



EdgeADC

ADMINISTRATION GUIDE

Inhalt

Dokumenteneigenschaften	7
Haftungsausschluss für Dokumente	7
Copyrights	7
Markenzeichen	7
Edgenexus Unterstützung	7
Installieren des EdgeADC	8
VMware ESXi	8
Installation der VMXNET3-Schnittstelle	9
Microsoft Hyper-V	9
Citrix XenServer	10
Erste Boot-Konfiguration	12
Erster Start - Manuelle Netzwerkdetails	12
Erster Boot - DHCP erfolgreich	12
Erster Start - DHCP schlägt fehl	12
Ändern der Management-IP-Adresse	13
Ändern der Subnetzmaske für eth0	13
Zuweisen eines Standard-Gateways	13
Überprüfen des Wertes für das Standard-Gateway	13
Zugriff auf die Weboberfläche	13
Befehlsreferenztafel	14
Starten der ADC Web-Konsole	16
Standard-Anmeldeinformationen	16
Das Haupt-Dashboard	17
Dienstleistungen	18
IP-Dienste	18
Virtuelle Dienste	18
Echte Server	25
Bibliothek	39
Add-Ons	39
Apps	39
Kauf eines Add-ons	39
Bereitstellen einer App	40
Authentifizierung	41
Einrichten der Authentifizierung - ein Workflow	41
Authentifizierungsserver	41
Authentifizierungsregeln	42

Single Sign-On.....	43
Formulare	43
Cache.....	45
flightPATH.....	47
Echte Server-Monitore.....	55
Details.....	55
Real Server Monitor Beispiele	58
SSL-Zertifikate	60
Was macht der ADC mit dem SSL-Zertifikat?.....	61
Zertifikat erstellen.....	61
Zertifikat verwalten.....	63
Importieren eines Zertifikats.....	66
Importieren von mehreren Zertifikaten	66
Widgets.....	67
Ansicht.....	74
Armaturenbrett	74
Verwendung des Dashboards.....	74
Geschichte	76
Anzeigen von grafischen Daten.....	76
Logs.....	78
W3C-Protokolle herunterladen.....	78
Statistik	78
Komprimierung	78
Treffer und Verbindungen	79
Zwischenspeichern.....	80
Hardware	80
Status	81
Virtuelle Dienstleistung Details.....	81
System	84
Clustering.....	84
Rolle	84
Einstellungen.....	87
Verwaltung	87
Ändern der Priorität eines ADCs.....	89
Datum und Uhrzeit.....	89
Manuelles Datum und Uhrzeit	89
Datum und Uhrzeit synchronisieren (UTC)	90

E-Mail-Ereignisse	91
Adresse	91
Mail-Server (SMTP)	91
Benachrichtigungen und Alarmer	92
Warnungen	93
Systemgeschichte	93
Daten sammeln.....	93
Wartung	94
Lizenz	94
Lizenz-Details.....	94
Einrichtungen	95
Lizenz installieren.....	96
Loggen.....	96
W3C-Protokollierungsdetails	96
Entfernter Syslog-Server.....	98
Fernspeicherung von Logs.....	98
Log-Dateien löschen.....	101
Netzwerk	101
Grundeinstellung.....	101
Adapter-Details	101
Schnittstellen	102
Kleben.....	103
Statische Route.....	105
Details zur statischen Route	105
Erweiterte Netzwerkeinstellungen.....	105
SNAT	106
Leistung.....	107
Sicherheit	108
SNMP	109
SNMP-Einstellungen.....	109
SNMP-MIB.....	110
MIB herunterladen	110
ADC OID.....	110
Historische Diagramme	111
Benutzer und Audit-Protokolle.....	111
Benutzer	111
Audit-Protokoll	113

Fortgeschrittene	115
Konfiguration	115
Herunterladen einer Konfiguration	115
Hochladen einer Konfiguration	115
Globale Einstellungen.....	116
Host-Cache-Timer.....	116
Abfluss	116
SSL.....	116
Protokoll	116
Server zu stark ausgelastet	116
Weitergeleitet für	117
HTTP-Komprimierungseinstellungen.....	118
Globale Komprimierungsausschlüsse	120
Software.....	120
Details zum Software-Upgrade.....	120
Download aus der Cloud	121
Software auf ALB hochladen	121
Software anwenden, die auf dem ALB gespeichert ist	122
Fehlersuche.....	122
Dateien unterstützen	122
Spurensuche	123
Ping.....	124
Erfassen	124
Was ist ein jetPACK.....	126
Herunterladen eines jetPACKs	126
Microsoft Exchange	126
Microsoft Lync 2010/2013	Error! Bookmark not defined.
Web-Dienste	128
Microsoft Remote Desktop	128
DICOM - Digitale Bildgebung und Kommunikation in der Medizin.....	128
Oracle e-Business Suite	128
VMware Horizon View	128
Globale Einstellungen.....	128
Chiffre-Optionen	128
flightPATHs.....	129
Anlegen eines jetPACKs	129
Erstellen eines jetPACKs.....	129

Einführung in flightPATH	133
Was ist flightPATH?	133
Was kann flightPATH leisten?	133
Zustand	133
Beispiel	136
Auswertung	136
Aktion	139
Aktion.....	139
Ziel	139
Daten	139
Gemeinsame Verwendungen	141
Anwendungsfirewall und Sicherheit.....	141
Eigenschaften	142
Vorgefertigte Regeln	142
HTML-Erweiterung.....	142
Index.html.....	142
Ordner schließen.....	143
CGI-BBIN ausblenden:	143
Log Spider	143
HTTPS erzwingen	144
Media Stream:.....	144
HTTP auf HTTPS umstellen.....	144
Kreditkarten ausblenden	145
Inhalt Verfall	145
Spoof-Server-Typ	146
Web-Anwendungs-Firewall (edgeWAF)	148
Ausführen der WAF	148
Beispiel Architektur	149
WAF mit externer IP-Adresse.....	149
WAF mit interner IP-Adresse.....	150
Zugriff auf Ihr WAF-Add-on	150
Regeln aktualisieren	152
Globaler Server-Lastausgleich (edgeGSLB)	153
Einführung.....	153
Ausfallsicherheit und Disaster Recovery	153
Lastausgleich und Geolokalisierung	153
Kommerzielle Überlegungen.....	153

Überblick über das Domain Name System	153
DNS besteht aus drei Hauptkomponenten:	153
Eine typische DNS-Transaktion wird im Folgenden erläutert:	153
Zwischenspeichern.....	154
Zeit zu leben.....	154
GSLB Übersicht.....	154
GSLB-Konfiguration.....	154
Kundenspezifische Standorte	160
Private Netzwerke.....	160
Wie es funktioniert.....	161
Wie konfigurieren wir dieses Aussehen auf dem GSLB?	161
Verkehrsfluss	163
Technische Unterstützung.....	164

Dokument-Eigenschaften

Dokument-Nummer: 2.0.6.8.21.17.06

Erstellungsdatum des Dokuments: 30. April 2021

Dokument wurde zuletzt bearbeitet: June 8, 2021

Dokument Autor: Jay Savoor

Dokument Zuletzt bearbeitet von:

Dokument Verweis: EdgeADC - Version 4.2.7.1890

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.

Copyrights

© 2021 Alle Rechte vorbehalten.

Die Informationen in diesem Dokument können ohne vorherige Ankündigung geändert werden und stellen keine Verpflichtung seitens des Herstellers dar. Kein Teil dieses Handbuchs darf ohne ausdrückliche schriftliche Genehmigung des Herstellers in irgendeiner Form oder mit irgendwelchen Mitteln, elektronisch oder mechanisch, einschließlich Fotokopien und Aufzeichnungen, für irgendwelche Zwecke vervielfältigt oder übertragen werden. Eingetragene Warenzeichen sind Eigentum der jeweiligen Inhaber. Es wird jede Anstrengung unternommen, dieses Handbuch so vollständig und genau wie möglich zu gestalten, aber es wird keine Garantie für die Eignung übernommen. Die Autoren und der Herausgeber übernehmen keine Verantwortung oder Haftung für Verluste oder Schäden, die durch die Verwendung der in diesem Handbuch enthaltenen Informationen entstehen.

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 des EdgeADC

Das Produkt EdgeADC (von nun an ADC genannt) kann mit verschiedenen Methoden installiert werden. Für jedes Plattformziel ist ein eigenes Installationsprogramm erforderlich, und diese stehen Ihnen alle zur Verfügung.

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 aktuelle 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 aus 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**
- Anschließend werden Ihnen Informationen zum Produkt angezeigt; 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 auf Power > Power-On
- Ihr VA bootet dann, und der ADC-Boot-Bildschirm wird auf der Konsole angezeigt.

```
UXL Software FusionADC

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

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

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

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

Installieren der VMXNET3-Schnittstelle

Der VMXnet3-Treiber wird unterstützt, aber Sie müssen zunächst 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 Installation oder Aktualisierung der VMware-Tools, **sondern** 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 (**beachten Sie die Reihenfolge der NICs in der Liste!**)
3. Löschen Sie beide NICs aus der VM
4. Aktualisieren Sie die VM-Hardware (starten Sie keine Installation oder Aktualisierung der VMware-Tools, sondern führen Sie **nur** das Hardware-Upgrade durch)
5. Fügen Sie zwei NICs hinzu und wählen Sie diese als VMXNET3
6. Stellen Sie die MAC-Adressen für die neuen NICs entsprechend Schritt 2 ein
7. Neustart der VA

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

Microsoft Hyper-V

Die ADC Virtual Appliance ist kompatibel mit der Installation auf einem Microsoft Hyper-V Server.

- Extrahieren Sie die Hyper-V ADC VA-Zip-Datei auf Ihren lokalen Rechner oder Server.
- Öffnen Sie den Hyper-V-Manager.
- Klicken Sie in Ihrem Hyper-V-Manager mit der rechten Maustaste auf den Server und wählen Sie **"Virtuelle Maschine importieren"**.
- Wechseln Sie zu dem Ordner, der die ADC Hyper-V-Dateien enthält.
- Klicken Sie auf **"Kopieren der virtuellen Maschine (Erstellen einer neuen eindeutigen ID)"**
- Aktivieren Sie das Kontrollkästchen **"Alle Dateien duplizieren, damit die gleiche virtuelle Maschine erneut importiert werden kann."**
- Klicken Sie auf **"Importieren"**.
- Ihre Maschine importiert mit dem Namen **"ADC ADC VA für Hyper-V"**.
- Stellen Sie sicher, dass Sie das richtige Netzwerk auf der NIC auswählen
- Wenn Sie mehr als eine virtuelle Appliance installieren, müssen Sie jede Appliance mit einer eindeutigen MAC-Adresse konfigurieren
- Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine, die Sie gerade erstellt haben, und klicken Sie auf **"Verbinden"**.
- Klicken Sie auf die grüne Schaltfläche "Start" oder auf **"ActionStart"**.

- Ihr VA wird hochgefahren, und der Bildschirm der ADC-Konsole wird angezeigt.

```
UXL Software FusionADC

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

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

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

- Sobald Sie die Netzwerkeigenschaften konfiguriert haben, startet die 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 nach der OVA-Datei, wählen Sie diese aus und klicken Sie 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 aus, 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 steht Eth0; 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, in der Regel Netzwerk 0, und belassen 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 **"FINISH"**.
- Ihre VM beginnt mit der Übertragung der virtuellen Festplatte "ADC ADC" und wird nach Abschluss 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.

```
UXL Software FusionADC

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

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

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

_
```

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

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.

```
UXL Software FusionADC

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

Management interface: eth0   MAC: 00:0c:29:5e:eb:62

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

Erster Start - Manuelle Netzwerkdetails

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 unter "[ÄNDERN DER MANAGEMENT-IP-ADRESSE](#)" und die nachfolgenden Abschnitte 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 derzeit 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 Standardgateway 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_
```

Überprüfen des Wertes für das Standard-Gateway

Um zu überprüfen, ob das Standardgateway hinzugefügt wurde und korrekt ist, verwenden Sie den Befehl **route**. Dieser Befehl zeigt die Netzwerkrouen 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 Weboberfläche

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**

Befehlsreferenztablelle

Befehl	Parameter 1	Parameter 2	Beschreibung	Beispiel
Datum			Zeigt das aktuell konfigurierte Datum und die konfigurierte Uhrzeit an	Di 3. Sept. 13:00 UTC 2013
Voreinstellungen			Legen Sie die Werkseinstellungen für Ihr Gerät fest	
Ausgang			Abmelden von der Kommandozeilenschnittstelle	
Hilfe			Zeigt alle gültigen Befehle an	
ifconfig	[leer]		Anzeigen der Schnittstellenkonfiguration für alle Schnittstellen	ifconfig
	eth0		Nur die Schnittstellenkonfiguration von eth0 anzeigen	ifconfig eth0
Maschinennummer			Dieser Befehl liefert die zur Lizenzierung des ADC verwendete machineid	EF4-3A35-F79
kündigen			Abmelden von der Kommandozeilenschnittstelle	
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		Einstellen der Management-IP-Adresse für ADC	set greenside=192.168.101.1
	Maske		Stellen Sie die Subnetzmaske für eine Schnittstelle ein. 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	Protokollmeldungen anzeigen

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

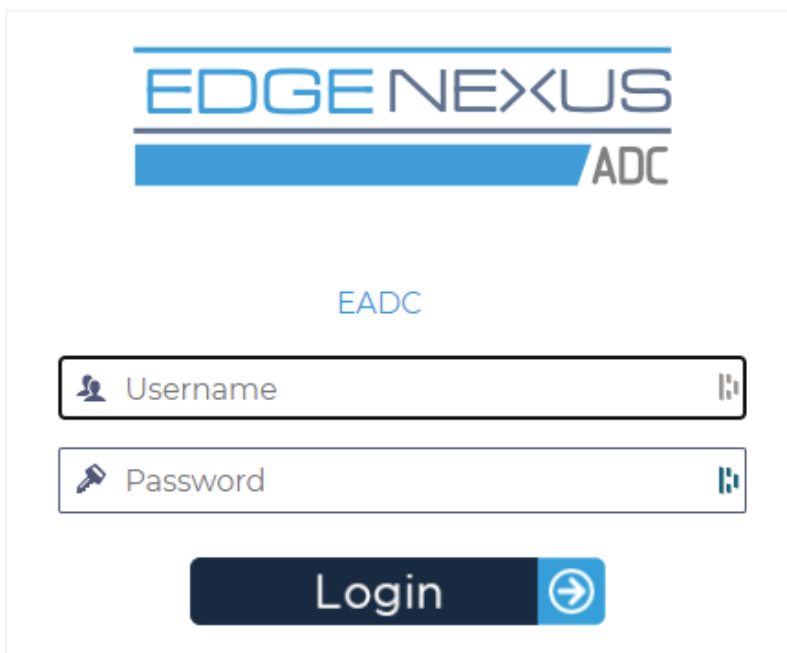
Starten der ADC Web-Konsole

Alle Vorgänge auf dem ADC (auch ADC genannt) werden über die Webkonsole konfiguriert und ausgeführt. Der Zugriff auf die Webkonsole 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 Webkonsole des ADC wie unten abgebildet aus und Sie können sich als Admin-Benutzer anmelden.

The screenshot shows the login page of the EdgeNexus ADC web console. At the top, the logo 'EDGENEXUS' is displayed in a blue, sans-serif font, with 'ADC' in a smaller font to its right. Below the logo, the text 'EADC' is centered. There are two input fields: the first is labeled 'Username' with a user icon on the left and a clear button on the right; the second is labeled 'Password' with a key icon on the left and a clear button on the right. Below these fields is a dark blue 'Login' button with a white right-pointing arrow icon.

Standard-Anmeldeinformationen

Die Standard-Anmeldedaten sind:

- Benutzername: admin
- Kennwort: 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.

The screenshot displays the EdgeADC main dashboard. At the top, there's a navigation bar with the 'EDGE NEXUS' logo, tabs for 'IP-Services' and 'Software', and a top right area with 'GUI Status', 'Home', 'Help', and a user dropdown 'admin'. A left sidebar contains a 'NAVIGATION' menu with options like 'Services', 'App Store', 'IP-Services', 'Library', 'View', 'System', 'Advanced', and 'Help'. The main content area is divided into two primary sections: 'Virtual Services' and 'Real Servers'.

Virtual Services Section:

- Buttons: 'Copy Service', 'Add Service', 'Remove Service'.
- Table with columns: Primary, VIP, VS, Enabled, IP Address, SubNet Mask / Prefix, Port, Service Name, Service Type.
- Table Data:

Primary	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
☐	☒	☒	☒	192.168.1.222	255.255.255.0	80	TEST WEB RR	HTTP

Real Servers Section:

- Tabs: 'Server', 'Basic', 'Advanced', 'flightPATH'.
- Group Name: 'Server Group'.
- Buttons: 'Copy Server', 'Add Server', 'Remove Server'.
- Table with columns: Status, Activity, Address, Port, Weight, Calculated Weight, Notes, ID.
- Table Data:

Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
☒	Online	192.168.1.200	80	100	100	Site 1	
☒	Online	192.168.1.201	80	100	100	Site 2	

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, weshalb 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 des 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 am oberen Rand des Bildschirms, 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. Wenn Sie auf das Element "Service" klicken, wird dieses erweitert, um die verfügbaren Auswahlmöglichkeiten anzuzeigen.

IP-Dienste

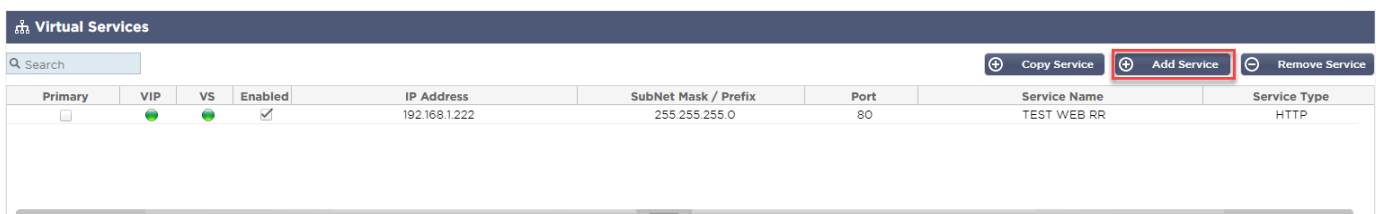
Im Bereich IP-Dienste des ADC können Sie die verschiedenen virtuellen IP-Dienste, die Sie für Ihren speziellen Anwendungsfall benötigen, hinzufügen, löschen und konfigurieren. Die Einstellungen und Optionen sind in die folgenden Abschnitte unterteilt. Diese Abschnitte befinden sich auf der rechten Seite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

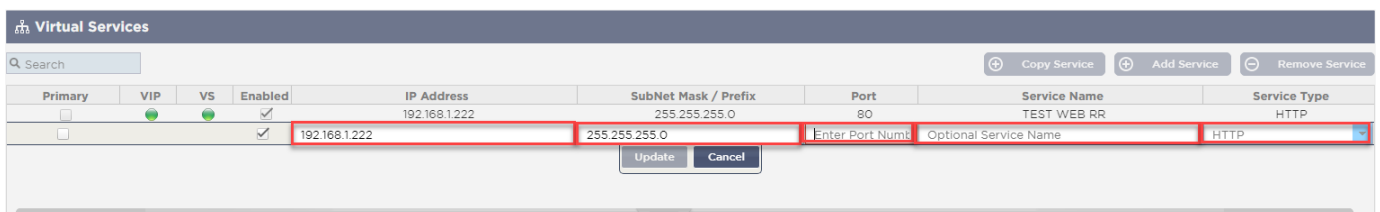
Der ADC bestimmt, wie der Datenverkehr auf die Server umverteilt wird, basierend auf einer Lastausgleichsrichtlinie, die auf der Registerkarte "Basic" im Abschnitt "Real Servers" festgelegt wurde.

Erstellen eines neuen virtuellen Dienstes unter Verwendung eines neuen VIP



Virtual Services									
Search									
Primary	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type	
☐	●	●	☒	192.168.1.222	255.255.255.0	80	TEST WEB RR	HTTP	

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



Virtual Services									
Search									
Primary	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type	
☐	●	●	☒	192.168.1.222	255.255.255.0	80	TEST WEB RR	HTTP	
☐	●	●	☒	192.168.1.222	255.255.255.0	Enter Port Num	Optional Service Name	HTTP	

- 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, um auf die Anwendung mit Lastausgleich zuzugreifen.
Subnetzmaske/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 Real-Server 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.
Service 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:

Real Servers

Server Basic Advanced flightPATH

Group Name:
+ Add Server - Remove

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

Update Cancel

Feld	Beschreibung
Aktivität	Über das Feld Aktivität kann der Status des lastverteilten realen Servers angezeigt und geändert werden. 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, damit die Persistenz geleert und der Server in einen Offline-Zustand versetzt werden kann, ohne dass die Benutzer beeinträchtigt werden. 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 auf dem 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 zunächst grau und dann grün, wenn der Server Health Check erfolgreich war. Sie leuchtet rot, wenn der Real Server Monitor fehlschlägt.
- Ein Server, dessen Statusleuchte rot leuchtet, wird nicht im Lastausgleich betrieben.

Beispiel für einen abgeschlossenen virtuellen Dienst

Virtual Services

Search

Copy Service

Add Service

Remove Service

Primary	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
☐	☒	☒	☒	192.168.1.222	255.255.255.0	80	TEST WEB RR	HTTP

Real Servers

Server

Basic

Advanced

flightPATH

Group Name: Server Group

Copy Server

Add Server

Remove Server

Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
☒	Online	192.168.1.200	80	100	100	Site 1	
☒	Online	192.168.1.201	80	100	100	Site 2	

Erstellen eines neuen virtuellen Dienstes unter Verwendung eines vorhandenen VIP

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

Virtual Services

Search + Copy Service + Add Service - Remove Service

Primary	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
☐			☒	192.168.1.222	255.255.255.0	80	TEST WEB RR	HTTP
☐			☒	192.168.1.222	255.255.255.0	80	TEST WEB RR	HTTP

Update Cancel

- 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 Diensttyp
- Sie können nun die Schaltfläche Aktualisieren drücken, um diesen Abschnitt zu speichern und automatisch zum Abschnitt Real Server weiter unten zu springen

Real Servers

Server Basic Advanced flightPATH

Group Name: + Add Server - Remove

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

Update Cancel

- Belassen Sie die Option "Serveraktivität" auf "Online" - das bedeutet, dass er 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 zuerst grau und dann grün, wenn der Server Health Check erfolgreich war. Sie leuchtet 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

Primary	VIP Status	Service Status	Enabled	IP Address	SubNet Mask	Port	Service Name	Service Type
☐			☒	192.168.1.248	255.255.255.0	80	VIP1	HTTP
☐			☒	192.168.1.251	255.255.255.0	80	VS2	HTTP
☒			☒	192.168.1.253	255.255.255.0	80	VIP2	HTTP

- Doppelklicken Sie auf das IP-Adressfeld für diesen Dienst

Primary	VIP Status	Service Status	Enabled	IP Address	SubNet Mask	Port	Service Name	Service Type
☐			☒	192.168.1.248	255.255.255.0	80	VIP1	HTTP
☐			☒	192.168.1.251	255.255.255.0	80	VS2	HTTP
☐			☒	192.168.1.254	255.255.255.0	80	VIP2	HTTP
				Update	Cancel			

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

Primary	VIP Status	Service Status	Enabled	IP Address	SubNet Mask	Port	Service Name	Service Type
☐			☒	192.168.1.248	255.255.255.0	80	VIP1	HTTP
☐			☒	192.168.1.251	255.255.255.0	80	VS2	HTTP
☒			☒	192.168.1.254	255.255.255.0	80	VIP2	HTTP

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 Copy Service kopiert einen kompletten 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 ändern, z. B. eine Lastausgleichsrichtlinie, den Real-Server-Monitor 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.

IP-Services

Dashboard

Virtual Services

Copy Service

10.4.8.191

Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port
Stand-alone			☒	10.4.8.191	255.255.255.0	80
			☒	10.4.8.191	255.255.255.0	81
			☒	10.4.8.191	255.255.255.0	82
			☒	10.4.8.191	255.255.255.0	443

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.

Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
	Online	192.168.1.200	80	☒ Status	100	Site 1	
	Online	192.168.1.201	80	☒ Activity	100	Site 2	
				☒ Address			
				☒ Port			
				☒ Weight			
				☒ Calculated Weight			
				☒ Notes			
				☒ ID			

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

Verstehen der Spalten für virtuelle Dienste

Primär/Modus

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

Clustering

Role

☒ **Cluster**
 Enable ALB-X to act as part of a Cluster, providing High Availability in Active-Passive mode - automatic synchronisation of appliances

☐ **Manual**
 Enable ALB-X to act in High Availability mode, either Active-Active or Active-Passive - manual configuration of appliance

☐ **Stand-alone**
 This ALB acts completely independently without high-availability

Option	Beschreibung
Cluster	Cluster ist die Standardrolle für das ADC bei der Installation, und die Spalte Primary/Mode zeigt den Modus an, in dem es 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	Mit der Rolle "Manuell" kann das ADC-Paar im Aktiv-Aktiv-Modus für verschiedene virtuelle IP-Adressen betrieben werden. In solchen Fällen enthält die Spalte "Primary" (Primär) ein Kästchen neben jeder eindeutigen virtuellen IP, das für "Active" (aktiv) angekreuzt oder für "Passive" (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, jedoch 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 Standardeinstellung 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"

Subnetzmaske/Präfix

Geben Sie Ihre Subnetzmaske in dezimaler Punktschreibweise 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](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".

