアプリを保護されたコンテナとしてデプロイし、Delete ボタンは ADC 内からアプリを削除します。

購入アプリ



最初に注目するのは、Associated App Store User（関連する App Store ユーザー）とその関連ボタンです。ADC が App Store に関連付けられるように、App Store の認証情報を使用してログインする必要があります。この下に、アカウントに関連付けられている App が表示されます。

App Store に直接、または内蔵ポータルからログインすると、App を購入することができます。購入したアプリはこのセクションに表示され、ADC にアップロードして配備することができます。



各アプリにはいくつかのボタンがある : **Deploy**、**Download App**、**Delete** です。これに加えて、右側に **App Store Info** リンクがあり、関連する **App Store** ページに移動し、アドオンの情報を表示します。

デプロイ

Add-Ons 内の **Apps** セクションには、購入、ダウンロード、デプロイした **Apps** の詳細が表示されます。デプロイされると、**App** は **Downloaded** セクションに表示されます。

アプリをダウンロード

このアプリは、このボタンをクリックして **App Store** からダウンロードできます。

削除

ダウンロードしたアプリを削除したい場合。

認証

Library> Authentication ページでは、認証サーバーを設定し、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

サービスに認証を適用するには、最低限以下の手順を実行してください。

1. 認証サーバーを作成する。
2. 認証サーバーを使用する認証ルールを作成する。
3. 認証ルールを使用する flightPATH ルールを作成する。
4. サービスに flightPATH ルールを適用する

認証サーバー

認証方法を設定するには、まず認証サーバーを設定しなければならない。

最初の段階は、必要な認証方法を選択することである。

- Add Server をクリックする。
- ドロップダウンメニューからメソッドを選択します。

▲ Authentication Servers

⊕ Add Server ⊖ Remove Server

Method: ←

⊕ Update ⊖ Cancel

Name	Description	Method	Domain	Server Address

「認証サーバー」機能は動的であり、選択した認証方法に必要なフィールドのみが表示されます。

- サーバーへの適切な接続を確保するため、フィールドに正確に入力してください。

LDAP、LDAP-MD5、LSAPS、LDAPS-MD5、Radius、SAML 用オプション

▲ Authentication Servers

⊕ Add Server ⊖ Remove Server

Method:

Name:

Server Address:

Port:

Domain:

Login Format:

Description:

Search Base:

Search Condition:

Search User:

Password:

⊕ Update ⊖ Cancel

Name	Description	Method	Domain	Server Address

オプション

説明

方法	<p>認証方法を選択する</p> <p>LDAP - 基本的な LDAP で、ユーザー名とパスワードは平文で LDAP サーバーに送られる。</p> <p>LDAP-MD5 - 基本的な LDAP で、ユーザー名は平文、パスワードはセキュリティを高めるために MD5 ハッシュ化されています。</p> <p>LDAPS - 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平文で送信する。</p> <p>LDAPS-MD5 - LDAP over SSL。パスワードは、ADC と LDAP サーバー間の暗号化されたトンネル内でセキュリティを強化するために MD5 ハッシュ化されます。</p>
名称	サーバーを識別するために名前を付けます - この名前はあらゆるルールで使用されます。
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を追加する。
ポート	LDAP と LDAPS のポートは、デフォルトで 389 と 636 に設定されている。 ラディウスの場合、ポートは通常 1812。 SAML の場合、ポートは ADC で設定される。
ドメイン	LDAP サーバーのドメイン名を追加します。
ログイン形式	<p>必要なログイン形式を使用してください。</p> <p>ユーザー名 - この形式を選択すると、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とドメインの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。</p> <p>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： <i>mycompany=jdoe OR jdoe@mycompany</i>。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。空白 - ADC は、ユーザが入力したものをすべて受け入れ、認証サーバに送信する。このオプションは、MD5 を使用する場合に使用される。</p>
説明	説明を加える
検索ベース	この値は、LDAP データベースにおける検索の開始点となる。 例 <i>dc=mycompany,dc=local</i>
検索条件	検索条件は RFC4515 に準拠しなければならない。例 (MemberOf=CN=電話 VPN,CN=Users,DC=mycompany,DC=local)。
ユーザー検索	ディレクトリサーバー内でドメイン管理ユーザーを検索する。
パスワード	ドメイン管理ユーザーのパスワード。
デッドタイム	非アクティブなサーバーが再びアクティブとしてマークされるまでの時間

SAML 認証のオプション

重要： SAML 経由の認証を設定する場合、Entra ID 認証用の Enterprise App を作成する必要がある。この手順については、Microsoft EntraでのEntra ID認証アプリケーションのセットアップ

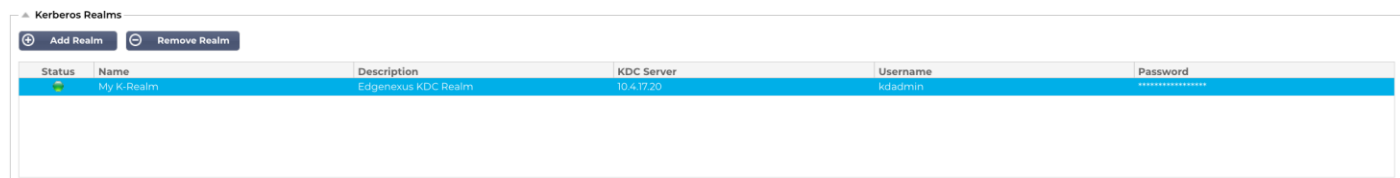
The screenshot displays the 'Authentication Servers' configuration interface. At the top, there are 'Add Server' and 'Remove Server' buttons. The main form is for configuring a SAML server. It includes a 'Method' dropdown set to 'SAML', a 'Name' text field, and a 'Description' text field. Under the 'Identity Provider' section, there is a checkbox for 'IdP Certificate match' and several text fields for 'IdP Entity ID', 'IdP SSO URL', 'IdP Logoff URL', and 'IdP Certificate'. The 'Server Provider' section includes a text field for 'SP Entity ID', a dropdown for 'SP Signing Certificate', and a dropdown for 'SP Session Timeout' set to '900'. At the bottom of the form are 'Update' and 'Cancel' buttons. Below the form is a table with the following columns: Name, Description, Method, Domain, and Server Address. The table is currently empty.

オプション	説明
方法	<p>認証方法を選択する</p> <p>LDAP - 基本的な LDAP で、ユーザー名とパスワードは平文で LDAP サーバーに送られる。</p> <p>LDAP-MD5 - 基本的な LDAP で、ユーザー名は平文、パスワードはセキュリティを高めるために MD5 ハッシュ化されています。</p> <p>LDAPS - 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平文で送信する。</p> <p>LDAPS-MD5 - LDAP over SSL。パスワードは、ADC と LDAP サーバー間の暗号化されたトンネル内でセキュリティを強化するために MD5 ハッシュ化されます。</p>
名称	サーバーを識別するために名前を付けます - この名前はあらゆるルールで使用されます。
アイデンティティ・プロバイダー	
IdP 証明書的一致	IdP Certificate Match とは、SAML アサーションに署名するために ID プロバイダ (IdP) が使用する デジタル証明書が、サービス・プロバイダ (SP) が信頼する証明書と一致することを検証するプロセスのことである。この検証により、IdP が正当であり、IdP が送信するアサーションが真正かつ変更されていないことが保証される。SP は通常、IdP の証明書をメタデータに格納し、SAML アサーションに埋め込まれた証明書と格納された証明書とを比較して一致を判断する。
IdP エンティティ ID	SAML IdP エンティティ ID は、SAML (Security Assertion Markup Language) エコシステム内の ID プロバイダ (IdP) の確定アドレスとして機能するグローバルに一意的な識別子である。この識別子は、通常 URL または URI であり、SAML ベースの認証および認可プロセスに関与する他のエンティティから IdP を一意に区別する。これは、信頼を確立し、IdP、サービスプロバイダ (SP)、およびユーザー間の安全な通信を促進する上で重要な役割を果たす。
IdP SSO URL	IdP SSO URL (Single Sign-On URL の略) は、ID プロバイダ (IdP) が提供する特定のエンドポイント URL であり、シングルサインオン (SSO) セッションを開始するための認証ゲートウェイとして機能する。ユーザをこの URL にリダイレクトすると、IdP は認証情報を使用して認証するようユーザに促し、認証に成功すると、ユーザの ID 情報を含むアサーションとともにユーザをサービス・プロバイダ (SP) にリダイレクトする。このアサーションは SP によって検証され、ユーザは再認証することなく SP のリソースにアクセスできるようになる。
IdP ログオフ URL	SAML IdP ログオフ URL は、シングルサインオン (SSO) セッションのログアウトプロセスを開始および管理する ID プロバイダ (IdP) の特定のエンドポイントである。ユーザがアプリケーションでログアウトボタンをクリックすると、アプリケーションはユーザを IdP のログオフ URL にリダイレクトする。その後、IdP は、SSO 認証に関連するすべての依頼当事者上のユーザのセッションを無効にし、アプリケーションにログアウト応答を返送して、接続されているすべてのアプリケーションからユーザを効果的にログアウトする。
IdP 証明書	<p>SAML IdP 証明書は、SAML (Security Assertion Markup Language) 認証プロトコルに参加する ID プロバイダ (IdP) に対して、信頼される機関が発行する X.509 デジタル証明書である。この証明書は、IdP の身元を検証し、IdP とサービス・プロバイダ (SP) 間で交換される SAML メッセージの完全性と機密性を認証する安全な手段として機能する。</p> <p>ドロップダウンメニューを使用して、ADC にインストールする IdP 証明書を選択できます。</p>
説明	定義の説明。
ユーザー検索	ドメイン管理ユーザーを検索する。
パスワード	admin ユーザーのパスワードを指定する。

サーバー・プロバイダー	
SP エンティティ ID	SP エンティティ ID は、SAML プロトコルのコンテキストにおいて、特定のサービス・プロバイダ (SP) のグローバル・アドレスとして機能する一意の識別子である。これは SP を識別する標準化された方法であり、通常は URL またはその他の URI で、SP の SAML メタデータを特定する。
SP 署名証明書	SAML SP 署名証明書は、サービス・プロバイダ (SP) が SAML 応答に署名するために使用する X.509 証明書であり、シングル・サイン・オン (SSO) 認証中に SP と ID プロバイダ (IdP) 間で交換されるメッセージの真正性と完全性を保証する。SP はその秘密鍵を使用して応答に署名し、IdP は証明書に関連付けられた公開鍵を使用して署名を検証し、送信者の身元とメッセージの内容が改ざんされていないことを確認する。
SP セッションタイムアウト	SP セッション・タイムアウトとは、アイデンティティ・プロバイダ (IdP) を介したシングル・サインオン (SSO) に成功した後、サービス・プロバイダ (SP) 側でユーザーの認証セッションが有効とみなされる最大時間のことである。この指定時間を過ぎると、SP はセッションを終了し、保護されたリソースへのアクセスを回復するためにユーザーに再認証を要求する。このメカニズムにより、不正アクセスを防止し、ユーザー・セッションが長時間アイドル状態にならないようにすることができる。

KDC レルム

KDC レルムとは、Kerberos 認証プロトコル内のコンフィギュレーションを指し、各レルムは基本的に、単一の鍵配布センター (KDC) の下で運用されるドメインまたはネットワークである。この設定は、同じマスター KDC の下で管理されるシステムのグループを定義し、ネットワーク全体で安全な認証とチケット付与メカニズムを容易にする。レルムは階層的または非階層的であることができ、レルム間の安全な認証のためにレルム間で信頼関係を確立することができる。



上の画像に示すように、ADC で提供されるユーザー・インターフェースでは、Kerberos レルムを定義できる。この情報は、認証ルール内で使用できる。

認証ルール

次の段階では、サーバ定義で使用する認証ルールを作成する。

フィールド	説明
名称	認証ルールに適切な名前を追加する。
説明	適切な説明を加える。
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、これは空白のままにしておかなければならない。
認証サーバー	これは、あなたが設定したサーバーを含むドロップダウンボックスです。
クライアント認証 :	ニーズに応じて適切な値を選択する : Basic (401) - この方法は、標準的な 401 認証方法を使用します。 フォーム - ADC のデフォルトフォームをユーザーに表示します。フォーム内にメッセージを追加することができます。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	適切な値を選んでください。 なし - サーバ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 Basic 認証 (401) が有効になっている場合は、 BASIC を選択します。 NTLM - サーバで NTLM 認証が有効になっている場合は、 NTLM を選択する。
フォーム	適切な値を選ぶ デフォルト - このオプションを選択すると、ADC はその内蔵フォームを使用する。 カスタム - あなたがデザインしたフォームを追加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します。タイムアウトを過ぎると、ユーザーは再度認証を要求されます。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あることに注意してください。

ユーザーにシングルサインオンを提供する場合は、「Root Domain」フィールドにドメインを入力します。この例では、**mycompany.com** です。これで、**edgenexus.io** をルートドメインとして使用する複数のサービスを持つことができ、ログインは一度だけで済みます。以下のサービスを考えてみましょう :

- [SharePoint.mycompany.com](#)
- [usercentral.mycompany.com](#)
- [App Store.mycompany.com](#)

これらのサービスは 1 つの VIP に常駐させることも、3 つの VIP に分散させることもできる。**usercentral.mycompany.com** に初めてアクセスするユーザーには、使用する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る。同じユーザーが **App Store.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、この非アクティブ期間に達すると、強制的に認証されます。

フォーム

▲ **Forms**

Form Name:

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でほとんどの目的には十分ですが、企業独自のアイデンティティをユーザーに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が入力する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** または **HTML** 形式でなければなりません。

オプション	説明
名称	フォーム名 = loginform アクション = %JNURL メソッド = POST
ユーザー名	構文 : name = "JNUSER"
パスワード	name="JNPASS"
任意のメッセージ 1 :	JNMESSAGE
オプションのメッセージ 2 :	jnauthmessage%。
画像	画像を追加したい場合は、 Base64 エンコーディングを使っ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

