EdgeADC

GUIDA ALL'AMMINISTRAZIONE

VERSIONE SOFTWARE

4.2.7.1906

Contenuto

Proprietà del documento

Numero del documento: 2.0.10.22.21.14.10

Data di creazione del documento: 30 aprile 2021

Ultima modifica del documento: October 22, 2021

Autore del documento: Jay Savoor

Documento modificato l'ultima volta da:

Riferimento del documento: EdgeADC - Versione 4.2.7.1906

Dichiarazione di non responsabilità del documento

Le schermate e i grafici di questo manuale possono differire leggermente dal vostro prodotto a causa delle differenze di versione del vostro prodotto. Edgenexus assicura di compiere ogni ragionevole sforzo per garantire che le informazioni contenute nel presente documento siano complete e accurate. Edgenexus non si assume alcuna responsabilità per eventuali errori. Edgenexus apporta modifiche e correzioni alle informazioni contenute in questo documento nelle versioni future quando se ne presenta la necessità.

Copyrights

Marchi

Supporto Edgenexus

Se avete domande tecniche su questo prodotto, sollevate un ticket di supporto all'indirizzo: support@edgenexus.io

InstallazioneEdgeADC

Il prodotto EdgeADC (indicato come ADC) è disponibile per l'installazione utilizzando diversi metodi. Ogni target di piattaforma richiede il suo installatore, e questi sono tutti disponibili per voi.

Questi sono i vari modelli di installazione disponibili.

- VMware ESXi
- KVM
- Microsoft Hyper-V
- Oracle VM
- ISO per hardware BareMetal

Il dimensionamento della macchina virtuale che userete per ospitare l'ADC dipende dallo scenario del caso d'uso e dal throughput dei dati.

VMware ESXi

ADC è disponibile per l'installazione su VMware ESXi sono 5.x e superiori.

- Scarica l'ultimo pacchetto OVA di installazione di ADC utilizzando il link appropriato fornito con l'e-mail di download.
- Una volta scaricato, decomprimere in una directory adatta sul vostro host ESXi o SAN.
- Nel tuo client vSphere, seleziona File: Deploy OVA/OVF Template.
- Sfogliare e selezionare la posizione in cui avete salvato i vostri file; scegliere il file OVF e cliccare su **NEXT**
- Il server ESX richiede il nome dell'appliance. Digitare un nome adatto e fare clic su **NEXT**
- Seleziona il datastore da cui la tua appliance ADC verrà eseguita.
- Selezionare un datastore con spazio sufficiente e cliccare su **NEXT**
- Poi ti verranno date informazioni sul prodotto; clicca su **NEXT**
- Fare clic su **AVANTI.**
- Una volta che avete copiato i file nel datastore, potete installare il dispositivo virtuale.

Lancia il tuo client vSphere per vedere la nuova appliance virtuale ADC.

- Cliccate con il tasto destro del mouse sul VA e andate su Power > Power-On
- Il vostro VA si avvierà e la schermata di avvio ADC apparirà sulla console.

Installazione dell'interfaccia VMXNET3

Il driver VMXnet3 è supportato, ma dovrai prima apportare delle modifiche alle impostazioni della NIC.

Nota *- NON aggiornare i VMware-tools*

Abilitare l'interfaccia VMXNET3 su una VA appena importata (mai avviata)

1. Elimina entrambe le NIC dalla VM

2. Aggiornare l'hardware della VM - - Fare clic con il tasto destro del mouse sulla VA nell'elenco e selezionare Upgrade Virtual Hardware (non avviare l'installazione o l'aggiornamento degli strumenti VMware, **ma solo l'**aggiornamento dell'hardware)
3. Aggiungere due NIC e selezionarle come VMXNET3
4. Avviare la VA utilizzando il metodo standard. Funzionerà con il VMXNET3

Abilitare l'interfaccia VMXNET3 su una VA già in funzione

1. Fermare la VM (comando CLI shutdown o GUI power-off)
2. Ottieni gli indirizzi MAC di entrambe le NIC (ricorda l'ordine delle NIC nella lista!)
3. Elimina entrambe le NIC dalla VM
4. Aggiornare l'hardware della VM (non avviare l'installazione o l'aggiornamento degli strumenti VMware, **ma solo l'**aggiornamento dell'hardware)
5. Aggiungere due NIC e selezionarle come VMXNET3
6. Impostare gli indirizzi MAC per le nuove NIC di conseguenza al passo 2
7. Riavviare il VA

Supportiamo VMware ESXi come piattaforma di produzione. Per scopi di valutazione, è possibile utilizzare VMware Workstation e Player.

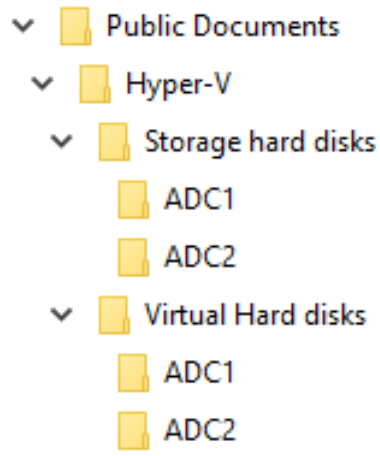
Fate riferimento alla sezione **CONFIGURAZIONE DEL PRIMO AVVIO** per procedere oltre.

Microsoft Hyper-V

L'appliance Edgenexus ADC Virtual può essere facilmente installata all'interno di un framework di virtualizzazione Microsoft Hyper-V. Questa guida presuppone che tu abbia specificato e configurato correttamente il tuo sistema Hyper-V e le risorse di sistema per ospitare l'ADC e la sua architettura di bilanciamento del carico.

Si noti che ogni apparecchio richiede un indirizzo MAC unico.

- Estrai il file ADC-VA compatibile con Hyper-V scaricato sulla tua macchina o server locale.
- Aprite Hyper-V Manager.
- Creare una nuova cartella per contenere il "disco rigido virtuale" ADC VA e un'altra nuova cartella per contenere il "disco rigido di archiviazione", per esempio, C:\Users\PublicDocuments\Hyper-V\Dischi rigidi virtuali\ADC1 e C:\Users\PublicDocuments\Hyper-V\Dischi rigidi di archiviazione\ADC1
- **Nota**: nuove sottocartelle specifiche ADC per i dischi rigidi virtuali e i dischi rigidi di archiviazione devono essere create per ogni installazione di istanza ADC virtuale, come mostrato di seguito:



- Copiare il file EdgeADC .vhd estratto nella cartella 'Storage hard disk' creata in precedenza.
- Nel vostro client Hyper-V Manager, cliccate con il tasto destro sul server e selezionate "Importa macchina virtuale".
- Sfogliare la cartella che contiene il file immagine ADC VA scaricato ed estratto in precedenza

- Seleziona macchina virtuale - evidenzia la macchina virtuale da importare e clicca su Avanti
- Seleziona macchina virtuale - evidenzia la macchina virtuale da importare e clicca su Avanti
- Scegliere Import Type - selezionare "**Copy the virtual machine (create a new unique ID)**" cliccare su next
- Scegliere le cartelle per i file della macchina virtuale - la destinazione può essere lasciata come quella predefinita di Hyper-V o si può scegliere di selezionare una posizione diversa
- Individuare i dischi rigidi virtuali - sfogliare e selezionare la cartella dei dischi rigidi virtuali creata in precedenza e fare clic su Avanti
- Scegliere le cartelle per memorizzare i dischi rigidi virtuali - sfogliare e selezionare la cartella dei dischi rigidi di archiviazione creata in precedenza e fare clic su Avanti
- Verificare che i dettagli nella finestra Completamento dell'importazione guidata siano corretti e fare clic su Fine
- Cliccate con il tasto destro del mouse sulla macchina virtuale **ADC** appena importata e selezionate Start

NOTA: COME PER HTTP://SUPPORT.MICROSOFT.COM/KB/2956569 SI DOVREBBE IGNORARE IL MESSAGGIO DI STATO "DEGRADATO (È RICHIESTO L'AGGIORNAMENTO DEI SERVIZI DI INTEGRAZIONE)", CHE PUÒ ESSERE VISUALIZZATO COME SEGUE DOPO L'AVVIO DELLA VA. NON È RICHIESTA ALCUNA AZIONE E IL SERVIZIO NON È DEGRADATO

- Mentre la VM si sta inizializzando, puoi fare clic con il tasto destro del mouse sulla voce della VM e selezionare Connect...Ti verrà quindi presentata la console EdgeADC.

- Una volta configurate le proprietà di rete, il VA si riavvia e presenta il logon alla console del VA.

Fate riferimento alla sezione **CONFIGURAZIONE DEL PRIMO AVVIO** per procedere oltre.

Citrix XenServer

Il dispositivo ADC Virtual è installabile su Citrix XenServer.

- Estrai il file ADC OVA ALB-VA sul tuo computer o server locale.
- Aprite Citrix XenCenter Client.
- Nel tuo client XenCenter, seleziona **"File: Import".**
- Sfogliare e selezionare il file **OVA**, quindi fare clic su **"Open Next".**
- Seleziona la posizione di creazione della VM quando ti viene chiesto.
- Scegliete quale XenServer desiderate installare e cliccate su **"NEXT".**
- Seleziona il repository dello storage (SR) per il posizionamento del disco virtuale quando ti viene chiesto.
- Seleziona un SR con spazio sufficiente e clicca su **"NEXT".**
- Mappate le vostre interfacce di rete virtuali. Entrambe le interfacce diranno Eth0; tuttavia, notate che l'interfaccia inferiore è Eth1.
- Selezionare la rete di destinazione per ogni interfaccia e fare clic su **AVANTI**
- **NON** spuntare la casella "Use Operating System Fixup".
- Fare clic su **"AVANTI".**
- Scegli l'interfaccia di rete da utilizzare per la VM di trasferimento temporaneo.
- Scegliete l'interfaccia di gestione, di solito Rete 0, e lasciate le impostazioni di rete su DHCP. Tieni presente che devi assegnare dettagli di indirizzo IP statico se non hai un server DHCP funzionante per il trasferimento. In caso contrario, l'importazione dirà Connecting continuously e poi failed. Fare clic su **"AVANTI".**

- Rivedere tutte le informazioni e controllare poi le impostazioni corrette. Fare clic su **"FINISH".**
- La tua VM inizierà a trasferire il disco virtuale "ADC ADC" e, una volta completata, apparirà sotto il tuo XenServer.
- All'interno del vostro client XenCenter, sarete ora in grado di vedere la nuova macchina virtuale. Fai clic destro sulla VA e clicca su "**START**".
- La tua VM si avvierà quindi, e la schermata di avvio ADC apparirà.

- Una volta configurato, si presenta il logon alla VA.

Fate riferimento alla sezione **CONFIGURAZIONE DEL PRIMO AVVIO** per procedere oltre.

Nutanix AHV

La seguente sezione mostra come installare EdgeADC su una piattaforma Nutanix AHV.

Requisiti e versioni

Questa guida è rilevante per EdgeADC 4.2.6 e superiori.

Tutte le versioni dell'hypervisor Nutanix sono compatibili, ma la certificazione è stata eseguita su Nutanix versione 5.10.9.

- Il primo passo è quello di accedere a Nutanix Prism Central.

Caricamento dell'immagine EdgeADC

- Spostarsi su Infrastruttura virtuale > Immagini
- Fare clic sul pulsante Aggiungi immagine
- Seleziona il file immagine EdgeADC che hai scaricato e clicca sul pulsante Open per caricare l'immagine.
- Inserisci un nome per l'immagine nel campo Image Description.
- Seleziona una categoria appropriata
- Seleziona l'immagine e clicca sul tasto freccia destra
- Seleziona Tutte le immagini e clicca su Salva.

Creare la VM

- Vai a Infrastruttura virtuale > VM
- Fare clic sul pulsante Create VM (Crea VM)
- Inserisci un nome per la VM, il numero di CPU che desideri avere e il numero di core che vuoi assegnare alla VM.
- Poi scorri verso il basso nella finestra di dialogo e inserisci la quantità di memoria che vuoi assegnare alla VM. Puoi iniziare con 4GB e aumentarla a seconda dell'utilizzo.

Aggiungere il disco

- Successivamente, clicca sul link Aggiungi nuovo disco
- Seleziona l'opzione Clone from Image Service nel menu a tendina Operation.
- Seleziona l'immagine EdgeADC che hai aggiunto e fai clic sul pulsante Aggiungi.
- Selezionate il disco che sarà il disco avviabile.

Aggiungere la NIC, la rete e l'affinità

- Poi, clicca sul pulsante Add New NIC. Avrai bisogno di due NIC.
- Seleziona la Rete e clicca sul pulsante Aggiungi
- Fare clic sul pulsante Imposta affinità
- Seleziona gli host Nutanix su cui la VM può essere eseguita, quindi fai clic sul pulsante Salva.
- Verifica le impostazioni che hai fatto e clicca sul pulsante Salva

Accendere la VM

- Dall'elenco delle VM, clicca sul nome della VM che hai appena creato
- Fare clic sul pulsante Power On per la VM
- Una volta che la VM si è accesa, clicca sul pulsante Launch Console

Configurazione della rete EdgeADC

- Seguite le istruzioni nella sezione Primo ambiente di avvio.
- EdgeADC è ora pronto per l'uso, e sarà possibile accedere alla sua GUI utilizzando il browser e l'indirizzo IP di gestione.

Configurazione del primo avvio

Al primo avvio, l'ADC VA visualizza la seguente schermata che richiede la configurazione per le operazioni di produzione.

Primo avvio - Dettagli di rete manuali

Al primo avvio, avrete 10 secondi per interrompere l'assegnazione automatica dei dettagli IP tramite DHCP

Per interrompere questo processo, cliccate nella finestra della console e premete un tasto qualsiasi. Potete quindi inserire manualmente i seguenti dettagli.

- Indirizzo IP
- Maschera di sottorete
- Gateway
- Server DNS

Queste modifiche sono persistenti e sopravvivono a un riavvio e non hanno bisogno di essere configurate di nuovo sulla VA.

Primo avvio - DHCP riuscito

Se non interrompi il processo di assegnazione della rete, il tuo ADC contatterà un server DHCP dopo un timeout per ottenere i suoi dettagli di rete. Se il contatto ha successo, alla tua macchina verranno assegnate le seguenti informazioni.

- Indirizzo IP
- Maschera di sottorete
- Gateway predefinito
- Server DNS

Consigliamo di non utilizzare l'ADC VA usando un indirizzo DHCP a meno che quell'indirizzo IP si colleghi permanentemente all'indirizzo MAC del VA all'interno del server DHCP. Consigliamo sempre di usare un **INDIRIZZO IP FISSO** quando si usa il VA. Seguire i passi in **CAMBIARE L'INDIRIZZO IP DI GESTIONE** e le sezioni successive fino a completare la configurazione della rete.

Primo avvio - DHCP fallisce

Se non avete un server DHCP o la connessione fallisce, verrà assegnato l'indirizzo IP 192.168.100.100. L'indirizzo IP aumenterà di '1' finché il VA non troverà un indirizzo IP libero. Allo stesso modo, il VA controllerà per vedere se l'indirizzo IP è attualmente in uso, e se è così, incrementerà di nuovo e ricontrollerà.

Cambiare l'indirizzo IP di gestione

Potete cambiare l'indirizzo IP del VA in qualsiasi momento usando il comando **set greenside=n.n.n.n.n,** come mostrato qui sotto.

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

Cambiare la maschera di sottorete per eth0

Le interfacce di rete usano il prefisso 'eth'; l'indirizzo di rete base è chiamato eth0. La subnet mask o netmask può essere cambiata usando il comando **set mask eth0 n.n.n.n.** Potete vedere un esempio qui sotto.

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

Assegnare un gateway predefinito

La VA ha bisogno di un gateway predefinito per le sue operazioni. Per impostare il gateway predefinito, usate il comando **route add default gw n.n.n.n** come mostrato nell'esempio seguente.

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

Controllare il valore del gateway predefinito

Per controllare se il gateway predefinito è stato aggiunto ed è corretto, usate il comando **route**. Questo comando visualizzerà le rotte di rete e il valore del gateway predefinito. Vedi l'esempio qui sotto.

```
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
```

Ora puoi accedere all'interfaccia grafica utente (GUI) per configurare l'ADC per la produzione o l'uso di valutazione.

Accesso all'interfaccia web

È possibile utilizzare qualsiasi browser Internet con Javascript per configurare, monitorare e distribuire l'ADC in uso operativo.

Nel campo URL del browser, digitare **HTTPS://{INDIRIZZO IP} o HTTPS://{FQDN}**

L'ADC, per default, usa un certificato SSL autofirmato. Puoi cambiare l'ADC per usare il certificato SSL di tua scelta.

Una volta che il tuo browser raggiunge l'ADC, ti mostrerà la schermata di accesso. Le credenziali predefinite per l'ADC sono:

Nome utente predefinito = **admin** / Password predefinita = **jetnexus**

Tabella di riferimento dei comandi

Comando	Parametro1	Parametro2	Descrizione	Esempio
data			Mostra la data e l'ora attualmente configurate	mar 3 settembre 13:00 UTC 2013
default			Assegnare le impostazioni predefinite di fabbrica per l'apparecchio	
uscire			Esci dall'interfaccia a riga di comando	
aiutare			Visualizza tutti i comandi validi	
ifconfig	[vuoto]		Visualizza la configurazione dell'interfaccia per tutte le interfacce	ifconfig
	eth0		Visualizza solo la configurazione dell'interfaccia eth0	ifconfig eth0
machineid			Questo comando fornirà il machineid utilizzato per abilitare l'ADC ADC	EF4-3A35-F79
lasciare			Esci dall'interfaccia a riga di comando	
riavvio			Terminare tutte le connessioni e riavviare l'ADC ADC	riavvio
riavviare			Riavviare i servizi virtuali ADC ADC	
percorso	[vuoto]		Visualizzare la tabella di routing	percorso
	aggiungere	gw predefinito	Aggiungere l'indirizzo IP del gateway predefinito	route add default gw 192.168.100.254
impostare	greenside		Impostare l'indirizzo IP di gestione per l'ADC	set greenside=192.168.101.1
	maschera		Imposta la subnet mask per un'interfaccia. I nomi delle interfacce sono eth0, eth1....	impostare la maschera eth0 255.255.255.0
mostra			Visualizza le impostazioni di configurazione globale	
spegnimento			Terminare tutte le connessioni e spegnere l'ADC ADC	
stato			Visualizza le statistiche dei dati correnti	
top			Visualizza le informazioni sul processo come la CPU e la memoria	
viewlog	messaggi		Visualizza i messaggi grezzi di syslog	Visualizzare i messaggi di log

Nota: i comandi non fanno distinzione tra maiuscole e minuscole. Non c'è una cronologia dei comandi.

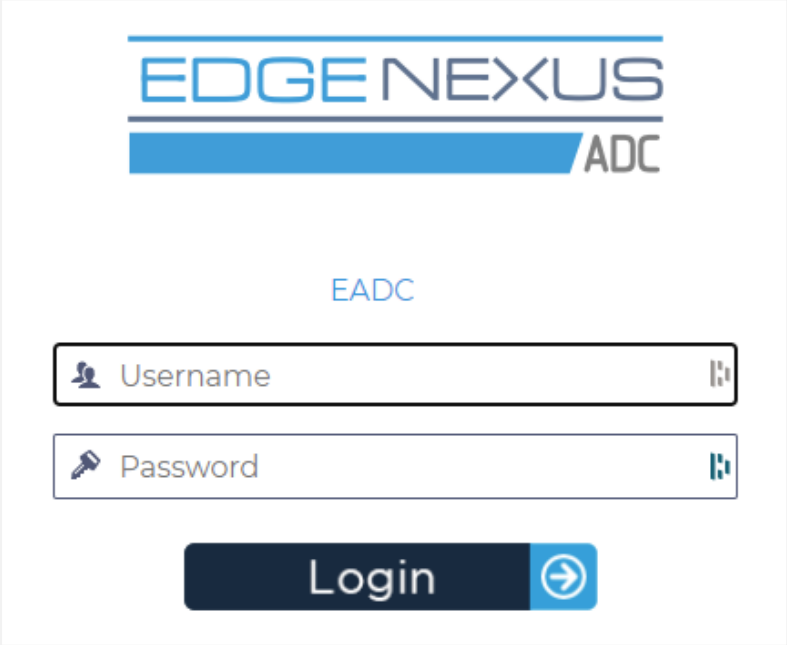
Lanciare la console web ADC

Tutte le operazioni sull'ADC (chiamato anche ADC) sono configurate ed eseguite tramite la console web. Si accede alla console web utilizzando qualsiasi browser con Javascript.

Per lanciare la console web ADC, inserisci l'URL o l'indirizzo IP dell'ADC nel campo URL. Useremo l'esempio di adc.company.com come esempio:

https://adc.company.com

Quando viene lanciata, la console web dell'ADC è come mostrato di seguito, permettendoti di accedere come utente admin.



Credenziali di accesso predefinite

Le credenziali di accesso predefinite sono:

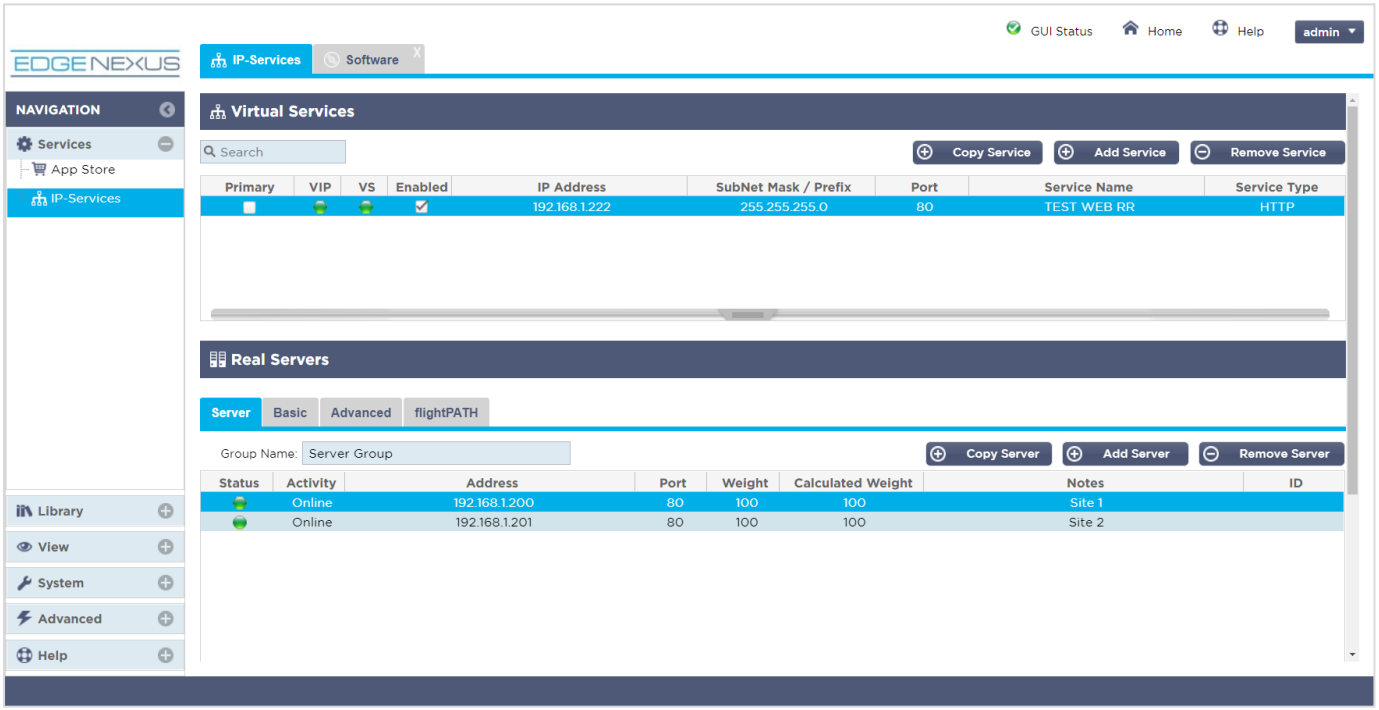
- Nome utente: admin
- Password: jetnexus

Puoi cambiarlo in qualsiasi momento usando le funzionalità di configurazione degli utenti che si trovano in *Sistema* > *Utenti*.

Una volta effettuato con successo l'accesso, viene visualizzata la dashboard principale dell'ADC.

Il cruscotto principale

L'immagine qui sotto illustra come appare il cruscotto principale o 'home page' dell'ADC. Potremmo fare alcuni cambiamenti di tanto in tanto per motivi di miglioramento, ma tutte le funzioni rimarranno.



Per essere il più conciso possibile, daremo per scontato che questa prima introduzione alle sezioni dello schermo si dimostri sufficientemente consapevole delle diverse sezioni dell'area di configurazione dell'ADC, quindi non le descriveremo in dettaglio man mano che avanziamo ma ci concentreremo piuttosto sugli elementi di configurazione.

Andando da sinistra a destra, abbiamo prima la Navigazione. La sezione Navigazione consiste nelle diverse aree all'interno di ADC. Quando clicchi su una scelta particolare all'interno di Navigation, questo visualizzerà la sezione corrispondente sul lato destro dello schermo. Puoi anche vedere la sezione di configurazione scelta a schede nella parte superiore dello schermo, adiacente al logo del prodotto. Le schede consentono una navigazione più rapida verso le aree già utilizzate della configurazione dell'ADC.

Servizi

La sezione servizi dell'ADC ha diverse aree al suo interno. Quando clicchi sulla voce Servizio, questa si espanderà per mostrare le scelte disponibili.

Servizi IP

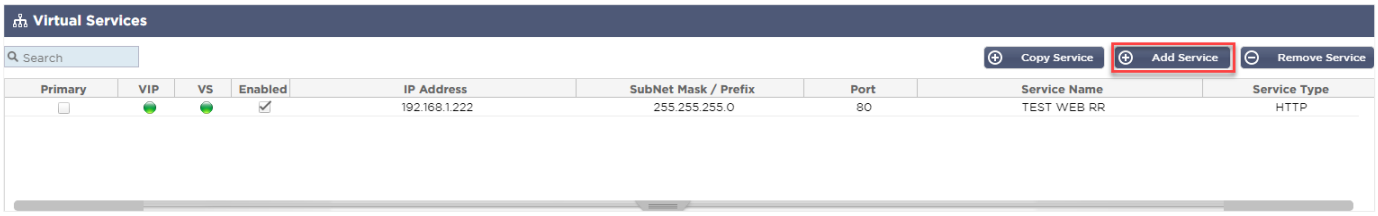
La sezione Servizi IP dell'ADC ti permette di aggiungere, cancellare e configurare i vari servizi IP virtuali di cui hai bisogno per il tuo particolare caso d'uso. Le impostazioni e le opzioni rientrano nelle sezioni seguenti. Queste sezioni si trovano sul lato destro della schermata dell'applicazione.

Servizi virtuali

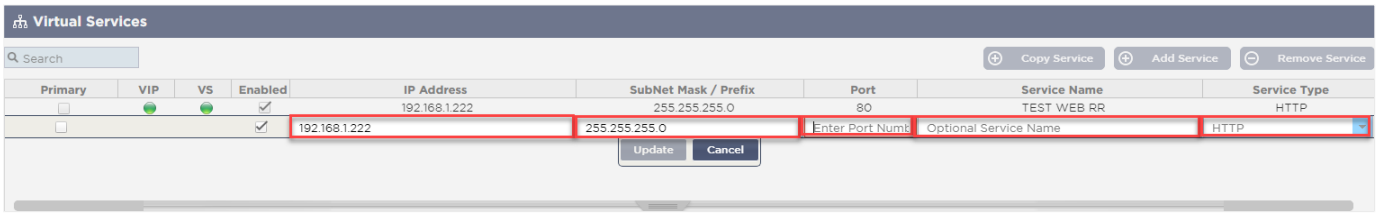
Un servizio virtuale combina un IP virtuale (VIP) e una porta TCP/UDP su cui l'ADC ascolta. Il traffico che arriva all'IP del servizio virtuale è reindirizzato a uno dei Real Server associati a quel servizio. L'indirizzo IP del servizio virtuale non può essere lo stesso dell'indirizzo di gestione dell'ADC, cioè eth0, eth1 ecc.

L'ADC determina come il traffico viene ridistribuito ai server in base a una politica di bilanciamento del carico impostata nella scheda Basic nella sezione Real Servers.

Creare un nuovo servizio virtuale usando un nuovo VIP



- Cliccate sul pulsante Add Virtual Service come indicato sopra.

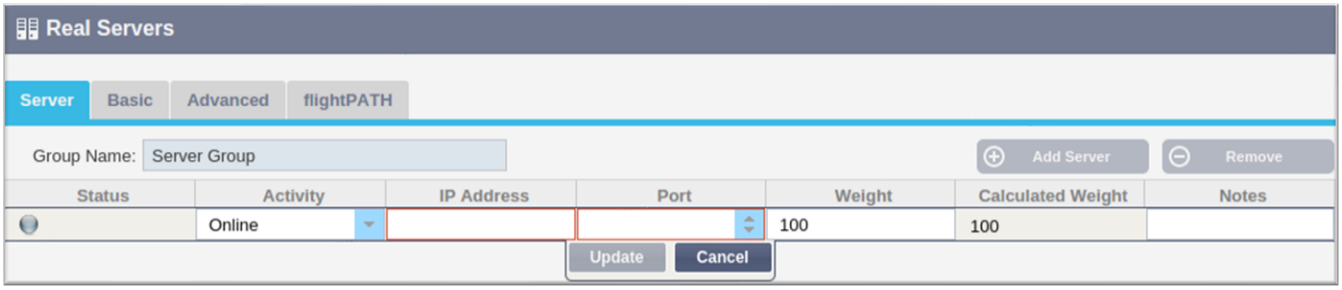


- Entrerete quindi nella modalità di **modifica della riga.**
- Completa i quattro campi evidenziati per procedere, e poi fai clic sul pulsante di aggiornamento.

Si prega di utilizzare il tasto TAB per navigare attraverso i campi.

Campo	Descrizione
Indirizzo IP	Inserisci un nuovo indirizzo IP virtuale per essere il punto di ingresso di destinazione per l'accesso al Real Server. Questo IP è dove gli utenti o le applicazioni punteranno per accedere all'applicazione con bilanciamento del carico.
Subnet Mask/Prefix	Questo campo è per la subnet mask relativa alla rete su cui si trova l'ADC
Porto	La porta d'ingresso utilizzata quando si accede al VIP. Questo valore non deve necessariamente essere lo stesso del Real Server se usi il Reverse Proxy.
Nome del servizio	Il nome del servizio è una rappresentazione testuale dello scopo del VIP. È facoltativo, ma ti consigliamo di fornirlo per chiarezza.
Tipo di servizio	Ci sono molti diversi tipi di servizio disponibili per voi da selezionare. I tipi di servizio Layer 4 non possono usare la tecnologia flightPATH.

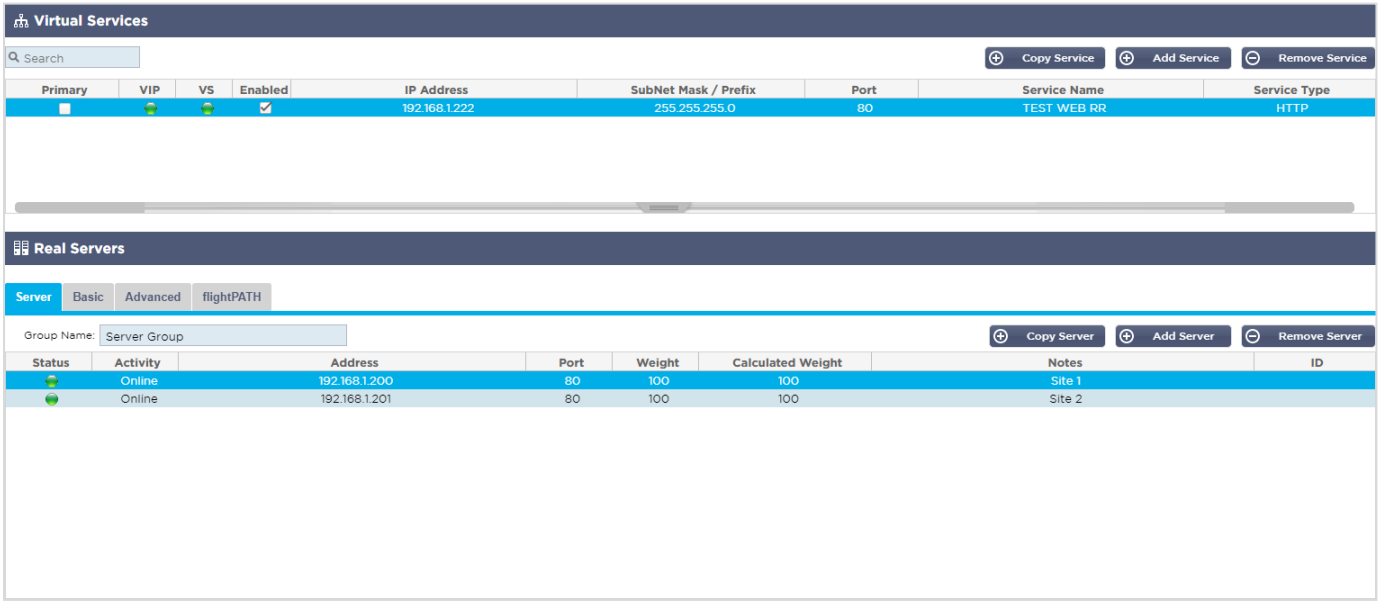
Ora puoi premere il pulsante Update per salvare questa sezione e passare automaticamente alla sezione Real Server dettagliata qui sotto:



Campo	Descrizione
Attività	Il campo Attività può essere usato per mostrare e cambiare lo stato del server reale bilanciato. Online - Indica che il server è attivo e sta ricevendo richieste bilanciate Offline - Il server è offline e non riceve richieste Drenaggio - Il server è stato messo in modalità di drenaggio in modo che la persistenza possa essere scaricata e il server spostato in uno stato offline senza influenzare gli utenti. Standby - Il server è stato messo in uno stato di standby
Indirizzo IP	Questo valore è l'indirizzo IP del Real Server. Deve essere preciso e non deve essere un indirizzo DHCP.
Porto	La porta di destinazione di accesso sul Real Server. Quando si utilizza un reverse proxy, questo può essere diverso dalla porta d'ingresso specificata sul VIP.
Ponderazione	Questa impostazione di solito è configurata automaticamente dall'ADC. Puoi cambiarla se vuoi cambiare la ponderazione della priorità.

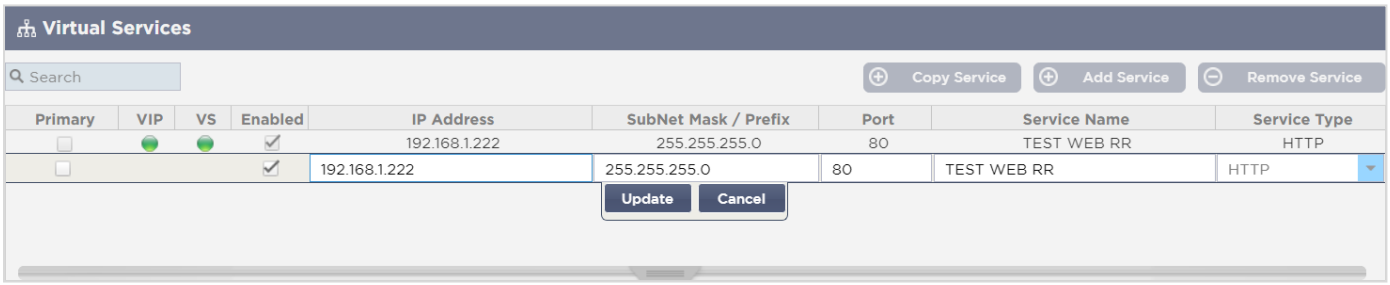
- Fare clic sul pulsante Aggiorna o premere Invio per salvare le modifiche
- La luce di stato diventerà prima grigia, seguita da verde se il controllo dell'integrità del server ha successo. Diventerà rossa se il Real Server Monitor fallisce.
- Un server che ha una luce di stato rossa non sarà bilanciato.

Esempio di un servizio virtuale completato

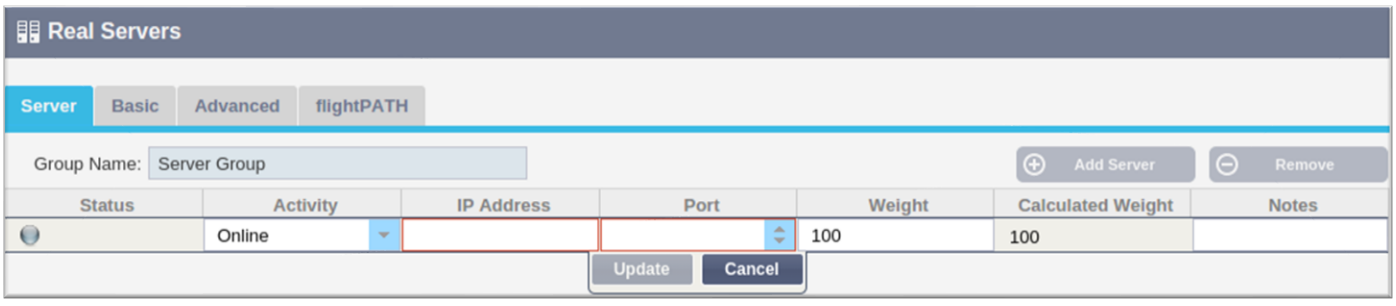


Creare un nuovo servizio virtuale usando un VIP esistente

- Evidenziare un servizio virtuale che si desidera copiare
- Fare clic su Add Virtual Service per entrare nella modalità di modifica della riga



- L'indirizzo IP e la maschera di sottorete si copiano automaticamente
- Inserisci il numero di porta per il tuo servizio
- Inserire un nome di servizio opzionale
- Selezionare un tipo di servizio
- Ora puoi premere il pulsante Update per salvare questa sezione e passare automaticamente alla sezione Real Server qui sotto



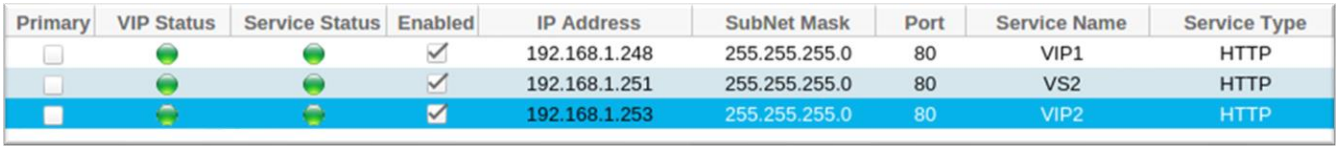
- Lascia l'opzione Attività del server come Online - questo significa che sarà bilanciato se passa il controllo di salute predefinito di TCP Connect. Questa impostazione può essere cambiata in seguito, se necessario.
- Inserire un indirizzo IP del Real Server
- Inserire un numero di porta per il server reale
- Inserisci un nome opzionale per il Real Server
- Clicca su Update per salvare le tue modifiche

- La luce di stato diventerà prima grigia, poi verde se il controllo dell'integrità del server ha successo. Diventa rossa se il Real Server Monitor fallisce.
- Un server che ha una luce di stato rossa non sarà bilanciato nel carico

Cambiare l'indirizzo IP di un servizio virtuale

Puoi cambiare l'indirizzo IP di un servizio virtuale o di un VIP esistente in qualsiasi momento.

- Evidenziare il servizio virtuale di cui si vuole cambiare l'indirizzo IP



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

- Fare doppio clic sul campo dell'indirizzo IP per quel servizio

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

Update Cancel

- Cambia l'indirizzo IP con quello che vuoi usare
- Clicca sul pulsante Update per salvare le modifiche.

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

Nota: cambiare l'indirizzo IP di un servizio virtuale cambierà l'indirizzo IP di tutti i servizi associati al VIP

Creare un nuovo servizio virtuale usando Copy Service

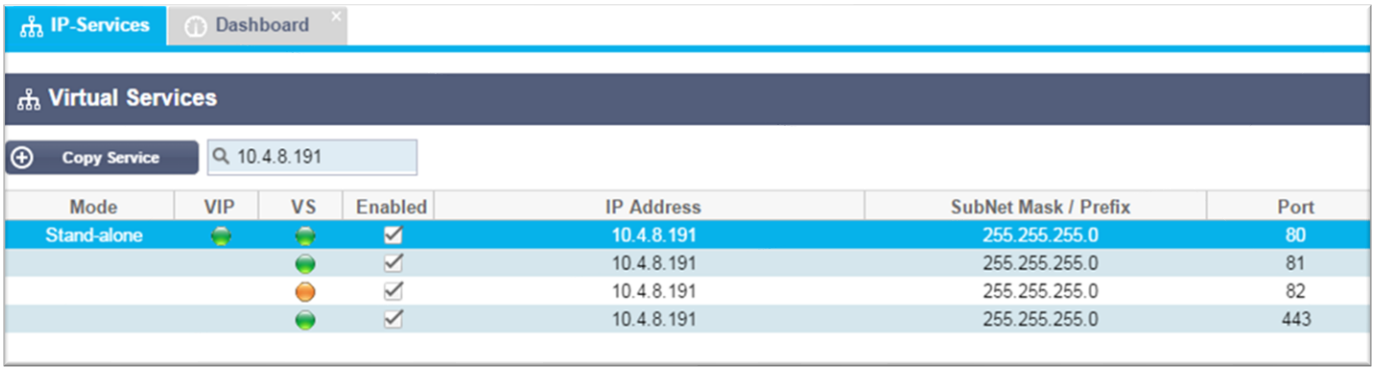
- Il pulsante Copy Service copierà un intero servizio, compresi tutti i Real Server, le impostazioni di base, le impostazioni avanzate e le regole flightPATH ad esso associate
- Evidenziare il servizio che si desidera duplicare e fare clic su Copy Service
- L'editor di riga apparirà con il cursore lampeggiante sulla colonna Indirizzo IP
- Devi cambiare l'indirizzo IP in modo che sia unico, o se vuoi mantenere l'indirizzo IP, devi modificare la porta in modo che sia unica per quell'indirizzo IP

Non dimenticare di modificare ogni scheda se cambi un'impostazione come una politica di bilanciamento del carico, il monitor Real Server, o rimuovi una regola flightPATH.

Filtrare i dati visualizzati

Ricerca di un termine specifico

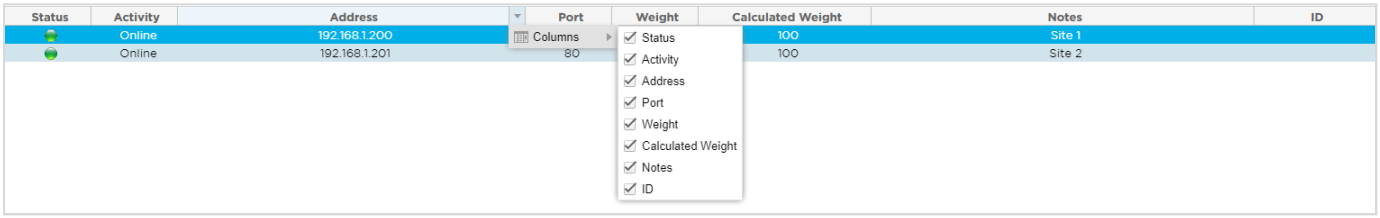
La casella di ricerca permette di cercare nella tabella usando qualsiasi valore, come gli ottetti dell'indirizzo IP o il nome del servizio.



L'esempio qui sopra mostra il risultato della ricerca di un indirizzo IP specifico di 10.4.8.191.

Selezione della visibilità delle colonne

Puoi anche selezionare le colonne che desideri visualizzare nella dashboard.

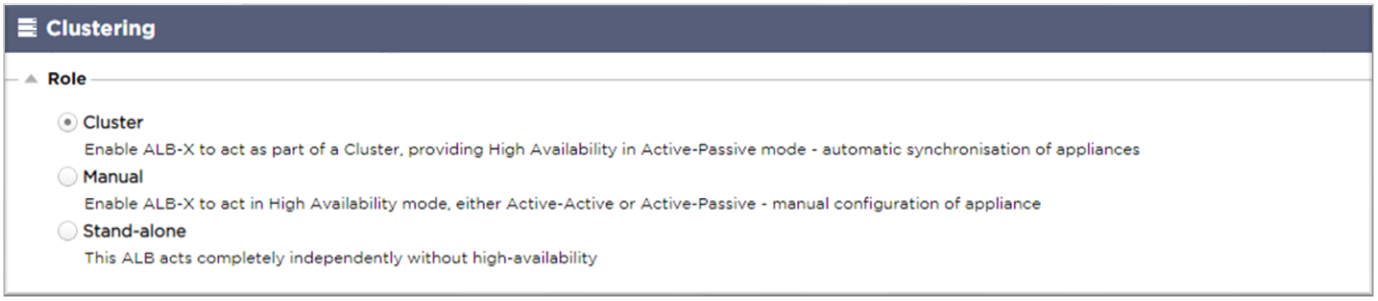


- Muovi il mouse su una qualsiasi delle colonne
- Vedrai apparire una piccola freccia sul lato destro della colonna
- Facendo clic sulle caselle di controllo si selezionano le colonne che si desidera vedere nel dashboard.

Capire le colonne dei servizi virtuali

Primario/Modo

La colonna Primary/Mode indica il ruolo di alta disponibilità selezionato per il VIP corrente. Usa le opzioni disponibili in Sistema > Clustering per configurare questa opzione.



Opzione	Descrizione
Cluster	Cluster è il ruolo predefinito per l'ADC all'installazione, e la colonna Primary/Mode indicherà la modalità in cui è attualmente in esecuzione. Quando hai una coppia HA di apparecchi ADC nel tuo centro dati, uno di essi mostrerà Active e l'altro Passive
Manuale	Il ruolo Manual permette alla coppia ADC di funzionare in modalità Active-Active per diversi indirizzi IP virtuali. In questi casi, la colonna Primary conterrà una casella accanto ad ogni unico Virtual IP che può essere spuntata per Active o lasciata deselezionata per Passive.
Stand-Alone	L'ADC sta agendo come un dispositivo stand-alone e non è in modalità High Availability. Come tale, la colonna Primary indicherà Stand-alone.

VIP

Questa colonna fornisce un feedback visivo sullo stato di ogni servizio virtuale. Gli indicatori sono codificati a colori e sono i seguenti:

LED	Significato
●	Online
●	Failover-Standby. Questo servizio virtuale è hot-standby
●	Indica che un "secondario" sta aspettando un "primario".
●	Il servizio ha bisogno di attenzione. Questa indicazione può derivare da un Real Server che fallisce un controllo dello stato di salute o è stato cambiato manualmente in Offline. Il traffico continuerà a fluire ma con una capacità ridotta del Real Server
●	Offline. I server di contenuto non sono raggiungibili, o nessun server di contenuto abilitato
●	Trovare lo stato
●	IP virtuali non concessi in licenza o concessi in licenza superati

Abilitato

L'impostazione predefinita per questa opzione è Enabled, e la casella di controllo appare spuntata. Puoi disabilitare il servizio virtuale facendo doppio clic sulla linea, deselezionando la casella di controllo e cliccando sul pulsante Update.

Indirizzo IP

Aggiungi il tuo indirizzo IPv4 in notazione decimale punteggiata o un indirizzo IPv6. Questo valore è l'indirizzo IP virtuale (VIP) per il tuo servizio. Esempio IPv4 "192.168.1.100". Esempio Ipv6 "2001:0db8:85a3:0000:0000:8a2e:0370:7334"

Subnet Mask/Prefix

Aggiungete la vostra subnet mask in notazione decimale punteggiata. Esempio "255.255.255.0". O per IPv6, aggiungi il tuo prefisso. Per maggiori informazioni su IPv6, vedi HTTPS://EN.WIKIPEDIA.ORG/WIKI/IPV6_ADDRESS

Porto

Aggiungi il numero di porta associato al tuo servizio. La porta può essere un numero di porta TCP o UDP. Esempio TCP "80" per il traffico web e TCP "443" per il traffico web protetto.

Nome del servizio

Aggiungete un nome amichevole per identificare il vostro servizio. Esempio: "Production Web Servers".

Tipo di servizio

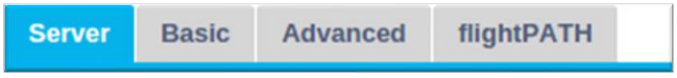
Si prega di notare che con tutti i tipi di servizio "Layer 4", l'ADC non interagisce o modifica il flusso di dati, quindi flightPATH non è disponibile con i tipi di servizio Layer 4. I servizi Layer 4 semplicemente bilanciano il traffico secondo la politica di bilanciamento del carico:

Tipo di servizio	Porta/Protocollo	Strato di servizio	Commento
Layer 4 TCP	Qualsiasi porta TCP	Livello 4	L'ADC non altera alcuna informazione nel flusso di dati ed esegue il bilanciamento standard del traffico secondo la politica di bilanciamento del carico

Livello 4 UDP	Qualsiasi porta UDP	Livello 4	Come con il Layer 4 TCP, l'ADC non altera alcuna informazione nel flusso di dati ed esegue il bilanciamento standard del traffico secondo la politica di bilanciamento del carico
Layer 4 TCP/UDP	Qualsiasi porta TCP o UDP	Livello 4	È ideale se il vostro servizio ha un protocollo primario come UDP ma ricadrà su TCP. L'ADC non altera alcuna informazione nel flusso di dati ed esegue il bilanciamento standard del traffico secondo la politica di bilanciamento del carico
DNS	TCP/UDP	Livello 4	Usato per bilanciare il carico dei server DNS.
HTTP	Protocollo HTTP o HTTPS	Livello 7	L'ADC può interagire, manipolare e modificare il flusso di dati utilizzando flightPATH.
FTP	Protocollo per il trasferimento di file	Livello 7	Usare connessioni di controllo e dati separate tra client e server
SMTP	Protocollo semplice di trasferimento della posta	Livello 4	Da usare per il bilanciamento del carico dei server di posta
POP3	Protocollo dell'ufficio postale	Livello 4	Da usare per il bilanciamento del carico dei server di posta
IMAP	Protocollo di accesso ai messaggi Internet	Livello 4	Da usare per il bilanciamento del carico dei server di posta
RDP	Protocollo desktop remoto	Livello 4	Da usare per il bilanciamento del carico dei server Terminal Services
RPC	Chiamata di procedura remota	Livello 4	Usare quando si bilanciano i sistemi di carico usando chiamate RPC
RPC/ADS	Exchange 2010 RPC statico per il servizio di rubrica	Livello 4	Da usare per il bilanciamento del carico dei server Exchange
RPC/CA/PF	Exchange 2010 RPC statico per accesso client e cartelle pubbliche	Livello 4	Da usare per il bilanciamento del carico dei server Exchange
DICOM	Imaging digitale e comunicazioni in medicina	Livello 4	Usare quando si bilanciano i server che usano i protocolli DICOM

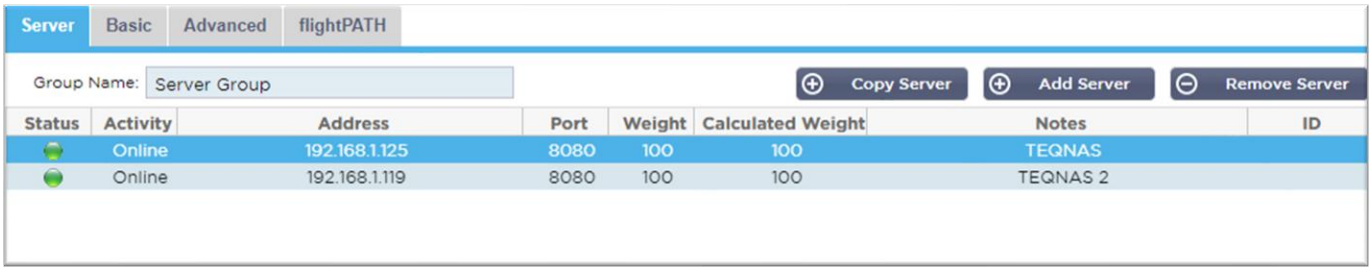
Server reali

Ci sono diverse schede nella sezione Real Servers della dashboard: Server, Basic, Advanced e flightPATH.



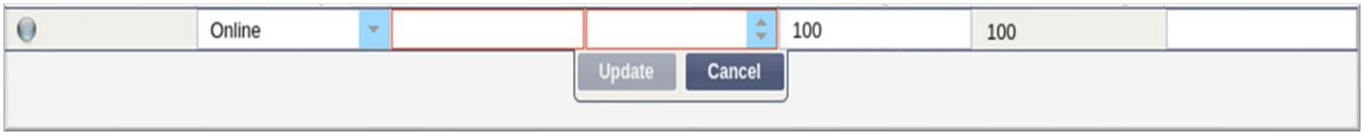
Server

La scheda Server contiene le definizioni dei server reali di back-end abbinati al servizio virtuale attualmente selezionato. È necessario aggiungere almeno un server alla sezione Real Servers.



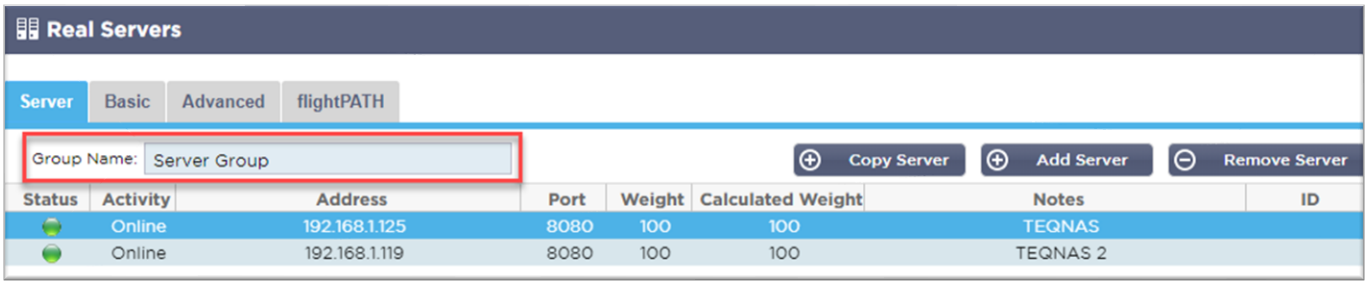
Aggiungere il server

- Seleziona il VIP appropriato che hai precedentemente definito.
- Fare clic su Add Server
- Apparirà una nuova riga con il cursore lampeggiante sulla colonna dell'indirizzo IP



- Inserisci l'indirizzo IPv4 del tuo server in notazione decimale punteggiata. Il server reale può essere sulla stessa rete del tuo servizio virtuale, qualsiasi rete locale direttamente collegata, o qualsiasi rete che il tuo ADC può instradare. Esempio "10.1.1.1".
- Vai alla colonna Port e inserisci il numero di porta TCP/UDP per il tuo server. Il numero di porta può essere lo stesso del numero di porta del servizio virtuale o un altro numero di porta per la connettività Reverse Proxy. L'ADC tradurrà automaticamente questo numero.
- Vai alla sezione Note per aggiungere qualsiasi dettaglio rilevante per il server. Esempio: "IIS Web Server 1"

Nome del gruppo



Quando hai aggiunto i server che compongono l'insieme bilanciato, puoi anche allegare un nome di gruppo. Una volta modificato questo campo, il contenuto viene salvato senza bisogno di premere il pulsante Update.

Luci di stato del server reale

Puoi vedere lo stato di un Real Server dal colore chiaro nella colonna Stato. Vedi sotto:

LED	Significato
●	Collegato
○	Non monitorato
●	Drenaggio di

●	Offline
●	Standby
●	Non collegato
●	Trovare lo stato
●	Server reali non licenziati o con licenza superata

Attività

Puoi cambiare l'attività di un Real Server in qualsiasi momento utilizzando il menu a tendina. Per farlo, fai doppio clic su una riga del Real Server per metterla in modalità di modifica.

Opzione	Descrizione
Online	Tutti i Real Server assegnati online riceveranno il traffico secondo la politica di bilanciamento del carico impostata nella scheda Base.
Scarico	Tutti i Real Server assegnati come Drenaggio continueranno a servire le connessioni esistenti ma non accetteranno nuove connessioni. La luce di stato lampeggerà verde/blu mentre il drenaggio è in corso. Una volta che le connessioni esistenti si sono chiuse naturalmente, i Real Server andranno offline e la luce di stato sarà blu fissa. Puoi anche visualizzare queste connessioni navigando nella sezione Navigazione > Monitor > Stato.
Offline	Tutti i Real Server impostati come Offline saranno immediatamente messi offline e non riceveranno alcun traffico.
Standby	Tutti i Real Server impostati come Standby rimarranno offline fino a quando **TUTTI** i server del gruppo Online non falliranno i controlli del Server Health Monitor. Il traffico viene ricevuto dal gruppo Standby secondo la politica di bilanciamento del carico quando questo accade. Se un server del gruppo Online passa il controllo del Server Health Monitor, questo server Online riceverà tutto il traffico, e il gruppo Standby smetterà di ricevere il traffico.

Indirizzo IP

Questo campo è l'indirizzo IP del tuo Real Server. Esempio "192.168.1.200".

Porto

Numero di porta TCP o UDP che il Real Server sta ascoltando per il servizio. Esempio "80" per il traffico web.

Peso

Questa colonna diventa modificabile quando viene specificata una politica di bilanciamento del carico appropriata.

Il peso di default per un Real Server è 100, e puoi inserire valori da 1-100. Un valore di 100 significa carico massimo, e 1 significa carico minimo.

Un esempio per tre server potrebbe essere qualcosa del genere:

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

Se consideriamo che la politica di bilanciamento del carico è impostata su Least Connections, e ci sono 200 connessioni client totali;

- Il server 1 riceverà 100 connessioni simultanee
- Il server 2 riceverà 50 connessioni simultanee
- Il server 3 riceverà 50 connessioni simultanee

Se dovessimo usare Round Robin come metodo di bilanciamento del carico, che fa ruotare le richieste attraverso l'insieme di server bilanciati, alterare i pesi influisce su quanto spesso i server vengono scelti come obiettivo.

Se crediamo che la politica di bilanciamento del carico più veloce utilizzi il tempo più breve impiegato per ottenere una risposta, la regolazione dei pesi altera il bias in modo simile a Least Connections.

Peso calcolato

Il peso calcolato di ogni server può essere visualizzato dinamicamente e viene calcolato automaticamente e non è modificabile. Il campo mostra la ponderazione effettiva che ADC sta usando quando considera la ponderazione manuale e la politica di bilanciamento del carico.

