EdgeADC

ADMINISTRATIONSLEITFADEN

Inhalt

Dokument-Eigenschaften

Dokument-Nummer: 2.0.6.16.21.18.06

Erstellungsdatum des Dokuments: April 30, 2021

Das Dokument wurde zuletzt bearbeitet: June 16, 2021

Dokument Autor: Jay Savoor

Dokument Zuletzt bearbeitet von:

Dokument Überweisung: EdgeADC - Version 4.2.7.1895

Dokument-Haftungsausschluss

Screenshots und Grafiken in diesem Handbuch können aufgrund von Unterschieden in Ihrer Produkt-Release-Version leicht von Ihrem Produkt abweichen. Edgenexus versichert, dass sie alle angemessenen Anstrengungen unternehmen, um sicherzustellen, dass die Informationen in diesem Dokument vollständig und korrekt sind. Edgenexus übernimmt keine Haftung für eventuelle Fehler. Edgenexus nimmt Änderungen und Korrekturen an den Informationen in diesem Dokument in zukünftigen Versionen vor, wenn sich die Notwendigkeit ergibt.

Urheberrechte

Markenzeichen

Das Edgenexus-Logo, Edgenexus, EdgeADC, EdgeWAF, EdgeGSLB, EdgeDNS sind alle Marken oder eingetragene Marken von Edgenexus Limited. Alle anderen Marken sind Eigentum der jeweiligen Inhaber und werden anerkannt.

Edgenexus Unterstützung

Wenn Sie technische Fragen zu diesem Produkt haben, erstellen Sie bitte ein Support-Ticket unter: support@edgenexus.io

Installieren Sie den EdgeADC

Das Produkt EdgeADC (von nun an ADC genannt) kann auf verschiedene Arten installiert werden. Für jedes Plattformziel ist ein eigenes Installationsprogramm erforderlich, und diese sind alle für Sie verfügbar.

Dies sind die verschiedenen verfügbaren Installationsmodelle.

- VMware ESXi
- KVM
- Microsoft Hyper-V
- Oracle VM
- ISO für BareMetal-Hardware

Die Dimensionierung der virtuellen Maschine, die Sie zum Hosten des ADC verwenden, hängt vom Anwendungsszenario und dem Datendurchsatz ab.

VMware ESXi

ADC ist für die Installation auf VMware ESXi 5.x und höher verfügbar.

- Laden Sie das neueste Installations-OVA-Paket von ADC über den entsprechenden Link in der Download-E-Mail herunter.
- Nach dem Download entpacken Sie bitte in ein geeignetes Verzeichnis auf Ihrem ESXi-Host oder SAN.
- Wählen Sie in Ihrem vSphere-Client Datei: OVA/OVF-Vorlage bereitstellen.
- Durchsuchen Sie das Verzeichnis, in dem Sie Ihre Dateien gespeichert haben, wählen Sie die OVF-Datei und klicken Sie auf **NEXT**
- Der ESX-Server fordert den Appliance-Namen an. Geben Sie einen geeigneten Namen ein und klicken Sie auf **NEXT**
- Wählen Sie den Datenspeicher aus, auf dem Ihre ADC-Appliance laufen soll.
- Wählen Sie einen Datenspeicher mit ausreichend Platz und klicken Sie auf **NEXT**
- Sie erhalten dann Informationen über das Produkt; klicken Sie auf **NEXT**
- Klicken Sie auf **NEXT.**
- Sobald Sie die Dateien in den Datenspeicher kopiert haben, können Sie die virtuelle Appliance installieren.

Starten Sie Ihren vSphere-Client, um die neue virtuelle ADC-Appliance zu sehen.

- Klicken Sie mit der rechten Maustaste auf die VA und gehen Sie zu Power > Power-On
- Ihr VA bootet dann und der ADC-Boot-Bildschirm wird auf der Konsole angezeigt.

Installieren der VMXNET3-Schnittstelle

Der VMXnet3-Treiber wird unterstützt, aber Sie müssen zuerst Änderungen an den NIC-Einstellungen vornehmen.

***Hinweis** - Aktualisieren Sie NICHT die VMware-Tools*

Aktivieren der VMXNET3-Schnittstelle auf einer frisch importierten VA (nie gestartet)

1. Löschen Sie beide NICs aus der VM
2. Aktualisieren Sie die VM-Hardware - - Klicken Sie mit der rechten Maustaste auf die VA in der Liste und wählen Sie Virtuelle Hardware aktualisieren (starten Sie keine VMware-Tools-Installation oder -Update, führen Sie **nur** das Hardware-Upgrade durch)
3. Fügen Sie zwei NICs hinzu und wählen Sie diese als VMXNET3
4. Starten Sie die VA mit der Standardmethode. Es funktioniert mit dem VMXNET3

Aktivieren der VMXNET3-Schnittstelle auf einer bereits laufenden VA

1. Anhalten der VM (CLI-Befehl zum Herunterfahren oder GUI-Ausschalten)
2. Holen Sie sich die MAC-Adressen der beiden NICs (merken Sie sich die Reihenfolge der NICs in der Liste!)
3. Löschen Sie beide NICs aus der VM
4. Aktualisieren Sie die VM-Hardware (starten Sie keine VMware-Tools-Installation oder -Update, führen **Sie nur** das Hardware-Upgrade durch)
5. Fügen Sie zwei NICs hinzu und wählen Sie sie als VMXNET3
6. Stellen Sie die MAC-Adressen für die neuen NICs entsprechend Schritt 2 ein
7. Starten Sie die VA neu

Wir unterstützen VMware ESXi als Produktionsplattform. Für Evaluierungszwecke können Sie VMware Workstation und Player verwenden.

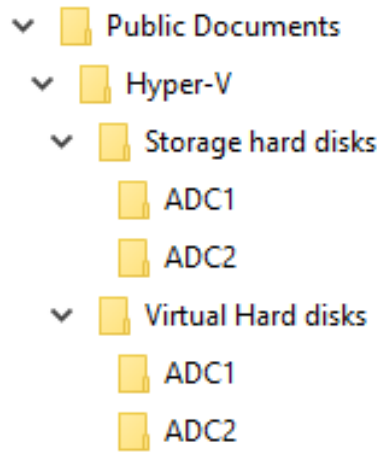
Lesen Sie bitte den Abschnitt **ERSTE BOOT-KONFIGURATION**, um fortzufahren.

Microsoft Hyper-V

Die Edgenexus ADC Virtual Appliance kann problemlos innerhalb eines Microsoft Hyper-V-Virtualisierungsrahmens installiert werden. Diese Anleitung setzt voraus, dass Sie Ihr Hyper-V-System und Ihre Systemressourcen korrekt spezifiziert und konfiguriert haben, um den ADC und seine Lastausgleichsarchitektur unterzubringen.

Beachten Sie, dass jede Appliance eine eindeutige MAC-Adresse benötigt.

- Extrahieren Sie die heruntergeladene Hyper-V-kompatible ADC-VA-Datei auf Ihren lokalen Rechner oder Server.
- Öffnen Sie den Hyper-V Manager.
- Erstellen Sie einen neuen Ordner, der die ADC VA "Virtuelle Festplatte" enthält, und einen weiteren neuen Ordner, der die "Speicherfestplatte" enthält, z. B. C:\Benutzer\Öffentlichkeit\Dokumente\Hyper-V\Virtuelle Festplatten\ADC1 und C:\Benutzer\Öffentlichkeit\Dokumente\Hyper-V\Speicherfestplatten\ADC1
- **Hinweis:** Für jede Installation einer virtuellen ADC-Instanz müssen neue ADC-spezifische Unterordner für die virtuellen Festplatten\ und Speicherfestplatten\ erstellt werden, wie unten gezeigt:



- Kopieren Sie die extrahierte EdgeADC .vhd-Datei in den oben angelegten Ordner 'Speicherfestplatte'.
- Klicken Sie in Ihrem Hyper-V Manager-Client mit der rechten Maustaste auf den Server und wählen Sie "Virtuelle Maschine importieren".
- Navigieren Sie zu dem Ordner, der die heruntergeladene ADC VA-Image-Datei enthält, die zuvor extrahiert wurde
- Virtuelle Maschine auswählen - markieren Sie die zu importierende virtuelle Maschine und klicken Sie auf Weiter
- Virtuelle Maschine auswählen - markieren Sie die zu importierende virtuelle Maschine und klicken Sie auf Weiter
- Wählen Sie "Importtyp" - wählen Sie "**Die virtuelle Maschine kopieren (eine neue eindeutige ID erstellen)**" Klicken Sie auf "Weiter
- Wählen Sie Ordner für Dateien der virtuellen Maschine - das Ziel kann als Hyper-V-Standard belassen werden oder Sie können einen anderen Speicherort wählen
- Virtuelle Festplatten suchen - navigieren Sie zu dem oben erstellten Ordner für virtuelle Festplatten, wählen Sie ihn aus und klicken Sie auf Weiter
- Wählen Sie Ordner zum Speichern virtueller Festplatten - navigieren Sie zu dem zuvor erstellten Ordner Speicherfestplatten und wählen Sie ihn aus und klicken Sie auf Weiter
- Überprüfen Sie, ob die Angaben im Fenster Zusammenfassung des Importassistenten korrekt sind und klicken Sie auf Fertig stellen
- Klicken Sie mit der rechten Maustaste auf die neu importierte virtuelle ADC-Maschine und wählen Sie Start

HINWEIS: GEMÄß HTTP://SUPPORT.MICROSOFT.COM/KB/2956569 SOLLTEN SIE DIE STATUSMELDUNG "DEGRADED (INTEGRATION SERVICES UPGRADE REQUIRED)" IGNORIEREN, DIE NACH DEM START DER VA MÖGLICHERWEISE WIE FOLGT ANGEZEIGT WIRD. ES IST KEINE AKTION ERFORDERLICH, UND DER DIENST IST NICHT HERABGESTUFT

- Während die VM initialisiert wird, können Sie mit der rechten Maustaste auf den VM-Eintrag klicken und "Verbinden" wählen... Sie erhalten dann die EdgeADC-Konsole.

- Sobald Sie die Netzwerkeigenschaften konfiguriert haben, startet der VA neu und präsentiert die Anmeldung an der VA-Konsole.

Lesen Sie bitte den Abschnitt **ERSTE BOOT-KONFIGURATION**, um fortzufahren.

Citrix XenServer

Die ADC Virtual Appliance ist auf Citrix XenServer installierbar.

- Extrahieren Sie die ADC OVA ALB-VA-Datei auf Ihren lokalen Rechner oder Server.
- Öffnen Sie Citrix XenCenter Client.
- Wählen Sie in Ihrem XenCenter-Client **"Datei: Importieren".**
- Suchen Sie die OVA-Datei, wählen Sie sie aus und klicken Sie dann auf **"Weiter öffnen".**
- Wählen Sie den Ort der VM-Erstellung, wenn Sie dazu aufgefordert werden.
- Wählen Sie, welchen XenServer Sie installieren möchten und klicken Sie auf **"NEXT".**
- Wählen Sie das Speicher-Repository (SR) für die Platzierung der virtuellen Festplatte, wenn Sie dazu aufgefordert werden.
- Wählen Sie eine SR mit ausreichend Platz und klicken Sie auf **"NEXT".**
- Ordnen Sie Ihre virtuellen Netzwerkschnittstellen zu. Auf beiden Schnittstellen wird Eth0 stehen; beachten Sie jedoch, dass die untere Schnittstelle Eth1 ist.
- Wählen Sie das Zielnetzwerk für jede Schnittstelle und klicken Sie auf **NEXT**
- Aktivieren Sie **NICHT das Kontrollkästchen** "Use Operating System Fixup".
- Klicken Sie auf **"NEXT"**
- Wählen Sie die Netzwerkschnittstelle, die für die temporäre Transfer-VM verwendet werden soll.
- Wählen Sie die Management-Schnittstelle, normalerweise Netzwerk 0, und lassen Sie die Netzwerkeinstellungen auf DHCP. Bitte beachten Sie, dass Sie statische IP-Adressangaben vergeben müssen, wenn Sie keinen funktionierenden DHCP-Server für die Übertragung haben. Wenn Sie dies nicht tun, wird der Import mit der Meldung "Connecting continuously then failed" angezeigt. Klicken Sie auf **"NEXT"**
- Überprüfen Sie alle Informationen und kontrollieren Sie dann die korrekten Einstellungen. Klicken Sie auf **"BEENDEN".**
- Ihre VM beginnt mit der Übertragung der virtuellen Festplatte "ADC ADC" und wird, sobald sie fertig ist, unter Ihrem XenServer angezeigt.
- In Ihrem XenCenter-Client können Sie nun die neue virtuelle Maschine sehen.
  Klicken Sie mit der rechten Maustaste auf die VA und klicken Sie auf "**START**".
- Ihre VM wird dann gebootet und der ADC-Boot-Bildschirm wird angezeigt.

- Einmal konfiguriert, präsentiert sich die Anmeldung an der VA.

Lesen Sie bitte den Abschnitt **ERSTE BOOT-KONFIGURATION**, um fortzufahren.

Erste Boot-Konfiguration

Beim ersten Start zeigt die ADC VA den folgenden Bildschirm an, der zur Konfiguration für den Produktionsbetrieb auffordert.

Erster Start - Manuelle Netzwerk-Details

Beim ersten Start haben Sie 10 Sekunden Zeit, um die automatische Zuweisung von IP-Angaben über DHCP zu unterbrechen

Um diesen Vorgang zu unterbrechen, klicken Sie in das Konsolenfenster und drücken eine beliebige Taste. Sie können dann die folgenden Angaben manuell eingeben.

- IP-Adresse
- Subnetz-Maske
- Gateway
- DNS-Server

Diese Änderungen sind persistent und überleben einen Neustart und müssen nicht erneut auf der VA konfiguriert werden.

Erster Boot - DHCP erfolgreich

Wenn Sie den Prozess der Netzwerkzuweisung nicht unterbrechen, kontaktiert Ihr ADC nach einem Timeout einen DHCP-Server, um seine Netzwerkdetails zu erhalten. Wenn der Kontakt erfolgreich ist, dann werden Ihrem Gerät die folgenden Informationen zugewiesen.

- IP-Adresse
- Subnetz-Maske
- Standard-Gateway
- DNS-Server

Wir raten Ihnen, den ADC VA nicht mit einer DHCP-Adresse zu betreiben, es sei denn, diese IP-Adresse ist dauerhaft mit der MAC-Adresse des VA innerhalb des DHCP-Servers verknüpft. Wir empfehlen, immer eine **FIXED IP ADDRESS zu** verwenden, wenn Sie den VA verwenden. Führen Sie die Schritte in **ÄNDERN DER MANAGEMENT-IP-ADRESSE** und den nachfolgenden Abschnitten aus, bis Sie die Netzwerkkonfiguration abgeschlossen haben.

Erster Start - DHCP schlägt fehl

Wenn Sie keinen DHCP-Server haben oder die Verbindung fehlschlägt, wird die IP-Adresse 192.168.100.100 zugewiesen.
Die IP-Adresse wird um '1'

erhöht, bis die VA eine freie IP-Adresse findet. Ebenso prüft die VA, ob die IP-Adresse gerade in Gebrauch ist, und wenn ja, wird sie erneut inkrementiert und erneut geprüft.

Ändern der Management-IP-Adresse

Sie können die IP-Adresse der VA jederzeit mit dem Befehl **set greenside=n.n.n.n** ändern**,** wie unten gezeigt.

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

Ändern der Subnetzmaske für eth0

Die Netzwerkschnittstellen verwenden das Präfix 'eth'; die Basis-Netzwerkadresse wird eth0 genannt. Die Subnetzmaske oder Netzmaske kann mit dem Befehl **set mask eth0 n.n.n.n** geändert werden. Ein Beispiel sehen Sie unten.

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

Zuweisen eines Standard-Gateways

Die VA benötigt ein Standard-Gateway für ihren Betrieb. Um das Standard-Gateway einzustellen, verwenden Sie den Befehl **route add default gw n.n.n.n** wie im folgenden Beispiel gezeigt.

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

Prüfen des Wertes für das Standard-Gateway

Um zu prüfen, ob das Standard-Gateway hinzugefügt wurde und korrekt ist, verwenden Sie den Befehl **route**. Dieser Befehl zeigt die Netzwerkrouten und den Wert des Standardgateways an. Siehe das Beispiel unten.

```
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
```

Sie können nun auf die grafische Benutzeroberfläche (GUI) zugreifen, um den ADC für den Produktions- oder Evaluierungseinsatz zu konfigurieren.

Zugriff auf die Web-Oberfläche

Sie können jeden Internet-Browser mit Javascript verwenden, um den ADC zu konfigurieren, zu überwachen und in Betrieb zu nehmen.

Geben Sie in das URL-Feld des Browsers entweder **HTTPS://{IP ADDRESS} oder HTTPS://{FQDN}** ein.

Der ADC verwendet standardmäßig ein selbstsigniertes SSL-Zertifikat. Sie können das ADC so ändern, dass es das SSL-Zertifikat Ihrer Wahl verwendet.

Sobald Ihr Browser den ADC erreicht, zeigt er Ihnen den Anmeldebildschirm an. Die werkseitig voreingestellten Anmeldedaten für den ADC sind:

Standard-Benutzername = **admin** / Standard-Passwort = **jetnexus**

Befehlsreferenztabelle

Befehl	Parameter1	Parameter2	Beschreibung	Beispiel
Datum			Zeigt das aktuell konfigurierte Datum und die Uhrzeit an	Di 3. Sept. 13:00 UTC 2013
Voreinstellungen			Weisen Sie die werkseitigen Standardeinstellungen für Ihre Appliance zu	
beenden			Abmelden von der Befehlszeilenschnittstelle	
Hilfe			Zeigt alle gültigen Befehle an	
ifconfig	[leer]		Anzeigen der Schnittstellenkonfiguration für alle Schnittstellen	ifconfig
	eth0		Nur die Schnittstellenkonfiguration von eth0 anzeigen	ifconfig eth0
machineid			Dieser Befehl liefert die Maschinennummer, die zur Lizenzierung des ADC verwendet wird	EF4-3A35-F79
kündigen			Abmelden von der Befehlszeilenschnittstelle	
Neustart			Beenden Sie alle Verbindungen und starten Sie den ADC neu	Neustart
Neustart			Starten Sie die virtuellen ADC-Dienste neu	
Route	[leer]		Anzeigen der Routing-Tabelle	Route
	hinzufügen	Standard-GW	Fügen Sie die IP-Adresse des Standard-Gateways hinzu	route add default gw 192.168.100.254
einstellen	Grünseiten		Stellen Sie die Management-IP-Adresse für ADC ein	set greenside=192.168.101.1
	Maske		Legen Sie die Subnetzmaske für eine Schnittstelle fest. Schnittstellennamen sind eth0, eth1....	Maske eth0 255.255.255.0 setzen
anzeigen			Zeigt die globalen Konfigurationseinstellungen an	
Herunterfahren			Beenden Sie alle Verbindungen und schalten Sie den ADC aus	

Status		Zeigt die aktuelle Datenstatistik an	
oben		Anzeigen der Prozessinformationen wie CPU und Speicher	
viewlog	Meldungen	Zeigt die rohen Syslog-Meldungen an	Log-Meldungen anzeigen

Bitte beachten Sie: Bei den Befehlen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Es gibt keine Befehlshistorie.

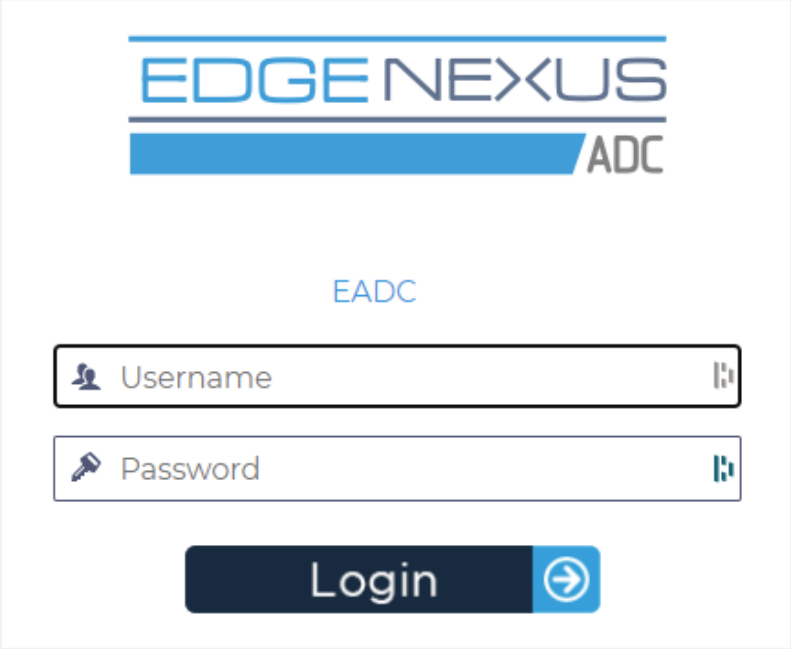
Starten der ADC Web-Konsole

Alle Vorgänge auf dem ADC (auch ADC genannt) werden über die Web-Konsole konfiguriert und ausgeführt. Der Zugriff auf die Web-Konsole erfolgt über einen beliebigen Browser mit Javascript.

Um die ADC-Webkonsole zu starten, geben Sie die URL oder IP-Adresse des ADC in das URL-Feld ein. Wir verwenden das Beispiel adc.company.com als Beispiel:

https://adc.company.com

Nach dem Start sieht die Web-Konsole des ADC wie unten dargestellt aus und Sie können sich als Admin-Benutzer anmelden.



Standard-Anmeldeinformationen

Die Standard-Anmeldeinformationen sind:

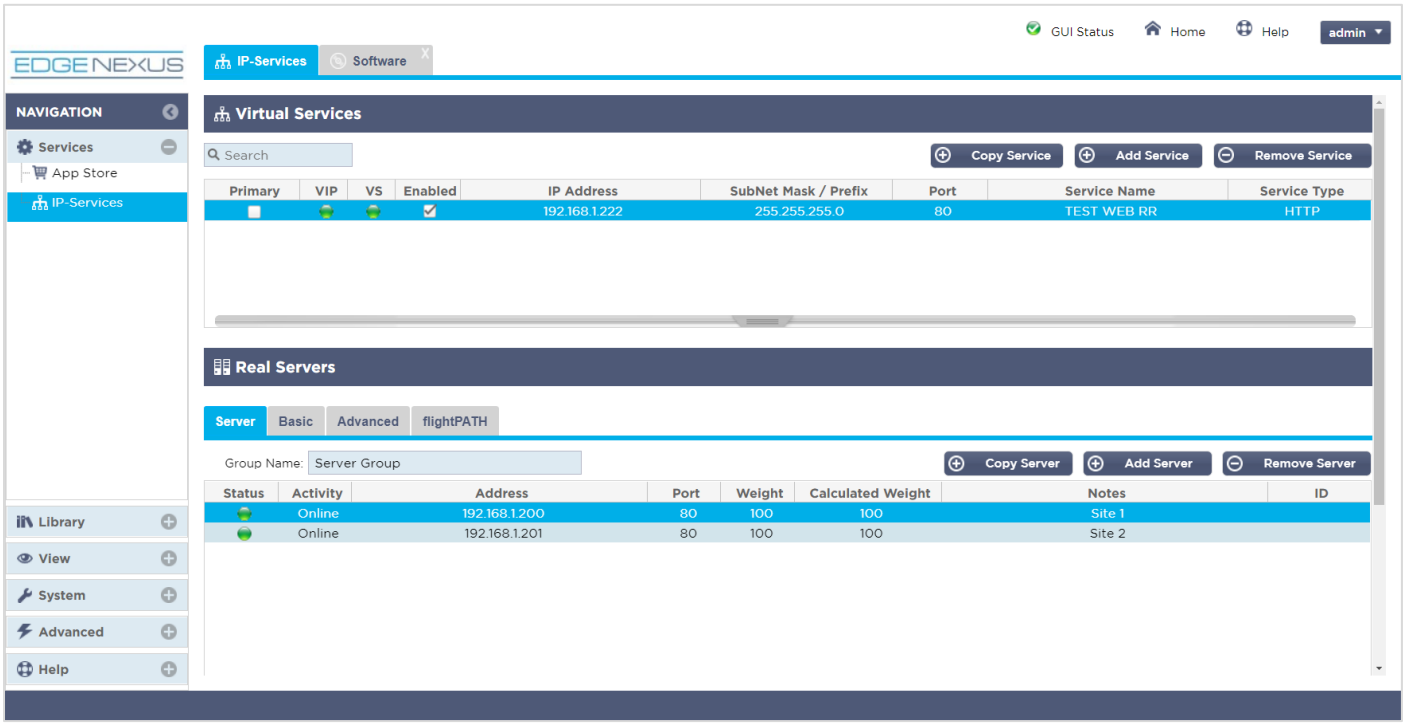
- Benutzername: admin
- Passwort: jetnexus

Sie können dies jederzeit über die Benutzerkonfigurationsfunktionen unter *System* > *Benutzer* ändern.

Sobald Sie sich erfolgreich angemeldet haben, wird das Haupt-Dashboard des ADC angezeigt.

Das Haupt-Dashboard

Das Bild unten zeigt, wie das Haupt-Dashboard oder die "Startseite" des ADC aussieht. Wir können von Zeit zu Zeit aus Gründen der Verbesserung einige Änderungen vornehmen, aber alle Funktionen bleiben erhalten.



Um uns so kurz wie möglich zu fassen, gehen wir davon aus, dass diese erste Einführung in die Bildschirmabschnitte die verschiedenen Abschnitte des ADC-Konfigurationsbereichs hinreichend bekannt macht, so dass wir sie im weiteren Verlauf nicht im Detail beschreiben, sondern uns auf die Konfigurationselemente konzentrieren.

In der Reihenfolge von links nach rechts haben wir zunächst die Navigation. Der Abschnitt Navigation besteht aus den verschiedenen Bereichen innerhalb von ADC. Wenn Sie auf eine bestimmte Auswahl innerhalb der Navigation klicken, wird der entsprechende Bereich auf der rechten Seite des Bildschirms angezeigt. Außerdem sehen Sie den gewählten Konfigurationsbereich als Registerkarten oben auf dem Bildschirm, neben dem Produktlogo. Die Registerkarten ermöglichen eine schnellere Navigation zu bereits verwendeten Bereichen der ADC-Konfiguration.

Dienste

Der Bereich "Dienste" des ADC hat mehrere Bereiche innerhalb des ADCs. Wenn Sie auf den Punkt Service klicken, wird dieser erweitert, um die verfügbaren Auswahlmöglichkeiten anzuzeigen.

IP-Dienste

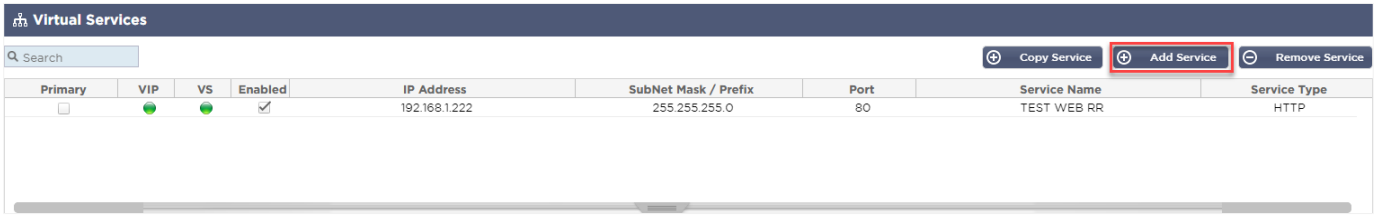
Im Bereich IP-Dienste des ADC können Sie die verschiedenen virtuellen IP-Dienste, die Sie für Ihren speziellen Anwendungsfall benötigen, hinzufügen, löschen und konfigurieren. Die Einstellungen und Optionen sind in die folgenden Abschnitte unterteilt. Diese Abschnitte befinden sich auf der rechten Seite des Anwendungsbildschirms.

Virtuelle Dienste

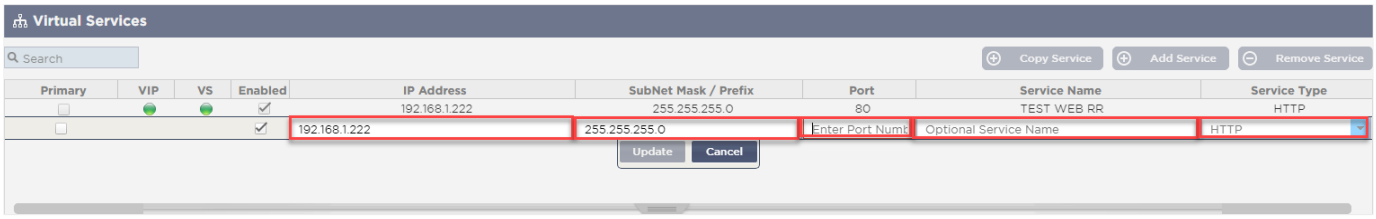
Ein virtueller Dienst kombiniert eine virtuelle IP (VIP) und einen TCP/UDP-Port, auf dem der ADC lauscht. Verkehr, der an der Virtual Service IP ankommt, wird an einen der Real Server umgeleitet, die mit diesem Dienst verbunden sind. Die Virtual Service IP-Adresse kann nicht mit der Management-Adresse des ADC identisch sein. d. h. eth0, eth1 usw...

Der ADC bestimmt, wie der Datenverkehr auf die Server umverteilt wird, basierend auf einer Lastausgleichsrichtlinie, die auf der Registerkarte Basic im Abschnitt Real Servers eingestellt ist.

Erstellen eines neuen virtuellen Dienstes unter Verwendung eines neuen VIP



- Klicken Sie wie oben angegeben auf die Schaltfläche Virtuellen Dienst hinzufügen.

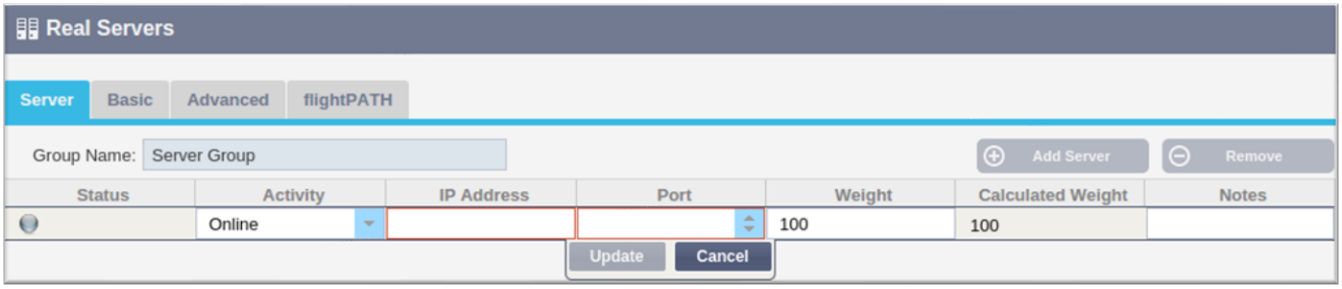


- Sie gelangen dann in den Modus "**Zeile bearbeiten"**.
- Füllen Sie die vier markierten Felder aus, um fortzufahren, und klicken Sie dann auf die Schaltfläche Aktualisieren.

Bitte verwenden Sie die TAB-Taste, um durch die Felder zu navigieren.

Feld	Beschreibung
IP-Adresse	Geben Sie eine neue virtuelle IP-Adresse ein, die als Zieleinstiegspunkt für den Zugriff auf den Real-Server dienen soll. Diese IP ist der Punkt, auf den Benutzer oder Anwendungen zeigen werden, um auf die Anwendung mit Lastausgleich zuzugreifen.
Subnetz-Maske/Präfix	Dieses Feld ist für die Subnetzmaske, die für das Netzwerk relevant ist, in dem sich der ADC befindet
Hafen	Der Eingangsport, der beim Zugriff auf das VIP verwendet wird. Dieser Wert muss nicht unbedingt mit dem des Realen Servers übereinstimmen, wenn Sie Reverse Proxy verwenden.
Dienst Name	Der Dienstname ist eine textuelle Darstellung des Zwecks des VIPs. Er ist optional, aber wir empfehlen Ihnen, ihn aus Gründen der Übersichtlichkeit anzugeben.
Dienst-Typ	Es gibt viele verschiedene Diensttypen, die Sie auswählen können. Layer-4-Diensttypen können die flightPATH-Technologie nicht verwenden.

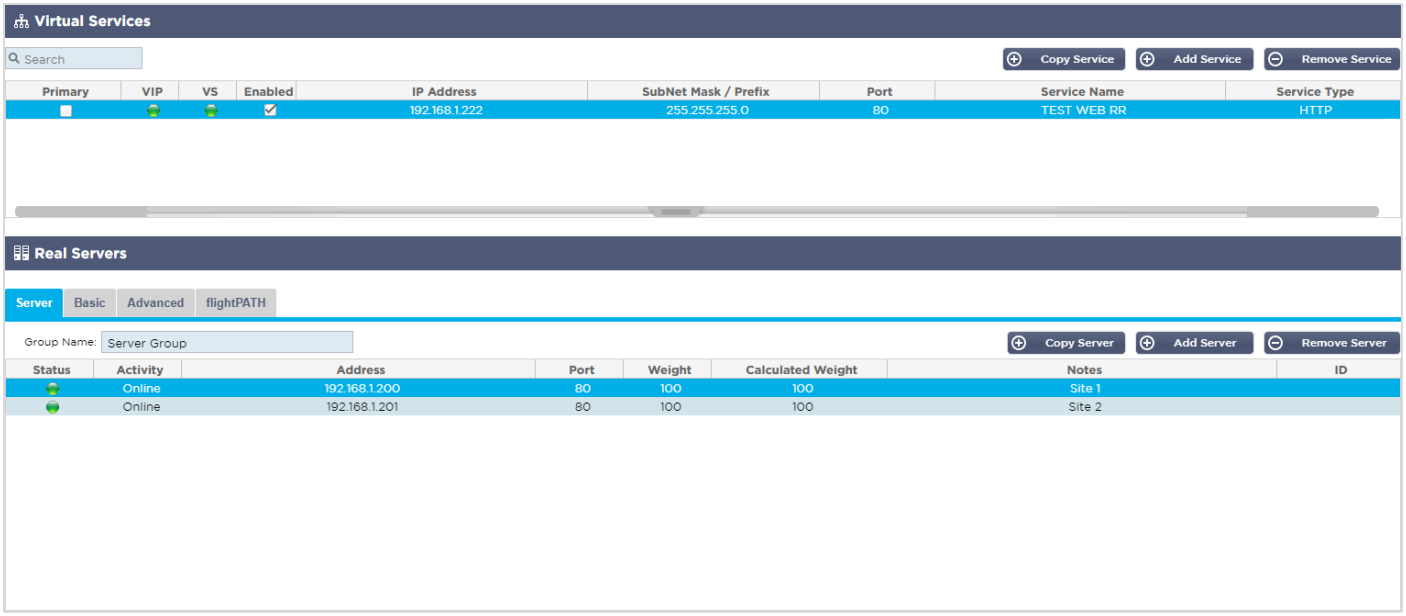
Sie können nun die Schaltfläche Aktualisieren drücken, um diesen Abschnitt zu speichern und automatisch zum Abschnitt Real Server zu springen, der weiter unten beschrieben wird:



Feld	Beschreibung
Aktivität	Das Feld Aktivität kann verwendet werden, um den Status des lastverteilten realen Servers anzuzeigen und zu ändern. Online - Zeigt an, dass der Server aktiv ist und Lastausgleichsanfragen empfängt Offline - Der Server ist offline und empfängt keine Anfragen Drain - Der Server wurde in den Drain-Modus versetzt, so dass die Persistenz geleert und der Server in einen Offline-Zustand versetzt werden kann, ohne dass die Benutzer davon betroffen sind. Standby - Der Server wurde in einen Standby-Zustand versetzt
IP-Adresse	Dieser Wert ist die IP-Adresse des Real-Servers. Sie muss genau sein und sollte keine DHCP-Adresse sein.
Hafen	Der Ziel-Port des Zugriffs auf dem Real-Server. Bei Verwendung eines Reverse-Proxys kann dieser von dem im VIP angegebenen Eingangs-Port abweichen.
Gewichtung	Diese Einstellung wird normalerweise automatisch vom ADC konfiguriert. Sie können dies ändern, wenn Sie die Prioritätsgewichtung ändern möchten.

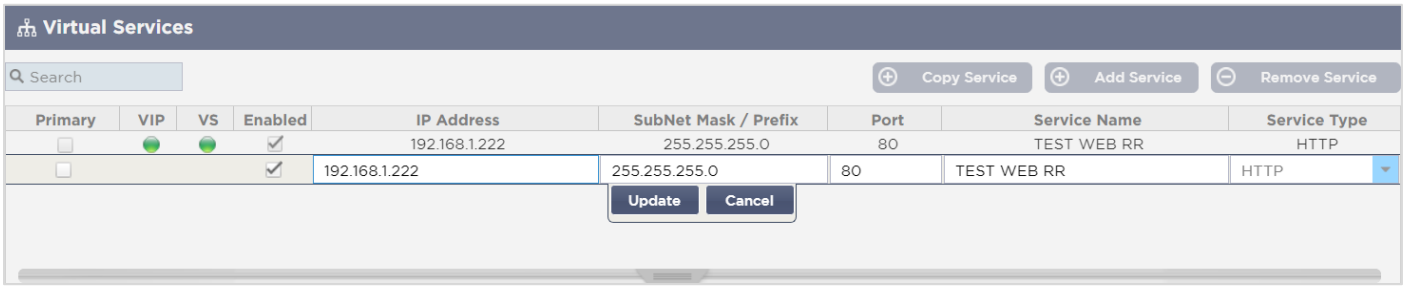
- Klicken Sie auf die Schaltfläche Aktualisieren oder drücken Sie die Eingabetaste, um Ihre Änderungen zu speichern
- Die Statusanzeige leuchtet zuerst grau und dann grün, wenn der Server Health Check erfolgreich war. Sie wird rot, wenn der Real Server Monitor fehlschlägt.
- Ein Server, dessen Statusleuchte rot leuchtet, wird nicht im Lastausgleich betrieben.

Beispiel für einen abgeschlossenen virtuellen Dienst

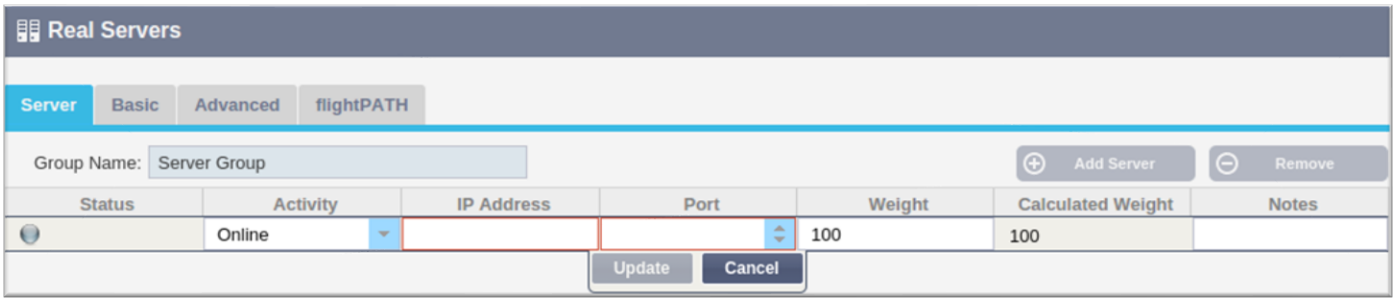


Erstellen eines neuen virtuellen Dienstes unter Verwendung eines vorhandenen VIPs

- Markieren Sie einen virtuellen Dienst, den Sie kopieren möchten
- Klicken Sie auf Virtuellen Dienst hinzufügen, um in den Zeilenbearbeitungsmodus zu gelangen



- Die IP-Adresse und die Subnetzmaske werden automatisch übernommen
- Geben Sie die Port-Nummer für Ihren Dienst ein
- Geben Sie einen optionalen Dienstnamen ein
- Wählen Sie einen Service-Typ
- Sie können nun auf die Schaltfläche Aktualisieren klicken, um diesen Abschnitt zu speichern und automatisch zum Abschnitt Real Server weiter unten zu springen

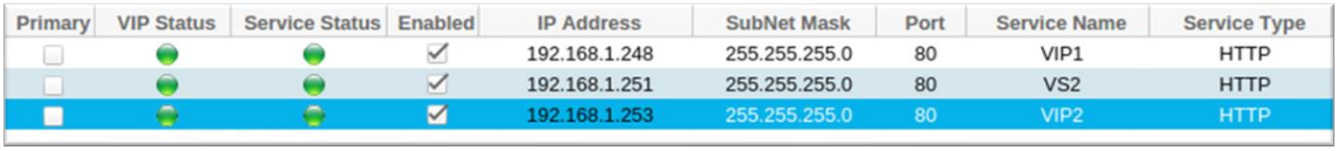


- Belassen Sie die Server-Aktivitätsoption auf Online - das bedeutet, dass der Server einen Lastausgleich erhält, wenn er die standardmäßige Zustandsüberwachung von TCP Connect besteht. Diese Einstellung kann bei Bedarf später geändert werden.
- Geben Sie eine IP-Adresse des Real-Servers ein
- Geben Sie eine Port-Nummer für den Real-Server ein
- Geben Sie einen optionalen Namen für den Real-Server ein
- Klicken Sie auf Aktualisieren, um Ihre Änderungen zu speichern
- Die Statusanzeige leuchtet erst grau, dann grün, wenn der Server Health Check erfolgreich war. Sie wird rot, wenn der Real Server Monitor fehlschlägt.
- Ein Server, der eine rote Statusleuchte hat, wird nicht im Lastausgleich betrieben

Ändern der IP-Adresse eines virtuellen Dienstes

Sie können die IP-Adresse eines vorhandenen virtuellen Dienstes oder VIPs jederzeit ändern.

- Markieren Sie den virtuellen Dienst, dessen IP-Adresse Sie ändern möchten



- Doppelklicken Sie auf das IP-Adressfeld für diesen Dienst

- Ändern Sie die IP-Adresse auf diejenige, die Sie verwenden möchten
- Klicken Sie auf die Schaltfläche Aktualisieren, um die Änderungen zu speichern.

Hinweis: Wenn Sie die IP-Adresse eines virtuellen Dienstes ändern, wird die IP-Adresse aller mit dem VIP verbundenen Dienste geändert

Erstellen eines neuen virtuellen Dienstes mit Copy Service

- Die Schaltfläche Dienst kopieren kopiert einen gesamten Dienst, einschließlich aller Real-Server, Grundeinstellungen, erweiterten Einstellungen und flightPATH-Regeln, die mit ihm verbunden sind

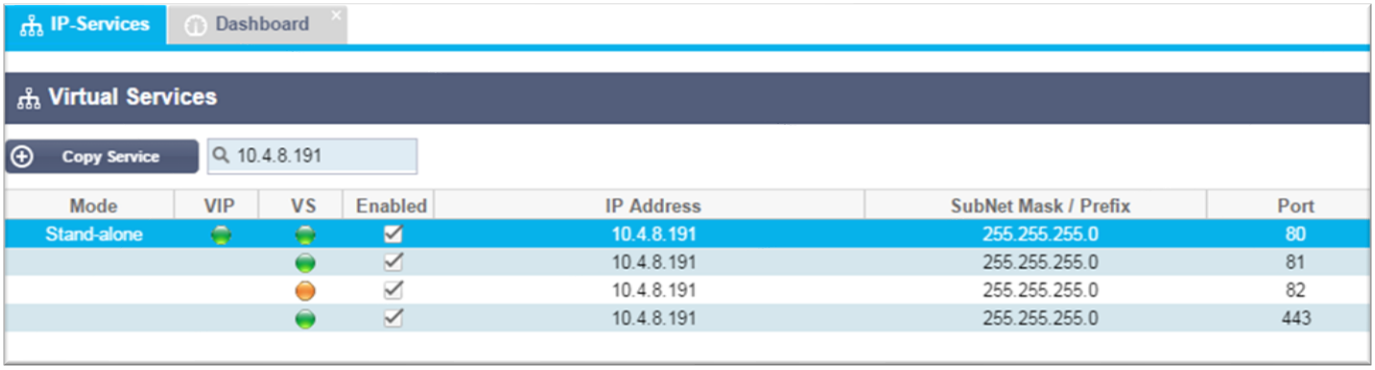
- Markieren Sie den Dienst, den Sie duplizieren möchten, und klicken Sie auf Dienst kopieren
- Der Zeileneditor erscheint mit dem blinkenden Cursor in der Spalte IP-Adresse
- Sie müssen die IP-Adresse so ändern, dass sie eindeutig ist, oder wenn Sie die IP-Adresse beibehalten möchten, müssen Sie den Port so bearbeiten, dass er für diese IP-Adresse eindeutig ist

Vergessen Sie nicht, die einzelnen Registerkarten zu bearbeiten, wenn Sie eine Einstellung wie z. B. eine Lastausgleichsrichtlinie oder den Real-Server-Monitor ändern oder eine flightPATH-Regel entfernen.

Filtern der angezeigten Daten

Suche nach einem bestimmten Begriff

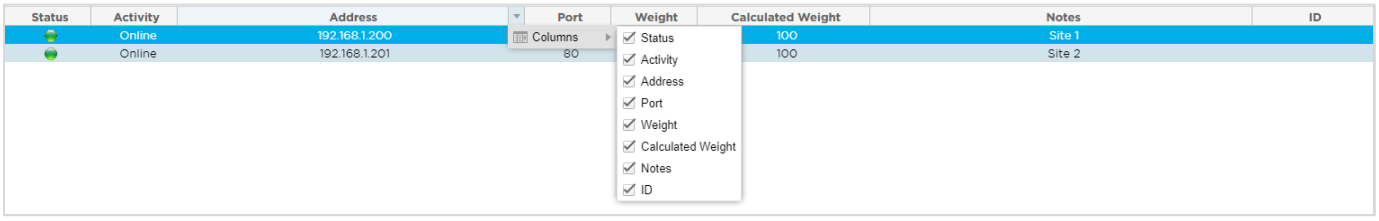
Im Feld Suchen können Sie die Tabelle anhand eines beliebigen Wertes durchsuchen, z. B. anhand der Oktette der IP-Adresse oder des Namens des Dienstes.



Das obige Beispiel zeigt das Ergebnis der Suche nach einer bestimmten IP-Adresse von 10.4.8.191.

Sichtbarkeit der Spalte auswählen

Sie können auch die Spalten auswählen, die Sie im Dashboard anzeigen möchten.

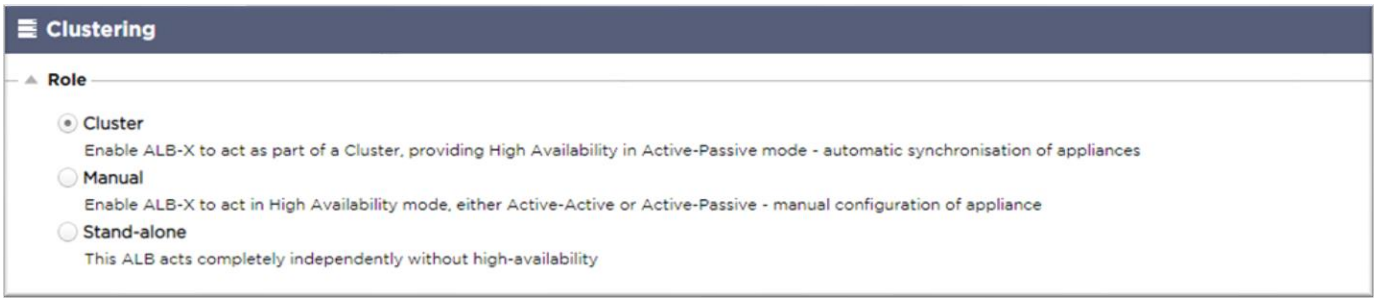


- Bewegen Sie die Maus über eine der Spalten
- Sie sehen einen kleinen Pfeil auf der rechten Seite der Spalte erscheinen
- Durch Anklicken der Kontrollkästchen wählen Sie die Spalten aus, die Sie im Dashboard sehen möchten.

Verstehen der Spalten für virtuelle Dienste

Primär/Modus

Die Spalte Primär/Modus zeigt die für das aktuelle VIP ausgewählte Hochverfügbarkeitsrolle an. Verwenden Sie die unter System > Clustering verfügbaren Optionen, um diese Option zu konfigurieren.



Option	Beschreibung
Cluster	Cluster ist die Standardrolle für den ADC bei der Installation, und die Spalte Primary/Mode zeigt den Modus an, in dem er gerade läuft. Wenn Sie ein HA-Paar von ADC-Appliances in Ihrem Rechenzentrum haben, wird eine von ihnen als Aktiv und die andere als Passiv angezeigt
Handbuch	Die Rolle Manuell ermöglicht es, dass das ADC-Paar im Aktiv-Aktiv-Modus für verschiedene virtuelle IP-Adressen läuft. In solchen Fällen enthält die Spalte Primär ein Kästchen neben jeder einzelnen Virtuellen IP, das für Aktiv angekreuzt oder für Passiv nicht angekreuzt werden kann.
Stand-Alone	Der ADC agiert als eigenständiges Gerät und befindet sich nicht im Hochverfügbarkeitsmodus. In der Spalte "Primär" wird daher "Stand-alone" angezeigt.

VIP

Diese Spalte bietet eine visuelle Rückmeldung über den Status der einzelnen virtuellen Dienste. Die Indikatoren sind farbcodiert und lauten wie folgt:

LED	Bedeutung
●	Online
●	Failover-Standby. Dieser virtuelle Dienst ist hot-standby
●	Zeigt an, dass ein "Sekundär" auf einen "Primär" wartet.
●	Dienst benötigt Aufmerksamkeit. Diese Anzeige kann daraus resultieren, dass ein Real Server eine Zustandsüberprüfung nicht bestanden hat oder manuell auf Offline geändert wurde. Der Datenverkehr fließt weiter, aber mit reduzierter Real-Server-Kapazität
●	Offline. Inhaltsserver sind nicht erreichbar, oder keine Inhaltsserver aktiviert
●	Status finden
●	Nicht lizenziert oder lizenzierte virtuelle IPs überschritten

Aktiviert

Die Vorgabe für diese Option ist Aktiviert, und das Kontrollkästchen wird als aktiviert angezeigt. Sie können den virtuellen Dienst deaktivieren, indem Sie auf die Zeile doppelklicken, das Kontrollkästchen deaktivieren und dann auf die Schaltfläche Aktualisieren klicken.

IP-Adresse

Fügen Sie Ihre IPv4-Adresse in dezimaler Punktschreibweise oder eine IPv6-Adresse ein. Dieser Wert ist die virtuelle IP-Adresse (VIP) für Ihren Dienst. Beispiel IPv4 "192.168.1.100". Beispiel Ipv6 "2001:0db8:85a3:0000:0000:8a2e:0370:7334"

Subnetz-Maske/Präfix

Fügen Sie Ihre Subnetzmaske in dezimaler gepunkteter Notation ein. Beispiel "255.255.255.0". Oder fügen Sie für IPv6 Ihr Präfix ein. Weitere Informationen zu IPv6 finden Sie unter **HTTPS://DE.WIKIPEDIA.ORG/WIKI/IPV6_ADDRESS**

Hafen

Fügen Sie die Portnummer hinzu, die mit Ihrem Dienst verbunden ist. Der Port kann eine TCP- oder UDP-Portnummer sein. Beispiel TCP "80" für Webverkehr und TCP "443" für gesicherten Webverkehr.

Dienst Name

Geben Sie einen freundlichen Namen ein, um Ihren Dienst zu identifizieren. Beispiel "Production Web Servers".

Dienst-Typ

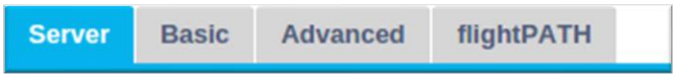
Bitte beachten Sie, dass bei allen "Layer 4"-Diensttypen der ADC nicht interagiert und den Datenstrom nicht verändert, so dass flightPATH bei Layer 4-Diensttypen nicht verfügbar ist. Layer 4-Dienste führen einfach einen Lastausgleich des Datenverkehrs gemäß der Lastausgleichsrichtlinie durch:

Dienst-Typ	**Port/Protokoll**	**Dienst-Schicht**	**Kommentar**
Schicht 4 TCP	Beliebiger TCP-Port	Schicht 4	Der ADC verändert keine Informationen im Datenstrom und führt einen Standard-Lastausgleich des Datenverkehrs gemäß der Lastausgleichsrichtlinie durch
Schicht 4 UDP	Beliebiger UDP-Port	Schicht 4	Wie bei Layer 4 TCP verändert der ADC keine Informationen im Datenstrom und führt einen Standard-Lastausgleich des Datenverkehrs gemäß der Lastausgleichsrichtlinie durch
Schicht 4 TCP/UDP	Beliebiger TCP- oder UDP-Port	Schicht 4	Es ist ideal, wenn Ihr Dienst ein primäres Protokoll wie UDP hat, aber auf TCP zurückgreifen wird. Der ADC ändert keine Informationen im Datenstrom und führt den Standard-Lastausgleich des Datenverkehrs gemäß der Lastausgleichsrichtlinie durch
DNS	!!!		
HTTP	HTTP- oder HTTPS-Protokoll	Ebene 7	Der ADC kann den Datenstrom mit flightPATH interagieren, manipulieren und modifizieren.
FTP	Dateiübertragungsprotokoll Protokoll	Ebene 7	Verwendung getrennter Steuer- und Datenverbindungen zwischen Client und Server
SMTP	Simple Mail Transfer Protocol	Schicht 4	Verwendung beim Lastausgleich von Mailservern
POP3	Postamt-Protokoll	Schicht 4	Verwendung beim Lastausgleich von Mailservern

IMAP	Internet Message Access Protocol	Schicht 4	Verwendung beim Lastausgleich von Mailservern
RDP	Remote-Desktop-Protokoll	Schicht 4	Verwendung beim Lastausgleich von Terminaldienste-Servern
RPC	Remote Procedure Call	Schicht 4	Verwendung beim Lastausgleich von Systemen mit RPC-Aufrufen
RPC/ADS	Exchange 2010 Statischer RPC für Adressbuchdienst	Schicht 4	Verwendung beim Lastausgleich von Exchange-Servern
RPC/CA/PF	Exchange 2010 Statischer RPC für Client-Zugriff & Öffentliche Ordner	Schicht 4	Verwendung beim Lastausgleich von Exchange-Servern
DICOM	Digitale Bildgebung und Kommunikation in der Medizin	Schicht 4	Verwendung beim Lastausgleich von Servern mit DICOM-Protokollen

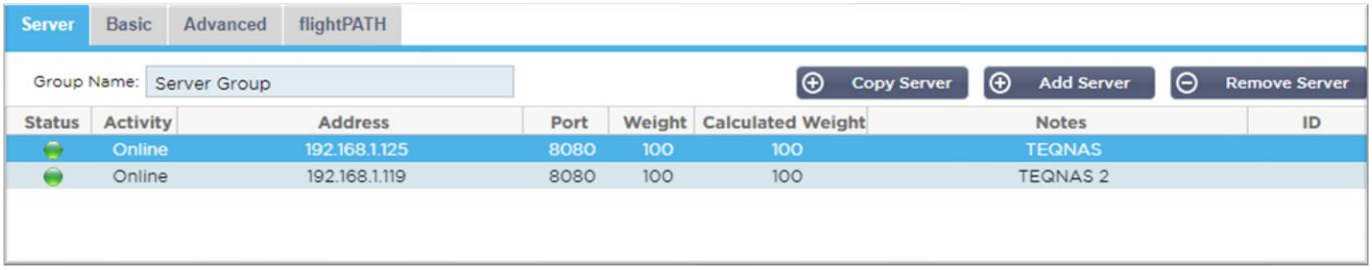
Echte Server

Im Abschnitt Real Servers des Dashboards gibt es mehrere Registerkarten: Server, Basic, Advanced und flightPATH.



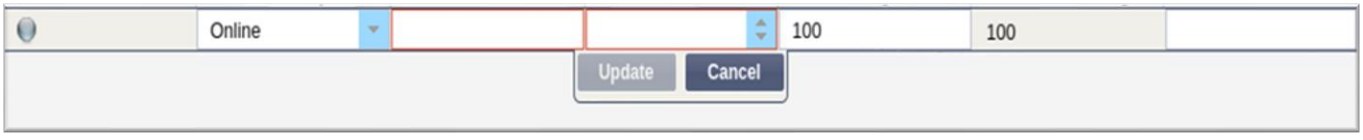
Server

Die Registerkarte Server enthält die Definitionen der realen Backend-Server, die mit dem aktuell ausgewählten virtuellen Dienst gekoppelt sind. Sie müssen mindestens einen Server zum Abschnitt Reale Server hinzufügen.



Server hinzufügen

- Wählen Sie das entsprechende VIP, das Sie zuvor definiert haben.
- Klicken Sie auf Server hinzufügen
- Es erscheint eine neue Zeile, in der der Cursor in der Spalte IP-Adresse blinkt

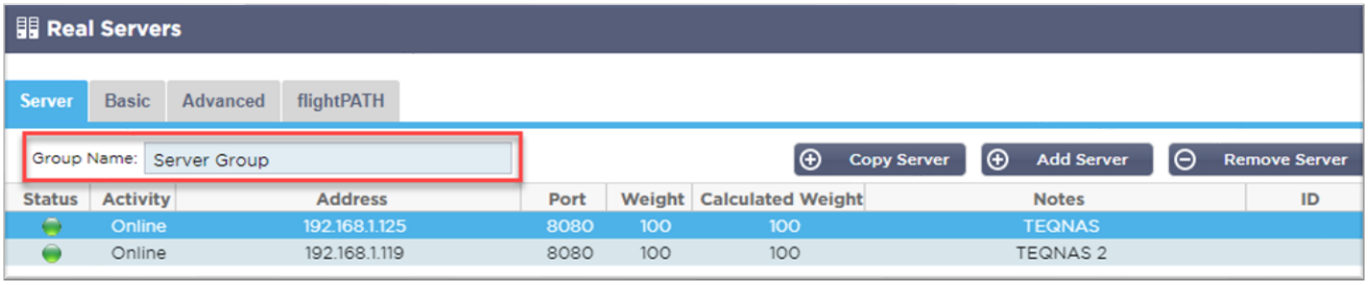


- Geben Sie die IPv4-Adresse Ihres Servers in punktierter Dezimalschreibweise ein. Der reale Server kann sich im gleichen Netzwerk wie Ihr virtueller Dienst, in einem direkt angeschlossenen lokalen Netzwerk oder in einem Netzwerk befinden, das Ihr ADC routen kann. Beispiel "10.1.1.1".
- Wechseln Sie zur Spalte Port und geben Sie die TCP/UDP-Portnummer für Ihren Server ein. Die Portnummer kann dieselbe sein wie die Portnummer des virtuellen Dienstes oder eine andere

Portnummer für die Reverse-Proxy-Konnektivität. Der ADC wird automatisch auf diese Nummer umgestellt.

- Wechseln Sie in den Bereich Notizen, um alle relevanten Details für den Server hinzuzufügen. Beispiel: "IIS Web Server 1"

Gruppe Name



Wenn Sie die Server, aus denen das Load-Balanced-Set besteht, hinzugefügt haben, können Sie ihnen auch einen Gruppennamen zuweisen. Sobald Sie dieses Feld bearbeitet haben, wird der Inhalt gespeichert, ohne dass Sie die Schaltfläche Aktualisieren drücken müssen.

Real Server Status Lights

Sie können den Status eines Real-Servers an der Lichtfarbe in der Spalte Status erkennen. Siehe unten:

LED	Bedeutung
●	Verbunden
◎	Nicht überwacht
●	Entleeren
●	Offline
●	Standby
●	Nicht verbunden
●	Status der Suche
●	Nicht lizenzierte oder lizenzierte Real-Server überschritten

Aktivität

Sie können die Aktivität eines Real-Servers jederzeit über das Dropdown-Menü ändern. Doppelklicken Sie dazu auf eine Real Server-Zeile, um sie in den Bearbeitungsmodus zu versetzen.

Option	Beschreibung
Online	Alle Real-Server, die online zugewiesen sind, erhalten den Datenverkehr gemäß der Lastausgleichsrichtlinie, die auf der Registerkarte Basis eingestellt ist.
Ablassen	Alle Real-Server, die als Drain zugewiesen sind, bedienen weiterhin bestehende Verbindungen, nehmen aber keine neuen Verbindungen an. Die Statusanzeige blinkt grün/blau, während die Entleerung läuft. Sobald die bestehenden Verbindungen natürlich geschlossen sind, gehen die Real-Server offline und die Statusanzeige leuchtet durchgehend blau. Sie können diese Verbindungen auch anzeigen, indem Sie zum Bereich Navigation > Monitor > Status navigieren.
Offline	Alle Real-Server, die als Offline eingestellt sind, werden sofort offline genommen und erhalten keinen Datenverkehr.
Standby	Alle Real-Server, die als Standby eingestellt sind, bleiben offline, bis **ALLE** Server der Online-Gruppe ihre Server Health Monitor-Prüfungen nicht bestehen. Der Verkehr wird von der Standby-Gruppe gemäß der Lastausgleichsrichtlinie empfangen, wenn dies geschieht. Wenn ein Server in der Online-Gruppe die Server Health Monitor-Prüfung besteht, erhält dieser Online-Server den gesamten Datenverkehr, und die Standby-Gruppe erhält keinen Datenverkehr mehr.

IP-Adresse

Dieses Feld ist die IP-Adresse für Ihren Real-Server. Beispiel "192.168.1.200".

Hafen

TCP- oder UDP-Portnummer, auf der der Real-Server für den Dienst lauscht. Beispiel "80" für Webverkehr.

Gewicht

Diese Spalte wird bearbeitbar, wenn eine entsprechende Lastausgleichsrichtlinie angegeben ist.

Die Standardgewichtung für einen Real Server ist 100, und Sie können Werte von 1-100 eingeben. Ein Wert von 100 bedeutet maximale Last, und 1 bedeutet minimale Last.

Ein Beispiel für drei Server könnte etwa so aussehen:

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

Wenn wir davon ausgehen, dass die Lastausgleichsrichtlinie auf "Least Connections" eingestellt ist und es insgesamt 200 Client-Verbindungen gibt;

- Server 1 wird 100 gleichzeitige Verbindungen erhalten
- Server 2 wird 50 gleichzeitige Verbindungen erhalten
- Server 3 wird 50 gleichzeitige Verbindungen erhalten

Wenn wir Round Robin als Lastausgleichsmethode verwenden, bei der die Anfragen durch die Servergruppe mit Lastausgleich rotieren, wirkt sich die Änderung der Gewichte darauf aus, wie oft die Server als Ziel ausgewählt werden.

Wenn wir davon ausgehen, dass die Lastausgleichsrichtlinie Fastest die kürzeste Zeit verwendet, die für das GET einer Antwort benötigt wird, ändert das Anpassen der Gewichte die Verzerrung ähnlich wie bei Least Connections.

Berechnetes Gewicht

Die berechnete Gewichtung jedes Servers kann dynamisch angezeigt werden und wird automatisch berechnet und ist nicht editierbar. Das Feld zeigt die tatsächliche Gewichtung an, die ADC unter Berücksichtigung der manuellen Gewichtung und der Lastausgleichsrichtlinie verwendet.

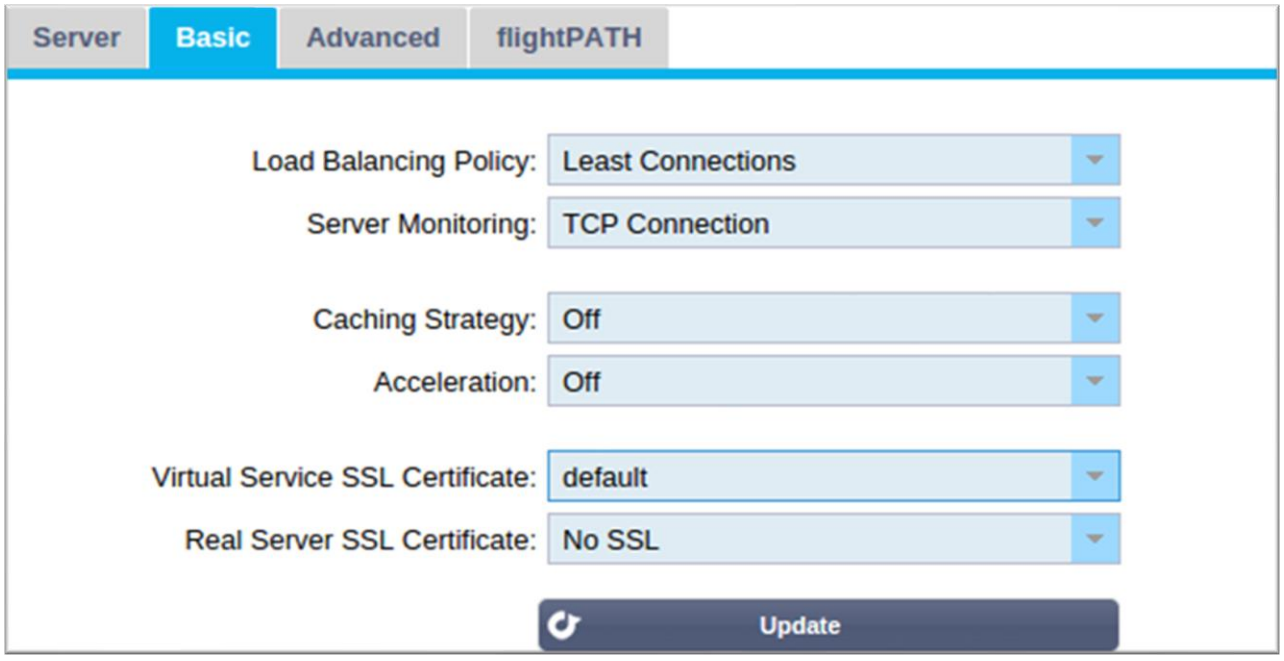
Anmerkungen

Geben Sie in das Feld Notizen besondere Hinweise ein, die bei der Beschreibung des definierten Eintrags hilfreich sind. Beispiel "IIS Server1 - London DC".