Service Typ

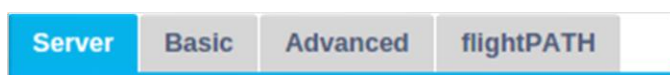
Bitte beachten Sie, dass bei allen "Layer 4"-Diensttypen die ADC nicht mit dem Datenstrom interagiert oder diesen modifiziert, so dass flightPATH bei Layer 4-Diensttypen nicht verfügbar ist. Layer 4-Dienste führen lediglich einen Lastausgleich des Datenverkehrs gemäß der Lastausgleichsrichtlinie durch:

Service Typ	Anschluss/Protokoll	Dienstschicht	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
HTTP	HTTP- oder HTTPS-Protokoll	Schicht 7	Der ADC kann mit flightPATH interagieren, den Datenstrom manipulieren und modifizieren.
FTP	Dateiübertragungsprotokoll	Schicht 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 für Terminaldienste-Server
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 Static 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 Back-End-Server, die mit dem aktuell ausgewählten virtuellen Dienst gekoppelt sind. Sie müssen mindestens einen Server zum Abschnitt "Real Servers" hinzufügen.

Server

Basic

Advanced

flightPATH

Group Name:

⊕

Copy Server

⊕

Add Server

⊖

Remove Server

Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
	Online	192.168.1.125	8080	100	100	TEQNAS	
	Online	192.168.1.119	8080	100	100	TEQNAS 2	

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

	Online			100	100	
Update Cancel						

- Geben Sie die IPv4-Adresse Ihres Servers in punktierter Dezimalschreibweise ein. Der reale Server kann sich im selben 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 die gleiche sein wie die Portnummer des virtuellen Dienstes oder eine andere Portnummer für die Reverse-Proxy-Konnektivität. Das ADC wird automatisch auf diese Nummer umgestellt.
- Wechseln Sie zum Abschnitt "Notizen", um alle relevanten Details für den Server hinzuzufügen. Beispiel: "IIS Web Server 1"

Gruppe Name

Real Servers

Server

Basic

Advanced

flightPATH

Group Name:

+

Copy Server

+

Add Server

-

Remove Server

Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
	Online	192.168.1.125	8080	100	100	TEQNAS	
	Online	192.168.1.119	8080	100	100	TEQNAS 2	

Wenn Sie die Server hinzugefügt haben, aus denen das Load-Balanced-Set besteht, 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 angeschlossen
- 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 auf der Registerkarte "Basic" eingestellten Lastausgleichsrichtlinie.
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 durchgeführt wird. Sobald die bestehenden Verbindungen auf natürliche Weise geschlossen wurden, 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 erhält 100 gleichzeitige Verbindungen
- Server 2 erhält 50 gleichzeitige Verbindungen
- Server 3 erhält 50 gleichzeitige Verbindungen

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

Wenn wir davon ausgehen, dass die Lastausgleichsrichtlinie Fastest die kürzeste Zeit für das GET einer Antwort verwendet, ändert die Anpassung der Gewichte die Ausrichtung 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.

Hinweise

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

Basic

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

Lastausgleichsrichtlinie

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

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

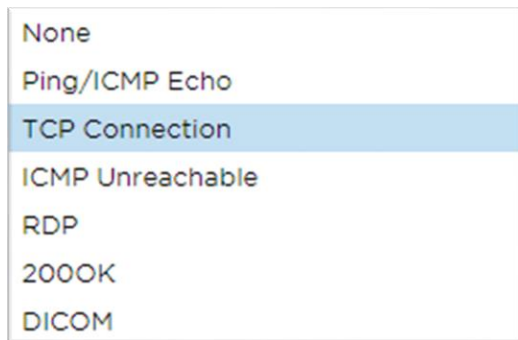
Option	Beschreibung
Schnellste	Die Richtlinie Schnellster Lastausgleich berechnet automatisch die Antwortzeit für alle Anfragen pro Server geglättet über die Zeit. Die Spalte Berechnetes Gewicht enthält den automatisch berechneten Wert. Eine manuelle Eingabe ist nur bei Verwendung dieser Lastausgleichsrichtlinie 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 herstellen müssen, z. B. bei der Suche nach Webservern. 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.
Schicht 3 Sitzungsaffinität/Persistenz - IP Bound	In diesem Modus bildet die IP-Adresse des Clients die Grundlage für die Auswahl des Real-Servers, der die Anfrage erhält. 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, und somit wäre die Last nicht gleichmäßig. Bei HTTP wird die Header-Information (X-Forwarder-For) verwendet, wenn sie vorhanden ist, um mit Proxies 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 geführt, dies kann jedoch mit einem jetPACK geändert werden.
Schicht 7 Session Affinität/Persistenz - ALB Session Cookie	Dieser Modus ist die am häufigsten verwendete 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 selben Back-End-Server gehen muss. Das Cookie läuft ab, sobald die Sitzung geschlossen wird.
Schicht 7 Session Affinität/Persistenz - ALB Persistent 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 selben 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 aktiviert ist, behält das ADC die Sitzungspersistenz 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 "Least Connections" 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 der Erkennung eines neuen ASP-Cookies wird ein Lastausgleich mit dem Algorithmus "Least Connections" 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 dem Algorithmus "Least Connections" 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 Sitzungspersistenz zum selben 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 dem Least Connections-Algorithmus 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 der 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 <code>h=[^;]+</code> verwendet. Diese Methode verwendet den Wert, der im Notizfeld "ID=X;" des Realservers 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 des Realen Servers (die zur Ladezeit eingelesen wird). Der Standardwert ist <code>CookieIDName="h"</code>; 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 <code>h=</code> durch den neuen Wert zu ersetzen. Der letzte Punkt ist, dass, wenn ein unbekannter Cookie-Wert ankommt und mit einer der Realserver-IDs übereinstimmt, dieser Server ausgewählt werden soll; andernfalls wird die nächste Methode (delegieren.) verwendet.

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 beispielsweise 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 Ausgangspunkt.

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 zuerst mit den Monitoren der unteren Schichten. 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:

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

Wir können sehen, dass Layer 3 Ping und Layer 4 TCP Connect erfolgreich waren, wenn wir uns die obere Zeile ansehen, 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 Library > 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 Legacy-Systeme zu hosten, die nicht primär für den H/A-Betrieb sind. Verwenden Sie diese Überwachungsmethode mit jedem Dienstyp.
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 Dienstyp verwendbar.
TCP-Verbindung	In diesem Modus wird eine TCP-Verbindung zum Real-Server aufgebaut und sofort wieder abgebaut, ohne Daten zu senden. Wenn die Verbindung erfolgreich ist, hält die ADC den Real Server für betriebsbereit. Diese Überwachungsmethode ist mit jedem Dienstyp 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, stuft das ADC den Real Server als betriebsbereit ein. 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 war, 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 funktionsfähig. Wenn die ADC aus irgendeinem Grund keinen "200 OK"-Antwortcode empfängt, einschließlich Timeouts, Verbindungsfehler 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 behandelt wird.
DICOM	Eine TCP-Verbindung wird zum Real-Server im DICOM-Modus initialisiert, und bei der Verbindung 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 Realserver-Überwachung konfiguriert wurde, wird in der Liste angezeigt.

Caching-Strategie

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

Off

By Host

By Virtual Service

Detaillierte Cache-Einstellungen finden Sie auf der Seite Configure Cache (Cache konfigurieren). Beachten Sie, dass komprimierte Objekte nicht zwischengespeichert werden, wenn die Zwischenspeicherung auf ein VIP mit dem beschleunigten Diensttyp "HTTP" angewendet wird.

Option	Beschreibung
Nach Host	Das Caching pro Host basiert auf der Anwendung pro Hostname. Für jede Domäne/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 gibt nur einen Cache für alle Domänen/Hostnamen, die den virtuellen Dienst durchlaufen.

Diese Option ist eine spezielle Einstellung für die Verwendung mit mehreren Klonen einer einzelnen Site.

Beschleunigung

Option	Beschreibung
Aus	Komprimierung für den virtuellen Dienst ausschalten
Komprimierung	Wenn diese Option aktiviert ist, schaltet sie die Komprimierung für den ausgewählten virtuellen Dienst ein. Das ADC komprimiert den Datenstrom zum Client auf Anforderung 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 über den Abschnitt "Globale Ausschlüsse" ausschließen.

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.

Virtueller Dienst SSL-Zertifikat (Verschlüsselung zwischen Client und dem ADC)

Die Standardeinstellung ist "No SSL". Wenn Ihr Diensttyp "HTTP" oder "Layer4 TCP" ist, können Sie in der Dropdown-Liste 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. Durch diesen Vorgang wird die SNI-Erweiterung automatisch aktiviert, 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.
Standard	Diese Option führt dazu, dass ein lokal erstelltes Zertifikat mit dem Namen "Standard" auf die Browserseite des Kanals angewendet wird. Verwenden Sie diese Option, um SSL zu testen, wenn noch keines erstellt oder importiert wurde.
Vom Benutzer importierte SSL-Zertifikate	Alle Zertifikate, die Sie in den ADC importiert haben, werden hier angezeigt.

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

Die Standardeinstellung für diese Option ist No SSL. Wenn Ihr Server eine verschlüsselte Verbindung erfordert, muss dieser Wert etwas anderes als "No SSL" sein. Zertifikate, die erstellt oder importiert wurden, werden in dieser Liste angezeigt.

No SSL
Any
SNI
default

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 einen so genannten "SSL Offload" zu ermöglichen.
Beliebig	Der ADC fungiert als Client und akzeptiert jedes Zertifikat, das der Real Server vorlegt. Der Verkehr vom ADC zum Real Server wird verschlüsselt, wenn diese Option ausgewählt ist. Verwenden Sie die Option "Any", 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 Verkehr vom ADC zum Real Server wird verschlüsselt, wenn diese Option ausgewählt ist. Verwenden Sie die Option "Any", wenn auf der Seite des virtuellen Dienstes ein Zertifikat angegeben ist, das eine so genannte "SSL-Überbrückung" oder "SSL-Neuverschlüsselung" bietet. Wählen Sie diese Option, um SNI auf der Serverseite zu aktivieren.
Vom Benutzer importierte SSL-Zertifikate	Hier erscheinen alle Zertifikate, die Sie in den ADC importiert haben.

Erweitert

Real Servers

Server

Basic

Advanced

flightPATH

Connectivity:

Reverse Proxy

Cipher Options:

Defaults

Client SSL Renegotiation: ☒

Client SSL Resumption: ☒

SNI Default Certificate:

None

Security Log:

On

Connection Timeout (sec):

600

Monitoring Interval (sec):

10

Monitoring Timeout (sec):

10

Monitoring In Count:

2

Monitoring Out Count:

3

Max. Connections (Per Real Server):

Update

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 oder 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-Lastverteilung geeignet. Daher sind Caching und Komprimierung bei dieser Option nicht verfügbar. Der Schicht-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 die Unterstützung der Quell-IP-Persistenz der einzige verfügbare Typ ist. DSR erfordert auch Änderungen am Realserver, die durchgeführt werden müssen. Bitte lesen Sie den Abschnitt Änderungen am realen 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 virtuellen ADC-Maschinen 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 die Persistenz gibt, die nicht auf IP-Listen basiert. Diese Methode erfordert, dass der Real Server sein Standardgateway auf die lokale Schnittstellenadresse (eth0, eth1 usw.) des ADCs setzt. Lesen Sie dazu den Abschnitt Real Server Changes.

Verschlüsselungsoptionen

Sie können Chiffren auf einer Ebene pro Dienst einstellen und 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 Client-initiierte SSL-Neuaushandlung zulassen möchten. Deaktivieren Sie die Client-SSL-Neuaushandlung, 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 Wiederverwendung einer Sitzung vorschlägt, versucht der Server, die Sitzung wiederzuverwenden, wenn 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 clientseitigem SNI die angeforderte Domain mit keinem der dem Dienst zugewiesenen Zertifikate übereinstimmt, präsentiert der ADC das SNI-Standardzertifikat. Die Standardeinstellung hierfür ist "None" (Keines), wodurch die Verbindung effektiv abgebrochen wird, wenn keine exakte Übereinstimmung vorhanden ist. Wählen Sie eines der installierten Zertifikate aus der Dropdown-Liste aus, um es zu präsentieren, wenn eine exakte SSL-Zertifikatsübereinstimmung fehlschlägt.

Sicherheitsprotokoll

'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 > Logging", auf der Sie die Einstellungen der W3C-Protokollierung überprüfen können.

Verbindungs-Timeout

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 Realserver-Monitore auf der Registerkarte "Basic". 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 beträgt 1 Sekunde. Während 1s für die meisten Anwendungen akzeptabel ist, kann es für andere Anwendungen oder während des Testens von Vorteil sein, dies zu erhöhen.

Überwachung Timeout

Der Timeout-Wert gibt an, wie lange 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 von 2 gibt an, dass der Real-Server zwei erfolgreiche Prüfungen des Zustandsmonitors 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 genommen wird. Durch Verringern dieses Wertes wird der Server schneller in Betrieb genommen.

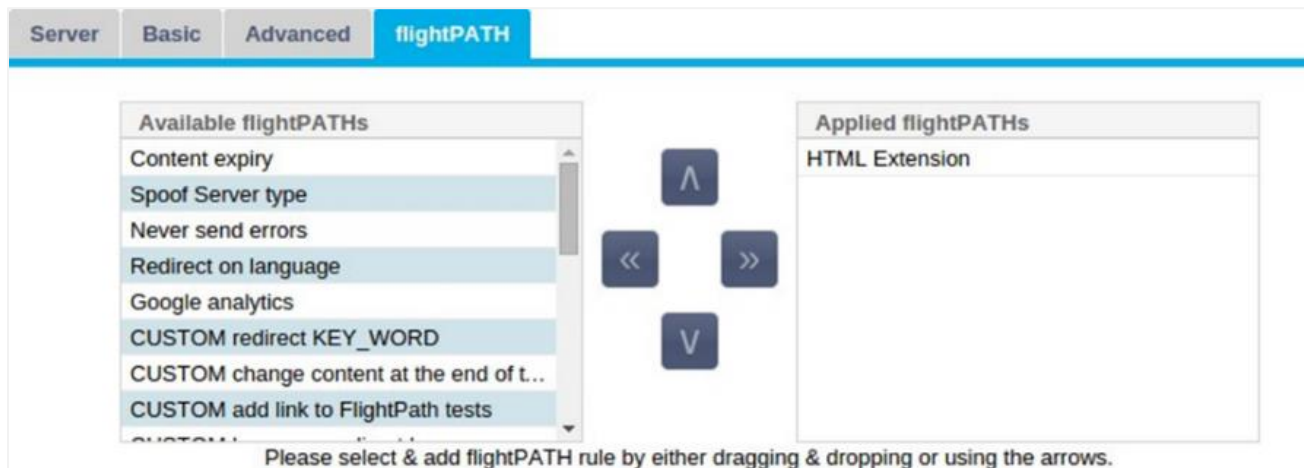
Überwachung der Anzahl der Ausgänge

Der Standardwert für diese Einstellung ist 3, was bedeutet, dass der Real-Server-Monitor dreimal fehlschlagen muss, bevor das 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 das ADC benötigt, um das Senden von Datenverkehr an diesen Server zu stoppen.

Max. Anschlüsse

Begrenzt die Anzahl der gleichzeitigen Real-Server-Verbindungen und wird pro Dienst eingestellt. Wenn Sie dies zum Beispiel 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, wenn dieses Limit auf allen Servern erreicht ist, damit die Benutzer verstehen, warum eine Nichtantwort oder Verzögerung aufgetreten ist. Für unbegrenzte Verbindungen lassen Sie dieses Feld leer. 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 Skripteingabekonzole. Stattdessen verwendet es eine grafische Benutzeroberfläche, um die verschiedenen Parameter, Bedingungen und Aktionen auszuwählen, die ausgeführt werden sollen, um das zu erreichen, was sie benötigen. 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 im obigen Bild sehen können, befindet sich auf der linken Seite eine Liste der verfügbaren Regeln und auf der rechten Seite 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 der 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 den Regelbestand 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.

Bibliothek

Add-Ons

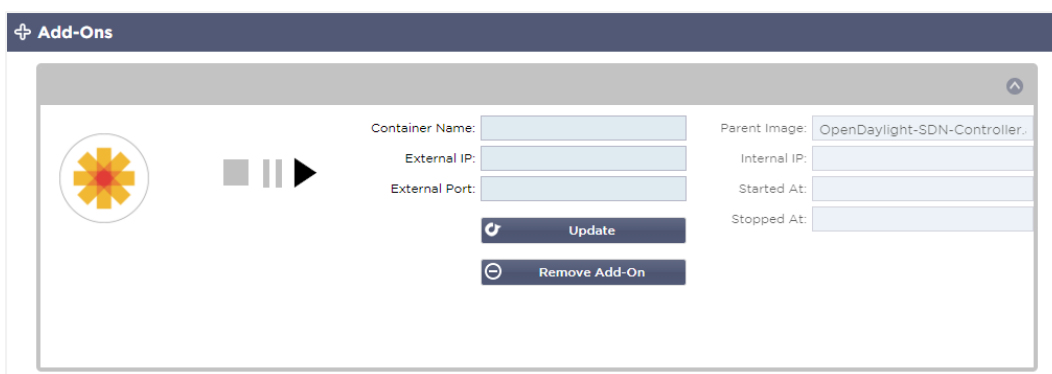
Add-ons sind Docker-basierte Container, die in einem isolierten Modus innerhalb der ADC laufen können. Beispiele für Add-ons könnten eine Anwendungsfirewall oder sogar eine Mikroinstanz des ADC selbst sein.

Apps

Der Abschnitt "Apps" innerhalb von Add-Ons enthält Details zu den Apps, die Sie erworben, heruntergeladen und bereitgestellt haben.

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

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 des ADC-Dashboards.

Hier können Sie die App auswählen, die Sie herunterladen und anschließend 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, sodass Sie sie herunterladen können.

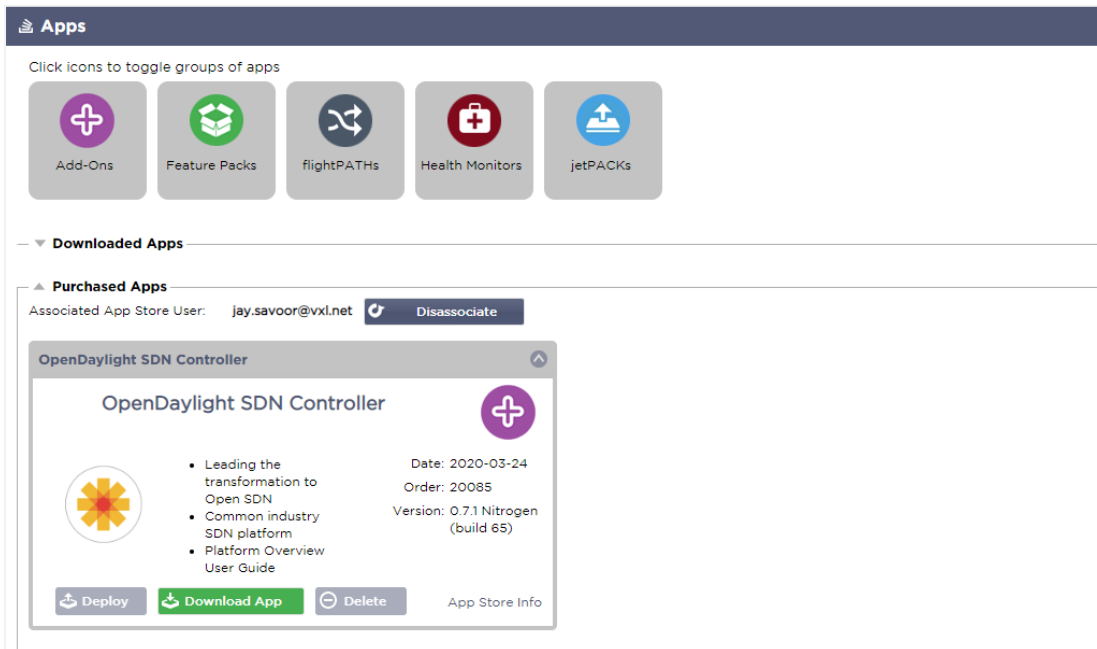
Die Apps verbinden sich mit den ADCs, die Sie besitzen und registriert haben.

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:

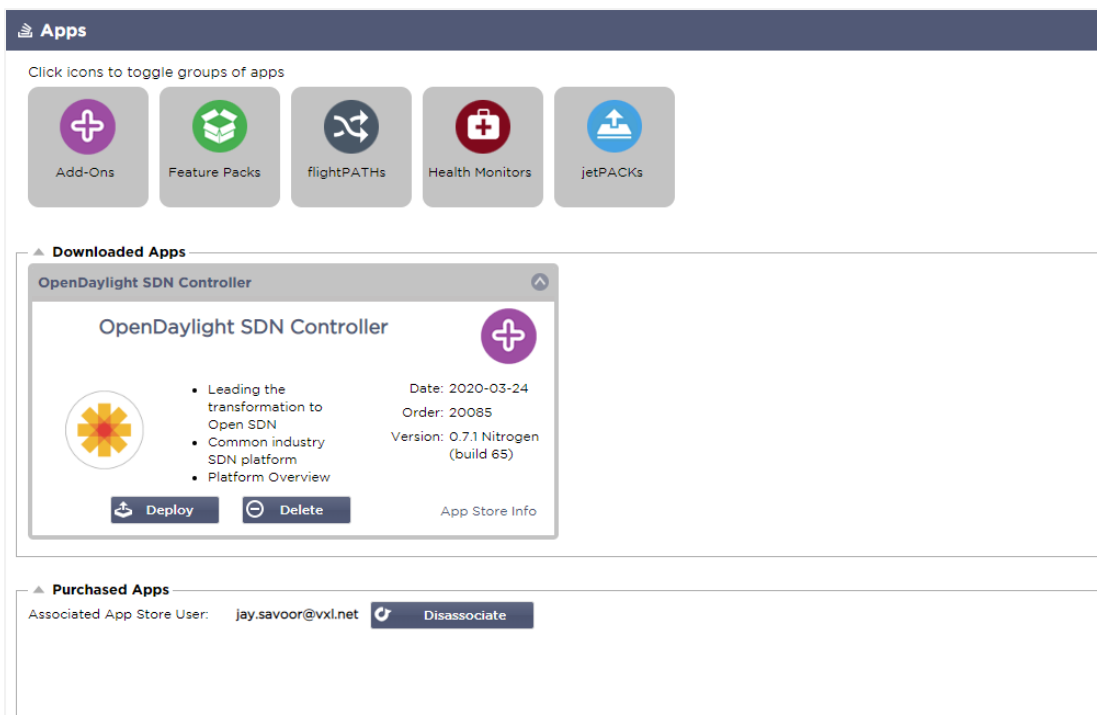
- Add-Ons: [HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/ADD-ONS/](https://appstore.edgenexus.io/product-category/add-ons/)
- Gesundheits-Monitore: [HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/SERVER-HEALTH-MONITORS/](https://appstore.edgenexus.io/product-category/server-health-monitors/)
- jetPACKS: [HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/JETPACKS/](https://appstore.edgenexus.io/product-category/jetpacks/)
- Feature Packs: [HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/EDGENEXUS-FEATURE-PACK/](https://appstore.edgenexus.io/product-category/edgenexus-feature-pack/)

- flightPATH-Regeln: [HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/FLIGHTPATH/](https://appstore.edgenexus.io/product-category/flightpath/)
- Software-Updates: [HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/EDGENEXUS-SOFTWARE-UPDATE/](https://appstore.edgenexus.io/product-category/edgenexus-software-update/)



Bereitstellen einer App

Nachdem 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 nimmt je nach den für den ADC verfügbaren Ressourcen einige Zeit in Anspruch. Nach der Bereitstellung wird die App im Bereich "Heruntergeladene Apps" angezeigt.



Authentifizierung

Auf der Seite Bibliothek > Authentifizierung können Sie Authentifizierungsserver einrichten und Authentifizierungsregeln mit Optionen für clientseitiges Basic oder Forms und serverseitiges NTLM oder BASIC erstellen.

Einrichten der Authentifizierung - ein Workflow

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

Authentifizierungsserver

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

Name	Authentication Method	Domain	Server Address	Port	Login Format
MKD-LDAP-MD5	LDAP-MD5	jetnexusO	mkdomserve.jetnexus.local		Blank
MKD-LDAP	LDAP	jetnexusO	192.168.3.200		Username Only
MKD-LDAPS	LDAPS	jetnexusO	192.168.3.200		Username Only
MKD-LDAPS-MD5	LDAPS-MD5	jetnexusO	mkdomserve.jetnexus.local		Blank

- 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
Authentifizierungsverfahren	Wählen Sie eine Authentifizierungsmethode LDAP - einfaches LDAP mit Benutzernamen und Kennwörtern, 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 Domännennamen 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 müssen die Portnummer für LDAP und LDAPS nicht hinzufügen. 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).
Suche Basis	Dieser Wert ist der Startpunkt für die Suche in der LDAP-Datenbank. Beispiel <i>dc=meineFirma,dc=lokal</i>
Anmeldeformat	Verwenden Sie das gewünschte Anmeldeformat. Benutzername - wenn Sie dieses Format wählen, müssen Sie nur den Benutzernamen eingeben. 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: <i>mycompany\gchristie ODER jemand@mycompany</i> . 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.

Authentication Rules								
+ Add Rule - Remove Rule								
Name	Description	Root Domain	Authentication Server	Client Authentication	Server Authentication	Form	Message	Timeout (s)
Rule 1	Test Auth Rule	jetnexus.com	MKDC	Forms	NONE	default	Test for user Guide	600

Feld	Beschreibung
Name	Fügen Sie einen geeigneten Namen für Ihre Authentifizierungsregel hinzu.
Beschreibung	Fügen Sie eine passende Beschreibung hinzu.
Wurzel-Domäne	Dieses Feld muss leer gelassen werden, es sei denn, Sie benötigen eine Einzelanmeldung über Subdomänen hinweg.
Authentifizierungs-Server	Dies ist ein Dropdown-Feld mit Servern, die Sie konfiguriert haben.
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 keine vorhandene Authentifizierung hat, wählen Sie diese Einstellung. Diese Einstellung bedeutet, dass Sie Authentifizierungsfähigkeiten zu einem Server hinzufügen können, der zuvor keine hatte. Basic - wenn Ihr Server die Basisauthentifizierung (401) aktiviert hat, wählen Sie BASIC. NTLM - wenn Ihr Server die NTLM-Authentifizierung aktiviert hat, 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.