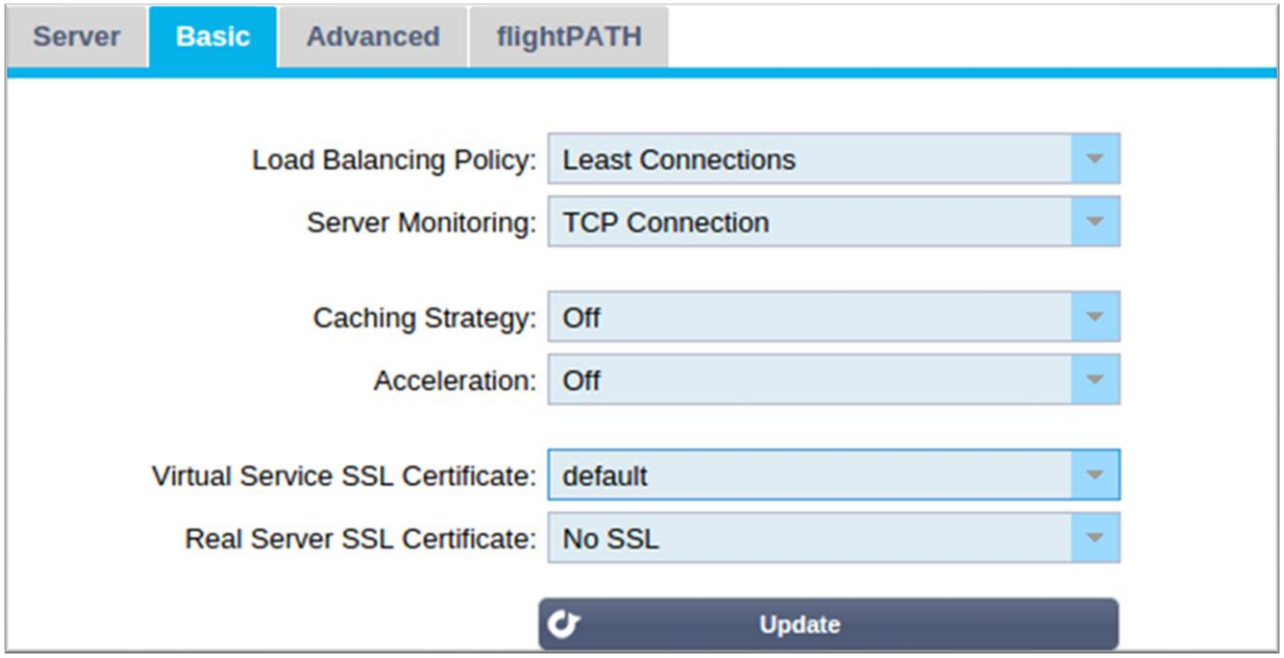
Note

Inserite qualsiasi nota particolare utile per descrivere la voce definita nel campo Note. Esempio "IIS Server1 - London DC".

ID

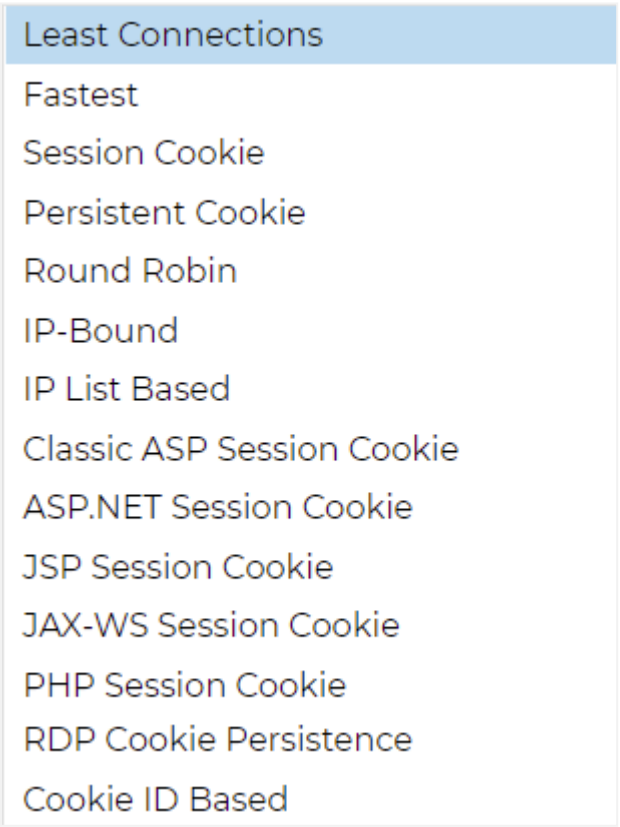
Il campo ID è utilizzato all'interno della politica di bilanciamento del carico dell'ID del cookie. Il numero ID qui inserito è utilizzato per identificare

Base



Politica di bilanciamento del carico

L'elenco a discesa mostra le politiche di bilanciamento del carico attualmente supportate e disponibili per l'uso. Un elenco delle politiche di bilanciamento del carico, insieme ad una spiegazione, è qui sotto.



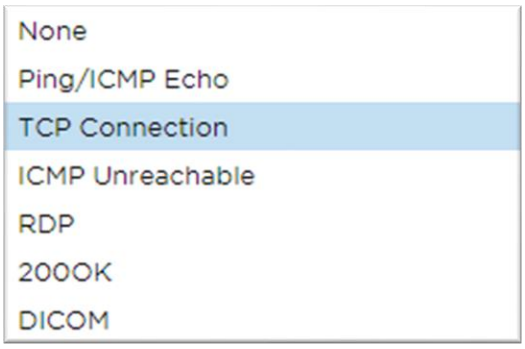
Opzione	**Descrizione**
Il più veloce	La politica di bilanciamento del carico più veloce calcola automaticamente il tempo di risposta per tutte le richieste per server livellato nel tempo. La colonna Calculated Weight contiene il valore calcolato automaticamente. L'inserimento

	manuale è possibile solo quando si usa questa politica di bilanciamento del carico.
Round Robin	Round Robin è comunemente usato nei firewall e nei bilanciatori di carico di base ed è il metodo più semplice. Ogni Real Server riceve una nuova richiesta in sequenza. Questo metodo è appropriato solo quando è necessario bilanciare il carico di richieste ai server in modo uniforme; un esempio potrebbe essere il look-up dei server web. Tuttavia, quando è necessario bilanciare il carico in base al carico dell'applicazione o al carico del server, o anche assicurarsi di utilizzare lo stesso server per la sessione, il metodo Round Robin è inappropriato.
Meno connessioni	Il bilanciatore di carico terrà traccia del numero di connessioni correnti a ciascun Real Server. Il Real Server con il minor numero di connessioni riceve la nuova richiesta successiva.
IP Bound Affinità/Persistenza di sessione del livello 3	In questa modalità, l'indirizzo IP del client costituisce la base per selezionare quale Real Server riceverà la richiesta. Questa azione fornisce persistenza. I protocolli HTTP e Layer 4 possono utilizzare questa modalità. Questo metodo è utile per le reti interne dove la topologia di rete è nota, e si può essere sicuri che non ci siano "super proxy" a monte. Con il Layer 4 e i proxy, tutte le richieste possono apparire come se provenissero da un solo client, e come tali, il carico non sarebbe uniforme. Con HTTP, l'informazione dell'intestazione (X-Forwarder-For) viene utilizzata quando presente per far fronte ai proxy.
Lista IP basata su Affinità/Persistenza di sessione del livello 3	La connessione al Real Server inizia usando "Least connections" quindi, l'affinità di sessione è ottenuta in base all'indirizzo IP del client. Un elenco è mantenuto per 2 ore per impostazione predefinita, ma questo può essere cambiato utilizzando un jetPACK.
Cookie di sessione Layer 7 Affinità/Persistenza della sessione	Questa modalità è il metodo di persistenza più popolare per il bilanciamento del carico HTTP. In questa modalità, l'ADC utilizza il bilanciamento del carico basato su liste IP per ogni prima richiesta. Inserisce un cookie nelle intestazioni della prima risposta HTTP. Dopo di che, l'ADC usa il cookie del client per instradare il traffico allo stesso server back-end. Questo cookie viene utilizzato per la persistenza quando il client ha bisogno di andare allo stesso server back-end ogni volta. Il cookie scade una volta chiusa la sessione.
Cookie persistente Layer 7 Affinità/Persistenza della sessione	La modalità di bilanciamento del carico basata sull'elenco IP viene utilizzata per ogni prima richiesta. L'ADC inserisce un cookie nelle intestazioni della prima risposta HTTP. Dopo di che, l'ADC usa il cookie del client per instradare il traffico verso lo stesso server back-end. Questo cookie viene utilizzato per la persistenza quando il client deve andare ogni volta allo stesso server di back-end. Il cookie scade dopo 2 ore, e la connessione sarà bilanciata secondo un algoritmo IP List Based. Questo tempo di scadenza è configurabile usando un jetPACK.
Cookie di sessione - Classico cookie di sessione ASP	Active Server Pages (ASP) è una tecnologia Microsoft lato server. Con questa opzione selezionata, l'ADC manterrà la persistenza della sessione sullo stesso server se un cookie ASP viene rilevato e trovato nella sua lista di cookie conosciuti. Al rilevamento di un nuovo cookie ASP, sarà bilanciato il carico utilizzando l'algoritmo Least Connections.
Cookie di sessione - Cookie di sessione ASP.NET	Questa modalità si applica a **ASP.net.** Con questa modalità selezionata, l'ADC manterrà la persistenza della sessione sullo stesso server se un cookie ASP.NET viene rilevato e trovato nella sua lista di cookie conosciuti. Al rilevamento di un nuovo cookie ASP, sarà bilanciato il carico utilizzando l'algoritmo Least Connections.
Cookie di sessione - JSP Session Cookie	Java Server Pages (JSP) è una tecnologia Oracle lato server. Con questa modalità selezionata, l'ADC manterrà la persistenza della sessione sullo stesso server se un cookie JSP viene rilevato e trovato nella sua lista di cookie conosciuti. Al rilevamento di un nuovo cookie JSP, sarà bilanciato il carico utilizzando l'algoritmo Least Connections.
Cookie di sessione - Cookie di sessione JAX-WS	Java web services (JAX-WS) è una tecnologia Oracle lato server. Con questa modalità selezionata, l'ADC manterrà la persistenza della sessione allo stesso server se un cookie JAX-WS viene rilevato e trovato nella sua lista di cookie

	conosciuti. Al rilevamento di un nuovo cookie JAX-WS, il carico sarà bilanciato utilizzando l'algoritmo Least Connections.
Cookie di sessione - PHP Session Cookie	Personal Home Page (PHP) è una tecnologia open-source lato server. Con questa modalità selezionata, l'ADC manterrà la persistenza della sessione sullo stesso server quando viene rilevato un cookie PHP.
Cookie di sessione - persistenza del cookie RDP	Questo metodo di bilanciamento del carico utilizza il cookie RDP creato da Microsoft basato su nome utente/dominio per fornire persistenza a un server. Il vantaggio di questo metodo significa che è possibile mantenere una connessione a un server anche se l'indirizzo IP del client cambia.
Basato su cookie-ID	Un nuovo metodo molto simile a "PhpCookieBased" e ad altri metodi di bilanciamento del carico, ma usando CookieIDBased e cookie RegEx h=[^;]+ Questo metodo userà il valore impostato nel campo note del Real Server "ID=X;" come valore del cookie per identificare il server. Questo, quindi, significa che è una metodologia simile a CookieListBased ma usa un nome di cookie diverso e memorizza un valore di cookie unico, non l'IP criptato, ma l'ID del Real Server (letto al momento del caricamento). Il valore predefinito è CookieIDName="h"; tuttavia, se c'è un valore di override nella configurazione delle impostazioni avanzate del server virtuale, usa invece questo. **NOTA**: sovrascriviamo l'espressione del cookie di cui sopra per sostituire h= con il nuovo valore se questo valore è impostato. L'ultimo bit è che se arriva un valore di cookie sconosciuto e corrisponde a uno degli ID del server reale, dovrebbe selezionare quel server; altrimenti, usa il metodo successivo (delegare).
Lista IP condivisa basata su	Questo tipo di servizio è disponibile solo quando la modalità di connettività è impostata su Gateway o Direct Server Return. È stato aggiunto principalmente per il supporto al bilanciamento del carico VMware.

Monitoraggio del server

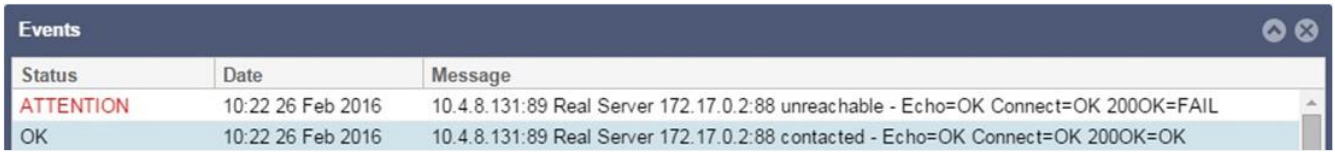
Il tuo ADC contiene sei metodi standard di monitoraggio di Real Server elencati di seguito.



Scegli il metodo di monitoraggio che vuoi applicare al servizio virtuale (VIP).

È essenziale scegliere il monitor giusto per il servizio. Per esempio, se il Real Server è un server RDP, un monitor 200OK non è rilevante. Se non sei sicuro di quale monitor scegliere, il default TCP Connection è un ottimo punto di partenza.

Puoi scegliere più monitor cliccando a turno su ogni monitor che vuoi applicare al servizio. I monitor selezionati vengono eseguiti nell'ordine in cui li hai selezionati; quindi inizia prima con i monitor dei livelli inferiori. Per esempio, impostando i monitor Ping/ICMP Echo, TCP Connection, e 200OK verranno visualizzati nel Dashboard Events come l'immagine sottostante:

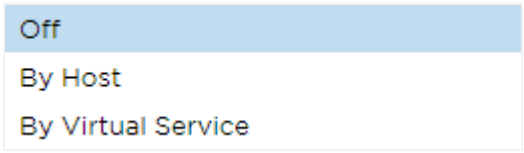


Possiamo vedere che il Layer 3 Ping e il Layer 4 TCP Connect sono riusciti se guardiamo la linea superiore, ma il Layer 7 200OK è fallito. Questi risultati di monitoraggio forniscono abbastanza informazioni per indicare che il routing è OK e che c'è un servizio in esecuzione sulla relativa porta, ma il sito web non risponde correttamente alla pagina richiesta. E' ora il momento di guardare il webserver e la sezione Library > Real Server Monitor per vedere i dettagli del monitoraggio che fallisce.

Opzione	**Descrizione**
Nessuno	In questa modalità, il Real Server non viene monitorato ed è sempre attivo e funzionante correttamente. L'impostazione None è utile per le situazioni in cui il monitoraggio sconvolge un server e per i servizi che non dovrebbero partecipare all'azione di fail-over dell'ADC. È un percorso per ospitare sistemi inaffidabili o legacy che non sono primari per le operazioni H/A. Utilizzare questo metodo di monitoraggio con qualsiasi tipo di servizio.
Eco Ping/ICMP	In questa modalità, l'ADC invia una richiesta ICMP echo all'IP del content server. Se viene ricevuta una risposta echo valida, l'ADC considera il Real Server attivo e funzionante, e il traffico verso il server continua. Inoltre manterrà il servizio disponibile su una coppia H/A. Questo metodo di monitoraggio è utilizzabile con qualsiasi tipo di servizio.
Connessione TCP	Una connessione TCP viene fatta al Real Server e immediatamente interrotta senza inviare alcun dato in questa modalità. Se la connessione riesce, l'ADC ritiene che il Real Server sia attivo e funzionante. Questo metodo di monitoraggio è utilizzabile con qualsiasi tipo di servizio, e i servizi UDP non sono attualmente appropriati per il monitoraggio della connessione TCP.
ICMP irraggiungibile	L'ADC invierà un controllo di salute UDP al server e contrassegnerà il Real Server come non disponibile se riceve un messaggio ICMP port unreachable. Questo metodo può essere utile quando è necessario controllare se una porta di servizio UDP è disponibile su un server, come la porta DNS 53.
RDP	In questa modalità, una connessione TCP si inizializza come spiegato nel metodo ICMP Unreachable. Dopo l'inizializzazione della connessione, viene richiesta una connessione RDP Layer 7. Se il collegamento viene confermato, l'ADC ritiene che il Real Server sia attivo e funzionante. Questo metodo di monitoraggio è utilizzabile con qualsiasi terminal server Microsoft.
200 OK	In questo metodo, una connessione TCP si inizializza al Real Server. Dopo che la connessione ha successo, l'ADC invia al Real Server una richiesta HTTP. Si attende una risposta HTTP e si controlla il codice di risposta "200 OK". L'ADC considera il Real Server attivo e funzionante se viene ricevuto il codice di risposta "200 OK". Se l'ADC non riceve un codice di risposta "200 OK" per qualsiasi motivo, inclusi timeout, mancata connessione e altri motivi, l'ADC segna il Real Server non disponibile. Questo metodo di monitoraggio è valido solo per l'uso con i tipi di servizio HTTP e HTTP accelerato. Se un tipo di servizio Layer 4 viene utilizzato per un server HTTP, è utilizzabile se SSL non è in uso sul Real Server o gestito in modo appropriato dalla funzione "Content SSL".
DICOM	Una connessione TCP si inizializza al Real Server in modalità DICOM, e una "Associate Request" di Echoscu viene fatta al Real Server sulla connessione. Una conversazione che include un "Associate Accept" dal content server, un trasferimento di una piccola quantità di dati seguito da un "Release Request", poi "Release Response" conclude con successo il monitor. Se il monitor non si conclude con successo, allora il Real Server è considerato inattivo per qualsiasi motivo.
Definito dall'utente	Qualsiasi monitor configurato nella sezione Monitoraggio del server reale apparirà nell'elenco.

Strategia di caching

Per impostazione predefinita, la strategia di caching è disabilitata e impostata come Off. Se il tuo tipo di servizio è HTTP, allora puoi applicare due tipi di strategia di caching.



Fai riferimento alla pagina Configure Cache per configurare le impostazioni dettagliate della cache. Nota che quando la cache è applicata ad un VIP con il tipo di servizio "HTTP" accelerato, gli oggetti compressi non vengono memorizzati nella cache.

Opzione	**Descrizione**
Per ospite	La cache per host è basata sull'applicazione per hostname. Una cache separata esisterà per ogni dominio/nome di host. Questa modalità è ideale per i server web che possono servire più siti web a seconda del dominio.
Per servizio virtuale	La cache per servizio virtuale è disponibile quando si sceglie questa opzione. Solo una cache esisterà per tutti i domini/nomi di host che passano attraverso il servizio virtuale. Questa opzione è un'impostazione specialistica per l'uso con più cloni di un singolo sito.

Accelerazione

Opzione	**Descrizione**
Off	Disattivare la compressione per il servizio virtuale
Compressione	Quando è selezionata, questa opzione attiva la compressione per il servizio virtuale selezionato. L'ADC comprime dinamicamente il flusso di dati al client su richiesta. Questo processo si applica solo agli oggetti che contengono l'intestazione content-encoding: gzip. Un esempio di contenuto include HTML, CSS o Javascript. Puoi anche escludere certi tipi di contenuto usando la sezione Global Exclusions.

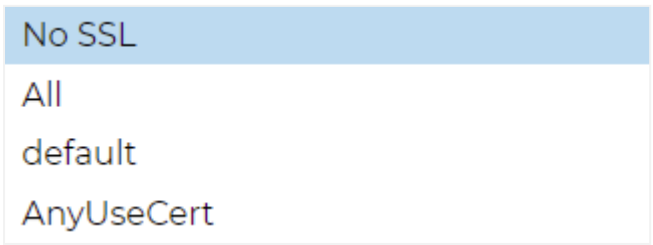
Nota: se l'oggetto è cacheable, l'ADC memorizza una versione compressa e la serve staticamente (dalla memoria) finché il contenuto non scade e viene riconvalidato.

Certificato SSL del servizio virtuale (crittografia tra il client e l'ADC)

Per impostazione predefinita, l'impostazione è No SSL. Se il tuo tipo di servizio è "HTTP" o "Layer4 TCP", puoi selezionare un certificato dal menu a tendina da applicare al servizio virtuale. I certificati che sono stati creati o importati appariranno in questa lista. Puoi evidenziare più certificati da applicare a un servizio. Questa operazione abiliterà automaticamente l'estensione SNI per consentire un certificato basato sul "Domain Name" richiesto dal client.

Indicazione del nome del server

Questa opzione è un'estensione del protocollo di rete TLS con cui il client indica a quale hostname sta tentando di connettersi all'inizio del processo di handshaking. Questa impostazione permette all'ADC di presentare più certificati sullo stesso indirizzo IP virtuale e porta TCP.



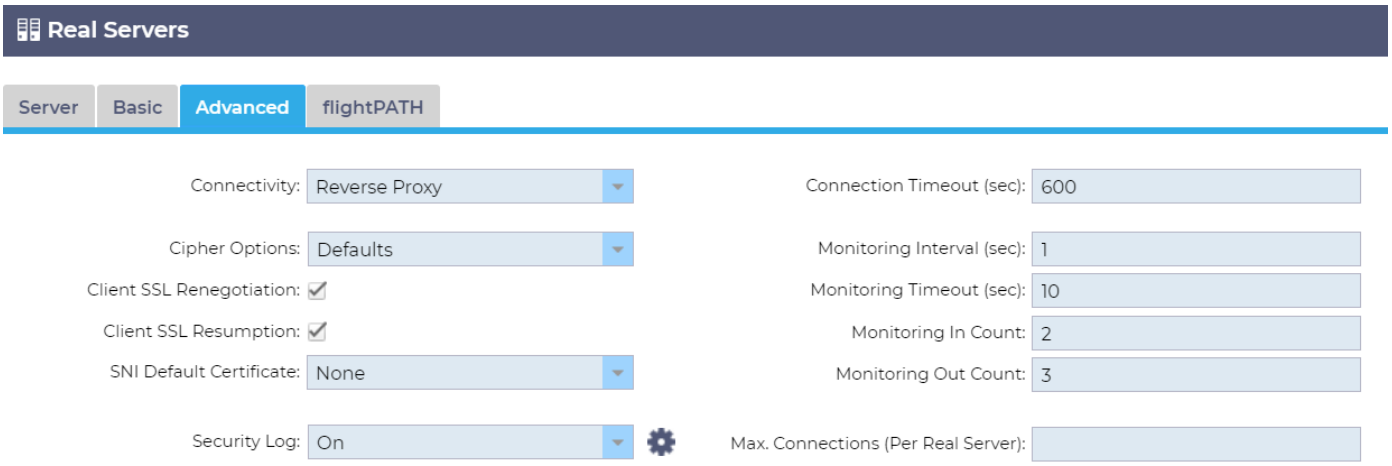
Opzione	**Descrizione**
No SSL	Il traffico dalla sorgente all'ADC non è criptato.
Tutti	Carica tutti i certificati disponibili per l'uso
Default	Questa opzione ha come risultato l'applicazione di un certificato creato localmente chiamato "Default" al lato del browser del canale. Usa questa opzione per testare SSL quando non ne è stato creato o importato uno.
AnyUseCert	Utilizzare qualsiasi certificato presente sull'ADC che l'utente ha caricato o generato

Certificato SSL del server reale (crittografia tra l'ADC e il server reale)

L'impostazione predefinita per questa opzione è No SSL. Se il tuo server richiede una connessione criptata, questo valore deve essere diverso da No SSL. I certificati che sono stati creati o importati appariranno in questa lista.

Opzione	**Descrizione**
No SSL	Il traffico dall'ADC al Real Server non è criptato. La selezione di un certificato sul lato del browser significa che "No SSL" può essere scelto lato client per fornire ciò che è noto come "SSL Offload".
Qualsiasi	L'ADC agisce come un client e accetta qualsiasi certificato presentato dal Real Server. Il traffico dall'ADC al Real Server è criptato quando questa opzione è selezionata. Usa l'opzione "Any" quando un certificato è specificato sul lato del servizio virtuale, fornendo ciò che è noto come "SSL Bridging" o "SSL Re-Encryption".
SNI	L'ADC agisce come un client e accetterà qualsiasi certificato presentato dal Real Server. Il traffico dall'ADC al Real Server è criptato se questo è selezionato. Usa l'opzione "Any" quando un certificato è specificato sul lato Virtual Service, fornendo ciò che è noto come "SSL Bridging" o "SSL Re-Encryption". Scegliete questa opzione per abilitare SNI sul lato server.
AnyUseCert	Tutti i certificati che hai generato o importato nell'ADC appaiono qui.

Avanzato



Connettività

Il vostro servizio virtuale è configurabile con diversi tipi di connettività. Selezioni la modalità di connettività da applicare al servizio.

Opzione	**Descrizione**
Proxy inverso	Reverse Proxy è il valore predefinito e funziona a Layer7 con compressione e caching. E a Layer4 senza caching o compressione. In questa modalità, il tuo ADC agisce come un reverse proxy e diventa l'indirizzo sorgente visto dai Real Server.
Ritorno diretto al server	Direct Server Return o DSR come è ampiamente conosciuto (DR - Direct Routing in alcuni circoli) permette al server dietro il bilanciatore di carico di rispondere direttamente al client bypassando l'ADC sulla risposta. DSR è adatto solo per l'uso con il bilanciamento del carico a livello 4. Pertanto, il caching e la compressione non sono disponibili con questa opzione scelta. **Questa modalità può essere usata solo con i tipi di servizio TCP, UDP e TCP/UDP.** Il bilanciamento del carico al livello 7 non funziona con questo DSR. Inoltre, non c'è alcun supporto di persistenza diverso dall'IP List Based. Il bilanciamento del carico SSL/TLS con questo metodo non è ideale in quanto il supporto di persistenza Source IP è l'unico tipo disponibile. Il DSR richiede anche modifiche al Real Server per essere fatto. Si prega di fare riferimento alla sezione Modifiche al server reale.
Gateway	La modalità gateway consente di instradare tutto il traffico attraverso l'ADC, permettendo ai Real Server di essere indirizzati attraverso l'ADC ad altre reti tramite le macchine virtuali ADC o le interfacce hardware. L'utilizzo del dispositivo come dispositivo gateway per i Real Server è ideale quando si esegue in modalità multi-interfaccia. Il bilanciamento del carico al livello 7 con questo metodo non funziona in quanto non c'è alcun supporto di persistenza oltre a quello basato sull'elenco IP. Questo metodo richiede che il Real Server imposti il suo gateway predefinito all'indirizzo dell'interfaccia locale dell'ADC (eth0, eth1, ecc.). Fai riferimento alla sezione Modifiche del Real Server. ***Si prega di notare che la modalità Gateway non supporta il failover in un ambiente cluster.***

Opzioni di cifratura

È possibile impostare i cifrari a livello di servizio, ed è rilevante solo per i servizi con SSL/TLS abilitato. L'ADC esegue la scelta automatica del cifrario, ed è possibile aggiungere diversi cifrari usando i jetPACK. Aggiungendo il jetPACK appropriato, è possibile impostare le opzioni Cipher per servizio. Il vantaggio di questo è che puoi creare diversi servizi con diversi livelli di sicurezza. Siate consapevoli che i client più vecchi non sono compatibili con i cifrari più recenti, e per ridurre il numero di client, più sicuro è il servizio.

Rinegoziazione SSL del client

Spuntate questa casella se volete permettere la rinegoziazione SSL avviata dal client. Disabilita la rinegoziazione SSL del client per prevenire eventuali attacchi DDOS contro il livello SSL, deselezionando questa opzione.

Ripresa SSL del client

Spuntare questa casella se si desidera abilitare le sessioni del server di ripresa SSL aggiunte alla cache della sessione. Quando un client propone il riutilizzo di una sessione, il server cercherà di riutilizzare la sessione se trovata. Se la casella Resumption è deselezionata, non ha luogo alcun caching di sessione per il client o il server.

Certificato predefinito SNI

Durante una connessione SSL con l'SNI lato client abilitato, se il dominio richiesto non corrisponde a nessuno dei certificati assegnati al servizio, l'ADC presenterà il certificato SNI Default. L'impostazione predefinita per questo è None, che in effetti farebbe cadere la connessione se non ci fosse una corrispondenza esatta. Scegliere uno qualsiasi dei certificati installati dal menu a tendina da presentare nel caso in cui una corrispondenza esatta del certificato SSL fallisca.

Registro di sicurezza

'On' è il valore predefinito ed è su base per servizio, abilitando il servizio di registrazione delle informazioni di autenticazione nei log del W3C. Facendo clic sull'icona Cog si accede alla pagina System > Logging, dove è possibile controllare le impostazioni del log W3C.

Timeout della connessione

Il timeout predefinito della connessione è di 600 secondi o 10 minuti. Questa impostazione regolerà il tempo di timeout della connessione quando non c'è attività. Riducetelo per il traffico web senza stato di breve durata, che in genere è di 90s o meno. Aumentate questa cifra per le connessioni statiche come RDP a qualcosa come 7200 secondi (2 ore) o più, a seconda della vostra infrastruttura. L'esempio del timeout RDP significa che se un utente ha un periodo di inattività di 2 ore o meno, le connessioni rimarranno aperte.

Impostazioni di monitoraggio

Queste impostazioni si riferiscono ai Real Server Monitors nella scheda Basic. Ci sono voci globali nella configurazione per contare il numero di monitor riusciti o falliti prima che lo stato di un server sia segnato online o fallito.

Intervallo

L'intervallo è il tempo in secondi tra i monitor. L'intervallo predefinito è di 1 secondo. Mentre 1s è accettabile per la maggior parte delle applicazioni, può essere utile aumentarlo per altre o durante i test.

Timeout di monitoraggio

Il valore di timeout è quando l'ADC aspetterà che un server risponda a una richiesta di connessione. Il valore predefinito è 2s. Aumentate questo valore per i server occupati.

Monitoraggio nel conteggio

Il valore predefinito per questa impostazione è 2. Il valore di 2 indica che il Real Server deve passare due controlli dello stato di salute con successo prima di essere online. Aumentando questo valore aumenterà la probabilità che il server possa servire il traffico ma ci vorrà più tempo per entrare in servizio a seconda dell'intervallo. Diminuendo questo valore il server entrerà in servizio prima.

Monitoraggio del conteggio delle uscite

Il valore predefinito per questa impostazione è 3, il che significa che il monitor Real Server deve fallire tre volte prima che l'ADC smetta di inviare il traffico al server, ed esso venga contrassegnato come ROSSO e irraggiungibile. Aumentando questo valore si otterrà un servizio migliore e più affidabile a scapito del tempo che impiega l'ADC a smettere di inviare traffico a questo server.

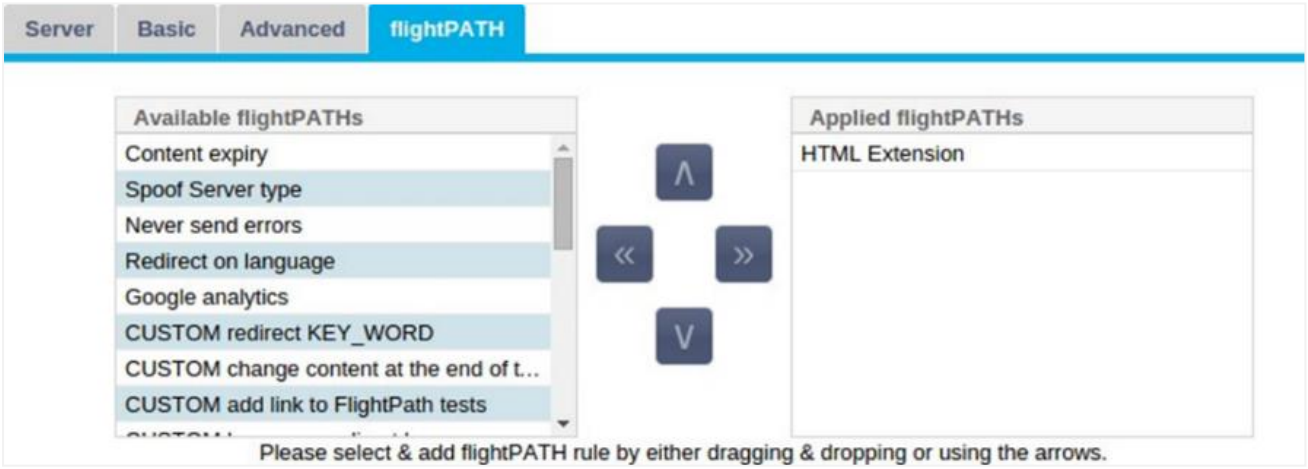
Passa a Offline in caso di guasto

Quando questo è selezionato, i Real Server che falliscono il loro controllo di salute sono messi offline e possono essere messi online solo manualmente.

Max. Connessioni

Limita il numero di connessioni simultanee del Real Server ed è impostato per servizio. Per esempio, se lo configuri a 1000 e hai due Real Server, l'ADC limita **ogni** Real Server a 1000 connessioni simultanee. Puoi anche scegliere di presentare una pagina "Server troppo occupato" una volta raggiunto questo limite su tutti i server, aiutando gli utenti a capire perché si è verificata una mancata risposta o un ritardo. Lascia questo campo vuoto per connessioni illimitate. Quello che imposti qui dipende dalle risorse del tuo sistema.

flightPATH



flightPATH è un sistema progettato da Edgenexus e disponibile esclusivamente all'interno dell'ADC. A differenza dei motori basati su regole di altri fornitori, flightPATH non opera attraverso una linea di comando o una console di inserimento di script. Invece, utilizza una GUI per selezionare i diversi parametri, condizioni e azioni da eseguire per ottenere ciò di cui hanno bisogno. Queste caratteristiche rendono flightPATH estremamente potente e permettono agli amministratori di rete di manipolare il traffico HTTPS in modi molto efficaci.

flightPATH è disponibile solo per l'uso con connessioni HTTPS, e questa sezione non è visibile quando il tipo di servizio virtuale non è HTTP.

Si può vedere dall'immagine qui sopra; c'è una lista di regole disponibili sulla sinistra e le regole applicate al servizio virtuale sulla destra.

Aggiungi una regola disponibile trascinandola dal lato sinistro a quello destro o evidenziando una regola e cliccando sulla freccia destra per spostarla sul lato destro.

L'ordine di esecuzione è essenziale e inizia con la regola superiore eseguita per prima. Per cambiare l'ordine di esecuzione, evidenziare la regola e spostarsi su e giù usando le frecce.

Per rimuovere una regola, trascinala di nuovo nell'inventario delle regole sulla sinistra o evidenzia la regola e clicca sulla freccia a sinistra.

Puoi aggiungere, rimuovere e modificare le regole di flightPATH nella sezione Configurare flightPATH di questa guida.

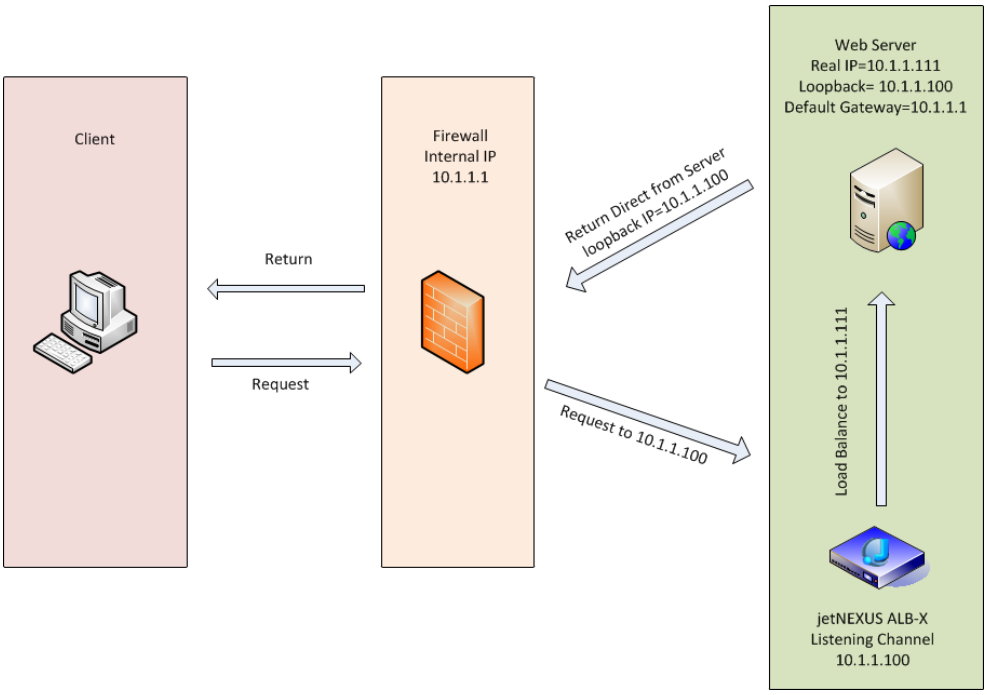
Modifiche al server reale per il ritorno del server diretto

Direct Server Return o DSR come è ampiamente conosciuto (DR - Direct Routing in alcuni circoli) permette al server dietro l'ADC di rispondere direttamente al client, bypassando l'ADC sulla risposta. DSR è adatto solo per l'uso con il bilanciamento del carico al livello 4. Caching e compressione non sono disponibili quando sono abilitati.

Il bilanciamento del carico al livello 7 con questo metodo non funzionerà perché non c'è supporto di persistenza oltre all'IP di origine. Il bilanciamento del carico SSL/TLS con questo metodo non è ideale in quanto c'è solo il supporto della persistenza dell'IP di origine.

Come funziona

- Il cliente invia una richiesta al jetNEXUS ALB-X
- Richiesta ricevuta da edgeNEXUS
- Richiesta inoltrata ai server di contenuto
- Risposta inviata direttamente al cliente senza passare attraverso edgeNEXUS



Configurazione richiesta del server dei contenuti

Generale

- Il gateway predefinito del content server deve essere configurato normalmente. (Non tramite l'ADC)
- Il content server e il load balancer devono trovarsi nella stessa subnet

Windows

- Il content server deve avere un loopback o un Alias configurato con l' indirizzo IP del canale o del VIP
  - La metrica di rete deve essere 254 per impedire la risposta alle richieste ARP
  - Aggiungere un adattatore di loopback in Windows Server 2012 - Clicca qui
  - Aggiungere un adattatore di loopback in Windows Server 2003/2008 - Clicca qui
- Esegui quanto segue in un prompt dei comandi per ogni interfaccia di rete che hai configurato sui Windows Real Server

netsh interface ipv4 set interface "nome interfaccia di rete Windows" 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

- Aggiungere un'interfaccia di loopback permanente
- Modifica "/etc/sysconfig/network-scripts"

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

- Modificare "/etc/sysctl.conf"

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

- Eseguire "sysctl - p"

Modifiche al server reale - Modalità gateway

La modalità gateway permette di instradare tutto il traffico attraverso l'ADC, e questo permette al traffico proveniente dai content server di essere instradato attraverso l'ADC verso altre reti tramite le interfacce sull'unità ADC. L'uso dell'apparecchio come dispositivo gateway per i server di contenuti dovrebbe essere usato quando funziona in modalità multi-interfaccia.

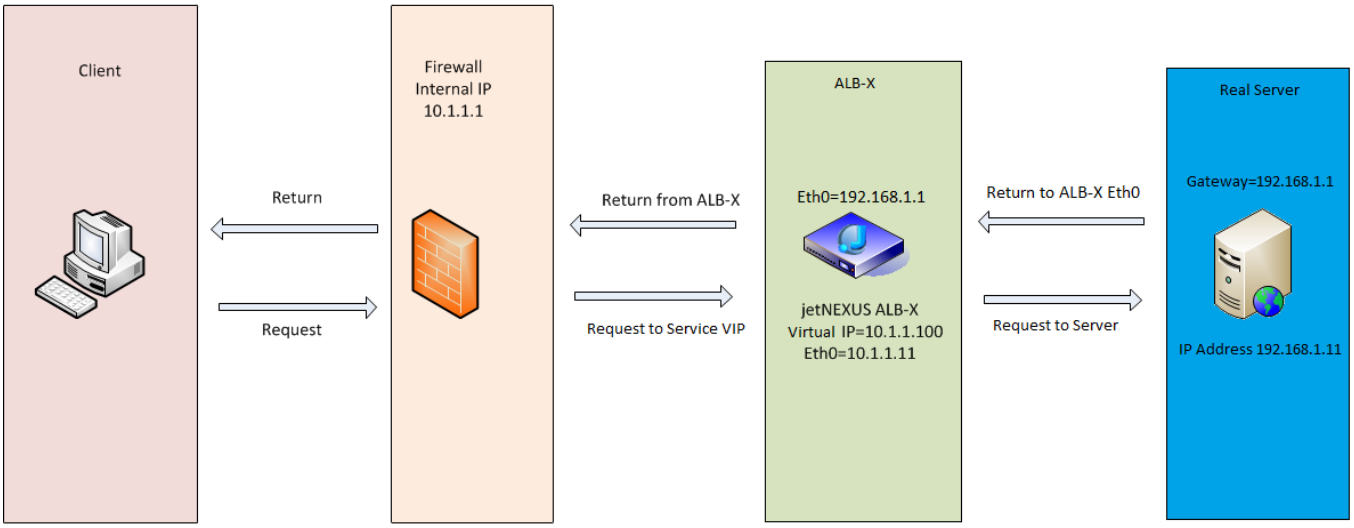
Come funziona

- Il cliente invia una richiesta al jetNEXUS ALB-X
- Una richiesta viene ricevuta da edgeNEXUS
- Richiesta inviata ai server di contenuto
- Risposta inviata a edgeNEXUS
- ADC instrada la risposta al cliente

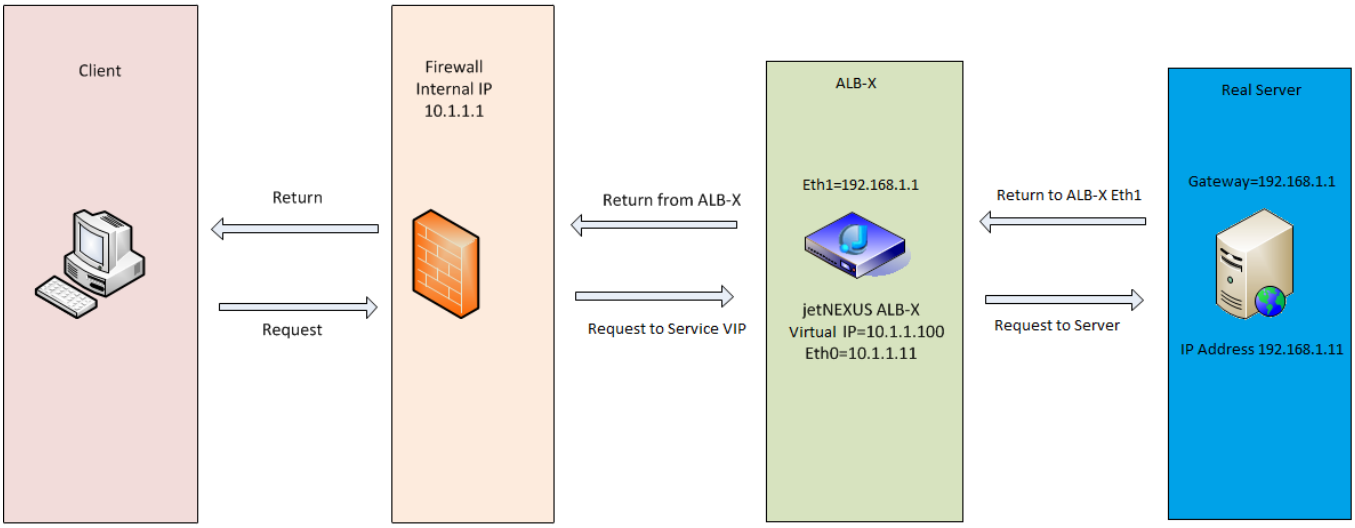
Configurazione richiesta del server dei contenuti

- Modalità Single Arm - viene utilizzata un'interfaccia, ma il servizio VIP e i Real Server devono essere su sottoreti diverse.
- Dual Arm Mode - due interfacce sono utilizzate, ma il servizio VIP e i server reali devono essere su sottoreti diverse.
- In ogni caso, Single e Dual Arm, i Real Server devono configurare il loro default gateway all'indirizzo dell'interfaccia ADC sulla relativa subnet.

Esempio di braccio singolo



Esempio di braccio doppio



Biblioteca

Add-Ons

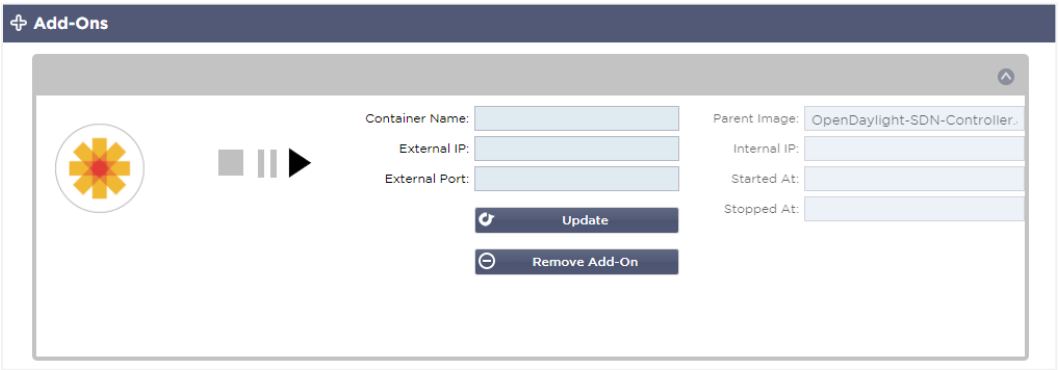
Gli add-on sono contenitori basati su Docker che possono essere eseguiti in una modalità isolata all'interno dell'ADC. Esempi di componenti aggiuntivi potrebbero essere un firewall applicativo o anche una micro istanza dell'ADC stesso.

Applicazioni

La sezione Apps all'interno di Add-Ons dettaglia le Apps che hai acquistato, scaricato e distribuito.

Se non ci sono App presenti, questa sezione mostrerà un messaggio che ti inviterà a procedere alla sezione App e a scaricare e distribuire un'App.

Una volta che hai distribuito un'app, questa apparirà nell'area delle app.



Acquisto di un componente aggiuntivo

Per acquistare un'App, è necessario registrarsi all'App Store. L'acquisto viene effettuato tramite l'ADC stesso. Troverai

Vai alla pagina Library > Apps della dashboard di ADC.

Qui puoi selezionare l'App che vuoi scaricare e poi installare.

Se lo stai facendo dalla dashboard ADC, seleziona solo 1 elemento. È possibile possedere più set ADC e le applicazioni devono essere associate all'ADC su cui vengono distribuite.

Se si accede all'App Store tramite il desktop e il browser, si possono scaricare tutte quelle che si desiderano. Per esempio, quattro istanze di WAF o GSLB. Appariranno nell'area Purchased Apps del tuo ADC in modo che tu possa scaricarle.

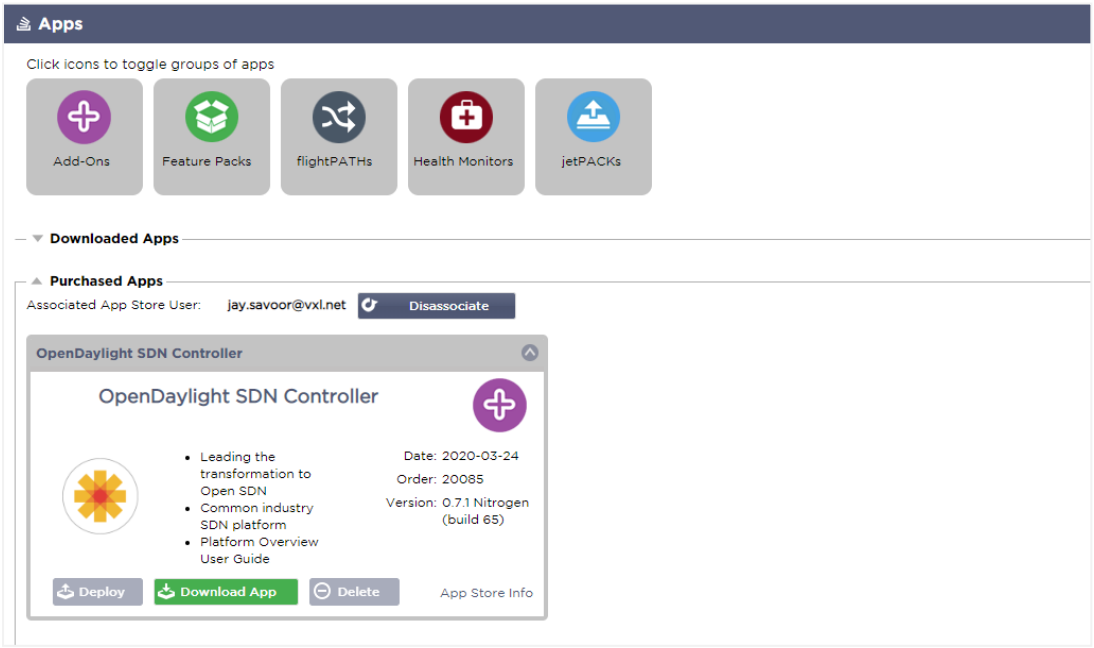
Le App si associano agli ADC che possiedi e che hai registrato.

Quando scegliete di scaricare un'App, vi verrà chiesto l'ID della macchina, dopo di che l'App viene criptata e collegata all'ID della macchina ADC.

I link all'App Store sono:

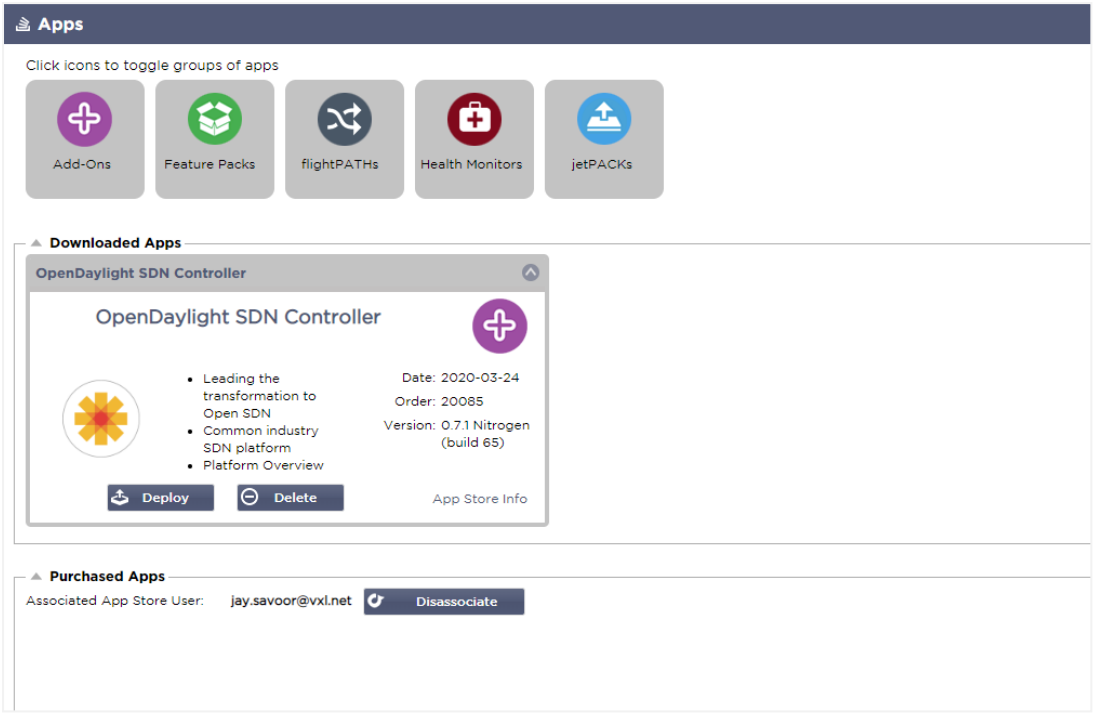
- Componenti aggiuntivi: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/ADD-ON/**
- Monitoraggio della salute: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/SERVER-HEALTH-MONITORS/**
- jetPACKS: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/JETPACKS/**
- Pacchetti di caratteristiche: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/EDGENEXUS-FEATURE-PACK/**
- regole di flightPATH: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/FLIGHTPATH/**

- Aggiornamenti software: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/EDGENEXUS-SOFTWARE-UPDATE/**



Distribuire un'applicazione

Una volta scaricata sull'ADC, l'applicazione sarà spostata nella sezione Downloaded Apps e distribuita sull'ADC usando il pulsante Deploy. Questo processo richiede un po' di tempo a seconda delle risorse disponibili per l'ADC. Una volta distribuita, apparirà nella sezione Downloaded Apps.



Autenticazione

La pagina Library > Authentication ti permette di impostare i server di autenticazione e creare regole di autenticazione con opzioni per il lato client Basic o Forms e il lato server NTLM o BASIC.

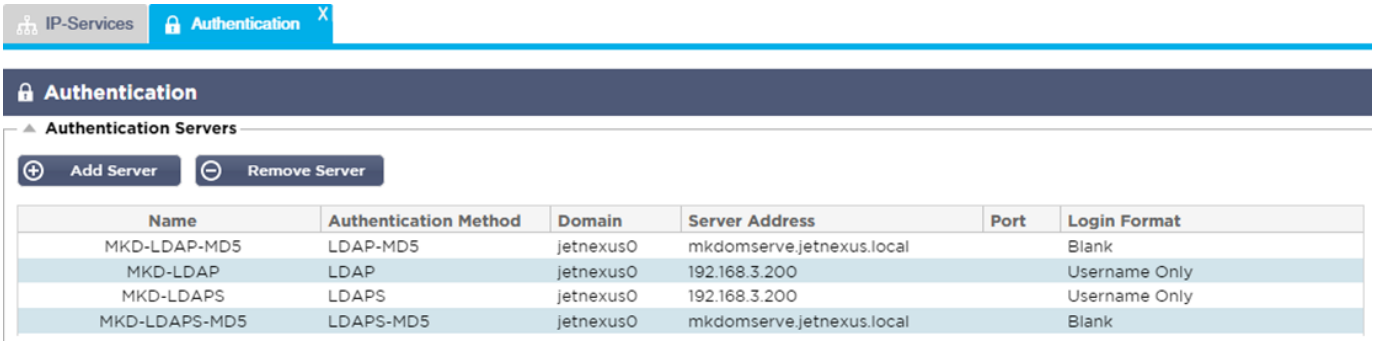
Impostare l'autenticazione - un flusso di lavoro

Per favore, esegui i seguenti passi come minimo per applicare l'autenticazione al tuo servizio.

1. Creare un server di autenticazione.
2. Crea una regola di autenticazione che utilizza un server di autenticazione.
3. Crea una regola flightPATH che utilizza una regola di autenticazione.
4. Applicare la regola flightPATH a un servizio

Server di autenticazione

Per impostare un metodo di autenticazione funzionante, dobbiamo prima impostare un server di autenticazione.



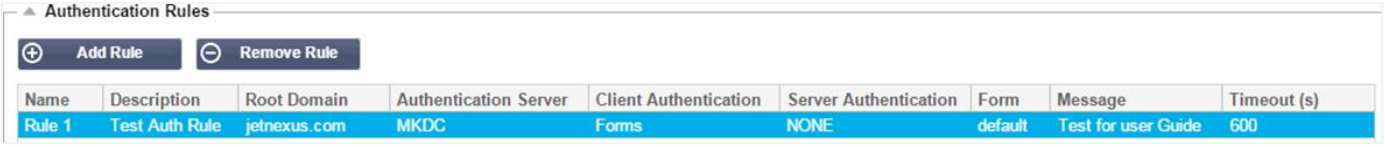
- Fare clic sul pulsante Add Server.
- Questa azione produrrà una riga vuota pronta per il completamento.

Opzione	Descrizione
Nome	Dai un nome al tuo server per l'identificazione - questo nome è usato nelle regole
Descrizione	Aggiungere una descrizione
Metodo di autenticazione	Scegliere un metodo di autenticazione LDAP - LDAP di base con nomi utente e password inviati in chiaro al server LDAP. LDAP-MD5 - LDAP di base con nome utente in chiaro e password con hash MD5 per una maggiore sicurezza. LDAPS - LDAP su SSL. Invia la password in chiaro all'interno di un tunnel criptato tra l'ADC e il server LDAP. LDAPS-MD5 - LDAP su SSL. La password è sottoposta a hash MD5 per una maggiore sicurezza all'interno di un tunnel crittografato tra l'ADC e il server LDAP.
Dominio	Aggiungi il nome del dominio per il server LDAP.
Indirizzo del server	Aggiungere l'indirizzo IP o il nome host del server di autenticazione LDAP - Indirizzo IPv4 o nome host. LDAP-MD5 - solo hostname (l'indirizzo IPv4 non funziona) LDAPS - Indirizzo IPv4 o nome host. LDAPS-MD5 - solo hostname (l'indirizzo IPv4 non funziona).
Porto	Usa la porta 389 per LDAP e la porta 636 per LDAPS per impostazione predefinita. Non è necessario aggiungere il numero di porta per LDAP e LDAPS. Quando saranno disponibili altri metodi, potrai configurarli qui
Condizioni di ricerca	Le condizioni di ricerca devono essere conformi a RFC 4515. Esempio: (MemberOf=CN=Phone- VPN,CN=Users,DC=mycompany,DC=local).
Base di ricerca	Questo valore è il punto di partenza per la ricerca nel database LDAP. Esempio *dc=mycompany,dc=local*
Formato di accesso	Usa il formato di login che ti serve. Nome utente - con questo formato scelto, è necessario inserire solo il nome utente. Qualsiasi informazione su utente e dominio inserita dall'utente viene cancellata, e vengono usate le informazioni sul dominio dal server. Nome utente e dominio - L'utente deve inserire l'intero dominio e la sintassi del nome utente. Esempio: *mycompany\gchristie OR someone@mycompany*. Le informazioni sul dominio inserite a livello di server vengono ignorate. Blank - l'ADC accetterà qualsiasi cosa l'utente inserisca e la invierà al server di autenticazione. Questa opzione è usata quando si usa MD5.

Passphrase	Questa opzione non è usata in questa versione.
Tempo morto	Non utilizzato in questa versione

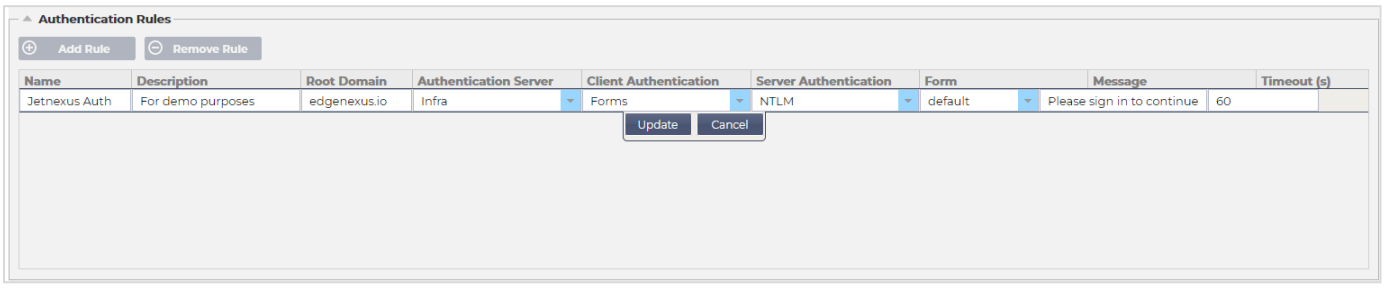
Regole di autenticazione

La fase successiva è quella di creare le regole di autenticazione da usare con la definizione del server.