ID

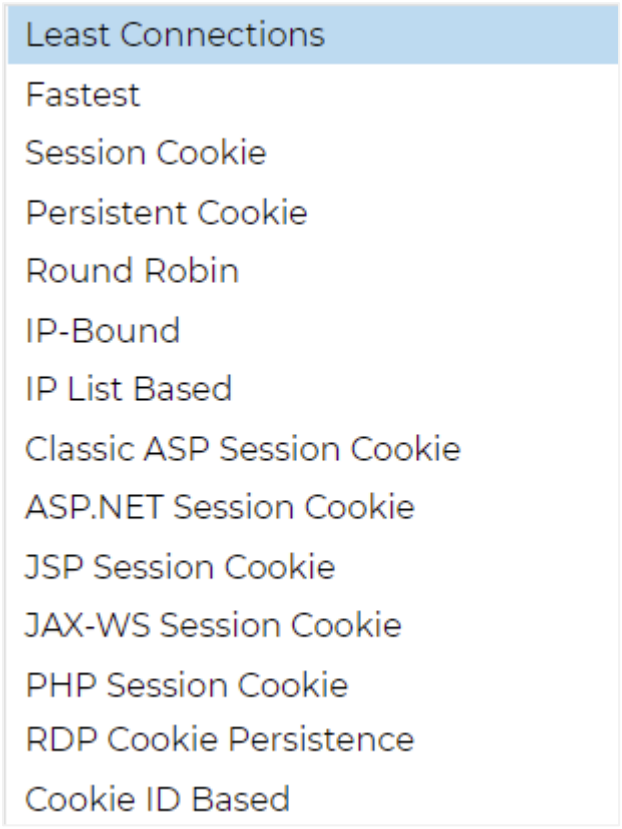
Das ID-Feld wird innerhalb der Cookie-ID-Lastausgleichsrichtlinie verwendet. Die hier platzierte ID-Nummer wird verwendet, um zu identifizieren

Basic



Lastausgleichsrichtlinie

Die Dropdown-Liste zeigt Ihnen die aktuell unterstützten Lastausgleichsrichtlinien an, die zur Verwendung zur Verfügung stehen. Eine Liste der Lastausgleichsrichtlinien, zusammen mit einer Erklärung, finden Sie unten.



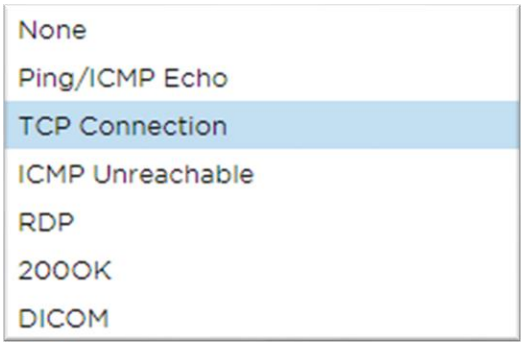
Option	Beschreibung
Schnellste	Die Richtlinie Schnellster Lastausgleich berechnet automatisch die Antwortzeit für alle Anfragen pro Server geglättet über die Zeit. Die Spalte Berechnetes Gewicht enthält den automatisch berechneten Wert. Eine manuelle Eingabe ist nur bei Verwendung dieser Lastausgleichsrichtlinie möglich.
Runde Robin	Round Robin wird häufig in Firewalls und einfachen Lastverteilern verwendet und ist die einfachste Methode. Jeder Real Server erhält nacheinander eine neue Anfrage. Diese Methode ist nur dann geeignet, wenn Sie einen gleichmäßigen Lastausgleich zwischen den Servern vornehmen müssen; ein Beispiel dafür wären Lookup-Webserver. Wenn Sie jedoch einen Lastausgleich basierend auf der Anwendungslast oder der Serverlast benötigen oder sogar sicherstellen müssen, dass Sie denselben Server für die Sitzung verwenden, ist die Round-Robin-Methode ungeeignet.
Geringste Verbindungen	Der Load Balancer behält die Anzahl der aktuellen Verbindungen zu jedem Real Server im Auge. Der Real Server mit der geringsten Anzahl von Verbindungen erhält die nachfolgende neue Anfrage.
Layer 3 Session Affinity/Persistence - IP Bound	In diesem Modus bildet die IP-Adresse des Clients die Grundlage für die Auswahl des Real-Servers, der die Anfrage erhalten soll. Diese Aktion bietet Persistenz. HTTP und Layer-4-Protokolle können diesen Modus verwenden. Diese Methode ist hilfreich für interne Netzwerke, in denen die Netzwerktopologie bekannt ist und Sie sicher sein können, dass keine "Super-Proxys" vorgeschaltet sind. Bei Layer 4 und Proxies können alle Anfragen so aussehen, als kämen sie von einem einzigen Client, so dass die Last nicht gleichmäßig wäre. Bei HTTP wird die Header-Information (X-Forwarder-For) verwendet, wenn sie vorhanden ist, um mit Proxys fertig zu werden.

Layer 3 Sitzungsaffinität/Persistenz - IP-Listenbasiert	Die Verbindung zum Real-Server wird mit "Least connections" initiiert, dann wird eine Sitzungsaffinität basierend auf der IP-Adresse des Clients erreicht. Standardmäßig wird eine Liste für 2 Stunden aufrechterhalten, aber dies kann mit einem jetPACK geändert werden.
Schicht 7 Session-Affinität/Persistenz - Session-Cookie	Dieser Modus ist die beliebteste Persistenzmethode für den HTTP-Lastausgleich. In diesem Modus verwendet der ADC den IP-Listen-basierten Lastausgleich für jede erste Anfrage. Er fügt ein Cookie in die Header der ersten HTTP-Antwort ein. Danach verwendet der ADC das Client-Cookie, um den Datenverkehr an denselben Back-End-Server zu leiten. Dieses Cookie wird für die Persistenz verwendet, wenn der Client jedes Mal zum gleichen Back-End-Server gehen muss. Das Cookie läuft ab, sobald die Sitzung geschlossen wird.
Schicht 7 Sitzungsaffinität/Persistenz - Persistentes Cookie	Der IP-Listen-basierte Lastausgleichsmodus wird für jede erste Anfrage verwendet. Die ADC fügt ein Cookie in die Header der ersten HTTP-Antwort ein. Danach verwendet die ADC das Client-Cookie, um den Datenverkehr an denselben Back-End-Server zu leiten. Dieses Cookie wird für die Persistenz verwendet, wenn der Client jedes Mal zum gleichen Back-End-Server gehen muss. Das Cookie läuft nach 2 Stunden ab und die Verbindung wird nach einem IP-Listen-basierten Algorithmus ausgeglichen. Diese Verfallszeit ist mit einem jetPACK konfigurierbar.
Session-Cookie - Klassisches ASP-Session-Cookie	Active Server Pages (ASP) ist eine serverseitige Technologie von Microsoft. Wenn diese Option ausgewählt ist, behält das ADC die Sitzung auf demselben Server bei, wenn ein ASP-Cookie erkannt und in seiner Liste der bekannten Cookies gefunden wird. Bei der Erkennung eines neuen ASP-Cookies wird ein Lastausgleich mit dem Algorithmus der kleinsten Verbindungen durchgeführt.
Sitzungs-Cookie - ASP.NET-Sitzungs-Cookie	Dieser Modus gilt für **ASP.net.** Wenn dieser Modus ausgewählt ist, behält das ADC die Sitzungspersistenz zum selben Server bei, wenn ein ASP.NET-Cookie erkannt und in seiner Liste der bekannten Cookies gefunden wird. Bei Erkennung eines neuen ASP-Cookies wird ein Lastausgleich mit dem Algorithmus der kleinsten Verbindungen durchgeführt.
Session-Cookie - JSP-Session-Cookie	Java Server Pages (JSP) ist eine serverseitige Technologie von Oracle. Wenn dieser Modus ausgewählt ist, behält das ADC die Sitzungspersistenz auf demselben Server bei, wenn ein JSP-Cookie erkannt und in seiner Liste der bekannten Cookies gefunden wird. Bei der Erkennung eines neuen JSP-Cookies wird ein Lastausgleich mit Hilfe des Algorithmus der kleinsten Verbindungen durchgeführt.
Sitzungs-Cookie - JAX-WS Sitzungs-Cookie	Java Web Services (JAX-WS) ist eine serverseitige Technologie von Oracle. Wenn dieser Modus ausgewählt ist, behält das ADC die Sitzung auf demselben Server bei, wenn ein JAX-WS-Cookie erkannt und in seiner Liste der bekannten Cookies gefunden wird. Bei Erkennung eines neuen JAX-WS-Cookies wird ein Lastausgleich mit Hilfe des Algorithmus der kleinsten Verbindungen durchgeführt.
Session-Cookie - PHP-Session-Cookie	Personal Home Page (PHP) ist eine serverseitige Open-Source-Technologie. Wenn dieser Modus ausgewählt ist, behält das ADC die Sitzungspersistenz auf demselben Server bei, wenn ein PHP-Cookie erkannt wird.
Sitzungs-Cookie - RDP-Cookie Persistenz	Diese Lastausgleichsmethode verwendet das von Microsoft erstellte RDP-Cookie, das auf Benutzername/Domäne basiert, um die Verbindung zu einem Server aufrechtzuerhalten. Der Vorteil dieser Methode ist, dass die

	Aufrechterhaltung einer Verbindung zu einem Server auch dann möglich ist, wenn sich die IP-Adresse des Clients ändert.
Cookie-ID-basiert	Eine neue Methode, die "PhpCookieBased" und anderen Lastausgleichsmethoden sehr ähnlich ist, aber CookieIDBased und Cookie RegEx h=[^;]+ verwendet. Diese Methode verwendet den Wert, der im Notizfeld "ID=X;" des Real-Servers eingestellt ist, als Cookie-Wert zur Identifizierung des Servers. Es handelt sich also um eine ähnliche Methode wie CookieListBased, verwendet aber einen anderen Cookie-Namen und speichert einen eindeutigen Cookie-Wert, nicht die verschlüsselte IP, sondern die ID vom Realen Server (die zur Ladezeit eingelesen wird). Der Standardwert ist CookieIDName="h"; wenn es jedoch einen Überschreibungswert in der Konfiguration der erweiterten Einstellungen des virtuellen Servers gibt, verwenden Sie stattdessen diesen. **HINWEIS**: Wenn dieser Wert gesetzt ist, überschreiben wir den obigen Cookie-Ausdruck, um h= durch den neuen Wert zu ersetzen. Der letzte Punkt ist, dass, wenn ein unbekannter Cookie-Wert eintrifft und mit einer der Real-Server-IDs übereinstimmt, dieser Server ausgewählt werden soll; andernfalls verwenden Sie die nächste Methode (delegieren.)

Server-Überwachung

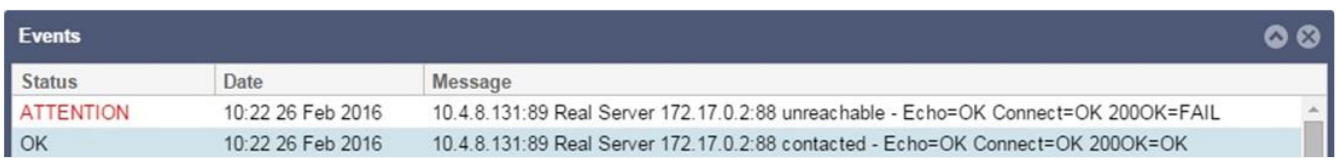
Ihr ADC enthält sechs standardmäßige Real-Server-Überwachungsmethoden, die unten aufgeführt sind.



Wählen Sie die Überwachungsmethode, die Sie auf den virtuellen Dienst (VIP) anwenden möchten.

Es ist wichtig, dass Sie den richtigen Monitor für den Dienst wählen. Wenn der Real-Server z. B. ein RDP-Server ist, ist ein 200OK-Monitor nicht relevant. Wenn Sie sich nicht sicher sind, welchen Monitor Sie wählen sollen, ist die Standard-TCP-Verbindung ein hervorragender Startpunkt.

Sie können mehrere Monitore auswählen, indem Sie nacheinander auf jeden Monitor klicken, den Sie auf den Dienst anwenden möchten. Die ausgewählten Monitore werden in der Reihenfolge ausgeführt, in der Sie sie auswählen; beginnen Sie also mit den Monitoren der unteren Schichten zuerst. Wenn Sie z. B. die Monitore Ping/ICMP Echo, TCP-Verbindung und 200OK einstellen, werden die Ereignisse im Dashboard wie in der folgenden Abbildung dargestellt:



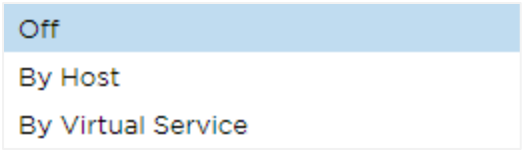
Wir können sehen, dass Layer 3 Ping und Layer 4 TCP Connect erfolgreich waren, wenn wir die obere Zeile betrachten, aber Layer 7 200OK ist fehlgeschlagen. Diese Überwachungsergebnisse liefern genügend Informationen, um anzuzeigen, dass das Routing in Ordnung ist und ein Dienst auf dem entsprechenden Port läuft, aber die Website nicht korrekt auf die angeforderte Seite antwortet. Es ist nun an der Zeit, sich den Webserver und den Abschnitt Bibliothek > Real Server Monitor anzusehen, um die Details des fehlgeschlagenen Monitors zu sehen.

Option	Beschreibung
Keine	In diesem Modus wird der Real-Server nicht überwacht und läuft immer korrekt. Die Einstellung Keine ist hilfreich für Situationen, in denen die Überwachung einen Server stört, und für Dienste, die nicht an der Failover-Aktion des ADC teilnehmen sollen. Es ist ein Weg, um unzuverlässige oder ältere Systeme zu hosten, die nicht primär für den H/A-Betrieb sind. Verwenden Sie diese Überwachungsmethode mit jedem Diensttyp.
Ping/ICMP-Echo	In diesem Modus sendet der ADC eine ICMP-Echo-Anfrage an die IP des Content-Servers. Wenn eine gültige Echo-Antwort empfangen wird, betrachtet der ADC den Real-Server als betriebsbereit, und der Verkehrsdurchsatz zum Server wird fortgesetzt. Außerdem wird der Dienst auf einem H/A-Paar verfügbar gehalten. Diese Überwachungsmethode ist mit jedem Diensttyp verwendbar.
TCP-Verbindung	In diesem Modus wird eine TCP-Verbindung zum Real-Server hergestellt und sofort wieder unterbrochen, ohne Daten zu senden. Wenn die Verbindung erfolgreich ist, hält die ADC den Real-Server für betriebsbereit. Diese Überwachungsmethode ist mit jedem Diensttyp verwendbar. Nur UDP-Dienste sind derzeit nicht für die TCP-Verbindungsüberwachung geeignet.
ICMP unerreichbar	Der ADC sendet eine UDP-Zustandsprüfung an den Server und markiert den Real-Server als nicht verfügbar, wenn er eine ICMP-Port-Unreachable-Meldung erhält. Diese Methode kann hilfreich sein, wenn Sie prüfen müssen, ob ein UDP-Dienstport auf einem Server verfügbar ist, wie z. B. DNS-Port 53.
RDP	In diesem Modus wird eine TCP-Verbindung initialisiert, wie in der Methode ICMP Unreachable beschrieben. Nachdem die Verbindung initialisiert wurde, wird eine Layer-7-RDP-Verbindung angefordert. Wenn die Verbindung bestätigt wird, hält der ADC den Real Server für betriebsbereit. Diese Überwachungsmethode ist mit jedem Microsoft-Terminalserver verwendbar.
200 OK	Bei dieser Methode wird eine TCP-Verbindung zum Real-Server initialisiert. Nachdem die Verbindung erfolgreich hergestellt wurde, sendet der ADC eine HTTP-Anfrage an den Real-Server. Es wird auf eine HTTP-Antwort gewartet und auf den Antwortcode "200 OK" geprüft. Wenn der Antwortcode "200 OK" empfangen wird, betrachtet die ADC den Real-Server als betriebsbereit. Wenn die ADC aus irgendeinem Grund keinen "200 OK"-Antwortcode erhält, einschließlich Timeouts, Verbindungsabbrüche und andere Gründe, markiert die ADC den Real Server als nicht verfügbar. Diese Überwachungsmethode ist nur für die Verwendung mit HTTP- und beschleunigten HTTP-Diensttypen gültig. Wenn ein Layer 4-Diensttyp für einen HTTP-Server verwendet wird, ist er verwendbar, wenn SSL auf dem Real-Server nicht verwendet wird oder durch die "Content SSL"-Funktion entsprechend gehandhabt wird.
DICOM	Eine TCP-Verbindung zum Real-Server wird im DICOM-Modus initialisiert, und beim Verbindungsaufbau wird eine Echoscu-"Associate Request" an den Real-Server gesendet. Eine Konversation, die ein "Associate Accept" vom Content Server, eine Übertragung einer kleinen Datenmenge, gefolgt von einem "Release Request" und einer "Release Response" umfasst, schließt den Monitor erfolgreich ab. Wenn der Monitor aus irgendeinem Grund nicht erfolgreich abgeschlossen werden kann, wird der Real-Server als ausgefallen betrachtet.

Benutzerdefiniert	Jeder Monitor, der im Abschnitt Real-Server-Überwachung konfiguriert wurde, erscheint in der Liste.

Caching-Strategie

Standardmäßig ist die Caching-Strategie deaktiviert und auf Aus eingestellt. Wenn Ihr Diensttyp HTTP ist, dann können Sie zwei Arten von Caching-Strategie anwenden.



Auf der Seite Cache konfigurieren können Sie detaillierte Cache-Einstellungen vornehmen. Beachten Sie, dass bei der Anwendung von Caching auf ein VIP mit dem Diensttyp Beschleunigtes "HTTP" komprimierte Objekte nicht gecached werden.

Option	Beschreibung
Nach Host	Das Caching pro Host basiert auf der Anwendung pro Hostname. Für jede Domain/jeden Hostnamen existiert ein eigener Cache. Dieser Modus ist ideal für Webserver, die je nach Domain mehrere Websites bedienen können.
Durch virtuellen Service	Caching pro virtuellem Dienst ist verfügbar, wenn Sie diese Option wählen. Es wird nur ein Cache für alle Domänen/Hostnamen existieren, die den virtuellen Dienst durchlaufen. Diese Option ist eine spezielle Einstellung für die Verwendung mit mehreren Klonen einer einzelnen Site.

Beschleunigung

Option	Beschreibung
Aus	Schalten Sie die Komprimierung für den virtuellen Dienst aus
Komprimierung	Wenn diese Option ausgewählt ist, schaltet sie die Komprimierung für den ausgewählten virtuellen Dienst ein. Das ADC komprimiert den Datenstrom zum Client auf Anfrage dynamisch. Dieser Vorgang gilt nur für Objekte, die den Header content-encoding: gzip enthalten. Beispielinhalte sind HTML, CSS oder Javascript. Sie können auch bestimmte Inhaltstypen ausschließen, indem Sie den Abschnitt Globale Ausschlüsse verwenden.

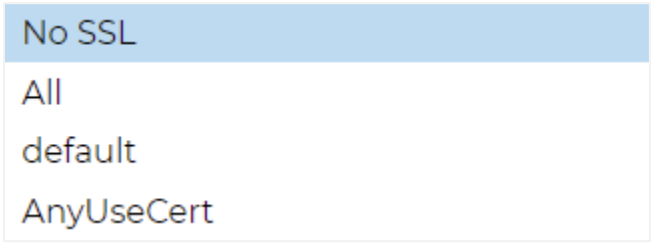
Hinweis: Wenn das Objekt cachefähig ist, speichert die ADC eine komprimierte Version und stellt diese statisch (aus dem Speicher) bereit, bis der Inhalt abläuft und erneut validiert wird.

Virtual Service SSL-Zertifikat (Verschlüsselung zwischen Client und ADC)

Standardmäßig ist die Einstellung "Kein SSL". Wenn Ihr Diensttyp "HTTP" oder "Layer4 TCP" ist, können Sie aus dem Dropdown-Menü ein Zertifikat auswählen, das auf den virtuellen Dienst angewendet werden soll. Zertifikate, die erstellt oder importiert wurden, werden in dieser Liste angezeigt. Sie können mehrere Zertifikate markieren, um sie auf einen Dienst anzuwenden. Dieser Vorgang aktiviert automatisch die SNI-Erweiterung, um ein Zertifikat basierend auf dem vom Client angeforderten "Domain Name" zuzulassen.

Anzeige des Servernamens

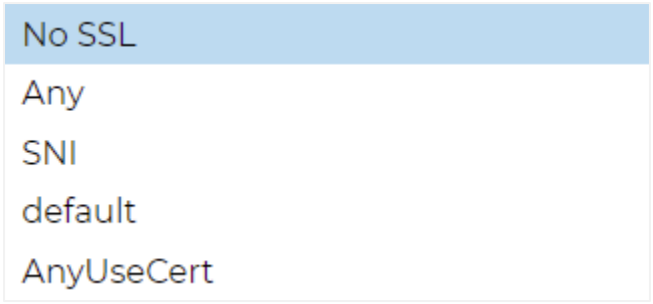
Diese Option ist eine Erweiterung des TLS-Netzwerkprotokolls, mit der der Client zu Beginn des Handshaking-Prozesses angibt, mit welchem Hostnamen er sich zu verbinden versucht. Diese Einstellung ermöglicht es dem ADC, mehrere Zertifikate auf derselben virtuellen IP-Adresse und demselben TCP-Port zu präsentieren.



Option	Beschreibung
Kein SSL	Der Verkehr von der Quelle zum ADC wird nicht verschlüsselt.
Alle	Lädt alle verfügbaren Zertifikate zur Verwendung
Standard	Diese Option führt dazu, dass ein lokal erstelltes Zertifikat namens "Standard" auf die Browserseite des Kanals angewendet wird. Verwenden Sie diese Option, um SSL zu testen, wenn noch keins erstellt oder importiert wurde.
AnyUseCert	Verwenden Sie ein auf dem ADC vorhandenes Zertifikat, das der Benutzer hochgeladen oder generiert hat

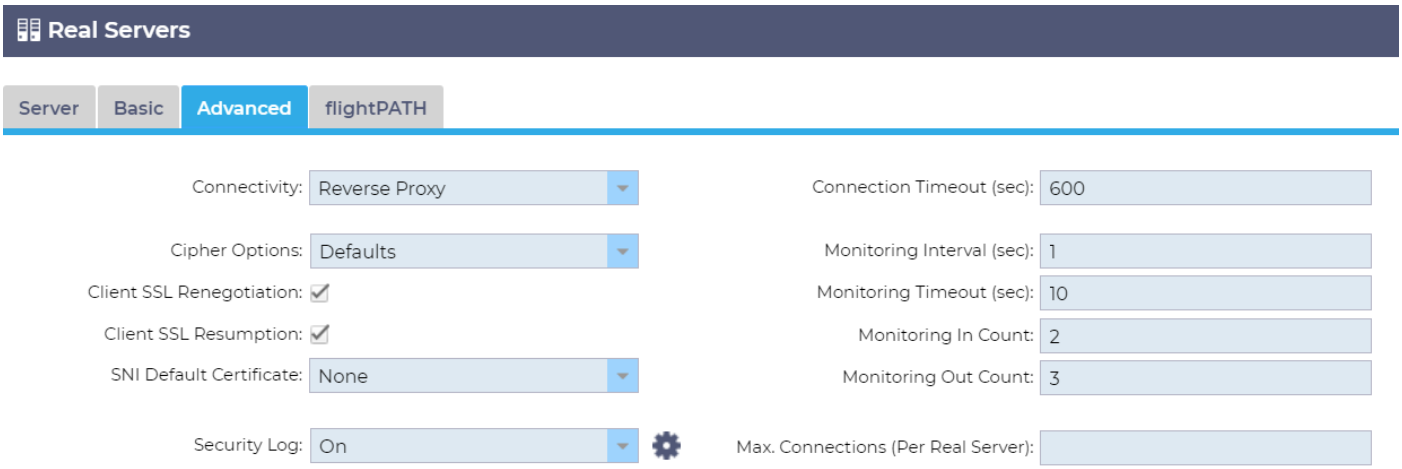
Real Server SSL-Zertifikat (Verschlüsselung zwischen dem ADC und Real Server)

Die Standardeinstellung für diese Option ist Kein SSL. Wenn Ihr Server eine verschlüsselte Verbindung erfordert, muss dieser Wert etwas anderes als Kein SSL sein. Zertifikate, die erstellt oder importiert wurden, werden in dieser Liste angezeigt.



Option	Beschreibung
Kein SSL	Der Verkehr vom ADC zum Real-Server wird nicht verschlüsselt. Die Auswahl eines Zertifikats auf der Browserseite bedeutet, dass "No SSL" clientseitig gewählt werden kann, um eine so genannte "SSL-Offload" zu ermöglichen.
Beliebig	Der ADC agiert als Client und akzeptiert jedes Zertifikat, das der Real-Server vorlegt. Der Datenverkehr vom ADC zum Real Server wird verschlüsselt, wenn diese Option ausgewählt ist. Verwenden Sie die Option "Beliebig", wenn auf der Seite des virtuellen Dienstes ein Zertifikat angegeben ist, wodurch eine sogenannte "SSL-Überbrückung" oder "SSL-Wiederverschlüsselung" bereitgestellt wird.
SNI	Der ADC agiert als Client und akzeptiert jedes Zertifikat, das der Real-Server vorlegt. Der Datenverkehr vom ADC zum Real Server wird verschlüsselt, wenn dies ausgewählt ist. Verwenden Sie die Option "Beliebig", wenn ein Zertifikat auf der Seite des virtuellen Dienstes angegeben ist, wodurch eine so genannte "SSL-Überbrückung" oder "SSL-Neuverschlüsselung" bereitgestellt wird. Wählen Sie diese Option, um SNI auf der Server-Seite zu aktivieren.
AnyUseCert	Hier erscheinen alle Zertifikate, die Sie erzeugt oder in den ADC importiert haben.

Erweitert



Konnektivität

Ihr virtueller Dienst ist mit vier verschiedenen Arten von Konnektivität konfigurierbar. Bitte wählen Sie den Konnektivitätsmodus, der für den Dienst gelten soll.

Option	Beschreibung
Umgekehrter Proxy	Reverse Proxy ist der Standardwert und arbeitet auf Layer7 mit Komprimierung und Caching. Und auf Layer4 ohne Caching und Komprimierung. In diesem Modus fungiert Ihr ADC als Reverse-Proxy und wird zur Quelladresse, die von den Real-Servern gesehen wird.
Direkte Server-Rückgabe	Direct Server Return oder DSR, wie es weithin bekannt ist (DR - Direct Routing in einigen Kreisen), ermöglicht es dem Server hinter dem Load Balancer, direkt auf den Client zu antworten, indem er den ADC bei der Antwort umgeht. DSR ist nur für den Einsatz mit Layer 4-Lastausgleich geeignet. Daher sind Caching und Komprimierung bei dieser gewählten Option nicht verfügbar. Der Layer-7-Lastausgleich funktioniert nicht mit diesem DSR. Außerdem gibt es keine andere Persistenzunterstützung als IP-Listen-basiert. Der SSL/TLS-Lastausgleich mit dieser Methode ist nicht ideal, da nur die Quell-IP-Persistenzunterstützung verfügbar ist. DSR erfordert auch Änderungen am Real Server. Bitte lesen Sie den Abschnitt Änderungen am Real-Server.
Gateway	Im Gateway-Modus können Sie den gesamten Datenverkehr über den ADC leiten, so dass der Datenverkehr von den Real Servern über den ADC zu anderen Netzwerken über die ADC-Virtual Machines oder Hardware-Schnittstellen geleitet werden kann. Die Verwendung des Geräts als Gateway-Gerät für Real Server ist ideal, wenn es im Multi-Interface-Modus betrieben wird. Der Layer-7-Lastausgleich mit dieser Methode funktioniert nicht, da es keine Unterstützung für Persistenz gibt, außer IP-Listen-basiert. Diese Methode erfordert, dass der Real-Server sein Standard-Gateway auf die lokale Schnittstellenadresse (eth0, eth1, etc.) des ADCs setzt. Lesen Sie dazu den Abschnitt Real-Server-Änderungen. ***Bitte beachten Sie, dass der Gateway-Modus keine Ausfallsicherung in einer Cluster-Umgebung unterstützt.***

Chiffre-Optionen

Sie können Chiffren auf einer Ebene pro Dienst einstellen, und es ist nur für Dienste mit aktiviertem SSL/TLS relevant. Der ADC führt eine automatische Auswahl der Chiffre durch, und Sie können verschiedene Chiffren mit jetPACKS hinzufügen. Beim Hinzufügen des entsprechenden jetPACKs können

Sie die Cipher-Optionen pro Dienst einstellen. Dies hat den Vorteil, dass Sie mehrere Dienste mit unterschiedlichen Sicherheitsstufen erstellen können. Beachten Sie, dass ältere Clients nicht mit neueren Chiffren kompatibel sind, um die Anzahl der Clients zu reduzieren, je sicherer der Dienst ist.

Client SSL-Neuverhandlung

Aktivieren Sie dieses Kontrollkästchen, wenn Sie die vom Client initiierte SSL-Neuaushandlung zulassen wollen. Deaktivieren Sie die Client-SSL-Neuverhandlung, um mögliche DDOS-Angriffe gegen die SSL-Schicht zu verhindern, indem Sie diese Option deaktivieren.

Client-SSL-Wiederaufnahme

Aktivieren Sie dieses Kontrollkästchen, wenn Sie dem Sitzungscache hinzugefügte SSL Resumption Server-Sitzungen aktivieren möchten. Wenn ein Client die Wiederaufnahme einer Sitzung vorschlägt, versucht der Server, die Sitzung wieder aufzunehmen, falls er sie findet. Wenn Wiederaufnahme nicht aktiviert ist, findet kein Sitzungs-Caching für Client oder Server statt.

SNI-Standard-Zertifikat

Wenn bei einer SSL-Verbindung mit aktiviertem Client-seitigem SNI die angeforderte Domain mit keinem der dem Dienst zugewiesenen Zertifikate übereinstimmt, präsentiert der ADC das SNI-Standardzertifikat. Die Standardeinstellung hierfür ist Keines, was die Verbindung effektiv abbrechen würde, wenn es keine exakte Übereinstimmung gibt. Wählen Sie eines der installierten Zertifikate aus dem Dropdown-Menü, um es zu präsentieren, wenn eine exakte SSL-Zertifikatsübereinstimmung fehlschlägt.

Sicherheits-Log

'Ein' ist der Standardwert und aktiviert auf einer Pro-Service-Basis den Dienst der Protokollierung von Authentifizierungsinformationen in den W3C-Protokollen. Wenn Sie auf das Zahnradsymbol klicken, gelangen Sie zur Seite System > Protokollierung, auf der Sie die Einstellungen der W3C-Protokollierung überprüfen können.

Zeitüberschreitung der Verbindung

Der Standard-Timeout für die Verbindung beträgt 600 Sekunden oder 10 Minuten. Diese Einstellung passt die Zeit an, nach der die Verbindung bei keiner Aktivität einen Timeout erleidet. Verringern Sie diesen Wert für kurzlebigen zustandslosen Webverkehr, der typischerweise 90 Sekunden oder weniger beträgt. Erhöhen Sie diesen Wert für zustandsabhängige Verbindungen wie RDP auf etwa 7200 Sekunden (2 Stunden) oder mehr, abhängig von Ihrer Infrastruktur. Das RDP-Timeout-Beispiel bedeutet, dass die Verbindungen offen bleiben, wenn ein Benutzer eine Inaktivitätsperiode von 2 Stunden oder weniger hat.

Überwachungseinstellungen

Diese Einstellungen beziehen sich auf die Real-Server-Monitore auf der Registerkarte Basis. Es gibt globale Einträge in der Konfiguration, um die Anzahl der erfolgreichen oder fehlgeschlagenen Monitore zu zählen, bevor der Status eines Servers als online oder fehlgeschlagen markiert wird.

Intervall

Das Intervall ist die Zeit in Sekunden zwischen den Monitoren. Das Standardintervall ist 1 Sekunde. Während 1s für die meisten Anwendungen akzeptabel ist, kann es für andere oder während des Testens von Vorteil sein, dies zu erhöhen.

Überwachung Timeout

Der Timeout-Wert gibt an, wann das ADC auf die Antwort eines Servers auf eine Verbindungsanfrage wartet. Der Standardwert ist 2s. Erhöhen Sie diesen Wert für ausgelastete Server.

Überwachung in Count

Der Standardwert für diese Einstellung ist 2. Der Wert 2 gibt an, dass der Real-Server zwei erfolgreiche Health-Monitor-Prüfungen bestehen muss, bevor er online geht. Wenn Sie diesen Wert erhöhen, erhöht sich die Wahrscheinlichkeit, dass der Server Datenverkehr bedienen kann, aber es dauert je nach Intervall länger, bis er in Betrieb geht. Durch Verringern dieses Wertes wird der Server früher in Betrieb genommen.

Überwachung der Auszählung

Der Standardwert für diese Einstellung ist 3, was bedeutet, dass der Real-Server-Monitor dreimal fehlschlagen muss, bevor der ADC aufhört, Datenverkehr an den Server zu senden, und dieser als ROT und unerreichbar markiert wird. Das Erhöhen dieser Zahl führt zu einem besseren und zuverlässigeren Dienst auf Kosten der Zeit, die der ADC benötigt, um das Senden von Datenverkehr an diesen Server zu stoppen.

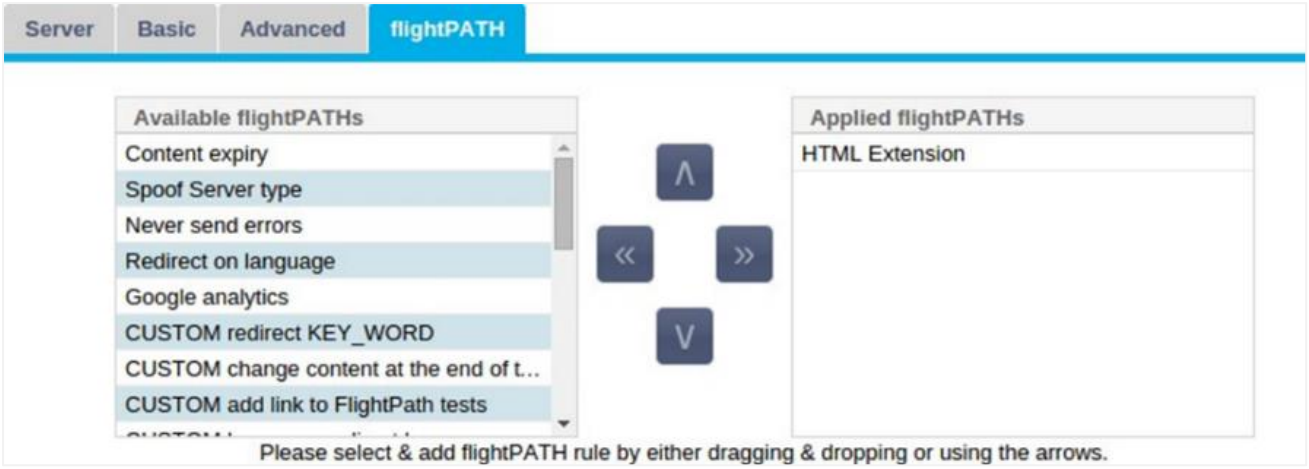
Bei Ausfall auf Offline schalten

Wenn diese Option aktiviert ist, werden die Real-Server, deren Gesundheitsprüfung fehlschlägt, offline gestellt und können nur manuell online gestellt werden.

Max. Verbindungen

Begrenzt die Anzahl der gleichzeitigen Real-Server-Verbindungen und wird pro Dienst eingestellt. Wenn Sie dies z. B. auf 1000 konfigurieren und zwei Real Server haben, begrenzt der ADC **jeden** Real Server auf 1000 gleichzeitige Verbindungen. Sie können auch eine Seite "Server zu beschäftigt" anzeigen lassen, sobald dieses Limit auf allen Servern erreicht ist, damit die Benutzer verstehen, warum eine Nicht-Antwort oder eine Verzögerung aufgetreten ist. Lassen Sie dies leer für unbegrenzte Verbindungen. Was Sie hier einstellen, hängt von Ihren Systemressourcen ab.

flightPATH



flightPATH ist ein von Edgenexus entwickeltes System, das ausschließlich innerhalb des ADC verfügbar ist. Im Gegensatz zu den regelbasierten Engines anderer Anbieter arbeitet flightPATH nicht über eine Kommandozeile oder eine Skripteingabekonsole. Stattdessen verwendet es eine grafische Benutzeroberfläche, um die verschiedenen Parameter, Bedingungen und Aktionen auszuwählen, die ausgeführt werden sollen, um das zu erreichen, was sie brauchen. Diese Funktionen machen flightPATH extrem leistungsfähig und ermöglichen es Netzwerkadministratoren, den HTTPS-Verkehr auf äußerst effektive Weise zu manipulieren.

flightPATH ist nur für die Verwendung mit HTTPS-Verbindungen verfügbar, und dieser Abschnitt ist nicht sichtbar, wenn der Virtual Service Type nicht HTTP ist.

Wie Sie in der obigen Abbildung sehen können, befindet sich links eine Liste der verfügbaren Regeln und rechts die Regeln, die auf den virtuellen Dienst angewendet werden.

Fügen Sie eine verfügbare Regel hinzu, indem Sie die Regel von der linken Seite auf die rechte Seite ziehen oder eine Regel markieren und auf den Rechtspfeil klicken, um sie auf die rechte Seite zu verschieben.

Die Reihenfolge für die Ausführung ist entscheidend und beginnt mit der obersten Regel, die zuerst ausgeführt wird. Um die Reihenfolge der Ausführung zu ändern, markieren Sie die Regel und bewegen Sie sich mit den Pfeilen nach oben und unten.

Um eine Regel zu entfernen, ziehen Sie sie zurück in das Regelinventar auf der linken Seite oder markieren Sie die Regel und klicken Sie auf den Pfeil nach links.

Sie können flightPATH-Regeln im Abschnitt Konfigurieren von flightPATH in dieser Anleitung hinzufügen, entfernen und bearbeiten.

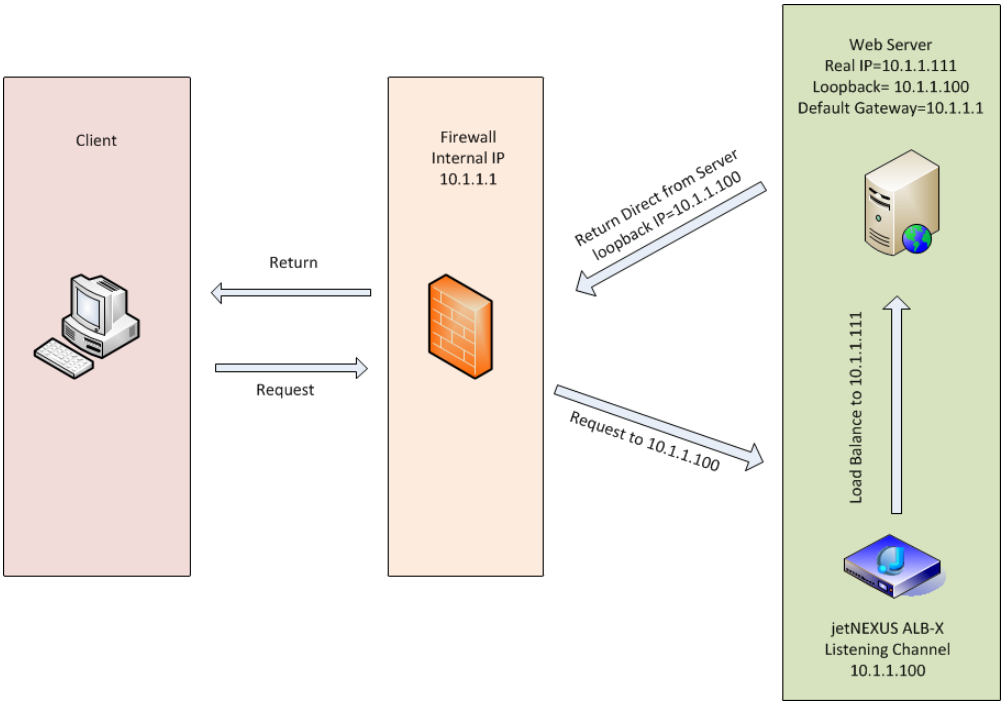
Reale Server-Änderungen für direkte Server-Rückgabe

Direct Server Return oder DSR, wie es weithin bekannt ist (DR - Direct Routing in einigen Kreisen), ermöglicht es dem Server hinter dem ADC, direkt an den Client zu antworten und den ADC bei der Antwort zu umgehen. DSR ist nur für den Einsatz mit Layer 4-Lastverteilung geeignet. Caching und Komprimierung sind bei Aktivierung nicht verfügbar.

Der Layer-7-Lastausgleich mit dieser Methode funktioniert nicht, da es außer der Quell-IP keine Persistenzunterstützung gibt. Der SSL/TLS-Lastausgleich mit dieser Methode ist nicht ideal, da es nur Quell-IP-Persistenz-Unterstützung gibt.

Wie es funktioniert

- Client sendet eine Anfrage an den jetNEXUS ALB-X
- Von edgeNEXUS empfangene Anfrage
- Anforderung wird an Content-Server weitergeleitet
- Antwort wird direkt an den Client gesendet, ohne den Umweg über edgeNEXUS



Erforderliche Content-Server-Konfiguration

Allgemein

- Das Standard-Gateway des Inhaltsservers sollte normal konfiguriert werden. (Nicht über den ADC)
- Der Content-Server und der Load Balancer müssen sich im selben Subnetz befinden

Windows

- Der Content-Server muss einen Loopback oder Alias haben, der mit der IP-Adresse des Channels oder VIPs konfiguriert ist
  - Netzwerk-Metrik muss 254 sein, um eine Antwort auf ARP-Anfragen zu verhindern
  - Hinzufügen eines Loopback-Adapters in Windows Server 2012 - Klicken Sie hier
  - Hinzufügen eines Loopback-Adapters in Windows Server 2003/2008 - Klicken Sie hier
- Führen Sie Folgendes in einer Eingabeaufforderung für jede Netzwerkschnittstelle aus, die Sie auf den Windows Real-Servern konfiguriert haben

netsh interface ipv4 set interface "Name der Windows-Netzwerkschnittstelle" weakhostreceive=enable

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

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

Linux

- Hinzufügen einer permanenten Loopback-Schnittstelle
- Bearbeiten Sie "/etc/sysconfig/network-scripts"

ifcfg-lo:1DEVICE=lo
:1IPADDR=x
.x.x.xNETMASK=255
.255.255.255BROADCAST=x
.x.x.xONBOOT=ja

- Bearbeiten Sie "/etc/sysctl.conf"

net.ipv4.conf.all.arp_ignore = 1net
.ipv4.conf.eth0.arp_ignore = 1net
.ipv4.conf.eht1.arp_ignore = 1net
.ipv4.conf.all.arp_announce = 2net
.ipv4.conf.eth0.arp_announce = 2net
.ipv4.conf.eth1.arp_announce = 2

- Führen Sie "sysctl - p" aus

Real Server Änderungen - Gateway-Modus

Im Gateway-Modus können Sie den gesamten Datenverkehr über den ADC leiten. Dadurch kann der von den Inhaltsservern ausgehende Datenverkehr über den ADC in andere Netzwerke über die Schnittstellen des ADC-Geräts geleitet werden. Die Verwendung des Geräts als Gateway-Gerät für Inhaltsserver sollte im Multi-Interface-Modus verwendet werden.

Wie es funktioniert

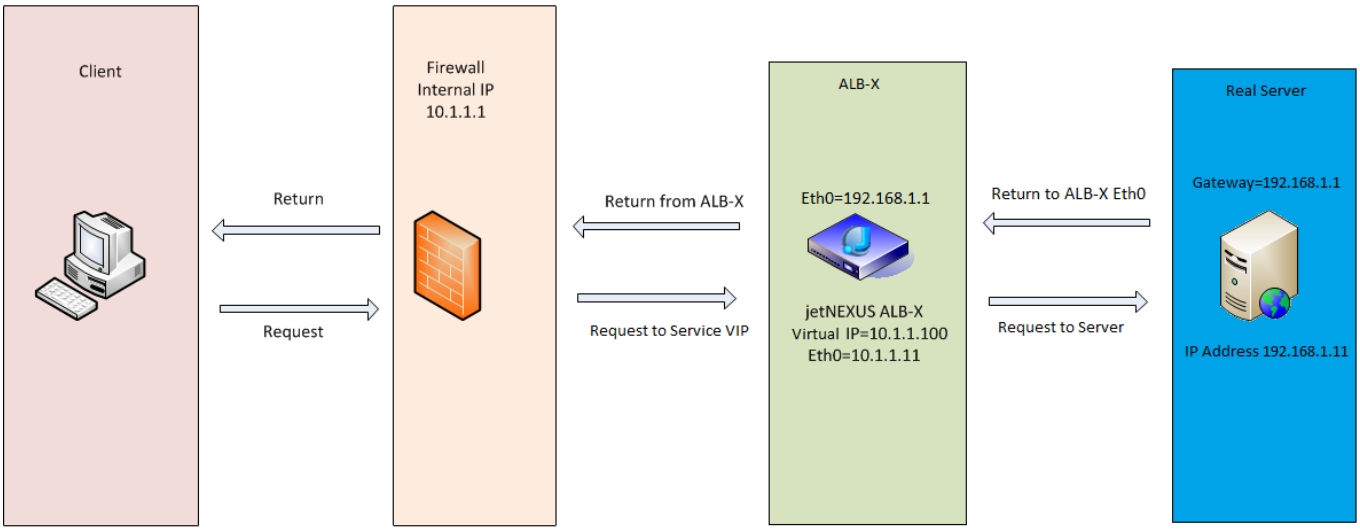
- Der Client sendet eine Anfrage an den jetNEXUS ALB-X
- Eine Anfrage wird von edgeNEXUS empfangen

- Anfrage an Content-Server gesendet
- Antwort an edgeNEXUS gesendet
- ADC leitet die Antwort an den Client weiter

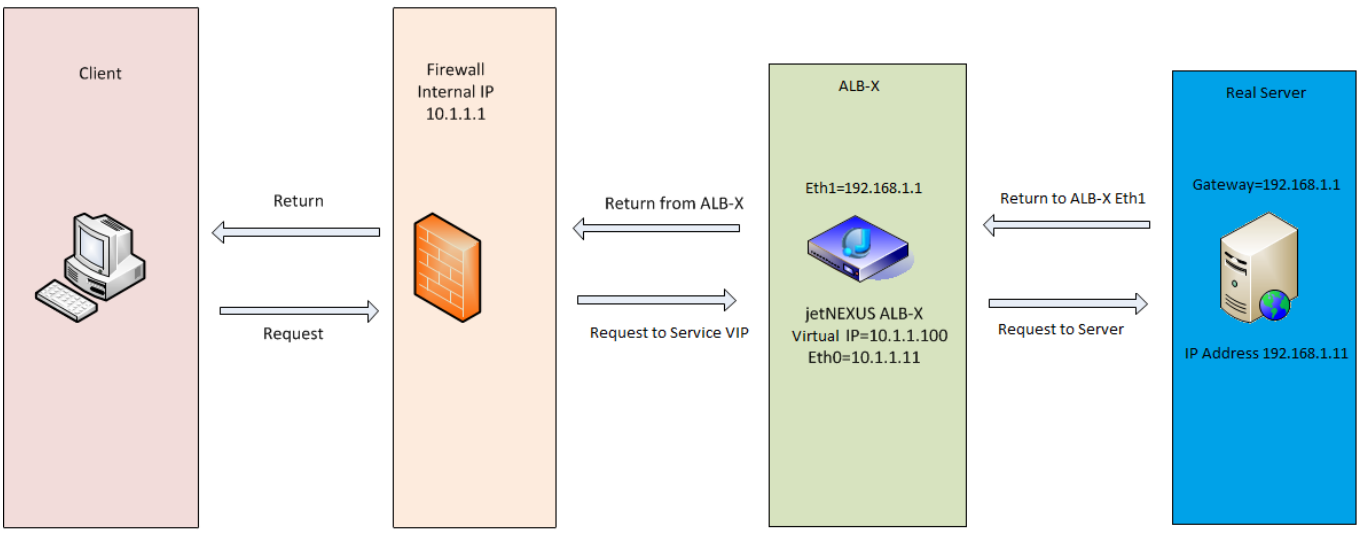
Erforderliche Content-Server-Konfiguration

- Einzelarm-Modus - eine Schnittstelle wird verwendet, aber das Service-VIP und die Real-Server müssen sich in verschiedenen Subnetzen befinden.
- Dual-Arm-Modus - es werden zwei Schnittstellen verwendet, aber der Service-VIP und die realen Server müssen sich in unterschiedlichen Subnetzen befinden.
- In jedem Fall, Single und Dual Arm, müssen die Real-Server ihr Standard-Gateway auf die ADC-Schnittstellenadresse im jeweiligen Subnetz konfigurieren.

Beispiel für einen einzelnen Arm



Dual Arm Beispiel



Bibliothek

Add-Ons

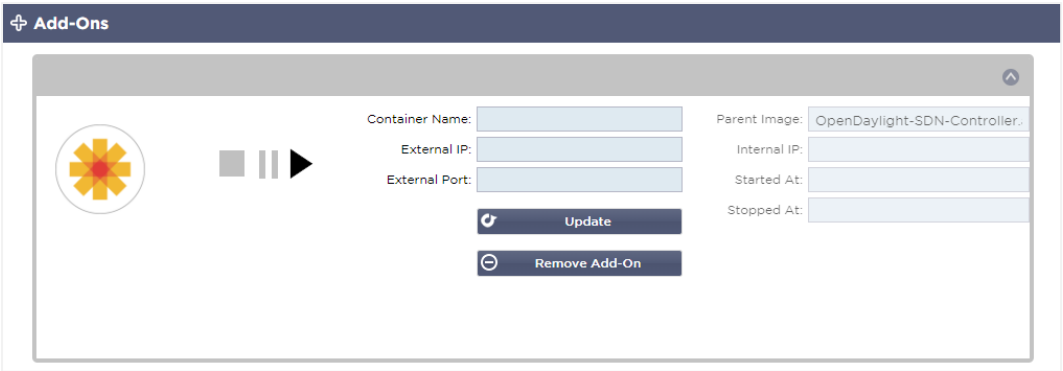
Add-ons sind Docker-basierte Container, die in einem isolierten Modus innerhalb der ADC laufen können. Beispiele für Add-ons könnten eine Anwendungs-Firewall oder sogar eine Mikro-Instanz des ADC selbst sein.

Apps

Der Abschnitt Apps innerhalb von Add-Ons enthält Details zu den Apps, die Sie gekauft, heruntergeladen und eingesetzt haben.

Wenn keine Apps vorhanden sind, wird in diesem Bereich eine Meldung angezeigt, die Sie auffordert, zum Bereich Apps zu gehen und eine App herunterzuladen und einzusetzen.

Sobald Sie eine App bereitstellen, wird sie im Bereich Apps angezeigt.



Kauf eines Add-ons

Um eine App zu kaufen, müssen Sie sich im App Store registrieren. Der Kauf wird über den ADC selbst getätigt. Sie finden

Navigieren Sie zur Seite Bibliothek > Apps im ADC-Dashboard.

Hier können Sie die App auswählen, die Sie herunterladen und dann installieren möchten.

Wenn Sie dies über das ADC-Dashboard tun, wählen Sie bitte nur 1 Element aus. Sie können mehrere ADC-Sets besitzen, und Anwendungen müssen dem ADC zugeordnet werden, auf dem sie bereitgestellt werden.

Wenn Sie über Ihren Desktop und Browser auf den App Store zugreifen, können Sie so viele herunterladen, wie Sie möchten. Zum Beispiel vier Instanzen der WAF oder GSLB. Sie werden im Bereich "Gekaufte Apps" Ihres ADCs angezeigt, so dass Sie sie herunterladen können.

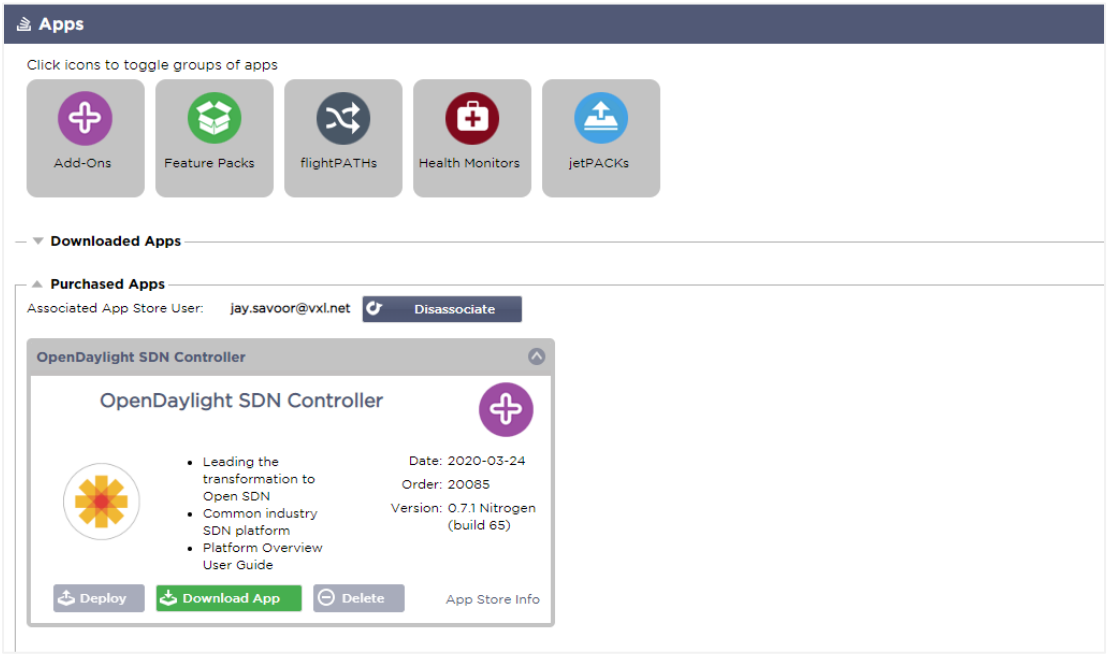
Die Apps verbinden sich mit den ADCs, die Sie besitzen und registriert haben.

Wenn Sie sich für das Herunterladen einer App entscheiden, werden Sie nach der Geräte-ID gefragt, woraufhin die App verschlüsselt und mit der ADC-Geräte-ID verknüpft wird.

Die Links zum App Store sind:

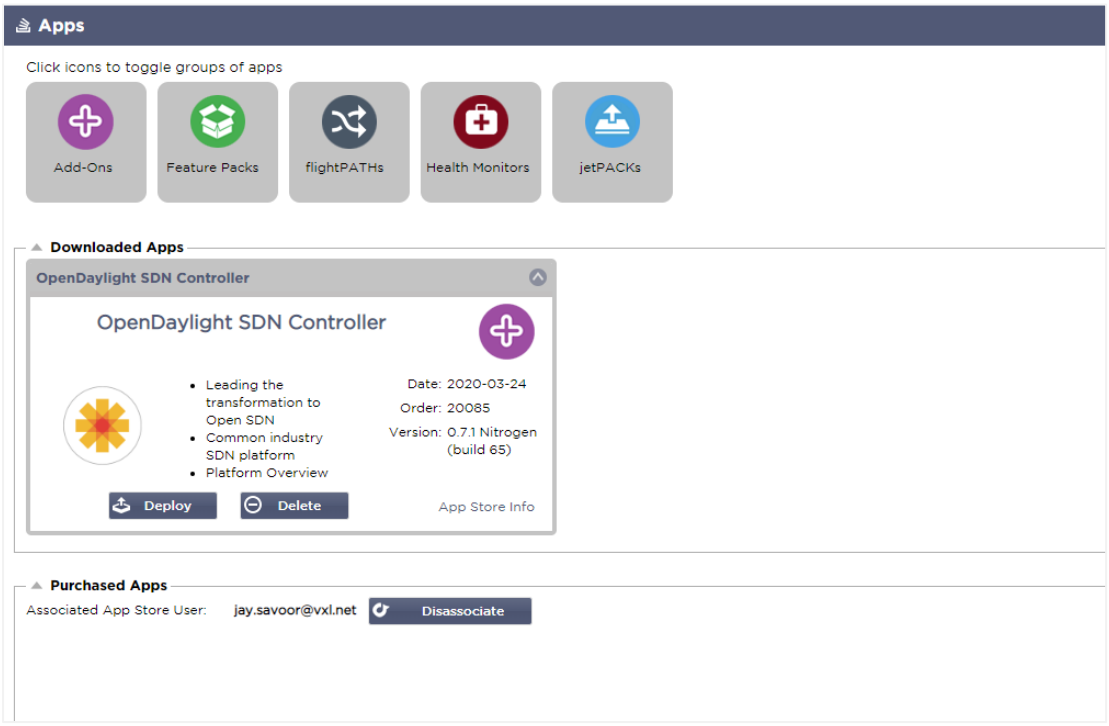
- Add-Ons: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/ADD-ONS/**
- Gesundheits-Monitore: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/SERVER-HEALTH-MONITORS/**
- jetPACKS: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/JETPACKS/**

- Feature Packs: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/EDGENEXUS-FEATURE-PACK/**
- flightPATH-Regeln: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/FLIGHTPATH/**
- Software-Aktualisierungen: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/EDGENEXUS-SOFTWARE-UPDATE/**



Bereitstellen einer App

Sobald die App auf den ADC heruntergeladen wurde, wird sie in den Bereich "Heruntergeladene Apps" verschoben und über die Schaltfläche "Bereitstellen" auf dem ADC bereitgestellt. Dieser Vorgang dauert einige Zeit, abhängig von den für den ADC verfügbaren Ressourcen. Nach der Bereitstellung erscheint sie im Bereich Heruntergeladene Apps.



Authentifizierung

Auf der Seite Bibliothek > Authentifizierung können Sie Authentifizierungsserver einrichten und Authentifizierungsregeln mit Optionen für client-seitiges Basic oder Forms und server-seitiges NTLM oder BASIC erstellen.

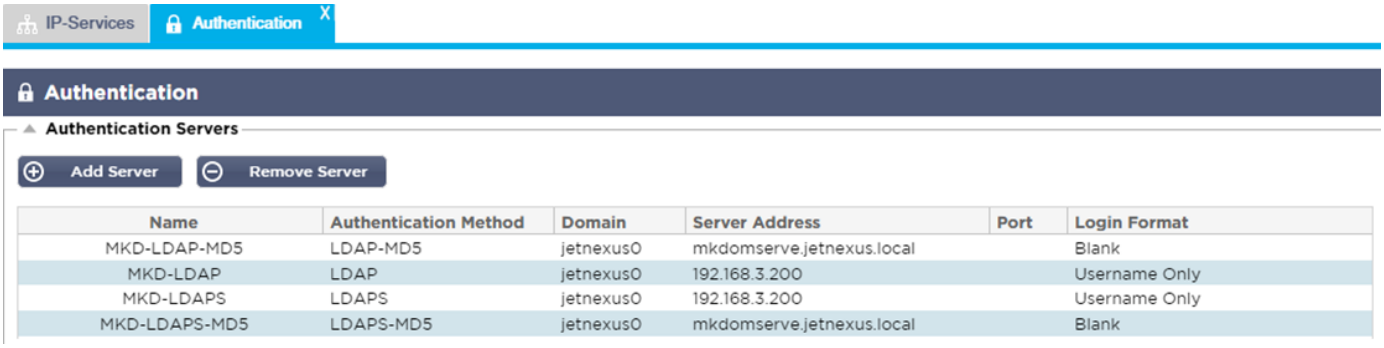
Einrichten der Authentifizierung - Ein Arbeitsablauf

Bitte führen Sie mindestens die folgenden Schritte aus, um die Authentifizierung für Ihren Dienst anzuwenden.

1. Erstellen Sie einen Authentifizierungsserver.
2. Erstellen Sie eine Authentifizierungsregel, die einen Authentifizierungsserver verwendet.
3. Erstellen Sie eine flightPATH-Regel, die eine Authentifizierungsregel verwendet.
4. Anwenden der flightPATH-Regel auf einen Dienst

Authentifizierungs-Server

Um eine funktionierende Authentifizierungsmethode einzurichten, müssen wir zunächst einen Authentifizierungsserver einrichten.



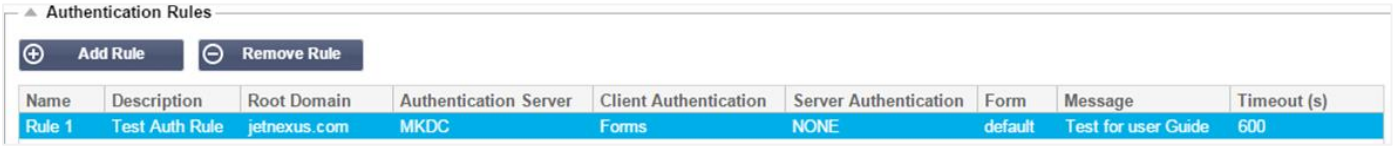
- Klicken Sie auf die Schaltfläche Server hinzufügen.
- Diese Aktion erzeugt eine leere Zeile, die zum Ausfüllen bereit ist.

Option	Beschreibung
Name	Geben Sie Ihrem Server einen Namen zur Identifizierung - dieser Name wird in den Regeln verwendet
Beschreibung	Eine Beschreibung hinzufügen
Methode zur Authentifizierung	Wählen Sie eine Authentifizierungsmethode LDAP - einfaches LDAP mit Benutzernamen und Passwörtern, die im Klartext an den LDAP-Server gesendet werden. LDAP-MD5 - einfaches LDAP mit Benutzernamen im Klartext und Passwort MD5-gehasht für erhöhte Sicherheit. LDAPS - LDAP über SSL. Sendet das Passwort im Klartext innerhalb eines verschlüsselten Tunnels zwischen dem ADC und dem LDAP-Server. LDAPS-MD5 - LDAP über SSL. Das Passwort wird für zusätzliche Sicherheit innerhalb eines verschlüsselten Tunnels zwischen dem ADC und dem LDAP-Server mit einem MD5-Hash versehen
Domain	Geben Sie den Domänennamen für den LDAP-Server ein.
Server-Adresse	Fügen Sie die IP-Adresse oder den Hostnamen des Authentifizierungsservers hinzu LDAP - IPv4-Adresse oder Hostname. LDAP-MD5 - nur Hostname (IPv4-Adresse funktioniert nicht) LDAPS - IPv4-Adresse oder Hostname. LDAPS-MD5 - nur Hostname (IPv4-Adresse funktioniert nicht).
Hafen	Verwenden Sie standardmäßig Port 389 für LDAP und Port 636 für LDAPS. Sie brauchen die Port-Nummer für LDAP und LDAPS nicht hinzuzufügen. Wenn andere Methoden verfügbar werden, können Sie sie hier konfigurieren

Suchbedingungen	Die Suchbedingungen müssen dem RFC 4515 entsprechen. Beispiel: (MemberOf=CN=Phone- VPN,CN=Users,DC=mycompany,DC=local).
Basis suchen	Dieser Wert ist der Startpunkt für die Suche in der LDAP-Datenbank. Beispiel *dc=meineFirma,dc=lokal*
Login-Format	Verwenden Sie das gewünschte Anmeldeformat. Benutzername - wenn Sie dieses Format wählen, brauchen Sie nur den Benutzernamen einzugeben. Alle vom Benutzer eingegebenen Benutzer- und Domäneninformationen werden gelöscht, und die Domäneninformationen vom Server werden verwendet. Benutzername und Domäne - Der Benutzer muss die gesamte Syntax der Domäne und des Benutzernamens eingeben. Beispiel: *mycompany\gchristie ODER jemand@mycompany*. Die auf der Serverebene eingegebenen Domäneninformationen werden ignoriert. Leer - das ADC akzeptiert alle Eingaben des Benutzers und sendet sie an den Authentifizierungsserver weiter. Diese Option wird bei Verwendung von MD5 verwendet.
Passphrase	Diese Option wird in dieser Version nicht verwendet.
Totzeit	In dieser Version nicht verwendet

Authentifizierungsregeln

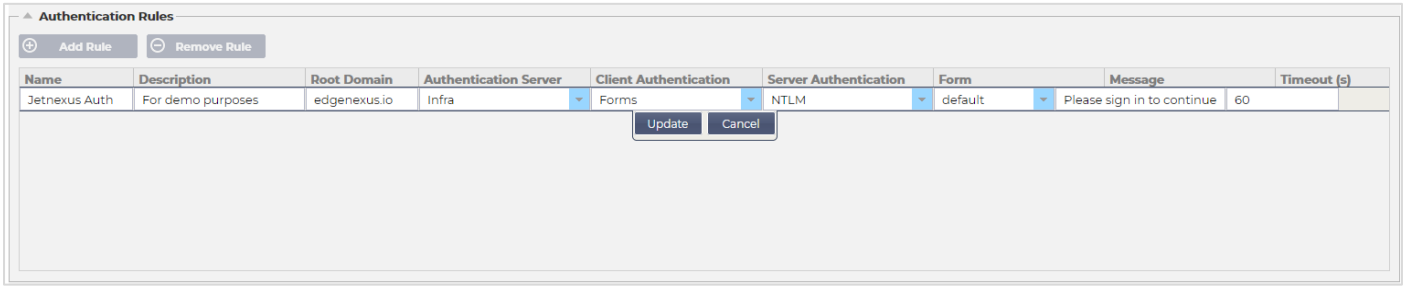
Der nächste Schritt ist die Erstellung der Authentifizierungsregeln für die Verwendung mit der Serverdefinition.



