
# EdgeADC

GUIDA ALL'AMMINISTRAZIONE

# Contenuto

# Proprietà del documento

Numero del documento: 2.0.6.16.21.18.06

Data di creazione del documento: 30 aprile 2021

Ultima modifica del documento: June 16, 2021

Autore del documento: Jay Savoor

Documento modificato l'ultima volta da:

Riferimento del documento: EdgeADC - Versione 4.2.7.1895

## Esclusione di responsabilità del documento

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

## Copyrights



## Marchi



## Assistenza Edgenexus

Se ha domande tecniche su questo prodotto, sollevi un ticket di supporto a: support@edgenexus.io

# Installazione di EdgeADC

Il prodotto EdgeADC (d'ora in poi chiamato ADC) è disponibile per l'installazione con diversi metodi. Ogni piattaforma target richiede il suo installatore, e questi sono tutti disponibili.

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 userà per ospitare l'ADC dipende dallo scenario del caso d'uso e dal throughput dei dati.

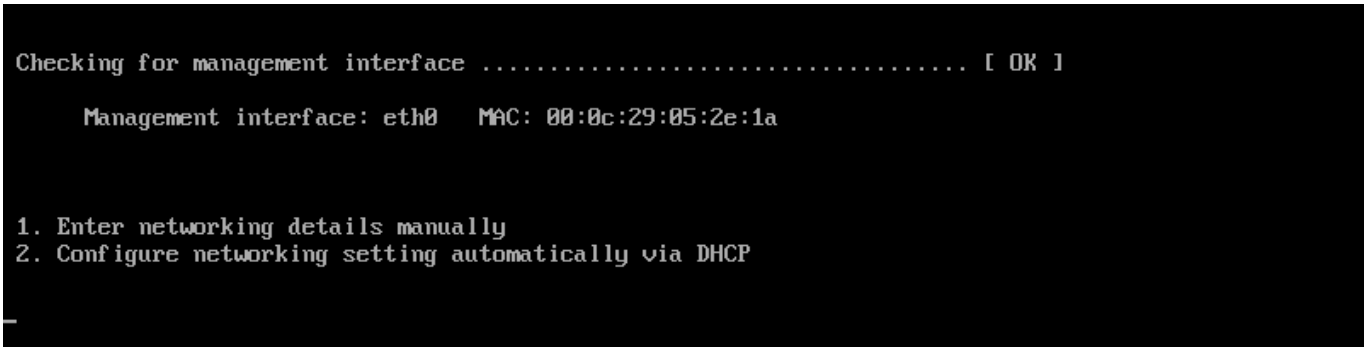
## VMware ESXi

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

- Scarichi l'ultimo pacchetto OVA di installazione di ADC usando il link appropriato fornito con l'e-mail di download.
- Una volta scaricato, lo decomprima in una directory adatta sul suo host ESXi o SAN.
- Nel suo client vSphere, selezioni File: Deploy OVA/OVF Template.
- Sfogliare e selezionare la posizione in cui ha salvato i suoi file; scegliere il file OVF e cliccare **AVANTI**
- Il server ESX richiede il nome dell'appliance. Digiti un nome adatto e clicchi su **AVANTI**
- Selezioni il datastore da cui la sua appliance ADC verrà eseguita.
- Selezioni un datastore con spazio sufficiente e clicchi su **AVANTI**
- Le verranno fornite informazioni sul prodotto; clicchi su **AVANTI**
- Clicchi su **AVANTI.**
- Una volta copiati i file nel datastore, può installare il dispositivo virtuale.

Lanci il suo client vSphere per vedere il nuovo dispositivo virtuale ADC.

- Clicchi con il tasto destro del mouse sul VA e vada su Power > Power-On
- Il suo VA si avvierà quindi e la schermata di avvio ADC apparirà sulla console.




### Installazione dell'interfaccia VMXNET3

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

***Nota** - NON aggiornare il VMware-tools*

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

1. Cancelli entrambe le NIC dalla VM
2. Aggiornare l'hardware della VM - -Cliccare con il tasto destro del mouse sulla VA nell'elenco e selezionare Upgrade Virtual Hardware (non avviare un'installazione o un aggiornamento degli strumenti VMware, eseguire **solo** l'aggiornamento dell'hardware)
3. Aggiunga due NIC e le selezioni come VMXNET3
4. Avvii il VA usando il metodo standard. Funzionerà con il VMXNET3

### Abilitare l'interfaccia VMXNET3 su una VA già in funzione

1. Arrestare la VM (comando CLI shutdown o GUI power-off)
2. Prenda gli indirizzi MAC di entrambi i NIC (si ricordi l'ordine dei NIC nella lista! )
3. Cancelli entrambe le NIC dalla VM
4. Aggiornare l'hardware della VM (non avviare un'installazione o un aggiornamento degli strumenti VMware, eseguire **solo** l'aggiornamento dell'hardware)
5. Aggiunga due NIC e le selezioni come VMXNET3
6. Impostare gli indirizzi MAC per le nuove NIC secondo il passo 2
7. Riavviare il VA

Supportiamo VMware ESXi come piattaforma di produzione.  Per scopi di valutazione, può usare VMware Workstation e Player.