Single Sign-On

Name	Description	Root Domain	Authentication Server	Client Authentication	Server Authentication	Form	Message	Timeout (s)
Jetnexus Auth	For demo purposes	edgenexus.io	Infra	Forms	NTLM	default	Please sign in to continue	60

Wenn Sie eine Einzelanmeldung für Benutzer bereitstellen 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 sich dann mit appstore. mycompany.com verbinden 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 Abschnitt können Sie ein benutzerdefiniertes Formular hochladen.

So erstellen Sie Ihr benutzerdefiniertes Formular

Obwohl das vom ADC bereitgestellte Basisformular für die meisten Zwecke ausreichend ist, wird es Fälle geben, in denen Unternehmen dem Benutzer ihre eigene Identität präsentieren möchten. Sie können ein eigenes Formular erstellen, das die Benutzer in solchen Fällen ausfüllen sollen. 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 für ein sehr einfaches und grundlegendes Formular

```

<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 Abschnitt Formulare hinzufügen.

The screenshot shows a web interface titled 'Forms'. It contains a form with the following fields and buttons:

- Form Name:** TestForm
- File Path:** C:\fakepath\TestForm.html
- Buttons:** Browse (highlighted with a red rectangle), Upload, Preview, and Remove.

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

Vorschau auf Ihr benutzerdefiniertes Formular

Um das soeben hochgeladene benutzerdefinierte Formular anzusehen, wählen Sie es aus und klicken auf Vorschau. In diesem Bereich können Sie auch Formulare löschen, die nicht mehr benötigt werden.

Forms

Form Name:

default

TestForm

Cache

Das ADC ist in der Lage, Daten in seinem internen Speicher zwischenspeichern und diesen Cache periodisch in den internen Speicher des ADC zu leeren. Die Einstellungen, die diese Funktionalität verwalten, werden in diesem Abschnitt beschrieben.

Global Cache Settings

Maximum Cache Size (MB):

Desired Cache Size (MB):

Default Caching Time (D/HH:MM): /

Cacheable HTTP Response Codes:

Cache Checking Timer (D/HH:MM): /

Cache-Fill Count:

☒

Force a check on the cache size

Remove all items from the cache

Globale Cache-Einstellungen

Maximale Cache-Größe (MB)

Dieser Wert bestimmt den maximalen RAM-Speicher, den der Cache verbrauchen kann. Der ADC-Cache ist ein speicherinterner 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-Speicher an, auf den der Cache getrimmt wird. Während die maximale Cache-Größe die absolute Obergrenze des Cache darstellt, ist die gewünschte Cache-Größe als die optimale Größe gedacht, die der Cache bei jeder automatischen oder manuellen Überprüfung der Cache-Größe anstreben sollte. 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 entfernen. Auch hier kann es effektiver sein, den Standardwert (30 MB) zu akzeptieren und die Größe des Cache unter "Monitor -> Statistik" regelmäßig zu überprüfen, um die richtige Größe zu ermitteln.

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

Der hier eingegebene Wert stellt die Lebensdauer von Inhalten ohne expliziten Ablaufwert 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 das 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 - 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.

Zeit der Cache-Prüfung (T/HH:MM)

Diese Einstellung bestimmt das Zeitintervall zwischen den Cache-Trimoperationen.

Cache-Fill Count

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

Cache-Regel anwenden

▲ Apply Cache Rule

Other Domains Served

Domain Name: ⊕ Add Domain ⊖ Remove Domain

⊕ Add Records ⊖ Remove Records

Name	Caching Rulebase
www.jetnexus.com	Images
www.domain2.com	File
demo.jn.com	Images

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

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

Cache-Regel erstellen

Create Cache Rule

Cache Content Selection Rulebases: include directory Enter Object Name + Add

+ Add Records - Remove Records

Rule Name	Description	Conditions
Images	Caches most images	include *.jpg include *.gif include *.png

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 eingeben oder die Funktion Bedingung hinzufügen

So fügen Sie eine Bedingung mithilfe der Auswahlregelbasis hinzu:

- Wählen Sie Einschließen oder Ausschließen
- Alle JPEG-Bilder auswählen
- Klicken Sie auf das Symbol + Hinzufügen
- Sie sehen, dass nun 'include *.jpg' 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 integrierte Technologie zur Verwaltung des Datenverkehrs. flightPATH ermöglicht es Ihnen, HTTP- und HTTPS-Datenverkehr in Echtzeit zu inspizieren und Aktionen auf der Grundlage von 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, um die Regel auszulösen.
3. Auswertung, die die Definition von Variablen erlaubt, die innerhalb von Aktionen verwendet werden können
4. Aktionen, die dazu dienen, zu steuern, was passieren soll, wenn Bedingungen erfüllt sind

Details

Details		
+ Add New	- Remove	Filter Keyword
flightPATH Name	Applied To VS	Description
HTML Extension	Not in use	Fixes all .htm requests to .html
index.html	Not in use	Force to use index.html in requests to folders
Close Folders	Not in use	Deny requests to folders
Hide CGI-BIN	Not in use	Hides cgi-bin catalog in requests to CGI scripts
Log Spider	Not in use	Log spider requests of popular search engines
Force HTTPS	Not in use	Force to use HTTPS for certain directory
Media Stream	Not in use	Redirects Flash Media Stream to appropriate channel

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

Details		
+ Add New	- Remove	Filter Keyword
flightPATH Name	Applied To VS	Description
Never send errors	Not in use	Client never gets any errors from your site
Redirect on language	Not in use	Find the language code and redirect to the related country domain
Google analytics	Not in use	Insert the code required by google for the analytics - Please change the value MYGOO...
IPv6 Gateway	Not in use	Adjust Host Header for IIS IPv4 Servers on IPv6 Services
Restrict Access	Not in use	Restrict Access by URL content
Access Only from LAN	Not in use	ST
Kill KeepAlive	Not in use	
Test if host is jumble.com		This is used to filter for host JUMBLE.COM

Feld	Beschreibung
FlightPATH Name	Dieses Feld ist für den Namen der flightPATH-Regel vorgesehen. 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, wird die Spalte "Applied To" automatisch mit einer IP-Adresse und einem Port-Wert ausgefüllt
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.

▲ Condition

+ Add New - Remove

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

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

▲ Condition

+ Add New - Remove

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

Update Cancel

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 "Formular hat nicht die Länge 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	Drop-Down, das GET, POST, etc. enthält
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 Subnetz 10\1\2\3 10\1\2\4 Verwenden Sie für mehrere IP's
Pfad	Pfad der Website	/meinewebsite/index.asp
POST	POST-Abfrageverfahren	Prüfen von Daten, die auf eine Website hochgeladen werden
Abfrage	Name und Wert einer Abfrage, und kann entweder den Abfragenamen oder auch einen Wert annehmen	"Best=jetNEXUS", wobei die Übereinstimmung "Best" 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	Beliebiger HTTP-Header	Referrer, User-Agent, Von, Datum
Version anfordern	Die HTTP-Version	HTTP/1.0 ODER HTTP/1.1
Antwort Körper	Eine benutzerdefinierte Zeichenkette im Antwortkörper	Server UP
Antwort-Code	Der HTTP-Code für die Antwort	200 OK, 304 Nicht geändert
Antwort Cookie	Der Name eines vom Server gesendeten Cookies	MS-WSMAN=afYfn1CDqqCDqUD::
Antwort-Kopfzeile	Beliebiger HTTP-Header	Referrer, User-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 eine Auswahlliste oder ein Textwert sein und ist abhängig vom Wert im Feld "Bedingung" definierbar. Wenn die Bedingung z. B. auf Host eingestellt ist, ist das Feld "Match" nicht verfügbar. Wenn die Bedingung auf <form> gesetzt ist, wird das Feld "Match" als Textfeld angezeigt, und wenn die Bedingung auf POST gesetzt ist, wird das Feld "Match" als Dropdown mit den 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 Teilinhaltsbereichstypen dieser Server unterstützt	Accept-Ranges: bytes
Autorisierung	Anmeldeinformationen für die HTTP-Authentifizierung	Berechtigung: Basic QWxhZGRpbjpvGVuIHNIc2FtZQ==

Charge-To	Enthält Kontoinformationen zu den Kosten für die Anwendung der angeforderten Methode	
Content-Encoding	Die Art der verwendeten Kodierung	Content-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 erzeugt 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 Format RFC 2822	Last-Modified: 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 User-Agents	Benutzer-Agent: Mozilla/5.0 (kompatibel; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Variieren	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 Webanwendung unterstützt	X-Powered-By: PHP/5.4.0

Sense

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

Prüfen Sie

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

Folgende Optionen stehen zur Auswahl: Enthalten, Ende, Gleich, Vorhanden, Länge haben, RegEx anpassen, Liste anpassen, Start, Länge überschreiten

CHECK	BESCHREIBUNG	BEISPIEL
Existieren	Dabei spielt es keine Rolle, wie die Bedingung im Detail aussieht, sondern nur, dass sie existiert/nicht existiert	Host - Existiert - Existiert
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	Request Header - Accept - Does - Contain - image
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	Absender-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 im Bereich Bedingung auf die Schaltfläche Neu hinzufügen.
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 eine Prüfung. Zum Beispiel, Enthalten
5. Wählen Sie einen Wert. Zum Beispiel, mycompany.com

Condition				
+ Add New		- Remove		
Condition	Match	Sense	Check	Value
Request Header		Does	Contain	image
Host		Does	Equal	www.imagepool.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 grafische Benutzeroberfläche 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 fest kodiert, 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\$
- Antwortcode (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.

Action	Target	Data
Rewrite Path	\$path\$	

In diesem Beispiel soll der Pfadteil der URL umgeschrieben werden, um die vom Benutzer eingegebene URL wiederzugeben.

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

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

Anwenden der flightPATH-Regel

Die Anwendung einer flightPATH-Regel erfolgt innerhalb der flightPATH-Registerkarte des jeweiligen 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 aus, die Sie konfiguriert haben, oder eine der vorgefertigten Regeln, 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

Monitoring

Details

+

 Add Monitor

-

 Remove

Name	Description	Monitoring Meth	Page Location	Required Conter	Applied To VS	User	Password	Threshold
200OK	Check home pag HTTP 200 OK	/			Not in use			
DICOM	Monitor DICOM s DICOM				Not in use			

Upload Monitor

Monitor Name:

Browse

Upload New Monitor

Custom Monitors

Remove

Wenn der Lastausgleich eingerichtet ist, ist es hilfreich, den Zustand der realen 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 Library > Real Server Monitors können Sie benutzerdefinierte Überwachungen hinzufügen, anzeigen und bearbeiten. Dabei handelt es sich um Layer 7-Server-"Health Checks". Wählen Sie diese aus dem Feld "Server Monitoring" innerhalb der Registerkarte "Basic" des von Ihnen definierten virtuellen Dienstes aus.

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

- Details
- Hochladen
- Kundenspezifische Monitore

Details

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

Details

+

 Add Monitor

-

 Remove

Name	Description	Monitoring Method	Page Location	Required Content	Applied To VS	User	Password	Threshold
200OK	Check home page for 200 HTTP 200 OK	/			Not in use			
DICOM	Monitor DICOM server	DICOM			Not in use			

Name

Name Ihrer Wahl für Ihren Monitor.

Beschreibung

Textbeschreibung 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 zum Real-Server hergestellt. Nach dem Herstellen der Verbindung 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 Realserver betriebsbereit ist. Wenn aus irgendeinem Grund der "200 OK"-Antwortcode nicht empfangen wird, einschließlich Zeitüberschreitungen oder Verbindungsabbrüche, wird der Real-Server als ausgefallen und nicht verfügbar betrachtet. Diese Überwachungsmethode kann wirklich nur mit HTTP- und Accelerated HTTP-Diensttypen verwendet werden. Wenn jedoch ein Layer 4-Diensttyp für einen HTTP-Server verwendet wird, könnte sie dennoch 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 zum Realserver hergestellt und wie im vorherigen Beispiel erläutert geprüft. Anstatt jedoch 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 HTTP- und Accelerated HTTP-Diensttypen verwendet werden. Wenn jedoch ein Layer 4-Diensttyp für einen	Name: Server Up 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

	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.	
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 "Notes" jedes Servers einstellen. Sie finden die Spalte "Notes" innerhalb der IP Services-- -Virtuelle Dienste--Server Seite.	Name: DICOM Beschreibung: L7 Health Check für DICOM-Dienst Überwachungsmethode: DICOM Seite Standort: 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 Verkehrsport und wird verwendet, wenn Sie Dienste miteinander verbinden möchten	Name: TCP Out of Band Beschreibung: Monitor Out of Band/Traffic port Seite Standort: N/A Erforderlicher Inhalt: 555
Multi-Port-TCP-Monitor	Diese Methode ist wie die obige, mit dem Unterschied, dass Sie mehrere verschiedene Ports haben können. Der Monitor gilt nur dann als erfolgreich, wenn alle im Abschnitt "Required Content" angegebenen Ports korrekt antworten.	Name: Multi-Port-Monitor Beschreibung: Mehrere Ports auf Erfolg überwachen Seite Standort: 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 einen Monitor, der mit einem virtuellen Dienst verwendet wurde, nicht löschen.

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 keine "Chunked"-Antwort ist

Real Server Monitor Beispiele

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

Monitor hochladen

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

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

▲ Upload Monitor

Monitor Name: Test

C:\fakepath\test.pl

Browse

Upload New Monitor

- Geben Sie Ihrem Monitor einen Namen, damit Sie ihn in der Liste der Überwachungsmethoden 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.

Kundenspezifische Monitore

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

▲ Upload Monitor

Monitor Name: Test

C:\fakepath\test.pl

Browse

Upload New Monitor

- 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 richtet sich an Personen mit Erfahrung im Umgang und Schreiben in Perl

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, wie 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 Gesundheitschecks haben zwei Ergebnisse

- Erfolgreich
Rückgabewert 1 Drucken
einer Erfolgsmeldung an Syslog Markieren
des Real-Servers Online (sofern IN COUNT übereinstimmt)
- Erfolglos
Rückgabewert 2 Drucken Sie
eine Meldung mit dem Wort "Unsuccessful" an Syslog Markieren Sie
den Real Server Offline (sofern OUT Count übereinstimmt)

Beispiel für einen benutzerdefinierten Health Monitor

```
#Monitor-Name HTTPS_SNI
```

```
streng verwenden:
```

```
Warnhinweise 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-Anschluss
my Scontent= $_[2]; ### Zu suchender Inhalt (in der Webseite und den HTTP-Headern)
my Snotes=   $_[3]; ### Virtueller Rechnername
my Spage=    $_[4]; ### Der Teil der URL nach der Host-Adresse
my Suser=    $_[5]; ### domain/username (optional)
my Spasswort= $_[6]; ### Passwort (optional)
my $resolve;
my $auth     =;
wenn ($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 Schicht-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 herkömmlichen 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 die ADC die Daten untersuchen muss, muss sie diese 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.

Wie man ein lokales SSL-Zertifikat erstellt

Create Certificate

Certificate Name: MyCompanyCertificate

Organization: MyCompany

Organizational Unit: Support

City/Locality: New York

State/Province: NY

Country: US

Domain Name: www.mycompany.com

Key Length: 2048

Period (days): 365

☒

- Füllen Sie alle Details wie im obigen Beispiel aus
- Klicken Sie auf Lokales Zertifikat erstellen
- Nachdem 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.

▲ **Create Certificate**

Certificate Name:

Organization:

Organizational Unit:

City/Locality:

State/Province:

Country:

Domain Name:

Key Length:

Period (days):

 **Create Local Certificate**

☒ **Create Certificate Request**

Füllen Sie das Formular wie oben gezeigt mit allen relevanten Daten aus und klicken Sie dann auf die Schaltfläche Zertifikatsanforderung. Sie erhalten das Popup, das den von Ihnen angegebenen Daten entspricht.