Feld	**Beschreibung**
Name	Fügen Sie einen geeigneten Namen für Ihre Authentifizierungsregel hinzu.
Beschreibung	Fügen Sie eine passende Beschreibung hinzu.
Wurzel-Domäne	Dies muss leer gelassen werden, es sei denn, Sie benötigen eine Einzelanmeldung über Subdomänen hinweg.
Authentifizierungs-Server	Dies ist eine Dropdown-Box, die die von Ihnen konfigurierten Server enthält.
Client-Authentifizierung:	Wählen Sie den für Ihre Bedürfnisse geeigneten Wert: Basic (401) - Diese Methode verwendet die Standard-Authentifizierungsmethode 401 Formulare - damit wird dem Benutzer das ADC-Standardformular präsentiert. Innerhalb des Formulars können Sie eine Nachricht hinzufügen. Sie können ein Formular, das Sie hochgeladen haben, über den Abschnitt unten auswählen.
Server-Authentifizierung	Wählen Sie den entsprechenden Wert. Keine - wenn Ihr Server über keine vorhandene Authentifizierung verfügt, wählen Sie diese Einstellung. Diese Einstellung bedeutet, dass Sie Authentifizierungsfähigkeiten zu einem Server hinzufügen können, der vorher keine hatte. Basic - wenn Ihr Server die Basisauthentifizierung (401) aktiviert hat, dann wählen Sie BASIC. NTLM - wenn Ihr Server die NTLM-Authentifizierung aktiviert hat, dann wählen Sie NTLM.
Formular	Wählen Sie den entsprechenden Wert Standard - Die Auswahl dieser Option führt dazu, dass der ADC seine eingebaute Form verwendet.

	Benutzerdefiniert - Sie können ein von Ihnen entworfenes Formular hinzufügen und es hier auswählen.
Nachricht	Fügen Sie eine persönliche Nachricht in das Formular ein.
Zeitüberschreitung	Fügen Sie der Regel eine Zeitüberschreitung hinzu, nach der sich der Benutzer erneut authentifizieren muss. Beachten Sie, dass die Einstellung "Timeout" nur für die formularbasierte Authentifizierung gültig ist.

Einzel-Anmeldung



Wenn Sie eine Einzelanmeldung für Benutzer anbieten möchten, füllen Sie die Spalte Root-Domain mit Ihrer Domain aus. In diesem Beispiel haben wir edgenexus.io verwendet. Wir können nun mehrere Dienste haben, die edgenexus.io als Root-Domain verwenden, und Sie müssen sich nur einmal anmelden. Wenn wir die folgenden Dienste betrachten:

- Sharepoint.meinUnternehmen.de
- usercentral.mycompany.com
- appstore. mycompany.com

Diese Dienste können sich auf einem VIP befinden oder auf 3 VIPs verteilt sein. Ein Benutzer, der zum ersten Mal auf usercentral. mycompany.com zugreift, wird abhängig von der verwendeten Authentifizierungsregel mit einem Formular zur Anmeldung aufgefordert. Derselbe Benutzer kann dann eine Verbindung zu appstore. mycompany.com herstellen und wird automatisch vom ADC authentifiziert. Sie können den Timeout einstellen, der die Authentifizierung erzwingt, sobald dieser Zeitraum der Inaktivität erreicht ist.

Formulare

In diesem Bereich können Sie ein benutzerdefiniertes Formular hochladen.

Wie Sie Ihr benutzerdefiniertes Formular erstellen

Obwohl das vom ADC bereitgestellte Basisformular für die meisten Zwecke ausreichend ist, wird es Gelegenheiten geben, bei denen Unternehmen dem Benutzer ihre eigene Identität präsentieren möchten. Sie können ein eigenes Formular erstellen, das dem Benutzer in solchen Fällen zum Ausfüllen vorgelegt wird. Dieses Formular muss entweder im HTM- oder HTML-Format vorliegen.

Option	**Beschreibung**
Name	form name = loginform Aktion = %JNURL% Methode = POST
Benutzername	Syntax: name = "JNUSER"
Passwort:	name="JNPASS"

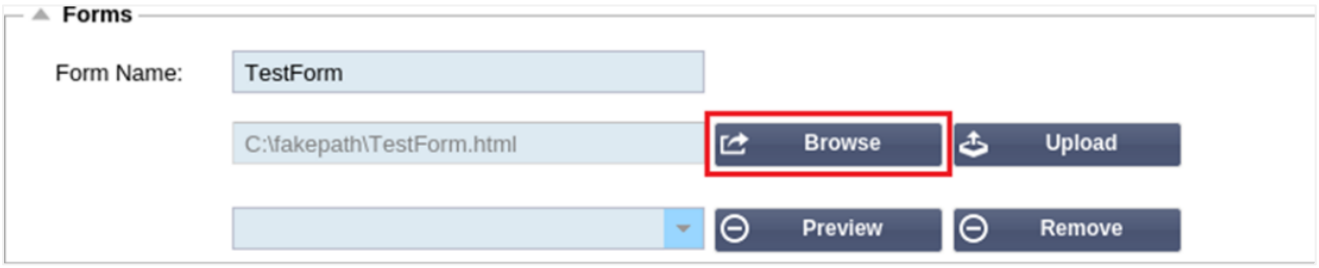
Optionale Meldung1:	%JNMESSAGE%
Optionale Meldung2:	%JNAUTHMESSAGE%
Bilder	Wenn Sie ein Bild hinzufügen möchten, dann fügen Sie es bitte in-line mit Base64-Kodierung ein.

Beispiel-HTML-Code eines sehr grundlegenden und einfachen Formulars

```
<HTML>
<KOPF>
<TITLE>BEISPIEL-AUTHENTIFIZIERUNGSFORMULAR</TITLE>
</HEAD>
<BODY>
%JNMESSAGE%<br>
<form name="loginform" action="%JNURL%" method="post"> USER: <input type="text" name="JNUSER" size="20" value=""></br>
PASS: <input type="password" name="JNPASS" size="20" value=""></br>
<input type="submit" name="submit" value="OK">
</form>
</BODY>
</HTML>
```

Hinzufügen eines benutzerdefinierten Formulars

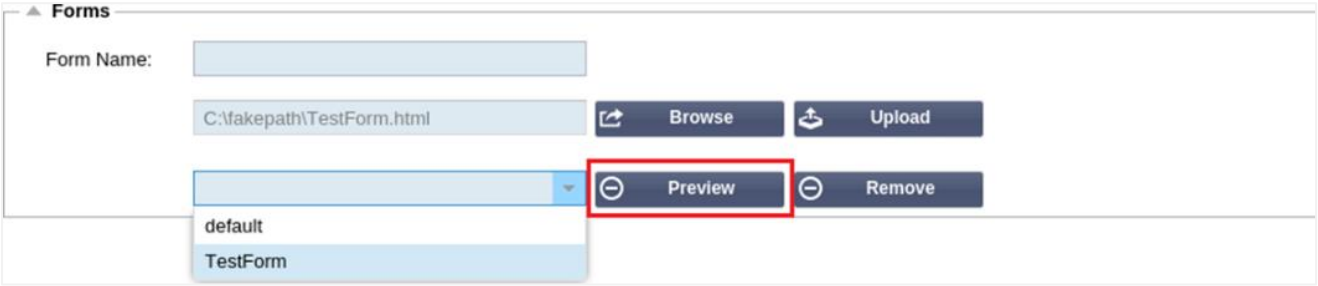
Sobald Sie ein benutzerdefiniertes Formular erstellt haben, können Sie es über den Bereich Formulare hinzufügen.



1. Wählen Sie einen Namen für Ihr Formular
2. Suchen Sie lokal nach Ihrem Formular
3. Klicken Sie auf Hochladen

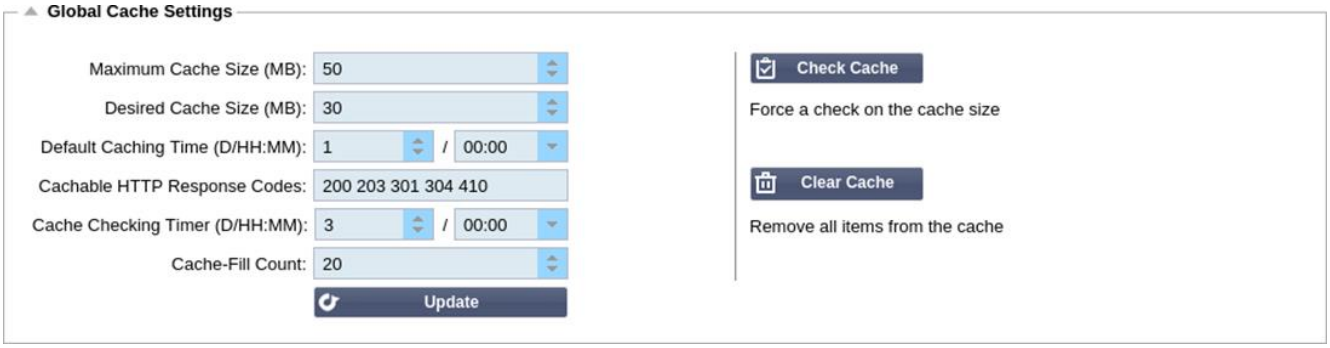
Vorschau auf Ihr benutzerdefiniertes Formular

Um das benutzerdefinierte Formular, das Sie gerade hochgeladen haben, zu betrachten, wählen Sie es aus und klicken auf Vorschau. Sie können diesen Bereich auch verwenden, um nicht mehr benötigte Formulare zu löschen.



Cache

Der ADC ist in der Lage, Daten in seinem internen Speicher zwischenzuspeichern und diesen Cache regelmäßig in den internen Speicher des ADC zu leeren. Die Einstellungen, die diese Funktionalität verwalten, finden Sie in diesem Abschnitt.



Globale Cache-Einstellungen

Maximale Cache-Größe (MB)

Dieser Wert bestimmt den maximalen RAM-Speicher, den der Cache verbrauchen kann. Der ADC-Cache ist ein In-Memory-Cache, der auch periodisch auf das Speichermedium gespült wird, um die Cache-Persistenz nach Neustarts, Reboots und Abschaltvorgängen aufrechtzuerhalten. Diese Funktionalität bedeutet, dass die maximale Cache-Größe in den Speicherbereich der Appliance (und nicht auf die Festplatte) passen muss und nicht mehr als die Hälfte des verfügbaren Speichers betragen sollte.

Gewünschte Cache-Größe (MB)

Dieser Wert gibt den optimalen RAM an, auf den der Cache getrimmt wird. Während die maximale Cache-Größe die absolute Obergrenze des Cache darstellt, ist die gewünschte Cache-Größe als optimale Größe gedacht, die der Cache immer dann zu erreichen versucht, wenn eine automatische oder manuelle Überprüfung der Cache-Größe durchgeführt wird. Die Lücke zwischen der maximalen und der gewünschten Cache-Größe dient dazu, das Eintreffen und die Überlappung neuer Inhalte zwischen den periodischen Überprüfungen der Cache-Größe zu berücksichtigen, um abgelaufene Inhalte zu kürzen. Auch hier kann es effektiver sein, den Standardwert (30 MB) zu akzeptieren und die Größe des Caches regelmäßig unter "Monitor -> Statistik" auf eine angemessene Größe zu überprüfen.

Standard-Cache-Zeit (T/HH:MM)

Der hier eingegebene Wert stellt die Lebensdauer von Inhalten ohne expliziten Verfallswert dar. Die Standard-Caching-Zeit ist der Zeitraum, für den Inhalte ohne "no-store"-Direktive oder explizite Ablaufzeit im Traffic-Header gespeichert werden.

Der Feldeintrag erfolgt in der Form "T/HH:MM" - ein Eintrag von "1/01:01" (Standard ist 1/00:00) bedeutet also, dass der ADC den Inhalt für einen Tag, "01:00" für eine Stunde und "00:01" für eine Minute speichern wird.

Cachable HTTP Response Codes

Einer der zwischengespeicherten Datensätze sind HTTP-Antworten. Die HTTP-Antwortcodes, die zwischengespeichert werden, sind:

- 200 - Standardantwort für erfolgreiche HTTP-Anfragen
- 203 - Kopfzeilen sind nicht endgültig, sondern werden aus einer lokalen Kopie oder einer Kopie eines Drittanbieters entnommen
- 301 - Der angeforderten Ressource wurde eine neue permanente URL zugewiesen
- 304 - Nicht geändert seit der letzten Anfrage & lokal gecachte Kopie sollte stattdessen verwendet werden
- 410 - Die Ressource ist auf dem Server nicht mehr verfügbar, und es ist keine Weiterleitungsadresse bekannt

Dieses Feld sollte mit Vorsicht bearbeitet werden, da die häufigsten cachefähigen Antwortcodes bereits aufgeführt sind.

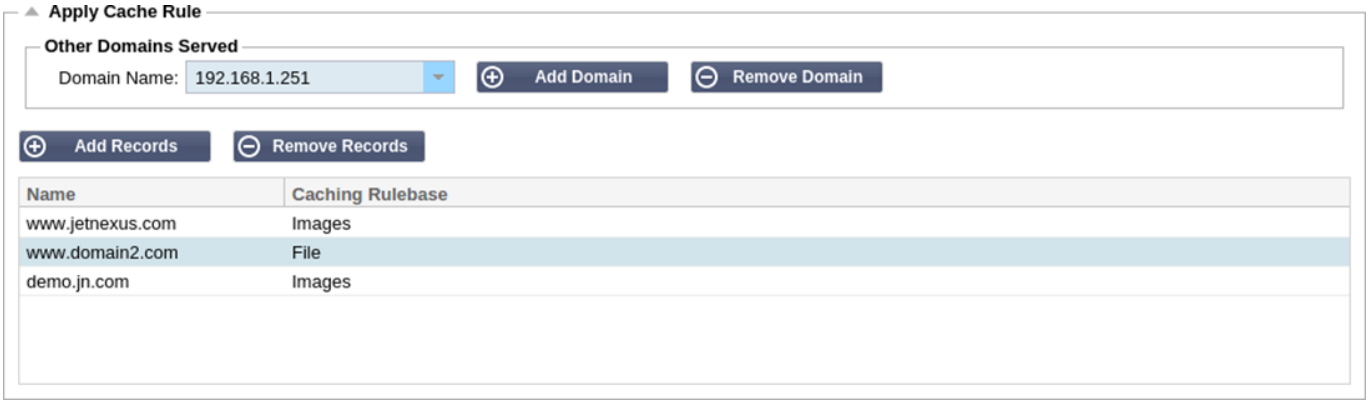
Cache-Prüfzeit (T/HH:MM)

Diese Einstellung bestimmt das Zeitintervall zwischen den Cache-Trimmoperationen.

Cache-Füllstand

Diese Einstellung ist eine Hilfsfunktion, um den Cache zu füllen, wenn eine bestimmte Anzahl von 304's erkannt wurde.

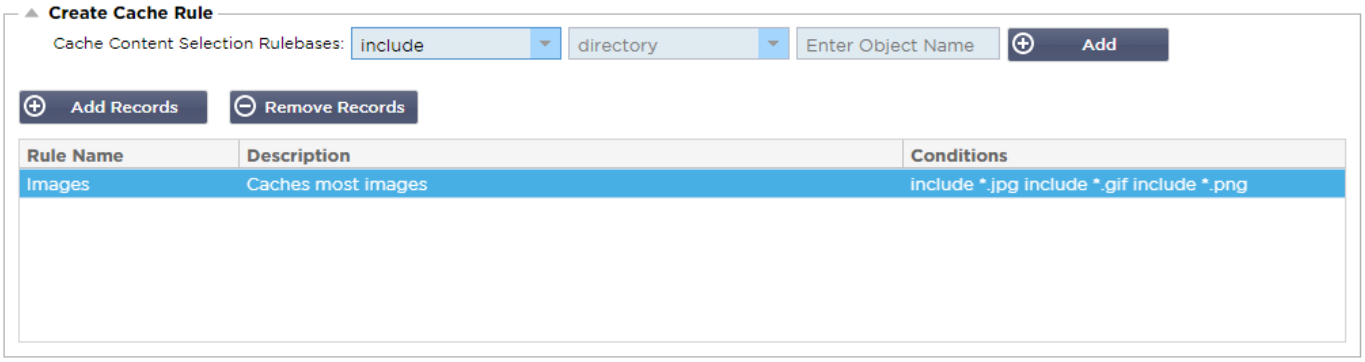
Cache-Regel anwenden



In diesem Abschnitt können Sie eine Cache-Regel auf eine Domain anwenden:

- Fügen Sie die Domain manuell mit der Schaltfläche Datensätze hinzufügen hinzu. Sie müssen einen voll qualifizierten Domänennamen oder eine IP-Adresse in Punkt-Dezimal-Notation verwenden. Beispiel www. mycompany.com oder 192.168.3.1:80
- Klicken Sie auf den Dropdown-Pfeil und wählen Sie Ihre Domain aus der Liste
- Die Liste wird aufgefüllt, solange der Datenverkehr einen virtuellen Dienst durchlaufen hat und eine Caching-Strategie auf den virtuellen Dienst angewendet wurde
- Wählen Sie Ihre Cache-Regel, indem Sie auf die Spalte Caching Rulebase doppelklicken und aus der Liste auswählen

Cache-Regel erstellen



In diesem Abschnitt können Sie mehrere verschiedene Caching-Regeln erstellen, die dann auf eine Domain angewendet werden können:

- Klicken Sie auf Datensätze hinzufügen und geben Sie Ihrer Regel einen Namen und eine Beschreibung
- Sie können Ihre Bedingungen entweder manuell eintippen oder die Funktion Bedingung hinzufügen

So fügen Sie eine Bedingung über die Auswahlregelbasis hinzu:

- Wählen Sie Einschließen oder Ausschließen
- Alle JPEG-Bilder auswählen
- Klicken Sie auf das Symbol + Hinzufügen
- Sie werden sehen, dass 'include *.jpg' nun zu den Bedingungen hinzugefügt wurde
- Sie können weitere Bedingungen hinzufügen. Wenn Sie sich dafür entscheiden, dies manuell zu tun, müssen Sie jede Bedingung in einer NEUEN Zeile hinzufügen. Bitte beachten Sie, dass Ihre Regeln in der gleichen Zeile angezeigt werden, bis Sie in das Feld Bedingungen klicken, dann werden sie in einer separaten Zeile angezeigt

flightPATH

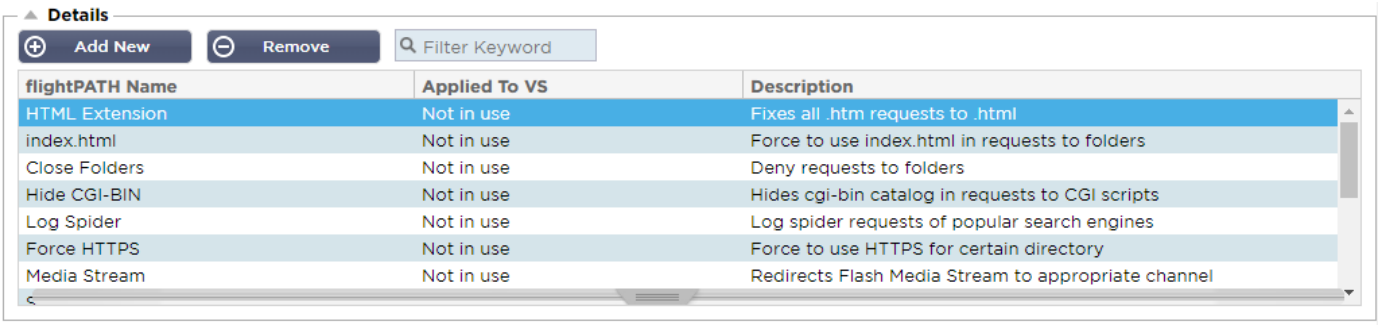
flightPATH ist die in den ADC eingebaute Technologie zur Verwaltung des Datenverkehrs. flightPATH ermöglicht es Ihnen, HTTP- und HTTPS-Datenverkehr in Echtzeit zu inspizieren und Aktionen basierend auf Bedingungen durchzuführen.

flightPATH-Regeln müssen auf ein VIP angewendet werden, wenn IP-Objekte innerhalb der Regeln verwendet werden.

Eine Flugwegregel besteht aus vier Elementen:

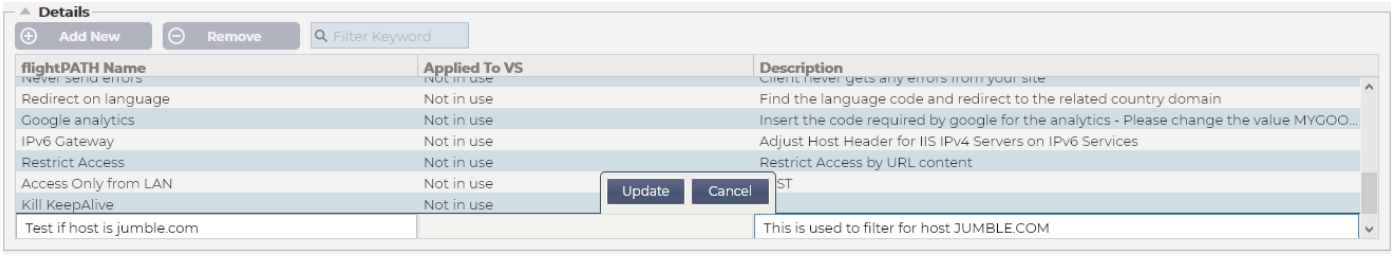
1. Details, wo Sie den flightPATH-Namen und den Dienst, an den er angehängt ist, definieren.
2. Bedingung(en), die definiert werden können und die Auslösung der Regel bewirken.
3. Auswertung, die die Definition von Variablen erlaubt, die innerhalb von Aktionen verwendet werden können
4. Aktionen, die verwendet werden, um zu verwalten, was passieren soll, wenn Bedingungen erfüllt sind

Details



Der Abschnitt Details zeigt die verfügbaren flightPATH-Regeln an. Sie können in diesem Abschnitt neue flightPATH-Regeln hinzufügen und definierte Regeln entfernen.

Hinzufügen einer neuen flightPATH-Regel



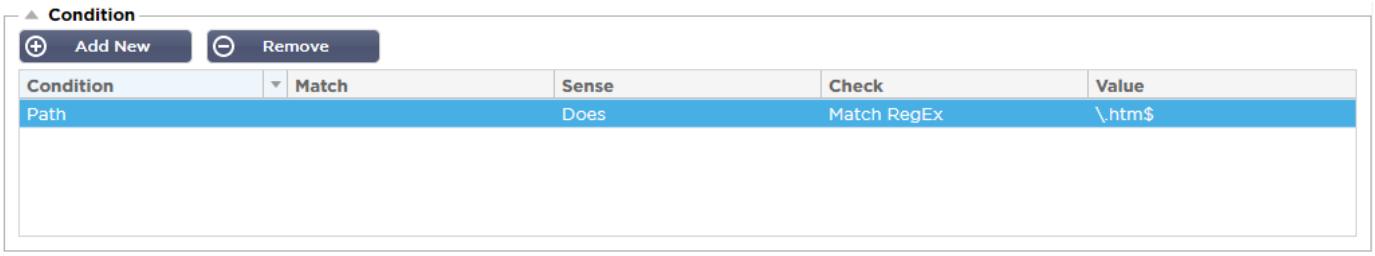
Feld	Beschreibung
FlightPATH Name	Dieses Feld ist für den Namen der flightPATH-Regel. Der Name, den Sie hier angeben, erscheint in anderen Teilen des ADC und wird darin referenziert.
Angewandt auf VS	Diese Spalte ist schreibgeschützt und zeigt das VIP, auf das die flightPATH-Regel angewendet wird.
Beschreibung	Wert, der eine Beschreibung darstellt, die aus Gründen der Lesbarkeit bereitgestellt wird.

Schritte zum Hinzufügen einer flightPATH-Regel

1. Klicken Sie zunächst auf die Schaltfläche Neu hinzufügen, die sich im Bereich Details befindet.
2. Geben Sie einen Namen für Ihre Regel ein. Beispiel Auth2
3. Geben Sie eine Beschreibung für Ihre Regel ein
4. Sobald die Regel auf einen Dienst angewendet wurde, sehen Sie, dass die Spalte Angewandt auf automatisch mit einer IP-Adresse und einem Port-Wert ausgefüllt wird
5. Vergessen Sie nicht, auf die Schaltfläche Aktualisieren zu klicken, um Ihre Änderungen zu speichern, oder wenn Sie einen Fehler machen, klicken Sie einfach auf Abbrechen, um zum vorherigen Zustand zurückzukehren.

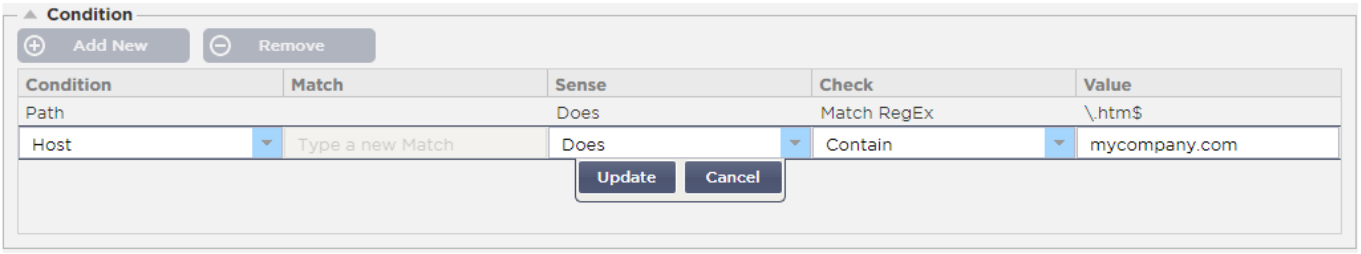
Zustand

Eine flightPATH-Regel kann eine beliebige Anzahl von Bedingungen haben. Die Bedingungen arbeiten auf einer UND-Basis, so dass Sie die Bedingung festlegen können, bei der die Aktion ausgelöst wird. Wenn Sie eine ODER-Bedingung verwenden möchten, erstellen Sie eine zusätzliche flightPATH-Regel und wenden Sie diese in der richtigen Reihenfolge auf das VIP an.



Sie können auch RegEx verwenden, indem Sie Match RegEx im Feld Check und den RegEx-Wert im Feld Value auswählen. Die Einbeziehung der RegEx-Auswertung erweitert die Möglichkeiten von flightPATH enorm.

Erstellen einer neuen flightPATH-Bedingung



Zustand

Wir bieten mehrere Bedingungen als vordefiniert innerhalb des Dropdowns an und decken alle vorhersehbaren Szenarien ab. Wenn neue Bedingungen hinzugefügt werden, werden diese über Jetpack-Updates verfügbar sein.

Zur Auswahl stehen folgende Optionen:

ZUSTAND	BESCHREIBUNG	BEISPIEL
<form>	HTML-Formulare werden verwendet, um Daten an einen Server zu übergeben	Beispiel "form doesn't have length 0"
GEO-Standort	Vergleicht die Quell-IP-Adresse mit den ISO 3166 Country Codes	GEO Standort ist gleich GB, ODER GEO Standort ist gleich Deutschland
Host	Aus der URL extrahierter Host	www.mywebsite.com oder 192.168.1.1
Sprache	Sprache extrahiert aus dem HTTP-Header language	Diese Bedingung erzeugt ein Dropdown-Menü mit einer Liste von Sprachen
Methode	Dropdown von HTTP-Methoden	Dropdown, das GET, POST, etc. beinhaltet
Herkunft IP	Wenn der Upstream-Proxy X-Forwarded-for (XFF) unterstützt, verwendet er die wahre Ursprungsadresse	Client-IP. Es können auch mehrere IPs oder Subnetze verwendet werden. 10\.1\.2\.* ist 10.1.2.0 /24 Subnetz10\ .1\.2\.3|10\.1\.2\.4 Verwenden Sie | für mehrere IP's
Pfad	Pfad der Website	/meinewebsite/index.asp
POST	POST-Anforderungsmethode	Prüfen von Daten, die auf eine Website hochgeladen werden
Abfrage	Name und Wert einer Abfrage, und kann entweder den Abfragenamen oder auch einen Wert akzeptieren	"Best=jetNEXUS" Wo die Übereinstimmung Best ist und der Wert edgeNEXUS ist
Abfrage-String	Die gesamte Abfragezeichenfolge nach dem Zeichen ?	

Cookie anfordern	Name eines von einem Client angeforderten Cookies	MS-WSMAN=afYfn1CDqqCDqUD::
Kopfzeile anfordern	Jeder HTTP-Header	Referrer, Benutzer-Agent, Von, Datum
Version anfordern	Die HTTP-Version	HTTP/1.0 ODER HTTP/1.1
Antwort Körper	Eine benutzerdefinierte Zeichenfolge im Antwortkörper	Server AUF
Antwort-Code	Der HTTP-Code für die Antwort	200 OK, 304 Nicht modifiziert
Antwort Cookie	Der Name eines vom Server gesendeten Cookies	MS-WSMAN=afYfn1CDqqCDqUD::
Antwort-Kopfzeile	Jeder HTTP-Header	Referrer, Benutzer-Agent, Von, Datum
Antwort Version	Die vom Server gesendete HTTP-Version	HTTP/1.0 ODER HTTP/1.1
Quelle IP	Entweder die Ursprungs-IP, die Proxy-Server-IP oder eine andere zusammengefasste IP-Adresse	ClientIP , Proxy IP, Firewall IP. Kann auch mehrere IP und Subnetze verwenden. Sie müssen die Punkte escapen, da diese RegEX sind. Beispiel 10\.1\.2\.3 ist 10.1.2.3

Spiel

Das Feld Übereinstimmung kann entweder ein Einblendmenü oder ein Textwert sein und ist in Abhängigkeit vom Wert im Feld Bedingung definierbar. Wenn die Bedingung z. B. auf Host eingestellt ist, ist das Feld Abgleichen nicht verfügbar. Wenn die Bedingung auf <Formular> eingestellt ist, wird das Feld Abgleich als Textfeld angezeigt, und wenn die Bedingung auf POST eingestellt ist, wird das Feld Abgleich als Dropdown mit entsprechenden Werten angezeigt.

Zur Auswahl stehen folgende Optionen:

MATCH	BESCHREIBUNG	BEISPIEL
Akzeptieren	Zulässige Content-Typen	Akzeptieren: text/plain
Accept-Encoding	Akzeptierte Kodierungen	Accept-Encoding: <compress | gzip | deflate | sdch | identity>
Accept-Language	Akzeptierte Sprachen für die Antwort	Accept-Language: en-US
Accept-Ranges	Welche partiellen Inhaltsbereichstypen dieser Server unterstützt	Accept-Ranges: bytes
Autorisierung	Anmeldeinformationen für die HTTP-Authentifizierung	Berechtigung: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Charge-To	Enthält Kontoinformationen für die Kosten der Anwendung der angeforderten Methode	
Content-Encoding	Der Typ der verwendeten Kodierung	Inhalt-Encoding: gzip

Inhalt-Länge	Die Länge des Antwortkörpers in Oktetten (8-Bit-Bytes)	Inhalt-Länge: 348
Inhalt-Typ	Der Mime-Typ des Body der Anfrage (wird bei POST- und PUT-Anfragen verwendet)	Inhalt-Typ: application/x-www-form-urlencoded
Keks	Ein HTTP-Cookie, das zuvor vom Server mit Set-Cookie (unten) gesendet wurde	Cookie: $Version=1; Skin=new;
Datum	Datum und Uhrzeit, zu der die Nachricht erstellt wurde	Datum = "Datum" ":" HTTP-Datum
ETag	Ein Bezeichner für eine bestimmte Version einer Ressource, oft ein Message Digest	ETag: "aed6bdb8e090cd1:0"
Von	Die E-Mail-Adresse des Benutzers, der die Anfrage stellt	Von: user@example.com
Wenn-geändert-seit	Ermöglicht die Rückgabe eines 304 Not Modified, wenn der Inhalt unverändert ist	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Zuletzt geändert	Das Datum der letzten Änderung für das angeforderte Objekt, im RFC 2822-Format	Zuletzt geändert: Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Implementierung: Spezifische Header, die an jeder Stelle der Anfrage-Antwort-Kette verschiedene Auswirkungen haben können.	Pragma: no-cache
Referrer	Adresse der vorherigen Webseite, von der aus ein Link zur aktuell angeforderten Seite verfolgt wurde	Referrer: HTTP://www.edgenexus.io
Server	Ein Name für den Server	Server: Apache/2.4.1 (Unix)
Set-Cookie	Ein HTTP-Cookie	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
Benutzer-Agent	Der User-Agent-String des Benutzer-Agenten	Benutzer-Agent: Mozilla/5.0 (kompatibel; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Variieren Sie	Sagt Downstream-Proxys, wie sie zukünftige Anfrage-Header abgleichen sollen, um zu entscheiden, ob die zwischengespeicherte Antwort verwendet werden kann, anstatt eine neue vom Ursprungsserver anzufordern	Vary: User-Agent
X-Powered-By	Gibt die Technologie (z. B. ASP.NET, PHP, JBoss) an, die die Web-Anwendung unterstützt	X-Powered-By: PHP/5.4.0

Sense

Das Feld Sense ist ein boolesches Dropdown-Feld und enthält entweder die Auswahl Does oder Doesn't.

Prüfen Sie

Das Feld Prüfung ermöglicht die Einstellung von Prüfwerten gegen die Bedingung.

Verfügbare Auswahlmöglichkeiten sind: Enthalten, Ende, Gleich, Vorhanden, Länge haben, RegEx anpassen, Liste anpassen, Start, Länge überschreiten

CHECK	BESCHREIBUNG	BEISPIEL
Existieren	Dabei ist es egal, wie die Bedingung im Detail aussieht, nur dass sie existiert/nicht existiert	Host - Existiert - Existieren
Start	Die Zeichenkette beginnt mit dem Wert	Pfad - Tut - Start - /sicher
Ende	Die Zeichenkette endet mit dem Wert	Pfad - Tut - Ende - .jpg
Enthält	Die Zeichenkette enthält den Wert	Anfrage-Header - Akzeptieren - Enthält - Bild
Gleiche	Die Zeichenkette ist gleich dem Wert	Host - Tut - Gleich - www.jetnexus.com
Länge haben	Die Zeichenkette hat eine Länge von dem Wert	Host - Hat - Länge - 16www.jetnexus.com = TRUEwww.jetnexus.co.uk = FALSE
RegEx abgleichen	Ermöglicht Ihnen die Eingabe eines vollständigen Perl-kompatiblen regulären Ausdrucks	Herkunfts-IP - Entspricht - Regex - 10\..* | 11\..*

Schritte zum Hinzufügen einer Bedingung

Das Hinzufügen einer neuen flightPATH-Bedingung ist sehr einfach. Ein Beispiel ist oben abgebildet.

1. Klicken Sie auf die Schaltfläche Neu hinzufügen im Bedingungsbereich.
2. Wählen Sie eine Bedingung aus dem Dropdown-Feld. Nehmen wir Host als Beispiel. Sie können auch in das Feld tippen, und das ADC zeigt den Wert in einem Dropdown-Feld an.
3. Wählen Sie eine Sense. Zum Beispiel, Hat
4. Wählen Sie einen Check. Zum Beispiel, Enthalten
5. Wählen Sie einen Wert. Zum Beispiel, mycompany.com

Das obige Beispiel zeigt, dass es zwei Bedingungen gibt, die beide WAHR sein müssen, damit die Regel ausgeführt wird

- Die erste ist die Überprüfung, ob das angeforderte Objekt ein Bild ist
- Die zweite prüft, ob der Host in der URL www.imagepool.com ist.

Auswertung

Die Möglichkeit, definierbare Variablen hinzuzufügen, ist eine zwingende Fähigkeit. Normale ADCs bieten diese Möglichkeit über Skripting oder Befehlszeilenoptionen, die nicht für jeden ideal sind. Mit dem ADC können Sie eine beliebige Anzahl von Variablen über eine einfach zu bedienende GUI definieren, wie unten gezeigt und beschrieben.

flightPATH-Variablendefinition umfasst vier Einträge, die vorgenommen werden müssen.

- Variable - dies ist der Name der Variable
- Quelle - eine Dropdown-Liste mit möglichen Quellpunkten
- Detail - wählen Sie Werte aus einer Dropdown-Liste oder geben Sie sie manuell ein.

- Wert - der Wert, den die Variable enthält und der ein alphanumerischer Wert oder ein RegEx zur Feinabstimmung sein kann.

Eingebaute Variablen:

Eingebaute Variablen sind bereits hartkodiert, so dass Sie für diese keinen Auswertungseintrag erstellen müssen.

Sie können jede der unten aufgeführten Variablen im Abschnitt Aktion verwenden.

Die Erklärung für jede Variable finden Sie in der Tabelle "Bedingung" oben.

- Methode = $Methode$
- Pfad = $Pfad$
- Querystring = $querystring$
- Quellip = $sourceip$
- Antwort-Code (Text auch "200 OK") = $resp$
- Host = $host$
- Version = $version$
- Clientport = $clientport$
- Clientip = $clientip$
- Geolocation = $geolocation$"

AKTION	TARGET
Aktion = Umleitung 302	Ziel = HTTPs://$host$/404.html
Aktion = Loggen	Ziel = Ein Client von $sourceip$:$sourceport$ hat soeben eine Anfrage $path$ Seite gestellt

Erläuterung:

- Ein Client, der auf eine Seite zugreift, die nicht existiert, würde normalerweise mit der 404-Fehlerseite des Browsers konfrontiert werden
- Stattdessen wird der Benutzer zum ursprünglichen Hostnamen, den er verwendet hat, umgeleitet, aber der falsche Pfad wird durch 404.html ersetzt
- Dem Syslog wird ein Eintrag hinzugefügt, der besagt: "Ein Client von 154.3.22.14:3454 hat gerade die Seite wrong.html angefordert."

Aktion

Der nächste Schritt im Prozess ist das Hinzufügen einer Aktion, die mit der flightPATH-Regel und -Bedingung verknüpft ist.

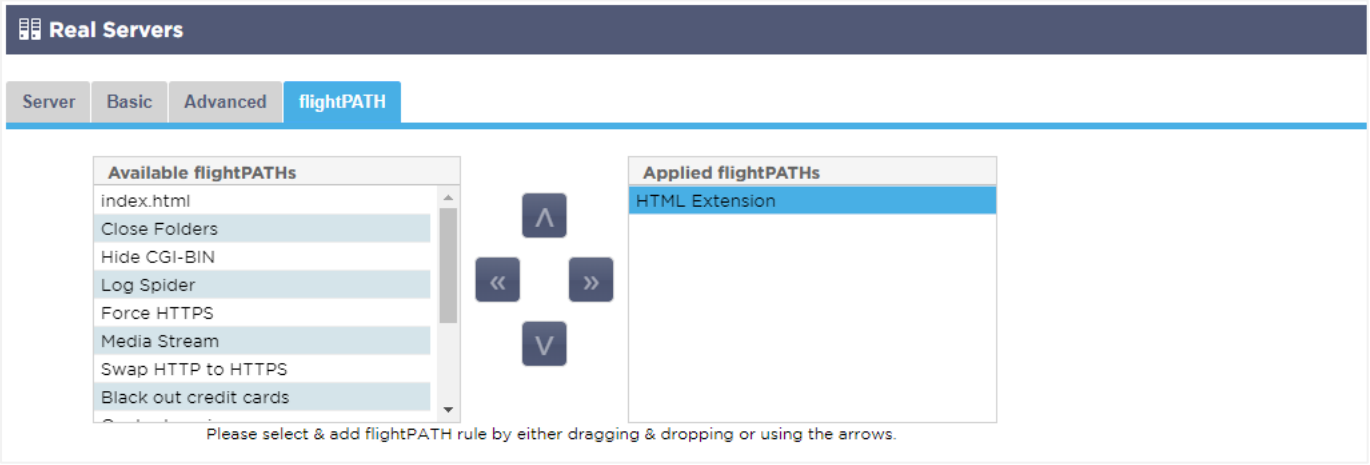
In diesem Beispiel wollen wir den Pfadteil der URL umschreiben, um die vom Benutzer eingegebene URL wiederzugeben.

- Klicken Sie auf Neu hinzufügen
- Wählen Sie Pfad neu schreiben aus dem Dropdown-Menü Aktion
- Geben Sie in das Feld Ziel $path$/myimages ein
- Klicken Sie auf Aktualisieren

Diese Aktion fügt /myimages an den Pfad an, so dass die endgültige URL www.imagepool.com/myimages wird.

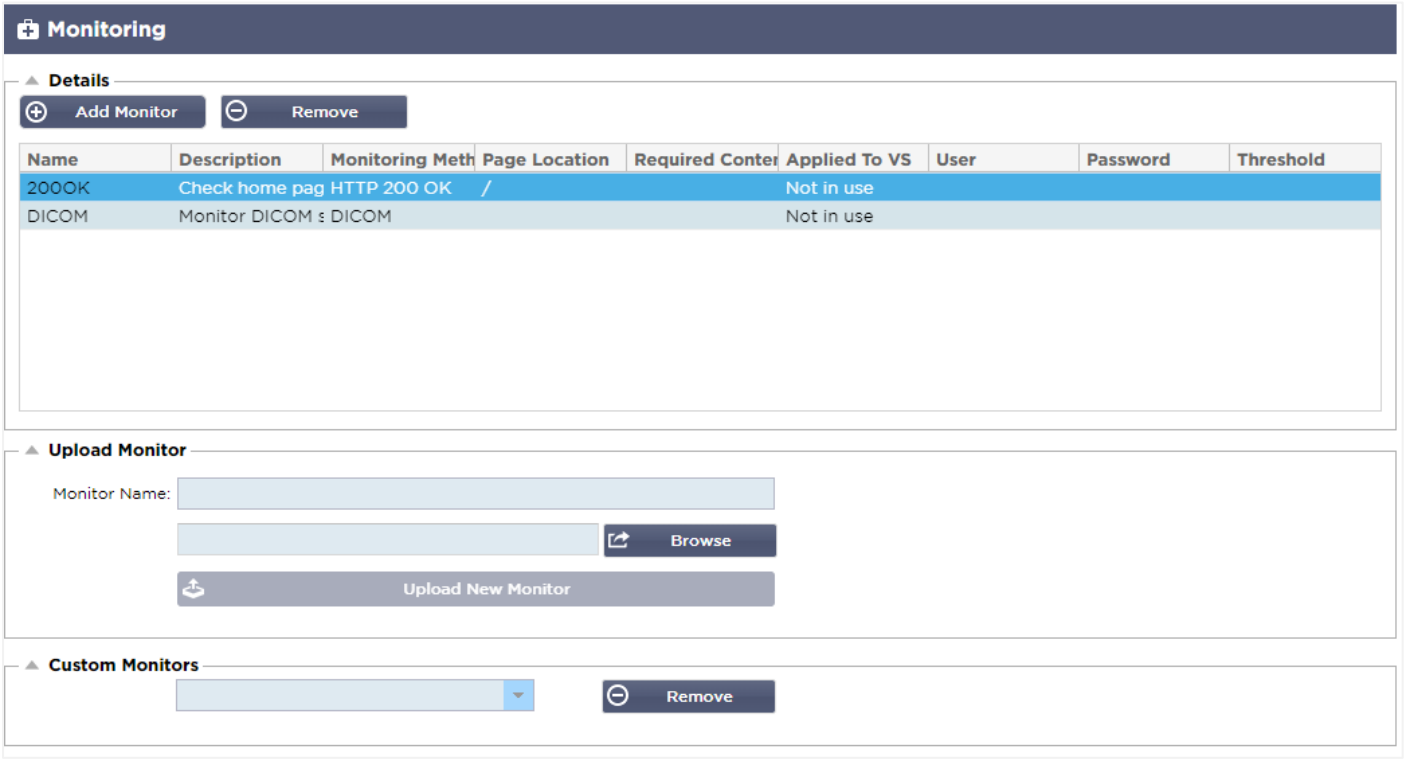
Anwenden der flightPATH-Regel

Die Anwendung einer flightPATH-Regel erfolgt innerhalb der flightPATH-Registerkarte eines jeden VIP/VS.



- Navigieren Sie zu Dienste > IP-Dienste und wählen Sie das VIP, dem Sie die flightPATH-Regel zuweisen möchten.
- Sie sehen die unten gezeigte Real-Server-Liste
- Klicken Sie auf die Registerkarte flightPATH
- Wählen Sie die flightPATH-Regel, die Sie konfiguriert haben, oder eine der vorgefertigten, die unterstützt werden. Sie können bei Bedarf mehrere flightPATH-Regeln auswählen.
- Ziehen Sie den ausgewählten Satz per Drag & Drop in den Bereich Applied flightPATHs oder klicken Sie auf die Pfeilschaltfläche >>.
- Die Regel wird auf die rechte Seite verschoben und automatisch angewendet.

Echte Server-Monitore



Wenn der Lastausgleich eingerichtet ist, ist es hilfreich, den Zustand der echten Server und der darauf laufenden Anwendungen zu überwachen. Bei Webservern können Sie z. B. eine bestimmte Seite einrichten, mit der Sie den Zustand überwachen können, oder eines der anderen Überwachungssysteme verwenden, über die der ADC verfügt.

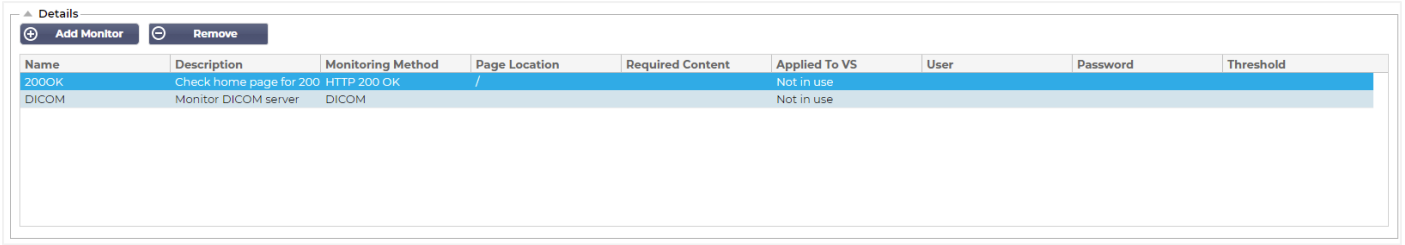
Auf der Seite Bibliothek > Reale Server-Überwachungen können Sie benutzerdefinierte Überwachungen hinzufügen, anzeigen und bearbeiten. Dabei handelt es sich um Layer 7-Server-"Health Checks", die Sie im Feld Server-Überwachung auf der Registerkarte Basis des von Ihnen definierten virtuellen Dienstes auswählen.

Die Seite Real-Server-Monitore ist in drei Abschnitte unterteilt.

- Details
- Hochladen
- Benutzerdefinierte Monitore

Details

Der Bereich Details wird verwendet, um neue Monitore hinzuzufügen und nicht benötigte zu entfernen. Sie können auch einen vorhandenen Monitor bearbeiten, indem Sie auf ihn doppelklicken.



Name

Name Ihrer Wahl für Ihren Monitor.

Beschreibung

Textliche Beschreibung für diesen Monitor, die am besten so aussagekräftig wie möglich sein sollte.

Überwachung Methode

Wählen Sie die Überwachungsmethode aus der Dropdown-Liste. Verfügbare Auswahlmöglichkeiten sind:

Überwachung Methode	Beschreibung	Beispiel
HTTP 200 OK	Es wird eine TCP-Verbindung mit dem Real-Server hergestellt. Nachdem die Verbindung hergestellt wurde, wird eine kurze HTTP-Anfrage an den Real-Server gesendet. Eine HTTP-Antwort des Servers wird abgewartet und dann auf den Antwortcode "200 OK" geprüft. Wenn der "200 OK"-Antwortcode empfangen wird, wird davon ausgegangen, dass der Real-Server betriebsbereit ist. Wenn aus irgendeinem Grund der "200 OK"-Antwortcode nicht empfangen wird, einschließlich Zeitüberschreitungen oder Verbindungsabbrüche, dann gilt der Real-Server als ausgefallen und nicht verfügbar. Diese Überwachungsmethode kann wirklich nur mit den Diensttypen HTTP und Accelerated HTTP verwendet werden. Wenn jedoch ein Layer 4-Diensttyp für einen HTTP-Server verwendet wird, könnte sie trotzdem verwendet werden, wenn SSL auf dem Real-Server nicht verwendet oder von der "Content SSL"-Funktion entsprechend behandelt wird.	Name: 200OK Beschreibung: Produktionswebseite prüfen Überwachungsmethode: HTTP 200 OK Standort der Seite: /main/index.html OR HTTP://www.edgenexus.io/main/index.html Erforderlicher Inhalt: N/A
HTTP-Antwort	Es wird eine Verbindung und eine HTTP-Anfrage/Antwort an den Real-Server hergestellt und wie im vorherigen Beispiel erklärt geprüft. Aber anstatt auf einen "200 OK"-Antwortcode zu prüfen, wird der Header der HTTP-Antwort auf benutzerdefinierten Textinhalt geprüft. Der Text kann ein vollständiger Header, ein Teil eines Headers, eine Zeile aus einem Teil einer Seite oder nur ein Wort sein. Wenn der Text gefunden wird, gilt der Real Server als funktionsfähig. Diese Überwachungsmethode kann wirklich nur mit den Diensttypen HTTP und Accelerated HTTP verwendet werden. Wenn jedoch ein Layer 4-Diensttyp für einen HTTP-Server verwendet wird, könnte sie trotzdem verwendet werden, wenn SSL auf dem Real-Server nicht verwendet oder von der "Content SSL"-Funktion entsprechend behandelt wird.	Name: Server hoch Beschreibung: Überprüfen Sie den Inhalt der Seite auf "Server Up. " Überwachungsmethode: HTTP-Antwort Standort der Seite: /main/index.html OR HTTP://www.edgenexus.io/main/index.html Erforderlicher Inhalt: Server hoch

DICOM	Wir senden ein DICOM-Echo mit dem Wert "Source Calling" AE Title in der gewünschten Inhaltsspalte. Sie können auch den Wert "Destination Called" AE Title im Abschnitt Notizen des jeweiligen Servers einstellen. Sie finden die Spalte Notizen innerhalb der IP-Dienste-. -Virtuelle Dienste--Server Seite.	Name: DICOM Beschreibung: L7-Zustandsprüfung für DICOM-Dienst Überwachungsmethode: DICOM Standort der Seite: N/A Erforderlicher Inhalt: AET-Wert
TCP Out of Band	Die TCP-Out-of-Band-Methode ist wie eine TCP-Verbindung, mit dem Unterschied, dass Sie in der Spalte "Gewünschter Inhalt" den Port angeben können, den Sie überwachen möchten. Dieser Port ist normalerweise nicht derselbe wie der Traffic-Port und wird verwendet, wenn Sie Dienste miteinander verbinden wollen	Name: TCP Out of Band Beschreibung: Monitor Out of Band/Traffic-Port Standort der Seite: N/A Erforderlicher Inhalt: 555
Multi-Port-TCP-Monitor	Diese Methode ist wie die obige, außer dass Sie mehrere verschiedene Ports haben können. Der Monitor gilt nur dann als erfolgreich, wenn alle im Abschnitt "Erforderlicher Inhalt" angegebenen Ports korrekt antworten.	Name: Multi-Port-Monitor Beschreibung: Überwachen Sie mehrere Ports auf Erfolg Standort der Seite: N/A Erforderlicher Inhalt: 135,59534,59535

Seite Standort

URL Seitenstandort für einen HTTP-Monitor. Dieser Wert kann ein relativer Link sein, wie z. B. /Ordner1/Ordner2/Seite1.html. Sie können auch einen absoluten Link verwenden, bei dem die Website an den Hostnamen gebunden ist.

Erforderlicher Inhalt

Dieser Wert enthält alle Inhalte, die der Monitor erkennen und verwerten muss. Der hier dargestellte Wert ändert sich je nach gewählter Überwachungsmethode.

Angewandt auf VS

Dieses Feld wird automatisch mit der IP/Port des virtuellen Dienstes ausgefüllt, auf den der Monitor angewendet wird. Sie können keinen Monitor löschen, der mit einem Virtuellen Dienst verwendet wurde.

Benutzer

Einige benutzerdefinierte Monitore können diesen Wert zusammen mit dem Passwortfeld verwenden, um sich bei einem Real Server anzumelden.

Passwort

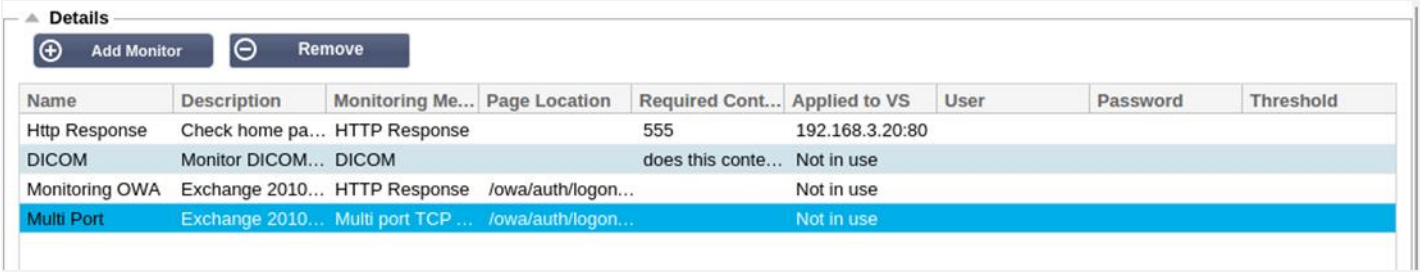
Einige benutzerdefinierte Monitore können diesen Wert zusammen mit dem Feld Benutzer verwenden, um sich bei einem Real-Server anzumelden.

Schwellenwert

Das Feld Schwellenwert ist eine allgemeine Ganzzahl, die in benutzerdefinierten Monitoren verwendet wird, in denen ein Schwellenwert wie z. B. der CPU-Pegel erforderlich ist.

HINWEIS: Bitte stellen Sie sicher, dass die Antwort vom Anwendungsserver nicht als "Chunked"-Antwort zurückkommt

Beispiele für Real Server Monitor



Monitor hochladen

Es wird viele Gelegenheiten geben, bei denen Benutzer ihre eigenen benutzerdefinierten Monitore erstellen möchten, und dieser Bereich ermöglicht es ihnen, diese in den ADC hochzuladen.

Benutzerdefinierte Monitore werden mit PERL-Skripten geschrieben und haben eine .pl-Dateierweiterung.

- Geben Sie Ihrem Monitor einen Namen, damit Sie ihn in der Liste Überwachungsmethode identifizieren können
- Suchen Sie nach der .pl-Datei
- Klicken Sie auf Neuen Monitor hochladen
- Ihre Datei wird an den richtigen Ort hochgeladen und ist als neue Überwachungsmethode sichtbar.

Benutzerdefinierte Monitore

In diesem Bereich können Sie hochgeladene benutzerdefinierte Monitore anzeigen und sie entfernen, wenn sie nicht mehr benötigt werden.

- Klicken Sie auf das Dropdown-Feld
- Wählen Sie den Namen des benutzerdefinierten Monitors
- Klicken Sie auf Entfernen
- Ihr benutzerdefinierter Monitor wird nicht mehr in der Liste der Überwachungsmethoden angezeigt

Erstellen eines benutzerdefinierten Monitor-Perl-Skripts

ACHTUNG: Dieser Abschnitt ist für Personen gedacht, die Erfahrung mit der Verwendung und dem Schreiben in Perl haben

Dieser Abschnitt zeigt Ihnen die Befehle, die Sie innerhalb Ihres Perl-Skripts verwenden können.

Der Befehl #Monitor-Name: ist der Name, der für das auf dem ADC gespeicherte Perl-Skript verwendet wird. Wenn Sie diese Zeile nicht einfügen, wird Ihr Skript nicht gefunden!

Die folgenden Angaben sind obligatorisch:

- #Monitor-Name
- streng verwenden;
- Warnung verwenden;

Die Perl-Skripte werden in einer CHROOTED-Umgebung ausgeführt. Sie rufen oft eine andere Anwendung wie WGET oder CURL auf. Manchmal müssen diese für eine bestimmte Funktion, z. B. SNI, aktualisiert werden.

Dynamische Werte

- my $host = $_[0]; - Dies verwendet die "Adresse" aus dem Abschnitt "IP-Dienste - Realer Server
- my $port = $_[1]; - Dies verwendet den "Port" aus dem Abschnitt IP-Dienste-Real-Server
- my $content = $_[2]; - Dies verwendet den Wert "Erforderlicher Inhalt" aus dem Abschnitt Library--Real Server Monitoring
- my $notes = $_[3]; - Dies verwendet die Spalte "Notes" im Abschnitt Real Server der IP-Dienste
- my $page = $_[4]; - Dies verwendet die "Page Location"-Werte aus dem Abschnitt Library--Real Server Monitor
- my $user = $_[5]; - Dies verwendet den Wert "User" aus dem Abschnitt Library--Real Server Monitor
- my $password = $_[6]; - Dies verwendet den Wert "Password" aus dem Abschnitt Library--Real Server Monitor

Benutzerdefinierte Gesundheitsprüfungen haben zwei Ergebnisse

- Erfolgreich
  Rückgabewert 1Drucken Sie
  eine Erfolgsmeldung an SyslogMarkieren Sie
  den Real-Server online (sofern IN COUNT übereinstimmt)
- Erfolglos
  Rückgabewert 2Drucken Sie
  eine Meldung mit dem Wort "Unsuccessful" an SyslogMarkieren Sie
  den Real Server Offline (sofern OUT Count übereinstimmt)

Beispiel für einen benutzerdefinierten Health Monitor

```
#Monitor-Name HTTPS_SNI

streng verwenden:

Warnungen verwenden;

# Der Monitorname wie oben wird in der Dropdown-Liste der verfügbaren Gesundheitsprüfungen angezeigt

# Es werden 6 Werte an dieses Skript übergeben (siehe unten)

# Das Skript gibt die folgenden Werte zurück

# 1 ist der Test erfolgreich

# 2 wenn der Test nicht erfolgreich ist sub monitor

{

my Shost=       $_[0]; ### Host IP oder Name

my Sport=       $_[1]; ### Host-Port

my Scontent=    $_[2]; ### Zu suchender Inhalt (in der Webseite und den HTTP-Headern)

my Snotes=      $_[3]; ### Virtueller Hostname

my Spage=       $_[4]; ### Der Teil der URL nach der Host-Adresse

my Suser=       $_[5]: ### domain/usemame (optional)

my Spassword=           $_[6]; ### Passwort (optional)
```

```
my $Auflösung;
my $auth          =;
if ($Port)
{
        $resolve = "$notes:$port:$host":
}
sonst {
        $resolve = "$notes:$host";
}
if ($Benutzer && $Passwort) {
        $auth = "-u $user:$password :
}
my @lines = 'curl -s -i -retry 1 -max-time 1 -k -H "Host:$notes --resolve $resolve $auth HTTPs://${notes}${page} 2>&1';
if(join(""@lines)=~/$content/)
        {
        print "HTTPs://$notes}${page} looking for - $content - Health check successful.\n";
        zurück(1);
        }
sonst
        {
        print "HTTPs://${notes}${page} looking for - $content - Health check failed.\n";
        zurück(2)
        }
}
Monitor(@ARGV):
```

HINWEIS: Benutzerdefinierte Überwachung - Die Verwendung von globalen Variablen ist nicht möglich. Verwenden Sie nur lokale Variablen - Variablen, die innerhalb von Funktionen definiert sind

SSL-Zertifikate

Um den Layer-7-Lastausgleich mit Servern, die verschlüsselte Verbindungen mit SSL verwenden, erfolgreich zu nutzen, muss der ADC mit den auf den Zielservern verwendeten SSL-Zertifikaten ausgestattet sein. Diese Anforderung besteht darin, dass der Datenstrom vor dem Senden an den Zielserver entschlüsselt, untersucht, verwaltet und dann wieder verschlüsselt werden kann.

Die SSL-Zertifikate können von selbstsignierten Zertifikaten, die der ADC generieren kann, bis hin zu den traditionellen Zertifikaten (einschließlich Wildcard) reichen, die von vertrauenswürdigen Anbietern erhältlich sind. Sie können auch domänensignierte Zertifikate verwenden, die von Active Directory generiert werden.

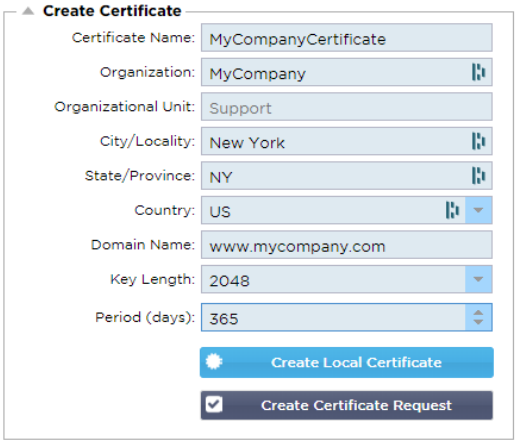
Was macht der ADC mit dem SSL-Zertifikat?

Der ADC kann Regeln zur Verkehrsverwaltung (flightPATH) durchführen, je nachdem, was die Daten enthalten. Diese Verwaltung kann nicht für SSL-verschlüsselte Daten durchgeführt werden. Wenn der ADC die Daten untersuchen muss, muss er sie zunächst entschlüsseln und benötigt dazu das vom Server verwendete SSL-Zertifikat. Nach der Entschlüsselung kann die ADC dann die flightPATH-Regeln untersuchen und ausführen. Anschließend werden die Daten mit dem SSL-Zertifikat erneut verschlüsselt und an den endgültigen Real-Server gesendet.

Zertifikat erstellen

Obwohl der ADC ein global vertrauenswürdiges SSL-Zertifikat verwenden kann, kann er ein selbstsigniertes SSL-Zertifikat erzeugen. Das selbstsignierte SSL ist perfekt für interne Lastausgleichsanforderungen. Ihre IT-Richtlinien erfordern jedoch möglicherweise ein vertrauenswürdiges oder Domain-CA-Zertifikat.

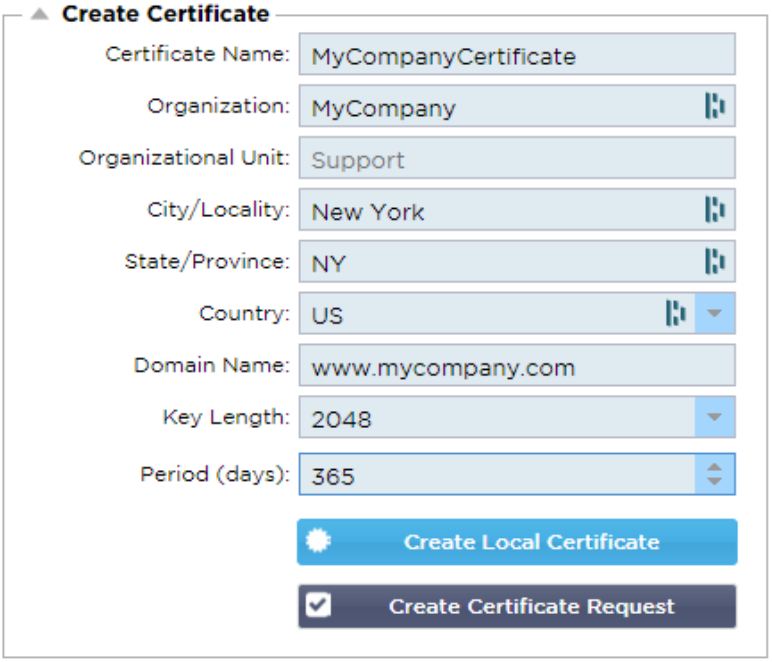
So erstellen Sie ein lokales SSL-Zertifikat



- Füllen Sie alle Details wie im obigen Beispiel aus
- Klicken Sie auf Lokales Zertifikat erstellen
- Sobald Sie dies angeklickt haben, können Sie das Zertifikat auf einen **VIRTUELLEN DIENST** anwenden.

