EdgeADC

EdgeADC-Verwaltungshandbuch

SOFTWARE-VERSION

5.0.0

Inhalt

Dokumenteneigenschaften

Dokumentnummer:2 .0.3.19.25.12.03

Erstellungsdatum des Dokuments:19 March 2025

Dieses Dokument wurde zuletzt bearbeitet: 19 March 2025

Autor des Dokuments: Jay Savoor

Dokument Zuletzt bearbeitet von:

Dokument: EdgeADC - Version 5.0.0

Haftungsausschluss für Dokumente

Die in diesem Handbuch enthaltenen Screenshots und Grafiken können aufgrund von Unterschieden in der Produktversion leicht von Ihrem Produkt abweichen. Edgenexus unternimmt alle angemessenen Anstrengungen, um sicherzustellen, dass die Informationen in diesem Dokument vollständig und korrekt sind. Edgenexus übernimmt keine Haftung für etwaige Fehler. Edgenexus behält sich vor, die Informationen in diesem Dokument in zukünftigen Versionen zu ändern und zu korrigieren, wenn dies erforderlich ist.

Urheberrechte

Markenzeichen

Edgenexus-Unterstützung

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

Einführung

Sie lesen diesen Leitfaden, weil Sie beabsichtigen, den Edgenexus EdgeADC einzusetzen und Ihre serverbasierten Anwendungen effizient und kostengünstig auszubalancieren.

Der EdgeADC basiert auf einer hochsicheren Engine, die hohe Skalierbarkeit, Sicherheit, hohe Leistung und eine sehr benutzerfreundliche Verwaltungsoberfläche bietet. Diese Faktoren stellen sicher, dass die von Ihnen bereitgestellte Lösung die bestmöglichen Betriebskosten bietet.

Der Zweck dieses Dokuments

Dieses Dokument wurde so verfasst, dass Sie den EdgeADC über seine einfache webbasierte Schnittstelle verwalten können. Die Funktionen und ihre Konfigurationen werden detailliert beschrieben, und wir hoffen, dass dies für Sie ausreicht, um den EdgeADC für Ihre Anforderungen zu konfigurieren.

Für wen ist dieses Dokument bestimmt?

Dieses Dokument richtet sich an Personen mit Netzwerkkenntnissen, insbesondere Protokollen, Anwendungen und Servern.

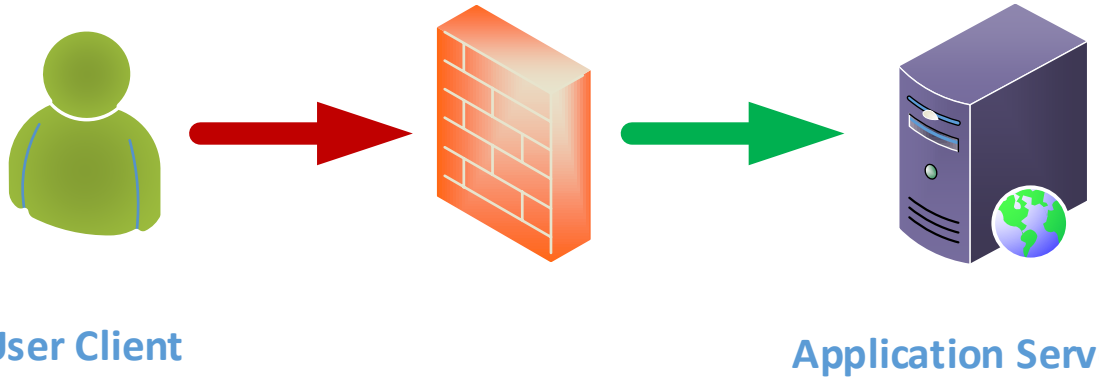
Lastausgleich 101

Was ist ein Load Balancer oder ADC?

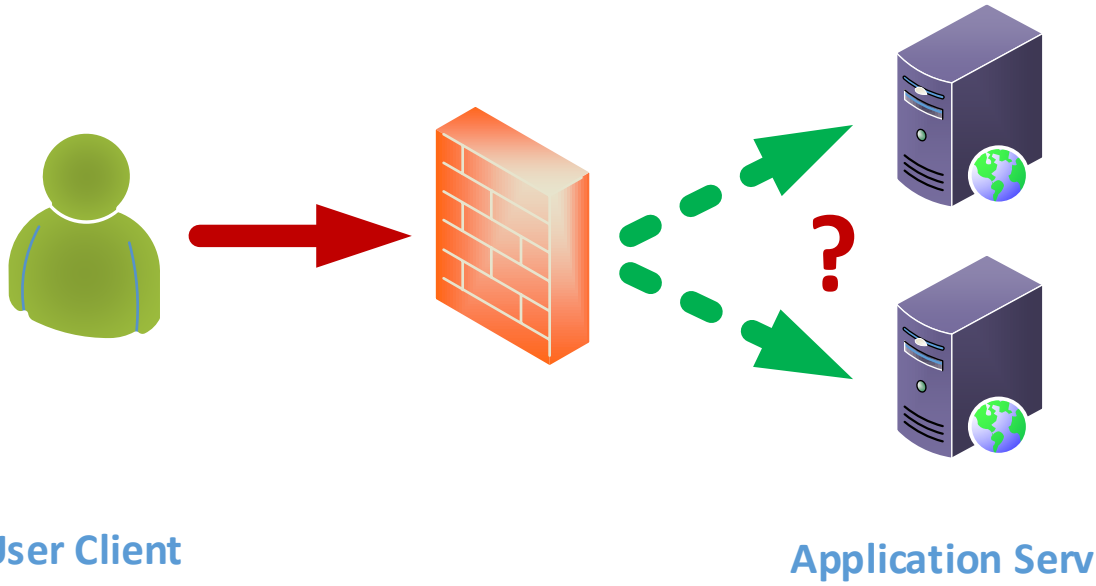
Load Balancer haben sich stark weiterentwickelt und verfügen über viel mehr Intelligenz als früher. Sie werden heute oft als Application Delivery Controller oder ADCs bezeichnet.

Bevor wir verstehen können, was ein Load Balancer oder ADC ist, müssen wir die Probleme der IT-Mitarbeiter und der Benutzer erkennen. Lassen Sie uns also ein Beispiel nehmen.

- Ein Unternehmen hat eine Webanwendung, die es im Internet veröffentlicht. Die Anwendung wird auf einem einzigen Webserver gehostet, wobei die Daten auf einem separaten Datenbankserver gespeichert sind.



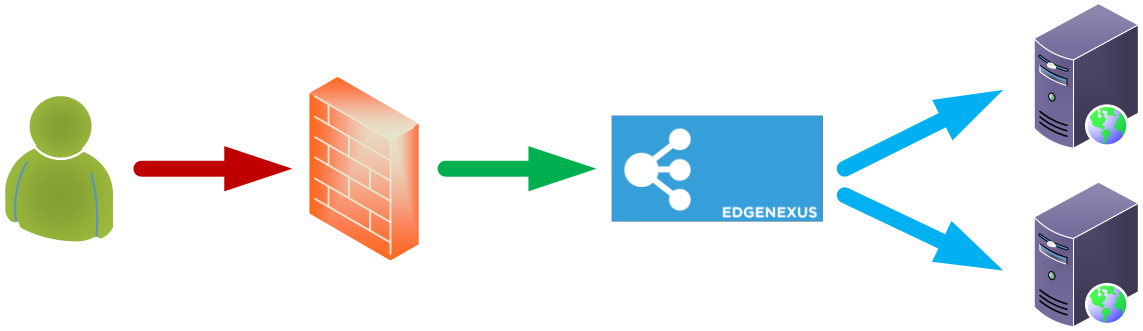
- Dieser Server verwendet als Beispiel die IP-Adresse 1.2.3.4.
- Die Zahl der Kunden, die auf die Anwendung zugreifen, nimmt regelmäßig zu, und einige haben darauf hingewiesen, dass die Leistung der Anwendung abnimmt.
- Die Analyse des Servers zeigt, dass der Datenverkehr, der auf den Server trifft, massiv zugenommen hat und weiter ansteigt.
- Daher wird beschlossen, einen weiteren Server zum Hosten der Anwendung hinzuzufügen.
- Der neue zweite Server verwendet die IP-Adresse 1.2.3.5.
- Das Problem besteht darin, den Client auf den neuen und den aktuellen Server zu leiten, um die Last zu verteilen und sicherzustellen, dass die Sitzung des Benutzers auf dem zuerst angemeldeten Server erhalten bleibt.



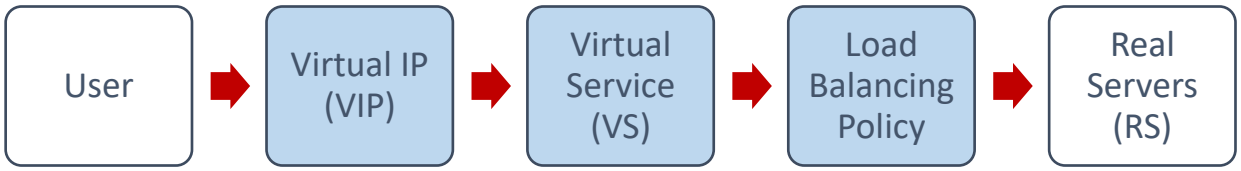
- Die Antwort ist ein Load Balancer oder ADC.

Und nun die Lösung.

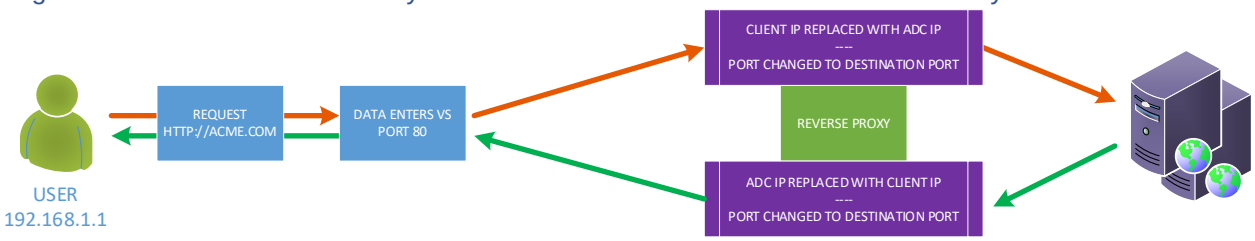
- Wir platzieren einen ADC vor den beiden Anwendungsservern.



- Der ADC wird eine nach außen gerichtete IP-Adresse von 1.2.3.6 haben, und die Firewall wird die Anfragen per NAT an diese Adresse statt an die frühere 1.2.3.4 umleiten
- Die IP der ADC, die die Anfragen empfängt, wird als VIP bezeichnet, und die Konfiguration wird als virtueller Dienst bezeichnet.
- Der ADC empfängt die Anfragen der Client-Benutzer und leitet sie unter Verwendung von Lastausgleichsrichtlinien an die echten Server weiter, während der Zustand der Anwendungsserver überwacht wird, um die Effizienz zu gewährleisten.



- Die ADC gleicht den Datenverkehr zu den Servern auf der Grundlage der verwendeten Lastausgleichsrichtlinie, der Art der Last und des Status der Anwendungsserver aus.
- Der Datenverkehr von den Servern wird über den ADC in umgekehrter Richtung an den Client zurückgesendet.
- Aufgrund der Art des Reverse Proxy sind der Server und der Client füreinander anonym.



- Die Reverse-Proxy-Technologie gewährleistet ein optimales Sicherheitsniveau.

VIPs und virtuelle Dienste (VS) erklärt

Bei einem VIP handelt es sich im Wesentlichen um eine IP-Adresse, die für die Verwendung auf dem EdgeADC definiert ist und Benutzern den Zugriff auf die damit verbundenen Dienste ermöglicht. Das ist so ziemlich alles, was ein VIP ist. Aufgrund der Funktionsweise des EdgeADC muss sich das VIP nicht im selben Subnetz wie die echten Server befinden, und diese Methode der Netzwerkadressübersetzung macht die Technologie sehr sicher vor Hackern, die versuchen, auf die internen Server zuzugreifen.

Hinweis: Die IP-Adresse des VIP darf nicht mit der für die Management-IP verwendeten IP-Adresse identisch sein.

Virtuelle Dienste bilden den Kern der EdgeADC-Proxy- und Lastausgleichstechnologien. Die virtuelle IP ist die Adresse, über die der virtuelle Dienst dem Netzwerk und der Welt bekannt gemacht wird und auf

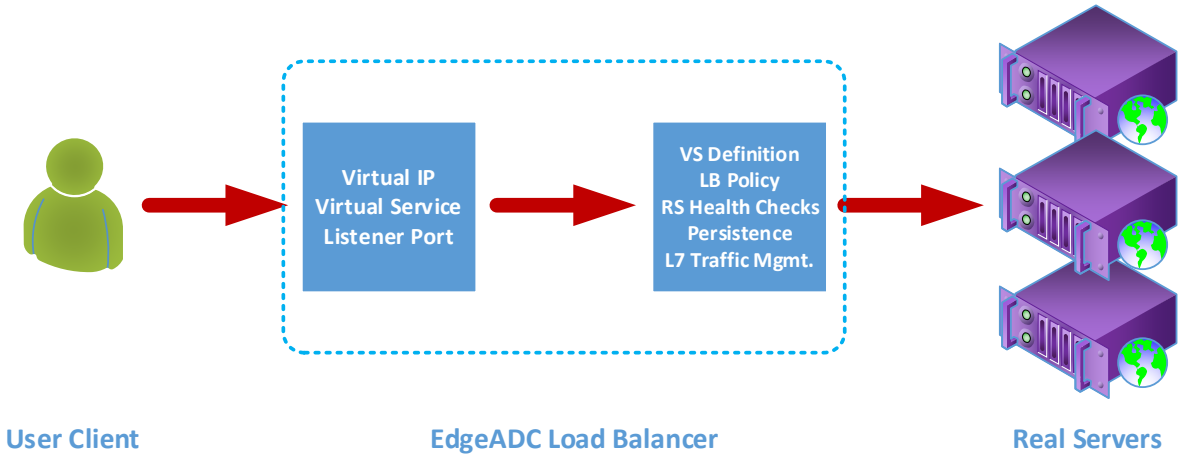
Datenverkehr und Anfragen von Clients wartet, die die von ihm bereitgestellten Anwendungen nutzen möchten.

Wenn Clients auf den VS treffen, wird der VS so konfiguriert, dass er zahlreiche Aktionen für den Datenverkehr durchführt, u. a:

- Proxy der Verbindung des Kunden
- Es werden spezifische Funktionen wie Komprimierung, Beschleunigung, Lastausgleich, Verkehrsüberwachung usw. ausgeführt.
- Weiterleitung der Client-Anfragen an Zielserver, die im Rahmen der Lastausgleichsrichtlinien des virtuellen Dienstes definiert sind.

Man kann sich den VS als mit einer IP-Adresse (VIP) verheiratet vorstellen, die der EdgeADC bei der Vorbereitung von Datenanforderungen abhört. Wenn Standard-TCP- oder -HTTP-Konfigurationen vorgenommen werden, stellt der Client eine Verbindung zum VIP her, und der EdgeADC verarbeitet die Anforderung gemäß der Definition, aus der die VS besteht. Sobald dies geschehen ist, leitet der EdgeADC den Datenverkehr an die angegebenen Real Server weiter.

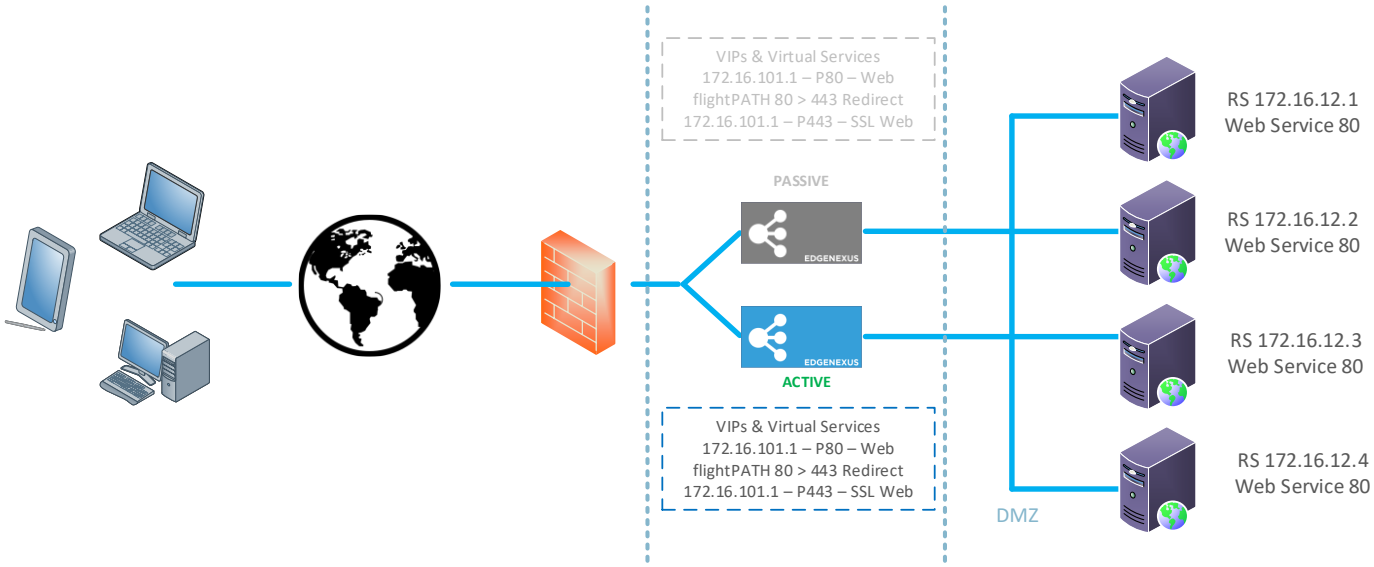
Der VS empfängt die Verbindung und die Daten in einer typischen Konfiguration und beendet sie dann oder leitet sie mithilfe der Reverse-Proxy-Engine im EdgeADC weiter. Der EdgeADC öffnet daraufhin eine neue Verbindung zu den Real-Servern und sendet die Daten weiter. Wenn die Realserver auf die Anfrage antworten, sendet das EdgeADC die Antwort über einen ähnlichen umgekehrten Pfad an den Client, je nach den Einstellungen in der Option Konnektivität auf der Registerkarte Lastausgleich der Realserver.



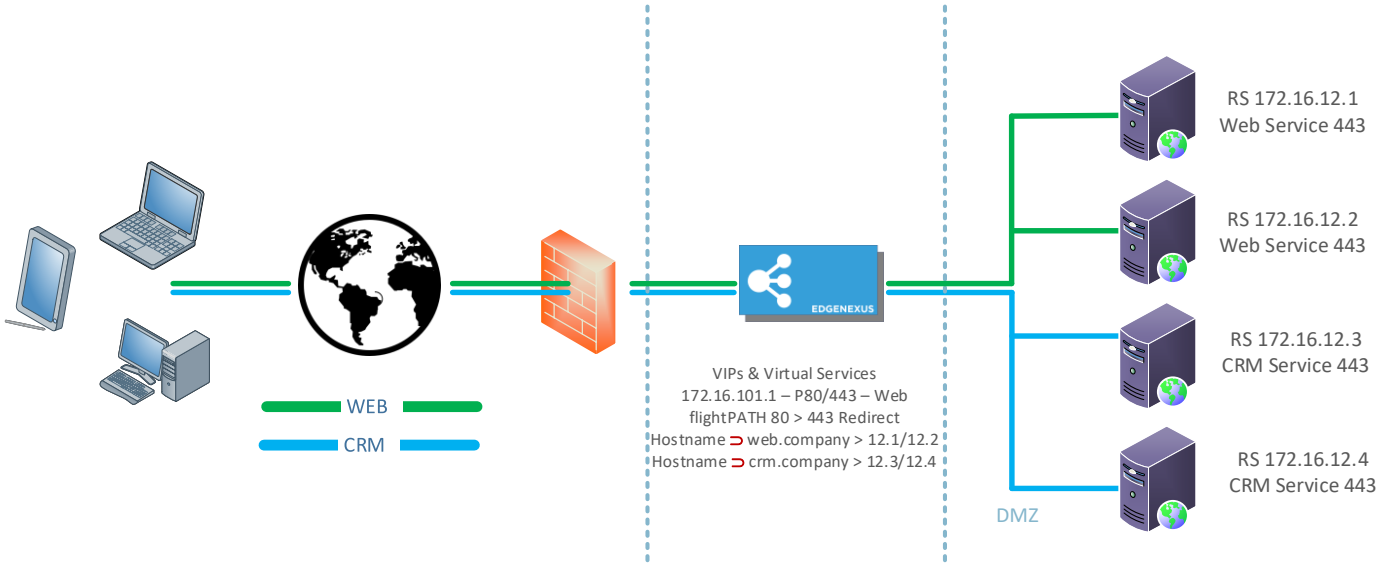
Eine virtuelle Dienstdefinition umfasst eine einzelne IP-Adresse (VIP) und eine Sammlung von Ports, die als Eingangspunkte zu verschiedenen Diensten dienen und eine Vielzahl von Protokollen verwenden.

Sie müssen zum Beispiel die Last einer Reihe von Webservern ausbalancieren, um Ausfallsicherheit zu gewährleisten. Nehmen wir nun an, dass der Zugriff auf diese Systeme über eine HTTPS-gesicherte Kommunikation mit https://myweb.company.com erfolgt.

Wenn man sich die Definition einer solchen Konfiguration ansieht, besteht sie aus einem einzigen VIP mit zwei Einträgen, einem für Port 80 und einem für Port 443. Dem VIP für Port 80 ist eine flightPATH-Regel zugeordnet, die den Datenverkehr zwangsweise in HTTPS umwandelt. Der zweite Eintrag für Port 443 leitet dann den Datenverkehr an die darunter definierten Real Server weiter. In ähnlicher Weise können Sie andere Dienste unter demselben VIP einrichten, um den Datenverkehr zu Mail-Servern oder anderen Anwendungsservern auszugleichen.



Bei weniger funktionalen ADCs würden Dienste, die dieselben Ports verwenden, unterschiedliche VIPs benötigen, aber der ADC und sein flightPATH-System ermöglichen die Verwendung eines einzigen VIPs für mehrere Dienste, die dieselben Ports verwenden. So könnten Sie zwei Anwendungen, die beide über 443 mit unterschiedlichen Hostnamen angesprochen werden, mit einem einzigen VIP betreiben. Ein Beispiel ist unten abgebildet.



Die Systeme des EdgeADC sind äußerst flexibel und ermöglichen die Definition sehr komplexer und funktionaler Konfigurationen.

Was ist ein Lastausgleichsdiensttyp?

Die Arten von Lastausgleichsdiensten bestehen aus Algorithmen und Methoden, die zur intelligenten Verteilung oder zum Lastausgleich des Datenverkehrs auf Serverpools verwendet werden. Die Methode und der Algorithmus, die die ADC zur Verfügung stellt, hängen von der Art des Dienstes oder der Anwendung ab, die auf den Servern verwendet wird, auf denen der Lastausgleich stattfindet, und auch vom Zustand des Netzwerks und der verwendeten Server. Es sollte beachtet werden, dass der von Ihnen gewählte Lastausgleichsdiensttyp auch von der Höhe des Datenverkehrs abhängt, der durch den ADC gesendet wird. Wenn also der Verkehrsdurchsatz oder die Last gering ist, können einfache Lastausgleichsdienste verwendet werden. Wenn die Last jedoch größer ist, müssen Sie möglicherweise komplexere Typen wählen, um eine effizientere Lastverteilung auf die Back-End-Server zu erreichen.

Die folgenden Arten von Lastausgleichsdiensten sind innerhalb des EdgeADC verfügbar.

DICOM	LAYER 4 UDP	RPC
FTP	SCHICHT 4 TCP/UDP	RPC/ADS
HTTP(S)	DNS	RPC/CA/PF
IMAP	POP3	SMTP
LAYER 4 TCP	RDP	GSLB

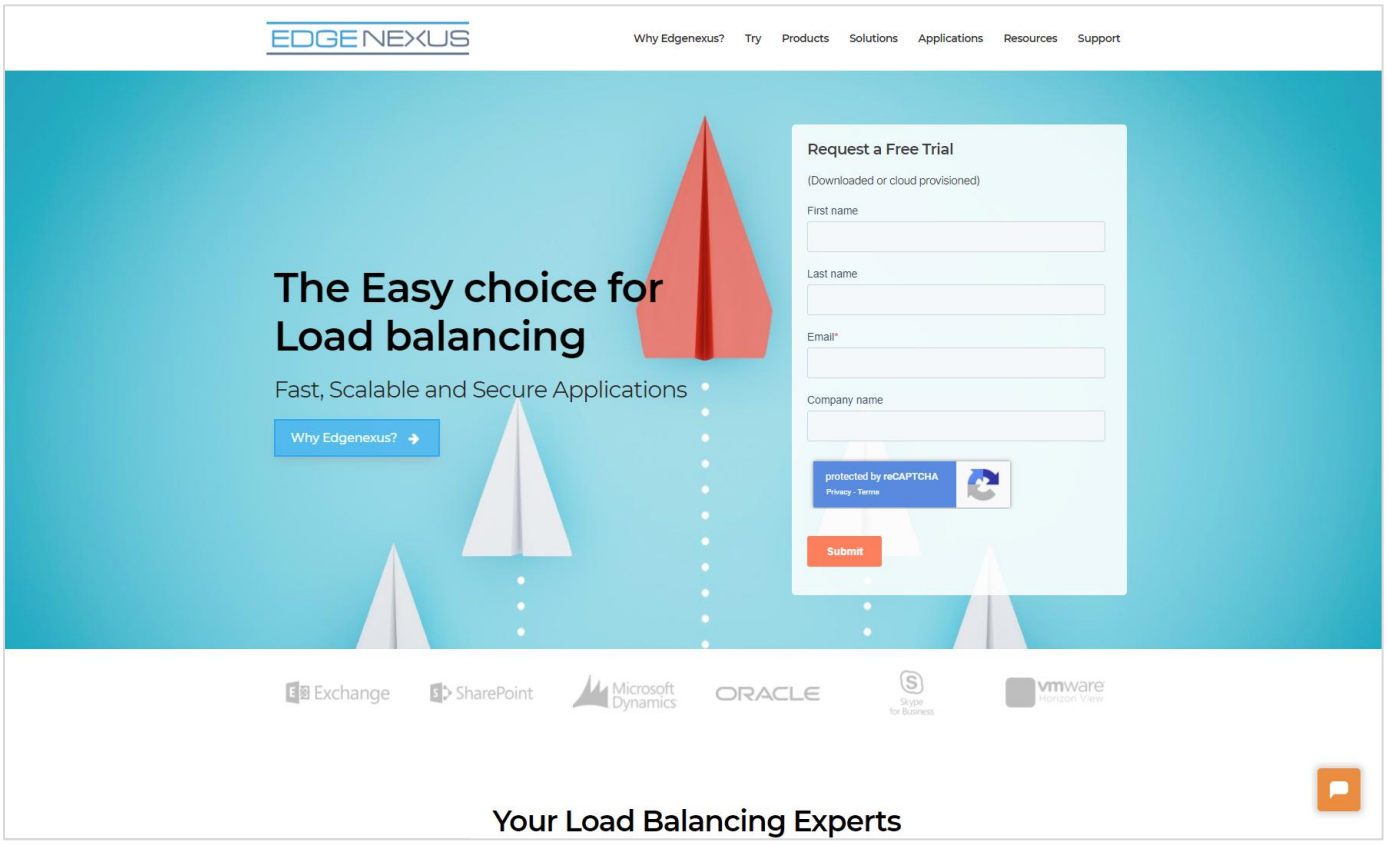
Der Beginn der Reise

Herunterladen des EdgeADC

Vor der Installation müssen Sie zunächst den EdgeADC herunterladen, der für Ihre Umgebung geeignet ist.

Wir bieten Editionen für die meisten virtualisierten Umgebungen und eine ISO-Edition für die direkte Installation auf Bare-Metal-Hardware.

Der erste Schritt ist das Ausfüllen des Bewertungsformulars, das Sie auf der Edgenexus-Website unter https://www.edgenexus.io/products/load-balancer/free-trial/ finden.



Das Verfahren ist einfach. Nachdem Sie das Formular ausgefüllt und abgeschickt haben, werden Sie zur Download-Seite weitergeleitet, wo Sie das richtige Bild für Ihre Umgebung auswählen können.

EdgeADC-Editionen sind für die folgenden Virtualisierungssysteme verfügbar:

- VMware ESX
- Microsoft Hyper-V
- Citrix XenServer
- Nutanix
- KVM

Sie können sich auch für einen Test in der Cloud entscheiden, indem Sie Microsoft Azure oder Amazon AWS Marketplace Editionen verwenden.

Wenn Sie die Software für eine Vor-Ort-Installation herunterladen, erhalten Sie den EdgeADC mit einer integrierten 14-Tage-Testlizenz. Wir empfehlen Ihnen, sich ansales@edgenexus.io zu wenden und einen 30-Tage-Lizenzschlüssel anzufordern, der alle Funktionen aktiviert.

Einrichtung

Installation ng des EdgeADC

Der EdgeADC (ADC) kann auf einer Vielzahl von Plattformen installiert werden, für die jeweils ein eigenes Installationsprogramm erforderlich ist, das Ihnen nach der Registrierung zum Download zur Verfügung gestellt wird.

Dies sind die verschiedenen verfügbaren Installationsmodelle.

- VMware ESXi
- KVM
- Citrix Xen
- Nutanix AHV
- Microsoft Hyper-V
- Oracle VM
- Proxmox (OVA verwenden)
- ISO für BareMetal-Hardware

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

Installieren auf VMware ESXi

Der ADC wird für die Installation auf VMware ESXi 5.x und höher unterstützt.

- Laden Sie das neueste OVA-Installationspaket von ADC über den entsprechenden Link in der Download-E-Mail herunter.
- Nach dem Download entpacken Sie die Datei bitte in ein geeignetes Verzeichnis auf Ihrem ESXi-Host oder SAN.
- Wählen Sie in Ihrem vSphere-Client Datei: OVA/OVF-Vorlage bereitstellen.
- Wählen Sie das Verzeichnis aus, in dem Sie Ihre Dateien gespeichert haben; wählen Sie die OVF-Datei und klicken Sie auf **NEXT**
- Der ESX-Server fordert den Namen der Appliance an. Geben Sie einen geeigneten Namen ein und klicken Sie auf **NEXT**
- Wählen Sie den Datenspeicher aus, auf dem Ihre ADC Appliance ausgeführt werden soll.
- Wählen Sie einen Datenspeicher mit ausreichend Platz und klicken Sie auf **NEXT**
- Sie erhalten dann Informationen über das Produkt; klicken Sie auf **NEXT**
- Klicken Sie auf **NEXT.**
- Nachdem 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 den VA und gehen Sie zu Power > Power-On
- Ihr VA wird dann gebootet und der ADC-Boot-Bildschirm wird auf der Konsole angezeigt.

Installation 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*

Aktivierung 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 sie als VMXNET3 aus
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. Ermitteln Sie die MAC-Adressen der beiden NICs (achten Sie auf 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 sie 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 Testzwecke können Sie VMware Workstation und Player verwenden.

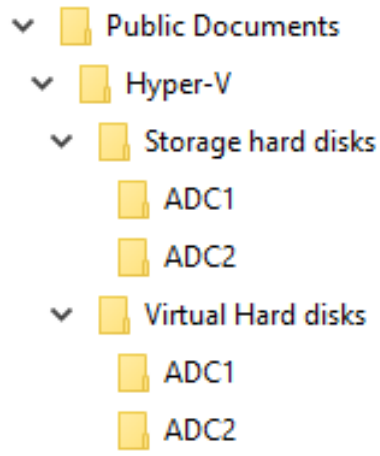
Bitte lesen Sie den Abschnitt **ERSTE BOOT-KONFIGURATION**, um fortzufahren.

Installieren unter Microsoft Hyper-V

Die Edgenexus ADC Virtual Appliance kann problemlos innerhalb einer Microsoft Hyper-V Virtualisierungsumgebung installiert werden. Diese Anleitung geht davon aus, dass Sie Ihr Hyper-V-System und Ihre Systemressourcen korrekt spezifiziert und konfiguriert haben, um den ADC und seine Lastausgleichsarchitektur unterzubringen.

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

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



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

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

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

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

Bitte lesen Sie den Abschnitt **ERSTE BOOT-KONFIGURATION**, um fortzufahren.

Installieren auf Citrix XenServer

Die ADC Virtual Appliance ist auf Citrix XenServer installierbar.

- Extrahieren Sie die ADC OVA ALB-VA-Datei auf Ihren lokalen Rechner oder Server.
- Öffnen Sie Citrix XenCenter Client.
- Wählen Sie in Ihrem XenCenter-Client **"Datei: Importieren".**
- Suchen Sie die OVA-Datei, wählen Sie sie aus und klicken Sie auf **"Weiter öffnen".**
- Wählen Sie den Ort der VM-Erstellung, wenn Sie dazu aufgefordert werden.
- Wählen Sie den XenServer, den Sie installieren möchten, und klicken Sie auf **"NEXT".**
- Wählen Sie das Storage Repository (SR) für die Platzierung der virtuellen Festplatte, wenn Sie dazu aufgefordert werden.
- Wählen Sie eine SR mit ausreichend Platz und klicken Sie auf **"NEXT".**
- Ordnen Sie Ihre virtuellen Netzwerkschnittstellen zu. Auf beiden Schnittstellen steht Eth0. Beachten Sie jedoch, dass die untere Schnittstelle Eth1 ist.
- Wählen Sie das Zielnetz 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 Verwaltungsschnittstelle, normalerweise Netzwerk 0, und lassen Sie die Netzwerkeinstellungen auf DHCP. Bitte beachten Sie, dass Sie statische IP-Adressangaben zuweisen 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" 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.

- Nach der Konfiguration wird die Anmeldung bei der VA angezeigt.

Bitte lesen Sie den Abschnitt **ERSTE BOOT-KONFIGURATION**, um fortzufahren.

Installieren auf KVM

Der folgende Abschnitt zeigt, wie der EdgeADC auf einer KVM-Plattform installiert wird. Die für diese Übung verwendete KVM-Plattform lief auf einem CentOS v8-Betriebssystem mit installiertem Cockpit und Virtualisierung.

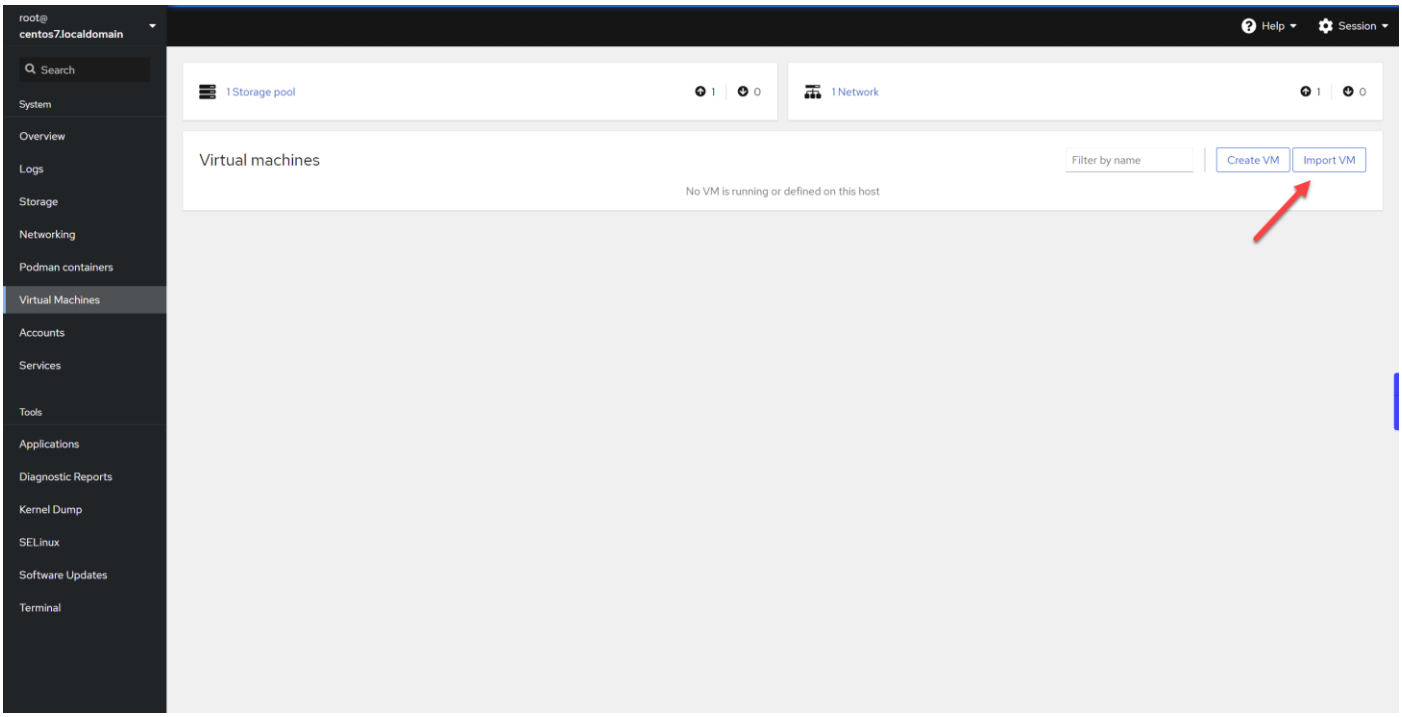
Anforderungen und Versionen

Diese Anleitung ist für EdgeADC 4.2.6 und höher relevant.

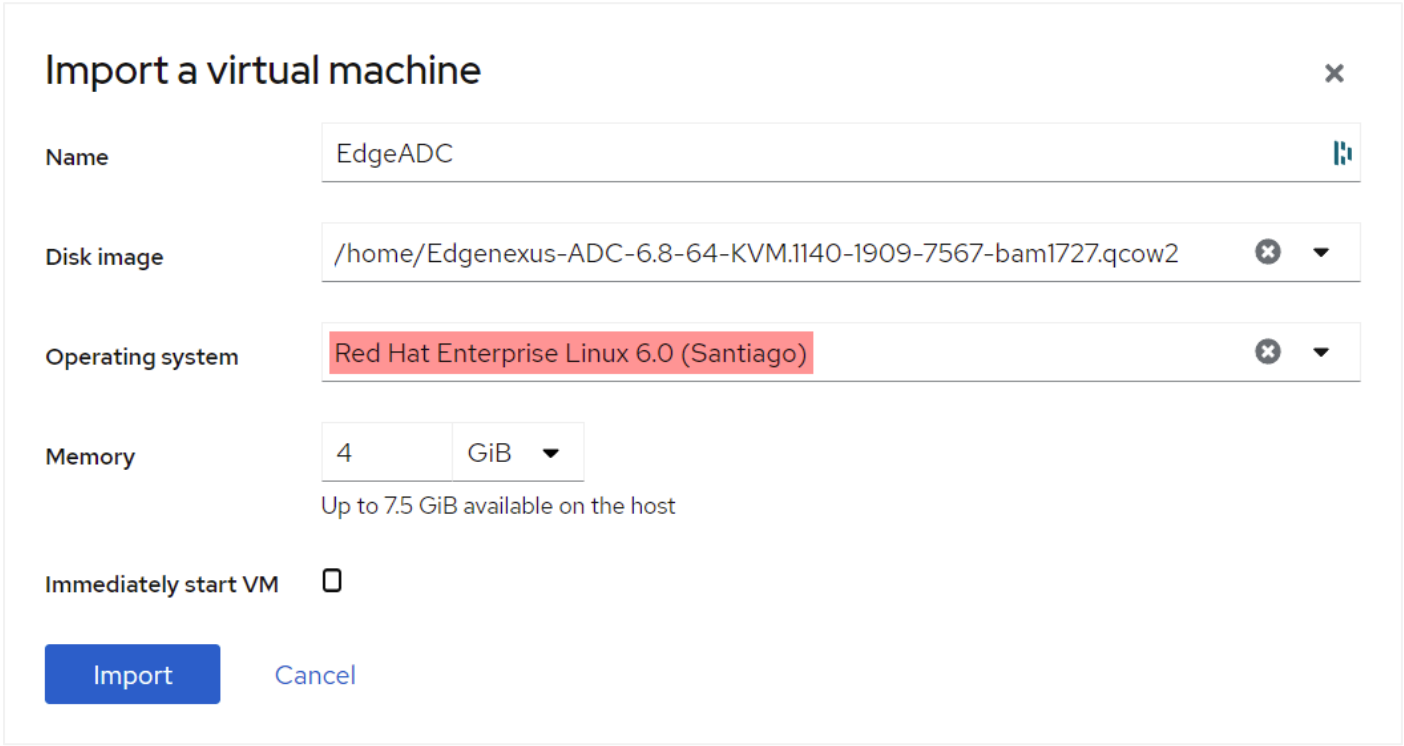
Die folgende Anleitung bezieht sich nicht auf die Installation von KVM oder dessen Vernetzung.

Wir sind davon ausgegangen, dass Sie die virtuelle KVM-Anwendung heruntergeladen und auf dem Host an einem zugänglichen Ort gespeichert haben.

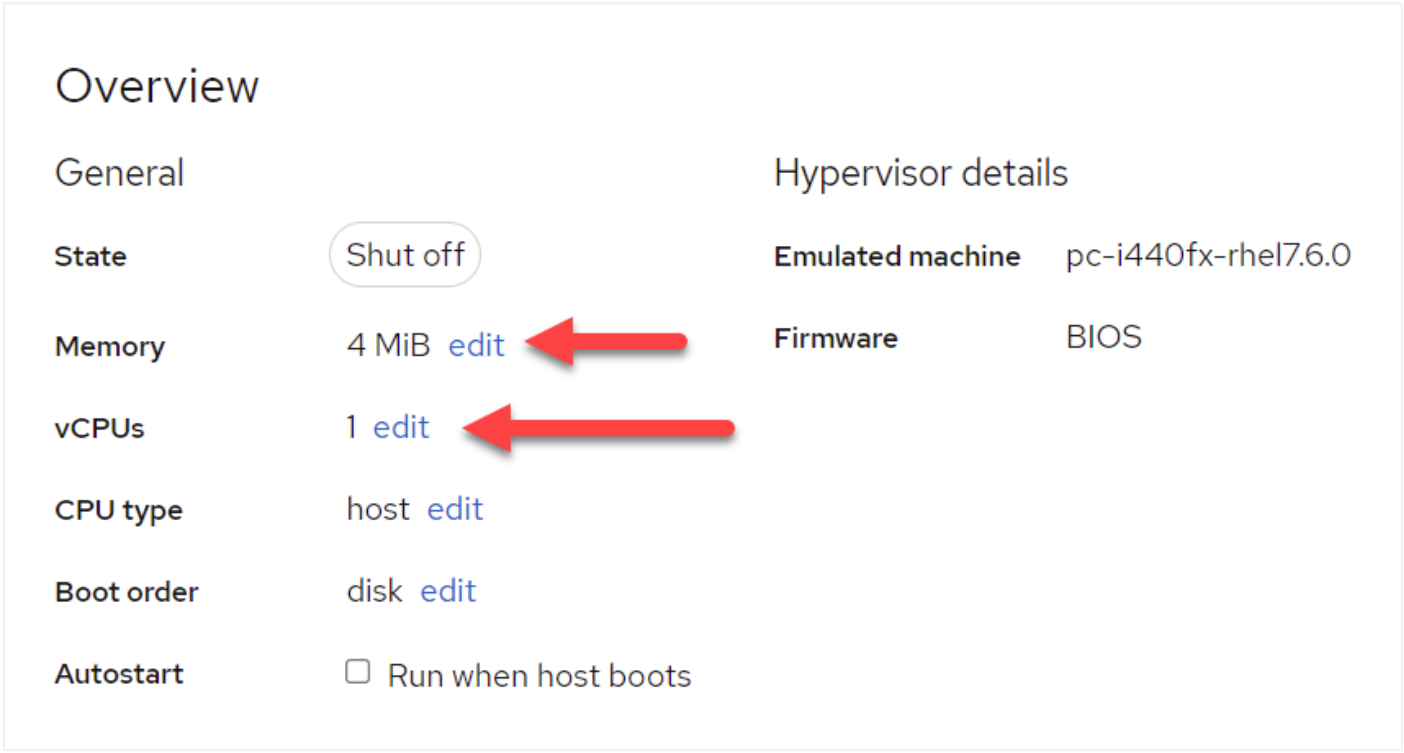
- Der erste Schritt ist die Anmeldung bei der Cockpit-Konsole.



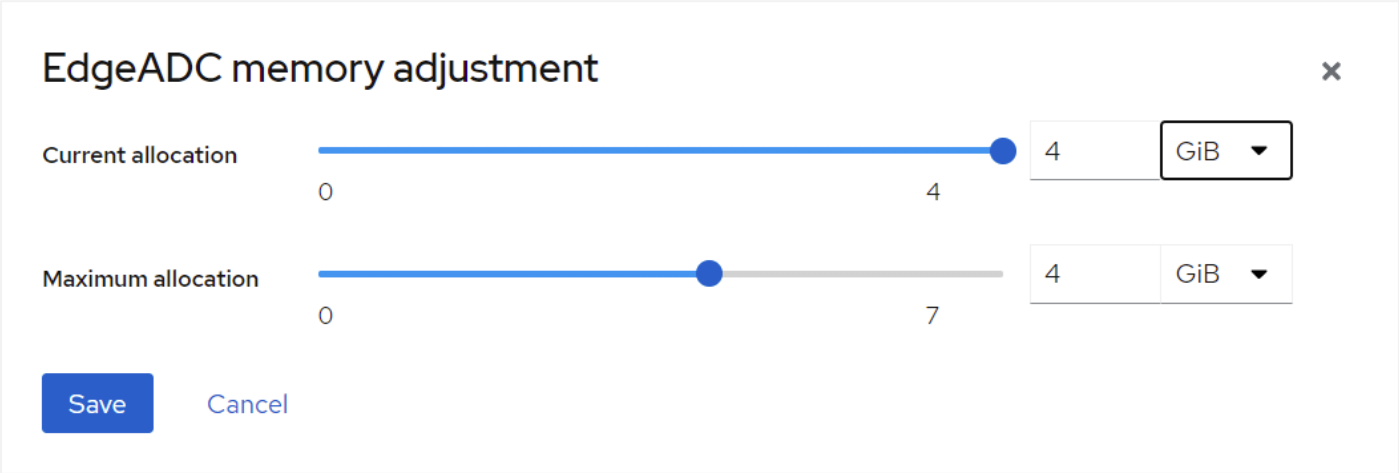
- Klicken Sie auf VM importieren
- Im ersten Dialogfeld müssen Sie die Details für den Import der virtuellen Appliance angeben. Der Inhalt der Felder ist in der Abbildung unten dargestellt. Sie müssen Red Hat Enterprise 6.0 als Betriebssystem angeben.



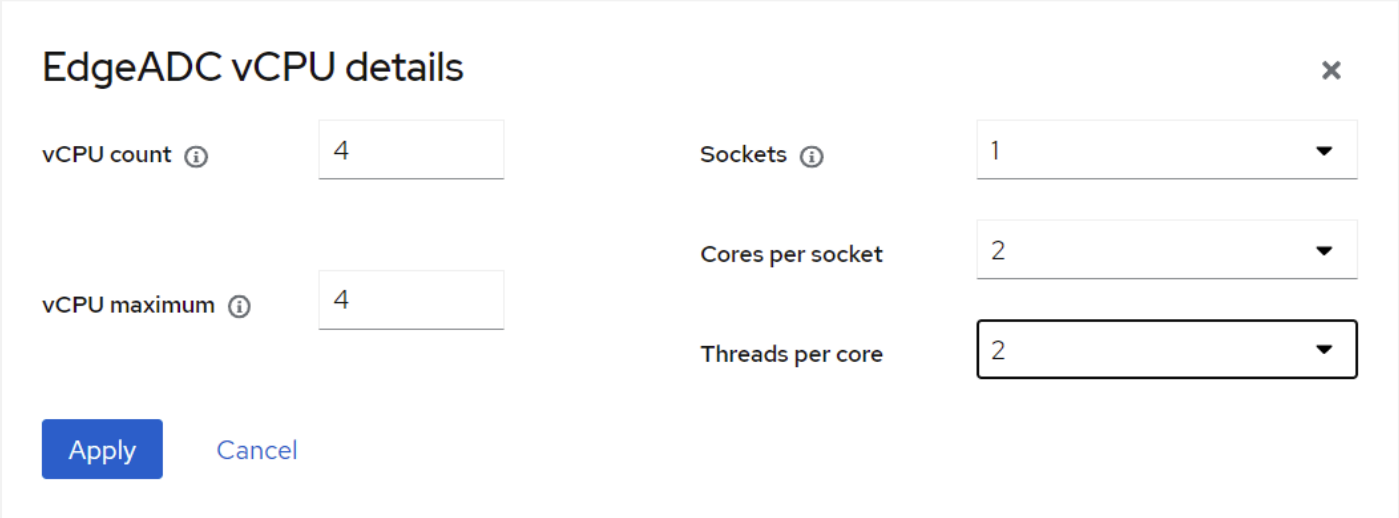
- Bitte stellen Sie sicher, dass Sie die Option "VM sofort starten" deaktiviert haben.
- Wenn Sie die Angaben gemacht haben, klicken Sie bitte auf die Schaltfläche Importieren.
- Der nächste Schritt ist die Angabe der vCPU und der Speicherzuweisung, die Sie verwenden möchten.



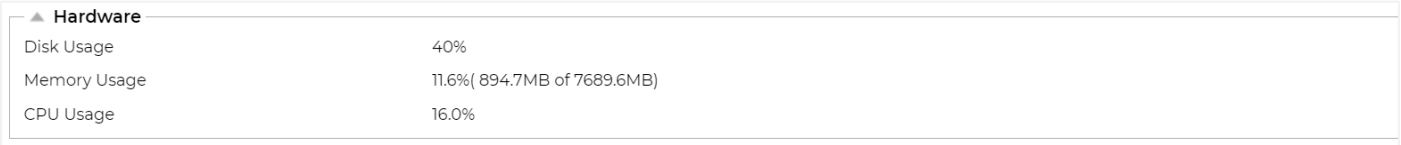
- Um den Speicher zuzuweisen, wird ein Dialogfeld ähnlich dem untenstehenden angezeigt.



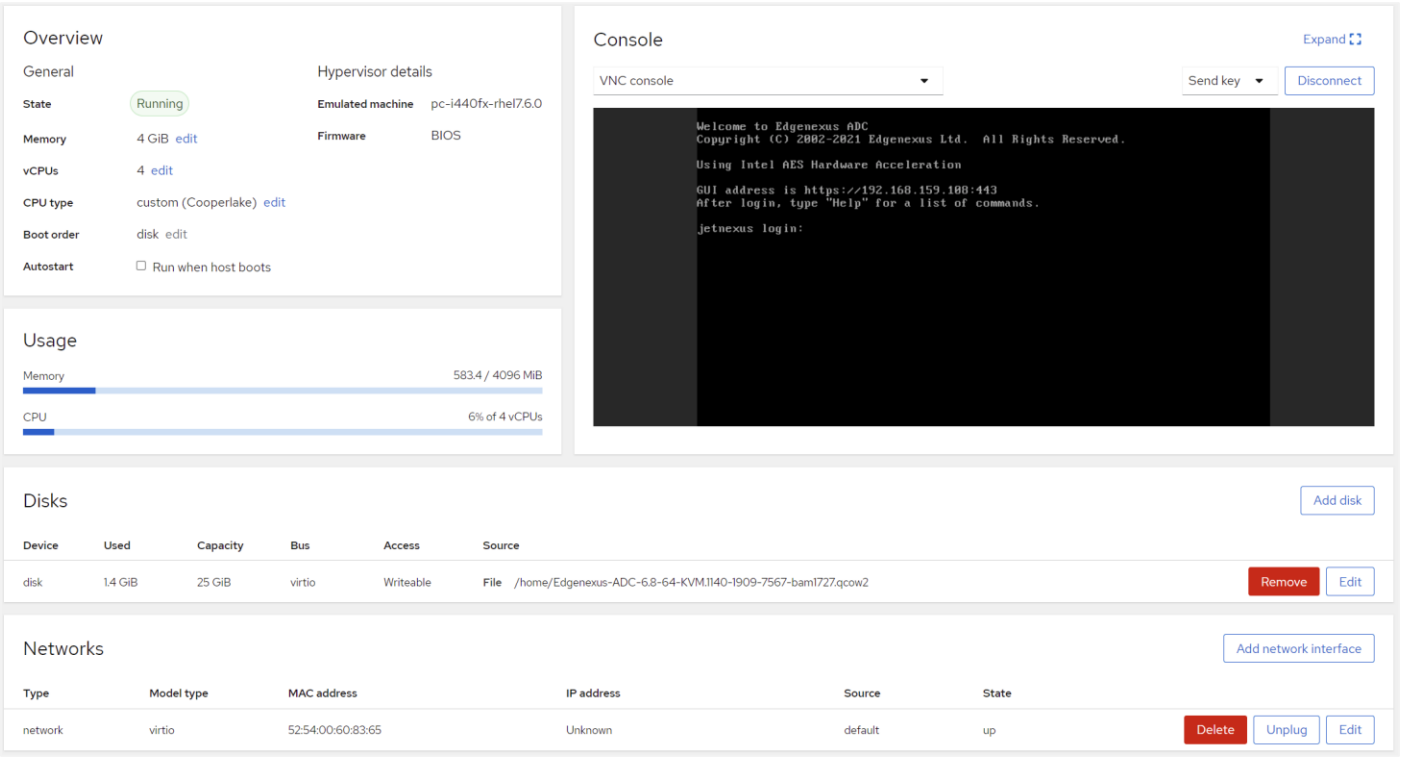
- Um die vCPU zuzuweisen, wird ein Dialogfeld ähnlich dem untenstehenden angezeigt.



- Die von uns getroffenen Entscheidungen sind nur Beispiele, aber praktikabel, es sei denn, Sie verwenden einen hohen Datendurchsatz mit SSL-Wiederverschlüsselung; in diesem Fall müssen Sie den Abschnitt Hardware unter Ansicht > Statistik entsprechend anpassen.



- Sie haben nun einen funktionierenden ADC in KVM installiert. Siehe Bild unten.



Installieren auf Nutanix AHV

Der folgende Abschnitt zeigt, wie das EdgeADC auf einer Nutanix AHV-Plattform installiert wird.

Anforderungen und Versionen

Diese Anleitung ist für EdgeADC 4.2.6 und höher relevant.

Alle Versionen des Nutanix-Hypervisors sind kompatibel, aber die Zertifizierung wurde auf Nutanix Version 5.10.9 durchgeführt.

- Der erste Schritt ist die Anmeldung bei Nutanix Prism Central.

Hochladen des EdgeADC-Bildes

- Navigieren Sie zu Virtuelle Infrastruktur > Bilder
- Klicken Sie auf die Schaltfläche Bild hinzufügen
- Wählen Sie die heruntergeladene EdgeADC-Bilddatei aus und klicken Sie auf die Schaltfläche Öffnen, um das Bild hochzuladen.
- Geben Sie einen Namen für das Bild in das Feld Bildbeschreibung ein.
- Wählen Sie eine passende Kategorie
- Wählen Sie das Bild aus und klicken Sie auf die rechte Pfeiltaste
- Wählen Sie Alle Bilder und klicken Sie auf Speichern.

Erstellen der VM

- Navigieren Sie zu Virtuelle Infrastruktur > VMs
- Klicken Sie auf die Schaltfläche VM erstellen
- Geben Sie einen Namen für die VM, die Anzahl der gewünschten CPUs und die Anzahl der Kerne ein, die Sie der VM zuweisen möchten.
- Blättern Sie dann im Dialogfeld nach unten und geben Sie die Menge an Speicher ein, die Sie der VM zuweisen möchten. Sie können mit 4 GB beginnen und diese Menge je nach Nutzung erhöhen.

Hinzufügen der Festplatte

- Klicken Sie anschließend auf den Link Add New Disk
- Wählen Sie in der Dropdown-Liste Operation die Option Clone from Image Service.
- Wählen Sie das hinzugefügte EdgeADC-Bild aus und klicken Sie auf die Schaltfläche Hinzufügen.
- Wählen Sie den Datenträger aus, der als bootfähiger Datenträger dienen soll.

Hinzufügen von NIC, Netzwerk und Affinität

- Klicken Sie anschließend auf die Schaltfläche Neue NIC hinzufügen. Sie müssen zwei NICS haben.
- Wählen Sie das Netzwerk und klicken Sie auf die Schaltfläche Hinzufügen
- Klicken Sie auf die Schaltfläche Affinität festlegen
- Wählen Sie die Nutanix-Hosts aus, auf denen die VM ausgeführt werden darf, und klicken Sie dann auf die Schaltfläche Speichern.
- Überprüfen Sie die von Ihnen vorgenommenen Einstellungen und klicken Sie auf die Schaltfläche Speichern

Einschalten der VM

- Klicken Sie in der Liste der VMs auf den Namen der VM, die Sie gerade erstellt haben
- Klicken Sie auf die Schaltfläche "Einschalten" für die VM
- Sobald die VM eingeschaltet ist, klicken Sie auf die Schaltfläche Konsole starten

Konfigurieren der EdgeADC-Vernetzung

- Folgen Sie den Anweisungen im Abschnitt Erste Boot-Umgebung.
- Der EdgeADC ist nun einsatzbereit, und Sie können über Ihren Browser und die Management-IP-Adresse auf die grafische Benutzeroberfläche zugreifen.

Installieren auf ProxMox

Die Installation von ProxMox ist einfach, erfordert aber ein paar zusätzliche Schritte.

Wir werden die VMWare OVA-Version der Installation verwenden. Dies ist ein mehrstufiger Prozess und erfordert Kenntnisse der Shell-Befehle in ProxMox. Wir haben die Anweisungen jedoch so einfach wie möglich gestaltet. Wir gehen davon aus, dass Sie mit ProxMox vertraut sind und werden daher nicht näher auf die Funktionen von ProxMox eingehen.

Hochladen der OVA in ProxMox

Da wir eine OVA-Version verwenden, müssen wir zunächst die OVA in ProxMox hochladen.

- Anmeldung an der ProxMox-Konsole
- Erstellen Sie einen Ordner namens OVA_Import.
- Sie müssen nun einen SFTP-Client wie WinSCP (Windows) oder CyberDuck (Mac) verwenden, um die OVA-Datei zu übertragen.
- Sobald die Datei übertragen ist, wird sie in dem von Ihnen erstellten Ordner angezeigt.
- Geben Sie den folgenden Befehl ein, um den Inhalt der OVA-Datei zu extrahieren.
- Tar xvf {Dateiname}. Siehe das Beispiel unten.

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

- Nach dem Extrahieren sollten Sie etwas wie das folgende Beispiel sehen.

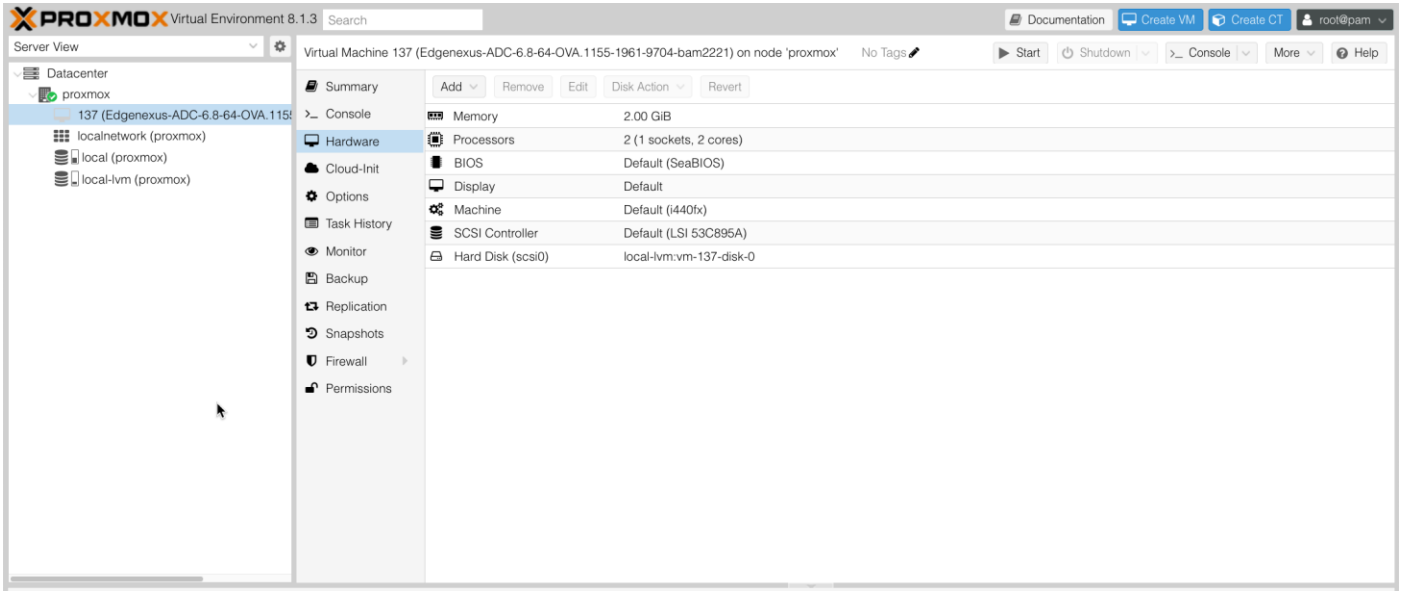
```
root@proxmox:~/OVA_Import# ls
Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.ova
root@proxmox:~/OVA_Import# tar xvf Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.ova
Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.ovf
```

```
Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.mf
Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221-disk1.vmdk
root@proxmox:~/OVA_Import#
```

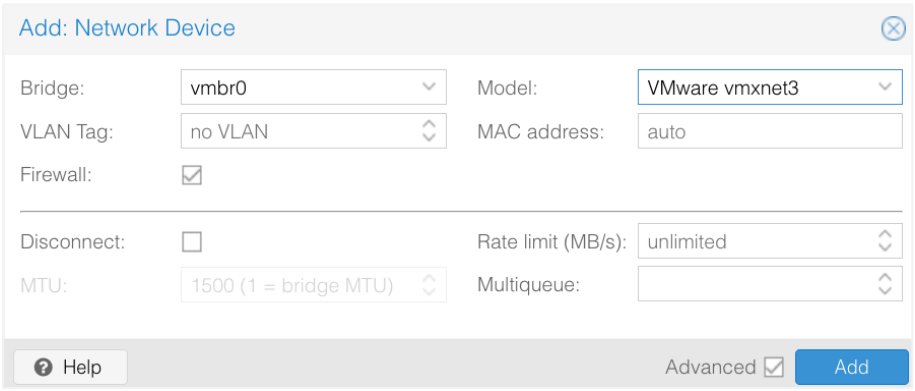
- Es gibt drei Dateien. Die .ovf und .mf sind die Konfiguration. Die .vmdk ist die virtuelle Festplatte, auf der sich der ADC befindet.
- Der nächste Schritt ist der Import des VMDK in ProxMox und die Erstellung der virtuellen Maschine.
- Geben Sie den folgenden Befehl ein, um die virtuelle Maschine unter Verwendung der Konfigurationsdateien zu erstellen.

```
qm importovf 137 ./{Dateiname.ovf} local-lvm --format qcow2
```

- In diesem Beispiel haben wir eine ID von 100 gegeben, aber dies kann für Ihre Installation anders sein, wenn Sie bereits virtuelle Maschinen in ProxMox erstellt haben. Sie können die nächste ID bestimmen, indem Sie den Prozess der VM-Erstellung in ProxMox starten, oder indem Sie eine Zahl höher als 100 wählen, die sicher außer Reichweite ist.
- Die VM ist nun erstellt.



- Der nächste Schritt besteht darin, der VM eine Netzwerkschnittstelle hinzuzufügen.
- Klicken Sie auf der rechten Seite auf Hardware.
- Klicken Sie auf Hinzufügen und wählen Sie eine Netzwerkschnittstelle aus.



- Konfigurieren Sie es wie in der Abbildung oben gezeigt. Es ist wichtig, das Modell als VMware vmxnet3 zu wählen.
- Klicken Sie nach der Konfiguration auf Hinzufügen.
- Sie können je nach Bedarf weitere Netzwerkadapter hinzufügen.
- Sie können nun die VM starten und mit den Anweisungen im Kapitel "Erste Boot-Konfiguration" fortfahren.

Erste Boot-Konfiguration

Beim ersten Start zeigt die ADC (im Folgenden auch VA genannt) den folgenden Bildschirm an, der zur Konfiguration für den Produktionsbetrieb auffordert.

Erster Start - Manuelle Netzwerkdetails

Beim ersten Start haben Sie 10 Sekunden Zeit, um die automatische Zuweisung von IP-Daten 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 dauerhaft und überleben einen Neustart und müssen nicht erneut auf der VA konfiguriert werden.

Erster Start - DHCP erfolgreich

Wenn Sie den Netzwerkzuweisungsprozess nicht unterbrechen, kontaktiert Ihr ADC nach einer Zeitüberschreitung einen DHCP-Server, um seine Netzwerkdaten zu erhalten. Wenn der Kontakt erfolgreich ist, werden Ihrem Gerät die folgenden Informationen zugewiesen.