Campo	Descrizione
Nome	Aggiungi un nome adatto alla tua regola di autenticazione.
Descrizione	Aggiungere una descrizione adeguata.
Dominio radice	Questo deve essere lasciato vuoto a meno che non sia necessario il single-sign-on tra i sottodomini.
Server di autenticazione	Questa è una casella a discesa che contiene i server che hai configurato.
Autenticazione del cliente:	Scegliete il valore adatto alle vostre esigenze: Basic (401) - Questo metodo usa il metodo di autenticazione standard 401 Forme - questo presenterà all'utente il modulo predefinito di ADC. All'interno del modulo, puoi aggiungere un messaggio. Puoi selezionare un modulo che hai caricato usando la sezione sottostante.
Autenticazione del server	Scegliere il valore appropriato. None - se il tuo server non ha alcuna autenticazione esistente, seleziona questa impostazione. Questa impostazione significa che puoi aggiungere capacità di autenticazione a un server che prima non ne aveva nessuna. Basic - se il tuo server ha l'autenticazione di base (401) abilitata, allora seleziona BASIC. NTLM - se il tuo server ha l'autenticazione NTLM abilitata, allora seleziona NTLM.
Modulo	Scegliere il valore appropriato Default - Selezionando questa opzione l'ADC userà il suo modulo integrato. Personalizzato - puoi aggiungere un modulo che hai progettato tu e selezionarlo qui.
Messaggio	Aggiungi un messaggio personale al modulo.
Timeout	Aggiungi un timeout alla regola, dopo il quale l'utente dovrà autenticarsi di nuovo. Nota che l'impostazione del timeout è valida solo per l'autenticazione basata sui moduli.

Singolo accesso



Se vuoi fornire un single sign-on per gli utenti, completa la colonna Root Domain con il tuo dominio. In questo esempio, abbiamo usato edgenexus.io. Ora possiamo avere più servizi che useranno edgenexus.io come dominio principale, e l'utente dovrà accedere solo una volta. Se consideriamo i seguenti servizi:

- Sharepoint.mycompany.com

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

Questi servizi possono risiedere su un VIP o possono essere distribuiti su 3 VIP. Un utente che accede a usercentral. mycompany.com per la prima volta sarà presentato con un modulo che gli chiederà di accedere a seconda della regola di autenticazione utilizzata. Lo stesso utente può poi connettersi a appstore. mycompany.com e sarà autenticato automaticamente dall'ADC. È possibile impostare il timeout, che forzerà l'autenticazione una volta raggiunto questo periodo di inattività.

Moduli

Questa sezione ti permetterà di caricare un modulo personalizzato.

Come creare il tuo modulo personalizzato

Anche se il modulo di base che l'ADC fornisce è sufficiente per la maggior parte degli scopi, ci saranno occasioni in cui le aziende desiderano presentare la propria identità all'utente. Puoi creare il tuo modulo personalizzato che gli utenti dovranno compilare in questi casi. Questo modulo deve essere in formato HTM o HTML.

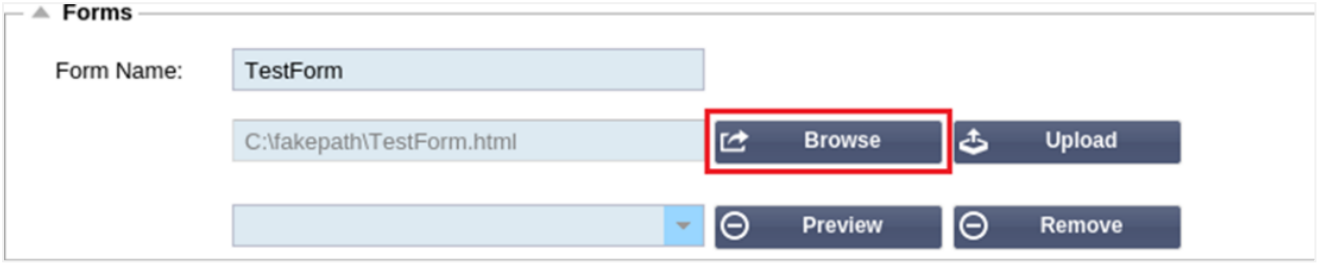
Opzione	Descrizione
Nome	nome del modulo = loginform azione = %JNURL% Metodo = POST
Nome utente	Sintassi: nome = "JNUSER"
Password:	nome="JNPASS"
Messaggio opzionale1:	%JNMESSAGE%
Messaggio opzionale2:	%JNAUTHMESSAGE%
Immagini	Se vuoi aggiungere un'immagine, aggiungila in linea usando la codifica Base64.

Esempio di codice html di un modulo molto semplice e basilare

```
<HTML>
<HEAD>
<TITOLO>ESEMPIO DI MODULO DI AUTORIZZAZIONE</TITOLO>
</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>
```

Aggiungere un modulo personalizzato

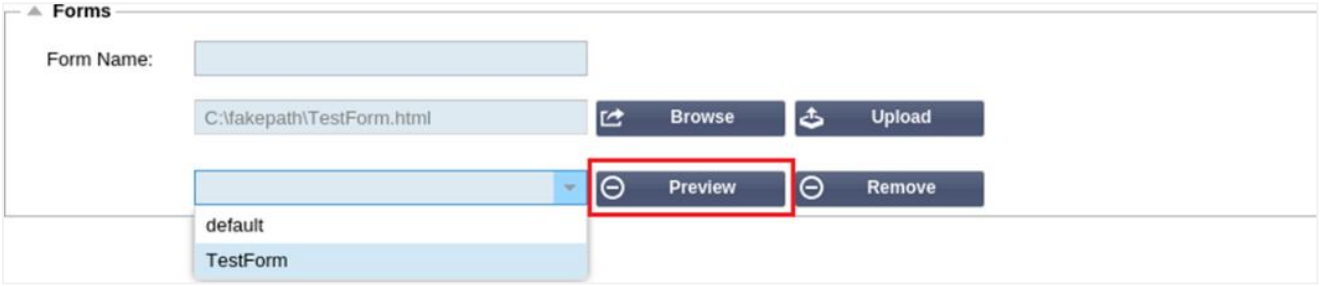
Una volta creato un modulo personalizzato, puoi aggiungerlo usando la sezione Forme.



1. Scegli un nome per il tuo modulo
2. Cerca localmente il tuo modulo
3. Fare clic su Carica

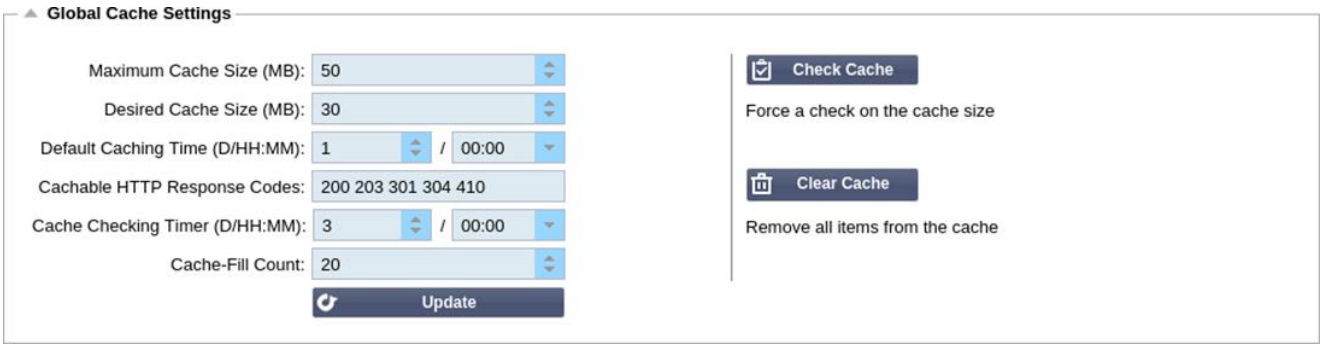
Anteprima del modulo personalizzato

Per visualizzare il modulo personalizzato che hai appena caricato, lo selezioni e clicchi su Anteprima. Puoi anche usare questa sezione per cancellare i moduli che non sono più necessari.



Cache

L'ADC è in grado di memorizzare i dati nella sua memoria interna e periodicamente lava questa cache nella memoria interna dell'ADC. Le impostazioni che gestiscono questa funzionalità sono fornite in questa sezione.



Impostazioni globali della cache

Dimensione massima della cache (MB)

Questo valore determina la RAM massima che la cache può consumare. La cache ADC è una cache in-memory che viene anche periodicamente scaricata sul supporto di memorizzazione per mantenere la persistenza della cache dopo i riavvii, i riavvii e le operazioni di spegnimento. Questa funzionalità significa che la dimensione massima della cache deve rientrare nell'ingombro della memoria dell'apparecchio (piuttosto che nello spazio su disco) e non dovrebbe essere superiore alla metà della memoria disponibile.

Dimensione desiderata della cache (MB)

Questo valore denota la RAM ottimale a cui la Cache sarà tagliata. Mentre la dimensione massima della cache rappresenta il limite superiore assoluto della cache, la dimensione desiderata della cache è intesa come la dimensione ottimale che la cache dovrebbe cercare di raggiungere ogni volta che viene effettuato un controllo automatico o manuale della dimensione della cache. Il divario tra la dimensione massima e quella desiderata della cache esiste per ospitare l'arrivo e la sovrapposizione di nuovi contenuti tra i controlli periodici della dimensione della cache per tagliare i contenuti scaduti. Ancora una volta, può essere più efficace accettare il valore predefinito (30 MB) e rivedere periodicamente la dimensione della cache sotto "Monitor -> Statistiche" per un dimensionamento appropriato.

Tempo di cache predefinito (D/HH:MM)

Il valore inserito qui rappresenta la durata del contenuto senza un valore di scadenza esplicito. Il tempo di caching predefinito è il periodo per il quale il contenuto senza una direttiva "no-store" o un tempo di scadenza esplicito nell'intestazione del traffico viene memorizzato.

L'inserimento del campo ha la forma "D/HH:MM" - così un inserimento di "1/01:01" (il default è 1/00:00) significa che l'ADC terrà il contenuto per un giorno, "01:00" per un'ora, e "00:01" per un minuto.

Codici di risposta HTTP memorizzabili

Uno degli insiemi di dati nella cache sono le risposte HTTP. I codici di risposta HTTP che sono nella cache sono:

- 200 - Risposta standard per richieste HTTP riuscite
- 203 - Le intestazioni non sono definitive ma sono raccolte da una copia locale o da una terza parte
- 301 - Alla risorsa richiesta è stato assegnato un nuovo URL permanente
- 304 - Non modificato dall'ultima richiesta e la copia nella cache locale dovrebbe essere usata al suo posto
- 410 - La risorsa non è più disponibile sul server e nessun indirizzo di inoltro è noto

Questo campo dovrebbe essere modificato con cautela poiché i codici di risposta cacheable più comuni sono già elencati.

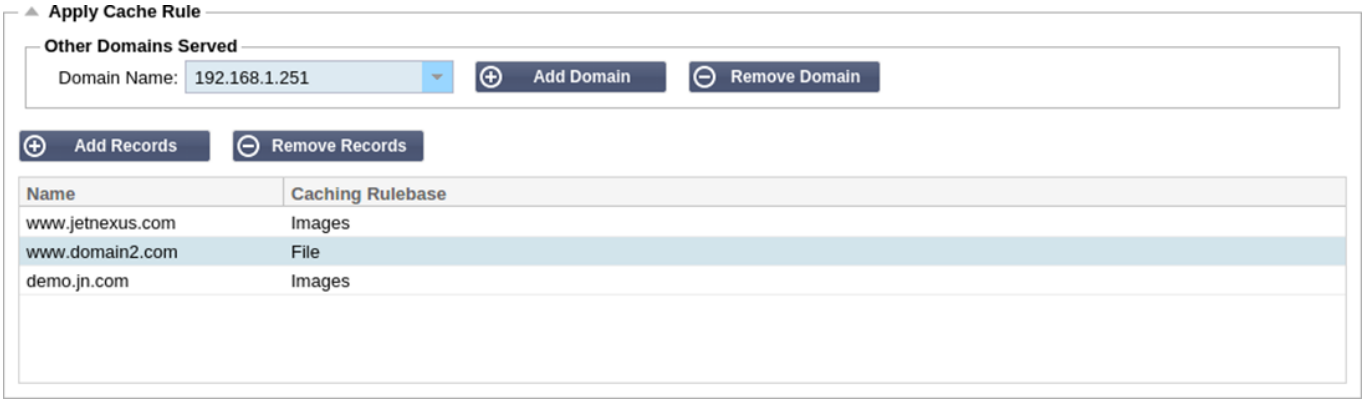
Tempo di controllo della cache (D/HH:MM)

Questa impostazione determina l'intervallo di tempo tra le operazioni di taglio della cache.

Conteggio del riempimento della cache

Questa impostazione è un aiuto per riempire la cache quando è stato rilevato un certo numero di 304.

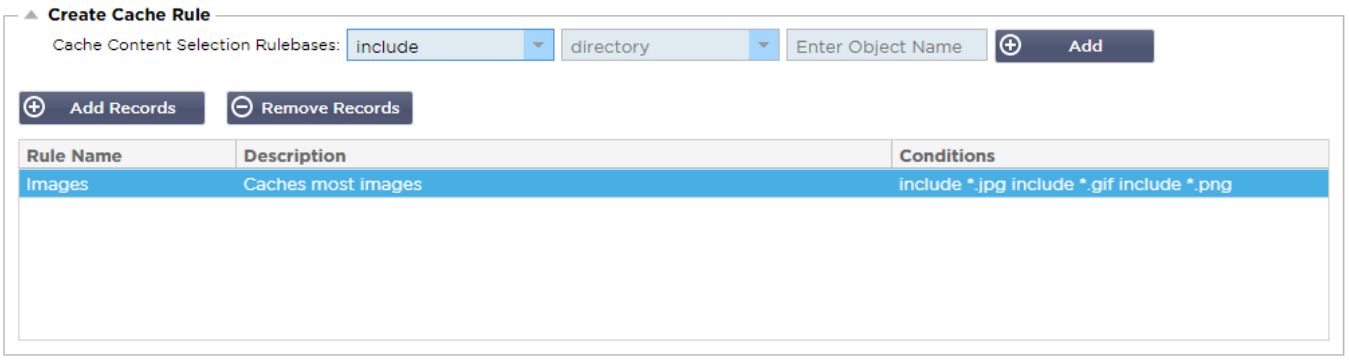
Applicare la regola della cache



Questa sezione ti permette di applicare una regola di cache a un dominio:

- Aggiungi il dominio manualmente con il pulsante Add Records. Devi usare un nome di dominio completamente qualificato o un indirizzo IP in notazione decimale punteggiata. Esempio www.mycompany.com o 192.168.3.1:80
- Clicca sulla freccia a discesa e scegli il tuo dominio dall'elenco
- L'elenco sarà popolato finché il traffico è passato attraverso un servizio virtuale e una strategia di caching è stata applicata al servizio virtuale
- Scegli la tua regola di cache facendo doppio clic sulla colonna Caching Rulebase e selezionando dall'elenco

Creare una regola di cache



Questa sezione permette di creare diverse regole di caching che possono essere applicate a un dominio:

- Clicca su Add Records e dai alla tua regola un nome e una descrizione
- Puoi digitare le tue condizioni manualmente o usare il pulsante Aggiungi condizione

Per aggiungere una condizione usando la Selection Rulebase:

- Scegliere Includi o Escludi
- Scegliere tutte le immagini JPEG
- Clicca sul simbolo + Add
- Vedrai che "include *.jpg" è stato aggiunto alle condizioni
- Puoi aggiungere più condizioni. Se scegli di farlo manualmente, devi aggiungere ogni condizione su una riga NUOVA. Nota che le tue regole saranno visualizzate sulla stessa linea fino a quando non cliccherai nella casella Condizioni, allora saranno visualizzate su una linea separata

flightPATH

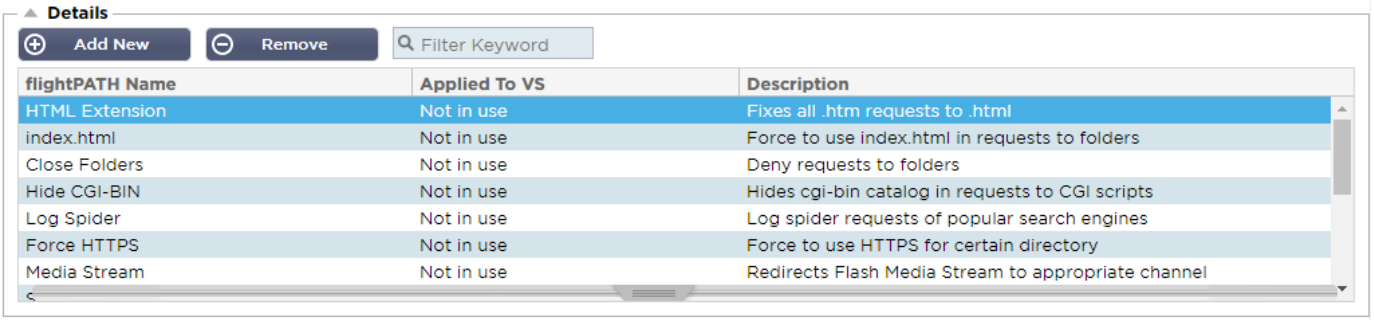
flightPATH è la tecnologia di gestione del traffico integrata nell'ADC. flightPATH permette di ispezionare il traffico HTTP e HTTPS in tempo reale e di eseguire azioni basate sulle condizioni.

Le regole flightPATH devono essere applicate ad un VIP quando gli oggetti IP sono utilizzati all'interno delle regole.

Una regola del percorso di volo è composta da quattro elementi:

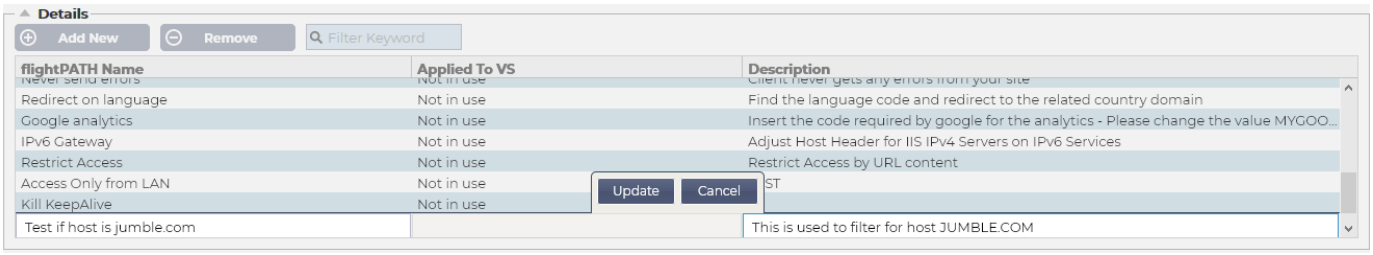
1. Details, dove si definisce il nome del flightPATH e il servizio a cui è collegato.
2. Condizioni che possono essere definite per far scattare la regola.
3. Valutazione che permette la definizione di variabili che possono essere utilizzate all'interno di Azioni
4. Azioni che sono usate per gestire ciò che dovrebbe accadere quando le condizioni sono soddisfatte

Dettagli



La sezione dei dettagli mostra le regole flightPATH disponibili. Puoi aggiungere nuove regole flightPATH e rimuovere quelle definite da questa sezione.

Aggiungere una nuova regola flightPATH



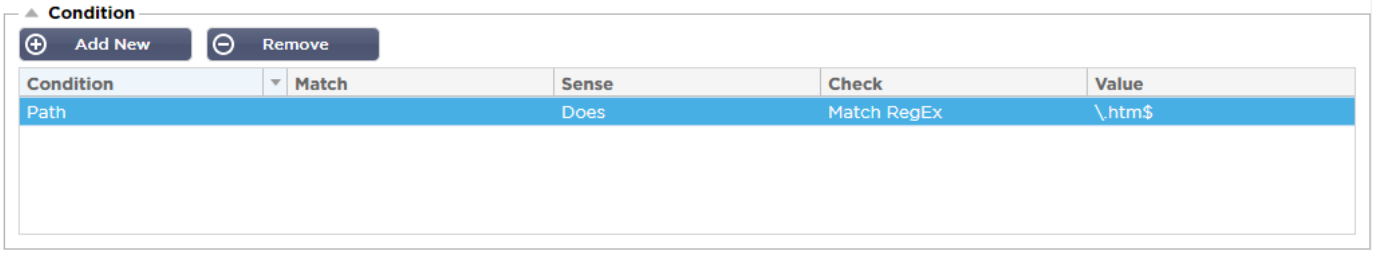
Campo	Descrizione
Nome di FlightPATH	Questo campo è per il nome della regola flightPATH. Il nome che fornisci qui appare ed è referenziato in altre parti dell'ADC.
Applicato a VS	Questa colonna è di sola lettura e mostra il VIP a cui è applicata la regola flightPATH.
Descrizione	Valore che rappresenta una descrizione fornita per motivi di leggibilità.

Passi per aggiungere una regola flightPATH

1. Per prima cosa, clicca sul pulsante Add New che si trova nella sezione Details.
2. Inserisci un nome per la tua regola. Esempio Auth2
3. Inserisci una descrizione della tua regola
4. Una volta che la regola è stata applicata a un servizio, vedrai la colonna Applied To riempirsi automaticamente con un indirizzo IP e un valore di porta
5. Non dimenticare di premere il pulsante Update per salvare le tue modifiche o se fai un errore, basta premere cancel per tornare allo stato precedente.

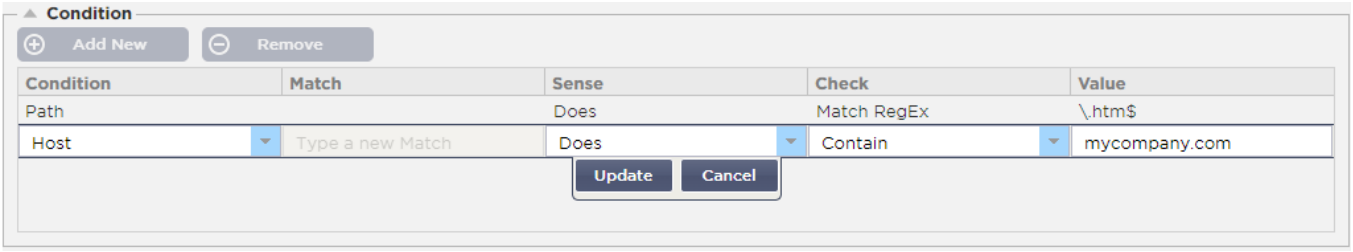
Condizione

Una regola di flightPATH può avere un numero qualsiasi di condizioni. Le condizioni funzionano su base AND e ti permettono di impostare la condizione in base alla quale viene attivata l'azione. Se vuoi usare una condizione OR, crea un'ulteriore regola flightPATH e applicala al VIP nell'ordine corretto.



Puoi anche usare RegEx selezionando Match RegEx nel campo Check e il valore RegEx nel campo Value. L'inclusione della valutazione RegEx estende enormemente la capacità di flightPATH.

Creare una nuova condizione flightPATH



Condizione

Forniamo diverse condizioni predefinite all'interno del menu a tendina e coprono tutti gli scenari previsti. Quando vengono aggiunte nuove condizioni, queste saranno disponibili attraverso gli aggiornamenti di Jetpack.

Le scelte disponibili sono:

CONDIZIONE	DESCRIZIONE	ESEMPIO
<form>	I moduli HTML sono usati per passare dati a un server	Esempio "il modulo non ha lunghezza 0"
Posizione GEO	Confronta l'indirizzo IP sorgente con i codici paese ISO 3166	La posizione GEO è uguale a GB, OPPURE la posizione GEO è uguale a Germania
Ospite	Host estratto dall'URL	www.mywebsite.com o 192.168.1.1
Lingua	Lingua estratta dall'intestazione HTTP della lingua	Questa condizione produrrà un menu a tendina con un elenco di lingue
Metodo	Dropdown dei metodi HTTP	Dropdown che include GET, POST, ecc.
Origine IP	Se il proxy a monte supporta X-Forwarded-for (XFF), userà il vero indirizzo Origin	IP del cliente. Può anche utilizzare più IP o subnet. 10\1\2\.* è 10.1.2.0 /24 subnet10\1\2\.3|10\1\2\.4 Usa | per più IP
Percorso	Percorso del sito web	/mywebsite/index.asp
POST	Metodo di richiesta POST	Controllare i dati che vengono caricati su un sito web
Interrogare	Nome e valore di una query, e può accettare il nome della query o anche un valore	"Best=jetNEXUS" dove la corrispondenza è Best e il valore è edgeNEXUS
Stringa di query	L'intera stringa della query dopo il carattere ?	
Richiesta di cookie	Nome di un cookie richiesto da un cliente	MS-WSMAN=afYfn1CDqCDqUD::
Intestazione della richiesta	Qualsiasi intestazione HTTP	Referrer, User-Agent, Da, Data
Richiesta Versione	La versione HTTP	HTTP/1.0 O HTTP/1.1
Corpo di risposta	Una stringa definita dall'utente nel corpo della risposta	Server UP
Codice di risposta	Il codice HTTP per la risposta	200 OK, 304 Non modificato
Risposta Cookie	Il nome di un cookie inviato dal server	MS-WSMAN=afYfn1CDqCDqUD::
Intestazione della risposta	Qualsiasi intestazione HTTP	Referrer, User-Agent, Da, Data

Versione di risposta	La versione HTTP inviata dal server	HTTP/1.0 O HTTP/1.1
Fonte IP	L'IP di origine, l'IP del server proxy o qualche altro indirizzo IP aggregato	ClientIP , Proxy IP, Firewall IP. Può anche usare più IP e sottoreti. Devi evitare i punti perché questi sono RegEX. Esempio 10\.1\.2\.3 è 10.1.2.3

Partita

Il campo Match può essere sia un menu a tendina che un valore di testo ed è definibile a seconda del valore nel campo Condition. Per esempio, se la Condizione è impostata su Host, il campo Match non è disponibile. Se la Condizione è impostata su <form>, il campo Match è mostrato come un campo di testo, e se la Condizione è POST, il campo Match è presentato come una tendina contenente i valori pertinenti.

Le scelte disponibili sono:

MATCH	DESCRIZIONE	ESEMPIO
Accettare	Tipi di contenuto accettabili	Accettare: text/plain
Accept-Encoding	Codifiche accettabili	Accept-Encoding: <compress | gzip | deflate | sdch | identity>
Accept-Language	Lingue accettabili per la risposta	Accetta la lingua: it-US
Accept-Range	Quali tipi di intervallo di contenuto parziale supporta questo server	Accetta: bytes
Autorizzazione	Credenziali di autenticazione per l'autenticazione HTTP	Autorizzazione: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Carica a	Contiene informazioni contabili per i costi dell'applicazione del metodo richiesto	
Content-Encoding	Il tipo di codifica usato	Codifica dei contenuti: gzip
Content-Length	La lunghezza del corpo della risposta in ottetti (byte a 8 bit)	Lunghezza del contenuto: 348
Content-Type	Il tipo mime del corpo della richiesta (usato con richieste POST e PUT)	Content-Type: application/x-www-form-urlencoded
Cookie	Un cookie HTTP precedentemente inviato dal server con Set-Cookie (sotto)	Cookie: $Version=1; Skin=new;
Data	Data e ora di origine del messaggio	Data = "Data" ":" HTTP-date
ETag	Un identificatore per una versione specifica di una risorsa, spesso un message digest	ETag: "aed6bdb8e090cd1:0"
Da	L'indirizzo e-mail dell'utente che fa la richiesta	Da: user@example.com
Se-Modificato-Da	Permette di restituire un 304 Not Modified se il contenuto è invariato	Se-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Ultimo-Modificato	La data dell'ultima modifica dell'oggetto richiesto, nel formato RFC 2822	Ultimo-Modificato: Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Attuazione: Intestazioni specifiche che possono avere vari effetti in qualsiasi punto della catena richiesta-risposta.	Pragma: no-cache
Referrer	Indirizzo della pagina web precedente da cui è stato seguito un link alla pagina attualmente richiesta	Referente: HTTP://www.edgenexus.io

Server	Un nome per il server	Server: Apache/2.4.1 (Unix)
Set-Cookie	Un cookie HTTP	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
User-Agent	La stringa dell'agente dell'utente	User-Agent: Mozilla/5.0 (compatibile; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Variare	Dice ai proxy a valle come abbinare le future intestazioni di richiesta per decidere se la risposta in cache può essere usata piuttosto che richiederne una nuova dal server d'origine	Vary: User-Agent
X-Powered-By	Specifica la tecnologia (ad esempio ASP.NET, PHP, JBoss) che supporta l'applicazione web	X-Powered-By: PHP/5.4.0

Senso

Il campo Sense è un campo booleano a discesa e contiene le scelte Does o Doesn't.

Controlla

Il campo Controllo permette l'impostazione di valori di controllo rispetto alla Condizione.

Le scelte disponibili sono: Contain, End, Equal, Exist, Have Length, Match RegEx, Match List, Start, Exceed Length

CONTROLLO	DESCRIZIONE	ESEMPIO
Esistere	Questo non si preoccupa del dettaglio della condizione, ma solo del fatto che esiste/non esiste	Host - Does - Exist
Iniziare	La stringa inizia con il valore	Path - Does - Start - /secure
Fine	La stringa termina con il valore	Percorso - Fa - Fine - .jpg
Contenere	La stringa contiene il valore	Intestazione della richiesta - Accept - Does - Contain - image
Uguale	La stringa equivale al valore	Host - Does - Equal - www.edgenexus.io
Avere lunghezza	La stringa ha una lunghezza del valore	Host - Does - Have Length - 16 www.edgenexus.io = VERO www.edgenexus.com = FALSO
Corrisponde a RegEx	Permette di inserire un'espressione regolare completamente compatibile con Perl	IP di origine - Fa - Regex match - 10\..* | 11\..*

Passi per aggiungere una condizione

Aggiungere una nuova condizione flightPATH è molto facile. Un esempio è mostrato qui sopra.

1. Fai clic sul pulsante Add New nell'area Condition.
2. Scegli una condizione dalla casella a discesa. Prendiamo Host come esempio. Puoi anche digitare nel campo, e l'ADC mostrerà il valore in un menu a tendina.
3. Scegli un senso. Per esempio, Fa
4. Scegliere un controllo. Per esempio, Contiene
5. Scegliete un valore. Per esempio, mycompany.com

L'esempio precedente mostra che ci sono due condizioni che devono essere entrambe VERE perché la regola sia completata

- Il primo è controllare che l'oggetto richiesto sia un'immagine
- Il secondo controlla se l'host nell'URL è www.imagepool.com

Valutazione

La capacità di aggiungere variabili definibili è una capacità irresistibile. I normali ADC offrono questa capacità utilizzando opzioni di scripting o di riga di comando che non sono ideali per chiunque. L'ADC permette di definire qualsiasi numero di variabili usando una GUI facile da usare, come mostrato e descritto qui sotto.

La definizione della variabile flightPATH comprende quattro voci che devono essere fatte.

- Variabile - questo è il nome della variabile
- Fonte - un elenco a discesa di possibili punti di origine
- Dettaglio - seleziona i valori da un menu a tendina o digitali manualmente.
- Value - il valore che la variabile tiene e può essere un valore alfanumerico o un RegEx per la messa a punto.

Variabili incorporate:

Le variabili Built-In sono già state hardcoded, quindi non è necessario creare una voce di valutazione per queste.

Puoi usare una qualsiasi delle variabili elencate di seguito nella sezione Azione.

La spiegazione di ogni variabile si trova nella tabella "Condizione" qui sopra.

- Metodo = $metodo$
- Percorso = $path$
- Querystring = $querystring$
- Sourceip = $sourceip$
- Codice di risposta (testo incluso anche "200 OK") = $resp$
- Host = $host$
- Versione = $versione$
- Clientport = $clientport$
- Clientip = $clientip$
- Geolocation = $geolocation$"

AZIONE	TARGET
Azione = Redirect 302	Target = HTTPs://$host$/404.html
Azione = Log	Target = Un cliente da $sourceip$:$sourceport$ ha appena fatto una richiesta $path$ pagina

Spiegazione:

- Un cliente che accede a una pagina che non esiste verrebbe normalmente presentato con la pagina di errore 404 del browser

- Invece, l'utente viene reindirizzato all'hostname originale che ha usato, ma il percorso errato viene sostituito con 404.html
- Viene aggiunta una voce al Syslog che dice: "Un cliente da 154.3.22.14:3454 ha appena richiesto la pagina wrong.html".

Azione

La fase successiva del processo consiste nell'aggiungere un'azione associata alla regola e alla condizione flightPATH.

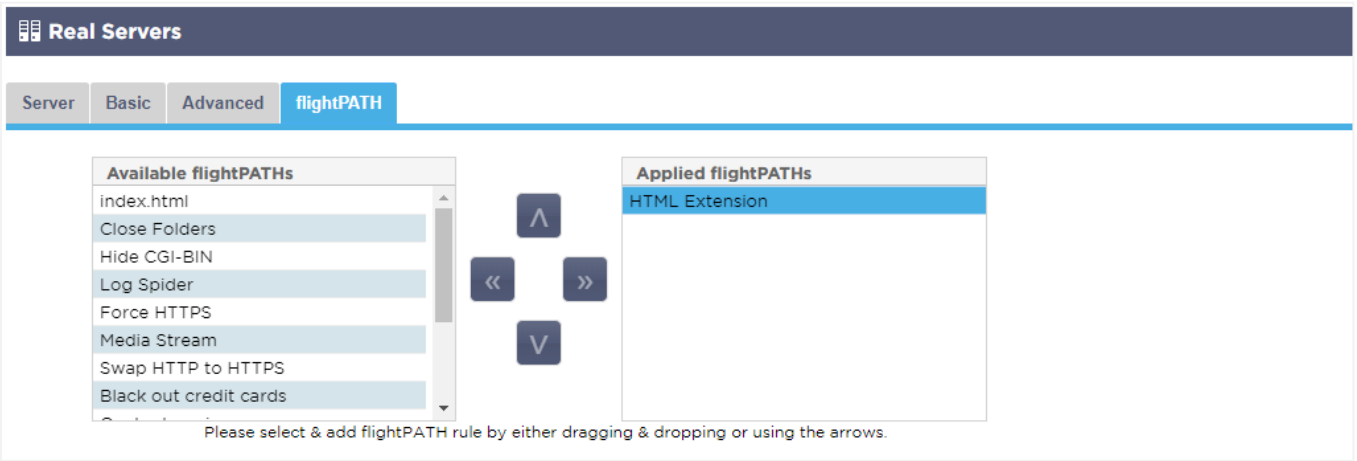
In questo esempio, vogliamo riscrivere la porzione di percorso dell'URL per riflettere l'URL digitato dall'utente.

- Fare clic su Aggiungi nuovo
- Scegliere Rewrite Path dal menu a discesa Action
- Nel campo Destinazione, digitate $path$/myimages
- Fare clic su Aggiorna

Questa azione aggiungerà /myimages al percorso, così l'URL finale diventa www.imagepool.com/myimages

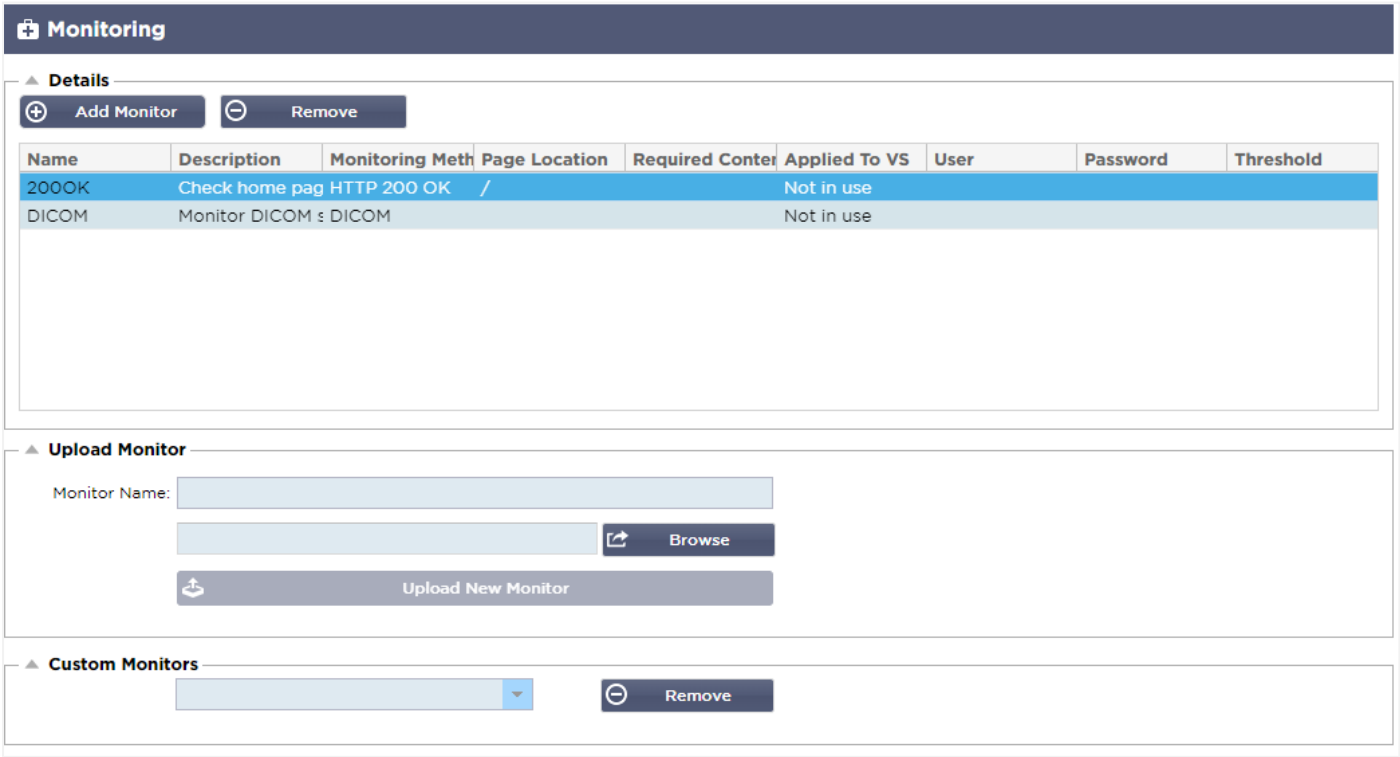
Applicare la regola flightPATH

L'applicazione di qualsiasi regola di flightPATH è fatta all'interno della scheda flightPATH di ogni VIP/VS.



- Vai a Servizi > Servizi IP e scegli il VIP a cui vuoi assegnare la regola flightPATH.
- Vedrai l'elenco di Real Server mostrato qui sotto
- Cliccare sulla scheda flightPATH
- Seleziona la regola flightPATH che hai configurato o una di quelle precostituite supportate. Puoi selezionare più regole flightPATH se necessario.
- Trascinate il set selezionato nella sezione Applied flightPATHs o cliccate sul pulsante freccia >>.
- La regola verrà spostata sul lato destro e applicata automaticamente.

Monitoraggio reale del server



Quando il bilanciamento del carico è impostato, è utile monitorare la salute dei server reali e le applicazioni in esecuzione su di essi. Per esempio, nei server web, è possibile impostare una pagina specifica che è possibile utilizzare per monitorare lo stato o utilizzare uno degli altri sistemi di monitoraggio che l'ADC ha.

La pagina Library > Real Server Monitors ti permette di aggiungere, visualizzare e modificare il monitoraggio personalizzato. Questi sono "controlli di salute" del server Layer 7 e li selezioni dal campo Server Monitoring all'interno della scheda Basic del servizio virtuale che definisci.

Tipi di monitor di server reali

Ci sono diversi Real Server Monitor disponibili, e la tabella qui sotto li spiega. È possibile, naturalmente, scrivere ulteriori monitor usando PERL.

Metodo di monitoraggio	Descrizione	Esempio
HTTP 200 OK	Viene effettuata una connessione TCP al Real Server. Dopo aver stabilito la connessione, viene inviata una breve richiesta HTTP al Real Server. Quando la risposta viene ricevuta, viene controllata per la stringa '200 OK'. Se è presente, il server è considerato operativo. Si prega di notare che utilizzando questo monitor si recupera l'intera pagina con i contenuti. Questo metodo di monitoraggio può essere usato solo con i tipi di servizio HTTP e Accelerated HTTP. Tuttavia, se un tipo di servizio Layer 4 è in uso per un server HTTP, potrebbe ancora essere usato se SSL non è in uso sul Real Server o gestito in modo appropriato dalla funzione "Content SSL".	**Richiesta** GET / HTTP/1.1 Host: 192.168.159.200 Accettare: */* Accetta la lingua: en-gb User-Agent: Edgenexus-ADC/4.0 Connessione: Keep-Alive Cache-Control: no-cache **Risposta** HTTP/1.1 200 OK Tipo di contenuto: text/html Ultimo-Modificato: Wed, 31 Jan 2018 15:08:18 GMT Accetta: bytes ETag: "0dd3253a59ad31:0" Server: Microsoft-IIS/10.0 Data: Tue, 13 Jul 2021 15:55:47 GMT Lunghezza del contenuto: 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"> <head> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /> <titolo>jetNEXUS</titolo> <style type="text/css"> <!-- corpo { colore:#FFFFFF; ... </body> </html>
HTTP 200 Head	Viene effettuata una connessione TCP al Real Server con il campo PATH che specifica la posizione da controllare. La porzione di testa della risposta viene recuperata dal server, con i contenuti scartati. La risposta viene controllata per 200 OK. Se è presente, il server è considerato operativo. Si prega di notare che usando questo monitor si recupera solo la parte della testa. Questo metodo di monitoraggio può essere usato solo con i tipi di servizio HTTP e Accelerated HTTP. Tuttavia, se un tipo di servizio Layer 4 è in uso per un server HTTP, potrebbe ancora essere usato se SSL non è in uso sul Real Server o gestito in modo appropriato dalla funzione "Content SSL".	**Richiesta** TESTA / HTTP/1.1 Host: 192.168.159.200 Accettare: */* Accetta la lingua: en-gb User-Agent: Edgenexus-ADC/4.0 Connessione: Keep-Alive Cache-Control: no-cache **Risposta** HTTP/1.1 200 OK Lunghezza del contenuto: 1364 Tipo di contenuto: text/html Ultimo-Modificato: Wed, 31 Jan 2018 15:08:18 GMT Accetta: bytes ETag: "0dd3253a59ad31:0" Server: Microsoft-IIS/10.0 Data: Tue, 13 Jul 2021 15:49:19 GMT
Opzioni HTTP 200	Viene effettuata una connessione TCP al Real Server e viene fatta una richiesta di opzioni. Le opzioni vengono restituite e controllate per il contenuto 200 OK. Se il contenuto 200 OK viene trovato, allora il server è considerato disponibile.	**Richiesta** OPZIONI / HTTP/1.1 Host: 192.168.159.200 Accettare: */* Accetta la lingua: en-gb User-Agent: Edgenexus-ADC/4.0 Connessione: Keep-Alive Cache-Control: no-cache **Risposta** HTTP/1.1 200 OK Permettere: OPZIONI, TRACCIA, GET, TESTA, POST Server: Microsoft-IIS/10.0 Pubblico: OPZIONI, TRACCIA, OTTENERE, TESTA, POSTA Data: Tue, 13 Jul 2021 16:23:39 GMT Contenuto-Lunghezza: 0
Testa HTTP	Il monitor HTTP Head ci permette di controllare un valore specifico nella porzione Head del flusso HTTP. Possiamo inserire un percorso e una risposta richiesta nei campi appropriati e poi controllare quel valore nella risposta. Se il valore Required Response viene trovato nell'Head, il server è considerato attivo e disponibile.	**Richiesta** HEAD /ispagethere.htm HTTP/1.1 Host: 192.168.159.200 Accettare: */* Accetta la lingua: en-gb User-Agent: Edgenexus-ADC/4.0 Connessione: Keep-Alive Cache-Control: no-cache **Risposta** HTTP/1.1 200 OK

	Possiamo anche usarlo su pagine specialmente protette che richiedono un nome utente e una password. In questo modo, il risultato del monitor può essere considerato accurato. Per esempio, fornire **/ispagethere.html** e i valori **200 OK** nei campi Path e Required Response restituirà un risultato di successo se il server è attivo, la pagina è disponibile e risponde alla richiesta. Questo metodo di monitoraggio può essere usato solo con i tipi di servizio HTTP e Accelerated HTTP. Tuttavia, se un tipo di servizio Layer 4 è in uso per un server HTTP, potrebbe ancora essere usato se SSL non è in uso sul Real Server o gestito in modo appropriato dalla funzione "Content SSL".	Lunghezza del contenuto: 1364 Tipo di contenuto: text/html Ultimo-Modificato: Wed, 31 Jan 2018 15:08:18 GMT Accetta: bytes ETag: "0dd3253a59ad31:0" Server: Microsoft-IIS/10.0 Data: Wed, 14 Jul 2021 08:28:18 GMT
Opzioni HTTP	Il monitor delle opzioni HTTP permette di controllare un valore specifico all'interno dei dati delle opzioni restituite. Inseriamo un Percorso e una Risposta richiesta nei campi appropriati e poi controlliamo la risposta. Se la risposta richiesta si trova nei dati delle opzioni, il server è disponibile e funzionante. I valori di risposta richiesti possono essere uno qualsiasi dei seguenti: OPTIONS, TRACE, GET, HEAD e POST. Per esempio, fornire **/ispagethere.html** e i valori **GET** nei campi Path e Required Response restituirà un risultato di successo se il server è attivo, la pagina è disponibile e risponde alla richiesta. Questo metodo di monitoraggio può essere usato solo con i tipi di servizio HTTP e Accelerated HTTP. Tuttavia, se un tipo di servizio Layer 4 è in uso per un server HTTP, potrebbe ancora essere usato se SSL non è in uso sul Real Server o gestito in modo appropriato dalla funzione "Content SSL".	**Richiesta** OPZIONI /ispagethere.htm HTTP/1.1 Host: 192.168.159.200 Accettare: */* Accetta la lingua: en-gb User-Agent: Edgenexus-ADC/4.0 Connessione: Keep-Alive Cache-Control: no-cache **Risposta** HTTP/1.1 200 OK Permettere: OPZIONI, TRACCIA, GET, TESTA, POST Server: Microsoft-IIS/10.0 Pubblico: OPZIONI, TRACCIA, OTTENERE, TESTA, POSTA Data: Wed, 14 Jul 2021 09:47:27 GMT Contenuto-Lunghezza: 0
Risposta HTTP	Una connessione e una richiesta/risposta HTTP vengono fatte al Real Server e controllate come spiegato negli esempi precedenti. Ma piuttosto che controllare un codice di risposta "200 OK", l'intestazione della risposta HTTP viene controllata per il contenuto del testo personalizzato. Il testo può essere un'intestazione completa, parte di un'intestazione, una riga di una parte di una pagina o solo una parola. Per esempio, nell'esempio mostrato a destra, abbiamo specificato **/ispagethere.htm** come percorso e **Microsoft-IIS** come risposta richiesta. Se il testo viene trovato, il Real Server è considerato attivo e funzionante. Questo metodo di monitoraggio può essere usato solo con i tipi di servizio HTTP e Accelerated HTTP.	**Richiesta** GET /ispagethere.htm HTTP/1.1 Host: 192.168.159.200 Accettare: */* Accetta la lingua: en-gb User-Agent: Edgenexus-ADC/4.0 Connessione: Keep-Alive Cache-Control: no-cache **Risposta** HTTP/1.1 200 OK Tipo di contenuto: text/html Ultimo-Modificato: Wed, 31 Jan 2018 15:08:18 GMT Accetta: bytes ETag: "0dd3253a59ad31:0" Server: Microsoft-IIS/10.0 Data: Wed, 14 Jul 2021 10:07:13 GMT Lunghezza del contenuto: 1364 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"

	Tuttavia, se un tipo di servizio Layer 4 è in uso per un server HTTP, potrebbe ancora essere usato se SSL non è in uso sul Real Server o gestito in modo appropriato dalla funzione "Content SSL".	"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /> <titolo>jetNEXUS</titolo> <style type="text/css"> <!-- corpo { colore:#FFFFFF; …
Monitor TCP multiporta	Questo metodo è come il precedente, eccetto che si possono avere diverse porte. Il monitor è considerato riuscito solo se tutte le porte specificate nella sezione del contenuto richiesto rispondono correttamente.	Nome: Monitor multi-porta Descrizione: Monitorare più porte per il successo Posizione della pagina: N/A Contenuto richiesto: 135,59534,59535
TCP fuori banda	Il metodo TCP Out of Band è come un TCP Connect, tranne che puoi specificare la porta che desideri monitorare nella colonna del contenuto richiesto. Questa porta non è tipicamente la stessa della porta del traffico e viene utilizzata quando si desidera legare i servizi insieme	Nome: TCP fuori banda Descrizione: Monitorare la porta Out of Band/Traffic Posizione della pagina: N/A Contenuto richiesto: 555
DICOM	Inviamo un eco DICOM usando il valore "Source Calling" AE Title nella colonna del contenuto richiesto. Potete anche impostare il valore AE Title "Destination Called" nella sezione Notes di ogni server. Potete trovare la colonna Note all'interno di IP Services-Servizi virtuali - pagina del server.	Nome: DICOM Descrizione: Controllo di salute L7 per il servizio DICOM Metodo di monitoraggio: DICOM Posizione della pagina: N/A Contenuto richiesto: Valore AET
LDAPS	Questo nuovo controllo dello stato di salute è usato per verificare lo stato e la risposta di un server LDAP/AD.	Nome: LDAPS Descrizione: Controllo della salute del server LDAP/AD I parametri di utilizzo sono i seguenti: **Nome utente**: cn=username,cn=users,dc=domainname, dc=local **Password**: DomainUserPassword **Contenuto**: 200OK
SNMP v2	Questo metodo di monitoraggio permette di controllare lo stato di disponibilità di un server usando la risposta SNMP MIB del server. Il valore Require Response dovrebbe contenere il Community Name.	
Controllo del server DNS	Quando si bilanciano i server DNS, è utile vedere se il server risponde alle query DNS. Il monitor può essere utilizzato come segue: • Il campo Path è usato per il FQDN che stai interrogando. Per esempio, se vuoi interrogare www.edgenexus.io, allora inserisci questo nel campo Path. • Se lasciate questo vuoto, allora il monitor userà il suo lookup predefinito per fare la query. • Il campo Required Response può essere lasciato vuoto, e il monitor assumerà che qualsiasi risposta sia considerata valida. Altrimenti, dovresti inserire l'IP previsto nel campo Required Response. Per esempio, questo potrebbe essere 101.10.10.100. Se la query restituisce questo valore, il monitor segnala un successo, altrimenti segnala un fallimento. Un risultato di successo indica che il server DNS che state bilanciando è operativo.	

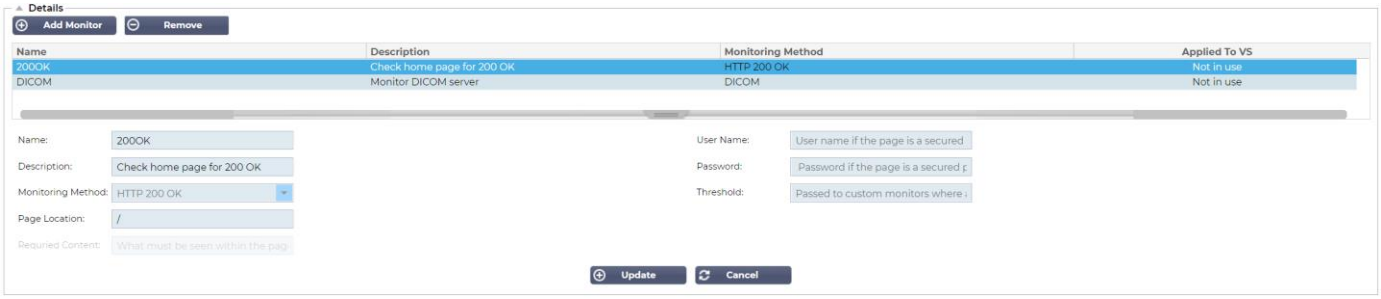
La pagina del Real Server Monitor

La pagina Real Server Monitors è divisa in tre sezioni.

- Dettagli
- Carica
- Monitor personalizzati

Dettagli

La sezione Dettagli è usata per aggiungere nuovi monitor e per rimuovere quelli che non ti servono. Puoi anche modificare un monitor esistente facendo doppio clic su di esso.



Nome

Nome di vostra scelta per il vostro monitor.

Descrizione

Descrizione testuale per questo Monitor, e raccomandiamo che sia meglio renderla il più descrittiva possibile.

Metodo di monitoraggio

Scegliere il metodo di monitoraggio dall'elenco a discesa. Le scelte disponibili sono:

- HTTP 200 OK
- HTTP 200 Head
- Opzioni HTTP 200
- Testa HTTP
- Opzioni HTTP
- Risposta HTTP
- Monitor TCP multiporta
- TCP fuori banda
- DICOM
- SNMP v2
- Controllo del server DNS
- LDAPS

Posizione della pagina

URL Posizione della pagina per un monitor HTTP. Questo valore può essere un link relativo come /folder1/folder2/page1.html. Puoi anche usare un link assoluto dove il sito web è legato all'hostname.

Contenuto richiesto

Questo valore contiene qualsiasi contenuto che il monitor deve rilevare e utilizzare. Il valore rappresentato qui cambierà a seconda del metodo di monitoraggio scelto.

Applicato a VS

Questo campo è automaticamente popolato con l'IP/Porta del servizio virtuale al quale il monitor è applicato. Non sarà possibile eliminare un monitor che è stato utilizzato con un servizio virtuale.

Utente

Alcuni monitor personalizzati possono usare questo valore insieme al campo password per accedere a un Real Server.

Password

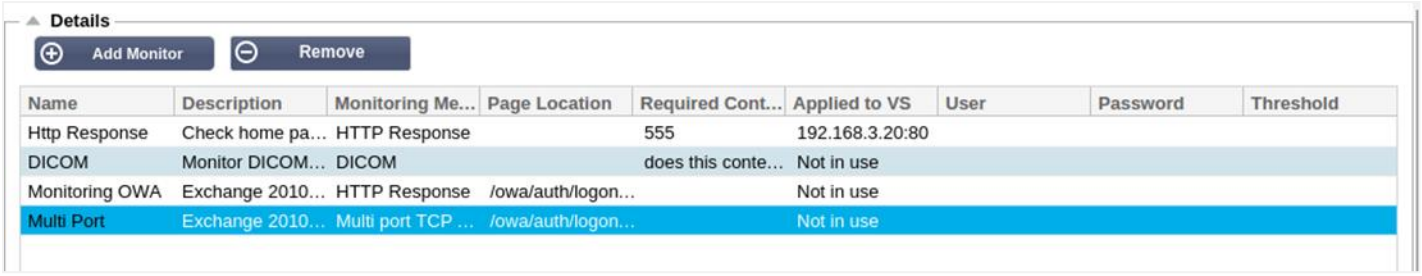
Alcuni monitor personalizzati possono usare questo valore insieme al campo User per accedere a un Real Server.

Soglia

Il campo Threshold è un intero generale usato nei monitor personalizzati dove è richiesta una soglia come il livello di CPU.

NOTA: Assicurati che la risposta del server dell'applicazione non sia una risposta "Chunked".

Esempi di Real Server Monitor



Caricare il monitor

Ci saranno molte occasioni in cui gli utenti desiderano creare i propri monitor personalizzati e questa sezione permette loro di caricarli sull'ADC.

I monitor personalizzati sono scritti usando script PERL e hanno un'estensione di file .pl.

- Date un nome al vostro monitor in modo da poterlo identificare nell'elenco Metodo di monitoraggio
- Cerca il file .pl
- Fare clic su Carica nuovo monitor
- Il tuo file verrà caricato nella posizione corretta e sarà visibile come un nuovo Metodo di monitoraggio.

Monitor personalizzati

In questa sezione, è possibile visualizzare i monitor personalizzati caricati e rimuoverli se non sono più necessari.

- Fare clic sulla casella a discesa
- Selezionare il nome del monitor personalizzato
- Fare clic su Rimuovi
- Il tuo monitor personalizzato non sarà più visibile nell'elenco Metodo di monitoraggio

Creare uno script Perl personalizzato per il monitoraggio

ATTENZIONE: Questa sezione è destinata a persone con esperienza nell'uso e nella scrittura in Perl

Questa sezione vi mostra i comandi che potete usare all'interno del vostro script Perl.

Il comando #Monitor-Name: è il nome usato per lo script Perl memorizzato sull'ADC. Se non includi questa linea, il tuo script non sarà trovato!

I seguenti sono obbligatori:

- #Nome-Monitor
- usare rigorosamente;
- avvertimento d'uso;

Gli script Perl sono eseguiti in un ambiente CHROOTED. Spesso chiamano un'altra applicazione come WGET o CURL. A volte questi hanno bisogno di essere aggiornati per caratteristiche specifiche, come SNI.

Valori dinamici

- my $host = $_[0]; - Questo usa l'"indirizzo" dalla sezione IP Services--Real Server
- my $port = $_[1]; - Questo usa la "porta" dalla sezione IP Services--Real Server
- my $content = $_[2]; - Questo usa il valore "Required Content" dalla sezione Library--Real Server Monitoring
- my $notes = $_[3]; - Questo usa la colonna "Note" nella sezione Real Server di IP Services
- my $page = $_[4]; - Questo usa i valori di "Page Location" dalla sezione Library--Real Server Monitor
- my $user = $_[5]; - Questo usa il valore "User" dalla sezione Library--Real Server Monitor
- my $password = $_[6]; - Questo usa il valore "Password" dalla sezione Library--Real Server Monitor

I controlli sanitari personalizzati hanno due risultati

- Successo
  Valore di ritorno
  1Stampa un messaggio di successo a SyslogMarca
  il Real Server Online (purché IN COUNT corrisponda)
- Unsuccessful
  Valore di ritorno 2Stampa
  un messaggio che dice Unsuccessful a SyslogMarca
  il Real Server Offline (a condizione che OUT Count corrisponda)

Esempio di un monitor di salute personalizzato

Nome del monitor: HTTPS_SNI
usare rigorosamente:
avvertenze d'uso;
Il nome del monitor come sopra viene visualizzato nel menu a tendina dei controlli sanitari disponibili.
Ci sono 6 valori passati a questo script (vedi sotto)
Lo script restituirà i seguenti valori
1 è il test è riuscito

```
# 2 se il test non ha successo sub monitor
{
my Shost=       $_[0]; ### Host IP o nome
my Sport=       $_[1]; ### Host Port
my Scontent=    $_[2]; ### Contenuto da cercare (nella pagina web e negli header HTTP)
my Snotes=      $_[3]; ### Nome host virtuale
my Spage=       $_[4]; ### La parte dell'URL dopo l'indirizzo dell'host
my Suser=       $_[5]: ### domain/usemame (opzionale)
my Spassword=           $_[6]; ### password (opzionale)
mio $resolve;
mio $auth       =;
se ($port)
{
        $resolve = "$notes:$port:$host":
}
else {
        $resolve = "$notes:$host";
}
se ($utente && $password) {
        $auth = "-u $user:$password :
}
my @lines = 'curl -s -i -retry 1 -max-time 1 -k -H "Host:$notes --resolve $resolve $auth HTTPs://${notes}${page} 2>&1';
if(join(""@lines)=~/$content/)
        {
        print "HTTPs://$notes}${page} alla ricerca di - $content - Health check successful.\n";
        ritorno(1);
        }
else
        {
        print "HTTPs://${notes}${page} in cerca di - $content - Health check failed.\n";
        ritorno(2)
        }
}
monitor(@ARGV):
```

NOTA: Monitoraggio personalizzato - L'uso di variabili globali non è possibile. Usare solo variabili locali - variabili definite all'interno di funzioni

Certificati SSL

Per utilizzare con successo il bilanciamento del carico Layer 7 con i server che utilizzano connessioni crittografate tramite SSL, l'ADC deve essere dotato dei certificati SSL utilizzati sui server di destinazione. Questo requisito è in modo che il flusso di dati possa essere decriptato, esaminato, gestito e poi ricriptato prima dell'invio al server di destinazione.