Erstellen einer Zertifikatsanforderung (CSR)

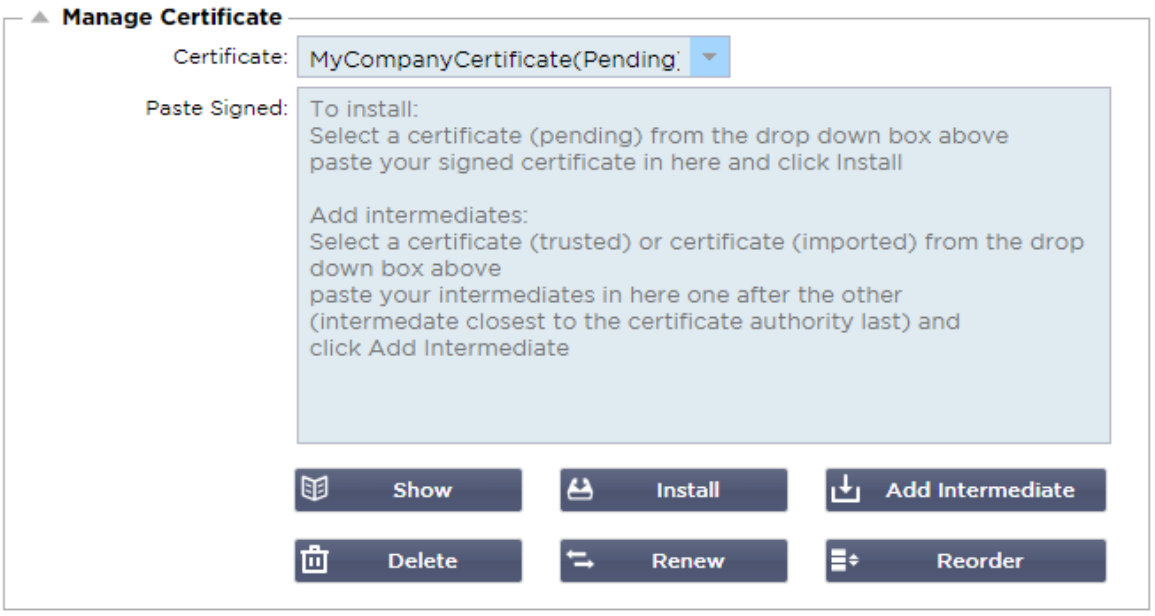
Wenn Sie ein global vertrauenswürdiges SSL von einem externen Anbieter beziehen müssen, benötigen Sie eine CSR, um das SSL-Zertifikat zu generieren.



Füllen Sie das Formular wie oben gezeigt mit allen relevanten Daten aus und klicken Sie dann auf die Schaltfläche Zertifikat anfordern. Es wird das Popup angezeigt, das den von Ihnen angegebenen Daten entspricht.

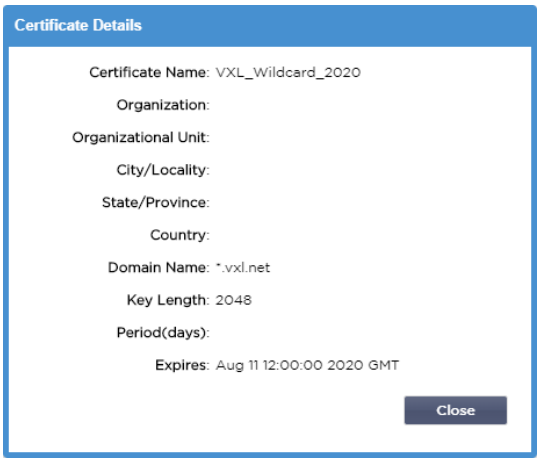
Sie müssen den Inhalt ausschneiden und in eine TEXT-Datei einfügen und diese mit einer CSR-Dateierweiterung benennen, z. B. *mycert.csr*. Diese CSR-Datei müssen Sie dann Ihrer Zertifizierungsstelle zur Verfügung stellen, um das SSL-Zertifikat zu erstellen.

Zertifikat verwalten



Dieser Unterabschnitt enthält verschiedene Werkzeuge, um die Verwaltung der SSL-Zertifikate zu ermöglichen, die Sie innerhalb des ADC haben.

anzeigen

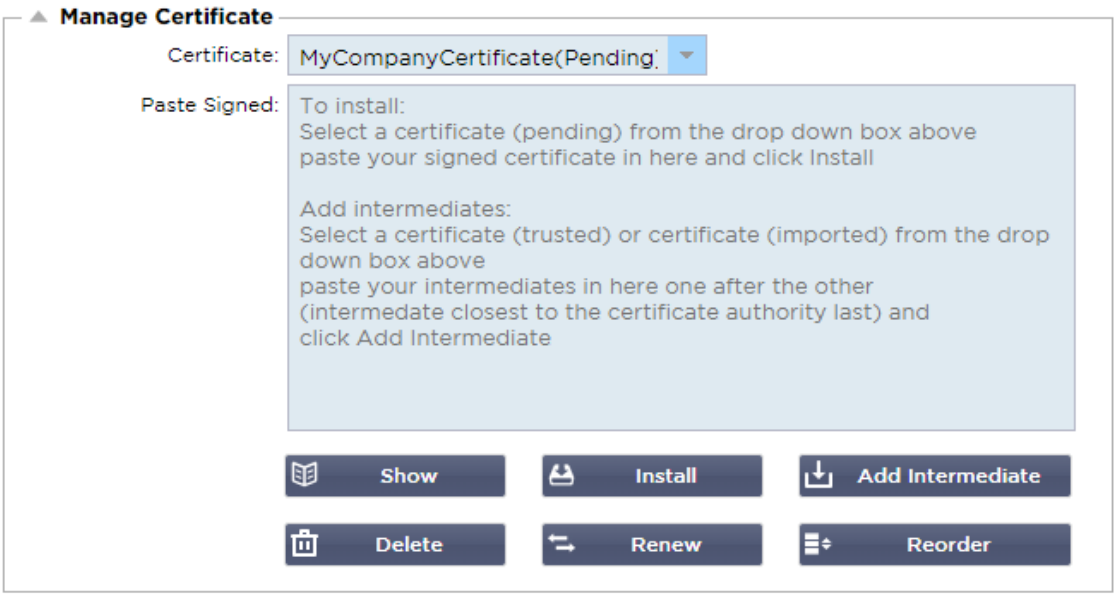


Es kann vorkommen, dass Sie sich die Details eines installierten SSL-Zertifikats ansehen möchten.

- Wählen Sie das Zertifikat aus dem Dropdown-Menü
- Klicken Sie auf die Schaltfläche Anzeigen
- Das unten gezeigte Popup wird mit den Details des Zertifikats angezeigt.

Installieren eines Zertifikats

Sobald Sie das Zertifikat von der vertrauenswürdigen Zertifizierungsstelle erhalten haben, müssen Sie es mit der generierten CSR abgleichen und innerhalb des ADC installieren.



- Wählen Sie ein Zertifikat, das Sie in den obigen Schritten erzeugt haben. An der Position wird der Status (Ausstehend) festgelegt. Im Beispiel ist MyCompanyCertificate in der obigen Abbildung zu sehen.
- Öffnen Sie die Zertifikatsdatei in einem Texteditor
- Kopieren Sie den gesamten Inhalt der Datei in die Zwischenablage
- Fügen Sie den Inhalt des signierten SSL-Zertifikats, das Sie von der vertrauenswürdigen Stelle erhalten haben, in das Feld Signiert einfügen ein.
- Sie können auch die Intermediates darunter einfügen, wobei Sie auf die richtige Reihenfolge achten müssen:
    1. (TOP) Ihr signiertes Zertifikat
    2. (2. von oben) Zwischenzeit 1

3. (3. von oben) Zwischenzeit 2
4. (Unten) Zwischenzeit 3
5. Root-Zertifizierungsstelle Diese müssen nicht hinzugefügt werden, da sie auf den Client-Rechnern vorhanden sind.
   (der ADC enthält auch ein Root-Bündel für die erneute Verschlüsselung, bei der er als Client zu einem Real Server fungiert).

- Klicken Sie auf Installieren
- Sobald Sie das Zertifikat installiert haben, sollten Sie den Status (Trusted) neben Ihrem Zertifikat sehen

Wenn Sie einen Fehler gemacht oder die falsche Zwischenreihenfolge eingegeben haben, dann wählen Sie das Zertifikat (vertrauenswürdig) und fügen Sie die Zertifikate (einschließlich des signierten Zertifikats) wieder in der richtigen Reihenfolge hinzu und klicken Sie auf Installieren

Zwischenzeitlich hinzufügen

Es ist gelegentlich erforderlich, Zwischenzertifikate separat hinzuzufügen. Es kann z. B. sein, dass Sie ein Zertifikat importiert haben, das nicht über die Zwischenzertifikate verfügt.

- Markieren Sie ein Zertifikat (vertrauenswürdig) oder ein Zertifikat (importiert)
- Fügen Sie die Zwischenprodukte untereinander ein und achten Sie darauf, dass das Zwischenprodukt, das der Zertifizierungsstelle am nächsten liegt, zuletzt eingefügt wird.
- Klicken Sie auf Zwischenablage hinzufügen.

Wenn Sie einen Fehler bei der Reihenfolge machen, können Sie den Vorgang wiederholen und die Zwischenschritte erneut hinzufügen. Diese Aktion überschreibt nur die vorherigen Zwischenschritte.

Ein Zertifikat löschen

Sie können ein Zertifikat mit der Schaltfläche Löschen löschen. Nach dem Löschen wird das Zertifikat vollständig aus dem ADC entfernt und muss ersetzt und dann bei Bedarf wieder auf die virtuellen Dienste angewendet werden.

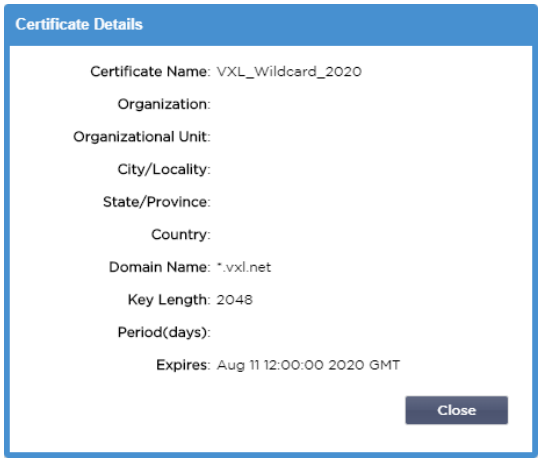
Hinweis: Stellen Sie sicher, dass das Zertifikat nicht an ein betriebsbereites VIP angehängt ist, bevor Sie es löschen.

Ein Zertifikat erneuern

Mit der Schaltfläche Erneuern können Sie eine neue Zertifikatssignierungsanforderung anfordern. Diese Aktion ist erforderlich, wenn das Zertifikat abläuft und erneuert werden muss.

- Wählen Sie ein Zertifikat aus der Dropdown-Liste; Sie können jedes Zertifikat mit dem Status (Ausstehend), (Vertrauenswürdig) oder (Importiert) wählen
- Klicken Sie auf Erneuern
- Kopieren Sie die neuen CSR-Details, damit Sie ein neues Zertifikat erhalten können

- Wenn Sie das neue Zertifikat erhalten, folgen Sie den Schritten, die in **ZEIGEN**



- **ES** kann vorkommen, dass Sie sich die Details eines installierten SSL-Zertifikats ansehen möchten.
- Wählen Sie das Zertifikat aus dem Dropdown-Menü
- Klicken Sie auf die Schaltfläche Anzeigen
- Das unten gezeigte Popup wird mit den Details des Zertifikats angezeigt.
- Installieren eines Zertifikats.
- Das neue und erneuerte Zertifikat wird nun im ADC installiert.

Importieren eines Zertifikats

In vielen Fällen müssen Unternehmen ihre domänensignierten Zertifikate als Teil ihres internen Sicherheitssystems verwenden. Die Zertifikate müssen im PKCS#12-Format vorliegen, und solche Zertifikate sind immer durch Passwörter geschützt.

Das Bild unten zeigt den Unterabschnitt zum Importieren eines einzelnen SSL-Zertifikats.

- Geben Sie Ihrem Zertifikat einen freundlichen Namen. Der Name identifiziert es in den im ADC verwendeten Dropdown-Listen. Er muss nicht mit dem Domänennamen des Zertifikats übereinstimmen, muss aber alphanumerisch sein und darf keine Leerzeichen enthalten. Andere Sonderzeichen als _ und - sind nicht erlaubt.
- Geben Sie das Passwort ein, das Sie zum Erstellen des PKCS#12-Zertifikats verwendet haben
- Suchen Sie nach der Datei {Zertifikatname}.pfx
- Klicken Sie auf Importieren.
- Ihr Zertifikat befindet sich nun in den entsprechenden SSL-Dropdown-Menüs innerhalb des ADC

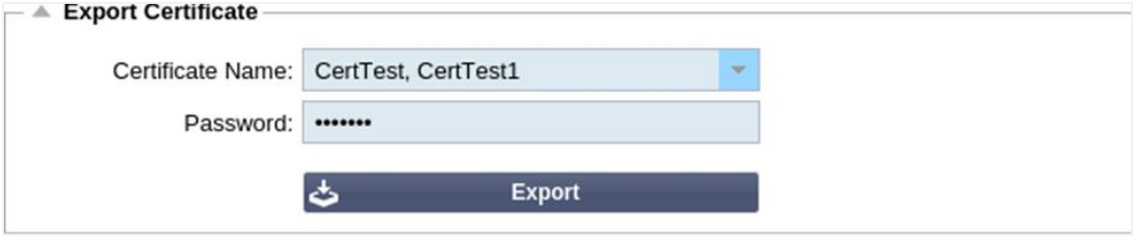
Importieren von mehreren Zertifikaten

In diesem Abschnitt können Sie eine JNBK-Datei importieren, die mehrere Zertifikate enthält. Eine JNBK-Datei wird verschlüsselt und von ADC erzeugt, wenn Sie mehrere Zertifikate exportieren.

- Suchen Sie nach Ihrer JNBK-Datei - Sie können eine solche Datei durch den Export mehrerer Zertifikate erstellen
- Geben Sie das Passwort ein, das Sie zum Erstellen der JNBK-Datei verwendet haben
- Klicken Sie auf Importieren.
- Ihre Zertifikate befinden sich nun in den entsprechenden SSL-Dropdown-Menüs innerhalb des ADC

Exportieren eines Zertifikats

Von Zeit zu Zeit möchten Sie vielleicht eines der im ADC gespeicherten Zertifikate exportieren. Das ADC wurde mit der Fähigkeit ausgestattet, dies zu tun.



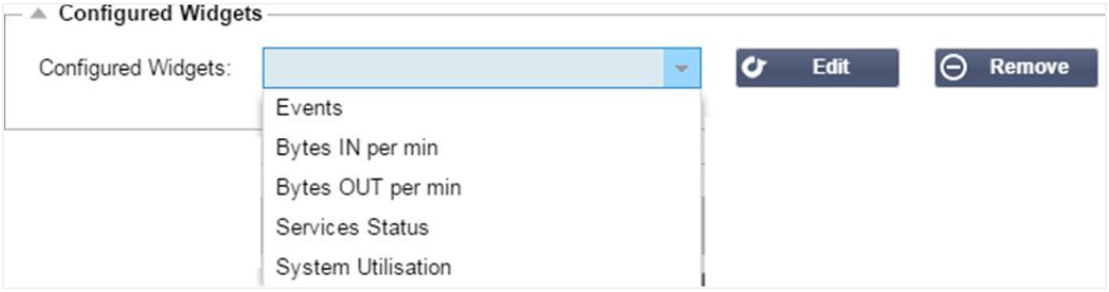
- Klicken Sie auf das Zertifikat oder die Zertifikate, die Sie installieren möchten. Sie können auch auf die Option Alle klicken, um alle aufgelisteten Zertifikate auszuwählen.
- Geben Sie ein Passwort ein, um die exportierte Datei zu schützen. Das Passwort muss mindestens sechs Zeichen lang sein. Es können Buchstaben, Zahlen und bestimmte Symbole verwendet werden. Die folgenden Zeichen sind **nicht** zulässig: < > " ' ( ) ; \ | \A3 % &
- Klicken Sie auf Exportieren
- Wenn Sie ein einzelnes Zertifikat exportieren, wird die resultierende Datei sslcert_{certname}.pfx genannt. Zum Beispiel sslcert_Test1Cert.pfx
- Im Falle eines Exports von mehreren Zertifikaten wird die resultierende Datei eine JNBK-Datei sein. Der Dateiname ist dann sslcert__pack.jnbk.

Hinweis: Eine JNBK-Datei ist eine verschlüsselte Container-Datei, die vom ADC erzeugt wird und nur für den Import in das ADC gültig ist

Widgets

Die Seite Bibliothek > Widgets ermöglicht es Ihnen, verschiedene leichtgewichtige visuelle Komponenten zu konfigurieren, die in Ihrem benutzerdefinierten Dashboard angezeigt werden.

Konfigurierte Widgets

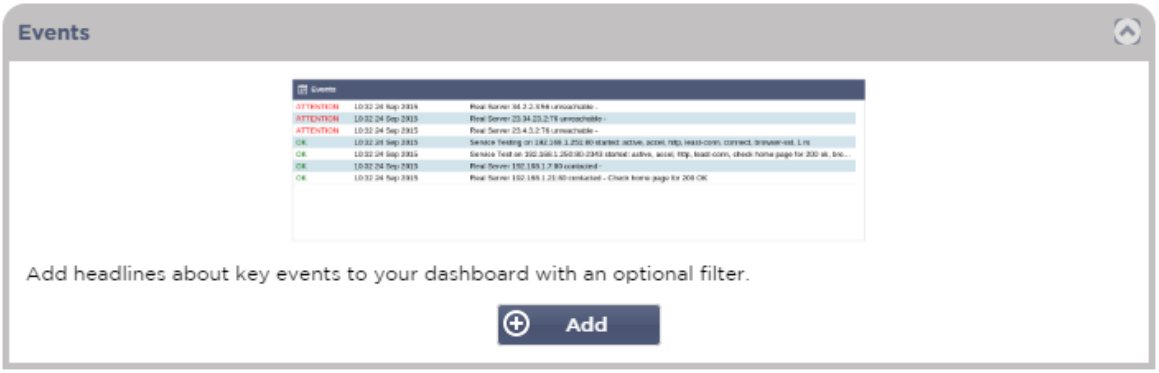


Im Bereich Konfigurierte Widgets können Sie alle erstellten Widgets aus dem Bereich Verfügbare Widgets anzeigen, bearbeiten oder entfernen.

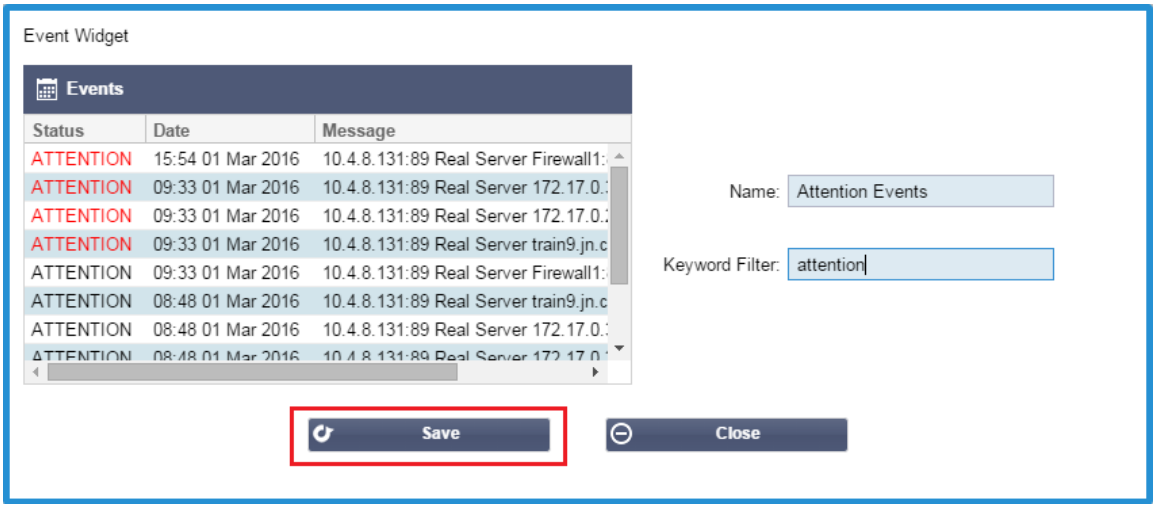
Verfügbare Widgets

Es gibt fünf verschiedene Widgets, die im ADC zur Verfügung stehen und die Sie nach Ihren Wünschen konfigurieren können.

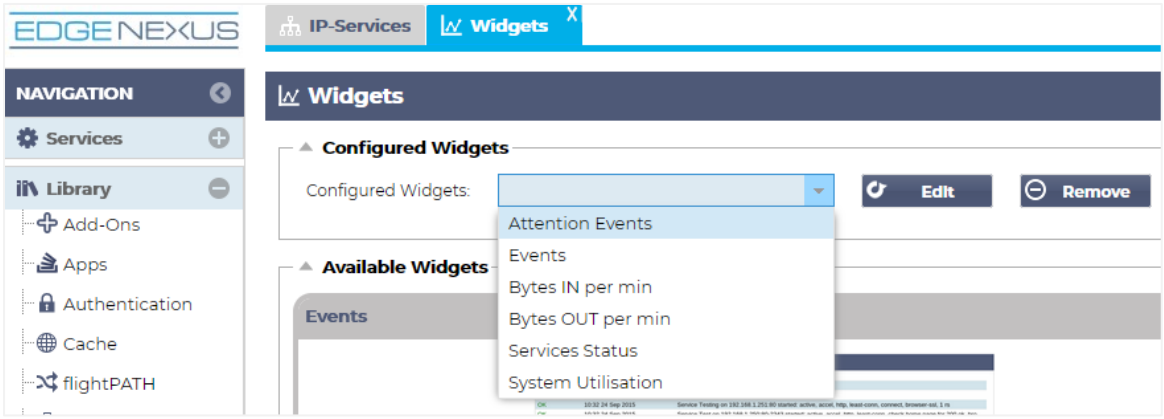
Das Ereignis-Widget



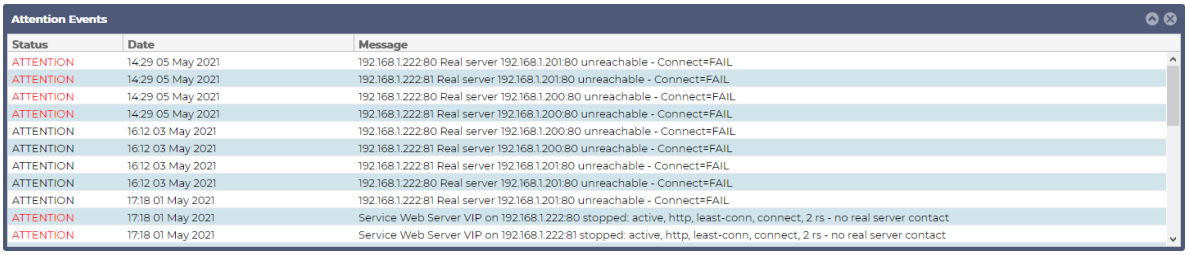
- Um ein Ereignis zum Ereignis-Widget hinzuzufügen, klicken Sie auf die Schaltfläche Hinzufügen.
- Geben Sie einen Namen für Ihr Ereignis an. In unserem Beispiel haben wir Aufmerksamkeitsereignisse als Namen für das Ereignis hinzugefügt.
- Fügen Sie einen Schlüsselwort-Filter hinzu. Wir haben auch den Filterwert von Achtung hinzugefügt



- Klicken Sie auf Speichern und dann auf Schließen
- Sie sehen nun ein zusätzliches Widget namens Aufmerksamkeitsereignisse in der Dropdown-Liste Konfigurierte Widgets.

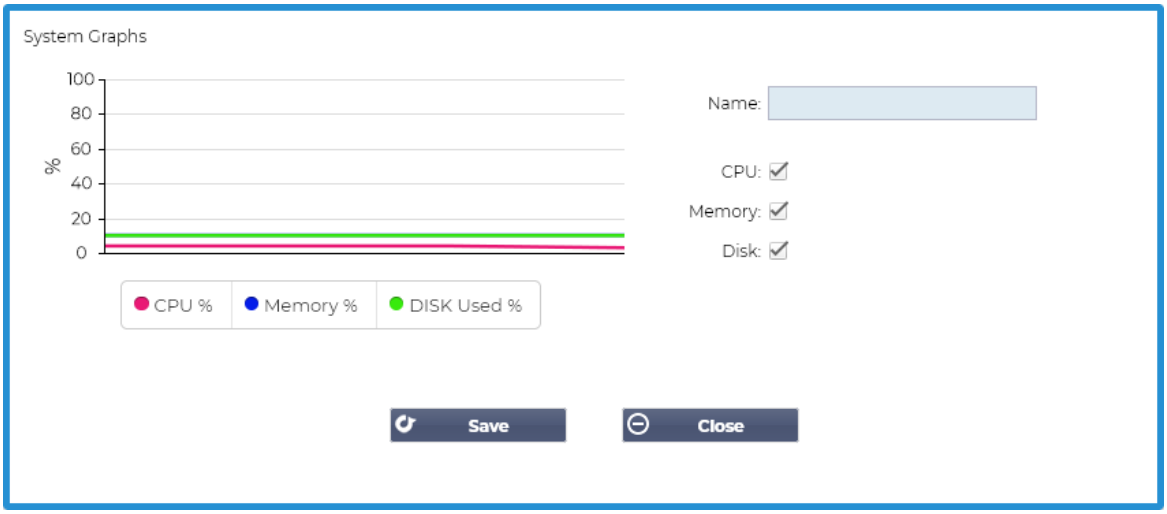


- Sie sehen, dass wir dieses Widget jetzt im Bereich Ansicht > Dashboard hinzugefügt haben.
- Wählen Sie das Widget Aufmerksamkeitsereignisse, um dieses im Dashboard anzuzeigen. Siehe unten.



Sie können den Live-Daten-Feed auch anhalten und neu starten, indem Sie auf die Schaltfläche Live-Daten anhalten klicken. Darüber hinaus können Sie jederzeit zum Standard-Dashboard zurückkehren, indem Sie auf die Schaltfläche Standard-Dashboard klicken.

Das Systemgrafik-Widget

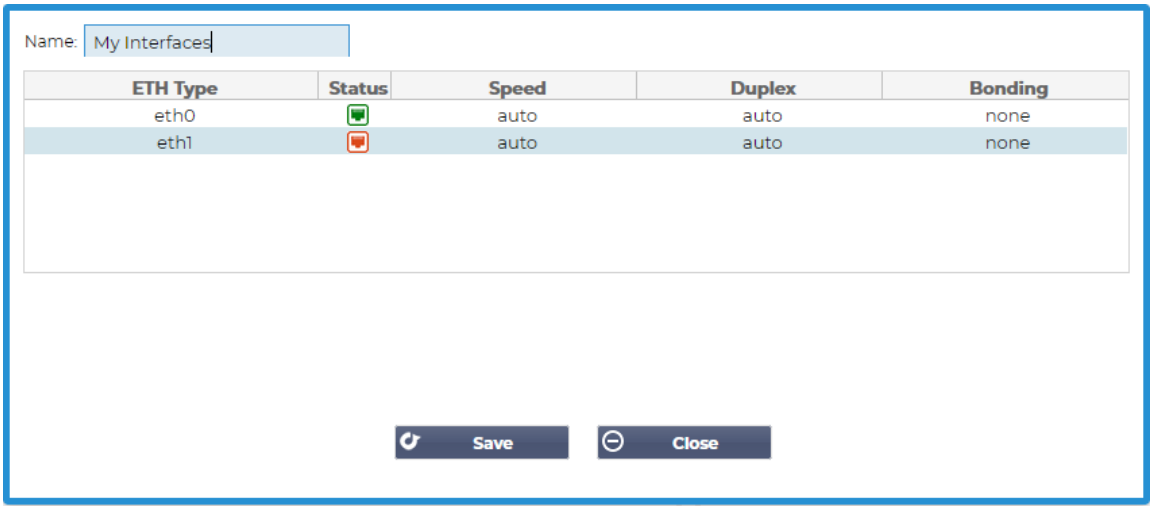


Der ADC verfügt über ein konfigurierbares Systemgrafik-Widget. Indem Sie auf die Schaltfläche Hinzufügen des Widgets klicken, können Sie die folgenden Überwachungsgrafiken zur Anzeige hinzufügen.

- CPU
- SPEICHER
- DISK

Sobald Sie sie hinzugefügt haben, sind sie einzeln im Widget-Menü des Dashboards verfügbar.

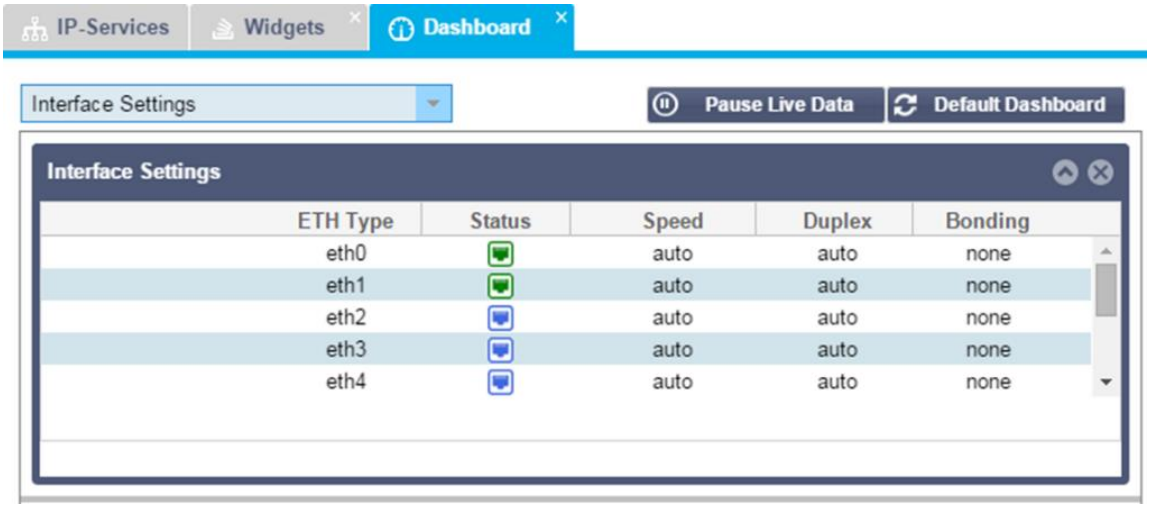
Interface-Widget



Mit dem Schnittstellen-Widget können Sie die Daten für die gewählte Netzwerkschnittstelle anzeigen, z. B. ETH0, ETH1 und so weiter. Die Anzahl der verfügbaren Schnittstellen zum Hinzufügen hängt davon ab, wie viele Netzwerkschnittstellen Sie für die virtuelle Appliance definiert oder innerhalb der Hardware-Appliance bereitgestellt haben.

Wenn Sie fertig sind, klicken Sie auf die Schaltfläche Speichern und dann auf die Schaltfläche Schließen.

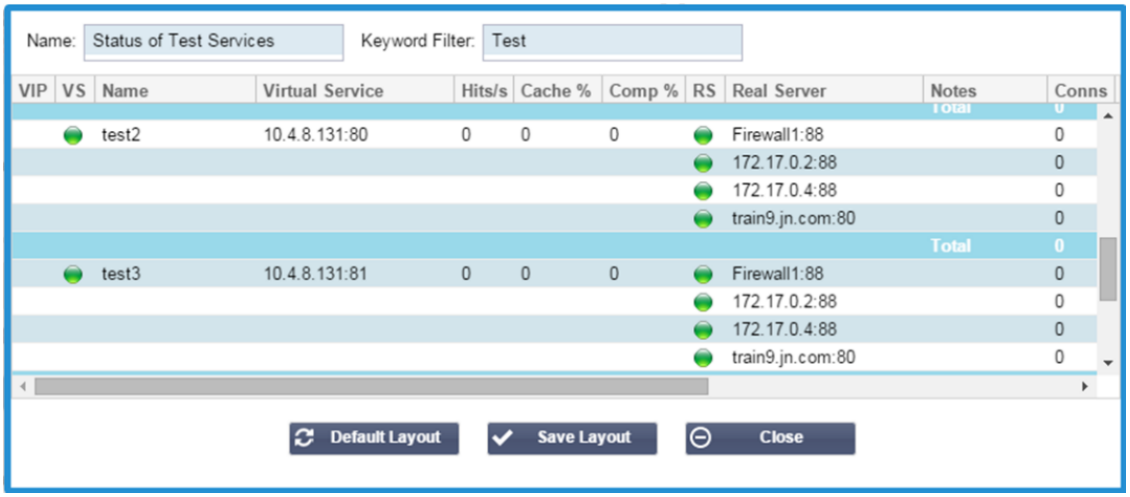
Wählen Sie das soeben angepasste Widget aus dem Widget-Dropdown-Menü im Dashboard. Sie sehen einen Bildschirm wie den unten abgebildeten.



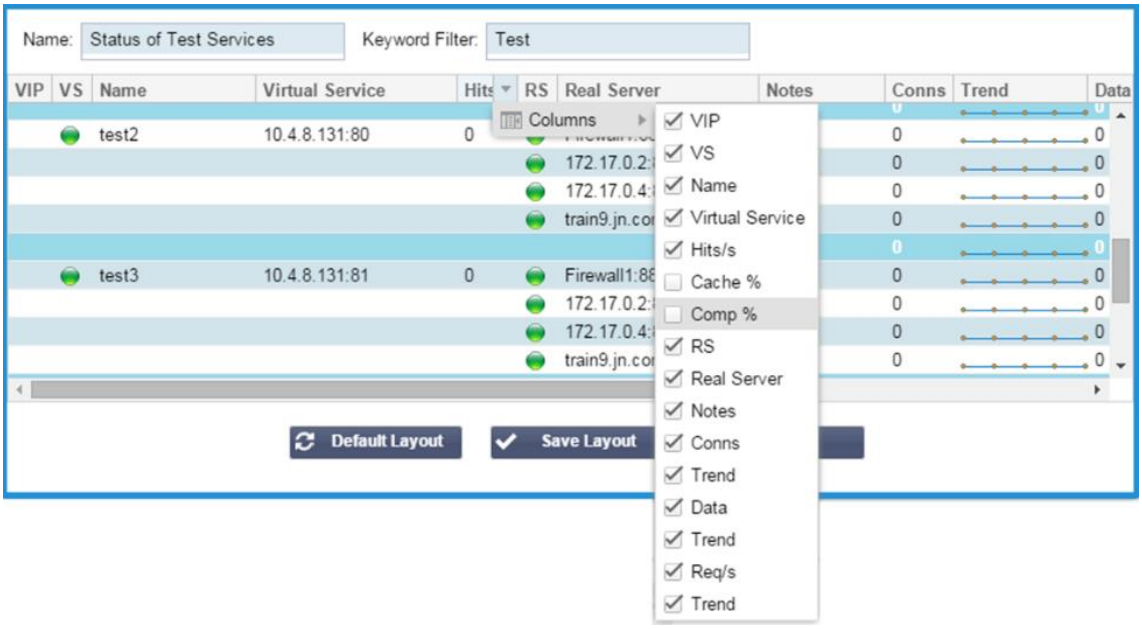
Status-Widget

Mit dem Status-Widget können Sie den Lastausgleich in Aktion sehen. Sie können die Ansicht auch filtern, um bestimmte Informationen anzuzeigen.

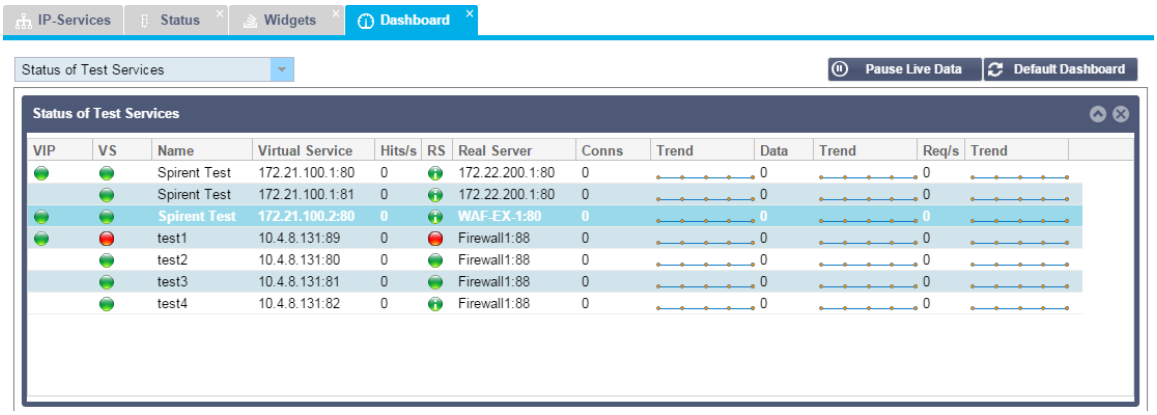
- Klicken Sie auf Hinzufügen.



- Geben Sie einen Namen für den Dienst ein, den Sie überwachen möchten
- Sie können auch wählen, welche Spalten Sie im Widget anzeigen möchten.

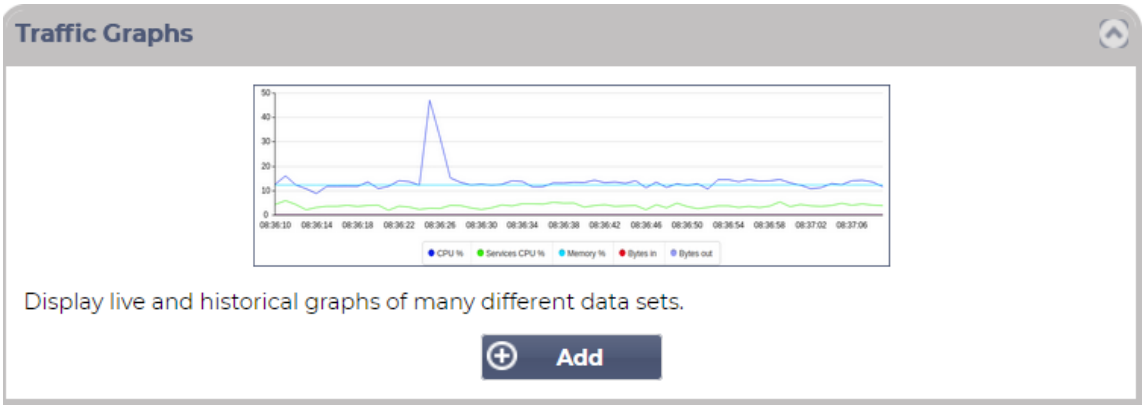


- Wenn Sie zufrieden sind, klicken Sie auf Speichern, gefolgt von Schließen.
- Das gewählte Status-Widget wird im Bereich Dashboard verfügbar sein.



Verkehrsgrafik-Widget

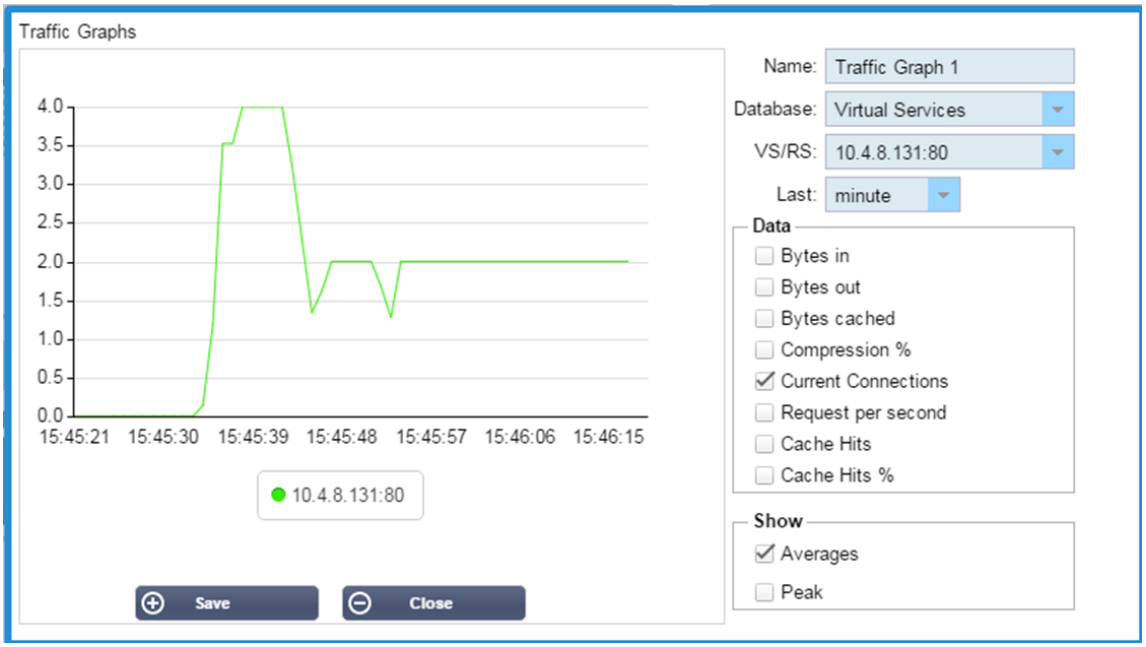
Dieses Widget kann so konfiguriert werden, dass es aktuelle und historische Verkehrsdaten pro Virtual Services und Real Servers anzeigt. Außerdem können Sie insgesamt aktuelle und historische Daten für den globalen Datenverkehr sehen



- Klicken Sie auf die Schaltfläche Hinzufügen
- Benennen Sie Ihr Widget.
- Wählen Sie eine Datenbank aus Virtuelle Dienste, Reale Server oder System.

- Wenn Sie Virtuelle Dienste wählen, können Sie einen virtuellen Dienst aus dem Dropdown-Menü VS/RS auswählen.
- Wählen Sie einen Zeitrahmen aus dem Dropdown-Menü Letzte.
    - Minute - letzte 60s
    - Stunde - aggregierte Daten aus jeder Minute für die letzten 60 Minuten
    - Tag - aggregierte Daten von jeder Stunde für die letzten 24 Stunden
    - Woche - aggregierte Daten von jedem Tag der letzten sieben Tage
    - Monat - aggregierte Daten aus jeder Woche für die letzten sieben Tage
    - Jahr - aggregierte Daten aus jedem Monat der letzten 12 Monate
- Wählen Sie die verfügbaren Daten je nach gewählter Datenbank
    - Datenbank für virtuelle Dienste
    - Bytes in
    - Bytes aus
    - Zwischengespeicherte Bytes
    - Komprimierung %
    - Aktuelle Verbindungen
    - Abfragen pro Sekunde
    - Cache-Treffer
    - Cache-Treffer %
- Echte Server
    - Bytes in
    - Bytes aus
    - Aktuelle Verbindungen
    - Anfrage pro Sekunde
    - Reaktionszeit
- System
    - CPU %
    - Dienste CPU
    - Speicher %
    - Platte Frei %
    - Bytes in
    - Bytes aus
- Wählen Sie, ob Sie Durchschnitts- oder Spitzenwerte anzeigen möchten
- Wenn Sie alle Optionen gewählt haben, klicken Sie auf Speichern und Schließen

Beispiel-Verkehrsdiagramm



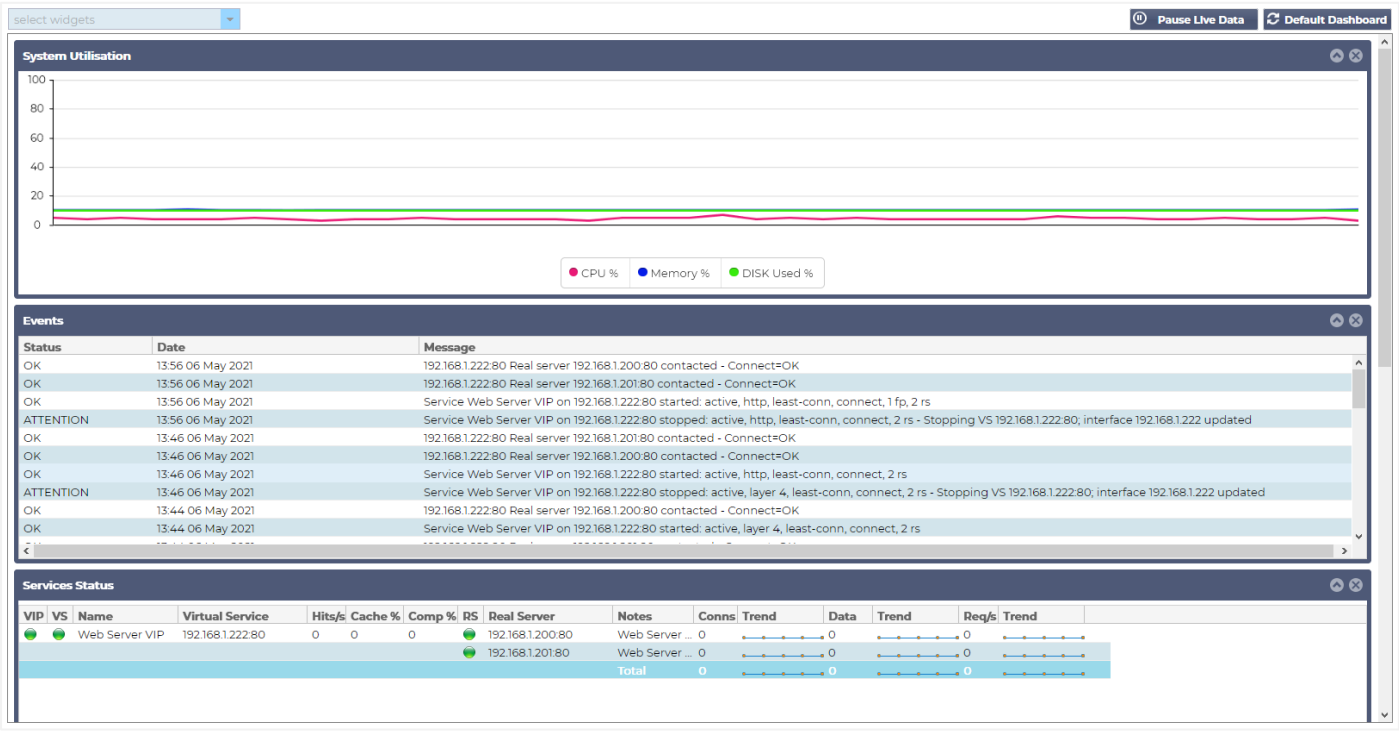
Sie können nun Ihr Traffic Graph-Widget zu Ansicht > Dashboard hinzufügen.

Ansicht

Dashboard

Wie bei allen Schnittstellen zur Verwaltung von IT-Systemen gibt es viele Gelegenheiten, bei denen Sie einen Blick auf die Leistungsmetriken und Daten werfen müssen, die der ADC verarbeitet. Wir bieten Ihnen ein anpassbares Dashboard, mit dem Sie dies auf einfache und aussagekräftige Weise tun können.

Das Dashboard ist über das Segment Ansicht des Navigatorpanels erreichbar. Wenn es ausgewählt ist, zeigt es mehrere Standard-Widgets an und ermöglicht es Ihnen, beliebige angepasste Widgets auszuwählen, die Sie definiert haben.



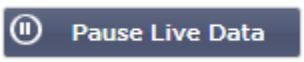
Dashboard-Verwendung

Es gibt vier Elemente im Dashboard U: Das Widgets-Menü, die Pause/Play-Taste und die Standard-Dashboard-Taste.

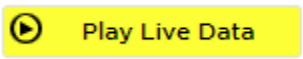
Das Menü Widgets

Über das Menü Widgets oben links im Dashboard können Sie alle von Ihnen definierten Standard- oder angepassten Widgets auswählen und hinzufügen. Um dieses zu verwenden, wählen Sie das Widget aus dem Dropdown-Menü.

Taste "Live-Daten anhalten



Mit dieser Schaltfläche können Sie auswählen, ob das ADC das Dashboard in Echtzeit aktualisieren soll. Nach dem Anhalten wird kein Dashboard-Widget aktualisiert, so dass Sie den Inhalt in aller Ruhe untersuchen können. Die Schaltfläche ändert ihren Zustand in die Anzeige Play Live Data, sobald eine Pause eingeleitet wird.



Wenn Sie fertig sind, klicken Sie einfach auf die Schaltfläche Live-Daten wiedergeben, um die Datenerfassung neu zu starten und das Dashboard zu aktualisieren.

Standard-Dashboard-Schaltfläche

Es kann vorkommen, dass Sie das Layout des Dashboards auf die Standardeinstellungen zurücksetzen möchten. Drücken Sie in einem solchen Fall die Schaltfläche Standard-Dashboard. Sobald Sie darauf klicken, gehen alle am Dashboard vorgenommenen Änderungen verloren.

Ändern der Größe, Minimieren, Umsortieren und Entfernen von Widgets

Größe eines Widgets ändern

Sie können die Größe eines Widgets sehr einfach ändern. Klicken Sie auf die Titelleiste des Widgets, halten Sie sie gedrückt und ziehen Sie sie an die linke oder rechte Seite des Dashboard-Bereichs. Sie sehen ein gepunktetes Rechteck, das die neue Größe des Widgets darstellt. Ziehen Sie das Widget in das Rechteck und lassen Sie die Maustaste los. Wenn Sie ein Widget mit geänderter Größe neben einem zuvor geänderten Widget ablegen möchten, sehen Sie, dass das Rechteck neben dem Widget erscheint, neben dem Sie es ablegen möchten.

Minimieren eines Widgets

Sie können Widgets jederzeit minimieren, indem Sie auf die Titelleiste des Widgets klicken. Durch diese Aktion wird das Widget minimiert und nur die Titelleiste angezeigt.

Reihenfolge der Widgets verschieben

Um ein Widget zu verschieben, können Sie es ziehen und ablegen, indem Sie auf die Titelleiste klicken, die Taste gedrückt halten und die Maus bewegen.

Entfernen eines Widgets

Sie können ein entfernen, indem Sie auf das ⊗Symbol in der Titelleiste des Widgets klicken.

Geschichte

Die Option Historie, die im Navigator ausgewählt werden kann, ermöglicht dem Administrator die Untersuchung der historischen Leistung des ADC. Historische Ansichten können für Virtual Services, Real Servers und System erstellt werden.

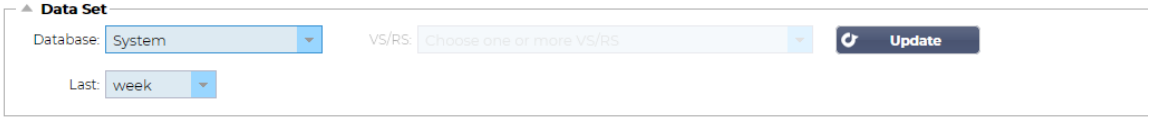
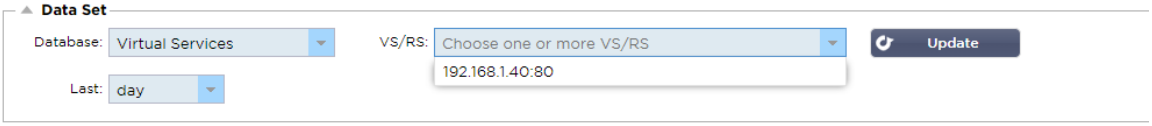
Es ermöglicht Ihnen auch, den Lastausgleich in Aktion zu sehen und hilft, Fehler oder Muster zu erkennen, die untersucht werden müssen. Beachten Sie, dass Sie die Verlaufsprotokollierung unter System > Verlauf aktivieren müssen, um diese Funktion nutzen zu können.

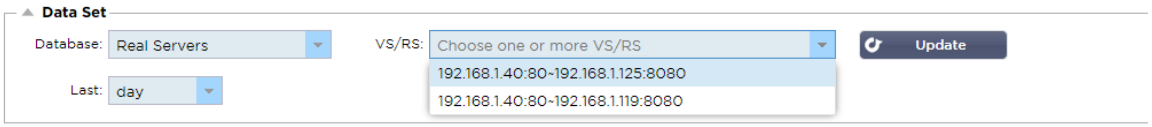
Anzeigen von grafischen Daten

Datensatz

Um die historischen Daten in einem grafischen Format zu betrachten, gehen Sie bitte wie folgt vor:

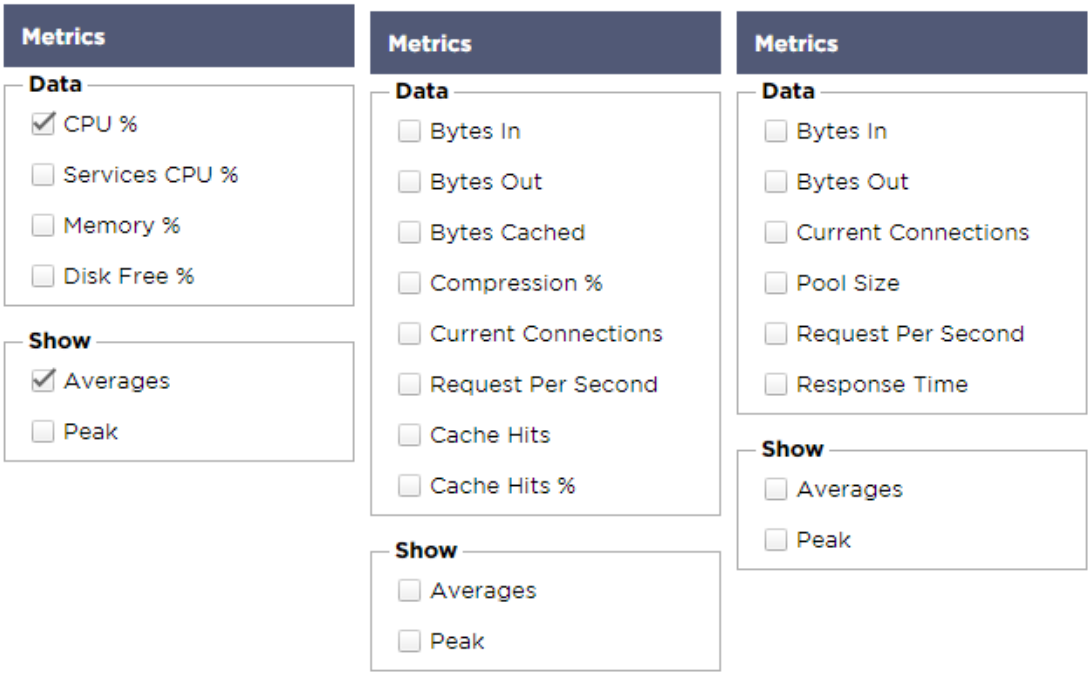
Der erste Schritt besteht darin, die Datenbank und den Zeitraum zu wählen, die für die Informationen relevant sind, die Sie ansehen möchten. Der Zeitraum, den Sie aus der Dropdown-Liste Letzte auswählen können, ist Minute, Stunde, Tag, Woche, Monat und Jahr.

Datenbank	Beschreibung
System	Wenn Sie diese Datenbank auswählen, können Sie CPU-, Speicher- und Festplattenspeicherplatz im Zeitverlauf sehen 
Virtuelle Dienste	Wenn Sie diese Datenbank auswählen, können Sie alle virtuellen Dienste in der Datenbank ab dem Zeitpunkt auswählen, an dem Sie mit der Datenaufzeichnung begonnen haben. Es wird eine Liste der virtuellen Dienste angezeigt, aus der Sie einen auswählen können. 
Echte Dienstleistungen	Wenn Sie diese Datenbank auswählen, können Sie alle Realserver in der Datenbank ab dem Zeitpunkt auswählen, an dem Sie mit der Aufzeichnung der Daten begonnen haben. Es wird eine Liste von Real-Servern angezeigt, aus der Sie einen auswählen können.

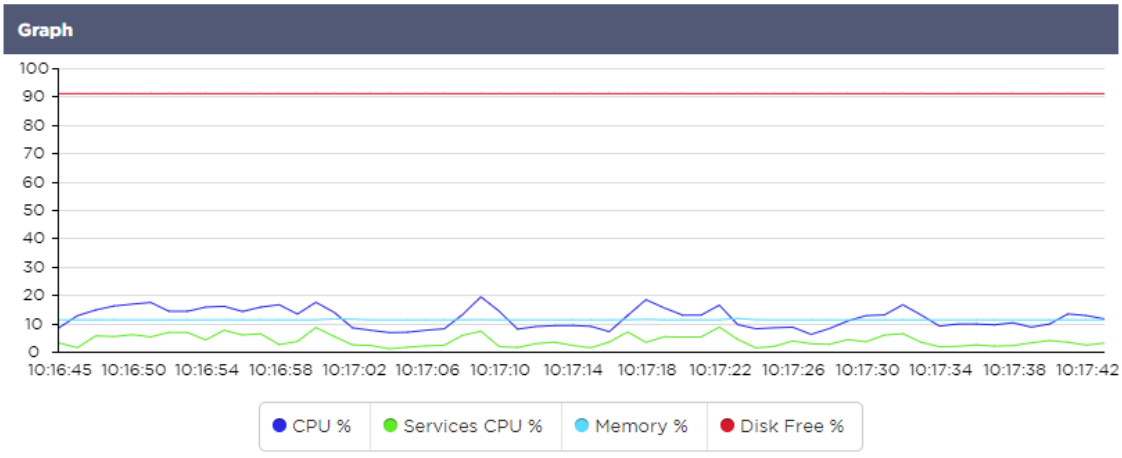


Metriken

Sobald Sie den zu verwendenden Datensatz ausgewählt haben, ist es an der Zeit, die anzuzeigenden Metriken zu wählen. Das Bild unten zeigt die Metriken, die dem Administrator zur Auswahl stehen: Diese Auswahlen entsprechen System, Virtuelle Dienste und Reale Server (von links nach rechts).



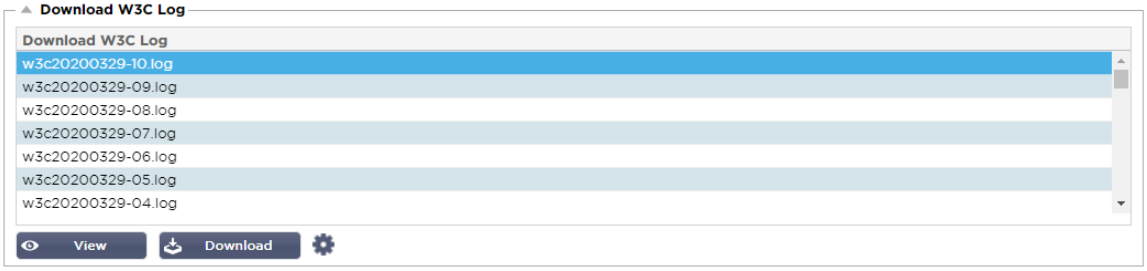
Beispiel-Grafik



Protokolle

Auf der Seite Protokolle im Bereich Ansicht können Sie die W3C- und Systemprotokolle in der Vorschau anzeigen und herunterladen. Die Seite ist in zwei Abschnitte unterteilt, wie unten beschrieben.

W3C-Protokolle herunterladen



Die W3C-Protokollierung wird über den Abschnitt System > Protokollierung aktiviert. Ein W3C-Protokoll ist ein Zugriffsprotokoll für Webserver, in dem Textdateien erzeugt werden, die Daten über jede Zugriffsanforderung enthalten, einschließlich der Quell-Internetprotokoll-(IP-)Adresse, der HTTP-Version, des Browsertyps, der Verweisseite und des Zeitstempels. W3C-Protokolle können sehr groß werden, abhängig von der Menge der Daten und der Kategorie der Protokollierung, die aufgezeichnet wird.

Im W3C-Bereich können Sie das gewünschte Protokoll auswählen und es dann ansehen oder herunterladen.

Schaltfläche anzeigen

Mit der Schaltfläche Ansicht können Sie das gewählte Protokoll in einem Texteditor-Fenster, z. B. Notepad, anzeigen.

Taste herunterladen

Mit dieser Schaltfläche können Sie das Protokoll auf Ihren lokalen Speicher herunterladen, um es später anzusehen.

Das Zahnrad-Symbol

Wenn Sie auf dieses Symbol klicken, gelangen Sie in den Bereich W3C-Protokolleinstellungen, der sich unter System > Protokollierung befindet. Wir werden dies im Abschnitt "Protokollierung" der Anleitung im Detail besprechen.

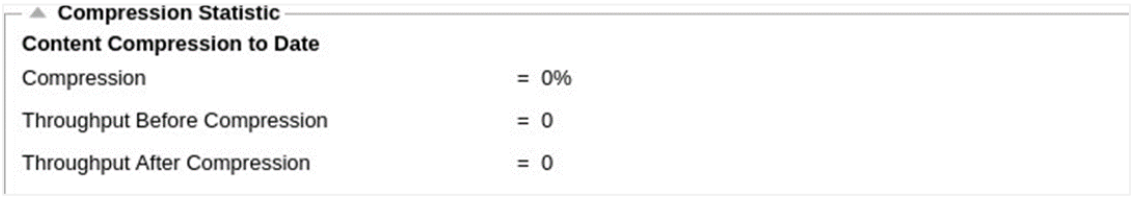
Statistik

Der Statistikbereich der ADC ist ein viel genutzter Bereich für Systemadministratoren, die sicherstellen wollen, dass die Leistung der ADC ihren Erwartungen entspricht.

Komprimierung

Der ganze Zweck des ADC besteht darin, Daten zu überwachen und sie an Real-Server zu leiten, die für den Empfang konfiguriert sind. Die Komprimierungsfunktion ist im ADC vorgesehen, um die Leistung des ADC zu erhöhen. Es wird Zeiten geben, in denen Administratoren die Datenkomprimierungsinformationen des ADC testen und überprüfen möchten; diese Daten werden im Komprimierungs-Panel innerhalb der Statistik bereitgestellt.

Inhaltliche Komprimierung bis heute



Die in diesem Abschnitt gezeigten Daten beschreiben den Grad der Komprimierung, den der ADC bei komprimierbaren Inhalten erreicht. Ein Wert von 60-80% ist das, was wir als typisch bezeichnen würden

Gesamtkomprimierung bis heute

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

Die in diesem Abschnitt angegebenen Werte geben an, wie viel Komprimierung der ADC bei allen Inhalten erreicht hat. Ein typischer Prozentsatz hierfür hängt davon ab, wie viele vorkomprimierte Bilder in Ihren Diensten enthalten sind. Je größer die Anzahl der Bilder ist, desto kleiner ist wahrscheinlich der Gesamtkomprimierungsprozentsatz.

Gesamt Input/Output

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

Die Zahlen für den Gesamteingang/-ausgang stellen die Menge der Rohdaten dar, die in den ADC hinein und aus ihm heraus übertragen werden. Die Maßeinheit ändert sich mit zunehmender Größe von kbps über Mbps bis Gbps.

Treffer und Verbindungen

Hits and Connections

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

Der Abschnitt "Hits und Verbindungen" enthält die Gesamtstatistik für Hits und Transaktionen, die das ADC durchlaufen. Was bedeuten also Treffer und Verbindungen?

- Ein Hit ist definiert als eine Layer 7-Transaktion. Typischerweise für Webserver verwendet, ist dies eine GET-Anfrage für ein Objekt wie z. B. ein Bild.
- Eine Verbindung ist definiert als eine Layer 4 TCP-Verbindung. Über 1 TCP-Verbindung können viele Transaktionen stattfinden.

Gezählte Gesamttreffer

Die Zahlen in diesem Abschnitt zeigen die kumulative Anzahl der nicht zwischengespeicherten Treffer seit dem letzten Zurücksetzen. Auf der rechten Seite zeigt die Abbildung die aktuelle Anzahl von Treffern pro Sekunde an.

Total Verbindungen

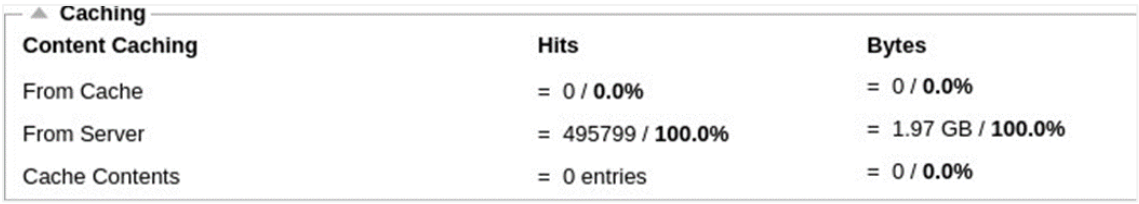
Der Wert Total Connections stellt die kumulative Anzahl der TCP-Verbindungen seit dem letzten Zurücksetzen dar. Die Zahl in der zweiten Spalte gibt die TCP-Verbindungen an, die pro Sekunde zum ADC hergestellt werden. Die Zahl in der rechten Spalte gibt die Anzahl der TCP-Verbindungen pro Sekunde an, die zu den Real-Servern hergestellt werden. Beispiel 6/8 Verbindungen/Sek. Im gezeigten Beispiel haben wir 6 TCP-Verbindungen pro Sekunde zum virtuellen Dienst und 6 TCP-Verbindungen pro Sekunde zu den Real-Servern.