Certificate Details

Certificate Name: MyCompanyCertificate

Certificate Text:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICojCCAYoCAQAwXTElMAkGA1UEBhMCVVMxCzAJBgNVBAGTAk5ZMR
EwDwYDVQQH
EwhOZXcgWW9yazESMBAGA1UEChMJTXIDb21wYW55MR0wGAYDVQQD
ExF3d3cubXlj
b21wYW55LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCgg
EBAMP8YIOq
D5L6vmbotxHmcnwGORAxzSgqOuQZLOj7h2LCN8Hh0/W8mLEIC+k8iBou
hSna23TJ
B2BrL5xVwIPISj6RDsAnegpavGUVsdlou2iu7ujHGvSSAqjSsBBG4Is6ay3fLTl
ZM2ZDsIUzjPYK0gW7LStS89bH2ELB/MPf+iILFeQmCGQ2i5pF67sOOPpNM
E7EqXU
MOv/beTQ2Kwf0/awUw2m2RZ2krdgBq/Fw2tzQq+KxS4nHhOsJwlPKBy9u
-----
```

Close

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 muss dann Ihrer Zertifizierungsstelle zur Verfügung gestellt werden, um das SSL-Zertifikat zu erstellen.

Zertifikat verwalten

▲ Manage Certificate

Certificate: MyCompanyCertificate(Pending)

Paste Signed:

To install:
Select a certificate (pending) from the drop down box above
paste your signed certificate in here and click Install

Add intermediates:
Select a certificate (trusted) or certificate (imported) from the drop down box above
paste your intermediates in here one after the other
(intermediate closest to the certificate authority last) and
click Add Intermediate

Show
Install
Add Intermediate

Delete
Renew
Reorder

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

anzeigen

Certificate Details

Certificate Name: VXL_Wildcard_2020

Organization:

Organizational Unit:

City/Locality:

State/Province:

Country:

Domain Name: *.vxl.net

Key Length: 2048

Period(days):

Expires: Aug 11 12:00:00 2020 GMT

Close

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

- Wählen Sie das Zertifikat aus dem Dropdown-Menü aus
- 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.

▲ **Manage Certificate**

Certificate: MyCompanyCertificate(Pending: ▼

Paste Signed:

To install:
Select a certificate (pending) from the drop down box above
paste your signed certificate in here and click Install

Add intermediates:
Select a certificate (trusted) or certificate (imported) from the drop
down box above
paste your intermediates in here one after the other
(intermediate closest to the certificate authority last) and
click Add Intermediate

 **Show**

 **Install**

 **Add Intermediate**

 **Delete**

 **Renew**

 **Reorder**

- Wählen Sie ein Zertifikat aus, das Sie in den obigen Schritten erzeugt haben. An der Position wird der Status (Ausstehend) festgelegt. Im Beispiel wird MyCompanyCertificate in der obigen Abbildung gezeigt.
- 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 "Paste Signed" 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)	Zwischenstufe 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 für einen 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. Sie haben z. B. ein Zertifikat importiert, 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 der Zertifizierungsstelle am nächsten liegende Zwischenprodukt zuletzt eingefügt wird.
- Klicken Sie auf Zwischenstufe hinzufügen.

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

Ein Zertifikat löschen

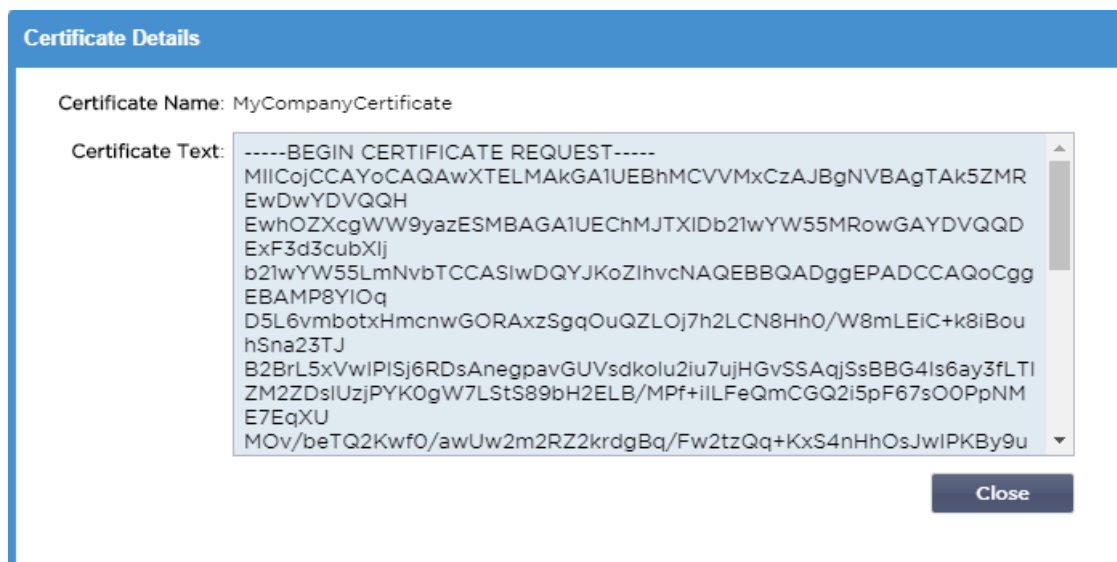
Sie können ein Zertifikat über die Schaltfläche "Delete" (Löschen) löschen. Nach dem Löschen wird das Zertifikat vollständig aus dem ADC entfernt und muss ersetzt und bei Bedarf wieder auf die virtuellen Dienste angewendet werden.

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

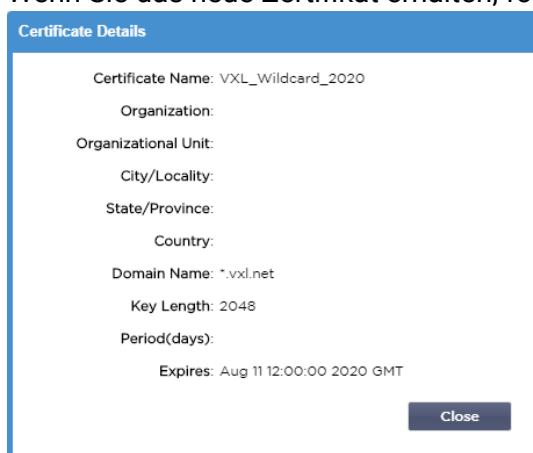
Ein Zertifikat erneuern

Mit der Schaltfläche Renew (Erneuern) können Sie eine neue Certificate Signing Request (Zertifikatsanforderung) anfordern. Diese Aktion ist erforderlich, wenn das Zertifikat abläuft und erneuert werden muss.

- Wählen Sie ein Zertifikat aus der Dropdown-Liste aus; 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 unter **ANZEIGEN**



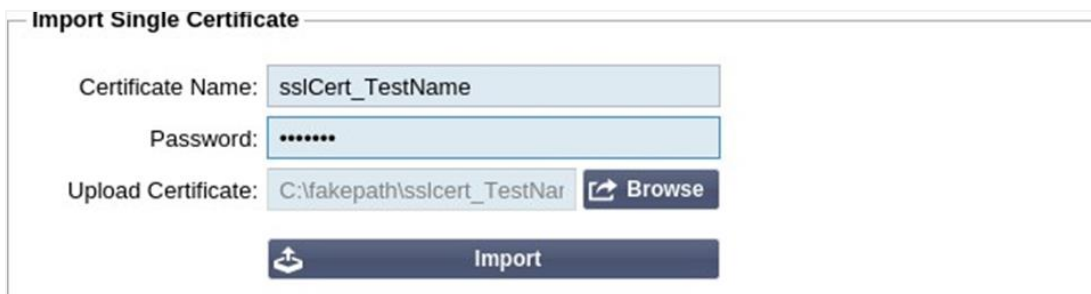
- Es kann vorkommen, dass Sie sich die Details eines installierten SSL-Zertifikats ansehen möchten.

- Wählen Sie das Zertifikat aus dem Dropdown-Menü aus
- 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 Sicherheitsregimes verwenden. Die Zertifikate müssen im PKCS#12-Format vorliegen, und solche Zertifikate sind immer durch Passwörter geschützt.

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



Import Single Certificate

Certificate Name: sslCert_TestName

Password:

Upload Certificate: C:\fakepath\sslcert_TestNar  Browse

 Import

- Geben Sie Ihrem Zertifikat einen freundlichen Namen. Der Name identifiziert es in den im ADC verwendeten Dropdown-Listen. Er muss nicht mit dem Domännennamen 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 mehrere Zertifikate exportiert werden.



Import Certificates from JNBK

Upload Certificate: C:\fakepath\sslcert_pack.jnt  Browse

Password:

 Import

- 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 verfügt über die Fähigkeit, 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 Kennwort 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 lautet sslcert__pack.jnbk.

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

Widgets

Auf der Seite Bibliothek > Widgets können Sie verschiedene leichtgewichtige visuelle Komponenten konfigurieren, die in Ihrem benutzerdefinierten Dashboard angezeigt werden.

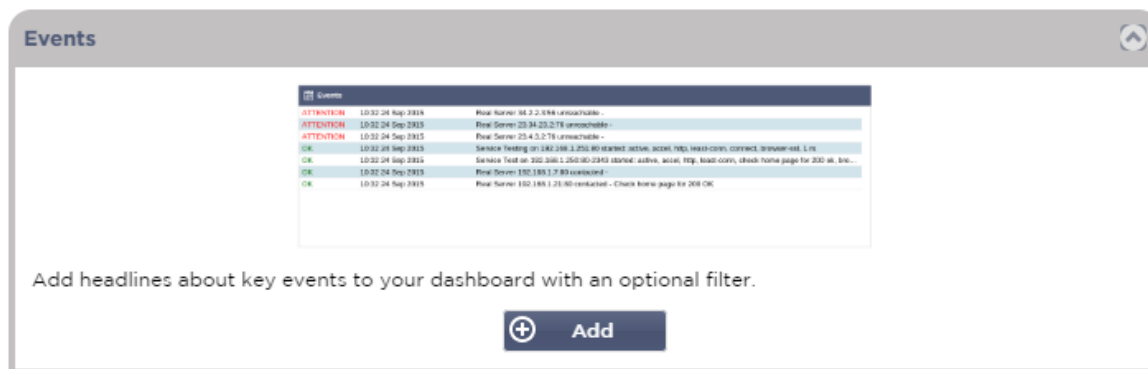
Konfigurierte Widgets

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

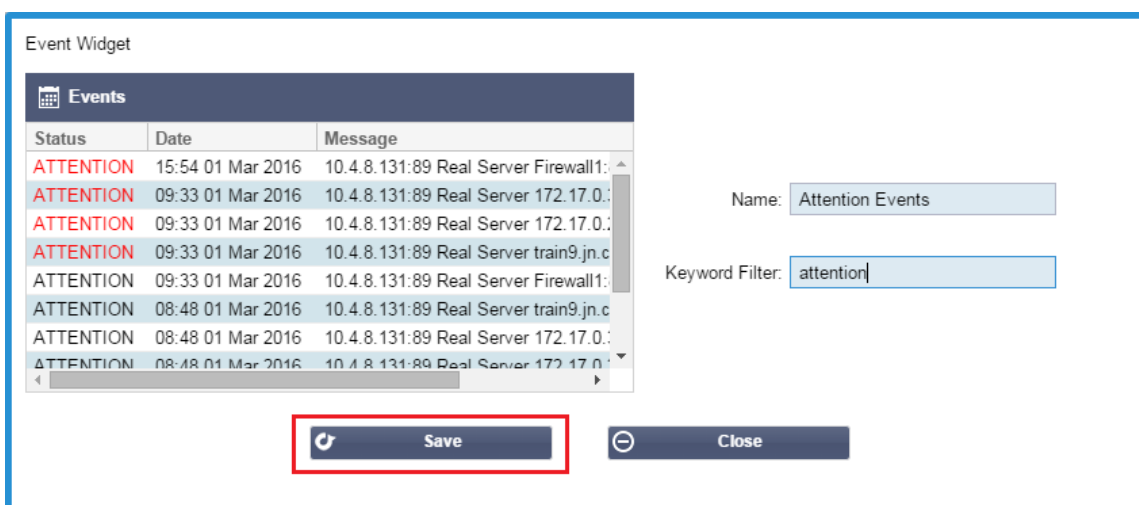
Verfügbare Widgets

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

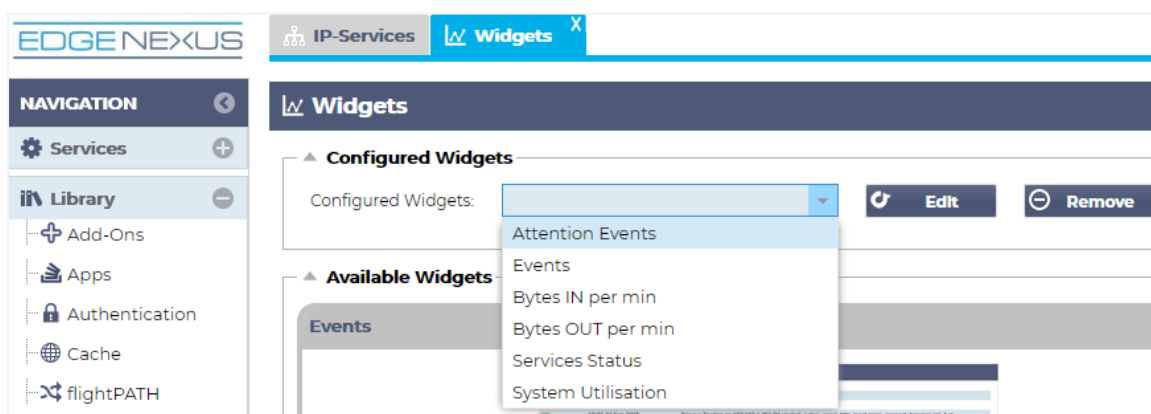
Das Ereignis-Widget



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



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

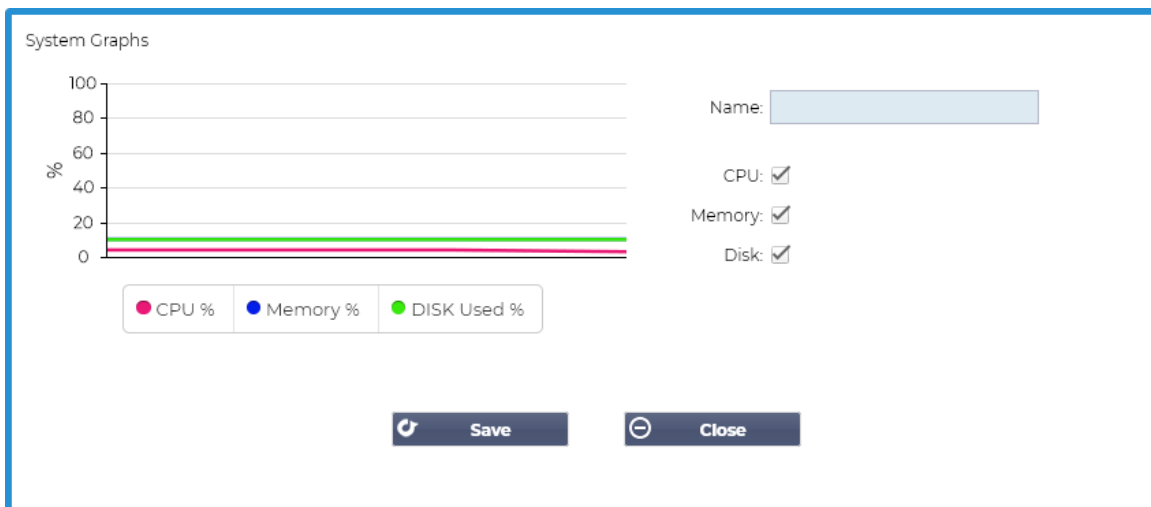


- Sie sehen, dass wir dieses Widget nun im Bereich Ansicht > Dashboard hinzugefügt haben.
- Wählen Sie das Widget "Achtung Ereignisse", um dieses im Dashboard anzuzeigen. Siehe unten.

Attention Events		
Status	Date	Message
ATTENTION	14:29 05 May 2021	192.168.1.222:80 Real server 192.168.1.201:80 unreachable - Connect=FAIL
ATTENTION	14:29 05 May 2021	192.168.1.222:81 Real server 192.168.1.201:80 unreachable - Connect=FAIL
ATTENTION	14:29 05 May 2021	192.168.1.222:80 Real server 192.168.1.200:80 unreachable - Connect=FAIL
ATTENTION	14:29 05 May 2021	192.168.1.222:81 Real server 192.168.1.200:80 unreachable - Connect=FAIL
ATTENTION	16:12 03 May 2021	192.168.1.222:80 Real server 192.168.1.200:80 unreachable - Connect=FAIL
ATTENTION	16:12 03 May 2021	192.168.1.222:81 Real server 192.168.1.200:80 unreachable - Connect=FAIL
ATTENTION	16:12 03 May 2021	192.168.1.222:81 Real server 192.168.1.201:80 unreachable - Connect=FAIL
ATTENTION	16:12 03 May 2021	192.168.1.222:80 Real server 192.168.1.201:80 unreachable - Connect=FAIL
ATTENTION	17:18 01 May 2021	Service Web Server VIP on 192.168.1.222:80 stopped: active, http, least-conn, connect, 2 rs - no real server contact
ATTENTION	17:18 01 May 2021	Service Web Server VIP on 192.168.1.222:81 stopped: active, http, least-conn, connect, 2 rs - no real server contact

Sie können den Live-Daten-Feed auch anhalten und neu starten, indem Sie auf die Schaltfläche Pause Live Data klicken. Außerdem können Sie jederzeit zum Standard-Dashboard zurückkehren, indem Sie auf die Schaltfläche Default Dashboard (Standard-Dashboard) klicken.

Das Systemgrafik-Widget



Das ADC verfügt über ein konfigurierbares Systemgrafik-Widget. Durch Klicken auf die Schaltfläche "Hinzufügen" des Widgets 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

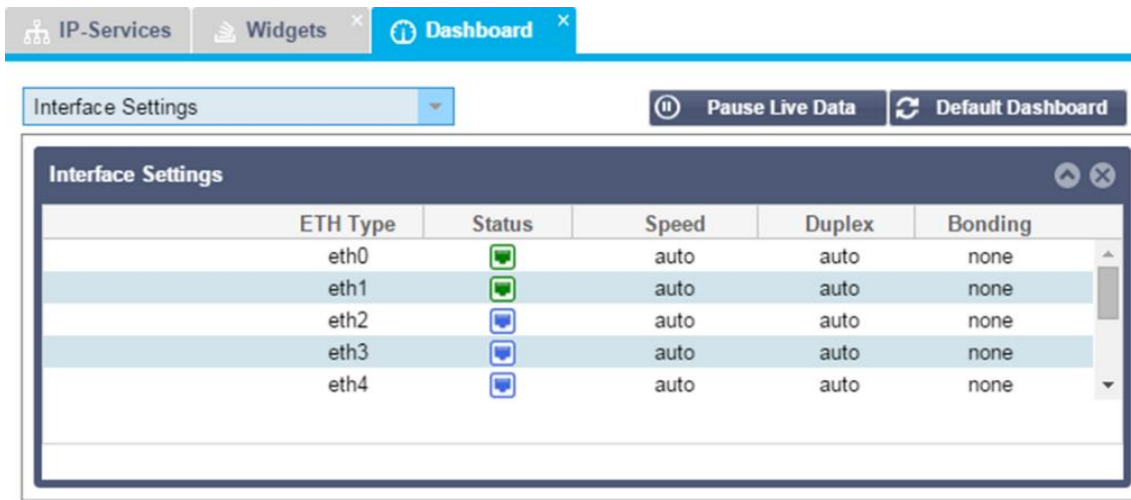
Name: My Interfaces				
ETH Type	Status	Speed	Duplex	Bonding
eth0		auto	auto	none
eth1		auto	auto	none

Save Close

Mit dem Schnittstellen-Widget können Sie die Daten für die gewählte Netzwerkschnittstelle anzeigen, wie 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.

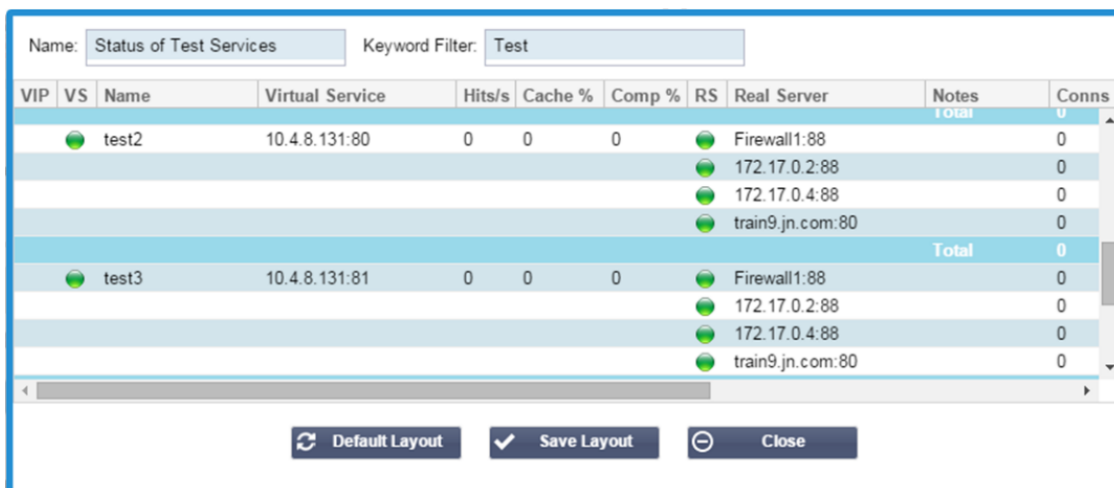
Wählen Sie das Widget, das Sie gerade angepasst haben, aus dem Widget-Dropdown-Menü im Dashboard aus. Es wird ein Bildschirm wie der unten abgebildete angezeigt.



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.

Name: Keyword Filter:

VIP	VS	Name	Virtual Service	Hits	RS	Real Server	Notes	Conns	Trend	Data
		test2	10.4.8.131:80	0		172.17.0.2		0		0
		test3	10.4.8.131:81	0		172.17.0.2		0		0

☒ VIP
☒ VS
☒ Name
☒ Virtual Service
☒ Hits/s
☐ Cache %
☐ Comp %
☒ RS
☒ Real Server
☒ Notes
☒ Conns
☒ Trend
☒ Data
☒ Trend
☒ Req/s
☒ Trend

Default Layout Save Layout

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

IP-Services Status Widgets Dashboard

Status of Test Services

Pause Live Data Default Dashboard

VIP	VS	Name	Virtual Service	Hits/s	RS	Real Server	Conns	Trend	Data	Trend	Req/s	Trend
		Spirent Test	172.21.100.1:80	0		172.22.200.1:80	0		0		0	
		Spirent Test	172.21.100.1:81	0		172.22.200.1:80	0		0		0	
		Spirent Test	172.21.100.2:80	0		WAF-EX-1:80	0		0		0	
		test1	10.4.8.131:89	0		Firewall1:88	0		0		0	
		test2	10.4.8.131:80	0		Firewall1:88	0		0		0	
		test3	10.4.8.131:81	0		Firewall1:88	0		0		0	
		test4	10.4.8.131:82	0		Firewall1:88	0		0		0	

Verkehrsgrafik-Widget

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

Traffic Graphs

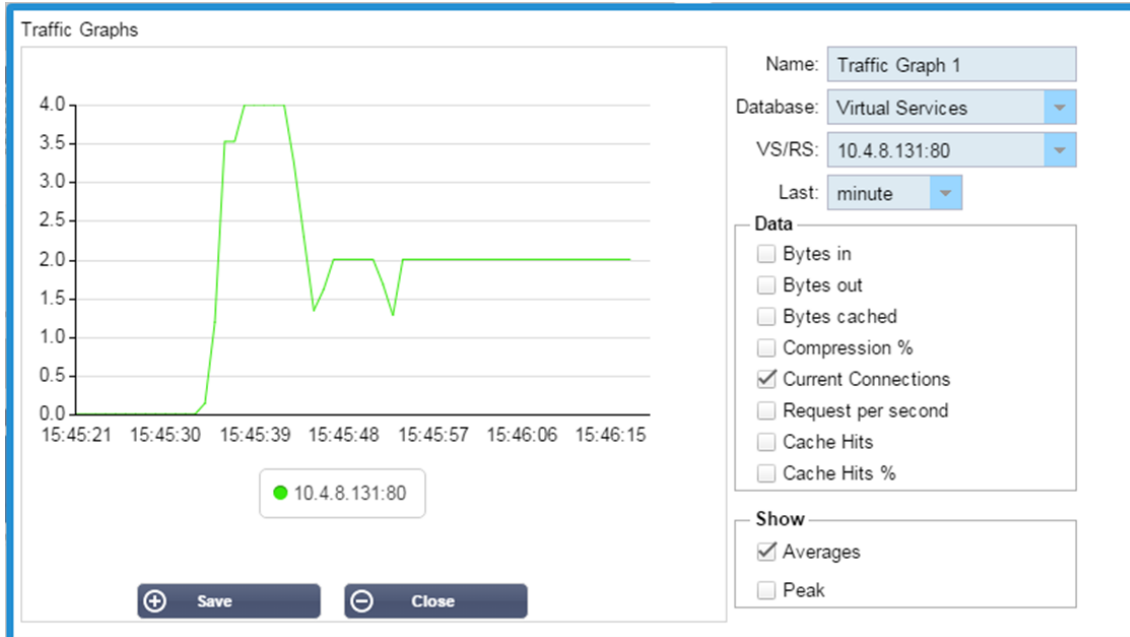
Display live and historical graphs of many different data sets.

Add

- 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 der Dropdown-Liste VS/RS auswählen.
- Wählen Sie einen Zeitrahmen aus der Dropdown-Liste "Letzte".
 - Minute - letzte 60s
 - Stunde - aggregierte Daten von 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 von 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 ausgewählt haben, klicken Sie auf Speichern und Schließen

Beispiel-Verkehrsdigramm



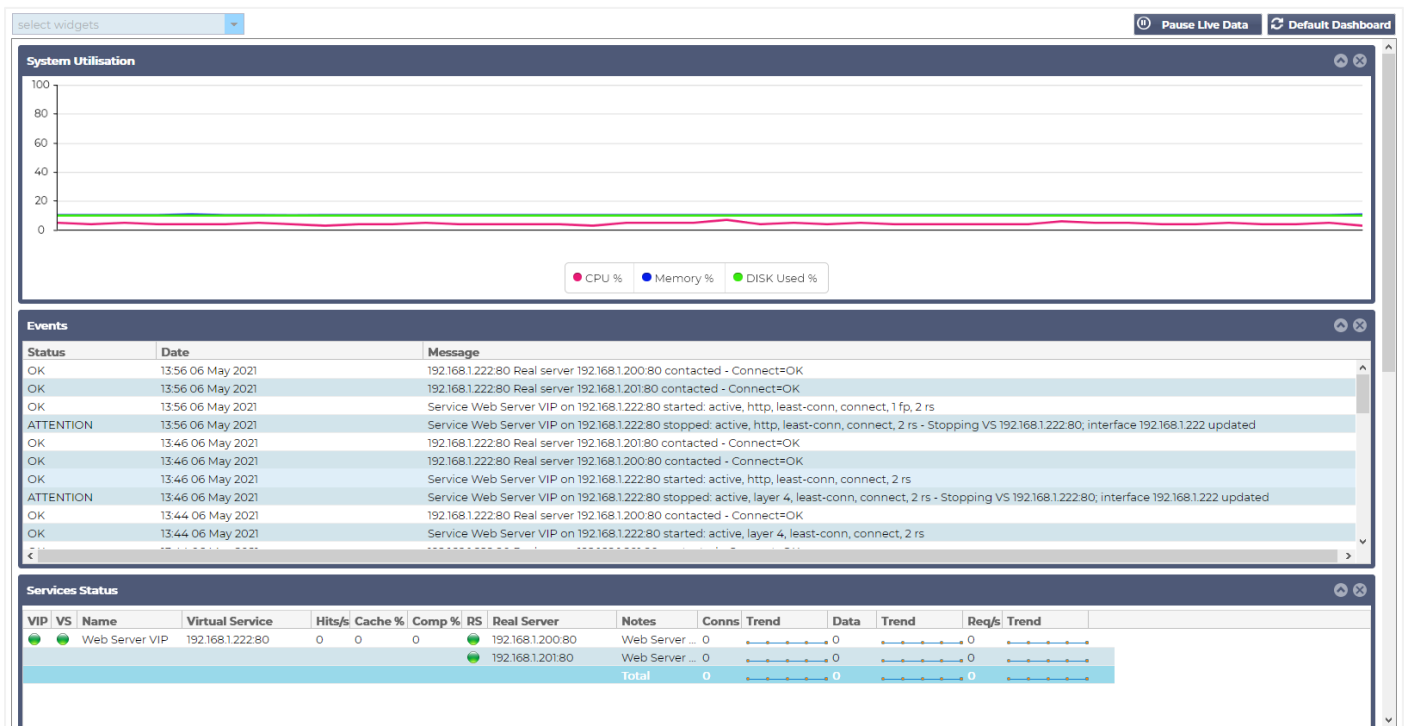
Sie können nun Ihr Traffic Graph Widget zu Ansicht > Dashboard hinzufügen.

Ansicht

Dashboard

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

Das Dashboard ist über das Segment "Ansicht" des Navigatorpanels zu erreichen. Wenn es ausgewählt ist, zeigt es mehrere Standard-Widgets an und ermöglicht die Auswahl von benutzerdefinierten Widgets, die Sie definiert haben.



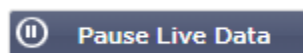
Verwendung des Dashboards

Das Dashboard U besteht aus vier Elementen: dem Menü "Widgets", der Schaltfläche "Pause/Play" und der Schaltfläche "Default Dashboard".

Das Menü "Widgets"

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

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, sodass Sie den Inhalt in aller Ruhe prüfen können. Die Schaltfläche ändert ihren Zustand in die Anzeige "Play Live Data", sobald eine Pause eingeleitet wird.

 **Play Live Data**

Wenn Sie fertig sind, klicken Sie einfach auf die Schaltfläche "Play Live Data", um die Datenerfassung neu zu starten und das Dashboard zu aktualisieren.

Standard-Dashboard-Schaltfläche

 **Default Dashboard**

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 Änderungen am Dashboard verloren.

Ändern der Größe, Minimieren, Umsortieren und Entfernen von Widgets



Ändern der Größe eines Widgets

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. Es wird ein gepunktetes Rechteck angezeigt, das die neue Widgetgröße 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 Maustaste 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 über den 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.

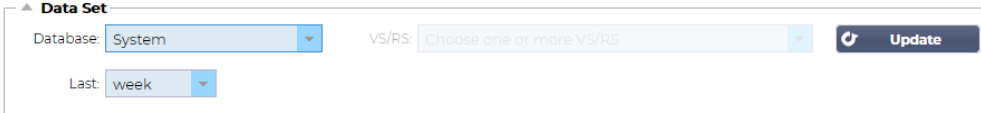
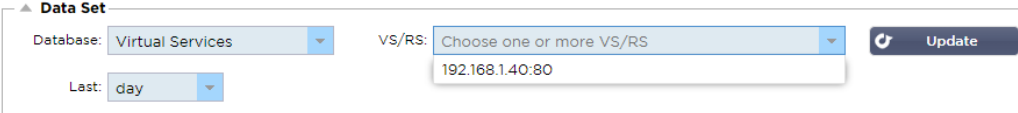
Außerdem können Sie so den Lastausgleich in Aktion sehen und Fehler oder Muster erkennen, die untersucht werden müssen. Beachten Sie, dass Sie die Verlaufsprotokollierung unter System > Verlauf aktivieren müssen, um diese Funktion nutzen zu können.

Anzeigen von grafischen Daten

Datensatz

Um die historischen Daten in grafischer Form 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 anzeigen möchten. Der Zeitraum, den Sie aus der Dropdown-Liste "Last" 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.

Data Set

Database: Real Servers VS/RS: Choose one or more VS/RS Update

Last: day

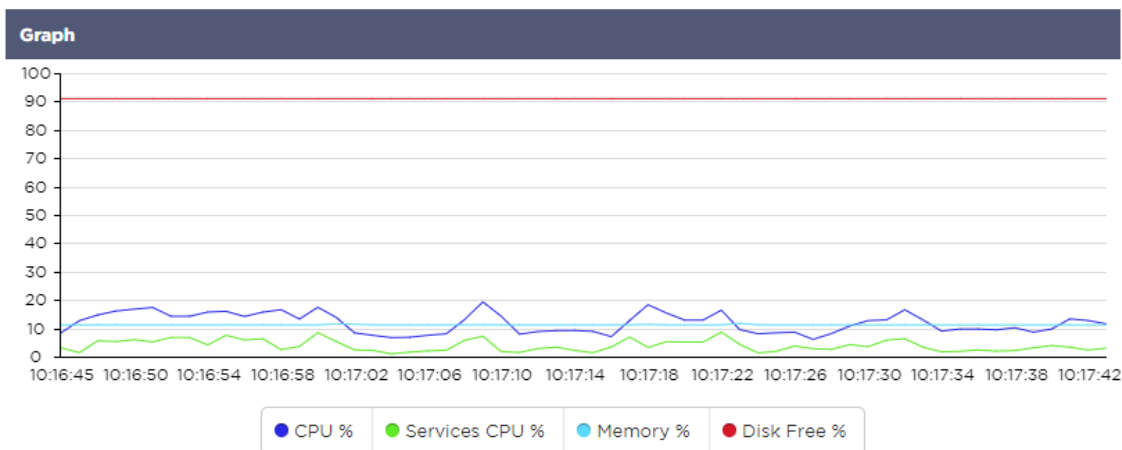
- 192.168.1.40:80-192.168.1.125:8080
- 192.168.1.40:80-192.168.1.119:8080

Metriken

Sobald Sie den zu verwendenden Datensatz ausgewählt haben, ist es an der Zeit, die anzuzeigenden Metriken zu wählen. Die Abbildung unten zeigt die Metriken, die dem Administrator zur Auswahl stehen: Diese Auswahlen entsprechen System, virtuellen Diensten und realen Servern (von links nach rechts).

Metrics	Metrics	Metrics
Data ☒ CPU % ☐ Services CPU % ☐ Memory % ☐ Disk Free %	Data ☐ Bytes In ☐ Bytes Out ☐ Bytes Cached ☐ Compression % ☐ Current Connections ☐ Request Per Second ☐ Cache Hits ☐ Cache Hits %	Data ☐ Bytes In ☐ Bytes Out ☐ Current Connections ☐ Pool Size ☐ Request Per Second ☐ Response Time
Show ☒ Averages ☐ Peak	Show ☐ Averages ☐ Peak	Show ☐ Averages ☐ Peak

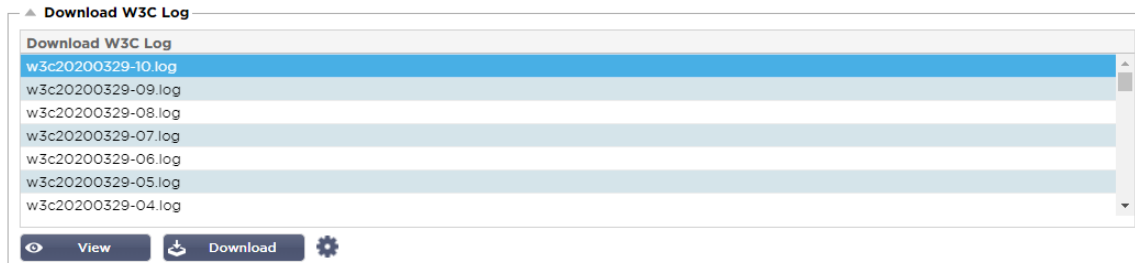
Beispielgrafik



Protokolle

Auf der Seite "Logs" im Bereich "View" 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 Internetprotokoll-(IP-)Adresse der Quelle, 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 anzeigen oder herunterladen.

Schaltfläche anzeigen

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

Schaltfläche 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 zu den W3C-Protokolleinstellungen, die sich unter System > Protokollierung befinden. Wir werden dies im Abschnitt "Protokollierung" in diesem Handbuch ausführlich besprechen.

Statistik

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

Komprimierung

Der gesamte Zweck des ADC besteht darin, Daten zu überwachen und sie an Real-Server zu leiten, die für den Empfang konfiguriert sind. Die Komprimierungsfunktion wird im ADC bereitgestellt, 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 Bereich "Komprimierung" der Statistik bereitgestellt.

Inhaltliche Komprimierung bis heute

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

Die in diesem Abschnitt gezeigten Daten geben den Grad der Komprimierung an, 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 höher 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 Gesamteingangs-/Ausgangszahlen 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 and Connections" (Treffer und Verbindungen) enthält die Gesamtstatistik für Treffer und Transaktionen, die das ADC durchlaufen. Was bedeuten also Treffer und Verbindungen?

- Ein Hit ist definiert als eine Schicht-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 Schicht-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 der Treffer pro Sekunde an.

Verbindungen insgesamt

Der Wert "Total Connections" stellt die kumulative Anzahl der TCP-Verbindungen seit dem letzten Zurücksetzen dar. Die Zahl in der zweiten Spalte gibt die pro Sekunde hergestellten TCP-Verbindungen zum ADC an. 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 Virtual Service und 6 TCP-Verbindungen pro Sekunde zu den Real Servern.

Peak-Verbindungen

Der Spitzenwert "Connections" stellt die maximale Anzahl der TCP-Verbindungen zum ADC dar. 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 Zwischenspeicherung 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.

▲ Caching		
Content Caching	Hits	Bytes
From Cache	= 0 / 0.0%	= 0 / 0.0%
From Server	= 495799 / 100.0%	= 1.97 GB / 100.0%
Cache Contents	= 0 entries	= 0 / 0.0%

Vom 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 Kilobyte 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 Gesamttransaktionen angegeben.

Bytes: Die zweite Spalte gibt die Gesamtdatenmenge in Kilobytes 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.

Hardware

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

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

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.

Speicherbelegung

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 schwankt.

Status

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

Virtueller Dienst Details

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

VIP-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. Realserver sind nicht erreichbar, oder es sind keine Realserver 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 weiterhin, jedoch mit reduzierter Real-Server-Kapazität.
	Offline. Realserver sind nicht erreichbar, oder es sind keine Realserver 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 verbundenen Real-Server aufgeführt.

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

Real Server

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

Hinweise

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

Conns (Verbindungen)

Durch die Darstellung der Anzahl der Verbindungen zu jedem Real-Server können Sie den Lastausgleich 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 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 eines Clusters für den ADC selbst deutlich. 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 erforderlich ist.
- 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.

Clustering

▲ **Role**

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

▲ **Settings**

Failover Latency (ms): Update

▲ **Management**

Unclaimed Devices

⬅
➡
⬆
⬆

Priority	Status	Cluster Members
1	●	192.168.1.220 EADC

Rolle

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

Cluster

▲ Role

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

- 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.
- Eine "Arbeitskonfiguration" umfasst alle Konfigurationsparameter, mit Ausnahme von Elementen, die eindeutig sein müssen, wie z. B. die Management-IP-Adresse, den ALB-Namen, die Netzwerkeinstellungen, die Schnittstellendetails und so weiter.
- 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
 - Geräteteil
 - Netzwerkbereich

Ausfall des Clustereigentümers

- Wenn ein Cluster-Eigentümer ausfällt, übernimmt automatisch eines der verbleibenden Mitglieder und führt den Lastausgleich des Datenverkehrs fort.
- Wenn der Eigentümer des Clusters 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 in 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 einem Verkehrsverlust kommt