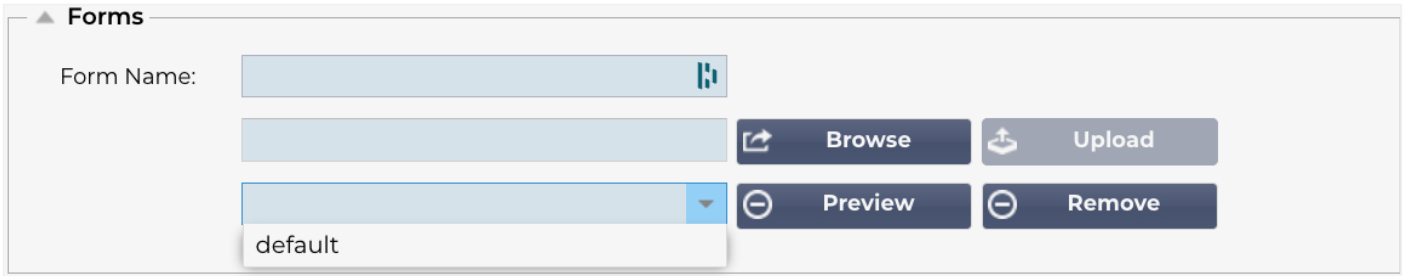
```
<HTML>
<ヘッド
<タイトル>認証フォームのサンプル</タイトル
</head>
<BODY
JNMESSAGE%<br>。
<form name="loginform" action="%JNURL%" method="post"> USER: <input type="text" name="JNUSER" size="20" value=""></br>
PASS: <input type="password" name="JNPASS" size="20" value=""></br>。
<input type="submit" name="submit" value="OK">。
</form>
</BODY>
</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. 現地でフォームを探す
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



▲ **Forms**

Form Name: 

 **Browse**  **Upload**

 **Preview**  **Remove**

default

アップロードした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。また、このセクションを使用して、不要になったフォームを削除することもできます

注意 : AdGuard などのクッキーフィルタリング製品を使用すると、**404** エラーメッセージが表示されることがあります。これを防ぐには、**ADC** の IP アドレスをホワイトリストに登録します。

キャッシュ

ADCはその内部メモリ内にデータをキャッシュすることができ、ウェブ・サービスの配信を強化します。この機能を管理する設定は、このセクションで提供されます。

▲ Global Cache Settings

Maximum Cache Size (MB):	50			
Desired Cache Size (MB):	30			
Default Caching Time (D/HH:MM):	1	/	00:00	
Cachable HTTP Response Codes:	200 203 301 304 410			
Cache Checking Timer (D/HH:MM):	0	/	03:00	
Cache-Fill Count:	20			

Check Cache
Force a check on the cache size

Clear Cache
Remove all items from the cache

Update

グローバルキャッシュ設定

最大キャッシュサイズ (MB)

この値は、キャッシュが消費できる最大 RAM を決定します。ADC キャッシュは、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、ストレージ媒体にも定期的にフラッシュされるメモリ内キャッシュです。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・フットプリント（ディスク・スペースではなく）に収まる必要があります、利用可能なメモリの半分以下である必要があることを意味します。

希望キャッシュサイズ (MB)

この値は、キャッシュを切り詰める最適な RAM を示します。最大キャッシュ・サイズがキャッシュの絶対的な上限を示すのに対して、希望キャッシュ・サイズは、キャッシュ・サイズの自動チェックまたは手動チェックが行われるたびに、キャッシュが達成しようと試みる最適なサイズとして意図されています。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する。繰り返しになりますが、デフォルト値（30MB）を受け入れ、「モニター -> 統計」でキャッシュのサイズを定期的に確認し、適切なサイズを設定する方が効果的な場合があります。

デフォルトのキャッシュ時間 (D/HH:MM)

ここに入力された値は、明示的な有効期限値のないコンテンツの寿命を表す。デフォルトのキャッシュ時間は、"no-store" ディレクティブやトラフィックヘッダに明示的な有効期限を持たないコンテンツが保存される期間です。

したがって、"1/01:01"（デフォルトは 1/00:00）という入力、ADC が 1 日、"01:00" が 1 時間、"00:01" が 1 分のコンテンツを保持することを意味する。

キャッシュ可能な HTTP レスポンスコード

キャッシュされるデータセットのひとつに HTTP レスポンスがある。キャッシュされる HTTP レスポンス・コードは以下の通り：

- 200 - HTTP リクエストが成功した場合の標準レスポンス

- 203 - ヘッダーは確定的なものではなく、ローカルまたはサードパーティーのコピーから収集したものである。
- 301 - リクエストされたリソースに新しい永続的な URL が割り当てられました。
- 304 - 直近のリクエストから変更されていないため、代わりに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タイマー (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。

キャッシュファイル回数

この設定は、一定数の 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

このセクションでは、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：

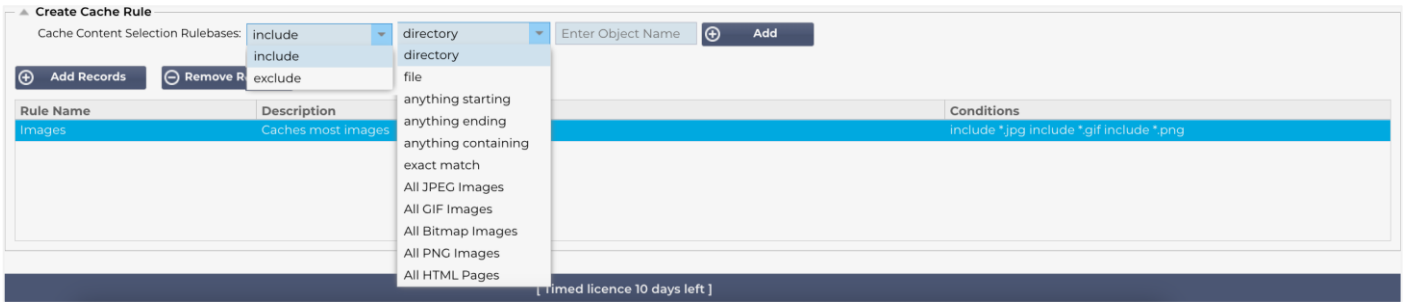
- **Add Records** ボタンでドメインを手動で追加する。完全修飾ドメイン名またはドット付き 10 進数表記の IP アドレスを使用する必要があります。例 **www.mycompany.com** または **192.168.3.1:80**
- ドロップダウンの矢印をクリックし、リストからドメインを選択します。
- このリストは、トラフィックが仮想サービスを通して、仮想サービスにキャッシュ戦略が適用されている限り表示されます。
- キャッシュ・ルールを選択するには、キャッシュ・ルールベース列をダブルクリックし、リストから選択します。

キャッシュ・ルールの作成

このセクションでは、ドメインに適用できる複数の異なるキャッシュルールを作成できます：

- レコードの追加をクリックし、ルールに名前と説明を付けます。
- 手動で条件を入力するか、条件の追加を使用します。

選択ルールベースを使って条件を追加する：



- Include または Exclude を選択します。
- すべての JPEG 画像など、選択基準を選択します。
- 追加マークをクリックしてください。
- 条件に「*.jpg を含む」が追加されているのがわかるだろう。
- さらに条件を追加することもできる。手動で行う場合は、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、ルールは同じ行に表示されます。

フライトパス

flightPATH は ADC に組み込まれたトラフィック管理技術で、HTTP と HTTPS のトラフィックをリアルタイムで検査し、条件に基づいてアクションを実行できる。

flightPATH 規則を使用するには、Real Servers セクションの flightPATH タブを使用して仮想サービスに適用する必要があります。

フライトパスのルールは 4 つの要素で構成される：

1. Details では、flightPATH 名と接続先のサービスを定義します。
2. ルールをトリガーさせる条件を定義することができる。
3. アクション内で使用できる変数を定義できる評価。
4. 条件が満たされたときに何が起こるべきかを管理するためのアクション。

詳細

flightPATH Name	Applied To VS	Description
AGFA-Header-Check-Server-1	Not in use	Redirection to server A101794
AGFA-Header-Check-Server-2	Not in use	Redirection to Server A101795
AGFA-Header-Check-Server-3	Not in use	Redirection to Server A101796
Block China	Not in use	
Block USA	Not in use	
Filter IPs	Not in use	

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。このセクションから新しい flightPATH ルールを追加したり、定義されたルールを削除することができます。

新しい flightPATH ルールを追加する

flightPATH Name	Applied To VS	Description
AGFA-Header-Check-Server-1	Not in use	Redirection to server A101794
AGFA-Header-Check-Server-2	Not in use	Redirection to Server A101795
AGFA-Header-Check-Server-3	Not in use	Redirection to Server A101796
Block China	Not in use	
Block USA	Not in use	
Filter IPs		Blocks IPs from a list

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	読みやすくするために提供される説明を表す値。

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します。
4. ルールがサービスに適用されると、Applied To 欄に IP アドレスとポート値が自動入力されます。

5. 更新ボタンを押して変更を保存するのをお忘れなく。もし間違えた場合は、キャンセルを押して前の状態に戻してください。

コンディション

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** ベースで動作するため、アクションがトリガーされる条件を設定できます。**OR** 条件を使用する場合は、追加の flightPATH ルールを作成し、正しい順序で VIP に適用します。

The screenshot shows a 'Condition' configuration window with a table containing one row:

Condition	Match	Sense	Check	Value
Path		Does	Match RegEx	\.htm\$

Check フィールドで Match RegEx を選択し、Value フィールドで RegEx 値を選択することで、RegEx を使用することもできます。RegEx 評価を含めることで、flightPATH の機能が飛躍的に向上します。

新しい flightPATH 条件の作成

The screenshot shows the 'Condition' configuration window with two rows. The second row is being edited:

Condition	Match	Sense	Check	Value
Path		Does	Match RegEx	\.htm\$
Host	Type a new Match	Does	Contain	mycompany.com

Buttons for 'Update' and 'Cancel' are visible below the table.

まず、条件欄から値を選択する必要がある。

私たちは、ドロップダウン内のいくつかの条件を提供し、予測されるすべてのシナリオをカバーしています。新しいコンディションが追加された場合は、Jetpack のアップデートで利用できるようになります。

選択肢は以下の通り：

コンディション	説明	例
<form>	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 "フォームの長さが 0 でない"
ゲオ所在地	送信元 IP アドレスを ISO 3166 Country Codes と比較する。	ゲオの所在地が GB である、またはゲオの所在地がドイツである
ホスト	URL から抽出されたホスト	www.mywebsite.com または 192.168.1.1
言語	言語 HTTP ヘッダーから抽出された言語	この条件は、言語のリストをドロップダウンメニューに表示します。
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	アップストリームプロキシが 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できる。 は 10.1.2.0 /24 サブネット 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

ポスト	POST リクエストメソッド	ウェブサイトにアップロードされるデータのチェック
クエリー	クエリーの名前と値。クエリー名または値も受け取ることができる。	「Best=jetNEXUS" マッチが Best で値が edgeNEXUS の場合
クエリー文字列	文字以降のクエリー文字列全体	
リクエストクッキー	クライアントが要求したクッキーの名前	MS-WSMAN=afYfn1CDqqCDqUD: :
リクエスト・ヘッダ	任意の HTTP ヘッダー	Referrer、User-Agent、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
回答本文	レスポンス・ボディのユーザー定義文字列	サーバーアップ
レスポンスコード	レスポンスの HTTP コード	200 OK, 304 Not Modified
レスポンス・クッキー	サーバーから送信されるクッキーの名前。	MS-WSMAN=afYfn1CDqqCDqUD: :
レスポンス・ヘッダ	任意の HTTP ヘッダー	Referrer、User-Agent、From、Date
レスポンス・バージョン	サーバーが送信した 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 IP アドレスのいずれか	クライアント IP、プロキシ IP、ファイアウォール IP。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 なのでエスケープする必要があります。例 10.1.1.2.3 は 10.1.2.3

試合

Match フィールドは、ドロップダウンまたはテキスト値で、**Condition** フィールドの値によって定義可能である。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** の場合、**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：

マッチ	説明	例
受け入れる	許容されるコンテンツ・タイプ	アクセプト: text/plain
Accept-Encoding	使用可能なエンコーディング	Accept-Encoding: <compress gzip deflate sdch identity>.
受諾言語	対応可能な言語	受諾言語: ja-US
アクセプト・レンジ	このサーバーがサポートする部分コンテンツ範囲タイプ	許容範囲: バイト
認可	HTTP 認証の認証情報	認証ベーシック QWxhZGRpbjpvvcGVuIHhlc2FtZQ==

EdgeADC - 管理ガイド

チャージ・トゥ	要求された方法の適用にかかる費用の勘定情報を含む。	
コンテンツエンコーディング	使用されるエンコーディングのタイプ	コンテンツ・エンコーディング : gzip
コンテンツ長	オクテット (8 ビットバイト) 単位のレスポンスボディの長さ	コンテンツ長: 348
コンテンツタイプ	リクエスト本文の MIME タイプ (POST および PUT リクエストで使用される)	Content-Type: application/x-www-form-urlencoded
クッキー	Set-Cookie (下記) でサーバーが以前に送信した HTTP クッキー。	Cookie: \$Version=1; Skin=new ;
日付	メッセージが発信された日時	日付 = "日付" ":" HTTP 日付
イータグ	リソースの特定のバージョンを示す識別子で、メッセージダイジェストであることが多い。	ETag : "aed6bdb8e090cd1:0"
より	リクエストを行うユーザーのメールアドレス	From: user@example.com
変更後	コンテンツが変更されていない場合、304 Not Modified が返されるようにする。	更新日時: Sat, 29 Oct 1994 19:43:31 GMT
最終更新日	リクエストされたオブジェクトの最終更新日 (RFC 2822 形式)	最終更新日火曜日, 15 11 月 1994 12:45:26 GMT
プラグマ	実装 : 実装: リクエストと応答の連鎖のどこかで、様々な効果を持つ可能性のある 特定のヘッダー。	プラグマ : no-cache
紹介者	現在リクエストされているページへのリンクがたどられた前のウェブページのアドレス。	リファラー : HTTP://www.edgenexus.io
サーバー	サーバー名	サーバーApache/2.4.1 (Unix)
セットクッキー	HTTP クッキー	Set-Cookie : UserID=JohnDoe; Max-Age=3600; Version=1
ユーザーエージェント	ユーザーエージェントの文字列	ユーザーエージェント Mozilla/5.0 (互換性あり; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
可変	ダウンストリームのプロキシに、将来のリクエストヘッダをどのようにマッチさせるかを指示する。 キャッシュされたレスポンスが使用可能かどうかを決定する。 を決定します。	値を変更します : ユーザーエージェント
X-Powered-By	ウェブアプリケーションをサポートするテクノロジー (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のブール値フィールドで、Does か Doesn't のどちらかを選択する。

チェック

チェックフィールドでは、コンディションに対するチェック値を設定することができます。

選択肢は以下の通り：Contain、End、Equal、Exist、Have Length、Match RegEx、Match List、Start、Exceed Length。

チェック	説明	例
存在する	これは状態の詳細を気にするものではなく、ただそれが存在する／しないだけである。	ホスト >> 存在する
スタート	文字列は値	Path> Does> Start /secure>
終了	文字列の最後は値	Path> Does> End - .jpg
コンテイン	文字列は値を含む	リクエスト・ヘッダ> Accept> Does> Contain> image
イコール	文字列は値と等しい	ホスト> Does> Equal> www.edgenexus.io
長さがある	文字列の長さは	ホスト >> は長さがあるか> 16 www.edgenexus.io = TRUE www.edgenexus.com = FALSE
マッチ RegEx	Perl 互換の完全な正規表現を入力できます。	オリジン IP >> 正規表現と一致する
マッチリスト	値のリストと値をマッチさせることができる。これは、例えば特定の IP アドレスとマッチさせる必要がある場合に便利である。値はカンマ(,)またはピップ()で区切られる。	ソース IP> Does > Match List > 10.10.10.1、10.10.10.2、10.10.10.3 など
エクシード・レングス	値が指定された長さを超えているかどうかをチェックできる。	パス > ドーズ > 長さの超過 > 200

コンディションを追加する手順

新しい flightPATH 条件を追加するのはとても簡単です。例を上を示す。

1. コンディションエリア内の「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する。ここでは Host を例にとって説明する。フィールドに入力することもでき、ADC はドロップダウンに値を表示する。
3. センスを選ぶ。例えば
4. チェックを選択します。例えば
5. 値を選択します。例：mycompany.com

Condition	Match	Sense	Check	Value
Request Header	Does	Does	Contain	image
Host	Does	Does	Equal	www.imagepool.com

上記の例では、ルールが完了するためには、以下の 2 つの条件が両方とも真でなければならないことを示している。

- まず、リクエストされたオブジェクトが画像であるかどうかをチェックする。
- 2 つ目は、URL のホストが www.imagepool.com。

評価

定義可能な変数を追加できることは、魅力的な機能だ。他の ADC では、スクリプトまたはコマンド・ライン・オプションを使用し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。EdgeADC では、以下に示すように、使いやすい GUI を使用して任意の数の変数を定義できます。

flightPATH 変数定義は、4つのエントリーを作成する必要がある。

- Variable - 変数の名前です。
- ソース - 可能なソースポイントのドロップダウンリスト。
- 詳細 - ドロップダウンから値を選択するか、手入力する。
- 値 - 変数が保持する値で、英数字か、微調整のための RegEx を指定します。

組み込み変数：

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

アクション・セクションには、以下のどの変数も使用できます。

- sourceip\$ - リクエストの送信元 IP アドレス
- sourceport\$ - 使用されたソースポート。
- clientip\$ - クライアントの IP アドレス
- clientport\$ - クライアントが使用するポート
- host\$ - リクエストで指定されたホスト
- method\$ - 使用されるメソッド：GET、POST など。
- path\$ - リクエストで指定されたパス
- querystring\$ - リクエストで使用されるクエリストリング。
- version\$ - REQUEST に含まれる HTTP リクエストのバージョン(現時点では 1 と 1.1 のみ許可)。
- resp\$ - サーバからの応答。例：200OK、404 など。
- geolocation\$ - リクエストが発信された GEO ロケーション。

アクション	ターゲット
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。

説明する：

- 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 エラー・ページが表示される。
- 代わりに、ユーザーは元のホスト名にリダイレクトされるが、間違ったパスは 404.html に置き換えられる。
- Syslog に「154.3.22.14:3454 のクライアントが間違った.html ページをリクエストしました」というエントリーが追加される。

アクション

プロセスの次の段階は、flightPATH ルールと条件に関連するアクションを追加することである。

Action	Target	Data
Rewrite Path	\$path\$!	

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たい。

- 新規追加をクリックする
- 「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。
- Target フィールドに `$path$/myimages` と入力する。
- 更新をクリック

このアクションはパスに `/myimages` を追加するので、最終的な URL は次のようになる。

www.imagepool.com/myimages

アクション	説明	例
リクエストクッキーの追加	Target セクションに詳細なリクエストクッキーを、Data セクションに値を追加する。	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
リクエストヘッダーを追加	Data セクションに値を持つ Target タイプのリクエストヘッダーを追加する。	ターゲット= Accept Data= image/png
レスポンス・クッキーの追加	レスポンス・クッキーの詳細をターゲット・セクションに追加し、データ・セクションに値を追加する。	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
レスポンス・ヘッダーの追加	Target セクションに詳細なリクエストヘッダーを追加し、Data セクションに値を追加する。	Target= Cache-Control Data= max-age=8888888
ボディ 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)
ボディ交換が先	レスポンス・ボディを検索し、最初のインスタンスだけを置き換える	Target= http:// (検索文字列) Data= https:// (置換文字列)
ボディは最後に交換する	レスポンス・ボディを検索し、最後のインスタンスだけを置き換える	Target= http:// (検索文字列) Data= https:// (置換文字列)
ドロップ	これは接続を切断する	目標=該当なし データ=該当なし

電子メール	Email Events で設定したアドレスにメールを送信します。アドレスまたはメッセージとして変数を使用できます。	Target="flightPATHはこのイベントにEメールを送った" Data= N/A
ログイベント	これは、システムログにイベントを記録します。	Target="flightPATHがsyslogにこれを記録した" Data= N/A
リダイレクト 301	これは恒久的なリダイレクトを発行する。	目標= http://www.edgenexus.io データ= 該当なし
リダイレクト 302	これは一時的なリダイレクトを発行する。	目標= http://www.edgenexus.io データ= 該当なし
リクエストクッキーの削除	ターゲット」セクションで詳述したリクエストクッキーを削除する	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
リクエストヘッダの削除	ターゲットセクションで詳述されているリクエストヘッダを削除する	ターゲット=サーバー データ=N/A
レスポンスの削除	対象」セクションで詳述したレスポンスクッキーを削除するクッキー	ターゲット=jnAccel
レスポンスの削除	ターゲット」セクションの「ヘッダー」に詳述されているレスポンスヘッダーを削除する。	ターゲット= Etag データ= N/A
リクエスト・クッキーの置き換え	Target セクションのリクエストクッキーを Data セクションの値に置き換える。	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
リクエスト・ヘッダの置換	ターゲットのリクエストヘッダをデータ値で置き換える	ターゲット= 接続 データ= keep-alive
	Target セクションのレスポンス・クッキーを Data セクションの値で置き換える。	Target=jnAccel=afYfn1CDqqCDqCVii Date=MSWSMAN=afYfn1CDqqCDqCVii
リプレース・レスポンス	Target セクションのレスポンス・ヘッダを Data セクションのヘッダで置き換える。	対象=サーバー データ=セキュリティのため非公開

パスの書き換え	これにより、リクエストは条件に基づいて新しい URL にリダイレクトされる。	Target= /test/path/index.html\$querystring\$ Data= 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またはバーチャルサービスを選択する	Target=192.168.101:443 Data=N/A
使用	使用するサーバーまたは仮想サービスを選択する	ターゲット= 192.168.101:80 データ= 該当なし
クッキーの暗号化	クッキーを 3DES 暗号化し、base64 エンコードします。	Data= 暗号化のためのパスフレーズを入力します。

flightPATH ルールのシナリオ

ある顧客が e コマースサイトを持っており、ブラウザの最新バージョンによってクッキーがブロックされるという問題を抱えている。

顧客は問題を追跡し、根本的な原因が問題のクッキーの「セキュア」と「同じサイト」のタグ付けの欠如にあることを発見しました。

flightPATH がどのように役立つかを見てみよう。

- wp_woocommerce_session_97929973749972642' という名前のクッキーがあります。
- クッキーの名前は「wp_woocommerce_session_」で、e コマース・システムによって生成されたランダムな一意の ID 値は「97929973749972642」です。
- same-site」と「secure」のタグは空白のようで、それゆえクッキーはブラウザの新しいセキュリティ制限によってブロックされています。
- これを防ぐには、次のような flightPATH ルールを作ればいい。
- セッション ID の flightPATH ルール
 - コンディション
空白のまま
 - 評価 :
変数 = \$variable_1\$
ソース = レスポンスクッキー
詳細 = wp_woocommerce_session_*
 - アクション = レスポンスクッキーを置き換える
ターゲット = wp_woocommerce_session_*
データ = \$variable_1\$
- タグの flightPATH ルール
 - 条件
条件 = レスポンスクッキー
マッチ = woocommerce_cart_hash
センス = する

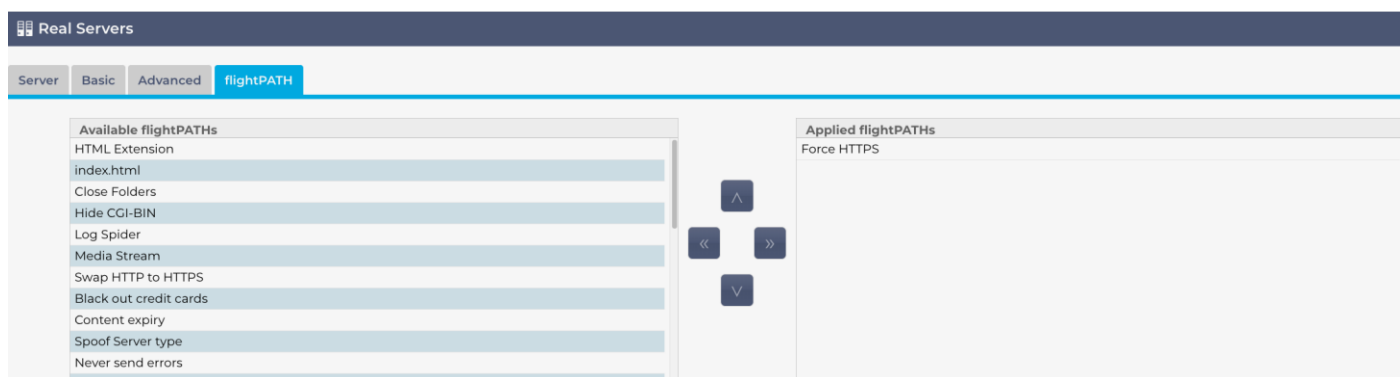
チェック = 存在する
 値 = 空白のまま

- 評価：
 - 変数 = `$variable_2$`
 - ソース = レスポンスクッキー
 - 詳細 = `woocommerce_cart_hash`
 - 値 = 空白のまま
- アクション
 - アクション = レスポンスクッキーを置き換える
 - ターゲット = `woocommerce_cart_hash`
 - データ = `$variable_2$,SameSite=None,Secure`

次に、ルールが必要な仮想サービスにルールを適用します。

flightPATH ルールの適用

フライトパスのルールの適用は、各 VIP/VS のフライトパスタブで行う。



- サービス] > [IP サービス] に移動し、flightPATH ルールを割り当てる VIP を選択します。
- 以下のようなリアルサーバーのリストが表示されます。
- flightPATH タブをクリック
- 設定した flightPATH ルールまたはサポートされている事前構築された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、自動的に適用される。

リアル・サーバー・モニター

Monitoring

Details

Add Monitor Remove

Name	Description	Monitoring Method	Applied To VS
200OK	Check home page for 200 OK	HTTP 200 OK	Not in use
DICOM	Monitor DICOM server	DICOM	Not in use
Check Page Returns	Check a page returns Success	HTTP Response	Not in use

Name: User Name:

Description: Password:

Monitoring Method: Threshold:

Page Location: SSL/TLS:

Required Content:

Update Cancel

実際のサーバーを監視することは、サーバーの問題を検出して対応し、バランスのとれた負荷分散を確保し、リソース利用を最適化し、重要なサービスに優先順位をつけ、ソフトウェアの脆弱性を特定して対処するために、負荷分散シナリオにおいて重要である。

ライブラリ > リアルサーバーモニター] ページではカスタムモニタリングを追加、表示、編集できます。これらはレイヤー 7 サーバーの「ヘルスチェック」で、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・モニターの種類

リアル・サーバー・モニターはいくつか用意されており、以下の表で説明している。もちろん、PERL を使って追加のモニターを書くこともできます。

モニタリング方法	説明	例
HTTP 200 OK	<p>リアル・サーバーに TCP 接続が行なわれる。接続が確立すると、Real Server に対して簡単な HTTP リクエストが送信される。レスポンスを受信すると、「200 OK」文字列があるかどうかチェックされる。この文字列が存在すれば、サーバーは稼働しているとみなされる。</p> <p>このモニターを使用すると、コンテンツを含むページ全体を取得することに注意してください。</p> <p>このモニタリング・メソッドは、HTTP と Accelerated HTTP サービス・タイプでのみ使用できる。しかし、HTTP サーバーでレイヤー 4 サービスタイプが使用されている場合、リアルサーバーで SSL が使用されていないか、「Content SSL」機能によって適切に処理されていれば、まだ使用できます。</p>	<p>リクエスト</p> <pre>GET / HTTP/1.1 Host: 192.168.159.200 受け入れる: /* 受諾言語: ja-gb ユーザーエージェント Edgenexus-ADC/4.0 接続キープアライブ キャッシュ制御: no-cache</pre> <p>応答</p> <pre>HTTP/1.1 200 OK コンテンツタイプ: text/html 最終更新日 Wed, 31 Jan 2018 15:08:18 GMT 受諾範囲: バイト ETag: "0dd3253a59ad31:0" サーバーマイクロソフト-IIS/10.0 日付火曜日, 13 7 月 2021 15:55:47 GMT コンテンツ長: 1364</pre> <pre><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"></pre>

		<pre><html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /> <タイトル>ジェットネクサス</タイトル> <style type="text/css">。 <!-- ボディ color:#FFFFFF ; ... </body> </html></pre>
HTTP 200 ヘッド	<p>PATH フィールドにチェックする場所を指定して、リアルサーバーに TCP 接続を行う。レスポンスの先頭部分がサーバーから取得され、内容は破棄される。レスポンスは 200 OK かどうかチェックされる。これが存在すれば、サーバーは稼働しているとみなされる。このモニターを使用すると、ヘッド部分のみを取得することに注意してください。このモニタリング・メソッドは、HTTP と Accelerated HTTP サービス・タイプでのみ使用できる。しかし、HTTP サーバーでレイヤー 4 サービスタイプが使用されている場合、リアルサーバーで SSL が使用されていないか、「Content SSL」機能によって適切に処理されていれば、まだ使用できます。</p>	<p>リクエスト ヘッド / http/1.1 ホスト : 192.168.159.200 受け入れる : /* 受諾言語: ja-gb ユーザーエージェント Edgenexus-ADC/4.0 接続キープアライブ キャッシュ制御: no-cache</p> <p>応答 HTTP/1.1 200 OK コンテンツ長 : 1364 コンテンツタイプ: text/html 最終更新日 Wed, 31 Jan 2018 15:08:18 GMT 許容範囲 : バイト ETag : "Odd3253a59ad31:0" サーバーマイクロソフト-IIS/10.0 日付火曜日, 13 7 月 2021 15 時 49 分 19 秒 GMT</p>
HTTP 200 オプション	<p>リアル・サーバーに TCP 接続を行い、オプション要求を行う。オプションが返され、200 OK の内容がチェックされる。200 OK のコンテンツが見つければ、サーバーは利用可能であると判断される。</p>	<p>リクエスト オプション / http/1.1 ホスト : 192.168.159.200 受け入れる : /* 受諾言語: ja-gb ユーザーエージェント Edgenexus-ADC/4.0 接続キープアライブ キャッシュ制御: no-cache</p> <p>応答 HTTP/1.1 200 OK 許可する : オプション、トレース、ゲット、ヘッド、ポスト サーバーマイクロソフト-IIS/10.0 公開 : オプション、トレース、ゲット、ヘッド、ポスト 日付火曜日, 13 7 月 2021 16 時 23 分 39 秒 GMT コンテンツ長: 0</p>
HTTP ヘッド	<p>HTTP ヘッド・モニターは、HTTP ストリームのヘッド部分にある特定の値をチェックすることができます。適切なフィールドに Path と Required Response を入力し、レスポンスでその値をチェックします。Required Response の値が Head に見つかった場合、サーバーは稼働しており、利用可能であるとみなされる。</p>	<p>リクエスト HEAD /ispagethere.htm HTTP/1.1 ホスト : 192.168.159.200 受け入れる : /* 受諾言語: ja-gb ユーザーエージェント Edgenexus-ADC/4.0 接続キープアライブ キャッシュ制御: no-cache</p>

	<p>また、ユーザー名とパスワードが必要な特別に保護されたページでも、これを使うことができる。こうすることで、モニターの結果を正確なもののみならずすることができる。</p> <p>例えば、/ispagethere.html を提供し、Path と Required Response フィールドに 200 OK を指定すると、サーバーが稼動しており、ページが利用可能で、リクエストに応答する場合、成功した結果が返されます。</p> <p>このモニタリング・メソッドは、HTTP と Accelerated HTTP サービス・タイプでのみ使用できる。しかし、HTTP サーバーでレイヤー 4 サービスタイプが使用されている場合、リアルサーバーで SSL が使用されていないか、「Content SSL」機能によって適切に処理されていれば、まだ使用できます。</p>	<p>応答 HTTP/1.1 200 OK コンテンツ長: 1364 コンテンツタイプ: text/html 最終更新日 Wed, 31 Jan 2018 15:08:18 GMT 許容範囲: バイト ETag : "Odd3253a59ad31:0" サーバーマイクロソフト-IIS/10.0 日付水曜日, 14 7 月 2021 08:28:18 GMT</p>
<p>HTTP オプション</p>	<p>HTTP オプション・モニターは、返されたオプション・データ内の特定の値をチェックすることができます。</p> <p>適切なフィールドに「パス」と「必須レスポンス」を入力し、レスポンスをチェックする。</p> <p>オプションデータに「必須レスポンス」が見つければ、サーバーは利用可能であり、稼動している。</p> <p>Required Response の値には、以下のいずれかを指定する: OPTIONS、TRACE、GET、HEAD、POST。</p> <p>例えば、/ispagethere.html を提供し、Path と Required Response フィールドに GET 値を指定すると、サーバーが稼動しており、ページが利用可能で、リクエストに応答する場合、成功した結果が返されます。</p> <p>このモニタリング・メソッドは、HTTP と Accelerated HTTP サービス・タイプでのみ使用できる。しかし、HTTP サーバーでレイヤー 4 サービスタイプが使用されている場合、リアルサーバーで SSL が使用されていないか、「Content SSL」機能によって適切に処理されていれば、まだ使用できます。</p>	<p>リクエスト オプション /ispagethere.htm HTTP/1.1 ホスト: 192.168.159.200 受け入れる: /* 受諾言語: ja-gb ユーザーエージェント Edgenexus-ADC/4.0 接続キープアライブ キャッシュ制御: no-cache</p> <p>応答 HTTP/1.1 200 OK 許可する: オプション、トレース、ゲット、ヘッド、ポスト サーバーマイクロソフト-IIS/10.0 公開: オプション、トレース、ゲット、ヘッド、ポスト 日付水曜日, 14 7 月 2021 09:47:27 GMT コンテンツ長: 0</p>
<p>HTTP レスポンス</p>	<p>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、前の例で説明したようにチェックされる。</p> <p>しかし、"200 OK"レスポンス・コードをチェックするのではなく、HTTP レスポンスのヘッダーにカスタム・テキスト・コンテンツがあるかどうかをチェックする。テキストは、完全なヘッダー、ヘッダーの一部、ページの一部からの行、あるいは単なる 1 語である。</p> <p>例えば、右図の例では、Path に /ispagethere.htm、Required Response に Microsoft-IIS を指定しています。</p>	<p>リクエスト GET /ispagethere.htm HTTP/1.1 ホスト: 192.168.159.200 受け入れる: /* 受諾言語: ja-gb ユーザーエージェント Edgenexus-ADC/4.0 接続キープアライブ キャッシュ制御: no-cache</p> <p>応答 HTTP/1.1 200 OK コンテンツタイプ: text/html 最終更新日 Wed, 31 Jan 2018 15:08:18 GMT 許容範囲: バイト ETag : "Odd3253a59ad31:0"</p>

	<p>テキストが見つければ、リアルサーバーは稼働しているとみなされる。</p> <p>このモニタリング・メソッドは、HTTP と Accelerated HTTP サービス・タイプでのみ使用できます。</p> <p>しかし、HTTP サーバーでレイヤー4のサービスタイプが使用されている場合、リアルサーバーでSSLが使用されていないか、「コンテンツSSL」機能によって適切に処理されていれば、レイヤー4のサービスタイプが使用される可能性がある。</p>	<p>サーバーマイクロソフト-IIS/10.0 日付水曜日, 14 7 月 2021 10:07:13 GMT コンテンツ長 : 1364</p> <pre><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /> <タイトル>ジェットネクサス</タイトル> <style type="text/css">. <!-- ボディ color:#FFFFFF ; ...</pre>
マルチポート TCP モニター	<p>この方法は、複数の異なるポートを指定できることを除けば、上記の方法と同じである。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る。</p>	<p>名前マルチポートモニター 説明複数のポートを監視する ページの場所該当なし 必要なコンテンツ 135,59534,59535</p>
TCP アウトオブバンド	<p>TCP アウト・オブ・バンド方式は、監視したいポートを必須コンテンツ欄に指定できる点を除けば、TCP コネクに似ている。このポートは通常、トラフィック・ポートとは異なり、サービスを結び付けたい場合に使用しません。</p>	<p>名前 TCP アウト・オブ・バンド 説明帯域外/トラフィックポートの監視 ページの場所該当なし 必須コンテンツ 555</p>
ディコム	<p>必須コンテンツ欄の "Source Calling" AE Title 値を使用して DICOM エコーを送信する。また、各サーバの Notes 欄で、"Destination Called" AE Title 値を設定することもできます。Notes カラムは、IP Services- の中にあります。 -仮想サービス--サーバーのページ。</p>	<p>名称 DICOM 説明 DICOM サービスの L7 ヘルスチェック モニタリング方法 DICOM ページの場所該当なし 必須コンテンツ AET バリユー</p>
LDAPS	<p>この新しい健全性チェックは、LDAP/AD サーバーの健全性と応答をチェックするために使用される。</p>	<p>名前 LDAPS 説明 LDAP/AD サーバのヘルスチェック 使用パラメータは以下の通り： ユーザー名 : cn=ユーザー名,cn=ユーザー,dc=ドメイン名,dc=ローカル パスワードドメインユーザーパスワード 内容物 200OK</p>
SNMP v2	<p>この監視方法では、サーバーの SNMP MIB 応答を使用して、サーバーの可用性ステータスをチェックすることができます。 Require Response の値には、コミュニティ名を含めるべきである。</p>	
DNS サーバーチェック	<p>DNS サーバーの負荷分散を行う場合、サーバーが DNS クエリに応答するかどうかを確認することは有益です。 モニターは以下のように使用できる：</p> <ul style="list-style-type: none"> Path フィールドは、クエリーする FQDN に使用する。例えば、www.edgenexus.io を照会したい場合、Path フィールドにこれを入力します。 これを空白にすると、モニターはデフォルトのルックアップを使用してクエリーを行います。 	

- **Required Response (必須レスポンス)** フィールドは空白のままにすることもでき、モニターはどのようなレスポンスも有効であるとみなす。そうでない場合は、**[Required Response]**フィールドに予想される IP を入力する。例えば、**101.10.10.100** である。クエリがこの値を返した場合、モニターは成功のフラグを立て、そうでなければ失敗のフラグを立てる。
成功の結果は、ロードバランシングしている DNS サーバーが稼働していることを示す。

リアル・サーバー・モニター」ページは 3 つのセクションに分かれています。

詳細

詳細」セクションは、新しいモニターを追加したり、不要なモニターを削除するために使用します。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。

Name	Description	Monitoring Method	Applied To VS
200OK	Check home page for 200 OK	HTTP 200 OK	Not in use
DICOM	Monitor DICOM server	DICOM	Not in use

Name: User Name:

 Description: Password:

 Monitoring Method: Threshold:

 Page Location:

 Required Content:

Update Cancel

名称

モニター名

説明

このモニターのテキストによる説明で、できるだけ説明的なものにすることを勧めます。

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。利用可能な選択肢は以下の通りです：

- HTTP 200 OK
- HTTP 200 ヘッド
- HTTP 200 オプション
- HTTP ヘッド
- HTTP オプション
- HTTP レスポンス
- マルチポート TCP モニター
- TCP アウトオブバンド
- ディコム
- SNMP v2
- DNS サーバーチェック
- LDAPS

ページ位置

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、Web サイトがホスト名にバインドされる絶対リンクを使用することもできます。

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る。ここで表される値は、選択されたモニタリング方法によって変化する。

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仮想サービスの IP / ポートが自動的に入力されます。仮想サービスで使用されたモニターは削除できません。

ユーザー

一部のカスタムモニターは、この値をパスワードフィールドとともに使用してリアルサーバーにログインすることができます。

パスワード

一部のカスタムモニターは、この値を「ユーザー」フィールドと共に使用してリアルサーバーにログインすることができます。

しきい値

Threshold (しきい値) 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。

SSL/TLS

このフィールドでは、SSL を使用するかどうかを強制することができます。設定は以下の通り：

- オン - SSL を強制します。
- オフ - SSL を無効にします。
- Auto - 現在の状態のままにします。

リアル・サーバー・モニターの例

Name	Description	Monitoring Me...	Page Location	Required Cont...	Applied to VS	User	Password	Threshold
Http Response	Check home pa...	HTTP Response		555	192.168.3.20:80			
DICOM	Monitor DICOM...	DICOM		does this conte...	Not in use			
Monitoring OWA	Exchange 2010...	HTTP Response	/owa/auth/logon...		Not in use			
Multi Port	Exchange 2010...	Multi port TCP ...	/owa/auth/logon...		Not in use			

アップロードモニター

ユーザーが独自のカスタム・モニターを作成したい場合が多々あると思いますが、このセクションではそれらを 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 スクリプトで記述され、拡張子は.pl です。

- 監視方法リストでモニターを識別できるように、モニターに名前を付けます。
- .pl ファイルをブラウズする
- 新しいモニターのアップロードをクリック
- 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・メソッド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する
- カスタムモニターの名前を選択する
- 削除をクリックする
- カスタムモニターは監視方法リストに表示されなくなります。

カスタムモニターPerl スクリプトの作成

注意: このセクションは、Perl の使用と記述の経験がある人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。この行を含めないと、スクリプトは見つかりません！

以下は必須項目である：

- #モニター名
- ストリクトを使う；
- 使用上の注意

Perl スクリプトは CHROOTED 環境で実行される。それらはしばしば WGET や CURL のような別のアプリケーションを呼び出します。SNI のような特定の機能のために、これらを更新する必要があることもある。

ダイナミック・バリュー

- `my $host = $_[0]; ### ホストの IP または名前(RS の詳細または OOB が使用されている場合)`
- `my $port = $_[1]; ### ホストポート(RS の詳細または OOB が使用されている場合)`
- `my $content = $_[2]; ### モニターの設定から必要な内容 (レスポンスに表示されなければならない内容)`
- `my $notes = $_[3]; ### IP サービスの RS の詳細からのメモ (各 RS モニターを一意にカスタマイズするためにこれを使用する)`

- my \$page = \$_[4]; ### モニター設定のページ位置
- my \$user = \$_[5]; ### モニター設定のユーザー名
- my \$password = \$_[6]; ### モニター設定のパスワード
- my \$threshold = \$_[7]; ### モニター設定のしきい値パラメーター
- my \$rsaddr = \$_[8]; ### RS IP (帯域外監視の場合は _[0] と異なる)
- my \$rsport = \$_[9]; ### RS ポート (帯域外モニタリングの場合は _[1] と異なる)
- my \$timeout = \$_[10]; ### IP Services > Real Server > Advanced > Monitoring Timeout からコンタクトタイムアウトを秒単位で監視する。

カスタム・ヘルスチェックには 2 つの結果がある。

- 成功
戻り値 1
成功メッセージを **Syslog** に出力する
リアルサーバをオンラインにする (**IN COUNT** が一致する場合)
- 失敗
戻り値 2
Syslog に「**Unsuccessful**」というメッセージを出力する。
リアルサーバをオフラインにする (**OUT Count** が一致する場合)

カスタムヘルスマニタの例

```
#モニター名 HTTPS_SNI
ストリクトを使う :
警告を使用する ;
# 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ます。
# このスクリプトには6つの値が渡される (下記参照) 。
# スクリプトは以下の値を返す。
# 1がテスト成功
テストが失敗した場合は# 2 サブモニター
{
私のシヨスト = $_[0]; ### ホストのIPまたは名前
マイ・スポーツ      = $_[1]; ### ホスト・ポート
My Scontent      = $_[2]; ### 探すコンテンツ (ウェブページとHTTPヘッダーの中)
my Snotes        = $_[3]; ### 仮想ホスト名
マイページ        = $_[4]; ### URLのホストアドレス以降の部分
私のスーザー      = $_[5]; ### ドメイン/ユーザー名 (オプション)
私のパスワード    = $_[6]; ### パスワード (オプション)
my $resolve ;
my $auth      =;
if ($port)
{
    resolve = "$notes:$port:$host" ;
}
さもなければ
    resolve = "$notes:$host" ;
```