Peak-Verbindungen

Der Spitzenwert Verbindungen stellt die maximale Anzahl von TCP-Verbindungen dar, die zum ADC hergestellt wurden. Die Zahl in der Spalte ganz rechts zeigt die aktuelle Anzahl der aktiven TCP-Verbindungen an.

Caching

Wie Sie sich erinnern werden, ist der ADC sowohl mit Komprimierung als auch mit Caching ausgestattet. Dieser Abschnitt zeigt die Gesamtstatistik in Bezug auf die Zwischenspeicherung, wenn sie auf einen Kanal angewendet wird. Wenn die Zwischenspeicherung nicht auf einen Kanal angewandt und korrekt konfiguriert wurde, sehen Sie 0 Cache-Inhalte.



Aus dem Cache

Treffer: Die erste Spalte gibt die Gesamtzahl der Transaktionen an, die seit dem letzten Zurücksetzen vom ADC-Cache bedient wurden. Es wird auch ein Prozentsatz der gesamten Transaktionen angegeben.

Bytes: Die zweite Spalte gibt die Gesamtdatenmenge in Kilobytes an, die aus dem ADC-Cache bedient wurde. Es wird auch ein Prozentsatz der Gesamtdaten angegeben.

Vom Server

Treffer: Spalte 1 gibt die Gesamtzahl der Transaktionen an, die von den Real-Servern seit dem letzten Zurücksetzen bedient wurden. Es wird auch ein Prozentsatz der gesamten Transaktionen angegeben.

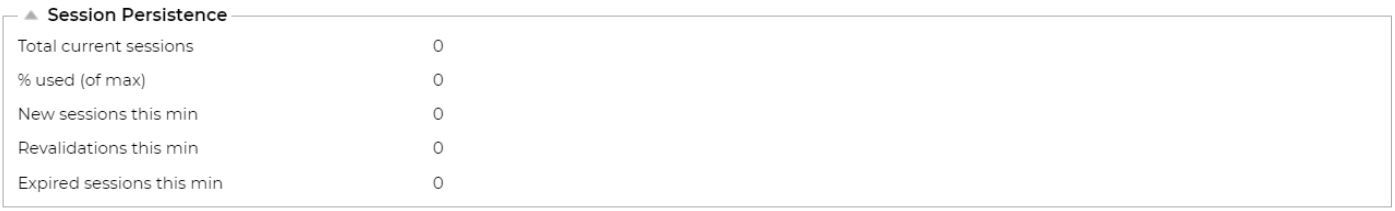
Bytes: Die zweite Spalte gibt die Gesamtdatenmenge in Kilobyte an, die von den Real-Servern geliefert wurde. Es wird auch ein Prozentsatz der Gesamtdaten angegeben.

Cache-Inhalt

Treffer: Diese Zahl gibt die Gesamtzahl der im ADC-Cache enthaltenen Objekte an.

Bytes: Die erste Zahl gibt die Gesamtgröße der ADC-Cache-Objekte in Megabyte an. Es wird auch ein Prozentsatz der maximalen Cache-Größe angegeben.

Session-Persistenz



Der Abschnitt Sitzungsaufrechterhaltung liefert Informationen für mehrere Parameter.

Feld	Beschreibung
Aktuelle Sitzungen insgesamt	Hier wird angezeigt, wie viele Persistenzsitzungen gerade laufen - minütlich aktualisiert
% Verwendet (von max)	Hier wird angezeigt, wie stark der gesamte für Sitzungsinformationen erlaubte Platz belegt ist
Neue Sitzung diese Minute	Dies zeigt innerhalb der letzten Minute an, wie viele neue Persistenzsitzungen hinzugefügt wurden
Revalidieren Sie dieses min	Dies zeigt innerhalb der letzten Minute an, wie viele bestehende Persistenz-Sitzungen durch mehr Verkehr neu validiert wurden
Abgelaufene Sitzungen in dieser Minute	Hier wird angezeigt, wie viele bestehende Persistenzsitzungen innerhalb der letzten Minute abgelaufen sind, weil innerhalb des Timeouts kein weiterer Datenverkehr stattfand

Hardware

Unabhängig davon, ob Sie den ADC in einer virtuellen Umgebung oder innerhalb von Hardware verwenden, erhalten Sie in diesem Abschnitt wertvolle Informationen über die Leistung der Appliance.

Festplattenverwendung

Der in Spalte 2 angegebene Wert gibt den Prozentsatz des aktuell belegten Speicherplatzes an und enthält Informationen über Protokolldateien und Cache-Daten, die periodisch auf dem Speicher abgelegt werden.

Speicherverwendung

Die zweite Spalte gibt den Prozentsatz des aktuell verwendeten Speichers an. Die bedeutendere Zahl in Klammern ist die Gesamtmenge des dem ADC zugewiesenen Speichers. Es wird empfohlen, dass dem ADC mindestens 2 GB RAM zugewiesen werden.

CPU-Auslastung

Einer der angegebenen kritischen Werte ist der Prozentsatz der CPU, der aktuell von ADC verwendet wird. Es ist normal, dass dieser Wert schwanken kann.

Status

Die Seite Ansicht > Status zeigt den Live-Verkehr an, der den ADC für die von Ihnen definierten virtuellen Dienste durchläuft. Sie zeigt auch die Anzahl der Verbindungen und Daten zu jedem Real Server, so dass Sie den Lastausgleich in Echtzeit erleben können.

Details zum virtuellen Dienst

VIP-Spalte

Die Farbe der Leuchte zeigt den Zustand der virtuellen IP-Adresse an, die mit einem oder mehreren virtuellen Diensten verbunden ist.

Status	Beschreibung
●	Online
●	Failover-Standby. Dieser virtuelle Dienst ist hot-standby
●	Zeigt an, dass ein "Passiv" auf ein "Aktiv" wartet
●	Offline. Reale Server sind nicht erreichbar, oder es sind keine realen Server aktiviert
●	Status finden
●	Nicht lizenziert oder lizenzierte virtuelle IPs überschritten

VS-Status-Spalte

Die Farbe der Leuchte zeigt den Zustand des virtuellen Dienstes an.

Status	Beschreibung
●	Online
●	Failover-Standby. Dieser virtuelle Dienst ist hot-standby
●	Zeigt an, dass ein "Passiv" auf ein "Aktiv" wartet
●	Dienst benötigt Aufmerksamkeit. Diese Statusanzeige kann daraus resultieren, dass ein Real Server eine Zustandsüberwachung nicht bestanden hat oder manuell auf Offline geändert wurde. Der Datenverkehr fließt weiter, aber mit reduzierter Real-Server-Kapazität.
●	Offline. Reale Server sind nicht erreichbar, oder es sind keine realen Server aktiviert
●	Status finden
●	Nicht lizenziert oder lizenzierte virtuelle IPs überschritten

Name

Der Name des virtuellen Dienstes

Virtueller Dienst (VIP)

Die virtuelle IP-Adresse und der Port für den Dienst und die Adresse, die Benutzer oder Anwendungen verwenden werden.

Treffer/Sek.

Layer 7-Transaktionen pro Sekunde auf der Client-Seite.

Cache%

Die hier angegebene Zahl stellt den Prozentsatz der Objekte dar, die aus dem RAM-Cache des ADC bedient wurden.

Komprimierung%.

Diese Zahl stellt den Prozentsatz der Objekte dar, die zwischen dem Client und dem ADC komprimiert wurden.

RS-Status (Remote Server)

In der folgenden Tabelle ist die Bedeutung des Status der mit dem VIP verknüpften Real-Server aufgeführt.

Status	Beschreibung
●	Verbunden
●	Nicht überwacht
●	Ablassen oder Offline
●	Standby
●	Nicht verbunden
●	Status finden
●	Nicht lizenziert oder lizenzierte virtuelle IPs überschritten

Real Server

Die IP-Adresse und der Port des Real-Servers.

Anmerkungen

Dieser Wert kann jede hilfreiche Anmerkung sein, damit andere den Zweck des Eintrags verstehen.

Verbindungen (Connections)

Durch die Darstellung der Anzahl der Verbindungen zu jedem Real Server können Sie die Lastverteilung in Aktion sehen. Sehr hilfreich, um zu überprüfen, ob Ihre Lastausgleichsrichtlinie korrekt funktioniert.

Daten

Der Wert in dieser Spalte zeigt die Datenmenge an, die an jeden Real-Server gesendet wird.

Req/Sec (Anfragen pro Sekunde)

Die Anzahl der Anfragen pro Sekunde, die an jeden Real-Server gesendet werden.

System

Das Segment "System" der Benutzeroberfläche des ADC ermöglicht Ihnen den Zugriff auf und die Steuerung aller systemweiten Aspekte des ADC.

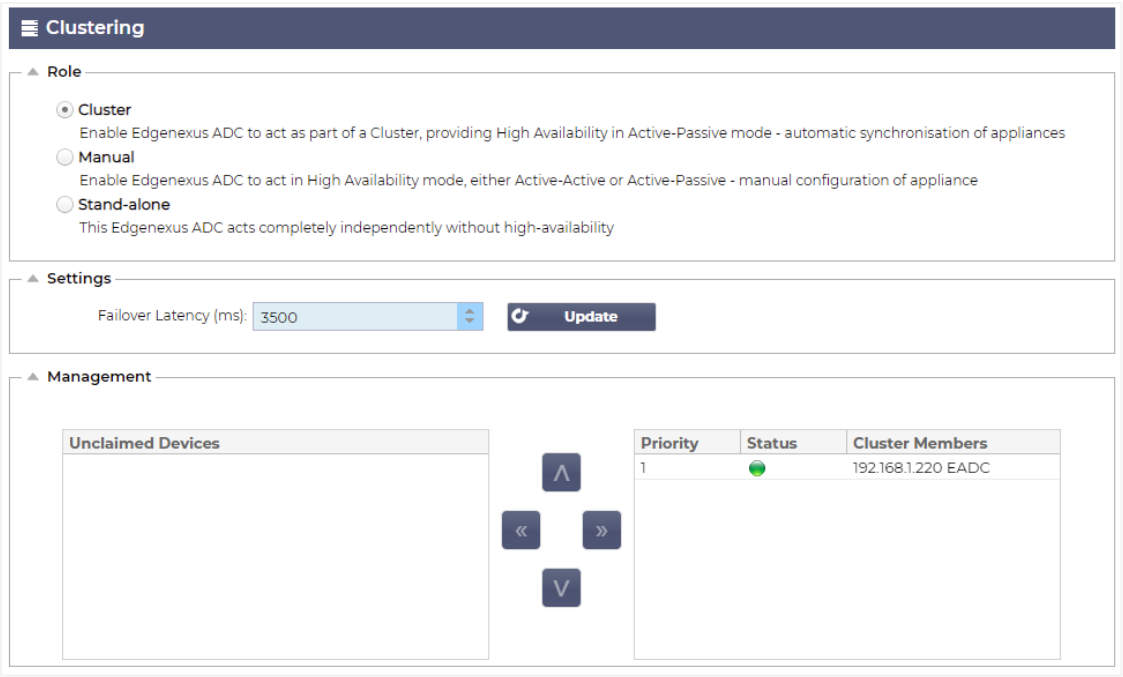
Clustering

Der ADC kann als einzelnes Standalone-Gerät verwendet werden, und das wird er auch perfekt tun. Wenn man jedoch bedenkt, dass der Zweck des ADC darin besteht, einen Lastausgleich zwischen mehreren Servern herzustellen, wird die Notwendigkeit, den ADC selbst zu clustern, offensichtlich. Das einfach zu navigierende UI-Design des ADC macht die Konfiguration des Clustering-Systems unkompliziert.

Auf der Seite System > Clustering konfigurieren Sie die Hochverfügbarkeit Ihrer ADC Appliances. Dieser Bereich ist in mehrere Abschnitte unterteilt.

Wichtiger Hinweis

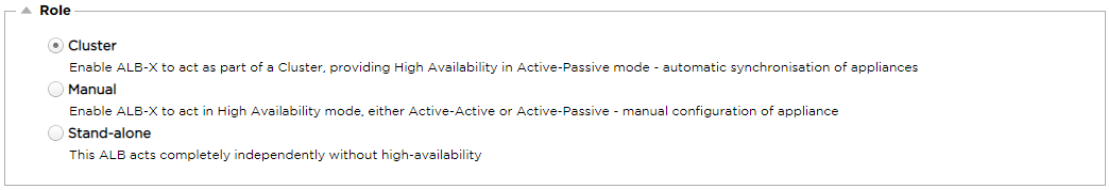
- Es ist kein dediziertes Kabel zwischen dem ADC-Paar erforderlich, um einen hochverfügbaren Heartbeat aufrechtzuerhalten.
- Der Heartbeat findet im selben Netzwerk statt wie der virtuelle Dienst, für den Hochverfügbarkeit eingerichtet werden muss.
- Es gibt kein Stateful Failover zwischen den ADC Appliances.
- Wenn Hochverfügbarkeit auf zwei oder mehr ADCs aktiviert ist, sendet jede Box über UDP die virtuellen Dienste, für die sie konfiguriert ist.
- Das hochverfügbare Failover verwendet Unicast-Messaging und Gratuitous ARP, um die neuen Active Load Balancer-Switches zu informieren.



Rolle

Es stehen drei Cluster-Rollen zur Verfügung, wenn Sie den ADC für hohe Verfügbarkeit konfigurieren.

Cluster



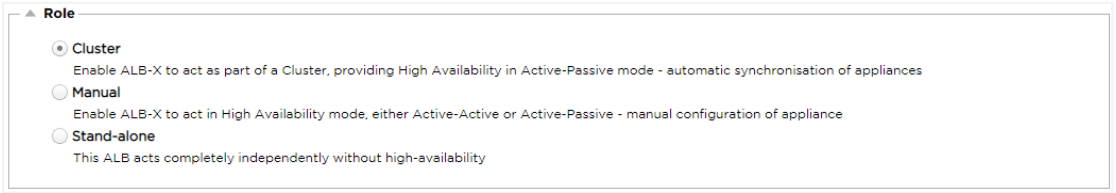
- Standardmäßig wird ein neuer ADC mit der Cluster-Rolle eingeschaltet. In dieser Rolle hat jedes Clustermitglied dieselbe "Arbeitskonfiguration", so dass immer nur ein ADC im Cluster aktiv ist.
- Unter einer "Arbeitskonfiguration" versteht man alle Konfigurationsparameter, mit Ausnahme von Elementen, die eindeutig sein müssen, wie z. B. die Management-IP-Adresse, der ALB-Name, die Netzwerkeinstellungen, die Schnittstellendetails usw.
- Der ADC in Priorität 1, der obersten Position, des Feldes Clustermitglieder ist der Clustereigentümer und der aktive Load Balancer, während alle anderen ADCs passive Mitglieder sind.
- Sie können jeden ADC im Cluster bearbeiten, und die Änderungen werden mit allen Cluster-Mitgliedern synchronisiert.
- Wenn Sie einen ADC aus dem Cluster entfernen, werden alle virtuellen Dienste von diesem ADC gelöscht.
- Sie können das letzte Mitglied des Clusters nicht auf Nicht beanspruchte Geräte entfernen. Um das letzte Mitglied zu entfernen, ändern Sie bitte die Rolle auf Manuell oder Stand-alone.
- Die folgenden Objekte werden nicht synchronisiert:
    - Manueller Bereich Datum & Zeit - (NTP-Bereich wird synchronisiert)
    - Failover-Latenzzeit (ms)
    - Hardware-Bereich
    - Abschnitt "Gerät
    - Netzwerk-Bereich

Ausfall des Clustereigentümers

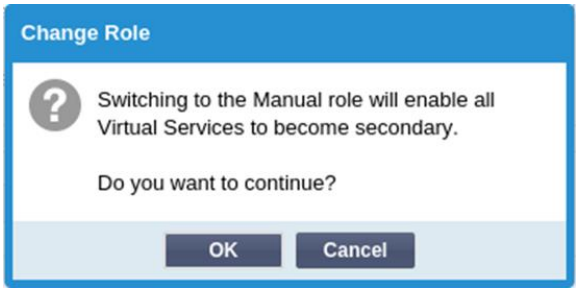
- Wenn ein Cluster-Eigentümer ausfällt, übernimmt automatisch eines der verbleibenden Mitglieder und führt den Lastausgleich des Datenverkehrs fort.
- Wenn der Clustereigentümer zurückkehrt, nimmt er den Lastausgleich wieder auf und übernimmt die Eigentümerrolle.
- Nehmen wir an, der Besitzer ist ausgefallen, und ein Mitglied hat den Lastausgleich übernommen. Wenn Sie möchten, dass das Mitglied, das den Lastausgleichsverkehr übernommen hat, der neue Besitzer wird, markieren Sie das Mitglied und klicken Sie auf den Pfeil nach oben, um es auf die Position Priorität 1 zu verschieben.
- Wenn Sie eines der verbleibenden Clustermitglieder bearbeiten und der Eigentümer ausgefallen ist, wird das bearbeitete Mitglied automatisch zum Eigentümer befördert, ohne dass es zu Verkehrsverlusten kommt

Ändern der Rolle von Cluster-Rolle auf Manuelle Rolle

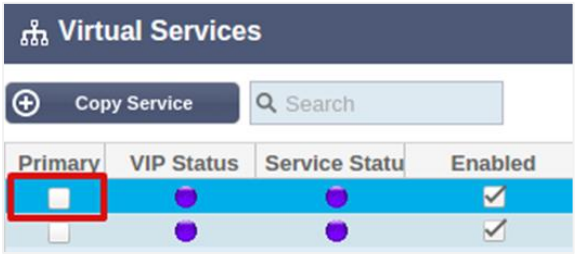
- Wenn Sie die Rolle von Cluster auf Manuell ändern möchten, klicken Sie auf das Optionsfeld neben der Rollenoption Manuell



- Nachdem Sie auf das Optionsfeld geklickt haben, wird die folgende Meldung angezeigt:



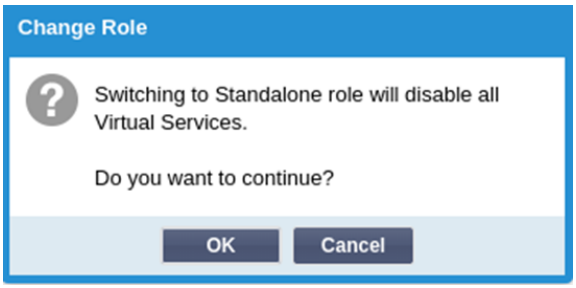
- Klicken Sie auf die Schaltfläche OK
- Prüfen Sie den Abschnitt Virtuelle Dienste. Sie werden feststellen, dass die Spalte Primär jetzt ein nicht angekreuztes Kästchen anzeigt.



- Es ist eine Sicherheitsfunktion und bedeutet, dass es keine Unterbrechung des Datenflusses gibt, wenn Sie einen anderen ADC mit denselben virtuellen Diensten haben.

Ändern der Rolle von Cluster zu Stand-alone

- Wenn Sie die Rolle von "Cluster" in "Standalone" ändern möchten, klicken Sie auf das Optionsfeld neben der Option "Standalone".
- Sie werden mit der folgenden Meldung darauf hingewiesen:



- Klicken Sie auf OK, um die Rollen zu ändern.
- Prüfen Sie Ihre virtuellen Dienste. Sie werden sehen, dass die Spalte Primary den Namen in Stand-alone ändert
- Sie werden auch sehen, dass alle Virtuellen Dienste aus Sicherheitsgründen deaktiviert (nicht angekreuzt) sind.
- Sobald Sie sicher sind, dass kein anderer ADC im selben Netzwerk über doppelte virtuelle Dienste verfügt, können Sie diese nacheinander aktivieren.

Manuell Rolle

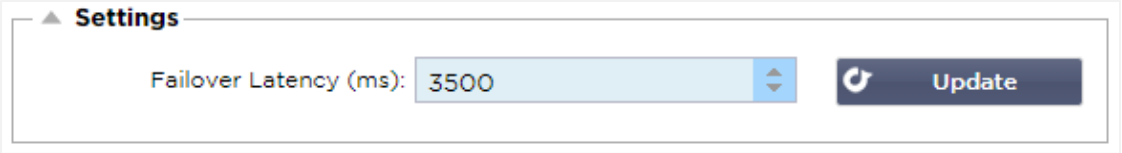
Ein ADC in der Rolle Manuell arbeitet mit anderen ADCs in der Rolle Manuell zusammen, um eine hohe Verfügbarkeit zu gewährleisten. Der Hauptvorteil gegenüber der Cluster-Rolle ist die Möglichkeit, festzulegen, welcher ADC für eine virtuelle IP aktiv ist. Der Nachteil ist, dass es keine Konfigurationssynchronisation zwischen den ADCs gibt. Alle Änderungen müssen manuell auf jeder Box über die GUI repliziert werden, oder für viele Änderungen können Sie ein jetPACK von einem ADC erstellen und dieses an den anderen senden.

- Um eine virtuelle IP-Adresse "aktiv" zu machen, aktivieren Sie das Kontrollkästchen in der primären Spalte (Seite IP-Dienste)
- Um eine virtuelle IP-Adresse "passiv" zu machen, lassen Sie das Kontrollkästchen in der primären Spalte (Seite IP-Dienste) leer
- Für den Fall, dass ein aktiver Dienst auf den passiven Dienst übergeht:
    - Wenn beide Primary Columns angekreuzt sind, findet ein Wahlprozess statt, und die niedrigste MAC-Adresse wird aktiv
    - Wenn beide nicht angekreuzt sind, findet der gleiche Wahlvorgang statt. Wenn beide nicht angekreuzt sind, gibt es außerdem keinen automatischen Rückgriff auf den ursprünglichen aktiven ADC

Stand-alone-Rolle

Ein ADC in der Rolle "Stand-alone" kommuniziert mit keinem anderen ADC bezüglich seiner Dienste, und daher bleiben alle Virtuellen Dienste im grünen Status und verbunden. Sie müssen sicherstellen, dass alle Virtuellen Dienste eindeutige IP-Adressen haben, sonst kommt es zu einem Konflikt in Ihrem Netzwerk.

Einstellungen

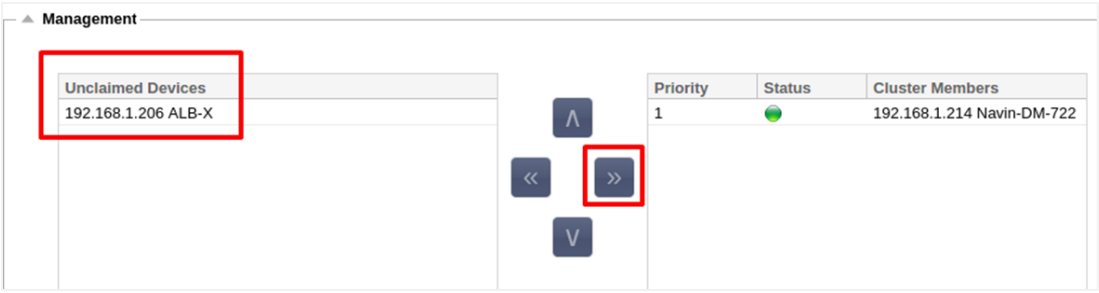


Im Bereich Einstellungen können Sie die Failover-Latenz in Millisekunden einstellen, also die Zeit, die ein passives ADC wartet, bevor es die virtuellen Dienste übernimmt, nachdem das aktive ADC ausgefallen ist.

Wir empfehlen, diesen Wert auf 10000ms oder 10 Sekunden einzustellen, aber Sie können diesen Wert je nach Netzwerk und Anforderungen verringern oder erhöhen. Akzeptable Werte liegen zwischen 1500ms und 20000ms. Wenn Sie bei einer niedrigeren Latenz Instabilität im Cluster feststellen, sollten Sie diesen Wert erhöhen.

Verwaltung

In diesem Bereich können Sie Clustermitglieder hinzufügen und entfernen und gleichzeitig die Priorität eines ADC im Cluster ändern. Der Abschnitt besteht aus zwei Bereichen und einer Reihe von Pfeiltasten dazwischen. Der Bereich auf der linken Seite sind die nicht beanspruchten Geräte, während der Bereich ganz rechts der Cluster selbst ist.

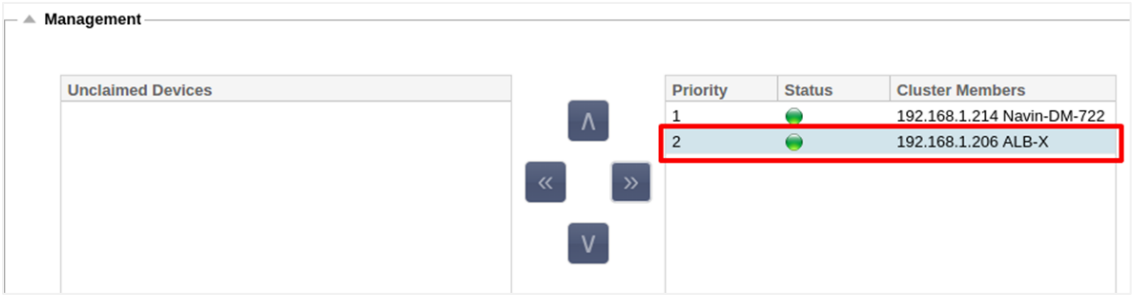


Hinzufügen eines ADCs zum Cluster

- Bevor Sie den ADC zum Cluster hinzufügen, müssen Sie sicherstellen, dass alle ADC-Appliances mit einem eindeutigen Namenssatz im Bereich System > Netzwerk versehen wurden.
- Sie sollten den ADC als Priorität 1 mit Status grün und seinem Namen unter der Spalte Cluster-Mitglieder im Verwaltungsbereich sehen. Dieser ADC ist die standardmäßige primäre Appliance.

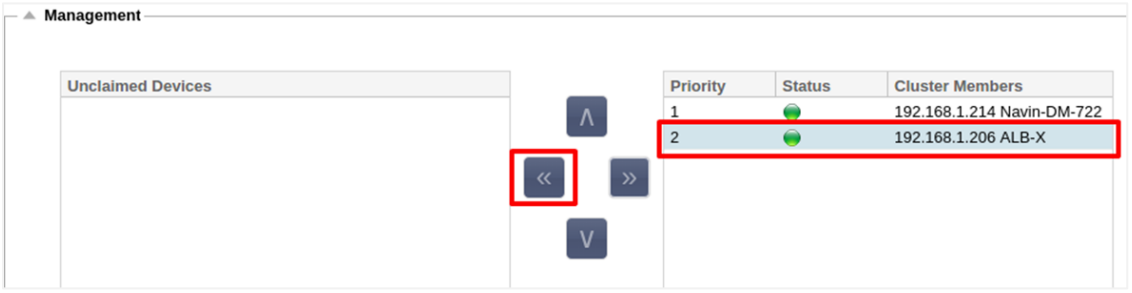
- Alle anderen verfügbaren ADCs werden im Fenster Nicht beanspruchte Geräte im Verwaltungsbereich angezeigt. Ein nicht beanspruchtes Gerät ist der ADC, der in der Cluster-Rolle zugewiesen wurde, aber keine virtuellen Dienste konfiguriert hat.
- Markieren Sie den ADC aus dem Fenster Nicht beanspruchte Geräte und klicken Sie auf die rechte Pfeiltaste.
- Sie sehen nun die folgende Meldung:

- Klicken Sie auf OK, um den ADC in den Cluster zu befördern.
- Ihr ADC sollte nun als Priorität 2 in der Liste der Clustermitglieder angezeigt werden.



Entfernen eines Clustermitglieds

- Markieren Sie das Cluster-Mitglied, das Sie aus dem Cluster entfernen möchten.
- Klicken Sie auf die linke Pfeiltaste.

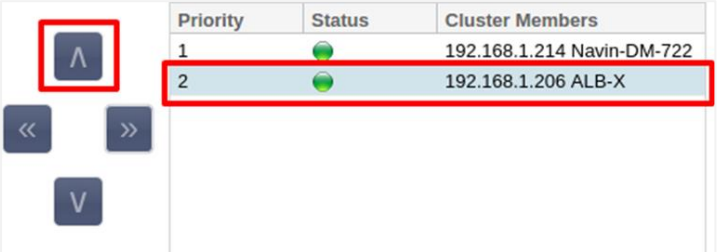


- Sie erhalten eine Bestätigungsaufforderung.
- Klicken Sie zur Bestätigung auf OK.
- Ihr ADC wird entfernt und auf der Seite "Nicht beanspruchte Geräte" angezeigt.

Ändern der Priorität eines ADCs

Es kann vorkommen, dass Sie die Priorität eines ADCs innerhalb der Mitgliederliste ändern möchten.

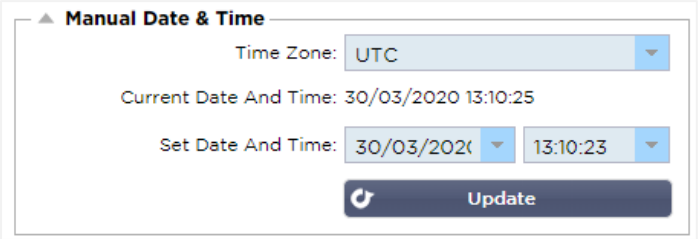
- Der ADC am Anfang der Liste der Cluster-Mitglieder erhält die Priorität 1 und ist der aktive ADC für alle virtuellen Dienste
- Der ADC, der an zweiter Stelle in der Liste steht, erhält Priorität 2 und ist der passive ADC für alle virtuellen Dienste
- Um zu ändern, welcher ADC aktiv ist, markieren Sie einfach den ADC und klicken Sie auf den Pfeil nach oben, bis er an der Spitze der Liste steht



Datum und Uhrzeit

Der Bereich Datum und Uhrzeit ermöglicht die Einstellung der Datums-/Zeitmerkmale des ADC, einschließlich der Zeitzone, in der sich das ADC befindet. Zusammen mit der Zeitzone spielen das Datum und die Uhrzeit eine wichtige Rolle bei den kryptografischen Prozessen im Zusammenhang mit der SSL-Verschlüsselung.

Manuelles Datum und Uhrzeit



Zeitzone

Der Wert, den Sie in diesem Feld einstellen, repräsentiert die Zeitzone, in der sich das ADC befindet.

- Klicken Sie auf das Dropdown-Feld für die Zeitzone und beginnen Sie, Ihren Standort einzugeben. Zum Beispiel London
- Wenn Sie mit der Eingabe beginnen, zeigt der ADC automatisch Stellen an, die den Buchstaben L enthalten.
- Fahren Sie mit der Eingabe von "Lon" fort und so weiter - die aufgelisteten Orte werden auf diejenigen eingegrenzt, die "Lon" enthalten. ’
- Wenn Sie sich z. B. in London befinden, dann wählen Sie Europa/London, um Ihren Standort einzustellen

Wenn das Datum und die Uhrzeit nach der obigen Änderung immer noch falsch sind, ändern Sie das Datum bitte manuell

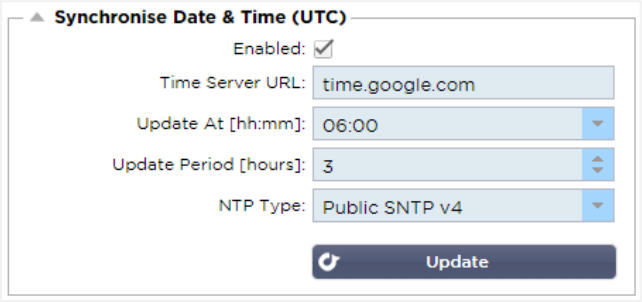
Datum und Uhrzeit einstellen

Diese Einstellung stellt das aktuelle Datum und die Uhrzeit dar.

- Wählen Sie das richtige Datum aus dem ersten Einblendmenü oder,
  alternativ können Sie das Datum im folgenden Format eingeben DD/MM/YYYY
- Geben Sie die Zeit im folgenden Format hh: mm: ss ein, z. B. 06:00:10 für 6 Uhr morgens und 10 Sekunden.
- Wenn Sie sie korrekt eingegeben haben, klicken Sie bitte auf Aktualisieren, um sie zu übernehmen.
- Sie sollten dann das neue Datum und die Uhrzeit in fetten Buchstaben sehen.

Datum und Uhrzeit synchronisieren (UTC)

Sie können NTP-Server verwenden, um Ihr Datum und Ihre Uhrzeit genau zu synchronisieren. Die NTP-Server befinden sich weltweit, und Sie können auch einen eigenen internen NTP-Server haben, wenn Ihre Infrastruktur Einschränkungen für den externen Zugriff hat.



Zeitserver-URL

Geben Sie eine gültige IP-Adresse oder einen vollständig qualifizierten Domänennamen (FQDN) für den NTP-Server ein. Wenn es sich bei dem Server um einen global aufgestellten Server im Internet handelt, empfehlen wir die Verwendung eines FQDN.

Aktualisierung um [hh:mm]

Wählen Sie die geplante Zeit, zu der sich der ADC mit dem NTP-Server synchronisieren soll.

Aktualisierungszeitraum [Stunden]:

Wählen Sie, wie oft die Synchronisierung erfolgen soll.

NTP Typ:

- Public SNTP V4 - Dies ist die aktuelle und bevorzugte Methode bei der Synchronisierung mit einem NTP-Server. **RFC 5905**
- NTP v1 Over TCP - Legacy-NTP-Version über TCP. **RFC 1059**
- NTP v1 Over UDP - Legacy NTP-Version über UDP. **RFC 1059**

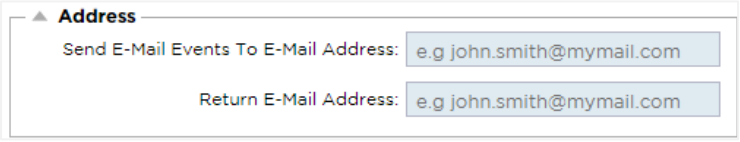
Hinweis: Bitte beachten Sie, dass die Synchronisierung nur in UTC erfolgt. Wenn Sie eine lokale Zeit einstellen möchten, kann dies nur manuell erfolgen. Diese Einschränkung wird in späteren Versionen geändert, um die Möglichkeit zu bieten, eine Zeitzone auszuwählen.

E-Mail-Ereignisse

Der ADC ist ein kritisches Gerät, und wie jedes wichtige System ist er mit der Fähigkeit ausgestattet, die Systemadministration über alle Probleme zu informieren, die möglicherweise Aufmerksamkeit erfordern.

Auf der Seite System > E-Mail-Ereignisse können Sie eine E-Mail-Serververbindung konfigurieren und Benachrichtigungen an Systemadministratoren senden. Die Seite ist in die folgenden Abschnitte unterteilt.

Adresse



Senden an E-Mail-Ereignisse an E-Mail-Adressen

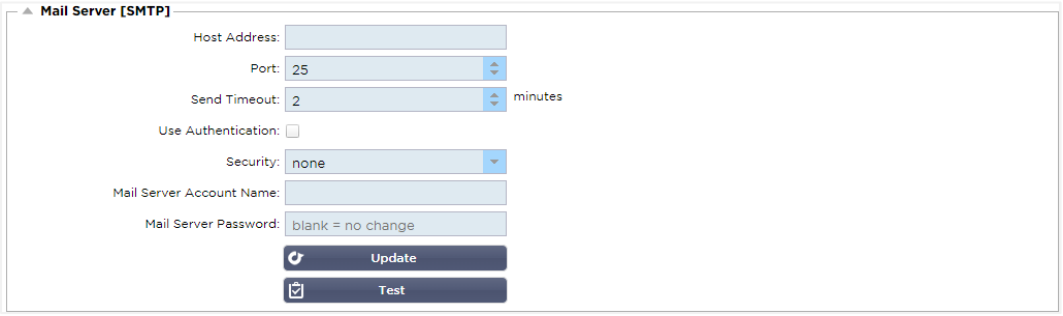
Fügen Sie eine gültige E-Mail-Adresse hinzu, an die die Alarme, Benachrichtigungen und Ereignisse gesendet werden sollen. Beispiel support@domain.com. Sie können auch mehrere E-Mail-Adressen mit einem Komma-Trennzeichen hinzufügen.

Rücksende-E-Mail-Adresse:

Fügen Sie eine E-Mail-Adresse ein, die im Posteingang erscheinen soll. Beispiel adc@domain.com.

Mail-Server (SMTP)

In diesem Abschnitt müssen Sie die Details des SMTP-Servers hinzufügen, der für den Versand der E-Mails verwendet werden soll. Bitte stellen Sie sicher, dass die E-Mail-Adresse, die Sie zum Senden verwenden, dazu berechtigt ist.



Host-Adresse

Geben Sie die IP-Adresse Ihres SMTP-Servers ein.

Hafen

Geben Sie den Port Ihres SMTP-Servers ein. Der Standard-Port für SMTP ist 25 oder 587, wenn Sie SSL verwenden.

Zeitüberschreitung senden

Fügen Sie eine SMTP-Zeitüberschreitung ein. Der Standardwert ist auf 2 Minuten eingestellt.

Authentifizierung verwenden

Aktivieren Sie das Kontrollkästchen, wenn Ihr SMTP-Server eine Authentifizierung erfordert.

Sicherheit

- Keine
- Die Standardeinstellung ist keine.
- SSL - Verwenden Sie diese Einstellung, wenn Ihr SMTP-Server eine Secure Sockets Layer-Authentifizierung erfordert.
- TLS - Verwenden Sie diese Einstellung, wenn Ihr SMTP-Server eine Transport Layer Security-Authentifizierung erfordert.

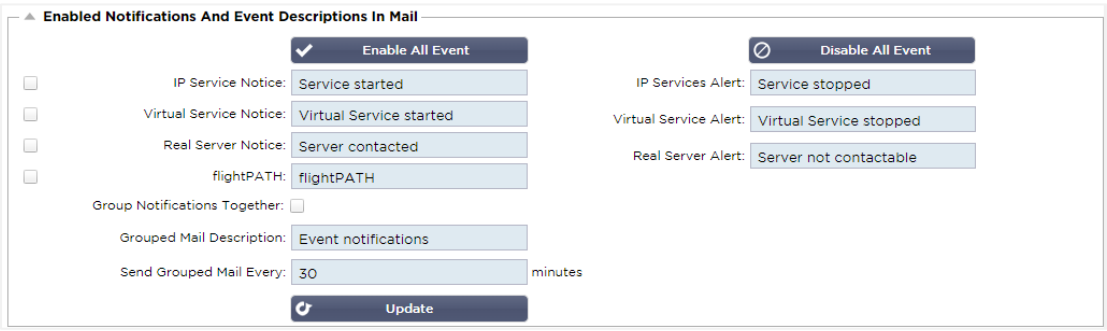
Hauptserver Kontoname

Geben Sie den für die Authentifizierung erforderlichen Benutzernamen ein.

Mail-Server-Passwort

Geben Sie das für die Authentifizierung erforderliche Passwort ein.

Benachrichtigungen und Alarme



Es gibt verschiedene Arten von Ereignisbenachrichtigungen, die das ADC an Personen sendet, die für deren Empfang konfiguriert sind. Sie können die Benachrichtigungen und Alarme, die versendet werden sollen, ankreuzen und aktivieren. Benachrichtigungen treten auf, wenn Real Servers kontaktiert oder Kanäle gestartet werden. Warnungen treten auf, wenn Real Server nicht kontaktiert werden können oder Kanäle nicht mehr funktionieren.

IP-Dienst

Die IP-Service-Benachrichtigung informiert Sie, wenn eine virtuelle IP-Adresse online ist oder nicht mehr funktioniert. Diese Aktion wird für alle Virtuellen Dienste ausgeführt, die zum VIP gehören.

Virtueller Dienst

Informiert den Empfänger, dass ein virtueller Dienst online ist oder nicht mehr funktioniert.

Real Server

Wenn ein Real-Server und ein Port verbunden oder nicht erreichbar sind, sendet der ADC eine Benachrichtigung an den Real-Server.

flightPATH

Diese Benachrichtigung ist eine E-Mail, die versendet wird, wenn eine Bedingung erfüllt ist und eine Aktion konfiguriert ist, die das ADC anweist, das Ereignis per E-Mail zu versenden.

Gruppen-Benachrichtigungen

Aktivieren Sie dieses Kontrollkästchen, um Benachrichtigungen zusammenzufassen. Wenn dieses Häkchen gesetzt ist, werden alle Benachrichtigungen und Alarme in einer E-Mail zusammengefasst.

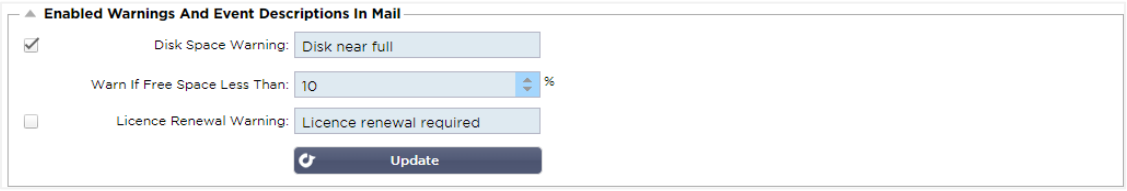
Gruppenmail Beschreibung

Geben Sie den relevanten Betreff für die Gruppenbenachrichtigungs-E-Mail an.

Gruppe Sendeintervall

Legen Sie fest, wie lange Sie warten möchten, bevor Sie eine Gruppenbenachrichtigungs-E-Mail senden. Die Mindestzeit beträgt 2 Minuten.

Warnungen



Es gibt zwei Arten von Warn-E-Mails, und beide sollten nicht ignoriert werden.

Speicherplatz

Stellen Sie den Prozentsatz des freien Speicherplatzes ein, vor dem die Warnung gesendet wird. Wenn dieser Wert erreicht ist, werden Sie per E-Mail benachrichtigt.

Ablauf der Lizenz

Mit dieser Einstellung können Sie die Warn-E-Mail zum Ablauf der Lizenz aktivieren oder deaktivieren, die an den Systemadministrator gesendet wird. Wenn diese erreicht ist, werden Sie per E-Mail benachrichtigt.

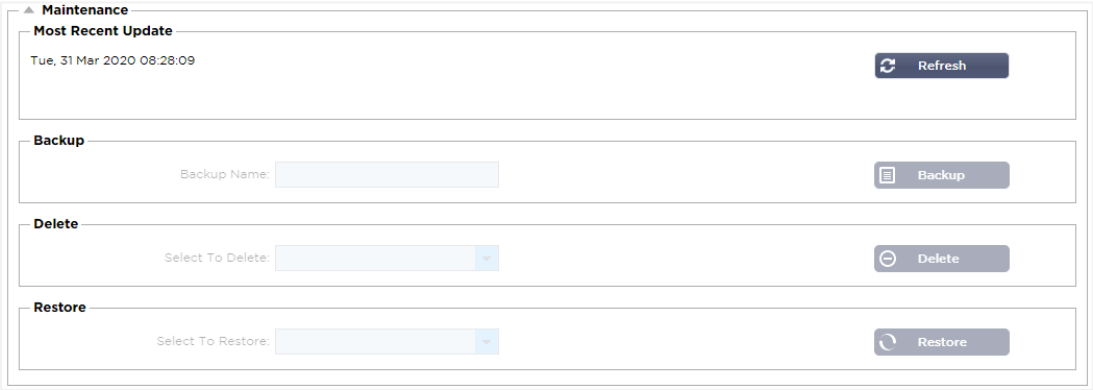
System-Historie

Im Bereich System gibt es die Option Systemverlauf, die die Lieferung von Verlaufsdaten für Elemente wie CPU, Speicher, Anfragen pro Sekunde und andere Funktionen ermöglicht. Sobald sie aktiviert ist, können Sie die Ergebnisse in grafischer Form über die Seite Ansicht > Verlauf anzeigen. Diese Seite ermöglicht es Ihnen auch, Ihre Verlaufsdateien auf dem lokalen ADC zu sichern oder wiederherzustellen.

Daten sammeln

- Um die Erfassung von Daten zu aktivieren, markieren Sie bitte das Kontrollkästchen.
- Stellen Sie als nächstes das Zeitintervall ein, in dem der ADC die Daten sammeln soll. Dieser Zeitwert kann zwischen 1-60 Sekunden liegen.

Wartung



Dieser Abschnitt ist ausgegraut, wenn Sie die historische Protokollierung aktiviert haben. Bitte deaktivieren Sie das Kontrollkästchen Aktiviert im Abschnitt Daten sammeln und klicken Sie auf Aktualisieren, um die Pflege der historischen Protokolle zu erlauben.

Sicherung

Geben Sie Ihrer Sicherung einen aussagekräftigen Namen. Klicken Sie auf Backup, um alle Dateien auf dem ADC zu sichern

Löschen

Wählen Sie eine Sicherungsdatei aus der Dropdown-Liste. Klicken Sie auf Löschen, um die Sicherungsdatei aus dem ADC zu entfernen

Wiederherstellen

Wählen Sie eine zuvor gespeicherte Sicherungsdatei. Klicken Sie auf Wiederherstellen, um die Daten aus dieser Sicherungsdatei aufzufüllen.

Lizenz

Der ADC ist für die Verwendung entweder mit einem der folgenden Modelle lizenziert, was von Ihren Kaufparametern und dem Kundentyp abhängt.

Lizenz-Typ	Beschreibung

Ewige	Sie, der Kunde, haben das Recht, das ADC und andere Software auf Dauer zu nutzen. Es schließt nicht aus, dass Sie Support erwerben müssen, um Unterstützung und Updates zu erhalten.
SaaS	SaaS oder Software-as-a-Service bedeutet, dass Sie die Software im Wesentlichen auf einer laufenden oder Pay-as-you-go-Basis mieten. Bei diesem Modell zahlen Sie eine jährliche Miete für die Software. Sie haben keine unbefristeten Rechte zur Nutzung der Software.
MSP	Managed Service Provider können den ADC als Service anbieten und die Lizenz auf einer Pro-VIP-Basis erwerben, die jährlich berechnet und bezahlt wird.

Lizenz Details

Jede Lizenz enthält spezifische Details, die für die Person oder Organisation, die sie erwirbt, relevant sind.

Lizenz-ID

Diese Lizenz-ID ist direkt mit der Maschinen-ID und anderen Details verbunden, die für Ihren Kauf und ADC spezifisch sind. Diese Informationen sind wichtig und werden benötigt, wenn Sie Updates und andere Artikel aus dem App Store abrufen möchten.

Geräte-ID

Die Maschinen-ID wird anhand der eth0-IP-Adresse einer virtuellen ADC Appliance und der MAC-ID eines hardwarebasierten ADCs generiert. Wenn Sie die IP-Adresse einer virtuellen ADC Appliance ändern, ist die Lizenz nicht mehr gültig. Sie müssen sich an den Support wenden, um Hilfe zu erhalten. Wir empfehlen, dass Ihre virtuelle(n) ADC Appliance(s) feste IP-Adressen haben mit der Anweisung, diese nicht zu ändern. Technischer Support ist verfügbar, indem Sie ein Ticket unter HTTPs://edgenexus.io erstellen.

Hinweis: Sie dürfen die IP-Adresse oder die MAC-ID Ihrer ADC-Appliances nicht ändern. Wenn Sie sich in einem virtualisierten Framework befinden, dann legen Sie bitte die MAC-ID und IP-Adresse fest.

Ausgegeben an

Dieser Wert enthält den Namen des Käufers, der mit der Maschinen-ID des ADC verbunden ist.

Kontaktperson

Dieser Wert enthält die zu kontaktierende Kontaktperson in der Firma des Kunden, die mit der Maschinen-ID verbunden ist

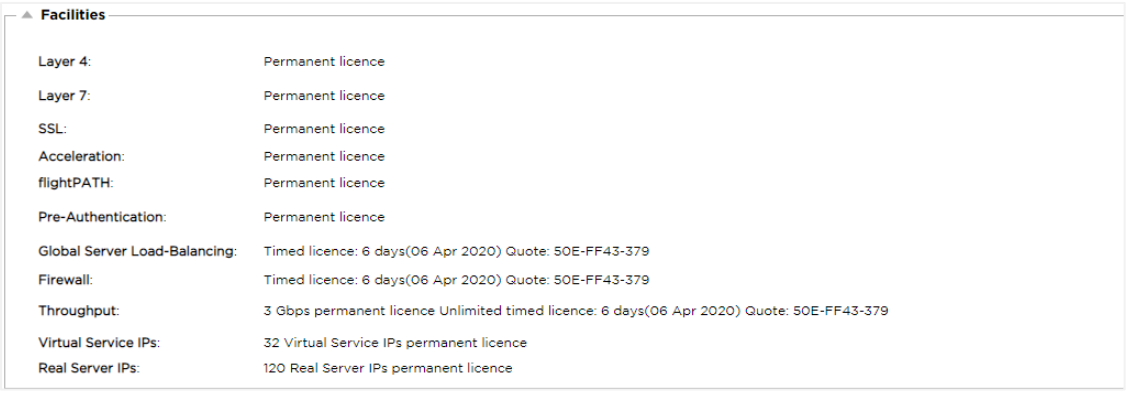
Datumsprobleme

Das Datum, an dem die Lizenz ausgestellt wurde

Name

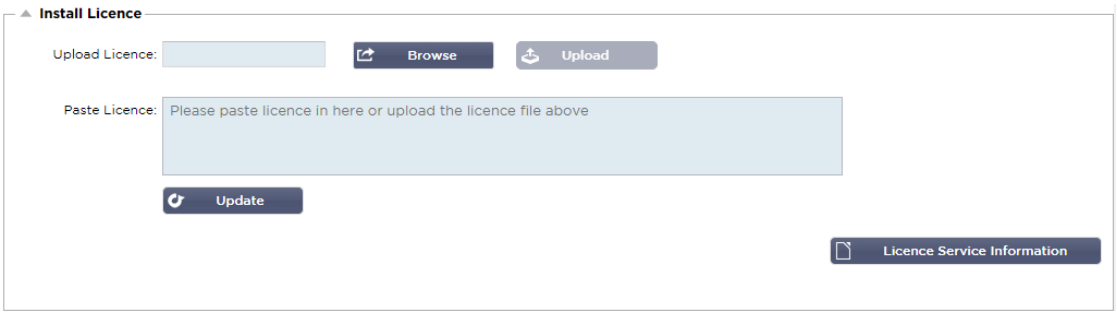
Dieser Wert zeigt den beschreibenden Namen für die ADC Appliance, den Sie angegeben haben.

Einrichtungen



Im Bereich Einrichtungen erhalten Sie Informationen darüber, welche Funktionen innerhalb des ADC für die Nutzung lizenziert wurden und welche Gültigkeit die Lizenz hat. Außerdem werden der Durchsatz, der für den ADC lizenziert wurde, und die Anzahl der Real Server angezeigt. Diese Informationen sind abhängig von der Lizenz, die Sie erworben haben.

Lizenzen installieren



- Das Installieren einer neuen Lizenz ist sehr einfach. Wenn Sie Ihre neue oder Ersatzlizenz von Edgenexus erhalten, wird sie in Form einer Textdatei gesendet. Sie können die Datei öffnen und dann den Inhalt kopieren und in das Feld "Lizenz einfügen" einfügen.
- Sie können es auch in den ADC hochladen, wenn Kopieren/Einfügen für Sie keine Option ist.
- Sobald Sie dies getan haben, klicken Sie bitte auf die Schaltfläche Aktualisieren
- Die Lizenz ist nun installiert.

Lizenz-Service-Informationen

Wenn Sie auf die Schaltfläche Lizenz-Service-Informationen klicken, werden alle Informationen zur Lizenz angezeigt. Diese Funktion kann dazu verwendet werden, die Details an das Support-Personal zu senden.

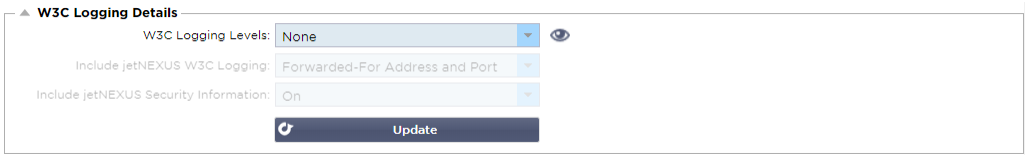
Loggen

Auf der Seite System > Protokollierung können Sie die W3C-Protokollierungsstufen einstellen und den Remote-Server angeben, auf den die Protokolle automatisch exportiert werden sollen. Die Seite ist in die vier folgenden Abschnitte unterteilt.

W3C-Protokollierungsdetails

Das Aktivieren der W3C-Protokollierung bewirkt, dass das ADC mit der Aufzeichnung einer W3C-kompatiblen Protokolldatei beginnt. Ein W3C-Protokoll ist ein Zugriffsprotokoll für Webserver, in dem Textdateien erzeugt werden, die Daten über jede Zugriffsanfrage enthalten, einschließlich der Quell-IP-Adresse (Internet Protocol), der HTTP-Version, des Browsertyps, der Verweisseite und des Zeitstempels. Das Format wurde vom World Wide Web Consortium (W3C) entwickelt, einer Organisation, die Standards für die Weiterentwicklung des Webs fördert. Die Datei ist im ASCII-Textformat mit durch Leerzeichen

getrennten Spalten. Die Datei enthält Kommentarzeilen, die mit dem Zeichen # beginnen. Eine dieser Kommentarzeilen ist eine Zeile, die die Felder angibt (mit Spaltennamen), damit die Daten ausgewertet werden können. Es gibt separate Dateien für HTTP- und FTP-Protokolle.



W3C-Protokollierungsebenen

Es sind verschiedene Protokollierungsebenen verfügbar, und je nach Diensttyp variieren die bereitgestellten Daten.

Die folgende Tabelle beschreibt die Protokollierungsstufen für W3C-HTTP.

Wert	Beschreibung
Keine	Die W3C-Protokollierung ist ausgeschaltet.
Kurz	Die vorhandenen Felder sind: #Felder: 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).
Vollständig	Dies ist ein besser prozessorkompatibles Format mit separaten Datums- und Zeitfeldern. Informationen zur Bedeutung der Felder finden Sie in der folgenden Zusammenfassung der Felder. Die vorhandenen Felder sind: #Felder: Datum Zeit 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).
Website	Dieses Format ist dem Format "Voll" sehr ähnlich, hat aber ein zusätzliches Feld. Lesen Sie die Zusammenfassung der Felder unten, um zu erfahren, was die Felder bedeuten. Die vorhandenen Felder sind: #Felder: 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).
Diagnostik	Dieses Format ist mit allen möglichen Informationen gefüllt, die für Entwicklungs- und Support-Mitarbeiter relevant sind. In der Zusammenfassung der Felder unten finden Sie Informationen über die Bedeutung der Felder. Die vorhandenen Felder sind: #Felder: date time c-ip c-port cs-username s-ip s-port x-xff x-xffcustom cs-host x-r-ip x-r-port cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent) referer x-c-version x-r-version cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x-round-trip-time x-trip-times(new,rcon,rqf,rql,tqf,tql,rsf,rsl,tsf,tsl,dis,log) x-closed-by x- compress-action x-sc(Content-Type) x-cache-action X-finish

Die folgende Tabelle beschreibt die Protokollierungsstufen für W3C FTP.

Wert	Beschreibung
Kurz	#Felder: Datum Zeit 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
Vollständig	#Felder: Datum Zeit 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
Diagnostik	#Felder: Datum Zeit 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-Protokollierung einbeziehen

Mit dieser Option können Sie einstellen, welche ADC-Informationen in die W3C-Protokolle aufgenommen werden sollen.

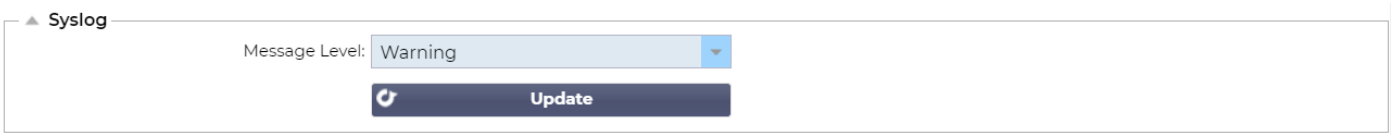
Wert	Beschreibung
Netzwerkadresse und Port des Clients	Der hier angezeigte Wert zeigt die tatsächliche Client-IP-Adresse zusammen mit dem Port an.
Netzwerkadresse des Clients	Mit dieser Option wird die tatsächliche Client-IP-Adresse einbezogen und nur angezeigt.
Weitergeleitet-für Adresse und Port	Diese Option zeigt die im XFF-Header enthaltenen Details an, einschließlich der Adresse und des Ports.
Weitergeleitet-für-Adresse	Mit dieser Option werden nur die im XFF-Header enthaltenen Details angezeigt, einschließlich der Adresse.

Sicherheitsinformationen einbeziehen

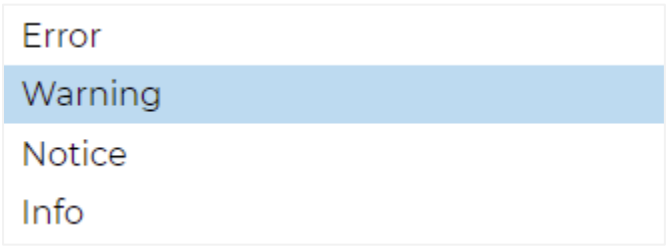
Dieses Menü besteht aus zwei Optionen:

Wert	Beschreibung
Auf	Diese Einstellung ist global. Wenn sie auf Ein gesetzt ist, wird der Benutzername an das W3C-Protokoll angehängt, wenn ein beliebiger virtueller Dienst die Authentifizierung verwendet und die W3C-Protokollierung aktiviert ist.
Aus	Dadurch wird die Möglichkeit, den Benutzernamen im W3C-Protokoll zu protokollieren, auf globaler Ebene ausgeschaltet.

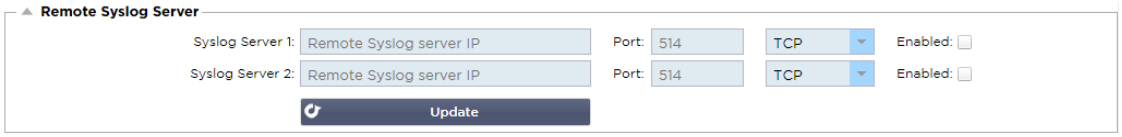
Syslog-Server



In diesem Abschnitt können Sie die Stufe der Nachrichtenprotokollierung einstellen, die auf dem SYSLOG-Server durchgeführt wird. Die verfügbaren Optionen sind wie folgt.



Entfernter Syslog-Server

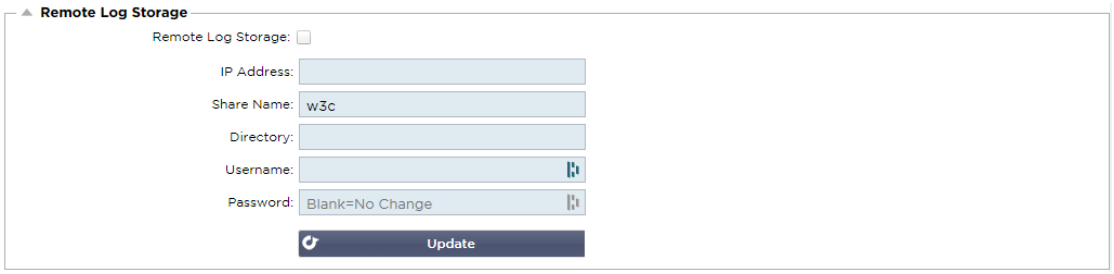


In diesem Abschnitt können Sie zwei externe Syslog-Server konfigurieren, um alle Systemprotokolle zu senden.

- Fügen Sie die IP-Adresse Ihres Syslog-Servers hinzu

- Fügen Sie den Port hinzu
- Wählen Sie, ob Sie TCP oder UDP verwenden möchten
- Aktivieren Sie das Kontrollkästchen Aktiviert, um mit der Protokollierung zu beginnen
- Klicken Sie auf Aktualisieren

Entfernte Log-Speicherung



Alle W3C-Protokolle werden stündlich in komprimierter Form auf dem ADC gespeichert. Die ältesten Dateien werden gelöscht, wenn 30 % des Speicherplatzes übrig sind. Sollten Sie diese zur sicheren Aufbewahrung auf einen entfernten Server exportieren wollen, können Sie dies über eine SMB-Freigabe konfigurieren. Bitte beachten Sie, dass das W3C-Protokoll erst dann an den entfernten Speicherort übertragen wird, wenn die Datei abgeschlossen und komprimiert ist. Da die Protokolle jede Stunde geschrieben werden, kann dies bei einer Appliance mit virtueller Maschine bis zu zwei Stunden und bei einer Hardware-Appliance bis zu fünf Stunden dauern.

Wir werden in zukünftigen Versionen eine Test-Schaltfläche einbauen, um Ihnen ein Feedback zu geben, ob Ihre Einstellungen korrekt sind.

Spalte1	Spalte2
Entfernte Log-Speicherung	Aktivieren Sie das Kontrollkästchen, um die entfernte Protokollspeicherung zu aktivieren
IP-Adresse	Geben Sie die IP-Adresse Ihres SMB-Servers an. Diese sollte in gepunkteter Dezimalschreibweise angegeben werden. Beispiel: 10.1.1.23
Aktie Name	Geben Sie den Freigabenamen auf dem SMB-Server an. Beispiel: w3c.
Verzeichnis	Geben Sie das Verzeichnis auf dem SMB-Server an. Beispiel: /log.
Benutzername	Geben Sie den Benutzernamen für die SMB-Freigabe an.
Passwort	Geben Sie das Passwort für die SMB-Freigabe an

Feld Zusammenfassung

Zustand	Beschreibung
Datum	Nicht lokalisiert = immer JJJJ-MM-TT (GMT/UTC)
Zeit	Nicht lokalisiert = HH:MM:SS oder HH:MM:SS.ZZZ (GMT/UTC) * Hinweis - leider hat dies zwei Formate (Site
	hat keine .ZZZ-Millisekunden)
x-mil	Nur Site-Format = Millisekunde des Zeitstempels
c-ip	Client-IP so gut wie möglich aus dem Netzwerk oder dem X-Forwarded-For-Header ableitbar
c-port	Client-Port, wie er am besten aus dem Netzwerk oder dem X-Forwarded-For-Header abgeleitet werden kann

cs-Benutzername	Abfragefeld für den Benutzernamen des Clients
s-ip	ALBs lauschender Port
s-port	ALBs hörender VIP
x-xff	Wert des X-Forwarded-For-Headers
x-xffcustom	Wert des konfigurierten Anfrage-Headers vom Typ X-Forwarded-For
cs-host	Hostname in der Anfrage
x-r-ip	IP-Adresse des verwendeten Real-Servers
x-r-port	Verwendeter Port des Real-Servers
cs-Methode	HTTP-Anforderungsmethode * außer Brief-Format
Methode	* Nur das Kurzformat verwendet diesen Namen für cs-method
cs-uri-stem	Pfad der angeforderten Ressource * außer Brief-Format
cs-uri-abfrage	Abfrage nach der angeforderten Ressource * außer Kurzformat
uri	* Das Kurzformat protokolliert einen kombinierten Pfad und Abfrage-String
sc-status	HTTP-Antwort-Code
cs(Benutzer-Agent)	User-Agent-String des Browsers (wie vom Client gesendet)
Referent	Verweisende Seite (wie vom Client gesendet)
x-c-version	Anfrage des Clients HTTP-Version
x-r-version	Content-Server's Antwort HTTP-Version
cs-bytes	Bytes vom Client, in der Anfrage
sr-Bytes	An den Real-Server weitergeleitete Bytes, in der Anfrage
rs-bytes	Bytes von Real Server, in der Antwort
sc-bytes	An den Client gesendete Bytes, in der Antwort
x-prozentig	Komprimierungsprozentsatz * = 100 * (1 - Ausgabe / Eingabe) einschließlich Header
Zeit genommen	Wie lange der Real-Server in Sekunden gebraucht hat
x-trip-times neu pcon	Millisekunde vom Verbinden bis zum Posten in der "Neulingsliste" Millisekunde vom Verbinden bis zum Stellen der Verbindung zum Real-Server
acon	Millisekunde vom Verbinden bis zum Beenden des Verbindungsaufbaus zum Real-Server
rcon	Millisekunde von connect bis zum Aufbau der Real-Server-Verbindung
rqf	Millisekunde vom Verbinden bis zum Empfang des ersten Bytes der Anfrage vom Client
rql	Millisekunde vom Verbinden bis zum Empfang des letzten Bytes der Anfrage vom Client
tqf	Millisekunde vom Verbinden bis zum Senden des ersten Bytes der Anfrage an den Real-Server
tql	Millisekunde vom Verbinden bis zum Senden des letzten Bytes der Anfrage an den Real-Server

rsf	Millisekunde vom Verbinden bis zum Empfang des ersten Bytes der Antwort vom Real-Server
rsl	Millisekunde von der Verbindung bis zum Empfang des letzten Bytes der Antwort vom Real-Server
tsf	Millisekunde vom Verbinden bis zum Senden des ersten Bytes der Antwort an den Client
tsl	Millisekunde von der Verbindung bis zum Senden des letzten Bytes der Antwort an den Client
dis	Millisekunde vom Verbinden bis zum Trennen der Verbindung (beide Seiten - die letzte, die die Verbindung trennt)
loggen	Millisekunde ab Verbindung zu diesem Protokolleintrag normalerweise gefolgt von (Lastausgleichsrichtlinie und Begründung)
x-round-trip-time	Wie lange ALB gebraucht hat in Sekunden
x-closed-by	Durch welche Aktion wurde die Verbindung geschlossen (oder offen gehalten)
x-compress-action	Wie die Komprimierung durchgeführt bzw. verhindert wurde
x-sc(Inhalts-Typ)	Inhalts-Typ der Antwort
x-cache-action	Wie die Zwischenspeicherung reagiert hat oder verhindert wurde
x-finish	Auslöser, der diese Protokollzeile verursacht hat

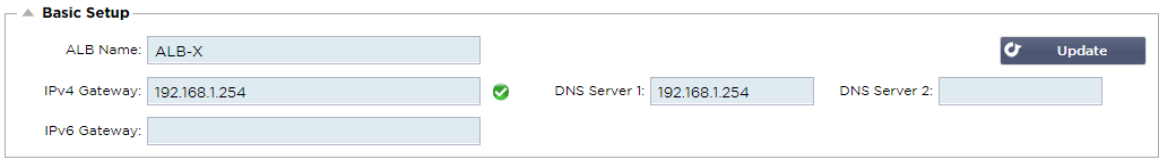
Log-Dateien löschen

Mit dieser Funktion können Sie die Protokolldateien aus dem ADC löschen. Sie können den Typ des Logs, den Sie löschen möchten, aus dem Dropdown-Menü auswählen und dann auf die Schaltfläche Löschen klicken.