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

Wir empfehlen Ihnen, den ADC nur dann mit einer DHCP-Adresse zu betreiben, wenn diese IP-Adresse dauerhaft mit der MAC-Adresse des ADC im DHCP-Server verknüpft ist. Wir empfehlen, bei der Verwendung der virtuellen Appliances immer eine **FIXED IP ADDRESS** zu 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 so lange um 1 erhöht, bis die VA eine freie IP-Adresse findet. Ebenso prüft die VA, ob

die IP-Adresse derzeit verwendet wird, und wenn dies der Fall ist, wird die Zahl erneut erhöht 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.

```
set greenside={IP-Adresse}
```

Ändern der Subnetzmaske für eth0

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

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

Zuweisen eines Standard-Gateways

Die VA benötigt ein Standard-Gateway für ihren Betrieb. Um das Standardgateway festzulegen, verwenden Sie den Befehl **route add default gw [GATEWAY IP]** wie im folgenden Beispiel gezeigt.

```
route add default gw {IP-Adresse}
```

Überprüfen des Standard-Gateways

Um zu überprüfen, ob das Standardgateway hinzugefügt wurde und korrekt ist, verwenden Sie den Befehl **route**. Dieser Befehl zeigt die Netzwerkrouten und den Wert des Standardgateways an. Siehe das folgende Beispiel.

```
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 Testbetrieb zu konfigurieren.

Zugriff auf die Webschnittstelle

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**.**

Die ADC verwendet standardmäßig ein selbstsigniertes SSL-Zertifikat. Sie können die ADC so ändern, dass sie ein SSL-Zertifikat Ihrer Wahl verwendet.

Sobald Ihr Browser das ADC erreicht, wird Ihnen der Anmeldebildschirm angezeigt. Die werkseitig voreingestellten Anmeldedaten für den ADC sind:

Username: admin / Pwd: jetnexus

Befehlsreferenztabelle

Befehl	Parameter1	Parameter2	Beschreibung	Beispiel
Datum			Zeigt das aktuell eingestellte Datum und die Uhrzeit an	Tue Sept 3 13:00 UTC 2013
Standardwerte			Legen Sie die Werkseinstellungen für Ihr Gerät fest	
Ausgang			Abmelden von der Befehlszeilenschnittstelle	
Hilfe			Zeigt alle gültigen Befehle an	
ifconfig	[leer]		Anzeigen der Schnittstellenkonfiguration für alle Schnittstellen	ifconfig
	eth0		Nur die Schnittstellenkonfiguration von eth0 anzeigen	ifconfig eth0
Maschinennummer			Dieser Befehl gibt die Maschinennummer an, die zur Lizenzierung des ADC verwendet wird ADC	EF4-3A35-F79
kündigen			Abmelden von der Befehlszeilenschnittstelle	
Neustart			Beenden Sie alle Verbindungen und starten Sie den ADC neu.	Neustart
Neustart			Neustart der virtuellen ADC-Dienste	
Route	[leer]		Anzeigen der Routing-Tabelle	Route
	hinzufügen.	Standard-GW	Hinzufügen der IP-Adresse des Standard-Gateways	route add default gw 192.168.100.254
einstellen.	Grünseiten		Einstellen der Management-IP-Adresse für ADC	set greenside=192.168.101.1
	Maske		Legen Sie die Subnetzmaske für eine Schnittstelle fest. Schnittstellennamen sind eth0, eth1....	Maske eth0 255.255.255.0 setzen
anzeigen			Zeigt die globalen Konfigurationseinstellungen an	
Abschaltung			Beenden Sie alle Verbindungen und schalten Sie den ADC aus.	
Status			Zeigt die aktuelle Datenstatistik an	
top			Anzeigen der Prozessinformationen wie CPU und Speicher	
viewlog	Nachrichten		Zeigt die rohen Syslog-Meldungen an	Logmeldungen anzeigen

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

Die Web-Konsole

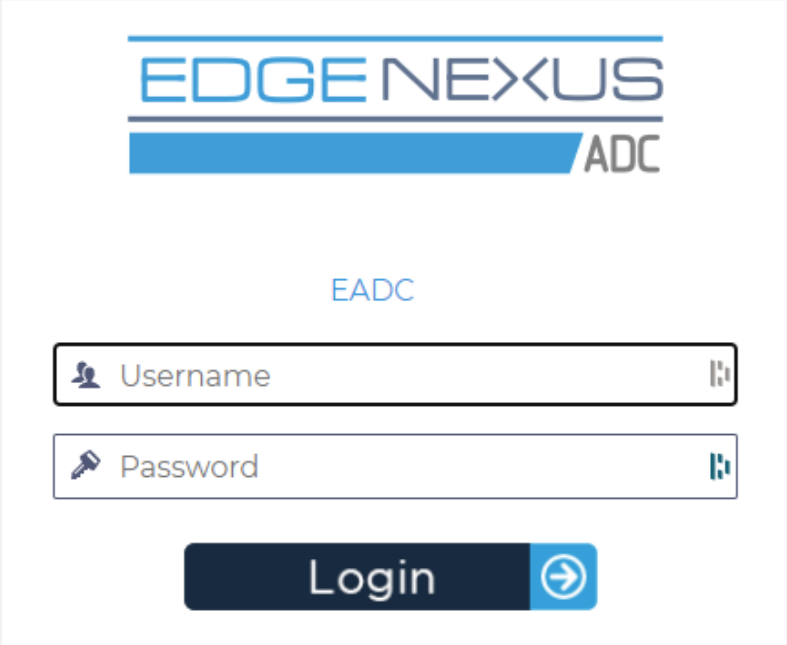
Starten der ADC Web-Konsole

Alle Funktionen des ADC 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 dargestellt aus und Sie können sich als Administrator anmelden.



Standard-Login-Anmeldeinformationen

Die Standard-Anmeldedaten sind:

Username: admin / Pwd: jetnexus

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

Sobald Sie sich erfolgreich angemeldet haben, wird das Haupt-Dashboard der ADC auf dem Bildschirm angezeigt.

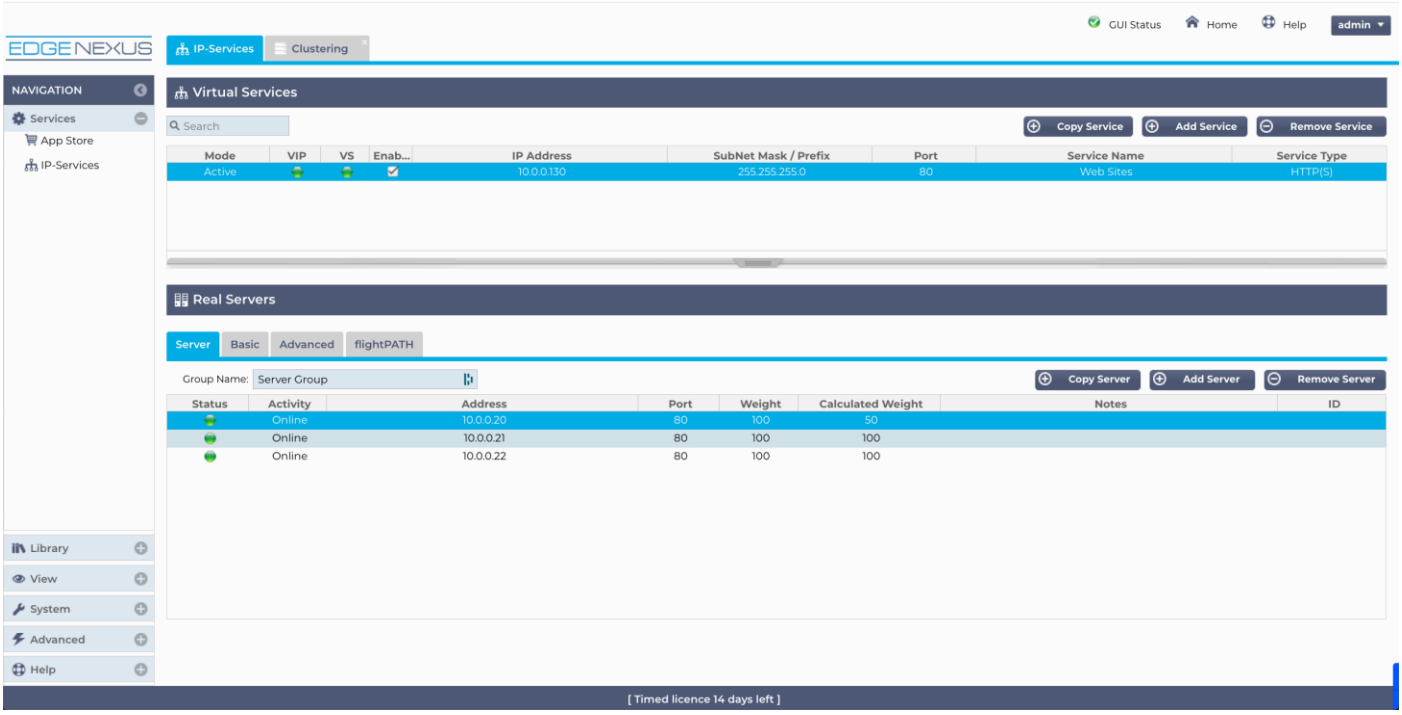
Verwendung eines externen Authentifizierungsdienstes

Wenn Sie einen externen Authentifizierungsdienst verwenden möchten, können Sie dies tun, indem Sie einen Authentifizierungsserver und einen Authentifizierungsdienst konfigurieren.

Informationen dazu finden Sie unterAuthentifizierung undAuthentifizierungsdienst

Das Haupt-Dashboard

Die folgende Abbildung zeigt, wie das Haupt-Dashboard oder die "Startseite" der ADC aussieht. Gelegentlich werden wir einige Änderungen zur Verbesserung vornehmen, aber alle Funktionen werden beibehalten.



Der Navigationsbereich auf der linken Seite ermöglicht Ihnen die Navigation durch die verschiedenen Funktionsbereiche des ADCs. Standardmäßig ist der Bereich Dienste ausgewählt und der Unterbereich IP-Dienste geöffnet, was durch die Registerkarte oberhalb des Bereichs Virtuelle Dienste angezeigt wird. Diese Registerkarte ist fest und wird immer angezeigt.

Wenn Sie auf einen Abschnitt in der Navigation klicken, wird dieser Abschnitt erweitert und sein Inhalt angezeigt. Wenn Sie auf eine Option innerhalb eines Abschnitts klicken, wird der Inhalt des Abschnitts auf der rechten Seite geöffnet, und oben wird eine Registerkarte eingeblendet, die einen schnellen Wechsel ermöglicht.

Die verschiedenen Navigationsbereiche werden in den folgenden Kapiteln ausführlich erläutert.

Dienstleistungen

IP-Dienste

Im Abschnitt 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.

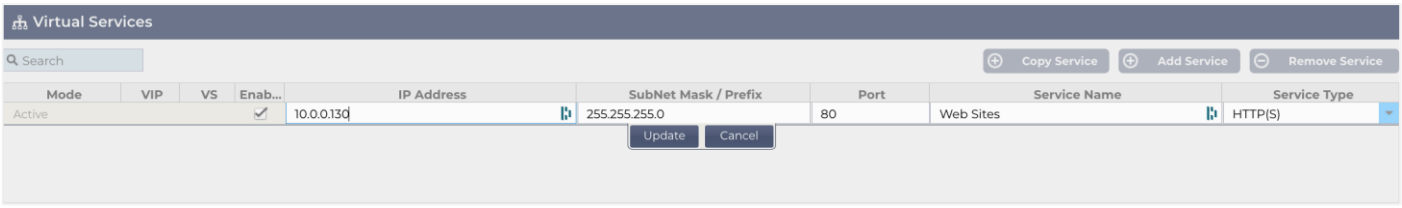
Virtuelle Dienste

Ein virtueller Dienst kombiniert eine virtuelle IP (VIP) und einen TCP/UDP-Port, auf den der ADC hört. Der an der virtuellen IP ankommende Verkehr wird an einen der mit diesem Dienst verbundenen realen Server weitergeleitet. Die virtuelle IP-Adresse kann nicht mit der Verwaltungsadresse des ADC identisch sein, d. h. eth0, eth1 usw...

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

Erstellen eines neuen virtuellen Dienstes unter Verwendung eines neuen VIP

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



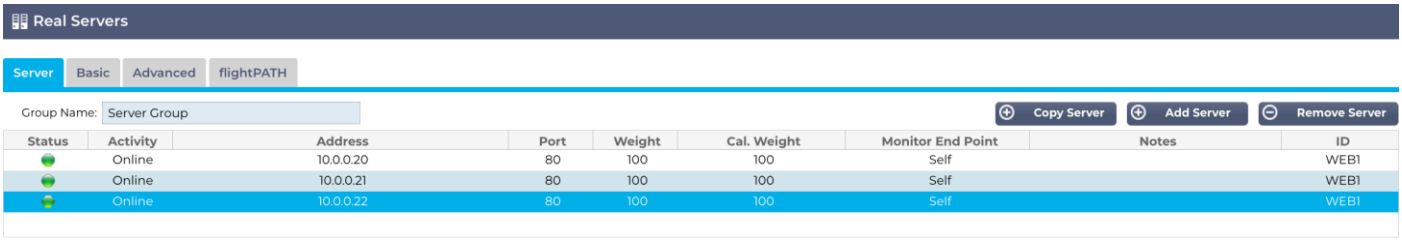
Sie gelangen dann in den Modus "**Zeile bearbeiten"**.

- Füllen Sie die vier markierten Felder aus, um fortzufahren, und klicken Sie dann auf die Schaltfläche Aktualisieren.

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

Feld	Beschreibung
IP-Adresse	Geben Sie eine neue virtuelle IP-Adresse ein, die als Zieleinstiegspunkt für den Zugriff auf den Realserver dienen soll. Diese IP-Adresse ist der Punkt, an dem Benutzer oder Anwendungen auf die Anwendung mit Lastausgleich zugreifen.
Teilnetzmaske/Präfix	Dieses Feld dient der Angabe der Subnetzmaske für das Netz, in dem sich die 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 Name des Dienstes ist eine textliche Darstellung des Zwecks des VIPs. Er ist optional, aber wir empfehlen Ihnen, ihn aus Gründen der Klarheit anzugeben. Beachten Sie, dass dieses Feld bei der Verwendung von GSLB für andere spezifische Zwecke verwendet wird.
Art der Dienstleistung	Es gibt viele verschiedene Diensttypen, die Sie auswählen können. Layer-4-Diensttypen können die flightPATH-Technologie nicht nutzen.

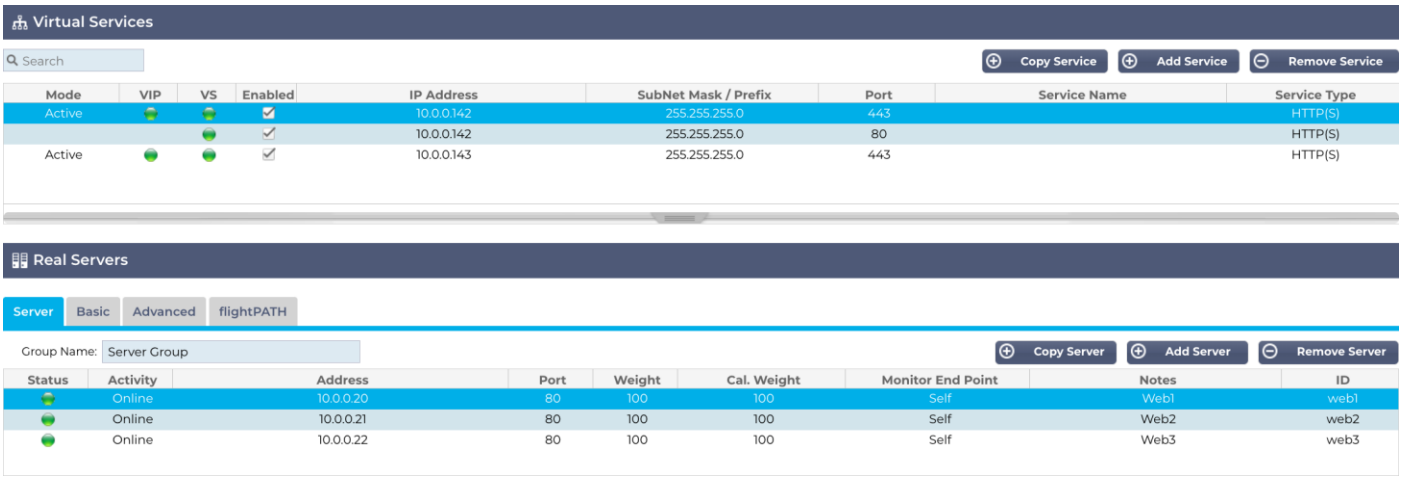
Sie können nun auf die Schaltfläche Aktualisieren klicken, um diesen Abschnitt zu speichern und automatisch zum unten beschriebenen Abschnitt Real Server zu wechseln:



Feld	Beschreibung
Tätigkeit	Über das Feld Aktivität kann der Status des realen Servers mit Lastausgleich 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 davon betroffen sind. Standby - Der Server wurde in einen Standby-Zustand versetzt
IP-Adresse	Dieser Wert ist die IP-Adresse des Real-Servers. Sie muss genau sein und sollte keine DHCP-Adresse sein.
Hafen	Der Ziel-Port des Zugriffs auf dem Real-Server. Bei Verwendung eines Reverse-Proxys kann dies ein anderer Port sein als der auf dem VIP angegebene Eingangs-Port.
Gewichtung	Diese Einstellung wird normalerweise automatisch von der OEZA konfiguriert. Sie können dies ändern, wenn Sie die Prioritätsgewichtung ändern möchten.
Kal. Gewicht	Wenn Sie die Gewichtung auf dem Standardwert belassen, berechnet die OEZA automatisch eine Gewichtung auf der Grundlage der Antwortzeiten.
Endpunkt überwachen	Der Standardwert hierfür ist "Selbst". Sie können diesen Wert jedoch in einen Port-Wert oder eine IP-Adresse:Port ändern. Das Feld wird verwendet, um einen anderen Endpunkt zu überwachen und zu bestimmen, ob der Verkehr an den virtuellen Dienst weitergeleitet werden soll. SieheSo verwenden Sie Monitor End Point .

- 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 ausgelastet.

Beispiel für einen abgeschlossenen virtuellen Dienst

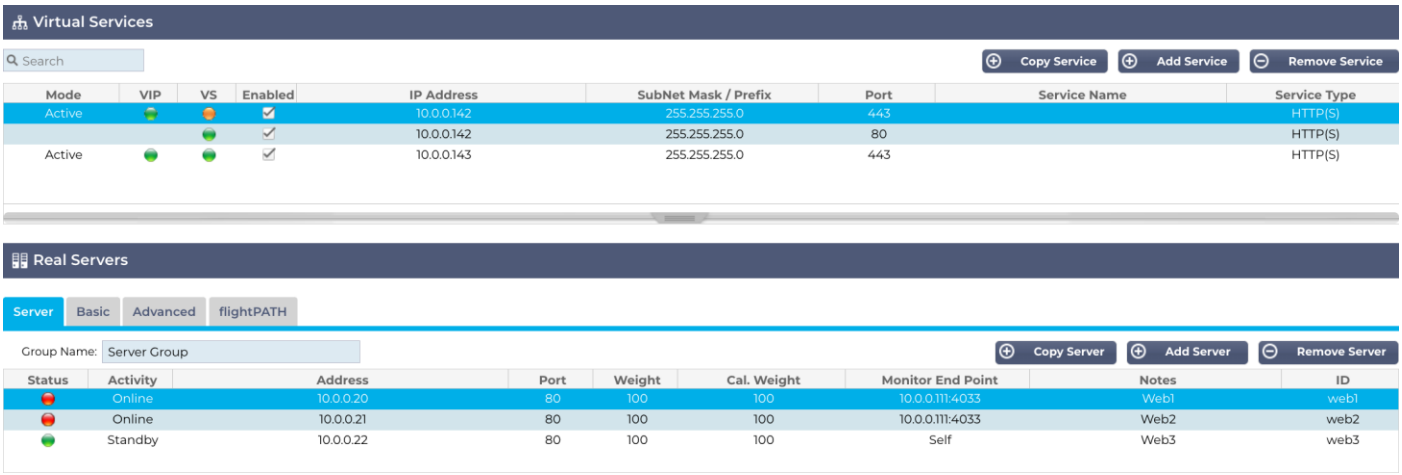


So verwenden Sie Monitor End Point

Beispiel 1

Nehmen wir als Beispiel eine Infrastruktur mit zwei lastverteilten Webservern, die eine Webanwendung für den Endbenutzer bereitstellen. Die Webanwendung ist mit einem Datenbankserver im Backend verbunden. Der Zugriff auf den Datenbankserver fällt aus, aber die Webanwendungsserver bleiben in Betrieb. Die Benutzer versuchen, die Webanwendung zu nutzen, und erhalten Fehler.

Die Lösung ist die Verwendung von Monitor End Point.



- Das Beispiel zeigt zwei Webserver, 10.0.0.20 und 10.0.0.21, zusammen mit einem dritten Webserver 10.0.0.22. Der Server 10.0.0.22 wurde in einen Standby-Modus versetzt.
- Die beiden aktiven Webserver wurden mit dem Überwachungsendpunkt 10.0.0.111:4033 konfiguriert, der die IP-Adresse und den Port der Datenbankserververbindung darstellt.
- Sollte die Verbindung zum Datenbankserver unterbrochen werden, werden die beiden aktiven Server in einen Offline-Modus versetzt, und der Standby-Server geht online und zeigt eine Webseite an, die den Kunden darüber informiert, dass die Systeme gewartet werden.

Beispiel 2

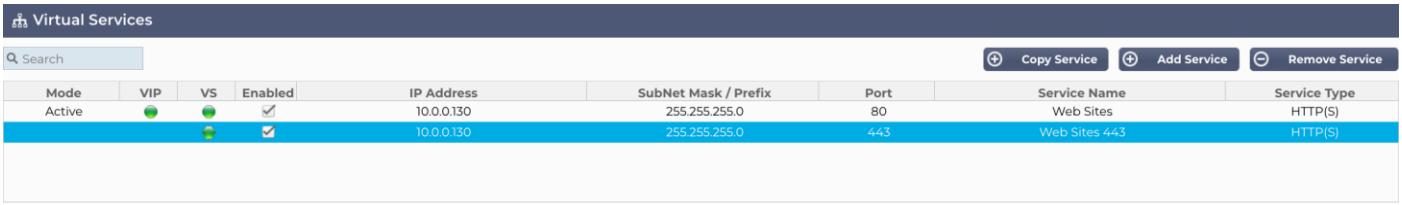
Ein weiteres Beispiel für die Verwendung von Monitor End Point ist die Lastverteilung von Servern mit UDP-Protokoll, z. B. bei Always-On-VPN. Wie Sie vielleicht wissen, werden UDP-Ports nicht zuverlässig überwacht, so dass es notwendig ist, einen TCP-Port zu überwachen.

Mit Monitor End Point können wir genau das tun. Der Hauptport, der von den Always-on-VPN-Servern verwendet wird, ist 53/udp, aber Sie wollen beispielsweise 8433/tcp überwachen. In einem solchen Fall müssen Sie nur den Portwert in das Feld Monitor Endpunkt eingeben.

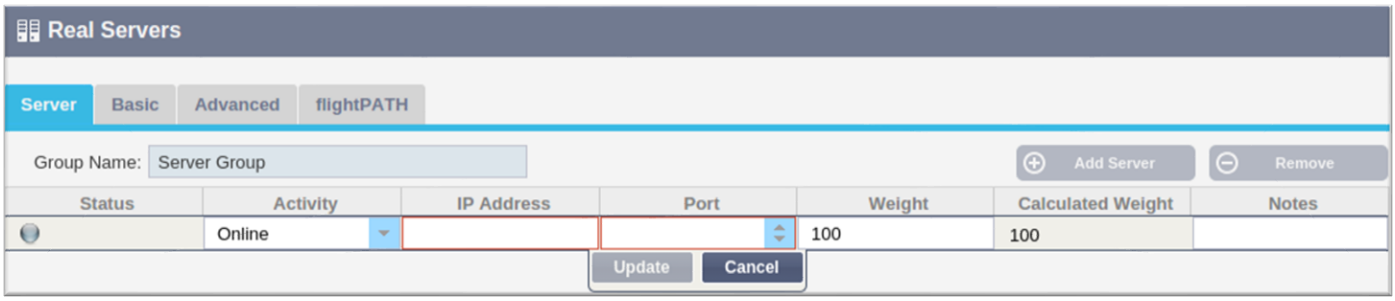
Virtuelle Teildienste erstellen

Sie können auch subvirtuelle Dienste einrichten, wenn Sie einen Lastausgleich über verschiedene Ports auf demselben VIP vornehmen müssen. Wenn Sie beispielsweise Server haben, auf die über dieselbe virtuelle IP auf den Ports 80, 8088 und 443 zugegriffen wird, müssen Sie subvirtuelle Dienste erstellen, um dies zu ermöglichen.

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



- Die IP-Adresse und die Subnetzmaske werden automatisch übernommen.
- Geben Sie die Portnummer für Ihren Dienst ein.
- Geben Sie einen optionalen Dienstnamen ein
- Wählen Sie einen Diensttyp.
- Sie können nun auf die Schaltfläche Aktualisieren klicken, um diesen Abschnitt zu speichern und automatisch zum folgenden Abschnitt Real Server zu wechseln



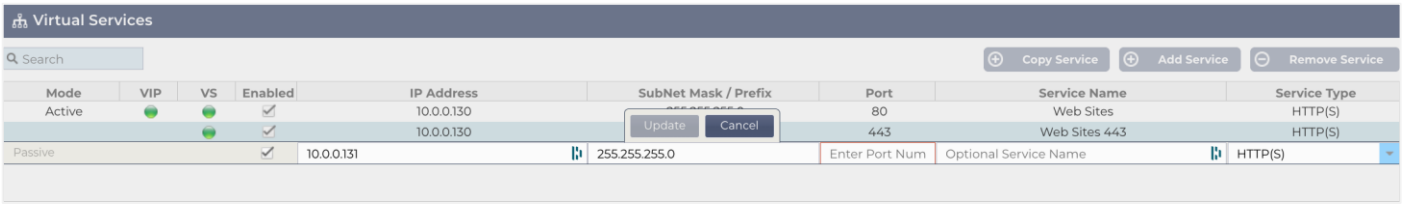
- Belassen Sie die Option "Aktivität" auf "Online" - das bedeutet, dass der Server einen Lastausgleich erhält, wenn er die standardmäßige Zustandsüberwachung von TCP Connect besteht. Diese Einstellung kann bei Bedarf später geändert werden.
- Geben Sie eine IP-Adresse für den Real-Server ein
- Geben Sie eine Portnummer für den Realserver ein
- Geben Sie im Feld Notizen einen optionalen Namen für den Real Server ein. Denken Sie daran, dass dieses Notizfeld für andere, spezifische Zwecke verwendet wird, z. B. in flightPATH-Variablen usw.
- Klicken Sie auf Aktualisieren, um Ihre Änderungen zu speichern.
- Die Statusanzeige leuchtet zuerst grau und dann grün, wenn der Real Server Monitor erfolgreich ist. Sie leuchtet rot, wenn der Real Server Monitor fehlschlägt.
- Ein Server, dessen Statusleuchte rot leuchtet, wird nicht ausgelastet.

Ändern der IP-Adresse eines virtuellen Dienstes

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

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

- Klicken Sie auf das IP-Adressfeld für diesen Dienst, um es in einen bearbeitbaren Status zu versetzen.



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

Hinweis: Wenn Sie die IP-Adresse eines virtuellen Dienstes ändern, ändert sich die IP-Adresse aller mit dem VIP verbundenen Dienste.

Erstellen eines neuen virtuellen Dienstes mit Copy Service

- Mit der Schaltfläche Dienst kopieren wird ein kompletter Dienst kopiert, 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 wird mit dem blinkenden Cursor in der Spalte IP-Adresse angezeigt.
- 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

Denken Sie daran, jede Registerkarte zu bearbeiten, wenn Sie eine Einstellung ändern, z. B. eine Lastausgleichsrichtlinie oder den Real Server Monitor, oder wenn Sie eine flightPATH-Regel entfernen.

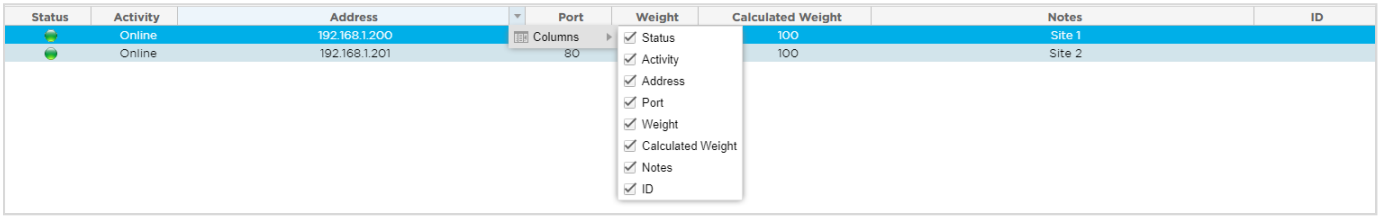
Filtern der angezeigten Daten

Suche nach einem bestimmten Begriff

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

Auswahl der Sichtbarkeit von Spalten

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



- Bewegen Sie die Maus über eine der Spalten
- Auf der rechten Seite der Spalte wird ein kleiner Pfeil angezeigt
- Durch Anklicken der Kontrollkästchen wählen Sie die Spalten aus, die Sie im Dashboard sehen möchten.

Die Säulen der virtuellen Dienste verstehen

Primär/Modus

Die Spalte Modus zeigt die für das aktuelle VIP ausgewählte Hochverfügbarkeitsrolle an. Informationen zu den Modi finden Sie unter System > Clustering>Rollen.

Option	Beschreibung

Aktiv	Im Clustermodus lautet der Wert dieses Feldes Aktiv. Wenn Sie ein HA-Paar von ADC-Appliances in Ihrem Rechenzentrum haben, wird eine davon als aktiv und die andere als passiv angezeigt. Wenn die aktuelle Appliance
Passiv	Wenn der ADC als sekundäres Mitglied eines Clusters fungiert, wird in der Spalte Modus "Passiv" angezeigt.
Handbuch	Die manuelle Rolle ermöglicht es dem ADC-Paar, im Aktiv-Aktiv-Modus für verschiedene virtuelle IP-Adressen zu arbeiten. In solchen Fällen enthält die Spalte "Primary" ein Kästchen neben jeder einzelnen virtuellen IP, das für "Active" ausgewählt oder für "Passive" nicht angekreuzt werden kann.
Eigenständig	Der ADC agiert als eigenständiges Gerät und befindet sich nicht im Hochverfügbarkeitsmodus. In der Spalte "Primär" wird daher "Stand-alone" angezeigt.

VIP

In dieser Spalte finden Sie visuelle Rückmeldungen zum 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 darauf zurückzuführen sein, dass ein Real Server eine Zustandsüberprüfung nicht bestanden hat oder manuell auf Offline gesetzt wurde. Der Datenverkehr fließt weiter, allerdings mit reduzierter Real Server Kapazität.
●	Offline. Inhaltsserver sind unerreichbar oder keine Inhaltsserver aktiviert
●	Status der Suche
●	Nicht lizenziert oder lizenzierte virtuelle IPs überschritten

Aktiviert

Die Standardeinstellung für diese Option ist Aktiviert, und das Kontrollkästchen ist angekreuzt. Sie können den virtuellen Dienst deaktivieren, indem Sie auf die Zeile doppelklicken, das Kontrollkästchen deaktivieren und dann auf die Schaltfläche Aktualisieren klicken.

IP-Adresse

Geben 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"

Teilnetzmaske/Präfix

Geben Sie Ihre Subnetzmaske in dezimaler Punktschreibweise ein. Beispiel "255.255.255.0". Sie können auch den Subnetzwert verwenden, z. B. /24, oder für IPv6 Ihr Präfix hinzufügen. Weitere Informationen über IPv6 finden Sie unter **HTTPS://DE.WIKIPEDIA.ORG/WIKI/IPV6_ADDRESS**

Hafen

Fügen Sie die Portnummer hinzu, die mit Ihrem Dienst verbunden ist. Der Port kann eine TCP- oder UDP-Portnummer sein. Beispiel TCP "80" für Webverkehr und TCP "443" für gesicherten Webverkehr. Sie können auch einen Wertebereich angeben, z. B. 80-87.

Derzeit ist es nicht möglich, durch Komma getrennte Werte zu verwenden, um nicht zusammenhängende Anschlusswerte anzugeben.

Dienst Name

Geben Sie einen freundlichen Namen ein, um Ihren Dienst zu identifizieren. Beispiel: "Production Web Servers". Dieses Feld wird auch bei der Verwendung von GSLB verwendet.

Art der Dienstleistung

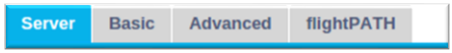
Bitte beachten Sie, dass bei allen "Layer 4"-Diensttypen die ADC nicht mit dem Datenstrom interagiert oder ihn modifiziert, so dass flightPATH bei Layer 4-Diensttypen nicht verfügbar ist. Layer 4-Dienste führen lediglich einen Lastausgleich des Datenverkehrs gemäß der Lastausgleichsrichtlinie durch:

Art der Dienstleistung	Anschluss/Protokoll	Dienstschicht	Kommentar
Schicht 4 TCP	Jeder TCP-Anschluss	Schicht 4	Die 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 ändert die ADC keine Informationen im Datenstrom und führt einen Standard-Lastausgleich des Datenverkehrs gemäß der Lastausgleichsrichtlinie durch.
Schicht 4 TCP/UDP	Jeder TCP- oder UDP-Port	Schicht 4	Es ist ideal, wenn Ihr Dienst ein primäres Protokoll wie UDP hat, aber auf TCP zurückgreift. Die ADC ändert keine Informationen im Datenstrom und führt den Standard-Lastausgleich des Datenverkehrs gemäß der Lastausgleichsrichtlinie durch
DNS	TCP/UDP	Schicht 4	Wird zum Lastausgleich von DNS-Servern verwendet.
HTTP(S)	HTTP- oder HTTPS-Protokoll	Schicht 7	Die ADC kann den Datenstrom mit flightPATH interagieren, manipulieren und verändern.
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 und 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

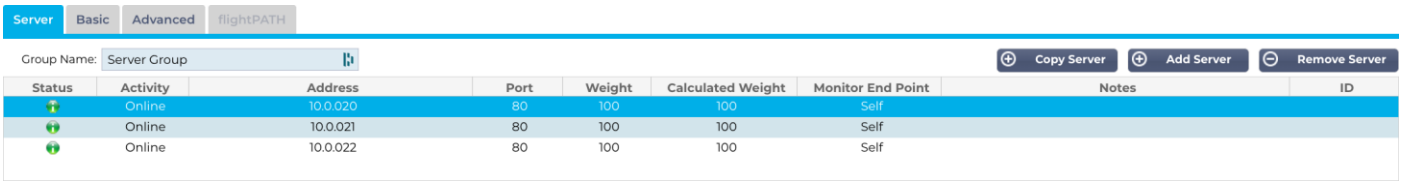
Echte Server

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



Server

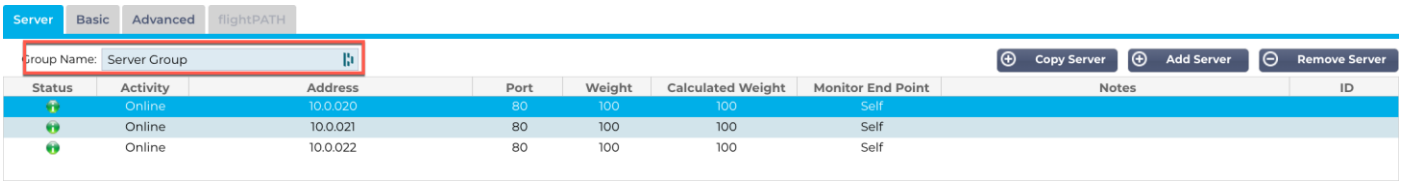
Die Registerkarte Server enthält die Definitionen der realen Backend-Server, die mit dem derzeit ausgewählten virtuellen Dienst gekoppelt sind. Sie müssen mindestens einen Server zum Abschnitt Reale Server hinzufügen.



Server hinzufügen

- Wählen Sie das entsprechende VIP, das Sie zuvor definiert haben.
- Klicken Sie auf Server hinzufügen
- Es erscheint eine neue Zeile, in der der Cursor in der Spalte IP-Adresse blinkt
- Geben Sie die IPv4-Adresse Ihres Servers in Dezimalpunktschreibweise 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 dieselbe sein wie die Portnummer des virtuellen Dienstes oder eine andere Portnummer für die Reverse-Proxy-Konnektivität. Der ADC wird automatisch auf diese Nummer umgestellt.
- Wechseln Sie zum Abschnitt Notizen, um alle relevanten Details für den Server einzugeben. Beispiel: "IIS Web Server 1"

Name der Gruppe



Wenn Sie die Server hinzugefügt haben, die das Load-Balanced-Set bilden, können Sie auch einen Gruppennamen hinzufügen. Sobald Sie dieses Feld bearbeitet haben, wird der Inhalt gespeichert, ohne dass Sie auf die Schaltfläche Aktualisieren klicken müssen.

Real Server Status Lights

Den Status eines Real-Servers erkennen Sie an der hellen Farbe in der Spalte Status. Siehe unten:

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

Tätigkeit

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

Option	Beschreibung
Online	Alle Real Server, die online zugewiesen sind, erhalten den Datenverkehr gemäß der Lastausgleichsrichtlinie, die auf der Registerkarte Basic eingestellt ist.
Abfluss	Alle Real Server, die als Drain zugewiesen sind, bedienen weiterhin bestehende Verbindungen, nehmen aber keine neuen Verbindungen an. Die Statusanzeige blinkt grün/blau, solange der Abfluss läuft. Sobald die bestehenden Verbindungen auf natürliche Weise geschlossen wurden, gehen die Real Server offline und die Statusanzeige leuchtet dauerhaft blau. Sie können diese Verbindungen auch anzeigen, indem Sie zum Abschnitt Navigation > Monitor > Status navigieren. Das Entleerungsverhalten kann auf der Registerkarte "Erweiterte Einstellungen" geändert werden.
Offline	Alle Real Server, die auf Offline gesetzt sind, werden sofort offline genommen und erhalten keinen Datenverkehr.
Bereitschaft	Alle Real-Server, die als Standby-Server eingestellt sind, bleiben offline, bis **ALLE** Server der Online-Gruppe ihre Server Health Monitor-Prüfungen nicht mehr bestehen. In diesem Fall wird der Verkehr gemäß der Lastausgleichsrichtlinie von der Standby-Gruppe empfangen. 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, die der Real-Server für den Dienst überwacht. Beispiel "80" für Webverkehr.

Gewicht

Diese Spalte wird bearbeitbar, wenn eine entsprechende Lastausgleichsrichtlinie festgelegt wurde.

Die Standardgewichtung für einen Realserver 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

Nehmen wir an, die Lastausgleichsrichtlinie ist auf "Least Connections" eingestellt, und es gibt insgesamt 200 Clientverbindungen;

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

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

Wenn wir davon ausgehen, dass bei der Lastausgleichsstrategie Schnellste die kürzeste Zeit für das ERHALTEN einer Antwort verwendet wird, ändert die Anpassung der Gewichte die Tendenz ähnlich wie bei Geringste Verbindungen.

Berechnetes Gewicht

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

Endpunkt überwachen

Mit dieser Funktion können Sie bestimmte Endpunkte angeben, die überwacht werden sollen, und so den Zustandsstatus des Eintrags für den Realserver bestimmen. Sie können die Funktion auf dem Standardwert "Selbst" belassen, so dass sie sich auf die für den virtuellen Dienst angegebenen Realserver-Monitore verlässt. Alternativ können Sie auch eine IP-Adresse, einen Port oder IP-Adresse:Port angeben, so dass Sie einen anderen Endpunkt in Ihrem Netzwerk überwachen können. Dies könnte beispielsweise ein Datenbankserver sein, von dem die Dienste abhängig sind.

Anmerkungen

Geben Sie in das Feld "Anmerkungen" alle besonderen Hinweise ein, die für die Beschreibung des definierten Eintrags hilfreich sind. Beispiel: "IIS Server1 - London DC". Dieses Feld kann für spezielle Anforderungen innerhalb von flightPATH-Regeln und GSLB verwendet werden.

ID

Diese Einstellung hat eine Reihe von Verwendungsmöglichkeiten.

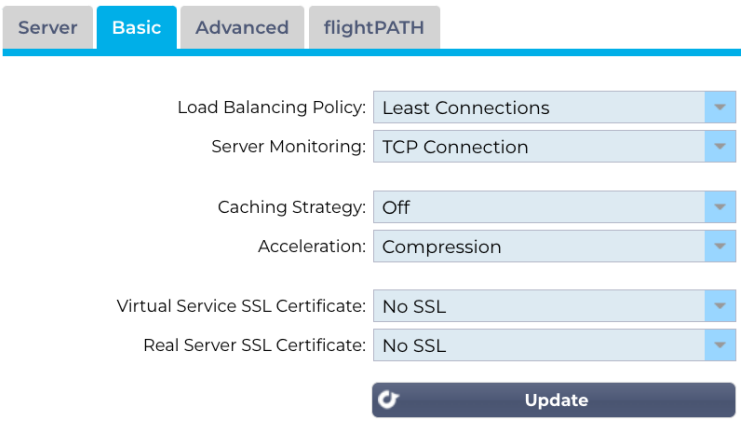
Persistenz

Der Wert kann in Verbindung mit der Cookie-ID-basierten Persistenzmethode verwendet werden. Diese Methode ähnelt der sitzungsbasierten Persistenz von PHP, verwendet aber eine neue Technik namens Cookie ID Based und Cookie RegEx h=[^;]+. Die auf der Cookie-ID basierende Persistenzmethode verwendet den Wert im ID-Feld, um ein Cookie zu erzeugen.

flightPATH Verwendung

Sie können den Wert in diesem Feld auch zur Lenkung des Verkehrs usw. verwenden.

Grundlegend



Lastausgleichsrichtlinie

Die Dropdown-Liste zeigt Ihnen die derzeit unterstützten Lastausgleichsrichtlinien an, die Sie verwenden können. Nachstehend finden Sie eine Liste der Lastausgleichsrichtlinien mit einer Erläuterung.

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

Option	Beschreibung
Geringste Verbindungen	Der Load Balancer verfolgt die Anzahl der aktuellen Verbindungen zu jedem Real Server. Der Real Server mit der geringsten Anzahl von Verbindungen erhält die nächste neue Anfrage.
Schnellste	Die Richtlinie für den schnellsten Lastausgleich berechnet automatisch die über die Zeit geglättete Antwortzeit für alle Anfragen pro Server. Die Spalte Berechnetes Gewicht enthält den automatisch berechneten Wert. Eine manuelle Eingabe ist nur möglich, wenn diese Lastausgleichsrichtlinie verwendet wird.
Dauerhafter Cookie	Schicht 7 Sitzungsaffinität/Persistenz 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.
Runde Robin	Round Robin wird häufig in Firewalls und einfachen Lastverteilern verwendet und ist die einfachste Methode. Jeder Realserver erhält nacheinander eine neue Anfrage. Diese Methode ist nur dann geeignet, wenn Sie die Last gleichmäßig auf die Server verteilen müssen, z. B. bei Look-up-Webservern. Wenn Sie jedoch

	einen Lastausgleich auf der Grundlage der Anwendungslast oder der Serverlast vornehmen oder sogar sicherstellen müssen, dass Sie denselben Server für die Sitzung verwenden, ist die Round-Robin-Methode ungeeignet.
IP-Grenze	Layer 3 Session Affinity/Persistence Cookie. 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, so dass die Belastung nicht gleichmäßig wäre. Bei HTTP wird die Header-Information (X-Forwarder-For) verwendet, wenn sie vorhanden ist, um mit Proxies fertig zu werden.
IP-Liste basiert	Die Verbindung zum Real Server wird über "Least connections" initiiert, wobei die Sitzungsaffinität auf der Grundlage der IP-Adresse des Clients erreicht wird. Standardmäßig wird eine Liste für 2 Stunden geführt, dies kann jedoch mit einem jetPACK geändert werden.
Gemeinsame IP-Liste basierend	Dieser Diensttyp ist nur verfügbar, wenn der Konnektivitätsmodus auf Direkte Serverrückkehr eingestellt ist. Er wurde in erster Linie zur Unterstützung des VMware-Lastausgleichs hinzugefügt.
Dauerhafter Cookie	Schicht 7 Sitzungsaffinität/Persistenz 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.
Klassisches ASP-Sitzungs-Cookie	Active Server Pages (ASP) ist eine serverseitige Technologie von Microsoft. Wenn diese Option aktiviert ist, behält die ADC die Sitzung auf demselben Server bei, wenn ein ASP-Cookie erkannt und in der Liste der bekannten Cookies gefunden wird. Wenn ein neues ASP-Cookie erkannt wird, erfolgt ein Lastausgleich nach dem Least-Connections-Algorithmus.
ASP.NET-Sitzungs-Cookie	Dieser Modus gilt für **ASP.net.** Wenn dieser Modus ausgewählt ist, behält die ADC die Sitzungspersistenz auf demselben Server bei, wenn ein ASP.NET-Cookie erkannt und in der Liste der bekannten Cookies gefunden wird. Wenn ein neues ASP-Cookie erkannt wird, erfolgt ein Lastausgleich nach dem Algorithmus der kleinsten Verbindungen.
JSP-Sitzungs-Cookie	Java Server Pages (JSP) ist eine serverseitige Technologie von Oracle. Wenn dieser Modus ausgewählt ist, behält die ADC die Sitzungspersistenz auf demselben Server bei, wenn ein JSP-Cookie erkannt und in seiner Liste der bekannten Cookies gefunden wird. Wenn ein neues JSP-Cookie erkannt wird, erfolgt ein Lastausgleich nach dem Least-Connections-Algorithmus.
JAX-WS Sitzungs-Cookie	Java Web Services (JAX-WS) ist eine serverseitige Technologie von Oracle. Wenn dieser Modus ausgewählt ist, behält die ADC die Sitzung auf demselben Server bei, wenn ein JAX-WS-Cookie erkannt und in der Liste der bekannten Cookies gefunden wird. Bei Erkennung eines neuen JAX-WS-Cookies erfolgt ein Lastausgleich nach dem Least-Connections-Algorithmus.
PHP-Sitzungs-Cookie	Personal Home Page (PHP) ist eine serverseitige Open-Source-Technologie. Wenn dieser Modus ausgewählt ist, hält die ADC die Sitzung auf demselben Server aufrecht, wenn ein PHP-Cookie erkannt wird.
Persistenz von RDP-Cookies	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 besteht darin, dass die

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

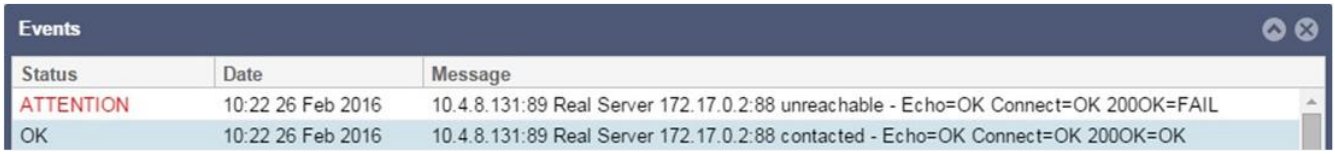
Server-Überwachung

Ihr ADC enthält mehrere vordefinierte Real Server Monitoring Methoden.

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

Es ist wichtig, den richtigen Monitor für den jeweiligen Dienst zu wählen. Wenn der Real-Server beispielsweise ein RDP-Server ist, ist ein 200OK-Monitor nicht relevant. Die Auswahl von TCP-Verbindung und 200OK macht ebenfalls keinen Sinn, da Sie eine funktionierende TCP-Verbindung benötigen, damit 200OK funktioniert. Wenn Sie sich nicht sicher sind, welchen Monitor Sie wählen sollen, ist die Standardeinstellung TCP-Verbindung ein guter Anfang

Sie können mehrere Monitore auswählen, indem Sie nacheinander auf jeden Monitor klicken, den Sie auf den Dienst anwenden möchten. Die ausgewählten Monitore werden in der Reihenfolge ausgeführt, in der Sie sie auswählen; beginnen Sie also mit den Monitoren der unteren Schichten. 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:



In der obersten Zeile können wir sehen, dass Layer 3 Ping und Layer 4 TCP Connect erfolgreich waren, aber Layer 7 200OK ist fehlgeschlagen. Diese Überwachungsergebnisse liefern genügend Informationen, um darauf hinzuweisen, dass das Routing in Ordnung ist und ein Dienst auf dem entsprechenden Port läuft, aber Website nicht korrekt auf die angeforderte Seite reagiert. Es ist nun an der Zeit, sich den Webserver und den Abschnitt Bibliothek > Realer 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. Dies ist

	ein Weg, um unzuverlässige oder veraltete Systeme zu hosten, die für den H/A-Betrieb nicht primär sind. Verwenden Sie diese Überwachungsmethode für jeden Diensttyp.
Ping/ICMP-Echo	In diesem Modus sendet der ADC eine ICMP-Echo-Anfrage an die IP-Adresse des Inhaltsservers. Wenn eine gültige Echo-Antwort empfangen wird, betrachtet die 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 kann für jeden Diensttyp verwendet werden.
TCP-Verbindung	In diesem Modus wird eine TCP-Verbindung zum Realserver hergestellt und sofort unterbrochen, ohne dass Daten gesendet werden. Wenn die Verbindung erfolgreich ist, betrachtet die ADC den Real Server als betriebsbereit. Diese Überwachungsmethode kann für jeden Diensttyp verwendet werden, wobei UDP-Dienste derzeit nicht für die Überwachung von TCP-Verbindungen geeignet sind.
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 wie in der Methode ICMP Unreachable beschrieben initialisiert. Nachdem die Verbindung initialisiert wurde, wird eine Layer-7-RDP-Verbindung angefordert. Wenn die Verbindung bestätigt wird, geht die ADC davon aus, dass der Real Server betriebsbereit ist. Diese Überwachungsmethode kann mit jedem Microsoft-Terminalserver verwendet werden.
200 OK	Bei dieser Methode wird eine TCP-Verbindung zum Real Server initialisiert. Nach erfolgreichem Verbindungsaufbau sendet die OEZA eine HTTP-Anfrage an den Realserver. Es wird auf eine HTTP-Antwort gewartet und auf den Antwortcode "200 OK" geprüft. Die OEZA betrachtet den Realserver als betriebsbereit, wenn der Antwortcode "200 OK" empfangen wird. Wenn die ADC aus irgendeinem Grund keinen "200 OK"-Antwortcode erhält, einschließlich Timeouts, Verbindungsabbrüche und andere Gründe, markiert die ADC den Real Server als nicht verfügbar. Diese Überwachungsmethode ist nur für die Verwendung mit HTTP- und beschleunigten HTTP-Diensttypen gültig. Wenn für einen HTTP-Server ein Layer-4-Diensttyp verwendet wird, kann er verwendet werden, wenn SSL auf dem Real Server nicht verwendet wird oder durch die "Content SSL"-Funktion entsprechend behandelt wird.
DICOM	Eine TCP-Verbindung zum Real-Server wird im DICOM-Modus initialisiert, und beim Verbindungsaufbau wird eine "Associate Request" von Echoscu 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 nicht erfolgreich abgeschlossen wird, gilt der Real Server aus irgendeinem Grund als ausgefallen.
Benutzerdefiniert	Jeder Monitor, der im Abschnitt Real Server Monitoring konfiguriert wurde, erscheint in der Liste.

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.

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

Option	**Beschreibung**
Vom Gastgeber	Das Caching pro Host basiert auf der Anwendung pro Hostname. Für jede Domäne/jeden Hostnamen gibt es einen eigenen Cache. Dieser Modus ist ideal für Webserver, die je nach Domäne mehrere Websites bedienen können.

Durch virtuellen Dienst	Wenn Sie diese Option wählen, ist Caching pro virtuellem Dienst möglich. Es gibt nur einen Cache für alle Domänen/Hostnamen, die den virtuellen Service durchlaufen. Diese Option ist eine spezielle Einstellung für die Verwendung mit mehreren Klonen einer einzelnen Site.

Beschleunigung

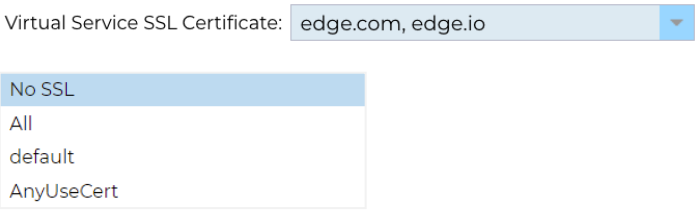
Option	**Beschreibung**
Aus	Deaktivieren Sie die Komprimierung für den virtuellen Dienst
Komprimierung	Wenn diese Option ausgewählt ist, wird die Komprimierung für den ausgewählten virtuellen Dienst aktiviert. Die ADC komprimiert den Datenstrom zum Client auf Anfrage dynamisch. Dieser Vorgang gilt nur für Objekte, die den Header content-encoding: gzip enthalten. Zu den Beispielinhalten gehören HTML, CSS oder JavaScript. Sie können auch bestimmte Inhaltstypen ausschließen, indem Sie den Abschnitt Globale Ausschlüsse verwenden.

Hinweis: Ist das Objekt cachefähig, 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 ADC)

Die Standardeinstellung ist "No SSL". Wenn Ihr Diensttyp "HTTP" ist, können Sie aus 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.

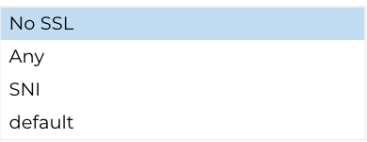
Sie können auch mehrere Zertifikate markieren, um sie auf einen Dienst anzuwenden. Durch diesen Vorgang wird die SNI-Erweiterung automatisch aktiviert, um ein Zertifikat auf der Grundlage des vom Kunden angeforderten "Domänennamens" zuzulassen.



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

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

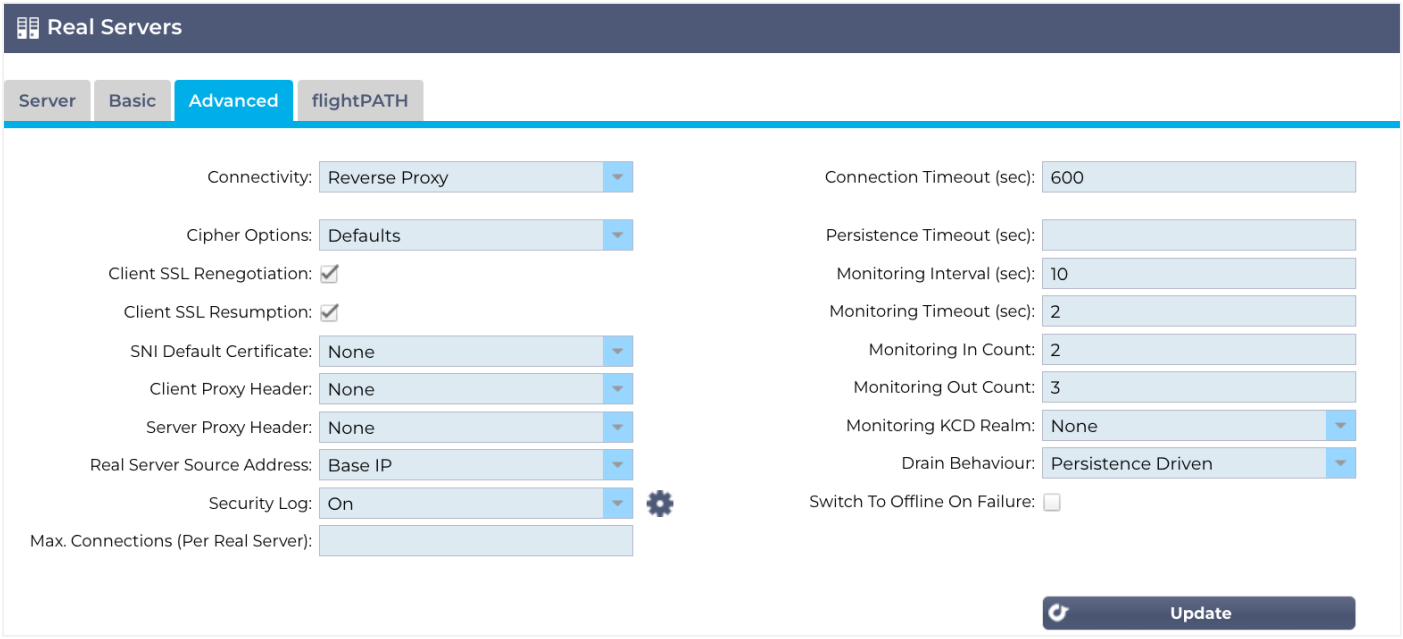
Die Standardeinstellung für diese Option ist No SSL. Wenn Ihr Server eine verschlüsselte Verbindung benötigt, muss dieser Wert etwas anderes als Kein SSL sein. Zertifikate, die erstellt oder importiert wurden, werden in dieser Liste angezeigt.



Option	**Beschreibung**

Kein SSL	Der Verkehr vom ADC zum Real Server wird nicht verschlüsselt. Die Auswahl eines Zertifikats auf der Browserseite bedeutet, dass "No SSL" auf der Client-Seite gewählt werden kann, um eine so genannte "SSL-Offload" zu ermöglichen.
Jede	Der ADC fungiert als Client und akzeptiert jedes vom Real Server vorgelegte Zertifikat. Der Datenverkehr vom ADC zum Realserver wird verschlüsselt, wenn diese Option ausgewählt ist. Verwenden Sie die Option "Beliebig", wenn auf der Seite des virtuellen Dienstes ein Zertifikat angegeben ist, um die so genannte "SSL-Überbrückung" oder "SSL-Wiederverschlüsselung" zu ermöglichen.
SNI	SNI (Server Name Indication) ist eine Erweiterung des TLS-Netzwerkprotokolls, mit der der Client zu Beginn des Handshaking-Prozesses angibt, mit welchem Hostnamen er sich zu verbinden versucht. Mit dieser Einstellung kann die ADC mehrere Zertifikate für dieselbe virtuelle IP-Adresse und denselben TCP-Port bereitstellen.
Standard	Alle selbstsignierten Zertifikate, die Sie erstellt haben, erscheinen hier.

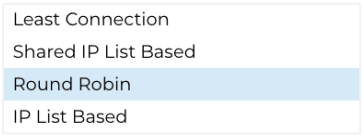
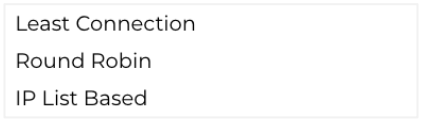
Fortgeschrittene



Konnektivität

Ihr virtueller Dienst kann mit verschiedenen Arten von Konnektivität konfiguriert werden. Bitte wählen Sie den Konnektivitätsmodus, der für den Dienst gelten soll.

Option	Beschreibung
Umgekehrter Proxy	Reverse Proxy ist der Standardwert und verwendet Komprimierung und Zwischenspeicherung, wenn er mit Layer 7 verwendet wird. Auf Layer 4 arbeitet Reverse Proxy 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 Serverrückgabe	Direct Server Return oder DSR, auch bekannt als DR - Direct Routing, ermöglicht es dem Server hinter dem Load Balancer, direkt an den Client zu antworten und dabei den ADC zu umgehen. DSR eignet sich nur für den Einsatz mit Layer 4-Lastausgleich. Daher sind Caching und Komprimierung bei dieser Option nicht verfügbar. **Dieser Modus kann nur mit den Diensttypen TCP, UDP und TCP/UDP verwendet werden.** Die Lastausgleichspersistenzrichtlinien sind außerdem auf Least Connections, Shared IP List Based, Round Robin und IP List Based beschränkt.

	 Die Verwendung von DSR erfordert auch Änderungen am Realserver, die vorgenommen werden müssen. Bitte lesen Sie den Abschnitt Änderungen am Realserver.
NAT	Standardmäßig verwendet der ADC die IP-Adresse des ADC als Quell-IP-Adresse, und die Real-Server senden dann die Antwort an den ADC zurück, um sie an den Client zu senden. Dies ist unter fast allen Umständen in Ordnung, aber es gibt Szenarien, in denen der Real Server die Quell-IP-Adresse des Clients und nicht des ADC sehen muss. Wenn der NAT-Modus angewendet wird, empfängt der ADC die eingehende Anfrage und sendet sie an den Realen Server, nachdem er die Quell-IP-Adresse wieder in die des Virtuellen Dienstes (VIP-Adresse) geändert hat. **Dieser Modus kann nur mit den folgenden Load Balancing Policies verwendet werden:** 
Gateway	Im Gateway-Modus können Sie den gesamten Datenverkehr über den ADC leiten, so dass die Real Server über den ADC an andere Netzwerke über die virtuellen ADC-Dienste oder Hardware-Schnittstellen weitergeleitet werden können. Die Verwendung des Geräts als Gateway-Gerät für Real Server ist ideal für den Betrieb im Multi-Interface-Modus. Die Lastausgleichspersistenzrichtlinien sind außerdem auf Least Connections, Shared IP List Based, Round Robin und IP List Based beschränkt.  Diese Methode erfordert, dass der Real Server sein Standardgateway auf die lokale Schnittstellenadresse des ADC (eth0, eth1 usw.) einstellt. Bitte lesen Sie den Abschnitt Real Server Änderungen. ***Bitte beachten Sie, dass der Gateway-Modus keine Ausfallsicherung in einer Cluster-Umgebung unterstützt.***

Verschlüsselungsoptionen

Chiffren bilden die Grundlage der SSL-Kryptografie und sind äußerst wichtig für eine erfolgreiche und sichere Bereitstellung von Webinhalten und -anwendungen.

Die ADC verfügt über einen integrierten Satz von Standardchiffren, die die aktuellsten und sichersten Chiffren umfassen, die für die Verwendung verfügbar sind.

Es gibt Gelegenheiten, bei denen der Benutzer die Verfügbarkeit eines bestimmten Satzes von Chiffren ankündigen möchte, und die ADC ermöglicht die Erstellung solcher Chiffren durch vom Benutzer erstellte jetPACKS. jetPACKS, die von Benutzern geschrieben wurden, können über Konfiguration > Software in die ADC importiert und dann über das Menü Chiffre-Optionen zur Auswahl bereitgestellt werden.

Die Verschlüsselungsoptionen sind spezifisch für jedes VIP und bieten hohe Flexibilität und Sicherheit.

Weitere Informationen zu Cipher Options finden Sie unter: *Chiffre*

Client SSL-Neuverhandlung

Aktivieren Sie dieses Kästchen, wenn Sie die vom Client initiierte SSL-Neuaushandlung zulassen möchten. Deaktivieren Sie die Client-SSL-Neuaushandlung, um mögliche DDOS-Angriffe auf die SSL-Schicht zu verhindern, indem Sie diese Option deaktivieren.

Client-SSL-Wiederaufnahme

Aktivieren Sie dieses Kästchen, wenn Sie SSL-Wiederaufnahme Server-Sitzungen, die dem Sitzungscache hinzugefügt wurden, aktivieren möchten. Wenn ein Client die Wiederverwendung einer Sitzung vorschlägt, versucht der Server, die Sitzung wieder zu verwenden, wenn er sie findet. Wenn die Wiederaufnahme nicht aktiviert ist, findet keine Sitzungszwischenspeicherung für den Client oder Server statt.

SNI-Standard-Zertifikat

Wenn bei einer SSL-Verbindung mit aktivierter clientseitiger SNI die angeforderte Domäne mit keinem der dem Dienst zugewiesenen Zertifikate übereinstimmt, präsentiert die ADC das SNI-Standardzertifikat. Die Standardeinstellung hierfür ist "Keine", wodurch die Verbindung bei fehlender exakter Übereinstimmung abgebrochen würde. Wählen Sie eines der installierten Zertifikate aus dem Dropdown-Menü aus, das angezeigt werden soll, wenn eine exakte SSL-Zertifikatsübereinstimmung fehlschlägt.

Das Proxy-Protokoll

Das Proxy-Protokoll wurde entwickelt, um Netzwerk-Proxys die Weiterleitung von Client-Verbindungsinformationen (wie z. B. die ursprüngliche IP-Adresse und Port-Nummer) an den empfangenden Server zu ermöglichen. Dieses Protokoll ist besonders nützlich in Szenarien, in denen die tatsächliche IP-Adresse des Endbenutzers beibehalten werden muss, während der Verkehr durch einen Load Balancer oder Reverse Proxy geleitet wird. Es hilft dabei, die ursprüngliche Client-IP-Adresse für Protokollierungs-, Statistik- oder Sicherheitszwecke beizubehalten, und verbessert die Fähigkeit, fundierte Entscheidungen auf der Grundlage der wahren Quelle des Datenverkehrs zu treffen.

Client-Proxy-Kopfzeile

Der Client-Proxy-Header bezieht sich auf einen Header, der von der ADC zur Client-Anfrage hinzugefügt wird und die ursprünglichen Verbindungsinformationen (wie die IP-Adresse und den Port des Clients) einkapselt. Dies ist von entscheidender Bedeutung in Umgebungen, in denen die ADC als Proxy fungiert und der Server die ursprünglichen Client-Details für Zwecke wie Protokollierung, Sicherheitsbewertungen und Aufrechterhaltung des kundenspezifischen Verhaltens kennen muss. Der Client Proxy Header stellt sicher, dass der Server trotz der Vermittlerrolle des ADC die ursprünglichen Verbindungsdaten des Clients genau identifizieren und mit ihnen interagieren kann.

Die Optionen umfassen:

Option	Beschreibung
Keine	Wenn kein Proxy-Header vorhanden ist oder dieser im aktuellen Diensttyp nicht unterstützt wird
entfernen	Entfernt den Proxy-Header aus dem TCP-Paket
Weiterleiten	Leitet den Proxy-Header an den Server weiter

Server-Proxy-Kopfzeile

Es gibt zwei Versionen von Server-Proxy-Headern: Version 1 und Version 2.

Option	Beschreibung
Version 1	• Textbasiertes Format, einfach zu implementieren und zu debuggen. • Liefert grundlegende Informationen über die Verbindung des Clients, einschließlich Quell-IP, Ziel-IP, Quell- und Ziel-Port. • Die Protokollzeile wird an den Anfang der TCP-Verbindung angehängt, wodurch sie für den Menschen lesbar wird, aber im Vergleich zu binären Formaten etwas weniger leistungsfähig ist.
Version 2	• Binäres Format, das für mehr Leistung und Effizienz ausgelegt ist. • Erweitert die Informationen, die über die Verbindung weitergegeben werden können, und unterstützt zusätzliche Daten wie Adressfamilie und protokollspezifische Informationen. • Bessere Kompatibilität mit modernen Netzwerkprotokollen und -funktionen, einschließlich Unterstützung für IPv6 und Transportprotokolle über TCP hinaus.

Die Optionen Client-Proxy-Header und Server-Proxy-Header sind nur für die HTTP-Diensttypen Layer 4 und Layer 7 verfügbar.

Quelladresse des realen Servers

Diese Einstellung funktioniert zusammen mit Reverse Proxy und entweder Layer 4 TCP, Layer 4 UDP oder HTTP(S)-Dienst. Die Einstellung bietet drei Optionen, aus denen Sie wählen können.

Option	Beschreibung
Basis-IP (Standard)	Verwendet die eth0- oder Basis-IP-Adresse des ADC als Quell-IP der Anfrage.
Virtuelle IP	Verwendet die virtuelle IP des Dienstes.
<IP-Adresse>	Ermöglicht es Ihnen, eine IP-Adresse anzugeben, die Teil des ADC ist. Dies kann eine andere Netzwerkschnittstelle oder ein anderes VIP sein.

Sicherheitsprotokoll

Der Standardwert "Ein" gilt für jeden Dienst und aktiviert die Protokollierung von Authentifizierungsinformationen in den W3C-Protokollen. Wenn Sie auf das Zahnradsymbol klicken, gelangen Sie zur Seite System > Protokollierung, auf der Sie die Einstellungen für die W3C-Protokollierung überprüfen können.

Max. Verbindungen

Begrenzt die Anzahl der gleichzeitigen Real Server-Verbindungen und wird pro Dienst festgelegt. Wenn Sie dies beispielsweise auf 1000 konfigurieren und zwei Real Server haben, begrenzt die ADC **jeden** Real Server auf 1000 gleichzeitige Verbindungen. Sie können auch eine Seite "Server zu beschäftigt" anzeigen lassen, sobald diese Grenze auf allen Servern erreicht ist, um den Benutzern zu helfen, zu verstehen, warum eine Nicht-Antwort oder Verzögerung aufgetreten ist. Für unbegrenzte Verbindungen lassen Sie dieses Feld leer. Was Sie hier einstellen, hängt von Ihren Systemressourcen ab.

Zeitüberschreitung der Verbindung

Der Standard-Timeout für die Verbindung beträgt 600 Sekunden oder 10 Minuten. Mit dieser Einstellung wird die Zeit angepasst, nach der die Verbindung bei fehlender Aktivität abbricht. Verringern Sie diesen Wert für kurzlebigen zustandslosen Webverkehr, der normalerweise 90 Sekunden oder weniger beträgt. Erhöhen Sie diesen Wert für zustandsabhängige Verbindungen wie RDP auf etwa 7200 Sekunden (2

Stunden) oder mehr, je nach Ihrer Infrastruktur. Das RDP-Timeout-Beispiel bedeutet, dass die Verbindungen offen bleiben, wenn ein Benutzer 2 Stunden oder weniger inaktiv ist.

Persistenz-Zeitüberschreitung

Die Persistenz-Timeout-Einstellung in Load Balancern gibt die Dauer an, für die ein Load Balancer die Sitzungsinformationen für einen Client aufrechterhält. Dadurch wird sichergestellt, dass nachfolgende Anfragen desselben Clients an denselben Backend-Server geleitet werden, was die Sitzungskonsistenz und die zustandsorientierte Kommunikation fördert. Wenn die angegebene Timeout-Periode ohne weitere Client-Aktivitäten verstreicht, werden die Sitzungsinformationen verworfen, und neue Anfragen können an einen anderen Server weitergeleitet werden.

Überwachungsintervall

Das Intervall ist die Zeit in Sekunden zwischen den Überwachungen. Das Standardintervall beträgt 1Sekunde. Während 1s für die meisten Anwendungen akzeptabel ist, kann es für andere Anwendungen oder während Tests von Vorteil sein, diesen Wert zu erhöhen.

Überwachung der Zeitüberschreitung

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

Überwachung in der Zählung

Der Standardwert für diese Einstellung ist 2. Der Wert 2 gibt an, dass der Real-Server zwei erfolgreiche Health-Monitor-Prüfungen bestehen muss, bevor er online geht. Wenn Sie diesen Wert erhöhen, erhöht sich die Wahrscheinlichkeit, dass der Server Datenverkehr verarbeiten kann, aber es dauert je nach Intervall länger, bis er in Betrieb genommen wird. Wenn Sie diesen Wert verringern, wird Ihr 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 die ADC aufhört, Datenverkehr an den Server zu senden, und dieser als ROT und unerreichbar markiert wird. Eine Erhöhung dieser Zahl führt zu einem besseren und zuverlässigeren Dienst auf Kosten der Zeit, die das ADC benötigt, um den Datenverkehr zu diesem Server zu stoppen.

Überwachung des KCD-Bereichs

Mit dieser Einstellung können Sie die Überwachung des eingeschränkten Kerberos-Delegationsbereichs aktivieren, den Sie in den Kerberos-Definitionen eingerichtet haben. Siehe Authentifizierung > Kerberos.

Abfluss-Verhalten

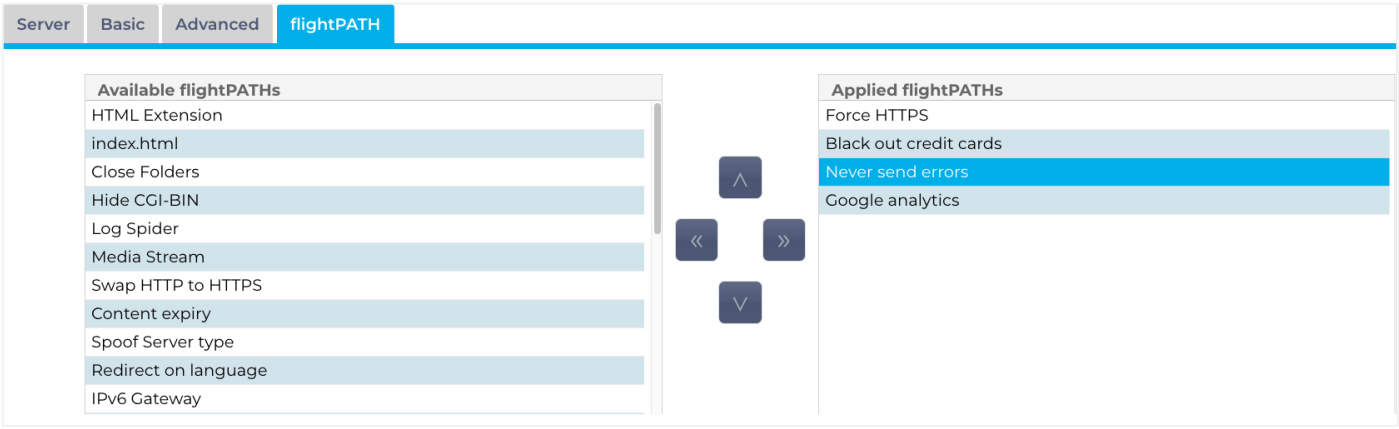
Wenn ein Real Server in den Drain-Modus versetzt wird, ist es immer besser, das Verhalten des an ihn gesendeten Datenverkehrs kontrollieren zu können. Das Menü Drain Behaviour ermöglicht die Auswahl des Verkehrsverhaltens für jeden virtuellen Dienst. Die Optionen sind:

Option	Beschreibung
Persistenzgesteuert	Dies ist die Standardauswahl. Immer wenn der Benutzer die Persistenzsitzung besucht, wird sie verlängert. Bei einer 24-stündigen Nutzung ist es möglich, dass der Abfluss nie erfolgt. Wenn die Anzahl der Verbindungen zum realen Server jedoch 0 erreicht, wird der Abfluss beendet, die Persistenzsitzungen werden gelöscht, und alle Besucher werden bei der nächsten Verbindung neu abgeglichen.
Besucher migrieren	Persistente Sitzung wird bei erneutem Verbindungsaufbau ignoriert - (altes Verhalten vor 2022) Neue TCP-Verbindungen (unabhängig davon, ob sie Teil einer bestehenden Sitzung sind oder nicht) werden immer zu einem realen Online-Server hergestellt. Wenn die Persistenzsitzung zu einem ablaufenden realen Server gehörte, wird sie überschrieben. Der virtuelle Dienst ignoriert die Persistenz neuer Verbindungen, und die Lastverteilung erfolgt auf einen neuen Server.
Sitzungen im Ruhestand	Dauerhafte Sitzungen werden nicht verlängert. Eingehende Benutzerverbindungen werden dem gewünschten Server zugewiesen, aber ihre Persistenzsitzung wird nicht verlängert. Wenn also die Zeit der Persistenzsitzung überschritten ist, werden sie als neue Verbindung behandelt und auf einen anderen Server verschoben.

Im Fehlerfall auf Offline schalten

Wenn diese Option aktiviert ist, werden die Real-Server, die ihre Gesundheitsprüfung nicht bestanden haben, offline gestellt und können nur manuell online gestellt werden.

flightPATH



flightPATH ist eine von Edgenexus entwickelte Verkehrsmanagement-Technologie, die exklusiv im ADC verfügbar ist. Im Gegensatz zu den regelbasierten Engines anderer Anbieter arbeitet flightPATH nicht über eine Befehlszeile oder eine Skripteingabekonsole. Stattdessen werden über eine grafische Benutzeroberfläche (GUI) die verschiedenen Parameter, Bedingungen und Aktionen ausgewählt, um die gewünschten Ergebnisse zu erzielen. 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 Typ des virtuellen Dienstes nicht HTTP ist.

Wie Sie in der obigen Abbildung 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.

Wenden Sie eine verfügbare Regel an, indem Sie sie von der linken 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.

Es ist wichtig zu verstehen, dass die flightPATH-Regeln in diesem Abschnitt der ADC auf einer booleschen ODER-Basis funktionieren, während die Bedingungen und Aktionen innerhalb des flightPATH-Definitionsbereichs auf einer UND-Basis funktionieren.

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

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

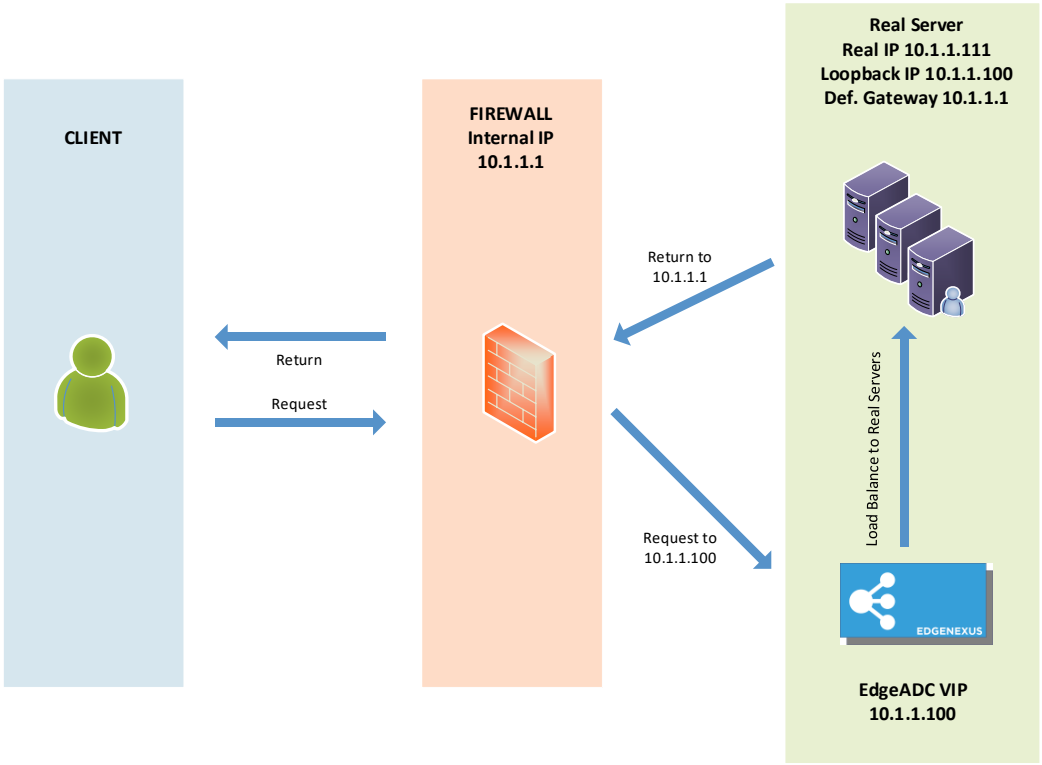
Reale Serveränderungen für die direkte Serverrückgabe

Direct Server Return oder DSR, wie es weithin bekannt ist (DR - Direct Routing in einigen Kreisen), ermöglicht es dem Server hinter dem ADC, direkt an den Client zu antworten, wobei der ADC bei der Antwort umgangen wird. DSR eignet sich nur für den Einsatz mit Layer-4-Lastausgleich. Caching und Komprimierung sind nicht verfügbar, wenn sie aktiviert sind.

Der Schicht-7-Lastausgleich mit dieser Methode funktioniert nicht, da es außer der Quell-IP keine Unterstützung für die Persistenz gibt. Der SSL/TLS-Lastausgleich mit dieser Methode ist nicht ideal, da nur die Quell-IP-Persistenz unterstützt wird.

Wie es funktioniert

- Der Client sendet eine Anfrage an den EdgeADC VIP
- Von EdgeADC empfangene Anfrage
- Weiterleitung der Anfrage an die Inhaltsserver
- Antwort wird direkt an den Client gesendet, ohne den EdgeADC zu passieren



Erforderliche Content-Server-Konfiguration

Allgemein

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

Windows

- Der Inhaltsserver muss einen Loopback oder Alias konfiguriert haben
  mit der IP-Adresse des Kanals oder VIPs
  - Die Netzwerkmetrik muss 254 sein, um eine Antwort auf ARP-Anfragen zu verhindern
  - Hinzufügen eines Loopback-Adapters in Windows Server 2012 - Klicken Sie hier

    - Hinzufügen eines Loopback-Adapters in Windows Server 2003/2008 - Klicken Sie hier
- Führen Sie in einer Eingabeaufforderung für jede Netzwerkschnittstelle, die Sie auf den Windows Real Servern konfiguriert haben, Folgendes aus

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

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

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

Linux

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

ifcfg-lo:1
GERÄT=lo:1
IPADDR=x.x.x.x
NETMASK=255.255.255.255
BROADCAST=x.x.x.x.x
ONBOOT=ja

- Bearbeiten Sie "/etc/sysctl.conf".

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

- Führen Sie "sysctl - p" aus.

Änderungen am Realserver - Gateway-Modus

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

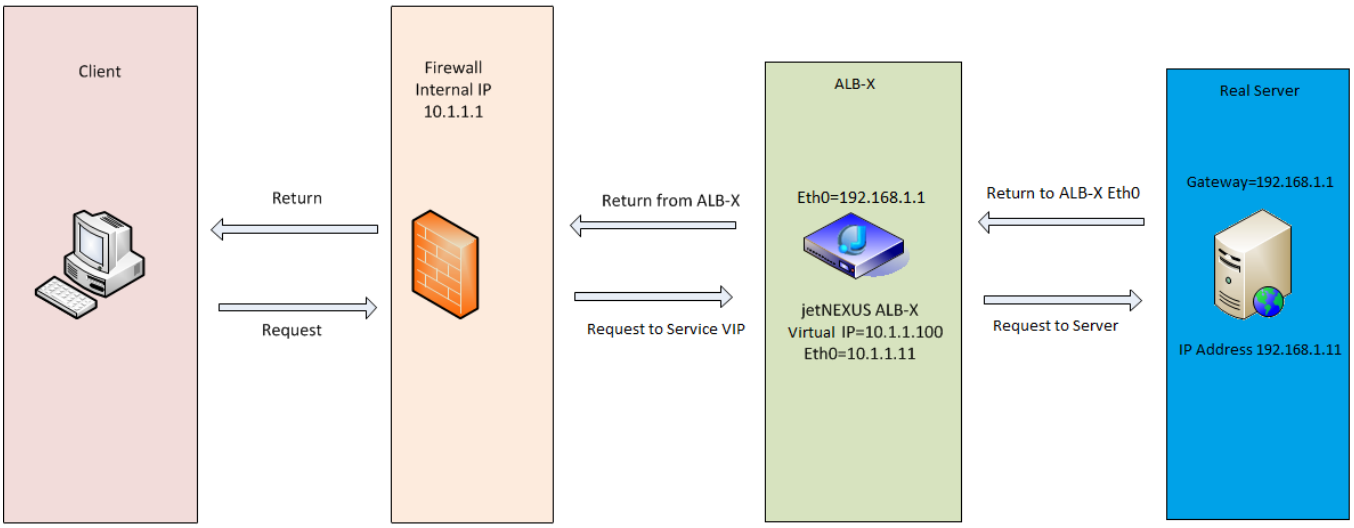
Wie es funktioniert

- Der Client sendet eine Anfrage an den EdgeADC
- Der EdgeADC erhält eine Anfrage
- Anfrage an Inhaltsserver gesendet
- Antwort an EdgeADC gesendet
- Die OEZA leitet die Antwort an den Kunden weiter

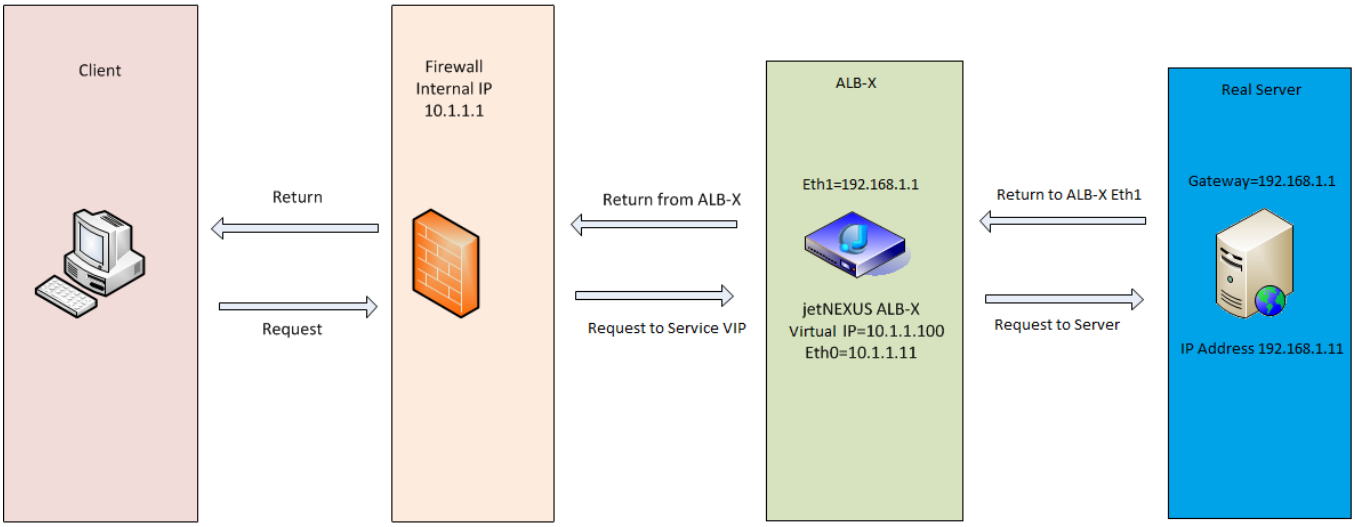
Erforderliche Content-Server-Konfiguration

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

Beispiel für einen einzelnen Arm



Beispiel eines Doppelarms

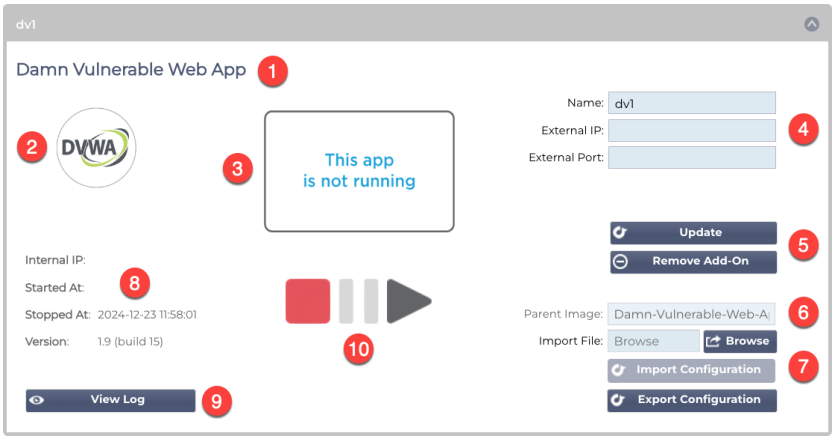


Bibliothek

Add-Ons

Add-ons sind Apps, die als Container geladen werden und in einem isolierten Modus innerhalb der ADC laufen. Beispiele für Add-ons könnten eine Anwendungsfirewall oder sogar eine Mikroinstanz des ADC selbst sein.

Eine App wird über die Seite "Apps" im Bereich "Add-Ons" bereitgestellt, wie in diesem Leitfaden beschrieben. Nach der Bereitstellung erscheint eine App wie folgt.



Wie Sie in der obigen Abbildung sehen können, sind mehrere Elemente hervorgehoben.

Artikel	Beschreibung
❶	App-Titel
❷	App-Symbol
❸	Anzeige der laufenden App. Wenn die App läuft, wird eine Miniaturansicht des Bildschirms angezeigt.
❹	Zugangsdaten: **Name**: Dies ist ein interner Name, den Sie verwenden, um im Bereich Virtuelle Dienste auf die App zu verweisen. Es ist nicht möglich, eine App über ihre IP-Adresse zu referenzieren. Nur alphanumerische Zeichen, keine Leerzeichen. **Externe IP**: Dies ist die IP-Adresse, die Sie für die App angeben müssen. Diese wird Teil Ihres Netzwerk-Subnetzes sein. **Externer Port**: Dies ist ein wichtiges Feld. Sie müssen die Ports angeben, die für den Zugriff auf die App verwendet werden sollen. Wenn der Datenverkehr von außen auf die App zugreift, müssen Sie ihn in der folgenden Schreibweise angeben: 53/tcp oder 53/udp. Darüber hinaus müssen Sie den UI-Port für die App angeben. Diese werden im Tooltip des Feldes für jede App angezeigt.
❺	Schaltfläche Aktualisieren: Wenn Sie die unter❸ angegebenen Daten eingegeben haben, klicken Sie auf diese Schaltfläche, um die Eingaben zu bestätigen und die App zu konfigurieren. Die Schaltfläche Add-On entfernen wird verwendet, um die App aus dem Bereich Apps zu entfernen. Um eine App zu entfernen, stellen Sie bitte sicher, dass alle Verweise auf die App ebenfalls entfernt werden, bevor Sie versuchen, sie zu entfernen.
❻	Parent Image ist ein informatives Feld und wird aus Sicht des Benutzers nicht verwendet.
❼	Das Importieren und Exportieren einer Konfiguration ist wichtig, um ein Backup der Einstellungen zu erhalten. Verwenden Sie dies, um die Import- und Exportfunktion auszuführen.
❽	Die Ausführungsdetails enthalten Informationen über die interne API-IP-Adresse, die Start- und Endzeit sowie die Versionsnummer der App.
❾	Mit dieser Schaltfläche können Sie das Protokoll herunterladen und anzeigen. Dies wird vor allem verwendet, wenn Sie ein Support-Ticket öffnen müssen.
❿	Die Bedienung der App erfolgt über diese Schaltflächen. Rot=Gestoppt, Gold=Pausiert und Grün=Läuft.

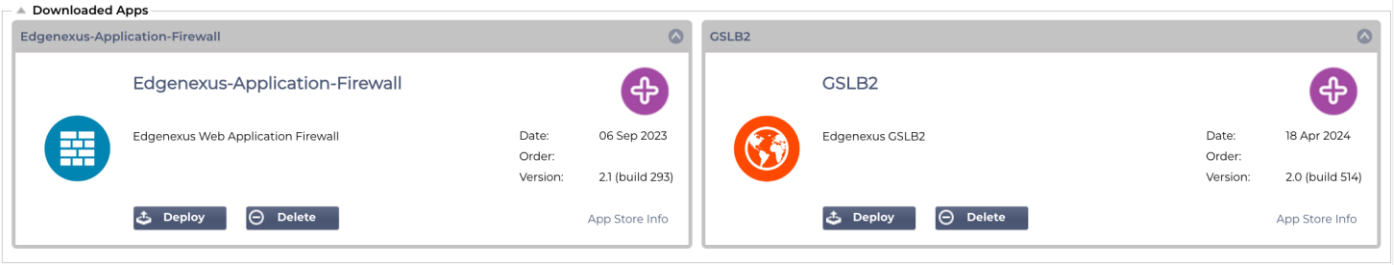
Apps

Der Abschnitt Apps hat mehrere Unterabschnitte, die die auf dem ADC verfügbaren Apps verwalten. Dies sind der Filter, heruntergeladene Apps und gekaufte Apps.

Der Filter

Mit dem Filter können Sie die Apps/Werkzeuge nach ihrem Typ filtern.

Heruntergeladene Apps

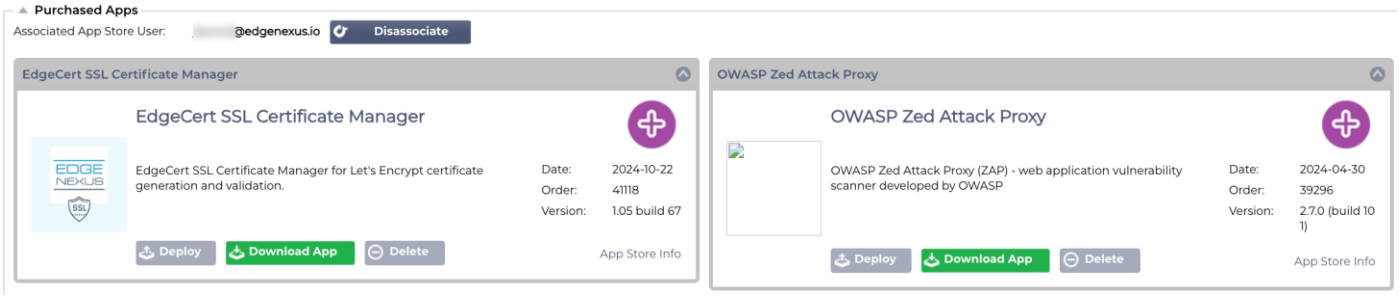


Dieser Abschnitt enthält die Apps, die auf den ADC heruntergeladen wurden. Sie können sie auf Ihren lokalen Desktop heruntergeladen und anschließend auf den ADC hochgeladen haben, oder Sie können sie über das integrierte App Store-Portal heruntergeladen haben.

Jede App ist mit zwei Schaltflächen sowie Daten ausgestattet, die ihre Versionsnummer und das Datum ihrer Veröffentlichung angeben.

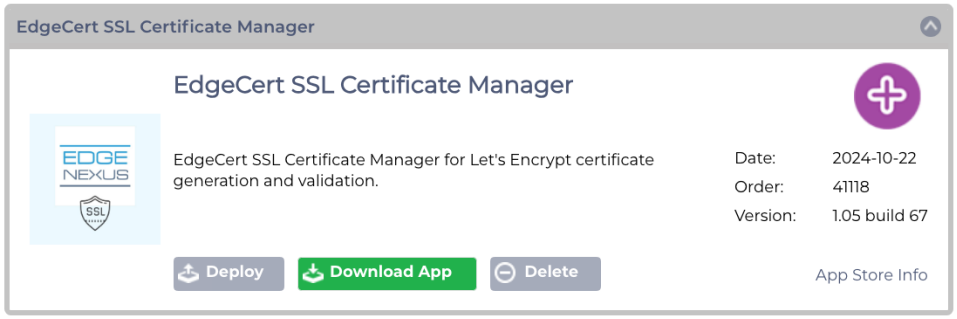
Die Schaltfläche Bereitstellen stellt die App als gesicherten Container bereit, während die Schaltfläche Löschen die App aus dem ADC löscht.

Gekaufte App



Das erste, was Sie sehen werden, ist der assoziierte App-Store-Benutzer und die dazugehörige Schaltfläche. Sie müssen sich mit Ihren App Store-Anmeldedaten anmelden, damit der ADC mit dem App Store verknüpft wird. Darunter finden Sie die mit Ihrem Konto verbundenen Apps.

Wenn Sie sich im App Store anmelden, entweder direkt oder über das eingebaute Portal, können Sie Apps kaufen. Diese werden in diesem Abschnitt angezeigt und können in den ADC hochgeladen werden, um dort bereitgestellt zu werden.



Jede App hat eine Reihe von Schaltflächen: Bereitstellen, App herunterladen und Löschen. Darüber hinaus gibt es auf der rechten Seite einen Link "App Store Info", der Sie zur entsprechenden App Store-Seite führt und Informationen über das Addon anzeigt.

Bereitstellung von

Im Abschnitt Apps innerhalb von Add-Ons werden die von Ihnen gekauften, heruntergeladenen und bereitgestellten Apps aufgeführt. Sobald die App bereitgestellt wurde, erscheint sie im Abschnitt Heruntergeladen.

App herunterladen

Die App kann im App Store heruntergeladen werden, indem Sie auf diese Schaltfläche klicken.

Löschen

Wenn Sie eine bereits heruntergeladene App löschen möchten.

Authentifizierung

Auf der Seite Bibliothek> Authentifizierung können Sie Authentifizierungsserver einrichten und Authentifizierungsregeln erstellen.

Einrichten der Authentifizierung - ein Arbeitsablauf

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

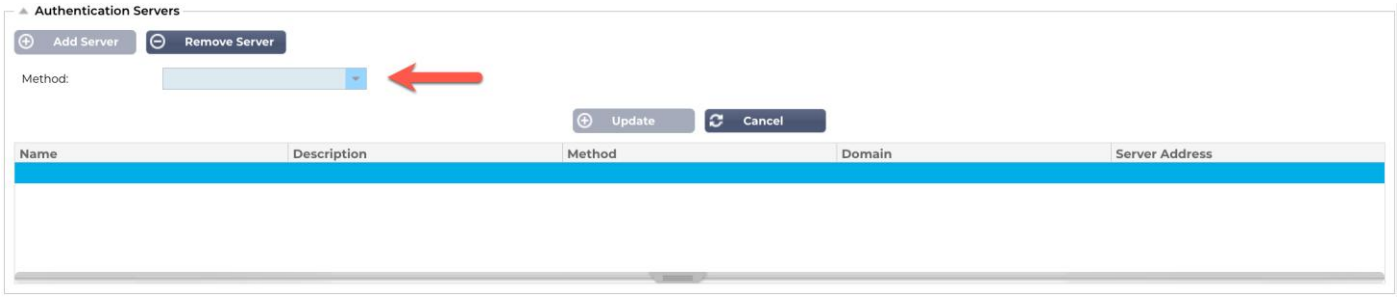
1. Erstellen Sie einen Authentifizierungsserver.
2. Erstellen Sie eine Authentifizierungsregel, die einen Authentifizierungsserver verwendet.
3. Erstellen Sie eine flightPATH-Regel, die eine Authentifizierungsregel verwendet.
4. Anwenden der flightPATH-Regel auf einen Dienst

Authentifizierungsserver

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

In einem ersten Schritt müssen Sie die gewünschte Authentifizierungsmethode auswählen.

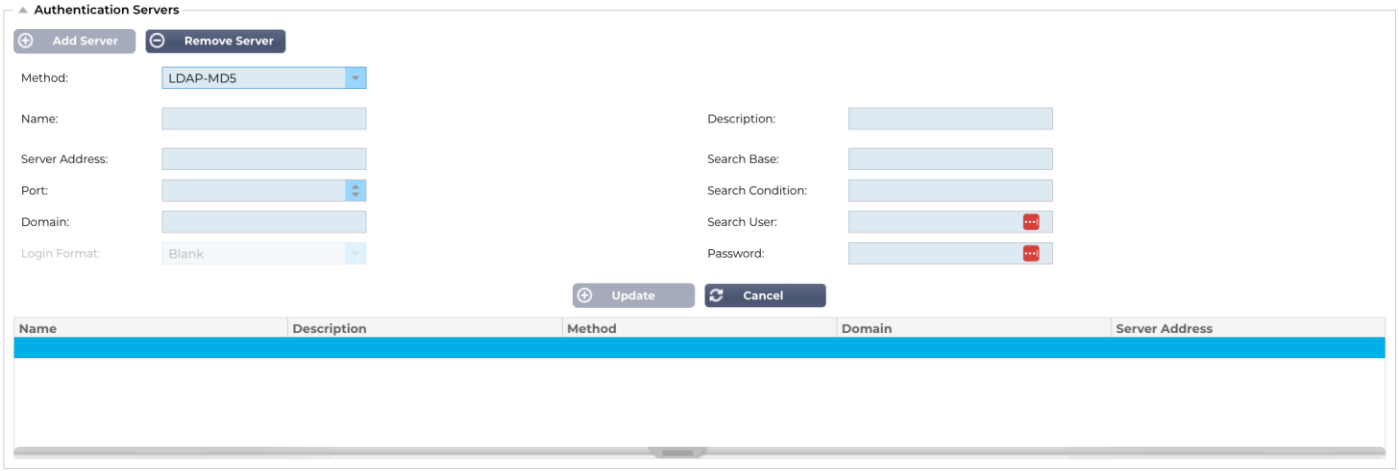
- Klicken Sie auf Server hinzufügen.
- Wählen Sie die Methode aus dem Dropdown-Menü.



Die Funktion Authentifizierungsserver ist dynamisch und zeigt nur die Felder an, die für die von Ihnen gewählte Authentifizierungsmethode erforderlich sind.

- Füllen Sie die Felder genau aus, um eine ordnungsgemäße Verbindung mit den Servern zu gewährleisten.

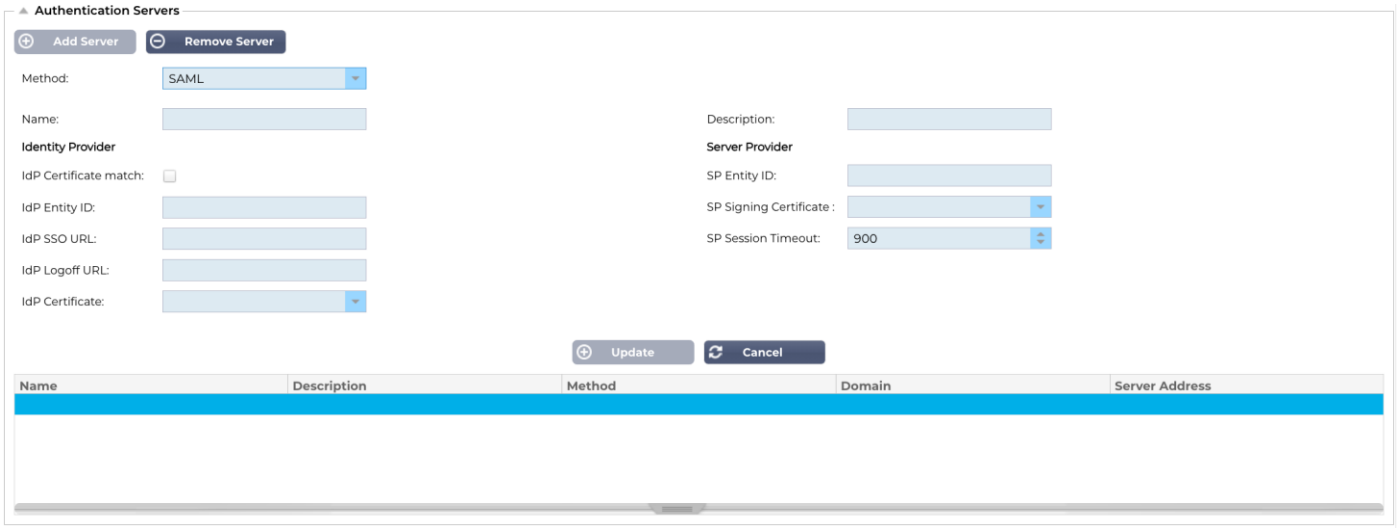
Optionen für LDAP, LDAP-MD5, LSAPS, LDAPS-MD5, Radius und SAML



Option	Beschreibung
Methode	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 mit MD5-Hash 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.
Name	Geben Sie Ihrem Server einen Namen zur Identifizierung - dieser Name wird in allen Regeln verwendet.
Server-Adresse	Fügen Sie die IP-Adresse oder den Hostnamen des Authentifizierungsservers hinzu
Hafen	Für LDAP und LDAPS sind die Ports standardmäßig auf 389 und 636 eingestellt. Für Radius ist der Hafen im Allgemeinen 1812. Für SAML werden die Ports in der ADC festgelegt.
Bereich	Geben Sie den Domänennamen für den LDAP-Server ein.
Anmeldeformat	Verwenden Sie das gewünschte Anmeldeformat. Benutzername - bei diesem Format 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 für Domäne und Benutzernamen eingeben. Beispiel: *mycompany\jdoe OR jdoe@mycompany*. Die auf der Serverebene eingegebenen Domäneninformationen werden ignoriert. Leer - die ADC akzeptiert alle Eingaben des Benutzers und sendet sie an den Authentifizierungsserver. Diese Option wird bei der Verwendung von MD5 verwendet.
Beschreibung	Eine Beschreibung hinzufügen
Suche Basis	Dieser Wert ist der Ausgangspunkt für die Suche in der LDAP-Datenbank. Beispiel *dc=meineFirma,dc=lokal*
Suche Bedingung	Die Suchbedingungen müssen dem RFC 4515 entsprechen. Beispiel: (MemberOf=CN=Phone- VPN,CN=Users,DC=mycompany,DC=local).
Benutzer suchen	Führen Sie eine Suche nach einem Domänenadministrator-Benutzer innerhalb des Verzeichnisservers durch.
Passwort	Passwort für den Domänenadmin-Benutzer.
Tote Zeit	Die Zeitspanne, nach der ein inaktiver Server wieder als aktiv markiert wird

Optionen für die SAML-Authentifizierung

WICHTIG: Wenn Sie die Authentifizierung über SAML einrichten, müssen Sie eine Enterprise App für die Entra ID Authentifizierung erstellen. Die Anleitung dazu finden Sie im KapitelEinrichten der Entra ID Authentifizierungsanwendung in Microsoft Entra

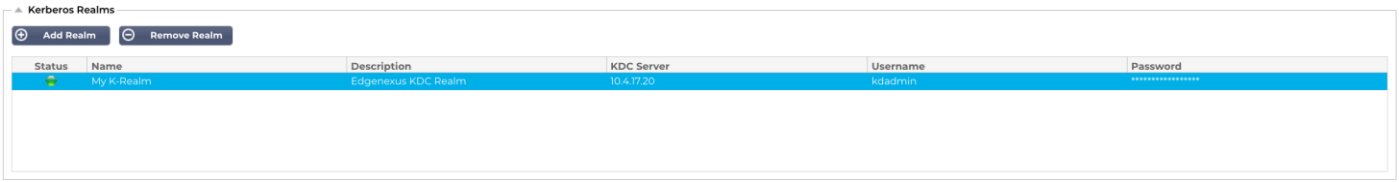


Option	Beschreibung
Methode	Wählen Sie eine Authentifizierungsmethode LDAP - einfaches LDAP mit Benutzernamen und Kennwörtern, die im Klartext an den LDAP-Server gesendet werden. LDAP-MD5 - einfaches LDAP mit Benutzernamen im Klartext und Passwort MD5-gehasht für erhöhte Sicherheit. LDAPS - LDAP über 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.
Name	Geben Sie Ihrem Server einen Namen zur Identifizierung - dieser Name wird in allen Regeln verwendet.
Identitätsanbieter	
IdP-Zertifikat-Abgleich	Der IdP-Zertifikatsabgleich bezieht sich auf den Prozess der Überprüfung, ob das von einem Identitätsanbieter (IdP) zum Signieren von SAML-Assertions verwendete digitale Zertifikat mit dem Zertifikat übereinstimmt, dem der Dienstanbieter (SP) vertraut. Diese Validierung stellt sicher, dass der IdP legitim ist und dass die von ihm gesendeten Assertions authentisch und unverändert sind. Der SP speichert in der Regel das Zertifikat des IdP in seinen Metadaten und vergleicht das in die SAML-Assertions eingebettete Zertifikat mit dem gespeicherten, um eine Übereinstimmung festzustellen.
IdP-Entitäts-ID	Eine SAML IdP Entity ID ist ein weltweit eindeutiger Bezeichner, der als endgültige Adresse für einen Identity Provider (IdP) innerhalb des Security Assertion Markup Language (SAML) Ökosystems dient. Bei dieser Kennung handelt es sich in der Regel um eine URL oder URI, die den IdP eindeutig von anderen an SAML-basierten Authentifizierungs- und Autorisierungsprozessen beteiligten Einheiten unterscheidet. Er spielt eine entscheidende Rolle beim Aufbau von Vertrauen und bei der Erleichterung der sicheren Kommunikation zwischen IdPs, Dienstanbietern (SPs) und Benutzern.
IdP SSO-URL	Eine IdP SSO-URL, kurz für Single Sign-On URL, ist eine spezifische Endpunkt-URL, die von einem Identitätsanbieter (IdP) bereitgestellt wird und als Authentifizierungs-Gateway für die Initiierung von Single Sign-On (SSO)-Sitzungen dient. Wenn ein Benutzer zu dieser URL weitergeleitet wird, fordert der IdP ihn auf, sich mit seinen Anmeldeinformationen zu authentifizieren, und leitet ihn nach erfolgreicher Authentifizierung mit einer Behauptung, die seine Identitätsinformationen enthält, an den Dienstanbieter (SP) zurück. Diese Behauptung wird dann vom SP validiert, so dass der Benutzer auf die Ressourcen des SP zugreifen kann, ohne sich erneut authentifizieren zu müssen.

IdP Abmelde-URL	Die SAML IdP Log off URL ist ein spezifischer Endpunkt auf dem Identity Provider (IdP), der den Abmeldeprozess für Single Sign-On (SSO) Sitzungen initiiert und verwaltet. Wenn ein Benutzer in einer Anwendung auf die Abmeldeschaltfläche klickt, leitet die Anwendung den Benutzer an die Abmelde-URL des IdP weiter. Der IdP macht dann die Sitzung des Benutzers bei allen vertrauenden Parteien ungültig, die mit der SSO-Authentifizierung verbunden sind, und sendet eine Abmeldeantwort zurück an die Anwendung, wodurch der Benutzer effektiv bei allen verbundenen Anwendungen abgemeldet wird.
IdP-Zertifikat	Ein SAML-IdP-Zertifikat ist ein digitales X.509-Zertifikat, das von einer vertrauenswürdigen Stelle für einen Identitätsanbieter (IdP) ausgestellt wird, der an SAML-Authentifizierungsprotokollen (Security Assertion Markup Language) teilnimmt. Dieses Zertifikat dient als sicheres Mittel zur Überprüfung der Identität des IdP und zur Authentifizierung der Integrität und Vertraulichkeit von SAML-Nachrichten, die zwischen dem IdP und Dienstanbietern (SPs) ausgetauscht werden. Sie können das IdP-Zertifikat, das Sie im ADC installiert haben, über das Dropdown-Menü auswählen.
Beschreibung	Eine Beschreibung für die Definition.
Benutzer suchen	Führen Sie eine Suche nach einem Domänen-Admin-Benutzer durch.
Passwort	Zum Festlegen des Passworts für den Benutzer admin.
Server-Anbieter	
SP Entitäts-ID	Eine SP Entity ID ist ein eindeutiger Bezeichner, der als globale Adresse für einen bestimmten Service Provider (SP) im Kontext des SAML-Protokolls dient. Es handelt sich um eine standardisierte Methode zur Identifizierung eines SP und in der Regel um eine URL oder einen anderen URI, der die SAML-Metadaten des SP aufzeigt, die wichtige Informationen wie Verschlüsselungszertifikate und Authentifizierungsendpunkte enthalten.
SP-Signatur-Zertifikat	Ein SAML SP Signing Certificate ist ein X.509-Zertifikat, das von einem Service Provider (SP) zum Signieren von SAML-Antworten verwendet wird, um die Authentizität und Integrität der zwischen dem SP und dem Identity Provider (IdP) während der SSO-Authentifizierung (Single Sign-On) ausgetauschten Nachrichten sicherzustellen. Der SP signiert die Antwort mit seinem privaten Schlüssel, und der IdP überprüft die Signatur mit dem öffentlichen Schlüssel, der dem Zertifikat zugeordnet ist, und bestätigt so die Identität des Absenders und die Unverfälschtheit des Inhalts der Nachricht.
SP Zeitüberschreitung der Sitzung	SP-Sitzungszeitüberschreitung bezieht sich auf die maximale Dauer, für die die Authentifizierungssitzung eines Benutzers auf der Seite des Dienstanbieters (SP) nach erfolgreicher einmaliger Anmeldung (SSO) über einen Identitätsanbieter (IdP) als gültig betrachtet wird. Nach Ablauf dieser Zeitspanne beendet der Dienstanbieter die Sitzung und fordert den Benutzer auf, sich erneut zu authentifizieren, um wieder Zugang zu geschützten Ressourcen zu erhalten. Dieser Mechanismus trägt zum Schutz vor unbefugtem Zugriff bei und stellt sicher, dass Benutzersitzungen nicht über längere Zeiträume ungenutzt sind.

KDC-Bereiche

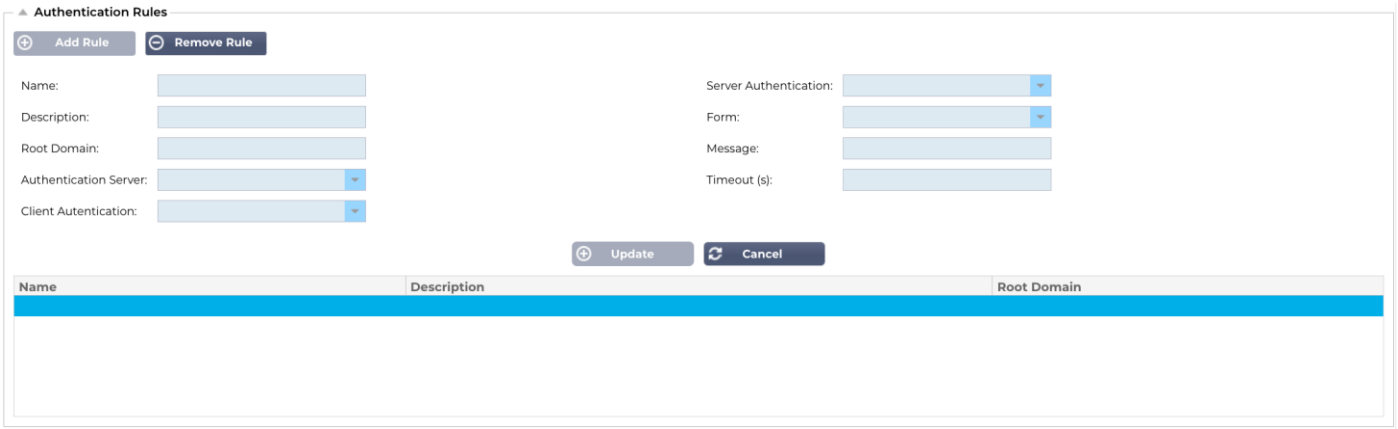
KDC-Realms beziehen sich auf Konfigurationen innerhalb des Kerberos-Authentifizierungsprotokolls, wobei jeder Realm im Wesentlichen eine Domäne oder ein Netzwerk ist, das unter einem einzigen Key Distribution Center (KDC) arbeitet. Mit dieser Einrichtung wird eine Gruppe von Systemen abgegrenzt, die unter demselben Haupt-KDC verwaltet werden, wodurch sichere Authentifizierungs- und Ticketvergabemechanismen im gesamten Netzwerk ermöglicht werden. Realms können hierarchisch oder nicht-hierarchisch sein, wobei die Möglichkeit besteht, Vertrauensbeziehungen zwischen ihnen aufzubauen, um eine sichere Authentifizierung zwischen den Realms zu ermöglichen.



Über die Benutzeroberfläche des ADC, wie in der obigen Abbildung dargestellt, können Sie Ihre Kerberos-Realms definieren. Diese Informationen können dann in den Authentifizierungsregeln verwendet werden.

Authentifizierungsregeln

Der nächste Schritt besteht darin, die Authentifizierungsregeln für die Serverdefinition zu erstellen.



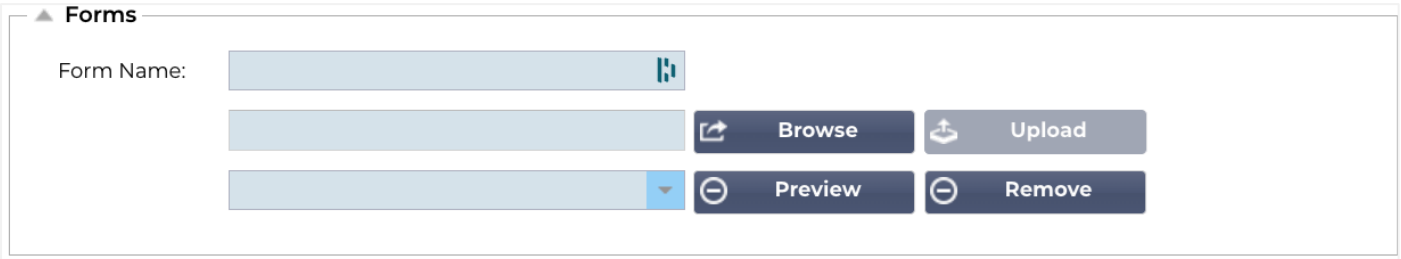
Feld	Beschreibung
Name	Fügen Sie einen geeigneten Namen für Ihre Authentifizierungsregel hinzu.
Beschreibung	Fügen Sie eine passende Beschreibung hinzu.
Wurzelbereich	Dieses Feld muss leer gelassen werden, es sei denn, Sie benötigen eine einmalige Anmeldung über Subdomänen hinweg.
Authentifizierungsserver	Dies ist eine Dropdown-Box mit den von Ihnen konfigurierten Servern.
Client-Authentifizierung:	Wählen Sie den für Ihre Bedürfnisse geeigneten Wert: Basic (401) - Diese Methode verwendet die Standard-Authentifizierungsmethode 401 Formulare - hier wird dem Benutzer das ADC-Standardformular präsentiert. Innerhalb des Formulars können Sie eine Nachricht hinzufügen. Sie können ein Formular auswählen, das Sie über den unten stehenden Abschnitt hochgeladen haben.
Server-Authentifizierung	Wählen Sie den entsprechenden Wert. Keine - Wählen Sie diese Einstellung, wenn auf Ihrem Server keine Authentifizierung vorhanden ist. Diese Einstellung bedeutet, dass Sie einem Server Authentifizierungsfähigkeiten hinzufügen können, der vorher keine hatte. Basic - wenn Ihr Server die Basic-Authentifizierung (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 - Wenn Sie diese Option wählen, verwendet der ADC sein eingebautes Formular. 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 Zeitüberschreitung nur für die formularbasierte Authentifizierung gültig ist.

Wenn Sie eine einmalige Anmeldung für Benutzer anbieten möchten, geben Sie in das Feld Root-Domäne Ihre Domäne ein. In diesem Beispiel: mycompany.com. Wir können nun mehrere Dienste haben, die edgenexus.io als Root-Domain verwenden, und Sie müssen sich nur einmal anmelden. Betrachten wir die folgenden Dienste:

- SharePoint.meinUnternehmen.de
- usercentral.meinUnternehmen.de
- App Store.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 mit einem Formular konfrontiert, das ihn auffordert, sich je nach der verwendeten Authentifizierungsregel anzumelden. Derselbe Benutzer kann dann eine Verbindung zu App Store.mycompany.com herstellen und wird automatisch von der ADC authentifiziert. Sie können eine Zeitüberschreitung festlegen, die eine Authentifizierung erzwingt, sobald die Zeit der Inaktivität erreicht ist.

Formulare



In diesem Abschnitt können Sie ein benutzerdefiniertes Formular hochladen.

Wie Sie Ihr benutzerdefiniertes Formular erstellen

Obwohl das von der ADC bereitgestellte Grundformular für die meisten Zwecke ausreicht, gibt es Fälle, in denen Unternehmen dem Nutzer ihre eigene Identität präsentieren möchten. Sie können ein eigenes Formular erstellen, das die Benutzer in solchen Fällen ausfüllen müssen. Dieses Formular muss entweder im HTM- oder HTML-Format vorliegen.

Option	Beschreibung
Name	Formularname = loginform Aktion = %JNURL% Methode = POST
Benutzername	Syntax: name = "JNUSER"
Kennwort:	name="JNPASS"
Fakultative Meldung1:	%JNMESSAGE%
Fakultative Meldung2:	%JNAUTHMESSAGE%
Bilder	Wenn Sie ein Bild hinzufügen möchten, fügen Sie es bitte in-line mit Base64-Kodierung ein.

Beispiel-HTML-Code für ein sehr einfaches Formular