```
}  
if ($user && $password) {  
    auth = "-u $user:$password :  
}  
my @lines = 'curl -s -i -retry 1 -max-time 1 -k -H "Host:$notes --resolve $resolve $auth HTTP://${notes}${page}.2>&1';  
if(join("@lines")=~/$content/)  
    {  
        print "HTTP://${notes}${page} looking for - $content - Health check successful. \n" ;  
        を返す(1) ;  
    }  
その他  
    {  
        print "HTTP://${notes}${page} looking for - $content - Health check failed. \n" ;  
        リターン(2)  
    }  
}  
モニター(@ARGV) :
```

注 :

カスタム監視 - グローバル変数の使用はできません。ローカル変数のみを使用 - 関数内部で定義された変数
RegEx の使用 - すべての正規表現は、Perl と互換性のある構文を使用しなければならない。

SSL証明書

SSLを使用して暗号化された接続を使用するサーバーでレイヤー7のロードバランシングを正常に使用するには、ADCがターゲットサーバーで使用されるSSL証明書を備えている必要があります。この要件は、データストリームを復号化、検査、管理し、ターゲットサーバーに送信する前に再暗号化できるようにするためである。

SSL証明書には、ADCが生成できる自己署名証明書から、信頼できるプロバイダーから入手できる従来の証明書（ワイルドカードを含む）まで、さまざまなものがある。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る。

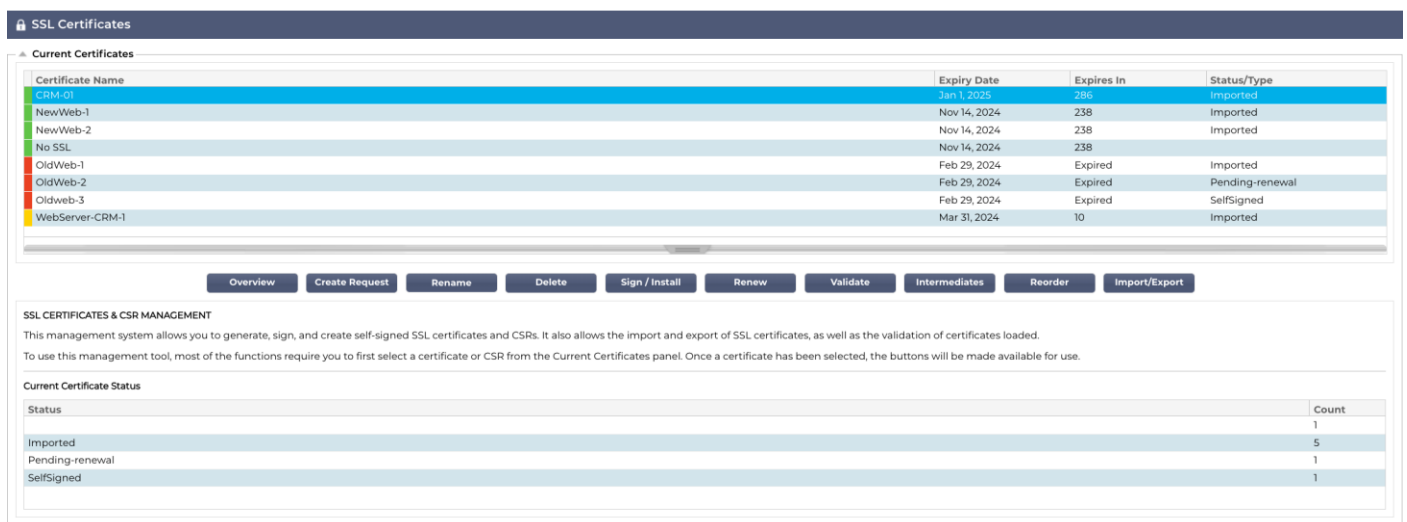
ADCはSSL証明書で何をしますか？

ADCは、データの内容に応じてトラフィック管理ルール（flightPATH）を実行できる。この管理は、SSL暗号化データに対しては実行できない。ADCがデータを検査する必要がある場合、まずデータを復号化する必要がある、そのためにはサーバーが使用するSSL証明書が必要である。復号化されると、ADCはflightPATHルールを検査し、実行できるようになる。その後、データはSSL証明書を使用して再暗号化され、最終的なりアル・サーバーに送信される。

SSL設定マネージャー

バージョン196X以降では、SSL証明書と証明書要求の設定と管理をより簡単に行えるようになりました。

。



The screenshot displays the 'SSL Certificates' management interface. At the top, there is a header 'SSL Certificates' with a lock icon. Below it, the 'Current Certificates' section shows a table with the following data:

Certificate Name	Expiry Date	Expires In	Status/Type
CRM-01	Jan 1, 2025	286	Imported
NewWeb-1	Nov 14, 2024	238	Imported
NewWeb-2	Nov 14, 2024	238	Imported
No SSL	Nov 14, 2024	238	Imported
OldWeb-1	Feb 29, 2024	Expired	Imported
OldWeb-2	Feb 29, 2024	Expired	Pending-renewal
Oldweb-3	Feb 29, 2024	Expired	SelfSigned
WebServer-CRM-1	Mar 31, 2024	10	Imported

Below the table, there are several action buttons: Overview, Create Request, Rename, Delete, Sign / Install, Renew, Validate, Intermediates, Reorder, and Import/Export. Underneath, there is a section titled 'SSL CERTIFICATES & CSR MANAGEMENT' with a brief description of the tool's capabilities. At the bottom, a 'Current Certificate Status' table shows the following data:

Status	Count
Imported	1
Pending-renewal	5
SelfSigned	1

SSL Configuration Managerには3つの主要なセクションがあります。

証明書リスト・エリア






Certificate Name	Expiry Date	Expires In	Status/Type
CRM-01	Jan 1, 2025	286	Imported
NewWeb-1	Nov 14, 2024	238	Imported
NewWeb-2	Nov 14, 2024	238	Imported
No SSL	Nov 14, 2024	238	Imported
OldWeb-1	Feb 29, 2024	Expired	Imported
OldWeb-2	Feb 29, 2024	Expired	Pending-renewal
OldWeb-3	Feb 29, 2024	Expired	SelfSigned
WebServer-CRM-1	Mar 31, 2024	10	Imported

Manager の上側には、使用可能な SSL 証明書、または信頼できる機関から有効化待ちの SSL 証明書が表示されます。

証明書は、証明書名、有効期限、Expires In（有効期限までの日数）、および証明書の Status/Type の 4 つのカラムで表示される。

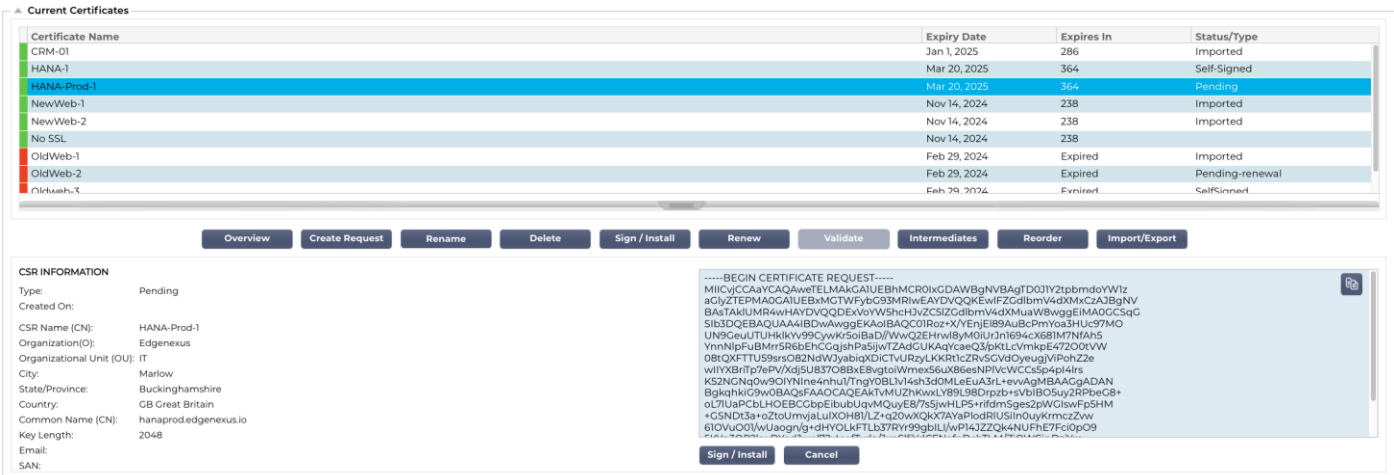
カラーコード

ご覧のように、各行は証明書と色分けされたブロックを示している。以下は、色分けされたブロックとその意味を示した表である。

カラーコード	意味
	証明書が最新であり、有効期限まで 60 日以上ある。
	証明書の有効期限は 30 日以内です。
	証明書の有効期限は 30 日から 60 日
	証明書の有効期限が残り 1 日となりました。
	証明書の有効期限が切れている

証明書/CSR 情報表示

証明書または CSR をクリックすると、その情報が下部のパネルに表示されます。下の画像を参照してください。



The screenshot shows the 'Current Certificates' interface. The top part is a table listing certificates with columns for Certificate Name, Expiry Date, Expires In, and Status/Type. The 'HANA-Prod-1' certificate is highlighted in blue. Below the table is a navigation bar with buttons: Overview, Create Request, Rename, Delete, Sign / Install, Renew, Validate, Intermediates, Reorder, Import/Export. The bottom part of the screenshot shows the 'CSR INFORMATION' panel for the selected certificate. It includes fields for Type (Pending), Created On, CSR Name (CN), Organization(O), Organizational Unit (OU), City, State/Province, Country, Common Name (CN), Key Length, Email, and SAN. To the right of the CSR information is a text area containing the certificate request text, starting with '-----BEGIN CERTIFICATE REQUEST-----' and ending with '-----END CERTIFICATE REQUEST-----'. At the bottom of the text area are 'Sign / Install' and 'Cancel' buttons.

アクションボタンと設定エリア

Overview Create Request Delete Install/Sign Renew Validate Intermediates Reorder Import/Export

SSL CERTIFICATES & CSR MANAGEMENT

This management system allows you to generate, sign, and create self-signed SSL certificates and CSRs. It also allows the import and export of SSL certificates, as well as the validation of certificates loaded.

To use this management tool, most of the functions require you to select a certificate from the table located to the left of the buttons. Once a certificate is selected, the buttons will be made available for use.

Current Certificate Status

Status	Count
Imported	2
Pending	1
SelfSigned	1

リスティングで証明書が選択されると、多くのアクションボタンが利用可能になり、実行されます。

概要

Current Certificate Status

Status	Count
Imported	1
Pending	5
Pending-renewal	1
Self-Signed	1
SelfSigned	1

「Overview」ボタンは、証明書の全体的な状況を下部に表示する。他のアクションとは異なり、「概要」ボタンは独立しており、証明書を選択する必要はない。

リクエストの作成

自己署名証明書または **CSR** を作成する場合は、**Create Request** ボタンをクリックする必要があります。これにより、必要なすべての詳細を入力できる共通入力パネルが表示されます。

CREATE SELF-SIGNED CERTIFICATE / CSR

AD Certificate Name (CN): CRM-Server

Organization (O): Jumping Jack Flash Inc

Organizational Unit (OU): IT

City/Locality: New York

State/Province: New York

Country: US United States

Common Name (FQDN): crm.jjf.com

Key Length: 2048

Period (days): 360

Email: flash@jjf.com

Subject Alternative Names: Email www.mysite.com

DNS: www.crm.jjf.com x IP: 10.5.6.7 x Email: admin@jjf.com x

Cancel Reset Create CSR Create Certificate

AD 証明書名 (CN)

これは、ADC に証明書の名前を表示するために使用される説明フィールドである。フィールドの入力は、スペースを含まない英数字で指定する。

組織 (O)

このフィールドは、証明書を使用する組織の名前を指定するために使用する。

組織単位 (OU)

通常、部門または組織単位を指定するために使用されます。

市町村

その名が示すように、一般的にユーザーは組織の所在地を指定する傾向がある。

都道府県

このフィールドに州、郡、または県を指定してください。

国名

これは必須項目であり、証明書を使用する国を選択して記入する必要があります。ここに記入された情報が正確であることを確認してください。

コモンネーム (FQDN)

これは重要なフィールドで、証明書を使用して保護するサーバの完全修飾ドメイン名(FQDN)を指定するために使用します。これは **www.edgenexus.io** や **edgenexus.io**、あるいはワイルドカード ***.edgenexus.io** のようなものです。証明書を IP アドレスにバインドしたい場合は、IP アドレスを使うこともできます。

キーの長さ

SSL 証明書の暗号化キーの長さを指定するために使用します。

期間 (日)

証明書の有効期間を日数で示す。この期間が経過すると、証明書は使用できなくなる。

電子メール

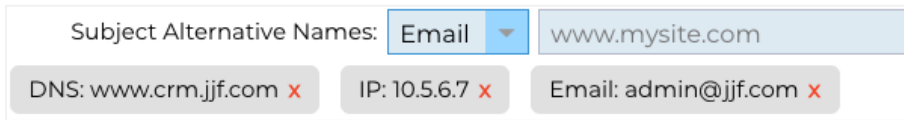
これは、証明書に使用される管理用電子メール ID である。

サブジェクトの別名 (SAN)

Subject Alternative Name (SAN) は、SSL 証明書の拡張機能で、複数のドメイン名を単一の証明書で保護することができます。この機能は、複数のサブドメインや異なるドメイン名を持つウェブサイトを保護するために特に有用であり、SSL 管理のより合理的で費用対効果の高いアプローチを可能にします。SAN を含めることで、1つの SSL 証明書でさまざまなドメイン名やサブドメインをカバーことができ、各ウェブアドレスに個別の証明書を発行する必要がなくなるため、ウェブ通信の保護プロセスが簡素化され、多様なドメイン間でデータの暗号化が保証されます。

このフィールドは、SAN のタイプを選択できるドロップダウンと、値を指定するテキストフィールドの 2 つの要素で構成されています。

EdgeADC では、以下の SAN が使用可能です : DNS、IP アドレス、電子メール・アドレス、URI。証明書または CSR に対して、複数の SAN を選択および指定することができます。



指定された SAN は、各 SAN の値にある赤い✕をクリックすることで削除できます。

- **DNS - DNS Subject Alternate Name (SAN)**では、証明書が有効なドメイン名を追加指定することができる。1つのドメインしか指定できない **Common Name (CN)** フィールドとは異なり、**SAN** フィールドには複数のドメイン名を含めることができるため、証明書管理に柔軟性と拡張性を提供することができる。これは、異なるドメインやサブドメインにまたがる複数のサービスをホストしている組織にとって特に有用である。単一の **SSL/TLS** 証明書でこれらすべてのエンティティの通信を保護できるため、管理が簡素化され、セキュリティが向上する。
- **IP アドレス - IP サブジェクト代替名(SAN)**は、証明書によって保護されるエンティティとして、ドメイン名とともに IP アドレスを含めることを可能にする。この機能は、IP アドレスを介したサービスへの直接アクセスを保護するために非常に重要であり、ドメイン名ではなく IP アドレスを介して直接サーバにアクセスする場合にも暗号化された接続を確立できることを保証する。IP SAN を組み込むことで、組織は、ドメインベースと IP ベースの両方の通信で **SSL/TLS** 暗号化を可能にし、内部リソースや特定のサービスへのアクセスにドメイン名が使用されなかったり、好まれなかったりする環境でも多目的に使用できるようにすることで、ネットワークセキュリティを強化することができる。
- **電子メールアドレス - 電子メールアドレスのサブジェクト代替名(SAN)**は、証明書が発行されたプライマリドメインまたはエンティティの他に、証明書に関連付けられる追加の電子メールアドレスを指定することを許可する。これにより、証明書は、単一のドメインまたはコモン・ネーム (CN) だけでなく、複数の電子メール・アドレスについて発行者の身元を検証することができる。特に、同じ組織やエンティティの下でさまざまな電子メールアドレスに対して安全な電子メール通信が必要とされるシナリオで有用であり、暗号化された電子メールの交換が認証され、証明書によって検証された発行者の身元に結びつけられることを保証します。これにより、**Email Address SAN** は、暗号化されたフレームワーク内での電子メール通信のセキュリティと信頼性を強化するための重要な機能となります。
- **URI - URI (Uniform Resource Identifier) SAN** は、証明書によって保護される単一のエンティティの URI で表される追加の ID を指定するために使用される。通常、ドメイン名 (DNS 名) または IP アドレスを含む従来の **SAN** エントリとは異なり、**URI SAN** は、証明書がエンティティを特定の URI (特定のリソースまたはサービス・エンドポイントへの URL など) に関連付けることを可能にする。これにより、より柔軟かつ正確な識別が可能になり、ドメイン自体の安全性を確保するだけでなく、ドメイン内の特定のリソースやサービスと安全な接続を確立できるようになり、**SSL/TLS** 証明書の粒度とスコープが強化される。

正しく記入されたら、証明書署名要求 (CSR) を作成し、認証局による署名のために送信するか、すぐに使用するために自己署名証明書を作成するかを選択できます。

キャンセルボタンはリクエスト全体をキャンセルし、リセットボタンはすべてのフィールドをリセットします。

名前変更

名前の変更] ボタンを使うと、仮想サービスで使用されていない証明書の名前を変更できます。

この機能を使うには

- 名前を変更したい証明書をクリックし、[Rename]ボタンをクリックします。
- 証明書の行が変わり、名前を変更できるようになります。

Certificate Name	Expiry Date	Expires In	Status/Type
HANA-1	Mar 20, 2025	364	Self-Signed
HANA-Prod-1	Mar 20, 2025	364	Pending
NewWeb-1	Nov 14, 2024	238	Imported
NewWeb-2	Nov 14, 2024	238	Imported
No SSL	Nov 14, 2024	238	
OldWeb-1	Feb 29, 2024	Expired	Imported
OldWeb-2	Feb 29, 2024	Expired	Pending-renewal
Oldweb-3	Feb 29, 2024	Expired	SelfSigned
WebServer-CRM-1	Mar 31, 2024	9	Imported

Buttons: Overview, Create Request, Rename, Delete, Sign / Install, Renew, Validate, Intermediates, Reorder, Import/Export

- 完了したら、更新ボタンをクリックします。
- 証明書をダブルクリックして、証明書の名前を変更することもできます。

削除

削除ボタンは、証明書が選択されているときのみ有効です。クリックすると、以下の内容が表示されます

CERTIFICATE/CSR DELETION

You have elected to delete the following SSL certificate:

Certificate/CSR Name: Web-Server-Certificate

If you are sure you want to delete, click Delete or to prevent deletion, click Cancel.

下のペインには、削除要求と、削除が要求された証明書の名前が表示される。

ペインの右下にある「削除」ボタンをクリックして削除を進めます。

インストール/サイン

SIGN / INSTALL CERTIFICATE

Certificate Name: Web-Server-Certificate

To sign a certificate, please upload the ZIP file provided by your certification authority. This must be an Apache-compliant file.

Upload Certificate:

Alternatively, you can also copy and paste the certificate below. Please take care when doing this and do not miss out any information. Intermediates can also be added below the certificates, and terminated with Root CA.

Certificate Text:

CSRを作成し、認証局（CA）による署名を希望する場合、CSRをCAに送付する。その見返りとして、CAは署名された証明書と秘密鍵ファイル、および証明書を正しく機能させるために必要な仲介物を送付します。

必要な要素がすべて入ったZIPファイルが送られてくるかもしれないので、右ペインの上部を使ってアップロードすることができる。

または、テキストエディタで証明書セットを作成し、その内容をペイン下部の「Certificate Text」フィールドに貼り付けることもできる。

いずれかの方法を使用したら、[署名]ボタンをクリックし、[適用]ボタンをクリックします。署名された証明書が左ペインに表示されます。

リニューアル

RENEW CERTIFICATE

You have chosen to **renew** the certificate shown below.

If you'd like to revoke or cancel this request, please click the CSR on the left-side table and select Cancel CSR.

Certificate Name (CN): Web-Server-Certificate

Important
A new CSR has been created for signing, but the original SSL certificate for which renewal was requested is still active. Please ensure you allocate the newly signed certificate to the correct CSR when importing.

証明書の有効期限を過ぎた場合、「Renew」ボタンをクリックすると、証明書の有効期限を延長し、更新することができます。更新には2種類あります。

自己署名証明書

自己署名証明書は、信頼された証明書とは異なり、CSRを使用して更新することはできない。その代わりに、自己署名証明書は、既存のデータを使用して新しいコンフィギュレーションを提示することで更新される。ユーザは、証明書の新しい名前と証明書の新しい有効期限を指定することができる。

これが完了すると、新しい自己署名証明書が作成され、証明書ストアに保存される。その後、証明書を使用する仮想サービスが時間内に再設定されるようにするのは、管理者の責任である。

信頼できる署名付き証明書

信頼され、認証局によって署名された証明書に関しては、CSRの使用が採用される。

トップパネルで期限切れの証明書をクリックし、「更新」をクリックすると、現在の証明書の詳細を使用した新しいCSRが表示されます。このCSRをダウンロードして認証局に提示し、署名を受けると、署名された証明書をインストールできます。

更新を依頼した証明書は、新しいステータス「更新中」になります。署名された証明書がインストールされると、証明書に新しい名前を割り当てるよう求められます。この名前は「信頼済み」と表示されます。元の証明書は保持され、それを使用しているサービスは、できるだけ早く新しい証明書を使用するように設定する必要があります。

証明書の検証

SSL証明書を構成する部品はいくつかあり、これらの部品が存在するだけでなく、正しい順序で配置されていることが不可欠です。第三者機関から取得したSSL証明書を検証する理由を以下に示します。

- **認証**：認証は、証明書が信頼できる機関から発行されたものであることを保証し、ウェブサイトまたはサーバーの身元を確認します。これは、攻撃者がクライアントとサーバー間の通信を傍受できる中間者攻撃を防ぐのに役立ちます。
- **完全性**：SSL証明書を検証することで、証明書が改ざんされていないことを確認できます。これは、安全な接続の完全性を維持するために非常に重要です。
- **トラスト・チェーンの検証** SSL証明書は認証局（CA）によって発行される。証明書の検証には、その証明書が信頼できるルート認証局にチェーンバックしているかどうかの検証も含まれます。このプロセスにより、証明書が正当なものであり、信頼できるものであることが保証されます。
- **失効ステータス**：検証中に、SSL証明書が発行CAによって失効されていないかどうかを確認することも重要です。誤って発行された場合、ウェブサイトの秘密鍵が漏洩した場合、サイトが証明書を必要としなくなった場合などに、証明書が失効することがあります。取り消された証明書をインポートすると、セキュリティの脆弱性につながる可能性があります。

- **有効期限の確認**：SSL 証明書には有効期限があります。インポート時に証明書を検証するには、その証明書の有効期限をチェックし、まだ有効であることを確認します。有効期限切れの証明書を使用すると、脆弱性につながり、ブラウザやクライアントが安全な接続を拒否する可能性があります。
- **コンフィグレーションと互換性**：検証は、証明書のコンフィグレーションがクライアントのセキュリティ・ポリシーおよびサーバまたはアプリケーションの技術要件に適合していることを保証する。これには、使用されるアルゴリズム、証明書の目的、その他の技術的な詳細の確認が含まれる。
- **コンプライアンス**特定の業界では、機密情報の安全な取り扱いを保証するために、**SSL 証明書**の検証を規制で義務付けている場合があります。これは、金融、医療、電子商取引などの分野で特に重要です。

ADC の SSL 管理システムは、インポートされた **SSL 証明書**の検証を可能にする。

- インポートした **SSL 証明書**を選択します。
- **Validate** ボタンをクリックする。
- その結果は、下の画像で表されるように、下のパネルで見ることができる。

VALIDATE CERTIFICATE		
The validation results are shown below:		
Certificate Name:	EdgeWild	
Test Name	Test Result	Test Status
Certificate file	/jetnexus/etc/sslcert_EdgeWild.pem: CN = *.edgenexus.io error 20 at 0 depth lookup:unable to get local iss	✓
Certificate expires	Certificate expired 114 days ago	✗
Private key check	OK	✓
Public key check	OK	✓

インターミディエイトを加える

先に述べたように、**SSL 証明書**はいくつかの部分から構成されており、そのうちのひとつが、完全なチェーンを構成するための中間証明書である。

ADC の **SSL Manager** で、不足している中間証明書を追加できる。

- 中間証明書を追加したい **SSL** をクリックします。
- 中級者ボタンをクリックする。
- 下の画像のようなパネルが表示される。

ADD INTERMEDIATES	
Certificate selected:	EdgeWild
Paste Certificate text here.	
Cancel	Apply

- 中間証明書の内容を貼り付ける。
- **Apply** をクリックする。

SSL 証明書が正しく検証されるように、中間証明書の順序を変更する必要がある場合があります。これは **Reorder** ボタンを使って行います。

再注文

SSL 証明書が正しく動作するためには、正しい順序で配置されていなければならない。

黄金律は、送信者の証明書が最初に来て、最終的なルート証明書がチェーンの最後に来ることである。一般的には、以下のような形になる：

オリジナル発行者 > 中間 1 > 最終ルート。

最終ルートは、認証局が提供する信頼できるルート証明書である。

場合によっては、複数の中間証明書が存在し、これらも正しい位置に配置されなければならない。基本的に、次の各証明書はその前の証明書を証明しなければならない。つまり、以下のようになります。

オリジナル発行者 > 中間 1 > 最終ルート

例えば、中間体 2 をインポートする場合、これはチェーンの最後に置かれる可能性があり、認証が有効でないことを意味する。したがって、順序を変えて、中間 2 を正しい位置（赤で示した位置）に置く必要がある。

だから、最終的にはこうなる：

オリジナル発行者 > 中間 1 > 中間 2 > 最終ルート

----証明書の書き出し

MIIFKTCBBGgAwIBAgISA/UUyBjJ71fucZuvpiLsdfsfdfdf

...

hoFWWJt3/SeBKn+ci03RRvZsdfsfdfw=

----終了証明書

----証明書の書き出し

MIIFJCCA v6gAwIBAgIRAJErCErPDBinsdfsfdfsfdf

....

nLRbwHqsDqD7hHwg==

----終了証明書

-----証明書の書き出し

MIIFYDCCBsdfSDFSDVzfsdfvqdsfgsT664ScbvsfGDGSDV

...

Dfvp700GAN6dEOM4+SDFSDZET+DFGDFQSD45Bddfghqsqf6Bsff

-----終了証明書

----証明書の書き出し

MIIFYDCCBsdfSDFSDVzfsdfvqdsfgsT664ScbvsfGDGSDV

...

Dfvp700GAN6dEOM4+SDFSDZET+DFGDFQSD45Bddfghqsqf6Bsff

-----終了証明書

証明書を選択し、「Reorder」ボタンを押すと、「Reorder」セクションは下図のようになります。

REORDER CERTIFICATE

Certificate selected: NewWeb-1