Ändern der Rolle von der Clusterrolle in die manuelle Rolle

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

Role

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

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

Change Role

? Switching to the Manual role will enable all Virtual Services to become secondary.

Do you want to continue?

OK Cancel

- Klicken Sie auf die Schaltfläche OK
- Prüfen Sie den Abschnitt Virtuelle Dienste. Sie werden feststellen, dass in der Spalte "Primary" jetzt ein nicht angekreuztes Kästchen angezeigt wird.

Virtual Services			
+ Copy Service		Search	
Primary	VIP Status	Service Status	Enabled
☐			☒
☐			☒

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

Wechsel 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:

Change Role

? Switching to Standalone role will disable all Virtual Services.

Do you want to continue?

OK Cancel

- Klicken Sie auf OK, um die Rollen zu ändern.
- Überprüfen 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 jeden einzelnen aktivieren.

Manuell Rolle

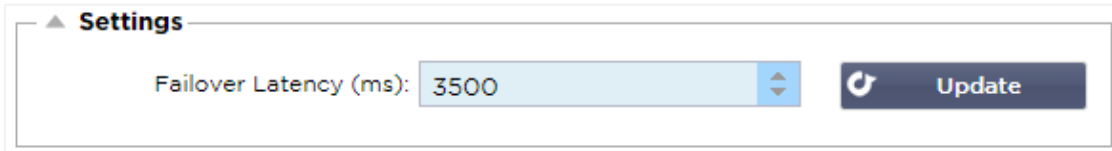
Ein ADC in der Rolle "Manual" arbeitet mit anderen ADCs in der Rolle "Manual" zusammen, um eine hohe Verfügbarkeit zu gewährleisten. Der Hauptvorteil gegenüber der Cluster-Rolle ist die Möglichkeit, festzulegen, welcher ADC für eine virtuelle IP aktiv ist. Der Nachteil ist, dass es keine Konfigurationssynchronisation 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 umschaltet:
 - Wenn beide Primary Columns angekreuzt sind, findet ein Wahlprozess statt, und die niedrigste MAC-Adresse ist aktiv
 - Wenn beide nicht angekreuzt sind, findet derselbe 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 in Bezug auf seine 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



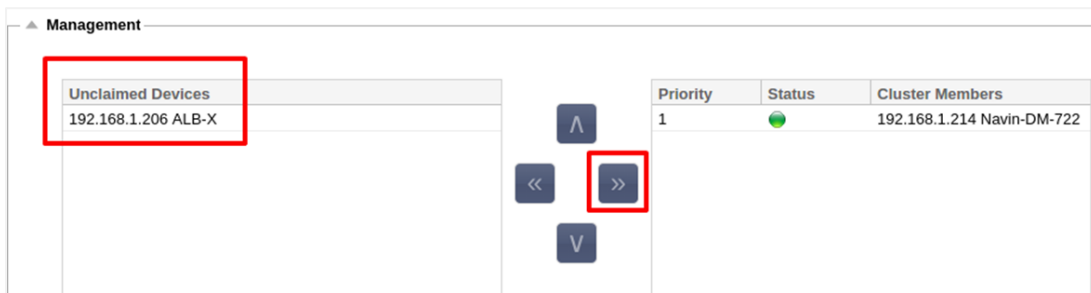
The screenshot shows a settings window titled "Settings" with a small triangle icon. Inside, there is a label "Failover Latency (ms):" followed by a text input field containing the value "3500". To the right of the input field is a small blue button with a double-headed vertical arrow. Further to the right is a dark blue button with a circular refresh icon and the text "Update".

Im Bereich Einstellungen können Sie die Failover-Latenz in Millisekunden einstellen, 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.

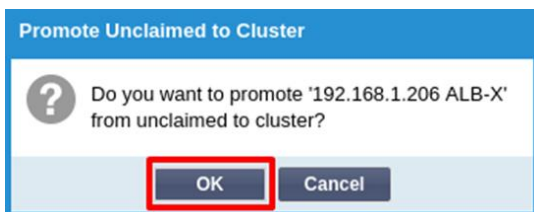
Verwaltung

In diesem Abschnitt können Sie Clustermitglieder hinzufügen und entfernen sowie 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 grünem Status und seinem Namen unter der Spalte Clustermitglieder 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 ein 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 Pfeilschaltfläche.
- Sie sehen nun die folgende Meldung:

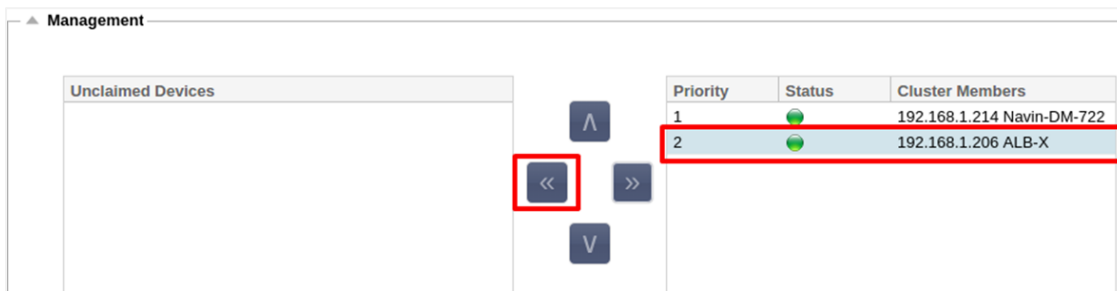


- Klicken Sie auf OK, um den ADC in den Cluster zu befördern.
- Ihr ADC sollte nun als Priorität 2 in der Liste der Clustermitglieder angezeigt werden.



Entfernen eines Clustermitglieds

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

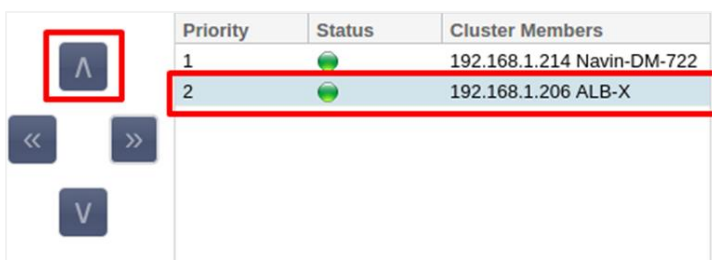


- Sie erhalten eine Bestätigungsaufforderung.
- Klicken Sie zur Bestätigung auf OK.
- Ihr ADC wird entfernt und auf der Seite "Nicht beanspruchte Geräte" angezeigt.

Ändern der Priorität eines ADCs

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

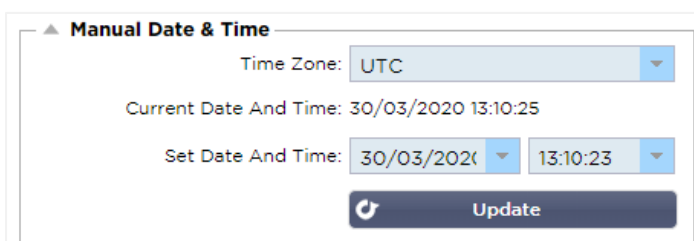
- Der ADC an der Spitze der Liste der Clustermittglieder erhält die Priorität 1 und ist der aktive ADC für alle virtuellen Dienste
- Der ADC, der an zweiter Stelle in der Liste steht, erhält Priorität 2 und ist der passive ADC für alle virtuellen Dienste
- Um zu ändern, welcher ADC aktiv ist, markieren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



Datum und Uhrzeit

Der Abschnitt "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 Verfahren im Zusammenhang mit der SSL-Verschlüsselung.

Manuelles Datum und Uhrzeit



Zeitzone

Der Wert, den Sie in diesem Feld einstellen, stellt die Zeitzone dar, 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 das 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, wählen Sie Europa/London, um Ihren Standort festzulegen

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 der ersten Dropdown-Liste oder, alternativ können Sie das Datum in folgendem Format eingeben DD/MM/YYYY
- Geben Sie die Uhrzeit im folgenden Format hh: mm: ss ein, z. B. 06:00:10 für 6 Uhr morgens und 10 Sekunden.
- Wenn Sie diese 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.

▲ Synchronise Date & Time (UTC)

Enabled: ☒

Time Server URL:

Update At [hh:mm]:

Update Period [hours]:

NTP Type:

Update

Zeitserver-URL

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

Aktualisierung um [hh:mm]

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

Aktualisierungszeitraum [Stunden]:

Wählen Sie aus, wie oft die Synchronisierung erfolgen soll.

NTP Typ:

- Public SNTP V4 - Dies ist die aktuelle und bevorzugte Methode für die 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](#)

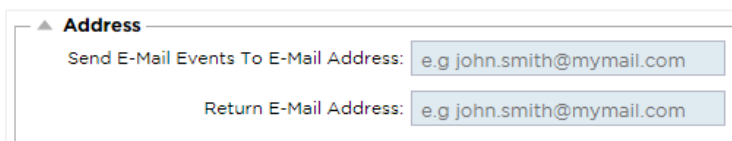
Hinweis: Bitte beachten Sie, dass die Synchronisation nur in UTC erfolgt. Wenn Sie eine lokale Zeit einstellen möchten, kann dies nur manuell erfolgen. Diese Einschränkung wird in späteren Versionen geändert, um die Möglichkeit zu schaffen, eine Zeitzone auszuwählen.

E-Mail-Ereignisse

Das ADC ist ein kritisches Gerät, und wie jedes wichtige System ist es 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

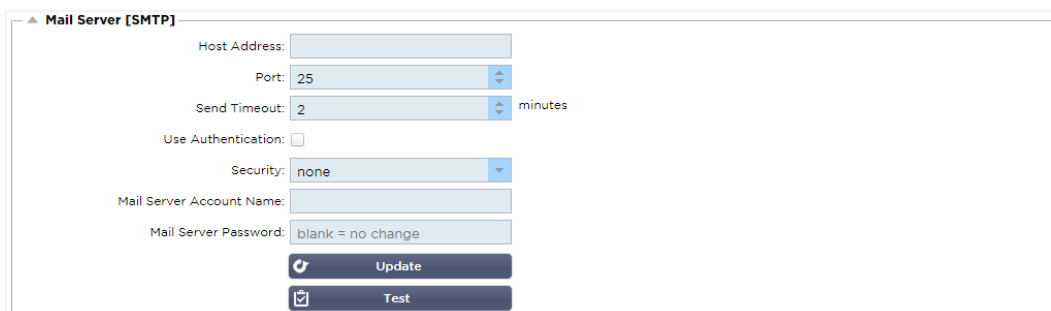
Fügen Sie eine gültige E-Mail-Adresse hinzu, an die die Alarmer, Benachrichtigungen und Ereignisse gesendet werden sollen. Beispiel support@domain.com.

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 eingeben, 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.

Sendezeitüberschreitung

Fügen Sie ein SMTP-Timeout 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 Alarmer

Es gibt verschiedene Arten von Ereignisbenachrichtigungen, die das ADC an Personen sendet, die dafür konfiguriert sind, sie zu empfangen. Sie können die Benachrichtigungen und Alarmer, die versendet werden sollen, ankreuzen und aktivieren. Benachrichtigungen treten auf, wenn Real Servers kontaktiert oder Kanäle gestartet werden. Warnungen treten auf, wenn Real Servers 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 durchgeführt, 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 das 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.

Gruppenbenachrichtigungen

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

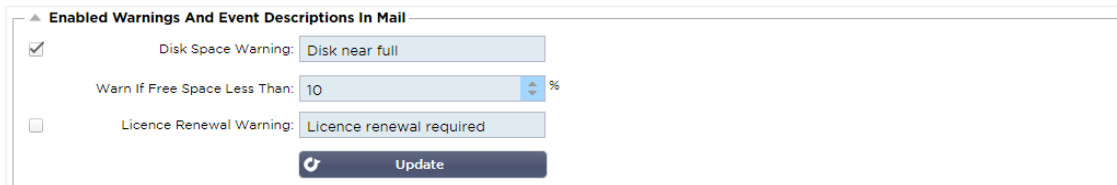
Gruppenmail Beschreibung

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

Gruppe Sendeintervall

Legen Sie die Zeit fest, die gewartet werden soll, bevor eine Gruppenbenachrichtigungs-E-Mail gesendet wird. 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 Abschnitt "System" gibt es die Option "Systemverlauf", die die Lieferung von Verlaufsdaten für Elemente wie CPU, Speicher, Anfragen pro Sekunde und andere Merkmale ermöglicht. Sobald diese Option aktiviert ist, können Sie die Ergebnisse in grafischer Form über die Seite Ansicht > Verlauf anzeigen. Auf dieser Seite können Sie auch Ihre Verlaufsdateien auf dem lokalen ADC sichern oder wiederherstellen.

Daten sammeln



- Um die Erfassung der Daten zu aktivieren, setzen Sie bitte einen Haken in die Checkbox.
- Stellen Sie als nächstes das Zeitintervall ein, in dem der ADC die Daten erfassen soll. Dieser Zeitwert kann zwischen 1-60 Sekunden liegen.

Wartung

Maintenance

Most Recent Update

Tue, 31 Mar 2020 08:28:09

Refresh

Backup

Backup Name:

Backup

Delete

Select To Delete:

Delete

Restore

Select To Restore:

Restore

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 ermöglichen.

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 aus. Klicken Sie auf Löschen, um die Sicherungsdatei aus dem ADC zu entfernen

Wiederherstellen

Wählen Sie eine zuvor gespeicherte Sicherungsdatei aus. 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 unbestimmte Zeit 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.

▲ Licence Details	
Licence ID:	EA5325D4-4796-48CC-B27E-70B2FFC3B79E
Machine ID:	F477F3B4-CC5
Issued To:	edgeNEXUS
Contact Person:	Greg Howett
Date Issued:	24 Nov 2020
Name:	Sergey Box

Lizenz-ID

Diese Lizenz-ID ist direkt mit der Maschinen-ID und anderen Details verknüpft, 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.

Maschinen-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 Unterstützung 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](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

▲ Facilities	
Layer 4:	Permanent licence
Layer 7:	Permanent licence
SSL:	Permanent licence
Acceleration:	Permanent licence
flightPATH:	Permanent licence
Pre-Authentication:	Permanent licence
Global Server Load-Balancing:	Timed licence: 6 days(06 Apr 2020) Quote: 50E-FF43-379
Firewall:	Timed licence: 6 days(06 Apr 2020) Quote: 50E-FF43-379
Throughput:	3 Gbps permanent licence Unlimited timed licence: 6 days(06 Apr 2020) Quote: 50E-FF43-379
Virtual Service IPs:	32 Virtual Service IPs permanent licence
Real Server IPs:	120 Real Server IPs permanent licence

Im Bereich Einrichtungen erhalten Sie Informationen darüber, welche Funktionen innerhalb des ADC zur Nutzung lizenziert wurden und wie lange die Lizenz gültig ist. 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 in das Feld "Lizenz einfügen" kopieren und einfügen.
- Sie können es auch in das ADC hochladen, wenn Kopieren/Einfügen für Sie keine Option ist.
- Wenn Sie dies getan haben, klicken Sie bitte auf die Schaltfläche Update
- Die Lizenz ist nun installiert.

Lizenz-Service-Informationen

Durch Klicken auf die Schaltfläche Lizenz-Service-Information werden alle Informationen zur Lizenz angezeigt. Diese Funktion kann zum Senden der Details an das Supportpersonal verwendet werden.

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 Zugriffsanforderung 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 stehen verschiedene Protokollierungsebenen zur Verfügung, und je nach Dienstyp 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 über die Bedeutung der Felder finden Sie in der nachstehenden Feldübersicht. 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. In der Zusammenfassung der Felder unten finden Sie Informationen zur Bedeutung der Felder. 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 Arten von Informationen gefüllt, die für Entwicklungs- und Supportmitarbeiter 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 diese angezeigt.
Weitergeleitet-für Adresse und Port	Mit dieser Option werden die im XFF-Header enthaltenen Details angezeigt, einschließlich Adresse und Port.
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 "on" 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.

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
- Hinzufügen des Ports
- Wählen Sie TCP oder UDP
- Markieren Sie das Kästchen
- Klicken Sie auf Aktualisieren

Fernspeicherung von Protokollen

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
Fernspeicherung von Protokollen	Aktivieren Sie das Kontrollkästchen, um die Remote-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 Standortformat = Millisekunde des Zeitstempels
c-ip	Client-IP so gut wie möglich aus Netzwerk oder X-Forwarded-For-Header ableiten
c-anschluss	Client-Port, wie er sich am besten aus dem Netzwerk oder dem X-Forwarded-For-Header ableiten lässt
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 die cs-Methode
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 Kunden 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 vom Real-Server, in der Antwort
sc-bytes	An den Client gesendete Bytes, in der Antwort
x-prozentig	Komprimierungsprozentsatz $\ast = 100 \ast (1 - \text{Ausgang} / \text{Eingang})$ einschließlich Header
Zeit genommen	Wie lange der Real-Server in Sekunden gebraucht hat
x-trip-Zeiten neu pcon	Millisekunde vom Verbinden bis zum Eintrag in die "Neulingsliste" Millisekunde von connect bis zum Aufbau der Verbindung zum Real-Server
acon	Millisekunde vom Verbinden bis zur Beendigung des Verbindungsaufbaus mit dem Real-Server
rcon	Millisekunde von connect bis zum Aufbau der Real-Server-Verbindung
rqi	Millisekunde vom Connect bis zum Empfang des ersten Bytes der Anfrage vom Client
rql	Millisekunde vom Connect bis zum Empfang des letzten Bytes der Anfrage vom Client
tqi	Millisekunde vom Connect bis zum Senden des ersten Bytes der Anfrage an den Real-Server
tql	Millisekunde vom Connect bis zum Senden des letzten Bytes der Anfrage an den Real-Server
rsf	Millisekunde vom Connect bis zum Empfang des ersten Bytes der Antwort vom Real-Server
rsl	Millisekunde vom Connect bis zum Empfang des letzten Bytes der Antwort vom Real-Server
tsf	Millisekunde vom Connect bis zum Senden des ersten Bytes der Antwort an den Client
tsl	Millisekunde vom Connect 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)
Protokoll	Millisekunde von der 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 (bzw. 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 reagierte 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 die Art des Protokolls, das Sie löschen möchten, aus dem Dropdown-Menü auswählen und dann auf die Schaltfläche "Löschen" klicken.

Netzwerk

Der Abschnitt "Network" in der Bibliothek ermöglicht die Konfiguration der Netzwerkschnittstellen des ADC und deren Verhalten.

Grundeinstellung

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 neben der IP-Adresse ein weißes Häkchen in einem grünen Kreis.

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 neben der IP-Adresse ein weißes Häkchen in einem grünen Kreis.

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.

Adapter Details

+ Add Adapter - Remove Adapter

Adapter	VLAN	IP Address	Subnet Mask	Gateway	RP Filter	Description	Web Console	REST
eth0		192.168.1.111	255.255.255.0		☒	Green side	☒	☒

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 durch Anklicken aus - ein Doppelklick versetzt die Auflistungszeile 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, ermöglicht aber eine einfachere Gruppierung von Endstationen, die sich nicht am gleichen Netzwerk-Switch befinden
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 vierfacher 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 vierfacher punktierter Dezimaldarstellung 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, von dieser Schnittstelle initiierte Verbindungen über diese Schnittstelle an den angegebenen Gateway-Router zurückzuleiten. 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: Das ADC benennt automatisch die erste Schnittstelle Grüne Seite, die zweite Schnittstelle Rote Seite und die dritte Schnittstelle Seite 3 usw. Sie können diese Namenskonventionen nach Belieben ändern.
Web-Konsole	Doppelklicken Sie auf die Spalte und aktivieren Sie das Kontrollkästchen, um die Schnittstelle als Verwaltungsadresse für die grafische Benutzeroberfläche Web Console zuzuweisen. Seien Sie bitte sehr vorsichtig, wenn Sie die Schnittstelle ändern, auf der die Web-Konsole lauschen soll. Sie müssen das richtige Routing eingerichtet haben oder sich im gleichen Subnetz wie die neue Schnittstelle befinden, um die Web Console 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 sich auf die Netzwerkschnittstelle beziehen. Sie können eine Netzwerkschnittstelle auch aus der Liste entfernen, indem Sie auf die Schaltfläche Entfernen klicken. Wenn Sie eine virtuelle Appliance verwenden, sind die hier angezeigten Schnittstellen durch das zugrunde liegende Virtualisierungs-Framework begrenzt.

Interfaces				
Remove				
ETH Type	Status	Speed	Duplex	Bonding
eth0		auto	auto	none
eth1		auto	auto	none

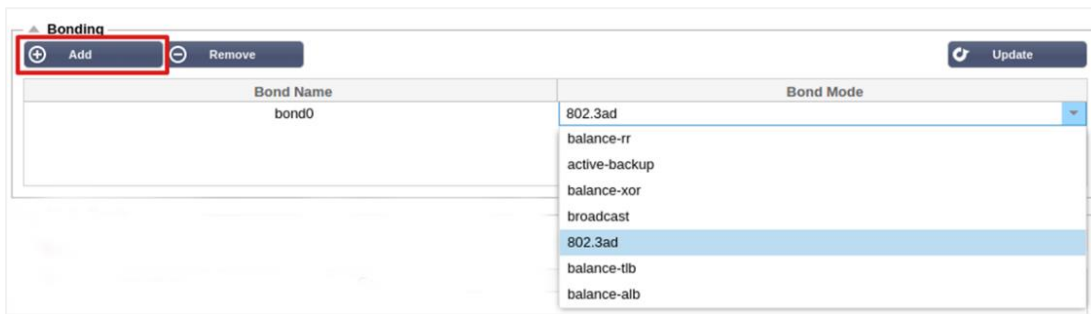
Säule	Beschreibung
ETH-Typ	Dieser Wert gibt die interne OS-Referenz auf die Netzwerkschnittstelle an. Dieses Feld kann nicht angepasst werden. Die Werte beginnen mit ETH0 und werden in Abhängigkeit von der Anzahl der Netzwerkschnittstellen fortgesetzt.
Status	Diese grafische Anzeige zeigt den aktuellen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

Kleben

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 integrierten Bonding-Treiber zum Zusammenfassen mehrerer physischer Netzwerkschnittstellen zu einer einzigen logischen Schnittstelle (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 Modusoptionen, die jeweils spezifische Lastausgleichs- und Fehlertoleranzmerkmale bieten. Diese sind in der folgenden Abbildung dargestellt.

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

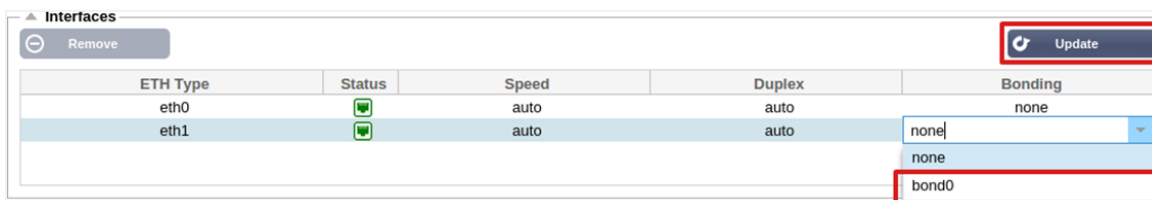


Erstellen eines Bonding-Profiles

- 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 nun Teil von bond0. Während Eth0 als Verwaltungsschnittstelle für sich allein bleibt.



Bonding-Modi

Bonding-Modus	Beschreibung
balance-rr:	Pakete werden sequentiell über jede Schnittstelle einzeln gesendet/empfangen.
Aktiv-Sicherung:	In diesem Modus ist eine Schnittstelle aktiv und die zweite Schnittstelle befindet sich im Standby-Modus. Diese zweite Schnittstelle wird nur dann aktiv, wenn die aktive Verbindung auf der ersten Schnittstelle ausfällt.
balance-xor:	Sendet basierend auf der Quell-MAC-Adresse, die mit der Ziel-MAC-Adresse XOR-verknüpft ist. 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:	Erstellt Aggregationsgruppen, die dieselben Geschwindigkeits- und Duplexeinstellungen verwenden und alle Slaves im aktiven Aggregator gemäß der 802.3ad-Spezifikation nutzen.
balance-tlb:	Der Bonding-Modus "Adaptive Transmit Load Balancing": Bietet Kanalbündelung, die keine spezielle Switch-Unterstützung erfordert. Der ausgehende Verkehr wird entsprechend der aktuellen Last (berechnet relativ 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.

Destination	Gateway	Mask	Adapter	Active
10.117.64	192.168.1.254	255.255.255.0	eth0	

Update Cancel

Hinzufügen einer statischen Route

- Klicken Sie auf die Schaltfläche Route hinzufügen