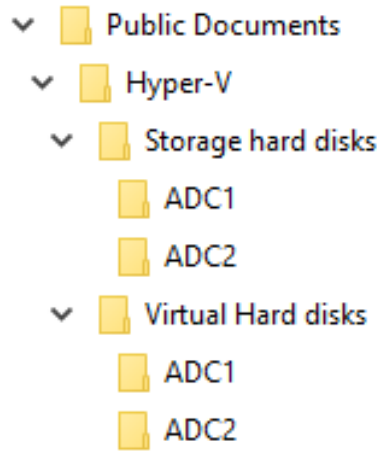
Si riferisca alla sezione **CONFIGURAZIONE DEL PRIMO AVVIO** per procedere oltre.

## Microsoft Hyper-V

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

*Noti che ogni apparecchio richiede un indirizzo MAC unico.*

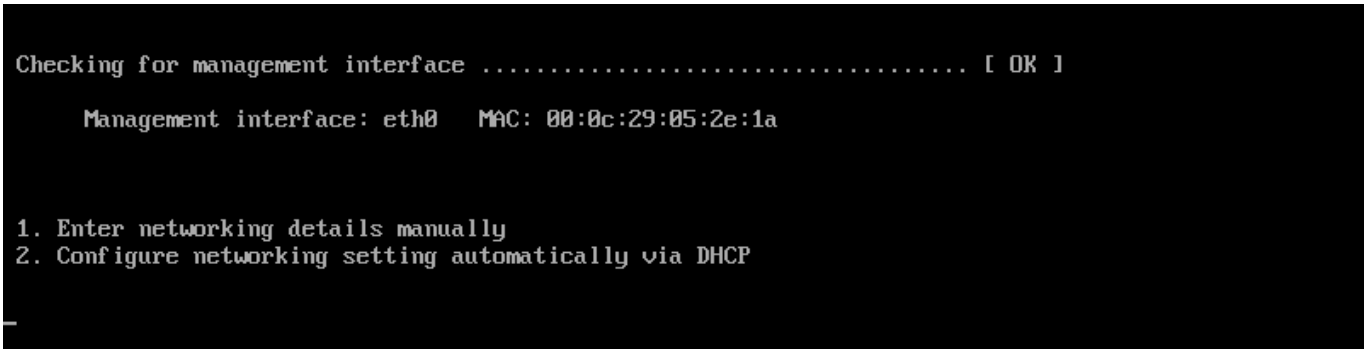
- Estragga il file ADC-VA compatibile con Hyper-V scaricato sulla sua macchina o server locale.
- Apra Hyper-V Manager.
- Crei una nuova cartella per contenere l'ADC VA 'Virtual hard disk' e un'altra nuova cartella per contenere il 'Storage hard disk', ad esempio C:\Users\Public\Documents\Hyper-V\V\Virtual hard disks\ADC1 e C:\Users\Public\Documents\Hyper-V\Storage hard disks\ADC1
- **Nota**: è necessario creare nuove sottocartelle specifiche ADC per i dischi rigidi virtuali e i dischi rigidi di stoccaggio per ogni installazione di istanza ADC virtuale, come mostrato di seguito:



- Copi il file EdgeADC .vhd estratto nella cartella 'Storage hard disk' creata sopra.
- Nel suo client Hyper-V Manager, clicchi con il tasto destro sul server e selezioni "Importa macchina virtuale".
- Naviga fino alla cartella che contiene il file immagine ADC VA scaricato ed estratto in precedenza
- Selezioni la macchina virtuale - evidenzi la macchina virtuale da importare e clicchi su Avanti
- Selezioni la macchina virtuale - evidenzi la macchina virtuale da importare e clicchi su Avanti
- Scelga Tipo di importazione - selezioni "**Copia la macchina virtuale (crea un nuovo ID unico)**" clicchi su successivo
- Scelga le cartelle per i file della macchina virtuale - la destinazione può essere lasciata come quella predefinita di Hyper-V o può scegliere di selezionare una posizione diversa
- Individui i dischi rigidi virtuali - sfogli e selezioni la cartella dei dischi rigidi virtuali creata in precedenza e clicchi su avanti
- Scelga Cartelle per memorizzare i dischi rigidi virtuali - sfogli e selezioni la cartella Storage hard disks creata in precedenza e clicchi su next
- Verifichi che i dettagli nella finestra Riepilogo della procedura guidata di importazione siano corretti e clicchi su Fine
- Clicchi con il tasto destro del mouse sulla macchina virtuale **ADC** appena importata e selezioni Start

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

- Mentre la VM si inizializza, può fare clic con il tasto destro del mouse sulla voce VM e selezionare Connect...Le 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.