```
-----BEGIN CERTIFICATE-----
MIIGqjCCBZKgAwIBAgIIHrAJZ3hAK90wDQYJKoZIhvcNAQELBQAwgbcQxCzAJBgNV
BAYTAVTRAwDgYDVQQQEwdBcm16b25hMRMwEQYDVQQHEwptY290dHNkYXNlMRow
GAYDVQQKExFhb0RlZGR5LmNvbSw5SjJlETMCSGAIECMMkafHR0cDovL2N1cnRz
LmdvZGFkZiHkuY291L3JicC9zaXRvcnkMTWwMqYDVQQDEyphbyBkYWRkeSBkZWN1
cmUgQ29yZGlmaWVhdG9yYXR5XRS1C0gRzlwHhcnNjMTE0MTAwNDAS5WhcN
MjQxMTE0MTAwNDAS5WAgMR4wHAYDVQQDEXVsb2FkYmF5SjZluc29mdHdhcmUw
ggEIMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCpOqsQqHUG6ePu5tu0Lnm
cAVXfkDCR6xCdxuAE3QTFKDtF9m7RRS/8tXq7ZmwnkBCw5eHar8t0xHkGJnhFEuU
R2iSbfcw5kfzTUIOJVZCW7E0+hQdNlPdFtY0KCsG0alkjo0w+ah4ngOf8Mlov9X
axM3M4PQ5LTbZ4nZdijJ4PTCanAgg/FjYfRsyOymr7NwWmUGbFJ/GAKq9YtzE
ziQZg0M0y5RHMH8832gEIo0msu/aqze8pk2Ybl9oBEAVuhr85i60JaYcYL7O6CGBs
jZIGZJhnbv9qtc9YtXUqi0WEFTpBQ29JOVKMahJwMF6k7O98b0UWBe6RICV
AgMBAAGjggNRMIIIDTAMBgNVHRMBAf8EAjAMB0CAIudJQQWMBQCCsGAQUFBwMB
BggrBgEFBQcDAJAQBgNVHQ8BAf8EBAMCBAAwQYDVRR0BDBWMDAuoCygk0yohHRO
cDovL2N1cnRzC5nb2RlZGR5LmNvbSw5SjZlETMCSGAIECMMkafHR0cDovL2N1cnRz
MEGCC2CSAGC/W0BBxcBMDkwNwYkwyBBQUHAQEwK2h0dHAG6Ly9jZXR0aWZpY2F0
ZXMuz29kYWRkeSBkZWN1cnRzNpdC9yeS8wCAYGZ4EMAQIBMHYGCcsGAQUFBwEB
BQowaDAkBggrBgEFBQcwAYYYaHR0cDovL29jc3AuZ29kYWRkeSBkZWN1cnRzC5nb2RlZGR5
AQUBzAChjRodHRwOiBvY29yZGlmaWVhdG9yYXR5LmdvZGFkZiHkuY291L3JicC9zaXRv
cnkvZ2RlZiZ3J0M0BBGAIUdlwQYMBAfEDCvSeOzD5DMKzI/tss/COLIDOMDsG
AIUdEQ0MDKCFWxvWVRiYXhbmNlcis2b2Z0d2FyZlZ3d3d3LmxyWVRiYXhbmNl
cis2b2Z0d2FyZlZ3d3d3LmxyWVRiYXhbmNlcis2b2Z0d2FyZlZ3d3d3LmxyWVRiYXhbmNl
BoEAdZ5AaOCBIBbOSCAWkZwBIA07N0GTV2xrOxV3nbtNE6lvh0Z8wOzewlFI
```

Cancel Apply

証明書セクションの順序を変更するには、ボックス内のテキストをコピーし、テキストエディタで内容を編集して順序を変更し、それを貼り付けて既存の内容を置き換えることができます。完了したら、「Apply」ボタンをクリックします。

インポート/エクスポート

IMPORT CERTIFICATE

Certificate Name: ProductionWebSiteCertificate

Upload Certificate: Browse pfx, .cer, .pem & .der supported

Upload Key File: Browse optional

Password: Used when PKCS#12 was created required for .pfx

Reset Import

EXPORT CERTIFICATE

Certificate Name: EdgeWild

Password: 6 or more letters and numbers

Reset Export

SSL 証明書プロバイダーから証明書を受け取る際、証明書は ZIP ファイルまたは一連のファイルとして提供されます。これらのファイルには、SSL 証明書、キーファイル、ルート CA、および中間ファイルが含まれています。

ADC にインポートする必要があるため、インポート方法を用意した。

SSL 証明書には、CER、DER、PEM、PFX など多くのフォーマットがあります。フォーマットによっては、インポート手順に KEY ファイルを追加する必要があります。PFX ファイルは、PFX 証明書をインポートするためにパスワードが必要です。

必要であれば、ADC から証明書をエクスポートする手段も提供している。エクスポートする場合、ファイルは PFX 形式となるため、エクスポートを作成するためのパスワードが必要となります。

バックアップ & リストア

バックアップ

Backup & Restore

BACKUP ALL SSL, CSR & INTERMEDIATE CERTIFICATES

Filename for Backup:

Certificate Name:

Password:

RESTORE CERTIFICATES, CSRs & INTERMEDIATES FROM BACKUP

Upload Certificate:

Password:

ADC の証明書ストアにある証明書をバックアップする :

- バックアップに使用するファイル名を追加します。
- ドロップダウンメニューを使用して、単一の証明書を選択するか、すべての証明書をバックアップする場合は **ALL** を選択します。
- パスワードを追加する
- バックアップの作成ボタンをクリックします。
- 作成されるファイルは暗号化された **JNBK** ファイルである。

重要

バックアップは、インポートされた **Trusted** 証明書に対してのみ機能する。

リストア

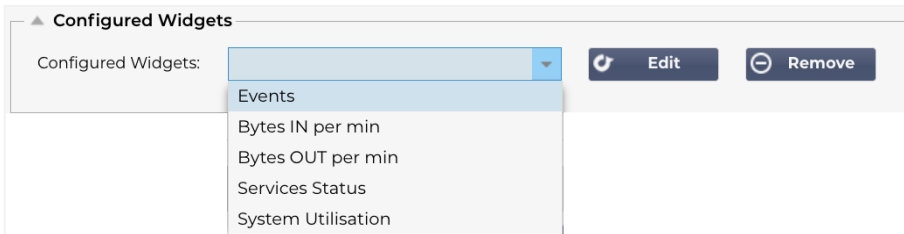
バックアップを復元する場合は、「バックアップと復元」の下でのセクションを使用します。

- バックアップファイルの場所を確認します。
- パスワードを入力する。
- **Restore** ボタンをクリックします。
- バックアップ・ファイル内の証明書はリストアされる。

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ビジュアルコンポーネントを設定できます。

設定されたウィジェット

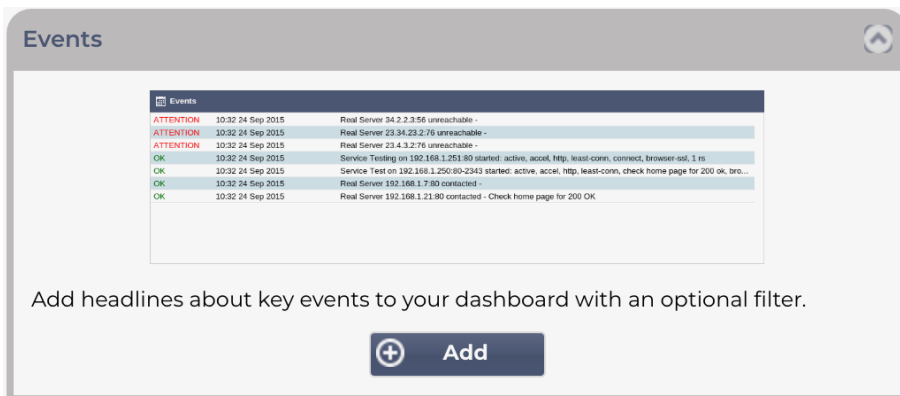


設定されたウィジェットセクションでは、利用可能なウィジェットセクションから作成されたウィジェットの表示、編集、削除ができます。

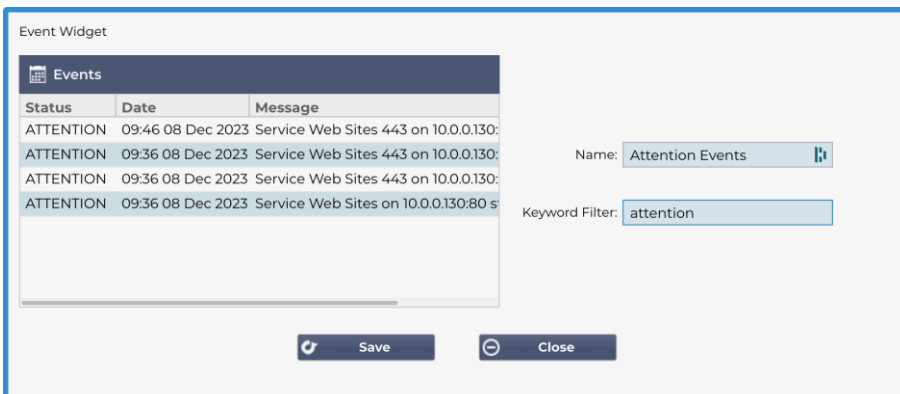
利用可能なウィジェット

ADCには5つの異なるウィジェットが用意されており、必要に応じて設定することができます。

イベント・ウィジェット

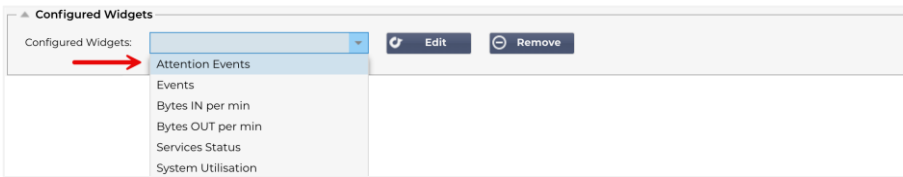


- イベント]ウィジェットにイベントを追加するには、[追加]ボタンをクリックします。
- イベント名を入力します。この例では、**Attention Events** をイベント名として追加しています。
- キーワードフィルターを追加。また、**Attention** のフィルター値を追加しました。



- 保存をクリックし、閉じる

- これで、[設定済みウィジェット]ドロップダウンに[注意イベント]という追加のウィジェットが表示されます。

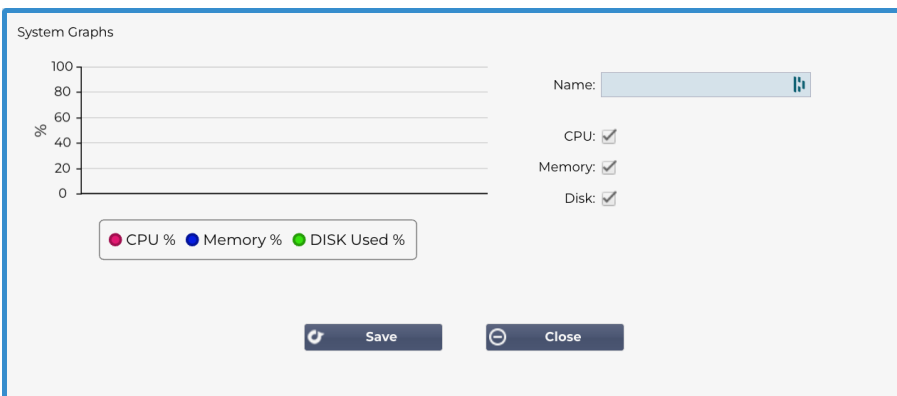


- 表示 > ダッシュボード」セクションにこのウィジェットが追加されていることがわかります。
- ダッシュボード内にこれを表示するには、[注意イベント]ウィジェットを選択します。以下を参照してください。

Status	Date	Message
ATTENTION	14:49 08 Dec 2023	Service on 10.0.0.125:443 stopped: active, accel, http, jsp, 200ok, browser-ssl, 3 rs - stop interface deleted
ATTENTION	10:51 07 Dec 2023	Service on 10.0.0.125:80 stopped: active, accel, http, jsp, 200ok, browser-ssl, 3 rs - Stopping VS 10.0.0.125:80; update interface 10.0.0.125 updated
ATTENTION	10:51 07 Dec 2023	Service on 10.0.0.125:80 stopped: active, accel, http, least-conn, connect, 1 rs - Stopping VS 10.0.0.125:80; update interface 10.0.0.125 updated
ATTENTION	12:12 30 Nov 2023	10.0.0.120:80 Real server myWAF2:80 unreachable - Connect=FAIL
ATTENTION	12:09 30 Nov 2023	10.0.0.120:80 Real server myWAF:80 unreachable - Connect=FAIL
ATTENTION	08:53 29 Nov 2023	Service on 10.0.0.125:443 stopped: active, accel, http, least-conn, connect, 3 rs - stop interface deleted
ATTENTION	10:39 23 Nov 2023	Service INGRESS on 10.0.0.120:80 stopped: active, http, least-conn, connect, 1 rs - Stopping VS 10.0.0.120:80; update interface 10.0.0.120 updated
ATTENTION	11:10 22 Nov 2023	Service on 10.0.0.125:443 stopped: active, accel, http, least-conn, connect, browser-ssl, 3 rs - Stopping VS 10.0.0.125:443; update interface 10.0.0.125 updated

ライブ・データの一時停止] ボタンをクリックすると、ライブ・データ・フィードを一時停止して再開することもできます。さらに、「デフォルト・ダッシュボード」ボタンをクリックすれば、いつでもデフォルト・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

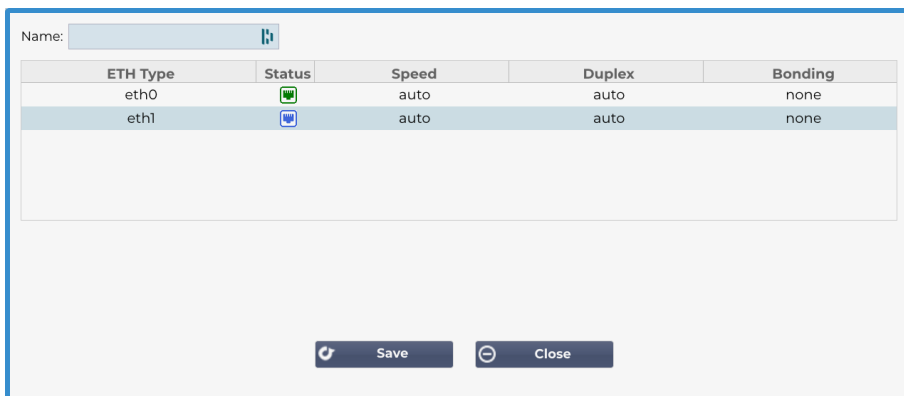


ADC には、設定可能なシステム・グラフ・ウィジェットがあります。ウィジェットの[Add]ボタンをクリックすると、以下のモニタリング・グラフを追加して表示できます。

- CPU
- メモリー
- ディスク

一度追加すると、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。

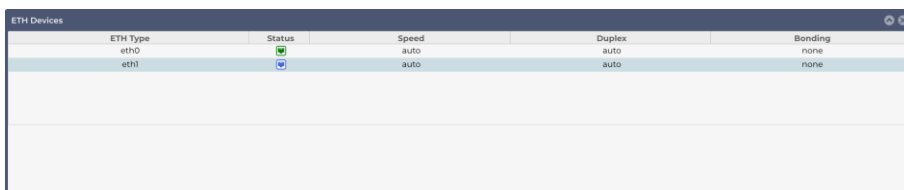
インターフェースウィジェット



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できます。追加可能なインターフェースの数は、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ースの数によって異なります。

終了したら、「保存」ボタンをクリックし、「閉じる」ボタンをクリックします。

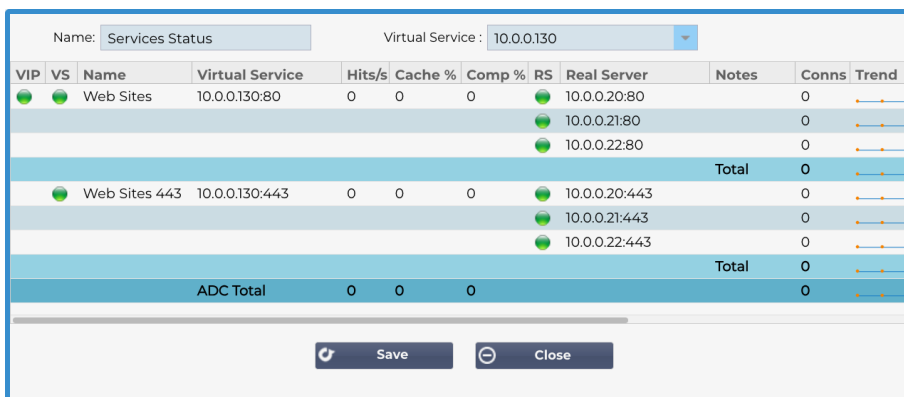
ダッシュボード内のウィジェットドロップダウンメニューからカスタマイズしたウィジェットを選択します。下のような画面が表示されます。



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できます。ビュー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。

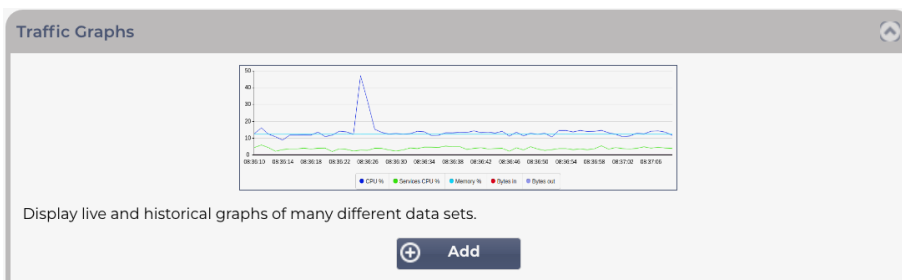
- 追加をクリックする。



- 監視するサービスの名前を入力します。
- 列のヘッダーをクリックして、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、「保存」をクリックし、「閉じる」をクリックします。
- 選択し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できるようになります。

トラフィック・グラフィック・ウィジェット

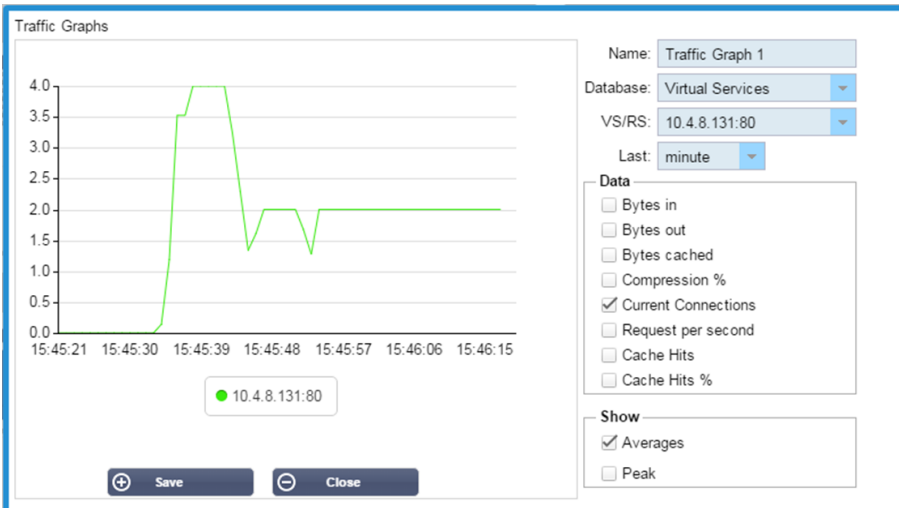
このウィジェットは仮想サービスとリアルサーバーごとに現在と過去のトラフィックデータを表示するように設定できます。さらに、グローバルトラフィックの現在と履歴データも表示できます。



- 追加ボタンをクリック
- ウィジェットに名前を付ける。
- 仮想サービス、リアルサーバー、システムからデータベースを選択します。
- **Virtual Services** を選択すると、**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
 - 時間-過去 60 分間の各分単位の集計データ
 - 日-過去 24 時間の各時間の集計データ
 - 週間-過去 7 日間の各日の集計データ
 - 月-過去 7 日間の各週の集計データ
 - 年-過去 12 ヶ月間の各月の集計データ
- 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。
 - 仮想サービス・データベース
 - バイト
 - 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
 - リクエスト/秒
 - キャッシュ・ヒット
 - キャッシュヒット率
- リアルサーバー
 - バイト
 - バイトアウト
 - 現在の接続
 - リクエスト/秒
 - 応答時間
- システム
 - CPU パーセント
 - サービス CPU
 - メモリー

- ディスク空き容量
- バイト
- バイトアウト
- 平均値またはピーク値のいずれかを表示するか選択
- 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



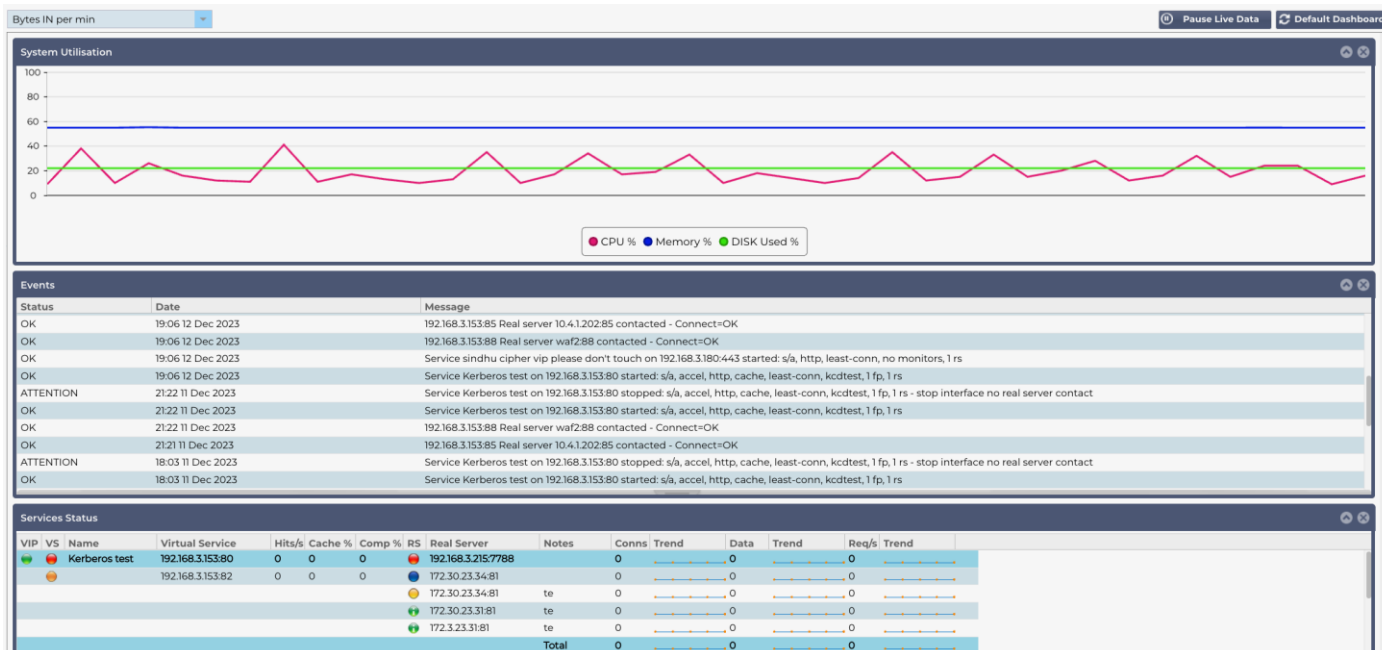
トラフィックグラフウィジェットをビュー>ダッシュボードに追加できるようになりました。

表示

ダッシュボード

すべての 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。ADC では、これを簡単かつ有意義な方法で実行できるよう、カスタマイズ可能なダッシュボードを提供しています。

ダッシュボードは、ナビゲーターパネルのビューセグメントを使用してアクセスできます。選択すると、いくつかのデフォルト・ウィジェットが表示され、定義したカスタマイズ・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い方

ダッシュボード U 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、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。

ライブデータの一時停止ボタン

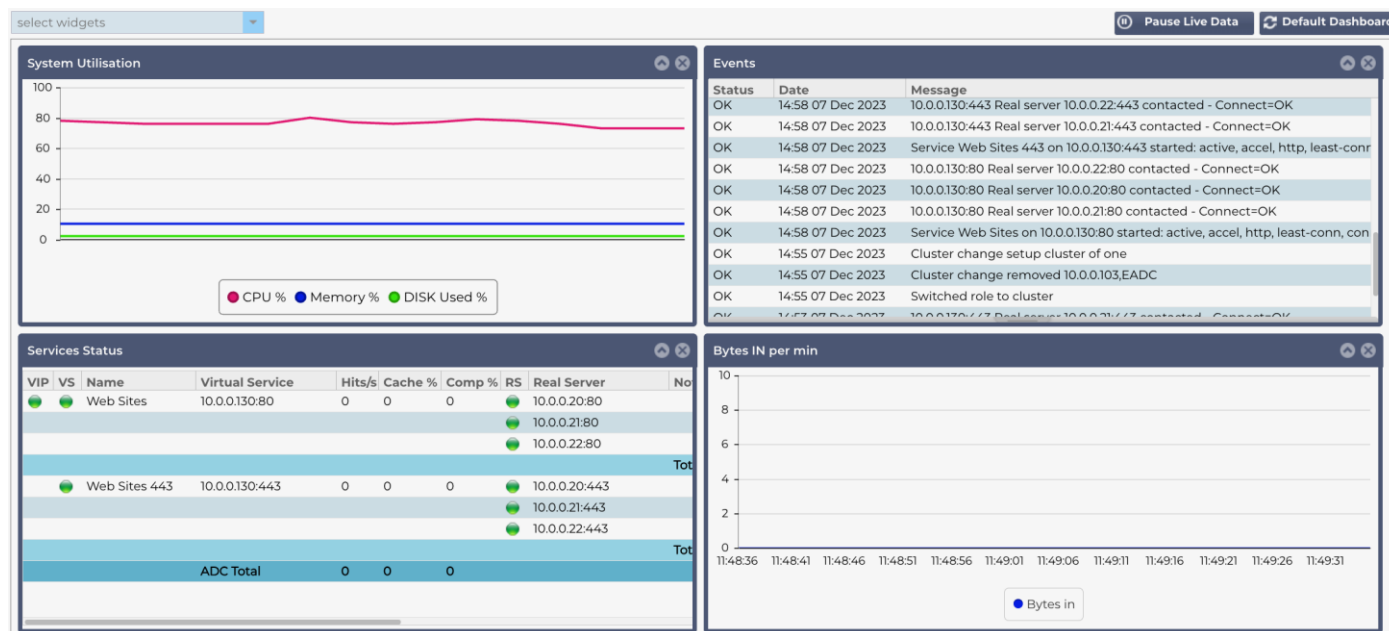
このボタンにより、ADC がリアルタイムでダッシュボードを更新するかどうかを選択できます。一時停止すると、ダッシュボード・ウィジェットは更新されないため、自由にコンテンツを調べることができます。一時停止が開始されると、ボタンは **Play Live Data** の表示に変わります。

終了したら、「ライブデータを再生」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場合があります。そのような場合は、デフォルト・ダッシュボード・ボタンを押してください。クリックすると、ダッシュボードに加えたすべての変更が失われます。

ウィジェットのサイズ変更、最小化、並べ替え、削除



ウィジェットのサイズ変更

ウィジェットのサイズは簡単に変更できます。ウィジェットのタイトルバーをクリックしたまま、ダッシュボード領域の左側または右側にドラッグします。新しいウィジェットサイズを表す点線の長方形が表示されます。ウィジェットを矩形内にドロップし、マウスボタンを放します。リサイズされたウィジェットを以前にリサイズされたウィジェットの横にドロップしたい場合、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できます。この操作でウィジェットが最小化され、タイトルバーだけが表示されます。

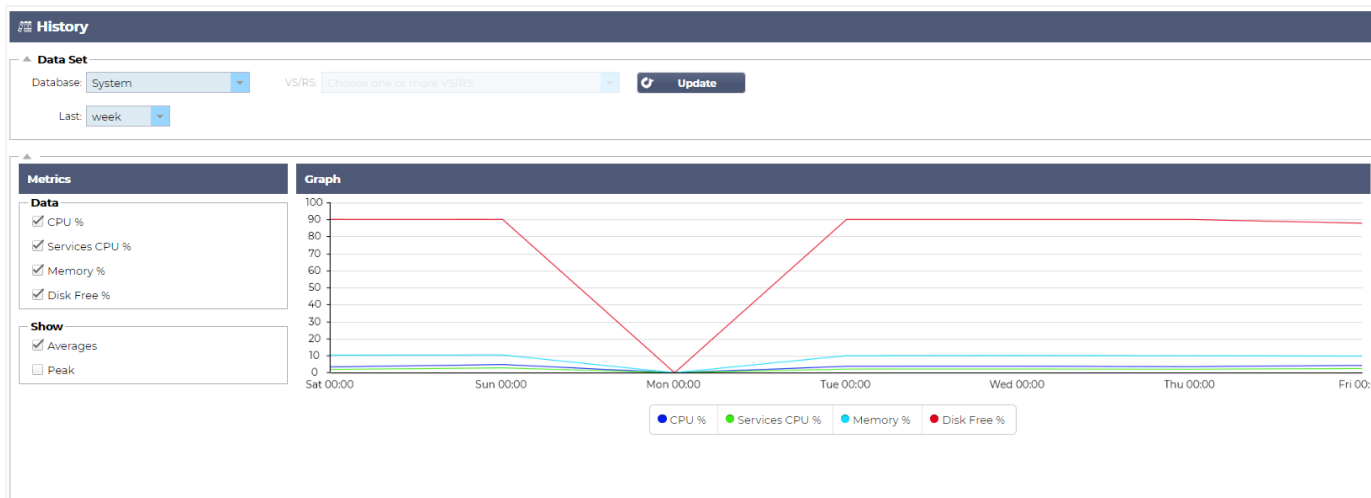
ウィジェットオーダーの移動

ウィジェットを移動するには、タイトルバーをクリックしたままマウスを動かすとドラッグ&ドロップできます。

ウィジェットの削除

ウィジェットタイトルバーの✖ アイコンをクリックして削除できます。

歴史



ナビゲータから選択可能な [History] オプションにより、管理者は ADC の履歴パフォーマンスを調べることができます。履歴ビューは、仮想サービス、リアルサーバー、およびシステムに対して生成できます。

また、ロードバランシングの動作を見ることができ、調査が必要なエラーやパターンをキャッチするのに役立ちます。この機能を利用するには、**System > History** で履歴ロギングを有効にする必要があることに注意してください。

グラフデータの表示

データセット

グラフ形式で過去のデータを見るには、以下の手順に従ってください：

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、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空き容量を時系列で見ることができます。 
パーティチャルサ	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仮想サービスを選択できます。仮想サービスのリストが表示され、そこから 1 つを選択できます。 

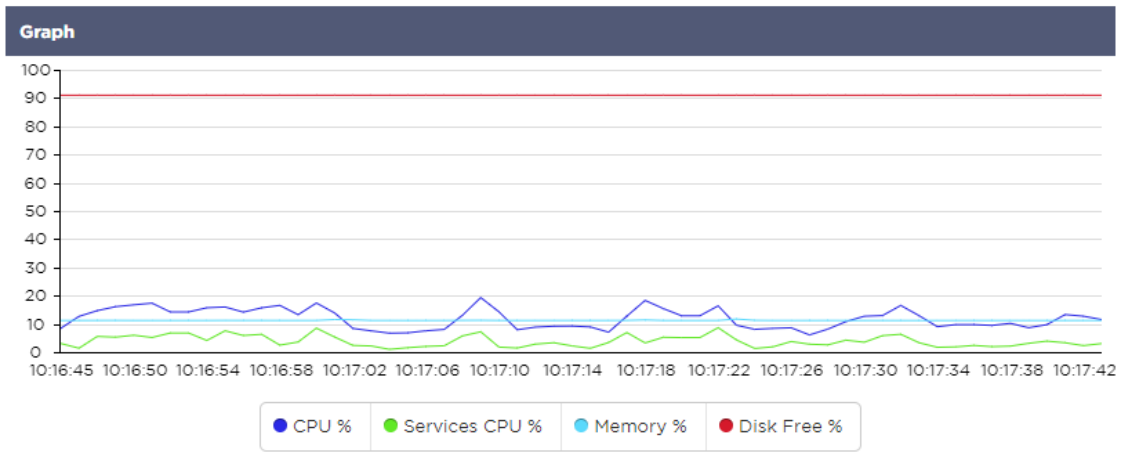
ー ビ ス	
リ ア ル サ ー ビ ス	<p>このデータベースを選択すると、データのロギングを開始した時点からデータベース内のすべてのリアルサーバーを選択できます。リアルサーバーのリストが表示されますので、その中から選択します。</p> <div style="border: 1px solid #ccc; padding: 5px;"> <p>▲ Data Set</p> <p>Database: Real Servers VS/RS: Choose one or more VS/RS Update</p> <p>Last: day</p> <ul style="list-style-type: none"> 192.168.1.40:80-192.168.1.125:8080 192.168.1.40:80-192.168.1.119:8080 </div>

指標

使用するデータセットを選択したら、表示するメトリックを選択します。下図は、管理者が選択可能なメトリックスを示しています。これらの選択は、システム、仮想サービス、リアルサーバーに対応しています（左から右）。

SYSTEM	VIRTUAL SERVICES	REAL SERVERS
<div style="background-color: #2c3e50; color: white; padding: 2px 5px; font-weight: bold;">Metrics</div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <p>Data</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> CPU % <input checked="" type="checkbox"/> Services CPU % <input checked="" type="checkbox"/> Memory % <input checked="" type="checkbox"/> Disk Free % </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <p>Show</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Averages <input type="checkbox"/> Peak </div>	<div style="background-color: #2c3e50; color: white; padding: 2px 5px; font-weight: bold;">Metrics</div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <p>Data</p> <ul style="list-style-type: none"> <input type="checkbox"/> Bytes In <input type="checkbox"/> Bytes Out <input type="checkbox"/> Bytes Cached <input type="checkbox"/> Compression % <input type="checkbox"/> Current Connections <input type="checkbox"/> Request Per Second <input type="checkbox"/> Cache Hits <input type="checkbox"/> Cache Hits % </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <p>Show</p> <ul style="list-style-type: none"> <input type="checkbox"/> Averages <input type="checkbox"/> Peak </div>	<div style="background-color: #2c3e50; color: white; padding: 2px 5px; font-weight: bold;">Metrics</div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <p>Data</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> CPU % <input checked="" type="checkbox"/> Services CPU % <input checked="" type="checkbox"/> Memory % <input checked="" type="checkbox"/> Disk Free % </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <p>Show</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Averages <input type="checkbox"/> Peak </div>

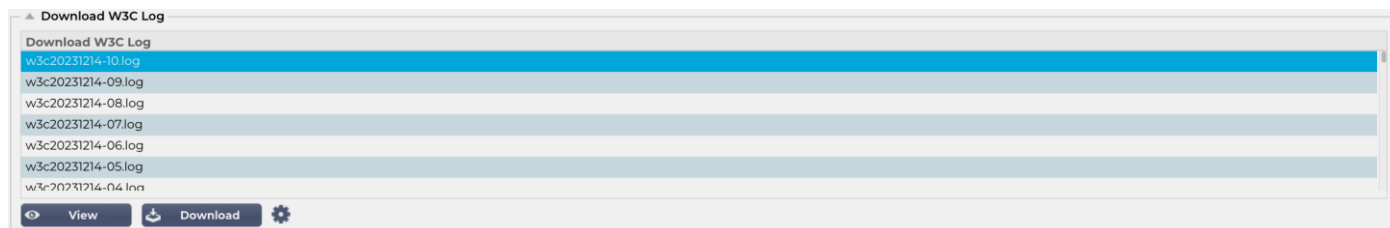
サンプルグラフ



過去ログ

表示」セクションの「ログ」ページでは、W3C とシステムのログをプレビューし、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



W3C ログを有効にするには、[システム] > [ログ] セクションを選択します。W3C ログとは、Web サーバーのアクセスログのことで、各アクセスリクエストに関するデータ（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）を含むテキストファイルが生成されます。W3C のログは、データ量や記録されるロギングのカテゴリによって、非常に大きくなることがあります。

W3C セクションから、必要なログを選択し、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

表示ボタンを押すと、メモ帳などのテキストエディタウィンドウで選択したログを表示することができます。

ダウンロードボタン

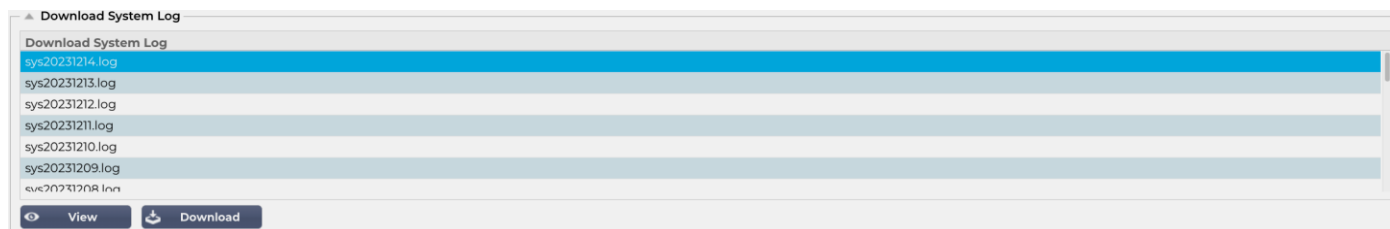
このボタンを押すと、ログをローカルストレージにダウンロードし、後で見ることができます。

歯車のアイコン

このアイコンをクリックすると、System > Logging にある W3C Log Settings セクションに移動します。これについては、このガイドのログのセクションで詳しく説明します。

システムログ

システムログは、ADC で何が起きているかをデバッグまたは調査するために重要です。これは、IT 部門内の経験豊富な人を対象としています。



ボタンを見る

表示ボタンを押すと、メモ帳などのテキストエディタウィンドウで選択したログを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、後で見ることができます。

統計

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よく使用するエリアである。

圧縮

ADC の全目的は、データを監視し、それを受信するように設定された **Real Servers** に指示することである。圧縮機能は、ADC のパフォーマンスを向上させるために ADC に提供されています。管理者は、ADC のデータ圧縮情報をテストおよびチェックしたい場合があります。このデータは、**Statistics** の **Compression** パネルで提供されます。

これまでのコンテンツ圧縮

Content Compression To Date	
Compression	0%
Throughput Before Compression	0
Throughput After Compression	0

このセクションで示すデータは、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である。60-80%という値は、私たちが典型的な圧縮率と呼ぶものです。

これまでの全体的な圧縮

Overall Compression To Date		Current Values
Compression	0%	0%
Throughput Before Compression	0	0.00 Mbps (data)
Throughput After Compression	0	0.00 Mbps (data)
Throughput From Cache	0	0.00 Mbps (data)
Total		0.00 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圧縮画像の数によって異なります。画像の数が多ければ多いほど、全体の圧縮率は小さくなります。

総入出力

Total Input	345.9 MB	Input/s	12.7 kbps
Total Output	296.8 MB	Output/s	25.7 kbps

Total Input/Output の数値は、ADC に入出力される生データの量を表します。測定単位は、kbps、Mbps、Gbps とサイズが大きくなるにつれて変化する。

ヒットとコネクション

Content Caching	Hits	Bytes
From Cache	0/-	0/-
From Server	0/-	0/-
Cache Contents	0 entries	0/0.0%

「ヒットと接続」セクションには、ADC を通過したヒットとトランザクションの全体的な統計が含まれる。では、ヒット数と接続数は何を意味するのか？

- **Hit** はレイヤ 7 トランザクションとして定義される。一般的にウェブサーバに使用され、画像などのオブジェクトに対する **GET** リクエストである。
- **コネクション** とは、レイヤ 4 の **TCP** コネクションのことである。1 つの **TCP** コネクション上で多くのトランザクションが発生する可能性がある。

全体ヒット数

このセクションの数値は、前回のリセット以降の非キャッシュ・ヒットの累積数を示しています。右側には、1 秒あたりの現在のヒット数が表示されます。

総接続数

Total Connections の値は、最後のリセット以降の **TCP** 接続の累積数を表します。2 番目の列の数値は、**ADC** に対して 1 秒あたりに行われた **TCP** 接続を示します。右側の列の数値は、リアル・サーバーへの 1 秒あたりの **TCP** 接続数です。例 **6/8** コネクション/秒。この例では、仮想サービスに対して 1 秒あたり 6 つの **TCP** 接続があり、リアルサーバーに対して 1 秒あたり 6 つの **TCP** 接続があります。

ピーク・コネクション

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、現在アクティブな **TCP** 接続数を示す。

キャッシング

ご記憶のとおり、**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、チャンネルに適用されたキャッシングに関連する全体的な統計を示します。キャッシュ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、キャッシュ・コンテンツは **0** と表示されます。

Content Caching	Hits	Bytes
From Cache	0/-	0/-
From Server	0/-	0/-
Cache Contents	0 entries	0/0.0%

キャッシュから

ヒット数：最初の列は、最後のリセット以降に **ADC** キャッシュから提供されたトランザクションの総数を示す。総トランザクションのパーセンテージも示される。

バイト：番目の列は、**ADC** キャッシュから提供されたキロバイト単位のデータ総量を示す。総データのパーセンテージも表示されます。

サーバーより

ヒット数：第 1 列は、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す。総トランザクション数に対するパーセンテージも表示されます。

バイト：番目の列は、リアルサーバーから提供されたキロバイト単位のデータ総量を示します。総データ量に対するパーセンテージも表示されます。

キャッシュの内容

ヒット数：**ADC** キャッシュに含まれるオブジェクトの総数。

バイト：最初の数字は、ADC キャッシュ・オブジェクトの全体のサイズをメガバイト単位で示します。最大キャッシュ・サイズのパーセンテージも表示されます。

アプリケーション・バッファ

Buffer Type	Connections Used/Free	Memory Used/Free	Average Buffer Fill Size
Low	0/5k(0%)	0/655MB(0%)	0
Medium	0/5k(0%)	0/30MB(0%)	0
High	0/10k(0%)	0/20MB(0%)	0

ADC におけるアプリケーション・バッファの使用は、パフォーマンスの最適化、スループットの向上、クライアントとサーバー間の信頼性の高い効率的なデータ・フローの確保に役立ちます。バッファサイズ、ハンドリングポリシー、その他のパラメータは、ADC によって最適化され、アプリケーションとインフラストラクチャの特定の要件に基づいて負荷を微調整します。

EdgeADC では、そのような大変な作業を EdgeADC が代行し、必要に応じてバッファのパラメータを自動的に調整します。

セッションの永続性

Total current sessions	0
% used (of max)	0
New sessions this min	0
Revalidations this min	0
Expired sessions this min	0

Session Persistence セクションは、いくつかのパラメータに関する情報を提供する。

現在のセッション数

これは、進行中の永続化セッションの数を示します。

使用率

これは、セッション情報用に許可された全領域のうち、どれだけの領域が使用されているかを示している。

この分の新しいセッション

これは、直近 1 分以内に、どれだけの新しい永続性セッションが追加されたかを示している。

この min を再検証する

これは、過去 1 分以内に、どれだけの既存の永続性セッションが、より多くのトラフィックによって再検証されたかを示している。

この分の有効期限切れセッション

これは、過去 1 分以内に、タイムアウト時間内にそれ以上のトラフィックがなかったために、既存のパーシステンス・セッションがどれだけ失効したかを示している。

ハードウェア

仮想環境で **ADC** を使用している場合でも、ハードウェア内で **ADC** を使用している場合でも、このセクション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。

Disk Usage	2%
Memory Usage	10.1%(185.4MB of 1832.7MB)
CPU Usage	76.0%

ディスク使用量

列目に表示される値は、現在使用されているディスク容量のパーセンテージを示し、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に関する情報も含まれる。

メモリ使用量

番目の列は現在使用されているメモリのパーセンテージを示す。括弧内の重要な数字は、**ADC** に割り当てられているメモリの総量である。**ADC** には最低 **2GB** の **RAM** を割り当てることを推奨する。