I certificati SSL possono andare dai certificati autofirmati che l'ADC può generare ai certificati tradizionali (jolly inclusi) disponibili da fornitori affidabili. Puoi anche usare certificati firmati dal dominio che sono generati da Active Directory.

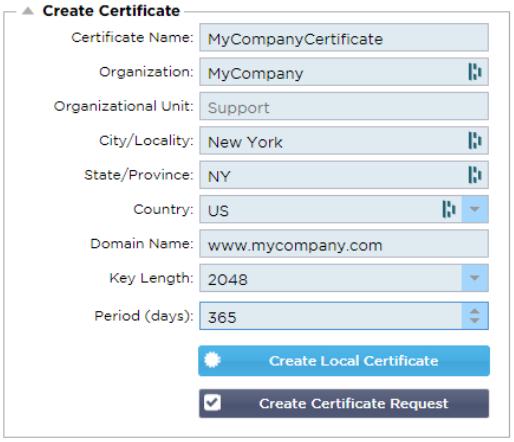
Cosa fa l'ADC con il certificato SSL?

L'ADC può eseguire delle regole di gestione del traffico (flightPATH) a seconda di ciò che i dati contengono. Questa gestione non può essere eseguita sui dati criptati SSL. Quando l'ADC deve ispezionare i dati, deve prima decifrarli, e per questo, deve avere il certificato SSL usato dal server. Una volta decrittato, l'ADC sarà in grado di esaminare ed eseguire le regole flightPATH. In seguito, i dati saranno nuovamente criptati utilizzando il certificato SSL e inviati al Real Server finale.

Crea certificato

Anche se l'ADC può usare un certificato SSL di fiducia globale, può generare un certificato SSL autofirmato. Il Self-Signed SSL è perfetto per i requisiti di bilanciamento del carico interno. Tuttavia, le tue politiche IT potrebbero richiedere un certificato CA di fiducia o di dominio.

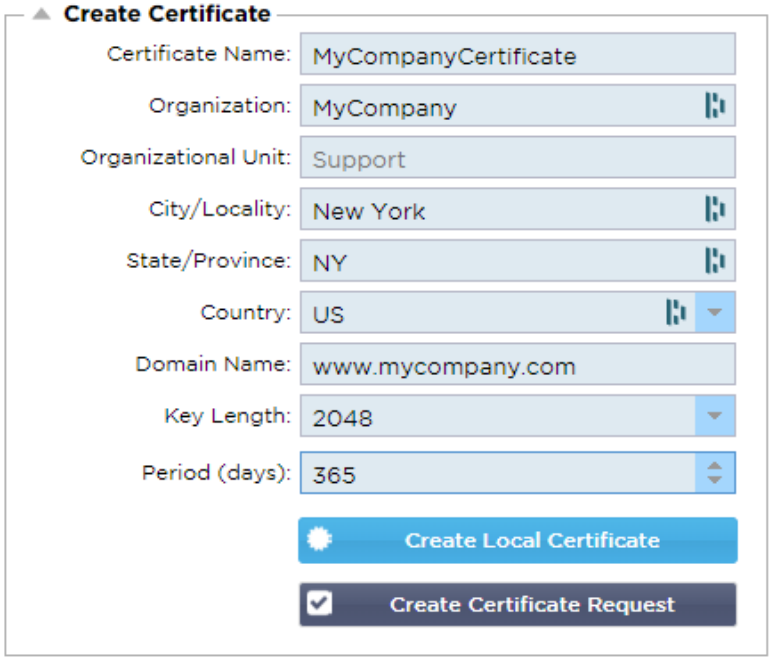
Come creare un certificato SSL locale



- Compila tutti i dettagli come l'esempio qui sopra
- Cliccare su Create Local Certificate
- Dopo aver fatto clic su questo, è possibile applicare il certificato a un **SERVIZIO VIRTUALE.**

Creare una richiesta di certificato (CSR)

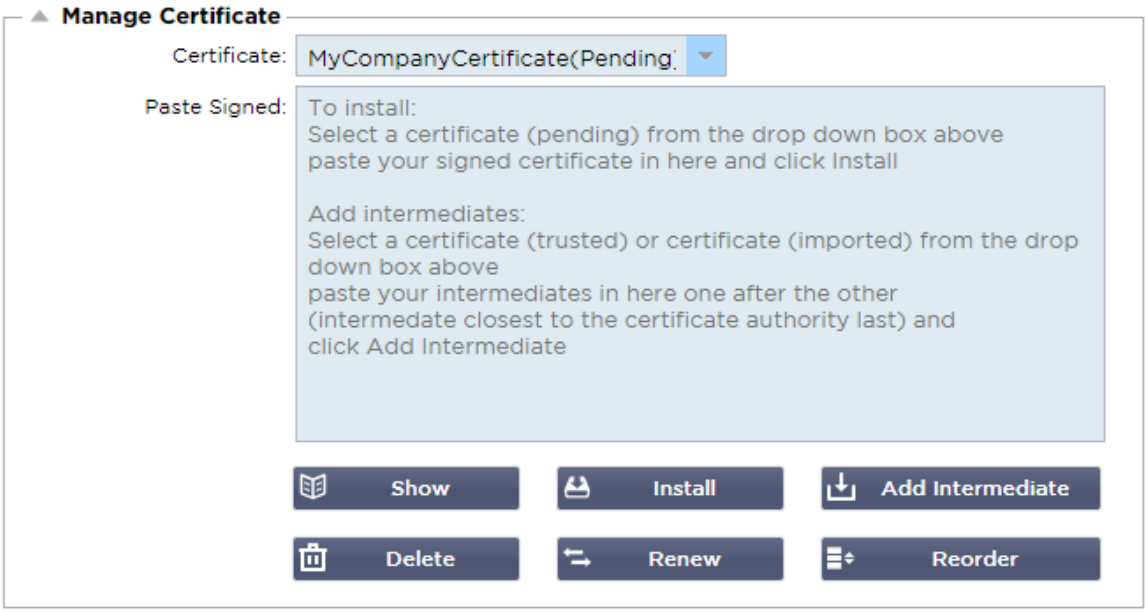
Quando hai bisogno di ottenere un SSL globalmente affidabile da un fornitore esterno, avrai bisogno di generare una CSR per generare il certificato SSL.



Compila il modulo come mostrato sopra con tutti i dati rilevanti, e poi clicca sul pulsante Certificate Request. Ti verrà presentato il popup corrispondente ai dati che hai fornito.

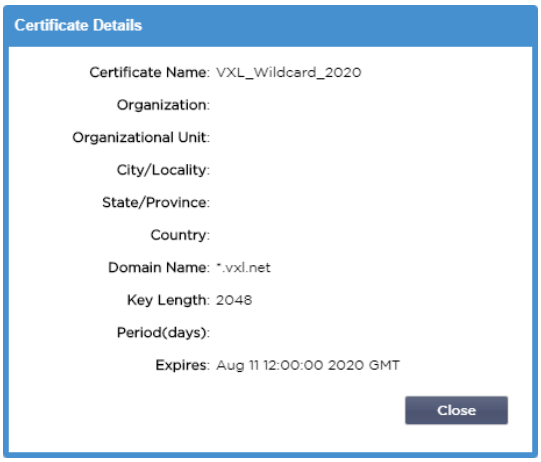
Dovrete tagliare e incollare il contenuto in un file di testo e nominarlo con l'estensione del file CSR, per esempio, *mycert.csr*. Questo file CSR dovrà poi essere fornito alla tua autorità di certificazione per creare il certificato SSL.

Gestire il certificato



Questa sottosezione contiene vari strumenti che permettono la gestione dei certificati SSL che hai all'interno dell'ADC.

Mostra

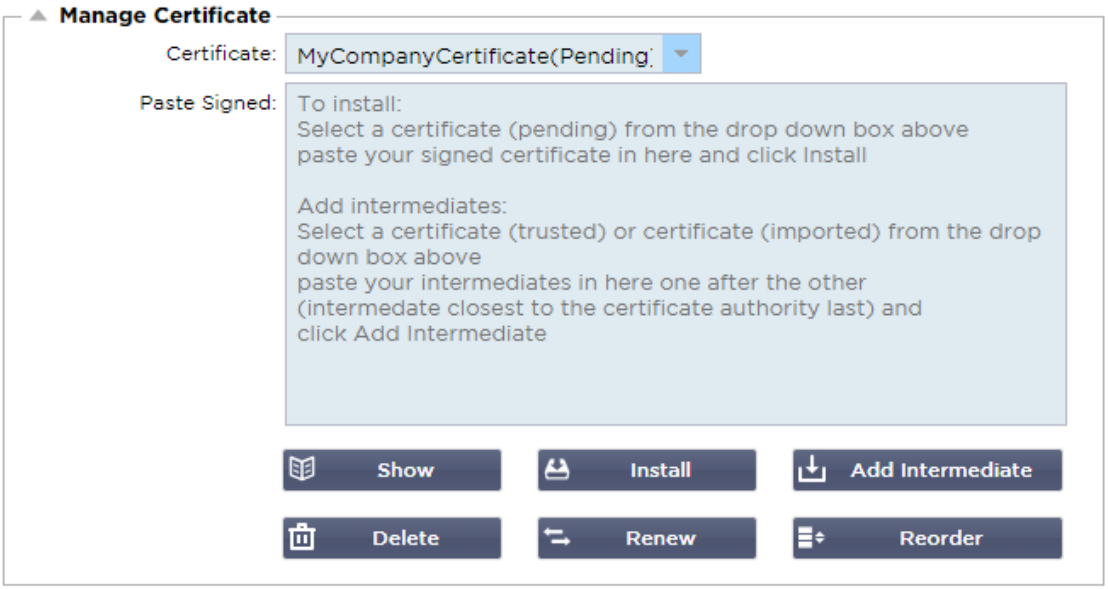


Ci possono essere momenti in cui si desidera guardare i dettagli di un certificato SSL installato.

- Seleziona il certificato dal menu a discesa
- Fare clic sul pulsante Mostra
- Il popup mostrato qui sotto presenterà i dettagli del certificato.

Installare un certificato

Una volta ottenuto il certificato dalla Trusted Certificate Authority, sarà necessario abbinarlo alla CSR generata e installarlo all'interno dell'ADC.



- Seleziona un certificato che hai generato nei passi precedenti. Ci sarà uno stato (Pending) fissato alla voce. Nell'esempio, MyCompanyCertificate è mostrato nell'immagine qui sopra.
- Aprire il file del certificato in un editor di testo
- Copiare l'intero contenuto del file negli appunti
- Incolla il contenuto del certificato SSL firmato che hai ricevuto dall'autorità di fiducia nel campo marcato Paste Signed.
- Puoi anche incollare gli Intermedi sotto questo, facendo attenzione a seguire l'ordine corretto:
    1. (TOP) Il tuo certificato firmato
    2. (2° dall'alto) Intermedio 1
    3. (3° dall'alto) Intermedio 2
    4. (In basso) Intermedio 3

5. Autorità di certificazione radice Non c'è bisogno di aggiungere questo perché esistono sulle macchine client.
   (l'ADC contiene anche un bundle di root per la ricrittografia dove agisce come client verso un Real Server)

- Fare clic su Installa
- Una volta installato il certificato, dovresti vedere lo stato (Trusted) accanto al tuo certificato

Se hai commesso un errore o hai inserito l'ordine intermedio sbagliato, allora seleziona il certificato (Trusted) e aggiungi nuovamente i certificati (incluso il certificato firmato) nell'ordine corretto e clicca su Install

Aggiungi intermedio

A volte è necessario aggiungere separatamente i certificati intermedi. Per esempio, potresti aver importato un certificato che non ha gli intermedi.

- Evidenziare un certificato (affidabile) o un certificato (importato)
- Incollate gli intermedi uno sotto l'altro facendo attenzione che l'intermedio più vicino all'autorità di certificazione sia incollato per ultimo.
- Fare clic su Aggiungi intermedio.

Se fai un errore con l'ordine, puoi ripetere il processo e aggiungere di nuovo gli intermedi. Questa azione sovrascriverà solo gli intermedi precedenti.

Cancellare un certificato

Puoi cancellare un certificato usando il pulsante Delete. Una volta cancellato, il certificato sarà rimosso interamente dall'ADC e dovrà essere sostituito, quindi riapplicato ai servizi virtuali se necessario.

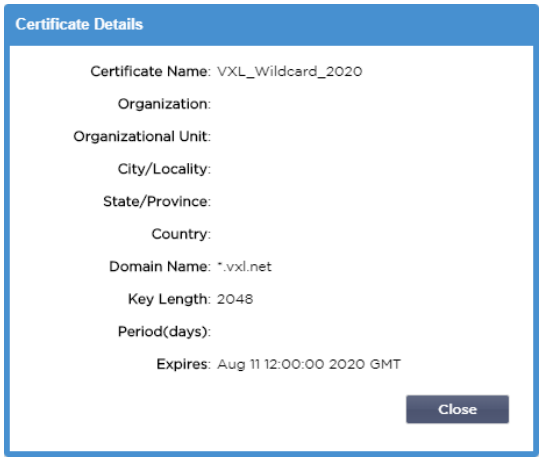
Nota: assicurati che il certificato non sia collegato ad un VIP operativo prima di cancellarlo.

Rinnovare un certificato

Il pulsante Renew permette di ottenere un nuovo Certificate Signing Request. Questa azione è necessaria quando il certificato sta per scadere e deve essere rinnovato.

- Seleziona un certificato dall'elenco a discesa; puoi scegliere qualsiasi certificato con lo stato (Pending), (Trusted) o (Imported)
- Clicca su Rinnova
- Copia i dettagli della nuova CSR per ottenere un nuovo certificato

- Quando ottenete il nuovo certificato, seguite i passi dettagliati in **SHOW**



- Ci possono essere momenti in cui si desidera guardare i dettagli di un certificato SSL installato.
- Seleziona il certificato dal menu a discesa
- Fare clic sul pulsante Mostra
- Il popup mostrato qui sotto presenterà i dettagli del certificato.
- Installazione di un certificato.
- Il certificato nuovo e rinnovato sarà ora installato nell'ADC.

Importare un certificato

In molti casi, le imprese aziendali avranno bisogno di usare i loro certificati firmati dal dominio come parte dei loro regimi di sicurezza interna. I certificati devono essere in formato PKCS#12, e le password proteggono invariabilmente tali certificati.

L'immagine qui sotto mostra la sottosezione per importare un singolo certificato SSL.

- Dai al tuo certificato un nome amichevole. Il nome lo identifica negli elenchi a discesa usati nell'ADC. Non è necessario che sia lo stesso del nome del dominio del certificato, ma deve essere alfanumerico senza spazi. Non sono ammessi caratteri speciali diversi da _ e -.
- Digita la password che hai usato per creare il certificato PKCS#12
- Cerca il {nome del certificato}.pfx
- Fare clic su Importa.
- Il tuo certificato sarà ora nei menu a discesa SSL pertinenti all'interno dell'ADC

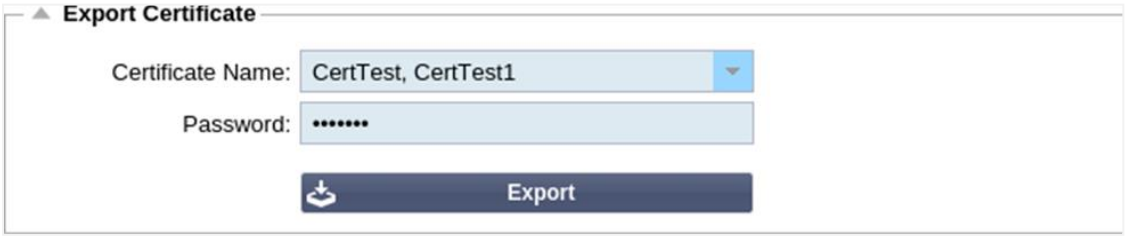
Importare certificati multipli

Questa sezione permette di importare un file JNBK che contiene più certificati. Un file JNBK è criptato e prodotto da ADC quando si esportano più certificati.

- Cerca il tuo file JNBK - puoi crearne uno esportando più certificati
- Digita la password che hai usato per creare il file JNBK
- Fare clic su Importa.
- I tuoi certificati saranno ora nei relativi menu a discesa SSL all'interno dell'ADC

Esportare un certificato

Di tanto in tanto, potresti voler esportare uno dei certificati tenuti all'interno dell'ADC. L'ADC è stato dotato della capacità di fare questo.



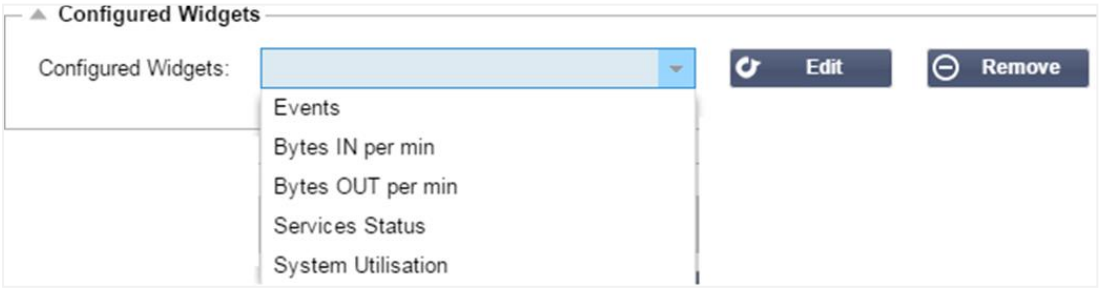
- Clicca sul certificato o sui certificati che vuoi installare. Puoi anche cliccare sull'opzione Tutti per selezionare tutti i certificati elencati.
- Digita una password per proteggere il file esportato. La password deve essere lunga almeno sei caratteri. Si possono usare lettere, numeri e alcuni simboli. I seguenti caratteri **non** sono accettabili: < > " ' ( ) ; \ | \A3 % &
- Fare clic su Esportazione
- Se state esportando un singolo certificato, il file risultante sarà chiamato sslcert_{certname}.pfx. Per esempio sslcert_Test1Cert.pfx
- Nel caso di un'esportazione multicertificato, il file risultante sarà un file JNBK. Il nome del file sarà sslcert__pack.jnbk.

Nota: un file JNBK è un file contenitore criptato prodotto dall'ADC e valido solo per l'importazione nell'ADC

Widget

La pagina Library > Widgets ti permette di configurare vari componenti visivi leggeri visualizzati nella tua dashboard personalizzata.

Widget configurati

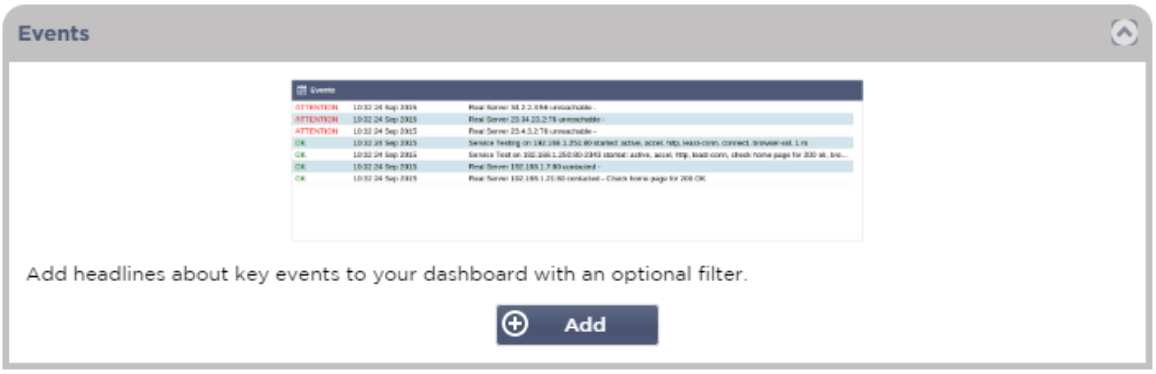


La sezione Configured Widgets ti permette di visualizzare, modificare o rimuovere qualsiasi widget creato dalla sezione dei widget disponibili.

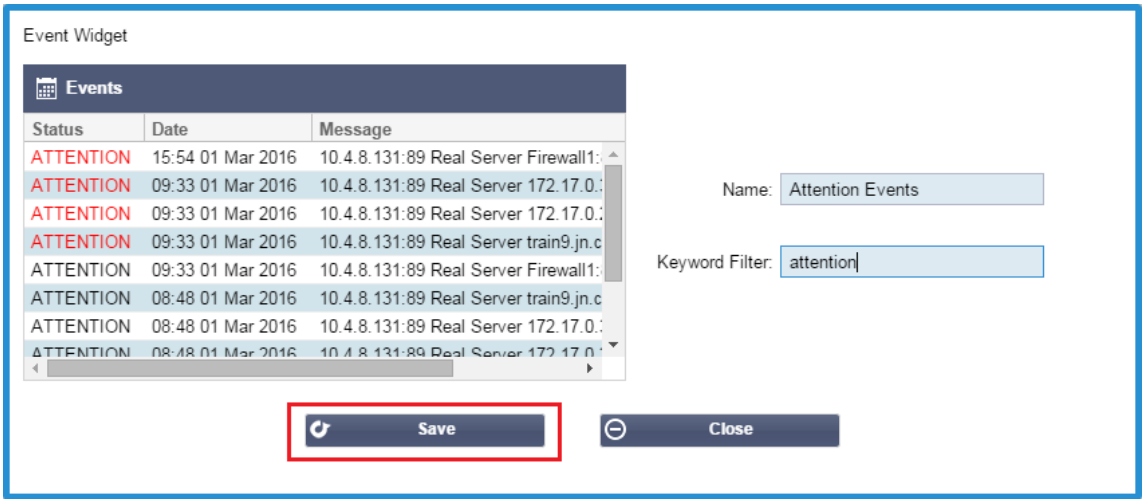
Widget disponibili

Ci sono cinque diversi widget forniti all'interno dell'ADC, e potete configurarli secondo le vostre esigenze.

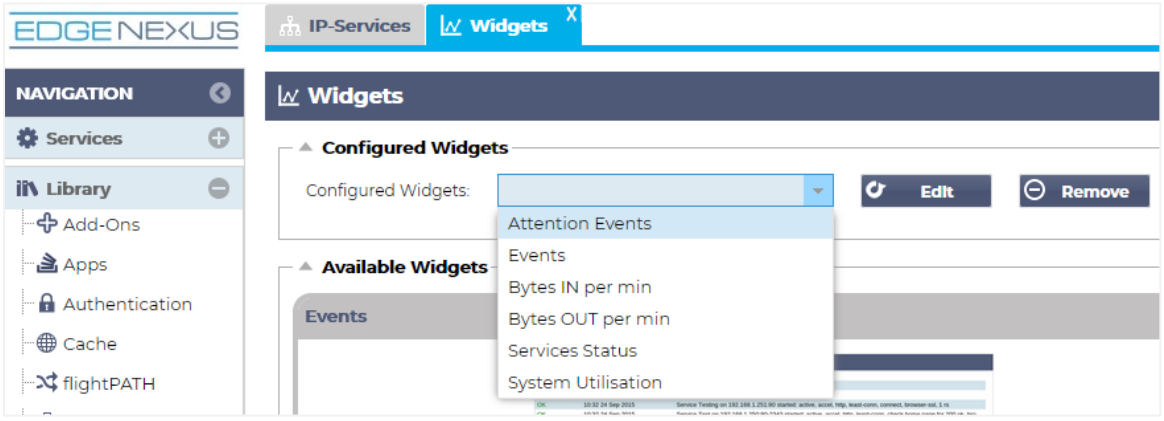
Il widget degli eventi



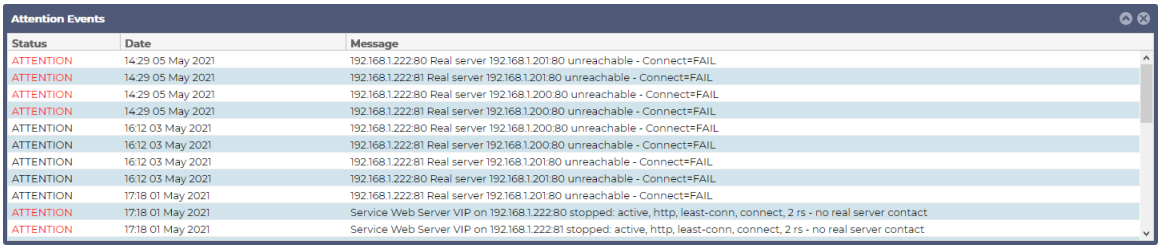
- Per aggiungere un evento al widget Eventi, clicca sul pulsante Aggiungi.
- Fornisci un nome per il tuo evento. Nel nostro esempio, abbiamo aggiunto Attention Events come nome dell'evento.
- Aggiungere un filtro per le parole chiave. Abbiamo anche aggiunto il valore del filtro di Attenzione



- Fare clic su Salva e poi su Chiudi
- Ora vedrai un widget aggiuntivo chiamato Eventi di attenzione nel menu a tendina Widget configurati.

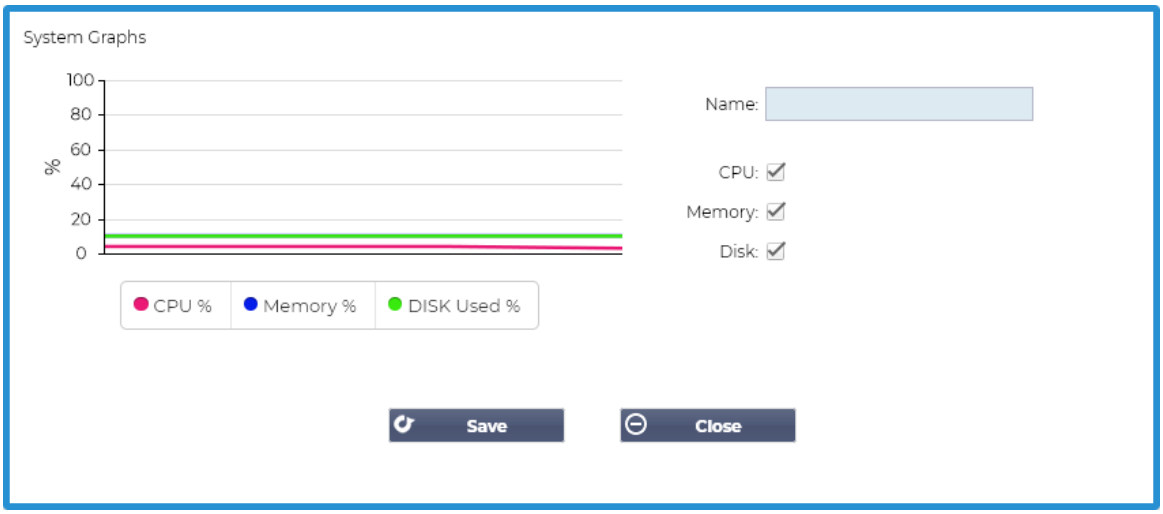


- Puoi vedere che ora abbiamo aggiunto questo widget nella sezione View > Dashboard.
- Seleziona il widget Eventi di attenzione per visualizzarlo nella Dashboard. Vedi sotto.



Puoi anche mettere in pausa e riavviare il flusso di dati dal vivo cliccando il pulsante Pause Live Data. Inoltre, puoi tornare al cruscotto di default in qualsiasi momento cliccando sul pulsante Default Dashboard.

Il widget dei grafici di sistema

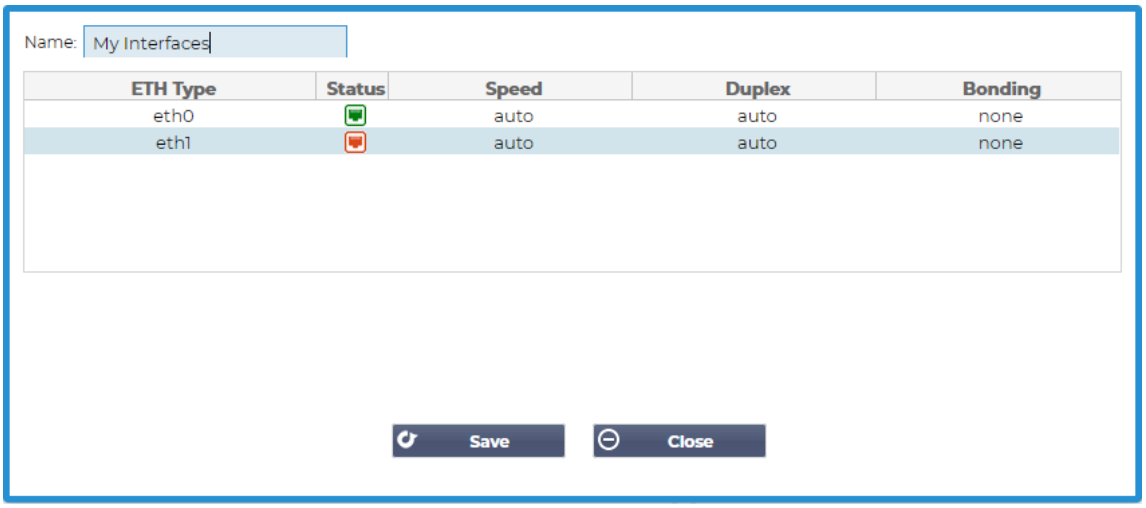


L'ADC ha un widget System Graph configurabile. Cliccando il pulsante Add sul widget, è possibile aggiungere i seguenti grafici di monitoraggio da visualizzare.

- CPU
- MEMORIA
- DISCO

Una volta che li hai aggiunti, saranno disponibili individualmente nel menu dei widget della Dashboard.

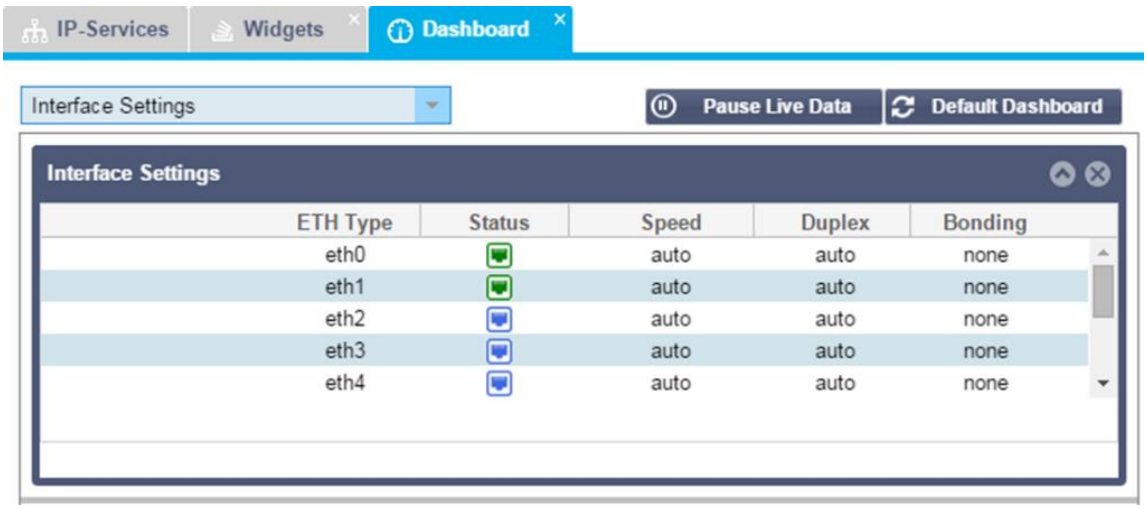
Widget dell'interfaccia



Il widget Interfaccia permette di visualizzare i dati per l'interfaccia di rete scelta, come ETH0, ETH1, e così via. Il numero di interfacce disponibili per l'aggiunta dipende dal numero di interfacce di rete che hai definito per il dispositivo virtuale o fornito all'interno del dispositivo hardware.

Una volta finito, clicca sul pulsante Save e poi su Close.

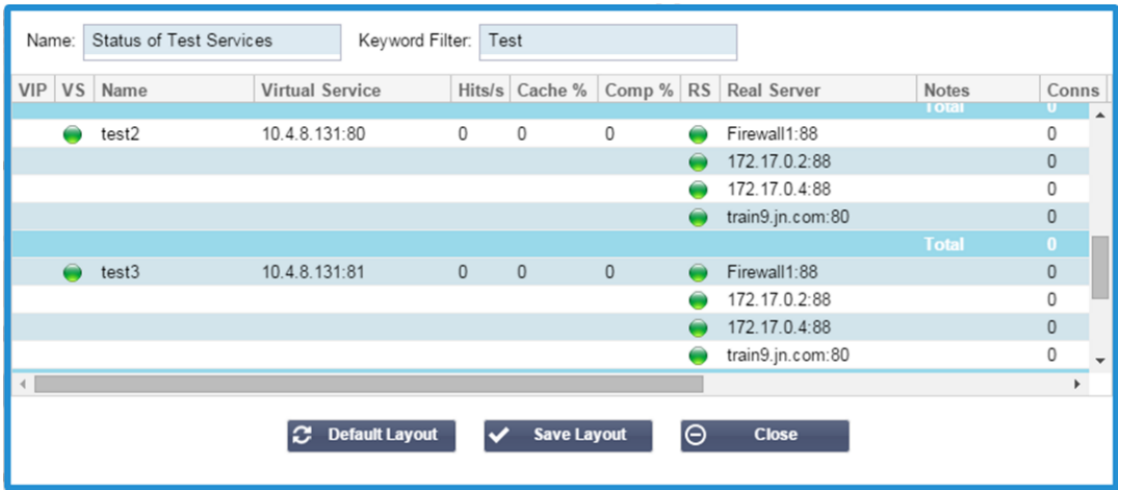
Seleziona il widget che hai appena personalizzato dal menu a discesa dei widget all'interno del Dashboard. Vedrai una schermata come quella qui sotto.



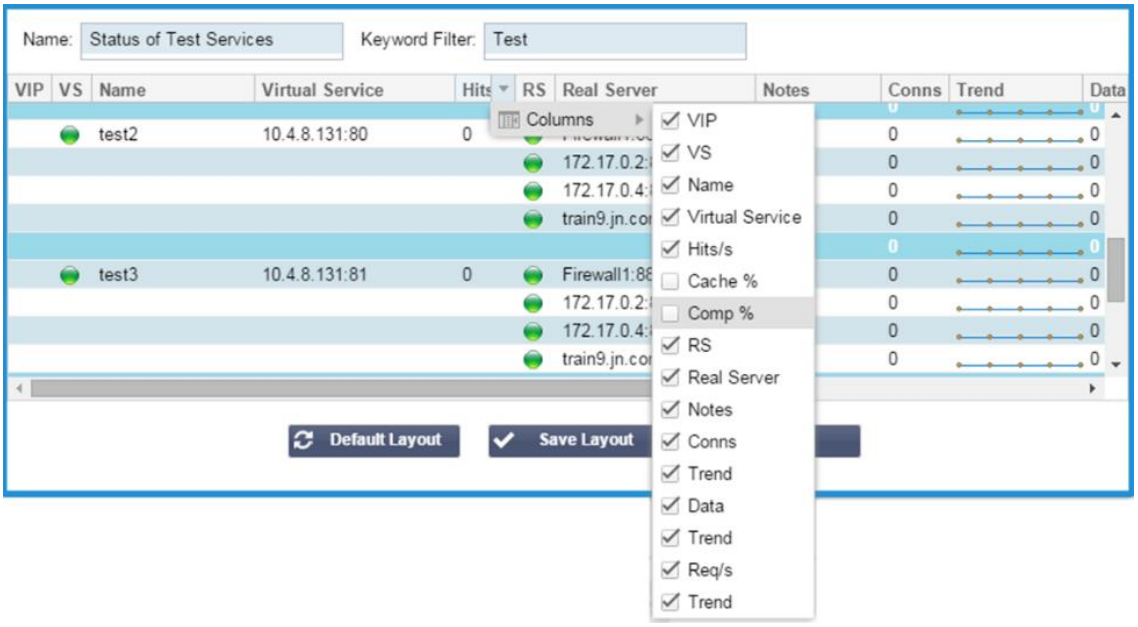
Widget di stato

Il widget di stato permette di vedere il bilanciamento del carico in azione. Si può anche filtrare la vista per mostrare informazioni specifiche.

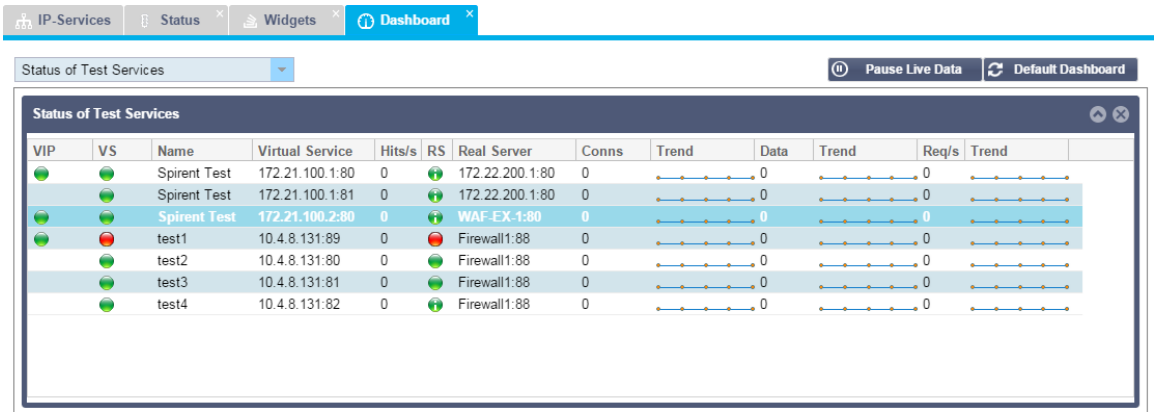
- Fare clic su Aggiungi.



- Inserisci un nome per il servizio che vuoi monitorare
- Puoi anche scegliere quali colonne desideri visualizzare nel widget.

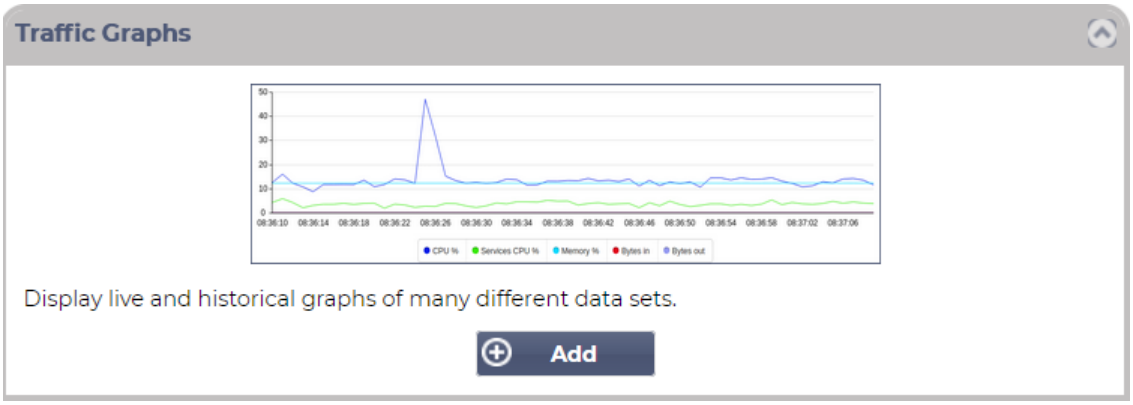


- Una volta che sei soddisfatto, clicca su Save, seguito da Close.
- Il widget di stato scelto sarà disponibile nella sezione Dashboard.



Widget di grafica del traffico

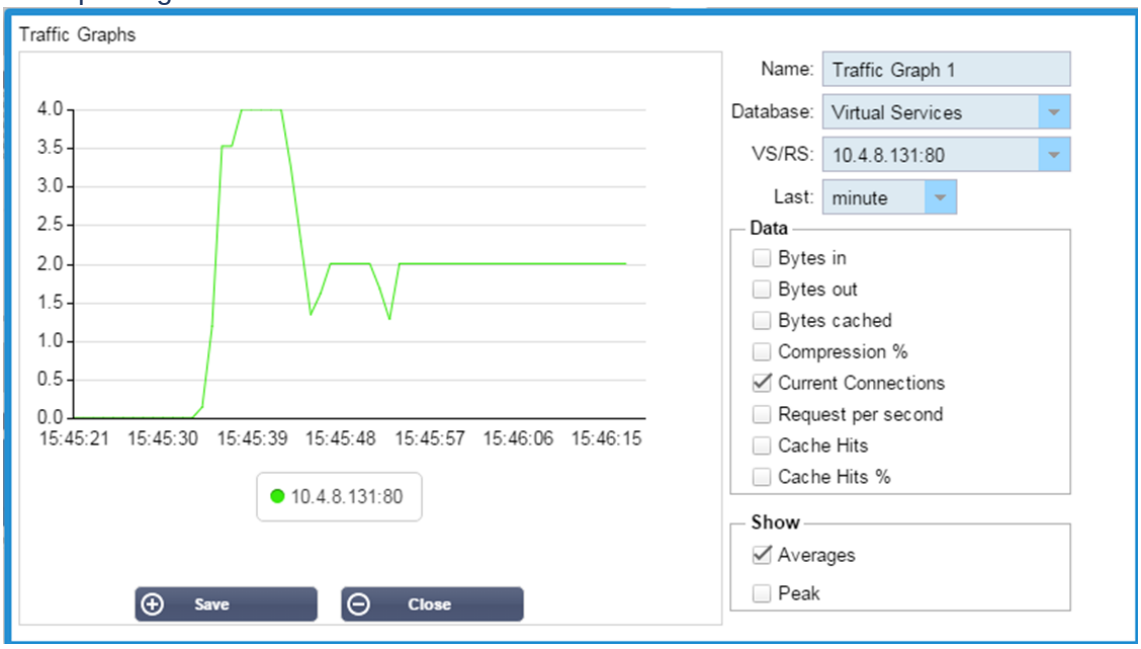
Questo widget può essere configurato per mostrare i dati di traffico attuali e storici per servizi virtuali e server reali. Inoltre, è possibile vedere i dati complessivi attuali e storici per il traffico globale



- Fare clic sul pulsante Aggiungi
- Dai un nome al tuo widget.
- Scegliete un database da Virtual Services, Real Servers o System.
- Se scegliete Servizi virtuali, potete selezionare un servizio virtuale dall'elenco a discesa VS/RS.
- Scegli un periodo di tempo dal menu a tendina Ultimo.

    - Minuti - ultimi 60
    - Ora - dati aggregati da ogni minuto per gli ultimi 60 minuti
    - Giorno - dati aggregati di ogni ora per le 24 ore precedenti
    - Settimana - dati aggregati di ogni giorno nei sette giorni precedenti
    - Mese - dati aggregati di ogni settimana per gli ultimi sette giorni
    - Anno - dati aggregati di ogni mese durante i 12 mesi precedenti
- Scegliete i Dati disponibili a seconda del database che avete scelto
    - Database dei servizi virtuali
    - Bytes in
    - Bytes fuori
    - Bytes nella cache
    - Compressione %
    - Connessioni correnti
    - Richieste al secondo
    - Colpi di cache
    - Cache Hits %
- Server reali
    - Bytes in
    - Bytes fuori
    - Connessioni correnti
    - Richiesta al secondo
    - Tempo di risposta
- Sistema
    - CPU
    - Servizi CPU
    - Memoria %
    - % di disco libero
    - Bytes in
    - Bytes fuori
- Scegliere di mostrare i valori medi o di picco
- Una volta scelte tutte le opzioni, clicca su Salva e chiudi

Esempio di grafico del traffico



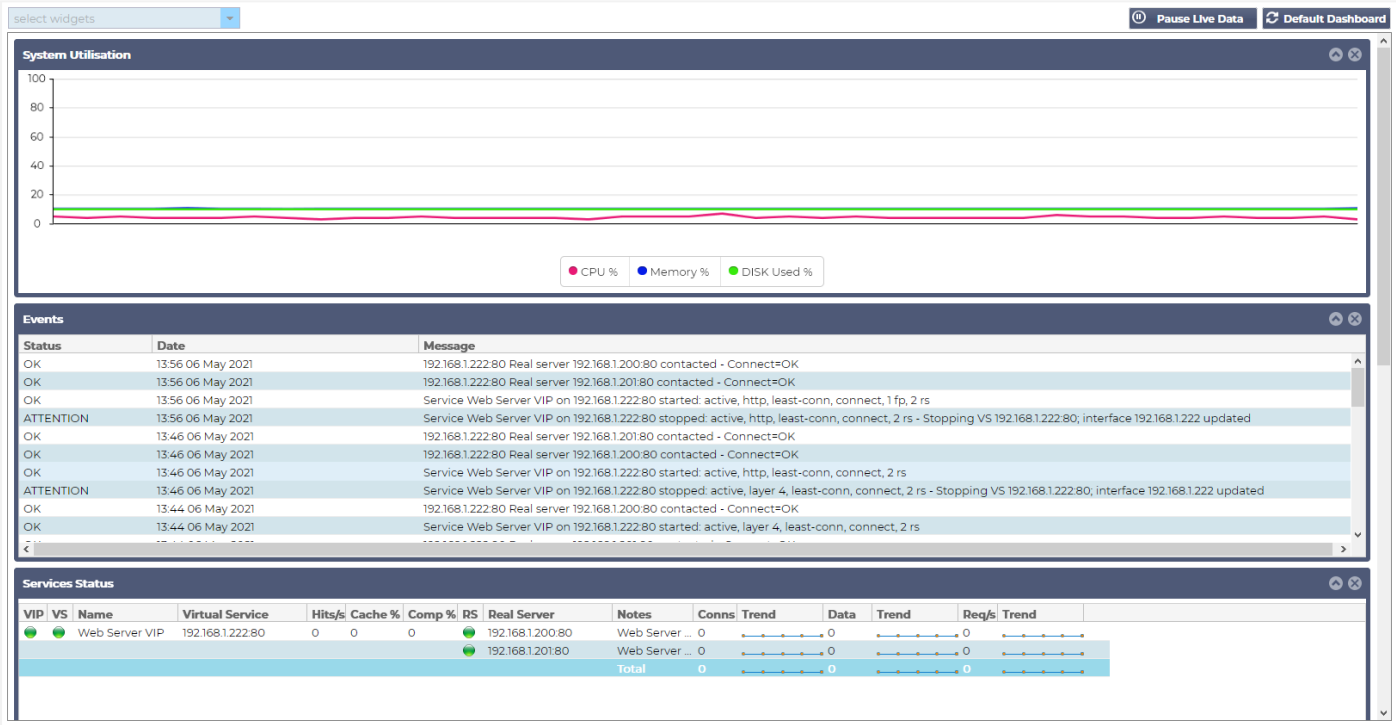
Ora puoi aggiungere il tuo widget Traffic Graph a View > Dashboard.

Vedi

Dashboard

Come tutte le interfacce di gestione dei sistemi IT, ci sono molte volte in cui è necessario guardare le metriche delle prestazioni e i dati che l'ADC sta gestendo. Noi forniamo una dashboard personalizzabile per fare questo in modo facile e significativo.

La Dashboard è raggiungibile utilizzando il segmento View del pannello di navigazione. Quando viene selezionato, mostra diversi widget predefiniti e ti permette di scegliere quelli personalizzati che hai definito.



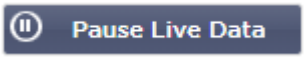
Uso del cruscotto

Ci sono quattro elementi nella Dashboard U: il menu dei widget, il pulsante Pausa/Riproduci e il pulsante Default Dashboard.

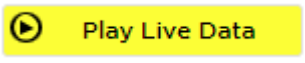
Il menu dei widget

Il menu Widget situato in alto a sinistra della dashboard ti permette di selezionare e aggiungere qualsiasi widget standard o personalizzato che hai definito. Per utilizzarlo, seleziona il widget dal menu a tendina.

Pulsante Pause Live Data



Questo pulsante permette di selezionare se l'ADC deve aggiornare la dashboard in tempo reale. Una volta messo in pausa, nessun widget del cruscotto sarà aggiornato, permettendoti di esaminare il contenuto a tuo piacimento. Il pulsante cambia stato per visualizzare Play Live Data una volta avviata la pausa.



Quando hai finito, clicca semplicemente sul pulsante Play Live Data per riavviare la raccolta dei dati e aggiornare la Dashboard.

Pulsante predefinito del cruscotto

Può capitare che tu voglia riportare il layout del cruscotto a quello predefinito. In tal caso, premi il pulsante Default Dashboard. Una volta cliccato, tutte le modifiche apportate al cruscotto saranno perse.

Ridimensionare, minimizzare, riordinare e rimuovere i widget

Ridimensionare un widget

Puoi ridimensionare un widget molto facilmente. Clicca e tieni premuto sulla barra del titolo del widget e trascinalo sul lato sinistro o destro dell'area Dashboard. Vedrai un rettangolo tratteggiato che rappresenta la nuova dimensione del widget. Trascina il widget nel rettangolo e lascia andare il pulsante del mouse. Se desideri rilasciare un widget ridimensionato accanto a un widget ridimensionato in precedenza, vedrai apparire il rettangolo adiacente al widget che vuoi rilasciare accanto.

Minimizzare un widget

Puoi minimizzare i widget in qualsiasi momento cliccando sulla barra del titolo del widget. Questa azione ridurrà a icona il widget e visualizzerà solo la barra del titolo.

Spostamento dell'ordine dei widget

Per spostare un widget, puoi trascinarlo cliccando e tenendo premuto sulla barra del titolo e muovendo il mouse.

Rimuovere un widget

È possibile rimuovere un cliccando sull'⊗icona nella barra del titolo del widget.

Storia

L'opzione Storia, selezionabile dal navigatore, permette all'amministratore di esaminare le prestazioni storiche dell'ADC. Le viste storiche possono essere generate per i servizi virtuali, i server reali e il sistema.

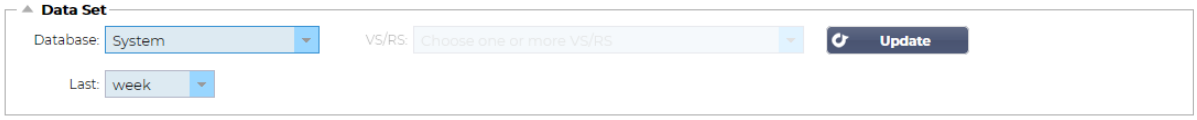
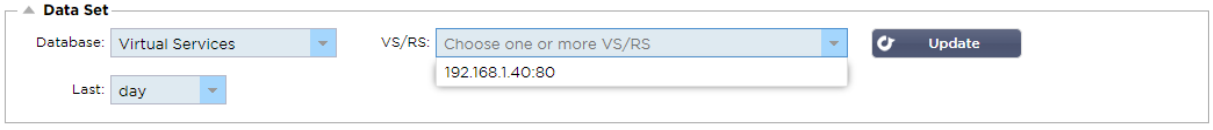
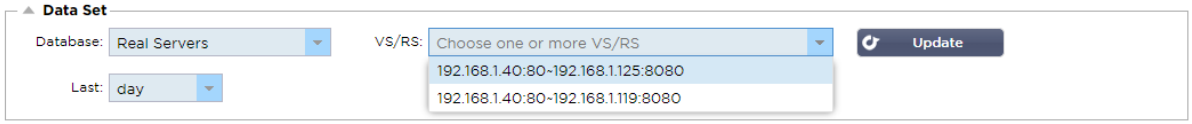
Permette anche di vedere il bilanciamento del carico in azione e aiuta a catturare eventuali errori o schemi che devono essere analizzati. Nota che devi abilitare la registrazione storica in System > History per usare questa caratteristica.

Visualizzazione di dati grafici

Set di dati

Per visualizzare i dati storici in formato grafico, procedere come segue:

Il primo passo è quello di scegliere il database e il periodo relativo alle informazioni che vuoi visualizzare. Il periodo che puoi selezionare dal menu a tendina Last è Minute, Hour, Day, Week, Month e Year.

Database	Descrizione
Sistema	La selezione di questo database vi permetterà di vedere la CPU, la memoria e lo spazio su disco nel tempo 
Servizi virtuali	Selezionando questo database vi permetterà di scegliere tutti i servizi virtuali nel database da quando avete iniziato a registrare i dati. Verrà visualizzato un elenco di servizi virtuali da cui è possibile selezionarne uno. 
Servizi reali	Selezionando questo database potrai scegliere tutti i Real Server presenti nel database da quando hai iniziato a registrare i dati. Verrà visualizzato un elenco di Real Server da cui è possibile selezionarne uno. 

Metriche

Una volta selezionato il set di dati da utilizzare, è il momento di scegliere le metriche che si desidera visualizzare. L'immagine qui sotto illustra le metriche disponibili per la selezione da parte dell'amministratore: queste selezioni corrispondono a Sistema, Servizi virtuali e Server reali (da sinistra a destra).

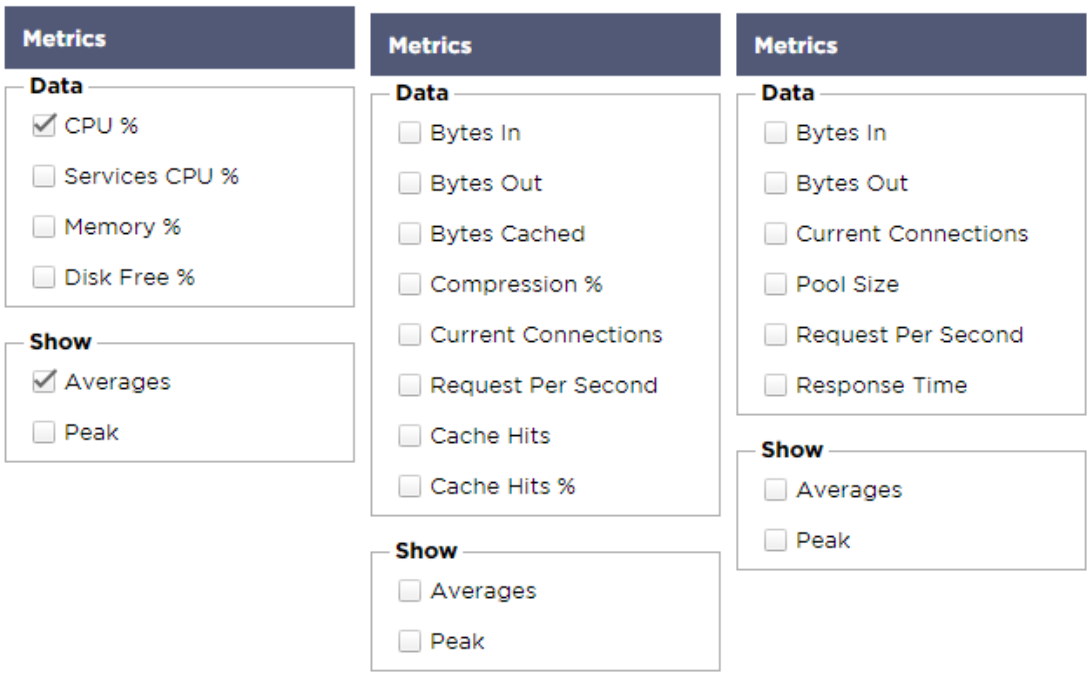
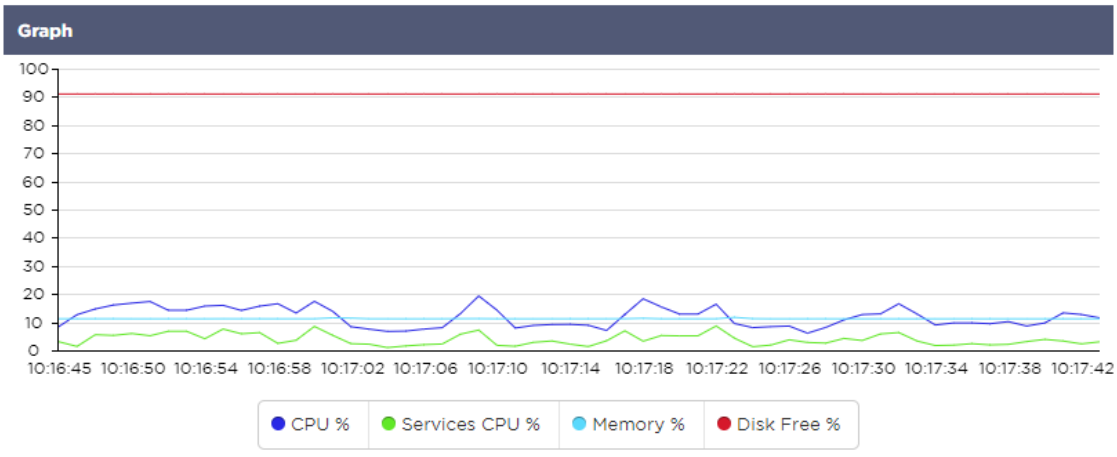


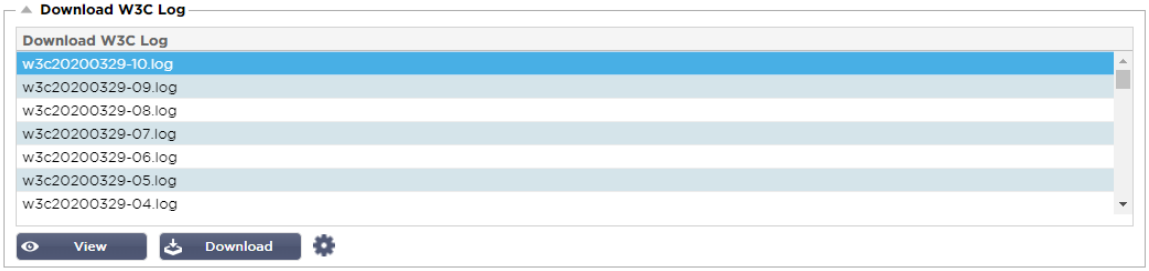
Grafico di esempio



Registri

La pagina dei Logs all'interno della sezione View ti permette di vedere in anteprima e scaricare i log del W3C e del sistema. La pagina è organizzata in due sezioni, come descritto di seguito.

Scarica i log del W3C



Il log W3C è abilitato dalla sezione System > Logging. Un log W3C è un registro di accesso per i server Web in cui vengono generati file di testo contenenti dati su ogni richiesta di accesso, compreso l'indirizzo Internet Protocol (IP) di origine, la versione HTTP, il tipo di browser, la pagina di riferimento e il timestamp. I log del W3C possono diventare molto grandi a seconda della quantità di dati e della categoria di registrazione.

Dalla sezione W3C, potete selezionare il registro di cui avete bisogno e poi visualizzarlo o scaricarlo.

Visualizza Pulsante

Il pulsante View permette di visualizzare il log scelto all'interno della finestra dell'editor di testo, come Notepad.

Scarica il pulsante

Questo pulsante ti permette di scaricare il registro nella tua memoria locale per visualizzarlo in seguito.

L'icona Cog

Cliccando su questa icona si accede alla sezione W3C Log Settings situata in System > Logging. Ne parleremo in dettaglio nella sezione Registrazione della guida.