```
<HTML>
<HEAD>
<TITLE>BEISPIEL FÜR EIN ANMELDEFORMULAR</TITLE>
</HEAD>
```

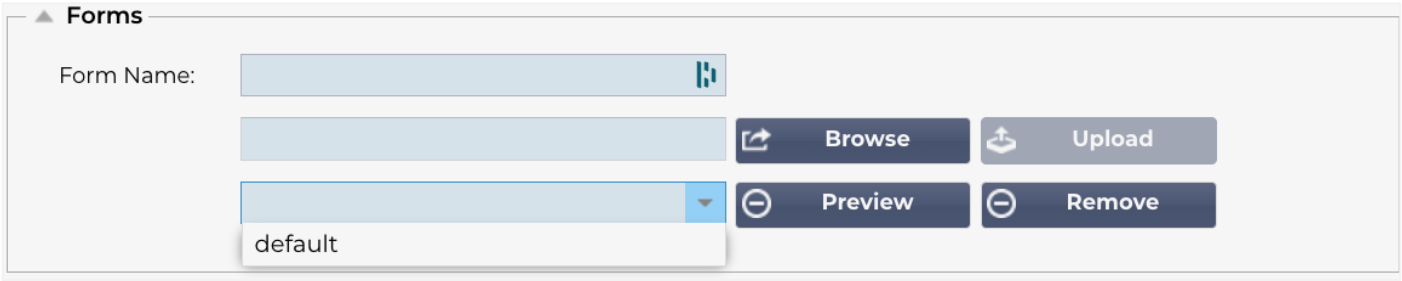
```
<BODY>
%JNMESSAGE%<br>
<form name="loginform" action="%JNURL%" method="post"> USER: <input type="text" name="JNUSER" size="20" value=""></br>
PASS: <input type="password" name="JNPASS" size="20" value=""></br>
<input type="submit" name="submit" value="OK">
</form>
</BODY>
</HTML>
```

Hinzufügen eines benutzerdefinierten Formulars

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

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

Vorschau auf Ihr benutzerdefiniertes Formular

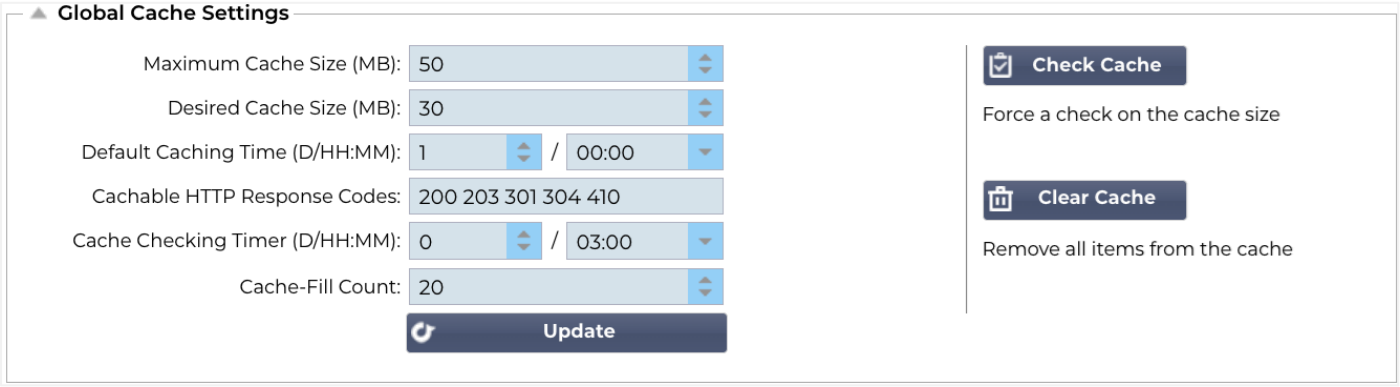


Um das soeben hochgeladene benutzerdefinierte Formular anzuzeigen, wählen Sie es aus und klicken auf Vorschau. In diesem Bereich können Sie auch Formulare löschen, die nicht mehr benötigt werden

Hinweis: Wenn Sie Produkte zum Filtern von Cookies wie AdGuard verwenden, erhalten Sie möglicherweise eine 404-Fehlermeldung. Setzen Sie die IP-Adresse des ADCs auf die Whitelist, um dies zu verhindern.

Cache

Die ADC ist in der Lage, Daten in ihrem internen Speicher zwischenzuspeichern und die Bereitstellung von Webdiensten zu verbessern. Die Einstellungen, die diese Funktionalität verwalten, werden in diesem Abschnitt beschrieben.



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 in regelmäßigen Abständen auf das Speichermedium übertragen wird, um den Cache auch nach Neustarts, Reboots und Abschaltungen aufrechtzuerhalten. Diese Funktionalität bedeutet, dass die maximale Cache-Größe in den Speicherbereich der Appliance (und nicht in den Festplattenbereich) 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 zu erreichen versucht. Die Lücke zwischen der maximalen und der gewünschten Cache-Größe dient dazu, das Eintreffen und die Überlappung neuer Inhalte zwischen den regelmäßigen Überprüfungen der Cache-Größe zu ermöglichen, um abgelaufene Inhalte zu entfernen. Auch hier kann es effektiver sein, den Standardwert (30 MB) zu akzeptieren und die Cache-Größe unter "Monitor -> Statistik" regelmäßig zu überprüfen, um die richtige Größe zu ermitteln.

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

Der hier eingegebene Wert steht für die Lebensdauer von Inhalten ohne expliziten Verfallswert. Die Standard-Caching-Zeit ist der Zeitraum, für den Inhalte ohne "no-store"-Anweisung 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 die ADC den Inhalt für einen Tag, "01:00" für eine Stunde und "00:01" für eine Minute speichert.

Zwischenspeicherbare HTTP-Antwort-Codes

Einer der zwischengespeicherten Datensätze sind HTTP-Antworten. Die im Cache gespeicherten HTTP-Antwortcodes sind:

- 200 - Standardantwort für erfolgreiche HTTP-Anfragen
- 203 - Kopfzeilen sind nicht endgültig, sondern stammen aus einer lokalen Kopie oder einer Kopie eines Dritten

- 301 - Der angeforderten Ressource wurde eine neue permanente URL zugewiesen
- 304 - Nicht geändert seit der letzten Anfrage, stattdessen sollte eine lokal gecachte Kopie verwendet werden
- 410 - Die Ressource ist auf dem Server nicht mehr verfügbar, und es ist keine Weiterleitungsadresse bekannt

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

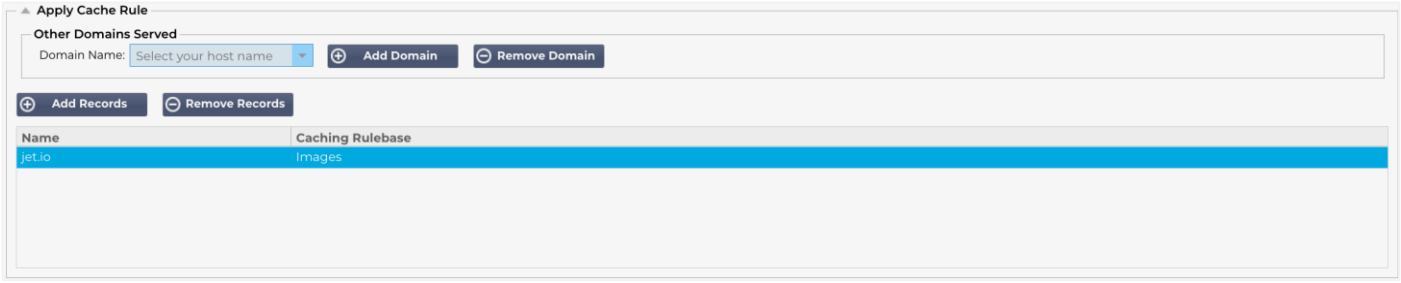
Cache-Prüfungstimer (T/HH:MM)

Diese Einstellung bestimmt das Zeitintervall zwischen den Cache-Trimmoperationen.

Cache-Fill Count

Bei dieser Einstellung handelt es sich um eine Hilfsfunktion, die den Cache füllt, wenn eine bestimmte Anzahl von 304's erkannt wurde.

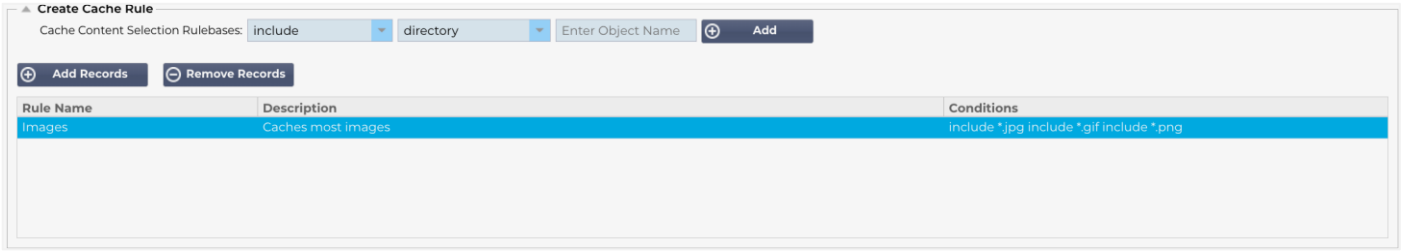
Cache-Regel anwenden



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

- Fügen Sie die Domäne manuell über die Schaltfläche Datensätze hinzufügen hinzu. Sie müssen einen vollständig qualifizierten Domänennamen oder eine IP-Adresse in Dezimalpunktschreibweise verwenden. Beispiel www.mycompany.com oder 192.168.3.1:80
- Klicken Sie auf den Dropdown-Pfeil und wählen Sie Ihre Domain aus der Liste
- Die Liste wird 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

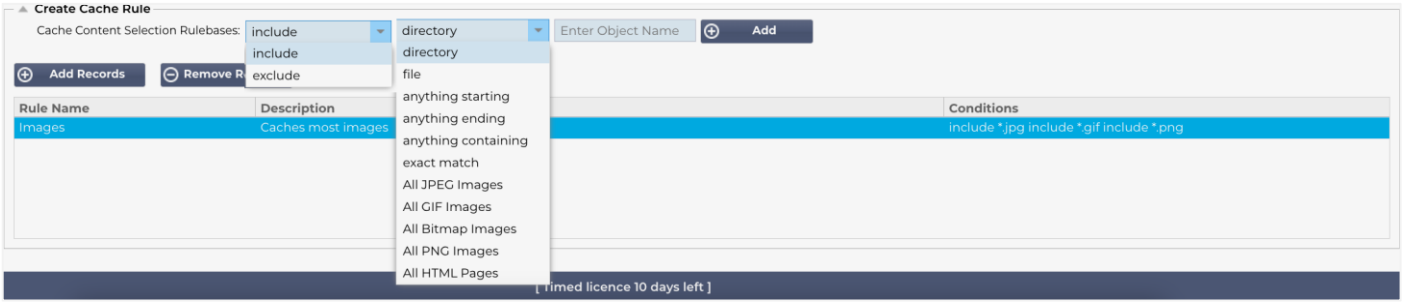
Cache-Regel erstellen



In diesem Abschnitt können Sie verschiedene Caching-Regeln erstellen, die dann auf eine Domäne 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 verwenden.

So fügen Sie eine Bedingung über die Auswahlregelbasis hinzu:



- Wählen Sie Einschließen oder Ausschließen.
- Wählen Sie ein Auswahlkriterium, zum Beispiel Alle JPEG-Bilder
- Klicken Sie auf das Symbol + Hinzufügen.
- Sie werden sehen, dass "include *.jpg" nun zu den Bedingungen hinzugefügt wurde.
- Sie können weitere Bedingungen hinzufügen. Wenn Sie dies manuell tun möchten, müssen Sie jede Bedingung in eine NEUE Zeile einfügen. Bitte beachten Sie, dass Ihre Regeln in der gleichen Zeile angezeigt werden, bis Sie auf das Feld Bedingungen klicken, dann werden sie in einer separaten Zeile angezeigt.

flightPATH

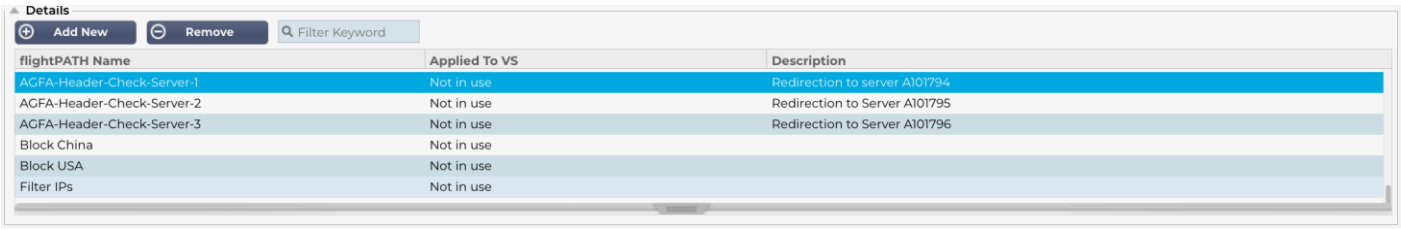
flightPATH ist eine in den ADC integrierte Technologie zur Verwaltung des Datenverkehrs, die es ermöglicht, den HTTP- und HTTPS-Datenverkehr in Echtzeit zu überprüfen und je nach Bedingungen Maßnahmen zu ergreifen.

Um flightPATH-Regeln verwenden zu können, müssen sie über die Registerkarte flightPATH im Abschnitt Real Servers auf einen virtuellen Dienst angewendet werden.

Eine Flugwegregel besteht aus vier Elementen:

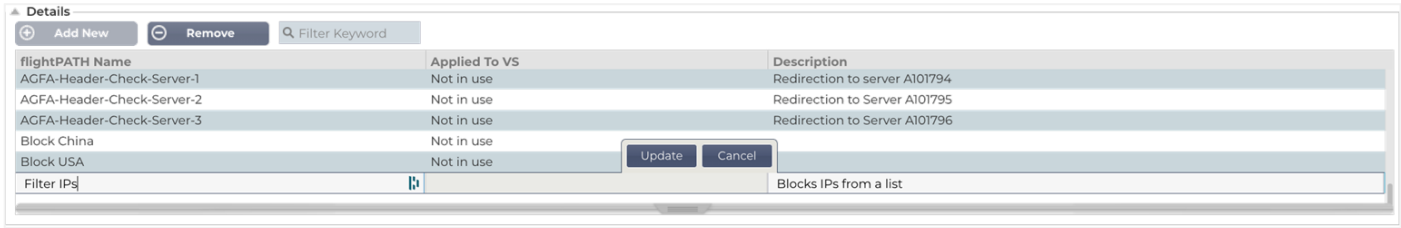
1. Details, wo Sie den flightPATH-Namen und den Dienst, dem er zugeordnet ist, definieren.
2. Bedingung(en), die definiert werden können, um die Regel auszulösen.
3. Auswertung, die die Definition von Variablen ermöglicht, die in Aktionen verwendet werden können.
4. Aktionen, die dazu dienen, zu steuern, was geschehen soll, wenn Bedingungen erfüllt sind.

Einzelheiten



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

Hinzufügen einer neuen flightPATH-Regel



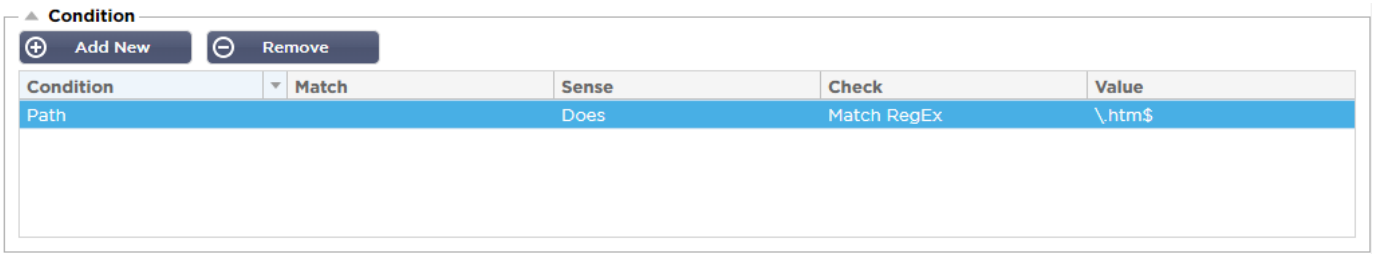
Feld	Beschreibung
FlightPATH Name	Dieses Feld ist für den Namen der flightPATH-Regel vorgesehen. Der hier angegebene Name erscheint in anderen Teilen der ADC und wird dort referenziert.
Angewandt auf VS	Diese Spalte ist schreibgeschützt und zeigt das VIP, auf das die flightPATH-Regel angewendet wird.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

Schritte zum Hinzufügen einer flightPATH-Regel

1. Klicken Sie zunächst im Bereich Details auf die Schaltfläche Neu hinzufügen.
2. Geben Sie einen Namen für Ihre Regel ein. Beispiel Auth2
3. Geben Sie eine Beschreibung Ihrer Regel ein
4. Sobald die Regel auf einen Dienst angewendet wurde, wird die Spalte Angewandt auf 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. Wenn Sie einen Fehler machen, klicken Sie einfach auf Abbrechen, um den vorherigen Zustand wiederherzustellen.

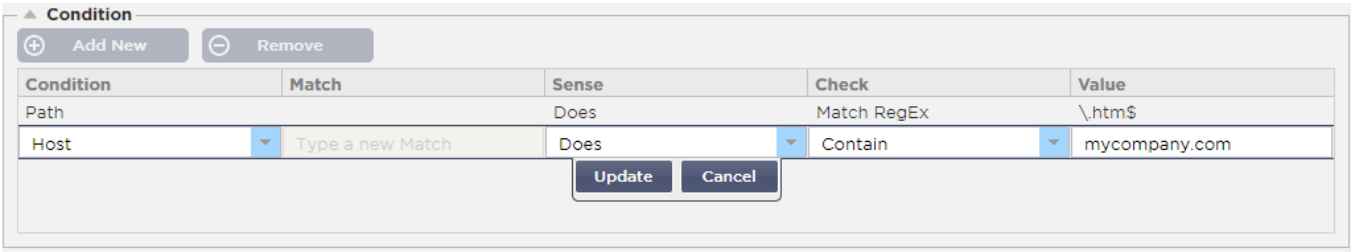
Zustand

Eine flightPATH-Regel kann eine beliebige Anzahl von Bedingungen enthalten. Die Bedingungen funktionieren auf einer UND-Basis und ermöglichen es Ihnen, die Bedingung festzulegen, bei der die Aktion ausgelöst wird. Wenn Sie eine ODER-Bedingung verwenden möchten, erstellen Sie zusätzliche flightPATH-Regeln und wenden Sie diese in der richtigen Reihenfolge auf das VIP an.



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

Erstellen einer neuen flightPATH-Bedingung



Sie müssen zunächst einen Wert aus der Spalte Bedingung auswählen.

Wir bieten mehrere Bedingungen im Dropdown-Menü an, die alle vorhersehbaren Szenarien abdecken. Wenn neue Bedingungen hinzugefügt werden, werden diese über Jetpack-Updates verfügbar sein.

Folgende Optionen stehen zur Auswahl:

ZUSTAND	BESCHREIBUNG	BEISPIEL
<form>	HTML-Formulare werden verwendet, um Daten an einen Server zu übermitteln	Beispiel "Formular hat nicht die Länge 0"
GEO-Standort	Vergleicht die Quell-IP-Adresse mit den ISO-3166-Ländercodes	GEO Ort ist gleich GB, ODER GEO Ort ist gleich Deutschland
Gastgeber	Aus der URL extrahierter Host	www.mywebsite.com oder 192.168.1.1
Sprache	Sprache, die aus dem HTTP-Header language extrahiert wird	Diese Bedingung erzeugt ein Dropdown-Menü mit einer Liste von Sprachen
Methode	Dropdown-Liste der HTTP-Methoden	Dropdown, das GET, POST, etc. umfasst
Herkunft IP	Wenn der Upstream-Proxy X-Forwarded-for (XFF) unterstützt, verwendet er die echte Herkunftsadresse	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 | für mehrere IP's verwenden
Pfad	Pfad der Website	/meinewebsite/index.asp
POST	POST-Anfrageverfahren	Überprüfung 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	Der gesamte Abfrage-String nach dem Zeichen ?	
Cookie anfordern	Name eines von einem Client angeforderten Cookies	MS-WSMAN=afYfn1CDqqCDqUD::
Kopfzeile anfordern	Jede HTTP-Kopfzeile	Referrer, Benutzer-Agent, Von, Datum
Version anfordern	Die HTTP-Version	HTTP/1.0 ODER HTTP/1.1
Antwortstelle	Eine benutzerdefinierte Zeichenfolge im Antwortkörper	Server UP
Antwort-Code	Der HTTP-Code für die Antwort	200 OK, 304 Nicht geändert
Antwort Keks	Der Name eines vom Server gesendeten Cookies	MS-WSMAN=afYfn1CDqqCDqUD::
Antwort-Kopfzeile	Jede HTTP-Kopfzeile	Referrer, Benutzer-Agent, Von, Datum
Antwort Version	Die vom Server gesendete HTTP-Version	HTTP/1.0 ODER HTTP/1.1
Quelle IP	Entweder die Herkunfts-IP, die Proxy-Server-IP oder eine andere zusammengefasste IP-Adresse	Client-IP, Proxy-IP, Firewall-IP. Sie können auch mehrere IP und Subnetze verwenden. Sie müssen die Punkte auslassen, da diese RegEX sind. Beispiel: 10.1.1\.2\.3 ist 10.1.2.3

Spiel

Das Feld Übereinstimmung kann entweder ein Dropdown- oder ein Textwert sein und ist abhängig vom Wert im Feld Bedingung definierbar. Wenn die Bedingung zum Beispiel auf Host eingestellt ist, ist das Feld "Match" nicht verfügbar. Wenn die Bedingung auf <Formular> gesetzt ist, wird das Feld "Übereinstimmung" als Textfeld angezeigt, und wenn die Bedingung auf POST gesetzt ist, wird das Feld "Übereinstimmung" als Dropdown-Liste mit entsprechenden Werten angezeigt.

Folgende Optionen stehen zur Auswahl:

MATCH	BESCHREIBUNG	BEISPIEL
Akzeptieren	Zulässige Inhaltstypen	Akzeptieren: text/plain
Accept-Encoding	Zulässige Kodierungen	Accept-Encoding: <compress | gzip | deflate | sdch | identity>
Accept-Language	Akzeptable Sprachen für die Antwort	Accept-Language: en-US
Accept-Ranges	Welche Teilinhaltsbereichstypen dieser Server unterstützt	Accept-Ranges: bytes
Autorisierung	Anmeldedaten für die HTTP-Authentifizierung	Berechtigung: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Charge-To	Enthält Kontoinformationen zu den Kosten für die Anwendung der beantragten Methode	
Content-Encoding	Die Art der verwendeten Kodierung	Inhaltskodierung: gzip

Inhalt-Länge	Die Länge des Antwortkörpers in Oktetten (8-Bit-Bytes)	Inhalt-Länge: 348
Inhalt-Typ	Der Mime-Typ des Anforderungskörpers (wird bei POST- und PUT-Anforderungen verwendet)	Inhalt-Typ: anwendung/x-www-form-urlencoded
Keks	Ein HTTP-Cookie, das zuvor vom Server mit Set-Cookie (siehe unten) gesendet wurde	Cookie: $Version=1; Skin=new;
Datum	Datum und Uhrzeit, zu der die Nachricht erstellt wurde	Datum = "Datum" ":" HTTP-Datum
ETag	Ein Identifikator für eine bestimmte Version einer Ressource, oft ein Message Digest	ETag: "aed6bdb8e090cd1:0"
Von	Die E-Mail-Adresse des Nutzers, der die Anfrage stellt	Von: user@example.com
Wenn-geändert-seit	Ermöglicht die Rückgabe eines 304 Not Modified, wenn der Inhalt unverändert ist	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Zuletzt geändert	Das Datum der letzten Änderung für das angeforderte Objekt im RFC 2822-Format	Zuletzt geändert: Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Umsetzung: Spezifische Kopfzeilen, die in der gesamten Anfrage-Antwort-Kette verschiedene Auswirkungen haben können.	Pragma: no-cache
Referent	Adresse der vorherigen Webseite, von der aus ein Link zur aktuell angeforderten Seite verfolgt wurde	Verweiser: 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 Sie	Weist nachgelagerte Proxys an, 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 "Bedeutung" ist ein boolesches Dropdown-Feld und enthält die Auswahlmöglichkeiten "tut" oder "tut nicht".

Siehe

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

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

CHECK	BESCHREIBUNG	BEISPIEL

Existieren	Dabei spielt es keine Rolle, wie der Zustand im Einzelnen aussieht, sondern nur, ob er existiert oder nicht.	Host> Existiert>
Start	Die Zeichenfolge beginnt mit dem Wert	Pfad> Startet> > /secure
Ende	Die Zeichenfolge endet mit dem Wert	Pfad> Endet> - .jpg
Enthält	Die Zeichenfolge enthält den Wert	Request Header> Accept> Enthält> > image
Gleichberechtigt	Die Zeichenkette ist gleich dem Wert	Host> Ist> gleich> www.edgenexus.io
Länge haben	Die Zeichenkette hat eine Länge des Wertes	Host> Hat> die Länge> 16 www.edgenexus.io = WAHR www.edgenexus.com = FALSCH
RegEx abgleichen	Ermöglicht Ihnen die Eingabe eines vollständigen Perl-kompatiblen regulären Ausdrucks	Herkunft IP> Entspricht> Regex
Spielliste	Ermöglicht es Ihnen, den Wert mit einer Liste von Werten abzugleichen. Dies ist nützlich, wenn beispielsweise bestimmte IP-Adressen abgeglichen werden müssen. Die Werte werden durch Kommas (,) oder Pip (|) getrennt.	Quell-IP> Tut > Trefferliste > 10.10.10.1, 10.10.10.2, 10.10.10.3 usw.
Länge überschreiten	Ermöglicht die Überprüfung, ob der Wert die angegebene Länge überschreitet.	Pfad > Does > Überschreitung der Länge > 200

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 der Dropdown-Box. Nehmen wir den Host als Beispiel. Sie können auch etwas in das Feld eingeben, und die ADC zeigt den Wert in einem Dropdown-Feld an.
3. Wählen Sie einen Sinn. Zum Beispiel: Hat
4. Wählen Sie eine Prüfung. Zum Beispiel, Enthalten
5. Wählen Sie einen Wert. Zum Beispiel: mycompany.com

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

- Zunächst wird geprüft, ob das angeforderte Objekt ein Bild ist
- Die zweite prüft, ob der Host in der URL www.imagepool.com ist.

Bewertung

Die Möglichkeit, definierbare Variablen hinzuzufügen, ist eine unwiderstehliche Fähigkeit. Andere ADCs bieten diese Möglichkeit über Skripting- oder Befehlszeilenoptionen, die nicht für jedermann ideal sind. Mit dem EdgeADC können Sie eine beliebige Anzahl von Variablen über eine benutzerfreundliche grafische Benutzeroberfläche definieren, wie unten gezeigt und beschrieben.

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

- Variable - dies ist der Name der Variablen
- Quelle - eine Dropdown-Liste mit möglichen Quellenpunkten

- 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.

- $sourceip$ - Die Quell-IP-Adresse der Anfrage
- $sourceport$ - Der Quellport, der verwendet wurde
- $clientip$ - Die IP-Adresse des Clients
- $clientport$ - Der vom Client verwendete Port
- $host$ - Der in der Anfrage genannte Host
- $method$ - Die verwendete Methode: GET, POST usw.
- $path$ - Der in der Anfrage angegebene Pfad
- $querystring$ - Der in der Anfrage verwendete Querystring
- $version$ - Die Version der HTTP-Anfrage in der REQUEST (zur Zeit nur 1 und 1.1 erlaubt).
- $resp$ - Die ANTWORT des Servers. z.B. 200OK, 404 usw.
- $geolocation$ - Der GEO-Standort, von dem aus die Anfrage gestellt wurde.

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

Erläuterung:

- Ein Kunde, der auf eine Seite zugreift, die nicht existiert, würde normalerweise die 404-Fehlerseite des Browsers angezeigt bekommen.
- Stattdessen wird der Benutzer zum ursprünglichen Hostnamen weitergeleitet, den er verwendet hat, 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 ist das Hinzufügen einer Aktion, die mit der flightPATH-Regel und der Bedingung verbunden ist.

In diesem Beispiel soll der Pfadteil der URL so umgeschrieben werden, dass er die vom Benutzer eingegebene URL wiedergibt.

- Klicken Sie auf Neu hinzufügen
- Wählen Sie Pfad umschreiben aus dem Dropdown-Menü Aktion
- Geben Sie in das Feld Ziel $path$/myimages ein
- Update anklicken

Durch diese Aktion wird /myimages zum Pfad hinzugefügt, so dass die endgültige URL wie folgt lautet www.imagepool.com/myimages

Aktion	Beschreibung	Beispiel
Anfrage Cookie hinzufügen	Fügen Sie das Anfrage-Cookie im Abschnitt "Ziel" mit dem Wert im Abschnitt "Daten" hinzu.	Ziel= Cookie Daten= MS-WSMAN=afYfn1CDqqCDqCVii
Anfrage-Kopfzeile hinzufügen	Fügen Sie einen Anfragekopf des Typs Target mit einem Wert im Abschnitt Data hinzu.	Ziel= Akzeptieren Daten= image/png
Antwort-Cookie hinzufügen	Antwort-Cookie im Abschnitt Ziel mit Wert im Abschnitt Daten hinzufügen	Ziel= Cookie Daten= MS-WSMAN=afYfn1CDqqCDqCVii
Antwort-Kopfzeile hinzufügen	Fügen Sie im Abschnitt "Ziel" den detaillierten Anforderungskopf mit dem Wert im Abschnitt "Daten" hinzu.	Ziel= Cache-Control Data= max-age=8888888
Körper Alle ersetzen	Durchsuchen Sie den Antwortkörper und ersetzen Sie alle Instanzen	Ziel= http:// (Suchzeichenfolge) Daten= https:// (Ersetzungszeichenfolge)
Körper zuerst austauschen	Durchsuchen Sie den Antwortkörper und ersetzen Sie nur die erste Instanz	Ziel= http:// (Suchzeichenfolge) Daten= https:// (Ersetzungszeichenfolge)
Körper Ersetzen Letzte	Den Antwortkörper durchsuchen und nur die letzte Instanz ersetzen	Ziel= http:// (Suchzeichenfolge) Daten= https:// (Ersetzungszeichenfolge)
Ablegen	Dadurch wird die Verbindung getrennt	Ziel= N/A Daten= N/A
e-Mail	Sendet eine E-Mail an die unter E-Mail-Ereignisse konfigurierte Adresse. Sie können eine Variable als Adresse oder Nachricht verwenden	Target= "flightPATH hat dieses Ereignis gemailt" Data= N/A
Ereignis protokollieren	Dadurch wird ein Ereignis in das Systemprotokoll aufgenommen.	Target= "flightPATH hat dies im Syslog protokolliert" Data= N/A
Umleitung 301	Dies führt zu einer permanenten Umleitung	Ziel= http://www.edgenexus.io Daten= N/A

Umleitung 302	Dies führt zu einer vorübergehenden Umleitung	Ziel= http://www.edgenexus.io Daten= N/A
Anfrage-Cookie entfernen	Entfernen Sie das im Abschnitt Ziel beschriebene Anfrage-Cookie	Ziel= Cookie Daten= MS-WSMAN=afYfn1CDqqCDqCVii
Anfrage-Kopfzeile entfernen	Entfernen Sie den im Abschnitt "Ziel" beschriebenen Anforderungskopf	Ziel=Server Daten=N/A
Antwort entfernen	Antwort-Cookie entfernen, der im Abschnitt Ziel-Cookie beschrieben ist	Ziel=jnAccel
Antwort entfernen	Entfernen Sie den Antwort-Header, der im Abschnitt Ziel-Kopfzeile beschrieben ist.	Ziel= Etag Daten= N/A
Ersetzen Sie Anfrage Cookie	Ersetzen Sie das im Abschnitt Ziel angegebene Anfrage-Cookie durch den Wert im Abschnitt Daten	Ziel= Cookie Daten= MS-WSMAN=afYfn1CDqqCDqCVii
Anfrage-Kopfzeile ersetzen	Ersetzen Sie den Anfragekopf im Ziel durch den Datenwert	Ziel= Verbindung Daten= keep-alive
Ersetzen	Ersetzen Sie das Antwort-Cookie, das im Abschnitt Ziel angegeben ist, durch den Wert im Abschnitt Daten Cookie	Ziel=jnAccel=afYfn1CDqqCDqCVii Datum=MSWSMAN=afYfn1CDqqCDqCVii
Ersetzen Antwort	Ersetzen Sie die im Abschnitt Ziel angegebene Kopfzeile der Antwort durch den Wert im Abschnitt Daten Kopfzeile	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	Auswahl des zu verwendenden sicheren Servers oder virtuellen Dienstes	Target=192.168.101:443 Data=N/A

verwenden	Auswahl des zu verwendenden Servers oder virtuellen Dienstes	Ziel= 192.168.101:80 Daten= 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 verwenden Data= Geben Sie eine Passphrase für die Verschlüsselung ein

Ein Szenario mit flightPATH-Regeln

Ein Kunde hat eine E-Commerce-Website und hat Probleme mit Cookies, die von den neuesten Versionen eines Browsers blockiert werden.

Der Kunde geht den Problemen nach und stellt fest, dass die Ursache in der fehlenden "sicheren" und "standortgleichen" Kennzeichnung der fraglichen Cookies liegt.

Sehen wir uns an, wie flightPATH helfen kann.

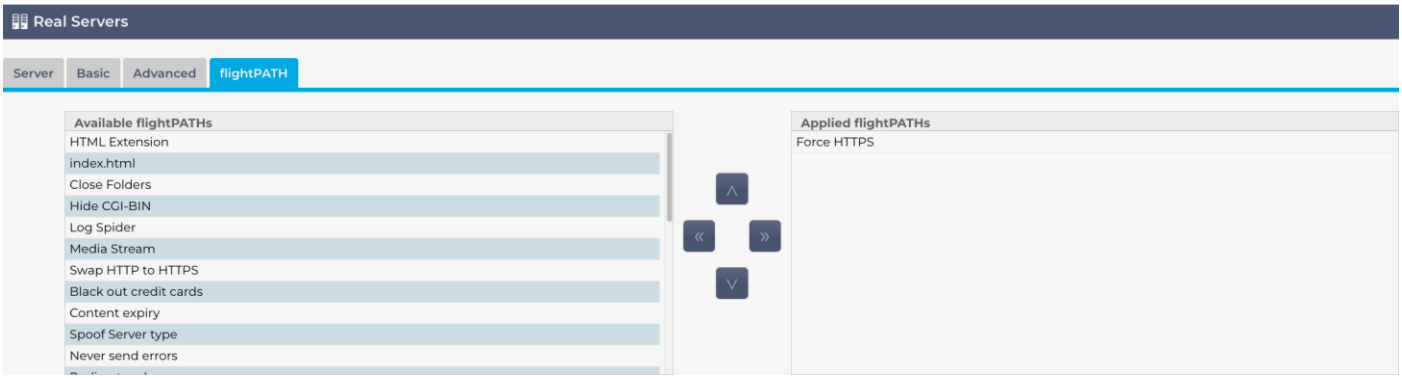
- Wir haben ein Cookie mit dem Namen 'wp_woocommerce_session_97929973749972642'.
- Der Name des Cookies ist "wp_woocommerce_session_" mit einem zufälligen, eindeutigen ID-Wert von "97929973749972642", der vom E-Commerce-System generiert wird.
- Die Tags für "same-site" und "secure" scheinen leer zu sein, so dass das Cookie durch die neuen Sicherheitsbeschränkungen des Browsers blockiert wird.
- Um dies zu verhindern, können wir die folgenden flightPATH-Regeln erstellen.
- **flightPATH-Regel für Sitzungs-ID**
  - **Bedingung**:
    Leer lassen
  - **Auswertung**:
    Variable = $variable_1$
    Quelle = Antwort-Cookie
    Ausschnitt = wp_woocommerce_session_*
  - Aktion
    Aktion = Antwort-Cookie ersetzen
    Ziel = wp_woocommerce_session_*
    Daten = $Variable_1$
- **flightPATH-Regel für Tags**
  - **Bedingung:**
    Bedingung = Antwort-Cookie
    Übereinstimmung = woocommerce_cart_hash
    Sense = Hat
    Prüfung = Vorhanden
    Wert = Leer lassen
  - **Auswertung:**
    Variable = $variable_2$
    Quelle = Antwort-Cookie
    Angabe = woocommerce_cart_hash
    Wert = Leer lassen
  - **Aktion:**
    Aktion = Ersetzen des Antwort-Cookies

Ziel = woocommerce_cart_hash
Daten = $variable_2$,SameSite=None,Sicher

Nun wenden Sie die Regeln auf die virtuellen Dienste an, die sie benötigen.

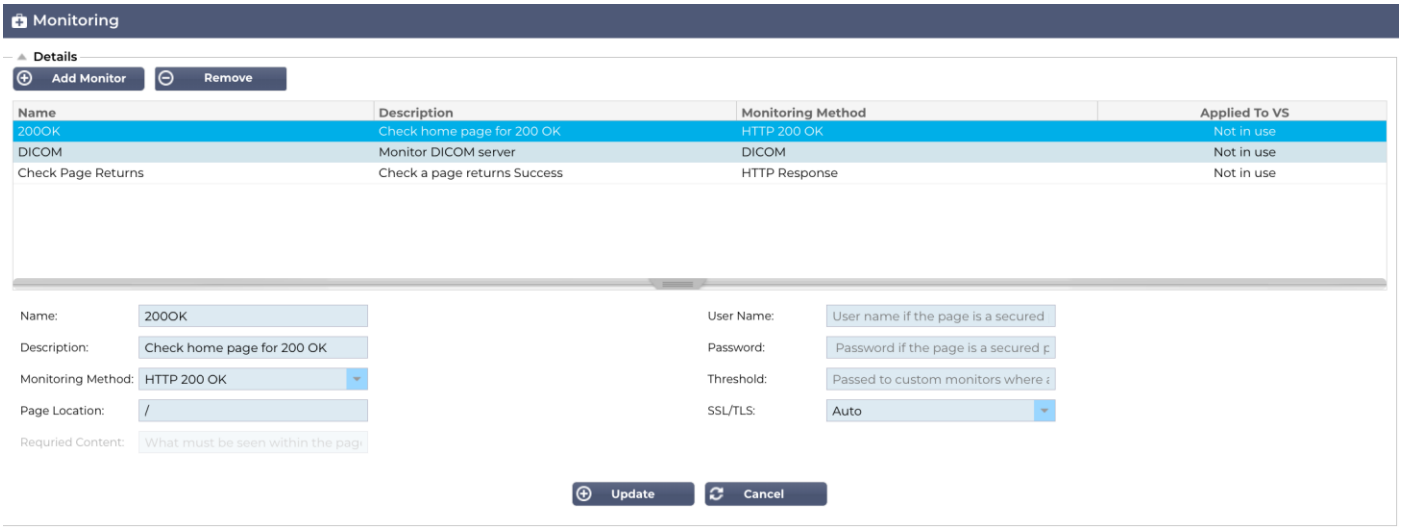
Anwendung der flightPATH-Regel

Die Anwendung einer flightPATH-Regel erfolgt in 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 abgebildete Liste der Realserver
- Klicken Sie auf die Registerkarte flightPATH
- Wählen Sie die von Ihnen konfigurierte flightPATH-Regel 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 Abschnitt Applied flightPATHs oder klicken Sie auf die Pfeilschaltfläche >>.
- Die Regel wird auf die rechte Seite verschoben und automatisch angewendet.

Echte Server-Monitore



Die Überwachung realer Server ist in einem Lastausgleichsszenario wichtig, um Serverprobleme zu erkennen und darauf zu reagieren, eine ausgewogene Lastverteilung zu gewährleisten, die Ressourcennutzung zu optimieren, kritische Dienste zu priorisieren und Software-Schwachstellen zu erkennen und zu beheben.

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", die Sie im Feld "Server Monitoring" auf der Registerkarte "Basic" des von Ihnen definierten virtuellen Dienstes auswählen.

Arten von Real-Server-Monitoren

Es gibt mehrere Real-Server-Monitore, die in der folgenden Tabelle erläutert werden. Sie können natürlich zusätzliche Monitore mit PERL schreiben.

Methode der Überwachung	Beschreibung	Beispiel
HTTP 200 OK	Es wird eine TCP-Verbindung zum Realserver hergestellt. Nach dem Herstellen der Verbindung wird eine kurze HTTP-Anfrage an den Real-Server gesendet. Wenn die Antwort eingeht, wird sie auf die Zeichenfolge "200 OK" geprüft. Wenn sie vorhanden ist, gilt der Server als betriebsbereit. Bitte beachten Sie, dass bei Verwendung dieses Monitors die gesamte Seite mit Inhalt abgerufen wird. Diese Überwachungsmethode kann nur für HTTP- und beschleunigte HTTP-Dienste verwendet werden. Wenn jedoch ein Layer-4-Diensttyp für einen HTTP-Server verwendet wird, kann sie auch dann verwendet werden, wenn SSL auf dem Realserver nicht verwendet oder von der "Content SSL"-Funktion entsprechend behandelt wird.	**Anfrage** GET / HTTP/1.1 Rechner: 192.168.159.200 Akzeptieren: */* Accept-Language: en-gb Benutzer-Agent: Edgenexus-ADC/4.0 Verbindung: Keep-Alive Cache-Kontrolle: no-cache **Antwort** HTTP/1.1 200 OK Inhalt-Typ: text/html Last-Modified: Wed, 31 Jan 2018 15:08:18 GMT Accept-Ranges: bytes ETag: "0dd3253a59ad31:0" Server: Microsoft-IIS/10.0 Date: Tue, 13 Jul 2021 15:55:47 GMT Inhalt-Länge: 1364 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"

		"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <Kopf> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /> <Titel>jetNEXUS</title> <style type="text/css"> <!-- Körper { Farbe:#FFFFFF; ... </body> </html>
HTTP 200 Kopf	Es wird eine TCP-Verbindung zum Real-Server hergestellt, wobei das Feld PATH den zu überprüfenden Ort angibt. Der Kopfteil der Antwort wird vom Server geholt, der Inhalt wird verworfen. Die Antwort wird auf 200 OK geprüft. Wenn dies der Fall ist, gilt der Server als betriebsbereit. Bitte beachten Sie, dass mit diesem Monitor nur der Kopfteil abgerufen wird. Diese Überwachungsmethode kann nur für HTTP- und beschleunigte HTTP-Dienste verwendet werden. Wenn jedoch ein Layer-4-Diensttyp für einen HTTP-Server verwendet wird, kann sie auch dann verwendet werden, wenn SSL auf dem Realserver nicht verwendet oder von der "Content SSL"-Funktion entsprechend behandelt wird.	**Anfrage** KOPF / HTTP/1.1 Rechner: 192.168.159.200 Akzeptieren: */* Accept-Language: en-gb Benutzer-Agent: Edgenexus-ADC/4.0 Verbindung: Keep-Alive Cache-Kontrolle: no-cache **Antwort** HTTP/1.1 200 OK Inhalt-Länge: 1364 Inhalt-Typ: text/html Last-Modified: Wed, 31 Jan 2018 15:08:18 GMT Accept-Ranges: bytes ETag: "0dd3253a59ad31:0" Server: Microsoft-IIS/10.0 Date: Tue, 13 Jul 2021 15:49:19 GMT
HTTP 200 Optionen	Es wird eine TCP-Verbindung zum Realserver hergestellt und eine Optionsanfrage gestellt. Die Optionen werden zurückgesendet und auf 200 OK-Inhalt geprüft. Wenn der Inhalt von 200 OK gefunden wird, gilt der Server als verfügbar.	**Anfrage** OPTIONEN / HTTP/1.1 Rechner: 192.168.159.200 Akzeptieren: */* Accept-Language: en-gb Benutzer-Agent: Edgenexus-ADC/4.0 Verbindung: Keep-Alive Cache-Kontrolle: no-cache **Antwort** HTTP/1.1 200 OK Erlauben: OPTIONS, TRACE, GET, HEAD, POST Server: Microsoft-IIS/10.0 Öffentlich: OPTIONS, TRACE, GET, HEAD, POST Date: Tue, 13 Jul 2021 16:23:39 GMT Inhalt-Länge: 0
HTTP-Kopf	Der HTTP-Head-Monitor ermöglicht es uns, nach einem bestimmten Wert im Head-Teil des HTTP-Streams zu suchen. Wir können einen Pfad und eine erforderliche Antwort in die entsprechenden Felder eingeben und dann nach diesem Wert in der Antwort suchen. Wird der Wert Required Response im Head gefunden, gilt der Server als betriebsbereit und verfügbar. Wir können dies auch auf besonders geschützten Seiten verwenden, die einen Benutzernamen und ein Passwort erfordern.	**Anfrage** HEAD /ispagethere.htm HTTP/1.1 Rechner: 192.168.159.200 Akzeptieren: */* Accept-Language: en-gb Benutzer-Agent: Edgenexus-ADC/4.0 Verbindung: Keep-Alive Cache-Kontrolle: no-cache **Antwort** HTTP/1.1 200 OK Inhalt-Länge: 1364 Inhalt-Typ: text/html

	Auf diese Weise kann das Ergebnis des Monitors als korrekt angesehen werden. Wenn Sie beispielsweise **/ispagethere.html** und die Werte **200 OK** in den Feldern "Pfad" und "Erforderliche Antwort" angeben, erhalten Sie ein erfolgreiches Ergebnis, wenn der Server verfügbar ist und die Seite auf die Anfrage antwortet. Diese Überwachungsmethode kann nur für HTTP- und beschleunigte HTTP-Dienste verwendet werden. Wenn jedoch ein Layer-4-Diensttyp für einen HTTP-Server verwendet wird, kann sie auch dann verwendet werden, wenn SSL auf dem Realserver nicht verwendet oder von der "Content SSL"-Funktion entsprechend behandelt wird.	Last-Modified: Wed, 31 Jan 2018 15:08:18 GMT Accept-Ranges: bytes ETag: "0dd3253a59ad31:0" Server: Microsoft-IIS/10.0 Date: Wed, 14 Jul 2021 08:28:18 GMT
HTTP-Optionen	Mit dem HTTP-Optionen-Monitor können Sie nach einem bestimmten Wert in den zurückgegebenen Optionsdaten suchen. Wir geben einen Pfad und eine erforderliche Antwort in die entsprechenden Felder ein und überprüfen dann die Antwort. Wenn die erforderliche Antwort in den Optionsdaten gefunden wird, ist der Server verfügbar und läuft. Die erforderlichen Antwortwerte können alle folgenden sein: OPTIONS, TRACE, GET, HEAD und POST. Wenn Sie z. B. **/ispagethere.html** und GET-Werte in den Feldern Pfad und Erforderliche Antwort angeben, wird ein erfolgreiches Ergebnis zurückgegeben, wenn der Server verfügbar ist und auf die Anfrage antwortet. Diese Überwachungsmethode kann nur für HTTP- und beschleunigte HTTP-Dienste verwendet werden. Wenn jedoch ein Layer-4-Diensttyp für einen HTTP-Server verwendet wird, kann sie auch dann verwendet werden, wenn SSL auf dem Realserver nicht verwendet oder von der "Content SSL"-Funktion entsprechend behandelt wird.	**Anfrage** OPTIONEN /ispagethere.htm HTTP/1.1 Rechner: 192.168.159.200 Akzeptieren: */* Accept-Language: en-gb Benutzer-Agent: Edgenexus-ADC/4.0 Verbindung: Keep-Alive Cache-Kontrolle: no-cache **Antwort** HTTP/1.1 200 OK Erlauben: OPTIONS, TRACE, GET, HEAD, POST Server: Microsoft-IIS/10.0 Öffentlich: OPTIONS, TRACE, GET, HEAD, POST Date: Wed, 14 Jul 2021 09:47:27 GMT Inhalt-Länge: 0
HTTP-Antwort	Es wird eine Verbindung und eine HTTP-Anfrage/Antwort zum Realserver hergestellt und wie in den vorangegangenen Beispielen beschrieben überprüft. Anstatt jedoch auf einen "200 OK"-Antwortcode zu prüfen, wird der Header der HTTP-Antwort auf benutzerdefinierten Textinhalt geprüft. Der Text kann eine vollständige Kopfzeile, ein Teil einer Kopfzeile, eine Zeile aus einem Teil einer Seite oder nur ein Wort sein. Im Beispiel auf der rechten Seite haben wir zum Beispiel **/ispagethere.htm** als Pfad und **Microsoft-IIS** als erforderliche Antwort angegeben. Wenn der Text gefunden wird, gilt der Realserver als betriebsbereit.	**Anfrage** GET /ispagethere.htm HTTP/1.1 Rechner: 192.168.159.200 Akzeptieren: */* Accept-Language: en-gb Benutzer-Agent: Edgenexus-ADC/4.0 Verbindung: Keep-Alive Cache-Kontrolle: no-cache **Antwort** HTTP/1.1 200 OK Inhalt-Typ: text/html Last-Modified: Wed, 31 Jan 2018 15:08:18 GMT Accept-Ranges: bytes ETag: "0dd3253a59ad31:0" Server: Microsoft-IIS/10.0 Date: Wed, 14 Jul 2021 10:07:13 GMT Inhalt-Länge: 1364

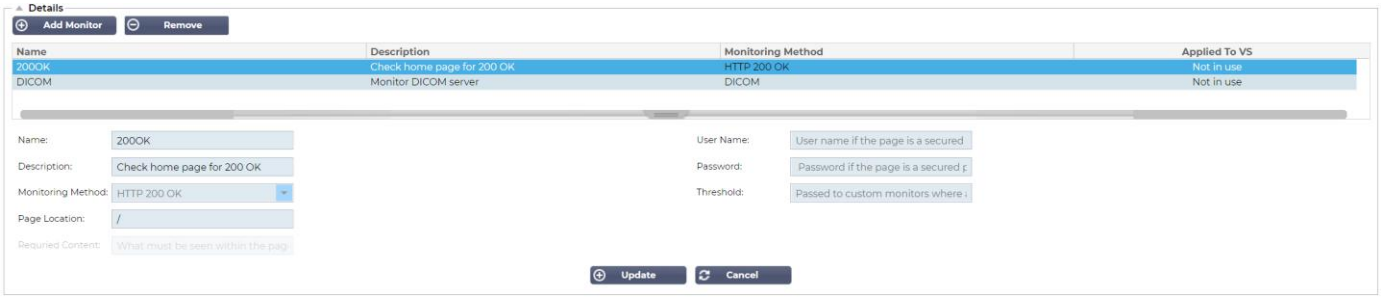
	Diese Überwachungsmethode kann nur bei den Diensttypen HTTP und Accelerated HTTP verwendet werden. Wenn jedoch ein Layer-4-Diensttyp für einen HTTP-Server verwendet wird, kann er immer noch verwendet werden, wenn SSL auf dem Realserver nicht verwendet wird oder von der "Content SSL"-Funktion entsprechend behandelt wird.	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <Kopf> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /> <Titel>jetNEXUS</title> <style type="text/css"> <!-- Körper { Farbe:#FFFFFF; ...
Multi-Port-TCP-Überwachung	Diese Methode entspricht der obigen, mit dem Unterschied, dass Sie mehrere verschiedene Ports haben können. Der Monitor gilt nur dann als erfolgreich, wenn alle im Abschnitt "Erforderlicher Inhalt" angegebenen Ports korrekt antworten.	Name: Multi-Port-Monitor Beschreibung: Mehrere Ports auf Erfolg überwachen Standort der Seite: N/A Erforderlicher Inhalt: 135,59534,59535
TCP Out of Band	Die TCP-Out-of-Band-Methode entspricht einer TCP-Verbindung, mit dem Unterschied, dass Sie in der Spalte "Erforderlicher Inhalt" den Port angeben können, den Sie überwachen möchten. Dieser Port ist in der Regel 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 Standort der Seite: N/A Erforderlicher Inhalt: 555
DICOM	Wir senden ein DICOM-Echo unter Verwendung des Wertes "Source Calling" AE Title in der Spalte "Required Content". Sie können auch den Wert für den AE-Titel "Destination Called" im Abschnitt "Notes" jedes Servers festlegen. Sie finden die Spalte "Notizen" in den IP-Diensten. -Virtuelle Dienste - Server-Seite.	Name: DICOM Beschreibung: L7-Zustandsprüfung für DICOM-Dienst Überwachungsmethode: DICOM Standort der Seite: N/A Erforderlicher Inhalt: AET-Wert
LDAPS	Dieser neue Gesundheitscheck wird verwendet, um den Zustand und die Reaktion eines LDAP/AD-Servers zu überprüfen.	Name: LDAPS Beschreibung: LDAP/AD-Server-Zustandsprüfung Die Verwendungsparameter sind wie folgt: **Benutzername**: cn=Benutzername,cn=Benutzer,dc=Domänenname,dc=Lokal **Kennwort**: DomainUserPassword **Inhalt**: 200OK
SNMP v2	Mit dieser Überwachungsmethode können Sie den Verfügbarkeitsstatus eines Servers anhand der SNMP-MIB-Antwort des Servers überprüfen. Der Wert der Require Response sollte den Community-Namen enthalten.	
DNS-Server-Prüfung	Beim Lastausgleich von DNS-Servern ist es hilfreich zu sehen, ob der Server auf DNS-Anfragen antwortet. Der Monitor kann wie folgt verwendet werden: • Das Feld Pfad wird für den FQDN verwendet, den Sie abfragen wollen. Wenn Sie zum Beispiel www.edgenexus.io abfragen möchten, geben Sie dies in das Feld Pfad ein. • Wenn Sie dieses Feld leer lassen, verwendet der Monitor seine Standard-Suchfunktion, um die Abfrage durchzuführen. • Das Feld Erforderliche Antwort kann leer gelassen werden, dann geht der Monitor davon aus, dass jede Antwort als gültig angesehen wird. Andernfalls sollten Sie die	

	erwartete IP-Adresse in das Feld "Erforderliche Antwort" eingeben. Dies kann zum Beispiel 101.10.10.100 sein. Wenn die Abfrage diesen Wert zurückgibt, meldet der Monitor einen Erfolg; andernfalls wird ein Fehler gemeldet. Ein erfolgreiches Ergebnis zeigt an, dass der DNS-Server, für den Sie den Lastausgleich durchführen, betriebsbereit ist.

Die Seite Real Server Monitors ist in drei Abschnitte unterteilt.

Einzelheiten

Im Bereich Details können Sie neue Monitore hinzufügen und nicht benötigte Monitore entfernen. Sie können auch einen vorhandenen Monitor bearbeiten, indem Sie auf ihn doppelklicken.



Name

Name Ihrer Wahl für Ihren Monitor.

Beschreibung

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

Methode der Überwachung

Wählen Sie die Überwachungsmethode aus der Dropdown-Liste. Folgende Optionen sind verfügbar:

- HTTP 200 OK
- HTTP 200 Kopf
- HTTP 200 Optionen
- HTTP-Kopf
- HTTP-Optionen
- HTTP-Antwort
- Multi-Port-TCP-Monitor
- TCP Out of Band
- DICOM
- SNMP v2
- DNS-Server-Prüfung
- LDAPS

Seite Standort

URL Seitenstandort für einen HTTP-Monitor. Dieser Wert kann ein relativer Link sein, 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 nutzen 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 Kennwortfeld für die Anmeldung bei einem Real Server verwenden.

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, wenn ein Schwellenwert wie der CPU-Level erforderlich ist.

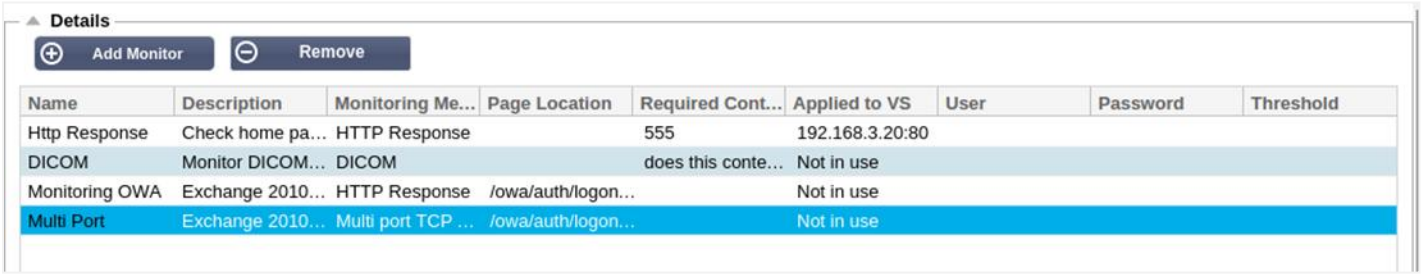
HINWEIS: Bitte stellen Sie sicher, dass die Antwort des Anwendungsservers keine "Chunked"-Antwort ist.

SSL/TLS

In diesem Feld können Sie festlegen, ob SSL verwendet werden soll oder nicht. Die Einstellungen sind wie folgt:

- Ein - Damit wird SSL erzwungen
- Aus - Damit wird SSL deaktiviert
- Auto - Der aktuelle Zustand wird beibehalten

Real Server Monitor Beispiele



Monitor hochladen

Es wird häufig vorkommen, dass 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 die Dateierweiterung .pl.

- 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.

Benutzerdefinierte Monitore

In diesem Abschnitt können Sie die hochgeladenen benutzerdefinierten Monitore anzeigen und sie entfernen, wenn sie nicht mehr benötigt werden.

- Klicken Sie auf die Dropdown-Box
- 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 Perl-Skripts für den Monitor

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

Dieser Abschnitt zeigt Ihnen die Befehle, die Sie in Ihrem Perl-Skript 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 angeben, wird Ihr Skript nicht gefunden!

Die folgenden Angaben sind obligatorisch:

- #Monitor-Name
- streng verwenden;
- Gebrauchswarnung;

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

Dynamische Werte

- my $host = $_[0]; ### Host-IP oder Name (kommt aus RS-Details oder OOB, falls verwendet)
- my $port = $_[1]; ### Host Port (kommt von RS Details oder OOB, falls verwendet)
- my $content = $_[2]; ### Erforderlicher Inhalt aus den Monitoreinstellungen (was in der Antwort zu sehen sein muss)
- my $notes = $_[3]; ### Notizen aus den RS-Details in den IP-Diensten (verwenden Sie dies, um jeden RS-Monitor individuell zu gestalten)
- my $page = $_[4]; ### Standort der Seite in den Monitoreinstellungen
- my $user = $_[5]; ### Benutzernamen aus den Monitoreinstellungen
- my $password = $_[6]; ### Passwort aus den Monitoreinstellungen
- my $threshold = $_[7]; ### Schwellenwertparameter aus den Monitoreinstellungen
- my $rsaddr = $_[8]; ### RS IP (anders als _[0] bei Out-of-Band-Überwachung)

- my $rsport = $_[9]; ### RS-Port (anders als _[1] bei Out-of-Band-Überwachung)
- my $timeout = $_[10]; ### Überwachung der Kontaktzeit in Sekunden von IP Services > Real Server > Advanced > Monitoring Timeout

Individuelle Gesundheitschecks haben zwei Ergebnisse

- Erfolgreich
  Rückgabewert 1
  Eine Erfolgsmeldung in Syslog ausgeben
  Markiere den Realserver als Online (sofern IN COUNT übereinstimmt)
- Erfolglos
  Rückgabewert 2
  Druckt eine Meldung mit dem Wort "Unsuccessful" ins Syslog
  Markiere den Real Server Offline (vorausgesetzt OUT Count stimmt überein)

Beispiel für einen benutzerdefinierten Gesundheitsmonitor