CPU 使用率

提供される重要な値のひとつは、**ADC** が現在使用している **CPU** の割合である。これが変動するのは当然である。

ステータス

View > Status]ページには、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が表示されます。また、各リアルサーバーへの接続数とデータも表示されるため、リアルタイムでロードバランシングを体験できます。

VIP	VS	Name	Virtual Service	Hits/s	Cache %	Comp %	RS	Real Server	Notes	Conns	Data	Req/s
●	●	Web Sites	10.0.0.130:80	0	0	0	●	10.0.0.20:80		0	0	0
							●	10.0.0.21:80		0	0	0
							●	10.0.0.22:80		0	0	0
Total										0	0	0
●		Web Sites 443	10.0.0.130:443	0	0	0	●	10.0.0.20:443		0	0	0
							●	10.0.0.21:443		0	0	0
							●	10.0.0.22:443		0	0	0
Total										0	0	0
ADC Total				0	0	0				0	0	0

バーチャルサービス詳細

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ている仮想 IP アドレ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バイ
●	パッシブ "が "アクティブ "のために控えていることを示す。
●	オフライン。リアルサーバーに到達できないか、リアルサーバーが有効になっていない。
●	調査状況
●	ライセンスを取得していない、またはライセンスを超えた仮想 IP

VS ステータス・コラム

ライトの色は仮想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バイ
●	パッシブ "が "アクティブ "のために控えていることを示す。
●	サービスには注意が必要です。このステータス表示は、リアルサーバーがヘルスマニターに失敗したか、手動でオフラインに変更されたために発生する可能性があります。トラフィックは流れ続けますが、リアルサーバーの容量は減少します。
●	オフライン。リアルサーバーに到達できないか、リアルサーバーが有効になっていない。
●	調査状況
●	ライセンスを取得していない、またはライセンスを超えた仮想 IP

名称

仮想サービス名

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、およびユーザーまたはアプリケーションが使用するアドレス。

ヒット/秒

クライアント側で 1 秒間にレイヤー7 のトランザクション。

キャッシュ

ここに示された数値は、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る。

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示す。

RS ステータス (リモートサーバー)

以下の表は、VIP にリンクされているリアルサーバーのステータスの意味の概要です。

ステータス	説明
●	接続済み
●	モニターなし
●	ドレインまたはオフライン
●	スタンバイ
●	未接続
●	調査状況
●	ライセンスを取得していない、またはライセンスを超えた仮想 IP

リアルサーバー

リアルサーバーの IP アドレスとポート。

備考

この値には、他の人にエントリーの目的を理解してもらうために、役立つメモを記入することができます。

コンズ (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が実際に行われていることを確認できます。ロードバランシングポリシーが正しく動作している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るデータ量を示す。

Req/Sec (1 秒あたりのリクエスト数)

各リアルサーバーに送信された 1 秒あたりのリクエスト数。

システム

クラスタリング

ADC は単一のスタンドアロンデバイスとして使用することができ、そうすることで完全に機能する。しかし、ADC の目的がサーバーセットの負荷分散であることを考えると、ADC 自体をクラスタリングする必要性が明らかになる。ADC の操作しやすい UI デザインにより、クラスタリングシステムの設定は簡単である。

システム > クラスタリング」 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

- 高可用性ハートビートを維持するために、ADC ペア間に専用ケーブルを敷設する必要はない。
- 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フェイルオーバーはありません。
- 2 台以上の ADC で高可用性を有効にすると、各ボックスは提供するように設定されている仮想サービスを 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はユニキャストメッセージングと Gratuitous ARP を使って新しい Active ロードバランサースイッチに通知する。

☰ Clustering

▲ Role

- Cluster**
Enable Edgenexus ADC to act as part of a Cluster, providing High Availability in Active-Passive mode - automatic synchronisation of appliances
- Manual**
Enable Edgenexus ADC to act in High Availability mode, either Active-Active or Active-Passive - manual configuration of appliance
- Stand-alone**
This Edgenexus ADC acts completely independently without high-availability

▲ Settings

Failover Latency (ms):

Failover Messaging:

▲ Management

Unclaimed Devices

Priority	Status	Cluster Members
1	●	10.0.0.103 EADC-103-BETA

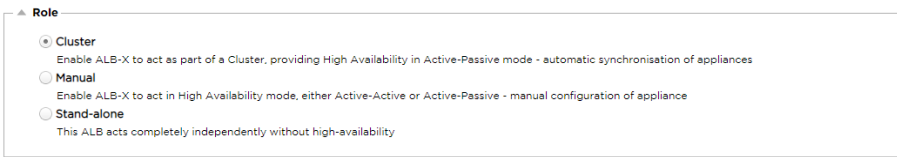
IP Address:

Machine Name:

役割

ADC を高可用性に設定する際に利用可能なクラスタの役割は 3 つあります。

クラスター



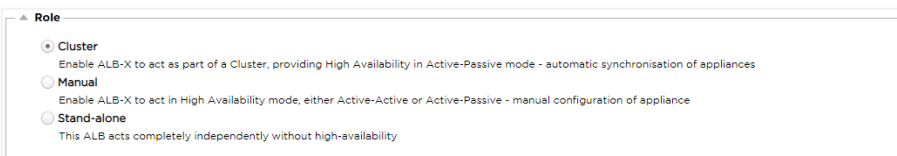
- デフォルトでは、新しい ADC は **Cluster** ロールを使用してパワーオンします。この役割では、各クラスター・メンバーは同じ "作業設定" を持つため、クラスター内の 1 つの ADC のみが常にアクティブになります。
- 「作業コンフィギュレーション」とは、管理 IP アドレス、ALB 名、ネットワーク設定、インターフェイス詳細など、一意である必要がある項目を除くすべてのコンフィギュレーションパラメータを意味する。
- **Cluster Members** ボックスの優先度 1、つまり一番上の位置にある ADC はクラスター所有者であり、**Active** ロードバランサです。
- クラスター内の任意の ADC を編集でき、変更はすべてのクラスター・メンバーに同期されます。
- クラスターから ADC を削除すると、その ADC からすべての仮想サービスが削除されます。
- クラスターの最後のメンバーを **Unclaimed Devices** 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ない：
 - 手動日付と時刻セクション - (NTP セクションは同期)
 - フェイルオーバー待ち時間 (ms)
 - ハードウェア部門
 - 家電セクション
 - ネットワーク部門

クラスターオーナーの故障

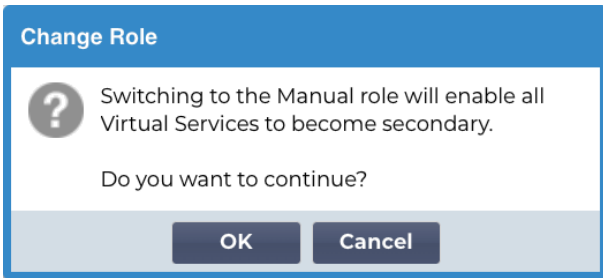
- クラスターオーナーが故障すると、残りのメンバーの 1 人が自動的に引き継ぎ、トラフィックの負荷分散を行う。
- クラスターオーナーが戻ると、ロードバランシングトラフィックを再開し、オーナーの役割を引き継ぎます。
- オーナーが故障し、メンバーがロードバランシングを引き継いだとします。ロードバランシングトラフィックを引き継いだメンバーを新しいオーナーにしたい場合は、そのメンバーをハイライトして上矢印をクリックし、優先順位 1 の位置に移動します。
- 残りのクラスター・メンバーの 1 つを編集し、オーナーがダウンした場合、編集されたメンバーはトラフィックを失うことなく自動的にオーナーに昇格します。

クラスターの役割からマニュアルの役割への変更

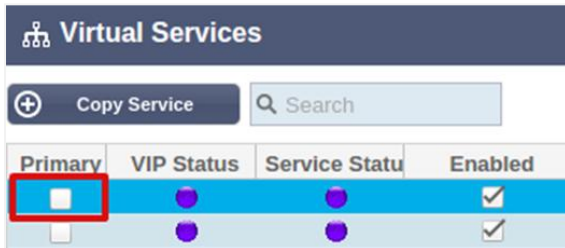
- ロールを **Cluster** から **Manual** に変更したい場合は、**Manual** ロールオプションの横にあるラジオボタンをクリックします。



- ラジオボタンをクリックすると、以下のメッセージが表示されます：



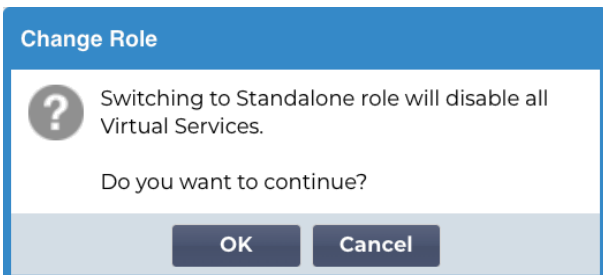
- OK ボタンをクリック
- Virtual Services セクションをチェックする。プライマリ] 列にチェックボックスがないことがわかります。



- これは安全機能であり、同じ仮想サービスを持つ別の ADC がある場合、トラフィックフローが中断されないことを意味する。

クラスタからスタンドアロンへの役割変更

- 役割をクラスタ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ます。
- 次のようなメッセージが表示されます：



- OK をクリックしてロールを変更する。
- 仮想サービスを確認します。プライマリ] 列の名前が [スタンドアロン] に変更されていることがわかります。
- また、安全上の理由から、すべての仮想サービスが無効（チェックなし）になっていることもわかります。
- 同じネットワーク上の他の ADC に重複する仮想サービスがないことを確認したら、各 ADC 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提供します。クラスタの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。欠点は、ADC 間で構成の同期がないことです。変更はすべて、GUI を介して各ボックスで手動で複製する必要がありますか、または多くの変更の場合は、一方の ADC から jetPACK を作成してこれをもう一方の ADC に送信できます。

- 仮想 IP アドレスを "Active "にするには、primary カラムのチェックボックスをオンにします (IP Services ページ)。

- 仮想 IP アドレスを「パッシブ」にするには、プライマリ列のチェックボックスを空白のままにします（IP サービスページ）。
- アクティブサービスがパッシブサービスにフェイルオーバーした場合：
 - プライマリ欄の両方にチェックが入っている場合、選挙が行われ、最も低い MAC アドレスがアクティブになります。
 - 両方がチェックされていない場合、同じ選出プロセスが行われる。さらに、両方のチェックが外された場合、元のアクティブ ADC への自動フォールバックはない。

単独での役割


スタンドアロン役割の ADC は、そのサービスに関して他の ADC と通信しないため、すべての仮想サービスはグリーンステータスのまま接続されます。すべての仮想サービスが固有の IP アドレスを持つようにしないと、ネットワーク上で衝突が発生します。

設定

▲ **Settings**

Failover Latency (ms):

Failover Messaging:

 **Update**

フェイルオーバー待ち時間 (ms)

フェイルオーバー遅延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の待機時間です。

この値は 10000ms または 10 秒に設定することを推奨するが、ネットワークや要件に合わせて増減できる。許容できる値は 1500ms から 20000ms の間です。レイテンシが低いとクラスタが不安定になる場合は、この値を増やす必要があります。

フェイルオーバー・メッセージング

▲ **Settings**

Failover Latency (ms):

Failover Messaging:

Broadcast

Unicast

Hybrid

デフォルトでは、ADC はフェイルオーバー・メッセージングにブロードキャストを使用します。しかし、一部のネットワークではブロードキャストがブロックされているため、ユニキャストと、ユニキャストとブロードキャストをミックスしたハイブリッドが用意されている。

デフォルトのブロードキャスト・モードで動作している場合、要求されていないデバイスは自動的にリストされ、ブロードキャスト・メッセージがフェイルオーバーに使用される。ハイブリッドモードで実行している場合、要求されていないデバイスは引き続きブロードキャストでアドバタイズされますが、フェイルオーバー通信はユニキャストで行われます。**Unicast** モードではブロードキャストされないため、クラスタメンバーを手動で入力する必要があります。

マネジメント

このセクションでは、クラスタ・メンバーを追加および削除し、クラスタ内の **ADC** の優先度を変更することができます。このセクションは 2 つのパネルとその間の矢印キーで構成されています。左側の領域は **Unclaimed Devices** で、右端の領域は **Cluster** そのものです。

▲ Management

Unclaimed Devices	Priority	Status	Cluster Members
10.0.0.110 EADC-110	1	●	10.0.0.103 EADC

▲ Management

Unclaimed Devices	Priority	Status	Cluster Members
10.0.0.110 EADC-110	1	●	10.0.0.103 EADC

クラスタへの ADC の追加

- **ADC** をクラスタに追加する前に、すべての **ADC** アプライアンスに [システム] > [ネットワーク] セクションで一意の名前が設定されていることを確認する必要があります。
- 管理セクションのクラスタ・メンバー列の下に、**ADC** が優先度 1、ステータスが緑、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。
- その他の利用可能な **ADC** はすべて、管理セクション内の [Unclaimed Devices] ウィンドウに表示されます。**Unclaimed Device** とは、クラスタ役割に割り当てられているが、仮想サービスが設定されていない **ADC** のことです。
- **Unclaimed Devices** ウィンドウから **ADC** をハイライトし、右矢印ボタンをクリックします。
- 次のようなメッセージが表示されます：

Promote Unclaimed to Cluster

Do you want to promote '10.0.0.110 EADC-110' from unclaimed to cluster?

OK Cancel

- **OK** をクリックして、**ADC** をクラスタに昇格させます。
- これで、**ADC** がクラスタ・メンバー・リストに優先度 2 として表示されるはずです。

Unclaimed Devices	Priority	Status	Cluster Members
	1	●	10.0.0.103 EADC
	2	●	10.0.0.110 EADC-110

クラスタに ADC を手動で追加する

Broadcast がブロックされているシステムでは、ADC をクラスタに追加するために Unicast または Hybrid モードを選択する必要があります。

▲ Management

Unclaimed Devices
10.0.0.110 EADC-110

Priority	Status	Cluster Members
1	●	10.0.0.103 EADC-103-BETA

IP Address:

Machine Name:

Add Server

ADC をクラスタに手動で追加するには

1. IP アドレスを入力
2. Machine Name (マシン名) を入力します。これは「System (システム)」 > 「Networking (ネットワーク)」セクションで入力できます。

▲ Basic Setup

Name:

IPv4 Gateway: ✔ DNS Server 1: DNS Server 2:

IPv6 Gateway: ✔ Update

3. サーバーの追加

その後、ADC がクラスタに追加される。

追加しようとしている ADC がすでにクラスタ内にある場合は、エラーメッセージで通知されます。

クラスタメンバーの削除

- クラスタから削除するクラスタメンバーを強調表示します。
- 左の矢印ボタンをクリックする。

Unclaimed Devices

Priority	Status	Cluster Members
1	●	10.0.0.103 EADC
2	●	10.0.0.110 EADC-110

- 確認要求が表示されます。
- OK をクリックして確認する。
- あなたの ADC は削除され、Unclaimed Devices 側に表示されます。

ADC の優先順位の変更

メンバーリスト内の ADC の優先順位を変更したい場合もあるだろう。

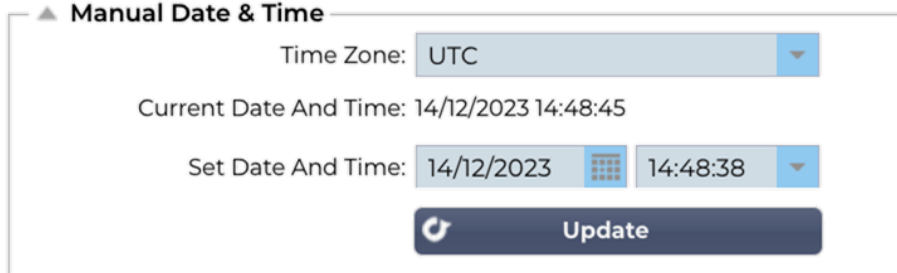
- クラスタメンバーリストの一番上の ADC には優先度 1 が与えられ、すべての仮想サービスのアクティブ ADC になります。
- リストの 2 番目にある ADC には優先度 2 が与えられ、すべての仮想サービスのパッシブ ADC となります。
- ADC をアクティブに変更するには、ADC をハイライトし、リストの一番上にくるまで上矢印をクリックします。

Priority	Status	Cluster Members
1	●	10.0.0.103 EADC
2	●	10.0.0.110 EADC-110

日時

日付と時刻のセクションでは、ADC が配置されているタイムゾーンを含む ADC の日付/時刻の特性を設定できます。タイムゾーンとともに、日付と時刻は SSL 暗号化に関連する暗号化プロセスにおいて重要な役割を果たします。

手動日付と時刻



▲ Manual Date & Time

Time Zone: UTC

Current Date And Time: 14/12/2023 14:48:45

Set Date And Time: 14/12/2023 14:48:38

Update

タイムゾーン

このフィールドに設定した値は、ADC が配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、現在地を入力します。
- 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する。
- 「Lon」と入力し続けると、「Lon」を含む場所に絞り込まれる。
- 例えばロンドンにいたのであれば、Europe/London を選択して場所を設定します。

上記の変更後も日付と時刻が正しくない場合は、手動で変更してください。

日時の設定

この設定は実際の日付と時刻を表します。

- 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、次の形式で日付を入力することもできます。
- 例えば、午前 6 時と 10 秒なら 06:00:10。
- 正しく入力したら、「更新」をクリックして申請してください。
- 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 サーバーを使えば、日付と時刻を正確に同期させることができます。NTP サーバーは世界各地に設置されていますが、インフラストラクチャーによって外部からのアクセスが制限されている場合は、社内に独自の NTP サーバーを設置することもできます。

▲ Synchronise Date & Time (UTC)


Enabled:

Time Server URL:

Update At [hh:mm]: 06:00 ▼

Update Period [hours]: 1 ▼

NTP Type: Public SNTP v4 ▼

 Update

タイムサーバー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) を入力します。サーバーがインターネット上にグローバルに配置されている場合は、FQDN を使用することをお勧めします。

hh:mm]で更新

ADC が NTP サーバーと同期するスケジュール時刻を選択します。

更新期間[時間]:

同期の頻度を選択します。

NTP タイプ:

- Public SNTP V4 - これは、NTP サーバーと同期する際に現在推奨されている方法である。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 - UDP 経由のレガシーNTP バージョン。RFC 1059

注：同期は UTC でのみ行われます。ローカルタイムを設定したい場合は、手動でのみ可能です。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。

メールイベント

ADCは重要なアプライアンスであり、他の重要なシステムと同様に、注意を要する問題をシステム管理者に通知する機能を備えている。

システム > E メールイベント] ページでは、E メールサーバー接続を設定し、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で構成されています。

住所

▲ Address

Send E-Mail Events To E-Mail Address:

Return E-Mail Address:

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して有効なメールアドレスを追加します。例 support@domain.com。カンマ区切りで複数のメールアドレスを追加することもできます。

返信用メールアドレス

受信トレイに表示されるメールアドレスを追加します。例 [.adc@domain.com](mailto: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 サーバーの詳細を追加する必要があります。送信に使用するメールアドレスが、送信を許可されていることを確認してください。

▲ Mail Server [SMTP]

Host Address:

Port:

Send Timeout: minutes

Use Authentication:

Security:

Mail Server Account Name:

Mail Server Password:

ホストアドレス

SMTP サーバーの FQDN または IP アドレスを追加します。

ポート

SMTP サーバーの Port を追加します。SMTP のデフォルトポートは 25、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。デフォルトは 2 分に設定されています。

認証を使用する

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
- デフォルト設定は「なし」。
- SSL - SMTP サーバーで **Secure Sockets Layer** 認証が必要な場合は、この設定を使用します。
- TLS - SMTP サーバーでトランスポート・レイヤー・セキュリティ認証が必要な場合は、この設定を使用します。

メインサーバーアカウント名

認証に必要なユーザー名を追加する。

メールサーバーパスワード

認証に必要なパスワードを追加する。

通知とアラート

ADC が受信するように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。送信する通知と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、リアルサーバーにコンタクトしたとき、またはチャンネルが開始したときに発生します。アラートはリアルサーバーに接続できなかったり、チャンネルが停止した場合に発生します。

IP サービス お知らせ

IP サービス通知は、仮想 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。このアクションは VIP に属するすべての仮想サービスに対して実行されます。

バーチャルサービス お知らせ

仮想サービスがオンラインであるか、または停止していることを受信者に通知します。

リアルサーバー お知らせ

リアルサーバーとポートが接続されている場合、または接続されていない場合、ADC はリアルサーバー通知を送信します。

フライトパス

この通知は、ある条件が満たされたときに送信される電子メールで、ADC にイベントを電子メールで送信するように指示するアクションが設定されている。

グループ通知

通知をグループ化する場合はチェックを入れてください。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。

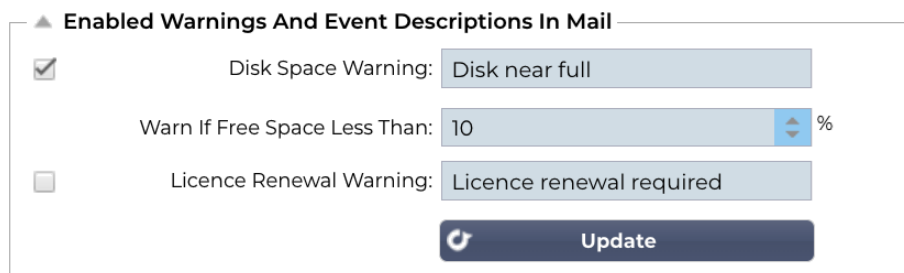
グループメールの説明

グループ通知メールに関連する件名を指定する。

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機時間を指定します。最短時間は 2 分です。デフォルトは 30 分に設定されています。

メールでの警告 と イベント 説明の有効化



▲ Enabled Warnings And Event Descriptions In Mail

Disk Space Warning: Disk near full

Warn If Free Space Less Than: 10 %

Licence Renewal Warning: Licence renewal required

Update

警告メールには 2 種類あり、どちらも無視してはならない。

ディスク容量

警告が送信されるまでのディスク空き容量のパーセンテージを設定します。この値に達すると、電子メールが送信されます。

空き容量が少ない場合は警告

ここにパーセンテージ値を設定することで、ADC はディスク容量がこの閾値を下回った場合に警告メールを送信することができます。

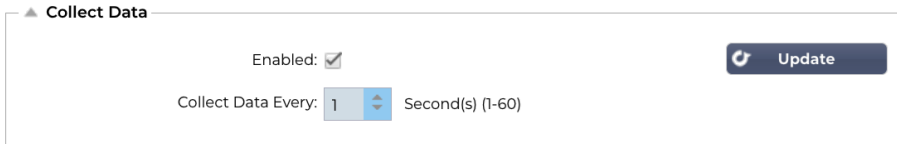
ライセンスの有効期限

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の有効/無効を設定できます。この期限に達すると、電子メールが送信されます。

歴史

System（システム）」セクションには、「System History（システム履歴）」オプションがあり、CPU、メモリ、毎秒リクエスト、その他の機能などの要素の履歴データを配信することができます。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 ADC にバックアップまたは復元することもできます。

データ収集



▲ Collect Data

Enabled:

Update

Collect Data Every: 1 Second(s) (1-60)

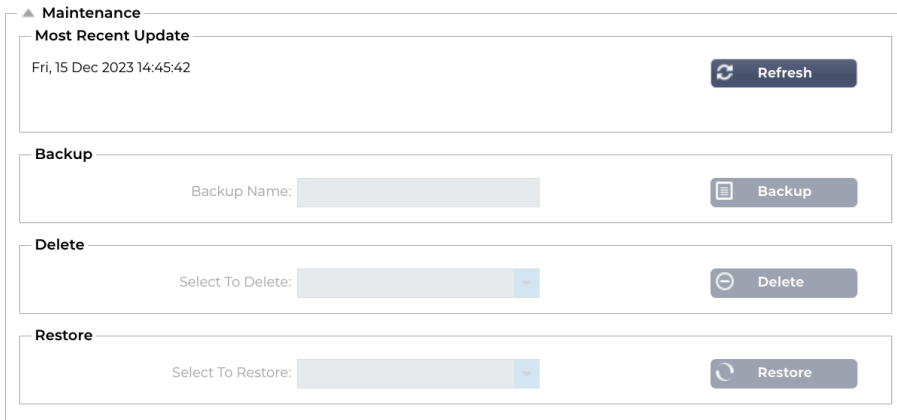
有効にする

データ収集を有効にするには、チェックボックスにチェックを入れてください。

毎回のデータ収集

次に、ADC にデータを収集させたい時間間隔を設定する。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



▲ Maintenance

Most Recent Update

Fri, 15 Dec 2023 14:45:42 Refresh

Backup

Backup Name: Backup

Delete

Select To Delete: Delete

Restore

Select To Restore: Restore

最新のアップデート

これは、ADC から最後の履歴データがいつ収集されたかを示す。

履歴ロギングを有効にしている場合、このセクションは灰色表示されます。データの収集」セクションの「有効」チェックボックスをオフにして、「更新」をクリックし、履歴ログのメンテナンスを許可してください。

HP エンタープライズベース ADC

このセクションの機能は、HPE ProLiant ベアメタルサーバーにインストールされ、ILO を使用する ADC に対してのみ有効です。

バックアップ

バックアップにわかりやすい名前を付けます。すべてのファイルを **ADC** にバックアップするには、[バックアップ]をクリックします。

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。このバックアップファイルからデータを入力するには、[復元] をクリックします。

ライセンス

ADC は、以下のモデルのいずれかを使用して使用するためのライセンスであり、購入パラメータと顧客タイプによって異なります。

ライセンスの種類	説明
永続的	お客様には、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があります。ただし、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 または Software-as-a-Service とは、基本的に継続的または従量制でソフトウェアをレンタルすることを意味する。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。ソフトウェアの永続的な使用権はありません。
けいざいつうかどうめい	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することができます。

ライセンス詳細

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

Licence Details		
Licence ID:	8090DD7C-	DE8D6A1
Machine ID:	F	F3
Issued To:	Edgenexus	
Contact Person:	Jay Savor	
Date Issued:	06 Dec 2023	
Name:		

ライセンス ID

ライセンス ID は、マシン ID および購入した ADC アプライアンスに固有のその他の詳細情報に直接リンクされています。この情報は不可欠であり、App Store からアップデートやその他のアイテムを取得する際に必要となります。

マシン ID

マシン ID は、ADC アプライアンスの eth0 IP アドレスを使用して生成されます。ADC アプライアンスの IP アドレスを変更すると、ライセンスは無効になります。サポートに問い合わせる必要があります。ADC アプライアンスに固定 IP アドレスを設定し、IT スタッフに変更しないよう指示することをお勧めします。テクニカルサポートは、<https://www.edgenexus.io/support> 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 アドレスは変更しないでください。仮想化フレームワークの場合は、MAC ID を固定し、静的 IP アドレスを使用してください。

発行先

この値には、ADC のマシン ID に関連付けられた購入者の名前が含まれる。

担当者

この値には、マシン ID に関連する顧客企業の連絡先担当者が含まれる。

発行日 d

ライセンスが発行された日付。

名称

この値は、[システム] > [ネットワーキング] で指定した ADC アプライアンスの記述名を示します。

設備

▲ Facilities	
Layer 4:	Permanent licence
Layer 7:	Permanent licence
SSL:	Permanent licence
Acceleration:	Permanent licence
flightPATH:	Permanent licence
Pre-Authentication:	Permanent licence
Global Server Load-Balancing:	Permanent licence
Firewall:	Permanent licence
Throughput:	3 Gbps permanent licence
Virtual Service IPs:	24 Virtual Service IPs permanent licence
Real Server IPs:	64 Real Server IPs permanent licence

facilities] セクションでは、ADC 内のどの機能が使用許可されているか、およびライセンスの有効期間に関する情報が提供されます。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、購入し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

▲ Install Licence

Upload Licence:

Paste Licence: Please paste licence in here or upload the licence file above

- 新しいライセンスのインストールはとても簡単です。Edgenexus から新しい、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、ライセンス貼り付けフィールドに内容をコピー&ペーストしてください。
- コピー&ペーストが難しい場合は、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できます。