- Füllen Sie das Feld aus und verwenden Sie dabei die Angaben in der nachstehenden Tabelle als Anleitung.
- Klicken Sie abschließend auf die Schaltfläche Aktualisieren.

Feld	Beschreibung
Zielort	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 punktierter Notation ein. Beispiel 255.255.255.0
Adapter	Geben Sie den Adapter an, 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 an dieser Schnittstelle nicht erreicht werden kann. Vergewissern Sie sich, dass Sie eine Schnittstelle und eine IP-Adresse im gleichen Netzwerk wie das Gateway eingerichtet haben

Details zur statischen Route

In diesem Abschnitt finden Sie Informationen zu allen auf dem ADC konfigurierten Routen.

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

Kernel IPv6 routing table

Erweiterte Netzwerkeinstellungen

Server Nagle: ☐

Client Nagle: ☐

Update

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 ZU NAGLE](#)

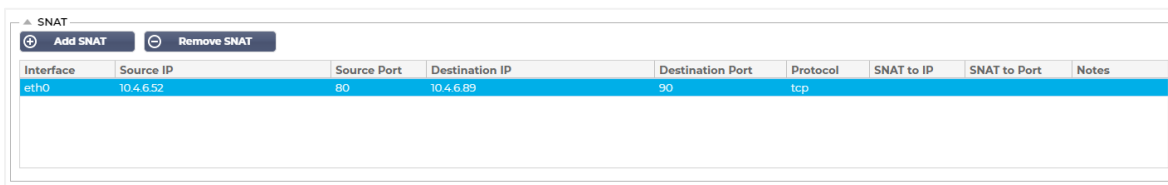
Server Nagle

Aktivieren Sie dieses Feld, 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 Servereinstellungen 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



Interface	Source IP	Source Port	Destination IP	Destination Port	Protocol	SNAT to IP	SNAT to Port	Notes
eth0	10.4.6.52	80	10.4.6.89	90	tcp			

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 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, die in der SNAT-Regel angegeben ist. SNAT kann in den Lastausgleichsmodi Layer 4 und Layer 7 verwendet werden.

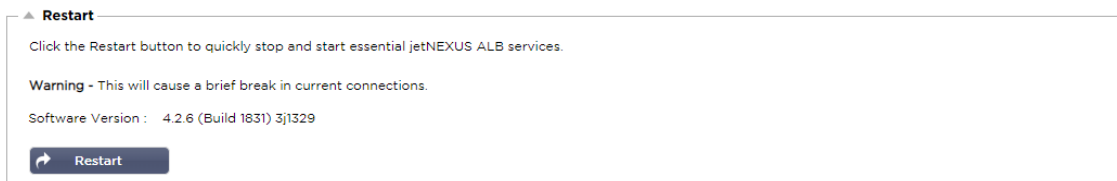
Feld	Beschreibung
Quelle IP	Die Quell-IP-Adresse ist optional, sie kann entweder eine Netzwerk-IP-Adresse (mit /mask) oder eine einfache IP-Adresse sein. Die Maske kann entweder eine Netzwerkmaske oder eine einfache Zahl sein, die die Anzahl der 1en auf der linken Seite der Netzwerkmaske angibt. So entspricht eine Maske von /24 der Adresse 255.255.255.0.
Ziel-IP	Die Ziel-IP-Adresse ist optional, sie 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 Hafen	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.
Zielhafen	Der Zielanschluss ist optional, er kann eine einzelne Zahl sein, in diesem Fall gibt er nur diesen Anschluss an, oder er kann einen Doppelpunkt enthalten, der einen Bereich von Anschlüssen angibt. Beispiele: 80 oder 5900:5905.

Protokoll	Sie können wählen, ob Sie SNAT auf ein einzelnes Protokoll oder auf alle Protokolle anwenden 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 zum Anschluss	Der SNAT to Port ist optional, er kann eine einzelne Zahl sein, in diesem Fall gibt er nur diesen Port an, oder er kann einen Bindestrich enthalten, der einen Bereich von Ports angibt. Beispiele: 80 oder 5900-5905.
Hinweise	Verwenden Sie dies, um einen freundlichen Namen zu setzen, um sich daran zu erinnern, warum die Regeln existieren ;-). Dies ist auch nützlich für die Fehlersuche im Syslog.

Leistung

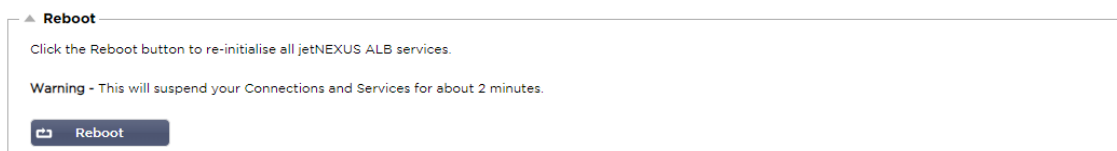
Mit dieser Funktion des ADC-Systems können Sie auch verschiedene strombezogene Aufgaben an Ihrem ADC durchführen.

Neustart



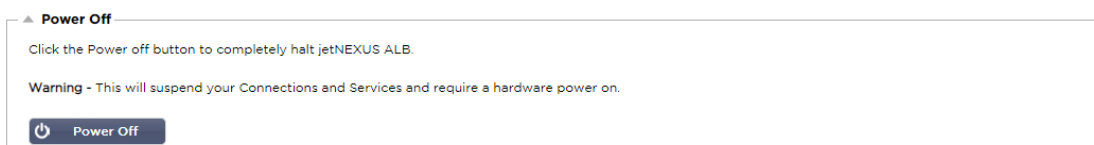
Diese Einstellung löst einen globalen Neustart aller Dienste aus und unterbricht damit alle derzeit aktiven Verbindungen. Alle Dienste werden nach einer kurzen Zeitspanne automatisch wieder aufgenommen, aber der Zeitpunkt hängt davon ab, wie viele Dienste konfiguriert sind. Es wird ein Popup-Fenster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

Neustart



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

Ausschalten



Durch Klicken auf die Schaltfläche "Power Off" (Ausschalten) 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 Kennwort für die Webkonsole ändern und den Secure Shell-Zugang aktivieren oder deaktivieren. Er ermöglicht auch die Aktivierung der REST-API-Fähigkeit.

SSH

▲ SSH

Secure Shell Remote Conn: ☒

Option	Beschreibung
Sichere Shell-Fernverbindung	Bitte kreuzen Sie das Kästchen an, wenn Sie per SSH Zugriff auf den ADC erhalten möchten. "Putty" ist eine hervorragende Anwendung dafür.

Web-Konsole

▲ Webconsole

SSL Certificate: default

Secure Port: 443

 Update

SSL-Zertifikat Wählen Sie in der Dropdown-Liste ein Zertifikat aus. 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 Abschnitt [SSL-ZERTIFIKATE](#) importieren.

Option	Beschreibung
Sicherer Anschluss	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.

▲ REST API

Enable REST: ☐

SSL Certificate: default

Port:

IP Address: 192.168.1.111 

 Update

Option	Beschreibung
REST freigeben	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 Cog-Link klicken, um auf die Netzwerkseite zuzugreifen und zu ändern, auf welchem Adapter der REST-Dienst aktiviert ist.
Zahnradverbindung	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 bei der Unterstützung von Abfragezeichenfolgen 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 Software von Drittanbietern abgefragt werden, die mit Geräten kommunizieren können, 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. Die Standard-Community-Zeichenfolge 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 Objektidentifikatoren (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 jetnexusGesamtEingabeBytes (1.3.6.1.4.1.38370.1.1.1.0)

.2 jetnexusGesamtAusgabeBytes (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)

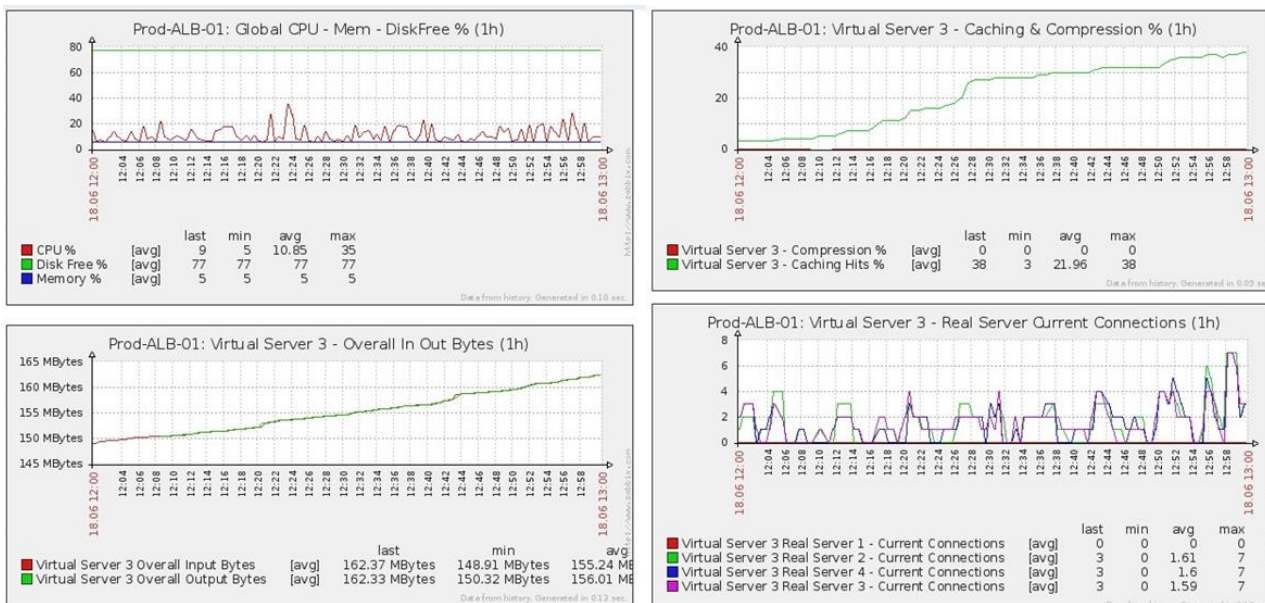
.2 jnrealserverIndexRealServer (1.3.6.1.4.1.38370.1.3.1.2)

.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 auf eine Managementkonsole Ihrer Wahl auszulagern. Nachfolgend finden Sie einige Beispiele von Zabbix, die einen ADC für verschiedene oben aufgeführte OID-Werte abfragen.



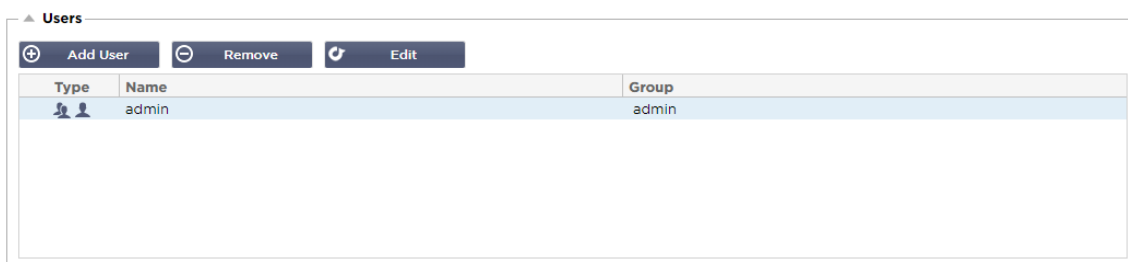
Benutzer und Audit-Protokolle

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

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

Benutzer

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



Benutzer hinzufügen

Klicken Sie auf die Schaltfläche "Benutzer hinzufügen" in der obigen Abbildung, um das Dialogfeld "Benutzer hinzufügen" aufzurufen.

Parameter	Beschreibung/Verwendung
Benutzername	Geben Sie einen Benutzernamen Ihrer Wahl ein Der Benutzername muss folgende Bedingungen erfüllen: • 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 Read - 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 hat • 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 Kennwort 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 aktuell angemeldeten Benutzer 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
- Aus Gründen der Abwärtskompatibilität können Sie den Admin-Benutzer 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 markieren und die
- Sie können auch das Passwort eines Benutzers ändern, sofern Sie über Administratorrechte verfügen

Audit-Protokoll

Der 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 "**Logs**" sehen. Zum Beispiel:

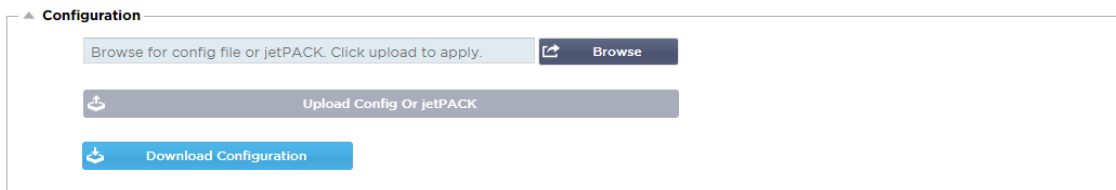
▲ **Audit Log**

Date/Time	Username	Section	Action
01:04:28 Thu 28 May 2015	admin	Network	from [. 0.0.0.0.0.0.0.192.168.1.1.0.] to []
01:02:27 Thu 28 May 2015	admin	error	ERROR:Subnet 192.168.1.214 must not overlap with subnet 192.168.1.215
01:02:27 Thu 28 May 2015	admin	Address	[Green side . 192.168.1.214/255.255.255.0,Red Side . 192.168.1.215/255.255.255.0]
00:54:48 Thu 28 May 2015	admin	error	Invalid uploaded licence format.
00:39:57 Thu 28 May 2015	admin	flightPATH Evaluatio...	Variable=\$variable1\$, Source=, Detail=, Value=
00:39:57 Thu 28 May 2015	admin	flightPATH Action	1 Action=use_server, Target=192.168.0.75, Value=
00:39:57 Thu 28 May 2015	admin	flightPATH Condition	1 Condition=host, Sense=does, Check=exist, Match=, Value=

 View  Download

Erweitert

Konfiguration



Es ist immer die beste Vorgehensweise, die Konfiguration des ADC herunterzuladen und zu speichern, sobald es 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 zur Verfügung gestellt, um Ihre Arbeit zu vereinfachen. Auch diese können über das Konfigurationsmodul in 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 erscheint ein Pop-up-Fenster, 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 lädt die Konfiguration hoch, wendet sie an und aktualisiert dann den Browser. Wenn der Browser nicht automatisch aktualisiert wird, klicken Sie bitte auf "Refresh" (Aktualisieren) im Browser.
- Sie werden nach Abschluss zur Dashboard-Seite weitergeleitet.

Hochladen eines jetPACKs

- Ein jetPACK ist ein Satz von Konfigurationsaktualisierungen 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.
- Bei komplexeren Bereitstellungen wie Microsoft Lync etc. kann der Import länger dauern.

Globale Einstellungen

Im Abschnitt "Globale Einstellungen" können Sie verschiedene Elemente ändern, einschließlich der kryptografischen SSL-Bibliothek.

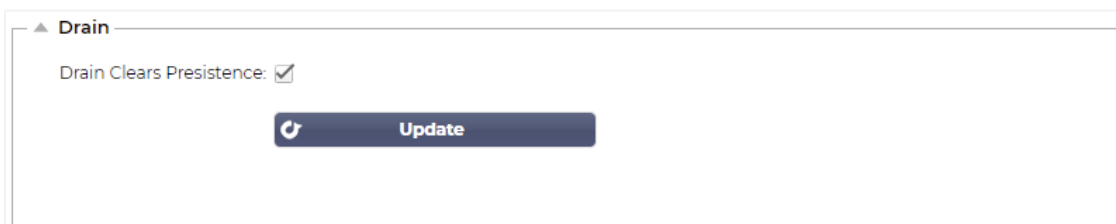
Host-Cache-Timer



The screenshot shows a configuration panel titled "HostCache Timer". It contains a text input field labeled "HostCache Timer (s):" with the value "1" entered. Below the input field is a dark blue button with a circular refresh icon and the text "Update".

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

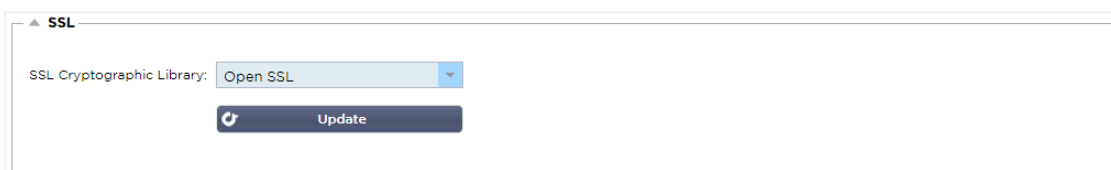
Ablassen



The screenshot shows a configuration panel titled "Drain". It contains a checkbox labeled "Drain Clears Persistence:" which is checked. Below the checkbox is a dark blue button with a circular refresh icon and the text "Update".

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

SSL



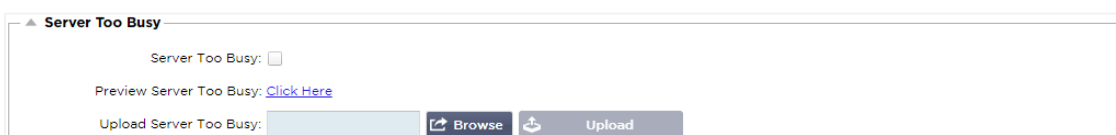
The screenshot shows a configuration panel titled "SSL". It contains a dropdown menu labeled "SSL Cryptographic Library:" with "Open SSL" selected. Below the dropdown is a dark blue button with a circular refresh icon and the text "Update".

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 wollten, könnte dies hier geändert werden.

Protokoll

Im Abschnitt "Protokoll" werden die vielen erweiterten Einstellungen für das HTTP-Protokoll vorgenommen.

Server zu stark ausgelastet



The screenshot shows a configuration panel titled "Server Too Busy". It contains a checkbox labeled "Server Too Busy:" which is unchecked. Below the checkbox is a link labeled "Preview Server Too Busy: [Click Here](#)". At the bottom, there is a text input field labeled "Upload Server Too Busy:" followed by two buttons: "Browse" (with a folder icon) and "Upload" (with an upload icon).

Angenommen, Sie haben die maximalen Verbindungen zu Ihren Real-Servern begrenzt; Sie können wählen, ob eine freundliche Webseite angezeigt werden soll, wenn dieses Limit erreicht wurde.

- 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 Ihre neu erstellte HTM(L)-Datei für die Webseite
- Hochladen anklicken
- Wenn Sie eine Vorschau der Seite wünschen, können Sie dies mit dem Link Hier klicken tun

Weitergeleitet für

Forwarded For:

Forwarded-For Output:

Forwarded-For Header:

 Update

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

Weiterleiten-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 einigen 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. Erstellen Sie nach dem Herunterladen ein benutzerdefiniertes Protokollierungsfeld namens X-Forwarded-For mit den folgenden Einstellungen.

Wählen Sie in der Liste Quellentyp die Option Standard aus, wählen Sie im Feld Quellenname die Option Anforderungskopf und geben Sie X-Forwarded-For ein.

[HTTP://www.iis.net/learn/extensions/advanced-logging-module/advanced-logging-for-iis-custom-logging](http://www.iis.net/learn/extensions/advanced-logging-module/advanced-logging-for-iis-custom-logging)

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 sind unten aufgeführt:

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" kombiniert 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 existiert, 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

HTTP Compression Settings

Initial Thread Memory [KB]: 128

Maximum Thread Memory [KB]: 99999

Increment Memory [KB]: 0
(0 to double)

Minimum Compression Size [Bytes]: 200

Safe Mode: ☐

Disable Compression: ☐

Compress As You Go: By Page Request

Update

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 kann. 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 Anforderung zuweist. Für maximale Leistung speichert und komprimiert die 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. 128 KB, dann 256 KB, dann 512 KB usw.), bis zu der durch die maximale Speichernutzung pro Thread festgelegten Grenze. 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 128 KB oder weniger groß, aber gelegentliche Antworten sind 1 MB 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 die ADC nicht versucht, zu komprimieren. Dies ist nützlich, da alles, was deutlich unter 200 Byte liegt, nicht gut komprimiert wird und aufgrund des Overheads der Komprimierungsheader sogar an Größe zunehmen 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, aber einige andere Proxy-Server, auch wenn sie behaupten, HTTP/1.1-konform zu sein, können komprimierte Stylesheets und JavaScript nicht korrekt transportieren. 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 Chunk, der vollständig dekomprimiert werden kann. AUS - Verwenden Sie "Compress As You Go" nicht auf dieser Seite. Nach Seitenanforderung - Verwenden Sie "Compress as You Go" nach Seitenanforderung.

Globale Komprimierungsausschlüsse

Global Compression Exclusions

Current Exclusions:

- *.css
- *.js

Update

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.

Software

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

Details zum Software-Upgrade

ALB Software Upgrade Details

User Name: admin

Machine ID: 50E-FF4

Licence ID: {C3E60CA1-6155-4E69-}

Licence Expiry: 2021-03-24

ALB Location: Altrincham, United Kingdom

Support Expiry: 2021-03-24

Support Type: Premium

Current Software Version: 4.2.6 (Build 1631) 3j1329

Refresh To View Available Software

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 from 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
- Zeigt das Ergebnis "ping: unknown host appstore.edgenexus.io. "
- Der ADC wird NICHT in der Lage sein, etwas aus der Cloud herunterzuladen

Download aus der Cloud

Download From Cloud					
Code Name	Release Date	Version	Build	Release Notes	Notes
ALB-X Version 4.2.0 - Not for 4.1...	2018-09-21	4.2.0	1727	Our Next Big Feature	Please DO NOT purchase this app
jetNEXUS ALB-X Version 4.1.4	2018-09-21	4.1.4	1653	Carbon SP3 4.2.4	jetNEXUS ALB-X Accelerating Lo
OWASP Core Rule Set 3.0.2 Upda...	2019-10-28	3.0.2_14.0...	jetNEXUS	The OWASP CRS is a	The OWASP CRS is a set of web
Curl Update 7.50.3	2018-09-21	7.50.3	jetNEXUS	This software update	This software update is a pre-req
Disable CBC mode Ciphers and W...	2017-03-14	1.0	jetNEXUS	This software update	This software update disables CB
ALB-X Version 4.2.1 - Not for 4.1.x...	2017-08-23	4.2.1	1734	Click here for release	Please DO NOT purchase this app
ALB-X Version 4.2.2 - Not for 4.1.x...	2017-08-23	4.2.2	1745	Click here for release	Please DO NOT purchase this app

Download Selected Software To ALB

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 das 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 auf ALB hochladen

Apps hochladen

Software Version: 4.2.6 (Build 1831) 3j1329

Browse for software file then click upload to apply.

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 Abschnitt Bibliothek> Apps.
- Sie müssen dann jede App in diesem Abschnitt einzeln bereitstellen.

Software

Software Version: 4.2.6 (Build 1831) 3j1329

Browse for software file then click upload to apply.

- 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 Abschnitt "Auf ALB gespeicherte Software" angezeigt, von wo aus Sie sie nach Belieben anwenden können.

Auf ALB gespeicherte Software anwenden

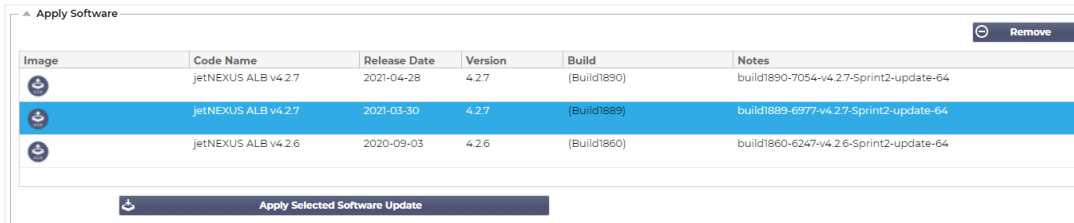


Image	Code Name	Release Date	Version	Build	Notes
	jetNEXUS ALB v4.2.7	2021-04-28	4.2.7	(Build1890)	build1890-7054-v4.2.7-Sprint2-update-64
	jetNEXUS ALB v4.2.7	2021-03-30	4.2.7	(Build1889)	build1889-6977-v4.2.7-Sprint2-update-64
	jetNEXUS ALB v4.2.6	2020-09-03	4.2.6	(Build1860)	build1860-6247-v4.2.6-Sprint2-update-64

Buttons: Remove, Apply Selected Software Update

In diesem Abschnitt werden alle Softwaredateien angezeigt, die auf dem ALB gespeichert und für die Bereitstellung verfügbar sind. Die Auflistung enthält 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 wird, 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 Ursache und Lösung zu kommen. In diesem Abschnitt können Sie das tun.

Support-Dateien



Support Files

Time Frame: 3 days

Download Support Files

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 im 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

Trace

Nodes To Trace:

Connections: ☐

Cache: ☐

Data: ☐

flightPATH:

Server Monitoring: ☒

Monitoring Unreachable: ☐

Auto-Stop Records:

Auto-Stop Duration:

Purpose:

Trace: ----- trace started for Monitoring -----
 Trace: Monitoring: Success: Connect: 192.168.1.40:80 192.168.1.119:8080 Connected in 1ms
 Trace: Monitoring: Success: Connect: 192.168.1.40:80 192.168.1.125:8080 Connected in 2ms
 Trace: Monitoring: Success: Connect: 192.168.1.40:80 192.168.1.125:8080 Connected in 2ms
 Trace: Monitoring: Success: Connect: 192.168.1.40:80 192.168.1.119:8080 Connected in 1ms
 Trace: Monitoring: Success: Connect: 192.168.1.40:80 192.168.1.125:8080 Connected in 9ms
 Trace: Monitoring: Success: Connect: 192.168.1.40:80 192.168.1.119:8080 Connected in 1ms
 Trace: Monitoring: Success: Connect: 192.168.1.40:80 192.168.1.125:8080 Connected in 14ms
 Trace: Monitoring: Success: Connect: 192.168.1.40:80 192.168.1.125:8080 Connected in 2ms
 Trace: Monitoring: Success: Connect: 192.168.1.40:80 192.168.1.119:8080 Connected in 3ms
 Trace: Monitoring: Success: Connect: 192.168.1.40:80 192.168.1.119:8080 Connected in 2ms
 Trace: Monitoring: Success: Connect: 192.168.1.40:80 192.168.1.125:8080 Connected in 3ms
 Trace: Monitoring: Success: Connect: 192.168.1.40:80 192.168.1.119:8080 Connected in 2ms