```
#Überwachungsname HTTPS_SNI
streng verwenden:
Gebrauchswarnungen;
# Der oben genannte Monitorname wird in der Dropdown-Liste der verfügbaren Gesundheitsprüfungen angezeigt.
# Es werden 6 Werte an dieses Skript übergeben (siehe unten).
# Das Skript gibt folgende Werte zurück
# 1 bedeutet, dass der Test erfolgreich ist
# 2 wenn der Test nicht erfolgreich ist sub monitor
{
my Schost       = $_[O]; ### 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 Hostname
my Spage        = $_[4]; ### Der Teil der URL nach der Host-Adresse
my Suser        = $_[5]: ### domain/usemame (optional)
my Spasswort    = $_[6]; ### Passwort (optional)
my $Auflösung;
my $auth        =;
wenn ($Port)
{
        $resolve = "$notes:$port:$host":
}
sonst {
        $resolve = "$notes:$host";
}
if ($Benutzer && $Kennwort) {
        $auth = "-u $Benutzer:$Kennwort :
}
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";
        Rückgabe(2)
        }
}
monitor(@ARGV):
```

HINWEIS:

Benutzerdefinierte Überwachung - Die Verwendung von globalen Variablen ist nicht möglich. Nur lokale Variablen verwenden - Variablen, die innerhalb von Funktionen definiert sind

Verwendung von RegEx - Alle regulären Ausdrücke müssen eine mit Perl kompatible Anweisungssyntax verwenden.

SSL-Zertifikate

Um den Schicht-7-Lastausgleich mit Servern, die verschlüsselte Verbindungen mit SSL verwenden, erfolgreich nutzen zu können, muss der ADC mit den auf den Zielservern verwendeten SSL-Zertifikaten ausgestattet sein. Dies ist erforderlich, damit der Datenstrom vor dem Senden an den Zielserver entschlüsselt, geprüft, verwaltet und erneut verschlüsselt werden kann.

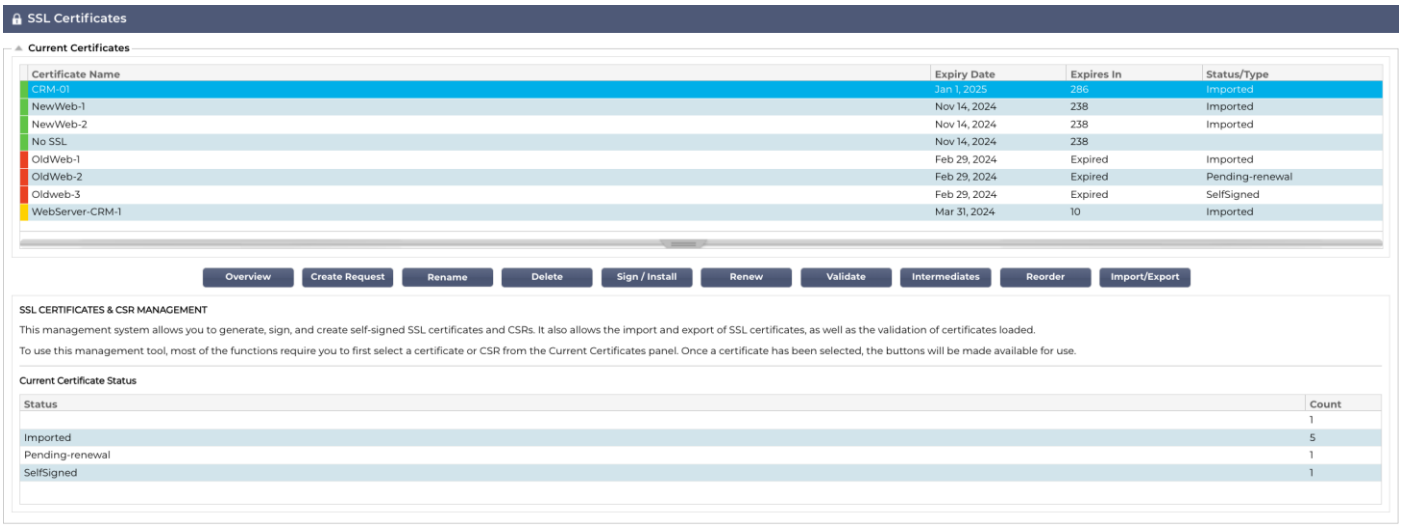
Die SSL-Zertifikate können von selbstsignierten Zertifikaten, die die ADC generieren kann, bis hin zu herkömmlichen Zertifikaten (einschließlich Wildcard) reichen, die von vertrauenswürdigen Anbietern erhältlich sind. Sie können auch domänensignierte Zertifikate verwenden, die von Active Directory generiert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

Was macht die ADC mit dem SSL-Zertifikat?

Die ADC kann Regeln für die Verkehrsverwaltung (flightPATH) in Abhängigkeit vom Inhalt der Daten anwenden. Diese Verwaltung kann nicht für SSL-verschlüsselte Daten durchgeführt werden. Wenn die ADC die Daten prüfen soll, muss sie sie zunächst entschlüsseln und benötigt dazu das vom Server verwendete SSL-Zertifikat. Nach der Entschlüsselung kann die ADC dann die flightPATH-Regeln prüfen und ausführen. Anschließend werden die Daten mit dem SSL-Zertifikat erneut verschlüsselt und an den endgültigen Real Server gesendet.

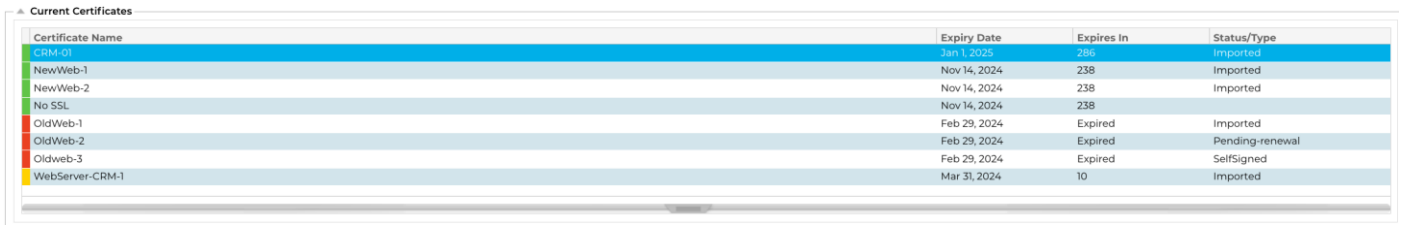
Der SSL-Konfigurationsmanager

Ab Version 196X gibt es eine neue und einfachere Methode zur Konfiguration und Verwaltung von SSL-Zertifikaten und Zertifikatsanfragen.



Der SSL-Konfigurationsmanager besteht aus drei Hauptbereichen.

Der Bereich für die Zertifikatsauflistung



Auf der oberen Seite des Managers werden die SSL-Zertifikate angezeigt, die zur Verwendung zur Verfügung stehen oder auf die Aktivierung durch eine vertrauenswürdige Stelle warten.

Die Zertifikate werden in einer vierspaltigen Anzeige dargestellt, die den Zertifikatsnamen, das Ablaufdatum, "Läuft ab in" (Anzahl der Tage bis zum Ablauf) und den Status/Typ des Zertifikats enthält.

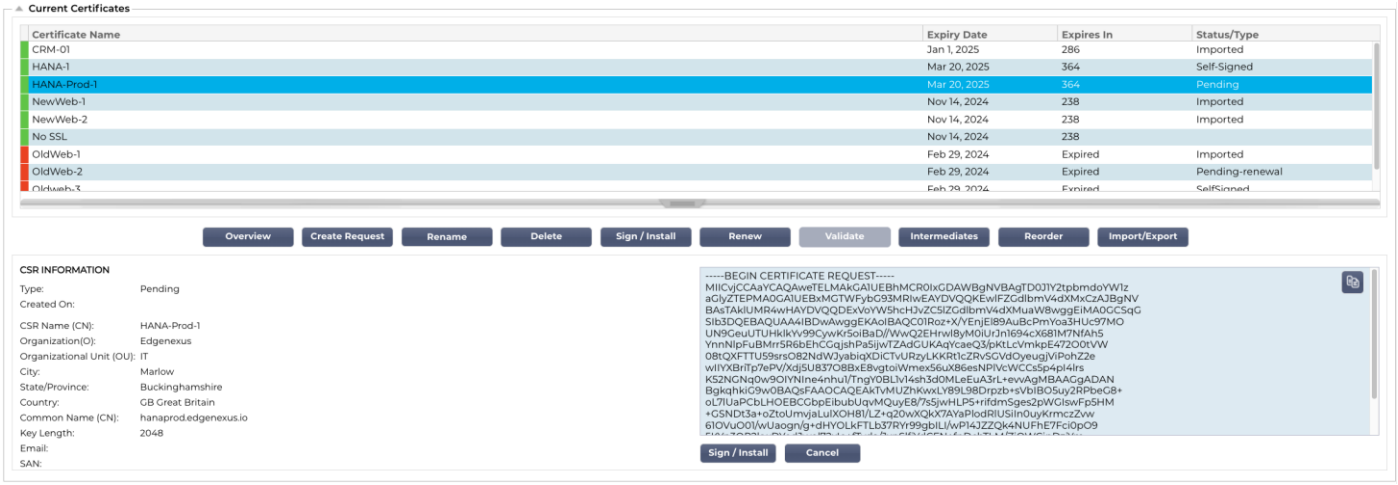
Farb-Codes

Wie Sie sehen können, zeigt jede Zeile eine Bescheinigung zusammen mit einem farbcodierten Block. Nachstehend finden Sie eine Tabelle, die die verschiedenen farbcodierten Blöcke und ihre Bedeutung zeigt.

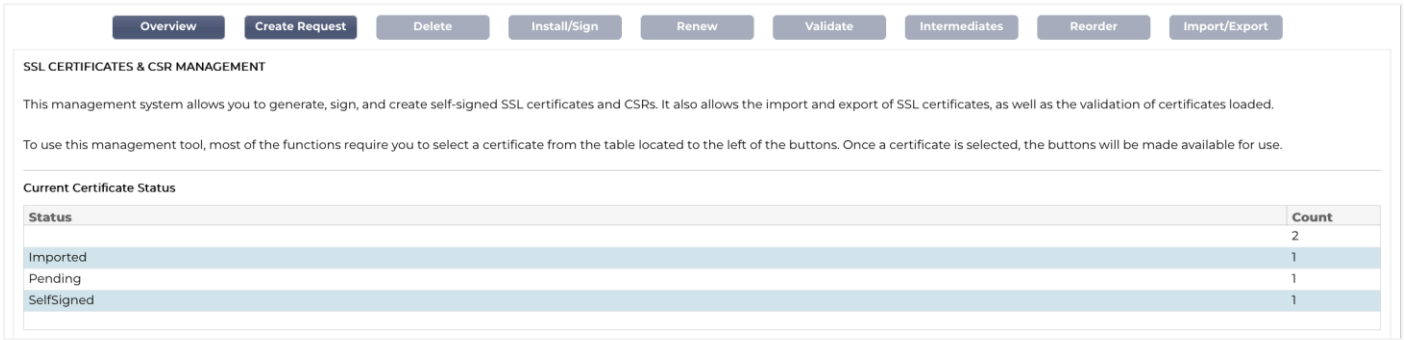
Farbcode	Bedeutung
	Das Zertifikat ist aktuell und hat noch mehr als 60 Tage bis zum Ablaufdatum
	Das Zertifikat wird in weniger als 30 Tagen ablaufen
	Das Zertifikat hat noch zwischen 30 und 60 Tagen Gültigkeit
	Das Zertifikat läuft in Kürze ab und hat noch <1 Tag Zeit
	Das Zertifikat ist abgelaufen

Zertifikat/CSR-Informationsanzeige

Wenn Sie auf ein Zertifikat oder eine CSR klicken, werden die entsprechenden Informationen im unteren Bereich angezeigt. Siehe Abbildung unten.

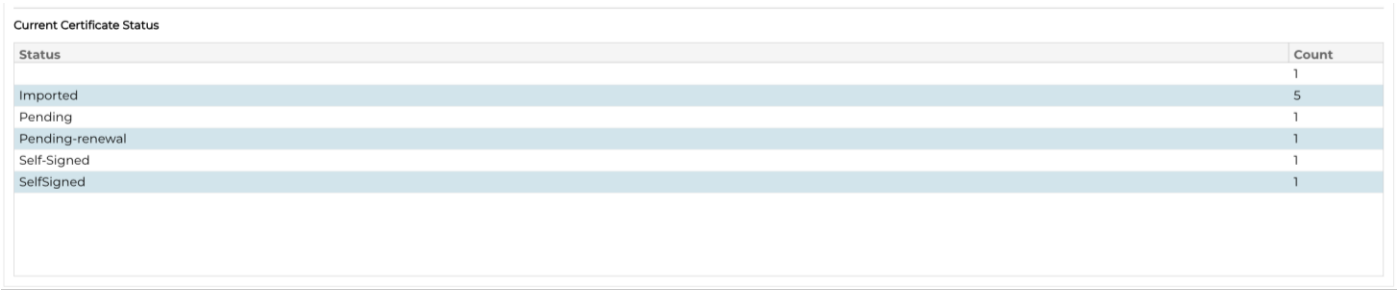


Die Aktionsschaltflächen und Konfigurationsbereiche



Es gibt eine Reihe von Aktionsschaltflächen, die verfügbar sind und ins Spiel kommen, wenn ein Zertifikat in der Liste ausgewählt wird.

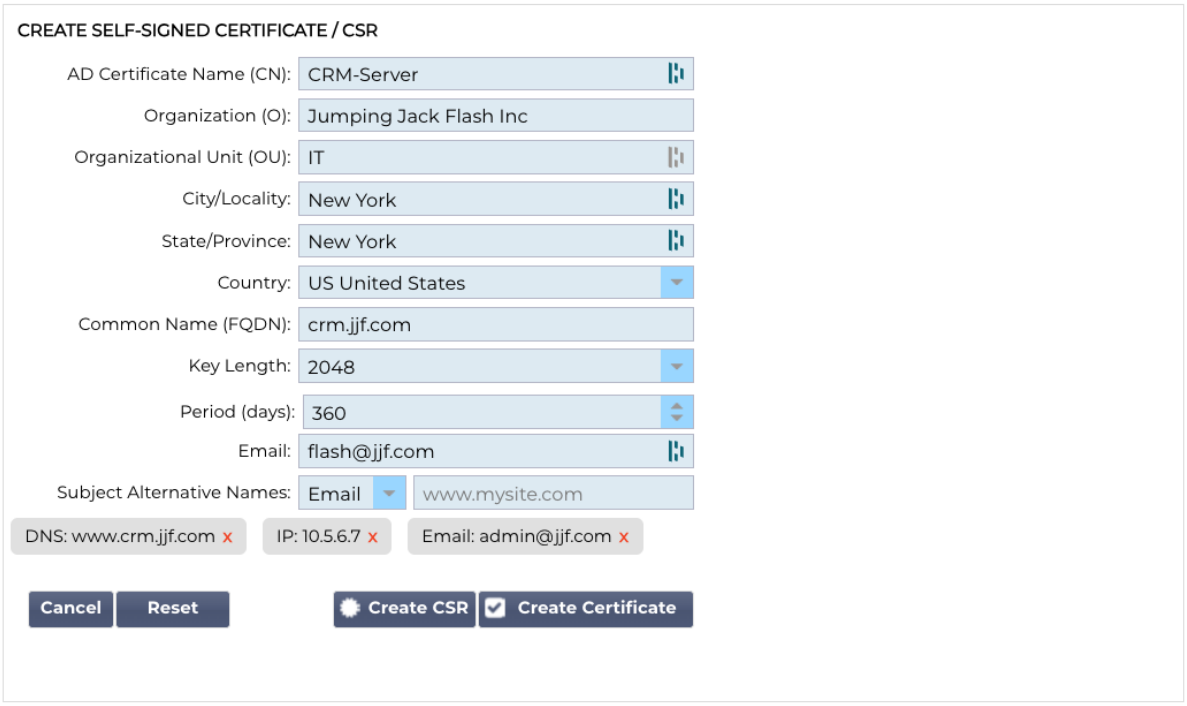
Übersicht



Die Schaltfläche Übersicht zeigt im unteren Bereich eine Gesamtsituation der Zertifikate an. Im Gegensatz zu anderen Aktionen ist die Schaltfläche "Übersicht" unabhängig und erfordert nicht die Auswahl eines Zertifikats.

Anfrage erstellen

Wenn Sie ein selbstsigniertes Zertifikat oder einen CSR erstellen möchten, müssen Sie auf die Schaltfläche Antrag erstellen klicken. Daraufhin wird ein allgemeines Eingabefeld angezeigt, in dem Sie alle erforderlichen Angaben machen können.



AD-Zertifikatsname (CN)

Dies ist ein beschreibendes Feld, das zur Anzeige des Namens der Bescheinigung in der ADC verwendet wird. Der Feldeintrag sollte alphanumerisch ohne Leerzeichen angegeben werden.

Organisation (O)

Dieses Feld wird verwendet, um den Namen der Organisation anzugeben, die das Zertifikat verwenden wird.

Organisatorische Einheit (OE)

Dies ist ein fakultatives Feld, das normalerweise zur Angabe der Abteilung oder Organisationseinheit verwendet wird.

Stadt/Gemeinde

Wie der Name schon sagt, geben die Benutzer in der Regel an, wo sich die Organisation befindet.

Staat/Provinz

Geben Sie in diesem Feld das Bundesland, den Bezirk oder die Provinz an.

Land

Dieses Feld ist obligatorisch und muss durch Auswahl des Landes, in dem das Zertifikat verwendet werden soll, ausgefüllt werden. Bitte stellen Sie sicher, dass die hier gemachten Angaben korrekt sind.

Allgemeiner Name (FQDN)

Dies ist ein wichtiges Feld, in dem der vollständig qualifizierte Domänenname (FQDN) des Servers/der Server angegeben wird, der/die durch das Zertifikat geschützt werden soll(en). Dies kann z. B. www.edgenexus.io, **edgenexus.io** oder sogar ein Platzhalter ***.edgenexus.io** sein. Sie können auch eine IP-Adresse verwenden, wenn Sie das Zertifikat an diese binden möchten.

Schlüssel Länge

Wird verwendet, um die Länge des Verschlüsselungsschlüssels für das SSL-Zertifikat anzugeben.

Zeitraum (Tage)

Die Länge der Zertifikatsgültigkeit in Tagen. Nach Ablauf dieser Frist ist das Zertifikat nicht mehr funktionsfähig.

E-Mail

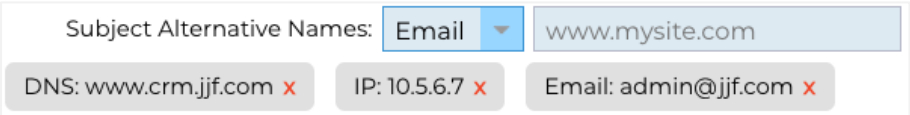
Dies ist die administrative E-Mail-ID, die für das Zertifikat verwendet wird.

Thema alternative Namen (SAN)

Subject Alternative Name (SAN) ist eine Erweiterung von SSL-Zertifikaten, mit der mehrere Domainnamen unter einem einzigen Zertifikat geschützt werden können. Diese Funktion ist besonders nützlich für die Absicherung von Websites mit mehreren Subdomains oder verschiedenen Domainnamen und ermöglicht einen schlankeren und kostengünstigeren Ansatz für die SSL-Verwaltung. Durch die Einbeziehung von SANs kann ein einziges SSL-Zertifikat eine Vielzahl von Domainnamen und Subdomains abdecken, wodurch die Notwendigkeit einzelner Zertifikate für jede Webadresse entfällt, was den Prozess der Sicherung der Webkommunikation vereinfacht und die Datenverschlüsselung über verschiedene Domains hinweg gewährleistet.

Dieses Feld besteht aus zwei Elementen, einem Dropdown-Feld, das die Auswahl des SAN-Typs ermöglicht, und einem Textfeld zur Angabe des Wertes.

Der EdgeADC verfügt über die folgenden SANs, die verwendet werden können: DNS, IP-Adresse, Email-Adresse und URI. Sie können mehrere SANs für ein Zertifikat oder eine CSR auswählen und angeben.



Festgelegte SANs können durch Klicken auf das rote **x** in jedem SAN-Wert entfernt werden.

- **DNS** - Mit dem DNS Subject Alternate Name (SAN) können Sie zusätzliche Domainnamen angeben, für die das Zertifikat gültig ist. Im Gegensatz zum Feld Common Name (CN), das nur eine Domäne zulässt, kann das SAN-Feld mehrere Domänennamen enthalten, was Flexibilität und Skalierbarkeit bei der Zertifikatsverwaltung bietet. Dies ist besonders nützlich für Organisationen, die mehrere Dienste in verschiedenen Domains und

Subdomains hosten, da sie die Kommunikation für alle diese Einheiten unter einem einzigen SSL/TLS-Zertifikat sichern können, was die Verwaltung vereinfacht und die Sicherheit verbessert.

- **IP-Adresse** - Der IP Subject Alternative Name (SAN) ermöglicht die Einbeziehung von IP-Adressen neben Domainnamen als durch das Zertifikat geschützte Einheiten. Diese Funktion ist entscheidend für die Absicherung des direkten Zugriffs auf Dienste über IP-Adressen und stellt sicher, dass verschlüsselte Verbindungen auch dann aufgebaut werden können, wenn der Zugriff auf einen Server nicht über seinen Domainnamen, sondern direkt über seine IP-Adresse erfolgt. Durch die Integration von IP-SANs können Unternehmen die Sicherheit ihres Netzwerks erhöhen, indem sie die SSL/TLS-Verschlüsselung sowohl für die domänenbasierte als auch für die IP-basierte Kommunikation aktivieren, was sie vielseitig für Umgebungen einsetzbar macht, in denen Domänennamen für den Zugriff auf interne Ressourcen oder bestimmte Dienste möglicherweise nicht verwendet oder bevorzugt werden.
- **E-Mail-Adresse** - Mit dem Subject Alternative Name (SAN) für die E-Mail-Adresse können Sie zusätzliche E-Mail-Adressen angeben, die mit dem Zertifikat verknüpft werden sollen, neben der primären Domäne oder Entität, für die es ausgestellt wurde. Dadurch kann das Zertifikat die Identität des Ausstellers für mehrere E-Mail-Adressen validieren, nicht nur für eine einzelne Domäne oder einen Common Name (CN). Es ist besonders nützlich in Szenarien, in denen eine sichere E-Mail-Kommunikation für verschiedene E-Mail-Adressen unter derselben Organisation oder Einrichtung erforderlich ist, um sicherzustellen, dass der verschlüsselte E-Mail-Austausch authentifiziert und mit der durch das Zertifikat verifizierten Identität des Ausstellers verknüpft ist. Dies macht das Email Address SAN zu einer Schlüsselfunktion für die Verbesserung der Sicherheit und Vertrauenswürdigkeit der E-Mail-Kommunikation in einem verschlüsselten Rahmen.
- **URI** - Das URI-SAN (Uniform Resource Identifier) wird verwendet, um zusätzliche Identitäten anzugeben, die durch URIs für eine einzelne durch das Zertifikat gesicherte Entität repräsentiert werden. Im Gegensatz zu herkömmlichen SAN-Einträgen, die in der Regel Domänennamen (DNS-Namen) oder IP-Adressen enthalten, ermöglicht ein URI-SAN dem Zertifikat, die Entität mit spezifischen URIs zu verknüpfen, z. B. mit einer URL zu einer bestimmten Ressource oder einem Dienstendpunkt. Dies ermöglicht eine flexiblere und präzisere Identifizierung, so dass sichere Verbindungen mit bestimmten Ressourcen oder Diensten innerhalb einer Domäne hergestellt werden können, anstatt nur die Domäne selbst zu sichern, wodurch die Granularität und der Anwendungsbereich von SSL/TLS-Zertifikaten verbessert werden.

Nach dem korrekten Ausfüllen können Sie wählen, ob Sie eine Zertifikatsignierungsanforderung (CSR) erstellen und diese zur Signierung durch eine Zertifizierungsstelle senden oder ein selbstsigniertes Zertifikat zur sofortigen Verwendung erstellen möchten.

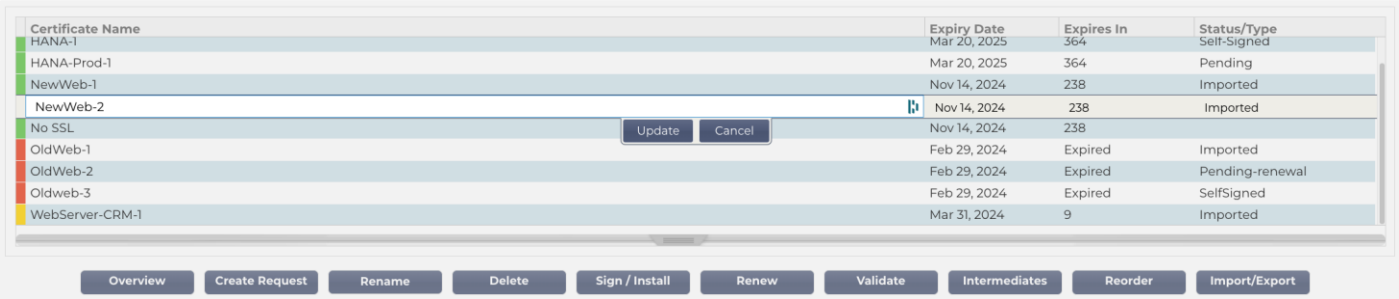
Mit der Schaltfläche Abbrechen wird die gesamte Anfrage abgebrochen, während die Schaltfläche Zurücksetzen alle Felder zurücksetzt.

Umbenennen

Mit der Schaltfläche Umbenennen können Sie Zertifikate umbenennen, die nicht für virtuelle Dienste verwendet werden.

Um diese Funktion zu nutzen:

- Klicken Sie auf das Zertifikat, das Sie umbenennen möchten, und klicken Sie auf die Schaltfläche Umbenennen.
- Die Zertifikatszeile ändert sich und Sie können ihren Namen ändern.

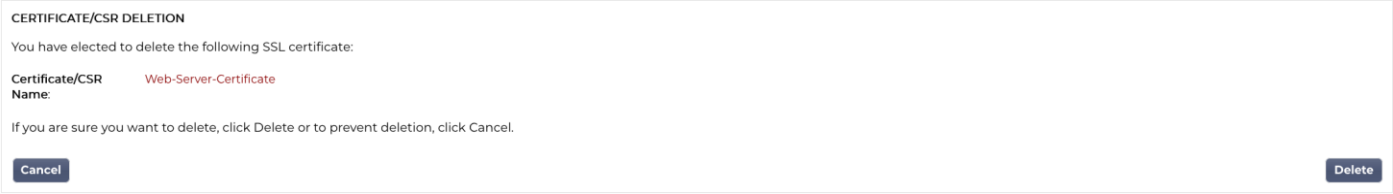


- Wenn Sie fertig sind, klicken Sie auf die Schaltfläche Aktualisieren.

- Sie können auch auf das Zertifikat doppelklicken, um es umzubenennen.

Löschen

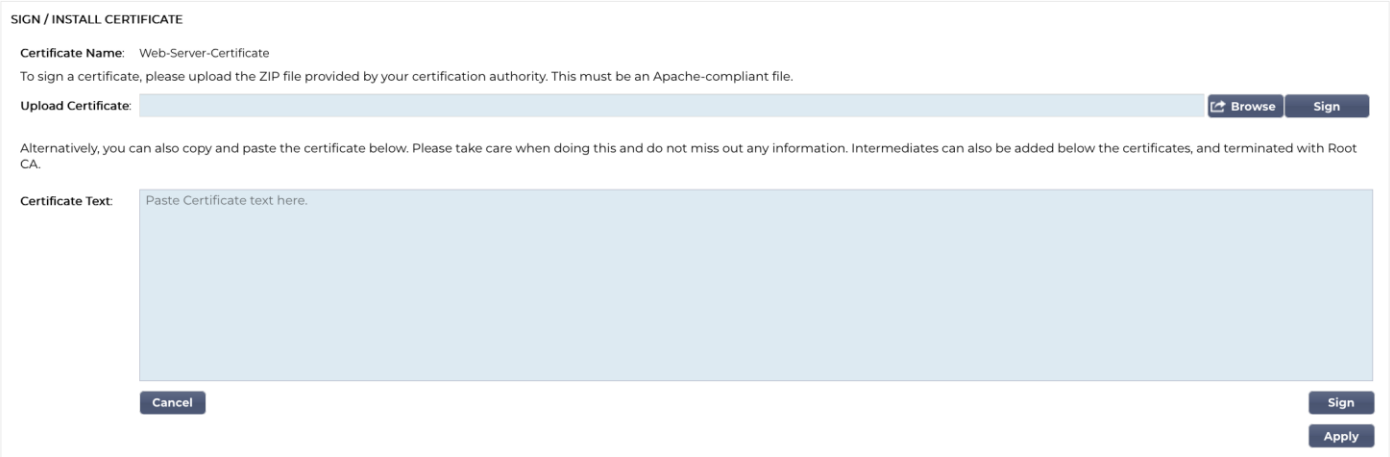
Die Schaltfläche Löschen ist nur verfügbar, wenn ein Zertifikat ausgewählt ist. Wenn Sie darauf klicken, wird der folgende Inhalt angezeigt



Im unteren Fensterbereich wird der Löschantrag zusammen mit dem Namen des Zertifikats angezeigt, für das die Löschung beantragt wurde.

Klicken Sie auf die Schaltfläche Löschen unten rechts im Fenster, um mit dem Löschen fortzufahren.

Installieren/Zeichnen



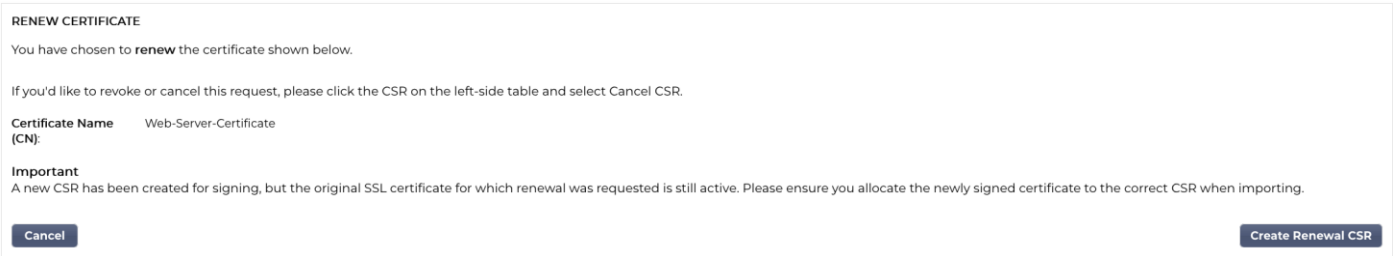
Wenn Sie eine CSR erstellen und den Antrag von einer Zertifizierungsstelle (CA) signieren lassen möchten, senden Sie die CSR an die CA. Im Gegenzug sendet die Zertifizierungsstelle das signierte Zertifikat zusammen mit der Datei des privaten Schlüssels und allen Zwischenprodukten, die für die ordnungsgemäße Funktion des Zertifikats erforderlich sind.

Möglicherweise erhalten Sie eine ZIP-Datei mit allen erforderlichen Elementen, die Sie dann im oberen Teil des rechten Fensters hochladen können.

Alternativ können Sie den Zertifikatssatz auch in einem Texteditor erstellen und den Inhalt in das Feld Zertifikatstext im unteren Bereich des Fensters einfügen.

Wenn Sie eine der beiden Methoden verwendet haben, klicken Sie auf die Schaltfläche Signieren und dann auf die Schaltfläche Übernehmen. Das signierte Zertifikat wird nun im linken Fensterbereich angezeigt.

Erneuern Sie



Wenn ein Zertifikat nach Ablauf seiner Gültigkeitsdauer abläuft, können Sie es mit der Schaltfläche Erneuern verlängern und erneuern. Es gibt zwei Arten der Erneuerung.

Selbstsignierte Zertifikate

Selbstsignierte Zertifikate können im Gegensatz zu vertrauenswürdigen Zertifikaten nicht mit einer CSR erneuert werden. Stattdessen wird das selbstsignierte Zertifikat erneuert, indem eine neue Konfiguration unter Verwendung der vorhandenen Daten vorgelegt wird. Der Benutzer kann dann einen neuen Namen für das Zertifikat zusammen mit einem neuen Ablaufwert für das Zertifikat angeben.

Sobald dies geschehen ist, wird das neue selbstsignierte Zertifikat erstellt und im Zertifikatsspeicher gespeichert. Es liegt dann in der Verantwortung des Administrators, dafür zu sorgen, dass die virtuellen Dienste, die das Zertifikat verwenden, rechtzeitig neu konfiguriert werden.

Vertrauenswürdige signierte Zertifikate

Wenn es um vertrauenswürdige Zertifikate geht, die von einer Zertifizierungsstelle unterzeichnet sind, wird die Verwendung von CSRs übernommen.

Wenn Sie im oberen Bereich auf ein auslaufendes Zertifikat klicken und auf Erneuern klicken, wird Ihnen eine neue CSR mit den aktuellen Zertifikatsdetails angezeigt. Die CSR kann dann heruntergeladen und der Zertifizierungsstelle zum Signieren vorgelegt werden, woraufhin das signierte Zertifikat installiert werden kann.

Das Zertifikat, dessen Erneuerung Sie beantragt hatten, erhält den neuen Status "Erneuern". Sobald das signierte Zertifikat installiert ist, werden Sie aufgefordert, dem Zertifikat einen neuen Namen zuzuweisen. Dieser wird dann als vertrauenswürdig angezeigt. Das ursprüngliche Zertifikat wird beibehalten und alle Dienste, die es verwenden, sollten so schnell wie möglich für die Verwendung des neuen Zertifikats konfiguriert werden.

Zertifikat validieren

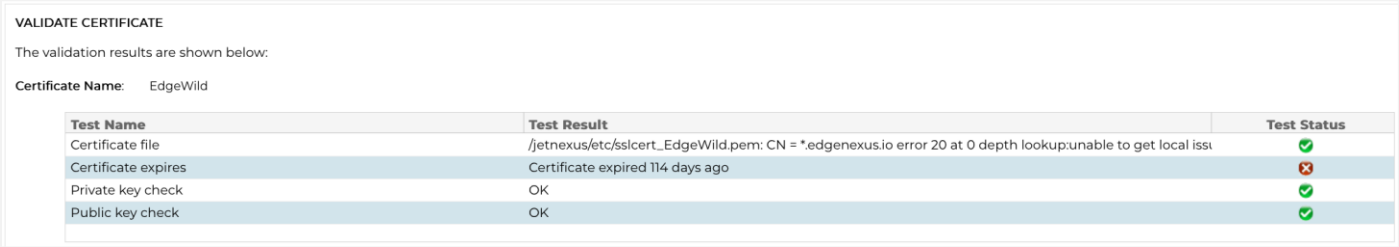
Ein SSL-Zertifikat besteht aus mehreren Teilen, und es ist wichtig, dass diese Teile nicht nur vorhanden sind, sondern auch in der richtigen Reihenfolge vorliegen. Die Gründe für die Validierung von SSL-Zertifikaten, die von Drittanbietern stammen, sind im Folgenden aufgeführt.

- **Authentifizierung**: Die Validierung stellt sicher, dass das Zertifikat von einer vertrauenswürdigen Stelle stammt und die Identität der Website oder des Servers überprüft. Dies hilft dabei, Man-in-the-Middle-Angriffe zu verhindern, bei denen ein Angreifer die Kommunikation zwischen einem Client und einem Server abfangen könnte.
- **Integrität**: Durch die Validierung eines SSL-Zertifikats können Sie sicherstellen, dass das Zertifikat nicht verfälscht oder verändert wurde. Dies ist entscheidend für die Aufrechterhaltung der Integrität der sicheren Verbindung.
- **Überprüfung der Vertrauenskette**: SSL-Zertifikate werden von Zertifizierungsstellen (CAs) ausgestellt. Bei der Validierung eines Zertifikats wird unter anderem überprüft, ob es zu einer vertrauenswürdigen Stammzertifizierungsstelle zurückverfolgt werden kann. Dieses Verfahren stellt sicher, dass das Zertifikat legitim ist und man ihm vertrauen kann.
- **Status der Sperrung**: Während der Validierung ist es auch wichtig zu prüfen, ob das SSL-Zertifikat von der ausstellenden Zertifizierungsstelle widerrufen wurde. Ein Zertifikat kann widerrufen werden, wenn es fälschlicherweise ausgestellt wurde, der private Schlüssel der Website kompromittiert wurde oder die Website das Zertifikat nicht mehr benötigt. Der Import eines widerrufenen Zertifikats kann zu Sicherheitslücken führen.
- **Ablaufprüfung**: SSL-Zertifikate sind für einen bestimmten Zeitraum gültig. Bei der Validierung eines Zertifikats beim Import wird auch das Ablaufdatum überprüft, um sicherzustellen, dass es noch gültig ist. Die Verwendung eines abgelaufenen Zertifikats kann zu Sicherheitslücken führen und Browser oder Clients dazu veranlassen, die sichere Verbindung abzulehnen.
- **Konfiguration und Kompatibilität**: Die Validierung stellt sicher, dass die Konfiguration des Zertifikats mit den Sicherheitsrichtlinien des Kunden und den technischen Anforderungen des Servers oder der Anwendung kompatibel ist. Dazu gehören die Überprüfung der verwendeten Algorithmen, der Zweck des Zertifikats und andere technische Details.

- **Einhaltung von Vorschriften**: In bestimmten Branchen kann die Validierung von SSL-Zertifikaten vorgeschrieben sein, um den sicheren Umgang mit sensiblen Daten zu gewährleisten. Dies ist besonders wichtig in Bereichen wie Finanzen, Gesundheitswesen und E-Commerce.

Das SSL-Verwaltungssystem der OEZA ermöglicht die Validierung eines importierten SSL-Zertifikats.

- Wählen Sie ein SSL-Zertifikat, das Sie importiert haben.
- Klicken Sie auf die Schaltfläche Validieren.
- Die Ergebnisse sind im unteren Feld zu sehen, wie in der folgenden Abbildung dargestellt.

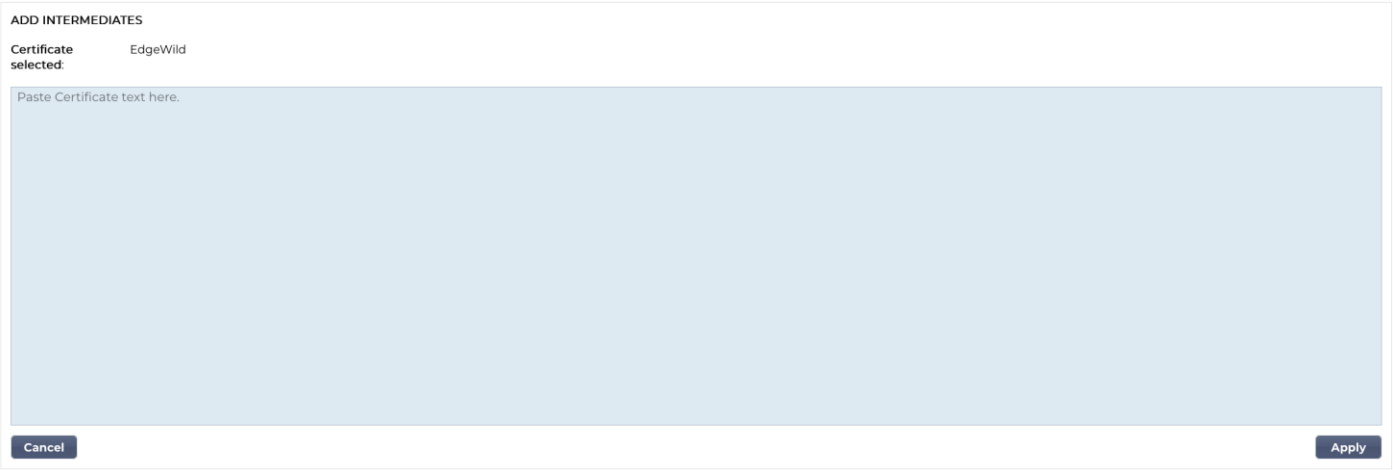


Hinzufügen von Zwischenprodukten

Wie bereits erwähnt, bestehen SSL-Zertifikate aus mehreren Teilen, von denen einer die Zwischenzertifikate sind, aus denen sich die gesamte Kette zusammensetzt.

Der SSL-Manager im ADC ermöglicht es Ihnen, fehlende Zwischenzertifikate hinzuzufügen.

- Klicken Sie auf das SSL, zu dem Sie das Zwischenzertifikat hinzufügen möchten.
- Klicken Sie auf die Schaltfläche Intermediates.
- Es wird ein Panel angezeigt, das dem untenstehenden Bild ähnelt.



- Fügen Sie den Inhalt des Zwischenzertifikats ein.
- Klicken Sie auf Anwenden.

Es kann vorkommen, dass Sie die Reihenfolge der Zwischenzertifikate ändern müssen, damit das SSL-Zertifikat korrekt validiert wird. Dies geschieht über die Schaltfläche Neu anordnen.

Nachbestellung

Damit ein SSL-Zertifikat korrekt funktioniert, muss es in der richtigen Reihenfolge vorliegen.

Die goldene Regel lautet, dass das Zertifikat des Absenders an erster Stelle und das endgültige Stammzertifikat an letzter Stelle in der Kette stehen muss. Im Allgemeinen sieht dies in etwa so aus wie in der folgenden Darstellung:

```
Ursprünglicher Emittent > Zwischenstufe 1 > Endgültige Wurzel.
```

Die endgültige Wurzel ist ein vertrauenswürdiges Stammzertifikat, das von einer Zertifizierungsstelle bereitgestellt wird.

In manchen Fällen gibt es mehrere Zwischenzertifikate, die ebenfalls an der richtigen Stelle platziert werden müssen. Im Wesentlichen muss jedes nachfolgende Zertifikat das vorangehende bestätigen. Es könnte also folgendermaßen aussehen.

```
Ursprünglicher Emittent > Zwischenstufe 1 > Endgültige Wurzel
```

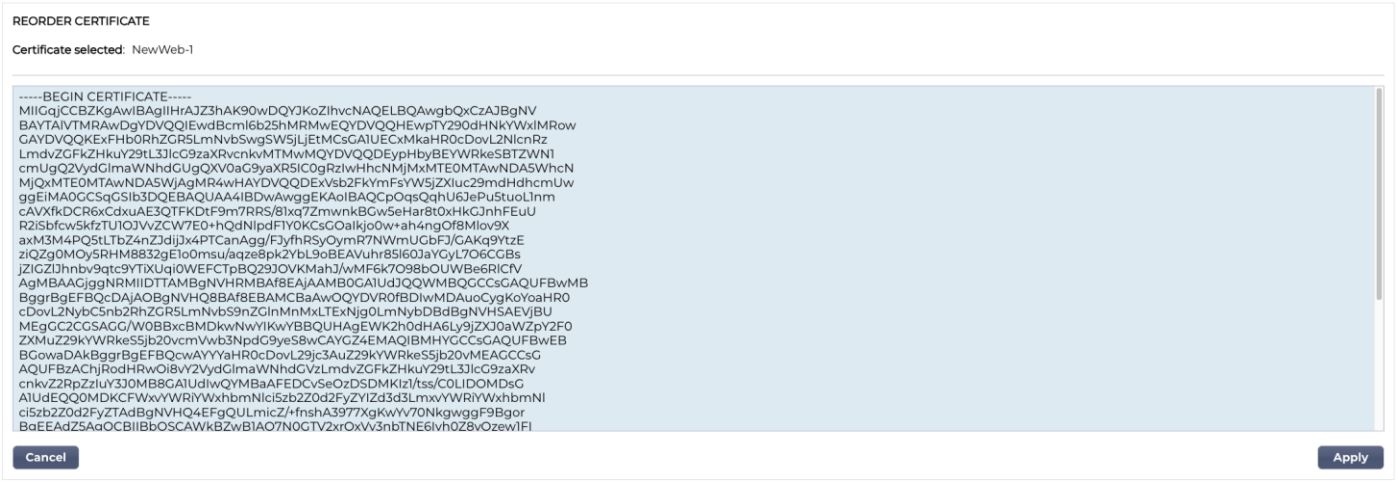
Wenn Sie z. B. Zwischenprodukt 2 importieren, könnte dieses am Ende der Kette stehen, was bedeuten würde, dass die Zertifizierung nicht gültig ist. Daher ist es notwendig, die Kette neu zu ordnen und Zwischenprodukt 2 an die richtige Stelle zu setzen (rot dargestellt).

Die endgültige Fassung würde also so aussehen:

```
Ursprünglicher Emittent > Zwischenhändler 1 > Zwischenhändler 2 >  Endgültige Wurzel
```

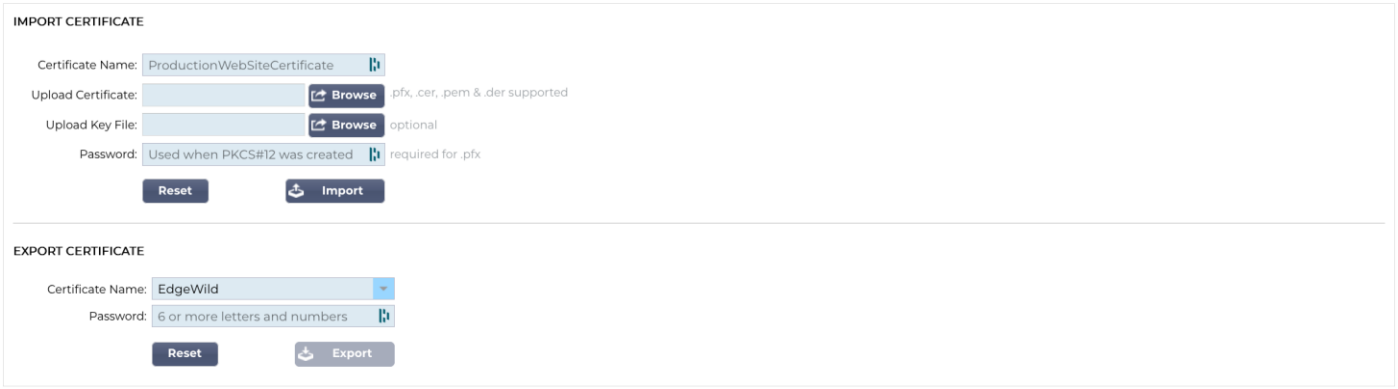
```
-----BEGIN CERTIFICATE-----
MIIFKTCCBBGgAwIBAgISA/UUyBjJ71fucZuvpiLsdfsfsdfsdfd
...
hoFWWJt3/SeBKn+ci03RRvZsdfdsfsdfw=
-----END BESCHEINIGUNG-----
-----BEGIN CERTIFICATE-----
MIIFFjCCAv6gAwIBAgIRAJErCErPDBinsdfsfsdfsdfdsfsdfsd
....
nLRbwHqsdqD7hHwg==
-----END BESCHEINIGUNG-----
-----BEGIN CERTIFICATE-----
MIIFYDCCBsdfSDFSDFVSDVzfsdffvqdsfgsT664ScbvsfGDGSDV
...
Dfvp7OOGAN6dEOM4+SDFSDZET+DFGDFQSD45Bddfghqsqf6Bsff
-----END BESCHEINIGUNG-----
-----BEGIN CERTIFICATE-----
MIIFYDCCBsdfSDFSDFVSDVzfsdffvqdsfgsT664ScbvsfGDGSDV
...
Dfvp7OOGAN6dEOM4+SDFSDZET+DFGDFQSD45Bddfghqsqf6Bsff
-----END BESCHEINIGUNG-----
```

Der Abschnitt "Neu bestellen" sieht wie in der folgenden Abbildung aus, wenn Sie ein Zertifikat auswählen und auf die Schaltfläche "Neu bestellen" klicken.



Um die Abschnitte des Zertifikats neu anzuordnen, können Sie den Text im Feld kopieren, den Inhalt in einem Texteditor bearbeiten und neu anordnen und dann wieder einfügen, um den bestehenden Inhalt zu ersetzen. Klicken Sie anschließend auf die Schaltfläche Übernehmen.

Import/Export



Wenn Sie ein Zertifikat von Ihrem SSL-Zertifikatsanbieter erhalten, wird es in Form einer ZIP-Datei oder eines Satzes von Dateien geliefert. Diese enthalten das SSL-Zertifikat, die Schlüsseldatei und die Root-Ca sowie alle Zwischenprodukte

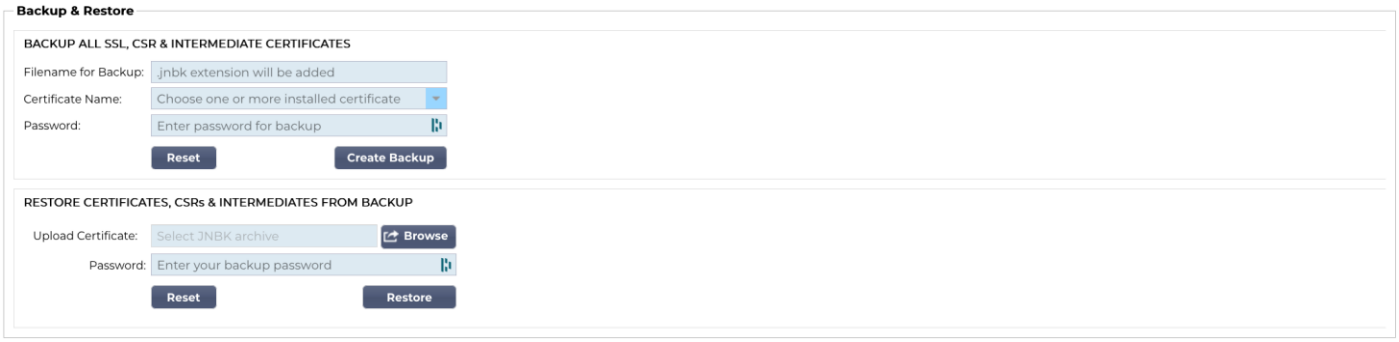
Sie müssen sie in die ADC importieren, und deshalb haben wir eine Methode bereitgestellt, um sie zu importieren.

Es gibt eine Reihe von Formaten für SSL-Zertifikate wie CER, DER, PEM und PFX. Einige Formate erfordern eine KEY-Datei, die dem Importvorgang hinzugefügt werden muss. PFX-Dateien erfordern das Passwort, um das PFX-Zertifikat zu importieren.

Wir haben auch die Möglichkeit vorgesehen, bei Bedarf eine Bescheinigung aus dem ADC zu exportieren. Beim Export wird die Datei im PFX-Format erstellt und erfordert daher ein Kennwort für die Erstellung des Exports.

Sichern und Wiederherstellen

Sicherung



Um die Zertifikate im Zertifikatspeicher des ADC zu sichern:

- Fügen Sie einen Dateinamen hinzu, der für die Sicherung verwendet werden soll.
- Verwenden Sie das Dropdown-Menü, um ein einzelnes Zertifikat auszuwählen, oder ALL, um alle Zertifikate zu sichern.
- Ein Passwort hinzufügen
- Klicken Sie auf die Schaltfläche Backup erstellen.
- Die erstellte Datei ist eine JNBK-Datei, die verschlüsselt ist.

WICHTIG

Die Sicherung funktioniert nur mit importierten vertrauenswürdigen Zertifikaten.

Wiederherstellen

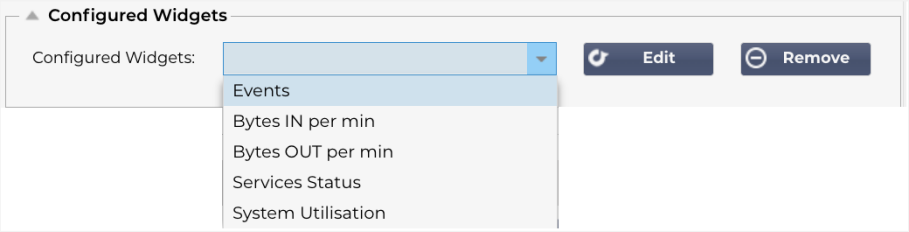
Wenn Sie die Sicherung wiederherstellen möchten, verwenden Sie den unteren Bereich des Abschnitts Sicherung und Wiederherstellung.

- Navigieren Sie zu der Sicherungsdatei und suchen Sie sie.
- Geben Sie das Passwort ein.
- Klicken Sie auf die Schaltfläche Wiederherstellen.
- Die Zertifikate in der Sicherungsdatei werden wiederhergestellt.

Widgets

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

Konfigurierte Widgets

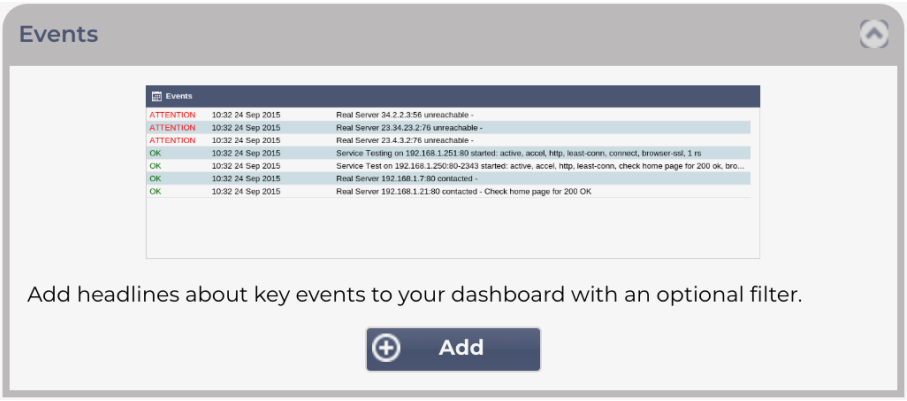


Im Abschnitt "Konfigurierte Widgets" können Sie alle Widgets anzeigen, bearbeiten oder entfernen, die im Abschnitt "Verfügbare Widgets" erstellt wurden.

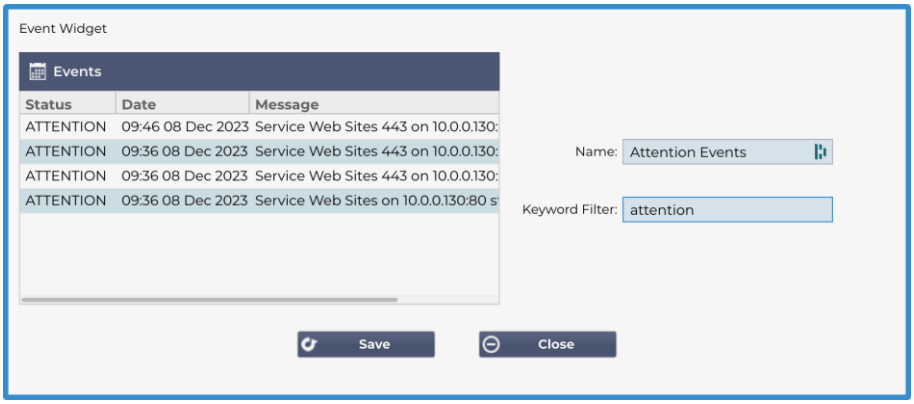
Verfügbare Widgets

Die ADC bietet fünf verschiedene Widgets, die Sie nach Ihren Wünschen konfigurieren können.

Das Veranstaltungs-Widget

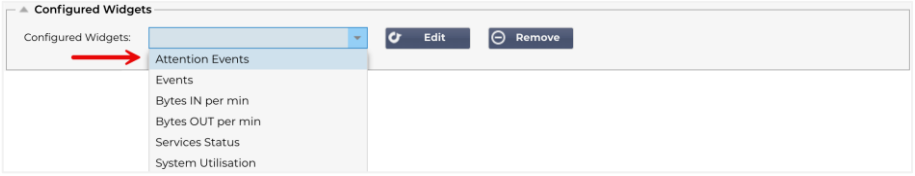


- Um ein Ereignis zum Ereignis-Widget hinzuzufügen, klicken Sie auf die Schaltfläche Hinzufügen.
- Geben Sie einen Namen für Ihr Ereignis ein. In unserem Beispiel haben wir "Attention Events" als Namen für das Ereignis angegeben.
- Fügen Sie einen Schlüsselwortfilter hinzu. Wir haben auch den Filterwert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



- Klicken Sie auf Speichern und dann auf Schließen.

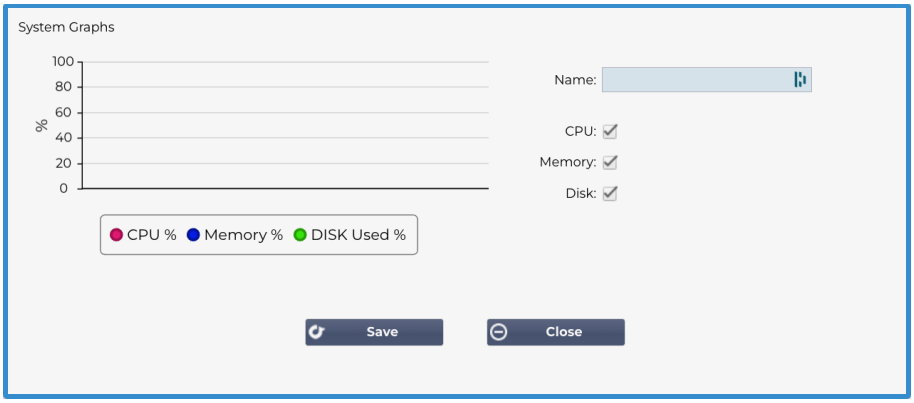
- Sie sehen nun ein zusätzliches Widget namens Aufmerksamkeitsereignisse in der Dropdown-Liste der konfigurierten Widgets.



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

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

Das Systemgrafik-Widget

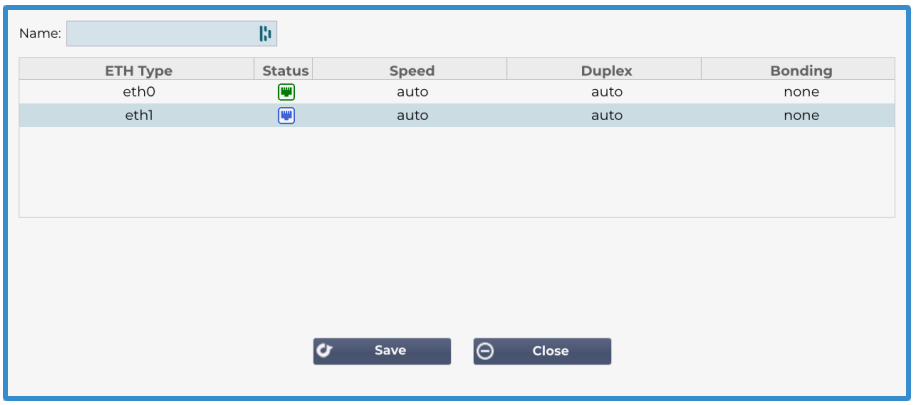


Der ADC verfügt über ein konfigurierbares Systemgrafik-Widget. Durch Klicken auf die Schaltfläche Hinzufügen des Widgets können Sie die folgenden Überwachungsgrafiken zur Anzeige hinzufügen.

- CPU
- SPEICHER
- DISK

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

Interface Widget



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

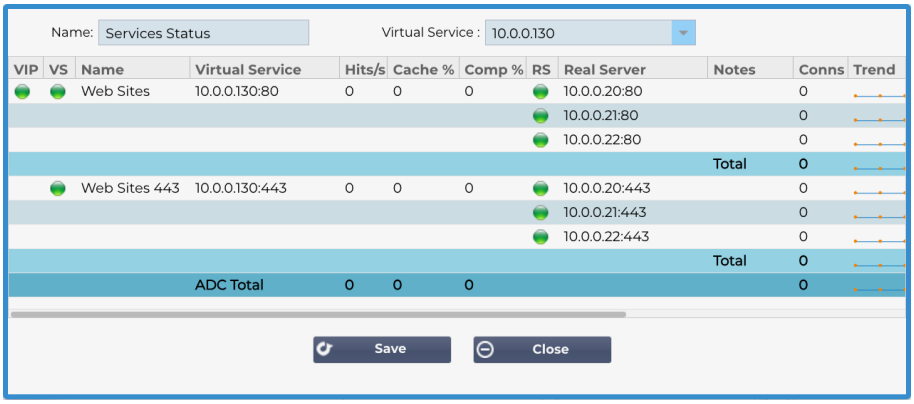
Wenn Sie fertig sind, klicken Sie auf die Schaltfläche Speichern und dann auf die Schaltfläche Schließen.

Wählen Sie das Widget, das Sie gerade angepasst haben, aus dem Dropdown-Menü des Dashboards aus. Sie sehen dann einen Bildschirm wie den unten abgebildeten.

Status-Widget

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

- Klicken Sie auf Hinzufügen.



- Geben Sie einen Namen für den Dienst ein, den Sie überwachen möchten
- Sie können auch auswählen, welche Spalten Sie im Widget anzeigen möchten, indem Sie auf die Spaltenüberschrift klicken.
- Wenn Sie zufrieden sind, klicken Sie auf Speichern und anschließend auf Schließen.
- Das ausgewählte Status-Widget wird im Abschnitt Dashboard verfügbar sein.

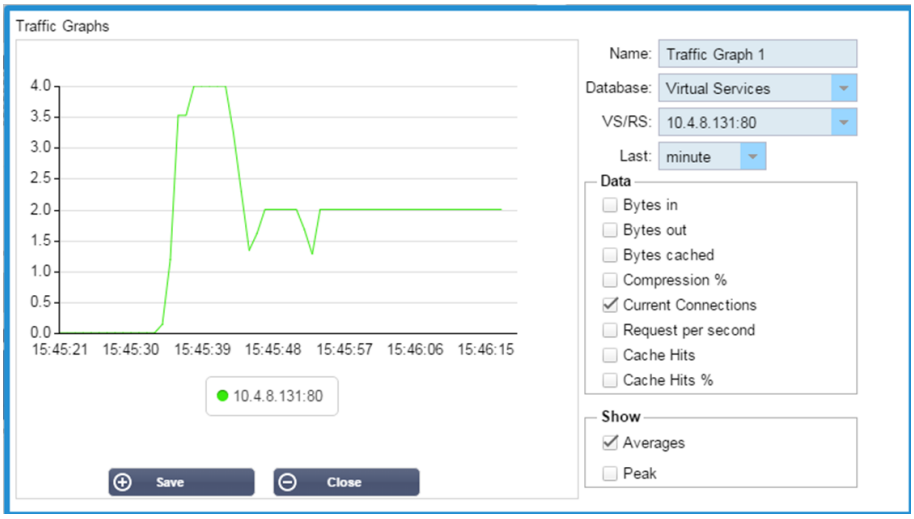
Verkehrsgrafik-Widget

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

- 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 Zeitraum aus der Dropdown-Liste Letzte.
    - Minute - letzte 60s
    - Stunde - aggregierte Daten von jeder Minute für die letzten 60 Minuten
    - Tag - aggregierte Daten aus jeder Stunde für die letzten 24 Stunden
    - Woche - aggregierte Daten von jedem Tag der vorangegangenen sieben Tage
    - Monat - aggregierte Daten aus jeder Woche für die letzten sieben Tage
    - Jahr - aggregierte Daten aus jedem Monat der letzten 12 Monate
- Wählen Sie die verfügbaren Daten je nach der von Ihnen gewählten 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 %.
    - Dienstleistungen 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-Verkehrsdiagramm



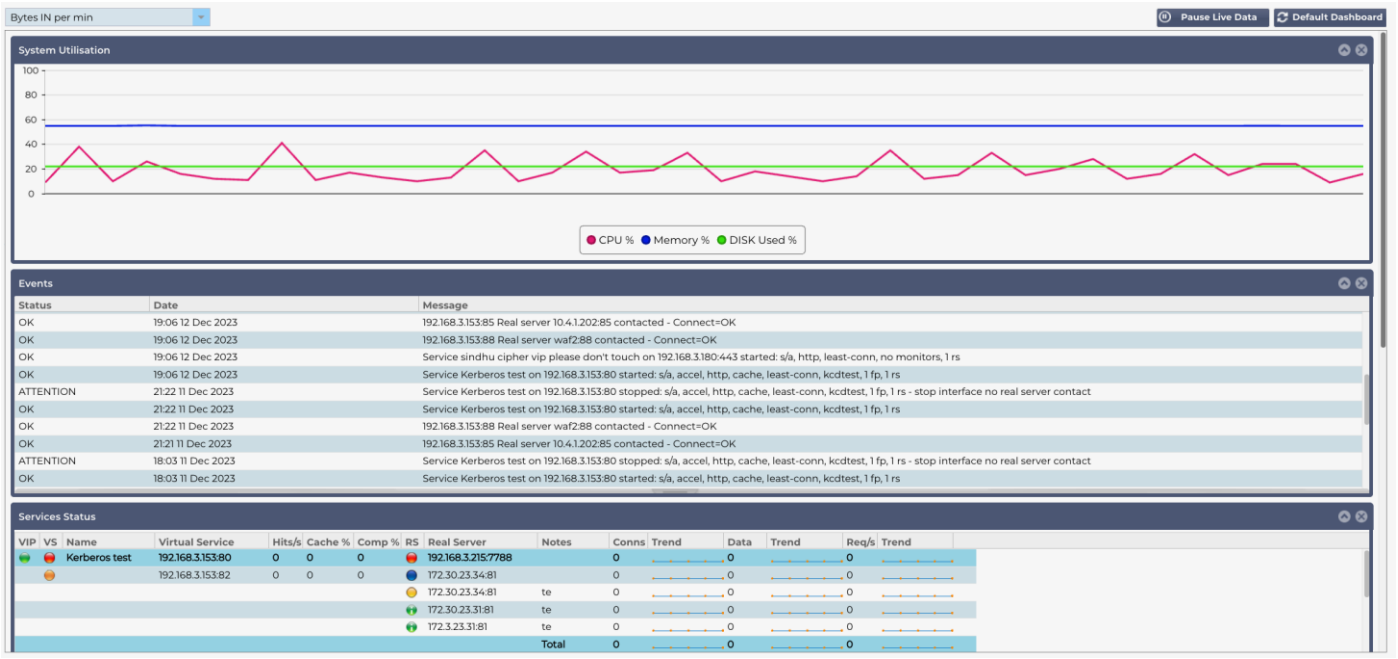
Sie können nun Ihr Verkehrsdiagramm-Widget zur Ansicht> Dashboard hinzufügen.

Siehe

Dashboard

Wie bei allen Schnittstellen zur Verwaltung von IT-Systemen kommt es immer wieder vor, dass Sie die Leistungskennzahlen und Daten, die die ADC verarbeitet, einsehen müssen. Wir bieten Ihnen ein anpassbares Dashboard, mit dem Sie dies auf einfache und aussagekräftige Weise tun können.

Das Dashboard ist über das Segment "Ansicht" im Navigationsbereich erreichbar. Wenn es ausgewählt ist, zeigt es mehrere Standard-Widgets an und ermöglicht Ihnen 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 Standard-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. Wählen Sie dazu das Widget aus der Dropdown-Liste aus.

Schaltfläche "Live-Daten anhalten

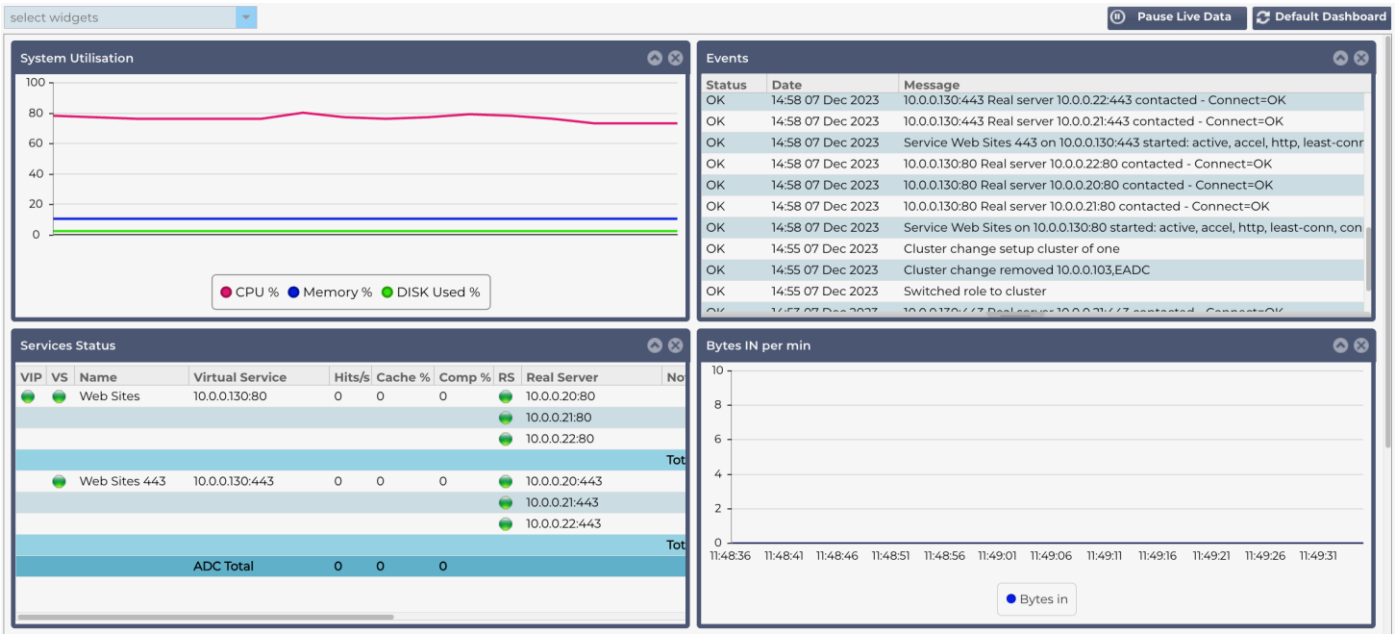
Mit dieser Schaltfläche können Sie auswählen, ob die ADC das Dashboard in Echtzeit aktualisieren soll. Nach dem Anhalten wird kein Dashboard-Widget aktualisiert, so dass Sie den Inhalt in aller Ruhe prüfen können. Die Schaltfläche ändert ihren Status und zeigt Live-Daten wiedergeben an, sobald eine Pause eingeleitet wird.

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

Standard-Schaltfläche für das Armaturenbrett

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

Ändern der Größe, Minimieren, Umsortieren und Entfernen von Widgets



Größe eines Widgets ändern

Sie können die Größe eines Widgets ganz einfach ändern. Klicken Sie auf die Titelleiste des Widgets, halten Sie sie gedrückt und ziehen Sie es an die linke oder rechte Seite des Dashboardbereichs. Es wird ein gepunktetes Rechteck angezeigt, das die neue Größe des Widgets darstellt. Ziehen Sie das Widget in das Rechteck und lassen Sie die Maustaste los. Wenn Sie ein Widget mit geänderter Größe neben einem zuvor geänderten Widget ablegen möchten, wird das Rechteck neben dem Widget angezeigt, neben dem Sie es ablegen möchten.

Ein Widget minimieren

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

Verschieben der Widget-Reihenfolge

Um ein Widget zu verschieben, klicken Sie auf die Titelleiste, halten Sie sie gedrückt und bewegen Sie die Maus.

Ein Widget entfernen

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

Geschichte

Mit der Option "Verlauf", die über den Navigator ausgewählt werden kann, kann der Administrator die historische Leistung des ADC untersuchen. Historische Ansichten können für Virtual Services, Real Servers und System erstellt werden.

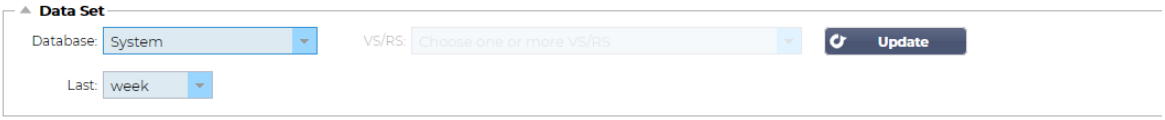
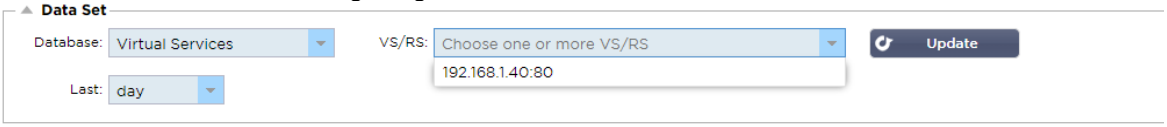
Außerdem können Sie so den Lastausgleich in Aktion sehen und Fehler oder Muster erkennen, die untersucht werden müssen. Beachten Sie, dass Sie die Verlaufsprotokollierung unter System > Verlauf aktivieren müssen, um diese Funktion nutzen zu können.

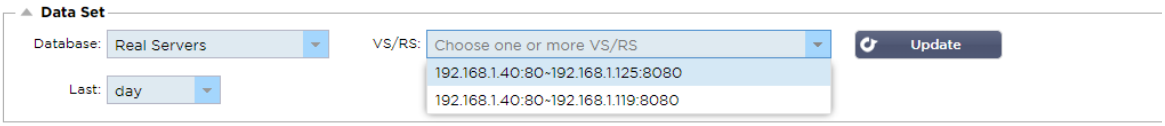
Anzeigen von grafischen Daten

Datensatz

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

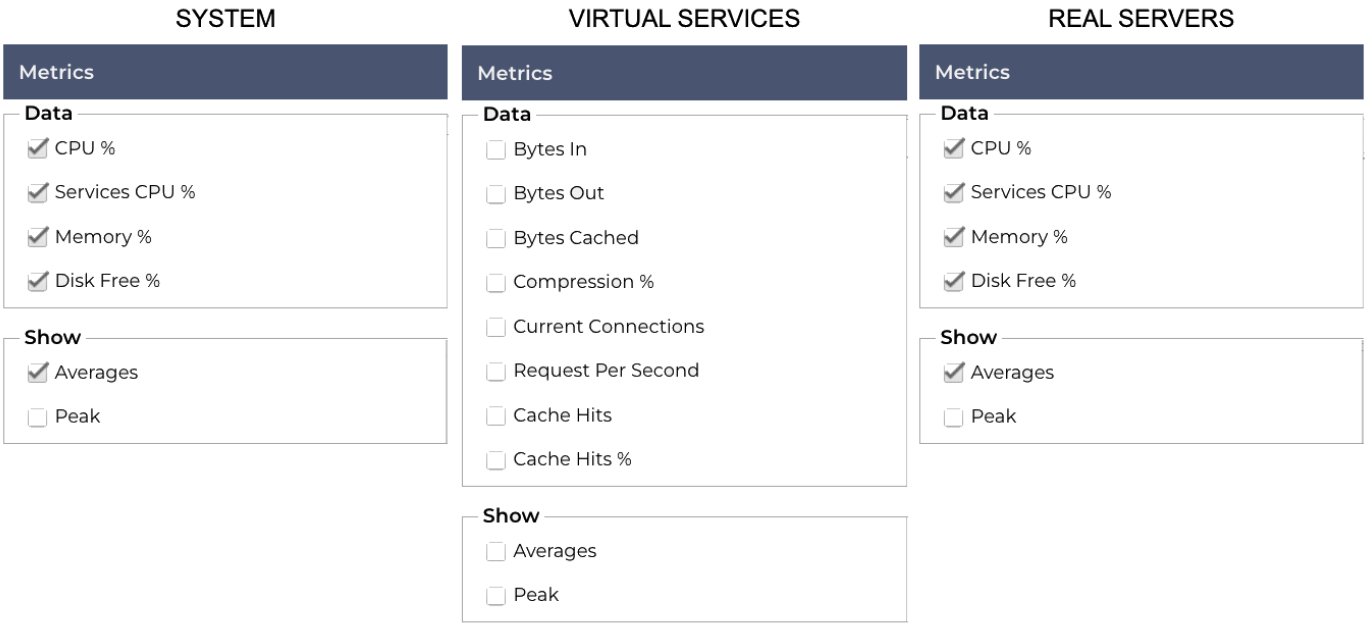
Der erste Schritt besteht darin, die Datenbank und den Zeitraum auszuwählen, die für die Informationen, die Sie anzeigen möchten, relevant sind. Der Zeitraum, den Sie aus der Dropdown-Liste Letzte auswählen können, ist Minute, Stunde, Tag, Woche, Monat und Jahr.

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

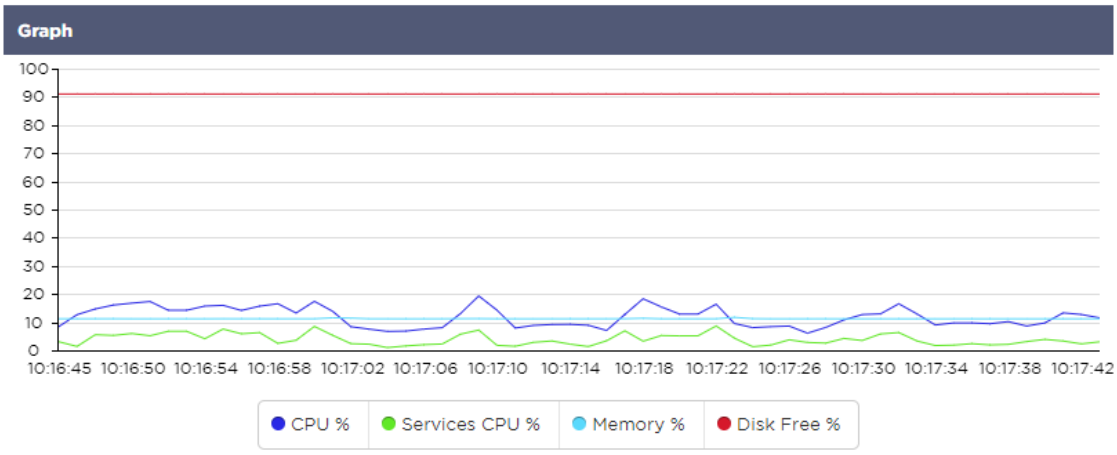


Metriken

Nachdem Sie den zu verwendenden Datensatz ausgewählt haben, müssen Sie die anzuzeigenden Metriken auswählen. Die nachstehende Abbildung zeigt die Metriken, die dem Administrator zur Auswahl stehen: Diese Auswahl entspricht dem System, den virtuellen Diensten und den realen Servern (von links nach rechts).



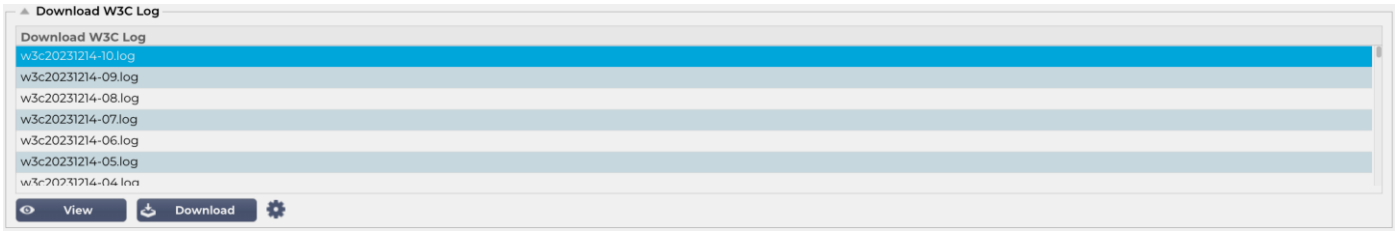
Beispielgrafik



Protokolle

Auf der Seite Protokolle im Abschnitt Ansicht können Sie die W3C- und Systemprotokolle anzeigen und herunterladen. Die Seite ist in zwei Abschnitte unterteilt, die im Folgenden beschrieben werden.

W3C-Protokolle



Die W3C-Protokollierung wird über den Abschnitt System > Protokollierung aktiviert. Ein W3C-Protokoll ist ein Zugriffsprotokoll für Webserver, in dem Textdateien mit Daten über jede Zugriffsanforderung erstellt werden, einschließlich der Internetprotokoll-(IP)-Quelladresse, der HTTP-Version, des Browsertyps, der Verweisseite und des Zeitstempels. W3C-Protokolle können sehr umfangreich werden, je nach der Menge der Daten und der Art der Protokollierung, die aufgezeichnet wird.

Im Abschnitt W3C können Sie das gewünschte Protokoll auswählen und es dann anzeigen oder herunterladen.

Schaltfläche anzeigen

Mit der Schaltfläche Anzeigen können Sie das ausgewählte Protokoll in einem Texteditor-Fenster (z. B. Notepad) anzeigen.

Schaltfläche herunterladen

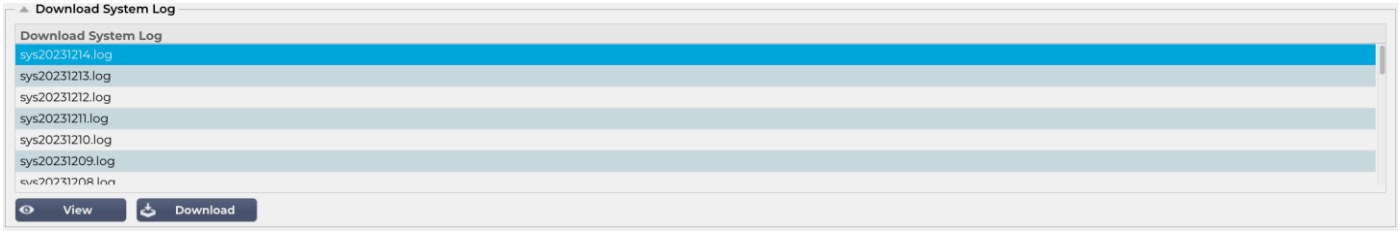
Mit dieser Schaltfläche können Sie das Protokoll auf Ihren lokalen Speicher herunterladen, um es später anzusehen.

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" des Handbuchs ausführlich behandeln.

System-Protokoll

Das Systemprotokoll ist von entscheidender Bedeutung für die Fehlersuche oder die Untersuchung der Vorgänge in der ADC. Es ist für einigermaßen erfahrene Personen in der IT-Abteilung gedacht.



Schaltfläche anzeigen

Mit der Schaltfläche Anzeigen können Sie das ausgewählte 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.

Statistik

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

Komprimierung

Die Aufgabe des ADC besteht darin, Daten zu überwachen und sie an die für den Empfang konfigurierten Real-Server weiterzuleiten. 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 durch das Komprimierungspanel innerhalb der Statistik bereitgestellt.

Inhaltliche Kompression bis heute

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

Die in diesem Abschnitt aufgeführten Daten geben Aufschluss über den Grad der Komprimierung, den die 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	0		0.00 Mbps (data)
Throughput After Compression	0		0.00 Mbps (data)
Throughput From Cache	0		0.00 Mbps (data)
		Total	0.00 Mbps (data)

Die in diesem Abschnitt angegebenen Werte geben an, wie stark die ADC den gesamten Inhalt komprimiert hat. Ein typischer Prozentsatz hängt davon ab, wie viele vorkomprimierte Bilder in Ihren Diensten enthalten sind. Je höher die Anzahl der Bilder ist, desto geringer ist wahrscheinlich der Gesamtkomprimierungsprozentsatz.

Input/Output insgesamt

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

Die Gesamteingangs-/Ausgangszahlen stellen die Menge der Rohdaten dar, die in den ADC ein- und aus ihm herausgeführt werden. Die Maßeinheit ändert sich mit zunehmender Größe von kbps über Mbps bis Gbps.

Treffer und Verbindungen

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

Der Abschnitt Treffer und Verbindungen enthält die Gesamtstatistiken für Treffer und Transaktionen, die die ADC durchlaufen. Was bedeuten also Treffer und Verbindungen?

- Ein Hit ist definiert als eine Schicht-7-Transaktion. In der Regel wird dies bei Webservern als GET-Anfrage für ein Objekt wie ein Bild verwendet.
- Eine Verbindung ist definiert als eine Schicht-4-TCP-Verbindung. Über eine 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 wird die aktuelle Anzahl der Treffer pro Sekunde angezeigt.

Verbindungen insgesamt

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

Peak-Verbindungen

Der Spitzenwert "Connections" gibt die maximale Anzahl der TCP-Verbindungen zum ADC an. Die Zahl in der Spalte ganz rechts zeigt die aktuelle Anzahl der aktiven TCP-Verbindungen an.

Caching

Wie Sie sich erinnern werden, ist die ADC sowohl mit Komprimierung als auch mit Caching ausgestattet. Dieser Abschnitt zeigt die Gesamtstatistiken in Bezug auf die Zwischenspeicherung, wenn diese auf einen Kanal angewendet wird. Wenn die Zwischenspeicherung nicht auf einen Kanal angewandt und korrekt konfiguriert wurde, werden 0 Zwischenspeicherinhalte angezeigt.

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

Aus dem Cache

Treffer: Die erste Spalte gibt die Gesamtzahl der Transaktionen an, die seit dem letzten Zurücksetzen aus dem ADC-Cache bedient wurden. Außerdem wird ein Prozentsatz der Gesamttransaktionen 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 seit dem letzten Zurücksetzen von den Real-Servern bedient wurden. Ein Prozentsatz der Gesamttransaktionen wird ebenfalls angegeben.

Bytes: Die zweite Spalte gibt die Gesamtdatenmenge in Kilobytes an, die von den Real-Servern geliefert wurde. Außerdem wird ein Prozentsatz der Gesamtdatenmenge 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.

Anwendungspuffer

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

Die Verwendung von Anwendungspuffern in der ADC hilft bei der Optimierung der Leistung, der Verbesserung des Durchsatzes und der Gewährleistung eines zuverlässigen und effizienten Datenflusses zwischen Clients und Servern. Puffergrößen, Verarbeitungsrichtlinien und andere Parameter werden von der ADC optimiert, um die Last auf der Grundlage der spezifischen Anforderungen der Anwendungen und der Infrastruktur fein abzustimmen.

Der EdgeADC nimmt Ihnen die harte Arbeit ab und passt die Pufferparameter automatisch nach Bedarf an.

Persistenz der Sitzung

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

Der Abschnitt Session Persistence liefert Informationen zu verschiedenen Parametern.

Aktuelle Sitzungen insgesamt

Hier wird angezeigt, wie viele Persistenzsitzungen im Gange sind - jede Minute aktualisiert

% verwendet (von max)

Hier wird angezeigt, wie viel des insgesamt für Sitzungsinformationen zur Verfügung stehenden Platzes genutzt wird

Neue Sitzung diese Minute

Dies zeigt, wie viele neue Persistenzsitzungen innerhalb der letzten Minute hinzugefügt wurden

Revalidiere dieses min

Dies zeigt, wie viele bestehende Persistenzsitzungen innerhalb der letzten Minute durch mehr Datenverkehr neu bestätigt wurden

Abgelaufene Sitzungen in dieser Minute

Hier wird angezeigt, wie viele bestehende Persistenzsitzungen in der letzten Minute abgelaufen sind, weil innerhalb der Zeitüberschreitung kein weiterer Datenverkehr stattfand.

Hardware

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

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

Nutzung der Festplatte

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

Speicherverbrauch

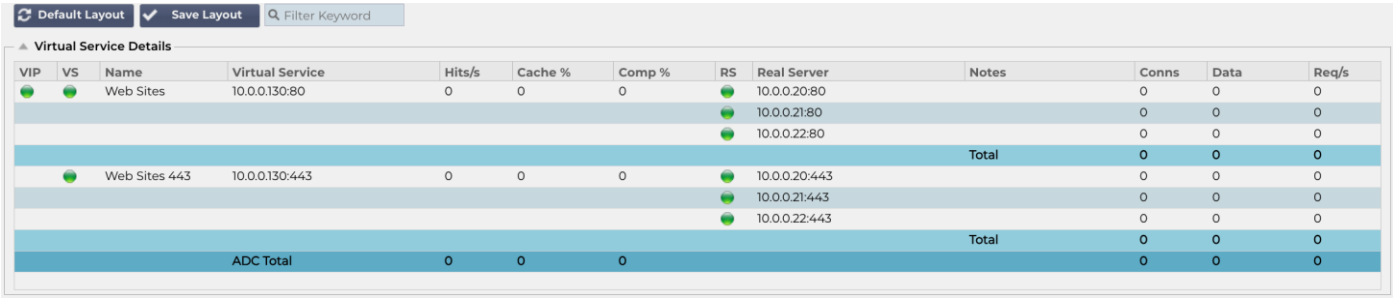
Die zweite Spalte gibt den Prozentsatz des derzeit verwendeten Speichers an. Die bedeutendere Zahl in Klammern ist der gesamte dem ADC zugewiesene Speicherplatz. Es wird empfohlen, dass der ADC mindestens 2 GB RAM zugewiesen werden.

CPU-Nutzung

Einer der kritischen Werte ist der Prozentsatz der CPU, der von der ADC verwendet wird. Es ist normal, dass dieser Wert schwankt.

Status

Auf der Seite Ansicht > Status wird der Live-Datenverkehr angezeigt, der für die von Ihnen definierten virtuellen Dienste durch den ADC fließt. 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

VIP-Säule

Die Farbe der Leuchte zeigt den Status 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 "Passiver" auf einen "Aktiven" wartet
●	Offline. Reale Server sind unerreichbar oder es sind keine realen Server aktiviert
●	Status der Suche
●	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 "Passiver" auf einen "Aktiven" wartet
●	Dienst benötigt Aufmerksamkeit. Diese Statusanzeige kann darauf zurückzuführen sein, dass ein Real Server eine Zustandsüberwachung nicht bestanden hat oder dass er manuell auf Offline gesetzt wurde. Der Datenverkehr fließt weiter, allerdings mit reduzierter Real Server-Kapazität.
●	Offline. Reale Server sind unerreichbar oder es sind keine realen Server aktiviert
●	Status der Suche
●	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 der ADC bedient wurden.

Komprimierung%.

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

RS-Status (Entfernter Server)

In der nachstehenden Tabelle ist die Bedeutung des Status der mit dem VIP verbundenen Real Server aufgeführt.

Status	Beschreibung
●	Verbunden
●	Nicht überwacht
●	Ablassen oder Offline
●	Bereitschaft
●	Nicht verbunden
●	Status der Suche
●	Nicht lizenziert oder lizenzierte virtuelle IPs überschritten

Echte Server

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

Anmerkungen

Dieser Wert kann eine hilfreiche Anmerkung sein, um anderen den Zweck des Eintrags verständlich zu machen.

Conns (Verbindungen)

Anhand der Anzahl der Verbindungen zu den einzelnen Real-Servern können Sie die Lastverteilung in Aktion sehen. Dies ist sehr hilfreich, um zu überprüfen, ob Ihre Lastausgleichspolitik korrekt funktioniert.

Daten

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

Req/Sec (Anfragen pro Sekunde)

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

System

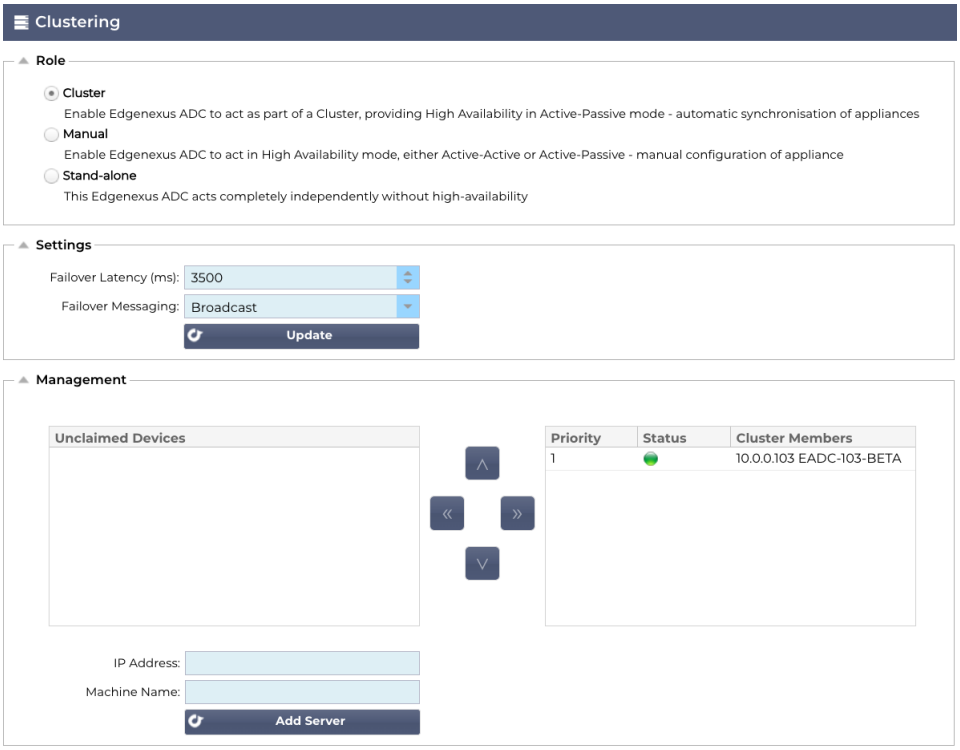
Clustering

Der ADC kann als einzelnes, unabhängiges Gerät verwendet werden, und das ist auch völlig in Ordnung so. Wenn man jedoch bedenkt, dass der Zweck des ADC darin besteht, einen Lastausgleich zwischen mehreren Servern herzustellen, wird die Notwendigkeit deutlich, den ADC selbst zu clustern. Das einfach zu navigierende UI-Design des ADC macht die Konfiguration des Clustering-Systems unkompliziert.

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

Wichtiger Hinweis

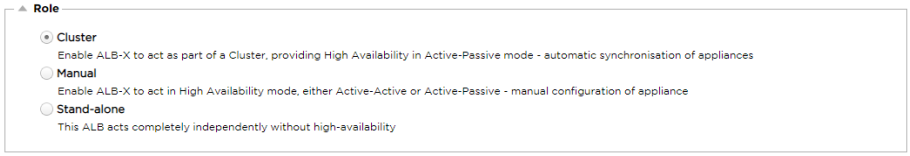
- Es ist kein spezielles Kabel zwischen den ADC-Paaren erforderlich, um einen hochverfügbaren Heartbeat aufrechtzuerhalten.
- Der Heartbeat findet im selben Netzwerk statt wie der virtuelle Dienst, für den Hochverfügbarkeit erforderlich ist.
- Zwischen den ADC Appliances gibt es kein Stateful Fail-over.
- 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 nutzt Unicast Messaging und Gratuitous ARP, um die neuen Active Load Balancer Switches zu informieren.



Rolle

Bei der Konfiguration des ADC für Hochverfügbarkeit sind drei Cluster-Rollen verfügbar.

Cluster



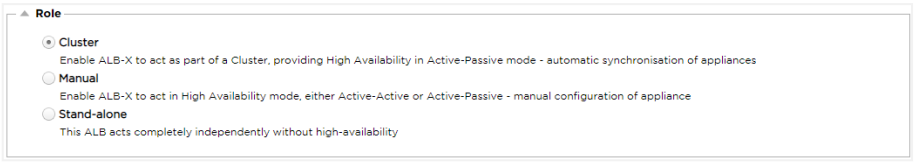
- Standardmäßig wird ein neuer ADC in der Cluster-Rolle eingeschaltet. In dieser Rolle hat jedes Clustermitglied dieselbe "Arbeitskonfiguration", so dass immer nur ein ADC im Cluster aktiv ist.
- Eine "Arbeitskonfiguration" umfasst alle Konfigurationsparameter mit Ausnahme von Elementen, die eindeutig sein müssen, wie z. B. die Management-IP-Adresse, den ALB-Namen, die Netzwerkeinstellungen, die Schnittstellendetails und so weiter.
- Der ADC mit der Priorität 1, der obersten Position, im Feld Clustermitglieder ist der Clustereigentümer und der aktive Lastausgleicher, 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 in Anspruch genommene Geräte entfernen. Um das letzte Mitglied zu entfernen, ändern Sie bitte die Rolle in Manuell oder Stand-alone.
- Die folgenden Objekte werden nicht synchronisiert:
    - Manueller Datums- und Zeitabschnitt - (NTP-Abschnitt wird synchronisiert)
    - Failover-Latenzzeit (ms)
    - Abschnitt Hardware
    - Abschnitt Geräte
    - Bereich Netzwerk

Versagen des Clustereigentümers

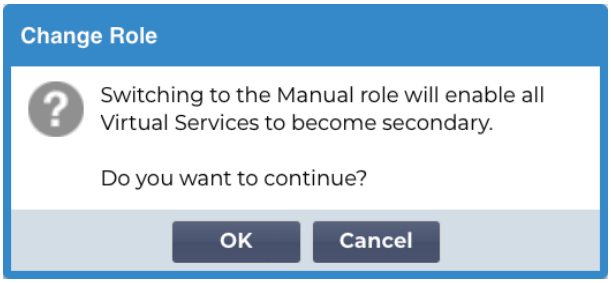
- Fällt ein Clustereigentümer aus, übernimmt automatisch eines der verbleibenden Mitglieder und führt den Lastausgleich des Datenverkehrs fort.
- Wenn der Clustereigentümer zurückkehrt, nimmt er den Lastausgleich wieder auf und übernimmt die Eigentümerrolle.
- Nehmen wir an, der Eigentümer ist ausgefallen und ein Mitglied hat den Lastausgleich übernommen. Wenn Sie möchten, dass das Mitglied, das den Lastausgleichsverkehr übernommen hat, der neue Eigentümer 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 nicht erreichbar ist, wird das bearbeitete Mitglied automatisch zum Eigentümer, ohne dass der Datenverkehr unterbrochen wird.

Ändern der Rolle von der Clusterrolle zur manuellen Rolle

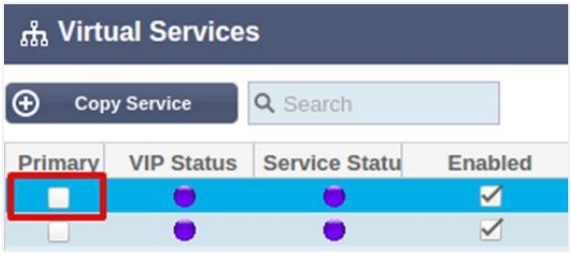
- Wenn Sie die Rolle von "Cluster" in "Manuell" ändern möchten, klicken Sie auf das Optionsfeld neben der Option "Manuell".



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



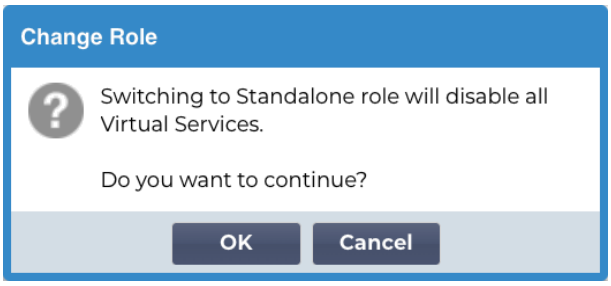
- Klicken Sie auf die Schaltfläche OK
- Prüfen Sie den Abschnitt Virtuelle Dienste. Sie werden feststellen, dass in der Spalte "Primär" jetzt ein nicht angekreuztes Kästchen angezeigt wird.



- Dies ist ein Sicherheitsmerkmal und bedeutet, dass der Verkehrsfluss nicht unterbrochen wird, wenn Sie eine andere 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:



- Klicken Sie auf OK, um die Rollen zu ändern.
- Überprüfen Sie Ihre virtuellen Dienste. Sie werden sehen, dass sich der Name der Spalte Primary 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 Dienst aktivieren.

Handbuch Rolle

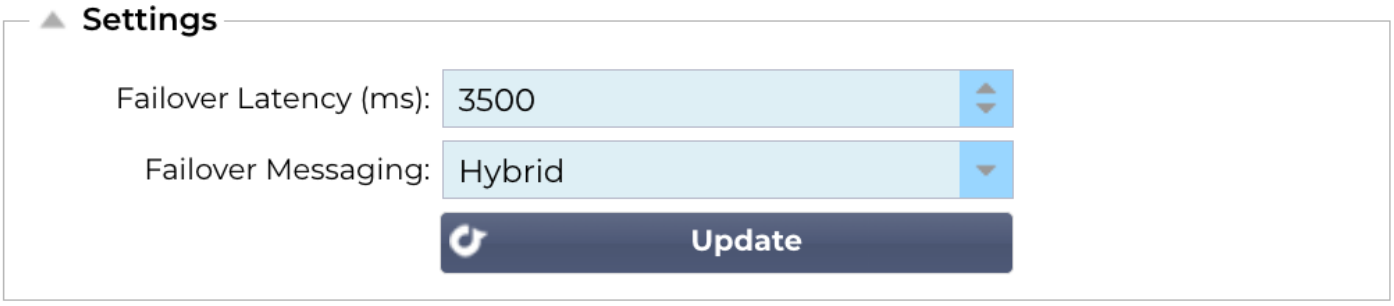
Ein ADC in der manuellen Rolle arbeitet mit anderen ADCs in der manuellen Rolle zusammen, um eine hohe Verfügbarkeit zu gewährleisten. Der Hauptvorteil gegenüber der Cluster-Rolle ist die Möglichkeit, festzulegen, welche ADC für eine virtuelle IP aktiv ist. Der Nachteil ist, dass es keine Konfigurationssynchronisation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

- Um eine virtuelle IP-Adresse "aktiv" zu machen, markieren 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.
- Falls ein aktiver Dienst auf den passiven Dienst übergeht:
    - Wenn beide Primärspalten angekreuzt sind, findet ein Wahlprozess statt, und die niedrigste MAC-Adresse wird aktiv.
    - Sind beide nicht angekreuzt, findet derselbe Wahlprozess statt. Wenn beide nicht angekreuzt sind, gibt es außerdem keinen automatischen Rückgriff auf die ursprüngliche aktive ADC

Eigenständige Rolle

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

Einstellungen

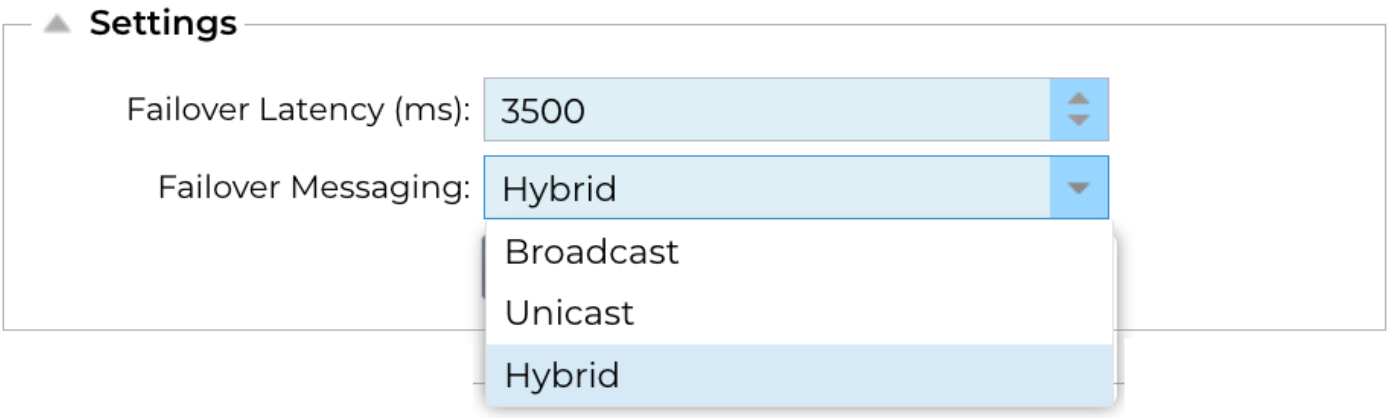


Failover-Latenzzeit (ms)

Sie können die Failover-Latenzzeit in Millisekunden festlegen. Dies ist 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 Latenzzeit Instabilitäten im Cluster feststellen, sollten Sie diesen Wert erhöhen.

Failover-Messaging



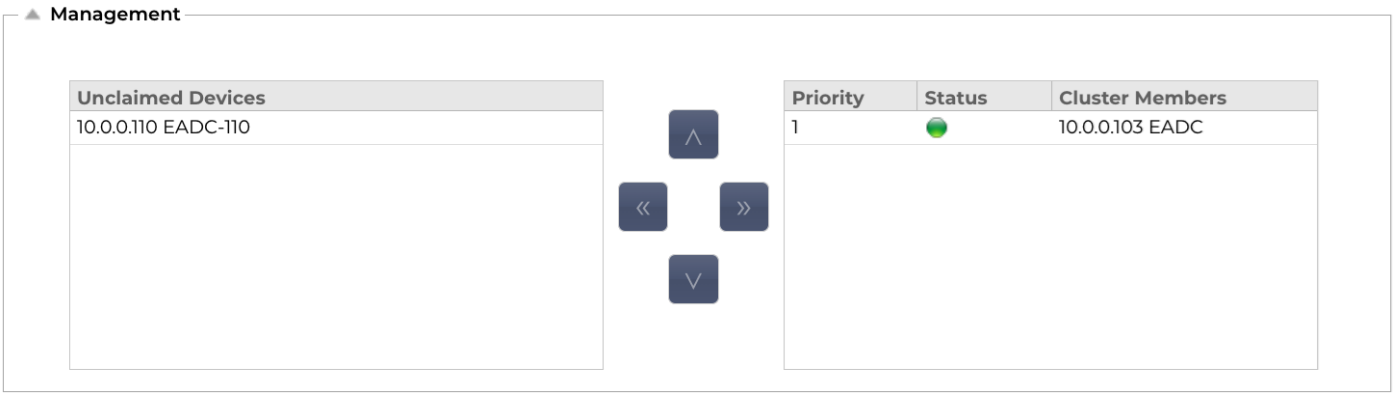
Standardmäßig verwendet der ADC Broadcast für seine Failover-Nachrichten. Einige Netzwerke blockieren jedoch Broadcast, daher haben wir Unicast und Hybrid, eine Mischung aus Unicast und Broadcast, bereitgestellt.

Im standardmäßigen Broadcast-Modus werden nicht beanspruchte Geräte automatisch aufgelistet, und Broadcast-Nachrichten werden für die Ausfallsicherung verwendet. Im Hybridmodus werden nicht beanspruchte Geräte weiterhin über Broadcast angekündigt, die Failover-Kommunikation erfolgt jedoch über Unicast. Im Unicast-Modus werden keine Broadcast-Nachrichten versendet, und Sie müssen die Clustermitglieder möglicherweise manuell eingeben.

Verwaltung

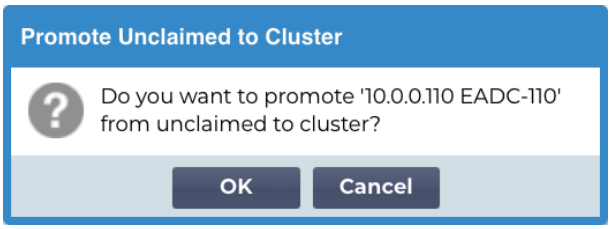
In diesem Bereich können Sie Clustermitglieder hinzufügen und entfernen sowie die Priorität eines ADCs im Cluster ändern. Der Bereich besteht aus zwei Feldern und einer Reihe von Pfeiltasten dazwischen. Der

Bereich auf der linken Seite sind die nicht beanspruchten Geräte, während der Bereich ganz rechts der Cluster selbst ist.

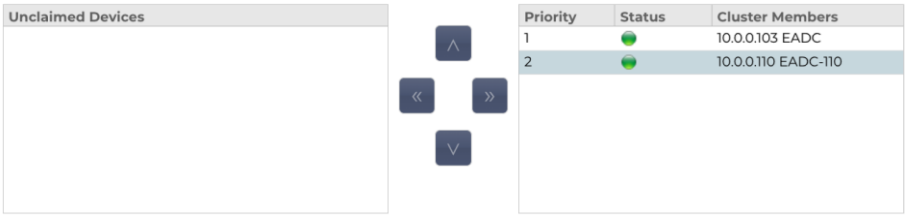


Hinzufügen eines ADC zum Cluster

- Bevor Sie den ADC zum Cluster hinzufügen, müssen Sie sicherstellen, dass alle ADC Appliances mit einem eindeutigen Namen versehen wurden, der im Abschnitt System > Netzwerk festgelegt wurde.
- Sie sollten den ADC als Priorität 1 mit grünem Status und seinem Namen in der Spalte Cluster-Mitglieder im Verwaltungsbereich sehen. Dieser ADC ist die standardmäßige primäre Appliance.
- Alle anderen verfügbaren ADCs werden im Fenster Nicht beanspruchte Geräte im Verwaltungsbereich angezeigt. Ein nicht beanspruchtes Gerät ist ein ADC, der in der Cluster-Rolle zugewiesen wurde, aber keine virtuellen Dienste konfiguriert hat.
- Markieren Sie den ADC im Fenster Nicht beanspruchte Geräte und klicken Sie auf die rechte Pfeiltaste.
- Sie sehen nun die folgende Meldung:

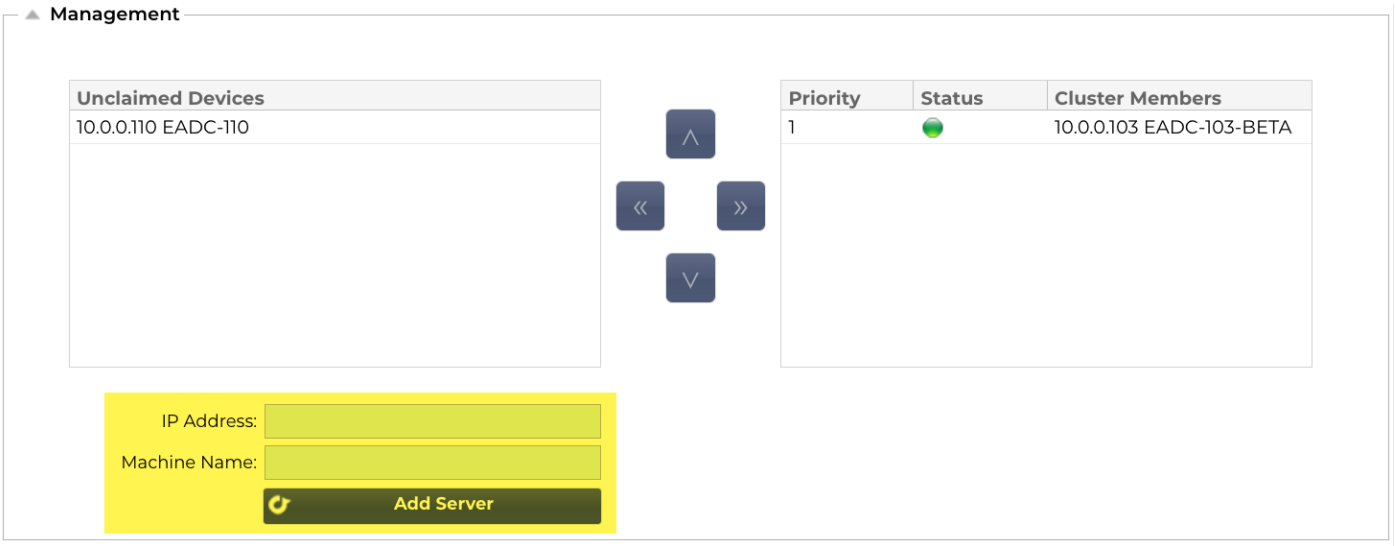


- Klicken Sie auf OK, um den ADC in den Cluster aufzunehmen.
- Ihr ADC sollte nun als Priorität 2 in der Liste der Clustermitglieder angezeigt werden.



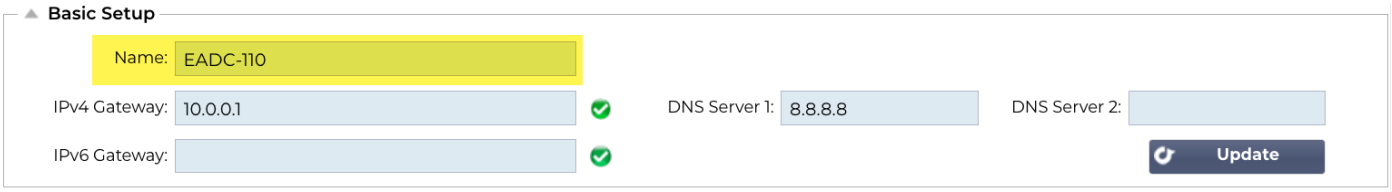
Manuelles Hinzufügen eines ADC zum Cluster

In Systemen, in denen Broadcast blockiert ist, müssen Sie den Unicast- oder Hybrid-Modus wählen, um einen ADC zum Cluster hinzuzufügen.



So fügen Sie einen ADC manuell zum Cluster hinzu:

1. Geben Sie seine IP-Adresse an
2. Geben Sie den Maschinennamen an - dieser ist im Abschnitt System > Netzwerk verfügbar.



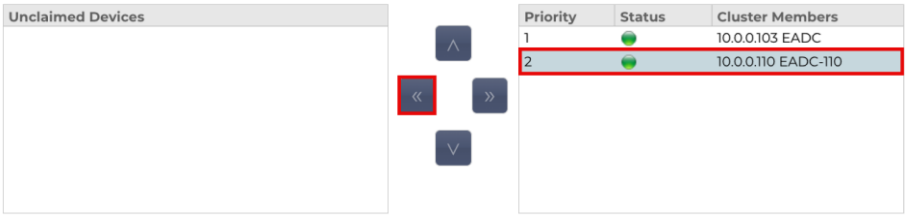
3. Klicken Sie auf Server hinzufügen

Der ADC wird dann dem Cluster hinzugefügt.

Wenn der ADC, den Sie hinzufügen möchten, bereits in einem Cluster ist, werden Sie durch eine Fehlermeldung darauf hingewiesen.

Entfernen eines Clustermitglieds

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



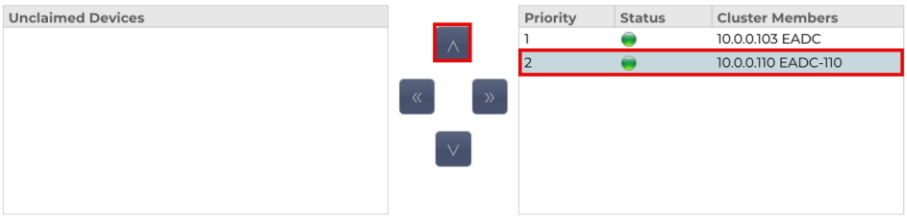
- Sie erhalten dann eine Bestätigungsanfrage.
- Klicken Sie zur Bestätigung auf OK.
- Ihr ADC wird entfernt und auf der Seite Nicht beanspruchte Geräte angezeigt.

Ändern der Priorität eines ADC

Es kann vorkommen, dass Sie die Priorität einer ADC innerhalb der Mitgliederliste ändern möchten.

- Der ADC an der Spitze der Liste der Clustermitglieder 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.

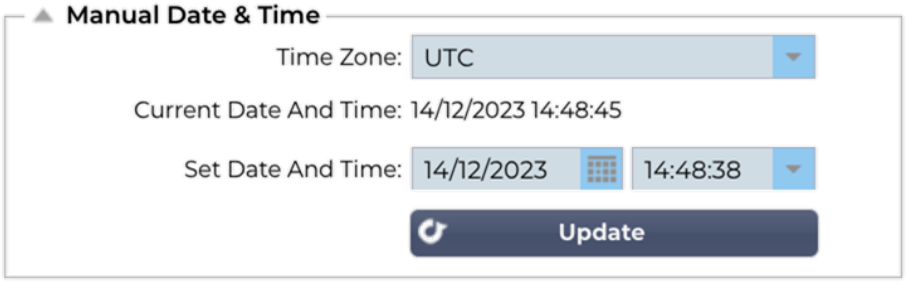
- Um zu ändern, welcher ADC aktiv ist, markieren Sie ADC und klicken Sie auf den Pfeil nach oben, bis er am Anfang der Liste steht.



Datum und Uhrzeit

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

Manuelles Datum und Uhrzeit



Zeitzone

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

- Klicken Sie auf das Dropdown-Feld für die Zeitzone und geben Sie Ihren Standort ein.
- Zum Beispiel London
- Wenn Sie mit der Eingabe beginnen, zeigt die ADC automatisch Stellen an, die den Buchstaben L enthalten.
- Fahren Sie mit der Eingabe von "Lon" usw. fort - 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

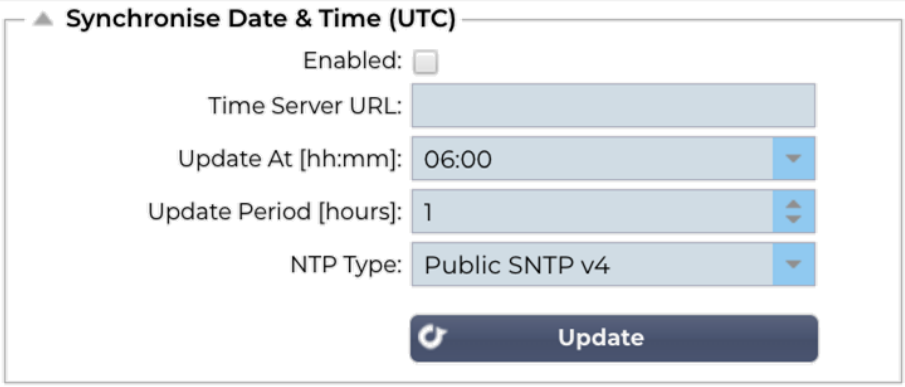
Datum und Uhrzeit einstellen

Diese Einstellung entspricht dem aktuellen Datum und der aktuellen Uhrzeit.

- Wählen Sie das richtige Datum aus der ersten Dropdown-Liste oder,
  alternativ können Sie das Datum in folgendem Format eingeben: TT/MM/JJJJ
- 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 die Daten korrekt eingegeben haben, klicken Sie bitte auf Aktualisieren, um sich anzumelden.
- Sie sollten dann das neue Datum und die neue 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 auf der ganzen Welt, und Sie können auch Ihren eigenen internen NTP-Server verwenden, wenn Ihre Infrastruktur Einschränkungen für den externen Zugriff hat.



Zeitserver-URL

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

Aktualisierung um [hh:mm]

Wählen Sie die geplante Zeit, zu der das ADC mit dem NTP-Server synchronisiert werden 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 über TCP - Ältere NTP-Version über TCP. **RFC 1059**
- NTP v1 über UDP - Ältere NTP-Version über UDP. **RFC 1059**

Hinweis: Bitte beachten Sie, dass die Synchronisierung nur in UTC erfolgt. Wenn Sie eine lokale Zeit einstellen möchten, können Sie dies nur manuell tun. Diese Einschränkung wird in späteren Versionen geändert, so dass die Möglichkeit besteht, eine Zeitzone auszuwählen.

E-Mail-Veranstaltungen

Das ADC ist ein kritisches Gerät, und wie jedes wichtige System ist es mit der Fähigkeit ausgestattet, den Systemadministrator über alle Probleme zu informieren, die möglicherweise Aufmerksamkeit erfordern.

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

Adresse

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

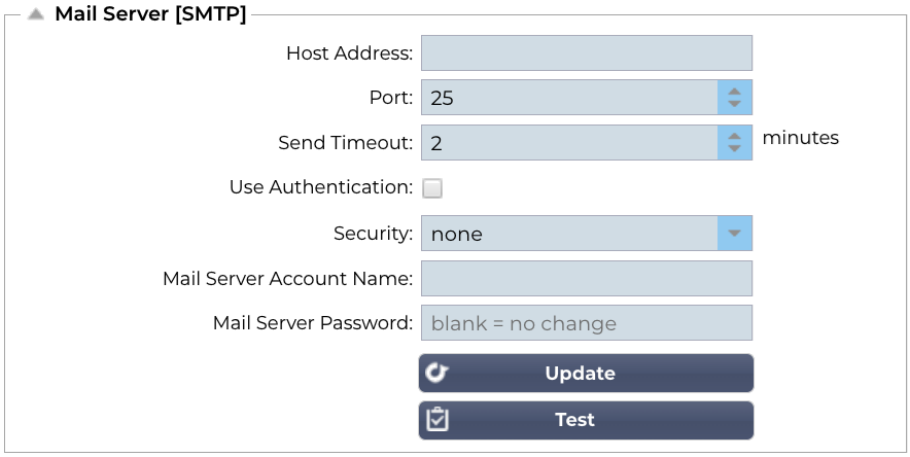
Fügen Sie eine gültige E-Mail-Adresse hinzu, an die die Alarme, Benachrichtigungen und Ereignisse gesendet werden sollen. Beispielsupport@domain.com . Sie können auch mehrere E-Mail-Adressen mit einem Komma als Trennzeichen hinzufügen.

Rücksende-E-Mail-Adresse:

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

Mail-Server (SMTP)

In diesem Abschnitt müssen Sie die Details des SMTP-Servers angeben, der für den Versand der E-Mails verwendet werden soll. Vergewissern Sie sich, dass die E-Mail-Adresse, die Sie für den Versand verwenden, für diesen Zweck zugelassen ist.



Host-Adresse

Geben Sie den FQDN oder 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 eine SMTP-Zeitüberschreitung ein. Der Standardwert ist auf 2 Minuten eingestellt.

Authentifizierung verwenden

Markieren Sie das Kästchen, 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-Kennwort

Geben Sie das für die Authentifizierung erforderliche Passwort ein.

Benachrichtigungen und Warnungen

Es gibt verschiedene Arten von Ereignisbenachrichtigungen, die die ADC an Personen sendet, die dafür konfiguriert sind, sie zu empfangen. Sie können die Benachrichtigungen und Alarme, die gesendet werden sollen, ankreuzen und aktivieren. Benachrichtigungen erfolgen, wenn Real Server kontaktiert oder Kanäle gestartet werden. Warnungen treten auf, wenn Real Server nicht kontaktiert werden können oder Kanäle nicht mehr funktionieren.

IP-Dienst Hinweis

Die IP-Service-Meldung 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 Hinweis

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

Real Server Hinweis

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

flightPATH

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

Gruppenbenachrichtigungen Zusammen

Markieren Sie diese Option, um Benachrichtigungen zu gruppieren. Wenn Sie dieses Kontrollkästchen aktivieren, werden alle Benachrichtigungen und Warnungen in einer einzigen E-Mail zusammengefasst.

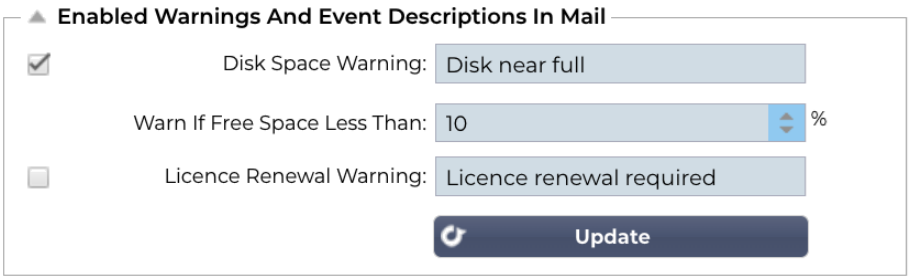
Gruppenpost Beschreibung

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

Gruppe Sendeintervall

Legen Sie fest, wie lange Sie warten möchten, bevor Sie eine Gruppenbenachrichtigung per E-Mail versenden. Die Mindestzeit beträgt 2 Minuten. Die Standardeinstellung ist 30 Minuten.

Aktivierte Warnungen und Ereignisbeschreibungen in Mail



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

Speicherplatz

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

Warnung, wenn der freie Speicherplatz kleiner ist als

Sie können hier einen prozentualen Wert festlegen, damit die ADC eine Warn-E-Mail senden kann, wenn der Speicherplatz unter diesen Schwellenwert fällt.

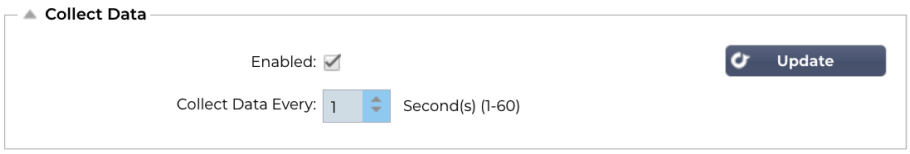
Ablauf der Lizenz

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

Geschichte

Im Abschnitt "System" gibt es die Option "Systemverlauf", die die Bereitstellung von Verlaufsdaten für Elemente wie CPU, Speicher, Anfragen pro Sekunde und andere Funktionen 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



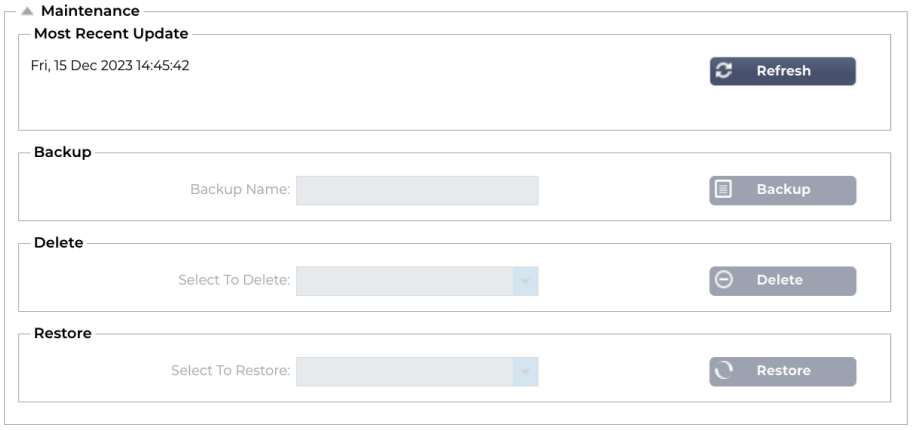
Aktivieren Sie

Um die Datenerfassung zu aktivieren, aktivieren Sie bitte das Kontrollkästchen.

Daten sammeln Jede

Als Nächstes stellen Sie das Zeitintervall ein, in dem der ADC die Daten erfassen soll. Dieser Zeitwert kann zwischen 1-60 Sekunden liegen.

Wartung



Letzte Aktualisierung

Hier wird angezeigt, wann die letzten Verlaufsdaten von der ADC erfasst wurden.

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

HP Enterprise-basierte ADCs

Dieser Abschnitt der Funktionen gilt nur für ADCs, die auf HPE ProLiant Bare Metal Servern installiert sind und ILO verwenden.

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 wiederherzustellen.

Lizenz

Der ADC wird für die Verwendung eines der folgenden Modelle lizenziert, die von Ihren Kaufparametern und Ihrem Kundentyp abhängen.

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

Lizenz-Details

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

Lizenz-ID

Die Lizenz-ID ist direkt mit der Geräte-ID und anderen Details verknüpft, die für Ihren Kauf und Ihre ADC Appliance spezifisch sind. Diese Informationen sind wichtig und werden benötigt, wenn Sie Updates und andere Elemente aus dem App Store abrufen möchten.

Maschinen-ID

Die Maschinen-ID wird anhand der eth0-IP-Adresse der ADC Appliance generiert. Wenn Sie die IP-Adresse der ADC Appliance ändern, ist die Lizenz nicht mehr gültig. Sie müssen den Support um Hilfe bitten. Wir empfehlen, dass Ihre ADC Appliance(s) feste IP-Adressen haben, mit der Anweisung an Ihr IT-Personal, diese nicht zu ändern. Technischen Support erhalten Sie, indem Sie ein Ticket unter https://www.edgenexus.io/support erstellen.

Hinweis: Sie dürfen die IP-Adresse Ihrer ADC Appliances nicht ändern. Wenn Sie sich in einem virtualisierten Rahmen befinden, legen Sie bitte die MAC-ID fest und verwenden Sie eine statische IP-Adresse.

Ausgestellt für

Dieser Wert enthält den Namen des Käufers in Verbindung mit der Maschinen-ID des ADC.

Kontaktperson

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

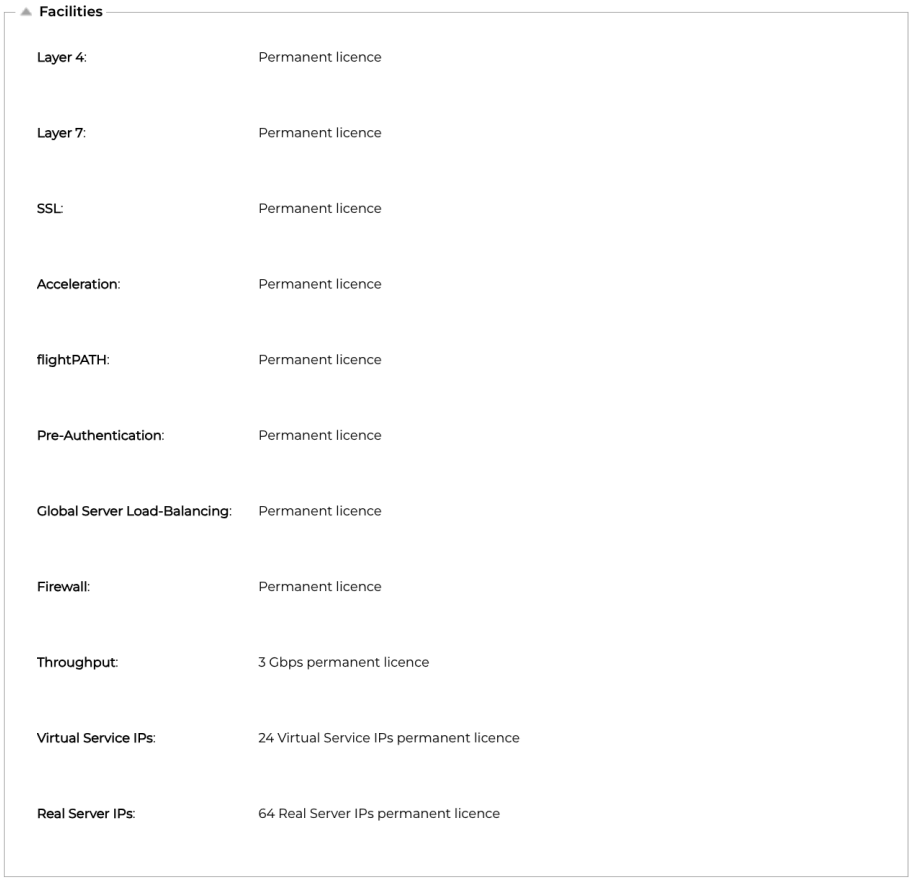
Datum Ausgabe d

Das Datum, an dem die Lizenz erteilt wurde.

Name

Dieser Wert zeigt den beschreibenden Namen für die ADC Appliance an, den Sie unter System > Networking angegeben haben.

Einrichtungen



Im Bereich Einrichtungen finden Sie Informationen darüber, welche Funktionen innerhalb des ADC für die 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 erworbenen Lizenz.

Lizenzen installieren e

- Die Installation einer neuen Lizenz ist sehr einfach. Wenn Sie Ihre neue oder Ersatzlizenz von Edgenexus erhalten, wird sie in Form einer Textdatei gesendet. Sie können die Datei öffnen und dann den Inhalt kopieren und in das Feld Lizenz einfügen einfügen.

- Sie können sie auch in die ADC hochladen, wenn Kopieren/Einfügen für Sie keine Option ist.
- Wenn Sie dies getan haben, klicken Sie bitte auf die Schaltfläche Aktualisieren.
- Die Lizenz ist nun installiert.

Lizenz-Service-Informationen

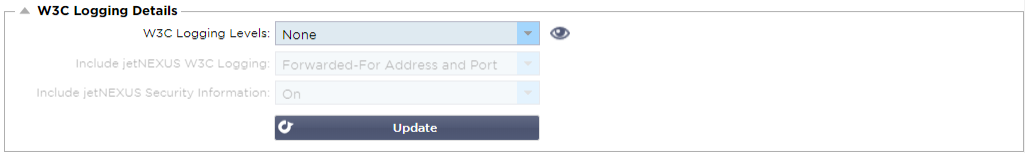
Wenn Sie auf die Schaltfläche Lizenzservice-Informationen klicken, werden alle Informationen über die Lizenz angezeigt. Diese Funktion kann verwendet werden, um die Details an das Supportpersonal zu senden.

Protokollierung

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

W3C-Protokollierungsdetails

Wenn Sie die W3C-Protokollierung aktivieren, beginnt die ADC mit der Aufzeichnung einer W3C-kompatiblen Protokolldatei. Ein W3C-Protokoll ist ein Zugriffsprotokoll für Webserver, in dem Textdateien erzeugt werden, die Daten über jede Zugriffsanfrage enthalten, einschließlich der Quell-IP-Adresse (Internet Protocol), der HTTP-Version, des Browsertyps, der Verweisseite und des Zeitstempels. Das Format wurde vom World Wide Web Consortium (W3C) entwickelt, einer Organisation, die Standards für die Weiterentwicklung des Internets fördert. Die Datei besteht aus ASCII-Text mit durch Leerzeichen getrennten Spalten. Die Datei enthält Kommentarzeilen, die mit dem Zeichen # beginnen. Eine dieser Kommentarzeilen ist eine Zeile, in der die Felder (mit Spaltennamen) angegeben werden, damit die Daten ausgewertet werden können. Es gibt separate Dateien für die Protokolle HTTP und FTP.



W3C-Protokollierungsebenen

Es stehen verschiedene Protokollierungsstufen zur Verfügung, und je nach Art des Dienstes variieren die bereitgestellten Daten.

Die obige Tabelle beschreibt die Protokollierungsstufen für W3C HTTP.

Wert	Beschreibung
Keine	Die W3C-Protokollierung ist ausgeschaltet.
Brief	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 prozessorfreundlicheres Format mit getrennten Datums- und Zeitfeldern. Informationen zur Bedeutung der Felder finden Sie in der nachstehenden Zusammenfassung. 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 "Full" sehr ähnlich, hat aber ein zusätzliches Feld. In der nachstehenden Zusammenfassung der Felder finden Sie Informationen über die 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 möglichen Informationen gefüllt, die für Entwicklungs- und Unterstützungspersonal relevant sind. In der nachstehenden Zusammenfassung der Felder 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
Brief	#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 festlegen, welche ADC-Informationen in die W3C-Protokolle aufgenommen werden sollen.

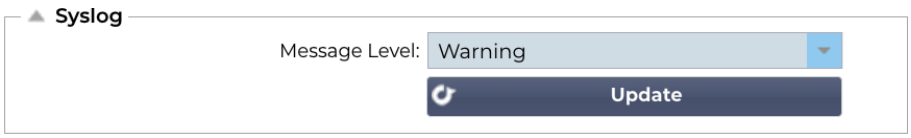
Wert	Beschreibung
Netzwerkadresse und Port des Kunden	Der hier angezeigte Wert zeigt die tatsächliche Client-IP-Adresse zusammen mit dem Port an.
Netzwerkadresse des Kunden	Mit dieser Option wird nur die tatsächliche Client-IP-Adresse angezeigt.
Weitergeleitet-für Adresse und Port	Diese Option zeigt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

Sicherheitsinformationen einbeziehen

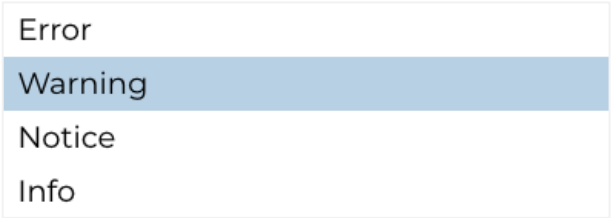
Dieses Menü besteht aus zwei Optionen:

Wert	Beschreibung
Auf	Diese Einstellung ist global. Wenn sie eingeschaltet ist, wird der Benutzername an das W3C-Protokoll angehängt, wenn ein virtueller Dienst die Authentifizierung verwendet und die W3C-Protokollierung aktiviert ist.
Aus	Damit wird die Möglichkeit, den Benutzernamen in das W3C-Protokoll aufzunehmen, auf globaler Ebene ausgeschaltet.

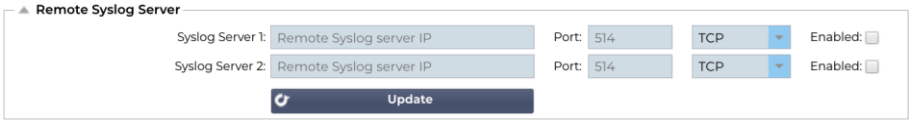
Syslog-Server



In diesem Abschnitt können Sie den Grad der Nachrichtenprotokollierung für den SYSLOG-Server festlegen. Die folgenden Optionen sind verfügbar.



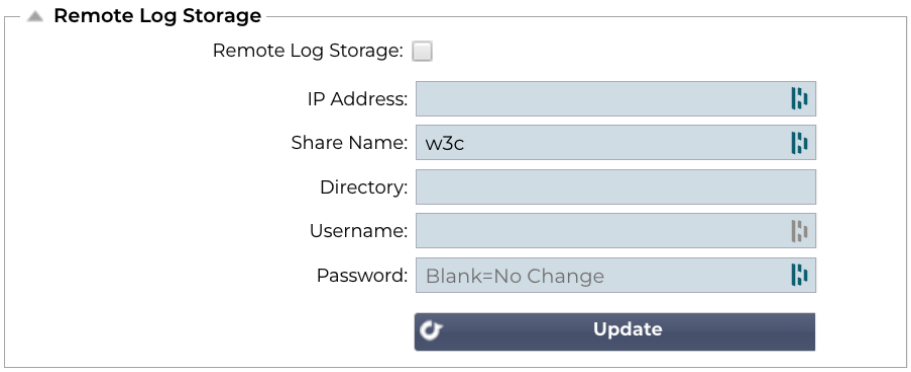
Entfernter Syslog-Server



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

- Fügen Sie die IP-Adresse Ihres Syslog-Servers hinzu
- Den Hafen hinzufügen
- Wählen Sie, ob Sie TCP oder UDP verwenden möchten
- Aktivieren Sie das Kontrollkästchen Aktiviert, um mit der Protokollierung zu beginnen.
- Update anklicken

Fernspeicherung von Protokollen



Alle W3C-Protokolle werden stündlich in komprimierter Form auf dem ADC gespeichert. Die ältesten Dateien werden gelöscht, wenn noch 30 % des Speicherplatzes verfügbar sind. Wenn Sie diese zur sicheren Aufbewahrung auf einen entfernten Server exportieren möchten, 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 fertiggestellt und komprimiert wurde. 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.

Spalte1	**Spalte2**
Fernspeicherung von Protokollen	Markieren Sie das Kästchen, um die Fernspeicherung von Protokollen zu aktivieren.
IP-Adresse	Geben Sie die IP-Adresse Ihres SMB-Servers an. Diese sollte in Dezimalpunktschreibweise 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 gibt es hier zwei Formate (Site
	hat keine .ZZZ Millisekunden)
x-mil	Nur Website-Format = Millisekunde des Zeitstempels
c-ip	Client-IP so gut wie möglich aus dem Netzwerk oder dem X-Forwarded-For-Header ableiten
c-anschluss	Client-Port so gut wie möglich aus dem Netzwerk oder dem X-Forwarded-For-Header ableitbar
cs-Benutzername	Anforderungsfeld für den Benutzernamen des Kunden
s-ip	ALBs abhörender Port
s-port	ALBs Zuhörer VIP
x-xff	Wert des X-Forwarded-For-Headers
x-xffcustom	Wert des konfigurierten X-Forwarded-For-Anfrage-Headers
cs-host	Hostname in der Anfrage
x-r-ip	IP-Adresse des verwendeten Real-Servers
x-r-port	Verwendeter Port von Real Server
cs-Methode	HTTP-Anforderungsmethode * außer Brief-Format
Methode	* Nur das Kurzformat verwendet diesen Namen für cs-method
cs-uri-stem	Pfad der angeforderten Ressource * außer Kurzformat
cs-uri-abfrage	Abfrage der angeforderten Ressource * außer Kurzformat
uri	* Kurzes Format 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 Kunden HTTP-Version
x-r-version	Inhalt - Antwort des Servers HTTP-Version
cs-bytes	Bytes vom Kunden, in der Anfrage
sr-bytes	An Real Server weitergeleitete Bytes in der Anfrage
rs-bytes	Bytes von Real Server, in der Antwort
sc-bytes	An den Kunden gesendete Bytes in der Antwort
x-prozentig	Komprimierungsprozentsatz * = 100 * (1 - Output / Input) einschließlich Header
Zeit genommen	Wie lange der Realserver in Sekunden brauchte
x-trip-zeiten neu pcon	Millisekunde von der Verbindung bis zum Eintrag in die "Neulingsliste" Millisekunde vom Verbindungsaufbau bis zum Aufbau der Verbindung zum Real-Server
acon	Millisekunde vom Verbindungsaufbau bis zur Beendigung des Verbindungsaufbaus mit dem Real-Server
rcon	Millisekunde von "Connect" bis zum Aufbau der Verbindung mit dem realen Server
rqf	Millisekunde vom Verbindungsaufbau bis zum Empfang des ersten Bytes der Anfrage des Kunden
rql	Millisekunde vom Verbindungsaufbau bis zum Empfang des letzten Bytes der Anfrage vom Client
tqf	Millisekunde vom Verbindungsaufbau bis zum Senden des ersten Bytes der Anfrage an den Real-Server

tql	Millisekunde vom Verbindungsaufbau bis zum Senden des letzten Bytes der Anfrage an den Real-Server
rsf	Millisekunde vom Verbindungsaufbau bis zum Empfang des ersten Bytes der Antwort vom Realserver
rsl	Millisekunde vom Verbindungsaufbau bis zum Empfang des letzten Bytes der Antwort vom Realserver
tsf	Millisekunde vom Verbindungsaufbau bis zum Senden des ersten Bytes der Antwort an den Client
tsl	Millisekunde vom Verbindungsaufbau bis zum Senden des letzten Bytes der Antwort an den Client
dis	Millisekunde vom Verbindungsaufbau bis zum Verbindungsabbau (beide Seiten - die letzte, die die Verbindung trennt)
Protokoll	Millisekunde von der Verbindung zu diesem Protokolleintrag, normalerweise gefolgt von (Lastausgleichspolitik und Begründung)
x-round-trip-time	Wie lange ALB in Sekunden gebraucht hat
x-closed-by	Durch welche Aktion wurde die Verbindung geschlossen (oder offen gehalten)
x-compress-Aktion	Wie die Kompression durchgeführt bzw. verhindert wurde
x-sc(Inhalts-Typ)	Inhalts-Typ der Antwort
x-cache-aktion	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 Netzwerk in der Bibliothek ermöglicht die Konfiguration der Netzwerkschnittstellen des ADC und ihres Verhaltens.

WICHTIG

Verwaltung virtueller Netzwerkschnittstellen in einer virtuellen Umgebung

Bei der Bereitstellung von VMs in einer virtualisierten Umgebung wie ESXi werden Netzwerkschnittstellen (z. B. eth0, eth1) automatisch erstellt und den Netzwerkadaptern der Hostkonfiguration zugeordnet (z. B. Netzwerkadapter 1, Netzwerkadapter 2). Diese Zuordnungen stimmen jedoch aufgrund von Betriebssystemregeln, die Schnittstellen an bestimmte MAC-Adressen binden, nicht immer überein. In diesem Abschnitt werden Schritte zur Verwaltung von Netzwerkschnittstellen auf dem Host beschrieben, um Unterbrechungen von Diensten zu vermeiden, wenn der Benutzer nicht auf die VM zugreifen kann.

Wichtige Überlegungen

1. **Persistenz der MAC-Adresse**:
    a. Das Betriebssystem weist Schnittstellennamen (z. B. eth0, eth1) auf der Grundlage von Regeln zu, die einen Namen mit einer bestimmten MAC-Adresse verknüpfen.
    b. Das Löschen und Neuanlegen einer VM-Netzwerkschnittstelle ohne Wiederverwendung der ursprünglichen MAC-Adresse kann zu einer inkonsistenten oder nicht funktionierenden Netzwerkkonfiguration führen.
2. **Interne Zuordnungen im ADC (EdgeOS)**:
    a. Virtuelle Netzwerkschnittstellen werden vom ADC (Application Delivery Controller) automatisch erkannt und intern abgebildet.
    b. Wenn eine Netzwerkschnittstelle vom VM-Host entfernt wird, können veraltete Zuordnungen im ADC zurückbleiben, wodurch der Verwaltungszugriff oder die Netzwerkdienste möglicherweise unterbrochen werden.

Empfohlene Schritte für die Hostkonfiguration

1. **Bevor Sie eine NIC entfernen**:
    a. Notieren Sie sich die MAC-Adresse der Schnittstelle, die Sie entfernen möchten. Diese kann in den Einstellungen der VM auf dem ESXi-Host eingesehen werden.
2. **Beim Hinzufügen einer Ersatz-NIC**:
    a. Weisen Sie die zuvor aufgezeichnete MAC-Adresse dem neuen Netzwerkadapter zu, um sicherzustellen, dass die Schnittstellen-Zuordnungen der VM konsistent bleiben.
3. **Verhindern Sie das versehentliche Löschen von kritischen NICs**:
    a. Ermitteln Sie, welche NICs kritischen ADC-Schnittstellen zugeordnet sind (z. B. ETH0 (Greenside) für den Verwaltungszugang). Vermeiden Sie es, diese NICs zu entfernen, wenn es nicht unbedingt notwendig ist.
4. **Überprüfen Sie die Konsistenz der MAC-Adresse**:
    a. Stellen Sie sicher, dass die den Netzwerkschnittstellen der VM zugewiesenen MAC-Adressen mit der erwarteten Konfiguration innerhalb des ADC übereinstimmen. Verwenden Sie die ESXi-Host-Tools, um diese Zuordnung zu bestätigen.
5. **Koordinieren Sie sich mit VM-Administratoren**:
    a. Wenn Änderungen erforderlich sind, die sich auf die interne VM-Konfiguration auswirken könnten, informieren Sie die VM-Administratoren, um sich auf mögliche Störungen vorzubereiten und sicherzustellen, dass die richtigen Zuordnungen beibehalten werden.

Beispiel-Szenario

1. **Ersteinrichtung**:
    a. ADC VM hat zwei NICs: NIC1 (MAC: 00:11:22:33:44:55) und NIC2 (MAC: 00:11:22:33:44:66).
2. **Aktion**: Entfernen Sie NIC1 und fügen Sie eine neue NIC (NIC3) hinzu.

    a. Weisen Sie NIC3 bei der Erstellung auf dem ESXi-Host die ursprüngliche MAC-Adresse (00:11:22:33:44:55) zu.
3. **Vermeidung von Auswirkungen**:
    a. Durch die Wiederverwendung der ursprünglichen MAC-Adresse bleiben die internen Zuordnungen des ADC (z. B. ETH0) konsistent, so dass es zu keiner Unterbrechung des Verwaltungszugangs oder der Netzwerkdienste kommt.

Bei der Verwaltung von Netzwerkschnittstellen in einer virtualisierten Umgebung ist es von entscheidender Bedeutung, die Konsistenz der MAC-Adresszuweisungen zu wahren. Wenn der Zugriff auf die VM nicht möglich ist, müssen alle notwendigen Schritte auf der Host-Seite durchgeführt werden, um einen nahtlosen Betrieb zu gewährleisten und Dienstunterbrechungen zu vermeiden. Stimmen Sie sich stets mit den zuständigen Administratoren ab, um potenzielle Auswirkungen effektiv anzugehen.

Vermeiden von häufigen vMotions für kritische Appliances

vMotion ist eine leistungsstarke Funktion von VMware, die die Live-Migration virtueller Maschinen (VMs) zwischen ESXi-Hosts ohne Ausfallzeiten ermöglicht. Obwohl vMotion für die Aufrechterhaltung der Flexibilität und Verfügbarkeit der Infrastruktur sehr nützlich ist, ist es nicht empfehlenswert, kritische Appliances wie Load Balancer häufig zu migrieren, insbesondere wenn sie aktiv ein hohes Volumen an Verbindungen verwalten.

Möglicherweise gibt es andere Technologien, die ähnlich sind und von anderen Anbietern bereitgestellt werden, aber für diesen Abschnitt gehen wir von VMware aus.

Warum häufige vMotion nicht empfohlen wird

1. **Unterbrechungen der Sitzung**:
    a. Lastausgleicher verwalten aktive Sitzungen zwischen Clients und Backend-Servern. Während einer vMotion-Operation wird der Netzwerkstatus für kurze Zeit neu initialisiert, wodurch diese Sitzungen möglicherweise unterbrochen werden.
    b. Die Unterbrechung kann zu Verbindungsabbrüchen führen, so dass die Clients ihre Sitzungen neu aufbauen müssen, was die Benutzerfreundlichkeit beeinträchtigen kann.
2. **Latenzzeit und Paketverlust**:
    a. Der Prozess der Migration einer VM beinhaltet die vorübergehende Unterbrechung und Synchronisierung ihres Speichers und Status. Bei Appliances, die Echtzeitverkehr verarbeiten, kann diese Pause zu Latenzzeiten oder sogar Paketverlusten führen.
    b. Bei Anwendungen, die auf Antworten mit geringer Latenz angewiesen sind, kann es zu Leistungseinbußen oder Timeouts kommen.
3. **Erhöhte Ressourcenauslastung**:
    a. vMotion erfordert CPU-, Speicher- und Netzwerkbandbreiten-Ressourcen für die Datensynchronisierung zwischen Quell- und Zielhosts.
    b. Häufige Migrationen können die Infrastrukturressourcen belasten und sich möglicherweise auf andere VMs und Services auswirken, die in derselben Umgebung gehostet werden.
4. **Auswirkungen auf Hochverfügbarkeitskonfigurationen**:
    a. In Umgebungen mit Hochverfügbarkeitskonfigurationen (HA) kann häufige vMotion mit Failover-Mechanismen in Konflikt geraten, was zu unerwartetem Verhalten oder Verzögerungen bei Failover-Aktionen führt.
5. **Operative Komplexität**:
    a. Das ständige Verschieben kritischer VMs erhöht die Komplexität der Netzwerkkonfigurationen, einschließlich VLAN-Zuordnungen und Firewall-Regeln, was zu Konfigurationsfehlern führen kann.

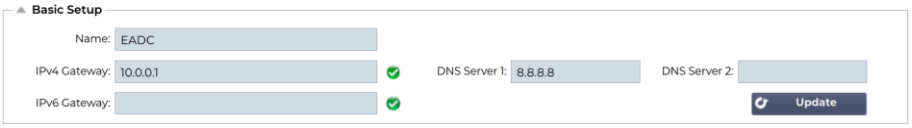
Empfehlungen für das Management kritischer Geräte

1. **Planen Sie vMotion-Vorgänge während der Wartungsfenster**:
    a. Planen Sie Migrationen in Zeiten mit geringem Datenverkehr, um die Auswirkungen auf aktive Sitzungen zu minimieren.
2. **Implementieren Sie Load Balancer Clustering**:

   a. Verwenden Sie Clustering- oder Hochverfügbarkeitskonfigurationen für Load Balancer, um Redundanz zu gewährleisten. Dadurch kann der Datenverkehr bei vMotion-Vorgängen nahtlos auf einen anderen Knoten umgeleitet werden.
3. **Infrastruktur-Ressourcen überwachen**:
   a. Vergewissern Sie sich, dass ausreichend CPU, Speicher und Netzwerkbandbreite verfügbar sind, bevor Sie vMotion initiieren, um Ressourcenkonflikte zu vermeiden.
4. **Minimierung der Migrationshäufigkeit**:
   a. Beschränken Sie die vMotion von kritischen Appliances auf Szenarien, in denen sie absolut notwendig ist, wie z. B. die Wartung von Hosts oder die Wiederherstellung bei einem Ausfall.
5. **Test vor der Produktion**:
   a. Testen Sie vMotion-Vorgänge in einer Staging-Umgebung, um deren Auswirkungen auf aktive Sitzungen zu verstehen und sicherzustellen, dass die Konfigurationen optimiert sind.

vMotion ist zwar ein unschätzbares Tool für das VM-Management, sollte aber mit Bedacht für kritische Appliances wie Load Balancer eingesetzt werden. Häufige Migrationen können die Services unterbrechen, die Latenz erhöhen und die Ressourcen belasten. Durch sorgfältige Planung von vMotion-Vorgängen und den Einsatz von Strategien wie Clustering und Wartungsplanung können Sie eine zuverlässige Servicebereitstellung gewährleisten und das Risiko von Unterbrechungen minimieren.

Grundlegende Einrichtung



ALB Name

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

IPv4-Gateway

Geben Sie die IPv4-Gateway-Adresse an. Diese Adresse muss sich in demselben Subnetz befinden wie ein vorhandener Adapter. Wenn Sie ein falsches Gateway eingeben, wird ein weißes Kreuz in einem roten Kreis angezeigt. 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 in demselben Subnetz befinden wie ein vorhandener Adapter. Wenn Sie ein falsches Gateway eingeben, wird ein weißes Kreuz in einem roten Kreis angezeigt. 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 und DNS-Server 2

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

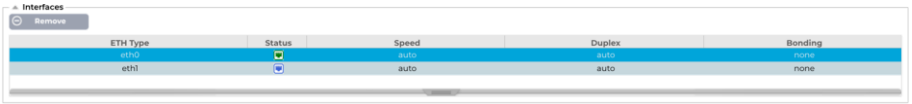
Details zum Adapter

In diesem Bereich des Netzwerkfensters werden die Netzwerkschnittstellen angezeigt, die in Ihrer ADC Appliance installiert sind. Sie können nach Bedarf Adapter hinzufügen und entfernen.

Säule	**Beschreibung**
Adapter	In dieser Spalte werden die auf Ihrer Appliance installierten physischen Adapter angezeigt. Wählen Sie einen Adapter aus der Liste der verfügbaren Adapter aus, indem Sie darauf klicken - ein Doppelklick versetzt die Zeile der Liste 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 der Endstationen, wenn diese nicht am gleichen Netzwerk-Switch angeschlossen sind.
IP-Adresse	Doppelklicken Sie, um die IP-Adresse hinzuzufügen, die mit der Adapterschnittstelle verbunden ist. 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 Dezimalschreibweise sein. Beispiel 255.255.255.0
Gateway	Hinzufügen eines Gateways für die Schnittstelle. Wenn dies hinzugefügt wird, richtet die ADC eine einfache Richtlinie ein, die es ermöglicht, dass Verbindungen, die von dieser Schnittstelle initiiert werden, über diese Schnittstelle an den angegebenen Gateway-Router weitergeleitet werden. Auf diese Weise kann der 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 gerne nach Ihren Vorstellungen ändern.
Web-Konsole	Doppelklicken Sie auf die Spalte und aktivieren Sie das Kontrollkästchen, um die Schnittstelle als Verwaltungsadresse für die Web-Konsole der grafischen Benutzeroberfläche festzulegen. Seien Sie bitte sehr vorsichtig, wenn Sie die Schnittstelle ändern, die die Web-Konsole abhören soll. Sie müssen das richtige Routing eingerichtet haben oder sich im selben Subnetz wie die neue Schnittstelle befinden, um die Webkonsole nach der Änderung zu erreichen. Die einzige Möglichkeit, dies wieder zu ändern, besteht darin, die Befehlszeile aufzurufen und den Befehl set greenside einzugeben. Dadurch werden alle Schnittstellen mit Ausnahme von eth0 gelöscht.

Schnittstellen

Der Abschnitt "Schnittstellen" im Bereich "Netzwerk" ermöglicht die Konfiguration bestimmter Elemente, die die Netzwerkschnittstelle betreffen. 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.



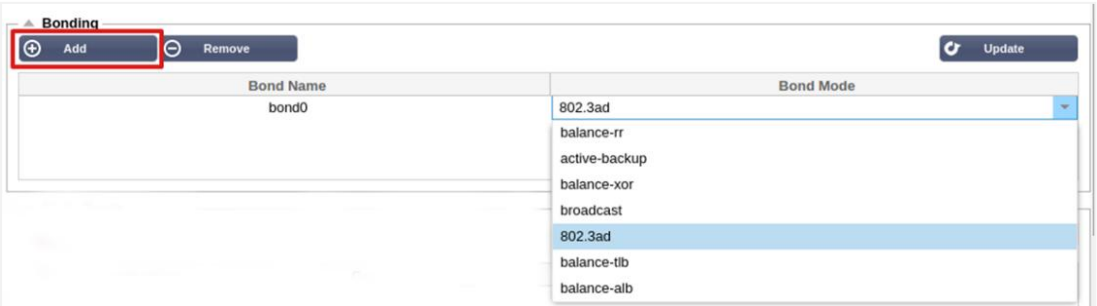
Säule	Beschreibung
ETH-Typ	Dieser Wert gibt den internen Betriebssystemverweis auf die Netzwerkschnittstelle an. Dieses Feld kann nicht angepasst werden. Die Werte beginnen mit ETH0 und werden in Abhängigkeit von der Anzahl der Netzwerkschnittstellen fortgesetzt.
Status	Diese grafische Anzeige zeigt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

Bindung

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-Bonded-Schnittstelle. Durch Bonding können zwei oder mehr Netzwerkschnittstellen als eine agieren, den Durchsatz erhöhen und Redundanz oder Ausfallsicherheit bieten.

Der ADC-Kernel verfügt über einen integrierten Bonding-Treiber, mit dem mehrere physische Netzwerkschnittstellen zu einer einzigen logischen Schnittstelle zusammengefasst werden können (z. B. Zusammenfassung von eth0 und eth1 zu bond0). Für jede gebondete Schnittstelle können Sie den Modus und die Link-Überwachungsoptionen festlegen. 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.



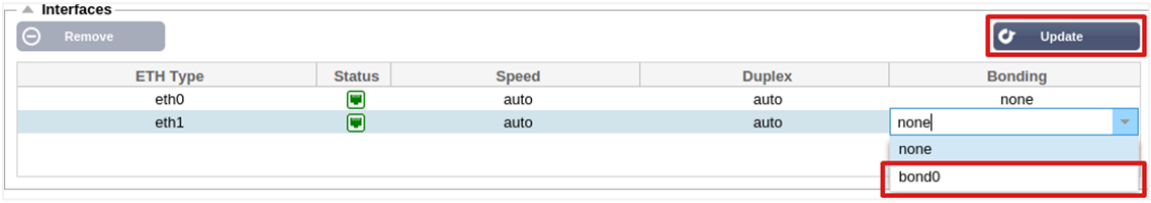
Erstellen eines Bonding-Profils

- Klicken Sie auf die Schaltfläche Hinzufügen, um eine neue Anleihe hinzuzufügen.

- Geben Sie einen Namen für die Bonding-Konfiguration an
- Wählen Sie den gewünschten Bonding-Modus

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. Eth0 bleibt als Verwaltungsschnittstelle für sich allein.

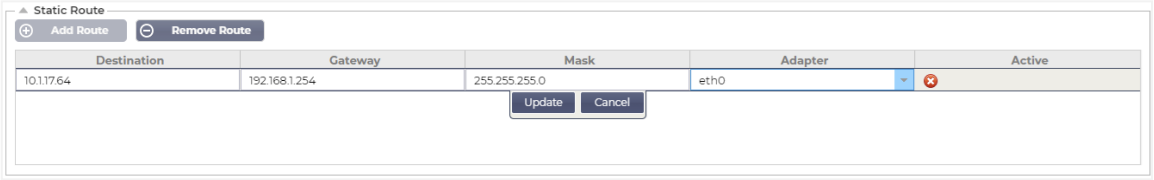


Modi der Bindung

Bonding-Modus	Beschreibung
balance-rr:	Die Pakete werden nacheinander über jede Schnittstelle gesendet/empfangen.
aktive Datensicherung:	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 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 haben und alle Slaves im aktiven Aggregator gemäß der 802.3ad-Spezifikation nutzen.
balance-tlb:	Der Bonding-Modus "Adaptiver Übertragungslastausgleich": Ermöglicht Kanalbündelung, die keine spezielle Switch-Unterstützung erfordert. Der ausgehende Verkehr wird entsprechend der aktuellen Last (berechnet im Verhältnis zur Geschwindigkeit) auf jeden 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 Verbund, so dass verschiedene Peers unterschiedliche Hardwareadressen für den Server verwenden.

Statische Route

Es kann vorkommen, dass Sie statische Routen für bestimmte Subnetze in Ihrem Netzwerk erstellen müssen. Die ADC bietet Ihnen die Möglichkeit, dies mit dem Modul "Statische Routen" zu tun.



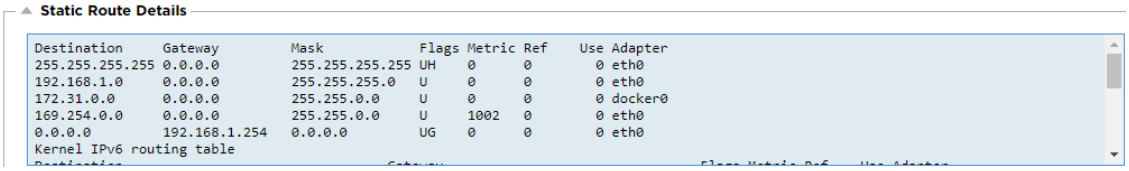
Hinzufügen einer statischen Route

- Klicken Sie auf die Schaltfläche Route hinzufügen
- Füllen Sie das Feld aus, wobei Sie sich an den Angaben in der nachstehenden Tabelle orientieren.
- Klicken Sie abschließend auf die Schaltfläche Aktualisieren.

Feld	Beschreibung
Reiseziel	Geben Sie die Zielnetzadresse in dezimaler Punktschreibweise ein. Beispiel 123.123.123.5
Gateway	Geben Sie die IPv4-Adresse des Gateways in punktierter Dezimalschreibweise ein. Beispiel 10.4.8.1
Maske	Geben Sie die Ziel-Subnetzmaske in dezimaler Punktschreibweise 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 auf dieser Schnittstelle nicht erreicht werden kann. Vergewissern Sie sich, dass Sie eine Schnittstelle und eine IP-Adresse im selben Netzwerk wie das Gateway eingerichtet haben

Details zur statischen Route

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



Erweiterte Netzwerkeinstellungen

Was ist Nagle?

Der Nagle-Algorithmus, auch bekannt als TCP-No-Delay-Algorithmus, ist eine Technik, die in der Netzkommunikation eingesetzt wird, um die Anzahl der erneut gesendeten Pakete aufgrund von Daten, die nicht in Ordnung sind, zu verringern. Der Algorithmus verzögert den Versand kleinerer Pakete, wenn für vorherige Pakete keine Bestätigung eingegangen ist. Dadurch wird sichergestellt, dass die Daten in der richtigen Reihenfolge ankommen, und die Belastung des Netzes verringert.

Siehe **WIKIPEDIA-ARTIKEL ÜBER NAGLE**

Server Nagle

Aktivieren Sie dieses Kästchen, um die Einstellung "Server Nagle" zu aktivieren. 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

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

SNAT

SNAT steht für Source Network Address Translation (Übersetzung der Quellennetzwerkadressen), und die Implementierung von SNAT wird von verschiedenen Anbietern leicht variiert. Eine einfache Erklärung des EdgeADC SNAT wäre wie folgt.

Unter normalen Umständen würden eingehende Anfragen an das VIP weitergeleitet, das die Quell-IP der Anfrage sehen würde. Hätte ein Browser-Endpunkt beispielsweise die IP-Adresse 81.71.61.51, wäre diese für das VIP sichtbar.

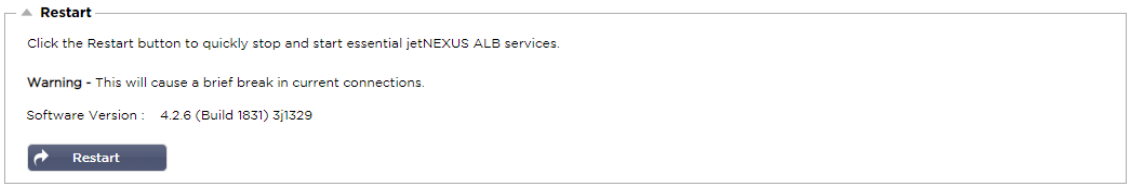
Wenn SNAT in Kraft ist, wird die ursprüngliche Quell-IP der Anfrage vor dem VIP verborgen, und stattdessen sieht es die IP-Adresse, die in der SNAT-Regel angegeben ist. Somit kann SNAT in den Modi Layer 4 und Layer 7 für den Lastausgleich verwendet werden.

Feld	Beschreibung
Quelle IP	Die Quell-IP-Adresse ist optional und kann entweder eine Netzwerk-IP-Adresse (mit /mask) oder eine einfache IP-Adresse sein. Die Maske kann entweder eine Netzwerkmaske oder eine einfache Zahl sein, die die Anzahl der 1en auf der linken Seite der Netzwerkmaske angibt. Eine Maske von /24 entspricht also 255.255.255.0.
Ziel-IP	Die Ziel-IP-Adresse ist optional und kann entweder eine Netzwerk-IP-Adresse (mit /mask) oder eine einfache IP-Adresse sein. Die Maske kann entweder eine Netzwerkmaske oder eine einfache Zahl sein, die die Anzahl der 1en auf der linken Seite der Netzwerkmaske angibt. Eine Maske von /24 entspricht also 255.255.255.0.
Quelle: Hafen	Der Quellport ist optional, er kann eine einzelne Zahl sein, die nur diesen Port angibt, 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, die nur diesen Anschluss angibt, 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 wollen. Um genauer zu sein, empfehlen wir Ihnen, spezifisch zu sein.
SNAT zu IP	SNAT to 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 Hafen	Die Angabe SNAT to Port ist optional, sie kann eine einzelne Zahl sein, die nur diesen Anschluss angibt, oder sie kann einen Bindestrich enthalten, der einen Bereich von Anschlüssen angibt. Beispiele: 80 oder 5900-5905.
Anmerkungen	Hier können Sie einen freundlichen Namen eingeben, um sich daran zu erinnern, warum die Regeln existieren. Dies ist auch für die Fehlersuche im Syslog nützlich.

Strom

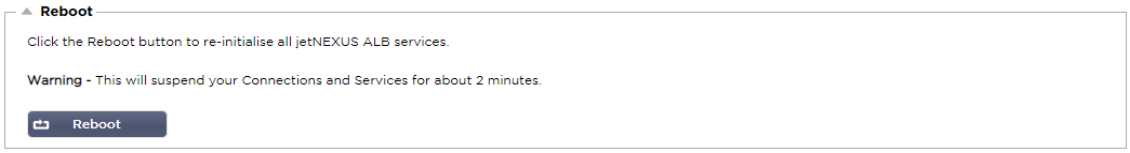
Mit dieser Funktion des ADC-Systems können Sie auch verschiedene stromverbrauchsbezogene Aufgaben mit Ihrem ADC durchführen.

Neustart



Diese Einstellung löst einen globalen Neustart aller Dienste aus und unterbricht folglich alle derzeit aktiven Verbindungen. Alle Dienste werden nach einer kurzen Zeitspanne automatisch wieder aufgenommen, aber der Zeitplan hängt davon ab, wie viele Dienste konfiguriert sind. Es wird ein Pop-up-Fenster angezeigt, in dem Sie aufgefordert werden, den Neustart zu bestätigen.

Neustart



Durch Klicken auf die Schaltfläche Neustart wird das ADC ausgeschaltet und automatisch wieder in einen aktiven Zustand versetzt. Es wird ein Pop-up-Fenster angezeigt, in dem Sie aufgefordert werden, den Neustart zu bestätigen.

Ausschalten

Wenn Sie auf die Schaltfläche Ausschalten klicken, wird der ADC ausgeschaltet. Wenn es sich um eine Hardware-Appliance handelt, müssen Sie physischen Zugang zum Gerät haben, um es wieder einzuschalten. Es wird ein Pop-up-Fenster angezeigt, in dem Sie aufgefordert werden, die Abschaltaktion zu bestätigen.

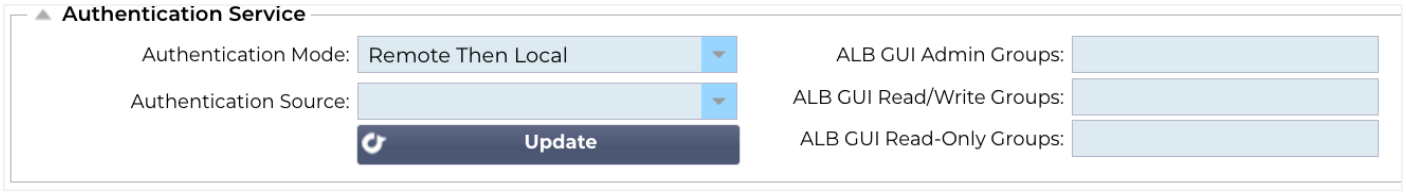
Sicherheit

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

SSH

Option	Beschreibung
Sichere Shell-Fernverbindung	Bitte kreuzen Sie das Kästchen an, wenn Sie über SSH Zugang zum ADC erhalten möchten. "Putty" ist eine hervorragende Anwendung dafür.

Authentifizierungsdienst



In den meisten Unternehmen ist es erforderlich, dass der Zugriff auf die Verwaltungsschnittstelle der ADC über die unternehmenseigenen Authentifizierungsdienste erfolgt.

Für solche Szenarien haben wir die hier beschriebene Funktion Authentifizierungsdienst bereitgestellt. Diese Funktion arbeitet sowohl mit lokalen Verzeichnisdiensten als auch mit externen Diensten wie SAML.

Option	Beschreibung
Authentifizierungsmodus	Nur lokal: Dies ist der Standardmodus und verwendet die lokale Datenbank innerhalb des ADC, zum Beispiel für den Benutzer admin. Fern und dann Lokal: Die ADC versucht, den Benutzer anhand des im Feld Authentifizierungsquelle angegebenen Remote-Authentifizierungsservers zu überprüfen. Wenn dies nicht erfolgreich ist, wird die lokale Datenbank als Quelle für die Überprüfung verwendet.
Quelle der Authentifizierung	In diesem Dropdown-Menü können Sie einen der Authentifizierungsserver auswählen, die Sie unter Bibliothek > Authentifizierung definiert haben.
ALB GUI Verwaltungsgruppen	Geben Sie die zulässigen Administratorgruppen an.
ALB GUI Lese-/Schreibgruppen	Geben Sie die erlaubten Lese-/Schreibgruppen an
ALB GUI Schreibgeschützte Gruppen	Geben Sie die erlaubten Nur-Lese-Gruppen an.

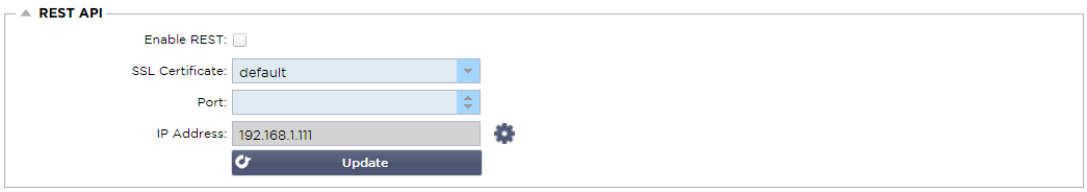
Web-Konsole

SSL-Zertifikat Wählen Sie ein Zertifikat aus der Dropdown-Liste 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 ADC erstellen oder eines aus dem Abschnitt **SSL-ZERTIFIKATE** importieren.

Option	**Beschreibung**
Sicherer Hafen	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 der ADC oder die Datenextraktion aus der ADC ermöglicht. Der Begriff REST steht für Representational State Transfer und wurde vom Informatiker Roy Fielding entwickelt.



Option	**Beschreibung**
REST aktivieren	Aktivieren Sie dieses Kästchen, um den Zugriff über die REST-API zu ermöglichen. Beachten Sie, dass Sie auch konfigurieren müssen, auf welchem Adapter REST aktiviert ist. Siehe den Hinweis auf den Cog-Link unten.
SSL-Zertifikat	Wählen Sie ein Zertifikat für den REST-Dienst. In der Dropdown-Liste werden alle auf dem ADC installierten Zertifikate angezeigt.
Hafen	Legen Sie den Port für den REST-Dienst fest. Es ist ratsam, 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.
Kogge Link	Wenn Sie auf diesen Link klicken, gelangen Sie zur Seite Netzwerk, auf der Sie einen Adapter für den REST konfigurieren können.

Dokumentation für REST API

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

Hinweis: Wenn Sie auf der Swagger-Seite Fehler erhalten, liegt das daran, dass sie ein Problem mit der Unterstützung von 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

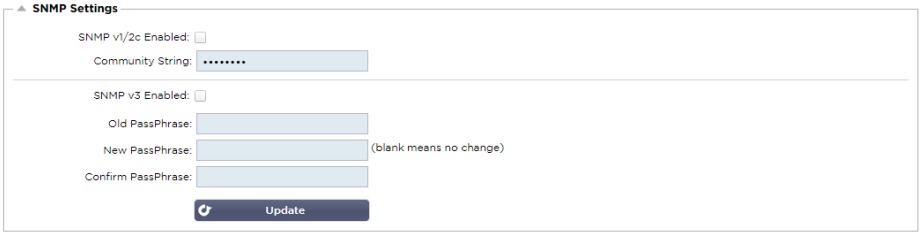
- Befehl