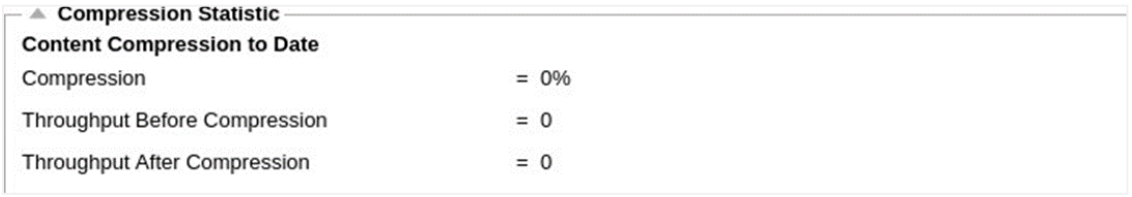
Statistiche

La sezione Statistiche dell'ADC è un'area molto usata dagli amministratori di sistema che vogliono assicurarsi che le prestazioni dell'ADC siano all'altezza delle loro aspettative.

Compressione

L'intero scopo dell'ADC è quello di monitorare i dati e indirizzarli ai Real Server configurati per riceverli. La funzione di compressione è fornita nell'ADC per aumentare le prestazioni dell'ADC. Ci saranno momenti in cui gli amministratori vorranno testare e controllare le informazioni sulla compressione dei dati dell'ADC; questi dati sono forniti dal pannello Compressione all'interno di Statistiche.

Compressione dei contenuti fino ad oggi



I dati mostrati in questa sezione dettagliano il livello di compressione raggiunto dall'ADC sul contenuto comprimibile. Un valore del 60-80% è quello che definiremmo tipico

Compressione complessiva fino ad oggi

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

I valori forniti in questa sezione riportano quanta compressione l'ADC ha raggiunto su tutti i contenuti. Una percentuale tipica per questo dipende da quante immagini precompresse sono contenute nei tuoi servizi. Maggiore è il numero di immagini, minore sarà probabilmente la percentuale di compressione complessiva.

Ingresso/uscita totale

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

Le cifre Total Input/Output rappresentano la quantità di dati grezzi attraversati dentro e fuori l'ADC. L'unità di misura cambia man mano che la dimensione cresce da kbps a Mbps a Gbps.

Colpi e collegamenti

Hits and Connections

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

La sezione Hits and Connections contiene le statistiche complessive per gli hit e le transazioni che passano attraverso l'ADC. Che cosa significano quindi gli hit e le connessioni?

- Un Hit è definito come una transazione di livello 7. Tipicamente usata per i server web, questa è una richiesta GET per un oggetto come un'immagine.
- Una connessione è definita come una connessione TCP di livello 4. Molte transazioni possono avvenire su 1 connessione TCP.

Colpi complessivi contati

Le cifre all'interno di questa sezione mostrano il numero cumulativo di hit non in cache dall'ultimo reset. Sul lato destro, la figura mostrerà il numero attuale di hit al secondo.

Connessioni totali

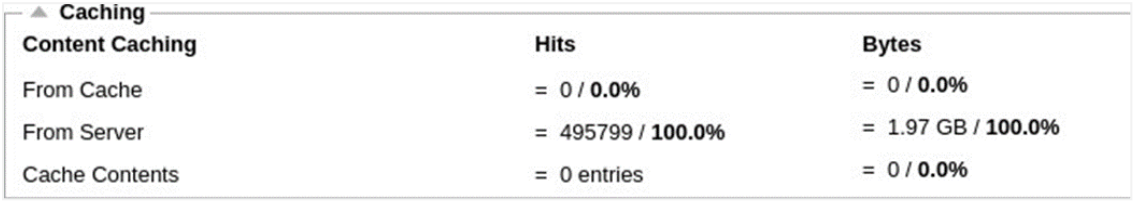
Il valore Total Connections rappresenta il numero cumulativo di connessioni TCP dall'ultimo reset. Il numero nella seconda colonna indica le connessioni TCP fatte al secondo verso l'ADC. Il numero nella colonna di destra è il numero di connessioni TCP al secondo effettuate verso i Real Server. Esempio 6/8 connessioni/sec. Abbiamo 6 connessioni TCP al secondo verso il servizio virtuale e 6 connessioni TCP al secondo verso i Real Server nell'esempio mostrato.

Connessioni di picco

Il valore di picco Connections rappresenta il numero massimo di connessioni TCP fatte all'ADC. Il numero sulla colonna più a destra indica il numero attuale di connessioni TCP attive.

Caching

Come ricorderai, l'ADC è dotato sia di compressione che di caching. Questa sezione mostra le statistiche complessive relative al caching quando è applicato a un canale. Se il caching non è stato applicato a un canale e configurato correttamente, vedrai 0 contenuti della cache.



Dalla cache

Colpi: La prima colonna dà il numero totale di transazioni servite dalla cache ADC dall'ultimo reset. Viene anche fornita una percentuale delle transazioni totali.

Bytes: La seconda colonna dà la quantità totale di dati in Kilobyte serviti dalla cache ADC. Viene anche fornita una percentuale dei dati totali.

Dal server

Colpi: La colonna 1 fornisce il numero totale di transazioni servite dai Real Server dall'ultimo reset. Viene anche fornita una percentuale delle transazioni totali.

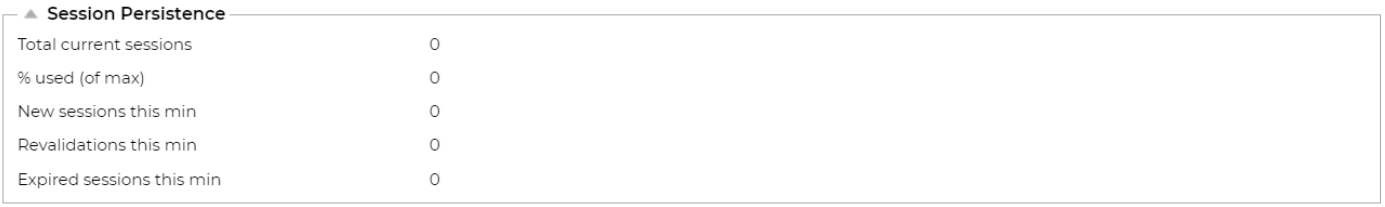
Bytes: La seconda colonna fornisce la quantità totale di dati in Kilobyte serviti dai Real Server. Viene anche fornita una percentuale dei dati totali.

Contenuto della cache

Hits: Questo numero dà il numero totale di oggetti contenuti nella cache ADC.

Bytes: Il primo numero dà la dimensione complessiva in Megabyte degli oggetti della cache ADC. Viene anche fornita una percentuale della dimensione massima della cache.

Persistenza della sessione



La sezione Session Persistence fornisce informazioni per diversi parametri.

Campo	Descrizione
Totale sessioni attuali	Questo mostra quante sessioni di persistenza sono in corso - aggiornate ogni minuto
% Usato (di max)	Questo mostra quanto è utilizzato lo spazio totale consentito per le informazioni di sessione
Nuova sessione questo min	Questo mostra, nell'ultimo minuto, quante nuove sessioni di persistenza sono state aggiunte
Convalidare questo min	Questo mostra, nell'ultimo minuto, quante sessioni di persistenza esistenti sono state riconvalidate da più traffico
Sessioni scadute questo min	Questo mostra, nell'ultimo minuto, quante sessioni di persistenza esistenti sono scadute a causa dell'assenza di ulteriore traffico entro il timeout

Hardware

Sia che tu stia usando l'ADC in un ambiente virtuale o all'interno dell'hardware, questa sezione ti fornirà informazioni preziose sulle prestazioni dell'apparecchio.

Uso del disco

Il valore fornito nella colonna 2 dà la percentuale di spazio su disco attualmente utilizzato e include informazioni sui file di log e sui dati di cache, che vengono periodicamente memorizzati sullo storage.

Uso della memoria

La seconda colonna dà la percentuale di memoria attualmente utilizzata. Il numero più significativo tra parentesi è la quantità totale di memoria assegnata all'ADC. Si raccomanda di assegnare all'ADC un minimo di 2GB di RAM.

Uso della CPU

Uno dei valori critici forniti è la percentuale di CPU attualmente utilizzata da ADC. È naturale che questa fluttui.

Stato

La pagina View > Status mostra il traffico live che attraversa l'ADC per i servizi virtuali che hai definito. Mostra anche il numero di connessioni e dati per ogni Real Server in modo da poter sperimentare il bilanciamento del carico in tempo reale.

Dettagli del servizio virtuale

Colonna VIP

Il colore della luce indica lo stato dell'indirizzo IP virtuale associato a uno o più servizi virtuali.

Stato	Descrizione
●	Online
●	Failover-Standby. Questo servizio virtuale è hot-standby
●	Indica che un "passivo" sta aspettando un "attivo".
●	Offline. I server reali non sono raggiungibili, o nessun server reale è abilitato
●	Trovare lo stato
●	IP virtuali non concessi in licenza o concessi in licenza superati

Colonna di stato VS

Il colore della luce indica lo stato del servizio virtuale.

Stato	Descrizione
●	Online
●	Failover-Standby. Questo servizio virtuale è hot-standby
●	Indica che un "passivo" sta aspettando un "attivo".
●	Il servizio ha bisogno di attenzione. Questa indicazione di stato può derivare da un Real Server che fallisce un controllo di salute o è stato cambiato manualmente in Offline. Il traffico continuerà a fluire ma con una capacità ridotta del Real Server.
●	Offline. I server reali non sono raggiungibili, o nessun server reale è abilitato
●	Trovare lo stato
●	IP virtuali non concessi in licenza o concessi in licenza superati

Nome

Il nome del servizio virtuale

Servizio virtuale (VIP)

L'indirizzo IP virtuale e la porta per il servizio e l'indirizzo che gli utenti o le applicazioni useranno.

Colpo/Sec

Layer 7 transazioni al secondo sul lato client.

Cache%

La cifra fornita qui rappresenta la percentuale di oggetti che sono stati serviti dalla cache RAM dell'ADC.

Compressione

Questa cifra rappresenta la percentuale di oggetti che sono stati compressi tra il client e l'ADC.

Stato RS (Server remoto)

La tabella seguente illustra il significato dello stato dei Real Server collegati al VIP.

Stato	Descrizione
●	Collegato
●	Non monitorato
●	Scarico o Offline
●	Standby
●	Non collegato
●	Trovare lo stato
●	IP virtuali non concessi in licenza o concessi in licenza superati

Server reale

L'indirizzo IP e la porta del Real Server.

Note

Questo valore può essere qualsiasi nota utile per far capire agli altri lo scopo della voce.

Conns (Connessioni)

Rappresentare il numero di connessioni ad ogni Real Server ti permette di vedere il bilanciamento del carico in azione. Molto utile per verificare che la tua politica di bilanciamento del carico funzioni correttamente.

Dati

Il valore in questa colonna mostra la quantità di dati inviati a ciascun Real Server.

Req/Sec (richieste al secondo)

Il numero di richieste al secondo inviate ad ogni Real Server.

Sistema

Il segmento System dell'interfaccia utente dell'ADC vi permette di accedere e controllare tutti gli aspetti del sistema dell'ADC.

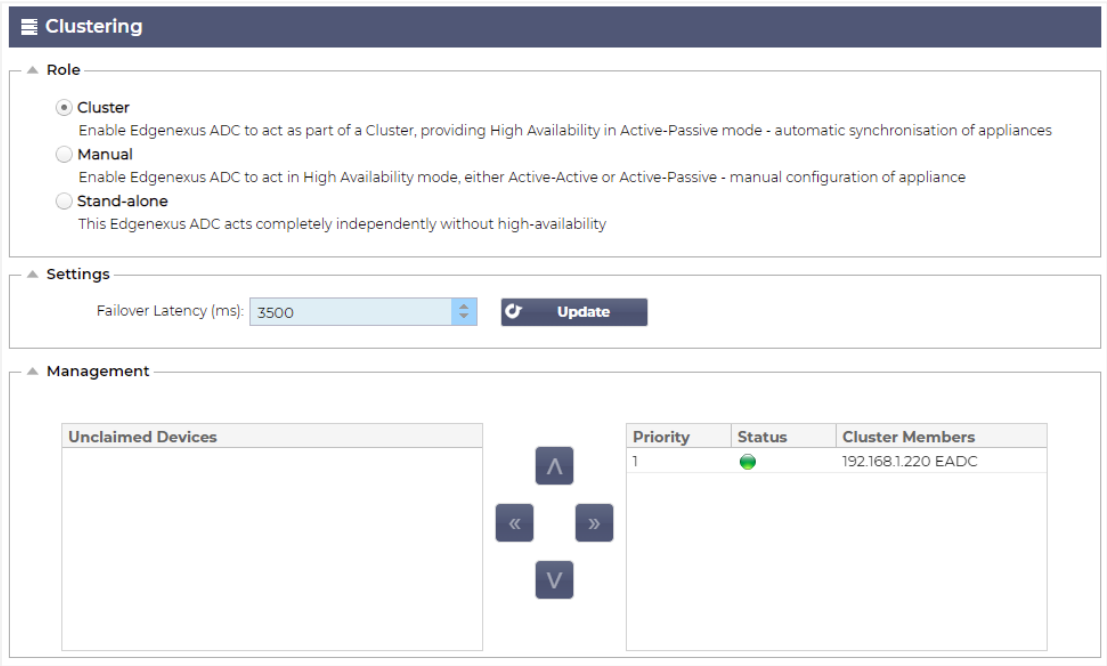
Clustering

L'ADC può essere usato come un singolo dispositivo stand-alone, e funzionerà perfettamente bene. Tuttavia, quando si considera che lo scopo dell'ADC è quello di bilanciare il carico di insiemi di server, la necessità di raggruppare l'ADC stesso diventa evidente. Il design dell'interfaccia utente dell'ADC, facilmente navigabile, rende la configurazione del sistema di clustering molto semplice.

La pagina Sistema > Clustering è dove configurerai l'alta disponibilità dei tuoi apparecchi ADC. Questa sezione è organizzata in diverse sezioni.

Nota importante

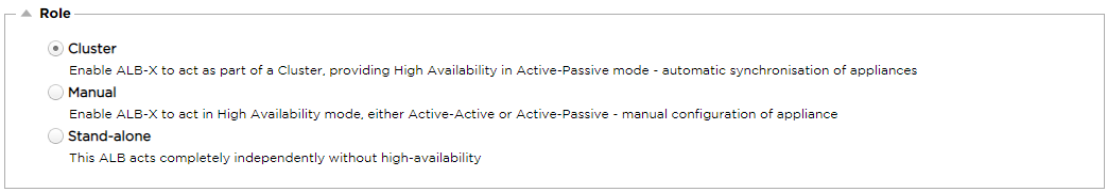
- Non c'è bisogno di un cavo dedicato tra la coppia ADC per mantenere un heartbeat ad alta disponibilità.
- L'heartbeat avviene sulla stessa rete del servizio virtuale che richiede un'alta disponibilità.
- Non c'è uno stateful fail-over tra gli apparecchi ADC.
- Quando l'alta disponibilità è abilitata su due o più ADC, ogni box trasmetterà via UDP i servizi virtuali che è configurato per fornire.
- Il fail-over ad alta disponibilità utilizza la messaggistica unicast e il Gratuitous ARP per informare i nuovi switch del bilanciatore di carico Active.



Ruolo

Ci sono tre ruoli di cluster disponibili quando si configura l'ADC per l'alta disponibilità.

Cluster



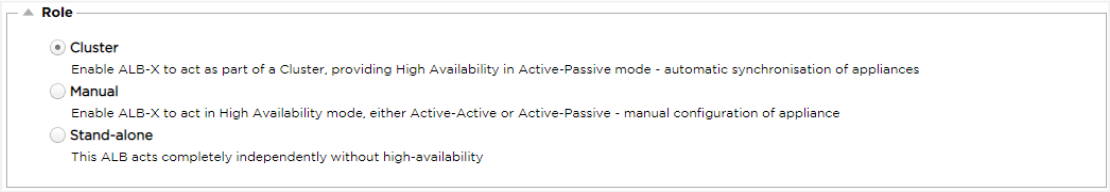
- Per impostazione predefinita, un nuovo ADC si accende utilizzando il ruolo Cluster. In questo ruolo, ogni membro del cluster avrà la stessa "configurazione di lavoro", e come tale, solo un ADC nel cluster sarà attivo in qualsiasi momento.
- Una "configurazione di lavoro" significa tutti i parametri di configurazione, tranne gli elementi che devono essere unici come l'indirizzo IP di gestione, il nome ALB, le impostazioni di rete, i dettagli dell'interfaccia e così via.
- L'ADC in priorità 1, la posizione più alta, della casella Membri del cluster è il proprietario del cluster e il bilanciatore di carico attivo, mentre tutti gli altri ADC sono membri passivi.
- Puoi modificare qualsiasi ADC nel cluster, e le modifiche saranno sincronizzate a tutti i membri del cluster.
- Quando si rimuove un ADC dal cluster, tutti i servizi virtuali saranno cancellati da quell'ADC.
- Non è possibile rimuovere l'ultimo membro del cluster in Dispositivi non reclamati. Per rimuovere l'ultimo membro, cambia il ruolo in Manual o Stand-alone.
- I seguenti oggetti non sono sincronizzati:
    - Sezione data e ora manuale - (la sezione NTP è sincronizzata)
    - Latenza di failover (ms)
    - Sezione hardware
    - Sezione apparecchiatura
    - Sezione rete

Fallimento del proprietario del cluster

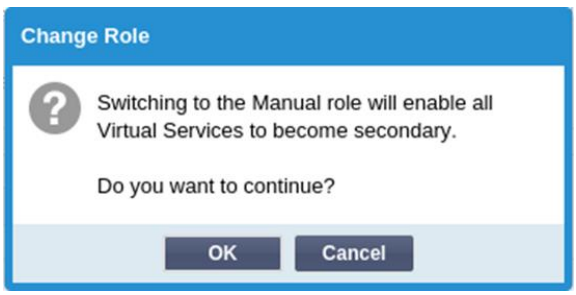
- Quando il proprietario di un cluster fallisce, uno dei membri rimanenti subentrerà automaticamente e continuerà a bilanciare il traffico.
- Quando il proprietario del cluster ritorna, riprenderà il traffico di bilanciamento del carico e assumerà il ruolo di proprietario.
- Supponiamo che il proprietario sia fallito e che un membro abbia assunto il bilanciamento del carico. Se vuoi che il membro che ha preso il controllo del traffico di bilanciamento del carico diventi il nuovo proprietario, evidenzia il membro e clicca sulla freccia in alto per spostarlo nella posizione di priorità 1.
- Se si modifica uno dei membri del cluster rimanenti e il proprietario è giù, il membro modificato si promuoverà automaticamente al proprietario senza perdita di traffico

Cambiare il ruolo da Cluster a Manuale

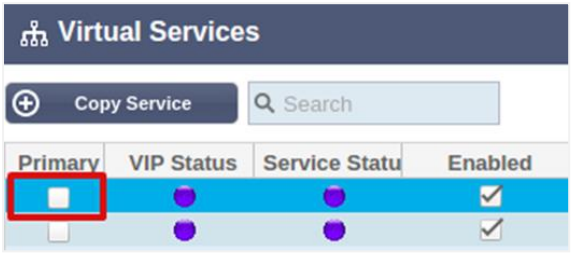
- Se vuoi cambiare il ruolo da Cluster a Manuale, fai clic sul pulsante di opzione accanto all'opzione del ruolo Manuale



- Dopo aver fatto clic sul pulsante radio, vedrete il seguente messaggio:



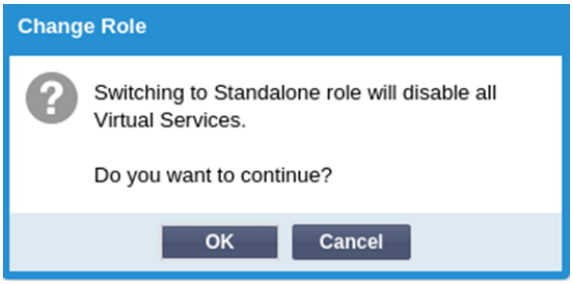
- Fare clic sul pulsante OK
- Controllate la sezione Servizi virtuali. Troverete che la colonna Primary ora mostra una casella non spuntata.



- È una caratteristica di sicurezza e significa che se avete un altro ADC con gli stessi servizi virtuali, allora non ci sarà alcuna interruzione del flusso di traffico.

Cambiare ruolo da Cluster a Stand-alone

- Se vuoi cambiare il ruolo da Cluster a Stand-alone, clicca sul pulsante radio accanto all'opzione Standalone.
- Vi verrà richiesto il seguente messaggio:



- Fare clic su OK per cambiare i ruoli.
- Controllate i vostri servizi virtuali. Vedrete che la colonna Primary cambia nome in Stand-alone
- Vedrete anche che tutti i servizi virtuali sono disabilitati (non spuntati) per ragioni di sicurezza.
- Una volta che siete sicuri che nessun altro ADC sulla stessa rete ha duplicato i servizi virtuali, potete abilitare ciascuno di essi a turno.

Ruolo manuale

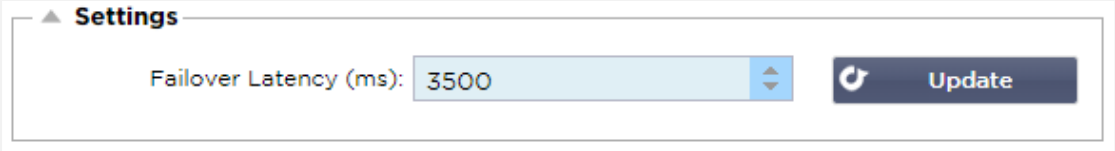
Un ADC nel ruolo Manual lavorerà con altri ADC nel ruolo Manual per fornire alta disponibilità. Il vantaggio principale rispetto al ruolo Cluster è la possibilità di impostare quale ADC è attivo per un IP virtuale. Lo svantaggio è che non c'è sincronizzazione della configurazione tra gli ADC. Qualsiasi cambiamento deve essere replicato manualmente su ogni box tramite la GUI, o per molti cambiamenti, è possibile creare un jetPACK da un ADC e inviarlo all'altro.

- Per rendere un indirizzo IP virtuale "attivo", spuntare la casella di controllo nella colonna primaria (pagina Servizi IP)
- Per rendere un indirizzo IP virtuale "passivo", lasciate la casella vuota nella colonna primaria (pagina Servizi IP)
- Nel caso in cui un servizio attivo fallisca su quello passivo:
    - Se entrambe le colonne primarie sono spuntate, allora ha luogo un processo di elezione e l'indirizzo MAC più basso sarà attivo
    - Se entrambi sono deselezionati, allora ha luogo lo stesso processo di elezione. Inoltre, se entrambi sono deselezionati, non c'è un fallback automatico all'ADC attivo originale.

Ruolo autonomo

Un ADC nel ruolo Stand-alone non comunicherà con nessun altro ADC per quanto riguarda i suoi servizi, e quindi tutti i servizi virtuali rimarranno in stato verde e connessi. Dovete assicurarvi che tutti i servizi virtuali abbiano indirizzi IP unici, o ci sarà uno scontro sulla vostra rete.

Impostazioni

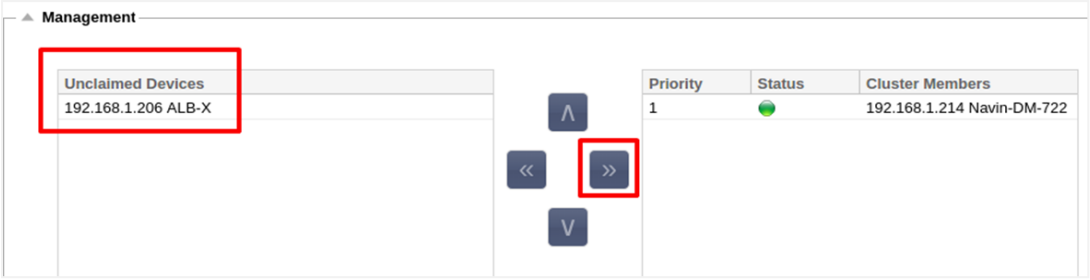


Nella sezione Settings, si può impostare la Failover Latency in millisecondi, il tempo che un ADC passivo aspetterà prima di prendere in consegna i servizi virtuali dopo che l'ADC attivo è fallito.

Raccomandiamo di impostarlo a 10000ms o 10 secondi, ma potete diminuire o aumentare questo valore per adattarlo alla vostra rete e alle vostre esigenze. I valori accettabili sono compresi tra 1500ms e 20000ms. Se sperimenti instabilità nel cluster con una latenza inferiore, dovresti aumentare questo valore.

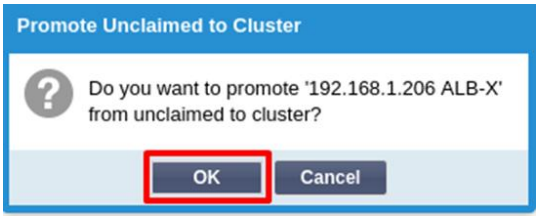
Gestione

In questa sezione, potete aggiungere e rimuovere i membri del cluster e anche cambiare la priorità di un ADC nel cluster. La sezione consiste di due pannelli e una serie di tasti freccia nel mezzo. L'area a sinistra è quella dei dispositivi non reclamati, mentre l'area più a destra è il cluster stesso.

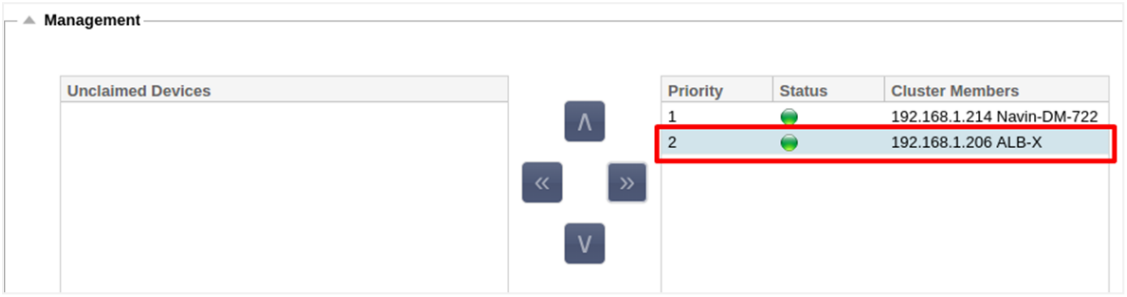


Aggiungere un ADC al cluster

- Prima di aggiungere l'ADC al cluster, è necessario assicurarsi che tutte le appliance ADC siano state dotate di un nome unico impostato nella sezione Sistema > Rete.
- Dovresti vedere l'ADC come priorità 1 con stato verde e il suo nome sotto la colonna dei membri del cluster nella sezione di gestione. Questo ADC è l'apparecchio primario predefinito.
- Tutti gli altri ADC disponibili appariranno nella finestra Unclaimed Devices nella sezione di gestione. Un Unclaimed Device è l'ADC che è stato assegnato nel Cluster Role ma non ha configurato alcun servizio virtuale.
- Evidenziate l'ADC dalla finestra Unclaimed Devices e cliccate sul pulsante con la freccia destra.
- Ora vedrete il seguente messaggio:

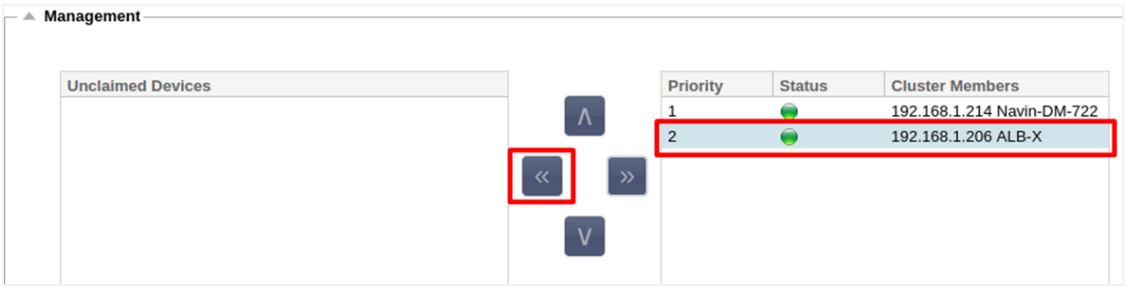


- Fate clic su OK per promuovere l'ADC al cluster.
- Il tuo ADC dovrebbe ora apparire come Priority 2 nell'elenco dei membri del cluster.



Rimozione di un membro del cluster

- Evidenzia il membro del cluster che vuoi rimuovere dal cluster.
- Fare clic sul pulsante con la freccia sinistra.



- Vi verrà presentata una richiesta di conferma.
- Fare clic su OK per confermare.
- Il tuo ADC verrà rimosso e sarà mostrato sul lato Unclaimed Devices.

Cambiare la priorità di un ADC

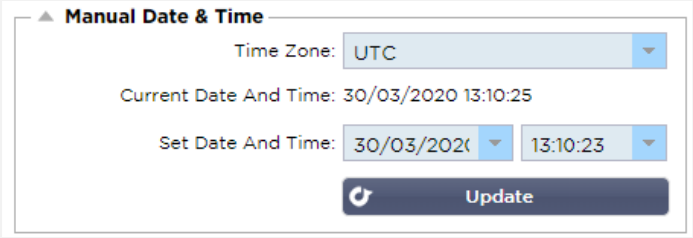
Ci possono essere momenti in cui vuoi cambiare la priorità di un ADC nella lista dei membri.

- L'ADC in cima all'elenco dei membri del cluster ha priorità 1 ed è l'ADC attivo per tutti i servizi virtuali
- L'ADC che è secondo nella lista ha la priorità 2 ed è l'ADC passivo per tutti i servizi virtuali
- Per cambiare quale ADC è attivo, basta evidenziare l'ADC e cliccare sulla freccia in alto fino a quando è in cima alla lista

Data e ora

La sezione data e ora permette l'impostazione delle caratteristiche data/ora dell'ADC, compreso il fuso orario in cui si trova l'ADC. Insieme al fuso orario, la data e l'ora giocano un ruolo vitale nei processi crittografici associati alla crittografia SSL.

Data e ora manuali



Fuso orario

Il valore impostato in questo campo rappresenta il fuso orario in cui si trova l'ADC.

- Clicca sulla casella a discesa per il fuso orario e inizia a digitare la tua posizione.
  Per esempio Londra
- Quando iniziate a digitare, l'ADC visualizzerà automaticamente le posizioni contenenti la lettera L.
- Continua a digitare "Lon," e così via - le località elencate si restringeranno a quelle che contengono "Lon". ’
- Se sei, per esempio, a Londra, scegli Europa/Londra per impostare la tua posizione

Se la data e l'ora non sono ancora corrette dopo la modifica di cui sopra, si prega di cambiare la data manualmente

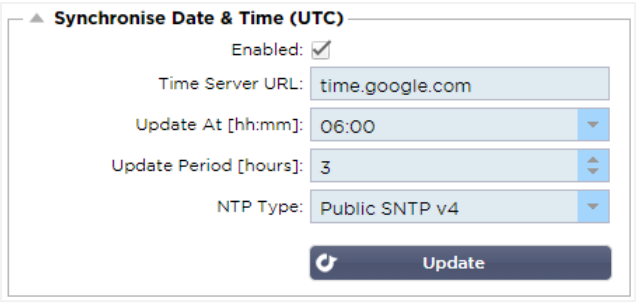
Imposta data e ora

Questa impostazione rappresenta la data e l'ora attuali.

- Scegliere la data corretta dal primo menu a tendina o,
  in alternativa, puoi digitare la data nel seguente formato GG/MM/AAAA
- Aggiungete l'ora nel seguente formato hh: mm: ss, per esempio, 06:00:10 per le 6 del mattino e 10 secondi.
- Una volta che l'hai inserito correttamente, clicca su Update per applicare.
- Dovresti quindi vedere la nuova data e ora in caratteri in grassetto.

Sincronizzare data e ora (UTC)

Puoi usare i server NTP per sincronizzare la data e l'ora con precisione. I server NTP si trovano a livello globale, e puoi anche avere il tuo server NTP interno quando la tua infrastruttura ha limitazioni di accesso esterno.



URL del server temporale

Inserisci un indirizzo IP valido o un nome di dominio pienamente qualificato (FQDN) per il server NTP. Se il server è un server situato globalmente su Internet, si raccomanda di usare un FQDN.

Aggiornamento alle [hh:mm]

Seleziona l'ora programmata alla quale vuoi che l'ADC si sincronizzi con il server NTP.

Periodo di aggiornamento [ore]:

Seleziona la frequenza con cui vuoi che la sincronizzazione avvenga.

Tipo NTP:

- Public SNTP V4 - Questo è il metodo corrente e preferito quando si sincronizza con un server NTP. **RFC 5905**
- NTP v1 Over TCP - versione legacy di NTP su TCP. **RFC 1059**
- NTP v1 Over UDP - versione legacy di NTP su UDP. **RFC 1059**

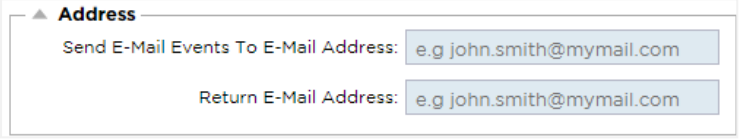
Nota: Si prega di notare che la sincronizzazione è solo in UTC. Se si desidera impostare un'ora locale, questo può essere fatto solo manualmente. Questa limitazione sarà cambiata nelle versioni successive per consentire la possibilità di selezionare un fuso orario.

Eventi e-mail

L'ADC è un apparecchio critico e, come ogni sistema essenziale, è dotato della capacità di informare l'amministrazione dei sistemi di qualsiasi problema che possa richiedere attenzione.

La pagina Sistema > Eventi email ti permette di configurare una connessione al server email e inviare notifiche agli amministratori di sistema. La pagina è organizzata nelle sezioni seguenti.

Indirizzo



Inviare a eventi e-mail a indirizzi e-mail

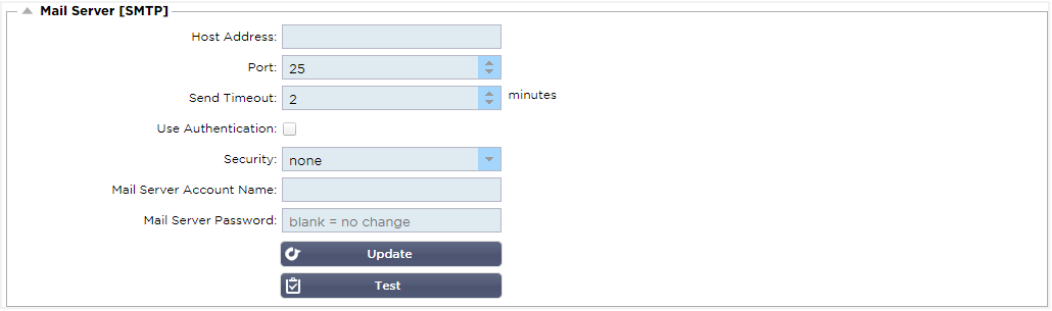
Aggiungi un indirizzo email valido a cui inviare gli avvisi, le notifiche e gli eventi. Esempio support@domain.com. Puoi anche aggiungere più indirizzi email usando un separatore a virgola.

Indirizzo e-mail di ritorno:

Aggiungete un indirizzo email che apparirà nella casella di posta. Esempio adc@domain.com.

Server di posta (SMTP)

In questa sezione, devi aggiungere i dettagli del server SMTP da utilizzare per inviare le e-mail. Assicurati che l'indirizzo email che usi per l'invio sia autorizzato a farlo.



Indirizzo dell'host

Aggiungi l'indirizzo IP del tuo server SMTP.

Porto

Aggiungi la porta del tuo server SMTP. La porta predefinita per SMTP è 25 o 587 se usi SSL.

Inviare timeout

Aggiungi un timeout SMTP. L'impostazione predefinita è di 2 minuti.

Usare l'autenticazione

Spunta la casella se il tuo server SMTP richiede l'autenticazione.

Sicurezza

- Nessuno
- L'impostazione predefinita è none.
- SSL - Usa questa impostazione se il tuo server SMTP richiede l'autenticazione Secure Sockets Layer.
- TLS - Usa questa impostazione se il tuo server SMTP richiede l'autenticazione Transport Layer Security.

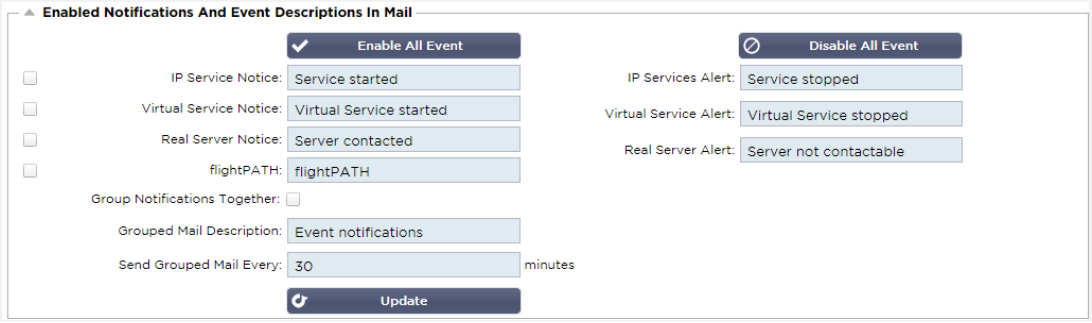
Nome dell'account del server principale

Aggiungete il nome utente richiesto per l'autenticazione.

Password del server di posta

Aggiungete la password richiesta per l'autenticazione.

Notifiche e avvisi



Ci sono diversi tipi di notifiche di eventi che l'ADC invierà alle persone configurate per riceverle. Puoi spuntare e abilitare le notifiche e gli avvisi che devono essere inviati. Le notifiche si verificano quando i Real Server vengono contattati o i canali avviati. Gli avvisi si verificano quando i Real Server non possono essere contattati o i canali smettono di funzionare.

Servizio IP

L'avviso del servizio IP ti informa quando un indirizzo IP virtuale è online o ha smesso di funzionare. Questa azione viene eseguita per tutti i servizi virtuali che appartengono al VIP.

Servizio virtuale

Informa il destinatario che un servizio virtuale è online o ha smesso di funzionare.

Server reale

Quando un Real Sever e una porta sono collegati o non sono contattabili, l'ADC invia un avviso al Real Server.

flightPATH

Questo avviso è un'e-mail inviata quando una condizione è stata soddisfatta, e c'è un'azione configurata che istruisce l'ADC a inviare l'evento via e-mail.

Notifiche di gruppo

Spunta per raggruppare le notifiche. Con questo segno di spunta, tutte le notifiche e gli avvisi saranno aggregati in un'unica e-mail.

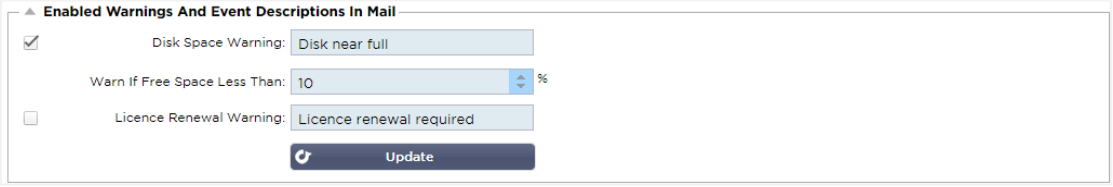
Descrizione della posta di gruppo

Specificare l'oggetto rilevante per l'e-mail di avviso del gruppo.

Intervallo di invio del gruppo

Stabilire la quantità di tempo che si desidera attendere prima di inviare un'e-mail di notifica di gruppo. Il tempo minimo è di 2 minuti.

Avvertenze



Ci sono due tipi di email di avvertimento, e nessuno dei due dovrebbe essere ignorato.

Spazio su disco

Imposta la percentuale di spazio libero su disco prima della quale viene inviato l'avviso. Quando questa viene raggiunta, ti verrà inviata un'email.

Scadenza della licenza

Questa impostazione permette di abilitare o disabilitare l'email di avviso di scadenza della licenza inviata all'amministratore del sistema. Quando questa viene raggiunta, ti verrà inviata un'email.

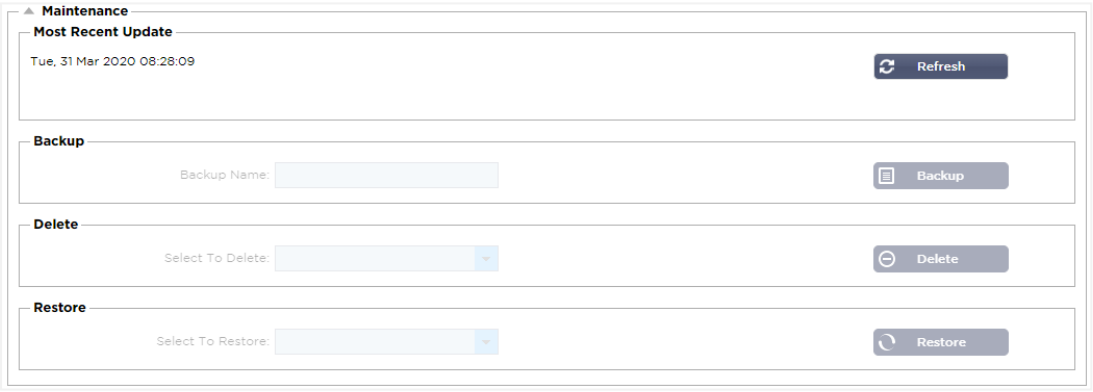
Storia del sistema

Nella sezione Sistema, c'è l'opzione Storia del sistema, che permette la consegna di dati storici per elementi come CPU, memoria, richieste al secondo, e altre caratteristiche. Una volta abilitata, è possibile visualizzare i risultati in forma grafica tramite la pagina View > History. Questa pagina vi permetterà anche di eseguire il backup o il ripristino dei file della cronologia sull'ADC locale.

Raccogliere dati

- Per abilitare la raccolta dei dati, spuntare la casella di controllo.
- Successivamente, impostare l'intervallo di tempo in cui si desidera che l'ADC raccolga i dati. Questo valore di tempo può variare tra 1-60 secondi.

Manutenzione



Questa sezione sarà grigia se hai abilitato la registrazione storica. Deseleziona la casella di controllo Enabled nella sezione Collect Data e clicca su Update per consentire il mantenimento dei log storici.

Backup

Dai al tuo backup un nome descrittivo. Fai clic su Backup per eseguire il backup di tutti i file sull'ADC

Cancellare

Seleziona un file di backup dall'elenco a discesa. Clicca su Elimina per rimuovere il file di backup dall'ADC

Ripristinare

Seleziona un file di backup precedentemente memorizzato. Clicca su Restore per popolare i dati da questo file di backup.

Licenza

L'ADC è concesso in licenza d'uso o utilizzando uno dei seguenti modelli, che dipende dai parametri di acquisto e dal tipo di cliente.

Tipo di licenza	Descrizione
Perpetuo	Lei, il cliente, ha il diritto di usare l'ADC e gli altri software in perpetuo. Ciò non vi impedisce di dover acquistare il supporto per ricevere assistenza e aggiornamenti.
SaaS	SaaS o Software-as-a-Service significa essenzialmente affittare il software su una base continua o pay-as-you-go. In questo modello, si paga un affitto annuale per il software. Non si hanno diritti perpetui per usare il software.
MSP	I Managed Service Provider possono offrire l'ADC come servizio e acquistare la licenza su base per-VIP, addebitata e pagata annualmente.

Dettagli della licenza

Ogni licenza include dettagli specifici pertinenti alla persona o all'organizzazione che la acquista.

ID della licenza

Questo ID di licenza è direttamente collegato all'ID della macchina e ad altri dettagli specifici del tuo acquisto e dell'ADC. Questa informazione è essenziale ed è richiesta quando si desidera recuperare gli aggiornamenti e altri elementi dall'App Store.

ID macchina

L'ID macchina viene generato utilizzando l'indirizzo IP eth0 di un'appliance ADC virtuale e il MAC ID di un ADC basato su hardware. Se cambi l'indirizzo IP di un'appliance ADC virtuale, la licenza non sarà più valida. Dovrai contattare il supporto per l'assistenza. Raccomandiamo che le tue appliance ADC virtuali abbiano indirizzi IP fissi con l'istruzione di non cambiarli. Il supporto tecnico è disponibile sollevando un ticket su HTTPs://edgenexus.io.

Nota: non devi cambiare l'indirizzo IP o il MAC ID dei tuoi apparecchi ADC. Se sei in un quadro virtualizzato, allora fissa il MAC ID e l'indirizzo IP.

Rilasciato a

Questo valore contiene il nome dell'acquirente associato all'ID macchina dell'ADC.

Persona di contatto

Questo valore contiene la persona da contattare presso l'azienda del cliente associata all'ID macchina

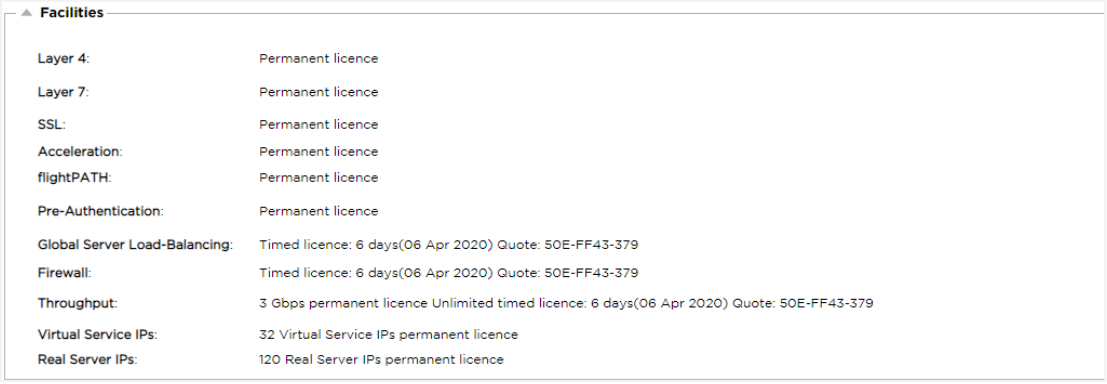
Problemi di data

La data in cui la licenza è stata rilasciata

Nome

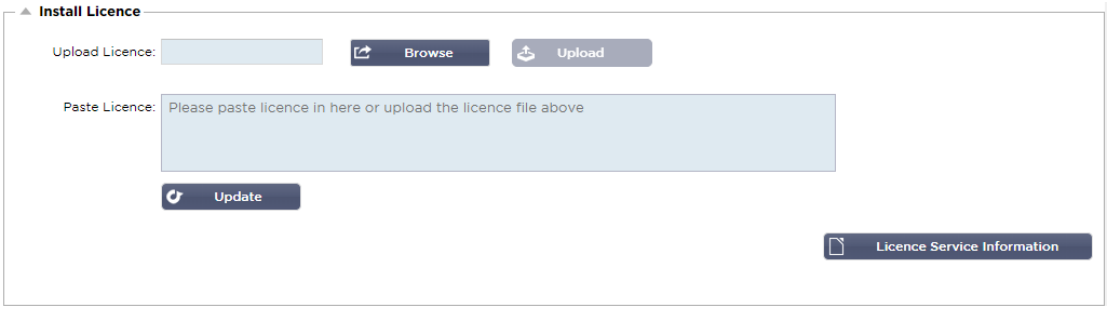
Questo valore mostra il nome descrittivo dell'ADC Appliance che avete fornito.

Strutture



La sezione strutture fornisce informazioni su quali funzioni all'interno dell'ADC sono state concesse in licenza d'uso e la validità della licenza. Viene anche visualizzato il throughput che è stato concesso in licenza per l'ADC e il numero di Real Server. Queste informazioni dipendono dalla licenza che hai acquistato.

Installare le licenze



- Installare una nuova licenza è molto semplice. Quando ricevi la tua licenza nuova o sostitutiva da Edgenexus, ti verrà inviata sotto forma di un file di testo. Puoi aprire il file e poi copiare e incollare il contenuto nel campo Incolla licenza.
- Puoi anche caricarlo sull'ADC se il copia/incolla non è un'opzione per te.
- Una volta fatto questo, cliccate sul pulsante di aggiornamento
- La licenza è ora installata.

Informazioni sul servizio di licenza

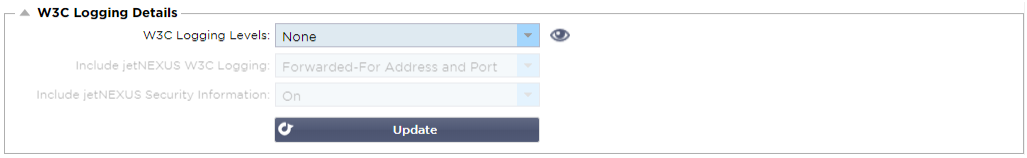
Facendo clic sul pulsante License Service Information si visualizzano tutte le informazioni sulla licenza. Questa funzione può essere utilizzata per inviare i dettagli al personale di supporto.

Registrazione

La pagina Sistema > Registrazione ti permette di impostare i livelli di registrazione W3C e di specificare il server remoto in cui i log saranno esportati automaticamente. La pagina è organizzata nelle quattro sezioni seguenti.

Dettagli di registrazione W3C

Abilitando la registrazione W3C, l'ADC inizierà a registrare un file di log compatibile W3C. Un log W3C è un log di accesso per server Web in cui vengono generati file di testo contenenti dati su ogni richiesta di accesso, tra cui l'indirizzo IP (Internet Protocol) di origine, la versione HTTP, il tipo di browser, la pagina di riferimento e l'orario. Il formato è stato sviluppato dal World Wide Web Consortium (W3C), un'organizzazione che promuove standard per l'evoluzione del Web. Il file è in testo ASCII, con colonne delimitate da spazi. Il file contiene linee di commento che iniziano con il carattere #. Una di queste linee di commento è una linea che indica i campi (fornendo i nomi delle colonne) in modo che i dati possano essere estratti. Ci sono file separati per i protocolli HTTP e FTP.



Livelli di registrazione W3C

Ci sono diversi livelli di registrazione disponibili, e a seconda del tipo di servizio, i dati forniti variano.

La tabella seguente descrive i livelli di registrazione per W3C HTTP.

Valore	Descrizione
Nessuno	La registrazione W3C è disattivata.
Breve	I campi presenti sono: #Campi: 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).
Completo	Questo è un formato più compatibile con i processori, con campi di data e ora separati. Vedi il riassunto dei campi qui sotto per informazioni sul significato dei campi. I campi presenti sono: #Campi: data ora 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).
Sito	Questo formato è molto simile a "Full" ma ha un campo aggiuntivo. Vedi il riassunto dei campi qui sotto per informazioni sul significato dei campi. I campi presenti sono: #Campi: data ora 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).
Diagnostica	Questo formato è pieno di ogni sorta di informazioni rilevanti per lo sviluppo e il personale di supporto. Vedi il riassunto dei campi qui sotto per informazioni sul significato dei campi. I campi presenti sono: campi: data ora 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

La tabella seguente descrive i livelli di registrazione per W3C FTP.

Valore	Descrizione
Breve	Campi: data ora 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
Completo	Campi: data ora 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
Diagnostica	Campi: data ora 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

Includere la registrazione W3C

Questa opzione permette di impostare quali informazioni ADC devono essere incluse nei log W3C.

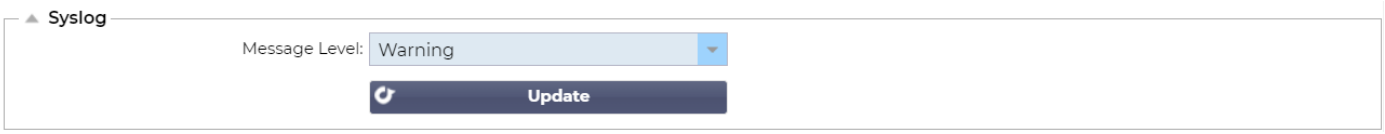
Valore	Descrizione
Indirizzo di rete e porta del cliente	Il valore mostrato qui mostra l'effettivo indirizzo IP del client insieme alla porta.
Indirizzo di rete del cliente	Questa opzione includerà e mostrerà solo l'effettivo indirizzo IP del client.
Indirizzo e porta di inoltro	Questa opzione mostrerà i dettagli contenuti nell'intestazione XFF, inclusi l'indirizzo e la porta.
Indirizzo per l'inoltro	Questa opzione mostrerà i dettagli contenuti nell'intestazione XFF, incluso solo l'indirizzo.

Includi informazioni sulla sicurezza

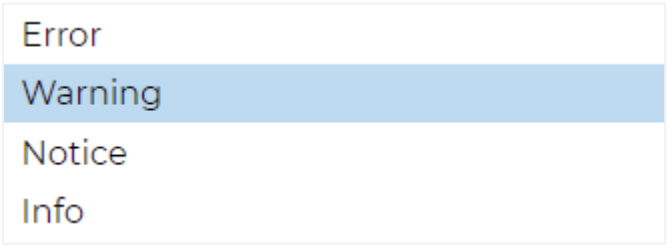
Questo menu consiste in due opzioni:

Valore	Descrizione
Su	Questa impostazione è globale. Quando è impostata su on, il nome utente sarà aggiunto al log W3C quando qualsiasi servizio virtuale sta usando l'autenticazione e ha il log W3C abilitato.
Off	Questo disattiverà la capacità di registrare il nome utente nel registro W3C a livello globale.

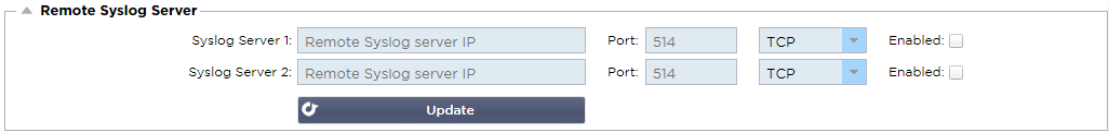
Server Syslog



Questa sezione permette di impostare il livello di registrazione dei messaggi verso il server SYSLOG. Le opzioni disponibili sono le seguenti.



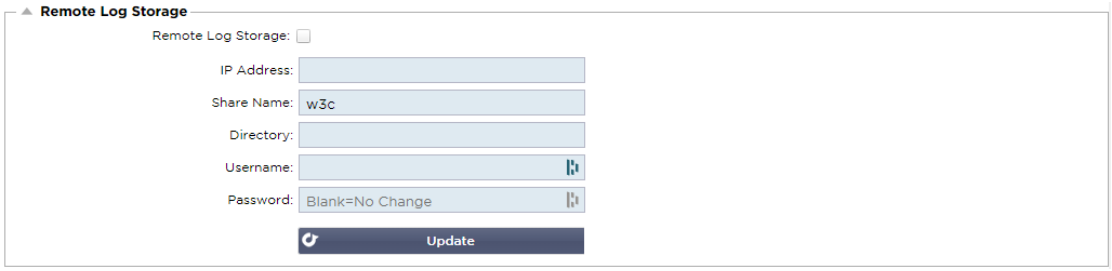
Server Syslog remoto



In questa sezione, è possibile configurare due server Syslog esterni per inviare tutti i log di sistema.

- Aggiungi l'indirizzo IP del tuo server Syslog
- Aggiungere la porta
- Scegliere se si desidera utilizzare TCP o UDP
- Spunta la casella di controllo Enabled per iniziare la registrazione
- Fare clic su Aggiorna

Memorizzazione remota del registro



Tutti i log del W3C sono memorizzati in forma compressa sull'ADC ogni ora. I file più vecchi vengono cancellati quando rimane il 30% dello spazio su disco. Se desideri esportarli su un server remoto per la conservazione, puoi configurarlo usando una condivisione SMB. Si prega di notare che il registro W3C non verrà trasferito alla posizione remota finché il file non sarà stato completato e compresso. Poiché i log vengono scritti ogni ora, questo potrebbe richiedere fino a due ore in un'appliance Virtual Machine e cinque ore per un'appliance hardware.

Col1	**Col2**
Memorizzazione remota del registro	Spunta la casella per abilitare la memorizzazione remota dei registri
Indirizzo IP	Specifica l'indirizzo IP del tuo server SMB. Questo dovrebbe essere in notazione decimale punteggiata. Esempio: 10.1.1.23
Condividi nome	Specificare il nome della condivisione sul server SMB. Esempio: w3c.
Directory	Specificare la directory sul server SMB. Esempio: /log.
Nome utente	Specificare il nome utente per la condivisione SMB.
Password	Specificare la password per la condivisione SMB

Includeremo un pulsante di prova nelle future versioni per fornire un feedback che le tue impostazioni siano corrette.

Riassunto del campo

Condizione	**Descrizione**
Data	Non localizzato = sempre YYYY-MM-DD (GMT/UTC)
Tempo	Non localizzato = HH:MM:SS o HH:MM:SS.ZZZ (GMT/UTC) * Nota: purtroppo questo ha due formati (Sito
	non ha .ZZZ millisecondi)

x-mil	Solo formato sito = millisecondo della marca temporale
c-ip	IP del cliente come meglio può essere derivato dalla rete o dall'intestazione X-Forwarded-For
c-port	Porta del client come meglio può essere derivata dalla rete o dall'intestazione X-Forwarded-For
cs-username	Campo di richiesta del nome utente del cliente
s-ip	Porta di ascolto di ALB
s-port	VIP in ascolto di ALB
x-xff	Valore dell'intestazione X-Forwarded-For
x-xffcustom	Valore dell'intestazione di richiesta di tipo X-Forwarded-For con nome configurato
cs-host	Nome dell'host nella richiesta
x-r-ip	Indirizzo IP del Real Server utilizzato
x-r-port	Porta del server reale utilizzata
cs-method	Metodo di richiesta HTTP * eccetto formato Brief
metodo	Solo il formato breve usa questo nome per cs-method
cs-uri-stem	Percorso della risorsa richiesta * eccetto formato breve
cs-uri-query	Interrogazione per la risorsa richiesta * eccetto formato breve
uri	* il formato breve registra un percorso combinato e una stringa di interrogazione
sc-status	Codice di risposta HTTP
cs(User-Agent)	Stringa User-Agent del browser (come inviata dal client)
referer	Pagina di riferimento (come inviata dal cliente)
x-c-version	Richiesta del cliente versione HTTP
x-r-version	Risposta del server al contenuto Versione HTTP
cs-bytes	Bytes dal cliente, nella richiesta
sr-bytes	Bytes inoltrati al Real Server, nella richiesta
rs-bytes	Bytes dal Real Server, nella risposta
sc-bytes	Bytes inviati al client, nella risposta
x-percentuale	Percentuale di compressione * = 100 * (1 - output / input) comprese le intestazioni
tempo preso	Quanto tempo ha impiegato il Real Server in secondi
x-trip-times nuovo pcon	millisecondo dalla connessione alla pubblicazione nella "lista dei nuovi arrivati". millisecondo dalla connessione al posizionamento della connessione al Real Server
acon	millisecondo dalla connessione al termine del posizionamento della connessione al Real Server
rcon	millisecondo dalla connessione all'instaurazione della connessione con il server reale
rqf	millisecondo dalla connessione alla ricezione del primo byte di richiesta dal client
rql	millisecondo dalla connessione alla ricezione dell'ultimo byte di richiesta dal client
tqf	millisecondo dalla connessione all'invio del primo byte di richiesta al Real Server
tql	millisecondo dalla connessione all'invio dell'ultimo byte di richiesta al Real Server
rsf	millisecondo dalla connessione alla ricezione del primo byte di risposta dal Real Server
rsl	millisecondo dalla connessione alla ricezione dell'ultimo byte di risposta dal Real Server
tsf	millisecondo dalla connessione all'invio del primo byte di risposta al client
tsl	millisecondo dalla connessione all'invio dell'ultimo byte di risposta al client

dis	millisecondo dalla connessione alla disconnessione (entrambi i lati - l'ultimo a disconnettersi)
log	millisecondo dalla connessione a questo record di log di solito seguito da (Politica di bilanciamento del carico e ragionamento)
x-round-trip-time	Quanto tempo ha impiegato ALB in secondi
x-closed-by	Quale azione ha causato la chiusura (o l'apertura) della connessione
x-compress-action	Come la compressione è stata effettuata o impedita
x-sc(Content-Type)	Content-Type della risposta
x-cache-action	Come il caching ha risposto, o è stato impedito
x-finish	Trigger che ha causato questa riga di log

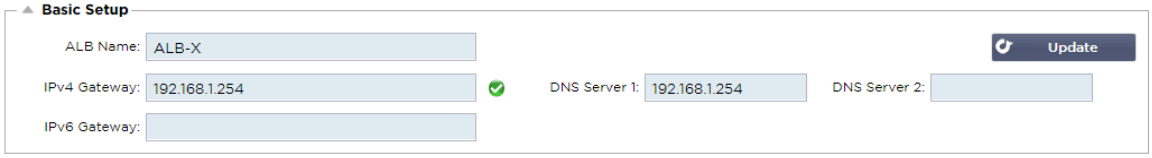
Cancellare i file di registro

Questa funzione permette di cancellare i file di log dall'ADC. Puoi selezionare il tipo di log che vuoi cancellare dal menu a tendina e poi cliccare sul pulsante Clear.