```

MAC Address: 00:0C:27:00:00:00
Current Version: 4.3.0 (Build 1965) c50631
Server Ref: EADC
OS Version: Linux jetnexus 2.6.32-754.31.1.el6.x86_64 #1 SN

Licence Configuration:
[jetnexusdaemon]
.001Licence="jetNEXUS ALB Licence"
.002Customer="Issued To,Edgenexus"
.003Contact="Contact Person,..."
.004Tel="Telephone,..."
.005LicenseID="License ID,(B090D[...] DE8D6A1)"
Customer="Edgenexus"
.100Details="Details"

System Configuration:
[jetnexusdaemon]
AdaptivePollingEnabled=1
AddXForwardedFor=1
AdvancedW3C="HTTP Layer4"
AllowCompressedUploads=0
AllowIdentity=0
AlwaysChunk=0
ApiSessionTimeout="525600"

System Log:
18 Dec 00:28:12 jetnexus software-monitoring:
Stats|HitCount=0|InputBytes=0|OutputBytes=0|CompressedInputBytes=0|CompressedOutputBytes=0|TotalClientConnections=0|TotalServerConnections=0|CurrentConnections=0|MaximumConnections=0|RefusedConnections=0|UploadInputBytes=0|UploadOutputBytes=0|UploadCompressedInputBytes=0|UploadCompressedOutputBytes=0|TotalInputBytes=461,445,645|TotalOutputBytes=378,426,680|Memory=184,552,448|MemoryUsagePercent=10|DiskFreeSpace=19,308,112|DiskFree=98|CPUPercent=3|CPUHostPercent=0|EthernetErrors=0|Runnable=1|Processes=424|Sessions=0|NewSess=0|ExpiredSess=0|RevalidatedSess=0|BLConn=0|BLMax=5,000|BLFill=0|BLAlloc=0|BLRoom=655,360,000|BMCon=0|BMMax=5,000|BMFill=0|BMAlloc=0|BMRoom=30,000,000|BTCon=0|BTMax=10,000|BTFill=0|BTAlloc=0|BTRoom=20,000,000|BMSecure=0|CONNECTIONS=5|TIME-WAIT=0|ALLOCSOCK=134|ORPHANSOCK=0|SOCKMEM=0|ESTABLISHED=0|SYN=0|PORTS=21
18 Dec 00:29:02 jetnexus software-monitoring:

```

ロギング

システム > ログ」 ページでは、W3C ログレベルを設定し、ログを自動的にエクスポートするリモートサーバーを指定できます。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 ログの詳細

W3C ログを有効にすると、ADC は W3C 互換ログファイルの記録を開始します。W3C ログとは、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（ソース IP アドレス、HTTP バージョン、ブラウザタイプ、リファラーページ、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、ウェブの進化のための標準化を推進する組織であるワールド・ワイド・ウェブ・コンソーシアム (W3C) によって開発された。ファイルは ASCII テキストで、列はスペースで区切られている。ファイルには # で始まるコメント行があります。これらのコメント行の 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（カラム名を示す）行である。HTTP と FTP プロトコル用に別々のファイルがある。

W3C ログレベル

利用可能なロギング・レベルはさまざまで、サービスの種類によって、提供されるデータは異なる。

上の表は、W3C HTTP のロギング・レベルについて説明しています。

価値	説明
なし	W3C ログはオフです。
概要	存在するフィールドは以下の通りである：#フィールド: 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離された、よりプロセッサと互換性のあるフォーマットである。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のこと。存在するフィールドは以下の通りである：#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、追加のフィールドがあります。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参照してください。存在するフィールドは以下のとおりである：#フィールド: 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、開発およびサポート・スタッフに関連するあらゆる種類の情報が記入されています。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。現在存在す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、 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 のログレベルについて説明している。

価値	説明
概要	#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 ログを含める

このオプションでは、W3C ログに含める ADC 情報を設定できます。

価値	説明
クライアントのネットワークアドレスとポート	ここに表示される値は、実際のクライアントの IP アドレスとポートを表示します。
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 アドレスのみを表示します。
転送先アドレスとポート	このオプションは、アドレスとポートを含む、XFF ヘッダーに保持されている詳細を表示します。
転送先住所	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する。

セキュリティ情報を含む

このメニューには 2 つのオプションがある：

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、仮想サービスが認証を使用している W3C ログが有効になっている場合、ユーザー名が W3C ログに追加されません。
オフ	これは、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をオフにします。

シスログ・サーバー

▲ Syslog

Message Level: Warning

Update

このセクションでは、SYSLOG サーバーに対して実行されるメッセージ・ロギングのレベルを設定することができる。使用可能なオプションは以下のとおりである。

Error

Warning

Notice

Info

リモートシスログサーバー

▲ Remote Syslog Server

Syslog Server 1:	Remote Syslog server IP	Port:	514	TCP	Enabled: <input type="checkbox"/>
Syslog Server 2:	Remote Syslog server IP	Port:	514	TCP	Enabled: <input type="checkbox"/>

このセクションでは、すべてのシステムログを送信するために、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 アドレスを追加する。
- ポートを追加する
- TCP と UDP のどちらを使用するかを選択します。
- ログイングを開始するには、「有効」チェックボックスをオンにします。
- 更新をクリック

リモート・ログ・ストレージ

▲ Remote Log Storage

Remote Log Storage:

IP Address:

Share Name: w3c

Directory:

Username:

Password: Blank=No Change

すべての W3C ログは、1時間ごとに圧縮された形で ADC に保存されます。ディスク容量が残り 30%になると、最も古いファイルが削除されます。これら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できます。W3C ログは、ファイルが完成して圧縮されるまで、リモートの場所に転送されないことに注意してください。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最大5時間かかる可能性があります。

Col1	コル2
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ボックスにチェックを入れる
IP アドレス	SMB サーバーの IP アドレスを指定する。ドット付き 10 進数で指定します。例 : 10.1.1.23
シェア名	SMB サーバー上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。
ユーザー名	SMB 共有のユーザー名を指定します。
パスワード	SMB 共有のパスワードを指定する

フィールド概要

コンディション	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	ローカライズされていない=HH:MM:SS または HH:MM:SS.ZZZ (GMT/UTC) *注-残念ながら、これには 2 つの形式があります (サイト .ZZZ ミリ秒がない)
エクスマイル	サイトフォーマットのみ=タイムスタンプのミリ秒
シーアイピー	ネットワークまたは X-Forwarded-For ヘッダーから得られる最善のクライアント IP
シーポート	ネットワークまたは X-Forwarded-For ヘッダーから得られる最善のクライアントポート
ユーザー名	クライアントのユーザー名リクエストフィールド
エスアイピー	ALB のリスニングポート
エスポート	ALB のリスニング VIP
x-xff	X-Forwarded-For ヘッダーの値
x-xffcustom	設定された名前の X-Forwarded-For 型リクエストヘッダの値
cs ホスト	リクエストのホスト名
エクスマイルアイピー	使用するリアルサーバーの IP アドレス
X-R ポート	使用するリアルサーバーのポート
cs メソッド	HTTP リクエストメソッド * ブリーフフォーマットを除く
方法	* cs-method でこの名前を使うのは brief フォーマットだけである。
CS-URI-システム	要求されたリソースのパス。
cs-uri-query	要求されたリソースのクエリー * ただし、ブリーフ形式を除く
ウリ	* パスとクエリー文字列を組み合わせたログを出力します。
ステータス	HTTP レスポンスコード
cs(ユーザーエージェント)	ブラウザの User-Agent 文字列 (クライアントから送信されたもの)
リファラ	参照ページ (クライアントから送信されたもの)
x-c バージョン	クライアントのリクエスト HTTP バージョン
X-R バージョン	コンテンツ・サーバーのレスポンス HTTP バージョン

クスバイト	クライアントからのリクエストのバイト数
sr バイト	リアルサーバーに転送されるバイト数。
rs バイト	リアル・サーバーからのレスポンスのバイト数
スキャンバイト	レスポンスでクライアントに送信されたバイト数
X パーセント	ヘッダーを含む圧縮率 * = 100 * (1 - 出力 / 入力)
タイムテイク	リアルサーバーにかかった時間 (秒)
x-trip-times 新着情報 プコン	接続から "初心者リスト"への投稿までのミリ秒 接続してからリアルサーバーに接続するまでのミリ秒
エーコン	接続からリアルサーバーへの接続完了までのミリ秒
アールコン	接続から実サーバー接続確立までのミリ秒
rqf	接続してからクライアントから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、クライアントから最後のバイトのリクエス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	接続からリアルサーバーへのリクエストの最後のバイトを送信するまでのミリ秒
アールエスエフ	接続からリアルサーバーからのレスポンスの最初のバイトを受信するまでのミリ秒
アールエスピー	接続からリアルサーバーからの最後のレスポンスバイト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レスポンスの最後のバイトを送信するまでのミリ秒
デイス	接続から切断までのミリ秒 (双方 - 最後に切断した方)
ログ	接続からこのログレコードまでのミリ秒は、通常、次のように続く (ロードバランスポリシーと推論)。
X-ラウンド・トリップ・タイム	ALB にかかった時間 (秒)
x クローズドバイ	接続がクローズされた (またはオープンされたままであった) 原因は何か。
X 圧縮アクション	どのように圧縮が行われたか、あるいは防がれたか
x-sc(コンテンツタイプ)	レスポンスの Content-Type
x-cache-action	キャッシングがどのように反応したか、あるいは阻止されたか
エックスフィニッシュ	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

▲ Clear Log Files

Log Type:

この機能により、ADC からログファイルをクリア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タイプを選択し、[クリア] 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できます。

重要

仮想環境における仮想ネットワークインターフェースの管理

ESXi などの仮想化環境内に VM をデプロイする場合、ネットワーク・インターフェース (eth0、eth1 など) が自動的に作成され、ホスト構成のネットワーク・アダプタ (ネットワーク・アダプタ 1、ネットワーク・アダプタ 2 など) にマッピングされます。ただし、インターフェースを特定の MAC アドレスにバインドするオペレーティング・システムのルールにより、これらのマッピングが常に一貫して一致するとは限りません。このセクションでは、ユーザが VM にアクセスできないときにサービスの中断を防ぐために、ホスト上のネットワーク・インターフェースを管理する手順の概要を説明します。

主な検討事項

1. **MAC アドレスの永続性 :**
 - a. オペレーティングシステムは、名前と特定の MAC アドレスを関連付けるルールに基づいて、インターフェース名 (eth0、eth1 など) を割り当てます。
 - b. 元の MAC アドレスを再利用せずに VM ネットワーク・インターフェースを削除して再作成すると、ネットワーク・コンフィグレーションに一貫性がなくなったり、機能しなくなったりすることがあります。
2. **ADC (EdgeOS) の内部マッピング :**
 - a. 仮想ネットワーク・インターフェースは、ADC (アプリケーション・デリバリー・コントローラー) によって自動的に認識され、内部でマッピングされる。
 - b. VM ホストからネットワーク・インターフェースを削除すると、ADC に古いマッピングが残り、管理アクセスやネットワーク・サービスが中断する可能性があります。

ホスト設定の推奨手順

1. **NIC を取り外す前に**
 - a. 削除するインターフェースの MAC アドレスを記録する。これは ESXi ホストの VM の設定で確認できる。
2. **交換用 NIC を追加する場合 :**
 - a. 以前に記録した MAC アドレスを新しいネットワーク・アダプタに割り当て、VM のインターフェース・マッピングが一貫性を保つようにする。
3. **重要な NIC の誤削除を防ぐ :**
 - a. どの NIC が重要な ADC インターフェース (例えば、管理アクセス用の ETH0 (グリーンサイド)) にマッピングされているかを特定する。絶対に必要な場合を除き、これらの NIC を取り外すことは避けてください。
4. **MAC アドレスの整合性を確認する :**
 - a. VM のネットワーク・インターフェースに割り当てられた MAC アドレスが、ADC 内で予想される構成と一致していることを確認します。ESXi ホスト・ツールを使用して、このマッピングを確認します。
5. **VM 管理者との調整 :**
 - a. VM の内部構成に影響を与えるような変更が必要な場合は、VM 管理者に通知して潜在的な混乱に備え、適切なマッピングが維持されるようにする。

シナリオ例

1. 初期設定：
 - a. ADC VMには2つのNICがある：NIC1（MAC：00:11:22:33:44:55）とNIC2（MAC：00:11:22:33:44:66）である。
2. アクションNIC1を削除し、新しいNIC（NIC3）を追加する。
 - a. ESXiホストの作成時に、元のMACアドレス（00:11:22:33:44:55）をNIC3に割り当てます。
3. 影響の回避：
 - a. 元のMACアドレスを再利用することで、ADCの内部マッピング（例えば、ETH0）は一貫性を保ち、管理アクセスやネットワークサービスの中断を回避します。

仮想化環境でネットワーク・インターフェイスを管理する場合、MACアドレス割り当ての一貫性を維持することが極めて重要である。VMへのアクセスができなくなった場合、シームレスな運用を確保し、サービスの中断を防ぐために、ホスト側に必要なすべての手順を完了する必要があります。潜在的な影響に効果的に対処するために、関連する管理者と常に調整する。

重要なアプライアンスの頻繁なvMotionの回避

vMotionは、ダウンタイムなしにESXiホスト間で仮想マシン（VM）のライブマイグレーションを可能にする、VMwareの強力な機能です。しかし、vMotionはインフラストラクチャの柔軟性と可用性を維持する上で非常に有用ですが、ロードバランサーのような重要なアプライアンスを頻繁に移行することは推奨されません。

似たようなテクノロジーは他のベンダーからも提供されているかもしれないが、ここではVMwareであることを前提に話を進める。

頻繁なvMotionが推奨されない理由

1. セッションの中断
 - a. ロードバランサーは、クライアントとバックエンドサーバ間のアクティブなセッションを管理します。vMotion操作の間、ネットワーク状態が再初期化される短い期間があり、これらのセッションが中断される可能性があります。
 - b. 接続が切断されると、クライアントがセッションを再確立する必要が生じ、ユーザー・エクスペリエンスが低下する可能性がある。
2. 遅延とパケットロス：
 - a. VMを移行するプロセスでは、一時的にVMを停止し、メモリと状態を同期させる。リアルタイムのトラフィックを処理するアプライアンスでは、この一時停止によってレイテンシが発生したり、パケットロスが発生することさえある。
 - b. 低遅延レスポンスに依存するアプリケーションでは、パフォーマンスの低下やタイムアウトが発生する可能性がある。
3. リソース利用の増加：
 - a. vMotionは、ソースホストとデスティネーションホスト間のデータ同期のために、CPU、メモリ、ネットワーク帯域幅のリソースを必要とします。
 - b. 頻繁なマイグレーションはインフラリソースを圧迫し、同じ環境でホストされている他のVMやサービスに影響を与える可能性があります。
4. 高可用性構成への影響：
 - a. 高可用性（HA）構成の環境では、頻繁なvMotionがフェイルオーバーメカニズムと衝突し、予期せぬ動作やフェイルオーバー動作の遅延につながる可能性があります。
5. オペレーションの複雑さ：

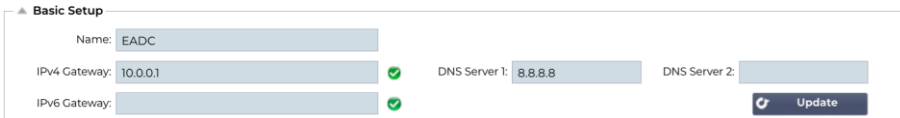
- a. クリティカルな VM を常に移動させることで、VLAN マッピングやファイアウォールルールを含むネットワークコンフィギュレーションの複雑さが増し、コンフィギュレーションエラーが発生する可能性があります。

クリティカル・アプライアンスの管理に関する推奨事項

1. メンテナンスウィンドウ中の vMotion 操作の計画
 - a. アクティブなセッションへの影響を最小限に抑えるため、トラフィックの少ない時間帯に移行をスケジュールする。
2. ロードバランサークラスタリングを実装する：
 - a. ロードバランサーにはクラスタリングまたは高可用性構成を使用して、冗長性を確保します。これにより、vMotion 操作中にトラフィックを別のノードにシームレスにリダイレクトできます。
3. インフラリソースを監視する：
 - a. リソースの競合を防ぐために、vMotion を開始する前に、十分な CPU、メモリ、およびネットワーク帯域幅が利用可能であることを確認します。
4. マイグレーションの頻度を最小限に抑える：
 - a. クリティカルなアプライアンスの vMotion は、ホストのメンテナンスや障害復旧など、絶対に必要なシナリオに限定します。
5. 本番前のテスト：
 - a. ステージング環境で vMotion 操作をテストし、アクティブなセッションへの影響を把握し、構成が最適化されていることを確認します。

vMotion は、VM 管理のための貴重なツールですが、ロードバランサーのような重要なアプライアンスに対しては、慎重に使用する必要があります。頻繁なマイグレーションは、サービスを中断させ、レイテンシを増加させ、リソースに負担をかける可能性があります。vMotion の運用を注意深く計画し、クラスタリングやメンテナンス・スケジューリングのような戦略を採用することで、信頼性の高いサービス提供を保証し、中断のリスクを最小限に抑えることができます。

基本設定



▲ Basic Setup

Name: EADC

IPv4 Gateway: 10.0.0.1 ✓ DNS Server 1: 8.8.8.8 DNS Server 2:

IPv6 Gateway: ✓ Update

ALB 名

ADC アプライアンスの名前を指定します。クラスタに複数のメンバーがいる場合、これは変更できないことに注意してください。クラスタリングのセクションを参照してください。

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、既存のアダプタと同じサブネットにある必要があります。ゲートウェイの追加に誤りがあると、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丸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、既存のアダプタと同じサブネットにある必要があります。ゲートウェイの追加に誤りがあると、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丸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 & DNS サーバー2

第一と第二（オプション）の DNS サーバーの IPv4 アドレスを追加します。

アダプター詳細

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、アダプタを追加および削除できます。

Adapter	VLAN	IP Address	Subnet Mask	Gateway	IP Filter	Description	Web Console	REST
eth0		192.168.101.2	255.255.255.0			Green side		


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、リスト行が編集モードになります。
バーチャル LAN	ダブルクリックして、アダプタの VLAN ID を追加します。VLAN は、ブロードキャストドメインを作成する仮想ローカルエリアネットワークです。VLAN は物理 LAN と同じ属性を持ちますが、エンドステーションが同じネットワークスイッチ上にない場合、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・インターフェースに関連付けられている IP アドレスを追加します。同じインターフェイスに複数の IP アドレスを追加できます。IP アドレスは、4 進ドット付き 10 進数表記の IPv4 32 ビット番号でなければなりません。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・インターフェースに割り当てられたサブネット・マスクを追加します。これは IPv4 の 32 ビット数で、4 進ドット付き 10 進表記にする必要があります。例 255.255.255.0
ゲートウェイ	インターフェースのゲートウェイを追加する。これが追加されると、ADC は、このインターフェースから開始された接続が、このインターフェースを経由して指定されたゲートウェイルーターに返されるようにするシンプル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手間を省き、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	<p>ダブルクリックして、アダプタの説明を追加します。パブリック・インターフェースの例</p> <p>注：ADC は自動的に最初のインターフェースに Green Side、2 番目のインターフェースに Red Side、3 番目のインターフェースに Side 3 等の名前を付けます。</p> <p>これらの命名規則は、ご自由に変更してください。</p>
ウェブコンソール	列をダブルクリックし、GUI Web コンソールの管理アドレスとしてインターフェイスを割り当てる場合は、ボックスにチェックを入れます。Web Console がリッスンするインターフェイスを変更する場合は、十分注意してください。変更後に Web コンソールにアクセスするには、正しいルーティングを設定するか、新しいインターフェースと同じサブネット内にある必要があります。これを元に戻す唯一の方法は、コマンドラインにアクセスして set greenside コマンドを実行することです。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「インターフェイス」セクションでは、ネットワーク・インターフェイスに関連する特定の要素を設定できます。また、[Remove] ボタンをクリックすると、一覧からネットワーク・イ

インターフェイスを削除できます。仮想アプライアンスを使用する場合、ここに表示されるインターフェイ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。

ETH Type	Status	Speed	Duplex	Bonding
eth0	UP	auto	auto	none
eth1	DOWN	auto	auto	none

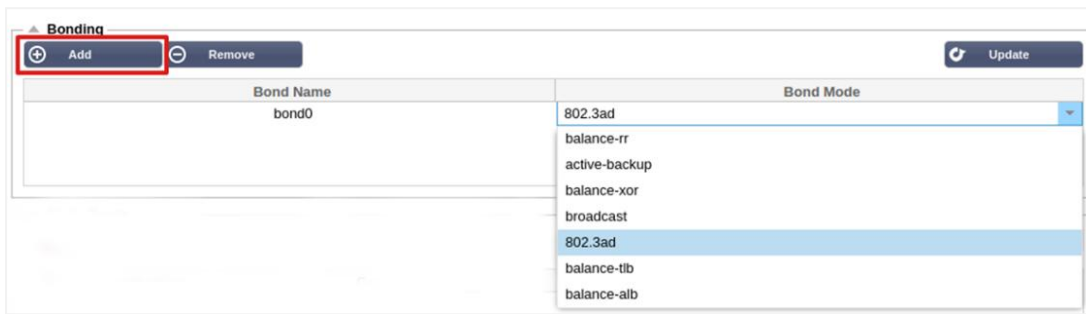
コラム	説明
ETH タイプ	この値は、ネットワーク・インターフェイスに対する OS 内部の参照を示す。このフィールドはカスタマイズできません。値は ETH0 から始まり、ネットワーク・インターフェイスの数に応じて順番に続きます。
ステータス	このグラフィカル表示は、ネットワークインターフェイスの現在のステータスを示します。緑色のステータスは、インターフェイスが接続され、起動していることを示します。その他のステータス・インジケータを以下に示します。  アダプターUP  アダプター・ダウン  アダプターを抜く  アダプター欠品
スピード	デフォルトでは、この値はオートネゴシエートスピードに設定されています。しかし、インターフェイスのネットワークスピードは、ドロップダウンで利用可能な任意の値（ 10/100/1000/AUTO ）に変更することができます。
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 （全二重）、 Half-Duplex （半二重）から選択できる。
ボンディング	定義したボンディング・タイプのいずれかを選択できる。詳細はボンディングのセクションを参照。

ボンディング

ネットワーク・インターフェイスのボンディングには、多くの名称が使われている：ポートランキング、チャンネルボンディング、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結合または集約して、シングル・チャンネル・ボンディング・インターフェイスにします。ボンディングは、2つ以上のネットワーク・インターフェイスを1つのものとして機能させ、スループットを向上させ、冗長性やフェイルオーバーを提供します。

ADC のカーネルには、複数の物理ネットワーク・インタフェースを1つの論理インタフェースにアグリゲートする（例えば、**eth0** と **eth1** を **bond0** にアグリゲートする）ための **Bonding** ドライバが組み込まれています。各ボンディング・インターフェイスに対して、モードとリンク・モニタリング・オプションを定義できます。7つの異なるモードオプションがあり、それぞれが特定のロードバランシングとフォールトトレランス特性を提供します。下図を参照してください。

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

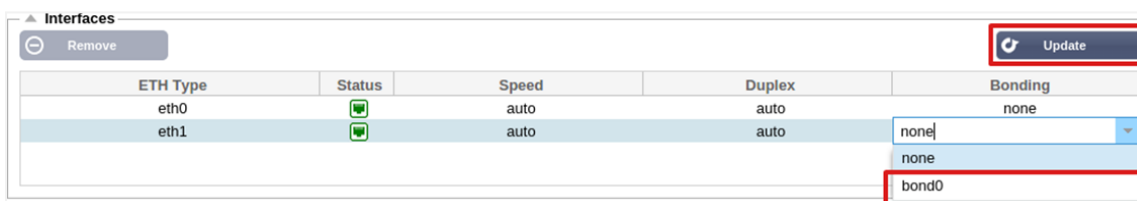


ボンディング・プロフィールの作成

- 新しいボンドを追加するには、**Add** ボタンをクリックしてください。
- ボンディング設定の名前を指定します。
- どのボンディング・モードを使用するかを選択する

次に、「**Interfaces**」セクションで、ネットワーク・インターフェイスの「**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** の一部になっている。一方、**Eth0** は管理インターフェースとして独立したままである。



ボンディング・モード

ボンディング・モード	説明
balance-rr :	パケットの送受信は、各インタフェースを通じて順次行われる。
アクティブ・バックアップ	このモードでは、1つのインターフェイスがアクティブになり、2つ目のインターフェイスはスタンバイになる。このセカンダリ・インターフェイスがアクティブになるのは、最初のインターフェイスのアクティブ接続に障害が発生した場合だけである。
balance-xor :	送信元 MAC アドレスと宛先 MAC アドレスの XOR に基づいて送信する。このオプションは、各宛先 MAC アドレスに対して同じスレーブを選択します。
を放送した :	このモードでは、すべてのスレーブ・インターフェイスのすべてのデータを送信する。
802.3ad :	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、802.3ad 仕様に従ってアクティブアグリゲータのすべてのスレーブを利用します。
balance-tlb :	アダプティブ送信負荷分散ボンディングモード：特別なスイッチサポートを必要としないチャンネルボンディングを提供する。送信トラフィックは、各スレーブの現在の負荷（速度に対して計算される）に従って分配される。現在のスレーブが着信トラフィックを受信する。受信スレーブが故障した場合、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: IPv4 トラフィックのための balance-tlb プラス受信ロードバランシング(rlb)も含まれ、特別なスイッチ・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達成される。ボンディングドライバは、ローカルシステムから送信された ARP リプライを途中でインターセプトし、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、ソー

スハードウェアアドレスを、ボンディング内のスレーブの1つのユニークなハードウェアアドレスで上書きします。

静的ルート

ネットワーク内の特定のサブネット用に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は、スタティックルートモジュールを使用してこれを行う機能を提供します。

Destination	Gateway	Mask	Adapter	Active
10.117.64	192.168.1.254	255.255.255.0	eth0	✖

静的ルートの追加

- **Add Route** ボタンをクリックします。
- 下表の詳細を参考に記入してください。
- 完了したら更新ボタンをクリックします。

フィールド	説明
目的地	宛先ネットワークアドレスを 10 進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 IPv4 アドレスを 10 進ドット表記で入力します。例 10.4.8.1
マスク	宛先サブネットマスクを 10 進ドット表記で入力します。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する。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す。赤い✖印は、そのインターフェースで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 アドレスを設定し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 に設定されたすべてのルートに関する情報を提供します。

Destination	Gateway	Mask	Flags	Metric	Ref	Use Adapter
255.255.255.255	0.0.0.0	255.255.255.255	UH	0	0	0 eth0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0 eth0
172.31.0.0	0.0.0.0	255.255.0.0	U	0	0	0 docker0
169.254.0.0	0.0.0.0	255.255.0.0	U	1002	0	0 eth0
0.0.0.0	192.168.1.254	0.0.0.0	UG	0	0	0 eth0

高度なネットワーク設定

ナグルとは?

TCP 遅延なしアルゴリズムとしても知られる **Nagle** のアルゴリズムは、ネットワーク通信で使用されるテクニックで、データの順序がずれているために再送されるパケットの数を減らすために使用される。これは、前のパケットに対する確認応答を受信していない場合、小さなパケットの送信を遅延させることで機能する。これにより、データが正しい順序で届くようになり、ネットワークの負荷が軽減される。

ナグル」に関する [WIKIPEDIA 記事を参照](#)

サーバー・ネーグル

Server Nagle 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。**Server Nagle** は、ネットワーク上で送信する必要のあるパケット数を減らすことで、**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、トランザクションのサーバー側に適用されます。**Nagle** と遅延 **ACK** はパフォーマンスに深刻な影響を与える可能性があるため、サーバー設定には注意が必要です。

クライアント・ネイグル

Client Nagle 設定を有効にするには、チェックボックスをオンにします。上記と同じですが、トランザクションのクライアント側に適用されます。

SNAT



SNAT 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る。**EdgeADC** の **SNAT** を簡単に説明すると、次のようになる。

通常、インバウンドリクエストはリクエストのソース **IP** を見る **VIP** に向けられる。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** の場合、これは **VIP** に見える。

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る。したがって、**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る。

フィールド	説明
ソース IP	ソース 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。マスクは、ネットワークマスクか、ネットワークマスクの左側の 1 の数を指定するプレーンな数値のどちらかである。したがって、/24 のマスクは 255.255.255.0 に相当する。
宛先 IP	宛先 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します。マスクは、ネットワークマスクか、ネットワークマスクの左側の 1 の数を指定するプレーンな数値のいずれかを指定することができます。したがって、/24 のマスクは 255.255.255.0 に相当する。
ソースポート	送信元ポートはオプションで、 1 つの数字にすることもでき、その場合はそのポートのみを指定し、コロンを含めることもでき、その場合はポートの範囲を指定する。例 80 または 5900:5905 。
目的地ポート	宛先ポートはオプションで、 1 つの数字にすることもでき、その場合はそのポートのみを指定し、コロンを含む場合はポートの範囲を指定する。例 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。より正確を期すために、具体的に指定することをお勧めします。
SNAT から IP へ	SNAT to IP は、必須 IP アドレスまたは IP アドレスの範囲です。例 10.0.0.1 または 10.0.0.1-10.0.0.3 。
ポートへの SNAT	SNAT to Port はオプションであり、単一の数値を指定することもでき、その場合はそのポートのみを指定し、ダッシュを含む場合はポートの範囲を指定する。例 80 または 5900-5905 。

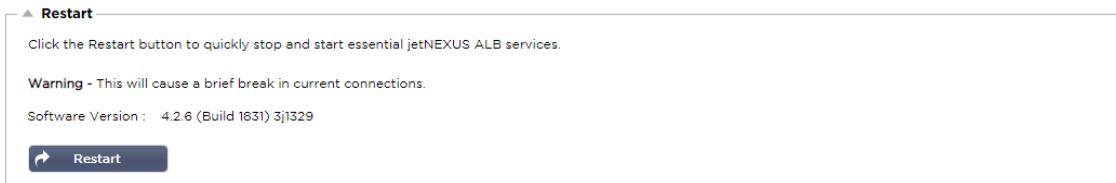
備考

なぜそのルールが存在するのかを思い出させるために、親しみやすい名前を付ける場合に使用する。これは **Syslog** でデバッグするときにも便利です。

パワー

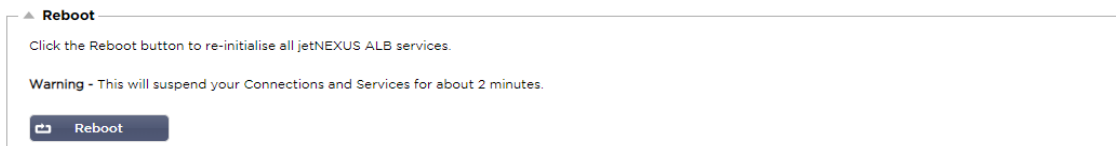
この ADC システム機能により、ADC 上でいくつかの電力関連タスクを実行することもできます。

リスタート



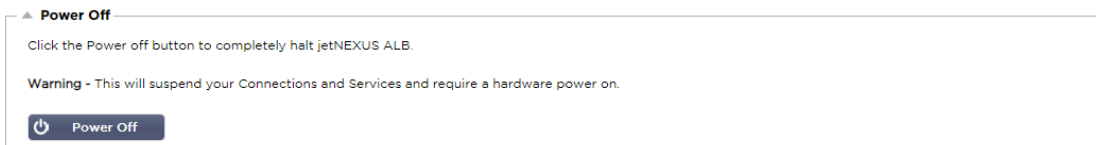
この設定により、すべてのサービスのグローバルな再起動が開始され、その結果、現在アクティブな接続がすべて切断されます。しばらくするとすべてのサービスが自動的に再開されますが、そのタイミングは設定されているサービスの数によって異なります。再起動の確認を求めるポップアップが表示されます。

リブート



Reboot（再起動）ボタンをクリックすると、ADC の電源が切断され、自動的にアクティブ状態に戻ります。リブート動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。これがハードウェア・アプライアンスである場合、電源を再投入するにはデバイスに物理的にアクセスする必要があります。シャットダウン操作の確認を要求す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、Web コンソールのパスワードを変更し、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

▲ SSH
Secure Shell Remote Conn:

オプション	説明
セキュア・シェル・リモート・コン	SSH を使用して ADC にアクセスしたい場合は、このボックスにチェックを入れてください。「Putty」はこれを行うための優れたアプリケーションです。

認証サービス

▲ Authentication Service

Authentication Mode: Remote Then Local

Authentication Source:

ALB GUI Admin Groups:

ALB GUI Read/Write Groups:

ALB GUI Read-Only Groups:

ほとんどの組織では、ADC の管理インタフェースへのアクセスは、企業独自の認証サービスを介して行う必要があるという要件がある。

このようなシナリオのために、ここで説明する認証サービス機能を提供した。この機能は、ローカル・ディレクトリ・サービスだけでなく、SAML などの外部サービスでも動作する。

オプション	説明
認証モード	Local Only : これはデフォルトのモードで、ADC 内のローカルデータベースを使用します。 リモート]、[ローカル] の順に選択します : ADC は、[認証ソース] フィールドで指定されたリモート認証サーバに対して、ユーザの検証を試みます。成功しなかった場合は、検証のソースとしてローカルデータベースを使用します。
認証ソース	このドロップダウンメニューでは、「ライブラリ」>「認証」で定義した認証サーバーのいずれかを選択できます。
ALB GUI 管理者グループ	許可する管理者グループを指定します。
ALB GUI 読み書きグループ	許可された Read/Write グループを指定する
ALB GUI 読み取り専用グループ	読み取り専用グループを指定します。

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イ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** セクションからインポートできます。

オプション	説明
セキュアポート	ウェブコンソールのデフォルトポートは TCP 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、ここで変更できます。

REST API

REST API は、RESTful API としても知られ、REST アーキテクチャ・スタイルに準拠し、ADC の設定や ADC からのデータ抽出を可能にするアプリケーション・プログラミング・インターフェースである。REST という用語は **representational state transfer** の略で、コンピュータ科学者の **Roy Fielding** 氏が考案した。

オプション	説明
REST を有効にする	REST API を使用した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。REST を有効にするアダプタも設定する必要があることに注意してください。以下の Cog リンクの注意を参照してください。
SSL 証明書	REST サービス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 サービスが関連付けられている IP アドレスが表示されます。Cog のリンクをクリックして Network ページにアクセスし、REST サービスが有効になっているアダプタを変更できます。
Cog リンク	このリンクをクリックすると Network ページが表示され、REST 用のアダプタを設定できます。

REST API のドキュメント

REST API の使用方法については、[jetAPI | 4.2.3](#) | [jetNEXUS](#) | [SwaggerHub](#) のドキュメントを参照してください。

注意: *Swagger* ページでエラーが表示される場合は、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** に移動する。

例

CURL を使用した **GUID**:

- 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 は 24 時間有効

ライセンス詳細

- コマンド

```
curl -k https://<休憩 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 を設定することができます。MIB は、SNMP を装備したデバイスと通信できるサードパーティ製ソフトウェアによって照会できます。

SNMP 設定

オプション	説明
SNMP v1 / V2C	チェックボックスをオンにすると、V1/V2C MIB が有効になります。 SNMP v1 は RFC-1157 に準拠しています。SNMP V2c は RFC-1901-1908 に準拠します。
SNMP v3	チェックボックスをオンにすると、V3 MIB が有効になります。RFC-3411-3418 を参照してください。 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	これはエージェントに設定された読み取り専用の文字列で、マネージャが SNMP 情報を取得するために使用します。デフォルトのコミュニティ文字列は jetnexus です。
パスフレーズ	これは、SNMP v3 が有効になっているときに必要なパスワードで、少なくとも 8 文字以上で、Aa~Zz のアルファベットと 0~9 の数字のみを含むものでなければなりません。デフォルトのパスフレーズは jetnexus です。

SNMP MIB

SNMP で閲覧可能な情報は、管理情報ベース (MIB) によって定義される。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 [ここから](#) ダウンロードできる :