Netzwerk

Der Abschnitt "Netzwerk" innerhalb der Bibliothek ermöglicht die Konfiguration der Netzwerkschnittstellen des ADC und deren Verhalten.

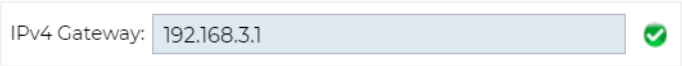
Grundlegende Einrichtung



ALB Name

Geben Sie einen Namen für Ihre ADC-Appliance an. Bitte beachten Sie, dass dieser nicht geändert werden kann, wenn es mehr als ein Mitglied im Cluster gibt. Lesen Sie dazu den Abschnitt über Clustering.

IPv4-Gateway



Geben Sie die IPv4-Gateway-Adresse an. Diese Adresse muss sich im gleichen Subnetz befinden wie ein vorhandener Adapter. Wenn Sie ein falsches Gateway hinzufügen, sehen Sie ein weißes Kreuz in einem roten Kreis. Wenn Sie ein korrektes Gateway hinzufügen, sehen Sie unten auf der Seite ein grünes Erfolgsbanner und ein weißes Häkchen in einem grünen Kreis neben der IP-Adresse.

IPv6-Gateway

Geben Sie die IPv6-Gateway-Adresse an. Diese Adresse muss sich im gleichen Subnetz befinden wie ein vorhandener Adapter. Wenn Sie ein falsches Gateway hinzufügen, sehen Sie ein weißes Kreuz in einem roten Kreis. Wenn Sie ein korrektes Gateway hinzufügen, sehen Sie unten auf der Seite ein grünes Erfolgsbanner und ein weißes Häkchen in einem grünen Kreis neben der IP-Adresse.

DNS-Server 1 & DNS-Server 2

Geben Sie die IPv4-Adresse Ihres ersten und zweiten (optionalen) DNS-Servers ein.

Adapter Details

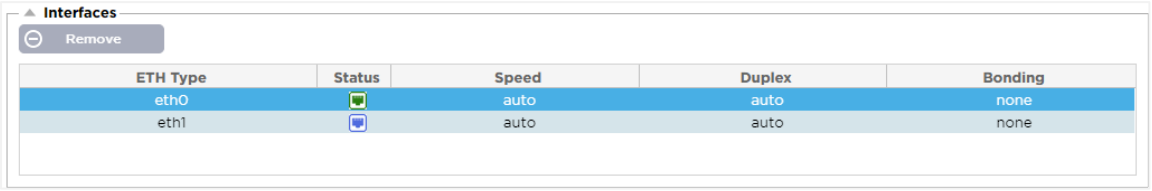
Dieser Abschnitt des Bedienfelds "Netzwerk" zeigt die Netzwerkschnittstellen, die in Ihrer ADC-Appliance installiert sind. Sie können nach Bedarf Adapter hinzufügen und entfernen.

Säule	Beschreibung
Adapter	In dieser Spalte werden die auf Ihrer Appliance installierten physikalischen Adapter angezeigt. Wählen Sie einen Adapter aus der Liste der verfügbaren Adapter aus, indem Sie darauf klicken - ein Doppelklick versetzt die Listenzeile in den Bearbeitungsmodus.
VLAN	Doppelklicken Sie, um die VLAN-ID für den Adapter hinzuzufügen. Ein VLAN ist ein virtuelles lokales Netzwerk, das eine eigene Broadcast-Domäne bildet. Ein VLAN hat die gleichen Attribute wie ein physisches LAN, aber es ermöglicht eine einfachere Gruppierung von Endstationen, wenn diese nicht am gleichen Netzwerk-Switch sind
IP-Adresse	Doppelklicken Sie, um die zur Adapterschnittstelle gehörende IP-Adresse hinzuzufügen. Sie können der gleichen Schnittstelle mehrere IP-Adressen hinzufügen. Dies sollte eine IPv4-32-Bit-Zahl in vierfach gepunkteter Dezimalschreibweise sein. Beispiel 192.168.101.2
Subnetz-Maske	Doppelklicken Sie, um die der Adapterschnittstelle zugewiesene Subnetzmaske hinzuzufügen. Dies sollte eine IPv4-32-Bit-Zahl in vierfach gepunkteter Dezimalschreibweise sein. Beispiel 255.255.255.0
Gateway	Fügen Sie ein Gateway für die Schnittstelle hinzu. Wenn dies hinzugefügt wird, richtet das ADC eine einfache Richtlinie ein, die es erlaubt, dass Verbindungen, die von dieser Schnittstelle initiiert werden, über diese Schnittstelle an den angegebenen Gateway-Router zurückgegeben werden. Auf diese Weise kann das ADC in komplexeren Netzwerkumgebungen installiert werden, ohne dass eine komplexe richtlinienbasierte Weiterleitung manuell konfiguriert werden muss.

Beschreibung	Doppelklicken Sie, um eine Beschreibung für Ihren Adapter hinzuzufügen. Beispiel Öffentliche Schnittstelle. Hinweis: Der ADC benennt automatisch die erste Schnittstelle Grüne Seite, die zweite Schnittstelle Rote Seite und die dritte Schnittstelle Seite 3 usw. Sie können diese Namenskonventionen gerne nach Ihren Vorstellungen ändern.
Web-Konsole	Doppelklicken Sie auf die Spalte und aktivieren Sie das Kontrollkästchen, um die Schnittstelle als Verwaltungsadresse für die Web-Konsole der grafischen Benutzeroberfläche zuzuweisen. Bitte seien Sie sehr vorsichtig, wenn Sie die Schnittstelle ändern, auf der die Web-Konsole lauscht. Sie müssen das richtige Routing eingerichtet haben oder sich im gleichen Subnetz wie die neue Schnittstelle befinden, um die Web-Konsole nach der Änderung zu erreichen. Die einzige Möglichkeit, dies wieder zu ändern, ist der Zugriff auf die Befehlszeile und die Eingabe des Befehls set greenside. Dadurch werden alle Schnittstellen mit Ausnahme von eth0 gelöscht.

Schnittstellen

Der Abschnitt "Schnittstellen" im Bedienfeld "Netzwerk" ermöglicht die Konfiguration bestimmter Elemente, die die Netzwerkschnittstelle betreffen. Sie können eine Netzwerkschnittstelle auch aus der Auflistung entfernen, indem Sie auf die Schaltfläche Entfernen klicken. Wenn Sie eine virtuelle Appliance verwenden, sind die Schnittstellen, die Sie hier sehen, durch das zugrunde liegende Virtualisierungs-Framework begrenzt.



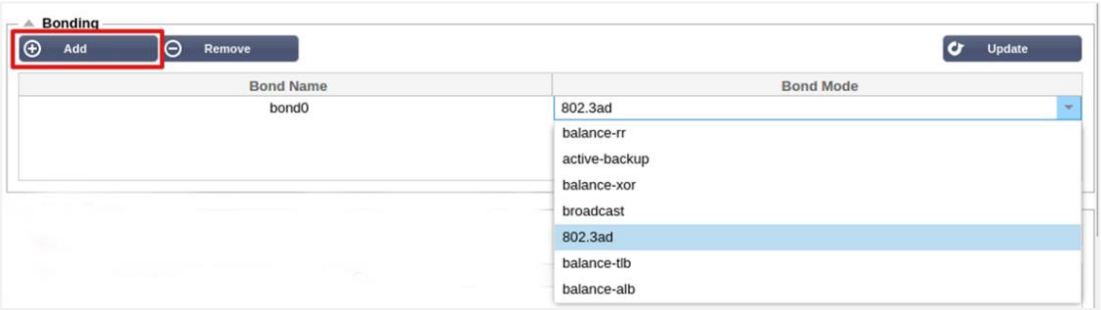
Säule	Beschreibung
ETH-Typ	Dieser Wert gibt die interne OS-Referenz auf die Netzwerkschnittstelle an. Dieses Feld kann nicht angepasst werden. Die Werte beginnen mit ETH0 und werden in Abhängigkeit von der Anzahl der Netzwerkschnittstellen fortgesetzt.
Status	Diese grafische Anzeige zeigt den aktuellen Status der Netzwerkschnittstelle an. Ein grüner Status zeigt an, dass die Schnittstelle verbunden und aktiv ist. Andere Statusanzeigen werden unten gezeigt. **Adapter UP** Adapter unten Adapter ausgesteckt Adapter fehlt
Geschwindigkeit	Standardmäßig ist dieser Wert so eingestellt, dass die Geschwindigkeit automatisch ausgehandelt wird. Sie können aber die Netzwerkgeschwindigkeit der Schnittstelle auf jeden im Dropdown-Menü verfügbaren Wert (10/100/1000/AUTO) ändern.
Duplex	Der Wert dieses Feldes ist anpassbar, und Sie können zwischen Auto (Standard), Voll-Duplex und Halb-Duplex wählen.
Binden	Sie können einen der Bindungstypen wählen, die Sie definiert haben. Weitere Einzelheiten finden Sie im Abschnitt über Bindung.

Binden

Für das Bonding von Netzwerkschnittstellen werden viele Namen verwendet: Port Trunking, Channel Bonding, Link Aggregation, NIC Teaming und andere. Bonding kombiniert oder aggregiert mehrere Netzwerkverbindungen zu einer einzigen Channel-Bonding-Schnittstelle. Durch Bonding können zwei oder mehr Netzwerkschnittstellen als eine agieren, den Durchsatz erhöhen und Redundanz oder Failover bieten.

Der ADC-Kernel verfügt über einen eingebauten Bonding-Treiber, um mehrere physische Netzwerkschnittstellen zu einer einzigen logischen Schnittstelle zusammenzufassen (z. B. Zusammenfassen von eth0 und eth1 zu bond0). Für jede gebondete Schnittstelle können Sie den Modus und die Link-Überwachungsoptionen definieren. Es gibt sieben verschiedene Modus-Optionen, die jeweils spezifische Lastausgleichs- und Fehlertoleranz-Eigenschaften bieten. Diese sind in der Abbildung unten dargestellt.

HINWEIS: BONDING KANN NUR FÜR HARDWAREBASIERTE ADC-APPLIANCES KONFIGURIERT WERDEN.

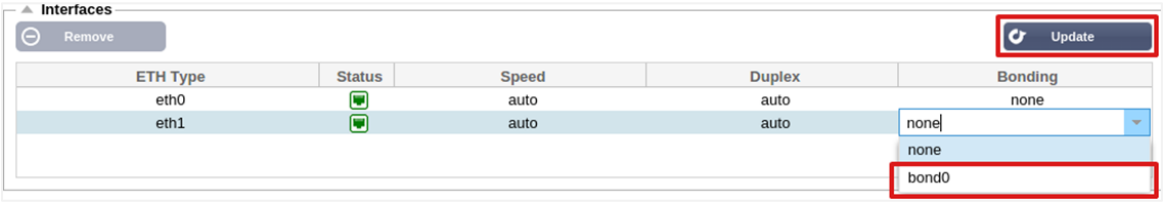


Erstellen eines Bonding-Profils

- Klicken Sie auf die Schaltfläche Hinzufügen, um eine neue Anleihe hinzuzufügen
- Geben Sie einen Namen für die Bonding-Konfiguration an
- Wählen Sie, welchen Bonding-Modus Sie verwenden möchten

Wählen Sie dann im Abschnitt Schnittstellen den gewünschten Bonding-Modus aus dem Dropdown-Feld Bindung für die Netzwerkschnittstelle aus.

Im folgenden Beispiel sind eth0, eth1 und eth2 jetzt Teil von bond0. Während Eth0 als Verwaltungsschnittstelle für sich alleine bleibt.



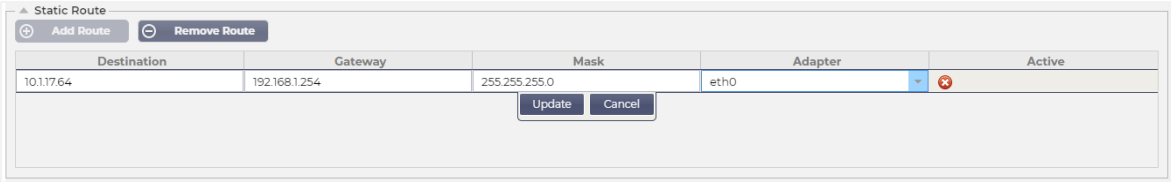
Bonding-Modi

Bonding-Modus	Beschreibung
balance-rr:	Pakete werden sequentiell über jede Schnittstelle einzeln gesendet/empfangen.
Aktiv-Backup:	In diesem Modus ist eine Schnittstelle aktiv und die zweite Schnittstelle befindet sich im Standby-Modus. Diese zweite Schnittstelle wird nur aktiv, wenn die aktive Verbindung auf der ersten Schnittstelle ausfällt.
balance-xor:	Sendet basierend auf der Quell-MAC-Adresse XOR'd mit der Ziel-MAC-Adresse. Diese Option wählt für jede Ziel-MAC-Adresse denselben Slave aus.
Sendung:	In diesem Modus werden alle Daten auf allen Slave-Schnittstellen übertragen.

802.3ad:	Erzeugt Aggregationsgruppen, die dieselben Geschwindigkeits- und Duplex-Einstellungen verwenden und alle Slaves im aktiven Aggregator gemäß der 802.3ad-Spezifikation nutzen.
balance-tlb:	Der Bonding-Modus Adaptiver Sende-Lastausgleich: Bietet Channel Bonding, das keine spezielle Switch-Unterstützung erfordert. Der ausgehende Verkehr wird entsprechend der aktuellen Last (berechnet im Verhältnis zur Geschwindigkeit) auf jedem Slave verteilt. Der aktuelle Slave empfängt den eingehenden Verkehr. Wenn der empfangende Slave ausfällt, übernimmt ein anderer Slave die MAC-Adresse des ausgefallenen empfangenden Slaves.
balance-alb:	Der Bonding-Modus Adaptiver Lastausgleich: umfasst ebenfalls balance-tlb plus Empfangslastausgleich (rlb) für IPV4-Verkehr und erfordert keine spezielle Switch-Unterstützung. Der Empfangslastausgleich wird durch ARP-Aushandlung erreicht. Der Bonding-Treiber fängt die vom lokalen System gesendeten ARP-Antworten auf ihrem Weg nach draußen ab und überschreibt die Quell-Hardwareadresse mit der eindeutigen Hardwareadresse eines der Slaves im Bond, so dass verschiedene Peers unterschiedliche Hardwareadressen für den Server verwenden.

Statische Route

Es wird Zeiten geben, in denen Sie statische Routen für bestimmte Subnetze innerhalb Ihres Netzwerks erstellen müssen. Der ADC bietet Ihnen die Möglichkeit, dies mit dem Modul "Statische Routen" zu tun.



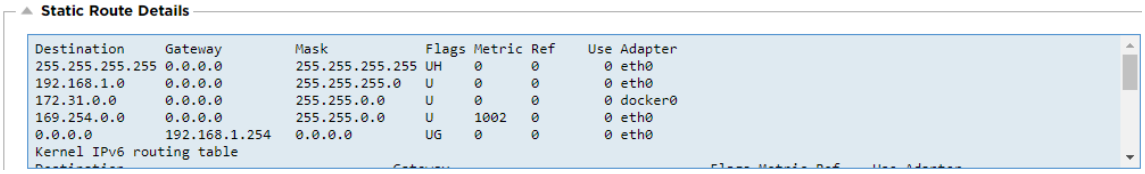
Hinzufügen einer statischen Route

- Klicken Sie auf die Schaltfläche Route hinzufügen
- Füllen Sie das Feld aus, indem Sie die Angaben in der Tabelle unten als Anleitung verwenden.
- Klicken Sie auf die Schaltfläche Aktualisieren, wenn Sie fertig sind.

Feld	**Beschreibung**
Ziel	Geben Sie die Ziel-Netzwerkadresse in dezimaler Punktschreibweise ein. Beispiel 123.123.123.5
Gateway	Geben Sie die IPv4-Adresse des Gateways in dezimaler Punktschreibweise ein. Beispiel 10.4.8.1
Maske	Geben Sie die Ziel-Subnetzmaske in dezimaler gepunkteter Notation ein. Beispiel 255.255.255.0
Adapter	Geben Sie den Adapter ein, über den das Gateway erreicht werden kann. Beispiel eth1.
Aktiv	Ein grünes Häkchen zeigt an, dass das Gateway erreicht werden kann. Ein rotes Kreuz zeigt an, dass das Gateway auf dieser Schnittstelle nicht erreicht werden kann. Bitte stellen Sie sicher, dass Sie eine Schnittstelle und eine IP-Adresse im gleichen Netzwerk wie das Gateway eingerichtet haben

Details zur statischen Route

Dieser Abschnitt enthält Informationen über alle auf dem ADC konfigurierten Routen.



Erweiterte Netzwerkeinstellungen

Was ist Nagle?

Der Nagle-Algorithmus verbessert die Effizienz von TCP/IP-Netzwerken, indem er die Anzahl der Pakete, die über das Netzwerk gesendet werden müssen, reduziert. Siehe **WIKIPEDIA-ARTIKEL ÜBER NAGLE**

Server Nagle

Aktivieren Sie dieses Kontrollkästchen, um die Einstellung "Server Nagle" zu aktivieren. Der Server Nagle ist ein Mittel zur Verbesserung der Effizienz von TCP/IP-Netzwerken, indem die Anzahl der Pakete, die über das Netzwerk gesendet werden müssen, reduziert wird. Diese Einstellung wird auf der Server-Seite der Transaktion angewendet. Bei den Server-Einstellungen ist Vorsicht geboten, da Nagle und verzögerte ACK die Leistung stark beeinträchtigen können.

Kunde Nagle

Aktivieren Sie das Kontrollkästchen, um die Einstellung Client Nagle zu aktivieren. Wie oben, aber angewendet auf die Client-Seite der Transaktion.

SNAT

SNAT steht für Source Network Address Translation, und verschiedene Hersteller haben leichte Variationen in der Implementierung von SNAT. Eine einfache Erklärung für den EdgeADC SNAT wäre wie folgt.

Unter normalen Umständen würden eingehende Anfragen an das VIP geleitet werden, das die Quell-IP der Anfrage sehen würde. Wenn also z. B. ein Browser-Endpunkt eine IP-Adresse von 81.71.61.51 hätte, wäre diese für das VIP sichtbar.

Wenn SNAT in Kraft ist, wird die ursprüngliche Quell-IP der Anfrage vor dem VIP verborgen, und stattdessen sieht es die IP-Adresse, wie sie in der SNAT-Regel angegeben ist. Somit kann SNAT im Layer-4- und Layer-7-Lastausgleichsmodus verwendet werden.

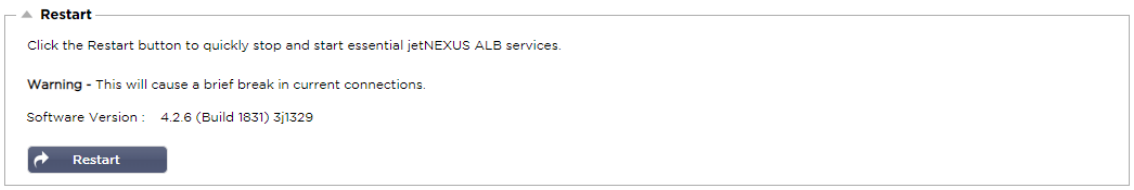
Feld	Beschreibung
Quelle IP	Die Quell-IP-Adresse ist optional und kann entweder eine Netzwerk-IP-Adresse (mit /mask) oder eine einfache IP-Adresse sein. Die Maske kann entweder eine Netzwerkmaske oder eine einfache Zahl sein, die die Anzahl der 1en auf der linken Seite der Netzwerkmaske angibt. So entspricht eine Maske von /24 der Adresse 255.255.255.0.
Ziel-IP	Die Ziel-IP-Adresse ist optional und kann entweder eine Netzwerk-IP-Adresse (mit /mask) oder eine einfache IP-Adresse sein. Die Maske kann entweder eine

	Netzwerkmaske oder eine einfache Zahl sein, die die Anzahl der 1en auf der linken Seite der Netzwerkmaske angibt. So entspricht eine Maske von /24 der Adresse 255.255.255.0.
Quelle Port	Der Quellport ist optional, er kann eine einzelne Zahl sein, in diesem Fall gibt er nur diesen Port an, oder er kann einen Doppelpunkt enthalten, der einen Bereich von Ports angibt. Beispiele: 80 oder 5900:5905.
Ziel-Hafen	Der Zielport ist optional, er kann eine einzelne Zahl sein, in diesem Fall gibt er nur diesen Port an, oder er kann einen Doppelpunkt enthalten, der einen Bereich von Ports angibt. Beispiele: 80 oder 5900:5905.
Protokoll	Sie können wählen, ob Sie SNAT für ein einzelnes Protokoll oder für alle Protokolle verwenden möchten. Wir empfehlen, spezifisch zu sein, um genauer zu sein.
SNAT zu IP	SNAT an IP ist eine obligatorische IP-Adresse oder ein Bereich von IP-Adressen. Beispiele: 10.0.0.1 oder 10.0.0.1-10.0.0.3.
SNAT an Port	Die Angabe SNAT to Port ist optional, sie kann eine einzelne Zahl sein, in diesem Fall gibt sie nur diesen Port an, oder sie kann einen Bindestrich enthalten, der einen Bereich von Ports angibt. Beispiele: 80 oder 5900-5905.
Anmerkungen	Verwenden Sie dies, um einen freundlichen Namen zu vergeben, um sich daran zu erinnern, warum die Regeln existieren. Dies ist auch nützlich für die Fehlersuche im Syslog.

Leistung

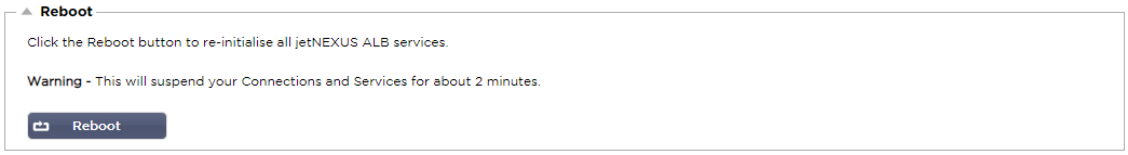
Mit dieser Funktion des ADC-Systems können Sie auch verschiedene strombezogene Aufgaben an Ihrem ADC durchführen.

Neustart



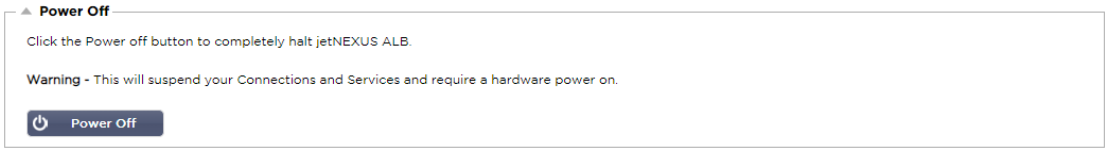
Diese Einstellung leitet einen globalen Neustart aller Dienste ein und unterbricht folglich alle derzeit aktiven Verbindungen. Alle Dienste werden nach einer kurzen Zeitspanne automatisch neu gestartet, aber der Zeitpunkt hängt davon ab, wie viele Dienste konfiguriert sind. Es wird ein Popup-Fenster angezeigt, das eine Bestätigung für den Neustart verlangt.

Neustart



Wenn Sie auf die Schaltfläche "Neustart" klicken, wird das ADC ausgeschaltet und automatisch in einen aktiven Zustand zurückversetzt. Es wird ein Popup-Fenster angezeigt, das eine Bestätigung für den Neustart verlangt.

Ausschalten



Wenn Sie auf die Schaltfläche Ausschalten klicken, wird der ADC ausgeschaltet. Wenn es sich um eine Hardware-Appliance handelt, benötigen Sie physischen Zugriff auf das Gerät, um es wieder einzuschalten. Es wird ein Popup-Fenster angezeigt, in dem Sie aufgefordert werden, die Abschaltaktion zu bestätigen.

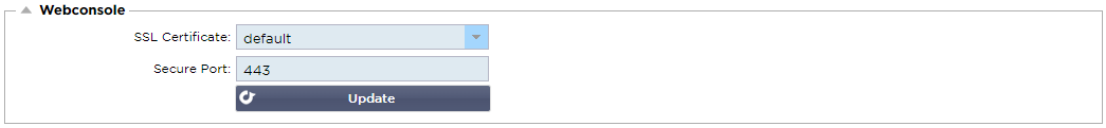
Sicherheit

In diesem Abschnitt können Sie das Passwort der Web-Konsole ändern und den Secure Shell-Zugang aktivieren oder deaktivieren. Er ermöglicht auch die Aktivierung der REST-API-Fähigkeit.

SSH

Option	Beschreibung
Sichere Shell-Fernverbindung	Bitte kreuzen Sie das Kästchen an, wenn Sie über SSH Zugriff auf den ADC erhalten möchten. "Putty" ist eine exzellente Anwendung, um dies zu tun.

Web-Konsole

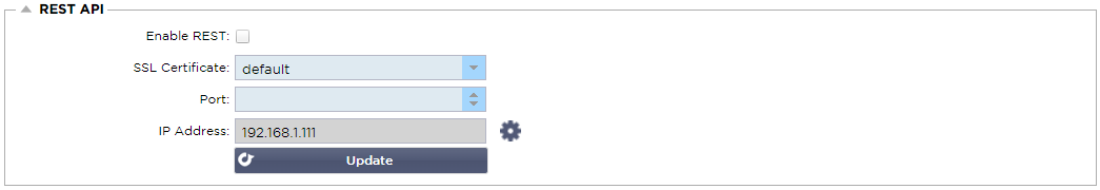


SSL-Zertifikat Wählen Sie ein Zertifikat aus der Dropdown-Liste. Das von Ihnen gewählte Zertifikat wird verwendet, um Ihre Verbindung zur Web-Benutzeroberfläche des ADC zu sichern. Sie können ein selbstsigniertes Zertifikat innerhalb des ADCs erstellen oder eines aus dem Bereich **SSL-ZERTIFIKATE** importieren.

Option	Beschreibung
Sicherer Port	Der Standardport für die Webkonsole ist TCP 443. Wenn Sie aus Sicherheitsgründen einen anderen Port verwenden möchten, können Sie ihn hier ändern.

REST-API

Die REST-API, auch bekannt als RESTful API, ist eine Anwendungsprogrammierschnittstelle, die dem REST-Architekturstil entspricht und die Konfiguration des ADC oder die Datenextraktion aus dem ADC ermöglicht. Der Begriff REST stand für Representational State Transfer und wurde vom Informatiker Roy Fielding geschaffen.



Option	Beschreibung

REST aktivieren	Markieren Sie dieses Feld, um den Zugriff über die REST-API zu aktivieren. Beachten Sie, dass Sie auch konfigurieren müssen, welcher Adapter auf welchem REST aktiviert ist. Siehe den Hinweis auf den Cog-Link unten.
SSL-Zertifikat	Wählen Sie ein Zertifikat für den REST-Dienst. Im Dropdown werden alle auf dem ADC installierten Zertifikate angezeigt.
Hafen	Legen Sie den Port für den REST-Dienst fest. Es ist eine gute Idee, einen anderen Port als 443 zu verwenden.
IP-Adresse	Dadurch wird die IP-Adresse angezeigt, an die der REST-Dienst gebunden ist. Sie können auf den Zahnrad-Link klicken, um auf die Seite Netzwerk zuzugreifen und zu ändern, auf welchem Adapter der REST-Dienst aktiviert ist.
Zahnrad-Link	Wenn Sie auf diesen Link klicken, gelangen Sie auf die Seite Netzwerk, auf der Sie einen Adapter für den REST konfigurieren können.

Dokumentation für REST-API

Dokumentation zur Verwendung der REST-API ist verfügbar: **jetAPI | 4.2.3 | jetNEXUS | SwaggerHub**

Hinweis: Wenn Sie auf der Swagger-Seite Fehler erhalten, liegt das daran, dass sie ein Problem mit der Unterstützung von Query-Strings haben
Scrollen Sie an den Fehlern vorbei zur jetNEXUS REST API

Beispiele

GUID mit CURL:

- Befehl

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

- wird zurückgegeben

```
{"Loginstatus": "OK", "Benutzername":"<Restbenutzername>", "GUID":"<guid>"}
```

- Gültigkeit
  - GUID ist 24 Stunden lang gültig

Lizenz Details

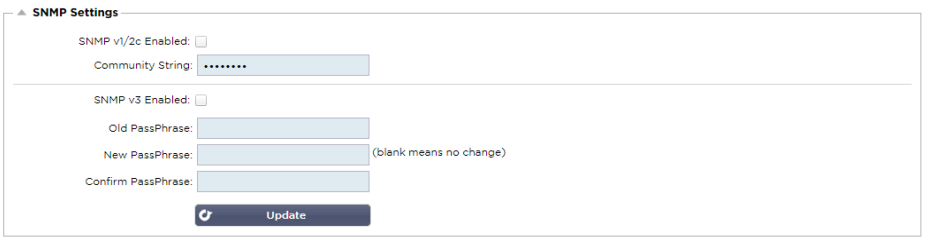
- Befehl

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

SNMP

Der SNMP-Bereich ermöglicht die Konfiguration der SNMP-MIB, die sich im ADC befindet. Die MIB kann dann von Drittanbieter-Software abgefragt werden, die in der Lage ist, mit Geräten zu kommunizieren, die mit SNMP ausgestattet sind.

SNMP-Einstellungen



Option	Beschreibung
SNMP v1 / V2C	Aktivieren Sie das Kontrollkästchen, um die V1/V2C-MIB zu aktivieren. SNMP v1 ist konform mit RFC-1157. SNMP V2c ist konform mit RFC-1901-1908
SNMP v3	Aktivieren Sie das Kontrollkästchen, um die V3-MIB zu aktivieren. RFC-3411-3418. Der Benutzername für v3 ist admin. Beispiel:- snmpwalk -v3 -u admin -A jetnexus -l authNoPriv 192.168.1.11 1.3.6.1.4.1.38370
Gemeinschaft String	Dies ist die schreibgeschützte Zeichenfolge, die auf dem Agenten eingestellt ist und vom Manager zum Abrufen der SNMP-Informationen verwendet wird. Der Standard-Community-String ist jetnexus
PassPhrase	Dies ist das Passwort, das benötigt wird, wenn SNMP v3 aktiviert ist. Es muss mindestens 8 Zeichen lang sein und darf nur die Buchstaben Aa-Zz und die Zahlen 0-9 enthalten. Die Standard-Passphrase lautet **jetnexus**

SNMP-MIB

Die über SNMP einsehbaren Informationen werden durch die Management Information Base (MIB) definiert. MIB's beschreiben die Struktur der Verwaltungsdaten und verwenden hierarchische Objektbezeichner (OID). Jede OID kann über eine SNMP-Management-Anwendung gelesen werden.

MIB Download

Die MIB kann hier heruntergeladen werden:

ADC OID

ROOT OID

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

Unsere OIDs

.38370 jetnexusMIB
.1 **jetnexusData (1**.3.6.1.4.1.38370.1)
.1 **jetnexusGlobal (1**.3.6.1.4.1.38370.1.1)
.2 **jetnexusVirtualServices (1**.3.6.1.4.1.38370.1.2)
.3 **jetnexusServer (1**.3.6.1.4.1.38370.1.3)
.1 **jetnexusGlobal (1**.3.6.1.4.1.38370.1.1)
.1 **jetnexusOverallInputBytes (1**.3.6.1.4.1.38370.1.1.1.0)
.2 **jetnexusOverallOutputBytes (1**.3.6.1.4.1.38370.1.1.2.0)
.3 **jetnexusCompressedInputBytes (1**.3.6.1.4.1.38370.1.1.3.0)
. 4 **jetnexusCompressedOutputBytes (1**.3.6.1.4.1.38370.1.1.4.0)
. 5 **jetnexusVersionInfo (1**.3.6.1.4.1.38370.1.1.5.0)
.6 **jetnexusTotalClientConnections (1**.3.6.1.4.1.38370.1.1.6.0)
.7 **jetnexusCpuPercent (1**.3.6.1.4.1.38370.1.1.7.0)
.8 **jetnexusDiskFreePercent (1**.3.6.1.4.1.38370.1.1.8.0)
.9 **jetnexusMemoryPercent (1**.3.6.1.4.1.38370.1.1.9.0)
.10 **jetnexusCurrentConnections (1**.3.6.1.4.1.38370.1.1.10.0)

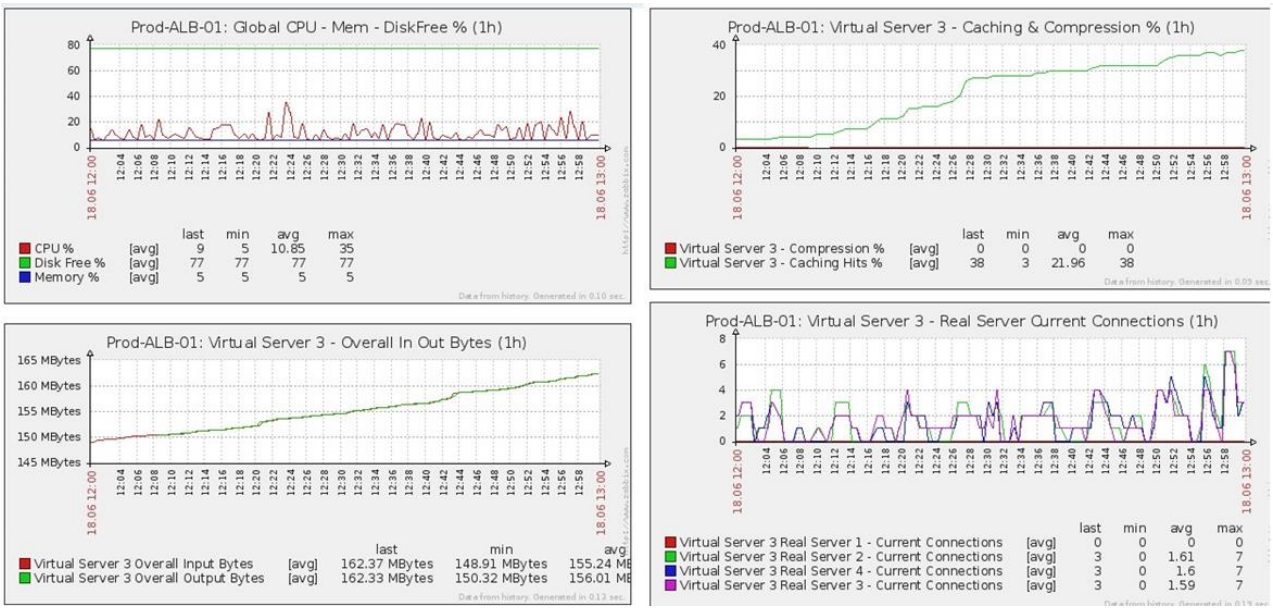
.2 **jetnexusVirtualServices (1**.3.6.1.4.1.38370.1.2)
.1 **jnvirtualserviceEntry (1**.3.6.1.4.1.38370.1.2.1)
.1 **jnvirtualserviceIndexvirtualservice (1**.3.6.1.4.1.38370.1.2.1.**1**)
.2 **jnvirtualserviceVSAddrPort (1**.3.6.1.4.1.38370.1.2.1.**2**)
.3 **jnvirtualserviceOverallInputBytes (1**.3.6.1.4.1.38370.1.2.1.**3**)
.4 **jnvirtualserviceOverallOutputBytes (1**.3.6.1.4.1.38370.1.2.1.**4**)
. 5 **jnvirtualserviceCacheBytes (1**.3.6.1.4.1.38370.1.2.1.**5**)
.6 **jnvirtualserviceCompressionPercent (1**.3.6.1.4.1.38370.1.2.1.**6**)
.7 **jnvirtualservicePresentClientConnections (1**.3.6.1.4.1.38370.1.2.1.**7**)
.8 **jnvirtualserviceHitCount (1**.3.6.1.4.1.38370.1.2.1.**8**)
.9 jnvirtualserviceCacheHits (1.3.6.1.4.1.38370.1.2.1.**9**)

. 10 **jnvirtualserviceCacheHitsPercent (1**.3.6.1.4.1.38370.1.2.1**.10**)
.11 **jnvirtualserviceVSStatus (1**.3.6.1.4.1.38370.1.2.1**.11**)

.3 **jetnexusRealServer (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**)

Historische Diagramme

Die beste Verwendung für die benutzerdefinierte SNMP-MIB des ADC ist die Möglichkeit, die historische grafische Darstellung an eine Management-Konsole Ihrer Wahl auszulagern. Nachfolgend finden Sie einige Beispiele von Zabbix, die einen ADC für verschiedene oben aufgeführte OID-Werte abfragen.



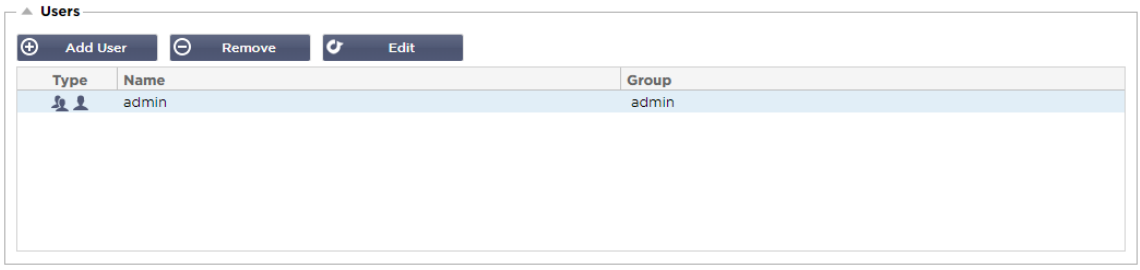
Benutzer und Audit-Protokolle

Die ADC bietet die Möglichkeit, eine interne Gruppe von Benutzern zu haben, um zu konfigurieren und zu definieren, was die ADC tut. Innerhalb des ADC definierte Benutzer können je nach der ihnen zugewiesenen Rolle eine Vielzahl von Operationen durchführen.

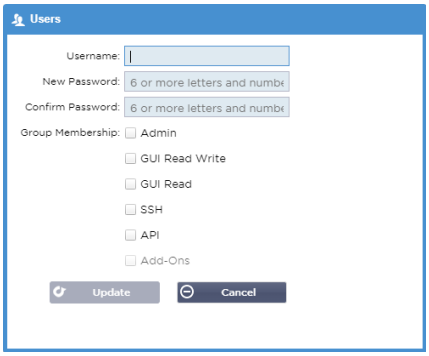
Es gibt einen Standardbenutzer namens **admin**, den Sie beim ersten Konfigurieren des ADC verwenden. Das Standardpasswort für admin lautet **jetnexus**.

Benutzer

Im Bereich Benutzer können Sie Benutzer erstellen, bearbeiten und aus dem ADC entfernen.



Benutzer hinzufügen



Klicken Sie auf die in der obigen Abbildung gezeigte Schaltfläche Benutzer hinzufügen, um den Dialog Benutzer hinzufügen aufzurufen.

Parameter	Beschreibung/Verwendung
Benutzername	Geben Sie einen Benutzernamen Ihrer Wahl ein Der Benutzername muss mit dem Folgenden übereinstimmen: • Minimale Anzahl von Zeichen 1 • Maximale Anzahl von Zeichen 32 • Buchstaben können groß und klein geschrieben werden • Zahlen können verwendet werden • Symbole sind nicht erlaubt
Passwort	Geben Sie ein **sicheres** Passwort ein, das den folgenden Anforderungen entspricht • Minimale Anzahl von Zeichen 6 • Maximale Anzahl von Zeichen 32 • Muss mindestens eine Kombination aus Buchstaben und Zahlen verwenden • Buchstaben können groß oder klein geschrieben werden • Symbole sind erlaubt, mit Ausnahme derjenigen im folgenden Beispiel **£**, **%**, **&** , **<** , **>**
Bestätigen Sie das Passwort	Bestätigen Sie das Passwort erneut, um sicherzustellen, dass es korrekt ist
Gruppenmitgliedschaft	Markieren Sie die Gruppe, zu der der Benutzer gehören soll. • Admin - Diese Gruppe kann alles tun • GUI Read Write - Benutzer in dieser Gruppe können auf die GUI zugreifen und Änderungen über die GUI vornehmen • GUI Lesen - Benutzer in dieser Gruppe können auf die GUI zugreifen, um nur Informationen anzuzeigen. Es können keine Änderungen vorgenommen werden • SSH - Benutzer in dieser Gruppe können über Secure Shell auf den ADC zugreifen. Diese Auswahl ermöglicht den Zugriff auf die Befehlszeile, die einen minimalen Satz von Befehlen zur Verfügung stellt • API - Benutzer in dieser Gruppe haben Zugriff auf die programmierbare SOAP- und REST-Schnittstelle. REST wird ab Software-Version 4.2.1 verfügbar sein

Benutzer-Typ

Lokaler Benutzer
Der ADC in der Rolle "Stand-Alone" oder "Manual H/A" erstellt nur lokale Benutzer
Standardmäßig ist ein lokaler Benutzer namens "admin" **ein Mitglied der Gruppe admin. Aus Gründen der Abwärtskompatibilität kann dieser Benutzer nie gelöscht werden**
Sie können das Passwort dieses Benutzers ändern oder ihn löschen, **aber Sie können nicht den letzten lokalen Admin löschen**

Cluster-Benutzer
Die ADC in Cluster-Rolle erstellt nur Cluster-Benutzer
Cluster-Benutzer werden über alle ADCs im Cluster synchronisiert
Jede Änderung an einem Cluster-Benutzer wirkt sich auf alle Mitglieder des Clusters aus
Wenn Sie als Cluster-Benutzer angemeldet sind, können Sie die Rollen nicht von Cluster auf Manuell oder Stand-Alone umschalten

Cluster und lokaler Benutzer
Alle Benutzer, die in der Rolle Stand-Alone oder Manuell erstellt wurden, werden in den Cluster kopiert
Wenn der ADC anschließend den Cluster verlässt, verbleiben nur noch die lokalen Benutzer
Das zuletzt konfigurierte Passwort für den Benutzer wird gültig sein

Entfernen eines Benutzers

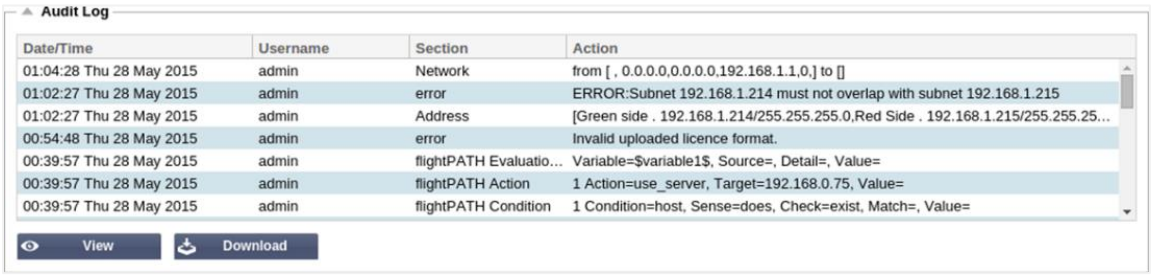
- Einen vorhandenen Benutzer markieren
- Klicken Sie auf Entfernen
- Sie können den Benutzer, der gerade angemeldet ist, nicht löschen
- Sie können den letzten lokalen Benutzer in der Admin-Gruppe nicht entfernen
- Sie können den letzten verbleibenden Cluster-Benutzer in der Admin-Gruppe nicht entfernen
- Sie können den Admin-Benutzer aus Gründen der Abwärtskompatibilität nicht löschen
- Wenn Sie den ADC aus dem Cluster entfernen, werden alle Benutzer außer den lokalen Benutzern gelöscht

Bearbeiten eines Benutzers

- Einen vorhandenen Benutzer markieren
- Klicken Sie auf Bearbeiten
- Sie können die Gruppenzugehörigkeit des Benutzers ändern, indem Sie die entsprechenden Kästchen ankreuzen und aktualisieren
- Sie können auch das Passwort eines Benutzers ändern, sofern Sie über Administratorrechte verfügen

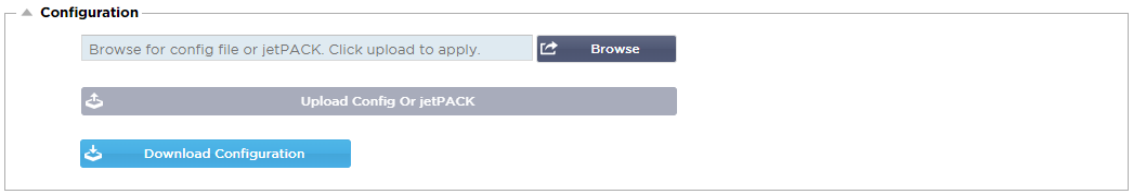
Audit-Protokoll

Das ADC protokolliert Änderungen an der ADC-Konfiguration, die von einzelnen Benutzern vorgenommen wurden. Das Audit-Protokoll enthält die letzten 50 Aktionen, die von allen Benutzern durchgeführt wurden. Sie können auch ALLE Einträge im Bereich **PROTOKOLLE** sehen. Zum Beispiel:



Erweitert

Konfiguration



Es ist immer die beste Praxis, die Konfiguration des ADC herunterzuladen und zu speichern, sobald er vollständig eingerichtet ist und wie gewünscht funktioniert. Sie können das Konfigurationsmodul verwenden, um eine Konfiguration sowohl herunter- als auch hochzuladen.

Jetpacks sind Konfigurationsdateien für Standardanwendungen und werden von Edgenexus bereitgestellt, um Ihre Arbeit zu vereinfachen. Auch diese können mit dem Konfigurationsmodul auf den ADC hochgeladen werden.

Eine Konfigurationsdatei ist im Wesentlichen eine textbasierte Datei und kann als solche von Ihnen mit einem Texteditor wie Notepad++ oder VI bearbeitet werden. Sobald die Konfigurationsdatei wie gewünscht bearbeitet wurde, kann sie in den ADC hochgeladen werden.

Herunterladen einer Konfiguration

- Um die aktuelle Konfiguration des ADC herunterzuladen, drücken Sie die Schaltfläche Konfiguration herunterladen.
- Es wird ein Popup-Fenster angezeigt, in dem Sie aufgefordert werden, die .conf-Datei zu öffnen oder zu speichern.
- Speichern Sie an einem geeigneten Ort.
- Sie können diese mit einem beliebigen Texteditor öffnen, z. B. Notepad++.

Hochladen einer Konfiguration

- Sie können eine gespeicherte Konfigurationsdatei hochladen, indem Sie nach der gespeicherten .conf-Datei suchen.
- Klicken Sie auf die Schaltfläche 'Config oder Jetpack hochladen'.
- Das ADC wird die Konfiguration hochladen und anwenden und dann den Browser aktualisieren. Wenn der Browser nicht automatisch aktualisiert wird, klicken Sie bitte auf Aktualisieren im Browser.
- Sie werden nach Abschluss zur Dashboard-Seite weitergeleitet.

Hochladen eines jetPACKs

- Ein jetPACK ist ein Satz von Konfigurations-Updates für die bestehende Konfiguration.
- Ein jetPACK kann so klein sein wie die Änderung des TCP-Timeout-Wertes bis hin zu einer kompletten anwendungsspezifischen Konfiguration wie Microsoft Exchange oder Microsoft Lync.
    - Sie können ein jetPACK über das am Ende dieser Anleitung aufgeführte Support-Portal beziehen.
- Suchen Sie nach der Datei jetPACK.txt.
- Klicken Sie auf Hochladen.
- Der Browser wird nach dem Hochladen automatisch aktualisiert.
- Sie werden nach Abschluss zur Dashboard-Seite weitergeleitet.
- Der Import kann bei komplexeren Implementierungen wie Microsoft Lync usw. länger dauern.

Globale Einstellungen

Im Bereich "Globale Einstellungen" können Sie verschiedene Elemente ändern, u. a. die kryptografische SSL-Bibliothek.

Host-Cache-Timer

Der Host-Cache-Timer ist eine Einstellung, die die IP-Adresse eines Real-Servers für einen bestimmten Zeitraum speichert, wenn der Domain-Name statt einer IP-Adresse verwendet wurde. Der Cache wird bei einem Ausfall eines Real-Servers geleert. Wenn Sie diesen Wert auf Null setzen, wird der Cache nicht geleert. Für diese Einstellung gibt es keinen Maximalwert.

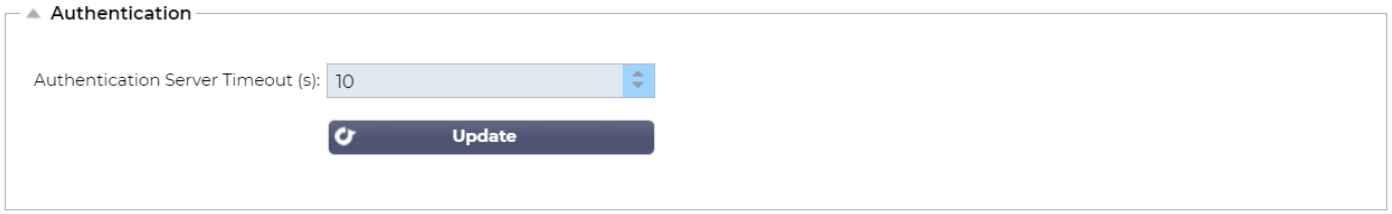
Ablassen

Die Drain-Funktion ist für jeden mit einem virtuellen Dienst verknüpften realen Server konfigurierbar. Standardmäßig ist die Einstellung Drain löscht Persistenz aktiviert, so dass Server, die in den Drain-Modus versetzt werden, Sitzungen ordnungsgemäß beenden können, so dass sie zur Wartung offline genommen werden können.

SSL

Mit dieser globalen Einstellung kann die SSL-Bibliothek nach Bedarf geändert werden. Die standardmäßig vom ADC verwendete SSL-Kryptobibliothek ist von OpenSSL. Wenn Sie eine andere Krypto-Bibliothek verwenden möchten, kann dies hier geändert werden.

Authentifizierung

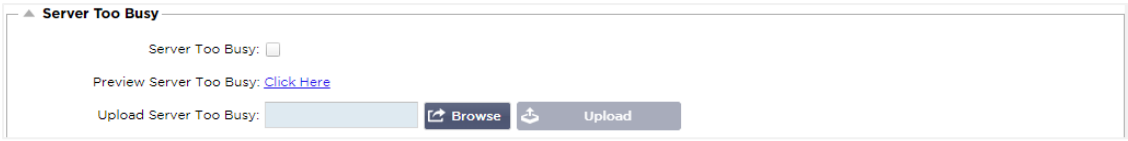


Dieser Wert legt den Timeout-Wert für die Authentifizierung fest, nach dem der Authentifizierungsversuch als fehlgeschlagen betrachtet wird.

Protokoll

Der Abschnitt Protokoll dient zum Festlegen der vielen erweiterten Einstellungen für das HTTP-Protokoll.

Server zu sehr ausgelastet



Angenommen, Sie haben die maximalen Verbindungen zu Ihren Real-Servern begrenzt; Sie können wählen, dass eine freundliche Webseite angezeigt wird, sobald dieses Limit erreicht ist.

- Erstellen Sie eine einfache Web-Seite mit Ihrer Nachricht. Sie können externe Links zu Objekten auf anderen Webservern und Websites einfügen. Wenn Sie alternativ Bilder auf Ihrer Webseite haben möchten, dann verwenden Sie inline base64-kodierte Bilder
- Suchen Sie nach Ihrer neu erstellten Webseiten-HTM(L)-Datei
- Klicken Sie auf Hochladen
- Wenn Sie eine Vorschau der Seite wünschen, können Sie dies mit dem Link Hier klicken tun

Weitergeleitet für

Forwarded For ist der De-facto-Standard für die Identifizierung der ursprünglichen IP-Adresse eines Clients, der sich über Layer-7-Loadbalancer und Proxy-Server mit einem Webserver verbindet.

Weitergeleitet-für Ausgang

Option	Beschreibung
Aus	ADC ändert den Forwarded-For-Header nicht.
Adresse und Port hinzufügen	Diese Auswahl fügt die IP-Adresse und den Port des Geräts oder Clients, der mit dem ADC verbunden ist, an den Forwarded-For-Header an.
Adresse hinzufügen	Bei dieser Auswahl wird die IP-Adresse des Geräts oder Clients, das mit dem ADC verbunden ist, an den Forwarded-For-Header angehängt.
Ersetzen Sie Adresse und Port	Bei dieser Auswahl wird der Wert des Forwarded-For-Headers durch die IP-Adresse und den Port des Geräts oder Clients ersetzt, das mit dem ADC verbunden ist.
Adresse ersetzen	Bei dieser Auswahl wird der Wert des Forwarded-For-Headers durch die IP-Adresse des mit ADC verbundenen Geräts oder Clients ersetzt.

Weitergeleitet-für-Kopfzeile

In diesem Feld können Sie den Namen angeben, der dem Forwarded-For-Header gegeben wird. Normalerweise ist dies "X-Forwarded-For", kann aber in manchen Umgebungen geändert werden.

Erweiterte Protokollierung für IIS - Benutzerdefinierte Protokollierung

Sie können die X-Forwarded-For-Informationen erhalten, indem Sie die IIS Advanced logging 64-bit App installieren. Nach dem Herunterladen erstellen Sie ein benutzerdefiniertes Protokollierungsfeld namens X-Forwarded-For mit den folgenden Einstellungen.

Wählen Sie in der Liste Quellentyp aus der Liste Kategorie die Option Standard, wählen Sie im Feld Quellenname die Option Abfragekopf und geben Sie X-Weitergeleitet-für ein.

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

Änderungen der Apache HTTPd.conf

Sie werden einige Änderungen am Standardformat vornehmen wollen, um die X-Forwarded-For-Client-IP-Adresse oder die tatsächliche Client-IP-Adresse zu protokollieren, wenn der X-Forwarded-For-Header nicht vorhanden ist.

Diese Änderungen finden Sie unten:

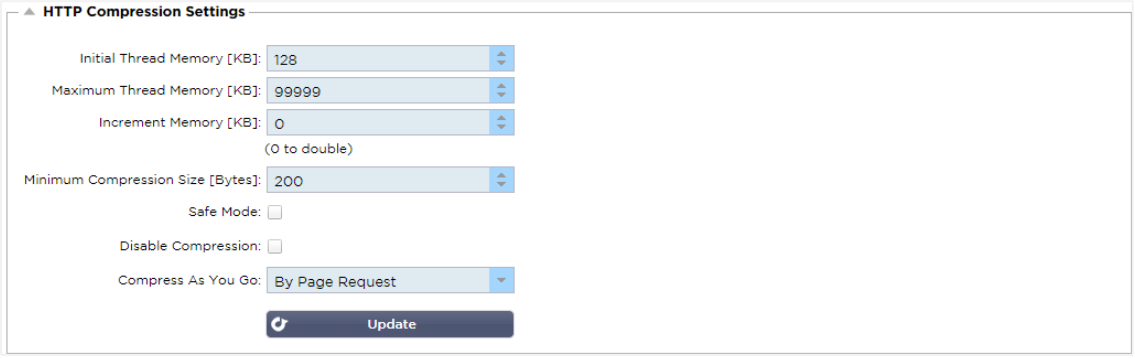
Typ	Wert
LogFormat:	"%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{Benutzer-Agent}i\"" kombiniert
LogFormat:	"%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" proxy SetEnvIf X- Forwarded-For "^.*\..*\..*\..*" weitergeleitet
CustomLog:	"logs/access_log" combined env=!forwarded
CustomLog:	"logs/access_log" proxy env=forwarded

Dieses Format nutzt die eingebaute Unterstützung des Apache für die bedingte Protokollierung auf der Basis von Umgebungsvariablen.

- Zeile 1 ist die standardmäßige kombinierte Protokollformatierung aus der Vorgabe.
- Zeile 2 ersetzt das Feld %h (Remote-Host) durch den/die Wert(e), der/die aus dem X-Forwarded-For-Header gezogen wurde(n), und setzt den Namen dieses Protokolldateimusters auf "proxy".
- Zeile 3 ist eine Einstellung für die Umgebungsvariable "forwarded", die einen losen regulären Ausdruck enthält, der auf eine IP-Adresse passt, was in diesem Fall in Ordnung ist, da es uns mehr interessiert, ob eine IP-Adresse im X-Forwarded-For-Header existiert.
- Außerdem könnte Zeile 3 wie folgt gelesen werden: "Wenn es einen X-Forwarded-For-Wert gibt, verwenden Sie ihn."
- In den Zeilen 4 und 5 wird dem Apache mitgeteilt, welches Protokollmuster er verwenden soll. Wenn ein X-Forwarded-For-Wert vorhanden ist, verwenden Sie das "proxy"-Muster, andernfalls verwenden Sie das "combined"-Muster für die Anfrage. Aus Gründen der Lesbarkeit nutzen die Zeilen 4 und 5 nicht die Apache-Protokollierungsfunktion "rotate logs" (piped), aber wir gehen davon aus, dass fast jeder sie verwendet.

Diese Änderungen führen dazu, dass für jede Anfrage eine IP-Adresse protokolliert wird.

HTTP-Komprimierungseinstellungen

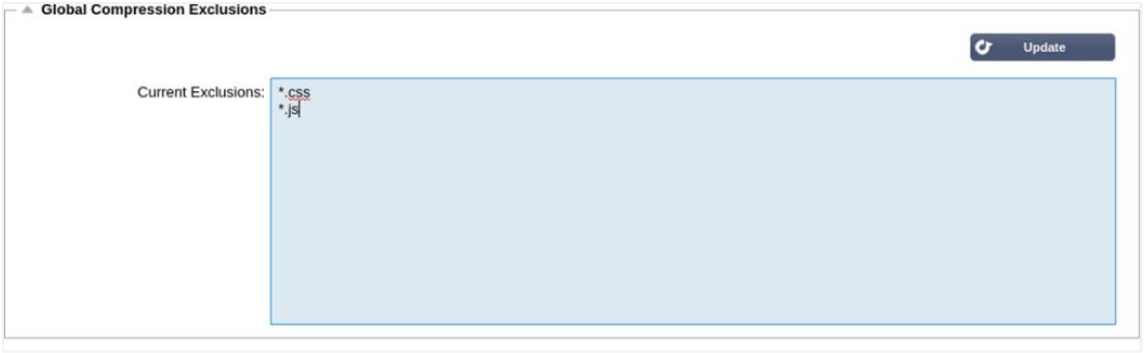


Die Komprimierung ist eine Beschleunigungsfunktion und wird für jeden Dienst auf der Seite IP-Dienste aktiviert.

WARNUNG - Gehen Sie beim Anpassen dieser Einstellungen äußerst vorsichtig vor, da ungeeignete Einstellungen die Leistung des ADC beeinträchtigen können

Option	Beschreibung
Initialer Thread-Speicher [KB]	Dieser Wert ist die Menge an Speicher, die jede vom ADC empfangene Anfrage anfänglich zuweisen darf. Um eine möglichst effiziente Leistung zu erzielen, sollte dieser Wert auf einen Wert eingestellt werden, der knapp über der größten unkomprimierten HTML-Datei liegt, die die Webserver wahrscheinlich senden werden.
Maximaler Thread-Speicher [KB]	Dieser Wert ist die maximale Menge an Speicher, die die ADC bei einer Anfrage zuweist. Für maximale Leistung speichert und komprimiert ADC normalerweise alle Inhalte im Speicher. WENN eine außergewöhnlich große Inhaltsdatei, die diese Menge überschreitet, verarbeitet wird, schreibt ADC auf die Festplatte und komprimiert die Daten dort.
Inkrement-Speicher [KB]	Dieser Wert legt die Menge an Speicher fest, die zur anfänglichen Thread-Speicherzuweisung hinzugefügt wird, wenn mehr benötigt wird. Die Standardeinstellung ist Null. Das bedeutet, dass ADC die Zuweisung verdoppelt, wenn die Daten die aktuelle Zuweisung überschreiten (z. B. 128Kb, dann 256Kb, dann 512Kb usw.), bis zu der Grenze, die durch Maximale Speichernutzung pro Thread festgelegt ist. Dies ist effizient, wenn die Mehrheit der Seiten eine gleichbleibende Größe hat, es aber gelegentlich größere Dateien gibt. (z.B. Die Mehrheit der Seiten ist 128Kb oder weniger groß, aber gelegentliche Antworten sind 1Mb groß.) In dem Szenario, in dem es große Dateien mit variabler Größe gibt, ist es effizienter, ein lineares Inkrement einer signifikanten Größe einzustellen (z. B. Antworten sind 2Mb bis 10Mb groß, eine anfängliche Einstellung von 1Mb mit Inkrementen von 1Mb wäre effizienter.).
Minimale Komprimierungsgröße [Bytes]	Dieser Wert ist die Größe in Bytes, unter der der ADC nicht versucht, zu komprimieren. Dies ist nützlich, da alles, was deutlich unter 200 Bytes liegt, nicht gut komprimiert wird und aufgrund des Overheads der Kompressions-Header sogar größer werden kann.
Abgesicherter Modus	Aktivieren Sie diese Option, um zu verhindern, dass ADC die Komprimierung auf Stylesheets oder JavaScript anwendet. Der Grund dafür ist, dass ADC zwar weiß, welche einzelnen Browser mit komprimierten Inhalten umgehen können, dass aber einige andere Proxy-Server, auch wenn sie behaupten, HTTP/1.1-konform zu sein, komprimierte Stylesheets und JavaScript nicht korrekt transportieren können. Wenn Probleme mit Stylesheets oder JavaScript über einen Proxyserver auftreten, dann verwenden Sie diese Option, um die Komprimierung dieser Typen zu deaktivieren. Dadurch wird jedoch der Gesamtumfang der Komprimierung von Inhalten verringert.
Komprimierung deaktivieren	Aktivieren Sie diese Option, um zu verhindern, dass ADC eine Antwort komprimiert.
Compress As You Go	EIN - Verwenden Sie "Compress as You Go" auf dieser Seite. Dies komprimiert jeden vom Server empfangenen Datenblock in einem diskreten Stück, das vollständig dekomprimierbar ist. AUS - Verwenden Sie Compress As You Go nicht auf dieser Seite. Nach Seitenanforderung - Verwenden Sie "Compress as you go" nach Seitenanforderung.

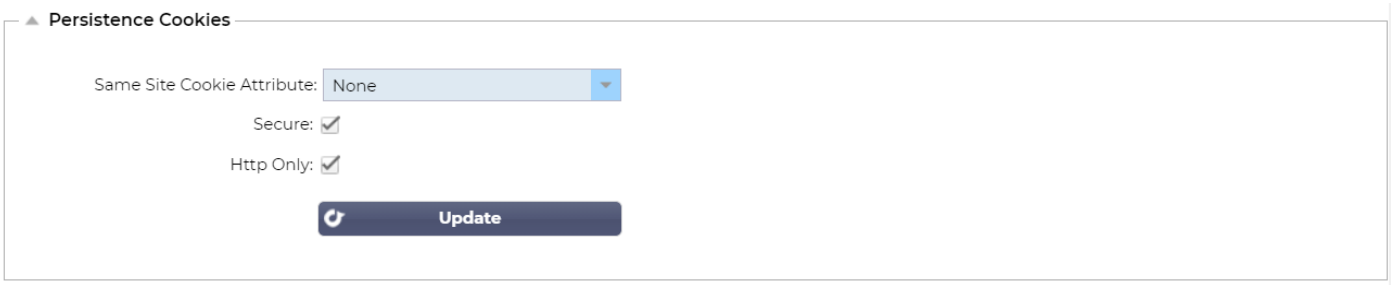
Globale Komprimierungsausschlüsse



Alle Seiten mit der hinzugefügten Erweiterung in der Ausschlussliste werden nicht komprimiert.

- Geben Sie den individuellen Dateinamen ein.
- Klicken Sie auf Aktualisieren.
- Wenn Sie einen Dateityp hinzufügen möchten, geben Sie einfach "*.css" für alle auszuschließenden Cascading Style Sheets ein.
- Jede Datei oder jeder Dateityp sollte in einer neuen Zeile hinzugefügt werden.