Rete

La sezione Network all'interno della Library permette la configurazione delle interfacce di rete dell'ADC e il loro comportamento.

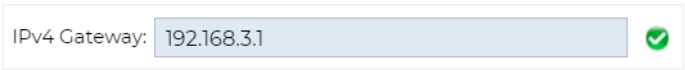
Impostazione di base



Nome ALB

Specifica un nome per la tua appliance ADC. Nota che questo non può essere cambiato se c'è più di un membro nel cluster. Vedi la sezione sul clustering.

Gateway IPv4



Specifica l'indirizzo IPv4 Gateway. Questo indirizzo dovrà essere nella stessa subnet di un adattatore esistente. Se aggiungi il Gateway in modo errato, vedrai una croce bianca in un cerchio rosso. Quando aggiungi un gateway corretto, vedrai un banner verde di successo in fondo alla pagina e un segno di spunta bianco in un cerchio verde accanto all'indirizzo IP.

Gateway IPv6

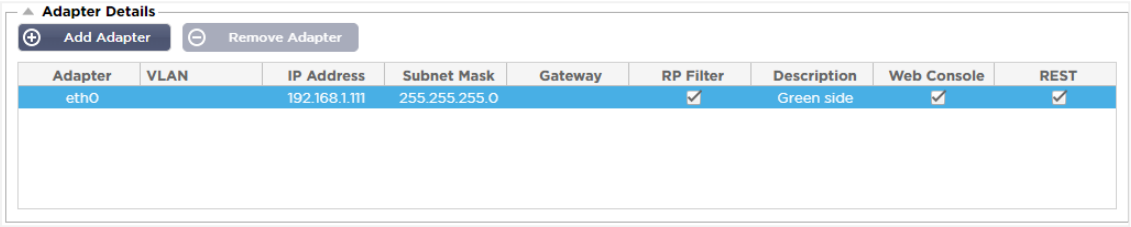
Specifica l'indirizzo IPv6 Gateway. Questo indirizzo dovrà essere nella stessa subnet di un adattatore esistente. Se aggiungi il Gateway in modo errato, vedrai una croce bianca in un cerchio rosso. Quando aggiungi un gateway corretto, vedrai un banner verde di successo in fondo alla pagina e un segno di spunta bianco in un cerchio verde accanto all'indirizzo IP.

Server DNS 1 & Server DNS 2

Aggiungete l'indirizzo IPv4 del vostro primo e secondo server DNS (opzionale).

Dettagli dell'adattatore

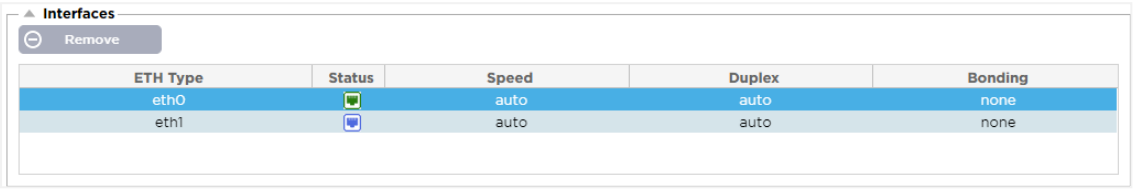
Questa sezione del pannello Network mostra le interfacce di rete che sono installate nella tua appliance ADC. Puoi aggiungere e rimuovere adattatori secondo necessità.



Colonna	**Descrizione**
Adattatore	Questa colonna mostra gli adattatori fisici installati sul tuo apparecchio. Scegli un adattatore dalla lista degli adattatori disponibili facendo clic su di esso - un doppio clic metterà la riga dell'elenco in modalità di modifica.
VLAN	Fai doppio clic per aggiungere l'ID VLAN per l'adattatore. Una VLAN è una Virtual Local Area Network che crea un dominio di trasmissione distinto. Una VLAN ha gli stessi attributi di una LAN fisica, ma permette alle stazioni finali di essere raggruppate più facilmente se non sono sullo stesso switch di rete
Indirizzo IP	Doppio clic per aggiungere l'indirizzo IP associato all'interfaccia dell'adattatore. Puoi aggiungere più indirizzi IP alla stessa interfaccia. Questo dovrebbe essere un numero IPv4 a 32 bit in notazione decimale punteggiata. Esempio 192.168.101.2
Maschera di sottorete	Doppio clic per aggiungere la subnet mask assegnata all'interfaccia dell'adattatore. Questo dovrebbe essere un numero IPv4 a 32 bit in notazione decimale punteggiata. Esempio 255.255.255.0
Gateway	Aggiungere un gateway per l'interfaccia. Quando questo viene aggiunto, l'ADC imposterà una semplice politica che permetterà alle connessioni iniziate da questa interfaccia di essere restituite attraverso questa interfaccia al router gateway specificato. Questo permette all'ADC di essere installato in ambienti di rete più complessi senza il problema di configurare manualmente un routing complesso basato su criteri.
Descrizione	Fate doppio clic per aggiungere una descrizione per il vostro adattatore. Esempio di interfaccia pubblica. Nota: L'ADC nominerà automaticamente la prima interfaccia Lato Verde, la seconda interfaccia Lato Rosso e la terza interfaccia Lato 3 ecc. Sentitevi liberi di cambiare queste convenzioni di denominazione a vostra scelta.
Console web	Fai doppio clic sulla colonna e spunta la casella per assegnare l'interfaccia come indirizzo di gestione per la Graphical User Interface Web Console. Fai molta attenzione quando cambi l'interfaccia su cui ascolterà la console web. Dovrai avere il corretto routing impostato o essere nella stessa subnet della nuova interfaccia per raggiungere la Console Web dopo il cambiamento. L'unico modo per cambiarla di nuovo è accedere alla linea di comando ed emettere il comando set greenside. Questo cancellerà tutte le interfacce tranne eth0.

Interfacce

La sezione Interfacce all'interno del pannello Rete permette la configurazione di alcuni elementi relativi all'interfaccia di rete. Puoi anche rimuovere un'interfaccia di rete dall'elenco facendo clic sul pulsante Remove. Quando usi un dispositivo virtuale, le interfacce che vedi qui sono limitate dal framework di virtualizzazione sottostante.



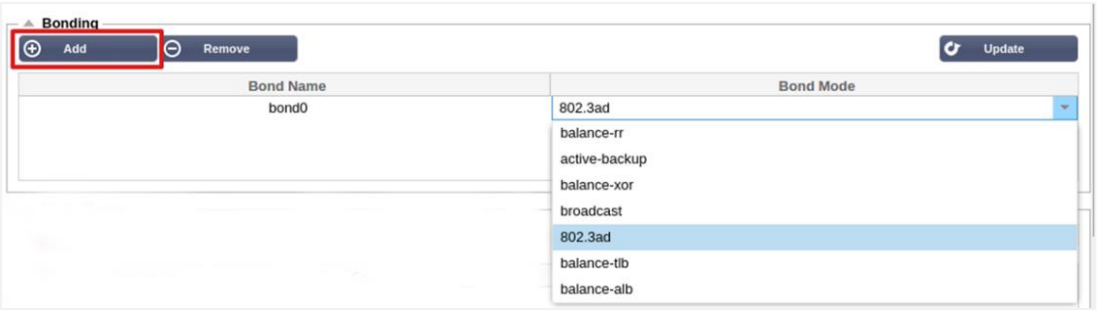
Colonna	Descrizione
Tipo ETH	Questo valore indica il riferimento interno del sistema operativo all'interfaccia di rete. Questo campo non può essere personalizzato. I valori iniziano con ETH0 e continuano in sequenza a seconda del numero di interfacce di rete.
Stato	Questa indicazione grafica mostra lo stato attuale dell'interfaccia di rete. Uno stato verde mostra che l'interfaccia è connessa e attiva. Altri indicatori di stato sono mostrati di seguito. **Adattatore UP** Adattatore giù Adattatore scollegato Adattatore mancante
Velocità	Per default, questo valore è impostato per auto-negoziare la velocità. Ma puoi cambiare la velocità di rete dell'interfaccia con qualsiasi valore disponibile nel menu a tendina (10/100/1000/AUTO).
Duplex	Il valore di questo campo è personalizzabile, e si può scegliere tra Auto (default), Full-Duplex e Half-Duplex.
Incollaggio	Puoi scegliere uno dei tipi di legame che hai definito. Vedi la sezione sui legami per maggiori dettagli.

Incollaggio

Molti nomi sono usati per denominare il bonding dell'interfaccia di rete: Port Trunking, Channel Bonding, Link Aggregation, NIC teaming e altri. Il bonding combina o aggrega più connessioni di rete in un'unica interfaccia a canale vincolato. Il bonding permette a due o più interfacce di rete di agire come una sola, aumentare il throughput e fornire ridondanza o failover.

Il kernel dell'ADC ha un driver Bonding integrato per aggregare più interfacce di rete fisiche in una singola interfaccia logica (per esempio, aggregando eth0 e eth1 in bond0). Per ogni interfaccia bondata, puoi definire la modalità e le opzioni di monitoraggio del collegamento. Ci sono sette diverse opzioni di modalità, ognuna delle quali fornisce specifiche caratteristiche di bilanciamento del carico e tolleranza agli errori. Queste sono mostrate nell'immagine qui sotto.

NOTA: IL BONDING PUÒ ESSERE CONFIGURATO SOLO PER LE APPLIANCE ADC BASATE SU HARDWARE.

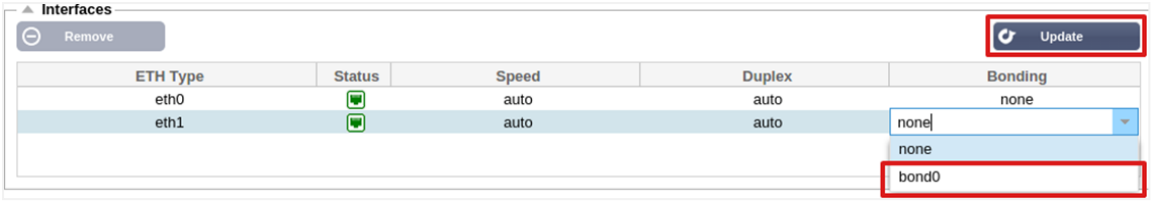


Creare un profilo di legame

- Cliccare su Aggiungi per aggiungere un nuovo legame
- Fornire un nome per la configurazione del bonding
- Scegliere quale modalità di incollaggio si desidera utilizzare

Poi dalla sezione Interfacce, seleziona la modalità di collegamento che vuoi usare dal campo a discesa Collegamento per l'interfaccia di rete.

Nell'esempio qui sotto, eth0, eth1 e eth2 sono ora parte di bond0. Mentre Eth0 rimane da sola come interfaccia di gestione.

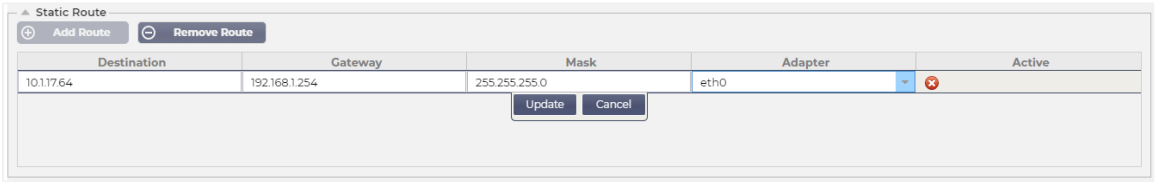


Modalità di legame

Modalità di legame	Descrizione
equilibrio-rr:	I pacchetti sono trasmessi/ricevuti in modo sequenziale attraverso ogni interfaccia uno per uno.
backup attivo:	In questa modalità, un'interfaccia sarà attiva e la seconda interfaccia sarà in standby. Questa interfaccia secondaria diventa attiva solo se la connessione attiva sulla prima interfaccia fallisce.
equilibrio-xor:	Trasmette in base all'indirizzo MAC sorgente XOR'd con l'indirizzo MAC destinazione. Questa opzione seleziona lo stesso slave per ogni indirizzo MAC di destinazione.
trasmissione:	Questa modalità trasmetterà tutti i dati su tutte le interfacce slave.
802.3ad:	Crea gruppi di aggregazione che condividono le stesse impostazioni di velocità e duplex e utilizza tutti gli slave nell'aggregatore attivo seguendo la specifica 802.3ad.
equilibrio-tlb:	La modalità bonding di bilanciamento del carico di trasmissione adattivo: Fornisce il channel bonding che non richiede alcun supporto speciale per lo switch. Il traffico in uscita è distribuito secondo il carico corrente (calcolato rispetto alla velocità) su ogni slave. Lo slave corrente riceve il traffico in entrata. Se lo slave ricevente fallisce, un altro slave prende l'indirizzo MAC dello slave ricevente fallito.
equilibrio-alb:	La modalità bonding Adaptive load balancing: include anche balance-tlb più receive load balancing (rlb) per il traffico IPV4 e non richiede alcun supporto speciale dello switch. Il bilanciamento del carico di ricezione è ottenuto tramite la negoziazione ARP. Il driver di bonding intercetta le risposte ARP inviate dal sistema locale in uscita e sovrascrive l'indirizzo hardware sorgente con l'indirizzo hardware unico di uno degli slave nel bond, in modo tale che diversi peer utilizzino diversi indirizzi hardware per il server.

Rotta statica

Ci saranno momenti in cui avrai bisogno di creare rotte statiche per specifiche sottoreti all'interno della tua rete. L'ADC ti dà la possibilità di fare questo usando il modulo Static Routes.



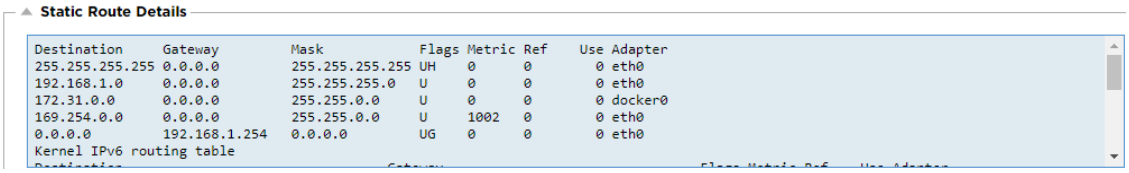
Aggiungere una rotta statica

- Fare clic sul pulsante Aggiungi rotta
- Compila il campo usando i dettagli nella tabella sottostante come guida.
- Clicca il pulsante Update quando hai finito.

Campo	Descrizione
Destinazione	Inserite l'indirizzo di rete di destinazione in notazione decimale punteggiata. Esempio 123.123.123.5
Gateway	Inserite l'indirizzo IPv4 del gateway in notazione decimale punteggiata. Esempio 10.4.8.1
Maschera	Inserite la subnet mask di destinazione in notazione decimale punteggiata. Esempio 255.255.255.0
Adattatore	Inserite l'adattatore su cui il gateway può essere raggiunto. Esempio eth1.
Attivo	Una casella verde indica che il gateway può essere raggiunto. Una croce rossa indicherà che il gateway non può essere raggiunto su quell'interfaccia. Assicurati di aver impostato un'interfaccia e un indirizzo IP sulla stessa rete del gateway

Dettagli delle rotte statiche

Questa sezione fornisce informazioni su tutte le rotte configurate sull'ADC.



Impostazioni di rete avanzate

Cos'è Nagle?

L'algoritmo di Nagle migliora l'efficienza delle reti TCP/IP riducendo il numero di pacchetti che devono essere inviati sulla rete. Vedere l'**ARTICOLO DI WIKIPEDIA SU NAGLE**

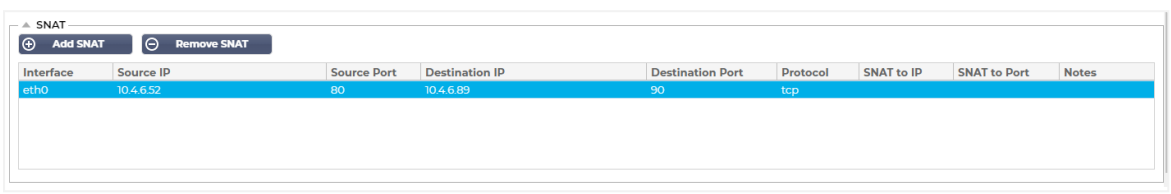
Server Nagle

Spunta questa casella per abilitare l'impostazione Server Nagle. Il Server Nagle è un mezzo per migliorare l'efficienza delle reti TCP/IP riducendo il numero di pacchetti che devono essere inviati sulla rete. Questa impostazione è applicata al lato server della transazione. È necessario prestare attenzione alle impostazioni del server poiché Nagle e ACK ritardati possono avere un forte impatto sulle prestazioni.

Cliente Nagle

Spuntare la casella per attivare l'impostazione Client Nagle. Come sopra, ma applicata al lato cliente della transazione.

SNAT



SNAT sta per Source Network Address Translation, e diversi venditori hanno leggere variazioni nell'implementazione di SNAT. Una semplice spiegazione di EdgeADC SNAT sarebbe la seguente.

In circostanze normali, le richieste in entrata sarebbero dirette al VIP che vedrebbe l'IP di origine della richiesta. Così, per esempio, se un endpoint del browser avesse un indirizzo IP di 81.71.61.51, questo sarebbe visibile al VIP.

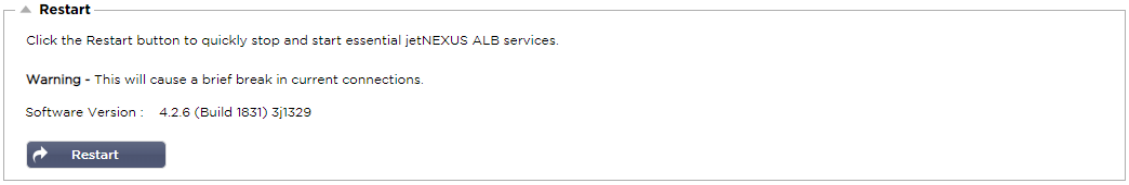
Quando SNAT è in vigore, l'IP di origine originale della richiesta sarà nascosto al VIP, e invece, vedrà l'indirizzo IP come fornito nella regola SNAT. Così, SNAT può essere utilizzato in modalità di bilanciamento del carico Layer 4 e Layer 7.

Campo	Descrizione
Fonte IP	L'indirizzo IP sorgente è opzionale, e può essere sia un indirizzo IP di rete (con /mask) che un indirizzo IP semplice. La maschera può essere sia una maschera di rete che un semplice numero, specificando il numero di 1 a sinistra della maschera di rete. Così, una maschera di /24 è equivalente a 255.255.255.0.
IP di destinazione	L'indirizzo IP di destinazione è opzionale, e può essere un indirizzo IP di rete (con /mask) o un indirizzo IP semplice. La maschera può essere sia una maschera di rete che un semplice numero, specificando il numero di 1 a sinistra della maschera di rete. Così, una maschera di /24 è equivalente a 255.255.255.0.
Fonte Porta	La porta di origine è opzionale, può essere un singolo numero, nel qual caso specifica solo quella porta, o può includere due punti, che specifica un intervallo di porte. Esempi: 80 o 5900:5905.
Porta di destinazione	La porta di destinazione è opzionale, può essere un numero singolo, nel qual caso specifica solo quella porta, o può includere due punti, che specifica un intervallo di porte. Esempi: 80 o 5900:5905.
Protocollo	Potete scegliere se usare SNAT su un solo protocollo o su tutti i protocolli. Suggeriamo di essere specifici per essere più precisi.
Da SNAT a IP	SNAT to IP è un indirizzo IP obbligatorio o un intervallo di indirizzi IP. Esempi: 10.0.0.1 o 10.0.0.1-10.0.0.3.
SNAT a Porta	Lo SNAT to Port è opzionale, può essere un numero singolo, nel qual caso specifica solo quella porta, o può includere un trattino, che specifica un intervallo di porte. Esempi: 80 o 5900-5905.
Note	Usalo per mettere un nome amichevole per ricordarti perché le regole esistono. Questo è anche utile per il debug nel Syslog.

Potenza

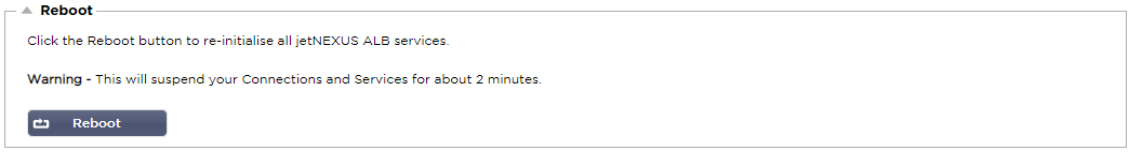
Questa caratteristica del sistema ADC vi permette anche di condurre diversi compiti relativi all'alimentazione sul vostro ADC.

Riavviare



Questa impostazione avvia un riavvio globale di tutti i servizi e di conseguenza interrompe tutte le connessioni attualmente attive. Tutti i servizi riprenderanno automaticamente dopo un breve periodo, ma i tempi dipenderanno da quanti servizi sono configurati. Verrà visualizzato un pop-up che richiede la conferma dell'azione di riavvio.

Riavvio



Cliccando il pulsante Reboot l'ADC verrà spento e riportato automaticamente ad uno stato attivo. Verrà visualizzato un pop-up che richiede la conferma dell'azione di riavvio.

Spegnimento

Facendo clic sul pulsante Power Off si spegne l'ADC. Se questo è un dispositivo hardware, avrai bisogno di un accesso fisico al dispositivo per riaccenderlo. Verrà visualizzato un pop-up che richiede la conferma dell'azione di spegnimento.

Sicurezza

Questa sezione permette di cambiare la password della console web e di abilitare o disabilitare l'accesso Secure Shell. Permette anche l'abilitazione della funzionalità REST API.

SSH

Opzione	Descrizione
Connessione remota Secure Shell	Spunta la casella se vuoi accedere all'ADC usando SSH. "Putty" è un'ottima applicazione per fare questo.

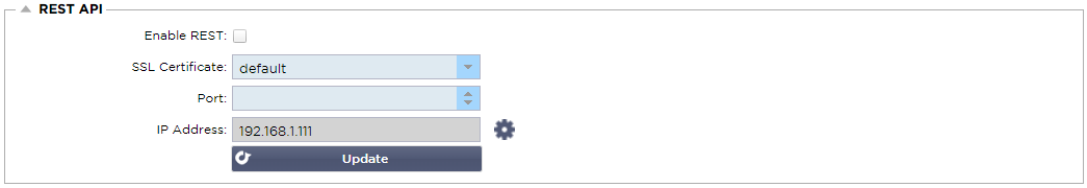
Console web

Certificato SSL Scegli un certificato dall'elenco a discesa. Il certificato che sceglierai sarà usato per proteggere la tua connessione all'interfaccia utente web dell'ADC. Puoi creare un certificato autofirmato all'interno dell'ADC o importarne uno dalla sezione **CERTIFICATI SSL.**

Opzione	Descrizione
Porta sicura	La porta predefinita per la console web è TCP 443. Se vuoi usare una porta diversa per ragioni di sicurezza, puoi cambiarla qui.

API REST

La REST API, conosciuta anche come RESTful API, è un'interfaccia di programmazione di applicazioni che è conforme allo stile architettonico REST e permette la configurazione dell'ADC o l'estrazione di dati dall'ADC. Il termine REST stava per representational state transfer e fu creato dall'informatico Roy Fielding.



Opzione	Descrizione
Abilitare REST	Spunta questa casella per abilitare l'accesso tramite l'API REST. Nota che dovrai anche configurare quale adattatore su cui REST è abilitato. Vedi la nota sul link Cog qui sotto.
Certificato SSL	Scegli un certificato per il servizio REST. Il menu a tendina mostrerà tutti i certificati installati sull'ADC.
Porto	Impostare la porta per il servizio REST. È una buona idea usare una porta diversa da 443.
Indirizzo IP	Questo mostrerà l'indirizzo IP a cui è legato il servizio REST. Puoi cliccare sul link Cog per accedere alla pagina Network per cambiare su quale adattatore il servizio REST è abilitato.
Collegamento a un ingranaggio	Cliccando su questo link si accede alla pagina Network dove è possibile configurare un adattatore per il REST.

Documentazione per REST API

La documentazione su come usare l'API REST è disponibile: **jetAPI | 4.2.3 | jetNEXUS | SwaggerHub**

Nota: se si ottengono errori sulla pagina Swagger è perché hanno un problema nel supportare le stringhe di query
Scorrere oltre gli errori fino a jetNEXUS REST API

Esempi

GUID usando CURL:

- Comando

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

- restituirà

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

- Validità
  - GUID è valido per 24 ore

Dettagli della licenza

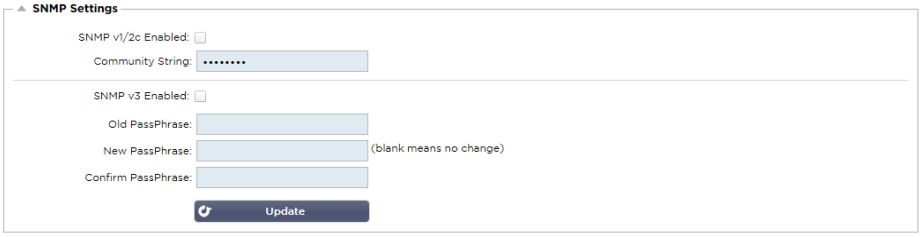
- Comando

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

SNMP

La sezione SNMP permette la configurazione della MIB SNMP che risiede nell'ADC. La MIB può poi essere interrogata da un software di terzi in grado di comunicare con i dispositivi dotati di SNMP.

Impostazioni SNMP



Opzione	Descrizione
SNMP v1/ V2C	Selezionare la casella di controllo per abilitare la MIB V1/V2C. SNMP v1 è conforme a RFC-1157. SNMP V2c è conforme a RFC-1901-1908
SNMP v3	Spuntare la casella di controllo per abilitare la V3 MIB. RFC-3411-3418. Il nome utente per la v3 è admin. Esempio:- snmpwalk -v3 -u admin -A jetnexus -l authNoPriv 192.168.1.11 1.3.6.1.4.1.38370
Stringa della comunità	Questa è la stringa di sola lettura impostata sull'agente e usata dal manager per recuperare le informazioni SNMP. La stringa di comunità predefinita è jetnexus
PassPhrase	Questa è la password necessaria quando SNMP v3 è abilitato e deve essere di almeno 8 caratteri e contenere solo lettere Aa-Zz e numeri 0-9. La passphrase di default è **jetnexus**

MIB SNMP

Le informazioni visualizzabili tramite SNMP sono definite dalla Management Information Base (MIB). Le MIB descrivono la struttura dei dati di gestione e usano degli identificatori gerarchici di oggetti (OID). Ogni OID può essere letto tramite un'applicazione di gestione SNMP.

Scaricare il MIB

Il MIB può essere scaricato qui:

OID ADC

OID RADICE

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

Le nostre OID

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

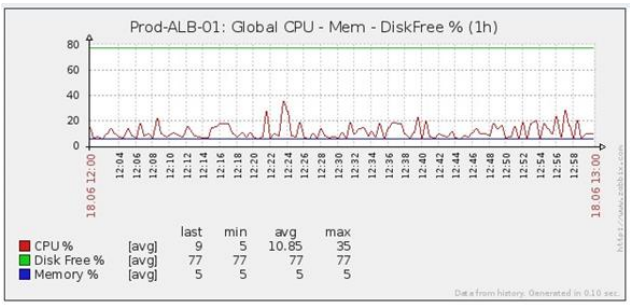
.2 **jetnexusVirtualServices (1**.3.6.1.4.1.38370.1.2)
.1 **jnvirtualserviceEntry (1**.3.6.1.4.1.38370.1.2.1)
.1 **jnvirtualserviceIndexvirtualservice (1**.3.6.1.4.1.38370.1.2.1.**1**)
.2 **jnvirtualserviceVSAddrPort (1**.3.6.1.4.1.38370.1.2.1.**2**)

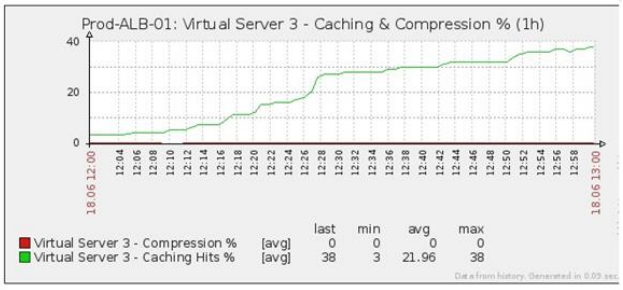
.3 **jnvirtualserviceOverallInputBytes (1**.3.6.1.4.1.38370.1.2.1**.3)**
.4 **jnvirtualserviceOverallOutputBytes (1**.3.6.1.4.1.38370.1.2.1**.4)**
. 5 **jnvirtualserviceCacheBytes (1**.3.6.1.4.1.38370.1.2.1**.5)**
.6 **jnvirtualserviceCompressionPercent (1**.3.6.1.4.1.38370.1.2.1**.6)**
.7 **jnvirtualservicePresentClientConnections (1**.3.6.1.4.1.38370.1.2.1**.7)**
.8 **jnvirtualserviceHitCount (1**.3.6.1.4.1.38370.1.2.1**.8)**
.9 jnvirtualserviceCacheHits (1.3.6.1.4.1.38370.1.2.1**.9)**
. 10 **jnvirtualserviceCacheHitsPercent (1**.3.6.1.4.1.38370.1.2.1**.10)**
.11 **jnvirtualserviceVSStatus (1**.3.6.1.4.1.38370.1.2.1**.11)**

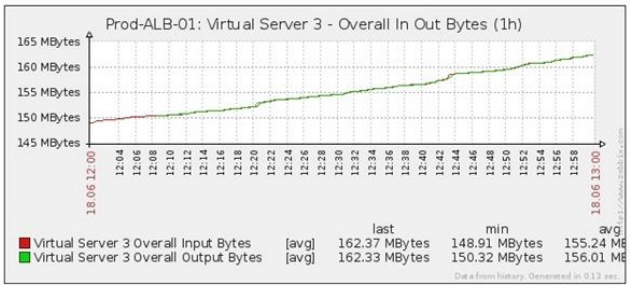
.3 **jetnexusRealServers (1**.3.6.1.4.1.38370.1.3**)**
.1 **jnrealserverEntry (1**.3.6.1.4.1.38370.1.3.**1)**
.1 **jnrealserverIndexVirtualService (1**.3.6.1.4.1.38370.1.3.1.**1)**
.2 **jnrealserverIndexRealServer (1**.3.6.1.4.1.38370.1.3.1.**2)**
.3 **jnrealserverChAddrPort (1**.3.6.1.4.1.38370.1.3.1.**3)**
. 4 **jnrealserverCSAddrPort (1**.3.6.1.4.1.38370.1.3.1.**4)**
.5 **jnrealserverOverallInputBytes (1**.3.6.1.4.1.38370.1.3.1.**5)**
.6 **jnrealserverOverallOutputBytes (1**.3.6.1.4.1.38370.1.3.1.**6)**
.7 **jnrealserverCompressionPercent (1**.3.6.1.4.1.38370.1.3.1.**7)**
.8 **jnrealserverPresentClientConnections (1**.3.6.1.4.1.38370.1.3.1.**8)**
. 9 **jnrealserverPoolUsage (1**.3.6.1.4.1.38370.1.3.1.**9)**
.10 **jnrealserverHitCount (1**.3.6.1.4.1.38370.1.3.1.**10)**
. 11 **jnrealserverRSStatus (1**.3.6.1.4.1.38370.1.3.1.**11)**

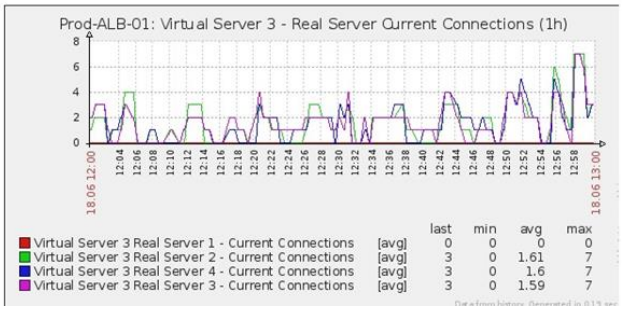
Grafici storici

L'uso migliore della MIB SNMP personalizzata dell'ADC è la capacità di scaricare il grafico storico su una console di gestione di vostra scelta. Di seguito sono riportati alcuni esempi da Zabbix che interrogano un ADC per vari valori OID elencati sopra.









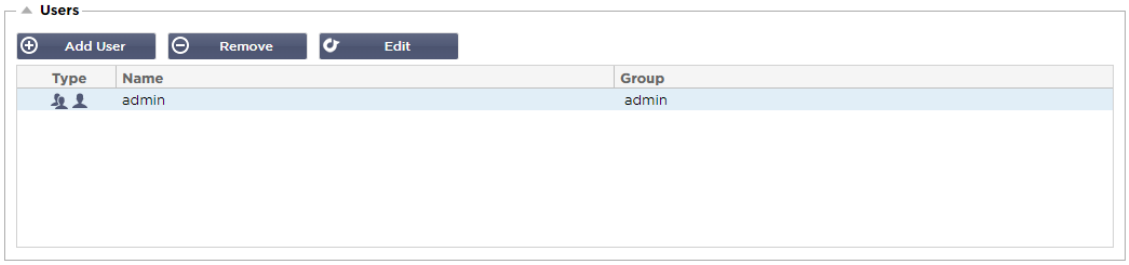
Utenti e registri di controllo

L'ADC fornisce la possibilità di avere un insieme interno di utenti per configurare e definire ciò che l'ADC fa. Gli utenti definiti all'interno dell'ADC possono eseguire una varietà di operazioni a seconda del ruolo collegato a loro.

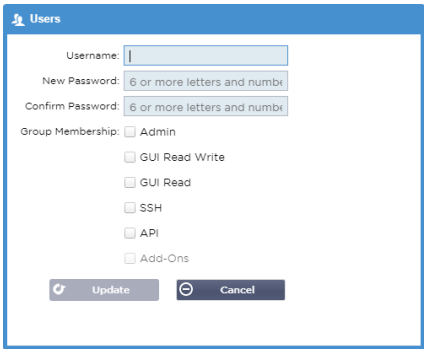
C'è un utente predefinito chiamato **admin** che si usa quando si configura l'ADC per la prima volta. La password di default per admin è **jetnexus**.

Utenti

La sezione Utenti ti permette di creare, modificare e rimuovere utenti dall'ADC.



Aggiungi utente



Fai clic sul pulsante Add User mostrato nell'immagine qui sopra per far apparire la finestra di dialogo Add User.

Parametro	**Descrizione/Utilizzo**
Nome utente	Inserisci un nome utente di tua scelta Il nome utente deve essere conforme a quanto segue: • Numero minimo di caratteri 1 • Numero massimo di caratteri 32 • Le lettere possono essere maiuscole e minuscole • I numeri possono essere usati • I simboli non sono ammessi
Password	Inserisci una password **forte** che sia conforme ai seguenti requisiti • Numero minimo di caratteri 6 • Numero massimo di caratteri 32 • Deve usare almeno una combinazione di lettere e numeri • Le lettere possono essere maiuscole o minuscole • I simboli sono permessi tranne quelli dell'esempio seguente **£**, **%**, **&** , **<** , **>**
Conferma la password	Confermare di nuovo la password per assicurarsi che sia corretta
Appartenenza al gruppo	Spunta il gruppo a cui vuoi che l'utente appartenga. • Admin - Questo gruppo può fare tutto • GUI Read Write - Gli utenti di questo gruppo possono accedere alla GUI e apportare modifiche tramite la GUI • GUI Read - Gli utenti di questo gruppo possono accedere alla GUI solo per visualizzare le informazioni. Nessuna modifica può essere fatta • SSH - Gli utenti di questo gruppo possono accedere all'ADC tramite Secure Shell. Questa scelta darà accesso alla linea di comando, che ha un set minimo di comandi disponibili • API - Gli utenti di questo gruppo avranno accesso all'interfaccia programmabile SOAP e REST. REST sarà disponibile dalla versione software 4.2.1

Tipo di utente

	**Utente** locale **L'ADC nel ruolo Stand-Alone o Manuale H/A creerà solo utenti locali** **Per impostazione predefinita, un** utente locale chiamato "admin" **è membro del gruppo admin.** **Per la compatibilità all'indietro**, **questo utente non può mai essere cancellato** **Puoi cambiare la password di questo utente o cancellarlo**, **ma non puoi cancellare l'ultimo admin locale**
	**Utente del cluster** Il ruolo ADC in Cluster creerà solo gli utenti del cluster Gli utenti del cluster sono sincronizzati tra tutti gli ADC nel cluster Qualsiasi modifica a un utente del cluster cambierà su tutti i membri del cluster Se sei connesso come utente del cluster, non sarai in grado di cambiare i ruoli da Cluster a Manual o Stand-Alone
	**Cluster e utente locale** Tutti gli utenti creati durante il ruolo Stand-Alone o Manuale saranno copiati nel Cluster Se l'ADC lascia successivamente il cluster, rimarranno solo gli utenti locali L'ultima password configurata per l'utente sarà valida

Rimozione di un utente

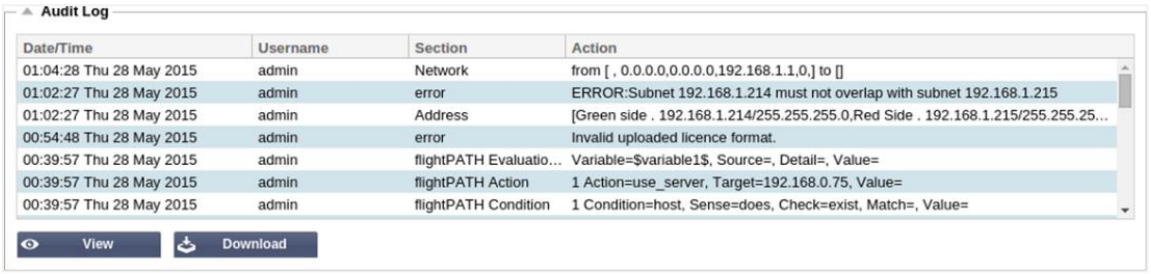
- Evidenziare un utente esistente
- Fare clic su Rimuovi
- Non sarà possibile eliminare l'utente che è attualmente iscritto
- Non sarà possibile rimuovere l'ultimo utente locale nel gruppo admin
- Non sarà possibile rimuovere l'ultimo utente del cluster rimasto nel gruppo admin
- Non sarà possibile eliminare l'utente admin per la compatibilità all'indietro
- Se si rimuove l'ADC dal cluster, tutti gli utenti tranne quelli locali saranno cancellati

Modifica di un utente

- Evidenziare un utente esistente
- Fare clic su Modifica
- Si può cambiare l'appartenenza dell'utente al gruppo spuntando le caselle appropriate e aggiornando
- Puoi anche cambiare la password di un utente, purché tu abbia i diritti di amministratore

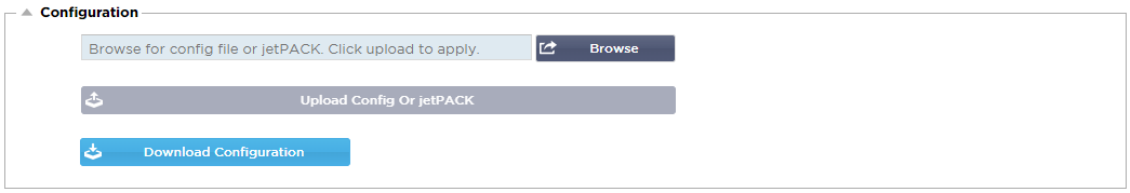
Registro di controllo

L'ADC registra le modifiche apportate alla configurazione dell'ADC dai singoli utenti. Il registro di controllo fornisce le ultime 50 azioni eseguite da tutti gli utenti. Puoi anche vedere TUTTE le voci nella sezione **Logs.** Per esempio:



Avanzato

Configurazione



È sempre una buona pratica scaricare e salvare la configurazione dell'ADC una volta che è completamente impostato e funzionante come richiesto. Puoi usare il modulo Configuration per scaricare e caricare una configurazione.

I Jetpacks sono file di configurazione per applicazioni standard e sono forniti da Edgenexus per semplificare il vostro lavoro. Anche questi possono essere caricati sull'ADC usando il modulo Configuration.

Un file di configurazione è essenzialmente un file di testo, e come tale, può essere modificato da voi usando un editor di testo come Notepad++ o VI. Una volta modificato come richiesto, il file di configurazione può essere caricato nell'ADC.

Scaricare una configurazione

- Per scaricare la configurazione corrente dell'ADC, premere il pulsante Download Configuration.
- Apparirà un pop-up che vi chiederà di aprire o salvare il file .conf.
- Salva in una posizione conveniente.
- Puoi aprirlo con qualsiasi editor di testo, come Notepad++.

Caricare una configurazione

- Puoi caricare un file di configurazione salvato cercando il file .conf salvato.
- Clicca sul pulsante "Carica la configurazione o Jetpack".
- L'ADC caricherà e applicherà la configurazione e poi aggiornerà il browser. Se non aggiorna il browser automaticamente, clicca su "refresh" sul browser.
- Al termine verrai reindirizzato alla pagina Dashboard.

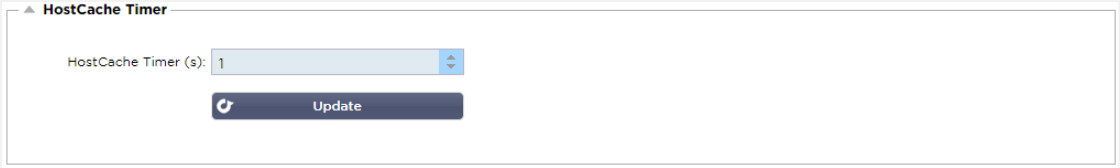
Carica un jetPACK

- Un jetPACK è un insieme di aggiornamenti di configurazione alla configurazione esistente.
- Un jetPACK può essere piccolo come cambiare il valore di timeout TCP fino a una configurazione completa specifica per un'applicazione come Microsoft Exchange o Microsoft Lync.
    - È possibile ottenere un jetPACK dal portale di supporto indicato alla fine di questa guida.
- Cerca il file jetPACK.txt.
- Fare clic su upload.
- Il browser si aggiornerà automaticamente dopo il caricamento.
- Al termine verrai reindirizzato alla pagina Dashboard.
- L'importazione può richiedere più tempo per distribuzioni più complesse come Microsoft Lync ecc.

Impostazioni globali

La sezione Global settings permette di cambiare vari elementi, inclusa la libreria crittografica SSL.

Timer della cache dell'host



L'Host Cache Timer è un'impostazione che memorizza l'indirizzo IP di un Real Server per un determinato periodo quando il nome di dominio è stato utilizzato al posto di un indirizzo IP. La cache viene lavata quando un Real Server fallisce. Impostando questo valore a zero si evita che la cache venga svuotata. Non c'è un valore massimo per questa impostazione.

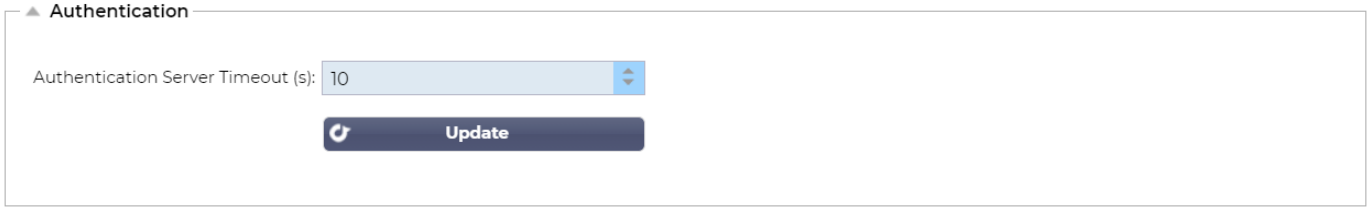
Scarico

La funzione di scarico è configurabile per ogni server reale collegato a un servizio virtuale. Per impostazione predefinita, l'impostazione Drain Clears Persistence è abilitata, permettendo ai server che sono messi in modalità Drain di terminare le sessioni con grazia in modo che possano essere messi offline per la manutenzione.

SSL

Questa impostazione globale permette di cambiare la libreria SSL secondo necessità. La libreria crittografica SSL predefinita usata dall'ADC è di OpenSSL. Se vuoi usare una libreria crittografica diversa, questa può essere cambiata qui.

Autenticazione

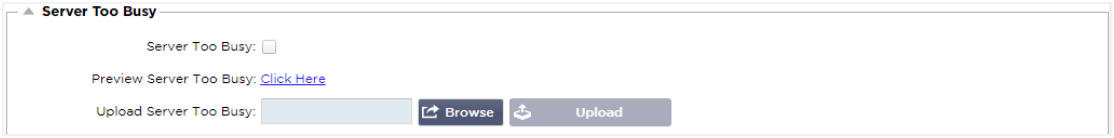


Questo valore imposta il valore di timeout per l'autenticazione, dopo il quale il tentativo di autenticazione sarà considerato fallito.

Protocollo

La sezione Protocollo è usata per impostare le molte impostazioni avanzate per il protocollo HTTP.

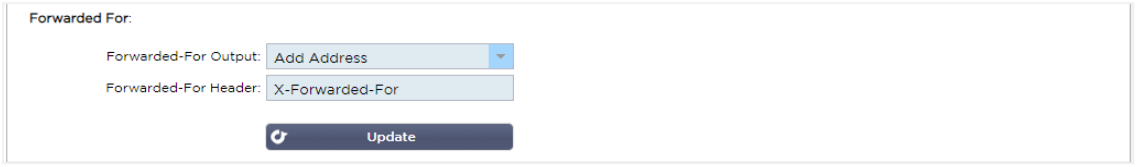
Server troppo occupato



Supponiamo che tu abbia limitato le connessioni massime ai tuoi Real Server; puoi scegliere di presentare una pagina web amichevole quando questo limite è stato raggiunto.

- Crea una semplice pagina web con il tuo messaggio. Puoi includere collegamenti esterni a oggetti su altri server e siti web. In alternativa, se vuoi avere immagini sulla tua pagina web, allora usa immagini codificate inline base64
- Cerca il file HTM(L) della tua pagina web appena creata
- Fare clic su Carica
- Se vuoi vedere l'anteprima della pagina, puoi farlo con il link Click Here

Inoltrato per



Forwarded For è lo standard de facto per identificare l'indirizzo IP di origine di un client che si connette a un server web attraverso bilanciatori di carico Layer- 7 e server proxy.

Inoltrato-per l'uscita

Opzione	**Descrizione**
Off	ADC non altera l'intestazione Forwarded-For.
Aggiungi indirizzo e porta	Questa scelta aggiungerà l'indirizzo IP e la porta del dispositivo o del client connesso all'ADC all'intestazione Forwarded-For.
Aggiungi indirizzo	Questa scelta aggiungerà l'indirizzo IP, del dispositivo o del client connesso all'ADC, all'intestazione Forwarded-For.
Sostituire indirizzo e porta	Questa scelta sostituirà il valore dell'intestazione Forwarded-For con l'indirizzo IP e la porta del dispositivo o client collegato all'ADC.
Sostituire l'indirizzo	Questa scelta sostituirà il valore dell'intestazione Forwarded-For con l'indirizzo IP del dispositivo o del client connesso all'ADC.

Intestazione inoltrata-per

Questo campo permette di specificare il nome dato all'intestazione Forwarded-For. Tipicamente, questo è "X-Forwarded-For" ma può essere cambiato per alcuni ambienti.

Registrazione avanzata per IIS - Registrazione personalizzata

Potete ottenere le informazioni X-Forwarded-For installando l'applicazione IIS Advanced logging 64-bit. Una volta scaricata, crea un campo di registrazione personalizzato chiamato X-Forwarded-For con le impostazioni seguenti.

Selezionate Default dall'elenco Source Type dall'elenco Category, selezionate Request Header nella casella Source Name e digitate X-Forwarded-For.

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

Modifiche di Apache HTTPd.conf

Vorrai fare diverse modifiche al formato predefinito per registrare l'indirizzo IP del client X-Forwarded-For o l'indirizzo IP effettivo del client se l'intestazione X-Forwarded-For non esiste.

Questi cambiamenti sono qui sotto:

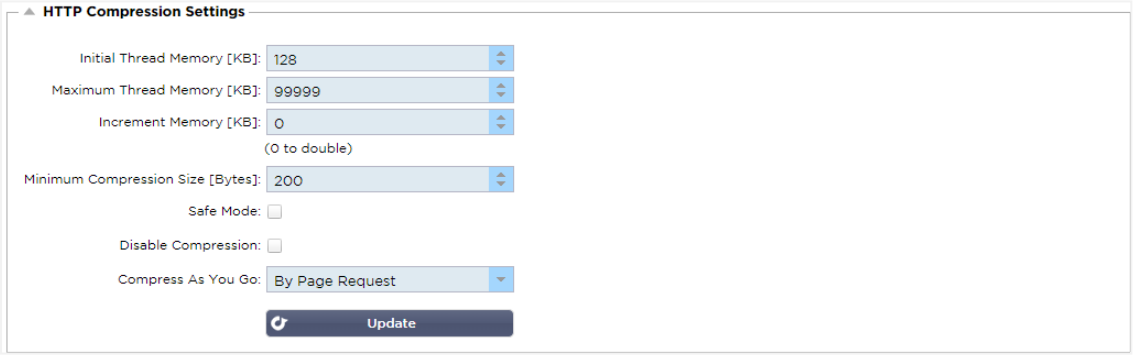
Tipo	Valore
LogFormat:	"%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" "%{User-Agent}i"" combinato
LogFormat:	"%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" proxy SetEnvIf X- Forwarded-For "^.*\..*\..*\..*" inoltrata
CustomLog:	"logs/access_log" combinato env=!forwarded
CustomLog:	"logs/access_log" proxy env=forwarded

Questo formato sfrutta il supporto integrato di Apache per il log condizionato basato su variabili ambientali.

- La linea 1 è la stringa formattata standard del registro combinato di default.
- La linea 2 sostituisce il campo %h (host remoto) con i valori estratti dall'intestazione X-Forwarded-For e imposta il nome di questo modello di file di log su "proxy".
- La linea 3 è un'impostazione per la variabile d'ambiente "forwarded" che contiene un'espressione regolare libera che corrisponde a un indirizzo IP, che va bene in questo caso, poiché ci interessa di più se un indirizzo IP esiste nell'intestazione X-Forwarded-For.
- Inoltre, la linea 3 potrebbe essere letta come: "Se c'è un valore X-Forwarded-For, usalo".
- Le linee 4 e 5 dicono ad Apache quale schema di log usare. Se esiste un valore X-Forwarded-For, usa lo schema "proxy", altrimenti usa lo schema "combined" per la richiesta. Per leggibilità, le linee 4 e 5 non approfittano della funzione di log rotate logs (piped) di Apache, ma si presume che quasi tutti la usino.

Queste modifiche comporteranno la registrazione di un indirizzo IP per ogni richiesta.

Impostazioni di compressione HTTP



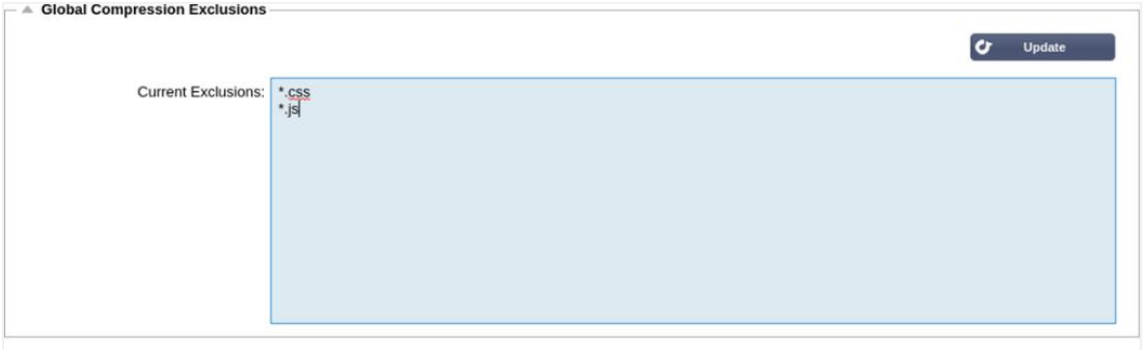
La compressione è una funzione di accelerazione ed è abilitata per ogni servizio nella pagina Servizi IP.

AVVERTENZA - Fate estrema attenzione quando regolate queste impostazioni, poiché impostazioni inappropriate possono influenzare negativamente le prestazioni dell'ADC

Opzione	Descrizione
Memoria iniziale del thread [KB]	Questo valore è la quantità di memoria che ogni richiesta ricevuta da ADC può inizialmente allocare. Per una prestazione più efficiente, questo valore dovrebbe essere impostato ad un valore appena superiore al più grande file HTML non compresso che i server web possono inviare.
Memoria massima del thread [KB]	Questo valore è la quantità massima di memoria che l'ADC alloca in una richiesta. Per la massima prestazione, ADC normalmente memorizza e comprime tutto il contenuto in memoria. Se viene elaborato un file di contenuto eccezionalmente grande che supera questa quantità, ADC scriverà su disco e comprimerà i dati lì.

Incremento di memoria [KB]	Questo valore imposta la quantità di memoria aggiunta all'allocazione iniziale della memoria del thread quando è richiesta una quantità maggiore. L'impostazione predefinita è zero. Questo significa che ADC raddoppierà l'allocazione quando i dati superano l'allocazione corrente (ad esempio 128Kb, poi 256Kb, poi 512Kb, ecc.) fino al limite impostato da Maximum Memory Usage per Thread. Questo è efficiente quando la maggior parte delle pagine sono di una dimensione consistente ma ci sono occasionalmente file più grandi. (es. la maggior parte delle pagine sono di 128Kb o meno, ma le risposte occasionali hanno una dimensione di 1Mb). Nello scenario in cui ci sono grandi file di dimensioni variabili, è più efficiente impostare un incremento lineare di una dimensione significativa (ad es. le risposte hanno dimensioni da 2Mb a 10Mb, un'impostazione iniziale di 1Mb con incrementi di 1Mb sarebbe più efficiente).
Dimensione minima di compressione [Bytes]	Questo valore è la dimensione, in byte, sotto la quale l'ADC non tenterà di comprimere. Questo è utile perché qualsiasi cosa sotto i 200 byte non comprime bene e può anche crescere in dimensione a causa delle intestazioni di compressione.
Modalità provvisoria	Spunta questa opzione per impedire ad ADC di applicare la compressione ai fogli di stile di JavaScript. La ragione di questo è che anche se ADC è consapevole di quali singoli browser possono gestire contenuti compressi, alcuni altri server proxy, anche se dichiarano di essere compatibili con HTTP/1.1 non sono in grado di trasportare correttamente fogli di stile e JavaScript compressi. Se si verificano problemi con fogli di stile o JavaScript attraverso un server proxy, allora usa questa opzione per disabilitare la compressione di questi tipi. Tuttavia, questo ridurrà la quantità complessiva di compressione del contenuto.
Disattivare la compressione	Spuntalo per impedire all'ADC di comprimere qualsiasi risposta.
Comprimere man mano che si va avanti	ON - Usa Compress as You Go su questa pagina. Questo comprime ogni blocco di dati ricevuti dal server in un chunk discreto che è completamente decomprimibile. OFF - Non usare Compress as you go su questa pagina. By Page Request - Usa Compress as You Go per richiesta di pagina.

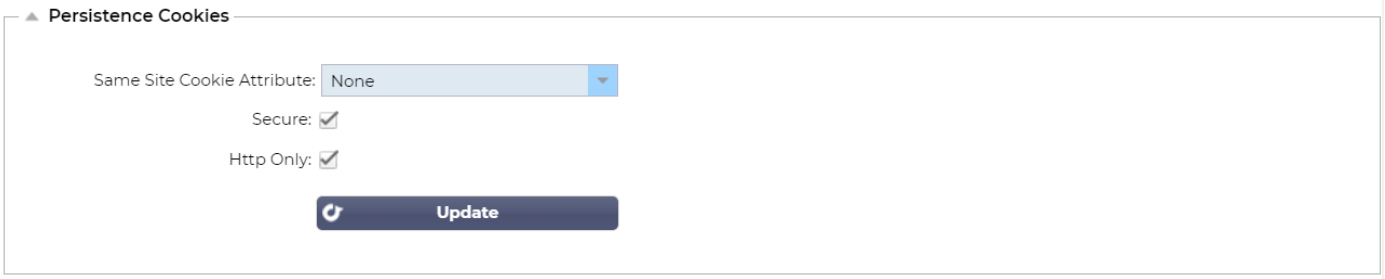
Esclusioni di compressione globale



Tutte le pagine con l'estensione aggiunta nella lista di esclusione non saranno compresse.

- Digitare il nome del singolo file.
- Fare clic su aggiorna.
- Se volete aggiungere un tipo di file, digitate semplicemente "*.css" per tutti i fogli di stile a cascata da escludere.
- Ogni file o tipo di file dovrebbe essere aggiunto in una nuova riga.

Cookie di persistenza



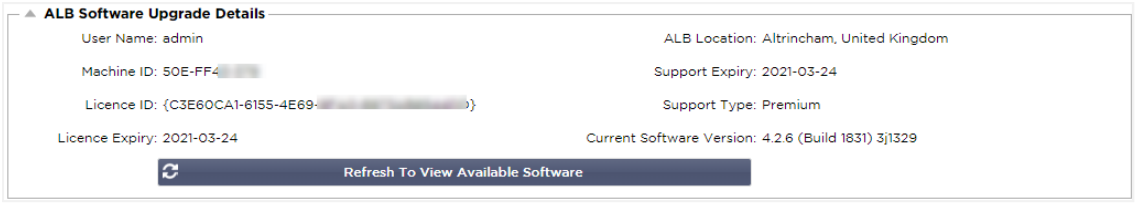
Questa impostazione permette di specificare come vengono gestiti i cookie di persistenza.