```
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 in der Lage ist, mit Geräten zu kommunizieren, die mit SNMP ausgestattet sind.

SNMP-Einstellungen



Option	Beschreibung
SNMP v1 / V2C	Aktivieren Sie das Kontrollkästchen, um die V1/V2C-MIB zu aktivieren. SNMP v1 ist konform mit RFC-1157. SNMP V2c ist konform mit RFC-1901-1908
SNMP v3	Aktivieren Sie das Kontrollkästchen, um die V3-MIB zu aktivieren. RFC-3411-3418. Der Benutzername für v3 ist admin. Beispiel:- snmpwalk -v3 -u admin -A jetnexus -l authNoPriv 192.168.1.11 1.3.6.1.4.1.38370
Gemeinschaftlicher 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 lautet 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. MIBs beschreiben die Struktur der Verwaltungsdaten und verwenden hierarchische Objektbezeichner (OID). Jede OID kann über eine SNMP-Verwaltungsanwendung gelesen werden.

MIB herunterladen

Die MIB kann hier heruntergeladen werden:

ADC OID

ROOT OID

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

Unsere OIDs

```
.38370 jetnexusMIB
    .1 jetnexusData   (1.3.6.1.4.1.38370.1)
        .1 jetnexusGlobal (1.3.6.1.4.1.38370.1.1)
        .2 jetnexusVirtualServices   (1.3.6.1.4.1.38370.1.2)
        .3 jetnexusServer   (1.3.6.1.4.1.38370.1.3)
            .1 jetnexusGlobal   (1.3.6.1.4.1.38370.1.1)
                .1 jetnexusOverallInputBytes   (1.3.6.1.4.1.38370.1.1.1.0)
                .2 jetnexusOverallOutputBytes   (1.3.6.1.4.1.38370.1.1.2.0)
                .3 jetnexusCompressedInputBytes   (1.3.6.1.4.1.38370.1.1.3.0)
                .4 jetnexusCompressedOutputBytes   (1.3.6.1.4.1.38370.1.1.4.0)
```

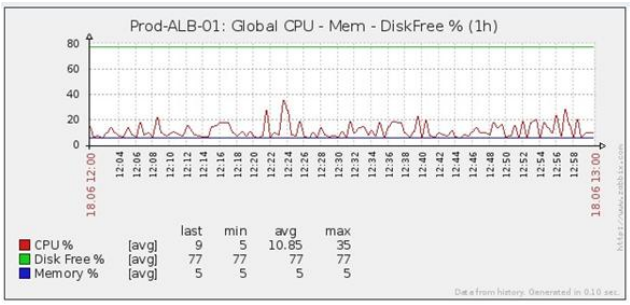
.5 **jetnexusVersionInfo** (1.3.6.1.4.1.38370.1.1.5.0)
.6 **jetnexusTotalClientConnections** (1.3.6.1.4.1.38370.1.1.6.0)
.7 **jetnexusCpuPercent** (1.3.6.1.4.1.38370.1.1.7.0)
.8 **jetnexusDiskFreePercent** (1.3.6.1.4.1.38370.1.1.8.0)
.9 **jetnexusMemoryPercent** (1.3.6.1.4.1.38370.1.1.9.0)
.10 **jetnexusCurrentConnections** (1.3.6.1.4.1.38370.1.1.10.0)

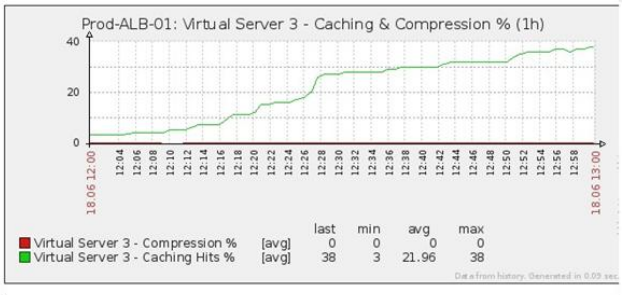
.2 **jetnexusVirtualServices** (1.3.6.1.4.1.38370.1.2)
.1 **jnvirtualserviceEntry** (1.3.6.1.4.1.38370.1.2.1)
.1 **jnvirtualserviceIndexvirtualservice** (1.3.6.1.4.1.38370.1.2.1.**1**)
.2 **jnvirtualserviceVSAddrPort** (1.3.6.1.4.1.38370.1.2.1.**2**)
.3 **jnvirtualserviceOverallInputBytes** (1.3.6.1.4.1.38370.1.2.1.**3**)
.4 **jnvirtualserviceOverallOutputBytes** (1.3.6.1.4.1.38370.1.2.1.**4**)
.5 **jnvirtualserviceCacheBytes** (1.3.6.1.4.1.38370.1.2.1.**5**)
.6 **jnvirtualserviceCompressionPercent** (1.3.6.1.4.1.38370.1.2.1.**6**)
.7 **jnvirtualservicePresentClientConnections** (1.3.6.1.4.1.38370.1.2.1.**7**)
.8 **jnvirtualserviceHitCount** (1.3.6.1.4.1.38370.1.2.1.**8**)
.9 **jnvirtualserviceCacheHits** (1.3.6.1.4.1.38370.1.2.1.**9**)
.10 **jnvirtualserviceCacheHitsPercent** (1.3.6.1.4.1.38370.1.2.1.**10**)
.11 **jnvirtualserviceVSStatus** (1.3.6.1.4.1.38370.1.2.1.**11**)

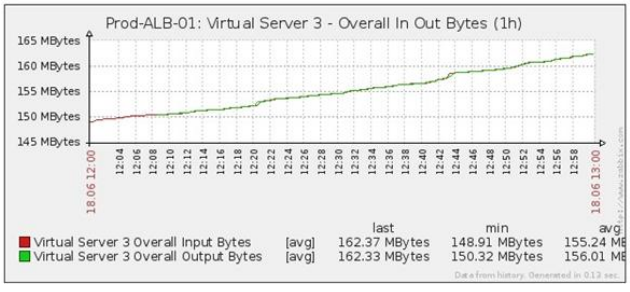
.3 **jetnexusRealServer** (1.3.6.1.4.1.38370.1.3)
.1 **jnrealserverEntry** (1.3.6.1.4.1.38370.1.3.**1**)
.1 **jnrealserverIndexVirtualService** (1.3.6.1.4.1.38370.1.3.1.**1**)
.2 **jnrealserverIndexRealServer** (1.3.6.1.4.1.38370.1.3.1.**2**)
.3 **jnrealserverChAddrPort** (1.3.6.1.4.1.38370.1.3.1.**3**)
.4 **jnrealserverCSAddrPort** (1.3.6.1.4.1.38370.1.3.1.**4**)
.5 **jnrealserverOverallInputBytes** (1.3.6.1.4.1.38370.1.3.1.**5**)
.6 **jnrealserverOverallOutputBytes** (1.3.6.1.4.1.38370.1.3.1.**6**)
.7 **jnrealserverCompressionPercent** (1.3.6.1.4.1.38370.1.3.1.**7**)
.8 **jnrealserverPresentClientConnections** (1.3.6.1.4.1.38370.1.3.1.**8**)
.9 **jnrealserverPoolUsage** (1.3.6.1.4.1.38370.1.3.1.**9**)
.10 **jnrealserverHitCount** (1.3.6.1.4.1.38370.1.3.1.**10**)
.11 **jnrealserverRSStatus** (1.3.6.1.4.1.38370.1.3.1.**11**)

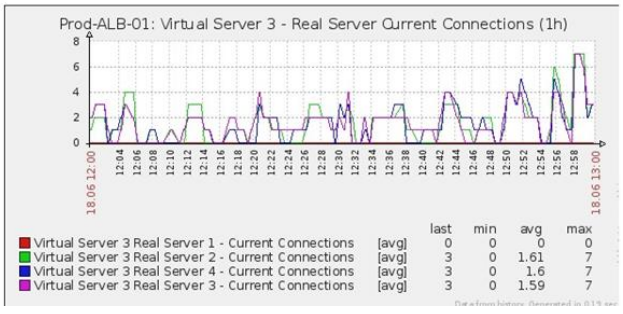
Historische Diagramme

Die beste Verwendung für die benutzerdefinierte SNMP-MIB des ADC ist die Möglichkeit, das historische Diagramm auf eine Managementkonsole Ihrer Wahl auszulagern. Nachfolgend finden Sie einige Beispiele von Zabbix, die einen ADC für verschiedene oben aufgeführte OID-Werte abfragen.









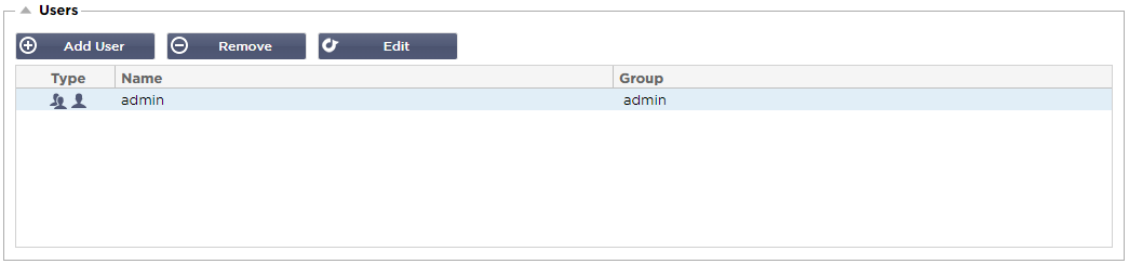
Benutzer und Audit-Protokolle

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

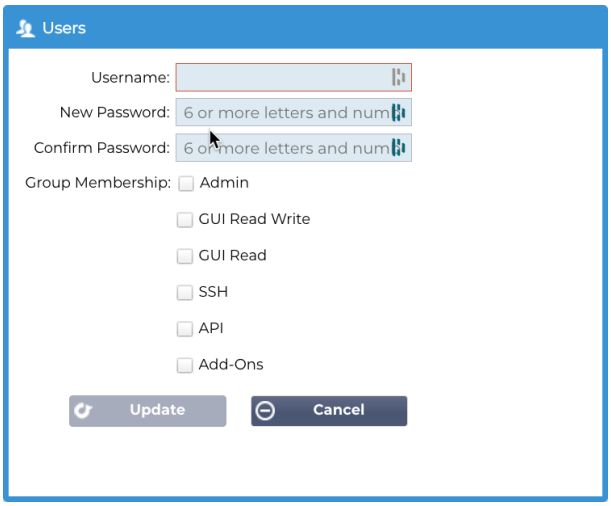
Es gibt einen Standardbenutzer namens **admin**, den Sie bei der Erstkonfiguration des ADC verwenden. Das Standardpasswort für admin lautet **jetnexus**.

Benutzer

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



Benutzer hinzufügen



Klicken Sie auf die Schaltfläche Benutzer hinzufügen (siehe Abbildung oben), um das Dialogfeld Benutzer hinzufügen aufzurufen.

Parameter	Beschreibung/Verwendung
Benutzername	Geben Sie einen Benutzernamen Ihrer Wahl ein. Der Benutzername muss die folgenden Bedingungen erfüllen: • Mindestanzahl von Zeichen 1 • Maximale Anzahl von Zeichen 32 • Die Buchstaben können sowohl groß als auch klein geschrieben werden. • Es können Zahlen verwendet werden. • Symbole sind nicht erlaubt
Passwort	Geben Sie ein **sicheres** Passwort ein, das den unten aufgeführten Anforderungen entspricht. • Mindestanzahl von Zeichen 6 • Maximale Anzahl von Zeichen 32 • Es muss mindestens eine Kombination aus Buchstaben und Zahlen verwendet werden. • Die Buchstaben können groß oder klein geschrieben werden. • Symbole sind erlaubt, außer denen im folgenden Beispiel **£**, **%**, &, **<** , **>**
Bestätigen Sie Ihr Passwort	Bestätigen Sie das Passwort erneut, um sicherzustellen, dass es korrekt ist.
Mitgliedschaft in der Gruppe	Markieren Sie die Gruppe, der der Benutzer angehören soll. • Admin - Diese Gruppe kann alles tun. • GUI Read Write - Benutzer in dieser Gruppe können auf die GUI zugreifen und Änderungen über die GUI vornehmen. • GUI Lesen - Benutzer in dieser Gruppe können auf die GUI zugreifen und nur Informationen anzeigen. 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 enthält. • API - Benutzer dieser Gruppe haben Zugang zu den programmierbaren Schnittstellen SOAP und REST. REST wird ab Software-Version 4.2.1 verfügbar sein. • Add-Ons - Die Berechtigung zum Zugriff auf Add-On-Konfigurationen wird erteilt.

Benutzertyp

	Lokaler Benutzer Die ADC in der Rolle Stand-Alone oder Manual H/A erstellt nur lokale Benutzer. Standardmäßig ist ein lokaler Benutzer namens "admin" Mitglied der Gruppe admin. Aus Gründen der Abwärtskompatibilität kann dieser Benutzer nie gelöscht werden. Sie können das Passwort dieses Benutzers ändern oder ihn löschen, aber Sie können den letzten lokalen Administrator nicht 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 nicht zwischen den Rollen "Cluster", "Manuell" oder "Stand-Alone" wechseln.
	Cluster und lokaler Benutzer Alle Benutzer, die in der Einzelplatz- oder manuellen Rolle erstellt wurden, werden in den Cluster kopiert. Wenn der ADC den Cluster später verlässt, bleiben nur noch die lokalen Benutzer übrig. Es gilt das zuletzt für den Benutzer konfigurierte Passwort.

Entfernen eines Benutzers

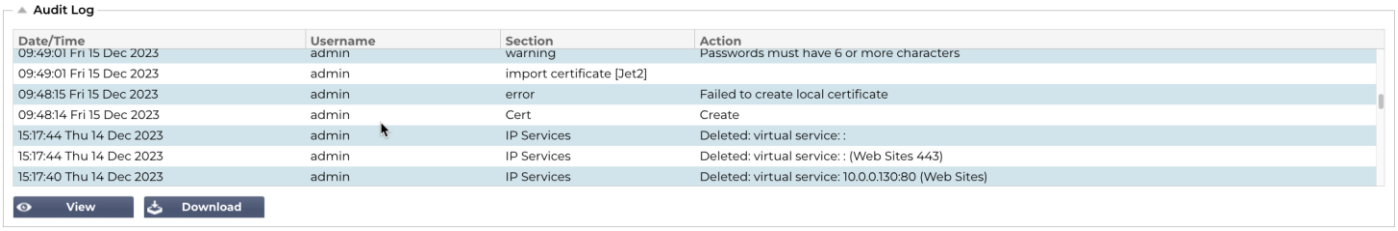
- Markieren Sie einen bestehenden Benutzer.
- Klicken Sie auf Entfernen.
- Sie können den derzeit angemeldeten Benutzer nicht löschen.
- Sie können den letzten lokalen Benutzer in der Administratorgruppe nicht entfernen.
- Sie können den letzten verbleibenden Cluster-Benutzer in der Administratorgruppe nicht entfernen.
- Aus Gründen der Abwärtskompatibilität können Sie den Benutzer admin nicht löschen.
- Wenn Sie den ADC aus dem Cluster entfernen, werden alle Benutzer mit Ausnahme der lokalen Benutzer gelöscht.

Bearbeiten eines Benutzers

- Markieren Sie einen bestehenden Benutzer.
- Klicken Sie auf Bearbeiten
- Sie können die Gruppenzugehörigkeit des Benutzers ändern, indem Sie die entsprechenden Kästchen ankreuzen und aktualisieren.
- Sie können auch das Passwort eines Benutzers ändern, sofern Sie über Administratorrechte verfügen.

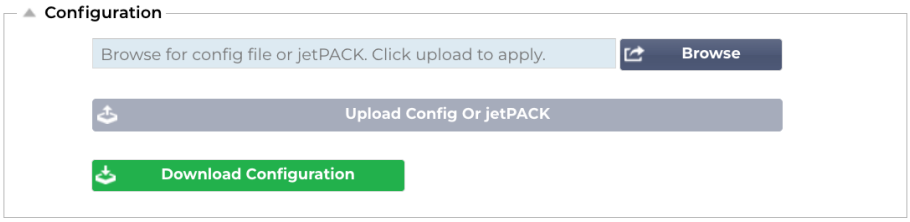
Audit-Protokoll

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



Fortgeschrittene

Konfiguration



Es ist immer die beste Praxis, 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 bereitgestellt, um Ihre Arbeit zu vereinfachen. Auch diese können mit dem Konfigurationsmodul auf den ADC hochgeladen werden.

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

VORSICHT!

Die Bearbeitung der Konfigurationsdatei des EdgeADC ist nur für geschulte Experten vorgesehen. Sollten Sie sich entscheiden, die Konfigurationsdatei selbst zu bearbeiten, und es kommt zu einem technischen Problem, kann der technische Support von Edgenexus das Produkt nicht mehr unterstützen.

Herunterladen einer Konfiguration

- Um die aktuelle Konfiguration des ADC herunterzuladen, drücken Sie die Schaltfläche Konfiguration herunterladen.
- Es erscheint ein Pop-up-Fenster, das Sie auffordert, 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".
- Die ADC wird die Konfiguration hochladen und anwenden und dann den Browser aktualisieren. Wenn der Browser nicht automatisch aktualisiert wird, klicken Sie bitte auf "Aktualisieren" im Browser.
- Nach Fertigstellung werden Sie zur Dashboard-Seite weitergeleitet.

Kritisch: Es ist wichtig, dass Sie nicht versuchen, die Konfiguration von einem ADC auf einen anderen zu kopieren, ohne sich vorher mit dem Edgenexus-Support zu beraten. Andernfalls kann Ihr ADC nicht mehr wiederhergestellt werden.

Hochladen eines JetPACKs

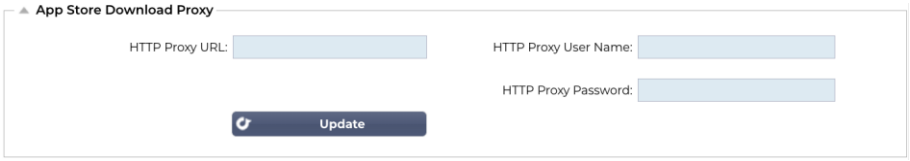
- Ein JetPACK ist ein Satz von Konfigurationsaktualisierungen der bestehenden Konfiguration.
- Ein JetPACK kann so klein sein wie eine Änderung des TCP-Timeout-Wertes bis hin zu einer kompletten anwendungsspezifischen Konfiguration wie Microsoft Exchange oder Microsoft Lync.
    - Sie können ein JetPACK über das Support-Portal am Ende dieses Handbuchs beziehen.
- Suchen Sie die Datei jetPACK.txt.
- Klicken Sie auf Hochladen.

- Der Browser wird nach dem Hochladen automatisch aktualisiert.
- Nach Fertigstellung werden Sie zur Dashboard-Seite weitergeleitet.
- Bei komplexeren Installationen wie Microsoft Lync usw. kann der Import länger dauern.

Globale Einstellungen

Im Abschnitt "Globale Einstellungen" können Sie verschiedene Elemente ändern, darunter auch die kryptografische SSL-Bibliothek.

App Store Download Proxy



Gesicherte Netzwerke erlauben im Allgemeinen keinen Zugriff auf das Internet, es sei denn, die Daten werden über die Proxy-Server des Unternehmens gesendet. Der EdgeADC ist ein Perimeter-Gerät und muss in der Lage sein, auf die Edgenexus-Server zuzugreifen, um die Gültigkeit des Supports festzustellen und auch auf den App Store zuzugreifen, um Updates und Anwendungen herunterzuladen.

HTTP-Proxy-URL

In diesem Feld können Sie den Hostnamen oder die IP-Adresse Ihres Proxyservers angeben.

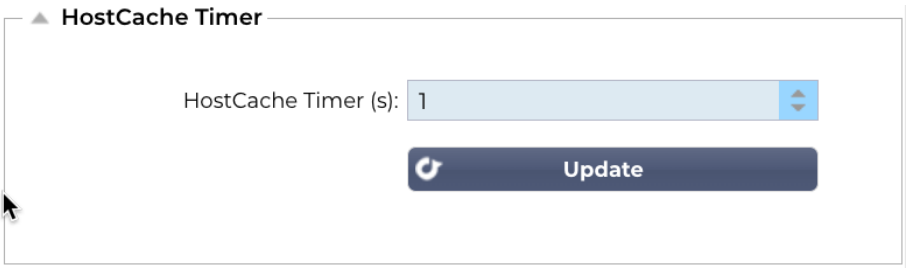
HTTP-Proxy-Benutzername

Geben Sie den Benutzernamen ein, der speziell für die Autorisierung von Geräten und Benutzern verwendet wird, die den Proxyserver nutzen.

HTTP-Proxy-Kennwort

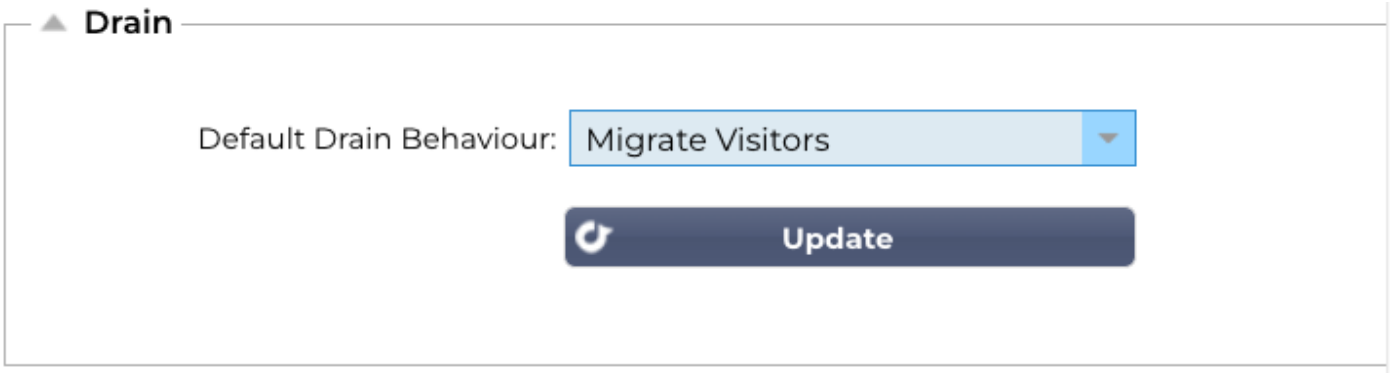
Der in HTTP-Proxy-Benutzername angegebene Benutzername ist ein gesicherter Benutzername. Sie müssen das zugehörige Passwort in dieses Feld eingeben.

Host-Cache-Timer



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 geleert, wenn ein Real Server ausfällt. Wenn Sie diesen Wert auf Null setzen, wird der Cache nicht geleert. Es gibt keinen Höchstwert für diese Einstellung.

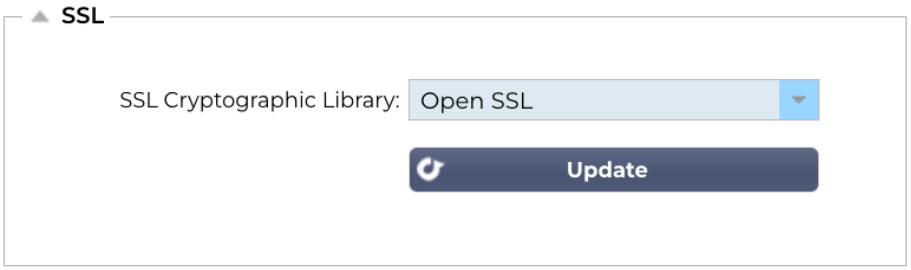
Abfluss



Wenn ein Real Server in den Drain-Modus versetzt wird, ist es immer besser, das Verhalten des an ihn gesendeten Datenverkehrs kontrollieren zu können. Das Menü Drain Behaviour ermöglicht die Auswahl des Verkehrsverhaltens für jeden virtuellen Dienst. Die Optionen sind:

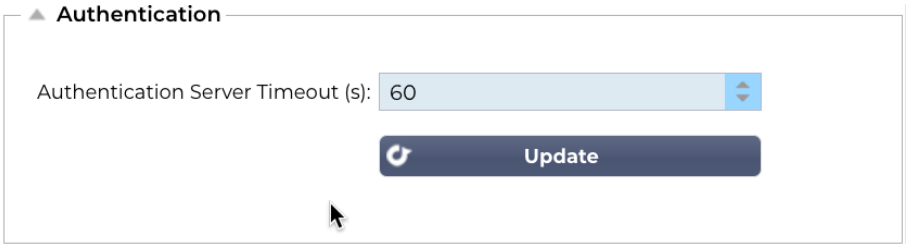
Option	Beschreibung
Persistenzgesteuert	Dies ist die Standardauswahl. Immer wenn der Benutzer die Persistenzsitzung besucht, wird sie verlängert. Bei einer 24-stündigen Nutzung ist es möglich, dass der Abfluss nie erfolgt. Wenn die Anzahl der Verbindungen zum realen Server jedoch 0 erreicht, wird der Abfluss beendet, die Persistenzsitzungen werden gelöscht, und alle Besucher werden bei der nächsten Verbindung neu abgeglichen.
Besucher migrieren	Persistente Sitzung wird bei erneutem Verbindungsaufbau ignoriert - (altes Verhalten vor 2022) Neue TCP-Verbindungen (unabhängig davon, ob sie Teil einer bestehenden Sitzung sind oder nicht) werden immer zu einem realen Online-Server hergestellt. Wenn die Persistenzsitzung zu einem leeren realen Server gehörte, wird sie überschrieben. Der virtuelle Dienst ignoriert die Persistenz neuer Verbindungen, und die Lastverteilung erfolgt auf einen neuen Server.
Sitzungen im Ruhestand	Dauerhafte Sitzungen werden nicht verlängert. Eingehende Benutzerverbindungen werden dem gewünschten Server zugewiesen, aber ihre Persistenzsitzung wird nicht verlängert. Wenn also die Zeit der Persistenzsitzung überschritten ist, werden sie wie eine neue Verbindung behandelt und auf einen anderen Server verschoben.

SSL



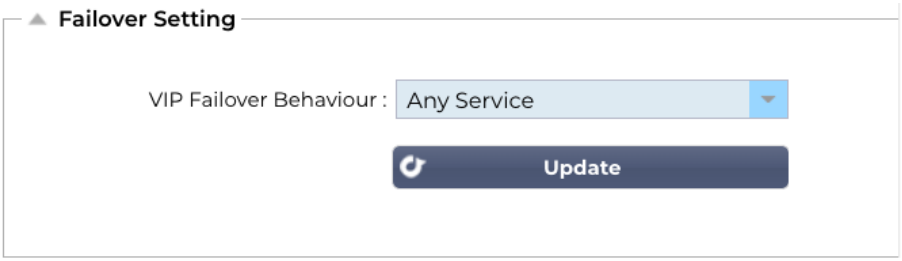
Mit dieser globalen Einstellung kann die SSL-Bibliothek nach Bedarf geändert werden. Die Standard-SSL-Kryptobibliothek, die von der ADC verwendet wird, ist von OpenSSL. Wenn Sie eine andere Kryptobibliothek verwenden möchten, können Sie dies hier ändern.

Authentifizierung



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

Failover-Einstellung



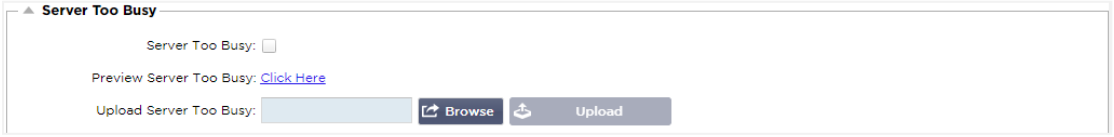
Wenn ein Cluster von ADCs erstellt wird, gibt es jetzt zwei Methoden, um festzulegen, wie ein virtueller Dienst ausfallen soll.

Option	Beschreibung
Jeder Dienst	Wenn diese Option gewählt wird, führt der Ausfall eines beliebigen Dienstes innerhalb des VIP dazu, dass das gesamte VIP mit seinen virtuellen Diensten auf den Clusterpartner ausfällt. Ein Beispiel: Sie haben ein VIP 10.0.100.101 mit virtuellen Diensten, die jeweils Port 443, 8080, 4399, 2020 usw. verwenden. Sollte einer dieser Unterdienste ausfallen, wird das gesamte VIP umgeschaltet.
Alle Dienstleistungen	Wenn diese Option gewählt wird, bleibt das VIP bei Ausfall eines oder mehrerer Sub-Services auf dem aktuellen Cluster-Mitglied. Das VIP wird nur dann auf den Clusterpartner übertragen, wenn **alle** Dienste ausfallen. Dies ist nützlich, wenn Sie einen bestimmten Dienst deaktivieren möchten, aber nicht wollen, dass der VIP ausfällt.

Protokoll

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

Server zu stark ausgelastet



Angenommen, Sie haben die maximale Anzahl der Verbindungen zu Ihren Real-Servern begrenzt; Sie können wählen, ob eine freundliche Webseite angezeigt werden soll, wenn diese Grenze erreicht ist.

- Erstellen Sie eine einfache Webseite mit Ihrer Nachricht. Sie können externe Links zu Objekten auf anderen Webservern und Websites einfügen. Wenn Sie Bilder auf Ihrer Webseite haben möchten, können Sie auch base64-kodierte Inline-Bilder verwenden.
- Suchen Sie die neu erstellte HTM(L)-Datei Ihrer Webseite.
- Hochladen anklicken
- Wenn Sie eine Vorschau der Seite sehen möchten, können Sie dies über den Link Hier klicken tun.

Weitergeleitet für

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

Weitergeleitet-für Ausgang

Option	**Beschreibung**
Aus	Die OEZA ändert den Forwarded-For-Header nicht.
Adresse und Anschluss hinzufügen	Mit dieser Option werden die IP-Adresse und der Port des mit dem ADC verbundenen Geräts oder Clients an den Forwarded-For-Header angehängt.
Adresse hinzufügen	Mit dieser Option wird die IP-Adresse des mit dem ADC verbundenen Geräts oder Clients an den Forwarded-For-Header angehängt.
Ersetzen Sie Adresse und Anschluss	Bei dieser Option wird der Wert des Forwarded-For-Headers durch die IP-Adresse und den Port des mit dem ADC verbundenen Geräts oder Clients ersetzt.
Adresse austauschen	Mit dieser Option wird der Wert des Forwarded-For-Headers durch die IP-Adresse des mit der ADC verbundenen Geräts oder Clients ersetzt.

Weitergeleitet-für-Kopfzeile

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

Erweiterte Protokollierung für IIS - Benutzerdefinierte Protokollierung

Sie können die X-Forwarded-For-Informationen erhalten, indem Sie die IIS Advanced Logging 64-bit App installieren. Erstellen Sie nach dem Herunterladen ein benutzerdefiniertes Protokollierungsfeld namens X-Forwarded-For mit den unten aufgeführten Einstellungen.

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

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

Änderungen an 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 existiert.

Diese Änderungen sind unten aufgeführt:

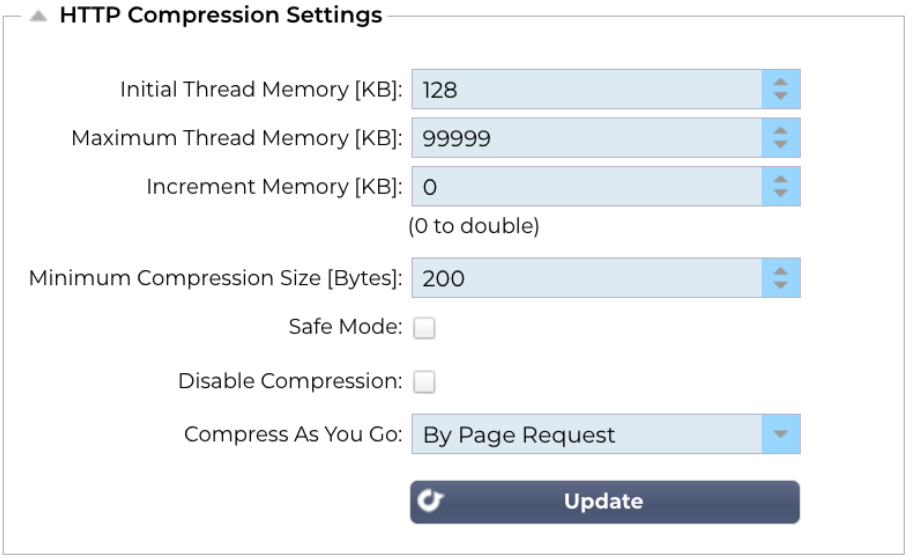
Typ	Wert
LogFormat:	"%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{Benutzer-Agent}i\"" kombiniert
LogFormat:	"%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{Benutzer-Agent}i\"" proxy SetEnvIf X- Forwarded-For "^.*\..*\..*\..*" forwarded
CustomLog:	"logs/access_log" combined env=!forwarded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

Dieses Format macht sich die eingebaute Unterstützung des Apache für die bedingte Protokollierung auf der Grundlage von Umgebungsvariablen zunutze.

- Zeile 1 ist die standardmäßige kombinierte, für das Protokoll formatierte Zeichenfolge aus der Voreinstellung.
- In Zeile 2 wird das Feld %h (Remote Host) durch den/die Wert(e) aus der Kopfzeile X-Forwarded-For ersetzt und der Name dieses Protokolldateimusters auf "proxy" gesetzt.
- 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 wir uns mehr darum kümmern, ob eine IP-Adresse im X-Forwarded-For-Header vorhanden ist.
- Außerdem könnte Zeile 3 wie folgt lauten: "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, wird das "proxy"-Muster verwendet, andernfalls das "combined"-Muster für die Anfrage. Aus Gründen der Lesbarkeit machen die Zeilen 4 und 5 keinen Gebrauch von der Apache-Protokollierungsfunktion "rotate logs" (piped), aber wir gehen davon aus, dass fast jeder sie verwendet.

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

HTTP-Komprimierungseinstellungen



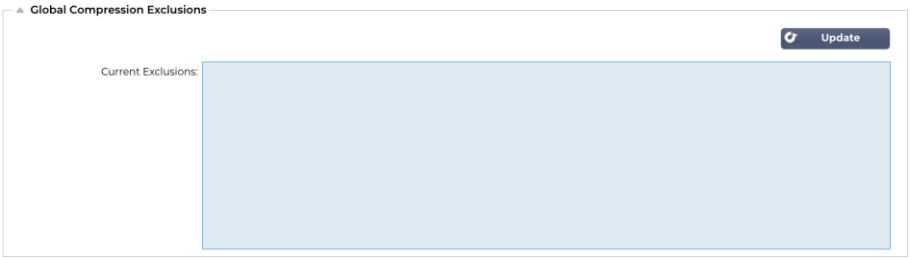
Die Komprimierung ist eine Beschleunigungsfunktion und wird für jeden Dienst auf der Seite IP-Dienste aktiviert.

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

Option	**Beschreibung**
Initialer Thread-Speicher [KB]	Dieser Wert ist die Menge an Speicher, die jede von der ADC empfangene Anfrage zunächst zuweisen kann. Um eine möglichst effiziente Leistung zu erzielen, sollte dieser Wert knapp über der größten unkomprimierten HTML-Datei liegen, die die Webserver wahrscheinlich senden werden.
Maximaler Thread-Speicher [KB]	Dieser Wert ist die maximale Speichermenge, die die ADC bei einer Anfrage zuweisen wird. Um maximale Leistung zu erzielen, speichert und komprimiert die ADC normalerweise alle Inhalte im Speicher. Wenn eine außergewöhnlich große Inhaltsdatei, die diesen Wert überschreitet, verarbeitet wird, schreibt die ADC die Daten auf die Festplatte und komprimiert sie dort.
Inkrement-Speicher [KB]	Dieser Wert legt die Menge an Speicher fest, die der anfänglichen Thread-Speicherzuweisung hinzugefügt wird, wenn mehr Speicher 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.), und zwar bis zu der durch die maximale Speichernutzung pro Thread festgelegten Grenze. Dies ist effizient, wenn die meisten Seiten eine gleichbleibende Größe haben, 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 einem Szenario, in dem große Dateien mit variabler Größe vorkommen, ist es effizienter, eine lineare Erhöhung einer signifikanten Größe festzulegen (z. B. sind Antworten 2Mb bis 10Mb groß, eine anfängliche Einstellung von 1Mb mit einer Erhöhung um 1Mb wäre effizienter).
Minimale Komprimierungsgröße [Bytes]	Dieser Wert ist die Größe in Bytes, unter der die ADC keine Komprimierung vornimmt. Dies ist nützlich, da alles unter 200 Bytes 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 das ADC die Komprimierung von Stylesheets und JavaScript anwendet. Der Grund dafür ist, dass ADC zwar weiß, welche einzelnen Browser mit komprimierten Inhalten umgehen können, dass aber einige andere Proxy-Server, auch wenn sie behaupten, HTTP/1.1-konform zu sein, nicht in der Lage sind, komprimierte Stylesheets und JavaScript korrekt zu

	transportieren. Wenn Probleme mit Stylesheets oder JavaScript über einen Proxyserver auftreten, 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 dieses Kontrollkästchen, um zu verhindern, dass ADC eine Antwort komprimiert.
Komprimieren während der Fahrt	EIN - Verwenden Sie auf dieser Seite "Compress as You Go". Dies komprimiert jeden vom Server empfangenen Datenblock in einem diskreten Stück, das vollständig dekomprimiert werden kann. AUS - Auf dieser Seite wird "Compress As You Go" nicht verwendet. Nach Seitenanforderung - Verwenden Sie "Compress as You Go" nach Seitenanforderung.

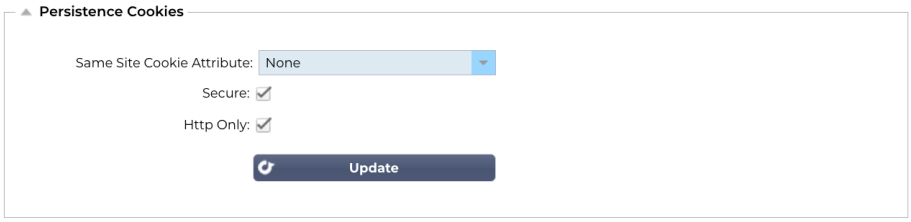
Globale Komprimierungsausschlüsse



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

- Geben Sie den individuellen Dateinamen ein.
- Klicken Sie auf Aktualisieren.
- Wenn Sie einen Dateityp hinzufügen möchten, geben Sie einfach "*.css" ein, damit alle Cascading Style Sheets ausgeschlossen werden.
- Jede Datei oder jeder Dateityp sollte in eine neue Zeile eingefügt werden.

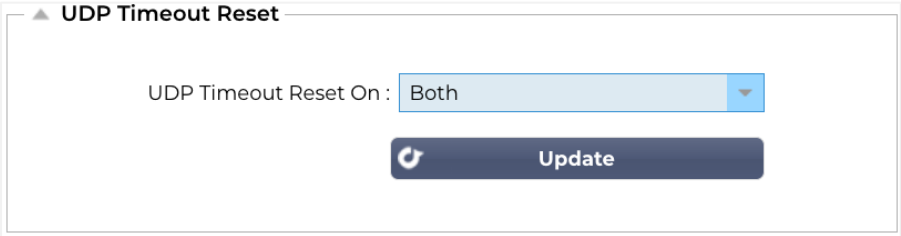
Persistenz-Cookies



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

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

UDP-Zeitüberschreitung zurücksetzen



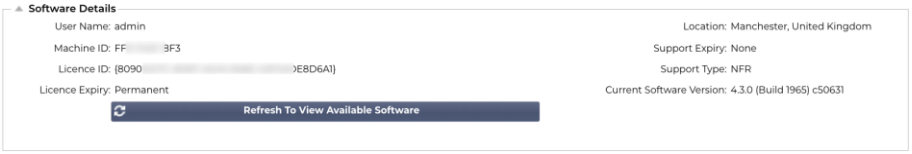
Das Zurücksetzen der UDP-Zeitüberschreitung ist ein Mechanismus, der in der Netzkommunikation verwendet wird und bei dem die Zeitüberschreitung einer UDP-Sitzung (User Datagram Protocol) neu gestartet wird. Das Zurücksetzen trägt dazu bei, die Sitzung als aktiv zu erhalten und einen kontinuierlichen Datenfluss ohne Unterbrechung zu gewährleisten.

Option	Beschreibung
Beide	Setzt die UDP-Zeitüberschreitung sowohl auf dem Server als auch auf dem Client zurück.
Server	Setzt das UDP-Timeout auf dem Server zurück.
Kunde	Setzt das UDP-Timeout auf dem Client zurück.

Software

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

Details zum Software-Upgrade



Die Informationen in diesem Abschnitt werden ausgefüllt, wenn Sie eine funktionierende Internetverbindung haben. Wenn Ihr Browser keine Verbindung zum Internet hat, ist dieser Bereich 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

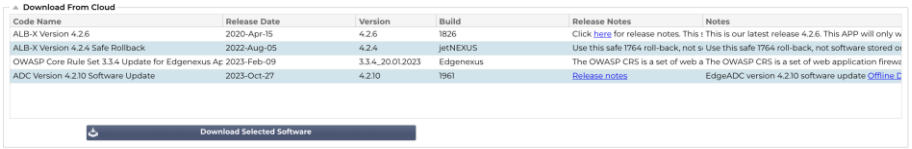
Der unten gezeigte Abschnitt Herunterladen aus der Cloud wird mit Informationen zu den Updates gefüllt, die Ihnen im Rahmen Ihres Supportplans zur Verfügung stehen. Achten Sie auf den Support-Typ und das Ablaufdatum des Supports.

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:

- Fortgeschrittene--Fehlerbehebung--Ping
- IP-Adresse - App Store.edgenexus.io
- Ping anklicken
- Wenn das Ergebnis "ping: unknown host App Store.edgenexus.io" anzeigt.
- Die ADC wird NICHT in der Lage sein, etwas aus der Cloud herunterzuladen.

Herunterladen aus der Cloud



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

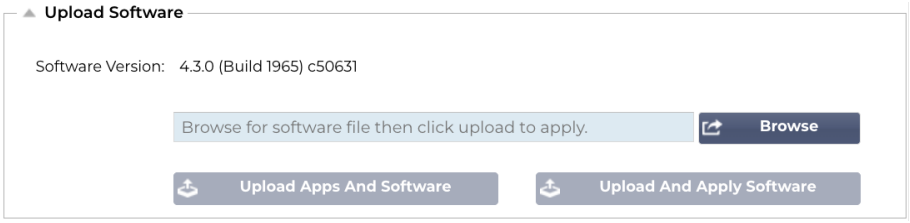
- Markieren Sie die Zeile, die Sie interessiert, und klicken Sie auf die Schaltfläche "Ausgewählte Software auf ALB herunterladen".
- Die ausgewählte Software wird auf Ihr ALB heruntergeladen, wenn Sie darauf klicken. Sie können sie im Abschnitt "Auf dem ALB gespeicherte Software anwenden" unten anwenden.

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

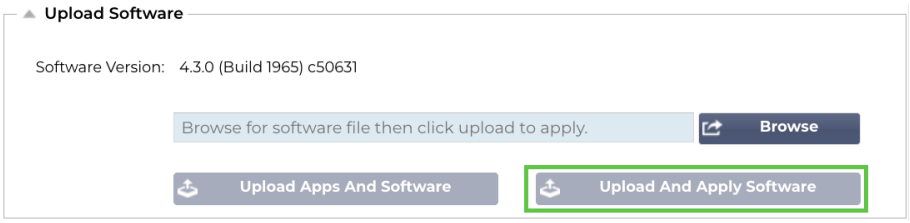
Download-Fehler, ALB kann nicht auf ADC Cloud Services zugreifen für Datei build1734-3236-v4.2.1-Sprint2-update-64.software.alb

Wenn Ihr Netzwerk durch einen Proxy-Server geschützt ist, lesen Sie bitteApp Store Download Proxy

Software hochladen



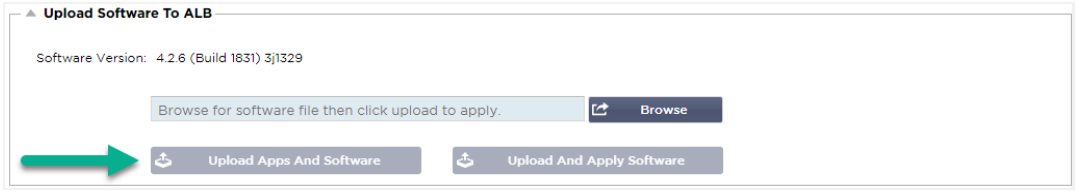
Apps hochladen



Wenn Sie eine App-Datei haben, die mit <Appname> .<Apptyp>.alb endet, können Sie sie mit dieser Methode hochladen.