 Trace: Monitoring: Success: Connect: 192.168.1.40:80 192.168.1.125:8080 Connected in 0ms
 Trace: Monitoring: Success: Connect: 192.168.1.40:80 192.168.1.119:8080 Connected in 0ms
 Full results can be obtained using download.

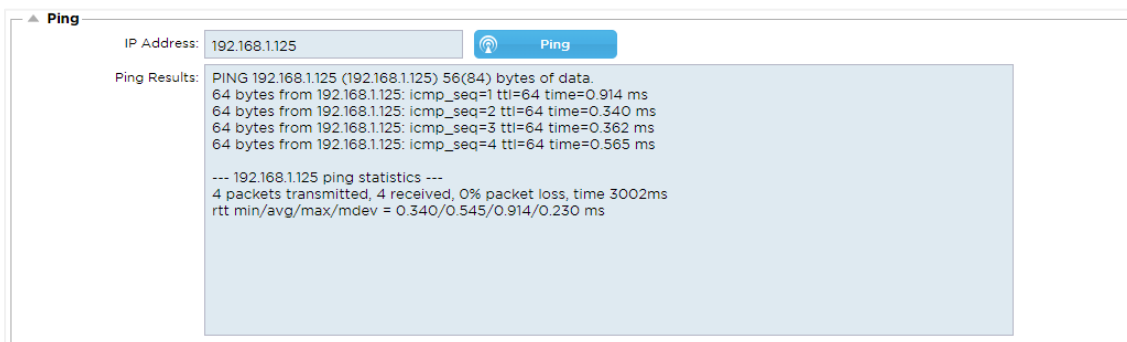
Im Abschnitt "Trace" können Sie Informationen einsehen, die die Fehlersuche im Problemfall ermöglichen. Die gelieferten Informationen hängen von den Optionen ab, die Sie in den Dropdown-Listen und den Kontrollkästchen auswählen.

Option	Beschreibung
Zu verfolgende Knoten	Your IP: Die Ausgabe wird nach der IP-Adresse gefiltert, von der aus Sie auf die GUI zugreifen (wählen Sie diese Option nicht für die Überwachung, da die Überwachung die Adresse der ADC-Schnittstelle verwendet). All IP: Es wird kein Filter angewendet. Es sollte beachtet werden, dass dies bei einer stark ausgelasteten Box die Leistung beeinträchtigen kann.
Verbindungen	Dieses Kontrollkästchen zeigt, wenn es aktiviert ist, Informationen über die client- und serverseitigen Verbindungen an.
Cache	Wenn dieses Kontrollkästchen aktiviert ist, werden 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-Zustandsüberwachungen und ihre jeweiligen Ergebnisse angezeigt.
Überwachung unerreichbar	Dieses Häkchen ist wie oben, außer dass es nur die fehlgeschlagenen Monitore anzeigt und somit wie ein Filter nur für diese Meldungen wirkt.
Auto-Stopp-Datensätze	Der Standardwert ist 1.000.000 Datensätze, danach wird die Trace-Funktion automatisch gestoppt. Dies 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. Dies ist eine Sicherheitsvorkehrung, um zu verhindern, dass Trace versehentlich eingeschaltet bleibt und die Leistung des ADCs beeinträchtigt.
Start	Klicken Sie auf , um die Trace-Einrichtung 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. Sie können das Trace.log herunterladen, um alle Informationen anzuzeigen, die während der verschiedenen Traces an diesem Tag gesammelt wurden. Dies ist im Grunde 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 dann aber manuell filtern.
Klar	Löscht das Trace-Protokoll

Ping

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



Ping

IP Address: Ping

Ping Results: PING 192.168.1.125 (192.168.1.125) 56(84) bytes of data:
 64 bytes from 192.168.1.125: icmp_seq=1 ttl=64 time=0.914 ms
 64 bytes from 192.168.1.125: icmp_seq=2 ttl=64 time=0.340 ms
 64 bytes from 192.168.1.125: icmp_seq=3 ttl=64 time=0.362 ms
 64 bytes from 192.168.1.125: icmp_seq=4 ttl=64 time=0.565 ms

--- 192.168.1.125 ping statistics ---
 4 packets transmitted, 4 received, 0% packet loss, time 3002ms
 rtt min/avg/max/mdev = 0.340/0.545/0.914/0.230 ms

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

Wenn Sie einen DNS-Server konfiguriert haben, können Sie den vollständig qualifizierten Domännennamen eingeben. 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



Capture

Adapter:

Packets:

Duration[Sec]:

Address:

Generate

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

- Füllen Sie die Optionen im Formular aus
- Klicken Sie auf Generieren
- Sobald die Erfassung ausgeführt wurde, wird Ihr Browser angezeigt und Sie werden gefragt, wo Sie die Datei speichern möchten. Sie wird das Format "jetNEXUS.cap.gz" haben.
- Erstellen Sie ein Support-Ticket im 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, typischerweise eth0 oder eth1. Sie können auch alle Schnittstellen mit "any" erfassen
Pakete	Dieser Wert ist die maximale Anzahl der zu erfassenden Pakete. Typischerweise 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 des Erfassungszeitraums unzugänglich
Adresse	Dieser Wert filtert nach jeder in das Feld eingegebenen 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.

Was ist ein jetPACK

jetPACKs sind eine einzigartige Methode zur sofortigen Konfiguration Ihres ADC für bestimmte Anwendungen. 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 eine virtuelle IP-Adresse von 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.
- Außerdem 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 Upload oder vorher mit Notepad++ ändern.
- Klicken Sie auf einen jetPACK-Link unten und speichern Sie den Link als jetPACK-VIP-Application.txt-Datei an einem Ort Ihrer Wahl

Microsoft Exchange

Anwendung	Download-Link	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, wird dieses jetPACK trotzdem funktionieren.	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 Virtueller Dienst 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 auf 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 sieht die Adresse der ALB-X-Schnittstelle als Quell-IP.	Globale Einstellungen: Service-Timeout 2 Stunden Monitore: Layer-7-Monitor für die Outlook-Web-App. Schicht-4-Out-of-Band-Monitor für den Client-Zugangsdienst Virtueller Dienst 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 auf HTTPS hinzu
	jetPACK-1.1.1.3-Exchange-2010-SMTP-DSR	Gleich 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. Schicht-4-Out-of-Band-Monitor für den Client-Zugangsdienst Virtueller Dienst IP: 1.1.1.1 Virtuelle Service Ports: 80, 443, 135, 59534, 59535, 25 (direkter Serverrücklauf) Reale Server: 127.1.1.1 127.2.2.2 flightPATH: Fügt Umleitung von HTTP auf HTTPS hinzu
Austausch 2013	jetPACK-2.2.2.1-Exchange-2013-Low-Resource	Dieses Setup 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: Schicht-7-Monitor für OWA, EWS, OA, EAS, ECP, OAB und ADS Virtueller Dienst 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 auf 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 auf HTTPS hinzu
	jetPACK-2.2.2.3-Exchange2013-High-Resource	Dieses jetPACK fügt eine eindeutige IP-Adresse und mehrere virtuelle Dienste auf verschiedenen Ports hinzu. flightPATH führt dann eine Kontextumschaltung basierend auf dem Zielpfad zum richtigen virtuellen Dienst durch. 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 auf 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 -End	jetPACK-3.3.3.3-Lync-Edge-Internal	jetPACK-3.3.3.4-Lync-Edge-External

Web Services

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 -ffload

[jetPACK-7.7.7..1-Oracle-EBS](#)

VMware Horizon View

Connection Servers – SSL-Offload	Security Servers – 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 16 MB erhöht

Verschlüsselungsoptionen

- Starke Chiffren - Damit wird die Möglichkeit hinzugefügt, "Starke Chiffren" aus der Liste der Chiffrieroptionen auszuwählen:
 - Verschlüsselung = ALL:RC4+RSA:+RC4:+HIGH:!DES-CBC3-SHA:!SSLv2:!ADH:!EXP:!ADHexport:!MD5

- Anti-Bestie - Dies fügt die Möglichkeit hinzu, "Anti-Bestie" in der Liste der Chiffrieroptionen auszuwählen:
 - Verschlüsselung = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH
- No SSLv3 - Damit wird die Möglichkeit hinzugefügt, "No SSLv3" aus der Liste der Verschlüsselungsoptionen auszuwählen:
 - 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 auszuwählen:
 - Verschlüsselung = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
- NO_TLSv1.1 -Damit wird die Möglichkeit hinzugefügt, "NO_TLSv1.1" in der Liste der Verschlüsselungsoptionen auszuwählen:
 - 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
- Durchsuchen nach jetPACK
- Hochladen anklicken
- 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 vorhandenen ALB-X

- Erweitert
- Software aktualisieren
- Aktuelle Konfiguration herunterladen
- Bearbeiten Sie diese Datei mit Notepad++
- Öffnen Sie ein neues txt-Dokument und nennen Sie es "ihurname-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 am Anfang des jetPACKs stehen, 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 Inhaltsserver-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 Regeln für die Serverüberwachung, die hier normalerweise über die Webkonsole konfiguriert werden.

Beispiel:

[jetnexusdaemon-Csm-Rules-0]

Inhalt="Server Up"

Desc="Monitor 1"

Method="CheckResponse"

Name="Health Check- Ist der Server hoch"

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

Abschnitt 3:

[jetnexusdaemon-LocalInterface]

Dieser Abschnitt enthält alle Details des Abschnitts "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 "Path" (Pfad).

Beispiel:

[jetnexusdaemon-LocalInterface1]

1.1="443"

1.2="104"

1.3="80"

1.4="81"

Freigegeben=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

ZertifikatName="Standard"

ClientCertificateName="Kein SSL"

Komprimieren=1

ConnectionLimiting=0

DSR=0

DSRProto="tcp"

Freigegeben=1

LoadBalancePolicy="CookieBased"

MaxVerbindungen=10000

MonitoringPolicy="1"

PassThrough=0

Protokoll="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 für ein bestimmtes Verzeichnis HTTPS verwendet wird"
Name="Gary - HTTPS erzwingen"
[jetnexusdaemon-Pfad-6-Bedingung-1]
Check="contain"
Bedingung="Pfad"
Spiel=
Sense="tut"
Value="/sicher/"
[jetnexusdaemon-Path-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 Dienstyp wählen, ist die Registerkarte flightPATH in IP Services 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, wenn die Regel ausgelöst hat.

Was kann flightPATH leisten?

flightPATH kann verwendet werden, um eingehende und ausgehende HTTP(s)-Inhalte und -Anfragen zu ändern.

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

Weitere Informationen zu RegEx finden 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 "Formular hat nicht die Länge 0"
GEO-Standort	Dies vergleicht die Quell-IP-Adresse mit dem ISO 3166 Country Code	GEO Standort ist gleich GB OR 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 Subnetz 10\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-Abfrageverfahren	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", wobei die Übereinstimmung "Best" 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, User-Agent, Von, Datum
Version anfordern	Dies ist die HTTP-Version	HTTP/1.0 ODER HTTP/1.1
Antwort Körper	Eine benutzerdefinierte Zeichenkette im Antwortkörper	Server UP
Antwort-Code	Der HTTP-Code für die Antwort	200 OK, 304 Nicht geändert
Antwort Cookie	Dies ist der Name eines vom Server gesendeten Cookies	MS-WSMAN=afYfn1CDqqCDqUD::
Antwort-Kopfzeile	Dies kann ein beliebiger HTTP-Header sein	Referrer, User-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. Die Punkte müssen entschlüsselt werden, da es sich um RegEX handelt. 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 Teilinhaltsbereichstypen dieser Server unterstützt	Accept-Ranges: bytes

Autorisierung	Anmeldeinformationen für die HTTP-Authentifizierung	Berechtigung: Basic QWxhZGRpbjpvGVuIHNIc2FtZQ==
Charge-To	Enthält Kontoinformationen zu den Kosten für die Anwendung der angeforderten Methode	
Content-Encoding	Die Art der Kodierung, die für die Daten verwendet wird.	Content-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 erzeugt 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 Format RFC 2822	Last-Modified: 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 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 User-Agents	Benutzer-Agent: Mozilla/5.0 (kompatibel; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Variieren	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 Webanwendung 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 - Existiert
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	Request Header - Accept - Does - Contain - image
Gleiche	Die Zeichenkette ist gleich dem Wert	Host - Tut - Gleich - www.jetnexus.com
Länge haben	Der String 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	Absender-IP - Entspricht - Regex - 10\..* 11\..*

Beispiel

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

- 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

Variable	Source	Detail	Value
\$variable1\$	Select a New Source	Select or Type a New Detail	Type a New Value

Update Cancel

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. Zum Beispiel könnten Sie 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\$
 - Antwortcode (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 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	Das Dropdown-Menü enthält GET, POST
Pfad	Dies ist der Pfad der Website	/meinewebsite/index.html
POST	POST-Abfrageverfahren	Prüfen von Daten, die auf eine Website hochgeladen werden
Abfrageelement	Dies ist der Name und der Wert einer Abfrage. Als solches kann es entweder	"Best=jetNEXUS", wobei die Übereinstimmung "Best" und der Wert "edgeNEXUS" ist

	den Abfragenamen oder auch einen Wert akzeptieren	
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 Teilinhaltsbereichstypen dieser Server unterstützt	Accept-Ranges: bytes
Autorisierung	Anmeldeinformationen für die HTTP-Authentifizierung	Berechtigung: Basic QWxhZGRpbjpvGVVlHNlc2FtZQ==
Charge-To	Enthält Kontoinformationen zu den Kosten für die Anwendung der angeforderten Methode	
Content-Encoding	Die Art der Kodierung, die für die Daten verwendet wird.	Content-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 verfasst 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 Format RFC 2822	Last-Modified: Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Implementierungsspezifische Header, die an jeder Stelle der Anfrage-Antwort-Kette	Pragma: no-cache

	verschiedene Auswirkungen haben können.	
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 User-Agents	Benutzer-Agent: Mozilla/5.0 (kompatibel; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Variieren	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 Webanwendung 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.

▲ Action

⊕ Add New
⊖ Remove

Action	Target	Data
Redirect 302	https://\$host\$\$path\$\$querystring\$	

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 die 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 das im Abschnitt "Ziel" angegebene Anfrage-Cookie mit dem Wert im Abschnitt "Daten" hinzu	Ziel= Cookie Daten= MS-WSMAN=afYfn1CDqqCDqCVii
Anforderungs-Kopfzeile hinzufügen	Fügen Sie einen Anfrage-Header vom Typ Target mit Wert im Abschnitt Data hinzu	Ziel= Übernehmen Daten= image/png
Antwort-Cookie hinzufügen	Antwort-Cookie im Abschnitt "Target" mit Wert im Abschnitt "Data" hinzufügen	Ziel= Cookie Daten= MS-WSMAN=afYfn1CDqqCDqCVii
Antwort-Kopfzeile hinzufügen	Anforderungskopf im Abschnitt Ziel mit Wert im Abschnitt Daten detailliert hinzufügen	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 zuerst austauschen	Den Antwortkörper durchsuchen und nur die erste Instanz ersetzen	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 im Abschnitt "Ziel" beschriebene Anfrage-Cookie	Ziel= Cookie Daten= MS-WSMAN=afYfn1CDqqCDqCVii
Anforderungs-Kopfzeile entfernen	Anforderungskopf entfernen, der im Abschnitt Ziel beschrieben ist	Ziel=ServerDaten=N/A
Antwort-Cookie entfernen	Antwort-Cookie entfernen, wie im Abschnitt "Ziel" beschrieben	Ziel=jnAccel
Antwort-Header entfernen	Entfernen Sie den im Abschnitt "Ziel" beschriebenen Antwort-Header	Ziel= Etag Daten= N/A

Anfrage-Cookie austauschen	Ersetzen Sie das im Abschnitt Ziel angegebene Anfrage-Cookie durch den Wert im Abschnitt Daten	Ziel= Cookie Daten= MS-WSMAN=afYfn1CDqqCDqCVii
Anforderungs-Kopfzeile ersetzen	Anfragekopf im Target durch Datenwert ersetzen	Ziel= Verbindung Daten= keep-alive
Antwort-Cookie austauschen	Ersetzen Sie das im Abschnitt "Target" angegebene Antwort-Cookie durch den Wert im Abschnitt "Data".	Ziel=jnAccel=afYfn1CDqqCDqCViiDatum=MS-WSMAN=afYfn1CDqqCDqCVii
Antwort-Header ersetzen	Ersetzen Sie den im Abschnitt "Target" angegebenen Antwort-Header durch den Wert im Abschnitt "Data".	Ziel= Server Daten= Aus Sicherheitsgründen vorenthalten
Pfad umschreiben	Damit können Sie die Anfrage auf eine neue URL umleiten, die auf der Bedingung	Ziel= /test/path/index.html\$querystring\$ Daten= N/A
Sicheren Server verwenden	Auswählen, welcher sichere Server oder virtuelle Dienst verwendet werden soll	Target=192.168.101:443Data=N/A
Server verwenden	Wählen Sie den zu verwendenden Server oder virtuellen Dienst	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:

+

Add New

−

Remove

Action	Target	Data
Redirect 302	https://\$host\$\$path\$\$querystring\$	

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

Merkmale

- Benutzer basierend auf dem 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-Alarm 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\$I

Index.html

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

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

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

Auswertung:

- Leer

Aktion:

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

Ordner schließen

Anfragen an Ordner ablehnen.

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

- Bedingung = das 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 zutrifft

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

Auswertung:

- Leer

Aktion:

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

Log Spider

Loggen Sie die Spider-Anfragen der gängigen Suchmaschinen.

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

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

Auswertung:

- Variable = \$Crawler\$

- Quelle = Request Header
- Detail = Benutzer-Agent

Aktion:

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

HTTPS erzwingen

Erzwingt die Verwendung von HTTPS für ein bestimmtes Verzeichnis. Wenn in diesem Fall ein Client auf etwas zugreift, das das Verzeichnis /secure/ enthält, wird er zur 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
- Prüfung = 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 = Response Code

- Sense = Tut
- Prüfen = Gleich
- Wert = 200 OK

Auswertung:

- Leer

Aktion:

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

Blanko-Kreditkarten ausgeben

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

Zustand:

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

Auswertung:

- Leer

Aktion:

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

Niemals Fehler senden

Der Kunde bekommt keine Fehler von Ihrer Seite.

Zustand

- Bedingung = Response 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 Analytics ein - Bitte ändern Sie den Wert MYGOOGLECODE in Ihre Google UA ID.