Campo	Descrizione
Stesso sito Cooke Attribute	**Nessuno**: Tutti i cookie sono accessibili agli script **Lassista**: Impedisce che i cookie siano accessibili da un sito all'altro, ma vengono memorizzati per diventare accessibili e inviati al sito proprietario se viene visitato **Strict**: impedisce l'accesso o la memorizzazione di qualsiasi cookie per un sito diverso **Off**: ritorna al comportamento predefinito del browser
Sicuro	Questa casella di controllo, quando è selezionata, applica la persistenza al traffico sicuro
Solo HTTP	Quando è spuntato, questo permette i Persistent Cookes solo sul traffico HTTP

Software

La sezione Software vi permette di aggiornare la configurazione e il firmware del vostro ADC.

Dettagli dell'aggiornamento del software



Le informazioni in questa sezione saranno popolate se hai una connessione Internet funzionante. Se il tuo browser non ha un collegamento a Internet, questa sezione sarà vuota. Una volta connesso, riceverai il messaggio del banner qui sotto.

La sezione Download dal Cloud mostrata qui sotto sarà popolata con informazioni che mostrano gli aggiornamenti disponibili per te sotto il tuo piano di supporto. Dovresti prestare attenzione al tipo di supporto e alla data di scadenza del supporto.

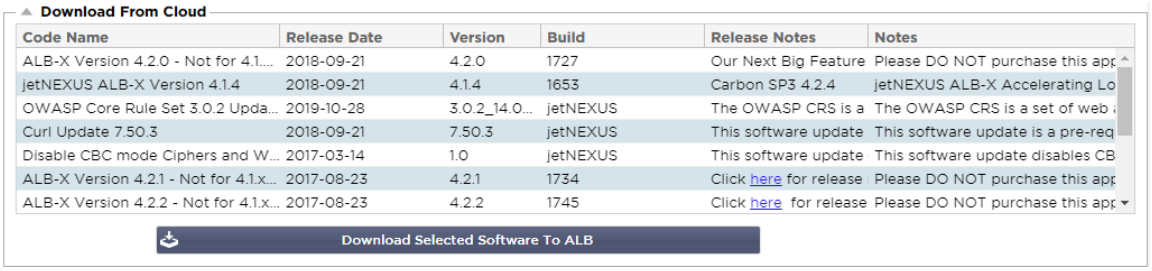
Nota: utilizziamo la connessione internet del tuo browser per visualizzare ciò che è disponibile da Edgenexus Cloud. Sarai in grado di scaricare gli aggiornamenti del software solo se l'ADC ha una connessione internet.

Per controllare questo:

- Avanzato--Risoluzione dei problemi--Ping
- Indirizzo IP - appstore.edgenexus.io
- Fare clic su Ping
- Se il risultato mostra "ping: host sconosciuto appstore.edgenexus.io. "

- L'ADC NON sarà in grado di scaricare nulla dal cloud

Scaricare da Cloud



Se il tuo browser è connesso a Internet, vedrai i dettagli del software disponibile nel cloud.

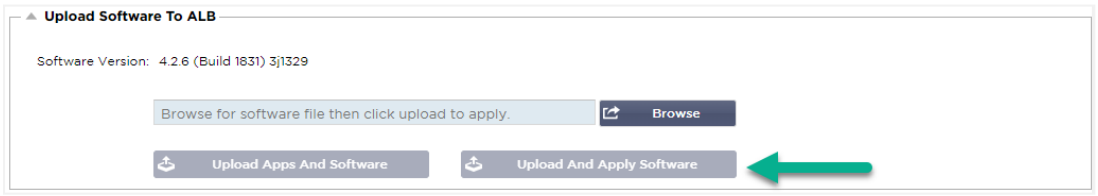
- Evidenzia la riga che ti interessa e clicca su "Scarica il software selezionato in ALB. ".
- Il software selezionato verrà scaricato nella tua ALB quando si clicca, e può essere applicato nella sezione "Applicare il software memorizzato nella ALB" qui sotto.

Nota: se l'ADC non ha un accesso diretto a Internet, riceverai un errore come quello che segue:

Errore di download, ALB non è in grado di accedere ai servizi ADC Cloud per il file build1734-3236-v4.2.1-Sprint2-update-64.software.alb

Caricare il software su ALB

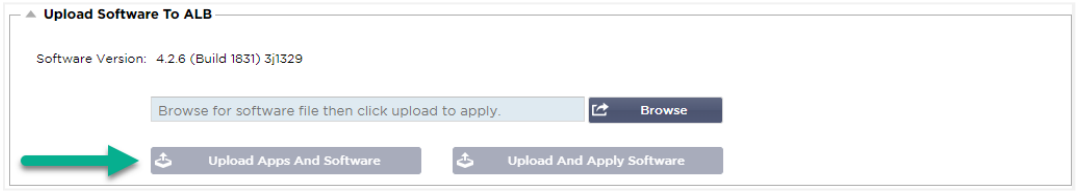
Caricamento delle applicazioni



Se hai un file App che finisce con <apptype>.alb puoi usare questo metodo per caricarlo.

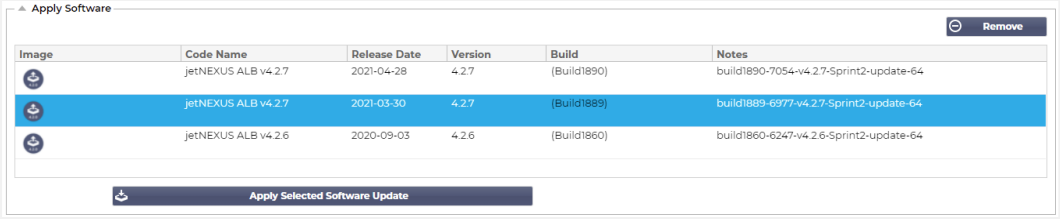
- Ci sono cinque tipi di App
  - <appname>flightpath.alb
  - <appname>.monitor.alb
  - <appname>.jetpack.alb
  - <appname>.addons.alb
  - <appname>.featurepack.alb
- Una volta caricata, ogni app si troverà nella sezione Biblioteca>Applicazioni.
- Devi poi distribuire ogni App in quella sezione individualmente.

Software



- Se vuoi caricare il software senza applicarlo, allora usa il pulsante evidenziato.
- Il file del software è <nome del software>.software.alb.
- Verrà quindi visualizzato nella sezione "Software Stored on ALB", da dove potrai applicarlo a tuo piacimento.

Applicare il software memorizzato su ALB



Questa sezione mostrerà tutti i file software memorizzati sull'ALB e disponibili per la distribuzione. L'elenco includerà le firme WAF (Web Application Firewall) aggiornate.

- Evidenzia la riga Software che ti interessa.
- Fare clic su "Applica software da selezionati".
- Se si tratta di un aggiornamento software dell'ALB, tieni presente che verrà caricato e poi riavviato l'ALB per essere applicato.
- Se l'aggiornamento che stai applicando è un aggiornamento della firma OWASP, si applicherà automaticamente senza riavviare.

Risoluzione dei problemi

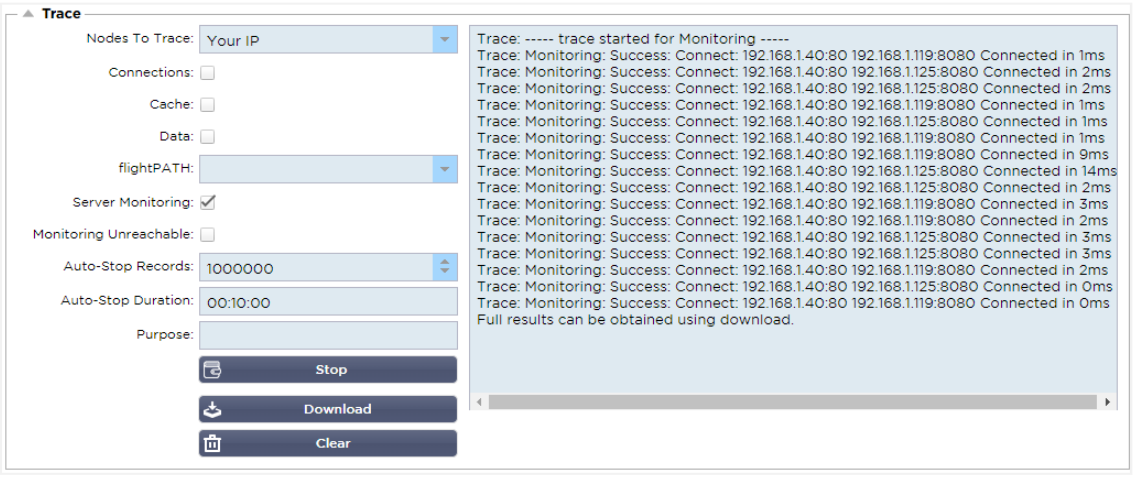
Ci sono sempre problemi che richiedono la risoluzione dei problemi per arrivare alla causa principale e alla soluzione. Questa sezione vi permette di farlo.

File di supporto

Se hai un problema con l'ADC e devi aprire un ticket di supporto, il supporto tecnico spesso richiederà diversi file diversi dall'appliance ADC. Questi file sono stati ora aggregati in un unico file .dat che può essere scaricato tramite questa sezione.

- Seleziona un periodo di tempo dal menu a tendina: È possibile scegliere tra 3, 7, 14 e Tutti i giorni.
- Fare clic su "Scarica i file di supporto".
- Verrà scaricato un file nel formato Support-jetNEXUS-yyymmddhh-NAME.dat
- Sollevare un ticket di supporto sul portale di supporto, i cui dettagli sono disponibili alla fine di questo documento.
- Assicurati di descrivere accuratamente il problema e di allegare il file .dat al biglietto.

Traccia

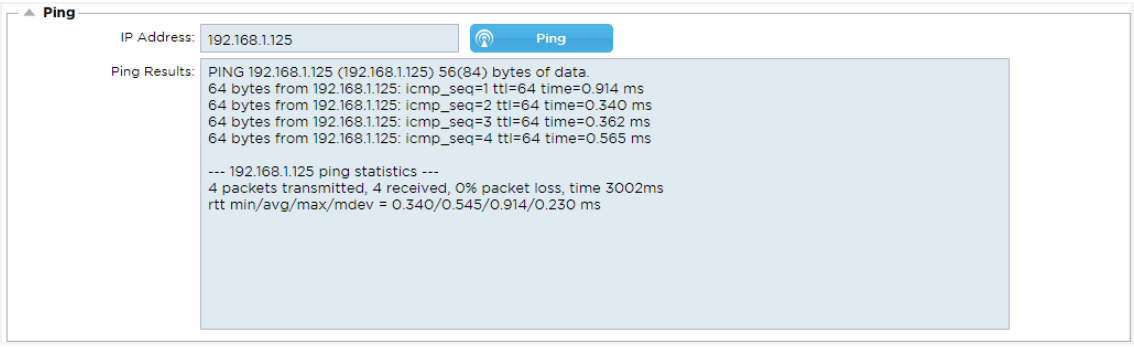


La sezione Trace ti permette di esaminare le informazioni che permettono il debugging del problema. Le informazioni fornite dipendono dalle opzioni scelte dai menu a tendina e dalle caselle di controllo.

Opzione	**Descrizione**
Nodi da tracciare	**Your IP**: Questo filtrerà l'output per utilizzare l'indirizzo IP da cui si sta accedendo alla GUI (Nota: non scegliere questa opzione per il monitoraggio, poiché il monitoraggio utilizzerà l'indirizzo dell'interfaccia ADC) **All IP**: Nessun filtro sarà applicato. Va notato che su un box occupato questo influenzerà negativamente le prestazioni.
Connessioni	Questa casella di controllo, se spuntata, mostrerà le informazioni sulle connessioni lato client e lato server.
Cache	Questa casella di controllo spuntata ti mostrerà le informazioni relative agli oggetti in cache.
Dati	Quando questa casella è spuntata, includerà i byte di dati grezzi gestiti in entrata e in uscita dall'ADC.
flightPATH	Il menu flightPATH ti permette di selezionare una particolare regola flightPATH da monitorare o Tutte le regole flightPATH.
Monitoraggio del server	Questa casella di controllo, se spuntata, mostrerà i monitor della salute del server attivi sull'ADC e i loro rispettivi risultati.
Monitoraggio non raggiungibile	Quando questa opzione è selezionata, il comportamento è molto simile a quello del monitoraggio del server, tranne che mostrerà solo i monitor falliti e quindi agisce come un filtro solo per questi messaggi.
Registrazioni auto-arresto	Il valore predefinito è 1.000.000 di record, dopo di che la funzione Trace si ferma automaticamente. Questa impostazione è una precauzione di sicurezza per evitare che Trace venga accidentalmente lasciato attivo e che influenzi le prestazioni dell'ADC.
Durata dell'Auto-Stop	Il tempo predefinito è impostato a 10 minuti, dopo i quali la funzione Trace si ferma automaticamente. Questa caratteristica è una precauzione di sicurezza per evitare che Trace venga accidentalmente lasciato acceso e influenzi le prestazioni dell'ADC.
Iniziare	Cliccate su questo per avviare manualmente la funzione Trace.
Fermare	Clicca per fermare manualmente la funzione Trace prima che venga raggiunto il record automatico o il tempo.
Scaricare	Anche se si può vedere il visualizzatore dal vivo sul lato destro, le informazioni possono essere visualizzate troppo velocemente. Invece, puoi scaricare il Trace.log per visualizzare tutte le informazioni raccolte durante le varie tracce di quel giorno. Questa funzione è una lista filtrata delle informazioni delle tracce. Se desideri visualizzare le informazioni delle tracce dei giorni precedenti, puoi scaricare il Syslog per quel giorno, ma dovrai filtrare manualmente.
Chiaro	Cancella il registro di tracciamento

Ping

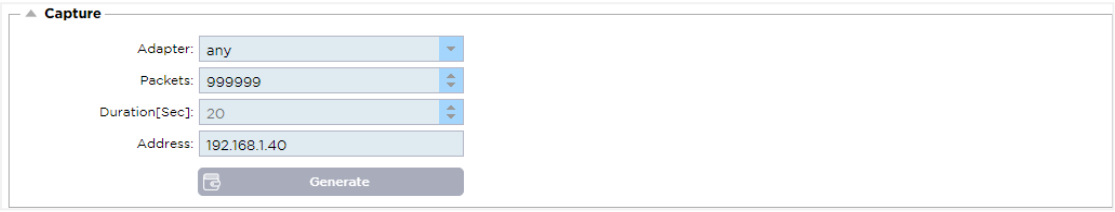
Puoi controllare la connettività di rete ai server e ad altri oggetti di rete nella tua infrastruttura usando lo strumento Ping.



Digita l'indirizzo IP dell'host che vuoi testare, per esempio, il gateway predefinito usando la notazione decimale punteggiata o un indirizzo IPv6. Potrebbe essere necessario attendere alcuni secondi per ottenere il risultato dopo aver premuto il pulsante "Ping".

Se avete configurato un server DNS, allora potete digitare il nome di dominio pienamente qualificato. Puoi configurare un server DNS nella sezione **DNS SERVER 1 & DNS SERVER 2**. Potrebbe essere necessario attendere qualche secondo per il risultato dopo aver premuto il pulsante "Ping".

Cattura



Per catturare il traffico di rete, seguite le semplici istruzioni qui sotto.

- Completa le opzioni nel modulo
- Fare clic su Genera
- Una volta che la cattura è stata eseguita, il tuo browser apparirà e ti chiederà dove vuoi salvare il file. Sarà nel formato "jetNEXUS.cap.gz".
- Sollevare un ticket di supporto sul portale di supporto, i cui dettagli sono disponibili alla fine di questo documento.
- Assicurati di descrivere accuratamente il problema e di allegare il file al biglietto.
- Puoi anche visualizzare il contenuto usando Wireshark

Opzione	**Descrizione**
Adattatore	Scegli il tuo adattatore dal menu a tendina, tipicamente eth0 o eth1. Puoi anche catturare tutte le interfacce con "any"
Pacchetti	Questo valore è il numero massimo di pacchetti da catturare. In genere, 99999
Durata	Scegli un tempo massimo per il quale la cattura verrà eseguita. Un tempo tipico è di 15 secondi per i siti ad alto traffico. La GUI sarà inaccessibile durante il periodo di cattura
Indirizzo	Questo valore filtrerà su qualsiasi indirizzo IP inserito nella casella. Lasciare vuoto per nessun filtro.

Per mantenere le prestazioni, abbiamo limitato il file di download a 10MB. Se trovi che questo non è sufficiente per catturare tutti i dati necessari, possiamo aumentare questa cifra.

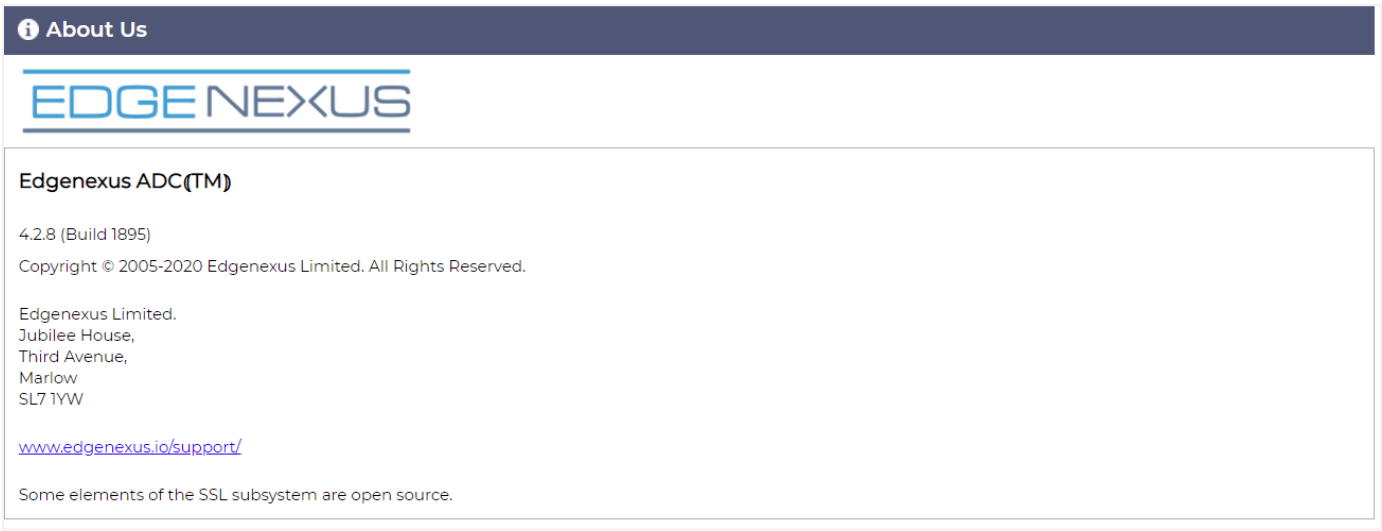
Nota: Questo avrà un impatto sulle prestazioni dei siti live. Per aumentare la dimensione di cattura disponibile, si prega di applicare un'impostazione globale jetPACK per aumentare la dimensione di cattura.

Aiuto

La sezione Aiuto fornisce l'accesso alle informazioni su Edgenexus e l'accesso alle guide utente e ad altre informazioni utili.

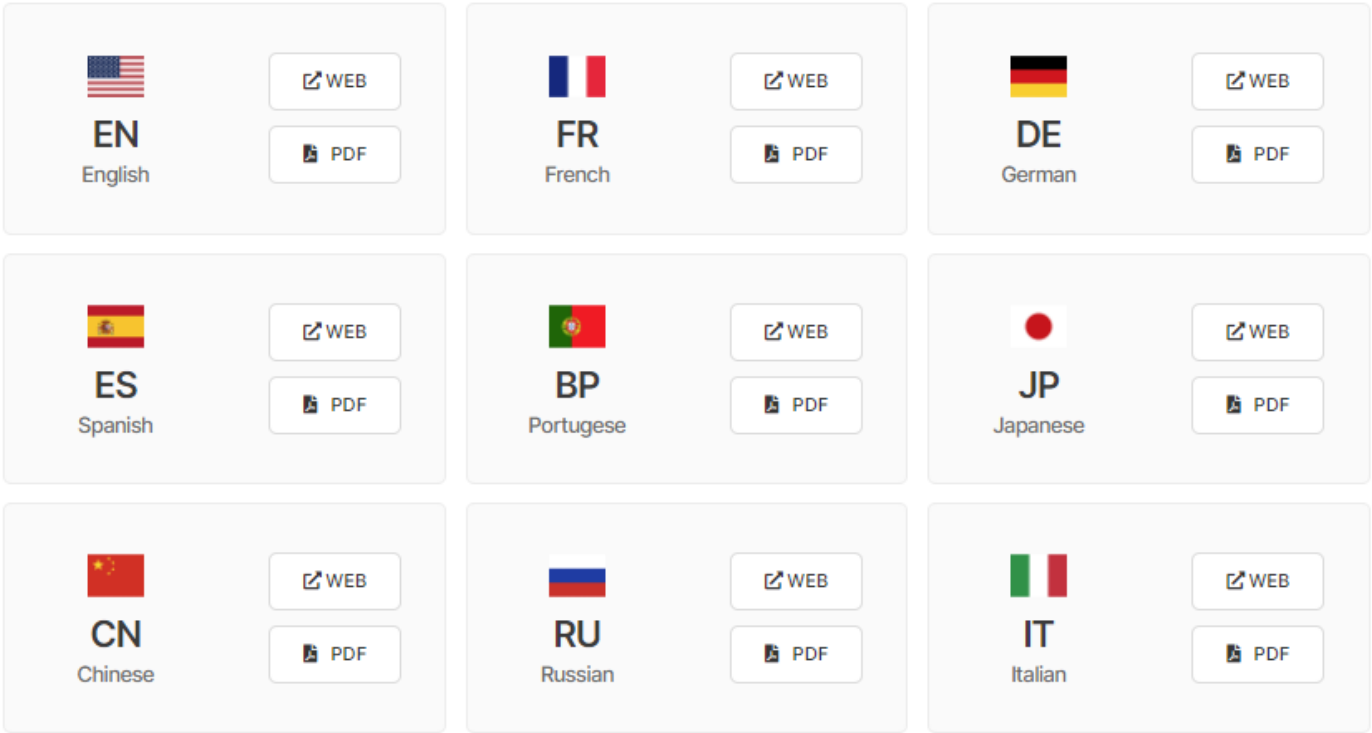
Chi siamo

Cliccando sull'opzione Chi siamo si visualizzeranno informazioni su Edgenexus e sul suo ufficio aziendale.



Riferimento

L'opzione di riferimento aprirà la pagina contenente le guide utente e altri documenti utili.



Se non trovate quello che state cercando, contattate support@edgenexus.io.

Cos'è un jetPACK

I jetPACK sono un metodo unico per configurare istantaneamente il vostro ADC per applicazioni specifiche. Questi modelli facili da usare sono preconfigurati e completamente sintonizzati con tutte le impostazioni specifiche dell'applicazione di cui hai bisogno per godere di un servizio ottimizzato dal tuo ADC. Alcuni dei jetPACK usano flightPATH per manipolare il traffico e devi avere una licenza flightPATH per far funzionare questo elemento. Per sapere se hai una licenza per flightPATH, fai riferimento alla pagina delle **LICENZE.**

Scaricare un jetPACK

- Ogni jetPACK qui sotto è stato creato con un unico indirizzo IP Virtuale contenuto nel titolo del jetPACK. Per esempio, il primo jetPACK qui sotto ha un indirizzo IP virtuale di 1.1.1.1
- Potete caricare questo jetPACK così com'è e cambiare l'indirizzo IP nella GUI o modificare il jetPACK con un editor di testo come Notepad++ e cercare e sostituire 1.1.1.1 con il vostro indirizzo IP virtuale.
- Inoltre, ogni jetPACK è stato creato con 2 Real Server con indirizzi IP di 127.1.1.1 e 127.2.2.2. Anche in questo caso potete cambiarli nella GUI dopo il caricamento o prima usando Notepad++.
- Fare clic su un link jetPACK qui sotto e salvare il link come file jetPACK-VIP-Application.txt nella posizione scelta

Microsoft Exchange

Applicazione	Scarica il link	Cosa fa?	Cosa è incluso?
Exchange 2010	jetPACK-1.1.1.1-Exchange-2010	Questo jetPACK aggiungerà le impostazioni di base per bilanciare il carico di Microsoft Exchange 2010. C'è una regola flightPATH inclusa per reindirizzare il traffico sul servizio HTTP a HTTPS, ma è un'opzione. Se non hai una licenza per flightPATH, questo jetPACK funzionerà comunque.	Impostazioni globali: Timeout di servizio 2 ore Monitor: Monitor di livello 7 per l'applicazione web di Outlook e monitor di livello 4 fuori banda per il servizio di accesso al client IP del servizio virtuale: 1.1.1.1 Porte di servizio virtuali: 80, 443, 135, 59534, 59535 Server reali: 127.1.1.1 127.2.2.2 flightPATH: aggiunge il reindirizzamento da HTTP a HTTPS
	jetPACK-1.1.1.2-Exchange-2010-SMTP-RP	Come sopra, ma aggiungerà un servizio SMTP sulla porta 25 in connettività reverse proxy. Il server SMTP vedrà l'indirizzo dell'interfaccia ALB-X come IP sorgente.	Impostazioni globali: Timeout di servizio 2 ore Monitor: Monitor di livello 7 per l'applicazione web di Outlook. Monitor di livello 4 fuori banda per il servizio di accesso al client IP del servizio virtuale: 1.1.1.1 Porte di servizio virtuali: 80, 443, 135, 59534, 59535, 25 (reverse proxy) Server reali: 127.1.1.1 127.2.2.2 flightPATH: aggiunge il reindirizzamento da HTTP a HTTPS
	jetPACK-1.1.1.3-Exchange-2010-SMTP-DSR	Come sopra, tranne che questo jetPACK configurerà il servizio SMTP per usare la connettività Direct Server Return. Questo jetPACK è necessario se il vostro server SMTP ha bisogno di vedere l'indirizzo IP effettivo del client.	Impostazioni globali: Timeout di servizio 2 ore Monitor: Monitor di livello 7 per l'applicazione web di Outlook. Monitor di livello 4 fuori banda per il servizio di accesso al client IP del servizio virtuale: 1.1.1.1

			Porte di servizio virtuali: 80, 443, 135, 59534, 59535, 25 (ritorno diretto al server) Server reali: 127.1.1.1 127.2.2.2 flightPATH: aggiunge il reindirizzamento da HTTP a HTTPs
Scambio 2013	jetPACK-2.2.2.1-Exchange-2013-Low-Resource	Questa configurazione aggiunge 1 VIP e due servizi per il traffico HTTP e HTTPS e richiede meno CPU. È possibile aggiungere più controlli di salute al VIP per controllare che ciascuno dei singoli servizi sia attivo	Impostazioni globali: Monitor: Monitor di livello 7 per OWA, EWS, OA, EAS, ECP, OAB e ADS IP del servizio virtuale: 2.2.2.1 Porte di servizio virtuali: 80, 443 Server reali: 127.1.1.1 127.2.2.2 flightPATH: aggiunge il reindirizzamento da HTTP a HTTPS
	jetPACK-2.2.3.1-Exchange-2013-Med-Resource	Questa configurazione utilizza un indirizzo IP unico per ogni servizio e quindi utilizza più risorse di quelle sopra. È necessario configurare ogni servizio come una voce DNS individuale Esempio owa. edgenexus.com, ews. edgenexus.com, ecc. Un monitor per ogni servizio sarà aggiunto e applicato al relativo servizio	Impostazioni globali: Monitor: Monitor di livello 7 per OWA, EWS, OA, EAS, ECP, OAB, ADS, MAPI e PowerShell Servizio virtuale 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 Porte di servizio virtuali: 80, 443 Server reali: 127.1.1.1 127.2.2.2 flightPATH: aggiunge il reindirizzamento da HTTP a HTTPs
	jetPACK-2.2.2.3-Exchange2013-HIgh-Resource	Questo jetPACK aggiungerà un unico indirizzo IP e diversi servizi virtuali su diverse porte. flightPATH quindi commuterà il contesto in base al percorso di destinazione al corretto servizio virtuale. Questo jetPACK richiede la maggior quantità di CPU per eseguire la commutazione di contesto	Impostazioni globali: Monitor: Monitor di livello 7 per OWA, EWS, OA, EAS, ECP, OAB, ADS, MAPI e PowerShell IP del servizio virtuale: 2.2.2.3 Porte di servizio virtuali: 80, 443, 1, 2, 3, 4, 5, 6, 7 Server reali: 127.1.1.1 127.2.2.2 flightPATH: aggiunge il reindirizzamento da HTTP a HTTPS

Microsoft Lync 2010/2013

Proxy inverso	Front End	Bordo interno	Bordo esterno
jetPACK-3.3.3.1-Lync-Reverse-Proxy	jetPACK-3.3.3.2-Lync-Front -End	jetPACK-3.3.3.3-Lync-Edge-Internal	jetPACK-3.3.3.4-Lync-Edge-External

Servizi web

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

Microsoft Remote Desktop

Normale

jetPACK-5.5.5.1-Remote-Desktop

DICOM - Digital Imaging and Communication in Medicine

HTTP normale
jetPACK-6.6.6.1-DICOM

Oracle e-Business Suite

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

VMware Horizon View

Server di connessione - SSL Offload	**Server di sicurezza - SSL Re-Encryption**
jetPACK-8.8.8.1-View-SSL-Offload	jetPACK-8.8.8.2-View-SSL-Re-encryption

Impostazioni globali

- GUI Secure Port 443 - questo jetPACK cambierà la porta sicura della GUI da 27376 a 443. HTTP://x.x.x.x
- GUI Timeout 1 giorno - la GUI ti chiederà di inserire la tua password ogni 20 minuti. Questa impostazione aumenterà la richiesta a 1 giorno
- ARP Refresh 10 - durante un failover tra apparecchi HA, questa impostazione aumenterà il numero di **ARP gratuiti** per assistere gli switch durante la transizione
- Dimensione di cattura 16MB - la dimensione di cattura predefinita è di 2MB. Questo valore aumenterà la dimensione fino a un massimo di 16MB

Opzioni di cifratura

- Strong Ciphers - Questo aggiungerà la possibilità di scegliere "Strong Ciphers" dalla lista delle opzioni Cipher:
  - Cipher = ALL:RC4+RSA:+RC4:+HIGH:!DES-CBC3-SHA:!SSLv2:!ADH:!EXP:!ADHexport:!MD5
- Anti-Bestia - Questo aggiungerà la possibilità di scegliere "Anti-Bestia" dalla lista delle Opzioni Cifra:
  - Cifra = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH
- No SSLv3 - Questo aggiungerà la possibilità di scegliere "No SSLv3" dall'elenco Cipher Options:
  - Cifra = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
- No SSLv3 no TLSv1 No RC4 - Questo aggiungerà la possibilità di scegliere "No-TLSv1 No-SSLv3 No-RC4" dalla lista Cipher Options:
  - Cifra = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
- NO_TLSv1.1 - Questo aggiungerà la possibilità di scegliere "NO_TLSv1.1" dall'elenco Cipher Options:
  - Cipher= ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:RSA+AESGCM:RSA+AES:HIGH:!3DES:!aNULL:!MD5:!DSS:!MD5:!aNULL:!EDH:!RC4

flightPATHs

- X-Content-Type-Options - aggiungi questa intestazione se non esiste e impostala su "nosniff" - impedisce che il browser faccia automaticamente "MIME-Sniffing".
- X-Frame-Options - aggiungi questa intestazione se non esiste e impostala su "SAMEORIGIN" - le pagine del tuo sito web possono essere incluse nei frame, ma solo su altre pagine all'interno dello stesso sito.
- X-XSS-Protection - aggiungere questa intestazione se non esiste e impostarla a "1; mode=block" - abilitare le protezioni cross-site scripting del browser
- Strict-Transport-Security - aggiungere l'intestazione se non esiste e impostarla a "max-age=31536000 ; includeSubdomains" - assicura che il client dovrebbe rispettare che tutti i link dovrebbero essere HTTPs:// per la max-age

Applicare un jetPACK

Potete applicare qualsiasi jetPACK in qualsiasi ordine, ma fate attenzione a non usare un jetPACK con lo stesso indirizzo IP virtuale. Questa azione causerà un indirizzo IP duplicato nella configurazione. Se lo fate per errore, potete cambiarlo nella GUI.

- Spostati su Avanzato > Aggiorna il software
- Sezione di configurazione
- Carica una nuova configurazione o jetPACK
- Cerca per jetPACK
- Fare clic su Carica
- Una volta che lo schermo del browser diventa bianco, clicca su refresh e aspetta che appaia la pagina Dashboard

Creare un jetPACK

Una delle grandi cose di jetPACK è che si può creare il proprio. Può darsi che abbiate creato la configurazione perfetta per un'applicazione e vogliate usarla per diverse altre scatole in modo indipendente.

- Iniziate copiando la configurazione corrente dal vostro ALB-X esistente
  - Avanzato
  - Aggiornare il software
  - Scarica la configurazione corrente
- Modifica questo file con Notepad++
- Aprite un nuovo documento txt e chiamatelo "yourname-jetPACK1.txt".
- Copiare tutte le sezioni rilevanti dal file di configurazione a "yourname-jetPACK1.txt"
- Salva una volta completato

IMPORTANTE: Ogni jetPACK è diviso in diverse sezioni, ma tutti i jetPACK devono avere #!jetpack all'inizio della pagina.

Le sezioni che si raccomanda di modificare/copiare sono elencate di seguito.

Sezione 0:

```
#!jetpack
```

Questa linea deve essere all'inizio del jetPACK, o la vostra configurazione attuale sarà sovrascritta.

Sezione1:

```
[jetnexusdaemon]
```

Questa sezione contiene impostazioni globali che, una volta modificate, si applicano a tutti i servizi. Alcune di queste impostazioni possono essere cambiate dalla console web, ma altre sono disponibili solo qui.

Esempi:

```
ConnectionTimeout=600000
```

Questo esempio è il valore di timeout TCP in millisecondi. Questa impostazione significa che una connessione TCP sarà chiusa dopo 10 minuti di inattività

```
ContentServerCustomTimer=20000
```

Questo esempio è il ritardo in millisecondi tra i controlli di salute del server dei contenuti per i monitor personalizzati come DICOM

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

Questo esempio cambierà il nome dell'intestazione del cookie usato nel bilanciamento del carico persistente dal predefinito "jnAccel" a "MS-WSMAN". Questa particolare modifica è necessaria per il reverse proxy di Lync 2010/2013.

Sezione 2:

[jetnexusdaemon-Csm-Rules]

Questa sezione contiene le regole di monitoraggio del server personalizzate che sono tipicamente configurate dalla console web qui.

Esempio:

```
[jetnexusdaemon-Csm-Rules-0]
Contenuto="Server Up"
Desc="Monitor 1″
Metodo="CheckResponse"
Nome="Controllo di salute - Il server è attivo"
Url="HTTP://demo.jetneus.com/healthcheck/healthcheck.html"
```

Sezione 3:

[jetnexusdaemon-LocalInterface]

Questa sezione contiene tutti i dettagli della sezione Servizi IP. Ogni interfaccia è numerata e include sotto-interfacce per ogni canale. Se il tuo canale ha una regola flightPATH applicata, allora conterrà anche una sezione Path.

Esempio:

```
[jetnexusdaemon-LocalInterface1]
1.1=”443″
1.2=”104″
1.3=”80″
1.4=”81″
Enabled=1
Netmask="255.255.255.0″
PrimaryV2="{A28B2C99-1FFC-4A7C-AAD9-A55C32A9E913}"
[jetnexusdaemon-LocalInterface1.1]
1=">,""Gruppo sicuro"",2000,"
2="192.168.101.11:80,Y,""IIS WWW Server 1″""
3="192.168.101.12:80,Y,""IIS WWW Server 2″""
AddressResolution=0
CachePort=0
CertificateName="predefinito"
ClientCertificateName="No SSL"
Comprimere=1
ConnectionLimiting=0
DSR=0
DSRProto="tcp"
Enabled=1
LoadBalancePolicy="CookieBased"
MaxConnections=10000
MonitoringPolicy="1″
PassThrough=0
Protocollo="Accelerare HTTP"
ServiceDesc="Secure Servers VIP"
SNAT=0
SSL=1
SSLClient=0
SSLInternalPort=27400
[jetnexusdaemon-LocalInterface1.1-Path]
1=”6″
```

Sezione 4:

[jetnexusdaemon-Path]

Questa sezione contiene tutte le regole di flightPATH. I numeri devono corrispondere a ciò che è stato applicato all'interfaccia. Nell'esempio qui sopra, vediamo che la regola flightPATH "6" è stata applicata al canale, includendo questo come esempio qui sotto.

Esempio:

```
[jetnexusdaemon-Path-6]
Desc="Forzare l'uso di HTTPS per certe directory"
Nome="Gary - Forza HTTPS"
[jetnexusdaemon-Path-6-Condition-1]
Controllare="contenere"
Condizione="percorso"
Match=
Senso="fa"
Valore="/sicuro/"
[jetnexusdaemon-Path-6-Evaluate-1]
Dettaglio=
Fonte="host"
Valore=
Variabile="$host$"[jetnexusdaemon-Path-6-Function-1]
Azione="redirect"
Target="HTTPs://$host$$path$$querystring$"
Valore=
```

Introduzione a flightPATH

Cos'è flightPATH?

flightPATH è un motore di regole intelligente sviluppato da Edgenexus per manipolare e instradare il traffico HTTP e HTTPS. È altamente configurabile, molto potente e tuttavia molto facile da usare.

Anche se alcuni componenti di flightPATH sono oggetti IP, come Source IP, flightPATH può essere applicato solo a un **tipo di servizio** uguale a HTTP. Se si sceglie qualsiasi altro tipo di servizio, la scheda flightPATH in IP Services sarà vuota.

Una regola flightPATH ha tre componenti:

Opzione	Descrizione
Condizione	Imposta più criteri per attivare la regola flightPATH.
Valutazione	Permette l'uso di variabili che possono essere utilizzate nell'area Azione.
Azione	Il comportamento una volta che la regola è scattata.

Cosa può fare flightPATH?

flightPATH può essere usato per modificare il contenuto e le richieste HTTP in entrata e in uscita.

Oltre a usare semplici corrispondenze di stringhe come "Inizia con" e "Finisce con" per esempio, si può implementare un controllo completo usando potenti espressioni regolari (RegEx) compatibili con Perl.

Per saperne di più su RegEx, consultate questo utile sito https://www.regexbuddy.com/regex.html

Inoltre, le variabili personalizzate possono essere create e utilizzate nell'area **Action** permettendo molte possibilità diverse.

Condizione

Condizione	Descrizione	Esempio
<form>	I moduli HTML sono usati per passare dati a un server	Esempio "il modulo non ha lunghezza 0"
Posizione GEO	Questo confronta l'indirizzo IP sorgente con il codice paese ISO 3166	La posizione GEO è uguale a GB o la posizione GEO è uguale a Germania
Ospite	Questo è l'host estratto dall'URL	www.mywebsite.com o 192.168.1.1
Lingua	Questa è la lingua estratta dall'intestazione HTTP della lingua	Questa condizione produrrà un menu a tendina con un elenco di lingue
Metodo	Questo è un menu a tendina dei metodi HTTP	Questo è un menu a tendina che include GET, POST ecc.
Origine IP	Se il proxy a monte supporta X-Forwarded-for (XFF), userà il vero indirizzo Origin	IP del cliente. Può anche utilizzare più IP o sottoreti. 10\1\2\.* è 10.1.2.0 /24 subnet10\1\2\.3|10\1\2\.4 Usa | per più IP
Percorso	Questo è il percorso del sito web	/mywebsite/index.asp
POST	Metodo di richiesta POST	Controllare i dati che vengono caricati su un sito web

Interrogare	Questo è il nome e il valore di una query come tale può accettare il nome della query o anche un valore	"Best=edgeNEXUS" dove la corrispondenza è Best e il valore è edgeNEXUS
Stringa di query	L'intera stringa della query dopo il carattere ?	
Richiesta di cookie	Questo è il nome di un cookie richiesto da un cliente	MS-WSMAN=afYfn1CDqCDqUD::
Intestazione della richiesta	Questo può essere qualsiasi intestazione HTTP	Referrer, User-Agent, Da, Data
Richiesta Versione	Questa è la versione HTTP	HTTP/1.0 O HTTP/1.1
Corpo di risposta	Una stringa definita dall'utente nel corpo della risposta	Server UP
Codice di risposta	Il codice HTTP per la risposta	200 OK, 304 Non modificato
Risposta Cookie	Questo è il nome di un cookie inviato dal server	MS-WSMAN=afYfn1CDqCDqUD::
Intestazione della risposta	Questo può essere qualsiasi intestazione HTTP	Referrer, User-Agent, Da, Data
Versione di risposta	La versione HTTP inviata dal server	HTTP/1.0 O HTTP/1.1
Fonte IP	Questo è l'IP di origine, l'IP del server proxy o qualche altro indirizzo IP aggregato	ClientIP , Proxy IP, Firewall IP. Può anche utilizzare più IP e sottoreti. Devi evitare i punti perché questi sono RegEX. Esempio 10\.1\.2\.3 è 10.1.2.3

Partita	**Descrizione**	**Esempio**
Accettare	Tipi di contenuto accettabili	Accettare: text/plain
Accept-Encoding	Codifiche accettabili	Accept-Encoding: <compress | gzip | deflate | sdch | identity>
Accept-Language	Lingue accettabili per la risposta	Accetta la lingua: it-US
Accept-Range	Quali tipi di intervallo di contenuto parziale supporta questo server	Accetta: bytes
Autorizzazione	Credenziali di autenticazione per l'autenticazione HTTP	Autorizzazione: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Carica a	Contiene informazioni contabili per i costi dell'applicazione del metodo richiesto	
Content-Encoding	Il tipo di codifica usato sui dati.	Codifica dei contenuti: gzip
Content-Length	La lunghezza del corpo della risposta in ottetti (byte a 8 bit)	Lunghezza del contenuto: 348
Content-Type	Il tipo mime del corpo della richiesta (usato con richieste POST e PUT)	Content-Type: application/x-www-form-urlencoded
Cookie	Un cookie HTTP precedentemente inviato dal server con Set-Cookie (sotto)	Cookie: $Version=1; Skin=new;
Data	Data e ora di origine del messaggio	Data = "Data" ":" HTTP-date

ETag	Un identificatore per una versione specifica di una risorsa, spesso un message digest	ETag: "aed6bdb8e090cd1:0"
Da	L'indirizzo e-mail dell'utente che fa la richiesta	Da: user@example.com
Se-Modificato-Da	Permette di restituire un 304 Not Modified se il contenuto è invariato	Se-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Ultimo-Modificato	La data dell'ultima modifica dell'oggetto richiesto, nel formato RFC 2822	Ultimo-Modificato: Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Le intestazioni specifiche dell'implementazione possono avere vari effetti in qualsiasi punto della catena richiesta-risposta.	Pragma: no-cache
Referrer	Questo è l'indirizzo della pagina web precedente da cui è stato seguito un collegamento alla pagina attualmente richiesta	Referente: HTTP://www.edgenexus.io
Server	Un nome per il server	Server: Apache/2.4.1 (Unix)
Set-Cookie	Un cookie HTTP	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
User-Agent	La stringa dell'agente dell'utente	User-Agent: Mozilla/5.0 (compatibile; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Variare	Dice ai proxy a valle come abbinare le future intestazioni di richiesta per decidere se la risposta in cache può essere usata piuttosto che richiederne una nuova dal server d'origine	Vary: User-Agent
X-Powered-By	Specifica la tecnologia (ad esempio ASP.NET, PHP, JBoss) che supporta l'applicazione web	X-Powered-By: PHP/5.4.0

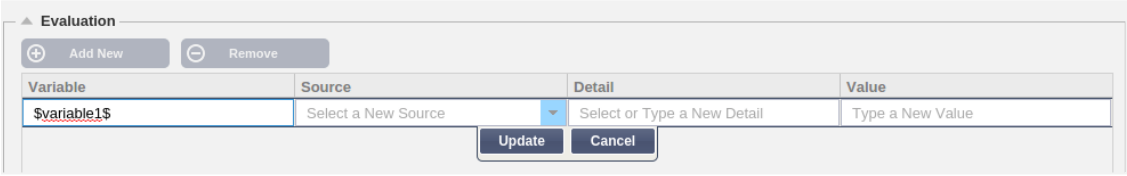
Controlla	**Descrizione**	**Esempio**
Esistere	Questo non si preoccupa del dettaglio della condizione, ma solo del fatto che esiste/non esiste	Host - Does - Exist
Iniziare	La stringa inizia con il valore	Path - Does - Start - /secure
Fine	La stringa termina con il valore	Percorso - Fa - Fine - .jpg
Contenere	La stringa contiene il valore	Intestazione della richiesta - Accept - Does - Contain - image
Uguale	La stringa equivale al valore	Host - Does - Equal - www.edgenexus.io
Avere lunghezza	La stringa ha la lunghezza del valore	Host - Does - Have Length - 16 www.edgenexus.io = VERO www.edgenexus.com = FALSO
Corrisponde a RegEx	Questo vi permette di inserire un'espressione regolare completamente compatibile con Perl	IP di origine - Fa - Regex match - 10\..* | 11\..*

Esempio

- L'esempio ha due condizioni, ed **entrambe** devono essere soddisfatte per eseguire l'azione

- Il primo è controllare che l'oggetto richiesto sia un'immagine
- Il secondo è il controllo di un hostname specifico

Valutazione



L'aggiunta di una variabile è una caratteristica interessante che vi permetterà di estrarre dati dalla richiesta e utilizzarli nelle azioni. Per esempio, si potrebbe registrare il nome utente o inviare un'e-mail se c'è un problema di sicurezza.

- Variabile: Deve iniziare e finire con il simbolo $. Per esempio $variabile1$
- Fonte: Selezionare dalla casella a discesa la fonte della variabile
- Dettaglio: Selezionare dalla lista quando è pertinente. Se il Source=Request Header, il Details potrebbe essere User-Agent
- Valore: Inserisci il testo o l'espressione regolare per mettere a punto la variabile.

Variabili incorporate:

- Le variabili Built-In sono già state codificate, quindi non è necessario creare una voce di valutazione per queste.
- Puoi usare una qualsiasi delle variabili elencate qui sotto nella tua azione
- La spiegazione di ogni variabile si trova nella tabella "Condizione" qui sopra
    - Metodo = $metodo$
    - Percorso = $path$
    - Querystring = $querystring$
    - Sourceip = $sourceip$
    - Codice di risposta (testo incluso anche "200 OK") = $resp$
    - Host = $host$
    - Versione = $versione$
    - Clientport = $clientport$
    - Clientip = $clientip$
    - Geolocation = $geolocation$"

Esempio di azione:

- Azione = Redirect 302
    - Target = HTTPs://$host$/404.html
- Azione = Log
    - Target = Un cliente da $sourceip$:$sourceport$ ha appena fatto una richiesta $path$ pagina

Spiegazione:

- Un cliente che accede a una pagina che non esiste verrebbe normalmente presentato con una pagina 404 del browser
- In questo caso l'utente viene reindirizzato all'hostname originale che ha usato, ma il percorso sbagliato viene sostituito con 404.html
- Viene aggiunta una voce al syslog che dice "Un client da 154.3.22.14:3454 ha appena fatto una richiesta alla pagina wrong.html".

Fonte	Descrizione	Esempio
Cookie	Questo è il nome e il valore dell'intestazione del cookie	MS-WSMAN=afYfn1CDqqCDqUD::Dove il nome è MS-WSMAN e il valore è afYfn1CDqCDqUD::
Ospite	Questo è l'hostname estratto dall'URL	www.mywebsite.com o 192.168.1.1

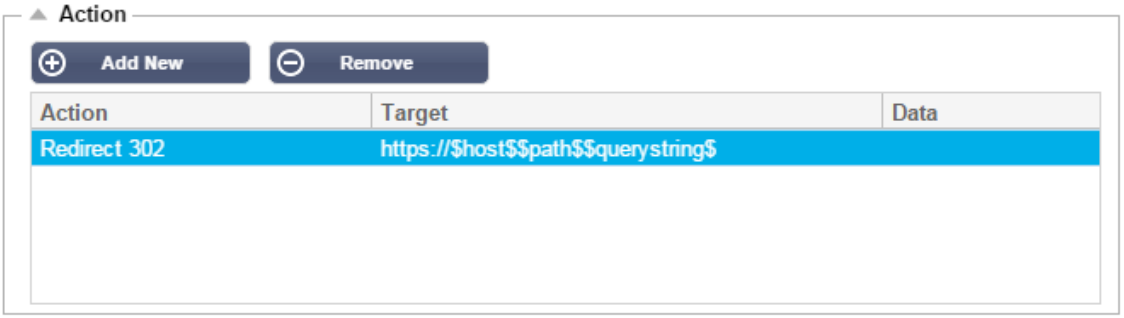
Lingua	Questa è la lingua estratta dall'intestazione HTTP Language	Questa condizione produrrà un menu a tendina con un elenco di lingue.
Metodo	Questo è un menu a tendina dei metodi HTTP	Il menu a tendina includerà GET, POST
Percorso	Questo è il percorso del sito web	/mywebsite/index.html
POST	Metodo di richiesta POST	Controllare i dati che vengono caricati su un sito web
Voce della query	Questo è il nome e il valore di una query. Come tale può accettare il nome della query o anche un valore	"Best=jetNEXUS" dove la corrispondenza è Best e il valore è edgeNEXUS
Stringa di query	Questa è l'intera stringa dopo il carattere ?	HTTP://server/path/programma?query_string
Intestazione della richiesta	Questa può essere qualsiasi intestazione inviata dal client	Referrer, User-Agent, From, Date...
Intestazione della risposta	Questa può essere qualsiasi intestazione inviata dal server	Referrer, User-Agent, From, Date...
Versione	Questa è la versione HTTP	HTTP/1.0 o HTTP/1.1

Dettaglio	**Descrizione**	**Esempio**
Accettare	Tipi di contenuto accettabili	Accettare: text/plain
Accept-Encoding	Codifiche accettabili	Accept-Encoding: <compress | gzip | deflate | sdch | identity>
Accept-Language	Lingue accettabili per la risposta	Accetta la lingua: it-US
Accept-Range	Quali tipi di intervallo di contenuto parziale supporta questo server	Accetta: bytes
Autorizzazione	Credenziali di autenticazione per l'autenticazione HTTP	Autorizzazione: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Carica a	Contiene informazioni contabili per i costi dell'applicazione del metodo richiesto	
Content-Encoding	Il tipo di codifica usato sui dati.	Codifica dei contenuti: gzip
Content-Length	La lunghezza del corpo della risposta in ottetti (byte a 8 bit)	Lunghezza del contenuto: 348
Content-Type	Il tipo mime del corpo della richiesta (usato con richieste POST e PUT)	Content-Type: application/x-www-form-urlencoded
Cookie	un cookie HTTP precedentemente inviato dal server con Set-Cookie (sotto)	Cookie: $Version=1; Skin=new;
Data	Data e ora in cui il messaggio è stato originato	Data = "Data" ":" HTTP-date
ETag	Un identificatore per una versione specifica di una risorsa, spesso un message digest	ETag: "aed6bdb8e090cd1:0"
Da	L'indirizzo e-mail dell'utente che fa la richiesta	Da: user@example.com
Se-Modificato-Da	Permette di restituire un 304 Not Modified se il contenuto è invariato	Se-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Ultimo-Modificato	La data dell'ultima modifica dell'oggetto richiesto, nel formato RFC 2822	Ultimo-Modificato: Tue, 15 Nov 1994 12:45:26 GMT

Pragma	Intestazioni specifiche dell'implementazione che possono avere vari effetti in qualsiasi punto della catena richiesta-risposta.	Pragma: no-cache
Referrer	Questo è l'indirizzo della pagina web precedente da cui è stato seguito un collegamento alla pagina attualmente richiesta	Referente: HTTP://www.edgenexus.io
Server	Un nome per il server	Server: Apache/2.4.1 (Unix)
Set-Cookie	un cookie HTTP	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
User-Agent	La stringa dell'agente dell'utente	User-Agent: Mozilla/5.0 (compatibile; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Variare	Dice ai proxy downstream come abbinare le future intestazioni di richiesta per decidere se la risposta in cache può essere usata piuttosto che richiederne una nuova dal server d'origine	Vary: User-Agent
X-Powered-By	Specifica la tecnologia (ad esempio ASP.NET, PHP, JBoss) che supporta l'applicazione web	X-Powered-By: PHP/5.4.0

Azione

L'azione è il compito o i compiti che sono attivati una volta che la condizione o le condizioni sono state soddisfatte.



Azione

Doppio clic sulla colonna Azione per visualizzare l'elenco a discesa.

Obiettivo

Fai doppio clic sulla colonna Target per visualizzare l'elenco a discesa. L'elenco cambierà a seconda dell'Azione.

Si può anche digitare manualmente con alcune azioni.

Dati

Fai doppio clic sulla colonna Data per aggiungere manualmente i dati che vuoi aggiungere o sostituire.

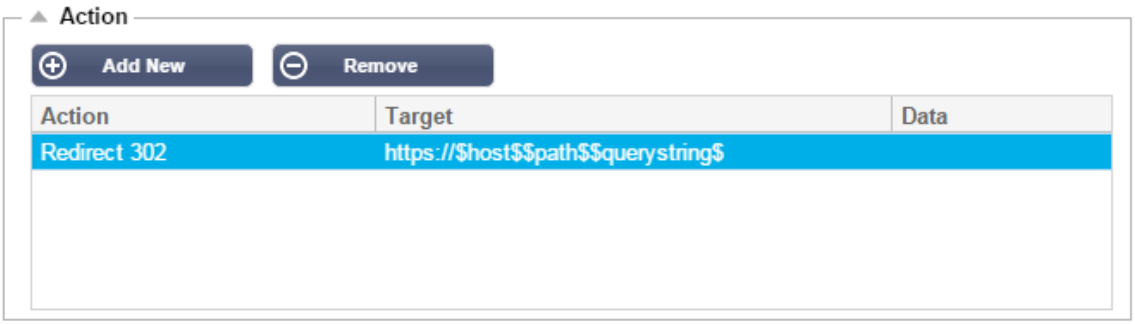
L'elenco di tutte le azioni sono dettagliate qui sotto:

Azione	Descrizione	Esempio

Aggiungi il cookie della richiesta	Aggiungere il cookie di richiesta dettagliato nella sezione Target con il valore nella sezione Data	Target= Cookie Dati= MS-WSMAN=afYfn1CDqqCDqCVii
Aggiungi l'intestazione della richiesta	Aggiungere un'intestazione di richiesta di tipo Target con valore nella sezione Data	Obiettivo= Accettare Dati= immagine/png
Aggiungi un cookie di risposta	Aggiungere il cookie di risposta dettagliato nella sezione Target con il valore nella sezione Data	Target= Cookie Dati= MS-WSMAN=afYfn1CDqqCDqCVii
Aggiungere l'intestazione della risposta	Aggiungere l'intestazione della richiesta dettagliata nella sezione Target con il valore nella sezione Data	Target= Cache-Control Dati= max-age=8888888
Corpo Sostituisci tutto	Cerca nel corpo della risposta e sostituisci tutte le istanze	Target= HTTP:// (stringa di ricerca) Data= HTTPs:// (stringa di sostituzione)
Il corpo si sostituisce prima	Cerca nel corpo della risposta e sostituisci solo la prima istanza	Target= HTTP:// (stringa di ricerca) Data= HTTPs:// (stringa di sostituzione)
Sostituire il corpo per ultimo	Cerca nel corpo della risposta e sostituisci solo l'ultima istanza	Target= HTTP:// (stringa di ricerca) Data= HTTPs:// (stringa di sostituzione)
Goccia	Questo farà cadere la connessione	Obiettivo= N/A Dati= N/A
e-Mail	Invierà un'email all'indirizzo configurato in Eventi email. Puoi usare una variabile come indirizzo o come messaggio	Target= "flightPATH ha inviato questo evento per email" Dati= N/A
Evento di registro	Questo registrerà un evento nel registro di sistema	Target= "flightPATH ha registrato questo nel syslog" Dati= N/A
Reindirizzare 301	Questo emetterà un reindirizzamento permanente	Target= HTTP://www.edgenexus.ioData= N/A
Reindirizzare 302	Questo emetterà un reindirizzamento temporaneo	Target= HTTP://www.edgenexus.ioData= N/A
Rimuovere il cookie di richiesta	Rimuovere il cookie di richiesta dettagliato nella sezione Target	Target= Cookie Dati= MS-WSMAN=afYfn1CDqqCDqCVii
Rimuovere l'intestazione della richiesta	Rimuovere l'intestazione della richiesta dettagliata nella sezione Target	Target=ServerData=N/A
Rimuovere il cookie di risposta	Rimuovere il cookie di risposta dettagliato nella sezione Target	Target=jnAccel
Rimuovere l'intestazione della risposta	Rimuovere l'intestazione di risposta dettagliata nella sezione Target	Target= Etag Dati= N/A
Sostituire il cookie della richiesta	Sostituire il cookie di richiesta dettagliato nella sezione Target con il valore nella sezione Data	Target= Cookie Dati= MS-WSMAN=afYfn1CDqqCDqCVii
Sostituire l'intestazione della richiesta	Sostituire l'intestazione della richiesta nel Target con il valore Data	Target= Connessione Data= keep-alive
Sostituire il cookie di risposta	Sostituire il cookie di risposta dettagliato nella sezione Target con il valore nella sezione Data	Target=jnAccel=afYfn1CDqqCDqCViiDate=MS-WSMAN=afYfn1CDqqCDqCVii

Sostituire l'intestazione della risposta	Sostituire l'intestazione di risposta dettagliata nella sezione Target con il valore nella sezione Data	Target= Server Dati= Trattenuti per sicurezza
Riscrivere il percorso	Questo vi permetterà di reindirizzare la richiesta a un nuovo URL in base alla condizione	Target= /test/path/index.html$querystring$ Dati= N/A
Utilizzare un server sicuro	Selezionare quale server sicuro o servizio virtuale utilizzare	Target=192.168.101: 443Data=N/A
Utilizzare il server	Selezionare quale server o servizio virtuale utilizzare	Target= 192.168.101:80Data= N/A
Crittografare il cookie	Questo cripterà i cookie in 3DES e poi li codificherà in base64	Target= Inserisci il nome del cookie da criptare, puoi usare * come carattere jolly alla fineData= Inserisci una pass phrase per la criptazione

Esempio:



L'azione qui sotto emetterà un reindirizzamento temporaneo al browser verso un servizio virtuale HTTPS sicuro. Utilizzerà lo stesso hostname, percorso e querystring della richiesta.