ADC OID

ルート OID

```
ISO.org.dod.internet.private.enterprise = .1.3.6.1.4.1
```

OID について

```
.38370 ジェットネクスMIB
.1 jetnexusData (1.3.6.1.4.1.38370.1)
.1.1 jetnexusGlobal (1.3.6.1.4.1.38370.1.1)
.1.2 jetnexusVirtualServices (1.3.6.1.4.1.38370.1.2)
.1.3 jetnexusServers (1.3.6.1.4.1.38370.1.3)
.1.1 jetnexusGlobal (1.3.6.1.4.1.38370.1.1)
.1.1.1 jetnexusOverallInputBytes (1.3.6.1.4.1.38370.1.1.1.0)
.1.1.2 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)

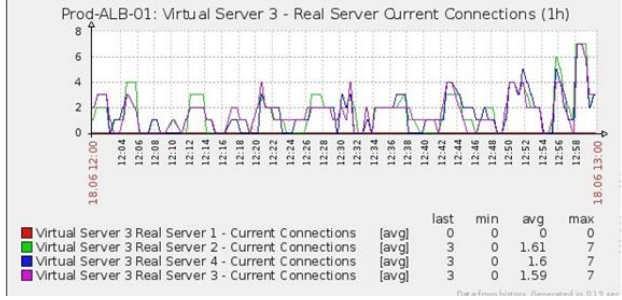
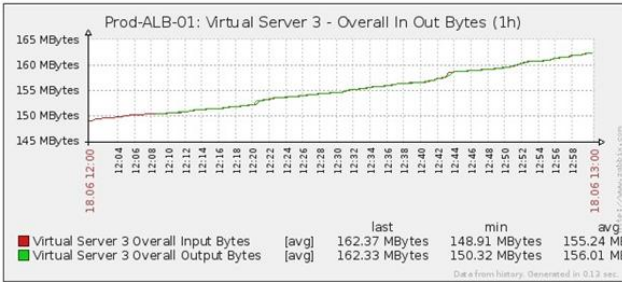
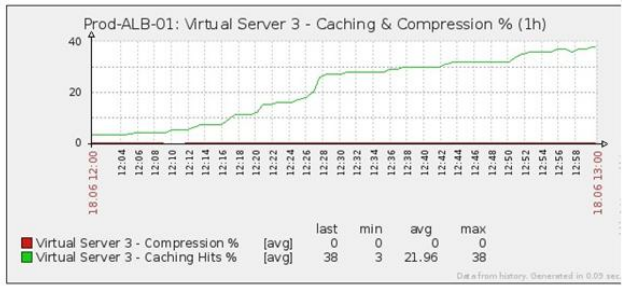
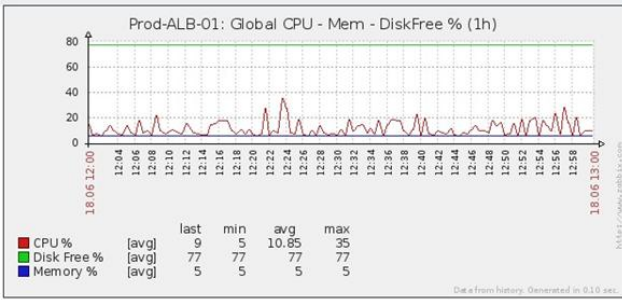
- .2 **jetnexusVirtualServices** (1.3.6.1.4.1.38370.1.2)
 - .1 **jnvirtualseviceEntry** (1.3.6.1.4.1.38370.1.2.1)
 - .1 **jnvirtualseviceIndexvirtualsevice** (1.3.6.1.4.1.38370.1.2.1.1)
 - .2 **jnvirtualseviceVSAddrPort** (1.3.6.1.4.1.38370.1.2.1.2)
 - .3 **jnvirtualseviceOverallInputBytes** (1.3.6.1.4.1.38370.1.2.1.3)
 - .4 **jnvirtualseviceOverallOutputBytes** (1.3.6.1.4.1.38370.1.2.1.4)
 - .5 **jnvirtualseviceCacheBytes** (1.3.6.1.4.1.38370.1.2.1.5)
 - .6 **jnvirtualseviceCompressionPercent** (1.3.6.1.4.1.38370.1.2.1.6)
 - .7 **jnvirtualsevicePresentClientConnections** (1.3.6.1.4.1.38370.1.2.1.7)
 - .8 **jnvirtualseviceHitCount** (1.3.6.1.4.1.38370.1.2.1.8)
 - .9 **jnvirtualseviceCacheHits** (1.3.6.1.4.1.38370.1.2.1.9)
 - .10 **jnvirtualseviceCacheHitsPercent** (1.3.6.1.4.1.38370.1.2.1.10)
 - .11 **jnvirtualseviceVSStatus** (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 の最適な使用法は、履歴グラフを任意の管理コンソールにオフロードする機能です。下記は、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。

EdgeADC - 管理ガイド



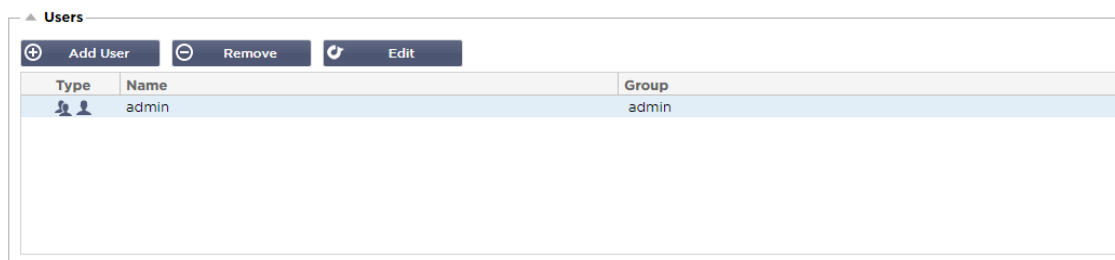
ユーザーと監査ログ

ADC は、ADC が何を行うかを設定および定義するために、内部ユーザーセットを持つ機能を提供する。ADC 内で定義されたユーザは、そのユーザに割り当てられた役割に応じて、さまざまな操作を実行できる。

ADC を最初に設定するとき使用する **admin** というデフォルトの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

Users セクションは、ADC からユーザーを作成、編集、削除するために提供されます。



ユーザー追加

The screenshot shows the 'Add User' dialog box. It has a title bar 'Users' and a blue header. The form contains the following fields and options:




- Username: [text input field]
- New Password: [password input field with strength indicator]
- Confirm Password: [password input field with strength indicator]
- Group Membership: Admin
- GUI Read Write
- GUI Read
- SSH
- API
- Add-Ons

At the bottom, there are two buttons: 'Update' and 'Cancel'.

上図の **Add User** ボタンをクリックし、**Add User** ダイアログを表示します。

パラメータ	説明/用途
ユーザー名	<p>お好きなユーザー名を入力してください。 ユーザーネームは以下に従わなければならない：</p> <ul style="list-style-type: none"> 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よい。 数字を使うこともできる。 記号は使用不可
パスワード	<p>以下の条件を満たす強力なパスワードを入力してください。</p> <ul style="list-style-type: none"> 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が必要。 文字は大文字でも小文字でもよい。 以下の例を除き、記号は使用できます。 £, %, &, <, >
パスワードの確認	パスワードが正しいことを再度確認する。
団体会員	<p>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。</p> <ul style="list-style-type: none"> 管理者 - このグループは何でもできる。 GUI Read Write - このグループのユーザーは GUI にアクセスし、GUI 経由で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表示することのみができます。変更はできません。 SSH - このグループのユーザーは、Secure Shell 経由で ADC にアクセスできます。この選択により、利用可能なコマンドの最小セットがあるコマンドラインにアクセスできるようになります。 API - このグループのユーザーは、SOAP と REST のプログラム可能なインターフェー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 から利用可能になります。 アドオン - アドオン設定へのアクセス許可が付与されます。

ユーザータイプ

	<p>ローカルユーザー</p> <p>スタンドアロンまたはマニュアル H/A ロールの ADC は、ローカルユーザーのみを作成します。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である。後方互換性のため、このユーザーは決してできない。 このユーザーのパスワードを変更したり、したりすることはできますが、最後のローカル管理者を削除することはできません。</p>
	<p>クラスタユーザー</p> <p>クラスタの ADC ロールはクラスタ・ユーザーのみを作成します。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・ユーザーへの変更は、クラスタの全メンバーに反映されます。クラスタユーザとしてログオンしている場合、クラスタから手動またはスタンドアロンにロールを切り替えることはできません。</p>
	<p>クラスタとローカルユーザー</p> <p>スタンドアロンまたはマニュアル・ロールの間に作成されたユーザは、クラスタにコピーされません。 ADC がその後クラスタから離脱した場合、ローカルユーザのみが残ります。最後に設定されたパスワードが有効となる。</p>

ユーザーの削除

- 既存のユーザーをハイライトする。
- 削除をクリックする。
- 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。
- 管理者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。
- 管理者グループに残ったクラスタユーザを削除することはできません。
- 後方互換性のため、管理ユーザーを削除することはできません。
- ADC をクラスタから削除すると、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

- 既存のユーザーをハイライトする。
- 編集をクリック
- 該当するボックスにチェックを入れて更新することで、ユーザーのグループメンバーシップを変更することができます。
- 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

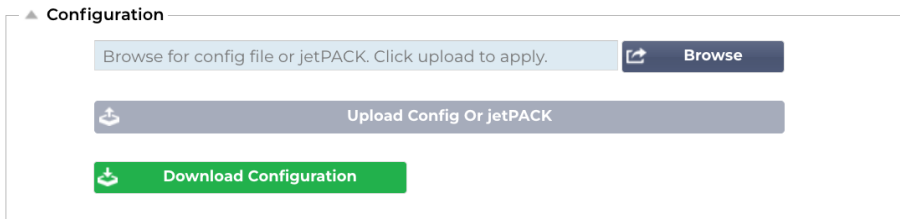
ADC は、個々のユーザーによって ADC 設定に加えられた変更をログに記録します。監査ログは、すべてのユーザーによって実行された最後の 50 のアクションを提供します。また、[\[ログ\]](#) セクションにすべてのエントリが表示されることもあります。例えば

Date/Time	Username	Section	Action
09:49:01 Fri 15 Dec 2023	admin	warning	Passwords must have 6 or more characters
09:49:01 Fri 15 Dec 2023	admin	import certificate [Jet2]	
09:48:15 Fri 15 Dec 2023	admin	error	Failed to create local certificate
09:48:14 Fri 15 Dec 2023	admin	Cert	Create
15:17:44 Thu 14 Dec 2023	admin	IP Services	Deleted: virtual service: :
15:17:44 Thu 14 Dec 2023	admin	IP Services	Deleted: virtual service: (Web Sites 443)
15:17:40 Thu 14 Dec 2023	admin	IP Services	Deleted: virtual service: 10.0.0.130:80 (Web Sites)

View Download

上級

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 の構成をダウンロードして保存することが常にベスト・プラクティスです。コンフィギュレーション・モジュールを使用して、コンフィギュレーション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。

Jetpacks は標準的なアプリケーションの設定ファイルで、Edgenexus から提供され、作業を簡素化します。これらも Configuration モジュールを使用して 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るため、メモ帳++、Nano、VI などのテキストエディタを使用して編集することができます。必要に応じて編集したら、設定ファイルを ADC にアップロードすることができます。

注意：

EdgeADC のコンフィギュレーションファイルの編集は、訓練を受けた専門家のみを対象としています。万が一、お客様ご自身で設定ファイルを編集され、技術的な問題が発生した場合、Edgenexus テクニカルサポートでは製品のサポートができなくなります。

設定のダウンロード

- 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。
- .conf ファイルを開くか保存するかを尋ねるポップアップが表示されます。
- 便利な場所に保存する。
- メモ帳++などのテキストエディタで開くことができる。

設定のアップロード

- 保存された設定ファイルをアップロードするには、保存された .conf ファイルを参照します。
- Upload Config or Jetpack」 ボタンをクリックします。
- ADC が設定をアップロードして適用し、ブラウザを更新します。ブラウザが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、ダッシュボードページにリダイレクトされます。

重要：Edgenexusサポートに事前に相談することなく、1つのADCから別のADCに設定をコピーしようとしませんが重要です。そうすることで、ADCが回復不可能になる可能性があります。

ジェットパックのアップロード

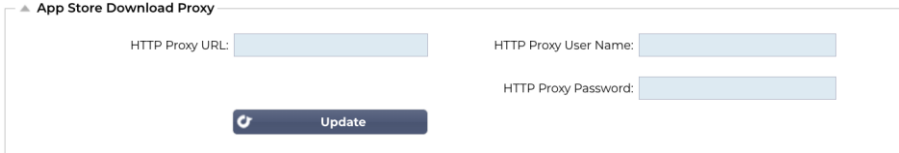
- JetPACK は、既存のコンフィギュレーションに対するコンフィギュレーション更新のセットである。
- JetPACK は、TCP タイムアウト値を変更するような小さなものから、Microsoft Exchange や Microsoft Lync のような完全なアプリケーション固有のコンフィギュレーションまで可能です。
 - JetPACK は、本ガイドの最後にあるサポートポータルから入手できます。
- jetPACK.txt ファイルを参照する。
- アップロードをクリックする。

- アップロード後、ブラウザは自動的に更新されます。
- 完了すると、ダッシュボードページにリダイレクトされます。
- **Microsoft Lync** など、より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

グローバル設定セクションでは、SSL 暗号ライブラリを含む様々な要素を変更することができます。

App Store ダウンロードプロキシ



セキュリティで保護されたネットワークでは通常、組織のプロキシサーバーを経由してデータを送信しない限り、インターネットへのアクセスが許可されません。EdgeADC は境界デバイスであり、サポートの有効性を確認したり、App Store にアクセスしてアップデートやアプリケーションをダウンロードしたりするために、Edgenexus のサーバーにアクセスできる必要があります。

HTTP プロキシ URL

このフィールドは、プロキシサーバーのホスト名または IP アドレスを指定するために使用します。

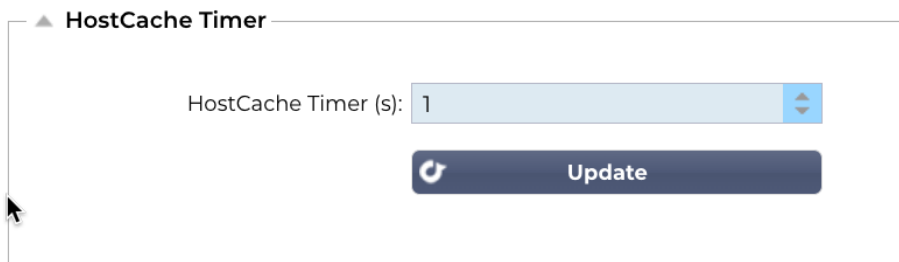
HTTP プロキシのユーザー名

プロキシサーバーを使用するデバイスやユーザーを認証するために使用するユーザー名を入力します。

HTTP プロキシパスワード

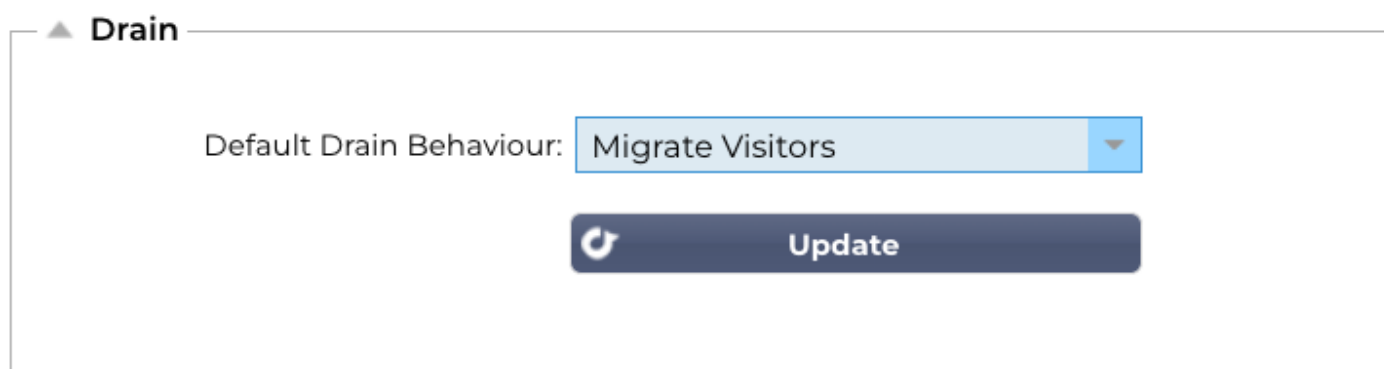
HTTP プロキシ Username で指定されたユーザー名は保護されたものになります。このフィールドに関連するパスワードを入力する必要があります。

ホストキャッシュタイマー



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が使用されている場合に、リアルサーバーの IP アドレスを一定期間保存する設定です。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。この値をゼロに設定すると、キャッシュがフラッシュされなくなります。この設定に最大値はありません。

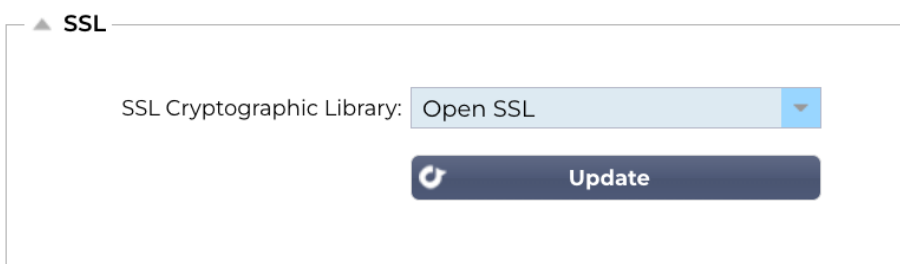
ドレイン



リアルサーバをドレインモードにするときは常に、送信されるトラフィックの動作を制御できる方がよいでしょう。**Drain Behaviour** メニューでは仮想サービスごとにトラフィックの動作を選択できます。オプションは以下の通りです：

オプション	説明
パーシステンス・ドリブン	これはデフォルトの選択である。 ユーザが永続性セッションを使用して訪問するたびに、そのセッションは拡張される。 24 時間使用すれば、ドレインが発生しない可能性もある。 しかし、実サーバーへの接続数が 0 になった場合、ドレインは終了し、永続セッションは削除され、すべての訪問者は次の接続でバランスを取り直す。
訪問者の移行	再接続時に永続セッションが無視される - (2022 年以前のレガシーな動作) 新しい TCP 接続は（既存のセッションの一部であるかどうかにかかわらず）、常にオンラインのリアルサーバーに対して行われる。 永続化セッションが消耗している実サーバーに対するものであった場合、それは上書きされる。 仮想サービスは新しい接続の永続性を実質的に無視し、新しいサーバーに負荷分散されます。
引退セッション	永続的なセッションは延長されない。 着信したユーザー接続は、希望するサーバーに割り当てられるが、永続セッションは延長されない。そのため、永続セッション時間を超えると、新しい接続として扱われ、別のサーバに移動します。

SSL



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

認証

▲ **Authentication**

Authentication Server Timeout (s):

Update

この値は認証のタイムアウト値を設定するもので、これを過ぎると認証は失敗したとみなされる。

フェイルオーバー設定

▲ **Failover Setting**

VIP Failover Behaviour:

Update

ADC のクラスタ化セットが作成されると、仮想サービスのフェイルオーバー方法を指定する 2 つの方法があります。

オプション	説明
あらゆるサービス	このオプションを選択すると、VIP 内のいずれかのサービスに障害が発生した場合、その仮想サービスを含む VIP 全体 がクラスタパートナーにフェイルオーバーされます。例えば、VIP 10.0.100.101 があり、各仮想サービスがポート 443、8080、4399、2020 などを使用しているとします。これらのサブサービスのいずれかに障害が発生すると、VIP 全体がフェイルオーバーします。
すべてのサービス	このオプションを選択すると、1 つ以上のサブサービスに障害が発生しても、VIP は現在のクラスタメンバーに残ります。 すべてのサービス に障害が発生した場合のみ、VIP はクラスタパートナーにフェイルオーバーされます。これは、ある特定のサービスを無効にしたいが、VIP をフェイルオーバーさせたくない場合に便利です。

プロトコル

Protocol セクションは、HTTP プロトコルに関する多くの詳細設定を行う。

サーバーがビジー状態

リアルサーバーへの最大接続数を制限しているとします。この制限に達すると、フレンドリーなウェブ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シンプルなウェブ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もできます。また、ウェブページに画像を使いたい場合は、インラインで **base64** エンコードされた画像を使用してください。
- 新しく作成したウェブページの **HTM(L)** ファイルを参照します。
- アップロードをクリック
- ページをプレビューしたい場合は、ここ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事実上の標準である。

フォワード・フォア出力

オプション	説明
オフ	ADC は Forwarded-For ヘッダーを変更しない。
アドレスとポートの追加	この選択により、ADC に接続されているデバイスまたはクライアントの IP アドレスとポートが、 Forwarded-For ヘッダーに追加される。
アドレスの追加	この選択により、ADC に接続されているデバイスまたはクライアントの IP アドレスが、 Forwarded-For ヘッダーに追加される。
アドレスとポートの置換	この選択は、 Forwarded-For ヘッダーの値を、ADC に接続されたデバイス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。
アドレスの置換	この選択は、 Forwarded-For ヘッダーの値を、ADC に接続されているデバイスまたはクライアントの IP アドレスに置き換える。

転送用ヘッダー

このフィールドでは、**Forwarded-For** ヘッダーに与えられる名前を指定できる。通常、これは "**X-Forwarded-For**" ですが、環境によっては変更されるかもしれません。

IIS の高度なログ - カスタムログ

IIS Advanced logging 64-bit アプリをインストールすると、X-Forwarded-For 情報を取得できます。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。

カテゴリ]リストから[ソースタイプ]リストから[デフォルト]を選択し、[ソース名]ボックスで[要求ヘッダー]を選択し、「X-Forwarded-For」と入力する。

[HTTP://www.iis.net/learn/extensions/advanced-logging-module/advanced-logging-for-iis-custom-logging](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 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 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たいでしょう。

変更点は以下の通り：

タイプ	価値
ログフォーマット：	<code>"%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{ユーザエージェント}i\" combined</code>
ログフォーマット：	<code>"%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b \"%{Referer}i\". \"%{User-Agent}i\" proxy SetEnvIf X- Forwarded-For \"^.*</code>
カスタムログ	<code>"logs/access_log "を組み合わせた env=!forwarded</code>
カスタムログ	<code>「logs/access_log "プロキシ env=forwarded</code>

この書式は、環境変数に基づいた条件付きロギングの Apache の組み込みサポートを利用します。

- 行目は、デフォルトの標準的な複合ログのフォーマット文字列である。
- 2行目は、%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を "proxy" に設定する。
- 行目は環境変数 "forwarded" の設定で、IP アドレスにマッチする緩い正規表現を含んでいる。
- また、3行目はこうも読める：「X-Forwarded-For 値があれば、それを使いなさい。
- 4行目と5行目は、どのログパターンを使うかを Apache に指示する。X-Forwarded-For 値が存在する場合は "proxy" パターンを使い、そうでない場合はリクエストに対して "combined" パターンを使います。読みやすくするために、4行目と5行目は Apache の rotate logs (piped) ログ機能を利用していませんが、ほとんどのすべての人が使っていると仮定します。

これらの変更により、リクエストごとに IP アドレスが記録されることになる。

HTTP 圧縮設定

▲ HTTP Compression Settings

Initial Thread Memory [KB]:

Maximum Thread Memory [KB]:

Increment Memory [KB]:
(0 to double)

Minimum Compression Size [Bytes]:

Safe Mode:

Disable Compression:

Compress As You Go:

圧縮はアクセラレーション機能であり、IP サービスページで各サービスごとに有効になります。

警告 - 不適切な設定は ADC の性能に悪影響を及ぼす可能性があるため、これらの設定を調整する際には細心の注意を払ってください。

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量です。最も効率的なパフォーマンスのために、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非圧縮 HTML ファイルをちょうど超える値に設定されるべきです。
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ある。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に保存し、圧縮します。この量を超える非常に大きなコンテンツファイルが処理される場合、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、より多くのメモリが必要な場合に、Initial Thread Memory Allocation に追加されるメモリ量を設定する。デフォルト設定はゼロ。これは、ADC が、データが現在の割り当てを超えたときに、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、割り当てを 2 倍にすることを意味します (例えば、128Kb、次に 256Kb、次に 512Kb など)。これは、ページの大部分は同じサイズであるが、たまに大きなファイルがある場合に効率的である。(例：ページの大部分は 128Kb 以下だが、たまに 1Mb のサイズのレスポンスがある) 大きな可変サイズのファイルが存在するシナリオでは、重要なサイズの線形インクリメントを設定する方が効率的です(例えば、レスポンスのサイズが 2Mb から 10Mb の場合、1Mb の初期設定と 1Mb のインクリメントがより効率的です)。
最小圧縮サイズ [バイト]	この値は、ADC が圧縮を試みないサイズをバイト数で表したものである。200 バイトを大きく下回ると圧縮がうまくいかず、圧縮ヘッダのオーバーヘッドによってサイズが大きくなる可能性があるため、この値は有用である。
セーフモード	ADC が JavaScript のスタイル・シート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 が圧縮されたコンテンツを処理できる個々のブラウザを認識しているにもかかわらず、HTTP/1.1 に準拠していると主張する他のプロキシ・サーバの中には、圧縮されたスタイル・シートや JavaScript を正しく転送できないものがあるからです。プロキシサーバーを経由してスタイルシートや 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、コンテンツの圧縮量は全体的に減少します。
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、このチェックボックスをオンにします。
圧縮しながら進む	<p>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で圧縮します。</p> <p>OFF - このページでは Compress As You Go を使用しません。</p> <p>By Page Request - ページ要求によって Compress as You Go を使用します。</p>

グローバル圧縮除外

除外リストに追加された拡張子を持つページは圧縮されません。

- 個々のファイル名を入力する。
- アップデートをクリックする。
- ファイルタイプを追加したい場合は、すべてのカスケーディング・スタイル・シートを除外するために「*.css」と入力してください。
- 各ファイルまたはファイルタイプは新しい行に追加する。

永続性クッキー


この設定により、Persistence Cookie の処理方法を指定できます。

フィールド	説明
クック属性	<p>なし：すべてのクッキーはスクリプトからアクセス可能</p> <p>緩い：クッキーは、サイト間でアクセスされることを防ぎますが、サイトが訪問された場合、アクセスできるように保存され、所有するサイトに送信されます。</p> <p>厳密：異なるサイトのクッキーがアクセスまたは保存されるのを防ぎます。</p> <p>オフ：ブラウザのデフォルト動作に戻る</p>
セキュア	このチェックボックスをオンにすると、セキュアなトラフィックにパーシステンスが適用されます。
HTTP のみ	チェックを入れると、HTTP トラフィックに対してのみ Persistent Cookies を許可します。

UDP タイムアウトリセット

▲ UDP Timeout Reset

UDP Timeout Reset On:

 Update

UDP タイムアウトリセットは、UDP (User Datagram Protocol) セッションに関連するタイムアウトを再開するネットワーク通信で使用されるメカニズムである。リセットはセッションをアクティブに維持するのに役立ち、中断のない継続的なデータフローを保証します。

オプション	説明
両方	サーバーとクライアント両方の UDP タイムアウトをリセットする。
サーバー	サーバーの UDP タイムアウトをリセットする。
クライアント	クライアントの UDP タイムアウトをリセットする。

ソフトウェア

ソフトウェア・セクションでは、ADC のコンフィギュレーションとファームウェアをアップデートできます。

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、インターネットに接続している場合に入力されます。ブラウザがインターネットにリンクしていない場合、このセクションは空白になります。接続が完了すると、以下のバナーメッセージが表示されます。

We have successfully connected to Cloud Services Manager to retrieve your Software Update Details

以下の「クラウドからダウンロード」のセクションには、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には、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：

- 高度な--トラブルシューティング--Ping
- IP アドレス - App Store.edgenexus.io
- Ping をクリック
- その結果、"ping: unknown host App Store.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ない。

クラウドからダウンロード

Code Name	Release Date	Version	Build	Release Notes	Notes
ALB-X Version 4.2.6	2020-Apr-15	4.2.6	1826	Click here for release notes. This is our latest release 4.2.6. This APP will only w	
ALB-X Version 4.2.4 Safe Rollback	2022-Aug-05	4.2.4	jetNEXUS	Use this safe 1764 roll-back, not s	Use this safe 1764 roll-back, not software stored o
OWASP Core Rule Set 3.3.4 Update for Edgenexus Ap	2023-Feb-09	3.3.4_20.01.2023	Edgenexus	The OWASP CRS is a set of web a	The OWASP CRS is a set of web application firew
ADC Version 4.2.10 Software Update	2023-Oct-27	4.2.10	1961	Release notes	EdgeADC version 4.2.10 software update Offling f

ブラウザがインターネットに接続されていれば、クラウドで利用可能なソフトウェアの詳細が表示される。

- 興味のある行をハイライトし、「選択したソフトウェアを ALB にダウンロード」ボタンをクリックします。
- 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、以下の「ALB に保存されているソフトウェアを適用する」セクションで適用できます。

注： ADC が直接インターネットにアクセスできない場合、以下のようなエラーが表示されます：

ダウンロードエラー、ALB が build1734-3236-v4.2.1-Sprint2-update-64.software.alb の ADC クラウドサービスにアクセスできません。

ネットワークがプロキシサーバーで保護されている場合は、App Store ダウンロードプロキシ をご覧ください。

ソフトウェアのアップロード

▲ Upload Software

Software Version: 4.3.0 (Build 1965) c50631

Browse for software file then click upload to apply.

アプリのアップロード

▲ Upload Software

Software Version: 4.3.0 (Build 1965) c50631

Browse for software file then click upload to apply.

<apptime> .<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できます。

- アプリには5つのタイプがある
 - <アプリ名>flightpath.alb
 - <アプリ名>.monitor.alb
 - <アプリ名>.jetpack.alb
 - <アプリ名>.addons.alb
 - <アプリ名>.featurepack.alb
- アップロードされると、各アプリは「ライブラリ」>「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アプリを個別にデプロイする必要があります。

ソフトウェア / ファームウェア ・ アップデート

▲ Upload Software To ALB

Software Version: 4.2.6 (Build 1831) 3j1329

Browse for software file then click upload to apply.

- 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ます。
- ソフトウェアファイルは<softwarename>.software.alb です。
- その後、"ALBに保存されているソフトウェア"セクションに表示され、そこから自分の都合に合わせて適用することができます。

ADC に保存されたソフトウェアを適用

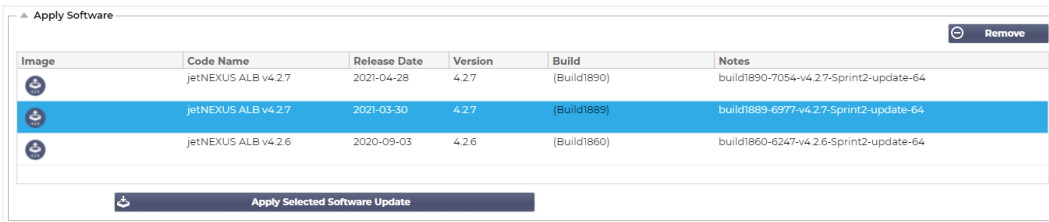


Image	Code Name	Release Date	Version	Build	Notes
	jeNEXUS.ALB v4.2.7	2021-04-28	4.2.7	(Build1890)	build1890-7054-v4.2.7-Sprint2-update-64
	jeNEXUS.ALB v4.2.7	2021-03-30	4.2.7	(Build1889)	build1889-6977-v4.2.7-Sprint2-update-64
	jeNEXUS.ALB v4.2.6	2020-09-03	4.2.6	(Build1860)	build1860-6247-v4.2.6-Sprint2-update-64

このセクションには、ALB に保存され、配備可能なすべてのソフトウェアファイルが表示されます。リストには、更新された Web Application Firewall (WAF) 署名が含まれます。

- 使用するソフトウェアの行をハイライトします。
- 選択したソフトウェアを適用」をクリックする
- ALB ソフトウェアアップデートの場合、アップロード後、ALB を再起動して適用されますのでご注意ください。
- 適用するアップデートが OWASP シグネチャのアップデートであれば、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を必要とする問題は常に存在する。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

▲ Support Files

Time Frame: 7 days

Download Support Files

ADCに問題があり、サポートチケットを開く必要がある場合、テクニカルサポートはADCアプライアンスから複数の異なるファイルを要求することがよくあります。これらのファイルは現在、1つの.datファイルに集約されており、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枠を選択します：3日、7日、14日、全日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。サポートチケットの詳細は、このドキュメントの最後に記載されています。
- 必ず問題を詳しく説明し、.dat ファイルをチケットに添付してください。

トレース

▲ Trace

Nodes To Trace: Your IP

Connections:

Cache:

Data:

Authentication:

flightPATH: No flightPATH trace

Server Monitoring:

Monitoring Unreachable:

Auto-Stop Records: 1000000

Auto-Stop Duration: 00:10:00

Purpose:

Start

Download

Clear

Full results can be obtained using download.

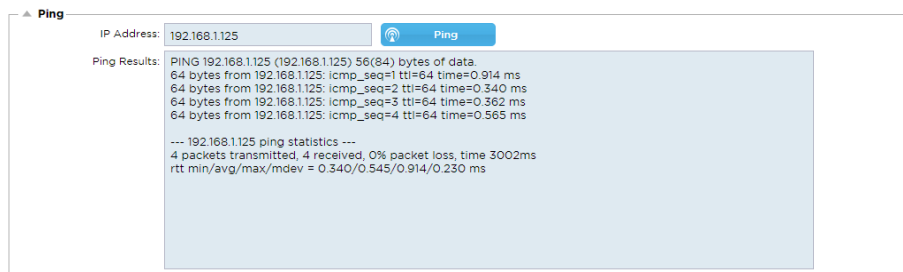
トレースセクションでは、問題のデバッグを可能にする情報を調べることができます。提供される情報は、ドロップダウンとチェックボックスから選択したオプションによって異なります。

オプション	説明
トレースするノード	<p>Your IP : GUIにアクセスしているIPアドレスを使用するように出力をフィルタリングします（モニタリングはADCインターフェース・アドレスを使用するため、モニタリング用にこのオプションを選択しないでください）。</p> <p>All IP : フィルターは適用されません。ビジー状態のボックスでは、これが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。</p>

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によって入出力される生のデータ・バイトが含まれます。
フライトパス	flightPATH メニューでは、監視する特定の 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マニターとそれぞれの結果が表示されます。
監視不能	このオプションを選択すると、失敗したモニターだけが表示され、これらのメッセージのフィルターとして機能することを除けば、動作はサーバーモニターとよく似ています。
オートストップ記録	デフォルト値は 1,000,000 レコードで、その後 Trace 機能は自動的に停止する。この設定は、Trace が誤ってオンのままになって ADC の性能に影響を与えるのを防ぐための安全予防措置である。
自動停止時間	デフォルト時間は 10 分に設定され、その後 Trace 機能は自動的に停止する。この機能は、Trace が誤ってオンのままになって ADC の性能に影響を与えるのを防ぐための安全予防措置である。
スタート	トレース機能を手動で開始するには、これをクリックします。
ストップ	クリックすると、自動記録または時間に達する前にトレース機能を手動で停止します。
ダウンロード	右側にライブビューアが表示されますが、情報が表示されるのが早すぎるかもしれません。その代わりに、Trace.log をダウンロードすることで、その日の様々なトレース中に収集されたすべての情報を見ることができます。この機能は、トレース情報のフィルタリングされたリストです。前の日のトレース情報を見たい場合は、その日の Syslog をダウンロードできますが、手動でフィルタリングする必要があります。
クリア	トレースログをクリアする

ピン

Ping ツールを使って、インフラ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チェックできます。



テストしたいホストの IP アドレスを入力します。例えば、ドット付き 10 進数表記を使ったデフォルトゲートウェイや IPv6 アドレスなどです。Ping ボタンを押してから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 サーバーを設定した場合は、完全修飾ドメイン名を入力できます。DNS サーバーは、**DNS サーバー 1** および **DNS サーバー 2** のセクションで設定できます。「Ping」ボタンを押すと、結果がフィードバックされるまで数秒待つ必要があります。

キャプチャ


▲ Capture

Adapter: ▼

Packets: ▲▼

Duration[Sec]: ▲▼

Address: 🏠

 Generate

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。

- フォームのオプションを入力してください。
- 「生成」をクリックする。
- キャプチャが実行されると、ブラウザがポップアップ表示され、ファイルの保存場所を尋ねられます。形式は "jetNEXUS.cap.gz" です。
- 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。サポートチケットの詳細は、このドキュメントの最後に記載されています。
- 必ず問題を詳細に説明し、ファイルをチケットに添付してください。
- また、Wireshark を使用してコンテンツを表示することもできます。

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する。また、"any" ですべてのインターフェイスをキャプチャすることもできる。
パケット	この値は、キャプチャするパケットの最大数である。通常、99999
期間	キャプチャを実行する最大時間を選択します。一般的な時間は、トラフィックの多いサイトでは 15 秒です。キャプチャ時間中は GUI にアクセスできなくなります。
住所	この値は、ボックスに入力された IP アドレスに対してフィルタリングを行います。フィルタしない場合は空白のままにします。

パフォーマンスを維持するため、ダウンロードファイルは **10MB** に制限しています。必要なデータをすべて取り込むには十分でないと思われる場合は、この数値を増やすことも可能です。

注：これは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。

ヘルプ

ヘルプセクションでは、**Edgenexus** に関する情報へのアクセスや、ユーザーガイド、その他の役立つ情報へのアクセスを提供します。

会社概要

会社概要をクリックすると、エドジェネクスとその本社に関する情報が表示されます。

About Us

EDGENEXUS

Edgenexus ADC(TM)

4.3.0 (Build 1965) c50631

Copyright © 2005-2020 Edgenexus Limited. All Rights Reserved.

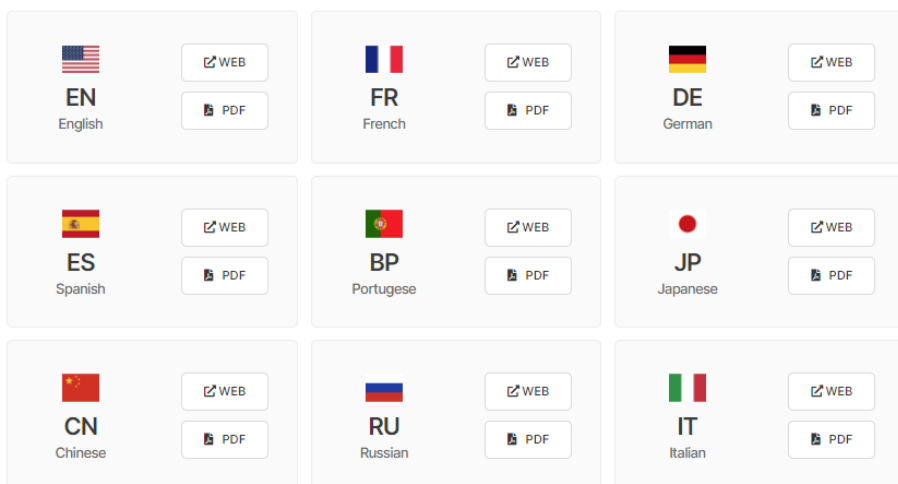
Edgenexus Limited.
Jubilee House,
Third Avenue,
Marlow
SL7 1YW

www.edgenexus.io/support/

Some elements of the SSL subsystem are open source.

参考

リファレンス・オプションを選択すると、ユーザーガイドおよびその他の有用な文書を含むウェブページが開きます。このウェブページは、<https://www.edgenexus.io/documentation>。



お探しのものが見つからない場合は、support@edgenexus.io までご連絡ください。

ジェットパック

Edgenexus jetPACK s

jetPACK は、特定のアプリケーション用に 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享受するために必要な、すべてのアプリケーション固有の設定で事前に構成され、完全に調整されています。jetPACK の中には、トラフィックを操作するために flightPATH を使用するものがあり、この要素を動作させるには flightPATH 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は、[ライセンス](#) ページをご覧ください。

jetPACK のダウンロード

- 以下の各 jetPACK は、jetPACK のタイトルに含まれる一意の仮想 IP アドレスで作成されています。例えば、以下の最初の jetPACK の仮想 IP アドレスは 1.1.1.1 です。
- この 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、メモ帳++などのテキストエディタで jetPACK を編集し、1.1.1.1 を検索して仮想 IP アドレスに置き換えます。
- さらに、各 jetPACK には、IP アドレスが 127.1.1.1 と 127.2.2.2 の 2 つのリアルサーバーが作成されています。この場合も、アップロード後に GUI で変更するか、メモ帳++を使用して事前に変更することができます。
- 以下の jetPACK リンクをクリックし、jetPACK-VIP-Application.txt ファイルとして保存してください。

マイクロソフト エクスチェンジ

申し込み	ダウンロード リンク	何をするのですか？	何が含まれますか？
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ための flightPATH ルールが含まれていますが、これはオプションです。flightPATH のライセンスを持っていない場合でも、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 モニターモニター：Outlook ウェブアプリのレイヤー7 モニター、クライアントアクセスサービスのレイヤー4 アウトオブバンドモニター 仮想サービス IP：1.1.1.1 仮想サービスポート 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する。
	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 の SMTP サービスを追加します。SMTP サーバーは ALB-X インターフェースのアドレスを送信元 IP 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：Outlook ウェブアプリのレイヤー7 モニター。クライアント・アクセス・サービスのレイヤー4 アウトオブバンド・モニター 仮想サービス IP：1.1.1.1 仮想サービスポート 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する。
	jetPACK-1.1.1.3-Exchange-	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	グローバル設定：サービスタイムアウト 2 時間

	2010-SMTP-DSR	、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。	モニター : Outlook ウェブアプリのレイヤー7 モニター。クライアント・アクセス・サービスのレイヤー4 アウトオブバンド・モニター 仮想サービス IP : 1.1.1.1 仮想サービスポート 80, 443, 135, 59534, 59535, 25 (サーバー直通) 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する。
Exchange 2013	jetPACK-2.2.2.1-Exchange-2013-Low-Resource	このセットアップでは、1つのVIPとHTTPと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は最小になります。 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をチェックすることも可能だ	グローバル設定 : モニターOWA、EWS、OA、EAS、ECP、OAB、ADSのレイヤー7モニター 仮想サービス IP : 2.2.2.1 仮想サービスポート 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する。
	jetPACK-2.2.3.1-Exchange-2013-Med-Resource	このセットアップ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.edgenexus.com、ews.edgenexus.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 仮想サービスポート 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する。
	jetPACK-2.2.2.3-Exchange2013-High-Resource	この jetPACK は、1つの一意のIPアドレスと、異なるポート上の複数の仮想サービスを追加します。flightPATHは、その後、正しい仮想サービスへの宛先パスに基づいてコンテキストを切り替えます。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 : 2.2.2.3 仮想サービスポート 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する。

Microsoft Lync 2010/2013

リバースプロキシ	フロントエンド	エッジ内部	エッジ外部
jetPACK-3.3.3.1-Lync-Reverse-Proxy	jetPACK-3.3.3.2-Lync-Front-終了	jetPACK-3.3.3-Lync-Edge-Internal	jetPACK-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 の再暗号化	SSL パススルー
jetPACK-4.4.4.1-Web-HTTP	jetPACK-4.4.4.2-Web-SSL-オフロード	jetPACK-4.4.4.3-Web-SSL-Re-Encryption	jetPACK-4.4.4-Web-SSL-パススルー

マイクロソフト リモートデスクトップ

ノーマル

[jetPACK-5.5.5.1-Remote-Desktop](#)

DICOM - 医学におけるデジタル画像と通信

通常の HTTP

[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

[ジェットパック-7.7.7.1-オラクル EBS](#)

VMware Horizon View

接続サーバー - SSL オフロード

[jetPACK-8.8.8.1-View-SSL-Offload](#)

セキュリティ・サーバー - SSL 再暗号化

[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 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。この設定により、この要求が 1 日に増えます。
- ARP Refresh 10 - HA アプライアンス間のフェイルオーバー時に、この設定により、移行中のスイッチを支援するために、**Gratuitous ARP** の数を増やす。
- キャプチャサイズ 16MB - デフォルトのキャプチャサイズは 2MB です。この値では最大 16MB まで増加します。

サイファー s と サイファー jetPACKs

EdgeADC には、ベストプラクティスの暗号が標準搭載されています。これらの暗号はそれぞれの TLS プロトコルと連動しているため、ユーザーはより簡単に利用できます。

必要であれば、追加の暗号セットを提供します。

強力な暗号

暗号オプションリストから「強力な暗号」を選択する機能を追加：

```
ALL:RC4+RSA:+RC4:+HIGH:!DES-CBC3-SHA:!SSLv2:!ADH:!EXP:!ADHexport:IMD5
```

アンチ・ビースト

暗号オプションリストから "Anti Beast "を選択する機能を追加：

```
ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4:HIGH:IMD5:!aNULL:!EDH
```

SSLv3 なし

暗号オプションリストから「SSLv3 なし」を選択する機能を追加：

```
ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
```

SSLv3 なし TLSv1 なし RC4 なし

暗号オプションリストから「No-TLSv1 No-SSLv3 No-RC4」を選択できるようにした：

```
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」を選択する機能を追加：

```
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
```

TLS-1.0-1.1 暗号を有効にする

ビルド 4.2.10 以降では、プロトコル TLS1.0 および TLS1.1 の Cipher サポートは廃止されました。しかし、一部の顧客はこれらの古いレガシーなプロトコルを内部サーバーで使用し続けています。以下のサイファアでは、TLS v1.0 および TLS v1.1 を有効にする機能が追加されています。

```
aes128-sha:aes256-sha:des-cbc-sha:des-cbc3-sha:exp-des-cbc-sha:rc4-sha:rc4-md5:dhe-rsa-aes128-sha:dhe-rsa-aes256-sha : EDH-RSA-DES-CBC-SHA:EDH-RSA-DES-CBC3-SHA:EXP-EDH-RSA-DES-CBC-SHA:EXP-RC2-CBC-MD5:AES128-SHA256:AES256-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-DSS-AES128-SHA256:DHE-DSS-AES256-SHA256:DHE-DSS-AES128-GCM-SHA256:DHE-DSS-AES256-GCM-SHA384:AES:ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
```

暗号例 jetPACK

暗号は、jetPACK を使用して ADC にインポートされる。jetPACK は、ADC が認識するパラメータを含むシンプルなテキストファイルです。以下の例では、Enable TLS-1.0-1.1 Cipher を使用した jetPACK を示しています。

```
#更新
```

```
[jetnexusdaemon-cipher-TLS1-0-TLS-1-1]
```

```
暗号="AES128-SHA:AES256-SHA:DES-CBC-SHA:DES-CBC3-SHA:EXP-DES-CBC-SHA:RC4-SHA:RC4-MD5:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA : EDH-RSA-DES-CBC-SHA:EDH-RSA-DES-CBC3-SHA:EXP-EDH-RSA-DES-CBC-SHA:EXP-RC2-CBC-MD5:AES128-SHA256:AES256-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-DSS-AES128-SHA256:DHE-DSS-AES256-SHA256:DHE-DSS-AES128-GCM-SHA256:DHE-DSS-AES256-GCM-SHA384:AES:ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM"
```

```
Cipher1=""
```

```
サイファア2=""
```

```
CipherOptions="-NO_TLSv1.0 -NO_TLSv1.1 -NO_TLSv1.2 -NO_TLSv1"
```

```
説明=" TLS v1.0 - v1.1 有効"
```

- **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 - ブラウザーが自動的に "MIME-Sniffing" するのを防ぐ。
- **X-Frame-Options** - このヘッダー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上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 - ブラウザのクロスサイト・スクリプティング保護を有効にする。

- Strict-Transport-Security - ヘッダーが存在しない場合は追加し、"max-age=31536000 ; includeSubdomains" に設定する。

jetPACK の適用

どの jetPACK をどの順番で適用しても構いませんが、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。この操作を行うと、コンフィギュレーション内で IP アドレスが重複してしまいます。間違っこの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 > ソフトウェアのアップデート
- コンフィギュレーション・セクション
- 新しい設定または jetPACK をアップロードする
- 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、ダッシュボードのページが表示されるまでお待ちください。

jetPACK の作成

jetPACK の素晴らしい点の 1 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場合があります。

- まず、既存の ALB-X から現在の設定をコピーします。
 - 上級
 - ソフトウェアの更新
 - 現在の設定をダウンロードする
- このファイルをメモ帳++で編集する
- 新しい txt ドキュメントを開き、"yourname-jetPACK1.txt" とする。
- コンフィグファイルから関連するセクションをすべて "yourname-jetPACK1.txt" にコピーする。
- 完了したら保存する