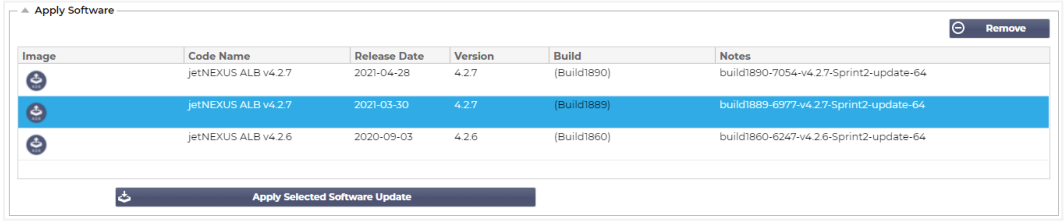
- Es gibt fünf Arten von Apps
  - <Anwendungsname>Flugweg.alb
  - <Anwendungsname>.monitor.alb
  - <Anwendungsname>.jetpack.alb
  - <Anwendungsname>.addons.alb
  - <Anwendungsname>.featurepack.alb
- Nach dem Hochladen befindet sich jede App im Abschnitt Bibliothek>Apps.
- Sie müssen dann jede App in diesem Abschnitt einzeln bereitstellen.

Software /Firmware-Aktualisierungen



- Wenn Sie die Software hochladen möchten, ohne sie anzuwenden, verwenden Sie die markierte Schaltfläche.
- Die Software-Datei lautet <Softwarename>.software.alb.
- Sie wird dann in der Rubrik "Auf dem ALB gespeicherte Software" angezeigt, von wo aus Sie sie nach Belieben anwenden können.

Software anwenden, die auf ADC gespeichert ist



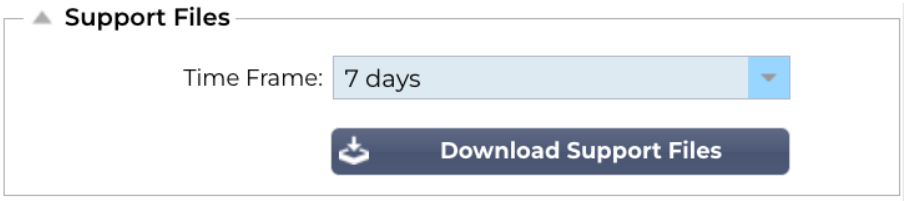
In diesem Abschnitt werden alle auf dem ALB gespeicherten und für die Bereitstellung verfügbaren Softwaredateien angezeigt. Die Liste enthält auch aktualisierte Signaturen der Web Application Firewall (WAF).

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

Fehlersuche

Es gibt immer wieder Probleme, die eine Fehlersuche erfordern, um die Ursache und die Lösung herauszufinden. In diesem Abschnitt können Sie das tun.

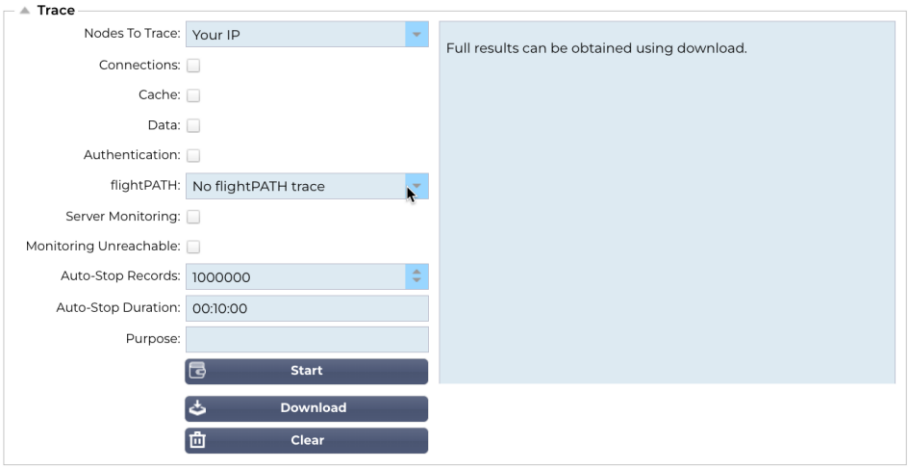
Support-Dateien



Wenn Sie ein Problem mit dem ADC haben und ein Support-Ticket eröffnen 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: Sie haben die Wahl zwischen 3, 7, 14 und allen Tagen.
- Klicken Sie auf "Support-Dateien herunterladen".
- Es wird eine Datei im Format Support-jetNEXUS-yyymmddhh-NAME.dat heruntergeladen.
- Erstellen Sie ein Support-Ticket auf dem Support-Portal, dessen Einzelheiten am Ende dieses Dokuments zu finden sind.
- Beschreiben Sie das Problem genau und fügen Sie die .dat-Datei an das Ticket an.

Spurensuche



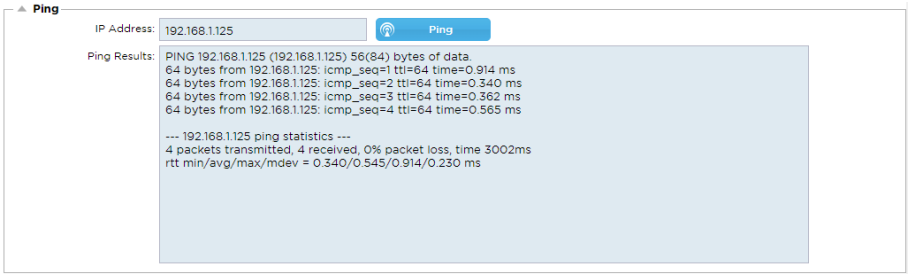
Im Abschnitt "Trace" können Sie Informationen einsehen, die die Fehlersuche im Problemfall ermöglichen. Die gelieferten Informationen hängen von den Optionen ab, die Sie in den Dropdown-Listen und den Kontrollkästchen auswählen.

Option	**Beschreibung**
Zu verfolgende Knoten	**Ihre IP**: Die Ausgabe wird nach der IP-Adresse gefiltert, von der aus Sie auf die grafische Benutzeroberfläche zugreifen (bitte wählen Sie diese Option nicht für die Überwachung, da die Überwachung die ADC-Schnittstellenadresse verwendet). **Alle IP**: Es wird kein Filter angewendet. Es ist zu beachten, dass dies bei einer stark ausgelasteten Box die Leistung beeinträchtigen kann.

Verbindungen	Wenn dieses Kontrollkästchen aktiviert ist, werden Informationen über die client- und serverseitigen Verbindungen angezeigt.
Cache	Wenn Sie dieses Kontrollkästchen aktivieren, erhalten Sie Informationen zu den zwischengespeicherten Objekten.
Daten	Wenn dieses Kontrollkästchen aktiviert ist, werden die vom ADC ein- und ausgehenden Rohdatenbytes einbezogen.
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	Wenn diese Option aktiviert ist, verhält sie sich ähnlich wie die Server-Überwachung, nur dass sie nur die fehlgeschlagenen Überwachungen anzeigt und somit als Filter nur für diese Meldungen dient.
Auto-Stopp-Aufzeichnungen	Der Standardwert ist 1.000.000 Datensätze, danach wird die Trace-Funktion automatisch beendet. Diese Einstellung ist eine Sicherheitsvorkehrung, um zu verhindern, dass Trace versehentlich eingeschaltet bleibt und die Leistung Ihres ADC beeinträchtigt.
Auto-Stop Dauer	Die Standardzeit ist auf 10 Minuten eingestellt, danach wird die Trace-Funktion automatisch beendet. Diese Funktion ist eine Sicherheitsvorkehrung, um zu verhindern, dass Trace versehentlich eingeschaltet bleibt und die Leistung des ADC beeinträchtigt.
Start	Klicken Sie auf diese Schaltfläche, um die Trace-Funktion manuell zu starten.
Stopp	Klicken Sie auf , um die Ablaufverfolgung manuell zu stoppen, bevor die automatische Aufzeichnung oder die Zeit erreicht ist.
Herunterladen	Obwohl Sie den Live-Viewer auf der rechten Seite sehen können, werden die Informationen möglicherweise zu schnell angezeigt. Stattdessen können Sie das Trace.log herunterladen, um alle Informationen zu sehen, die während der verschiedenen Traces an diesem Tag gesammelt wurden. Bei dieser Funktion handelt es sich um eine gefilterte Liste von Trace-Informationen. Wenn Sie die Trace-Informationen der vergangenen Tage anzeigen möchten, können Sie das Syslog für diesen Tag herunterladen, müssen aber manuell filtern.
Klar	Löscht das Trace-Protokoll

Ping

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

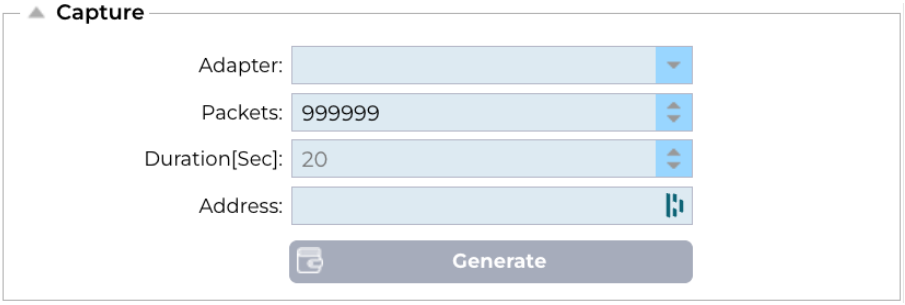


Geben Sie die IP-Adresse des Hosts ein, die Sie testen möchten, z. B. das Standard-Gateway in Dezimalpunktschreibweise oder eine IPv6-Adresse. Nachdem Sie die Schaltfläche "Ping" gedrückt haben, müssen Sie möglicherweise einige Sekunden warten, bis das Ergebnis angezeigt wird.

Wenn Sie einen DNS-Server konfiguriert haben, können Sie den vollständig qualifizierten Domänennamen eingeben. Sie können einen DNS-Server in den Abschnitten **DNS-SERVER 1 UND DNS-SERVER 2**

konfigurieren. Möglicherweise müssen Sie einige Sekunden warten, bis das Ergebnis angezeigt wird, nachdem Sie die Schaltfläche "Ping" gedrückt haben.

Erfassen Sie



Befolgen Sie die nachstehenden einfachen Anweisungen, um den Netzwerkverkehr zu erfassen.

- Füllen Sie die Optionen im Formular aus
- Klicken Sie auf Generieren
- Sobald die Erfassung ausgeführt wurde, fragt Ihr Browser Sie, wo Sie die Datei speichern möchten. Sie wird das Format "jetNEXUS.cap.gz" haben.
- Erstellen Sie ein Support-Ticket auf dem Support-Portal, dessen Einzelheiten am Ende dieses Dokuments zu finden sind.
- Beschreiben Sie das Problem genau und fügen Sie die Datei an das Ticket an.
- Sie können sich den Inhalt auch mit Wireshark ansehen

Option	**Beschreibung**
Adapter	Wählen Sie Ihren Adapter aus der Dropdown-Liste, normalerweise eth0 oder eth1. Sie können auch alle Schnittstellen mit "any" erfassen
Pakete	Dieser Wert gibt die maximale Anzahl der zu erfassenden Pakete an. Normalerweise 99999
Dauer	Wählen Sie eine maximale Zeitspanne für die Erfassung aus. Eine typische Zeitspanne ist 15 Sekunden für stark frequentierte Websites. 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.

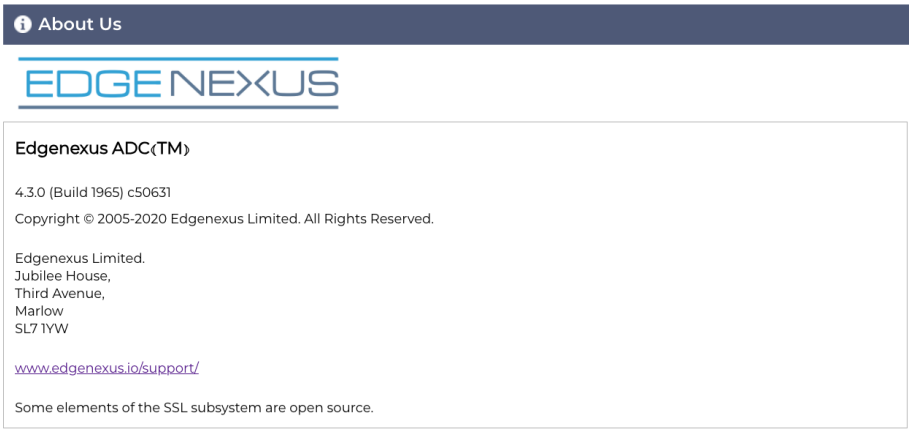
Hinweis: Dies hat Auswirkungen auf die Leistung von Live-Sites. Um die verfügbare Aufnahmegröße zu erhöhen, wenden Sie bitte eine globale Einstellung jetPACK an, um die Aufnahmegröße zu erhöhen.

Hilfe

Der Hilfebereich bietet Zugang zu den Informationen über Edgenexus sowie zu den Benutzerhandbüchern und anderen hilfreichen Informationen.

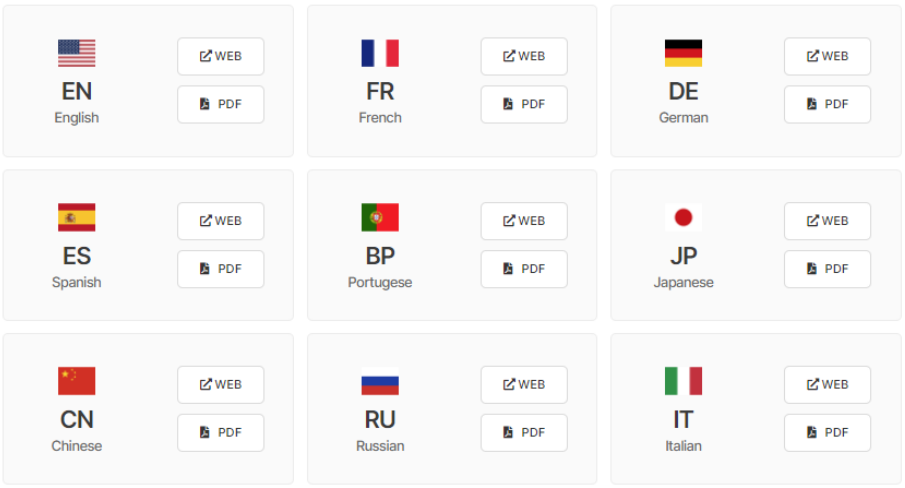
Über uns

Wenn Sie auf die Option Über uns klicken, erhalten Sie Informationen über Edgenexus und seine Geschäftsstelle.



Referenz

Mit der Option "Referenz" wird die Webseite mit den Benutzerhandbüchern und anderen hilfreichen Dokumenten geöffnet. Die Webseite kann auch über https://www.edgenexus.io/documentation aufgerufen werden.



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

JetPACKs

Edgenexus jetPACK s

jetPACKs sind eine einzigartige Methode zur sofortigen Konfiguration Ihres ADC für bestimmte Anwendungen. Diese benutzerfreundlichen Vorlagen sind vorkonfiguriert und mit allen anwendungsspezifischen Einstellungen versehen, die Sie für eine optimierte Servicebereitstellung durch Ihren ADC benötigen. Einige der jetPACKs verwenden flightPATH, um den Datenverkehr zu manipulieren, und Sie müssen über eine flightPATH-Lizenz verfügen, 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 der unten aufgeführten jetPACKs 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.
- Darüber hinaus wurde jedes jetPACK mit 2 Real Servern mit den IP-Adressen 127.1.1.1 und 127.2.2.2 erstellt. Auch hier können Sie diese in der GUI nach dem Hochladen oder vorher mit Notepad++ ändern.
- Klicken Sie auf einen jetPACK-Link unten und speichern Sie den Link als jetPACK-VIP-Application.txt-Datei an einem Ort Ihrer Wahl

Microsoft Exchange

Anmeldung	Link zum Herunterladen	Was bewirkt es?	Was ist inbegriffen?
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 Datenverkehr über den HTTP-Dienst auf HTTPS umzuleiten, aber es ist eine Option. Wenn Sie keine Lizenz für flightPATH haben, wird dieses jetPACK trotzdem funktionieren.	Globale Einstellungen: Dienst-Timeout 2 Stunden Monitore: Layer-7-Monitor für die Outlook-Webanwendung und Layer-4-Out-of-Band-Monitor für den Client-Zugangsdienst Virtueller Dienst IP: 1.1.1.1 Virtuelle Dienstanschlüsse: 80, 443, 135, 59534, 59535 Reale Server: 127.1.1.1 127.2.2.2 flightPATH: Fügt Umleitung von HTTP zu HTTPS hinzu
	jetPACK-1.1.1.2-Exchange-2010-SMTP-RP	Wie oben, aber es wird ein SMTP-Dienst an Port 25 in Reverse-Proxy-Konnektivität hinzugefügt. Der SMTP-Server sieht die Adresse der ALB-X-Schnittstelle als Quell-IP.	Globale Einstellungen: Dienst-Timeout 2 Stunden Monitore: Schicht-7-Monitor für die Outlook-Webanwendung. Schicht 4 Out-of-Band-Monitor für den Client-Zugangsdienst Virtueller Dienst IP: 1.1.1.1 Virtuelle Dienst-Ports: 80, 443, 135, 59534, 59535, 25 (Reverse-Proxy) Reale Server: 127.1.1.1 127.2.2.2 flightPATH: Fügt Umleitung von HTTP zu HTTPS hinzu
	jetPACK-1.1.1.3-Exchange-2010-SMTP-DSR	Wie oben, außer dass dieses jetPACK den SMTP-Dienst so konfiguriert, dass er eine direkte Server-Return-Verbindung verwendet. Dieses jetPACK wird benötigt, wenn Ihr SMTP-Server die tatsächliche IP-Adresse des Clients sehen muss.	Globale Einstellungen: Dienst-Timeout 2 Stunden Monitore: Schicht-7-Monitor für die Outlook-Webanwendung. Schicht 4 Out-of-Band-Monitor für den Client-Zugangsdienst

			Virtueller Dienst IP: 1.1.1.1 Virtuelle Dienst-Ports: 80, 443, 135, 59534, 59535, 25 (direkte Serverrückkehr) Reale Server: 127.1.1.1 127.2.2.2 flightPATH: Fügt eine Umleitung von HTTP zu HTTPs hinzu
Austausch 2013	jetPACK-2.2.2.1-Exchange-2013-Low-Resource	Diese Konfiguration fügt 1 VIP und zwei Dienste für HTTP- und HTTPS-Verkehr hinzu und erfordert die geringste CPU-Leistung. Es ist möglich, dem VIP mehrere Gesundheitsprüfungen hinzuzufügen, um zu prüfen, ob die einzelnen Dienste in Ordnung sind.	Globale Einstellungen: Überwacht: Schicht-7-Überwachung für OWA, EWS, OA, EAS, ECP, OAB und ADS Virtueller Dienst IP: 2.2.2.1 Virtuelle Dienstanschlüsse: 80, 443 Reale Server: 127.1.1.1 127.2.2.2 flightPATH: Fügt Umleitung von HTTP zu HTTPS hinzu
	jetPACK-2.2.3.1-Exchange-2013-Med-Resource	Bei dieser Konfiguration wird für jeden Dienst eine eigene IP-Adresse verwendet, weshalb mehr Ressourcen als oben angegeben benötigt werden. Sie müssen jeden Dienst als eigenen DNS-Eintrag konfigurieren Beispiel owa.edgenexus.com, ews.edgenexus.com usw. Ein Monitor für jeden Dienst wird hinzugefügt und auf den entsprechenden Dienst angewendet	Globale Einstellungen: Überwacht: Schicht-7-Überwachung 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 Dienstanschlüsse: 80, 443 Reale Server: 127.1.1.1 127.2.2.2 flightPATH: Fügt eine Umleitung von HTTP zu HTTPs hinzu
	jetPACK-2.2.2.3-Exchange2013-HIgh-Ressource	Dieses jetPACK fügt eine eindeutige IP-Adresse und mehrere virtuelle Dienste auf verschiedenen Ports hinzu. flightPATH schaltet dann den Kontext basierend auf dem Zielpfad auf den richtigen virtuellen Dienst um. Dieses jetPACK benötigt die meiste CPU-Leistung für die Durchführung der Kontextumschaltung	Globale Einstellungen: Überwacht: Layer 7-Monitor für OWA, EWS, OA, EAS, ECP, OAB, ADS, MAPI und PowerShell Virtueller Dienst IP: 2.2.2.3 Virtuelle Dienstanschlüsse: 80, 443, 1, 2, 3, 4, 5, 6, 7 Reale Server: 127.1.1.1 127.2.2.2 flightPATH: Fügt Umleitung von HTTP zu HTTPS hinzu

Microsoft Lync 2010/2013

Umgekehrter Proxy	Vorderseite	Kante Intern	Rand Extern
jetPACK-3.3.3.1-Lync-Reverse-Proxy	jetPACK-3.3.3.2-Lync-Front -Ende	jetPACK-3.3.3.3-Lync-Edge-Intern	jetPACK-3.3.3.4-Lync-Edge-Extern

Webdienste

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-Wiederverschlüsselung	jetPACK-4.4.4.4-Web-SSL-Passthrough

Microsoft Fern-Desktop

Normal

jetPACK-5.5.5.1-Remote-Desktop

DICOM - Digitale Bildgebung und Kommunikation in der Medizin

Normales HTTP
jetPACK-6.6.6.1-DICOM

Oracle e-Business Suite

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

VMware Horizon View

Verbindungsserver - SSL-Offload	**Sicherheitsserver - SSL-Wiederverschlüsselung**
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 auf, Ihr Passwort einzugeben. 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 während des Übergangs zu unterstützen
- Capture-Größe 16MB - die Standardgröße für Captures beträgt 2MB. Mit diesem Wert wird die Größe auf maximal 16 MB erhöht.

Chiffre s und Chiffre jetPACKs

Der EdgeADC ist standardmäßig mit bewährten Chiffren ausgestattet. Diese Chiffren sind mit ihren jeweiligen TLS-Protokollen gekoppelt, was die Arbeit für die Benutzer erleichtert.

Wir haben eine Reihe zusätzlicher Chiffren für Sie bereitgestellt, die Sie verwenden können, wenn Sie sie benötigen.

Starke Chiffren

Fügt die Möglichkeit hinzu, "Starke Chiffren" aus der Liste der Chiffrieroptionen auszuwählen:

```
ALL:RC4+RSA:+RC4:+HIGH:!DES-CBC3-SHA:!SSLv2:!ADH:!EXP:!ADHexport:!MD5
```

Anti-Bestie

Fügt die Möglichkeit hinzu, "Anti Beast" aus der Liste der Chiffrieroptionen auszuwählen:

```
ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH
```

Kein SSLv3

Fügt die Möglichkeit hinzu, "Kein SSLv3" aus der Liste der Verschlüsselungsoptionen auszuwählen:

```
ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
```

Kein SSLv3 kein TLSv1 kein RC4

Fügt die Möglichkeit hinzu, "No-TLSv1 No-SSLv3 No-RC4" aus der Liste der Verschlüsselungsoptionen auszuwählen:

```
ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
```

NO_TLSv1.1

Fügt die Möglichkeit hinzu, "NO_TLSv1.1" in der Liste der Verschlüsselungsoptionen auszuwählen:

```
ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:
DH+AES:RSA+AESGCM:RSA+AES:HIGH:!3DES:!aNULL:!MD5:!DSS:!MD5:!aNULL:!EDH:!RC4
```

TLS-1.0-1.1-Chiffren aktivieren

Ab Build 4.2.10 wurde die Cipher-Unterstützung für die Protokolle TLS1.0 und TLS 1.1 veraltet. Einige Kunden verwenden jedoch weiterhin diese älteren, veralteten Protokolle für ihre internen Server. Der unten stehende Cipher bietet die Möglichkeit, TLS v1.0 und TLS v1.1 zu aktivieren.

```
AES128-SHA:AES256-SHA:DES-CBC-SHA:DES-CBC3-SHA:EXP-DES-CBC-SHA:RC4-SHA:RC4-MD5:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:EDH-RSA-DES-CBC-SHA:EDH-RSA-DES-CBC3-SHA:EXP-EDH-RSA-DES-CBC-SHA:EXP-RC2-CBC-MD5:AES128-SHA256:AES256-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-DSS-AES128-SHA256:DHE-DSS-AES256-SHA256:DHE-DSS-AES128-GCM-SHA256:DHE-DSS-AES256-GCM-SHA384:AES:ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
```

Beispiel Cipher jetPACK

Chiffren werden mithilfe von jetPACKs in den ADC importiert. Ein jetPACK ist eine einfache Textdatei, die Parameter enthält, die vom ADC erkannt werden. Das folgende Beispiel zeigt ein jetPACK mit der Chiffre Enable TLS-1.0-1.1.

```
#!update

[jetnexusdaemon-cipher-TLS1-0-TLS-1-1]

Cipher="AES128-SHA:AES256-SHA:DES-CBC-SHA:DES-CBC3-SHA:EXP-DES-CBC-SHA:RC4-SHA:RC4-MD5:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:EDH-RSA-DES-CBC-SHA:EDH-RSA-DES-CBC3-SHA:EXP-EDH-RSA-DES-CBC-SHA:EXP-RC2-CBC-MD5:AES128-SHA256:AES256-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-DSS-AES128-SHA256:DHE-DSS-AES256-SHA256:DHE-DSS-AES128-GCM-SHA256:DHE-DSS-AES256-GCM-SHA384:AES:ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM"

Chiffre1=""

Cipher2=""

CipherOptions="-NO_TLSv1.0 -NO_TLSv1.1 -NO_TLSv1.2 -NO_TLSv1"

Description=" TLS v1.0 - v1.1 Aktiviert"
```

- 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" durchführt.
- X-Frame-Options - fügen Sie diesen Header hinzu, falls 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, wenn er nicht vorhanden ist, und setzen Sie ihn auf "1; mode=block" - aktivieren Sie den Browser-Schutz vor Cross-Site-Scripting
- Strict-Transport-Security - fügen Sie den Header hinzu, falls er nicht existiert und setzen Sie ihn auf "max-age=31536000 ; includeSubdomains" - stellt sicher, dass der Client alle Links als HTTPs:// für die max-age berücksichtigt

Anbringen 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 führt zu einer doppelten IP-Adresse in der Konfiguration. Wenn Sie dies versehentlich tun, können Sie dies in der GUI ändern.

- Navigieren Sie zu Erweitert > Software aktualisieren
- Abschnitt Konfiguration

- Neue Konfiguration oder jetPACK hochladen
- Suche nach jetPACK
- Hochladen anklicken
- Sobald der Browser-Bildschirm weiß wird, klicken Sie bitte auf Aktualisieren und warten Sie, bis die Dashboard-Seite erscheint.

Erstellen eines jetPACKs

Eine der großartigen Eigenschaften von jetPACK ist, dass Sie Ihre eigene Konfiguration erstellen können. Es kann sein, dass Sie die perfekte Konfiguration für eine Anwendung erstellt haben und diese unabhängig für mehrere andere Boxen verwenden möchten.

- Kopieren Sie zunächst die aktuelle Konfiguration von Ihrem bestehenden ALB-X
  - Fortgeschrittene
  - Software aktualisieren
  - Aktuelle Konfiguration herunterladen
- Bearbeiten Sie diese Datei mit Notepad++
- Öffnen Sie ein neues txt-Dokument und nennen Sie es "yourname-jetPACK1.txt".
- Kopieren Sie alle relevanten Abschnitte aus der Konfigurationsdatei in die Datei "yourname-jetPACK1.txt".
- Nach Abschluss 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.

Abschnitt 1:

```
[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 zeigt 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 ist für Lync 2010/2013 Reverse Proxy erforderlich.

Abschnitt 2:

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

Dieser Abschnitt enthält die benutzerdefinierten Serverüberwachungsregeln, die normalerweise über die Webkonsole konfiguriert werden.

Beispiel:

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

Abschnitt 3:

```
[jetnexusdaemon-LocalInterface]
```

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

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
Zertifikatsname="Standard"
ClientCertificateName="Kein SSL"
Komprimieren=1
ConnectionLimiting=0
DSR=0
DSRProto="tcp"
Freigegeben=1
LoadBalancePolicy="CookieBased"
MaxConnections=10000
MonitoringPolicy="1".
Durchreichen=0
Protocol="HTTP beschleunigen"
```

```
ServiceDesc="Secure Servers VIP"
SNAT=0
SSL=1
SSLClient=0
SSLInternalPort=27400
[jetnexusdaemon-LocalInterface1.1-Path]
1="6″
Abschnitt 4:
[jetnexusdaemon-Pfad]
```

Dieser Abschnitt enthält alle flightPATH-Regeln. Die Nummern müssen mit denen übereinstimmen, die auf die Schnittstelle angewendet wurden. Im obigen Beispiel sehen wir, dass die flightPATH-Regel "6" auf den Kanal angewandt wurde, einschließlich dieses Beispiels unten.

Beispiel:

```
[jetnexusdaemon-Pfad-6]
Desc="Erzwingen der Verwendung von HTTPS für ein bestimmtes Verzeichnis"
Name="Gary - HTTPS erzwingen"
[jetnexusdaemon-Pfad-6-Bedingung-1]
Check="contain"
Bedingung="Pfad"
Match=
Sense="tut"
Value="/secure/"
[jetnexusdaemon-Path-6-Evaluate-1]
Detail=
Quelle="host"
Wert=
Variable="$host$"[jetnexusdaemon-Path-6-Function-1]
Action="redirect"
Target="HTTPs://$host$$path$$querystring$"
Wert=
```

flightPATH

Einführung in flightPATH

Was ist flightPATH?

flightPATH ist ein intelligentes Regelwerk, das von Edgenexus entwickelt wurde, um den HTTP- und HTTPS-Verkehr zu manipulieren und weiterzuleiten. 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 Layer 7-Diensttyp angewendet werden, der HTTP(s) entspricht. Wenn Sie einen anderen Servicetyp wählen, ist die Registerkarte flightPATH in IP Services leer.

Was kann flightPATH tun?

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

Neben einfachen Übereinstimmungen von Zeichenketten, wie z.B. "Beginnt mit" und "Endet mit", kann auch eine vollständige Kontrolle über leistungsstarke Perl-kompatible reguläre Ausdrücke (RegEx) implementiert werden.

Weitere Informationen zu RegEx finden Sie auf dieser hilfreichen Website

Darüber hinaus können im Bereich Auswertung benutzerdefinierte Variablen erstellt werden, die im Bereich Aktion verwendet werden können und viele verschiedene Möglichkeiten bieten.

Eine flightPATH-Regel besteht aus drei Komponenten:

Option	Beschreibung
Einzelheiten	Dient zum Hinzufügen oder Entfernen eines flightPATH und zur Auflistung der verfügbaren flightPATHs
Zustand	Legen Sie mehrere Kriterien fest, um die flightPATH-Regel auszulösen.
Bewertung	Erlaubt die Verwendung von Variablen, die im Aktionsbereich verwendet werden können.
Aktion	Das Verhalten, wenn die Regel ausgelöst wurde.

Zustand

In diesem Abschnitt können Sie fünf individuelle Parameter angeben, die für eine Bedingung gelten. Diese werden im Folgenden mit einer Beschreibung der einzelnen Optionen und einem Beispiel erläutert.

Zustand	Beschreibung	Beispiel
<form>	HTML-Formulare werden verwendet, um Daten an einen Server zu übermitteln	Beispiel "Formular hat nicht die Länge 0"
GEO-Standort	Diese vergleicht die Quell-IP-Adresse mit dem ISO 3166 Country Code	GEO Standort ist gleich GB OR GEO Standort ist gleich Deutschland
Gastgeber	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 echte Herkunftsadresse	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 | für mehrere IP's verwenden
Pfad	Dies ist der Pfad der Website	/meinewebsite/index.asp
POST	POST-Anfrageverfahren	Überprüfung von Daten, die auf eine Website hochgeladen werden
Abfrage	Dies ist der Name und der Wert einer Abfrage, die entweder den Abfragenamen oder einen Wert enthalten kann	"Best=edgeNEXUS", wobei die Übereinstimmung "Best" und der Wert "edgeNEXUS" ist
Abfrage-String	Der gesamte Abfrage-String nach dem Zeichen ?	
Cookie anfordern	Dies ist der Name eines von einem Client angeforderten Cookies	MS-WSMAN=afYfn1CDqqCDqUD::
Kopfzeile anfordern	Dies kann eine beliebige HTTP-Kopfzeile sein	Referrer, Benutzer-Agent, Von, Datum
Version anfordern	Dies ist die HTTP-Version	HTTP/1.0 ODER HTTP/1.1
Antwortstelle	Eine benutzerdefinierte Zeichenfolge im Antwortkörper	Server UP
Antwort-Code	Der HTTP-Code für die Antwort	200 OK, 304 Nicht geändert
Antwort Keks	Dies ist der Name eines vom Server gesendeten Cookies	MS-WSMAN=afYfn1CDqqCDqUD::
Antwort-Kopfzeile	Dies kann eine beliebige HTTP-Kopfzeile sein	Referrer, Benutzer-Agent, Von, Datum
Antwort Version	Die vom Server gesendete HTTP-Version	HTTP/1.0 ODER HTTP/1.1
Quelle IP	Dies ist entweder die Ursprungs-IP, die Proxy-Server-IP oder eine andere aggregierte IP-Adresse	Kunde IP, Proxy IP, Firewall IP. Sie können auch mehrere IPs und Subnetze verwenden. Sie müssen die Punkte auslassen, da diese RegEX sind. Beispiel: 10.1.1\.2\.3 ist 10.1.2.3

Spiel

Der Parameter Match ist kontextsensitiv und hängt vom Wert des Parameters Condition ab.

Spiel	Beschreibung	Beispiel
Akzeptieren	Zulässige Inhaltstypen	Akzeptieren: text/plain
Accept-Encoding	Zulässige Kodierungen	Accept-Encoding: <compress | gzip | deflate | sdch | identity>
Accept-Language	Akzeptable Sprachen für die Antwort	Accept-Language: en-US
Accept-Ranges	Welche Teilinhaltsbereichstypen dieser Server unterstützt	Accept-Ranges: bytes
Autorisierung	Anmeldedaten für die HTTP-Authentifizierung	Berechtigung: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==

Charge-To	Enthält Kontoinformationen zu den Kosten für die Anwendung der beantragten Methode	
Content-Encoding	Die Art der Kodierung, die für die Daten verwendet wird.	Inhaltskodierung: gzip
Inhalt-Länge	Die Länge des Antwortkörpers in Oktetten (8-Bit-Bytes)	Inhalt-Länge: 348
Inhalt-Typ	Der Mime-Typ des Anforderungskörpers (wird bei POST- und PUT-Anforderungen verwendet)	Inhalt-Typ: anwendung/x-www-form-urlencoded
Keks	Ein HTTP-Cookie, das zuvor vom Server mit Set-Cookie (siehe unten) gesendet wurde	Cookie: $Version=1; Skin=new;
Datum	Datum und Uhrzeit, zu der die Nachricht erstellt wurde	Datum = "Datum" ":" HTTP-Datum
ETag	Ein Identifikator für eine bestimmte Version einer Ressource, oft ein Message Digest	ETag: "aed6bdb8e090cd1:0"
Von	Die E-Mail-Adresse des Nutzers, der die Anfrage stellt	Von: user@example.com
Wenn-geändert-seit	Ermöglicht die Rückgabe eines 304 Not Modified, wenn der Inhalt unverändert ist	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Zuletzt geändert	Das Datum der letzten Änderung für das angeforderte Objekt im RFC 2822-Format	Zuletzt geändert: Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Die implementierungsspezifischen Kopfzeilen können verschiedene Auswirkungen auf die gesamte Anfrage-Antwort-Kette haben.	Pragma: no-cache
Referent	Dies ist die Adresse der vorherigen Webseite, von der aus ein Link zu der aktuell angeforderten Seite hergestellt wurde	Verweiser: 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 Sie	Weist nachgelagerte Proxys an, 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 an (z. B. ASP.NET, PHP, JBoss), die die Webanwendung unterstützt	X-Powered-By: PHP/5.4.0

Siehe

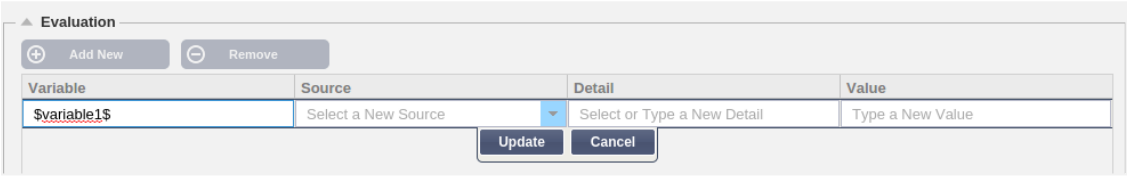
Siehe	Beschreibung	Beispiel
Existieren	Dabei spielt es keine Rolle, wie der Zustand im Einzelnen aussieht, sondern nur, ob er existiert oder nicht.	Host> Existiert>
Start	Die Zeichenfolge beginnt mit dem Wert	Pfad> Startet> > /secure
Ende	Die Zeichenfolge endet mit dem Wert	Pfad> Endet> > .jpg

Enthält	Die Zeichenfolge enthält den Wert	Request Header> Accept> Enthält> > Bild
Gleichberechtigt	Die Zeichenkette ist gleich dem Wert	Host> Ist> gleich> www.edgenexus.io
Länge haben	Die Zeichenkette hat die Länge des Wertes	Host> Hat> die Länge> 16 www.edgenexus.io = WAHR www.edgenexus.com = FALSCH
Länge überschreiten	Prüfen Sie, ob der Wert die angegebene Länge erreicht oder überschreitet.	Pfad > Tut > Länge überschreiten - 10
RegEx abgleichen	Damit können Sie einen vollständigen Perl-kompatiblen regulären Ausdruck eingeben	Herkunft IP> Entspricht> Regex> 10\..* | 11\..*
Spielliste	Ermöglicht die Bereitstellung einer durch PIPE (|) abgegrenzten Liste von Werten, gegen die Sie prüfen können.	Quell-IP > Does > Übereinstimmungsliste > 10.0.0.1 | 10.0.0.100 | 192.178.28.32

Beispiel

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

Bewertung



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. So können Sie zum Beispiel einen Benutzernamen protokollieren oder eine E-Mail senden, wenn ein Sicherheitsproblem vorliegt.

- Variable: Diese muss mit einem $-Symbol beginnen und enden. Zum Beispiel $variable1$
- Quelle: Wählen Sie aus der Dropdown-Box die Quelle der Variablen aus.
- Einzelheiten: Wählen Sie aus der Liste aus, wenn dies relevant ist. 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 Erläuterungen zu den einzelnen Variablen finden Sie in der obigen Tabelle "Bedingungen".
    - Methode = $Methode$
    - Pfad = $Pfad$
    - Abfragestring = $querystring$
    - Quellip = $Quellip$

- Antwortcode (Text enthält auch "200 OK") = $resp$
- Host = $host$
- Version = $version$
- Kundenanschluss = $Kundenanschluss$
- Clientip = $clientip$
- Geolocation = $geolocation$"

Beispiel Aktion:

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

Erläuterung:

- Ein Kunde, der auf eine Seite zugreift, die nicht existiert, würde normalerweise mit einer 404-Seite des Browsers konfrontiert werden.
- In diesem Fall wird der Benutzer an den ursprünglichen Hostnamen weitergeleitet, den er verwendet hat, 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 soeben eine Anfrage an die Seite wrong.html gestellt".

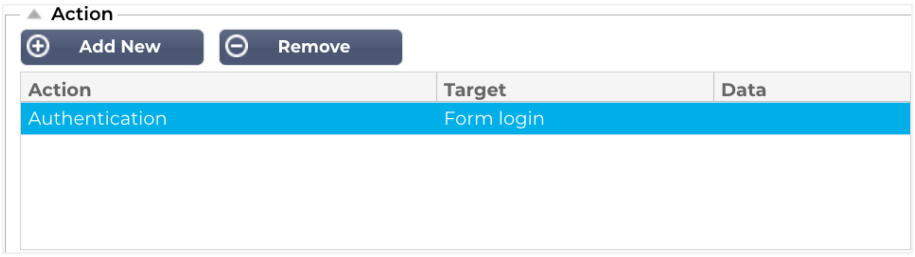
Quelle	Beschreibung	Beispiel
Keks	Dies ist der Name und der Wert des Cookie-Headers	MS-WSMAN=afYfn1CDqqCDqUD::Dabei ist der Name MS-WSMAN und der Wert afYfn1CDqqCDqUD::
Gastgeber	Dies ist der aus der URL extrahierte Hostname	www.mywebsite.com oder 192.168.1.1
Sprache	Dies ist die Sprache, die aus dem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

Einzelheiten	Beschreibung	Beispiel
Akzeptieren	Zulässige Inhaltstypen	Akzeptieren: text/plain

Accept-Encoding	Zulässige Kodierungen	Accept-Encoding: <compress | gzip | deflate | sdch | identity>
Accept-Language	Akzeptable Sprachen für die Antwort	Accept-Language: en-US
Accept-Ranges	Welche Teilinhaltsbereichstypen dieser Server unterstützt	Accept-Ranges: bytes
Autorisierung	Anmeldedaten für die HTTP-Authentifizierung	Berechtigung: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Charge-To	Enthält Kontoinformationen zu den Kosten für die Anwendung der beantragten Methode	
Content-Encoding	Die Art der Kodierung, die für die Daten verwendet wird.	Inhaltskodierung: gzip
Inhalt-Länge	Die Länge des Antwortkörpers in Oktetten (8-Bit-Bytes)	Inhalt-Länge: 348
Inhalt-Typ	Der Mime-Typ des Anforderungskörpers (wird bei POST- und PUT-Anforderungen verwendet)	Inhalt-Typ: anwendung/x-www-form-urlencoded
Keks	ein HTTP-Cookie, das zuvor vom Server mit Set-Cookie (siehe unten) gesendet wurde	Cookie: $Version=1; Skin=new;
Datum	Datum und Uhrzeit, zu der die Nachricht verfasst wurde	Datum = "Datum" ":" HTTP-Datum
ETag	Ein Identifikator für eine bestimmte Version einer Ressource, oft ein Message Digest	ETag: "aed6bdb8e090cd1:0"
Von	Die E-Mail-Adresse des Nutzers, der die Anfrage stellt	Von: user@example.com
Wenn-geändert-seit	Ermöglicht die Rückgabe eines 304 Not Modified, wenn der Inhalt unverändert ist	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Zuletzt geändert	Das Datum der letzten Änderung für das angeforderte Objekt im RFC 2822-Format	Zuletzt geändert: Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Implementierungsspezifische Kopfzeilen, die in der gesamten Anfrage-Antwort-Kette verschiedene Auswirkungen haben können.	Pragma: no-cache
Referent	Dies ist die Adresse der vorherigen Webseite, von der aus ein Link zu der aktuell angeforderten Seite hergestellt wurde	Verweiser: 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 Sie	Sagt nachgelagerten Proxys mit, 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.



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 je nach Aktion.

Bei einigen Aktionen können Sie auch manuell tippen.

Daten

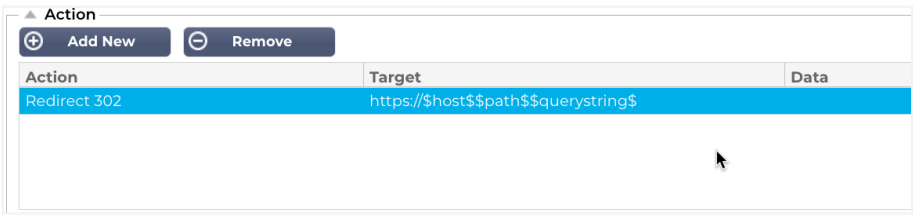
Doppelklicken Sie auf die Spalte Daten, um die Daten, die Sie hinzufügen oder ersetzen möchten, manuell hinzuzufügen.

Die Liste aller Aktionen ist nachstehend aufgeführt:

Aktion	Beschreibung	Beispiel
Anfrage Cookie hinzufügen	Fügen Sie das Anfrage-Cookie im Abschnitt "Ziel" mit dem Wert im Abschnitt "Daten" hinzu.	Ziel= Keks Daten= MS-WSMAN=afYfn1CDqqCDqCVii
Anfrage-Kopfzeile hinzufügen	Fügen Sie einen Anfragekopf des Typs Target mit einem Wert im Abschnitt Data hinzu.	Ziel= Akzeptieren Daten= image/png
Antwort-Cookie hinzufügen	Antwort-Cookie im Abschnitt Ziel mit Wert im Abschnitt Daten hinzufügen	Ziel= Keks Daten= MS-WSMAN=afYfn1CDqqCDqCVii
Antwort-Kopfzeile hinzufügen	Fügen Sie im Abschnitt "Ziel" den detaillierten Anforderungskopf mit dem Wert im Abschnitt "Daten" hinzu.	Ziel= Cache-Kontrolle Daten= max-age=8888888
Körper Alle ersetzen	Durchsuchen Sie den Antwortkörper und ersetzen Sie alle Instanzen	Ziel= HTTP:// (Suchbegriff) Data= HTTPs:// (Ersetzungszeichenfolge)
Körper zuerst austauschen	Durchsuchen Sie den Antwortkörper und ersetzen Sie nur die erste Instanz	Ziel= HTTP:// (Suchbegriff) Data= HTTPs:// (Ersetzungszeichenfolge)
Körper Ersetzen Letzte	Den Antwortkörper durchsuchen und nur die letzte Instanz ersetzen	Ziel= HTTP:// (Suchbegriff) Data= HTTPs:// (Ersetzungszeichenfolge)
Ablegen	Dadurch wird die Verbindung getrennt	Zielvorgabe= N/A Daten= N/A
e-Mail	Sendet eine E-Mail an die unter E-Mail-Ereignisse konfigurierte Adresse. Sie können eine Variable als Adresse oder Nachricht verwenden	Target= "flightPATH hat dieses Ereignis gemailt" Daten= N/A

Ereignis protokollieren	Dadurch wird ein Ereignis in das Systemprotokoll aufgenommen.	Target= "flightPATH hat dies im Syslog protokolliert" Daten= N/A
Umleitung 301	Dies führt zu einer permanenten Umleitung	Ziel= HTTP://www.edgenexus.io Daten= N/A
Umleitung 302	Dies führt zu einer vorübergehenden Umleitung	Ziel= HTTP://www.edgenexus.io Daten= N/A
Anfrage-Cookie entfernen	Entfernen Sie das im Abschnitt Ziel beschriebene Anfrage-Cookie	Ziel= Keks Daten= MS-WSMAN=afYfn1CDqqCDqCVii
Anfrage-Kopfzeile entfernen	Entfernen Sie den im Abschnitt "Ziel" beschriebenen Anforderungskopf	Ziel=Server Daten=N/A
Antwort-Cookie entfernen	Antwort-Cookie entfernen, wie im Abschnitt Ziel beschrieben	Ziel=jnAccel
Antwort-Kopfzeile entfernen	Entfernen Sie den Antwort-Header, der im Abschnitt Ziel beschrieben ist	Ziel= Etag Daten= N/A
Ersetzen Sie Anfrage Cookie	Ersetzen Sie das im Abschnitt Ziel angegebene Anfrage-Cookie durch den Wert im Abschnitt Daten	Ziel= Keks Daten= MS-WSMAN=afYfn1CDqqCDqCVii
Anfrage-Kopfzeile ersetzen	Ersetzen Sie den Anfragekopf im Ziel durch den Datenwert	Ziel= Verbindung Daten= keep-alive
Antwort-Cookie ersetzen	Ersetzen Sie das Antwort-Cookie, das im Abschnitt Ziel angegeben ist, durch den Wert im Abschnitt Daten	Ziel=jnAccel=afYfn1CDqqCDqCVii Datum=MS-WSMAN=afYfn1CDqqCDqCVii
Antwort-Kopfzeile ersetzen	Ersetzen Sie die im Abschnitt Ziel angegebene Kopfzeile der Antwort durch den Wert im Abschnitt Daten	Ziel= Server Daten= Aus Sicherheitsgründen vorenthalten
Pfad umschreiben	Damit können Sie die Anfrage auf eine neue URL umleiten, die auf der Bedingung	Ziel= /test/pfad/index.html$querystring$ Daten= N/A
Sicheren Server verwenden	Auswahl des zu verwendenden sicheren Servers oder virtuellen Dienstes	Target=192.168.101:443 Daten=N/A
Server verwenden	Auswahl des zu verwendenden Servers oder virtuellen Dienstes	Ziel= 192.168.101:80 Daten= 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 verwenden. Data= Geben Sie eine Passphrase für die Verschlüsselung ein

Beispiel:



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

Häufige Verwendungszwecke

Anwendungsfirewall und Sicherheit

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

Eigenschaften

- Umleitung von Nutzern basierend auf dem Pfad
- Einzelanmeldung über mehrere Systeme hinweg
- Segmentierung von Nutzern auf Basis von User ID oder Cookie
- Kopfzeilen für SSL-Offload hinzufügen
- Erkennung von Sprachen
- Benutzeranfrage umschreiben
- Fehlerhafte URLs korrigieren
- Protokoll und E-Mail-Warnung 404-Antwortcodes
- Verhindern des Verzeichniszugriffs/-durchsuchens
- Senden Sie Spidern andere Inhalte

Vorgefertigte Regeln

HTML-Erweiterung

Ändert alle .htm-Anfragen in .html

Zustand:

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

Bewertung:

- Leere

Aktion:

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

Index.html

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

Bedingung: Diese Bedingung ist eine allgemeine Bedingung, die auf die meisten Objekte zutrifft.

- Bedingung = Gastgeber

- Sense = Tut
- Prüfen = Vorhanden

Bewertung:

- Leere

Aktion:

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

Ordner schließen

Ablehnung von Anfragen an Ordner.

Bedingung: Diese Bedingung ist eine allgemeine Bedingung, die auf die meisten Objekte zutrifft.

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

Bewertung:

- Leere

Aktion:

- Aktion =
- Ziel =

CGI-BBIN ausblenden:

Versteckt den cgi-bin-Katalog in Anfragen an CGI-Skripte.

Bedingung: Diese Bedingung ist eine allgemeine Bedingung, die auf die meisten Objekte zutrifft.

- Bedingung = Gastgeber
- Sense = Tut
- Prüfen = Übereinstimmung mit RegEX
- Wert = \.cgi$

Bewertung:

- Leere

Aktion:

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

Log Spider

Protokollieren Sie die Spider-Anfragen der gängigen Suchmaschinen.

Bedingung: Diese Bedingung ist eine allgemeine Bedingung, die auf die meisten Objekte zutrifft.

- Bedingung = Anfrage-Kopfzeile
- Übereinstimmung = User-Agent
- Sense = Tut
- Prüfen = Übereinstimmung mit RegEX

- Wert = Googlebot|Slurp|bingbot|ia_archiver

Bewertung:

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

Aktion:

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

HTTPS erzwingen

Erzwingt die Verwendung von HTTPS für bestimmte Verzeichnisse. 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/

Bewertung:

- Leere

Aktion:

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

Media Stream:

Leitet den Flash Media Stream an den entsprechenden Dienst um.

Zustand:

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

Bewertung:

- Leere

Aktion:

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

HTTP in HTTPS umwandeln

Ändern Sie alle fest kodierten HTTP:// in HTTPS://

Zustand:

- Bedingung = Antwortcode
- Sense = Tut
- Prüfung = Gleich
- Wert = 200 OK

Bewertung:

- Leere

Aktion:

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

Blanko-Kreditkarten

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

Zustand:

- Bedingung = Antwortcode
- Sense = Tut
- Prüfung = Gleich
- Wert = 200 OK

Bewertung:

- Leere

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

Ablauf des Inhalts

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

Bedingung: Dies ist eine allgemeine Bedingung als Auffangtatbestand. Es wird empfohlen, diese Bedingung auf Ihre

- Bedingung = Antwortcode
- Sense = Tut
- Prüfung = Gleich
- Wert = 200 OK

Bewertung:

- Leere

Aktion:

- Aktion = Antwort-Kopfzeile hinzufügen
- Ziel = Cache-Kontrolle

- Daten = max-age=3600

Spoof-Server-Typ

Ermitteln Sie den Servertyp und ändern Sie ihn in einen anderen.

Bedingung: Dies ist eine allgemeine Bedingung als Auffangtatbestand. Es wird empfohlen, diese Bedingung auf Ihre

- Bedingung = Antwortcode
- Sense = Tut
- Prüfung = Gleich
- Wert = 200 OK

Bewertung:

- Leere

Aktion:

- Aktion = Ersetzen des Antwortkopfes
- Ziel = Server
- Daten = Geheim

Niemals Fehler senden

Der Kunde erhält keine Fehler von Ihrer Website.

Zustand

- Bedingung = Antwortcode
- Sense = Tut
- Prüfen = Enthalten
- Wert = 404

Bewertung

- Leere

Aktion

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

Umleitung über Sprache

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

Zustand

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

Bewertung

- 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 Analyse ein - bitte ändern Sie den Wert MYGOOGLECODE in Ihre Google UA ID.

Zustand

- Bedingung = Antwortcode
- Sense = Tut
- Prüfung = Gleich
- Wert = 200 OK

Bewertung

- leer

Aktion

- Aktion = Body Replace Last
- Ziel = </body>
- Daten = <script type='text/javascript'> var _gaq = _gaq || []; _gaq.push(['_setAccount', 'MY GOOGLE CODE']); _gaq.push(['_trackPageview']); (function() { var ga = document.createElement('script'); ga.type = 'text/javascript'; ga.async = true; ga.src = ('HTTPs' == document.location.protocol ?'HTTPs//ssl' 'HTTP//www') + '.google-analytics.com/ga.js'; var s = document.getElementsByTagName('script')[0];s.parentNode.insertBefore(ga, s); })(); </script> </body>

IPv6-Gateway

Host Header für IIS IPv4 Server auf 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

Bewertung

- leer

Aktion

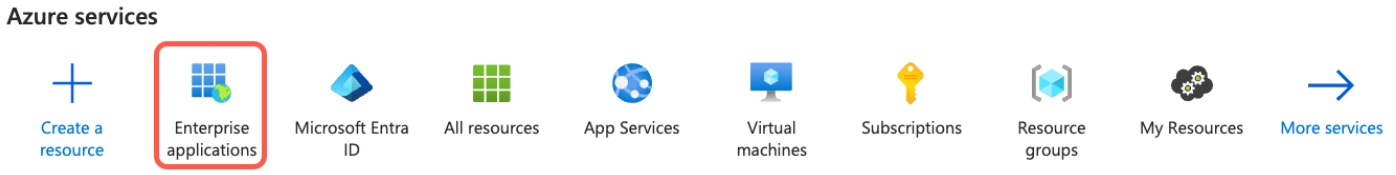
- Aktion = Ersetzen des Anfragekopfes
- Ziel = Host
- Daten =ipv4.host.header

SAML und Entra ID

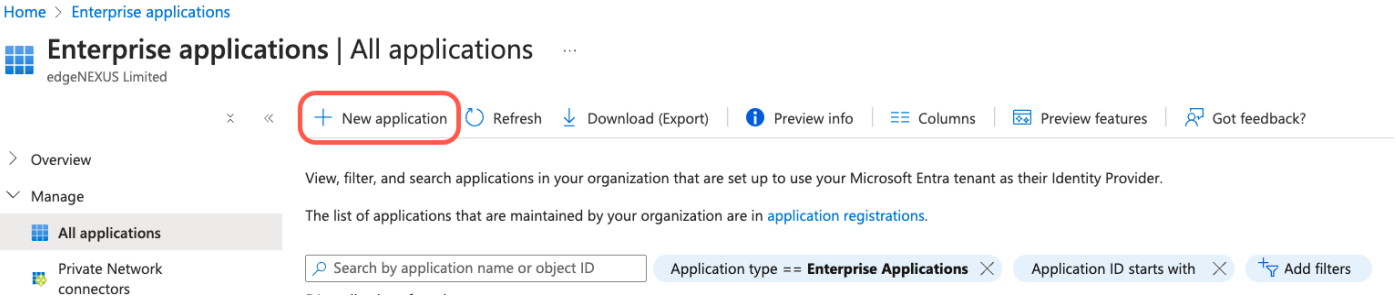
Einrichten der Entra ID Authentifizierungsanwendung in Microsoft Entra

Damit die SAML-Authentifizierung erfolgreich funktioniert, müssen Sie eine Unternehmensanwendung in Ihrem Microsoft Entra Admin Portal einrichten. Dies ist eine einfache Aufgabe und ermöglicht die Bereitstellung des Signierzertifikats, das für SAML-Authentifizierungsanfragen und Token benötigt wird, sowie der Konfigurations-XML-Daten.

Loggen Sie sich dazu zunächst in Ihr Microsoft Entra Portal (https://portal.azure.com) ein und vergewissern Sie sich, dass Sie sich auf der Seite Azure Services befinden, wo Sie oben auf der Seite eine Liste von Symbolen finden (siehe unten).

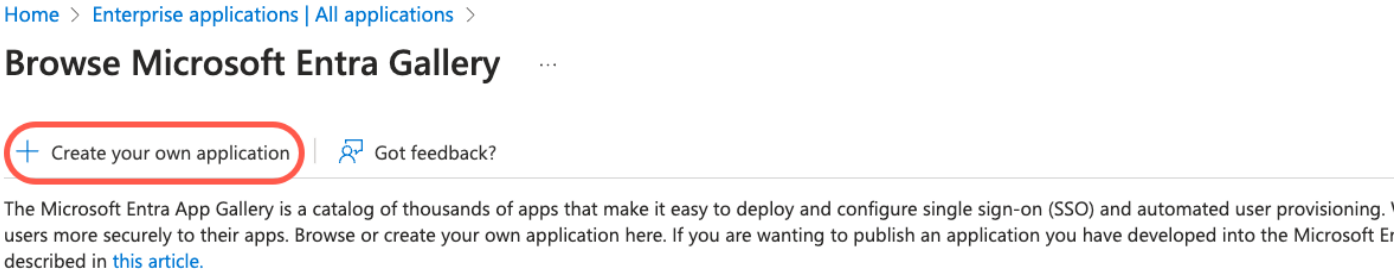


- Klicken Sie auf Unternehmensanwendungen. Wenn Sie Unternehmensanwendungen nicht in der Symbolliste finden, können Sie den Namen in die Suchleiste oben eingeben. Es wird eine Seite wie unten gezeigt angezeigt.

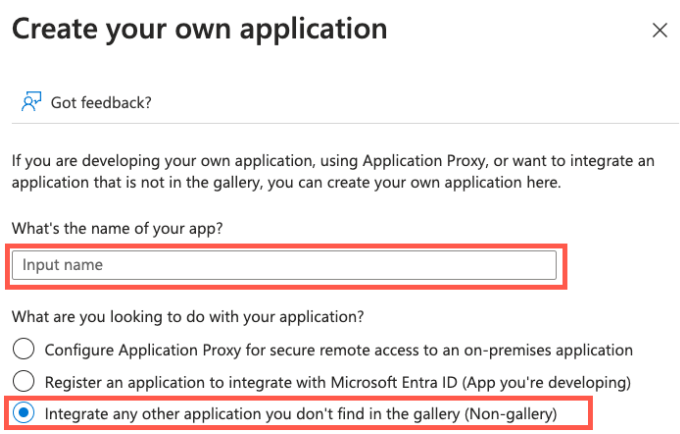


Klicken Sie auf *Neue Anwendung*

Auf der nächsten Seite klicken Sie auf *Eigene Anwendung erstellen*.

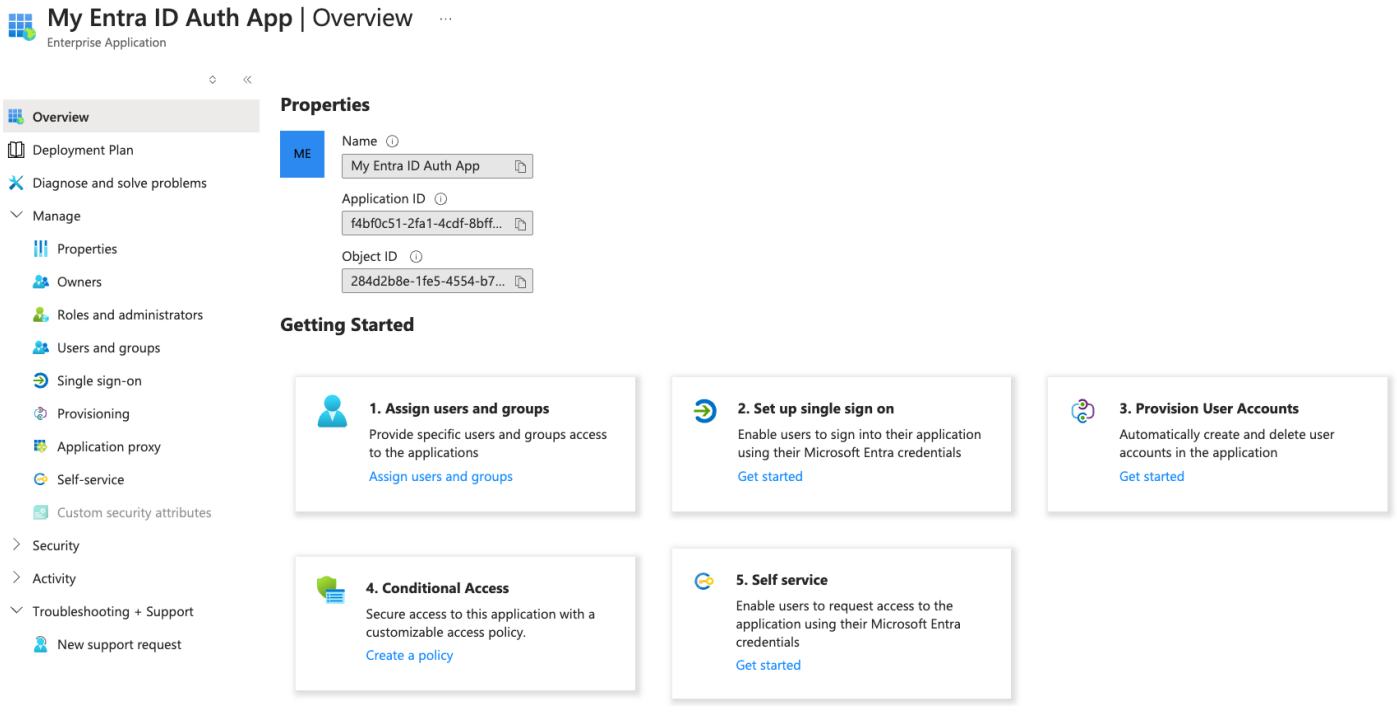


- Auf der rechten Seite öffnet sich ein Abschnitt mit der Überschrift "*Erstellen Sie Ihre eigene Anwendung*".

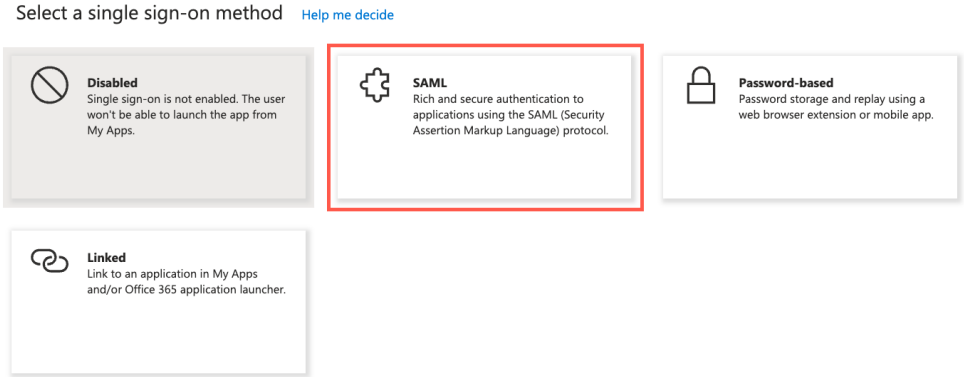


- Geben Sie einen Namen für Ihre Anwendung an, z. B. "My Entra ID Auth App". Sie können jeden beliebigen Namen wählen.
- Klicken Sie auf die Option *Jede andere Anwendung integrieren, die Sie nicht in der Galerie finden (Nicht-Galerie)*.
- Klicken Sie auf die Schaltfläche *Erstellen*.

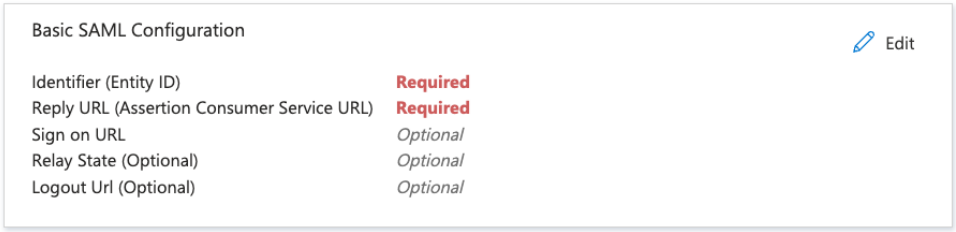
Sie werden nun eine Seite sehen, die wie die folgende aussieht.



- Klicken Sie in der linken Navigationsleiste auf die Option Single Sign-on.
- Markieren Sie das Feld SAML



- Sie sehen nun eine Seite mit dem Abschnitt für die grundlegende SAML-Konfiguration.



- Füllen Sie den Bereich SAML-Basiskonfiguration aus:
  - Identifikator (Entitäts-ID)
  - Antwort-URL (Assertion Consumer Service URL)
  - Anmelde-URL
  - Abmelde-URL (optional)
- Speichern Sie Ihre Konfiguration und testen Sie die App.

Eine ausführlichere Anleitung finden Sie in der Dokumentation Enable single sign-on for an enterprise application auf der Microsoft-Website.

Technische Unterstützung

Wir bieten technische Unterstützung für alle unsere Nutzer gemäß den Standardbedingungen des Unternehmens.

Wir bieten technischen Support, wenn Sie über einen aktiven Support- und Wartungsvertrag für EdgeADC, EdgeWAF oder EdgeGSLB verfügen.

Um ein Support-Ticket zu erstellen, besuchen Sie bitte unsere Website:

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