Usi comuni

Firewall e sicurezza delle applicazioni

- Bloccare gli IP indesiderati
- Forzare l'utente a HTTPS per contenuti specifici (o tutti)
- Bloccare o reindirizzare gli spider
- Prevenire e avvisare il cross-site scripting
- Prevenire e avvisare l'iniezione SQL
- Nascondere la struttura interna delle directory
- Riscrivere i cookie
- Directory sicura per utenti particolari

Caratteristiche

- Reindirizzare gli utenti in base al percorso
- Fornire l'accesso unico su più sistemi
- Segmentare gli utenti in base all'ID utente o al cookie
- Aggiungere intestazioni per SSL offload
- Rilevamento della lingua
- Riscrivere la richiesta dell'utente
- Fissare gli URL non funzionanti
- Log e Email Alert 404 codici di risposta
- Impedire l'accesso/la navigazione nelle directory
- Invia agli spider contenuti diversi

Regole pre-costruite

Estensione HTML

Cambia tutte le richieste .htm in .html

Condizione:

- Condizione = Percorso
- Senso = fa
- Controllare = Corrisponde a RegEx
- Valore = \"htm$

Valutazione:

- Vuoto

Azione:

- Azione = Riscrivere il percorso
- Obiettivo = $path$l

Indice.html

Forzare l'uso di index.html nelle richieste alle cartelle.

Condizione: questa condizione è una condizione generale che corrisponderà alla maggior parte degli oggetti

- Condizione = Host
- Senso = fa
- Controllare = Esistere

Valutazione:

- Vuoto

Azione:

- Azione = Redirect 302
- Target = HTTP://$host$$path$index.html$querystring$

Chiudere le cartelle

Negare le richieste di cartelle.

Condizione: questa condizione è una condizione generale che corrisponderà alla maggior parte degli oggetti

- Condizione = questo ha bisogno di una riflessione adeguata
- Senso =
- Controllare =

Valutazione:

- Vuoto

Azione:

- Azione =
- Obiettivo =

Nascondi CGI-BBIN:

Nasconde il catalogo cgi-bin nelle richieste agli script CGI.

Condizione: questa condizione è una condizione generale che corrisponderà alla maggior parte degli oggetti

- Condizione = Host
- Senso = fa
- Controllare = Corrisponde a RegEX
- Valore = \Cgi$

Valutazione:

- Vuoto

Azione:

- Azione = Riscrivere il percorso
- Obiettivo = /cgi-bin$path$

Ragno del tronco

Registra le richieste di spider dei motori di ricerca più popolari.

Condizione: questa condizione è una condizione generale che corrisponderà alla maggior parte degli oggetti

- Condizione = Intestazione della richiesta
- Partita = User-Agent
- Senso = fa
- Controllare = Corrisponde a RegEX
- Valore = Googlebot|Slurp|bingbot|ia_archiver

Valutazione:

- Variabile = $crawler$
- Fonte = Intestazione della richiesta
- Dettaglio = User-Agent

Azione:

- Azione = Registra evento
- Target = [$crawler$] $host$$path$$querystring$

Forza HTTPS

Forza l'uso di HTTPS per certe directory. In questo caso, se un client accede a qualcosa che contiene la directory /secure/, sarà reindirizzato alla versione HTTPs dell'URL richiesto.

Condizione:

- Condizione = Percorso
- Senso = fa
- Controllare = Contenere
- Valore = /sicuro/

Valutazione:

- Vuoto

Azione:

- Azione = Redirect 302
- Target = HTTPs://$host$$path$$querystring$

Flusso dei media:

Reindirizza Flash Media Stream al servizio appropriato.

Condizione:

- Condizione = Percorso
- Senso = fa
- Controllare = Fine
- Valore = .flv

Valutazione:

- Vuoto

Azione:

- Azione = Redirect 302
- Target = HTTP://$host$:8080/$path$

Scambiare HTTP con HTTPS

Cambiare qualsiasi HTTP:// hardcoded in HTTPS://

Condizione:

- Condizione = Codice di risposta
- Senso = fa
- Controllare = uguale
- Valore = 200 OK

Valutazione:

- Vuoto

Azione:

- Azione = Corpo Sostituisci tutto
- Obiettivo = HTTP://
- Dati = HTTPs://

Svuotare le carte di credito

Controlla che non ci siano carte di credito nella risposta e se ne viene trovata una, cancellala.

Condizione:

- Condizione = Codice di risposta
- Senso = fa
- Controllare = uguale
- Valore = 200 OK

Valutazione:

- Vuoto

Azione:

- Azione = Corpo Sostituisci tutto
- 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]+
- Dati = xxxx-xxxx-xxxx-xxxx

Scadenza del contenuto

Aggiungete una data di scadenza sensata del contenuto alla pagina per ridurre il numero di richieste e di 304.

Condizione: questa è una condizione generica che serve a prendere tutto. Si raccomanda di concentrare questa condizione sul tuo

- Condizione = Codice di risposta
- Senso = fa
- Controllare = uguale
- Valore = 200 OK

Valutazione:

- Vuoto

Azione:

- Azione = Aggiungi l'intestazione della risposta
- Obiettivo = Cache-Control
- Dati = max-age=3600

Tipo di server spoof

Prendete il tipo di Server e cambiatelo in qualcos'altro.

Condizione: questa è una condizione generica che serve a prendere tutto. Si raccomanda di concentrare questa condizione sul tuo

- Condizione = Codice di risposta
- Senso = fa
- Controllare = uguale
- Valore = 200 OK

Valutazione:

- Vuoto

Azione:

- Azione = Sostituire l'intestazione della risposta
- Obiettivo = Server
- Dati = Segreto

Non inviare mai errori

Il cliente non riceve mai errori dal vostro sito.

Condizione

- Condizione = Codice di risposta
- Senso = fa
- Controllare = Contenere
- Valore = 404

Valutazione

- Vuoto

Azione

- Azione = Redirect 302
- Obiettivo = HTTP//$host$/

Reindirizzamento sulla lingua

Trova il codice della lingua e reindirizza al dominio del paese relativo.

Condizione

- Condizione = Lingua
- Senso = fa
- Controllare = Contenere
- Valore = tedesco (standard)

Valutazione

- Variabile = $host_template$
- Fonte = Host
- Valore = .*\.

Azione

- Azione = Redirect 302
- Target = HTTP//$host_template$de$path$$querystring$

Google Analytics

Inserisci il codice richiesto da Google per l'analitica - Cambia il valore MYGOOGLECODE con il tuo Google UA ID.

Condizione

- Condizione = Codice di risposta
- Senso = fa
- Controllare = uguale
- Valore = 200 OK

Valutazione

- vuoto

Azione

- Azione = Corpo sostituire ultimo
- Obiettivo = </body>
- Data = <scripttype= 'text/javascript'> var _gaq = _gaq || []; _gaq.push(['_setAccount', 'MY GOOGLE CODE']); _gaq.push(['_trackPageview']); (function() { var ga = document.createElement('script'); ga.type = 'text/javascript'; ga.async = true; ga.src = ('HTTPs' == document.location.protocol ?'HTTPs//ssl' 'HTTP//www') + '.google-analytics.com/ga.js'; var s = document.getElementsByTagName('script')[0];s.parentNode.insertBefore(ga, s); })(); </script> </body>

Gateway IPv6

Regolare l'intestazione dell'host per i server IIS IPv4 sui servizi IPv6. Ai server IIS IPv4 non piace vedere un indirizzo IPV6 nella richiesta del client host, quindi questa regola lo sostituisce con un nome generico.

Condizione

- vuoto

Valutazione

- vuoto

Azione

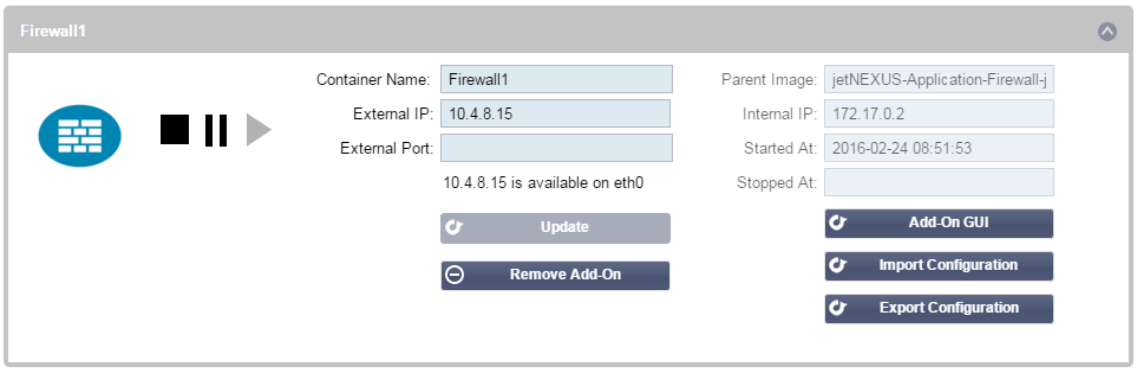
- Azione = Sostituisci l'intestazione della richiesta
- Obiettivo = Host
- Dati =ipv4.host.header

Web Application Firewall (edgeWAF)

Il Web Application Firewall (WAF) è disponibile su richiesta ed è concesso in licenza su base annuale a pagamento. L'installazione del WAF viene fatta usando la sezione Apps integrata nell'ADC.

Esecuzione del WAF

Eseguito in un contenitore Docker, il WAF ha bisogno di alcuni parametri di rete da impostare prima di avviarlo.

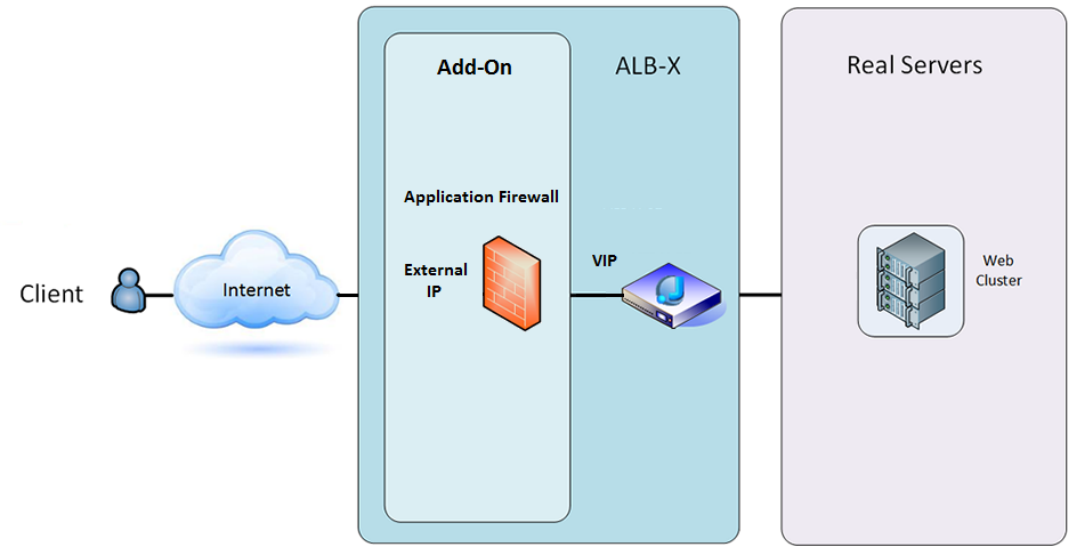


Opzione	**Descrizione**
Fermare	Sarà in grigio fino a quando non verrà avviata un'istanza Add-On. Premi questo pulsante per fermare l'istanza Docker.
Pausa	Questo pulsante mette in pausa l'Add-On.
Gioca	Avvierà l'Add-On con le impostazioni correnti.
Nome del contenitore	Dai al tuo contenitore un nome per identificarlo dagli altri contenitori. Questo deve essere unico. Puoi usarlo come nome per un Real Server se vuoi e si risolverà automaticamente all'indirizzo IP interno dell'istanza
IP esterno	Qui potete impostare un IP esterno per accedere al vostro modulo aggiuntivo. Questo può essere per accedere alla GUI dell'add-on così come al servizio che viene eseguito tramite l'add-on. Nel caso dell'add-on Firewall questo è l'indirizzo IP del vostro servizio HTTP. Il Firewall può quindi essere configurato per accedere a un server o a un ALB-X VIP che contiene più server per il bilanciamento del carico.
Porta esterna	Se lasciate questo vuoto, allora tutte le porte saranno inoltrate al vostro Firewall. Per limitare questo, basta aggiungere la lista di porte separate da virgole. Esempio 80, 443, 88. Nota l'indirizzo della GUI del Firewall sarà **HTTP//[IP esterno]88/waf.** Quindi, o lasciate vuota l'impostazione della porta esterna o aggiungete la porta 88 per accedere alla GUI se state limitando l'elenco delle porte.
Aggiornamento	Puoi aggiornare le impostazioni di un Add-On solo dopo che è stato fermato. Una volta che la tua istanza si è fermata puoi cambiare il nome del contenitore, l'IP esterno e le impostazioni della porta esterna.
Rimuovi Add-On	Rimuoverà completamente l'Add-On dalla pagina Add-On. Dovrai andare alla pagina Library-Apps per distribuire nuovamente l'Add-On.
Immagine del genitore	Indica l'immagine Docker da cui è costruito l'Add-On. Ci potrebbero essere diverse versioni di un Firewall o di un altro tipo di Add-On completamente, quindi questo aiuterà a distinguerle. Questa sezione è solo a scopo informativo e quindi è in grigio.
IP interno	Docker crea automaticamente l'indirizzo IP interno e, pertanto, non può essere modificato. Se si ferma l'istanza Docker e si riavvia, verrà emesso un nuovo indirizzo IP interno. È per questo motivo che dovreste usare un indirizzo IP esterno per il vostro servizio o usare il Container Name per il Real Server Address del vostro servizio.

Iniziato a	Questo indicherà la data e l'ora in cui l'Add-On è stato avviato. Esempio 2016-02-16 155721
Fermato a	Questo indicherà la data e l'ora in cui l'Add-On è stato fermato. Esempio 2016-02-24 095839

Esempio di architettura

WAF con indirizzo IP esterno

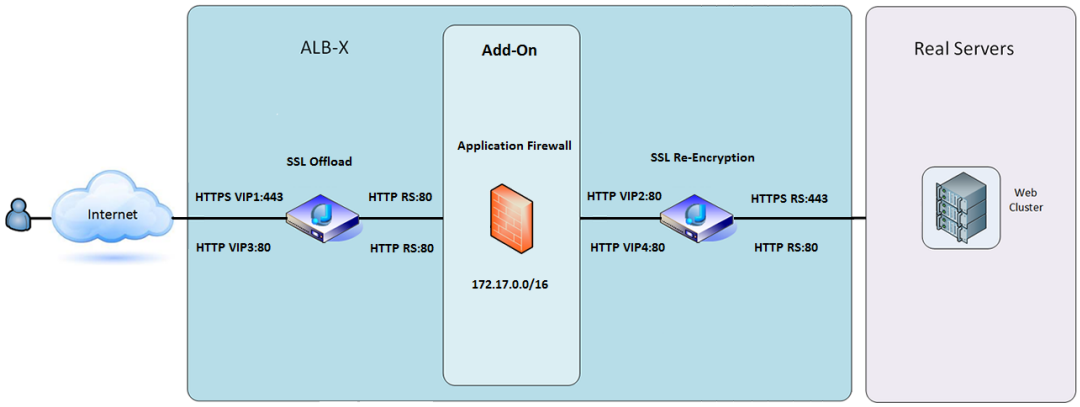


In questa architettura, solo HTTP può essere usato per il vostro servizio, poiché il Firewall non può ispezionare il traffico HTTPS.

Il Firewall dovrà essere configurato per inviare il traffico al VIP ALB-X.

Il VIP ALB-X, a sua volta, sarà configurato per bilanciare il traffico verso il tuo cluster web.

WAF utilizzando l'indirizzo IP interno



In questa architettura, è possibile specificare HTTP e HTTPS.

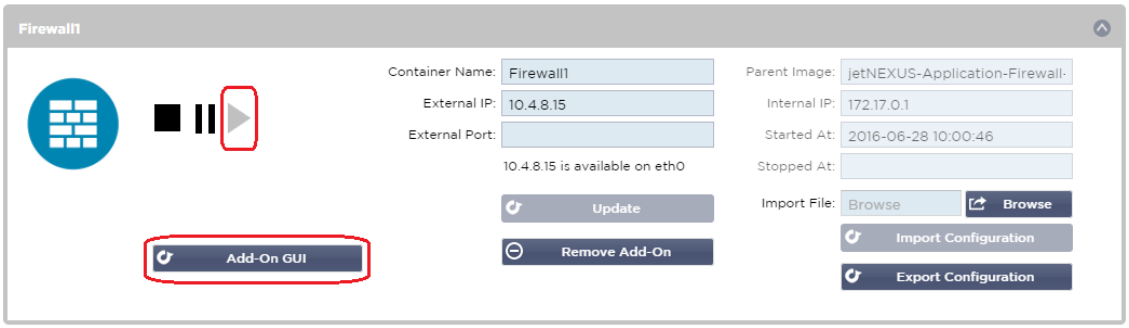
HTTPS può essere end-to-end dove le connessioni dal client all'ALB-X sono criptate e dall'ALB-X ai Real Server.

Il traffico da ALB-X all'indirizzo IP interno del firewall deve essere non criptato per poter essere ispezionato.

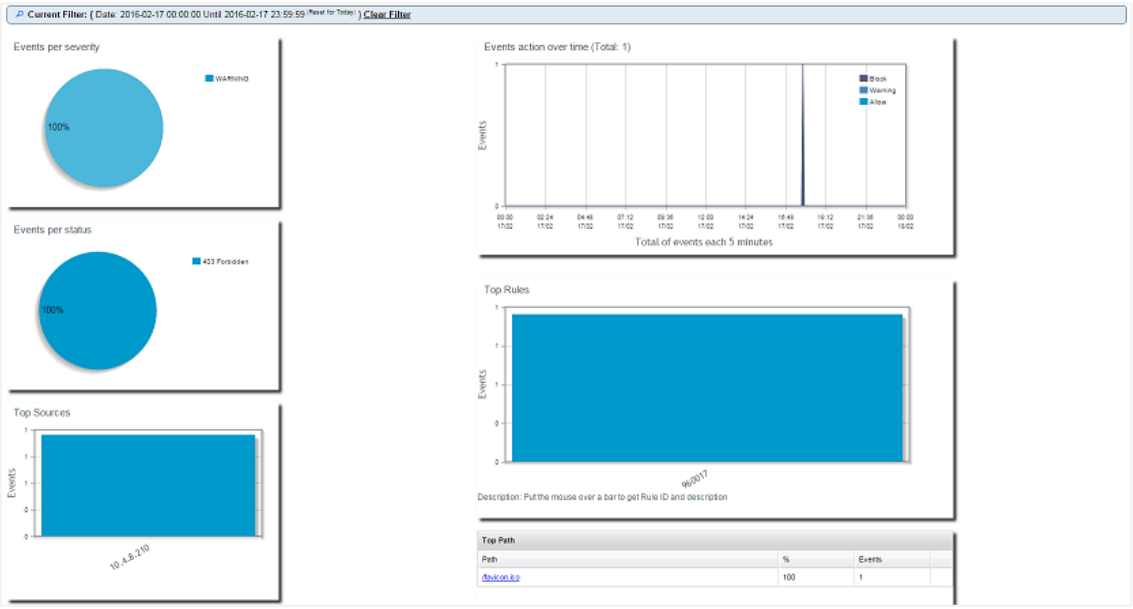
Una volta che il traffico è passato attraverso il firewall, viene poi inoltrato a un altro VIP che può ricodificare il traffico e bilanciare il carico verso server sicuri o semplicemente bilanciare il carico verso server non sicuri su HTTP.

Accesso all'add-on WAF

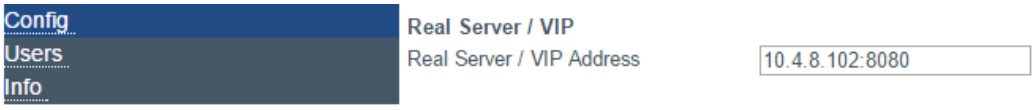
- Compila i dettagli del tuo Firewall
- Puoi limitare le tue porte a ciò di cui hai bisogno o lasciarlo vuoto per permettere tutte le porte
- Fare clic sul pulsante Play
- Apparirà un pulsante dell'interfaccia grafica Add-On



- Cliccando su questo pulsante, si aprirà un browser su HTTP://[IP esterno]:88/waf
- In questo esempio, sarà HTTP://10.4.8.15:88/waf
- Ti verrà presentata una finestra di dialogo di accesso.
- Inserisci le credenziali del tuo ADC.
- Una volta completato con successo il login, vi verrà presentata la pagina iniziale del WAF.

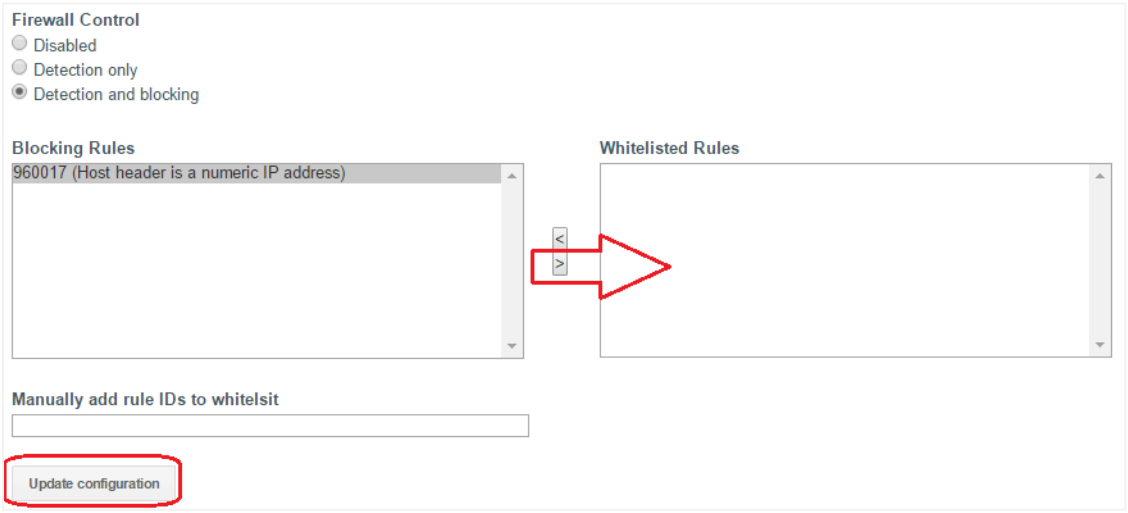


- La pagina iniziale mostra una panoramica grafica degli eventi, cioè delle azioni di filtraggio eseguite dall'Application Firewall.
- I grafici saranno molto probabilmente vuoti quando aprirete la pagina per la prima volta perché non ci saranno tentativi di accesso attraverso il firewall.
- È possibile configurare l'indirizzo IP o il nome di dominio del sito web a cui si desidera inviare il traffico dopo che il firewall lo ha filtrato.
- Questo può essere cambiato nella sezione Gestione > Config



- Il Firewall ispezionerà il traffico e poi lo invierà al Real Sever IP o all'indirizzo VIP qui. Puoi anche inserire una porta insieme all'indirizzo IP. Se inserisci un indirizzo IP da solo, la porta sarà assunta come porta 80. Fai clic sul pulsante "Aggiorna configurazione" per salvare questa nuova impostazione.

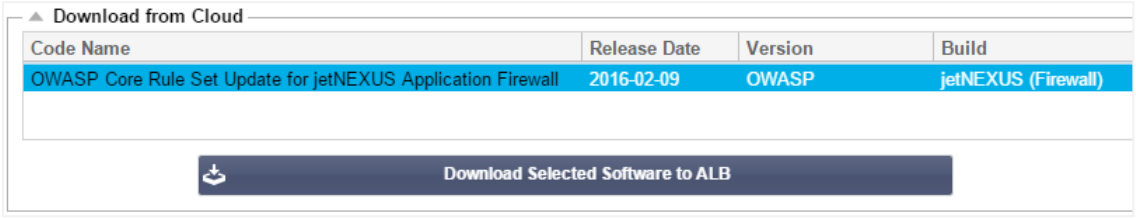
- Quando il Firewall blocca una risorsa dell'applicazione, la regola che sta bloccando il traffico apparirà nell'elenco Regole di blocco nella pagina Whitelist.
- Per evitare che il firewall blocchi la risorsa dell'applicazione valida, sposta la regola di blocco nella sezione Whitelist Rules.



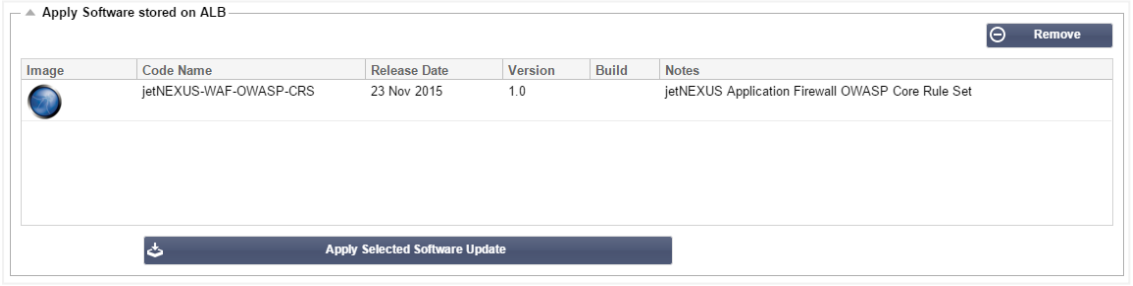
- Premi Aggiorna Configurazione quando hai trasferito tutte le regole dalla sezione Blocco alla sezione Whitelist.

Aggiornamento delle regole

- Le regole di Application Firewall possono essere aggiornate accedendo alla sezione Advanced - Software
- Fare clic su Refresh per visualizzare il pulsante del software disponibile nella sezione Software Upgrade Details
- Ora viene visualizzata una casella aggiuntiva chiamata Download from Cloud
- Controlla se c'è un set di regole OWASP Core disponibile

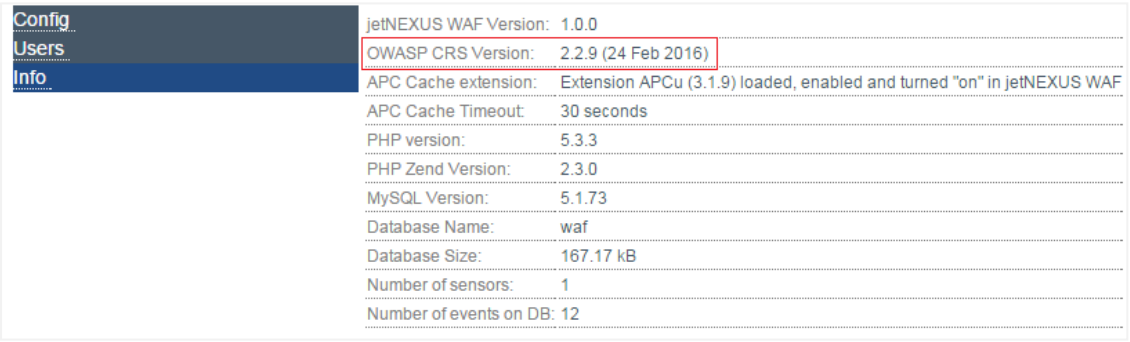


- Se è così, potete evidenziare e cliccare su Download Selected Software to ALB-X
- Questa azione scaricherà poi lo smart file nell'Apply Software memorizzato su ALB



- Evidenziare il jetNEXUS-WAF-OWASP-CRS e cliccare su Apply Selected Software Update e cliccare su Apply
- Il Firewall rileverà automaticamente il set di regole aggiornato, lo caricherà e lo applicherà.
- Gli ID delle regole Whitelisted saranno mantenuti. Tuttavia, le nuove regole possono iniziare a bloccare risorse di applicazioni valide.
- In questo caso controlla l'elenco delle regole di blocco nella pagina Whitelist.

- Puoi anche controllare la sezione Management Info della GUI del firewall per la versione di OWASP CRS



Bilanciamento globale del carico dei server(edgeGSLB)

Introduzione

Global Server Load Balancing (GSLB) è un termine usato per descrivere i metodi di distribuzione del traffico di rete su Internet. GSLB è diverso da Server Load Balancing (SLB) o Application Load Balancing (ALB), poiché è tipicamente usato per distribuire il traffico tra più data center, mentre un ADC/SLB tradizionale è usato per distribuire il traffico all'interno di un singolo data center.

GSLB è tipicamente usato nelle seguenti situazioni:

Resilienza e disaster recovery

Avete più data center e volete gestirli in una situazione attiva-passiva, in modo che se un data center fallisce, il traffico viene inviato all'altro.

Bilanciamento del carico e geo-localizzazione

Vorresti distribuire il traffico tra i data center in una situazione Active-Active in base a criteri specifici come le prestazioni del data center, la capacità del data center, il controllo della salute del data center e la posizione fisica del cliente (in modo da poterlo inviare al data center più vicino), ecc.

Considerazioni commerciali

Assicurarsi che gli utenti provenienti da specifiche località geografiche siano inviati a particolari centri dati. Assicurarsi che vengano serviti (o bloccati) contenuti diversi ad altri utenti, a seconda di diversi criteri come il paese in cui si trova il cliente, la risorsa che sta richiedendo, la lingua, ecc.

Panoramica del sistema dei nomi di dominio

GSLB può essere complesso; vale quindi la pena spendere del tempo per capire come funziona il misterioso sistema Domain Name Server (DNS).

Il DNS è composto da tre componenti chiave:

- Il resolver DNS, cioè il client: il resolver è responsabile dell'avvio delle query che alla fine portano alla risoluzione completa della risorsa richiesta.
- Nameserver: questo è il nameserver a cui il client si connette inizialmente per eseguire la risoluzione DNS.
- Server di nomi autoritativi: Includere i nameserver del dominio di primo livello (TLD) e i nameserver di root.

Una tipica transazione DNS è spiegata qui sotto:

- Un utente digita 'example.com' in un browser web, e la query viaggia in Internet e viene ricevuta da un resolver DNS ricorsivo.
- Il resolver interroga quindi un nameserver root DNS (.).
- Il root server risponde quindi al resolver con l'indirizzo di un server DNS del Top-Level Domain (TLD) (come .com o .net), che memorizza le informazioni per i suoi domini. Quando cerchiamo esempio.com, la nostra richiesta è indirizzata verso il TLD .com.
- Il resolver richiede quindi il TLD .com.
- Il server TLD risponde quindi con l'indirizzo IP del nameserver del dominio, example.com.
- Infine, il resolver ricorsivo invia una query al nameserver del dominio.
- L'indirizzo IP, per esempio.com, viene quindi restituito al resolver dal nameserver.
- Il resolver DNS risponde quindi al browser web con l'indirizzo IP del dominio richiesto inizialmente.
- Una volta che gli otto passi della ricerca DNS hanno restituito l'indirizzo IP, per esempio.com, il browser può richiedere la pagina web:

- Il browser fa una richiesta **HTTP** all'indirizzo IP.
- Il server a quell'IP restituisce la pagina web da rendere nel browser.

Questo processo può essere ulteriormente complicato:

Caching

I resolver di nomi in cache possono inviare la stessa risposta a molti client. I resolver e le applicazioni lato client possono avere diverse politiche di caching.

Nota: per i test, fermiamo e disabilitiamo il client DNS di Windows nella sezione servizi del sistema operativo. I nomi DNS continueranno ad essere risolti; tuttavia, non memorizzerà nella cache i risultati o registrerà il nome del computer. Il vostro amministratore di sistema dovrà decidere se questa è l'opzione migliore per il vostro ambiente, in quanto potrebbe influenzare altri servizi.

Tempo di vivere

Il server dei nomi che risolve può ignorare il Time To Live (TTL), cioè il tempo di caching della risposta.

Panoramica di GSLB

GSLB è basato su DNS e utilizza un meccanismo molto simile a quello descritto sopra.

L'ADC può cambiare la risposta in base a diversi fattori descritti più avanti nella guida. L'ADC fa uso dei monitor che controllano la disponibilità delle risorse remote accedendo alla risorsa stessa. Tuttavia, per applicare qualsiasi logica, il sistema deve prima ricevere la richiesta DNS.

Diversi design lo permettono. Il primo è quello in cui il GSLB agisce come nameserver autoritativo.

Il secondo design è l'implementazione più comune ed è simile alla configurazione del nameserver autoritativo ma usa un sottodominio. Il server DNS autoritativo primario non è sostituito da GSLB ma delega un sottodominio per la risoluzione. Delegare direttamente i nomi o usare i CNAME permette di controllare cosa viene e non viene gestito dal GSLB. In questo caso, non è necessario instradare tutto il traffico DNS al GSLB per i sistemi che non richiedono GSLB.

La ridondanza è fornita in modo che se un nameserver (GSLB) fallisce, allora il nameserver remoto emette automaticamente un'altra richiesta a un altro GSLB, evitando che il sito web vada giù.

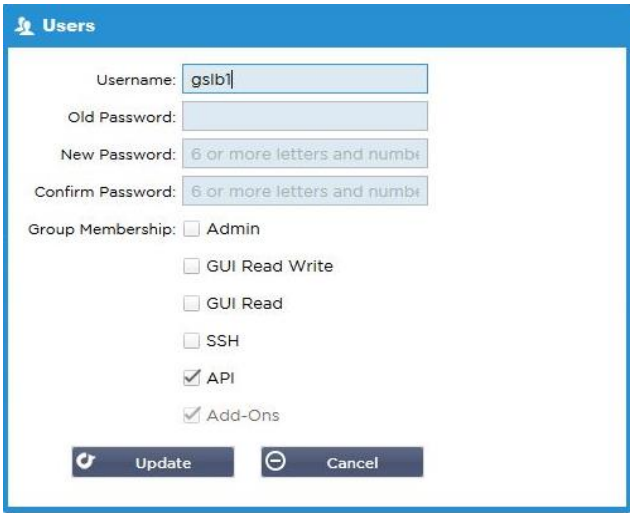
Configurazione GSLB

Dopo aver scaricato il GSLB Add-On, distribuiscilo visitando la pagina Library > Apps della GUI di ADC e cliccando sul pulsante "Deploy" come mostrato di seguito.

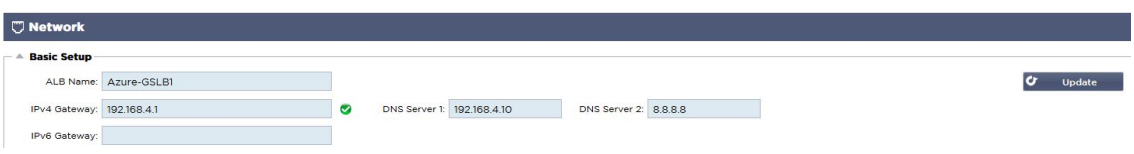
Dopo l'installazione, si prega di configurare i dettagli di GSLB Add-On, compreso il nome del contenitore, l'IP esterno e le porte esterne nella pagina Library > Add-Ons della GUI ADC come mostrato nella figura seguente.

- Container Name è un nome unico di un'istanza di Add-On in esecuzione, ospitata da ADC, viene utilizzato per distinguere più Add-On dello stesso tipo.
- L'IP esterno è l'IP della tua rete che sarà assegnato a GSLB.
- Devi configurare il GSLB per avere un indirizzo IP esterno se vuoi prendere decisioni basate su GEO, perché questo permetterà al GSLB di visualizzare l'indirizzo IP reale dei client.
- External Ports è la lista delle porte TCP e UDP di GSLB, a cui si può accedere da altri host di rete.
- Mettere "53/UDP, 53/TCP, 9393/TCP" nella casella di input External Ports per consentire le comunicazioni DNS (53/UDP, 53/TCP) e edgeNEXUS GSLB GUI (9393/TCP).
- Dopo aver configurato i dettagli dell'Add-On, clicca sul pulsante Update.
- Avvia il GSLB Add-On facendo clic sul pulsante Run.

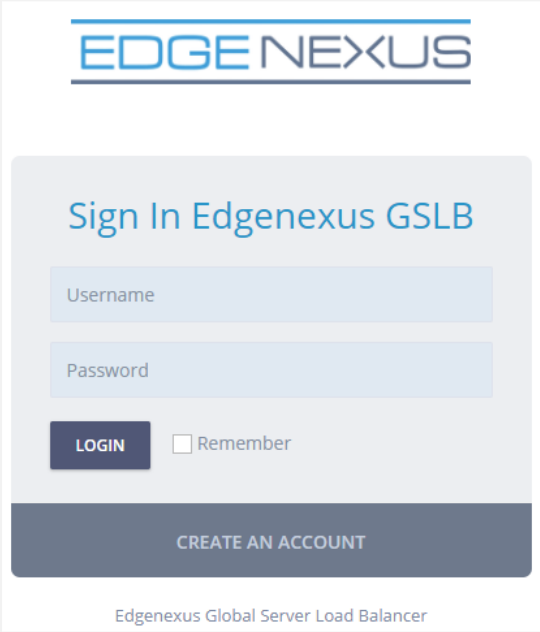
- Il passo successivo è permettere all'edgeNEXUS GSLB Add-On di leggere e modificare la configurazione ADC.
- Visita la pagina Sistema > Utenti di ADC GUI e modifica un utente con lo stesso nome del GSLB Add-On che hai distribuito, come mostrato nella figura seguente.
- Modifica l'utente "gslb1" e spunta API, poi clicca su Update - nelle versioni successive del software potrebbe essere già spuntato di default.



- Il prossimo passo è richiesto solo se state configurando GSLB per scopi di test o valutazione e non volete modificare alcun dato di zona DNS su internet.
- In questo caso, istruisci l'ADC ad usare GSLB Add-On come server primario di risoluzione DNS modificando "DNS Server 1 nella pagina Sistema > Rete dell'ADC GUI, come mostrato nella figura seguente.
- Il DNS Server 2 può essere configurato generalmente con il vostro server DNS locale o uno su Internet, come Google 8.8.8.8.

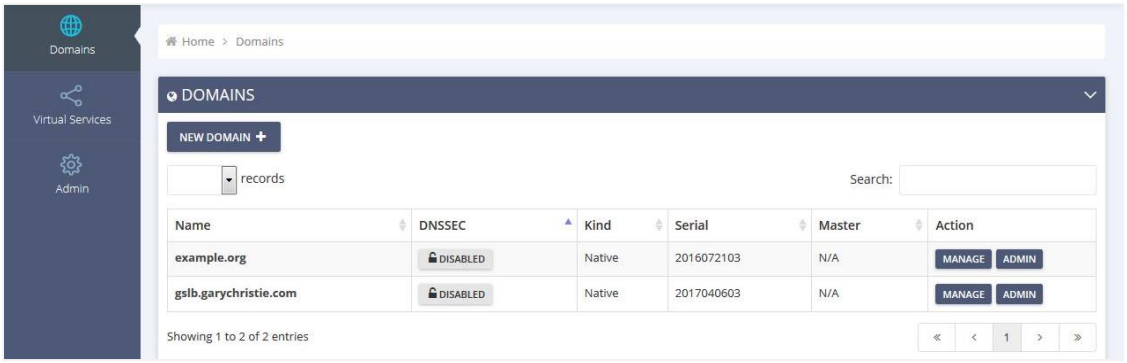


- Ora è il momento di accedere alla GUI di GSLB.
- Vai alla pagina Library > Add-Ons della GUI ADC e clicca sul pulsante Add-On GUI.
- Cliccando si aprirà una nuova scheda del browser che presenta la pagina di accesso alla GUI GSLB, come mostrato di seguito.

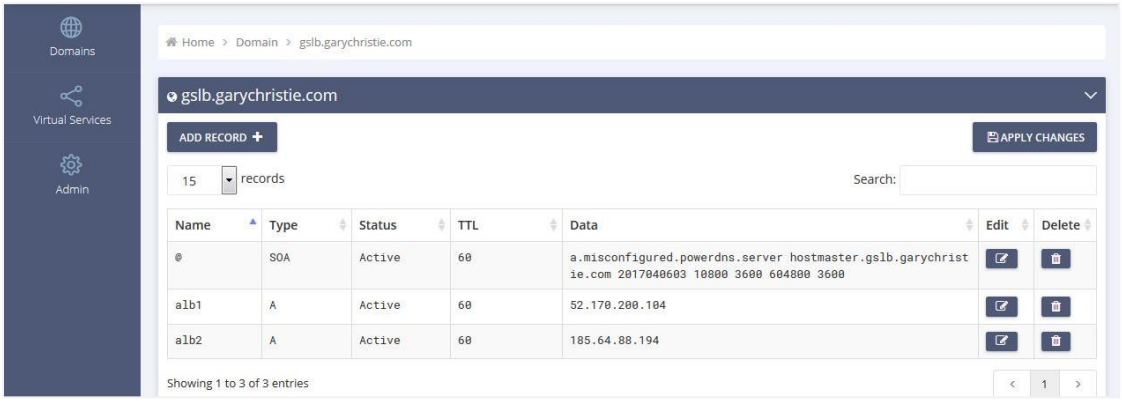


- Il nome utente predefinito è admin, e la password predefinita è jetnexus. Non dimenticare di cambiare la password nella pagina Amministratore > Il mio profilo di GSLB GUI.
- Il passo successivo nella sequenza di configurazione è quello di creare una zona DNS nel nameserver PowerDNS, che è una parte di GSLB, rendendolo o un nameserver autoritativo per la zona "example.org" o una zona di sottodominio, come il sottodominio "geo.example.org" menzionato nella sezione "Panoramica di GSLB basata su DNS" sopra.
- Per dettagli approfonditi sulla configurazione delle zone DNS, si prega di consultare la **DOCUMENTAZIONE DI POWERDNS NAMESERVER**. Un esempio di zona è mostrato nella Figura 6.

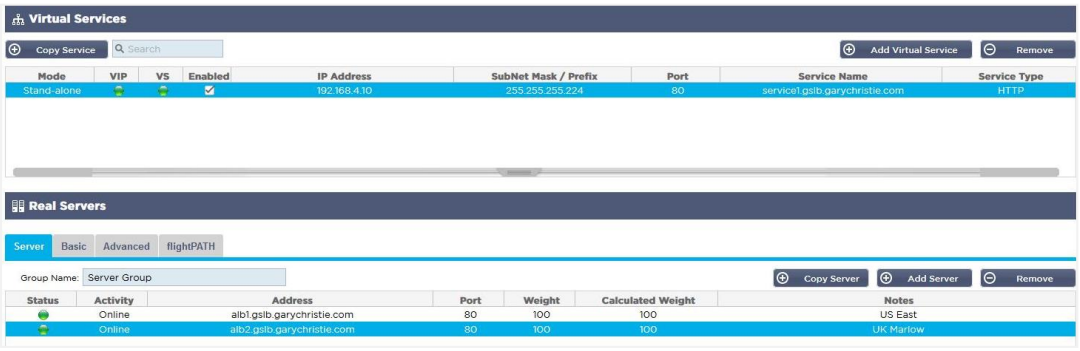
edgeNEXUS GSLB GUI è basato su un progetto Open Source PowerDNS-Admin.



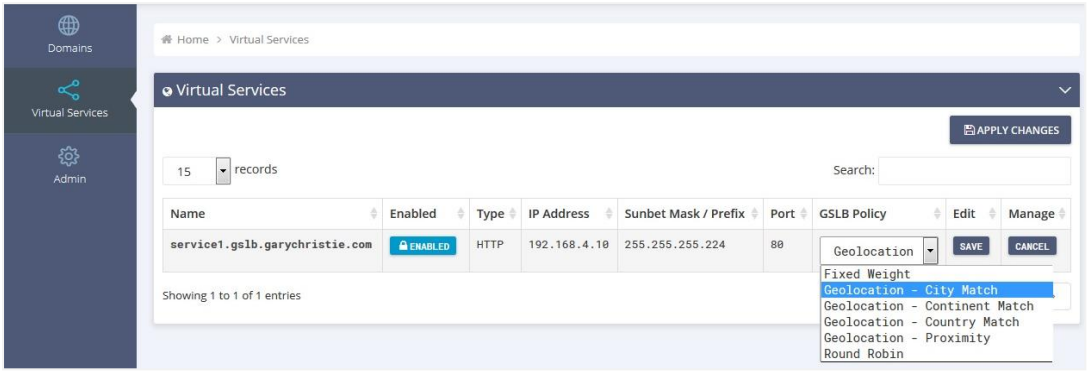
- Dopo aver creato una zona DNS, cliccate sul pulsante Manage e aggiungete gli hostname al dominio, come mostrato nella figura sottostante.
- Dopo aver modificato qualsiasi record esistente all'interno della GUI GSLB, premi il pulsante Salva.
- Dopo aver completato la creazione dei record di hostname, clicca sul pulsante Apply Changes. Se non clicchi su Apply e poi modifichi la pagina, perderai le tue modifiche.
- Qui sotto abbiamo creato dei record che sono record di indirizzi IPv4.
- Assicurati di creare un record per tutti i record che vuoi far risolvere, compresi i record AAAA per gli indirizzi IPv6.



- Ora, torniamo alla GUI ADC e definiamo un servizio virtuale che corrisponde alla zona DNS che abbiamo appena creato.



- Il servizio virtuale sarà utilizzato per il controllo dello stato di salute dei server nel dominio GSLB.
- Il GSLB sfrutta il meccanismo di controllo della salute dell'ADC, compresi i monitor personalizzati. Può essere utilizzato con qualsiasi tipo di servizio supportato dall'ADC.
- Vai alla pagina Services > IP-Services della GUI ADC e crea un servizio virtuale, come mostrato nella figura qui sotto.
- Assicuratevi di configurare il Service Name con il nome di dominio corretto che volete usare nel GSLB. GSLB leggerà questo tramite l'API e popolerà automaticamente la sezione Virtual Services nella GUI di GSLB.
- Aggiungi tutti i server nel dominio GSLB sotto la sezione Real Servers dell'immagine precedente.
- Potete specificare i server, sia per i loro nomi di dominio che per gli indirizzi IP.
- Se specificate i nomi di dominio, allora userà i record creati sul vostro GSLB.
- Puoi scegliere diversi metodi e parametri di monitoraggio della salute del server nelle schede Basic e Advanced.
- È possibile impostare l'attività di alcuni server su Standby per uno scenario attivo-passivo.
- In questo caso, se un server "Online" fallisce un controllo di salute e c'è un server Standby sano, Edgenexus EdgeGSLB risolverà il nome di dominio ad un indirizzo del server Standby.
- Fate riferimento alla sezione **SERVIZI VIRTUALI** per i dettagli sulla configurazione dei servizi virtuali.
- Ora, passiamo alla GUI di GSLB.
- Passate alla pagina dei servizi virtuali e selezionate una politica GSLB per il dominio dell'API recuperato dalla sezione dei servizi virtuali ADC.
- Questo è mostrato nella figura qui sotto.



- Il GSLB sostiene le seguenti politiche:

Politica	Descrizione
Peso fisso	Il GSLB seleziona il server con il peso più alto (il peso del server può essere assegnato dall'utente). Nel caso in cui più server abbiano il peso più alto, GSLB selezionerà uno di questi server a caso.
Round Robin ponderato	Scegli i server uno per uno, in fila. I server che hanno pesi più alti sono selezionati più spesso di quelli che hanno pesi più bassi.
Geolocalizzazione	Prossimità - scegliere un server che si trova più vicino alla posizione del cliente utilizzando i dati geografici di latitudine e longitudine. I server nello stesso paese del cliente sono preferiti, anche se sono più distanti dei server nei paesi vicini.
Geolocalizzazione	City match - scegli un server nella stessa città del client. Se non c'è un server nella città del cliente, seleziona un server nel paese del cliente. Se non c'è un server nel paese del cliente, seleziona un server nello stesso continente. Se questo non è possibile, seleziona un server che si trova più vicino alla posizione del client utilizzando i dati geografici di latitudine e longitudine.
Geolocalizzazione	Country match - sceglie un server nello stesso paese del client. Se non c'è un server nello stesso paese, prova lo stesso continente, poi prova la località più vicina.
Geolocalizzazione	Continent match - sceglie un server nello stesso continente del client. Se non c'è un server nello stesso continente, prova la posizione più vicina.

- Dopo aver selezionato una politica GSLB, non dimenticare di cliccare sul pulsante Apply Changes.
- Ora potete rivedere e regolare i dettagli del servizio virtuale cliccando sul pulsante Gestisci.
- Questo presenterà una pagina mostrata qui sotto.
- Se avete selezionato una delle politiche basate sul peso, potreste aver bisogno di regolare i pesi GSLB del server.
- Se hai selezionato una delle politiche GSLB basate sulla geo-localizzazione, potrebbe essere necessario specificare i dati geografici per i server.
- Se non si specifica alcun dato geografico per i server, il GSLB userà i dati forniti dal **DATABASE GEOLITE2 DI MAXMIND**.
- Puoi anche modificare il nome del server, la porta e l'attività in questa pagina.
- Queste modifiche saranno sincronizzate con l'ADC quando si clicca sul pulsante "Apply Changes".

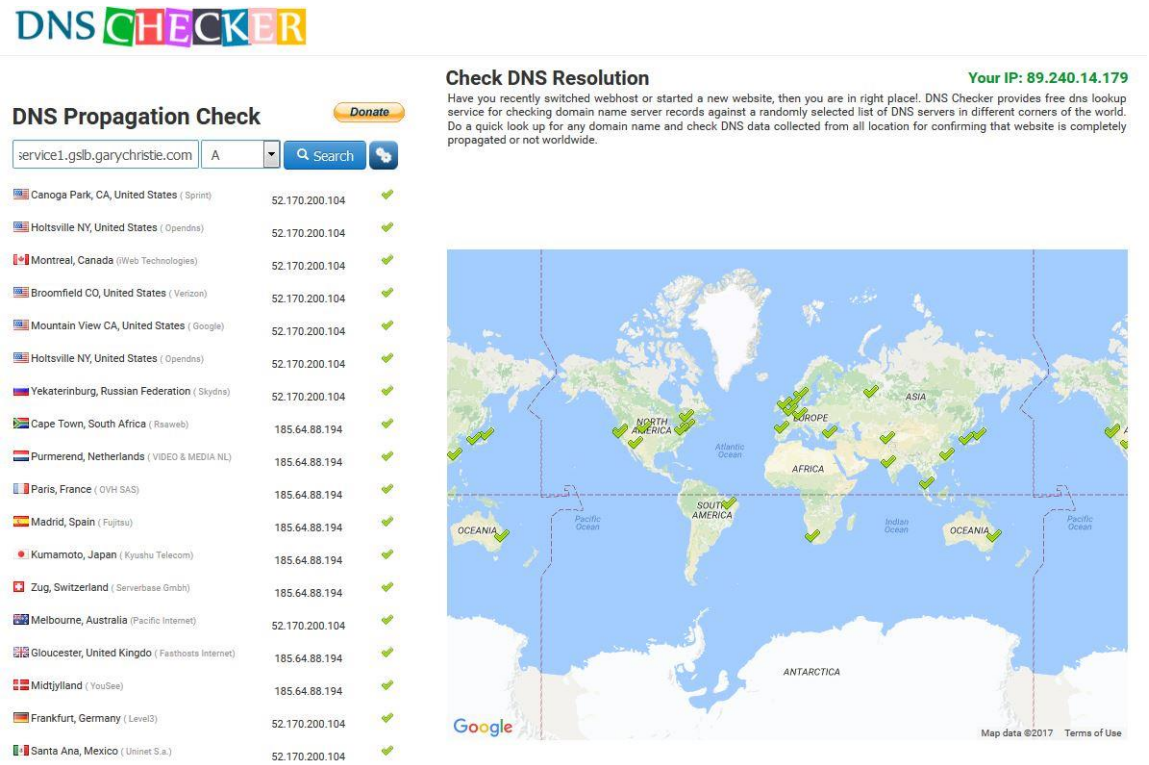
- Un ottimo modo per controllare quali risposte il GSLB rimanderà ai clienti è usare NSLOOKUP.
- Se state usando Windows, il comando è qui sotto.

NSLOOKUP service1.gslb.garychristie.com 192.168.4.10

- Dove service1.gslb.garychristie.com è il nome di dominio che volete risolvere.
- Dove 192.168.4.10 è l'indirizzo IP esterno del tuo GSLB.
- Per controllare quale indirizzo IP sarà restituito su internet, potete usare il server DNS di google 8.8.8.8.

Nslookup service1.gslb.garychristie.com 8.8.8.8.

- In alternativa, puoi usare qualcosa come HTTPs://dnschecker.org.
  Esempio HTTPs://dnschecker.org/#A/service1.gslb.garychristie.com.
- Vedi sotto per un esempio dei risultati.



Luoghi personalizzati

Reti private

Il GSLB può anche essere configurato per usare posizioni personalizzate in modo da poterlo usare su reti interne "private". Nello scenario sopra, il GSLB determina la posizione del client incrociando l'indirizzo IP pubblico del client con un database per determinare la sua posizione. Inoltre calcola la posizione dell'indirizzo IP del servizio dallo stesso database, e se la politica di bilanciamento del carico è impostata

su una politica GEO, restituirà l'indirizzo IP più vicino. Questo metodo funziona perfettamente con gli indirizzi IP pubblici, ma non c'è un simile database per gli indirizzi privati interni che sono conformi a RFC 1918 per gli indirizzi IPv4 e RFC 4193 per gli indirizzi IPv6.

Vedere la pagina di Wikipedia che spiega l'indirizzamento privato
HTTPS://EN.WIKIPEDIA.ORG/WIKI/PRIVATE_NETWORK

Come funziona

Tipicamente, l'idea dietro l'uso del nostro GSLB per le reti interne è che gli utenti da indirizzi specifici riceveranno una risposta diversa per un servizio a seconda della rete in cui si trovano. Quindi, consideriamo due data-center, Nord e Sud, che forniscono un servizio chiamato rispettivamente north.service1.gslb.com e south.service1.gslb.com. Quando un utente dal data-center Nord interroga il GSLB, vogliamo che il GSLB risponda con l'indirizzo IP associato a north.service1.gslb.com, purché il servizio funzioni correttamente. In alternativa, se un utente dal data-center Sud interroga il GSLB, vogliamo che il GSLB risponda con l'indirizzo IP associato a south.service1.gslb.com di nuovo, a condizione che il servizio funzioni correttamente.

Quindi, cosa dobbiamo fare per far sì che lo scenario di cui sopra si verifichi?

- Abbiamo bisogno di avere almeno due posizioni personalizzate, una per ogni centro dati
- Assegnare le varie reti private a queste posizioni
- Assegnare ogni servizio alla rispettiva posizione

Come si configura questo aspetto sul GSLB?

Aggiungere una posizione per il Centro Dati Nord

- Clicca su Posizioni personalizzate sul lato sinistro
- Fare clic su Aggiungi posizione
- Nome
  - Nord
- Aggiungete un indirizzo IP privato e una subnet mask per la vostra rete del Nord. Per questo esercizio, assumeremo che il servizio e gli indirizzi IP del client siano nella stessa rete privata
  - 10.1.1.0/24
- Aggiungere il codice del continente
  - UE
- Aggiungere il codice del paese
  - REGNO UNITO
- Aggiungi città
  - Enfield
- Aggiungere la latitudine - ottenuta da google
  - 51.6523
- Aggiungere la longitudine - ottenuta da google
  - 0.0807

Nota, si prega di utilizzare il codice corretto che può essere ottenuto da qui

Aggiungere una posizione per il Centro Dati Sud

- Clicca su Posizioni personalizzate sul lato sinistro
- Fare clic su Aggiungi posizione
- Nome
  - Sud
- Aggiungete un indirizzo IP privato e una subnet mask per la vostra rete meridionale. Assumeremo che il servizio e gli indirizzi IP del client siano nella stessa rete privata per questo esercizio.
  - 192.168.1.0/24
- Aggiungere il codice del continente
  - UE

- Aggiungere il codice del paese
  - REGNO UNITO
- Aggiungi città
  - Croydon
- Aggiungere la latitudine - ottenuta da google
  - 51.3762
- Aggiungere la longitudine - ottenuta da google
  - 0.0982

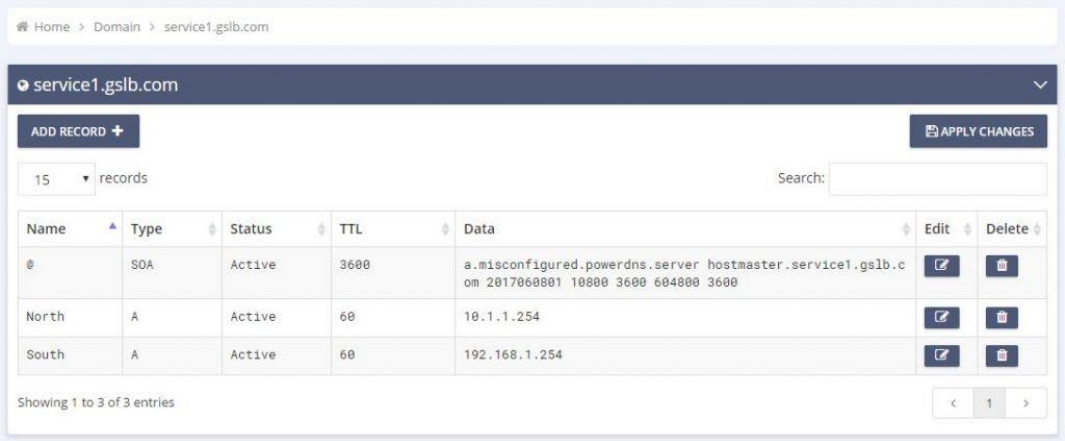
Nota, si prega di utilizzare il codice corretto che può essere ottenuto da **QUI**

Aggiungere un record A per north.service1.gslb.com

- Clicca sul dominio service1.gslb.com
- Fare clic su Aggiungi record
- Aggiungi nome
  - Nord
- Tipo
  - A
- Stato
  - Attivo
- TTL
  - 1 minuto
- Indirizzo IP
  - 10.1.1.254 (Nota: questo è nella stessa rete della località Enfield)

Aggiungere un record A per south.service1.gslb.com

- Clicca sul dominio service1.gslb.com
- Fare clic su Aggiungi record
- Aggiungi nome
  - Sud
- Tipo
  - A
- Stato
  - Attivo
- TTL
  - 1 minuto
- Indirizzo IP
  - 192.168.1.254 (Nota: questo è nella stessa rete della località Croydon)



Flusso di traffico

Esempio 1 - Cliente in un centro dati del nord

- IP cliente 10.1.1.23 interroga GSLB per service1.gslb.com
- GSLB cerca l'indirizzo IP 10.1.1.23 e lo abbina alla posizione personalizzata Enfield 10.1.1.0/24
- GSLB guarda i suoi record A per service1.gslb.com e corrisponde a north.service1.gslb.com poiché è anche nella rete 10.1.1.0/24
- GSLB risponde a 10.1.1.23 con l'indirizzo IP 10.1.1.254 per service1.gslb.com

Esempio 2 - Cliente in un data center del sud

- Client IP 192.168.1.23 interroga GSLB per service1.gslb.com
- GSLB cerca l'indirizzo IP 192.168.1.23 e lo abbina a Custom Location Croydon 192.168.1.0/24
- GSLB guarda i suoi record A per il service1.gslb.com e corrisponde a south.service1.gslb.com poiché è anche nella rete 192.168.1.0/24
- GSLB risponde a 192.168.1.23 con l'indirizzo IP 192.168.1.254 per service1.gslb.com

Supporto tecnico

Forniamo supporto tecnico a tutti i nostri utenti secondo i termini di servizio standard dell'azienda.

Forniremo tutto il supporto tramite l'assistenza tecnica se si dispone di un contratto di supporto e manutenzione attivo per edgeADC, edgeWAF o edgeGSLB.

Per sollevare un ticket di supporto, visitate il sito:

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