Zustand

- Bedingung = Response 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' : '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 = Request Header ersetzen
- Ziel = Host
- Daten = ipv4.host.header

Web-Anwendungs-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

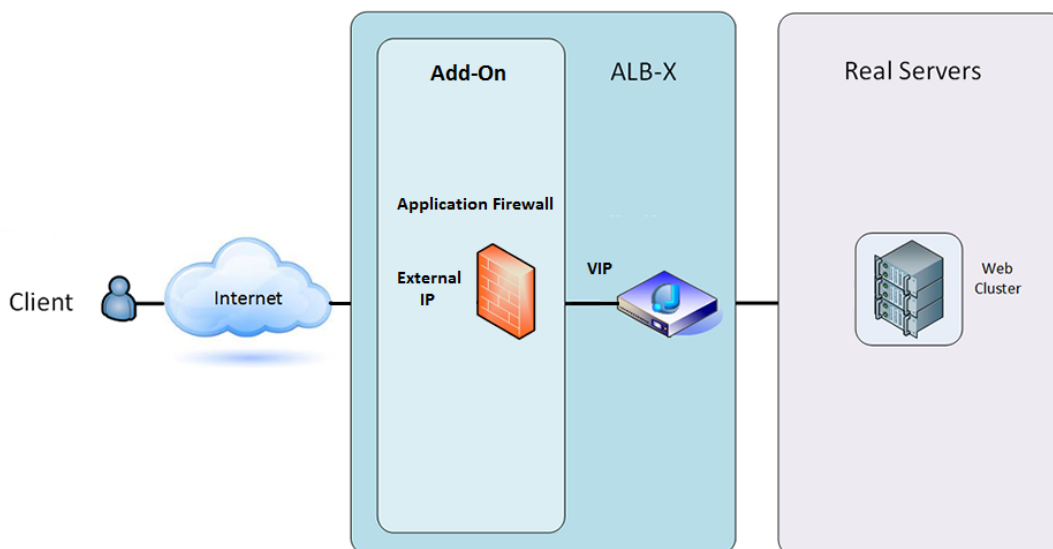
Da die WAF in einem Docker-Container läuft, müssen vor dem Start einige Netzwerkparameter eingestellt werden.

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 Falle 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 zum 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 GUI-Adresse der Firewall HTTP//[Externe IP]88/waf lautet. Lassen Sie also entweder die Einstellung "Externer Port" leer oder fügen Sie Port 88 hinzu, 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 Seite "Add-On". Sie müssen zur Seite Library-Apps gehen, um das Add-On erneut bereitzustellen.
Übergeordnetes Bild	Gibt das Docker-Image an, aus dem das Add-On erstellt wurde. Es kann mehrere Versionen einer Firewall oder eines anderen Add-On-Typs 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 am	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

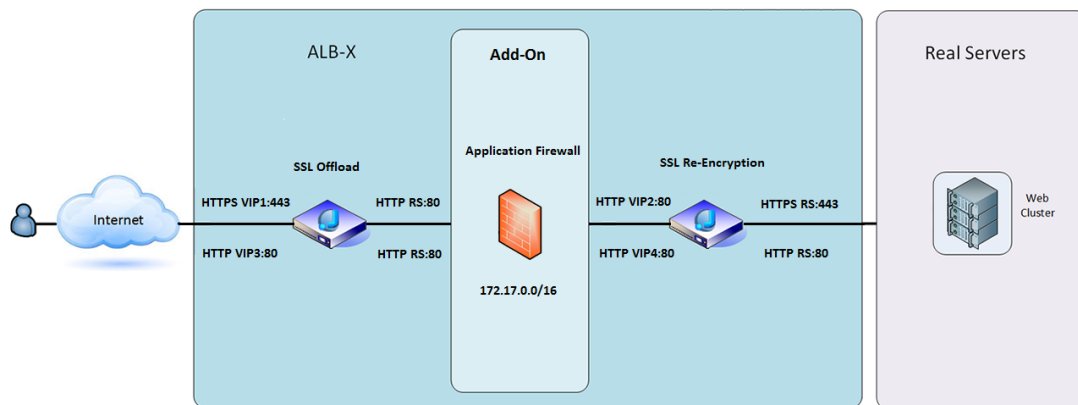


In dieser Architektur kann nur HTTP für Ihren Dienst verwendet werden, da die Firewall den HTTPS-Verkehr nicht prüfen kann.

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.

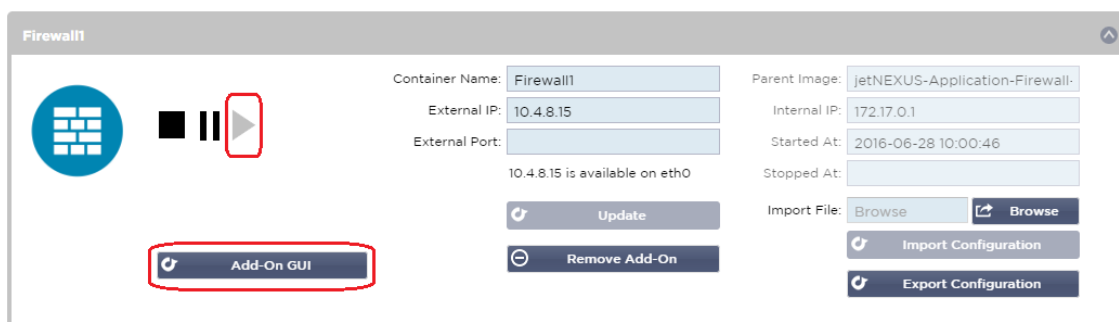
HTTPS kann End-to-End sein, wobei die Verbindungen vom Client zum ALB-X und vom ALB-X zu den Real-Servers verschlüsselt sind.

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

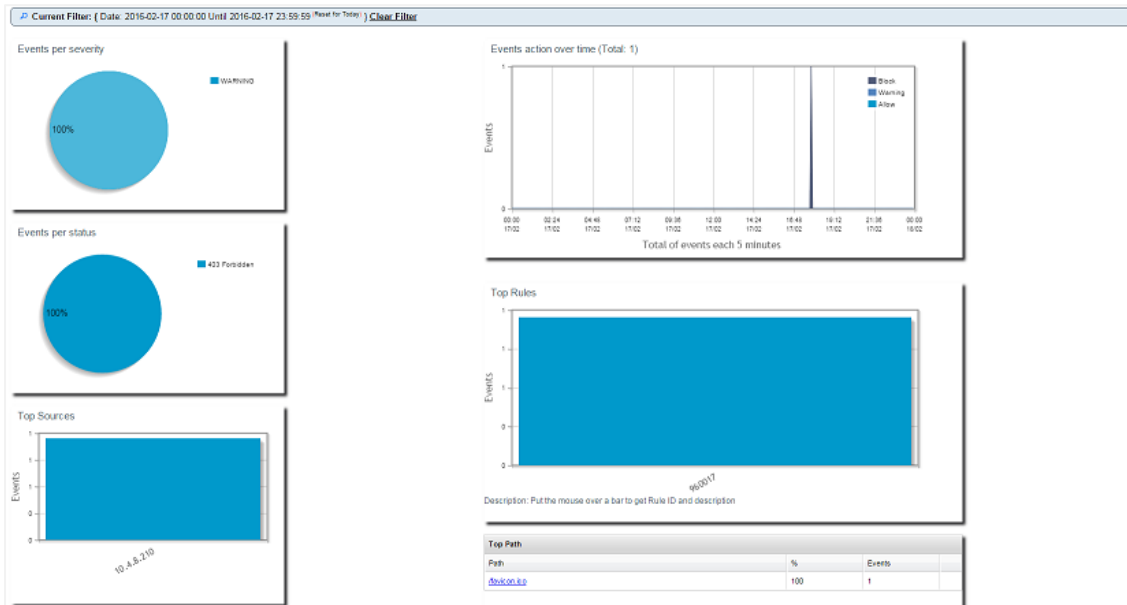
Sobald der Datenverkehr die Firewall passiert hat, wird er an ein anderes VIP weitergeleitet, das dann entweder den Datenverkehr erneut verschlüsseln und einen Lastausgleich zu sicheren Servern oder einfach einen Lastausgleich zu unsicheren Servern über HTTP durchführen kann.

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 "Play"
- 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 Ihr ADC ein.
- Nach erfolgreicher Anmeldung gelangen Sie auf die Startseite der WAF.



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

Config	Real Server / VIP	
Users	Real Server / VIP Address	10.4.8.102:8080
Info		

- 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 alleine 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, wird die Regel, die den Datenverkehr blockiert, in der Liste Blockierungsregeln auf der Seite Whitelist angezeigt.
- Um zu verhindern, dass die Firewall die gültige Anwendungsressource blockiert, verschieben Sie bitte die Blockierungsregel in den Bereich Whitelist-Regeln.

Firewall Control
☐ Disabled
☐ Detection only
☒ Detection and blocking

Blocking Rules
 960017 (Host header is a numeric IP address)

Whitelisted Rules

Manually add rule IDs to whitelistsit

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

Regeln aktualisieren

- Die Regeln der Anwendungsfirewall können im Bereich Erweitert - Software aktualisiert werden
- Klicken Sie auf "Aktualisieren", um die Schaltfläche "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

Download from Cloud

Code Name	Release Date	Version	Build
OWASP Core Rule Set Update for jetNEXUS Application Firewall	2016-02-09	OWASP	jetNEXUS (Firewall)

Download Selected Software to ALB

- 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

Apply Software stored on ALB

Image	Code Name	Release Date	Version	Build	Notes
	jetNEXUS-WAF-OWASP-CRS	23 Nov 2015	1.0		jetNEXUS Application Firewall OWASP Core Rule Set

Remove

Apply Selected Software Update

- 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 Blockierregeln auf der Seite Whitelist.
- Sie können auch im Abschnitt "Management Info" der Firewall-GUI nach der OWASP CRS-Version suchen

Config	jetNEXUS WAF Version: 1.0.0
Users	OWASP CRS Version: 2.2.9 (24 Feb 2016)
Info	APC Cache extension: Extension APCu (3.1.9) loaded, enabled and turned "on" in jetNEXUS WAF
	APC Cache Timeout: 30 seconds
	PHP version: 5.3.3
	PHP Zend Version: 2.3.0
	MySQL Version: 5.1.73
	Database Name: waf
	Database Size: 167.17 kB
	Number of sensors: 1
	Number of events on DB: 12

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 Ausfall eines Rechenzentrums der Datenverkehr an das andere weitergeleitet wird.

Lastausgleich und Geolokalisierung

Sie möchten den Datenverkehr zwischen den Rechenzentren in einer Active-Active-Situation auf der Grundlage bestimmter Kriterien wie der Leistung des Rechenzentrums, der Kapazität des Rechenzentrums, der Überprüfung des Zustands des Rechenzentrums und des physischen Standorts des Clients (damit Sie ihn an das nächstgelegene Rechenzentrum senden können) usw. verteilen.

Kommerzielle Überlegungen

Sicherstellen, dass Benutzer von bestimmten geografischen Standorten an bestimmte Datenzentren gesendet werden. Stellen Sie sicher, dass für andere Benutzer unterschiedliche Inhalte bereitgestellt (oder blockiert) werden, abhängig von verschiedenen 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.
- Zuletzt 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.
- Nachdem 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 Abschnitt "Dienste" Ihres Betriebssystems. Die DNS-Namen werden weiterhin aufgelöst, jedoch 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 zur Überprüfung der Verfügbarkeit von Remote-Ressourcen, indem sie auf die Ressource selbst zugreift. Um jedoch eine Logik anzuwenden, muss das System zuerst die DNS-Anfrage erhalten.

Dies ist auf verschiedene 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 für Systeme, die keinen GSLB benötigen, nicht den gesamten DNS-Verkehr an den GSLB weiterleiten.

Es ist eine Redundanz vorgesehen, so dass bei Ausfall eines Nameservers (GSLB) der entfernte Nameserver automatisch eine weitere Anfrage an einen anderen GSLB stellt und somit ein Ausfall der Website verhindert wird.

GSLB-Konfiguration

Nachdem Sie das GSLB-Add-On heruntergeladen haben, stellen Sie es bereit, indem Sie die Seite "Library > Apps" der ADC-GUI aufrufen 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 "Library > Add-Ons" der ADC-GUI, wie in der folgenden Abbildung dargestellt.

- Container Name ist ein eindeutiger Name einer laufenden Add-On-Instanz, die vom ADC gehostet wird, er wird verwendet, um mehrere Add-Ons der gleichen 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.



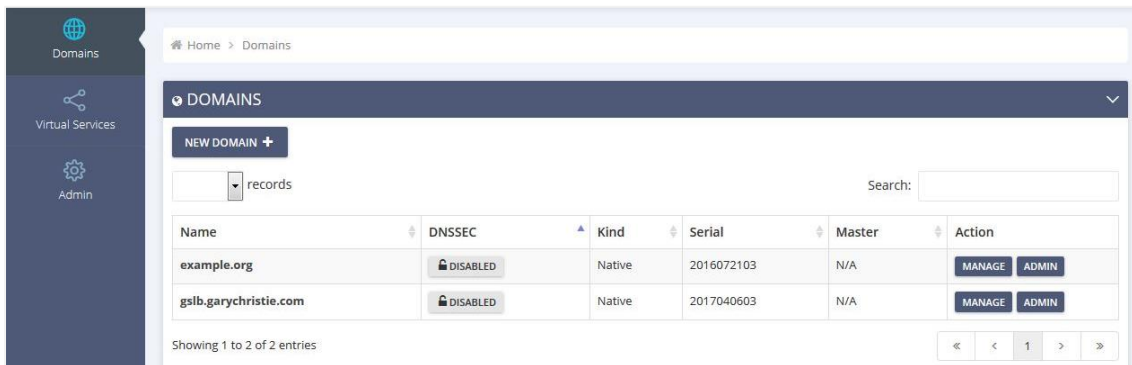
- Der nächste Schritt besteht darin, dass das edgeNEXUS GSLB Add-On die ADC-Konfiguration lesen und ändern kann.
- Rufen Sie die Seite "System > Users" der ADC GUI auf und bearbeiten Sie einen Benutzer mit demselben Namen wie das GSLB-Add-On, das Sie bereitgestellt haben, wie in der Abbildung unten gezeigt.
- Bearbeiten Sie den Benutzer "gslb1" und setzen Sie das Häkchen bei "API", dann klicken Sie auf "Aktualisieren" - in späteren Versionen der Software kann das Häkchen bereits standardmäßig gesetzt sein.

- Der nächste Schritt ist nur erforderlich, wenn Sie GSLB zu Test- oder Evaluierungszwecken konfigurieren und keine DNS-Zonendaten im Internet ändern möchten.
- 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 > Network" der ADC-GUI ändern, wie in der folgenden Abbildung gezeigt.
- DNS-Server 2 kann generell mit Ihrem lokalen DNS-Server oder einem im Internet konfiguriert werden, z. B. Google 8.8.8.8.

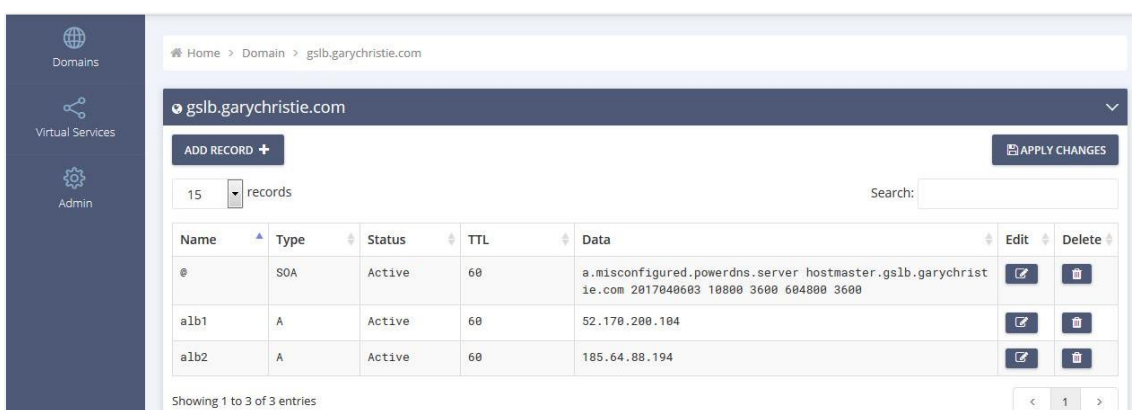
- Jetzt ist es an der Zeit, sich am GSLB GUI anzumelden.
- Bitte navigieren Sie auf der Seite Library > Add-Ons der ADC GUI und klicken Sie auf die Schaltfläche Add-On GUI.
- Durch Anklicken wird eine neue Browser-Registerkarte geöffnet, die die GSLB-GUI-Anmeldeseite darstellt, wie unten gezeigt.

- 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, und ihn entweder zu einem autoritativen Nameserver für die "example.org"-Zone oder eine Subdomain-Zone zu machen, wie z. B. die oben im Abschnitt "DNS-basierte GSLB-Übersicht" erwähnte Subdomain "geo.example.org".
- Ausführliche Details zur DNS-Zonenkonfiguration finden Sie in der [POWERDNS NAMESERVER-DOKUMENTATION](#). Eine Beispielizee ist in Abbildung 6 dargestellt.

* Die 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 dargestellt.
- Nachdem Sie einen bestehenden Datensatz innerhalb der GSLB-GUI bearbeitet haben, drücken Sie bitte die Schaltfläche Speichern.
- Nachdem Sie die Erstellung der Hostnamen-Einträge abgeschlossen haben, klicken Sie bitte auf die Schaltfläche Apply Changes (Änderungen übernehmen). Wenn Sie nicht auf "Apply" (Übernehmen) klicken und dann die Seite ändern, gehen Ihre Änderungen verloren.
- Im Folgenden haben wir Datensätze erstellt, die IPv4-Adressdatensätze 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.

Virtual Services

Copy Service

Search

Add Virtual Service

Remove

Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Stand-alone				192.168.4.10	255.255.255.224	80	service1.gslb.garychristie.com	HTTP

Real Servers

Server

Basic

Advanced

FlightPATH

Group Name: Server Group

Copy Server

Add Server

Remove

Status	Activity	Address	Port	Weight	Calculated Weight	Notes
	Online	alb1.gslb.garychristie.com	80	100	100	US East
	Online	alb2.gslb.garychristie.com	80	100	100	UK Marlow

- 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 Diensttypen verwendet werden.
- Bitte navigieren Sie zur Seite Services > IP-Services der ADC-GUI und erstellen Sie einen Virtual Service, wie in der folgenden Abbildung gezeigt.
- Stellen Sie sicher, dass Sie den Dienstnamen mit dem richtigen Domännennamen konfigurieren, den Sie in der GSLB verwenden möchten. Der GSLB liest dies über die API und füllt automatisch den Abschnitt "Virtual Services" 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 Domännennamen oder IP-Adressen angeben.
- Wenn Sie die Domännennamen angeben, werden die in Ihrem GSLB erstellten Datensätze verwendet.
- Sie können auf den Registerkarten "Basic" und "Advanced" verschiedene Methoden und Parameter zur Überwachung des Serverzustands auswählen.
- Sie können die Aktivität einiger Server für ein Aktiv-Passiv-Szenario auf Standby setzen.
- In diesem Fall, wenn ein "Online"-Server eine Zustandsprüfung nicht besteht und ein gesunder Standby-Server vorhanden ist, löst Edgenexus EdgeGSLB den Domännennamen in eine Adresse des Standby-Servers auf.
- Einzelheiten zur Konfiguration von Virtual Services finden Sie im Abschnitt **VIRTUAL SERVICES**.
- Wechseln wir nun zur GSLB-GUI.
- Navigieren Sie zur Seite "Virtuelle Dienste" und wählen Sie eine GSLB-Richtlinie für die Domäne der API aus, die aus dem Abschnitt "Virtuelle ADC-Dienste" abgerufen wurde.
- Dies ist in der folgenden Abbildung dargestellt.

 Domains

 Virtual Services

 Admin

Home > Virtual Services

Virtual Services

APPLY CHANGES

15 records

Search:

Name	Enabled	Type	IP Address	Subnet Mask / Prefix	Port	GSLB Policy	Edit	Manage
service1.gslb.garychristie.com	ENABLED	HTTP	192.168.4.10	255.255.255.224	80	Geolocation Fixed Weight Geolocation - City Match Geolocation - Continent Match Geolocation - Country Match Geolocation - Proximity Round Robin	SAVE	CANCEL

Showing 1 to 1 of 1 entries

- Die GSLB unterstützt die folgenden Richtlinien:

Richtlinie	Beschreibung
Festes Gewicht	Der GSLB wählt den Server mit der höchsten Gewichtung aus (die Servergewichtung kann vom Benutzer vergeben werden). Wenn mehrere Server

	die höchste Gewichtung haben, wählt der GSLB einen dieser Server nach dem Zufallsprinzip aus.
Gewichtetes Round Robin	Wählen Sie die Server nacheinander aus, in einer Reihe. Server mit höherer Gewichtung werden häufiger ausgewählt als Server mit niedrigerer Gewichtung.
Geolokalisierung	Proximity (Nähe) - wählen Sie einen Server aus, der sich anhand von geografischen Breiten- und Längengraden am nächsten zum Standort des Clients befindet. 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 aus, der dem Standort des Clients anhand der geografischen Breiten- und Längengraddaten 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	Kontinentvergleich - 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.
- Daraufhin wird die unten abgebildete Seite angezeigt.
- Wenn Sie eine der gewichtungsbasierten Richtlinien ausgewählt haben, müssen Sie möglicherweise die Server-GSLB-Gewichte anpassen.
- Wenn Sie eine der geostandortbasierten GSLB-Richtlinien ausgewählt haben, müssen Sie möglicherweise 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.

Home > Virtual Services > service1.gslb.garychristie.com

service1.gslb.garychristie.com

REFRESH APPLY CHANGES

15 records Search:

Status	Activity	Name	Port	GSLB Weight	Notes	Edit	Delete
Connected	Standby	alb1.gslb.garychristie.com	80	100			
Real Server unreachable	Online	alb2.gslb.garychristie.com	81	100			

Showing 1 to 2 of 2 entries

- Eine gute Möglichkeit zu prüfen, 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](https://dnschecker.org) verwenden.
Beispiel [HTTPs://dnschecker.org/#A/service1.gslb.garychristie.com](https://dnschecker.org/#A/service1.gslb.garychristie.com).
- Siehe unten für ein Beispiel der Ergebnisse.

DNS CHECKER

DNS Propagation Check

Canada Park, CA, United States (Sprint)	52.170.200.104	✓
Holtville NY, United States (Opends)	52.170.200.104	✓
Montreal, Canada (iWeb Technologies)	52.170.200.104	✓
Broomfield CO, United States (Verizon)	52.170.200.104	✓
Mountain View CA, United States (Google)	52.170.200.104	✓
Holtville NY, United States (Opends)	52.170.200.104	✓
Yekaterinburg, Russian Federation (Skydns)	52.170.200.104	✓
Cape Town, South Africa (Raaweb)	185.64.88.194	✓
Purmerend, Netherlands (VIDEO & MEDIA NL)	185.64.88.194	✓
Paris, France (OVH SAS)	185.64.88.194	✓
Madrid, Spain (Fujitsu)	185.64.88.194	✓
Kumamoto, Japan (Kyushu Telecom)	185.64.88.194	✓
Zug, Switzerland (Serverbase GmbH)	185.64.88.194	✓
Melbourne, Australia (Pacific Internet)	52.170.200.104	✓
Gloucester, United Kingdom (Fasthosts Internet)	185.64.88.194	✓
Midtjylland (YouSee)	185.64.88.194	✓
Frankfurt, Germany (Level3)	52.170.200.104	✓
Santa Ana, Mexico (Uninet S.A.)	52.170.200.104	✓

Check DNS Resolution

Your IP: 89.240.14.179

Have you recently switched webhost or started a new website, then you are in right place! DNS Checker provides free dns lookup service for checking domain name server records against a randomly selected list of DNS servers in different corners of the world. Do a quick look up for any domain name and check DNS data collected from all location for confirming that website is completely propagated or not worldwide.

Map data ©2017 Terms of Use

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. Wenn die Lastausgleichsrichtlinie auf eine GEO-Richtlinie eingestellt ist, wird die nächstgelegene IP-Adresse zurückgegeben. 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 beachten Sie die Wikipedia-Seite zur Erklärung der privaten Adressierung

[HTTPS://DE.WIKIPEDIA.ORG/WIKI/PRIVATE_NETWORK](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 anfragt, 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
- Ordnen Sie die verschiedenen privaten Netzwerke diesen Standorten zu
- Ordnen Sie jeden Dienst dem jeweiligen Standort zu

Wie konfigurieren wir dieses Aussehen auf dem GSLB?

Hinzufügen eines Standorts für das Northern Data Center

- Klicken Sie auf der linken Seite auf Benutzerdefinierte Standorte
- Klicken Sie auf Standort hinzufügen
- Name
 - Norden
- Fügen Sie eine private IP-Adresse und eine 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
- Hinzufügen des Kontinent-Codes
 - EU
- Hinzufügen des Ländercodes
 - 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 Rechenzentrum Süd

- Klicken Sie auf der linken Seite auf Benutzerdefinierte Standorte
- Klicken Sie auf Standort hinzufügen
- Name
 - Süd
- Fügen Sie eine private IP-Adresse und eine Subnetzmaske für Ihr Southern-Netzwerk hinzu. Wir gehen für diese Übung davon aus, dass sich die IP-Adressen des Dienstes und des Clients im selben privaten Netzwerk befinden.
 - 192.168.1.0/24
- Hinzufügen des Kontinentalcodes
 - EU

- Hinzufügen des Ländercodes
 - 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

The screenshot shows the 'Custom Locations' management interface. At the top, there is a header bar with 'Custom Locations' and a dropdown arrow. Below the header, there is a blue button 'ADD LOCATION +' and a blue button 'APPLY CHANGES'. A search bar is located on the right. Below the search bar, there is a table with the following columns: Name, IP Address, Subnet Mask / Prefix, Continent, Country, City, Latitude, Longitude, Edit, and Delete. The table contains two entries: 'North' with IP 10.1.1.0, Subnet 24, Continent EU, Country UK, City Enfield, Latitude 51.6523, and Longitude 0.0887; and 'South' with IP 192.168.1.0, Subnet 24, Continent EU, Country UK, City Croydon, Latitude 51.3762, and Longitude 0.0982. At the bottom, there is a pagination bar showing 'Showing 1 to 2 of 2 entries' and navigation buttons.

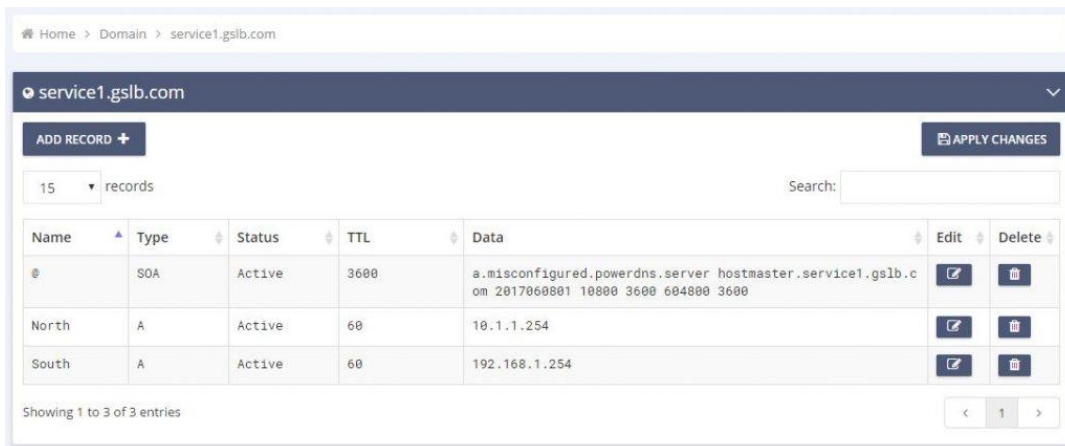
Name	IP Address	Subnet Mask / Prefix	Continent	Country	City	Latitude	Longitude	Edit	Delete
North	10.1.1.0	24	EU	UK	Enfield	51.6523	0.0887		
South	192.168.1.0	24	EU	UK	Croydon	51.3762	0.0982		

Hinzufügen eines A-Eintrags für north.service1.gslb.com

- 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 liegt)

Hinzufügen eines A-Eintrags für south.service1.gslb.com

- 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 (Hinweis: Dies ist im gleichen Netzwerk wie der Standort Croydon)



Home > Domain > service1.gslb.com

service1.gslb.com

ADD RECORD + APPLY CHANGES

15 records Search:

Name	Type	Status	TTL	Data	Edit	Delete
@	SOA	Active	3600	a.misconfigured.powerdns.server hostmaster.service1.gslb.com 2017060801 10800 3600 604800 3600		
North	A	Active	60	10.1.1.254		
South	A	Active	60	192.168.1.254		

Showing 1 to 3 of 3 entries

Verkehrsfluss

Beispiel 1 - Client im Rechenzentrum Nord

- 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 Rechenzentrum Süd

- 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/>