Persistenz-Cookies



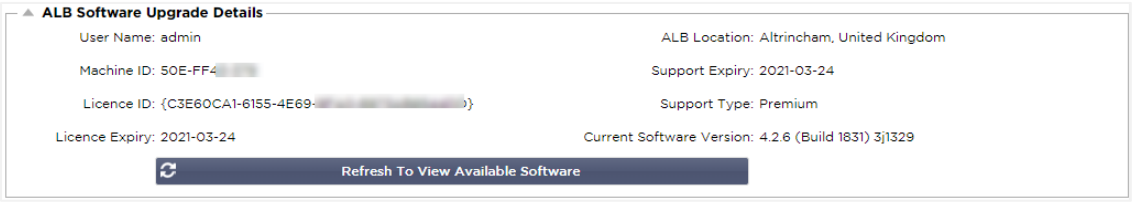
Mit dieser Einstellung können Sie festlegen, wie Persistenz-Cookies behandelt werden.

Feld	Beschreibung
Gleicher Standort Cooke-Attribut	**Keine**: Alle Cookies sind für Skripte zugänglich **Lax**: Verhindert den Zugriff auf Cookies über verschiedene Websites hinweg, aber sie werden so gespeichert, dass sie zugänglich werden und an die besitzende Website übermittelt werden, wenn diese besucht wird **Strikt**: verhindert, dass ein Cookie für eine andere Seite aufgerufen oder gespeichert wird **Aus**: kehrt zum Standardverhalten des Browsers zurück
Sicher	Wenn dieses Kontrollkästchen aktiviert ist, wird die Persistenz auf den sicheren Datenverkehr angewendet
Nur HTTP	Wenn diese Option aktiviert ist, erlaubt sie Persistent Cookes nur für HTTP-Verkehr

Software

Im Bereich Software können Sie die Konfiguration und die Firmware Ihres ADCs aktualisieren.

Details zum Software-Upgrade



Die Informationen in diesem Abschnitt werden ausgefüllt, wenn Sie eine funktionierende Internetverbindung haben. Wenn Ihr Browser keine Verbindung zum Internet hat, ist dieser Abschnitt leer. Sobald die Verbindung hergestellt ist, erhalten Sie die unten stehende Bannermeldung.

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

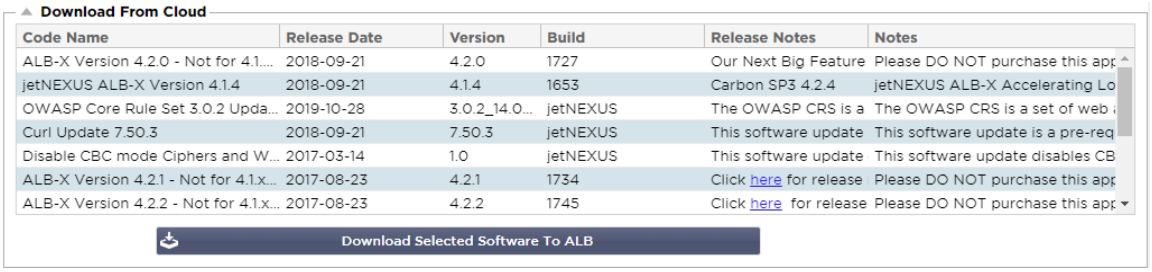
Der unten gezeigte Abschnitt Download aus der Cloud wird mit Informationen zu den Updates gefüllt, die Ihnen im Rahmen Ihres Supportplans zur Verfügung stehen. Sie sollten auf den Support-Typ und das Ablaufdatum des Supports achten.

Hinweis: Wir verwenden die Internetverbindung Ihres Browsers, um anzuzeigen, was in der Edgenexus Cloud verfügbar ist. Sie können nur dann Software-Updates herunterladen, wenn der ADC eine Internetverbindung hat.

Um dies zu überprüfen:

- Erweitert--Fehlerbehebung--Ping
- IP-Adresse - appstore.edgenexus.io
- Klicken Sie auf Ping
- Wenn das Ergebnis anzeigt "ping: unknown host appstore.edgenexus.io. "
- Der ADC wird NICHT in der Lage sein, etwas aus der Cloud herunterzuladen

Download aus der Cloud



Wenn Ihr Browser mit dem Internet verbunden ist, sehen Sie Details zu Software, die in der Cloud verfügbar ist.

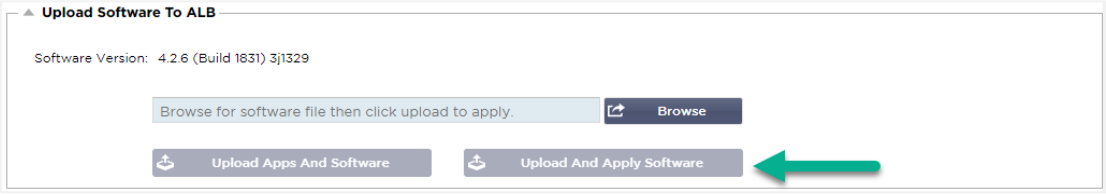
- Markieren Sie die Zeile, die Sie interessiert, und klicken Sie auf die Schaltfläche "Ausgewählte Software auf ALB herunterladen. " Schaltfläche
- Die gewählte Software wird auf Ihren ALB heruntergeladen, wenn Sie darauf klicken. Sie können sie im Abschnitt "Auf dem ALB gespeicherte Software anwenden" unten anwenden.

Hinweis: Wenn der ADC keinen direkten Internetzugang hat, erhalten Sie eine Fehlermeldung wie die folgende:

Download-Fehler, ALB kann nicht auf ADC Cloud Services zugreifen für Datei build1734-3236-v4.2.1-Sprint2-update-64.software.alb

Software zu ALB hochladen

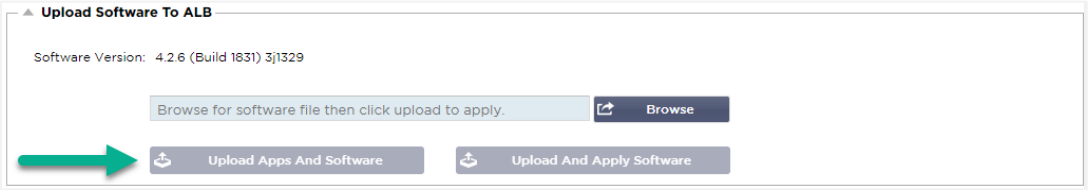
Apps hochladen



Wenn Sie eine App-Datei haben, die mit <apptype>.alb endet, können Sie diese Methode verwenden, um sie hochzuladen.

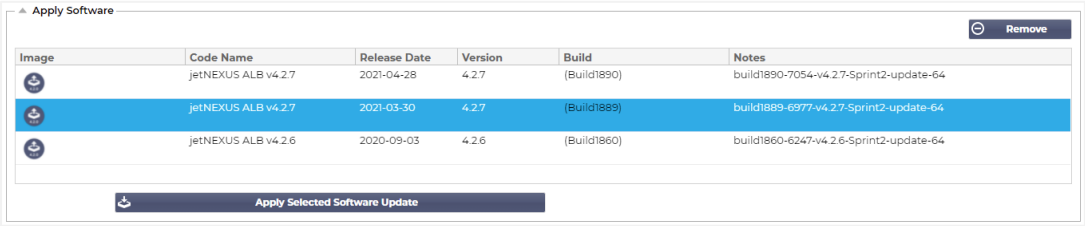
- Es gibt fünf Arten von Apps
  - <AppName>Flugweg.alb
  - <appname>.monitor.alb
  - <AppName>.jetpack.alb
  - <Appname>.addons.alb
  - <appname>.featurepack.alb
- Nach dem Hochladen finden Sie jede App im Bereich Bibliothek> Apps.
- Sie müssen dann jede App in diesem Bereich einzeln bereitstellen.

Software



- Wenn Sie Software hochladen möchten, ohne sie anzuwenden, dann verwenden Sie die markierte Schaltfläche.
- Die Software-Datei ist <softwarename>.software.alb.
- Sie wird dann im Bereich "Auf ALB gespeicherte Software" angezeigt, von wo aus Sie sie nach Belieben anwenden können.

Auf dem ALB gespeicherte Software anwenden



In diesem Abschnitt werden alle Software-Dateien angezeigt, die auf dem ALB gespeichert und für die Bereitstellung verfügbar sind. Die Auflistung enthält auch aktualisierte Signaturen der Web Application Firewall (WAF).

- Markieren Sie die Zeile Software, die Sie verwenden möchten.
- Klicken Sie auf "Software aus Auswahl übernehmen".
- Wenn es sich um ein ALB-Software-Update handelt, beachten Sie bitte, dass es hochgeladen und dann das ALB neu gestartet werden muss, um es anzuwenden.
- Wenn das Update, das Sie anwenden, ein OWASP-Signatur-Update ist, wird es automatisch ohne Neustart angewendet.

Fehlersuche

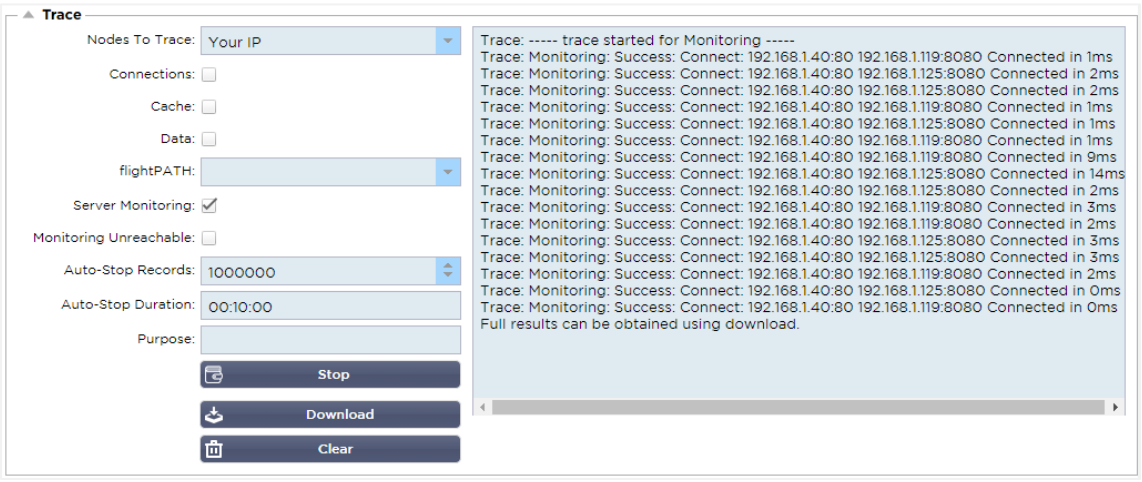
Es gibt immer wieder Probleme, die eine Fehlersuche erfordern, um zu einer Grundursache und Lösung zu kommen. In diesem Abschnitt können Sie das tun.

Dateien unterstützen

Wenn Sie ein Problem mit dem ADC haben und ein Support-Ticket öffnen müssen, wird der technische Support oft mehrere verschiedene Dateien von der ADC-Appliance anfordern. Diese Dateien wurden nun in einer einzigen .dat-Datei zusammengefasst, die über diesen Abschnitt heruntergeladen werden kann.

- Wählen Sie einen Zeitrahmen aus der Dropdown-Liste: Es stehen Ihnen 3, 7, 14 und Alle Tage zur Verfügung.
- Klicken Sie auf "Support-Dateien herunterladen".
- Es wird eine Datei im Format Support-jetNEXUS-yyymmddhh-NAME.dat heruntergeladen
- Erstellen Sie ein Support-Ticket auf dem Support-Portal, Details dazu finden Sie am Ende dieses Dokuments.
- Stellen Sie sicher, dass Sie das Problem gründlich beschreiben und die .dat-Datei an das Ticket anhängen.

Spurensuche



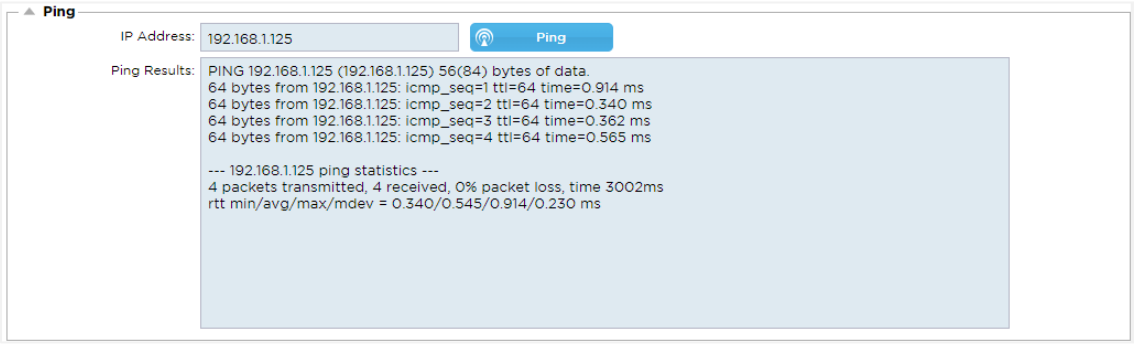
Im Abschnitt "Trace" können Sie Informationen einsehen, die die Fehlersuche im Problemfall ermöglichen. Die gelieferten Informationen hängen von den Optionen ab, die Sie aus den Dropdowns und den Kontrollkästchen auswählen.

Option	Beschreibung
Zu verfolgende Knoten	**Ihre IP**: Damit wird die Ausgabe so gefiltert, dass die IP-Adresse verwendet wird, von der Sie auf die GUI zugreifen (Hinweis: Wählen Sie diese Option nicht für die Überwachung, da die Überwachung die Adresse der ADC-Schnittstelle verwendet). **Alle IP**: Es wird kein Filter angewendet. Es ist zu beachten, dass dies bei einer stark ausgelasteten Box die Leistung beeinträchtigt.
Verbindungen	Wenn dieses Kontrollkästchen aktiviert ist, werden Ihnen Informationen über die client- und serverseitigen Verbindungen angezeigt.

Cache	Wenn dieses Kontrollkästchen aktiviert ist, werden Ihnen Informationen zu zwischengespeicherten Objekten angezeigt.
Daten	Wenn dieses Kontrollkästchen aktiviert ist, enthält es die Rohdatenbytes, die vom ADC ein- und ausgehend verarbeitet werden.
flightPATH	Im Menü flightPATH können Sie eine bestimmte flightPATH-Regel zur Überwachung auswählen oder Alle flightPATH-Regeln.
Server-Überwachung	Wenn dieses Kontrollkästchen aktiviert ist, werden die auf dem ADC aktiven Server-Zustandsmonitore und ihre jeweiligen Ergebnisse angezeigt.
Überwachung unerreichbar	Wenn diese Option ausgewählt ist, verhält sie sich ähnlich wie die Server-Überwachung, nur dass sie nur die fehlgeschlagenen Monitore anzeigt und somit als Filter nur für diese Meldungen fungiert.
Auto-Stopp-Datensätze	Der Standardwert ist 1.000.000 Datensätze, nach dem die Trace-Funktion automatisch gestoppt wird. Diese Einstellung ist eine Sicherheitsvorkehrung, um zu verhindern, dass Trace versehentlich eingeschaltet bleibt und die Leistung Ihres ADCs beeinträchtigt.
Auto-Stopp Dauer	Die Standardzeit ist auf 10 Minuten eingestellt, nach der die Trace-Funktion automatisch gestoppt wird. Diese Funktion ist eine Sicherheitsvorkehrung, um zu verhindern, dass Trace versehentlich eingeschaltet bleibt und die Leistung des ADCs beeinträchtigt.
Start	Klicken Sie hierauf, um die Trace-Funktion manuell zu starten.
Stopp	Klicken Sie auf , um die Trace-Funktion manuell zu stoppen, bevor die automatische Aufzeichnung oder die Zeit erreicht ist.
Herunterladen	Obwohl Sie den Live-Viewer auf der rechten Seite sehen können, werden die Informationen möglicherweise zu schnell angezeigt. Stattdessen können Sie das Trace.log herunterladen, um alle Informationen zu sehen, die während der verschiedenen Traces an diesem Tag gesammelt wurden. Diese Funktion ist eine gefilterte Liste von Trace-Informationen. Wenn Sie die Trace-Informationen der vorherigen Tage anzeigen möchten, können Sie das Syslog für diesen Tag herunterladen, müssen aber manuell filtern.
Klar	Löscht das Trace-Protokoll

Ping

Sie können die Netzwerkkonnektivität zu Servern und anderen Netzwerkobjekten in Ihrer Infrastruktur mit dem Tool Ping überprüfen.



Geben Sie die IP-Adresse des Hosts ein, die Sie testen möchten, z. B. das Standard-Gateway in punktierter Dezimalschreibweise oder eine IPv6-Adresse. Möglicherweise müssen Sie ein paar Sekunden warten, bis das Ergebnis zurückgemeldet wird, nachdem Sie die Schaltfläche "Ping" gedrückt haben.

Wenn Sie einen DNS-Server konfiguriert haben, dann können Sie den voll qualifizierten Domain-Namen eintippen. Sie können einen DNS-Server im Abschnitt **DNS-SERVER 1 & DNS-SERVER 2** konfigurieren. Möglicherweise müssen Sie ein paar Sekunden warten, bis das Ergebnis zurückgemeldet wird, nachdem Sie die Schaltfläche "Ping" gedrückt haben.

Erfassen

Um den Netzwerkverkehr aufzuzeichnen, folgen Sie den einfachen Anweisungen unten.

- Füllen Sie die Optionen im Formular aus
- Klicken Sie auf Erzeugen
- Sobald das Capture gelaufen ist, öffnet sich Ihr Browser und fragt Sie, wo Sie die Datei speichern möchten. Sie wird im Format "jetNEXUS.cap.gz" vorliegen.
- Erstellen Sie ein Support-Ticket auf dem Support-Portal, Details dazu finden Sie am Ende dieses Dokuments.
- Stellen Sie sicher, dass Sie das Problem gründlich beschreiben und die Datei an das Ticket anhängen.
- Sie können den Inhalt auch mit Wireshark betrachten

Option	Beschreibung
Adapter	Wählen Sie Ihren Adapter aus der Dropdown-Liste, normalerweise eth0 oder eth1. Sie können auch alle Schnittstellen mit "any" erfassen
Pakete	Dieser Wert ist die maximale Anzahl der zu erfassenden Pakete. Normalerweise 99999
Dauer	Wählen Sie eine maximale Zeit, für die die Erfassung laufen soll. Eine typische Zeit ist 15 Sekunden für stark frequentierte Sites. Die grafische Benutzeroberfläche ist während der Aufzeichnungszeit nicht zugänglich
Adresse	Dieser Wert filtert auf jede in das Feld eingegebene IP-Adresse. Lassen Sie diesen Wert leer, um nicht zu filtern.

Um die Leistung zu erhalten, haben wir die Download-Datei auf 10 MB begrenzt. Wenn Sie feststellen, dass dies nicht ausreicht, um alle benötigten Daten zu erfassen, können wir diese Zahl erhöhen.

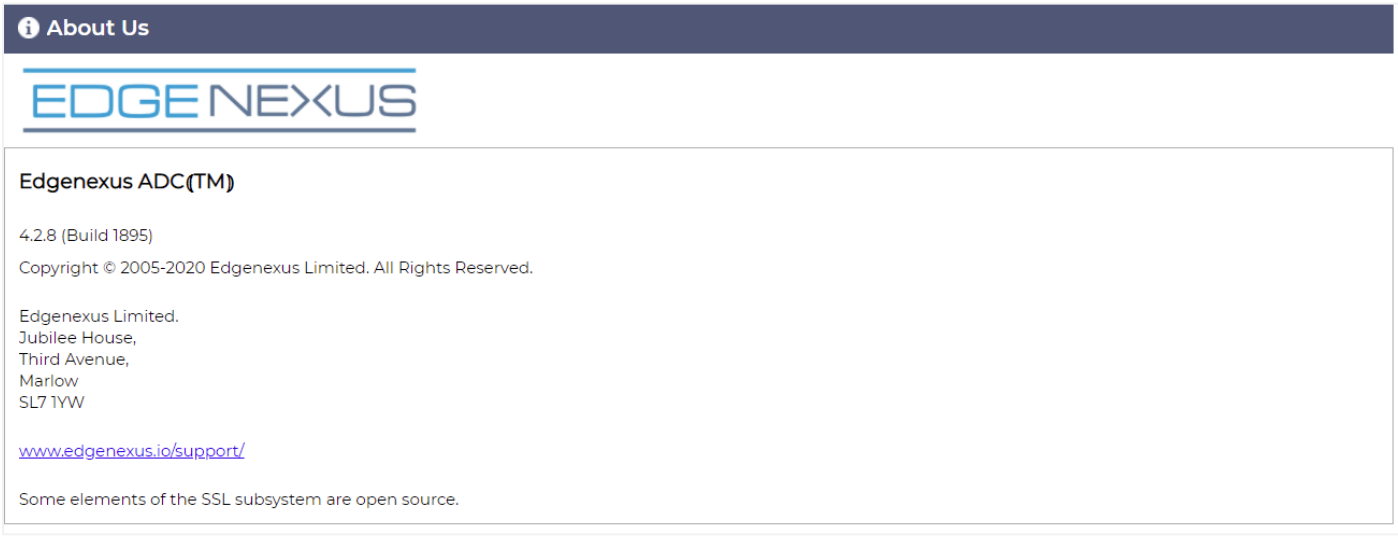
Hinweis: Dies hat Auswirkungen auf die Leistung von Live-Sites. Um die verfügbare Aufnahmegröße zu erhöhen, wenden Sie bitte eine globale Einstellung jetPACK an, um die Aufnahmegröße zu erhöhen.

Hilfe

Der Hilfe-Bereich bietet Zugang zu den Informationen über Edgenexus und Zugriff auf die Benutzerhandbücher und andere hilfreiche Informationen.

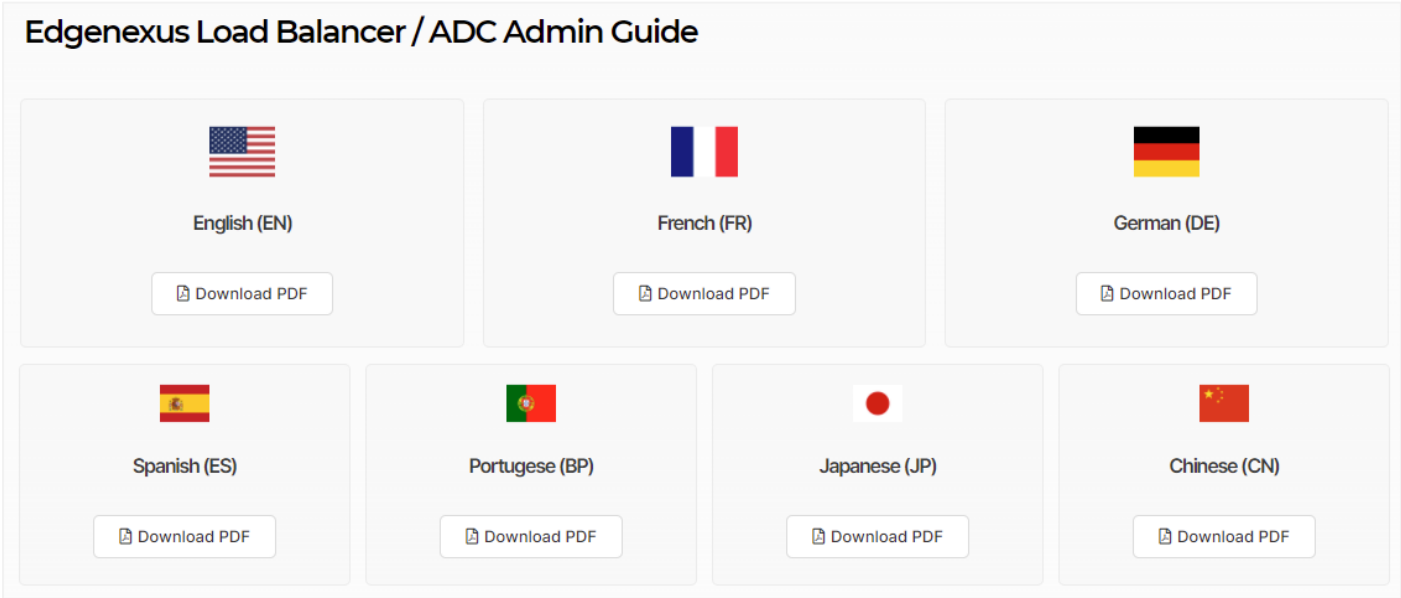
Über uns

Wenn Sie auf die Option "Über uns" klicken, werden Informationen über Edgenexus und dessen Firmensitz angezeigt.



Referenz

Die Option Referenz öffnet die Seite mit den Benutzerhandbüchern und anderen hilfreichen Dokumenten.



Wenn Sie nicht finden, was Sie suchen, wenden Sie sich bitte an support@edgenexus.io.

Was ist ein jetPACK

jetPACKs sind eine einzigartige Methode, um Ihren ADC sofort für bestimmte Anwendungen zu konfigurieren. Diese benutzerfreundlichen Vorlagen sind vorkonfiguriert und vollständig mit allen anwendungsspezifischen Einstellungen abgestimmt, die Sie für eine optimierte Servicebereitstellung durch Ihren ADC benötigen. Einige der jetPACKs verwenden flightPATH, um den Datenverkehr zu manipulieren, und Sie müssen eine flightPATH-Lizenz haben, damit dieses Element funktioniert. Um herauszufinden, ob Sie eine Lizenz für flightPATH haben, schauen Sie bitte auf der Seite **LIZENZ NACH**.

Herunterladen eines jetPACKs

- Jedes jetPACK unten wurde mit einer eindeutigen Virtuellen IP-Adresse erstellt, die im Titel des jetPACKs enthalten ist. Zum Beispiel hat das erste jetPACK unten die virtuelle IP-Adresse 1.1.1.1
- Sie können dieses jetPACK entweder so hochladen, wie es ist, und die IP-Adresse in der GUI ändern oder das jetPACK mit einem Texteditor wie Notepad++ bearbeiten und 1.1.1.1 mit Ihrer virtuellen IP-Adresse suchen und ersetzen.
- Darüber hinaus wurde jedes jetPACK mit 2 Real-Servern mit den IP-Adressen 127.1.1.1 und 127.2.2.2 erstellt. Auch hier können Sie diese in der GUI nach dem Hochladen oder vorher mit Notepad++ ändern.
- Klicken Sie unten auf einen jetPACK-Link und speichern Sie den Link als jetPACK-VIP-Application.txt-Datei an dem von Ihnen gewählten Ort

Microsoft Exchange

Anwendung	Link herunterladen	Was macht es?	Was ist enthalten?
Austausch 2010	jetPACK-1.1.1.1-Exchange-2010	Dieses jetPACK fügt die Grundeinstellungen für den Lastausgleich von Microsoft Exchange 2010 hinzu. Es ist eine flightPATH-Regel enthalten, um den Verkehr auf dem HTTP-Dienst auf HTTPS umzuleiten, aber es ist eine Option. Wenn Sie keine Lizenz für flightPATH haben, funktioniert dieses jetPACK trotzdem.	Globale Einstellungen: Service-Timeout 2 Stunden Monitore: Layer-7-Monitor für die Outlook-Web-App und Layer-4-Out-of-Band-Monitor für den Client-Zugriffsdienst Virtuelle Service-IP: 1.1.1.1 Virtuelle Service Ports: 80, 443, 135, 59534, 59535 Reale Server: 127.1.1.1 127.2.2.2 flightPATH: Fügt Umleitung von HTTP zu HTTPS hinzu
	jetPACK-1.1.1.2-Exchange-2010-SMTP-RP	Wie oben, aber es wird ein SMTP-Dienst auf Port 25 in Reverse-Proxy-Konnektivität hinzugefügt. Der SMTP-Server wird die Adresse der ALB-X-Schnittstelle als Quell-IP sehen.	Globale Einstellungen: Service-Timeout 2 Stunden Monitore: Layer-7-Monitor für die Outlook-Web-App. Layer-4-Out-of-Band-Monitor für den Client-Zugriffsdienst Virtuelle Service-IP: 1.1.1.1 Virtuelle Service Ports: 80, 443, 135, 59534, 59535, 25 (Reverse-Proxy) Reale Server: 127.1.1.1 127.2.2.2 flightPATH: Fügt Umleitung von HTTP zu HTTPS hinzu

	jetPACK-1.1.1.3-Exchange-2010-SMTP-DSR	Wie oben, außer dass dieses jetPACK den SMTP-Dienst so konfiguriert, dass er eine direkte Server-Return-Verbindung verwendet. Dieses jetPACK wird benötigt, wenn Ihr SMTP-Server die tatsächliche IP-Adresse des Clients sehen muss.	Globale Einstellungen: Service-Timeout 2 Stunden Monitore: Layer-7-Monitor für die Outlook-Web-App. Layer-4-Out-of-Band-Monitor für den Client-Zugriffsdienst Virtuelle Service-IP: 1.1.1.1 Virtuelle Service Ports: 80, 443, 135, 59534, 59535, 25 (direkte Server-Rückkehr) Reale Server: 127.1.1.1 127.2.2.2 flightPATH: Fügt Umleitung von HTTP zu HTTPs hinzu
Austausch 2013	jetPACK-2.2.2.1-Exchange-2013-Low-Resource	Diese Einrichtung fügt 1 VIP und zwei Dienste für HTTP- und HTTPS-Verkehr hinzu und benötigt die wenigste CPU. Es ist möglich, dem VIP mehrere Gesundheitsprüfungen hinzuzufügen, um zu prüfen, ob jeder der einzelnen Dienste in Ordnung ist	Globale Einstellungen: Monitore: Layer-7-Monitor für OWA, EWS, OA, EAS, ECP, OAB und ADS Virtuelle Service-IP: 2.2.2.1 Virtuelle Service Ports: 80, 443 Reale Server: 127.1.1.1 127.2.2.2 flightPATH: Fügt Umleitung von HTTP zu HTTPS hinzu
	jetPACK-2.2.3.1-Exchange-2013-Med-Resource	Diese Einrichtung verwendet eine eindeutige IP-Adresse für jeden Dienst und verbraucht daher mehr Ressourcen als oben. Sie müssen jeden Dienst als individuellen DNS-Eintrag konfigurieren Beispiel owa.jetnexus.com, ews.jetnexus.com, usw. Es wird ein Monitor für jeden Dienst hinzugefügt und auf den entsprechenden Dienst angewendet	Globale Einstellungen: Monitore: Layer 7-Monitor für OWA, EWS, OA, EAS, ECP, OAB,ADS, MAPI und PowerShell Virtueller Dienst 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 Virtuelle Service Ports: 80, 443 Reale Server: 127.1.1.1 127.2.2.2 flightPATH: Fügt Umleitung von HTTP zu HTTPs hinzu
	jetPACK-2.2.2.3-Exchange2013-HIgh-Ressource	Dieses jetPACK fügt eine eindeutige IP-Adresse und mehrere virtuelle Dienste auf verschiedenen Ports hinzu. flightPATH schaltet dann den Kontext basierend auf dem Zielpfad auf den richtigen virtuellen Dienst um. Dieses jetPACK benötigt die meiste CPU-Leistung, um die Kontextumschaltung auszuführen	Globale Einstellungen: Monitore: Layer 7-Monitor für OWA, EWS, OA, EAS, ECP, OAB, ADS, MAPI und PowerShell Virtuelle Service-IP: 2.2.2.3 Virtuelle Service Ports: 80, 443, 1, 2, 3, 4, 5, 6, 7 Reale Server: 127.1.1.1 127.2.2.2 flightPATH: Fügt Umleitung von HTTP zu HTTPS hinzu

Microsoft Lync 2010/2013

Umgekehrter Proxy	Vorderseite	Kante Intern	Kante Extern

jetPACK-3.3.3.1-Lync-Reverse-Proxy	jetPACK-3.3.3.2-Lync-Front -Ende	jetPACK-3.3.3.3-Lync-Edge-Intern	jetPACK-3.3.3.4-Lync-Edge-Extern

Web-Dienste

Normales HTTP	SSL-Offload	SSL-Neuverschlüsselung	SSL-Passthrough
jetPACK-4.4.4.1-Web-HTTP	jetPACK-4.4.4.2-Web-SSL-Offload	jetPACK-4.4.4.3-Web-SSL-Re-Encryption	jetPACK-4.4.4.4-Web-SSL Passthrough

Microsoft Remote Desktop

Normal
jetPACK-5.5.5.1-Remote-Desktop

DICOM - Digitale Bildgebung und Kommunikation in der Medizin

Normales HTTP
jetPACK-6.6.6.1-DICOM

Oracle e-Business Suite

SSL-Offload
jetPACK-7.7.7..1-Oracle-EBS

VMware Horizon View

Verbindungsserver - SSL-Offload	Sicherheitsserver - SSL-Neuverschlüsselung
jetPACK-8.8.8.1-View-SSL-Offload	jetPACK-8.8.8.2-View-SSL-Re-Encryption

Globale Einstellungen

- GUI Secure Port 443 - dieses jetPACK ändert Ihren sicheren GUI-Port von 27376 auf 443. HTTPs://x.x.x.x
- GUI Timeout 1 Tag - die GUI fordert Sie alle 20 Minuten zur Eingabe Ihres Passworts auf. Mit dieser Einstellung wird diese Aufforderung auf 1 Tag erhöht
- ARP Refresh 10 - bei einem Failover zwischen HA-Appliances wird mit dieser Einstellung die Anzahl der **Gratuitous ARP's** erhöht, um die Switches beim Übergang zu unterstützen
- Capture-Größe 16MB - die Standard-Capture-Größe beträgt 2MB. Mit diesem Wert wird die Größe auf maximal 16MB erhöht

Chiffre-Optionen

- Starke Chiffren - Damit wird die Möglichkeit hinzugefügt, "Starke Chiffren" aus der Liste der Chiffre-Optionen auszuwählen:
  - Verschlüsselung = ALL:RC4+RSA:+RC4:+HIGH:!DES-CBC3-SHA:!SSLv2:!ADH:!EXP:!ADHexport:!MD5
- Anti-Bestie - Dies fügt die Möglichkeit hinzu, "Anti-Bestie" aus der Liste der Cipher-Optionen zu wählen:
  - Verschlüsselung = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH

- Kein SSLv3 - Damit wird die Möglichkeit hinzugefügt, "Kein SSLv3" aus der Liste der Verschlüsselungsoptionen zu wählen:
  - Verschlüsselung = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
- No SSLv3 no TLSv1 No RC4 - Damit wird die Möglichkeit hinzugefügt, "No-TLSv1 No-SSLv3 No-RC4" aus der Liste der Verschlüsselungsoptionen zu wählen:
  - Verschlüsselung = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
- NO_TLSv1.1 -Damit wird die Möglichkeit hinzugefügt, "NO_TLSv1.1" aus der Liste der Verschlüsselungsoptionen zu wählen:
  - Verschlüsselung= ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:RSA+AESGCM:RSA+AES:HIGH:!3DES:!aNULL:!MD5:!DSS:!MD5:!aNULL:!EDH:!RC4

flightPATHs

- X-Content-Type-Options - fügen Sie diesen Header hinzu, wenn er nicht vorhanden ist, und setzen Sie ihn auf "nosniff" - verhindert, dass der Browser automatisch "MIME-Sniffing" betreibt.
- X-Frame-Options - fügen Sie diesen Header hinzu, wenn er nicht vorhanden ist, und setzen Sie ihn auf "SAMEORIGIN" - Seiten auf Ihrer Website können in Frames eingebunden werden, aber nur auf anderen Seiten innerhalb derselben Website.
- X-XSS-Protection - fügen Sie diesen Header hinzu, falls er nicht vorhanden ist, und setzen Sie ihn auf "1; mode=block" - aktivieren Sie den Browser-Cross-Site-Scripting-Schutz
- Strict-Transport-Security - fügen Sie den Header hinzu, falls er nicht vorhanden ist, und setzen Sie ihn auf "max-age=31536000 ; includeSubdomains" - stellt sicher, dass der Client alle Links als HTTPs:// für die max-age anerkennen sollte

Anlegen eines jetPACKs

Sie können jedes jetPACK in beliebiger Reihenfolge anwenden, aber achten Sie darauf, dass Sie kein jetPACK mit der gleichen virtuellen IP-Adresse verwenden. Diese Aktion wird eine doppelte IP-Adresse in der Konfiguration verursachen. Wenn Sie dies versehentlich tun, können Sie dies in der GUI ändern.

- Navigieren Sie zu Erweitert > Software aktualisieren
- Abschnitt Konfiguration
- Neue Konfiguration oder jetPACK hochladen
- Suche nach jetPACK
- Klicken Sie auf Hochladen
- Sobald der Browser-Bildschirm weiß wird, klicken Sie bitte auf Aktualisieren und warten Sie, bis die Dashboard-Seite erscheint

Erstellen eines jetPACKs

Eines der großartigen Dinge an jetPACK ist, dass Sie Ihre eigenen erstellen können. Es kann sein, dass Sie die perfekte Konfiguration für eine Anwendung erstellt haben und diese unabhängig für mehrere andere Boxen verwenden möchten.

- Beginnen Sie mit dem Kopieren der aktuellen Konfiguration von Ihrem bestehenden ALB-X
  - Erweitert
  - Software aktualisieren
  - Aktuelle Konfiguration herunterladen
- Bearbeiten Sie diese Datei mit Notepad++
- Öffnen Sie ein neues txt-Dokument und nennen Sie es "ihrname-jetPACK1.txt".

- Kopieren Sie alle relevanten Abschnitte aus der Konfigurationsdatei in "yourname-jetPACK1.txt"
- Nach Fertigstellung speichern

WICHTIG: Jedes jetPACK ist in verschiedene Abschnitte unterteilt, aber alle jetPACKs müssen #!jetpack oben auf der Seite haben.

Die Abschnitte, die zum Bearbeiten/Kopieren empfohlen werden, sind unten aufgeführt.

Abschnitt 0:

```
#!jetpack
```

Diese Zeile muss sich am Anfang des jetPACKs befinden, da sonst Ihre aktuelle Konfiguration überschrieben wird.

Abschnitt1:

```
[jetnexusdaemon]
```

Dieser Abschnitt enthält globale Einstellungen, die, sobald sie geändert werden, für alle Dienste gelten. Einige dieser Einstellungen können über die Webkonsole geändert werden, andere sind nur hier verfügbar.

Beispiele:

```
ConnectionTimeout=600000
```

Dieses Beispiel ist der TCP-Timeout-Wert in Millisekunden. Diese Einstellung bedeutet, dass eine TCP-Verbindung nach 10 Minuten der Inaktivität geschlossen wird

```
ContentServerCustomTimer=20000
```

Dieses Beispiel ist die Verzögerung in Millisekunden zwischen Content-Server-Zustandsprüfungen für benutzerdefinierte Monitore wie DICOM

```
jnCookieHeader="MS-WSMAN"
```

In diesem Beispiel wird der Name des Cookie-Headers, der beim persistenten Lastausgleich verwendet wird, vom Standard "jnAccel" in "MS-WSMAN" geändert. Diese spezielle Änderung wird für Lync 2010/2013 Reverse Proxy benötigt.

Abschnitt 2:

```
[jetnexusdaemon-Csm-Regeln]
```

Dieser Abschnitt enthält die benutzerdefinierten Server-Überwachungsregeln, die hier typischerweise über die Web-Konsole konfiguriert werden.

Beispiel:

```
[jetnexusdaemon-Csm-Rules-0]
Inhalt="Server hoch"
Desc="Monitor 1″
Method="CheckResponse"
Name="Gesundheitsprüfung - Ist der Server in Betrieb"
Url="HTTP://demo.jetneus.com/healthcheck/healthcheck.html"
```

Abschnitt 3:

```
[jetnexusdaemon-LocalInterface]
```

Dieser Abschnitt enthält alle Details aus dem Abschnitt IP-Dienste. Jede Schnittstelle ist nummeriert und enthält Unterschnittstellen für jeden Kanal. Wenn auf Ihren Kanal eine flightPATH-Regel angewendet wurde, enthält er auch einen Abschnitt Pfad.

Beispiel:

[jetnexusdaemon-LocalInterface1]

1.1=”443″

1.2=”104″

1.3=”80″

1.4=”81″

Aktiviert=1

Netmask="255.255.255.0″

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

[jetnexusdaemon-LocalInterface1.1]

1=">,""Sichere Gruppe"",2000,"

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

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

AdresseAuflösung=0

CachePort=0

CertificateName="default"

ClientCertificateName="No SSL"

Komprimieren=1

ConnectionLimiting=0

DSR=0

DSRProto="tcp"

Aktiviert=1

LoadBalancePolicy="CookieBased"

MaxVerbindungen=10000

MonitoringPolicy="1″

PassThrough=0

Protocol="HTTP beschleunigen"

ServiceDesc="Secure Servers VIP"

SNAT=0

SSL=1

SSLClient=0

SSLInternalPort=27400

[jetnexusdaemon-LocalInterface1.1-Path]

1=”6″

Abschnitt 4:

[jetnexusdaemon-Pfad]

Dieser Abschnitt enthält alle flightPATH-Regeln. Die Nummern müssen mit dem übereinstimmen, was auf die Schnittstelle angewendet wurde. Im obigen Beispiel sehen wir, dass die flightPATH-Regel "6" auf den Kanal angewandt wurde, auch dies als Beispiel unten.

Beispiel:

[jetnexusdaemon-Pfad-6]

Desc="Erzwingen, dass HTTPS für ein bestimmtes Verzeichnis verwendet wird"

Name="Gary - HTTPS erzwingen"

[jetnexusdaemon-Pfad-6-Bedingung-1]

Check="contain"

Bedingung="Pfad"

Spiel=

Sense="tut"

Value="/sicher/"

[jetnexusdaemon-Pfad-6-Evaluate-1]

Detail=

Quelle="host"

Wert=

Variable="$host$"[jetnexusdaemon-Path-6-Function-1]

Action="redirect"

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

Wert=

Einführung in flightPATH

Was ist flightPATH?

flightPATH ist eine intelligente Regel-Engine, die von Edgenexus entwickelt wurde, um den HTTP- und HTTPS-Verkehr zu manipulieren und zu routen. Sie ist hochgradig konfigurierbar, sehr leistungsfähig und dennoch sehr einfach zu bedienen.

Obwohl einige Komponenten von flightPATH IP-Objekte sind, wie z. B. Source IP, kann flightPATH nur auf einen **Diensttyp** gleich HTTP angewendet werden. Wenn Sie einen anderen Diensttyp wählen, dann ist die Registerkarte flightPATH in IP-Dienste leer.

Eine flightPATH-Regel hat drei Komponenten:

Option	Beschreibung
Zustand	Legen Sie mehrere Kriterien zum Auslösen der flightPATH-Regel fest.
Auswertung	Erlaubt die Verwendung von Variablen, die im Aktionsbereich verwendet werden können.
Aktion	Das Verhalten, sobald die Regel ausgelöst wurde.

Was kann flightPATH tun?

flightPATH kann verwendet werden, um den Inhalt und die Anfragen von eingehenden und ausgehenden HTTP(s) zu ändern.

Neben der Verwendung von einfachen String-Matches wie z.B. "Beginnt mit" und "Endet mit" kann auch eine vollständige Steuerung über leistungsfähige Perl-kompatible reguläre Ausdrücke (RegEx) implementiert werden.

Mehr über RegEx erfahren Sie auf dieser hilfreichen Seite https://www.regexbuddy.com/regex.html

Darüber hinaus können benutzerdefinierte Variablen erstellt und im Aktionsbereich verwendet werden, was viele verschiedene Möglichkeiten ermöglicht.

Zustand

Zustand	Beschreibung	Beispiel
<form>	HTML-Formulare werden verwendet, um Daten an einen Server zu übergeben	Beispiel "form doesn't have length 0"
GEO-Standort	Dies vergleicht die Quell-IP-Adresse mit dem ISO 3166 Country Code	GEO Standort ist gleich GB ODER GEO Standort ist gleich Deutschland
Host	Dies ist der aus der URL extrahierte Host	www.mywebsite.com oder 192.168.1.1
Sprache	Dies ist die Sprache, die aus dem HTTP-Header language extrahiert wurde	Diese Bedingung erzeugt ein Dropdown-Menü mit einer Liste von Sprachen
Methode	Dies ist eine Auswahlliste der HTTP-Methoden	Dies ist eine Auswahlliste, die GET, POST usw. enthält
Herkunft IP	Wenn der Upstream-Proxy X-Forwarded-for (XFF) unterstützt, verwendet er die wahre Ursprungsadresse	Client-IP. Kann auch mehrere IPs oder Subnetze verwenden. 10\.1\.2\.* ist 10.1.2.0 /24 Subnetz10\ .1\.2\.3|10\.1\.2\.4 Verwenden Sie | für mehrere IP's

Pfad	Dies ist der Pfad der Website	/meinewebsite/index.asp
POST	POST-Anforderungsmethode	Prüfen von Daten, die auf eine Website hochgeladen werden
Abfrage	Dies ist der Name und der Wert einer Abfrage, da er entweder den Abfragenamen oder auch einen Wert annehmen kann	"Best=jetNEXUS" Wo die Übereinstimmung Best ist und der Wert edgeNEXUS ist
Abfrage-String	Die gesamte Abfragezeichenfolge nach dem Zeichen ?	
Cookie anfordern	Dies ist der Name eines Cookies, der von einem Client angefordert wird	MS-WSMAN=afYfn1CDqqCDqUD::
Kopfzeile anfordern	Dies kann ein beliebiger HTTP-Header sein	Referrer, Benutzer-Agent, Von, Datum
Version anfordern	Dies ist die HTTP-Version	HTTP/1.0 ODER HTTP/1.1
Antwort Körper	Eine benutzerdefinierte Zeichenfolge im Antwortkörper	Server AUF
Antwort-Code	Der HTTP-Code für die Antwort	200 OK, 304 Nicht modifiziert
Antwort Cookie	Dies ist der Name eines vom Server gesendeten Cookies	MS-WSMAN=afYfn1CDqqCDqUD::
Antwort-Kopfzeile	Dies kann ein beliebiger HTTP-Header sein	Referrer, Benutzer-Agent, Von, Datum
Antwort Version	Die vom Server gesendete HTTP-Version	HTTP/1.0 ODER HTTP/1.1
Quelle IP	Dies ist entweder die Ursprungs-IP, die Proxy-Server-IP oder eine andere zusammengefasste IP-Adresse	ClientIP , Proxy IP, Firewall IP. Kann auch mehrere IPs und Subnetze verwenden. Sie müssen die Punkte escapen, da diese RegEX sind. Beispiel 10.1.1\.2\.3 ist 10.1.2.3

Spiel	**Beschreibung**	**Beispiel**
Akzeptieren	Zulässige Content-Typen	Akzeptieren: text/plain
Accept-Encoding	Akzeptierte Kodierungen	Accept-Encoding: <compress | gzip | deflate | sdch | identity>
Accept-Language	Akzeptierte Sprachen für die Antwort	Accept-Language: en-US
Accept-Ranges	Welche partiellen Inhaltsbereichstypen dieser Server unterstützt	Accept-Ranges: bytes
Autorisierung	Anmeldeinformationen für die HTTP-Authentifizierung	Berechtigung: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Charge-To	Enthält Kontoinformationen für die Kosten der Anwendung der angeforderten Methode	

Content-Encoding	Die Art der Kodierung, die für die Daten verwendet wird.	Inhalt-Encoding: gzip
Inhalt-Länge	Die Länge des Antwortkörpers in Oktetten (8-Bit-Bytes)	Inhalt-Länge: 348
Inhalt-Typ	Der Mime-Typ des Body der Anfrage (wird bei POST- und PUT-Anfragen verwendet)	Inhalt-Typ: application/x-www-form-urlencoded
Keks	Ein HTTP-Cookie, das zuvor vom Server mit Set-Cookie (unten) gesendet wurde	Cookie: $Version=1; Skin=new;
Datum	Datum und Uhrzeit, zu der die Nachricht erstellt wurde	Datum = "Datum" ":" HTTP-Datum
ETag	Ein Bezeichner für eine bestimmte Version einer Ressource, oft ein Message Digest	ETag: "aed6bdb8e090cd1:0"
Von	Die E-Mail-Adresse des Benutzers, der die Anfrage stellt	Von: user@example.com
Wenn-geändert-seit	Ermöglicht die Rückgabe eines 304 Not Modified, wenn der Inhalt unverändert ist	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Zuletzt geändert	Das Datum der letzten Änderung für das angeforderte Objekt, im RFC 2822-Format	Zuletzt geändert: Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Die implementierungsspezifischen Header können an jeder Stelle der Anfrage-Antwort-Kette verschiedene Auswirkungen haben.	Pragma: no-cache
Referrer	Dies ist die Adresse der vorherigen Webseite, von der aus ein Link zu der aktuell angeforderten Seite verfolgt wurde	Referrer: HTTP://www.edgenexus.io
Server	Ein Name für den Server	Server: Apache/2.4.1 (Unix)
Set-Cookie	Ein HTTP-Cookie	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
Benutzer-Agent	Der User-Agent-String des Benutzer-Agenten	Benutzer-Agent: Mozilla/5.0 (kompatibel; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Variieren Sie	Sagt Downstream-Proxys, wie sie zukünftige Anfrage-Header abgleichen sollen, um zu entscheiden, ob die zwischengespeicherte Antwort verwendet werden kann, anstatt eine neue vom Ursprungsserver anzufordern	Vary: User-Agent
X-Powered-By	Gibt die Technologie (z. B. ASP.NET, PHP, JBoss) an, die die Web-Anwendung unterstützt	X-Powered-By: PHP/5.4.0

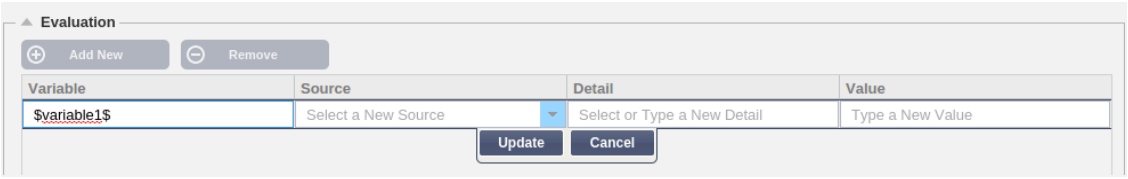
Prüfen Sie	**Beschreibung**	**Beispiel**
Existieren	Dabei spielt es keine Rolle, wie die Bedingung im Detail aussieht, sondern nur, dass sie existiert/nicht existiert	Host - Existiert - Existieren

Start	Die Zeichenkette beginnt mit dem Wert	Pfad - Tut - Start - /sicher
Ende	Die Zeichenkette endet mit dem Wert	Pfad - Tut - Ende - .jpg
Enthält	Die Zeichenkette enthält den Wert	Anfrage-Header - Akzeptieren - Enthält - Bild
Gleiche	Die Zeichenkette ist gleich dem Wert	Host - Tut - Gleich - www.jetnexus.com
Länge haben	Die Zeichenkette hat die Länge des Wertes	Host - Hat - Länge - 16www.jetnexus.com = TRUEwww.jetnexus.co.uk = FALSE
RegEx abgleichen	Damit können Sie einen vollständigen Perl-kompatiblen regulären Ausdruck eingeben	Herkunfts-IP - Entspricht - Regex - 10\..* | 11\..*

Beispiel

- Das Beispiel hat zwei Bedingungen, und **BEIDE** müssen erfüllt sein, um die Aktion auszuführen
- Die erste ist die Überprüfung, ob das angeforderte Objekt ein Bild ist
- Die zweite ist die Suche nach einem bestimmten Hostnamen

Auswertung



Das Hinzufügen einer Variable ist eine überzeugende Funktion, die es Ihnen ermöglicht, Daten aus der Anfrage zu extrahieren und sie in den Aktionen zu verwenden. Sie könnten z. B. einen Benutzernamen protokollieren oder eine E-Mail senden, wenn es ein Sicherheitsproblem gibt.

- Variable: Diese muss mit einem $-Symbol beginnen und enden. Zum Beispiel $variable1$
- Quelle: Wählen Sie aus der Dropdown-Box die Quelle der Variable aus
- Detail: Wählen Sie aus der Liste, wenn relevant. Wenn die Quelle=Request Header ist, könnten die Details User-Agent sein
- Wert: Geben Sie den Text oder den regulären Ausdruck zur Feinabstimmung der Variablen ein.

Eingebaute Variablen:

- Eingebaute Variablen sind bereits fest kodiert, so dass Sie für diese keinen Auswertungseintrag erstellen müssen.
- Sie können jede der unten aufgeführten Variablen in Ihrer Aktion verwenden
- Die Erklärung für jede Variable finden Sie in der Tabelle "Bedingung" oben
    - Methode = $Methode$
    - Pfad = $Pfad$
    - Querystring = $querystring$
    - Quellip = $sourceip$
    - Antwort-Code (Text auch "200 OK") = $resp$

  - Host = $host$
  - Version = $version$
  - Clientport = $clientport$
  - Clientip = $clientip$
  - Geolocation = $geolocation$"

Beispiel Aktion:

- Aktion = Umleitung 302
  - Ziel = HTTPs://$host$/404.html
- Aktion = Loggen
  - Ziel = Ein Client von $sourceip$:$sourceport$ hat soeben eine Anfrage $path$ Seite gestellt

Erläuterung:

- Ein Client, der auf eine Seite zugreift, die nicht existiert, würde normalerweise mit einer 404-Seite des Browsers konfrontiert werden
- In diesem Fall wird der Benutzer zum ursprünglichen Hostnamen, den er verwendet hat, umgeleitet, aber der falsche Pfad wird durch 404.html ersetzt
- Dem Syslog wird ein Eintrag hinzugefügt, der besagt: "Ein Client von 154.3.22.14:3454 hat gerade eine Anfrage an die Seite wrong.html gestellt"

Quelle	Beschreibung	Beispiel
Keks	Dies ist der Name und der Wert des Cookie-Headers	MS-WSMAN=afYfn1CDqqCDqUD::Dabei ist der Name MS-WSMAN und der Wert afYfn1CDqqCDqUD::
Host	Dies ist der aus der URL extrahierte Hostname	www.mywebsite.com oder 192.168.1.1
Sprache	Dies ist die Sprache, die aus dem HTTP-Header Language extrahiert wurde	Diese Bedingung erzeugt ein Dropdown-Menü mit einer Liste von Sprachen.
Methode	Dies ist eine Auswahlliste der HTTP-Methoden	Die Auswahlliste enthält GET, POST
Pfad	Dies ist der Pfad der Website	/meinewebsite/index.html
POST	POST-Anforderungsmethode	Prüfen von Daten, die auf eine Website hochgeladen werden
Abfrage-Element	Dies ist der Name und der Wert einer Abfrage. Als solches kann es entweder den Abfragenamen oder auch einen Wert akzeptieren	"Best=jetNEXUS" Wo die Übereinstimmung Best ist und der Wert edgeNEXUS ist
Abfrage-String	Dies ist die gesamte Zeichenkette nach dem Zeichen ?	HTTP://server/path/program?query_string
Kopfzeile anfordern	Dies kann jeder vom Client gesendete Header sein	Referrer, User-Agent, Von, Datum...
Antwort-Kopfzeile	Dies kann ein beliebiger Header sein, der vom Server gesendet wird	Referrer, User-Agent, Von, Datum...
Version	Dies ist die HTTP-Version	HTTP/1.0 oder HTTP/1.1

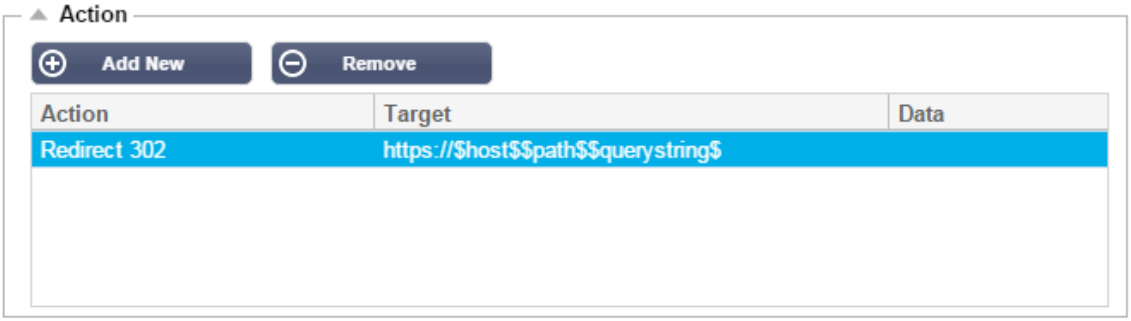
Detail	Beschreibung	Beispiel
Akzeptieren	Zulässige Content-Typen	Akzeptieren: text/plain

Accept-Encoding	Akzeptierte Kodierungen	Accept-Encoding: <compress | gzip | deflate | sdch | identity>
Accept-Language	Akzeptierte Sprachen für die Antwort	Accept-Language: en-US
Accept-Ranges	Welche partiellen Inhaltsbereichstypen dieser Server unterstützt	Accept-Ranges: bytes
Autorisierung	Anmeldeinformationen für die HTTP-Authentifizierung	Berechtigung: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Charge-To	Enthält Kontoinformationen für die Kosten der Anwendung der angeforderten Methode	
Content-Encoding	Die Art der Kodierung, die für die Daten verwendet wird.	Inhalt-Encoding: gzip
Inhalt-Länge	Die Länge des Antwortkörpers in Oktetten (8-Bit-Bytes)	Inhalt-Länge: 348
Inhalt-Typ	Der Mime-Typ des Body der Anfrage (wird bei POST- und PUT-Anfragen verwendet)	Inhalt-Typ: application/x-www-form-urlencoded
Keks	ein HTTP-Cookie, das zuvor vom Server mit Set-Cookie (unten) gesendet wurde	Cookie: $Version=1; Skin=new;
Datum	Datum und Uhrzeit, zu der die Nachricht erstellt wurde	Datum = "Datum" ":" HTTP-Datum
ETag	Ein Bezeichner für eine bestimmte Version einer Ressource, oft ein Message Digest	ETag: "aed6bdb8e090cd1:0"
Von	Die E-Mail-Adresse des Benutzers, der die Anfrage stellt	Von: user@example.com
Wenn-geändert-seit	Ermöglicht die Rückgabe eines 304 Not Modified, wenn der Inhalt unverändert ist	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Zuletzt geändert	Das Datum der letzten Änderung für das angeforderte Objekt, im RFC 2822-Format	Zuletzt geändert: Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Implementierungsspezifische Header, die an jeder Stelle der Anfrage-Antwort-Kette verschiedene Auswirkungen haben können.	Pragma: no-cache
Referrer	Dies ist die Adresse der vorherigen Webseite, von der aus ein Link zur aktuell angeforderten Seite verfolgt wurde	Referrer: HTTP://www.edgenexus.io
Server	Ein Name für den Server	Server: Apache/2.4.1 (Unix)
Set-Cookie	ein HTTP-Cookie	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
Benutzer-Agent	Der User-Agent-String des Benutzer-Agenten	Benutzer-Agent: Mozilla/5.0 (kompatibel; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Variieren Sie	Sagt Downstream-Proxys, wie sie zukünftige Anfrage-Header abgleichen sollen, um zu entscheiden, ob	Vary: User-Agent

	die zwischengespeicherte Antwort verwendet werden kann, anstatt eine neue vom Ursprungsserver anzufordern	
X-Powered-By	Gibt die Technologie (z. B. ASP.NET, PHP, JBoss) an, die die Web-Anwendung unterstützt	X-Powered-By: PHP/5.4.0

Aktion

Die Aktion ist die Aufgabe oder die Aufgaben, die aktiviert werden, sobald die Bedingung oder die Bedingungen erfüllt sind.



Aktion

Doppelklicken Sie auf die Spalte Aktion, um die Dropdown-Liste anzuzeigen.

Ziel

Doppelklicken Sie auf die Spalte Ziel, um die Dropdown-Liste anzuzeigen. Die Liste ändert sich abhängig von der Aktion.

Bei einigen Aktionen können Sie auch manuell tippen.

Daten

Doppelklicken Sie auf die Spalte Daten, um Ihre Daten, die Sie hinzufügen oder ersetzen möchten, manuell hinzuzufügen.

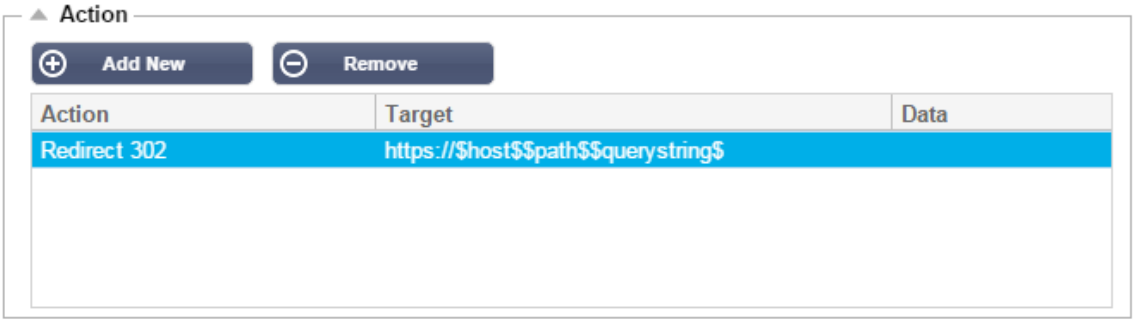
Die Liste aller Aktionen ist unten detailliert aufgeführt:

Aktion	Beschreibung	Beispiel
Anfrage Cookie hinzufügen	Fügen Sie ein Anfrage-Cookie hinzu, das im Abschnitt Ziel mit einem Wert im Abschnitt Daten angegeben ist	Ziel= Cookie Daten= MS-WSMAN=afYfn1CDqqCDqCVii
Anfrage-Kopfzeile hinzufügen	Fügen Sie einen Anfrage-Header vom Typ Target mit einem Wert im Abschnitt Data hinzu	Ziel= Akzeptieren Daten= image/png
Antwort-Cookie hinzufügen	Fügen Sie das Antwort-Cookie, das im Abschnitt Ziel angegeben ist, mit dem Wert im Abschnitt Daten hinzu	Ziel= Cookie Daten= MS-WSMAN=afYfn1CDqqCDqCVii
Antwort-Kopfzeile hinzufügen	Fügen Sie den Abfrage-Header detailliert im Abschnitt Ziel mit dem Wert im Abschnitt Daten hinzu	Ziel= Cache-Kontrolle Daten= max-age=8888888

Körper Alle ersetzen	Durchsuchen Sie den Antwortkörper und ersetzen Sie alle Instanzen	Ziel= HTTP:// (Suchbegriff) Data= HTTPs:// (Ersetzungszeichenfolge)
Körper Ersetzen Sie zuerst	Suchen Sie im Antwortkörper und ersetzen Sie nur die erste Instanz	Ziel= HTTP:// (Suchbegriff) Data= HTTPs:// (Ersetzungszeichenfolge)
Körper Ersetzen Letzte	Den Antwortkörper durchsuchen und nur die letzte Instanz ersetzen	Ziel= HTTP:// (Suchbegriff) Data= HTTPs:// (Ersetzungszeichenfolge)
Ablegen	Dadurch wird die Verbindung getrennt	Ziel= N/A Daten= N/A
e-Mail	Sendet eine E-Mail an die in E-Mail-Ereignisse konfigurierte Adresse. Sie können eine Variable als Adresse oder die Nachricht verwenden	Target= "flightPATH hat dieses Ereignis gemailt" Daten= N/A
Ereignis protokollieren	Dadurch wird ein Ereignis im Systemprotokoll aufgezeichnet	Target= "flightPATH hat dies im Syslog protokolliert" Daten= N/A
Umleitung 301	Dadurch wird eine permanente Umleitung ausgegeben	Ziel= HTTP://www.edgenexus.ioData= N/A
Umleitung 302	Dadurch wird eine temporäre Umleitung ausgegeben	Ziel= HTTP://www.edgenexus.ioData= N/A
Anfrage-Cookie entfernen	Entfernen Sie das Anfrage-Cookie, das im Abschnitt Ziel beschrieben ist	Ziel= Cookie Daten= MS-WSMAN=afYfn1CDqqCDqCVii
Anfrage-Kopfzeile entfernen	Entfernen Sie den im Abschnitt "Ziel" beschriebenen Anfragekopf	Ziel=ServerDaten=N/A
Antwort-Cookie entfernen	Antwort-Cookie entfernen, wie im Abschnitt Ziel beschrieben	Ziel=jnAccel
Antwort-Header entfernen	Entfernen Sie den Antwort-Header, der im Abschnitt Ziel beschrieben ist	Ziel= Etag Daten= N/A
Anfrage Cookie ersetzen	Ersetzen Sie das im Abschnitt Ziel angegebene Anfrage-Cookie durch den Wert im Abschnitt Daten	Ziel= Cookie Daten= MS-WSMAN=afYfn1CDqqCDqCVii
Anforderungs-Kopfzeile ersetzen	Abfragekopf im Ziel durch Datenwert ersetzen	Ziel= Verbindung Daten= keep-alive
Antwort-Cookie ersetzen	Ersetzen Sie das Antwort-Cookie, das im Abschnitt Ziel angegeben ist, durch den Wert im Abschnitt Daten	Ziel=jnAccel=afYfn1CDqqCDqCViiDatum=MS-WSMAN=afYfn1CDqqCDqCVii
Antwort-Header ersetzen	Ersetzen Sie den im Abschnitt Ziel angegebenen Antwort-Header durch den Wert im Abschnitt Daten	Ziel= Server Daten= Aus Sicherheitsgründen vorenthalten
Pfad umschreiben	Dies ermöglicht Ihnen, die Anfrage auf eine neue URL umzuleiten, die auf der Bedingung	Ziel= /test/path/index.html$querystring$ Daten= N/A

Sicheren Server verwenden	Wählen Sie, welchen sicheren Server oder virtuellen Dienst Sie verwenden möchten	Target=192.168.101: 443Data=N/A
Server verwenden	Wählen Sie, welchen Server oder virtuellen Dienst Sie verwenden möchten	Ziel= 192.168.101:80Daten= N/A
Cookie verschlüsseln	Damit werden Cookies 3DES-verschlüsselt und anschließend base64-kodiert	Target= Geben Sie den zu verschlüsselnden Cookie-Namen ein, Sie können den * als Platzhalter am Ende verwendenData= Geben Sie eine Passphrase für die Verschlüsselung ein

Beispiel:



Die folgende Aktion leitet den Browser vorübergehend zu einem sicheren virtuellen HTTPS-Dienst um. Es wird derselbe Hostname, Pfad und Querystring wie bei der Anfrage verwendet.