重要：各 jetPACK は異なるセクションに分かれています。すべての jetPACK はページの一番上に #!jetpack がなければなりません。

編集／コピーを推奨する箇所は以下の通り。

第 0 節

#ジェットパック

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

第 1 節

[ジェットネクサスデーモン]

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。Web コンソールから変更できる設定もありますが、ここでしか変更できない設定もあります。

例を挙げよう:

```
ConnectionTimeout=600000
```

この例は、ミリ秒単位の TCP タイムアウト値です。この設定は、TCP コネクションが 10 分間使用されないとクローズされることを意味します。

```
ContentServerCustomTimer=20000
```

この例は、DICOM のような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間のミリ秒単位の遅延です。

```
jnCookieHeader="MS-WSMAN"
```

この例では、永続的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 "に変更する。この特定の変更は、Lync 2010/2013 のリバースプロキシに必要です。

第 2 節

[jetnexusdaemon-Csm-Rules]を参照してください。

このセクションには、通常ウェブコンソールから設定するカスタムサーバー監視ルールが含まれます。

例

```
[jetnexusdaemon-Csm-Rules-0]。
コンテンツ="サーバーアップ"
Desc="モニター1
メソッド="CheckResponse"
Name="ヘルスチェック-サーバーの稼働状況"
URL="HTTP://demo.jetneus.com/healthcheck/healthcheck.html"
```

第 3 節

[jetnexusdaemon-LocalInterface]。

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る。各インターフェイスには番号が振られ、各チャンネルのサブインターフェイスが含まれます。チャンネルに flightPATH ルールが適用されている場合、Path セクションも含まれます。

例

```
[jetnexusdaemon-LocalInterface1]。
1.1="443"
1.2="104"
1.3="80"
1.4="81"
有効=1
Netmask="255.255.255.0"
PrimaryV2="{A28B2C99-1FFC-4A7C-AAD9-A55C32A9E913}"
[jetnexusdaemon-LocalInterface1.1]。
1=">,""セキュアグループ"",2000,""
2="192.168.101.11:80,Y,""IISのWWWサーバー1""
3="192.168.101.12:80,Y,""IISのWWWサーバー2""
AddressResolution=0
キャッシュポート=0
```

```

CertificateName="デフォルト"
ClientCertificateName="No SSL"
圧縮=1
接続制限=0
DSR=0
DSRProto="tcp"
有効=1
LoadBalancePolicy="CookieBased"
MaxConnections=10000
モニタリングポリシー="1"
パススルー=0
プロトコル="HTTPの高速化"
ServiceDesc="セキュアサーバーVIP"
SNAT=0
SSL=1
SSLClient=0
SSL内部ポート=27400
[jetnexusdaemon-LocalInterface1.1-Path]。
1="6"
第4節
[jetnexusdaemon-Path]

```

このセクションは全ての **flightPATH** ルールを含む。数字は、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らない。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る。

例

```

[jetnexusdaemon-Path-6]。
Desc="特定のディレクトリでHTTPSを強制的に使用する"
Name="ゲイリー - HTTPSを強制"
[jetnexusdaemon-Path-6-Condition-1]。
Check="contain"
条件="/パス"
マッチ
センス="する"
値="/secure/"
[jetnexusdaemon-Path-6-Evaluate-1]。
詳細
ソース="ホスト"
バリュー
変数="$host$"[jetnexusdaemon-Path-6-Function-1]。
Action="リダイレクト"
ターゲット="HTTPS://$host$$path$$querystring$"

```


バリュー

フライトパス

flightPATHの紹介

flightPATH とは?

flightPATH は Edgenexus が開発したインテリジェントなルールエンジンで、HTTP と HTTPS のトラフィックを操作し、ルーティングします。高度な設定が可能で、非常にパワフルでありながら、非常に使いやすくなっています。

flightPATH のいくつか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(s)と同じレイヤ 7 サービスタイプにのみ適用できます。他のサービスタイプを選択した場合、IP Services の flightPATH タブは空白になります。

flightPATH は何ができるのか?

flightPATH は、着信および発信 HTTP(s)コンテンツとリクエストを変更するために使用することができます。

例えば "Starts with "や "Ends With "のような単純な文字列マッチを使うだけでなく、強力な Perl 互換の正規表現 (RegEx) を使った完全な制御も実装できる。

RegEx の詳細については、こちらのお役立ちサイトをご覧ください。

さらに、評価セクションでカスタム変数を作成し、アクションエリアで使用することで、さまざまな可能性が広がります。

flightPATH ルールには 3 つの要素がある :

オプション	説明
詳細	flightPATH を追加または削除し、利用可能なものをリストアップするために使用します。
コンディション	flightPATH ルールをトリガーする複数の条件を設定する。
評価	アクションエリアで使用できる変数の使用を許可する。
アクション	ルールがトリガーされた後の動作。

コンディション

このセクションでは、コンディションに適用される 5 つのパラメータを指定することができる。以下に各オプションの説明と例を示す。

コンディション	説明	例
<form>	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 "フォームの長さが 0 でない"
ゲオ所在地	これは、ソース IP アドレスと ISO 3166 国コードを比較します。	ゲオの所在地が GB である OR ゲオの所在地がドイツである
ホスト	これは URL から抽出されたホストである。	www.mywebsite.com または 192.168.1.1
言語	これは、language HTTP ヘッダーから抽出された Language である。	この条件は、言語のリストをドロップダウンメニューに表示します。

EdgeADC - 管理ガイド

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	アップストリームプロキシが 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 またはサブネットを使用することもできます。 は 10.1.2.0 /24 サブネット 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である。	/mywebsite/index.asp
ポスト	POST リクエストメソッド	ウェブサイトにアップロードされるデータのチェック
クエリー	これはクエリーの名前と値であり、クエリー名または値を受け取ることができます。	「Best=edgeNEXUS" マッチが Best で値が edgeNEXUS の場合
クエリー文字列	文字以降のクエリー文字列全体	
リクエストクッキー	クライアントが要求したクッキーの名前。	MS-WSMAN=afYfn1CDqqCDqUD: :
リクエスト・ヘッダ	HTTP ヘッダ	Referrer、User-Agent、From、Date
リクエスト・バージョン	これは HTTP バージョンです。	http/1.0 または http/1.1
回答本文	レスポンス・ボディのユーザー定義文字列	サーバーアップ
レスポンスコード	レスポンスの HTTP コード	200 OK, 304 Not Modified
レスポンス・クッキー	これはサーバーから送られるクッキーの名前である。	MS-WSMAN=afYfn1CDqqCDqUD: :
レスポンス・ヘッダ	HTTP ヘッダ	Referrer、User-Agent、From、Date
レスポンス・バージョン	サーバーが送信した HTTP バージョン	http/1.0 または http/1.1
ソース IP	これは、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ある。	クライアント IP、プロキシ IP、ファイアウォール IP。複数の IP やサブネットを使用することもできます。この場合ドットは RegEX なのでエスケープする必要があります。例 10.1.1.2.3 は 10.1.2.3

試合

Match パラメーターは、Condition パラメーターの値によって文脈が変化します。

試合	説明	例
受け入れる	許容されるコンテンツ・タイプ	アクセプト: text/plain
Accept-Encoding	使用可能なエンコーディング	Accept-Encoding: <compress gzip deflate sdch identity>.
受諾言語	対応可能な言語	受諾言語: ja-US

EdgeADC - 管理ガイド

アクセプト・レンジ	このサーバーがサポートする部分コンテンツ範囲タイプ	許容範囲：バイト
認可	HTTP 認証の認証情報	認証ベーシック QWxhZGRpbjpvGcGVuIHNIc2FtZQ==
チャージ・トゥ	要求された方法の適用にかかる費用の勘定情報を含む。	
コンテンツエンコーディング	データに使われているエンコーディングの種類。	コンテンツ・エンコーディング：gzip
コンテンツ長	オクテット（8 ビットバイト）単位のレスポンスボディの長さ	コンテンツ長: 348
コンテンツタイプ	リクエスト本文の MIME タイプ（POST および PUT リクエストで使用される）	Content-Type: application/x-www-form-urlencoded
クッキー	Set-Cookie（下記）でサーバーが以前に送信した HTTP クッキー。	Cookie: \$Version=1; Skin=new ;
日付	メッセージが発信された日時	日付 = "日付" ":" HTTP 日付
イータグ	リソースの特定のバージョンを示す識別子で、メッセージダイジェストであることが多い。	ETag : "aed6bdb8e090cd1:0"
より	リクエストを行うユーザーのメールアドレス	From: user@example.com
変更後	コンテンツが変更されていない場合、304 Not Modified が返されるようにする。	更新日時: Sat, 29 Oct 1994 19:43:31 GMT
最終更新日	リクエストされたオブジェクトの最終更新日（RFC 2822 形式）	最終更新日火曜日, 15 11 月 1994 12:45:26 GMT
プラグマ	Implementation-specific ヘッダーは、リクエストと応答の連鎖のどこかで、様々な効果を持つかもしれない。	プラグマ：no-cache
紹介者	これは、現在要求されているページへのリンクがたどられた前のウェブページのアドレスである。	リファラー：HTTP://www.edgenexus.io
サーバー	サーバー名	サーバー Apache/2.4.1 (Unix)
セットクッキー	HTTP クッキー	Set-Cookie : UserID=JohnDoe; Max-Age=3600; Version=1
ユーザーエージェント	ユーザーエージェントの文字列	ユーザーエージェント Mozilla/5.0 (互換性あり; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
可変	ダウンストリームのプロキシに、将来のリクエストヘッダをどのようにマッチさせるかを指示する。 キャッシュされたレスポンスが使用可能かどうかを決定する。 を決定します。	値を変更します：ユーザーエージェント
X-Powered-By	ウェブアプリケーションをサポートするテクノロジー（ASP.NET、PHP、JBoss など）を指定します。	X-Powered-By : PHP/5.4.0

チェック

チェック	説明	例
存在する	これは状態の詳細を気にするものではなく、ただそれが存在する／しないだけである。	ホスト >> 存在する
スタート	文字列は値	Path> Does> Start /secure>
終了	文字列の最後は値	パス> Does> End> .jpg
コンティン	文字列は値を含む	リクエストヘッダ> Accept> Does> Contain> Image
イコール	文字列は値と等しい	ホスト> Does> Equal> www.edgenexus.io
長さがある	文字列は値の長さを持つ	ホスト >> は長さがあるか> 16 www.edgenexus.io = TRUE www.edgenexus.com = FALSE
エクシード・レンジス	値が指定された長さを超えるか超えないかをチェックする。	パス > ドーズ > 長さ超過 - 10
マッチ 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.
マッチリスト	PIPE () で区切られた、照合可能な値のリストを指定できます。	ソース IP > Does > マッチリスト > 10.0.0.1 10.0.0.100 192.178.28.32

例

Condition	Match	Sense	Check	Value
Request Header	image	Does	Contain	image
Host	www.imagepool.com	Does	Equal	www.imagepool.com

- この例には2つの条件があり、アクションを実行するには**両方**を満たさなければならない。
- まず、リクエストされたオブジェクトが画像であるかどうかをチェックする。
- つ目は、特定のホスト名をチェックすることである。

評価

Variable	Source	Detail	Value
\$variable1\$	Select a New Source	Select or Type a New Detail	Type a New Value

変数を追加することはリクエストからデータを抽出してアクションで利用することを可能にする魅力的な機能です。たとえば、セキュリティ問題がある場合、ユーザーユーザー名をログに記録したり、Eメールを送信したりできます。

- 変数：これは、\$記号で始まり、\$記号で終わらなければならない。例えば \$variable1\$ のように。
- 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する。Source=Request Header の場合、Detail は User-Agent になります。

- 値：テキストまたは正規表現を入力して、変数を微調整する。

組み込み変数:

- ビルトイン変数はすでにハードコーディングされているので、評価エントリーを作成する必要はありません。
- あなたのアクションには、以下のどの変数も使用できます。
- 各変数の説明は、上記の「コンディション」の表にある。
 - メソッド = \$method\$
 - パス = \$path\$
 - クエリストリング = \$querystring\$
 - ソース ip = \$sourceip\$
 - レスポンスコード (テキストは「200 OK」も含む) = \$resp\$
 - ホスト = \$host\$
 - バージョン = \$version\$
 - クライアントポート = \$clientport\$
 - クライアントチップ = \$clientip\$
 - ジオロケーション = \$ジオロケーション\$"

アクションの例:

- 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。

説明する:

- 存在しないページにアクセスしたクライアントは、通常ブラウザに 404 ページが表示されます。
- この例では、ユーザーは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 ページ" というエントリーが追加される。

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ある。	MS-WSMAN=afYfn1CDqqCDqUD::ここで、名前は MS-WSMAN であり、値は afYfn1CDqqCDqUD: である :
ホスト	これは URL から抽出されたホスト名である。	www.mywebsite.com または 192.168.1.1
言語	これは、Language HTTP ヘッダーから抽出された言語です。	この条件は、言語のリストをドロップダウンメニューに表示します。
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である。	/mywebsite/index.html
ポスト	POST リクエストメソッド	ウェブサイトにアップロードされるデータのチェック

EdgeADC - 管理ガイド

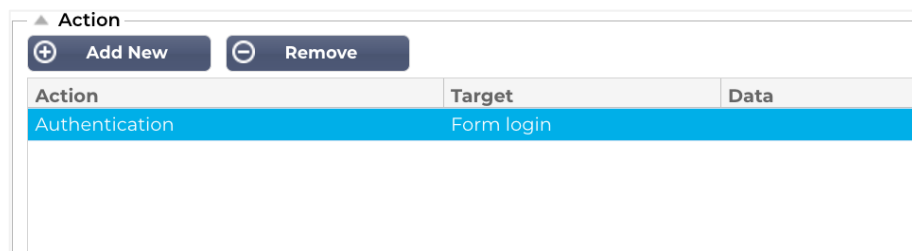
クエリ項目	これはクエリの名前と値です。そのため、クエリ名または値を受け取ることができます。	「Best=jetNEXUS" マッチが Best で値が edgeNEXUS の場合
クエリー文字列	これは、?文字の後の文字列全体である。	HTTP://server/path/program?query_string
リクエスト・ヘッダ	クライアントが送信するヘッダであれば何でもよい。	Referrer、User-Agent、From、Date...
レスポンス・ヘッダ	これはサーバーから送られるヘッダであれば何でもよい。	Referrer、User-Agent、From、Date...
バージョン	これは HTTP バージョンです。	HTTP/1.0 または HTTP/1.1

詳細	説明	例
受け入れる	許容されるコンテンツ・タイプ	アクセプト : text/plain
Accept-Encoding	使用可能なエンコーディング	Accept-Encoding: <compress gzip deflate sdch identity>.
受諾言語	対応可能な言語	受諾言語: ja-US
アクセプト・レンジ	このサーバーがサポートする部分コンテンツ範囲タイプ	許容範囲 : バイト
認可	HTTP 認証の認証情報	認証ベーシック QWxhZGRpbjpvYVUuHnlc2FtZQ==
チャージ・トゥ	要求された方法の適用にかかる費用の勘定情報を含む。	
コンテンツエンコーディング	データに使われているエンコーディングの種類。	コンテンツ・エンコーディング : gzip
コンテンツ長	オクテット (8 ビットバイト) 単位のレスポンスボディの長さ	コンテンツ長: 348
コンテンツタイプ	リクエスト本文の MIME タイプ (POST および PUT リクエストで使用される)	Content-Type: application/x-www-form-urlencoded
クッキー	Set-Cookie (下記) でサーバーが以前に送信した HTTP クッキー。	Cookie: \$Version=1; Skin=new ;
日付	メッセージの発信日時 メッセージの発信時刻	日付 = "日付" ":" HTTP 日付
イータグ	リソースの特定のバージョンを示す識別子で、メッセージダイジェストであることが多い。	ETag : "aed6bdb8e090cd1:0"
より	リクエストを行うユーザーのメールアドレス	From: user@example.com
変更後	コンテンツが変更されていない場合、304 Not Modified が返されることを許可する。	更新日時: Sat, 29 Oct 1994 19:43:31 GMT
最終更新日	リクエストされたオブジェクトの最終更新日 (RFC 2822 形式)	最終更新日火曜日, 15 11 月 1994 12:45:26 GMT
プラグマ	リクエストと応答の連鎖のどこかでさまざまな効果を持つかもしれない、実装固有のヘッダ。	プラグマ : no-cache

紹介者	これは、現在要求されているページへのリンクがたどられた前のウェブページのアドレスである。	リファラー : HTTP://www.edgenexus.io
サーバー	サーバー名	サーバー Apache/2.4.1 (Unix)
セットクッキー	HTTP クッキー	Set-Cookie : UserID=JohnDoe; Max-Age=3600; Version=1
ユーザーエージェント	ユーザーエージェントの文字列	ユーザーエージェント Mozilla/5.0 (互換性あり; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
可変	下流のプロキシに 下流のプロキシに、将来のリクエストヘッダをどのようにマッチさせて キャッシュされたレスポンスが使用可能かどうかを決定する。 を決定します。	値を変更します : ユーザーエージェント
X-Powered-By	ウェブアプリケーションをサポートするテクノロジー (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ある。



アクション

「アクション」列をダブルクリックしてドロップダウンリストを表示する。

ターゲット

「Target」列をダブルクリックしてドロップダウンリストを表示する。リストはアクションによって変わります。

いくつかのアクションを手動で入力することもできる。

データ

「Data」列をダブルクリックして、追加または置換したいデータを手動で追加する。

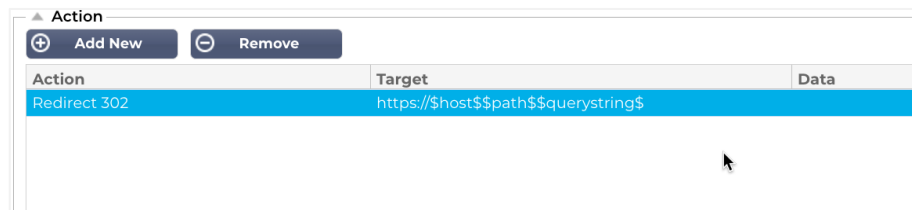
全アクションの詳細は以下の通り :

アクション	説明	例
リクエストクッキーの追加	Target セクションに詳細なリクエストクッキーを、Data セクションに値を追加する。	ターゲット=クッキー Data= MS-WSMAN=afYfn1CDqqCDqCVii

リクエストヘッダーを追加	Data セクションに値を持つ Target タイプのリクエストヘッダーを追加する。	ターゲット=受け入れる データ= image/png
レスポンス・クッキーの追加	レスポンス・クッキーの詳細をターゲット・セクションに追加し、データ・セクションに値を追加する。	ターゲット=クッキー Data= MS-WSMAN=afYfn1CDqqCDqCVii
レスポンス・ヘッダーの追加	Target セクションに詳細なリクエストヘッダーを追加し、 Data セクションに値を追加する。	ターゲット=キャッシュ制御 Data= max-age=8888888
ボディすべて交換	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)
ボディ交換が先	レスポンス・ボディを検索し、最初のインスタンスだけを置き換える	Target= HTTP:// (検索文字列) Data= HTTPs:// (置換文字列)
ボディは最後に交換する	レスポンス・ボディを検索し、最後のインスタンスだけを置き換える	Target= HTTP:// (検索文字列) Data= HTTPs:// (置換文字列)
ドロップ	これは接続を切断する	目標=該当なし データ= 該当なし
電子メール	Email Events で設定したアドレスにメールを送信します。アドレスまたはメッセージとして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= 該当なし
ログイベント	これは、システムログにイベントを記録します。	Target="flightPATHはsyslogにこれを記録した" データ= 該当なし
リダイレクト 301	これは恒久的なリダイレクトを発行する。	ターゲット= HTTP://www.edgenexus.io データ= 該当なし
リダイレクト 302	これは一時的なリダイレクトを発行する。	ターゲット= HTTP://www.edgenexus.io データ= 該当なし
リクエストクッキーの削除	ターゲット」セクションで詳述したリクエストクッキーを削除する	ターゲット=クッキー Data= MS-WSMAN=afYfn1CDqqCDqCVii
リクエストヘッダーの削除	ターゲットセクションで詳述されているリクエストヘッダーを削除する	ターゲット=サーバー データ=N/A
レスポンス・クッキーの削除	ターゲット」セクションで詳述したレスポンス・クッキーを削除する	ターゲット=jnAccel
レスポンス・ヘッダーの削除	ターゲットセクションで詳述したレスポンスヘッダーを削除する	ターゲット= Etag データ= 該当なし
リクエスト・クッキーの置き換え	Target セクションのリクエストクッキーを Data セクションの値に置き換える。	ターゲット=クッキー Data= MS-WSMAN=afYfn1CDqqCDqCVii
リクエスト・ヘッダーの置換	ターゲットのリクエストヘッダーをデータ値で置き換える	ターゲット=コネクション データ=キープアライブ
レスポンス・クッキーの置き換え	Target セクションのレスポンス・クッキーを Data セクションの値に置き換える。	ターゲット=jnAccel=afYfn1CDqqCDqCVii 日付=MS-WSMAN=afYfn1CDqqCDqCVii
レスポンス・ヘッダーの置換	Target セクションのレスポンスヘッダーを Data セクションの値に置き換える。	ターゲット=サーバー データ=セキュリティのため非公開
パスの書き換え	これにより、リクエストは条件に基づいて新しい URL にリダイレクトされる。	ターゲット= /test/path/index.html\$querystring\$ データ= 該当なし

セキュアサーバーの使用	使用するセキュアサーバーまたはバーチャルサービスを選択する	Target=192.168.101:443 データ=N/A
サーバーの使用	使用するサーバーまたは仮想サービスを選択する	ターゲット= 192.168.101:80 データ= 該当なし
クッキーの暗号化	クッキーを 3DES 暗号化し、 base64 エンコードします。	Target=暗号化する Cookie 名を入力します。最後にワイルドカードとして*を使用できます。 Data= 暗号化のためのパスフレーズを入力してください。

例



以下のアクションはブラウザに安全な **HTTPS** 仮想サービスへの一時的なリダイレクトを発行します。リクエストと同じホスト名、パス、クエリー文字列を使用します。

一般的な用途

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）コンテンツについて、ユーザーを強制的に **HTTPS** にする。
- スパイダーをブロックまたはリダイレクト
- 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
- 内部ディレクトリ構造を隠す
- クッキーを書き換える
- 特定ユーザー向け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
- 複数のシステムにまたがるシングルサインオンの提供
- ユーザーID またはクッキーに基づいてユーザーをセグメントする
- **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を書き換える
- 壊れた **URL** の修正
- ログと電子メールアラート **404** レスポンスコード
- ディレクトリへのアクセス/閲覧を防止
- スパイダーに異なるコンテンツを送る

事前ルール

HTML エクステンション

すべての .htm リクエストを .html に変更する。

コンディション

- 条件=パス
- センス=する
- チェック = RegEx に一致させる
- 値=\.htm\$

評価だ:

- ブランク

アクション

- アクション = パスの書き換え
- ターゲット = \$path\$

インデックス.html

フォルダへのリクエストで 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=する
- チェック=存在する

評価だ:

- 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\$

フォルダを閉じる

フォルダへの要求を拒否する。

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。

- コンディション=適切な考慮が必要
- センス
- チェック

評価だ:

- 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で `cgi-bin` カタログを隠す。

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 = する
- チェック = RegEX と一致
- 値 = `\.cgi$`

評価だ:

- ブランク

アクション

- アクション = パスの書き換え
- ターゲット = `/cgi-bin$path$`

ログ・スパイダー

人気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
- マッチ = ユーザーエージェント
- センス = する
- チェック = RegEX と一致
- 値 = `Googlebot|Slurp|bingbot|ia_archiver`

評価だ:

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

アクション

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

HTTPS を強制する

特定のディレクトリに対して HTTPS を強制的に使用します。この場合、クライアントが `/secure/` ディレクトリを含む何かにアクセスしている場合、リクエストされた URL の HTTPS バージョンにリダイレクトされます。

コンディション

- 条件 = パス
- センス = する

- チェック = 含む
- 値 = /secure/

評価だ：

- 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。

コンディション

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

評価だ：

- 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 を HTTPS に切り替える

ハードコードされた HTTP:// を HTTPS:// に変更する。

コンディション

- 条件 = レスポンス・コード
- センス = する
- チェック = イコール
- 値 = 200 OK

評価だ：

- ブランク

アクション

- アクション = ボディ 全置換
- 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ないことを確認し、見つかった場合は空欄にする。

コンディション

- 条件=レスポンス・コード
- センス=する
- チェック=イコール
- 値 = 200 OK

評価だ:

- ブランク

アクション

- アクション = ボディ 全置換
- 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

リクエストと 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する。

コンディション: これはキャッチオールとしての一般的なコンディションである。この条件は、あなたの

- 条件=レスポンス・コード
- センス=する
- チェック=イコール
- 値 = 200 OK

評価だ:

- ブランク

アクション

- アクション = レスポンス・ヘッダの追加
- ターゲット = キャッシュ制御
- データ = max-age=3600

スプーフ・サーバー・タイプ

サーバーの種類を取得し、別のものに変更する。

コンディション: これはキャッチオールとしての一般的なコンディションである。この条件は、あなたの

- 条件=レスポンス・コード
- センス=する
- チェック=イコール
- 値 = 200 OK

評価だ:

- ブランク

アクション

- アクション = レスポンス・ヘッダの置換
- ターゲット = サーバー
- データ = シークレット

エラーを送信しない

クライアントがあなたのサイトからエラーを受け取ることはありません。

コンディション

- 条件 = レスポンス・コード
- センス = する
- チェック = 含む
- 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、関連する国のドメインにリダイレクトします。

コンディション

- 条件 = 言語
- センス = する
- チェック = 含む
- 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$`

グーグル・アナリティクス

アナリティクスに必要な Google のコードを挿入します - MYGOOGLCODE の値を Google UA ID に変更してください。

コンディション

- 条件 = レスポンス・コード
- センス = する
- 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 = ボディ置換
- ターゲット = </body>
- データ = <script type='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>

IPv6 ゲートウェイ

IPv6 サービスの 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リクエストに 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。

コンディショニング

- ブランク

評価

- ブランク

アクション

- アクション = リプレース・リクエスト・ヘッダー
- ターゲット = ホスト
- データ = ipv4.host.header

SAMLとEntra ID

Microsoft EntraでのEntra ID認証アプリケーションのセットアップ

SAML 認証を正常に動作させるには、Microsoft Entra Admin ポータルで Enterprise Application をセットアップする必要があります。これは簡単な作業で、SAML 認証要求およびトークンに必要な署名証明書と構成 XML データのプロビジョニングが可能です。

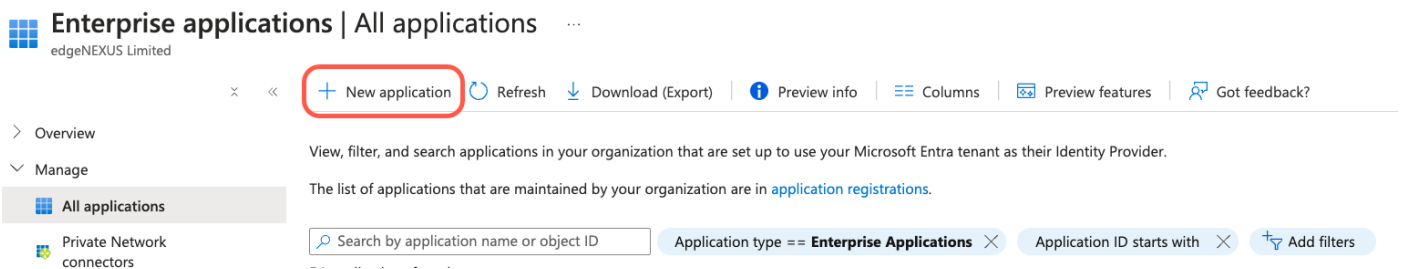
これを行うには、まず Microsoft Entra Portal (<https://portal.azure.com>) にログインし、ページの上部にアイコンのリストがある Azure Services ページにいることを確認してください（下図参照）。

Azure services



- Enterprise Applications をクリックします。アイコンのリストに Enterprise Applications が表示されない場合は、上部の Search バーに名前を入力してください。以下のようなページが表示されます。

Home > Enterprise applications



新規申込をクリック

次のページで、[Create your own application](#) をクリックします。

Home > Enterprise applications | All applications >

Browse Microsoft Entra Gallery




The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning.¹ users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Er described in [this article](#).

- ページの右側に「独自のアプリケーションを作成する」というタイトルのセクションが開きます。

Create your own application

×

 Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

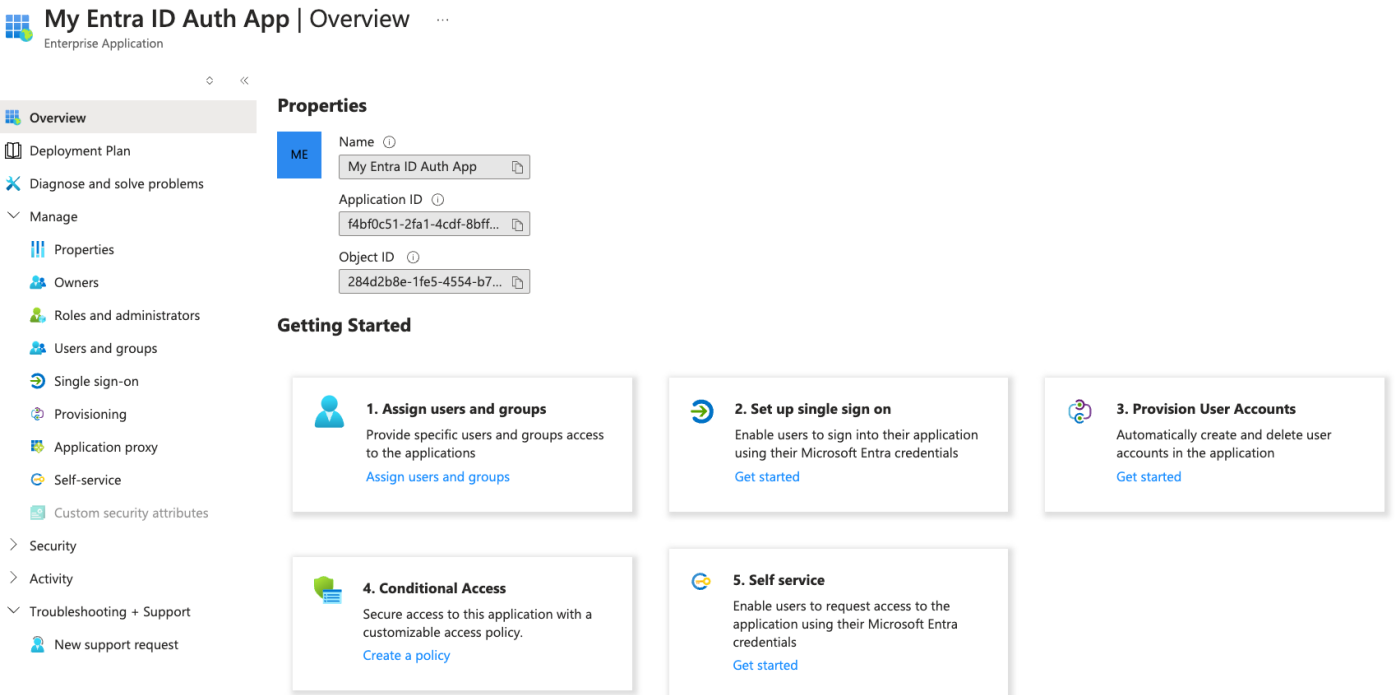
What's the name of your app?

What are you looking to do with your application?

- Configure Application Proxy for secure remote access to an on-premises application
- Register an application to integrate with Microsoft Entra ID (App you're developing)
- Integrate any other application you don't find in the gallery (Non-gallery)

- 例えば、"My Entra ID Auth App"のように、アプリケーションの名前を入力します。お好きな名前を選んでください。
- ギャラリーにない他のアプリケーションを統合する（ギャラリー以外）ラジオボタンオプションをクリックします。
- 作成ボタンをクリックする。

下のようページが表示されます。



My Entra ID Auth App | Overview ...
Enterprise Application

Properties


- Name: My Entra ID Auth App
- Application ID: f4bf0c51-2fa1-4cdf-8bff...
- Object ID: 284d2b8e-1fe5-4554-b7...


Getting Started


- 1. Assign users and groups**
Provide specific users and groups access to the applications
[Assign users and groups](#)
- 2. Set up single sign on**
Enable users to sign into their application using their Microsoft Entra credentials
[Get started](#)
- 3. Provision User Accounts**
Automatically create and delete user accounts in the application
[Get started](#)
- 4. Conditional Access**
Secure access to this application with a customizable access policy.
[Create a policy](#)
- 5. Self service**
Enable users to request access to the application using their Microsoft Entra credentials
[Get started](#)

- 左のナビゲーションバーにあるシングルサインオンオプションをクリックします。
- SAML ボックスを選択する。

Select a single sign-on method [Help me decide](#)


 **Disabled**
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

 **SAML**
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

 **Password-based**
Password storage and replay using a web browser extension or mobile app.

 **Linked**
Link to an application in My Apps and/or Office 365 application launcher.

- **SAML 基本構成** のセクションがあるページが表示されます。

Basic SAML Configuration  Edit

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	<i>Optional</i>
Relay State (Optional)	<i>Optional</i>
Logout Url (Optional)	<i>Optional</i>

- **基本 SAML 構成** エリアに入力する：
 - 識別子 (エンティティ ID)
 - 返信 URL (アサーション・コンシューマー・サービス URL)
 - サインオン URL
 - ログアウト URL (オプション)
- 設定を保存し、アプリをテストします。

より詳細なガイダンスについては、Microsoft サイトの [「Enable single sign-on for an enterprise application」](#) ドキュメントを参照してください。

テクニカルサポート

当社は、当社の標準利用規約に従って、すべてのユーザーにテクニカル・サポートを提供しています。

EdgeADC、EdgeWAF、または EdgeGSLB の有効なサポートおよびメンテナンス契約を結んでいる場合、テクニカルサポートを提供します。

サポートチケットを発行するには、こちらをご覧ください：

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