Häufige Verwendungen

Anwendungsfirewall und Sicherheit

- Unerwünschte IPs blockieren
- Benutzer für bestimmte (oder alle) Inhalte zu HTTPS zwingen
- Spider blockieren oder umleiten
- Verhindern und Warnen vor Cross-Site-Scripting
- Verhindern und Warnen vor SQL-Injection
- Interne Verzeichnisstruktur ausblenden
- Cookies umschreiben
- Sicheres Verzeichnis für bestimmte Benutzer

Eigenschaften

- Benutzer basierend auf Pfad umleiten
- Bieten Sie Single Sign On über mehrere Systeme hinweg
- Benutzer anhand von Benutzer-ID oder Cookie segmentieren
- Header für SSL-Offload hinzufügen
- Spracherkennung
- Benutzeranforderung umschreiben
- Fehlerhafte URLs korrigieren
- Protokoll und E-Mail-Warnung 404-Antwortcodes
- Verhindern des Verzeichniszugriffs/-durchsuchens
- Senden Sie Spidern andere Inhalte

Vorgefertigte Regeln

HTML-Erweiterung

Ändert alle .htm-Anfragen in .html

Zustand:

- Bedingung = Pfad
- Sense = Tut
- Prüfen = RegEx abgleichen
- Wert = \.htm$

Auswertung:

- Leer

Aktion:

- Aktion = Pfad umschreiben
- Ziel = $Pfad$l

Index.html

Erzwingt die Verwendung von index.html bei Anfragen an Ordner.

Bedingung: diese Bedingung ist eine allgemeine Bedingung, die auf die meisten Objekte passt

- Bedingung = Host
- Sense = Tut
- Prüfen = Vorhanden

Auswertung:

- Leer

Aktion:

- Aktion = Umleitung 302
- Ziel = HTTP://$host$$pfad$index.html$querystring$

Ordner schließen

Verweigern Sie Anfragen zu Ordnern.

Bedingung: diese Bedingung ist eine allgemeine Bedingung, die auf die meisten Objekte passt

- Bedingung = dies muss gut überlegt sein
- Sinn =
- Prüfen =

Auswertung:

- Leer

Aktion:

- Aktion =
- Ziel =

CGI-BBIN ausblenden:

Blendet den cgi-bin-Katalog in Anfragen an CGI-Skripte aus.

Bedingung: diese Bedingung ist eine allgemeine Bedingung, die auf die meisten Objekte passt

- Bedingung = Host
- Sense = Tut
- Prüfen = RegEX abgleichen
- Wert = \.cgi$

Auswertung:

- Leer

Aktion:

- Aktion = Pfad umschreiben
- Ziel = /cgi-bin$pfad$

Log Spider

Loggen Sie Spider-Anfragen beliebter Suchmaschinen.

Bedingung: diese Bedingung ist eine allgemeine Bedingung, die auf die meisten Objekte passt

- Bedingung = Anfrage-Kopfzeile
- Übereinstimmung = Benutzer-Agent
- Sense = Tut
- Prüfen = RegEX abgleichen
- Wert = Googlebot|Slurp|bingbot|ia_archiver

Auswertung:

- Variable = $Crawler$
- Quelle = Anfrage-Kopfzeile
- Detail = Benutzer-Agent

Aktion:

- Aktion = Ereignis protokollieren
- Ziel = [$crawler$] $host$$pfad$$querystring$

HTTPS erzwingen

Erzwingt die Verwendung von HTTPS für ein bestimmtes Verzeichnis. Wenn ein Client in diesem Fall auf etwas zugreift, das das Verzeichnis /secure/ enthält, wird er auf die HTTPs-Version der angeforderten URL umgeleitet.

Zustand:

- Bedingung = Pfad
- Sense = Tut
- Prüfen = Enthalten
- Wert = /sicher/

Auswertung:

- Leer

Aktion:

- Aktion = Umleitung 302
- Ziel = HTTPs://$host$$pfad$$querystring$

Media Stream:

Leitet den Flash Media Stream an den entsprechenden Dienst um.

Zustand:

- Bedingung = Pfad
- Sense = Tut
- Prüfen = Ende
- Wert = .flv

Auswertung:

- Leer

Aktion:

- Aktion = Umleitung 302
- Ziel = HTTP://$host$:8080/$path$

HTTP auf HTTPS umstellen

Ändern Sie alle hartcodierten HTTP:// in HTTPS://

Zustand:

- Bedingung = Antwort-Code
- Sense = Tut
- Prüfen = Gleich
- Wert = 200 OK

Auswertung:

- Leer

Aktion:

- Aktion = Körper Alle ersetzen
- Ziel = HTTP://
- Daten = HTTPs://

Kreditkarten ausblenden

Prüfen Sie, dass keine Kreditkarten in der Antwort vorhanden sind, und wenn eine gefunden wird, löschen Sie sie.

Zustand:

- Bedingung = Antwort-Code
- Sense = Tut
- Prüfen = Gleich
- Wert = 200 OK

Auswertung:

- Leer

Aktion:

- Aktion = Körper Alle ersetzen
- 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]+
- Daten = xxxx-xxxx-xxxx-xxxx

Inhalt Verfall

Fügen Sie der Seite ein sinnvolles Ablaufdatum für den Inhalt hinzu, um die Anzahl der Anfragen und 304s zu reduzieren.

Bedingung: Dies ist eine generische Bedingung als Auffanglösung. Es wird empfohlen, diese Bedingung auf Ihre

- Bedingung = Antwort-Code
- Sense = Tut
- Prüfen = Gleich
- Wert = 200 OK

Auswertung:

- Leer

Aktion:

- Aktion = Antwort-Kopfzeile hinzufügen
- Ziel = Cache-Kontrolle
- Daten = max-age=3600

Spoof-Server-Typ

Holen Sie sich den Servertyp und ändern Sie ihn in etwas anderes.

Bedingung: Dies ist eine generische Bedingung als Auffanglösung. Es wird empfohlen, diese Bedingung auf Ihre

- Bedingung = Antwort-Code
- Sense = Tut
- Prüfen = Gleich
- Wert = 200 OK

Auswertung:

- Leer

Aktion:

- Aktion = Antwort-Kopfzeile ersetzen
- Ziel = Server
- Daten = Geheim

Niemals Fehler senden

Der Kunde erhält keine Fehler von Ihrer Seite.

Zustand

- Bedingung = Antwort-Code
- Sense = Tut
- Prüfen = Enthalten
- Wert = 404

Auswertung

- Leer

Aktion

- Aktion = Umleitung 302
- Ziel = HTTP//$host$/

Umleitung auf Sprache

Suchen Sie den Sprachcode und leiten Sie auf die entsprechende Länderdomain um.

Zustand

- Bedingung = Sprache
- Sense = Tut
- Prüfen = Enthalten
- Wert = Deutsch (Standard)

Auswertung

- Variable = $host_template$
- Quelle = Host
- Wert = .*\.

Aktion

- Aktion = Umleitung 302
- Ziel = HTTP//$host_template$de$path$$querystring$

Google Analytics

Fügen Sie den von Google geforderten Code für die Analytik ein - Bitte ändern Sie den Wert MYGOOGLECODE in Ihre Google UA ID.

Zustand

- Bedingung = Antwort-Code
- Sense = Tut
- Prüfen = Gleich
- Wert = 200 OK

Auswertung

- leer

Aktion

- Aktion = Körper Ersetzen Letzte
- Ziel = </body>
- Daten = <scripttype= 'text/javascript'> var _gaq = _gaq || []; _gaq.push(['_setAccount', 'MY GOOGLE CODE']); _gaq.push(['_trackPageview']); (function() { var ga = document.createElement('script'); ga.type =

'text/javascript'; ga.async = true; ga.src = ('HTTPs' == document.location.protocol ?'HTTPs//ssl' 'HTTP//www') + '.google-analytics.com/ga.js'; var s = document.getElementsByTagName('script')[0];s.parentNode.insertBefore(ga, s); })(); </script> </body>

IPv6-Gateway

Host-Header für IIS IPv4-Server bei IPv6-Diensten anpassen. IIS-IPv4-Server mögen es nicht, eine IPV6-Adresse in der Host-Client-Anfrage zu sehen, daher ersetzt diese Regel diese durch einen generischen Namen.

Zustand

- leer

Auswertung

- leer

Aktion

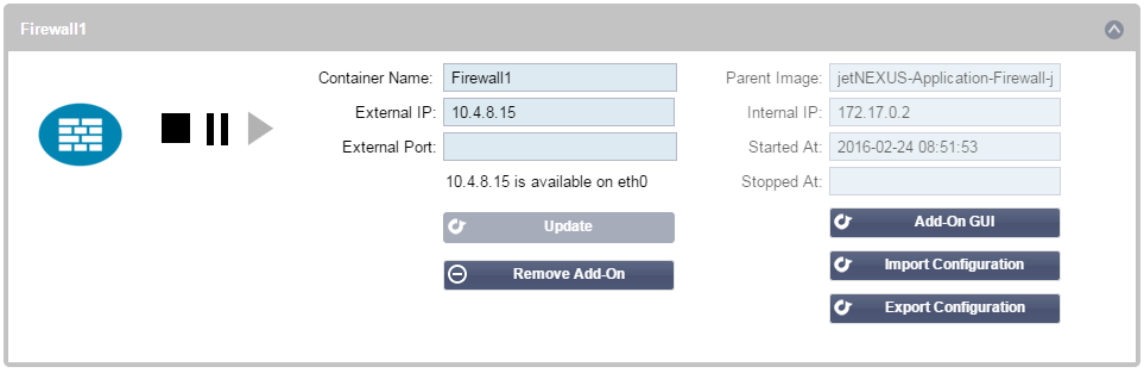
- Aktion = Anfrage-Header ersetzen
- Ziel = Host
- Daten =ipv4.host.header

Web Application Firewall (edgeWAF)

Die Web Application Firewall (WAF) ist auf Anfrage erhältlich und wird auf jährlicher kostenpflichtiger Basis lizenziert. Die Installation der WAF erfolgt über den eingebauten Apps-Bereich innerhalb des ADC.

Ausführen der WAF

Da die WAF in einem Docker-Container läuft, müssen vor dem Start einige Netzwerkparameter eingestellt werden.

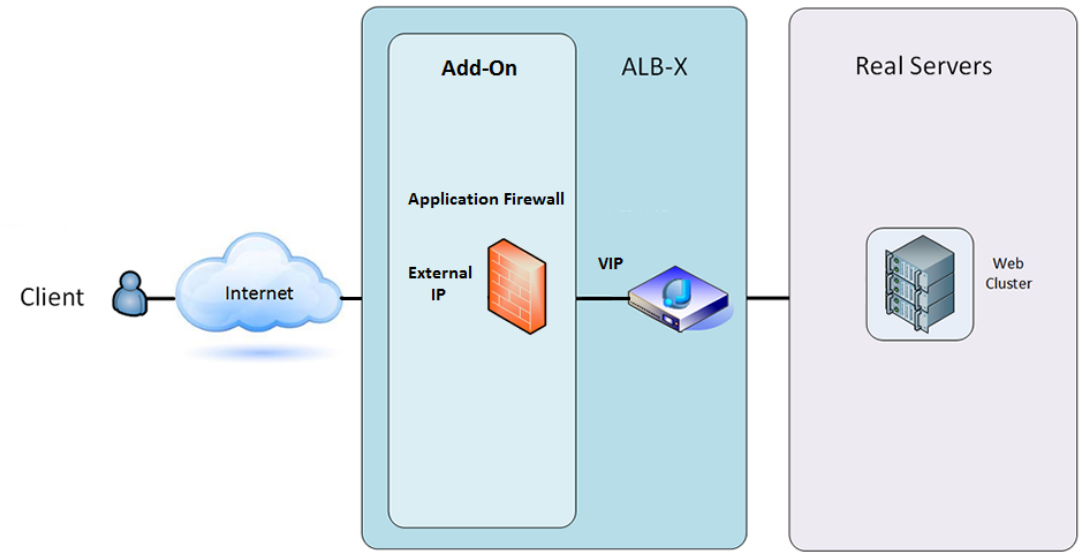


Option	Beschreibung
Stopp	Sie ist ausgegraut, bis eine Add-On-Instanz gestartet wird. Drücken Sie diese Schaltfläche, um die Docker-Instanz zu stoppen.
Pause	Mit dieser Schaltfläche wird das Add-On angehalten.
Spielen	Es wird das Add-On mit den aktuellen Einstellungen gestartet.
Container-Name	Geben Sie Ihrem Container einen Namen, um ihn von den anderen Containern zu unterscheiden. Dieser muss eindeutig sein. Sie können diesen Namen als Namen für einen Real-Server verwenden, wenn Sie möchten, und er wird automatisch in die interne IP-Adresse der Instanz aufgelöst
Externe IP	Hier können Sie eine externe IP für den Zugriff auf Ihr Add-On einstellen. Dies kann sowohl für den Zugriff auf die GUI des Add-Ons als auch für den Dienst sein, der über das Add-On läuft. Im Fall des Firewall-Add-Ons ist dies die IP-Adresse Ihres HTTP-Dienstes. Die Firewall kann dann so konfiguriert werden, dass sie auf einen Server oder ein ALB-X-VIP zugreift, das mehrere Server für den Lastausgleich enthält.
Externer Anschluss	Wenn Sie dies leer lassen, werden alle Ports an Ihre Firewall weitergeleitet. Um dies einzuschränken, fügen Sie einfach die kommagetrennte Portliste ein. Beispiel 80, 443, 88. Beachten Sie, dass die Firewall-GUI-Adresse **HTTP//[Externe IP]88/waf** sein wird**.** Lassen Sie also entweder die Einstellung "Externer Port" leer oder fügen Sie Port 88 ein, um auf die GUI zuzugreifen, wenn Sie die Portliste einschränken.
Update	Sie können die Einstellungen eines Add-Ons nur aktualisieren, wenn es gestoppt wurde. Sobald Ihre Instanz gestoppt ist, können Sie die Einstellungen für den Containernamen, die externe IP und den externen Port ändern.
Add-On entfernen	Entfernt das Add-On vollständig von der Add-On-Seite. Sie müssen auf die Seite Library-Apps gehen, um das Add-On erneut einzusetzen.
Übergeordnetes Bild	Gibt das Docker-Image an, aus dem das Add-On erstellt wird. Es kann mehrere Versionen einer Firewall oder einer anderen Art von Add-On geben, so dass dies hilft, sie zu unterscheiden. Dieser Abschnitt dient nur zu Informationszwecken und ist daher ausgegraut.

Interne IP	Docker erstellt die interne IP-Adresse automatisch und kann daher nicht bearbeitet werden. Wenn Sie die Docker-Instanz anhalten und neu starten, wird eine neue interne IP-Adresse ausgegeben. Aus diesem Grund sollten Sie entweder eine externe IP-Adresse für Ihren Dienst verwenden oder Sie verwenden den Containernamen für die reale Serveradresse Ihres Dienstes.
Gestartet bei	Hier wird das Datum und die Uhrzeit angegeben, zu der das Add-On gestartet wurde. Beispiel 2016-02-16 155721
Gestoppt bei	Hier wird das Datum und die Uhrzeit angegeben, zu der das Add-On gestoppt wurde. Beispiel 2016-02-24 095839

Beispiel Architektur

WAF mit externer IP-Adresse

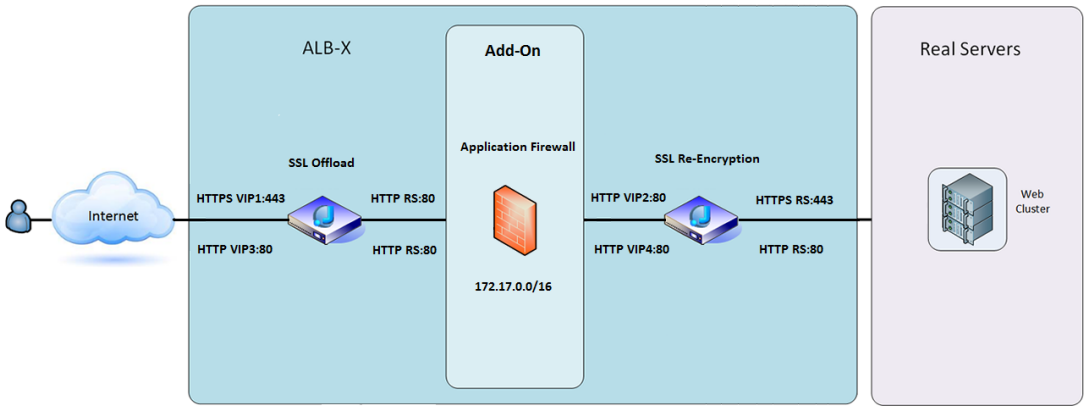


In dieser Architektur kann nur HTTP für Ihren Dienst verwendet werden, da die Firewall keinen HTTPS-Verkehr inspizieren kann.

Die Firewall muss so konfiguriert werden, dass sie den Datenverkehr an das ALB-X-VIP weiterleitet.

Der ALB-X VIP wiederum wird so konfiguriert, dass er den Datenverkehr zu Ihrem Web-Cluster ausgleicht.

WAF mit interner IP-Adresse



In dieser Architektur können Sie HTTP und HTTPS angeben.

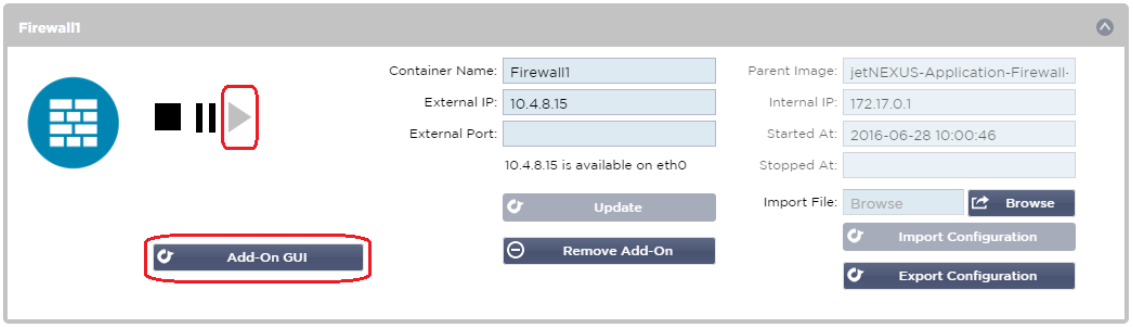
HTTPS kann End-to-End sein, wobei die Verbindungen vom Client zum ALB-X und vom ALB-X zu den Real-Servern verschlüsselt werden.

Der Verkehr vom ALB-X zur internen IP-Adresse der Firewall muss unverschlüsselt sein, damit er inspiziert werden kann.

Sobald der Datenverkehr die Firewall passiert hat, wird er an ein anderes VIP weitergeleitet, das dann entweder den Datenverkehr neu verschlüsseln und einen Lastausgleich zu sicheren Servern oder einfach einen Lastausgleich zu unsicheren Servern über HTTP durchführen kann.

Zugriff auf Ihr WAF-Add-on

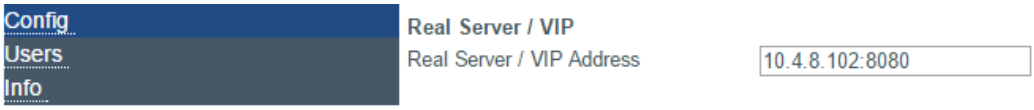
- Füllen Sie die Details für Ihre Firewall aus
- Sie können die Ports entweder auf das beschränken, was Sie benötigen, oder das Feld leer lassen, um alle Ports zuzulassen
- Klicken Sie auf die Schaltfläche Abspielen
- Eine Add-On-GUI-Schaltfläche wird angezeigt



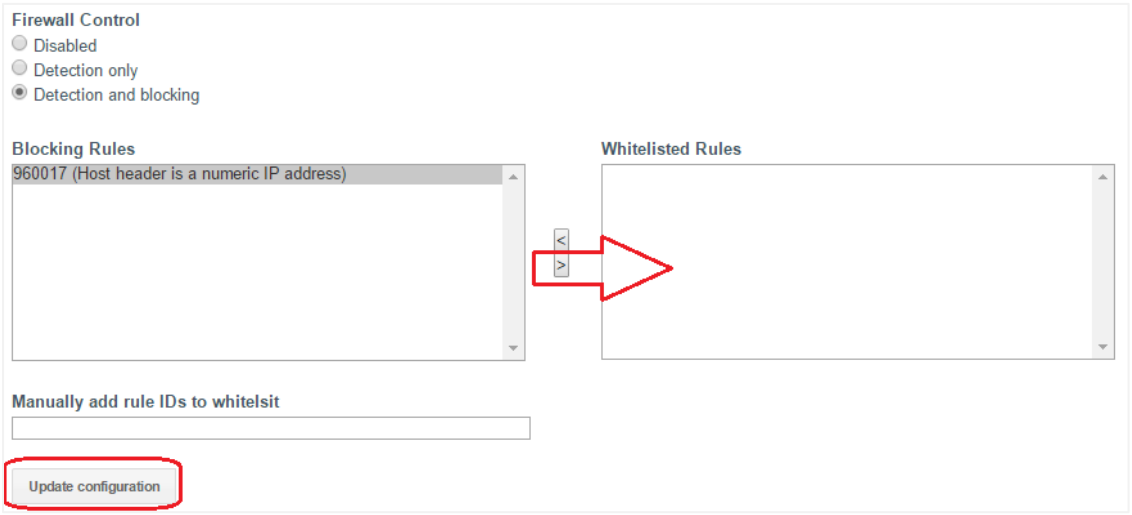
- Klicken Sie auf diese Schaltfläche, und es öffnet sich ein Browser auf HTTP://[Externe IP]:88/waf
- In diesem Beispiel wird es HTTP://10.4.8.15:88/waf sein
- Es wird ein Anmeldedialog angezeigt.
- Geben Sie die Anmeldeinformationen für Ihren ADC ein.
- Nach einer erfolgreichen Anmeldung wird Ihnen die Startseite der WAF angezeigt.

- Die Startseite zeigt eine grafische Übersicht über die Ereignisse, d. h. die von der Application Firewall durchgeführten Filteraktionen.

- Die Diagramme werden beim ersten Öffnen der Seite höchstwahrscheinlich leer sein, da es keine Zugriffsversuche durch die Firewall gibt.
- Sie können die IP-Adresse oder den Domainnamen der Website konfigurieren, an die Sie den Datenverkehr senden möchten, nachdem die Firewall ihn gefiltert hat.
- Dies kann im Bereich Verwaltung > Konfig geändert werden



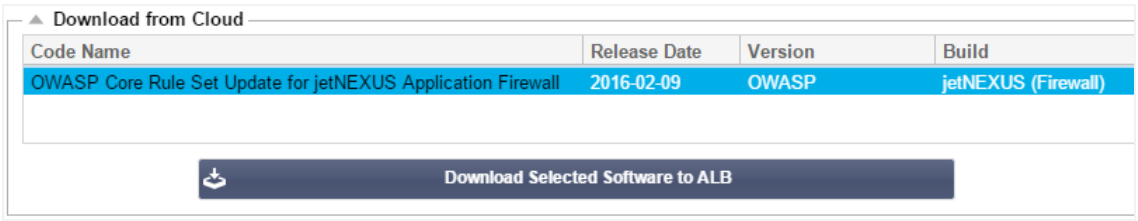
- Die Firewall prüft den Datenverkehr und sendet ihn dann an die hier angegebene Real-Sever-IP oder VIP-Adresse. Sie können auch einen Port zusammen mit Ihrer IP-Adresse eingeben. Wenn Sie eine IP-Adresse allein eingeben, wird der Port als Port 80 angenommen. Klicken Sie auf die Schaltfläche "Konfiguration aktualisieren", um diese neue Einstellung zu speichern.
- Wenn die Firewall eine Anwendungsressource blockiert, erscheint die Regel, die den Datenverkehr blockiert, in der Liste Blockierungsregeln auf der Seite Whitelist.
- Um zu verhindern, dass die Firewall die gültige Anwendungsressource blockiert, verschieben Sie die blockierende Regel bitte in den Bereich Whitelist-Regeln.



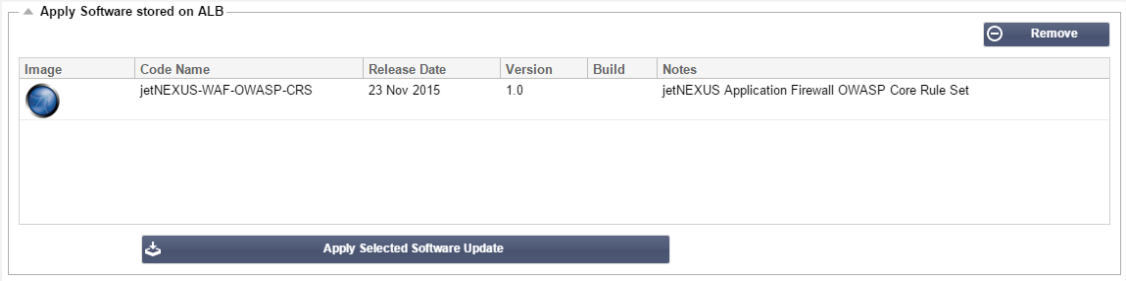
- Drücken Sie auf Konfiguration aktualisieren, wenn Sie alle Regeln aus dem Bereich Blockierung in den Bereich Whitelist übertragen haben.

Regeln aktualisieren

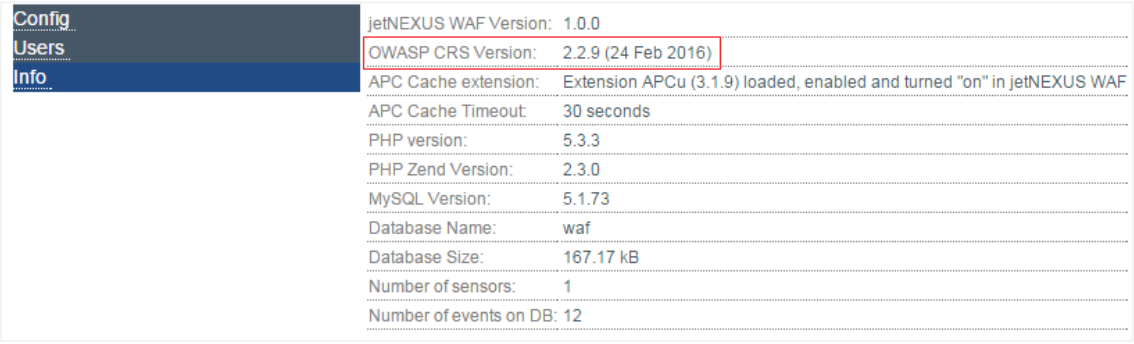
- Die Regeln der Application Firewall können über den Bereich Erweitert - Software aktualisiert werden
- Klicken Sie auf Aktualisieren, um die Schaltfläche für die verfügbare Software im Bereich Software-Upgrade-Details anzuzeigen
- Es wird nun ein zusätzliches Feld mit der Bezeichnung Download from Cloud angezeigt
- Prüfen Sie, ob ein OWASP Core-Regelsatz verfügbar ist



- Wenn dies der Fall ist, können Sie markieren und auf Ausgewählte Software auf ALB-X herunterladen klicken
- Diese Aktion lädt dann die Smart-Datei in die auf dem ALB gespeicherte Apply Software herunter



- Markieren Sie den jetNEXUS-WAF-OWASP-CRS und klicken Sie auf Ausgewähltes Software-Update anwenden und klicken Sie auf Anwenden
- Die Firewall erkennt den aktualisierten Regelsatz automatisch, lädt ihn und wendet ihn an.
- Die IDs von Whitelist-Regeln werden beibehalten. Neue Regeln können jedoch beginnen, gültige Anwendungsressourcen zu blockieren.
- Bitte überprüfen Sie in diesem Fall die Liste der Blockierungsregeln auf der Seite Whitelist.
- Sie können auch im Abschnitt Management Info der Firewall-GUI nach der OWASP CRS-Version suchen



Globaler Server-Lastausgleich (edgeGSLB)

Einführung

Global Server Load Balancing (GSLB) ist ein Begriff, der Methoden zur Verteilung des Netzwerkverkehrs im Internet beschreibt. GSLB unterscheidet sich von Server Load Balancing (SLB) oder Application Load Balancing (ALB), da es typischerweise verwendet wird, um den Datenverkehr zwischen mehreren Rechenzentren zu verteilen, während ein traditionelles ADC/SLB verwendet wird, um den Datenverkehr innerhalb eines einzelnen Rechenzentrums zu verteilen.

GSLB wird typischerweise in den folgenden Situationen verwendet:

Ausfallsicherheit und Disaster Recovery

Sie haben mehrere Rechenzentren und möchten diese in einer Aktiv-Passiv-Situation betreiben, so dass bei einem Ausfall eines Rechenzentrums der Datenverkehr an das andere gesendet wird.

Lastausgleich und Geolokalisierung

Sie möchten den Datenverkehr zwischen den Rechenzentren in einer Aktiv-Aktiv-Situation verteilen, basierend auf bestimmten Kriterien wie der Leistung des Rechenzentrums, der Kapazität des Rechenzentrums, der Überprüfung des Zustands des Rechenzentrums und dem physischen Standort des Clients (damit Sie ihn an das nächstgelegene Rechenzentrum schicken können) usw.

Kommerzielle Überlegungen

Sicherstellen, dass Benutzer von bestimmten geografischen Standorten an bestimmte Datenzentren gesendet werden. Stellen Sie sicher, dass anderen Benutzern unterschiedliche Inhalte serviert (oder blockiert) werden, abhängig von mehreren Kriterien wie dem Land, in dem sich der Client befindet, der angeforderten Ressource, der Sprache usw.

Übersicht über das Domain Name System

GSLB kann komplex sein; daher lohnt es sich, die Zeit zu investieren, um zu verstehen, wie das mysteriöse Domain Name Server (DNS)-System funktioniert.

DNS besteht aus drei Hauptkomponenten:

- Der DNS-Resolver, d. h. der Client: Der Resolver ist für die Initiierung der Abfragen verantwortlich, die letztendlich zu einer vollständigen Auflösung der gewünschten Ressource führen.
- Nameserver: Dies ist der Nameserver, mit dem sich der Client zunächst verbindet, um die DNS-Auflösung durchzuführen.
- Autoritative Nameserver: Umfassen die Nameserver der Top Level Domain (TLD) und die Root-Nameserver.

Eine typische DNS-Transaktion wird im Folgenden erläutert:

- Ein Benutzer tippt "example.com" in einen Webbrowser ein, und die Anfrage wandert ins Internet und wird von einem rekursiven DNS-Resolver empfangen.
- Der Resolver fragt dann einen DNS-Root-Nameserver ab (.).
- Der Root-Server antwortet dem Resolver dann mit der Adresse eines DNS-Servers der Top-Level-Domain (TLD) (z. B. .com oder .net), der die Informationen für seine Domains speichert. Wenn wir nach example.com suchen, wird unsere Anfrage auf die TLD .com gerichtet.
- Der Resolver fordert dann die TLD .com an.
- Der TLD-Server antwortet dann mit der IP-Adresse des Nameservers der Domain, example.com.

- Zum Schluss sendet der rekursive Resolver eine Anfrage an den Nameserver der Domain.
- Die IP-Adresse, z. B..com, wird dann vom Nameserver an den Resolver zurückgegeben.
- Der DNS-Resolver antwortet dann dem Webbrowser mit der IP-Adresse der ursprünglich angeforderten Domain.
- Sobald die acht Schritte des DNS-Lookups die IP-Adresse, z. B..com, zurückgegeben haben, kann der Browser die Webseite anfordern:
- Der Browser stellt eine HTTP-Anfrage an die IP-Adresse.
- Der Server an dieser IP gibt die Webseite zurück, die im Browser gerendert werden soll.

Dieser Prozess kann weiter verkompliziert werden:

Caching

Auflösende Nameserver, die Antworten zwischenspeichern, können die gleiche Antwort an viele Clients senden. Client-seitige Resolver und Anwendungen können unterschiedliche Caching-Richtlinien haben.

Hinweis: Zum Testen stoppen und deaktivieren wir den Windows DNS-Client im Bereich Dienste Ihres Betriebssystems. Die DNS-Namen werden weiterhin aufgelöst, allerdings werden die Ergebnisse nicht zwischengespeichert und der Name des Computers wird nicht registriert. Ihr Systemadministrator muss entscheiden, ob dies die beste Option für Ihre Umgebung ist, da es sich auf andere Dienste auswirken kann.

Zeit zu leben

Der auflösende Nameserver kann die Time To Live (TTL), d. h. die Zwischenspeicherzeit für die Antwort, ignorieren.

GSLB Übersicht

GSLB basiert auf DNS und verwendet einen sehr ähnlichen Mechanismus wie oben beschrieben.

Die ADC kann die Antwort basierend auf mehreren Faktoren ändern, die später in der Anleitung beschrieben werden. Die ADC nutzt die Monitore, die die Verfügbarkeit von Remote-Ressourcen prüfen, indem sie auf die Ressource selbst zugreifen. Um jedoch eine Logik anzuwenden, muss das System zuerst die DNS-Anfrage erhalten.

Dies ist auf mehrere Arten möglich. Das erste ist, dass der GSLB als autoritativer Nameserver fungiert.

Das zweite Design ist die häufigste Implementierung und ähnelt der autoritativen Nameserver-Konfiguration, verwendet aber eine Subdomain. Der primäre autoritative DNS-Server wird nicht durch GSLB ersetzt, sondern delegiert eine Sub-Domäne für die Auflösung. Durch die direkte Delegierung von Namen oder die Verwendung von CNAMEs können Sie steuern, was von der GSLB behandelt wird und was nicht. In diesem Fall müssen Sie nicht den gesamten DNS-Verkehr für Systeme, die keinen GSLB benötigen, an den GSLB weiterleiten.

Es ist eine Redundanz vorgesehen, so dass bei einem Ausfall eines Nameservers (GSLB) der entfernte Nameserver automatisch eine weitere Anfrage an einen anderen GSLB stellt und so verhindert, dass die Website ausfällt.

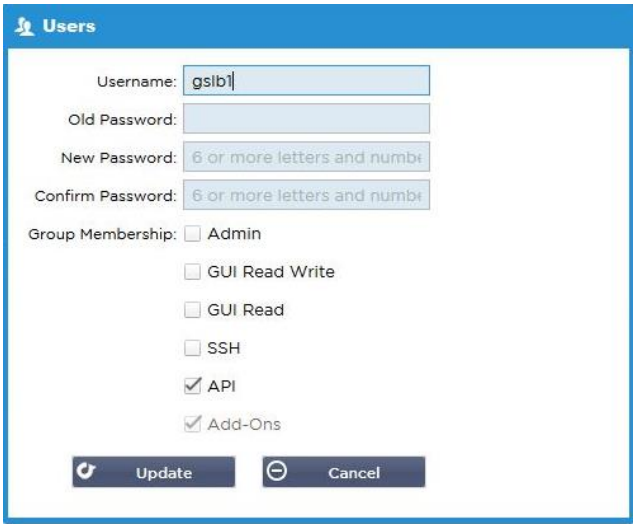
GSLB-Konfiguration

Nachdem Sie das GSLB-Add-On heruntergeladen haben, stellen Sie es bereit, indem Sie die Seite "Library > Apps" der ADC-GUI besuchen und auf die Schaltfläche "Deploy" klicken, wie unten gezeigt.

Nach der Installation konfigurieren Sie bitte die GSLB-Add-On-Details, einschließlich Containername, Externe IP und Externe Ports auf der Seite Bibliothek > Add-Ons der ADC-GUI, wie in der Abbildung unten gezeigt.

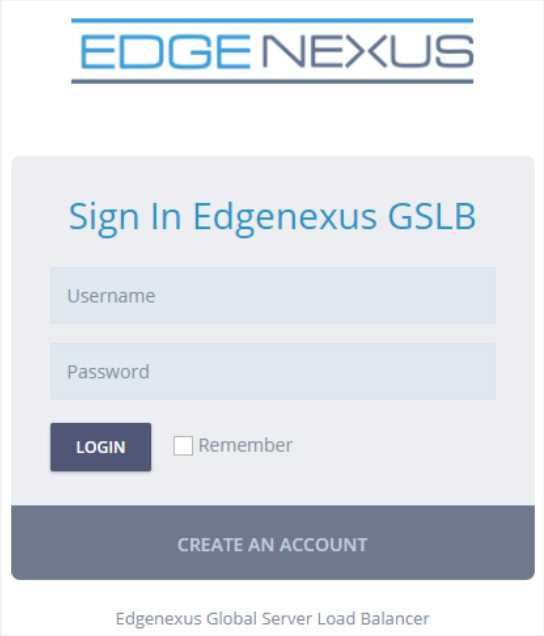
- Container Name ist ein eindeutiger Name einer laufenden Add-On-Instanz, die von ADC gehostet wird, er wird verwendet, um mehrere Add-Ons derselben Art zu unterscheiden.
- Externe IP ist die IP in Ihrem Netzwerk, die dem GSLB zugewiesen wird.
- Sie müssen den GSLB so konfigurieren, dass er eine externe IP-Adresse hat, wenn Sie GEO-basierte Entscheidungen treffen wollen, da dies dem GSLB ermöglicht, die echte IP-Adresse des Clients zu sehen.
- Externe Ports ist die Liste der TCP- und UDP-Ports des GSLB, auf die von anderen Netzwerkhosts zugegriffen werden kann.
- Bitte geben Sie "53/UDP, 53/TCP, 9393/TCP" in das Eingabefeld Externe Ports ein, um die Kommunikation mit DNS (53/UDP, 53/TCP) und edgeNEXUS GSLB GUI (9393/TCP) zu ermöglichen.
- Nachdem Sie die Add-On-Details konfiguriert haben, klicken Sie bitte auf die Schaltfläche Aktualisieren.
- Starten Sie das GSLB-Add-On, indem Sie auf die Schaltfläche Ausführen klicken.

- Der nächste Schritt besteht darin, dass das edgeNEXUS GSLB Add-On die ADC-Konfiguration lesen und ändern kann.
- Bitte besuchen Sie die Seite System > Benutzer der ADC GUI und bearbeiten Sie einen Benutzer mit dem gleichen Namen wie das GSLB Add-On, das Sie eingesetzt haben, wie in der Abbildung unten gezeigt.
- Bearbeiten Sie den Benutzer "gslb1" und setzen Sie ein Häkchen bei API, dann klicken Sie auf Aktualisieren - in späteren Versionen der Software ist das Häkchen möglicherweise bereits standardmäßig gesetzt.



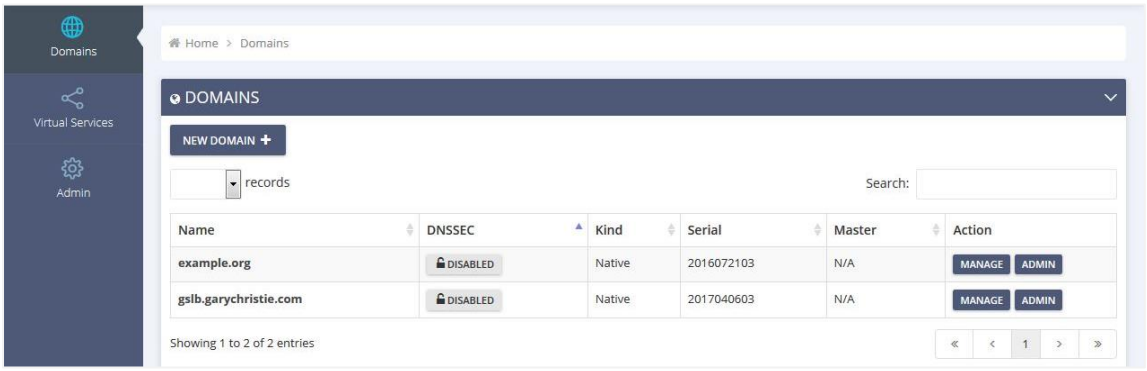
- Der nächste Schritt ist nur erforderlich, wenn Sie GSLB zu Test- oder Evaluierungszwecken konfigurieren und keine DNS-Zonendaten im Internet ändern wollen.
- In diesem Fall weisen Sie bitte den ADC an, GSLB Add-On als primären DNS-Auflösungsserver zu verwenden, indem Sie "DNS Server 1" auf der Seite "System > Netzwerk" der ADC-GUI ändern, wie in der Abbildung unten gezeigt.
- DNS-Server 2 kann generell mit Ihrem lokalen DNS-Server oder einem im Internet konfiguriert werden, z. B. Google 8.8.8.8.

- Jetzt ist es an der Zeit, sich bei GSLB GUI anzumelden.
- Bitte navigieren Sie zur Seite Bibliothek > Add-Ons der ADC-GUI und klicken Sie auf die Schaltfläche Add-On GUI.
- Wenn Sie darauf klicken, wird eine neue Browser-Registerkarte geöffnet, die die GSLB-GUI-Anmeldeseite präsentiert, wie unten gezeigt.

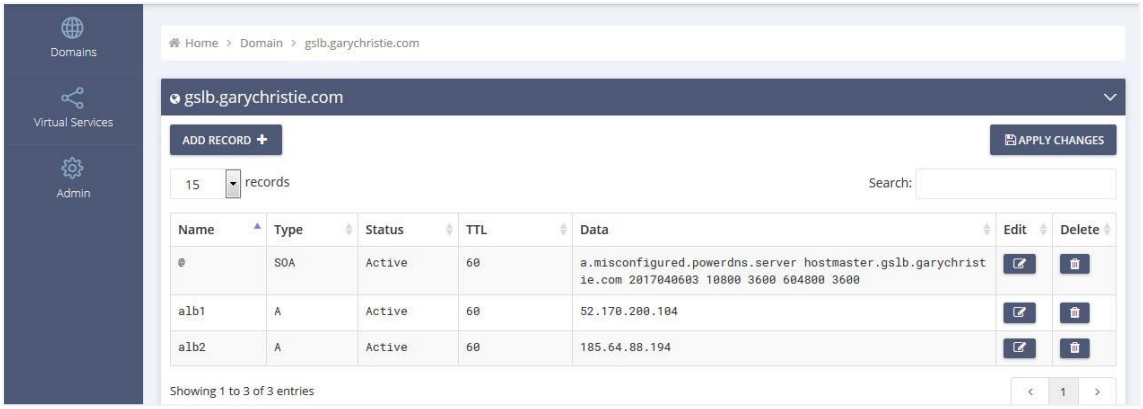


- Der Standard-Benutzername ist admin, und das Standard-Passwort ist jetnexus. Bitte vergessen Sie nicht, Ihr Passwort auf der Seite Administrator > Mein Profil der GSLB-GUI zu ändern.
- Der nächste Schritt in der Konfigurationssequenz besteht darin, eine DNS-Zone im PowerDNS-Nameserver zu erstellen, der ein Teil von GSLB ist. Dadurch wird er entweder zu einem autoritativen Nameserver für die Zone "example.org" oder zu einer Subdomain-Zone, wie z. B. die im Abschnitt "DNS-basierte GSLB-Übersicht" oben erwähnte Subdomain "geo.example.org".
- Ausführliche Details zur Konfiguration von DNS-Zonen finden Sie in der **PowerDNS Nameserver-Dokumentation**. Eine Beispielzone ist in Abbildung 6 dargestellt.

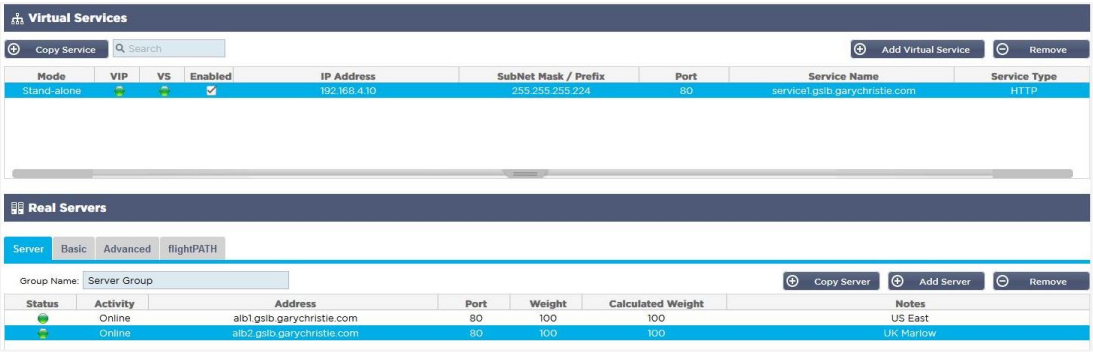
* edgeNEXUS GSLB GUI basiert auf dem Open Source Projekt PowerDNS-Admin.



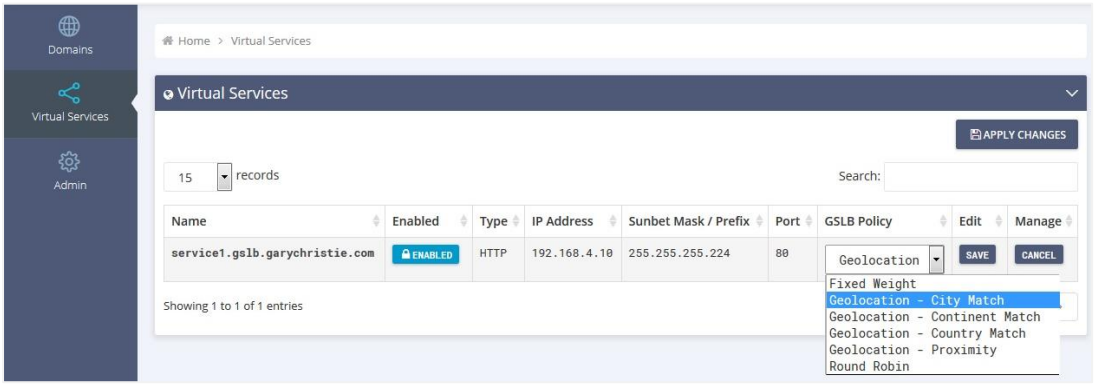
- Nachdem Sie eine DNS-Zone erstellt haben, klicken Sie bitte auf die Schaltfläche Verwalten und fügen der Domain Hostnamen hinzu, wie in der Abbildung unten gezeigt.
- Nachdem Sie bestehende Datensätze innerhalb der GSLB-GUI bearbeitet haben, drücken Sie bitte die Schaltfläche Speichern.
- Nachdem Sie das Erstellen von Hostnamen-Einträgen abgeschlossen haben, klicken Sie bitte auf die Schaltfläche Änderungen übernehmen. Wenn Sie nicht auf Übernehmen klicken und dann die Seite ändern, gehen Ihre Änderungen verloren.
- Im Folgenden haben wir Datensätze erstellt, die IPv4-Adresseinträge sind.
- Bitte stellen Sie sicher, dass Sie einen Datensatz für alle Datensätze erstellen, die Sie aufgelöst haben möchten, einschließlich AAAA-Datensätze für IPv6-Adressen.



- Gehen wir nun zurück zur ADC-GUI und definieren einen virtuellen Dienst, der der soeben erstellten DNS-Zone entspricht.



- Der virtuelle Dienst wird für die Zustandsprüfung der Server in der GSLB-Domäne verwendet.
- Die GSLB nutzt den ADC-Zustandsprüfungsmechanismus, einschließlich benutzerdefinierter Monitore. Er kann mit jedem der vom ADC unterstützten Service-Typen verwendet werden.
- Bitte navigieren Sie zur Seite Dienste > IP-Dienste der ADC-GUI und erstellen Sie einen virtuellen Dienst, wie in der Abbildung unten gezeigt.
- Stellen Sie sicher, dass Sie den Dienstnamen mit dem korrekten Domain-Namen konfigurieren, den Sie in der GSLB verwenden möchten. Der GSLB liest dies über die API und füllt automatisch den Abschnitt Virtuelle Dienste in der GSLB-Benutzeroberfläche aus.
- Fügen Sie bitte alle Server in der GSLB-Domäne unter dem Abschnitt Real Servers im obigen Bild hinzu.
- Sie können Server entweder durch ihre Domainnamen oder IP-Adressen angeben.
- Wenn Sie die Domänennamen angeben, werden die auf Ihrem GSLB erstellten Einträge verwendet.
- In den Registern Basis und Erweitert können Sie verschiedene Methoden und Parameter zur Überwachung des Serverzustands auswählen.
- Sie können die Aktivität einiger Server für ein Aktiv-Passiv-Szenario auf Standby setzen.
- Wenn in diesem Fall ein "Online"-Server eine Zustandsprüfung nicht besteht und ein gesunder Standby-Server vorhanden ist, löst Edgenexus EdgeGSLB den Domainnamen in eine Adresse des Standby-Servers auf.
- Einzelheiten zur Konfiguration von **VIRTUELLEN DIENSTEN** finden Sie im Abschnitt **VIRTUELLE DIENSTE**.
- Wechseln wir nun zur GSLB-GUI.
- Navigieren Sie zur Seite Virtuelle Dienste und wählen Sie eine GSLB-Richtlinie für die Domäne der API, die Sie aus dem Abschnitt ADC virtuelle Dienste abgerufen haben.
- Dies ist in der Abbildung unten dargestellt.



- Die GSLB unterstützt die folgenden Richtlinien:

Richtlinie	Beschreibung
Festes Gewicht	Die GSLB wählt den Server mit der höchsten Gewichtung aus (die Servergewichtung kann vom Benutzer zugewiesen werden). In dem Fall, dass

	mehrere Server die höchste Gewichtung haben, wählt der GSLB einen dieser Server nach dem Zufallsprinzip aus.
Gewichtetes Round Robin	Wählen Sie die Server nacheinander, in einer Reihe. Server mit höherer Gewichtung werden häufiger ausgewählt als Server mit niedrigerer Gewichtung.
Geolokalisierung	Nähe - wählen Sie einen Server, der dem Standort des Clients anhand von geografischen Breiten- und Längengraden am nächsten liegt. Server im gleichen Land wie der Client werden bevorzugt, auch wenn sie weiter entfernt sind als Server in Nachbarländern.
Geolokalisierung	Stadtübereinstimmung - wählen Sie einen Server in der gleichen Stadt wie der Client. Wenn es keinen Server in der Stadt des Clients gibt, wählen Sie einen Server im Land des Clients. Wenn es keinen Server im Land des Clients gibt, wählen Sie einen Server auf demselben Kontinent. Wenn dies nicht möglich ist, wählen Sie einen Server, der anhand der geografischen Längen- und Breitengraddaten dem Standort des Clients am nächsten liegt.
Geolokalisierung	Länderabgleich - wählen Sie einen Server im gleichen Land wie der Client. Wenn es keinen Server im gleichen Land gibt, versuchen Sie es mit dem gleichen Kontinent, dann mit dem nächstgelegenen Standort.
Geolokalisierung	Kontinentübereinstimmung - wählen Sie einen Server auf demselben Kontinent wie der Client. Wenn es keinen Server auf demselben Kontinent gibt, versuchen Sie den nächstgelegenen Standort.

- Nachdem Sie eine GSLB-Richtlinie ausgewählt haben, vergessen Sie bitte nicht, auf die Schaltfläche Änderungen übernehmen zu klicken.
- Jetzt können Sie die Details des virtuellen Dienstes überprüfen und anpassen, indem Sie auf die Schaltfläche Verwalten klicken.
- Dadurch wird die unten gezeigte Seite angezeigt.
- Wenn Sie eine der gewichtungsbasierten Richtlinien gewählt haben, müssen Sie eventuell die GSLB-Gewichte des Servers anpassen.
- Wenn Sie eine der geostandortbasierten GSLB-Richtlinien gewählt haben, müssen Sie eventuell geografische Daten für die Server angeben.
- Wenn Sie keine geografischen Daten für die Server angeben, verwendet der GSLB die von der **GeoLite2-Datenbank von MaxMind** bereitgestellten Daten.
- Sie können auf dieser Seite auch den Servernamen, den Port und die Aktivität ändern.
- Diese Änderungen werden mit dem ADC synchronisiert, wenn Sie auf die Schaltfläche "Änderungen übernehmen" klicken.

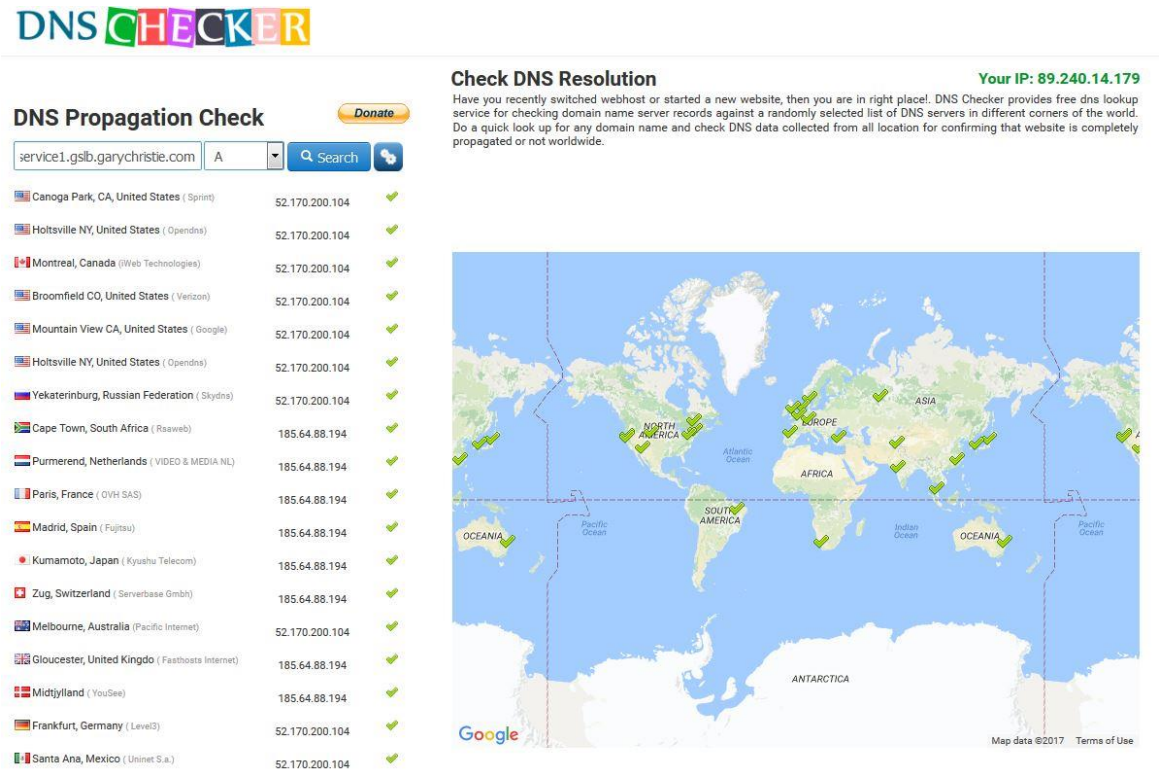
- Eine gute Möglichkeit zu überprüfen, welche Antworten der GSLB an die Clients zurücksendet, ist die Verwendung von NSLOOKUP.
- Wenn Sie Windows verwenden, lautet der Befehl wie folgt.

NSLOOKUP service1.gslb.garychristie.com 192.168.4.10

- Dabei ist service1.gslb.garychristie.com der Domainname, den Sie auflösen möchten.
- Dabei ist 192.168.4.10 die externe IP-Adresse Ihres GSLB.
- Um zu überprüfen, welche IP-Adresse im Internet ausgegeben wird, können Sie den Google-DNS-Server 8.8.8.8 verwenden.

Nslookup service1.gslb.garychristie.com 8.8.8.8.

- Alternativ können Sie auch etwas wie HTTPs://dnschecker.org verwenden. Beispiel HTTPs://dnschecker.org/#A/service1.gslb.garychristie.com.
- Siehe unten für ein Beispiel der Ergebnisse.



Benutzerdefinierte Standorte

Private Netzwerke

Der GSLB kann auch so konfiguriert werden, dass er benutzerdefinierte Standorte verwendet, so dass Sie ihn in internen "privaten" Netzwerken einsetzen können. Im obigen Szenario bestimmt der GSLB den Client-Standort, indem er die öffentliche IP-Adresse des Clients mit einer Datenbank abgleicht, um seinen Standort zu ermitteln. Er ermittelt auch den Standort der Service-IP-Adresse aus derselben Datenbank, und wenn die Lastausgleichsrichtlinie auf eine GEO-Richtlinie eingestellt ist, gibt er die nächstgelegene IP-Adresse zurück. Diese Methode funktioniert perfekt mit öffentlichen IP-Adressen, aber es gibt keine solche Datenbank für interne private Adressen, die mit RFC 1918 für IPv4-Adressen und RFC 4193 für IPv6-Adressen konform sind.

Bitte lesen Sie die Wikipedia-Seite zur Erklärung der privaten Adressierung
HTTPS://DE.WIKIPEDIA.ORG/WIKI/PRIVATE_NETWORK

Wie es funktioniert

Normalerweise ist die Idee hinter der Verwendung unseres GSLB für interne Netzwerke, dass Benutzer von bestimmten Adressen eine unterschiedliche Antwort für einen Dienst erhalten, je nachdem, in welchem Netzwerk sie sich befinden. Betrachten wir also zwei Rechenzentren, Nord und Süd, die einen Dienst

namens north.service1.gslb.com bzw. south.service1.gslb.com anbieten. Wenn ein Benutzer aus dem nördlichen Rechenzentrum eine Anfrage an den GSLB stellt, soll der GSLB mit der IP-Adresse antworten, die mit north.service1.gslb.com verbunden ist, vorausgesetzt, der Dienst funktioniert korrekt. Wenn ein Benutzer aus dem südlichen Rechenzentrum den GSLB abfragt, soll der GSLB wiederum mit der IP-Adresse antworten, die mit south.service1.gslb.com verbunden ist, vorausgesetzt, der Dienst funktioniert korrekt.

Was müssen wir also tun, damit das obige Szenario eintritt?

- Wir benötigen mindestens zwei benutzerdefinierte Standorte, einen für jedes Rechenzentrum
- Weisen Sie die verschiedenen privaten Netzwerke diesen Standorten zu
- Weisen Sie jeden Dienst dem jeweiligen Standort zu

Wie konfigurieren wir dieses Aussehen auf der GSLB?

Hinzufügen eines Standorts für das Northern Data Center

- Klicken Sie auf Benutzerdefinierte Standorte auf der linken Seite
- Klicken Sie auf Standort hinzufügen
- Name
  - Norden
- Fügen Sie eine private IP-Adresse und Subnetzmaske für Ihr nördliches Netzwerk hinzu. Für diese Übung gehen wir davon aus, dass sich die IP-Adressen des Dienstes und des Clients im selben privaten Netzwerk befinden
  - 10.1.1.0/24
- Fügen Sie den Kontinent-Code hinzu
  - EU
- Fügen Sie den Ländercode hinzu
  - UK
- Stadt hinzufügen
  - Enfield
- Breitengrad hinzufügen - erhalten von Google
  - 51.6523
- Längengrad hinzufügen - erhalten von Google
  - 0.0807

Hinweis: Bitte verwenden Sie die korrekten Codes, die Sie hier erhalten können

Hinzufügen eines Standorts für das Southern Data Center

- Klicken Sie auf Benutzerdefinierte Standorte auf der linken Seite
- Klicken Sie auf Standort hinzufügen
- Name
  - Süd
- Fügen Sie eine private IP-Adresse und Subnetzmaske für Ihr Southern-Netzwerk hinzu. Wir nehmen für diese Übung an, dass sich die IP-Adressen des Dienstes und des Clients im selben privaten Netzwerk befinden.
  - 192.168.1.0/24
- Fügen Sie den Kontinent-Code hinzu
  - EU
- Fügen Sie den Ländercode hinzu
  - UK
- Stadt hinzufügen
  - Croydon
- Breitengrad hinzufügen - erhalten von Google
  - 51.3762

- Längengrad hinzufügen - erhalten von Google
    - 0.0982

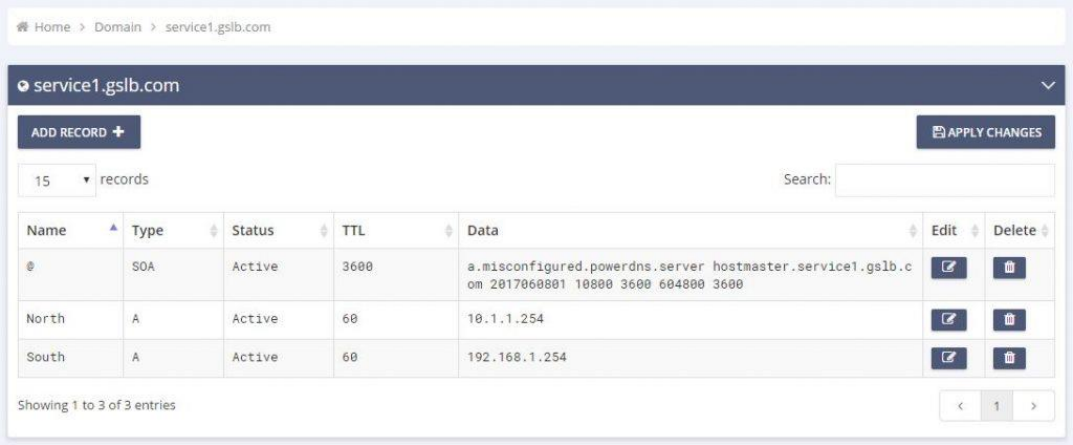
Hinweis: Bitte verwenden Sie die korrekten Codes, die Sie **HIER** erhalten können

Einen A-Eintrag für north.service1.gslb.com hinzufügen

- Klicken Sie auf die Domain service1.gslb.com
- Klicken Sie auf Datensatz hinzufügen
- Name hinzufügen
    - Norden
- Typ
    - A
- Status
    - Aktiv
- TTL
    - 1 Minute
- IP-Adresse
    - 10.1.1.254 (Beachten Sie, dass dies im gleichen Netzwerk wie der Standort Enfield ist)

Einen A-Eintrag für south.service1.gslb.com hinzufügen

- Klicken Sie auf die Domain service1.gslb.com
- Klicken Sie auf Datensatz hinzufügen
- Name hinzufügen
    - Süd
- Typ
    - A
- Status
    - Aktiv
- TTL
    - 1 Minute
- IP-Adresse
    - 192.168.1.254 (Beachten Sie, dass dies im gleichen Netzwerk ist wie der Standort Croydon)



Verkehrsfluss

Beispiel 1 - Client im nördlichen Rechenzentrum

- Client IP 10.1.1.23 fragt GSLB für service1.gslb.com ab
- GSLB sucht die IP-Adresse 10.1.1.23 und gleicht sie mit Custom Location Enfield 10.1.1.0/24 ab
- GSLB schaut sich seine A-Records für service1.gslb.com an und findet north.service1.gslb.com, da es sich ebenfalls im Netzwerk 10.1.1.0/24 befindet
- GSLB antwortet auf 10.1.1.23 mit der IP-Adresse 10.1.1.254 für service1.gslb.com

Beispiel 2 - Client im südlichen Rechenzentrum

- Client IP 192.168.1.23 fragt GSLB für service1.gslb.com ab
- GSLB sucht die IP-Adresse 192.168.1.23 und gleicht sie mit Custom Location Croydon 192.168.1.0/24 ab
- GSLB schaut sich seine A-Records für service1.gslb.com an und findet south.service1.gslb.com, da es sich ebenfalls im Netzwerk 192.168.1.0/24 befindet
- GSLB antwortet auf 192.168.1.23 mit der IP-Adresse 192.168.1.254 für service1.gslb.com

Technische Unterstützung

Wir bieten technischen Support für alle unsere Benutzer gemäß den Standard-Servicebedingungen des Unternehmens.

Wenn Sie einen aktiven Support- und Wartungsvertrag für das edgeADC, das edgeWAF oder das edgeGSLB haben, leisten wir den gesamten Support über den technischen Support.

Um ein Support-Ticket zu erstellen, besuchen Sie bitte:

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