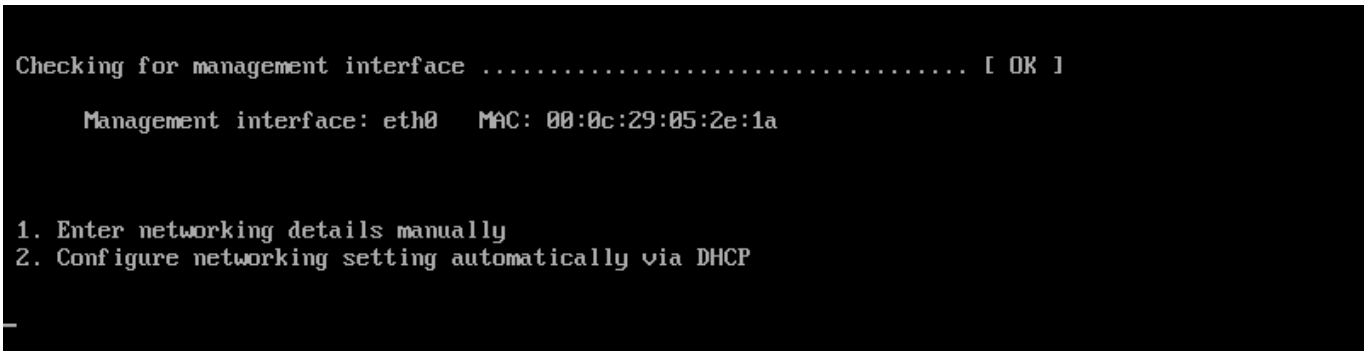
Si riferisca alla sezione **CONFIGURAZIONE DEL PRIMO AVVIO** per procedere oltre.

## Citrix XenServer

L'appliance ADC Virtual è installabile su Citrix XenServer.

- Estragga il file ADC OVA ALB-VA sulla sua macchina o server locale.
- Apra Citrix XenCenter Client.
- Nel suo client XenCenter, selezioni **"File: Import".**
- Cerchi e selezioni il file **OVA**, poi clicchi su **"Open Next".**
- Selezioni la posizione di creazione della VM quando le viene chiesto.
- Scelga quale XenServer desidera installare e clicchi su **"NEXT".**
- Selezioni il repository di stoccaggio (SR) per il posizionamento del disco virtuale quando le viene chiesto.
- Selezioni un SR con spazio sufficiente e clicchi su **"NEXT".**

- Mappi le sue interfacce di rete virtuali. Entrambe le interfacce diranno Eth0; tuttavia, noti che l'interfaccia inferiore è Eth1.
- Selezioni la rete di destinazione per ogni interfaccia e clicchi su **AVANTI**
- **NON** spunti la casella "Use Operating System Fixup".
- Clicchi su **"AVANTI".**
- Scelga l'interfaccia di rete da usare per la VM di trasferimento temporaneo.
- Scelga l'interfaccia di gestione, di solito Rete 0, e lasci le impostazioni di rete su DHCP. Tenga presente che deve assegnare dettagli di indirizzo IP statico se non ha un server DHCP funzionante per il trasferimento. Se non lo fa, l'importazione dirà Connessione continua e poi fallita. Cliccare su **"NEXT".**
- Riveda tutte le informazioni e controlli poi le impostazioni corrette. Clicchi su **"FINISH".**
- La sua VM inizierà a trasferire il disco virtuale "ADC ADC" e, una volta completato, apparirà sotto il suo XenServer.
- Nel suo client XenCenter potrà ora vedere la nuova macchina virtuale.
  Clicchi con il tasto destro del mouse sulla VA e clicchi su "**START**".
- La sua VM si avvierà quindi e apparirà la schermata di avvio ADC.




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

Si riferisca alla sezione **CONFIGURAZIONE DEL PRIMO AVVIO** per procedere oltre.

# Configurazione di 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, avrà 10 secondi per interrompere l'assegnazione automatica dei dettagli IP tramite DHCP

Per interrompere questo processo, clicchi nella finestra della console e prema un tasto qualsiasi. Può quindi inserire manualmente i seguenti dettagli.

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

Questi cambiamenti sono persistenti e sopravvivono ad un riavvio e non hanno bisogno di essere configurati di nuovo sul VA.

## Primo avvio - DHCP riuscito

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

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

Le consigliamo di non usare il VA ADC usando un indirizzo DHCP a meno che quell'indirizzo IP non sia collegato in modo permanente all'indirizzo MAC del VA all'interno del server DHCP. Consigliamo sempre di usare un **INDIRIZZO IP FISSO** quando si usa il VA. Segua 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 ha 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 trova un indirizzo IP libero. Allo stesso modo, il VA controllerà se l'indirizzo IP è attualmente in uso e, in tal caso, incrementerà di nuovo e ricontrollerà.

## Cambiare l'indirizzo IP di gestione

Può cambiare l'indirizzo IP del VA in qualsiasi momento usando il comando **set greenside=n.n.n.n,** come mostrato di seguito.

```
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 si chiama eth0. La subnet mask o netmask può essere cambiata usando il comando **set mask eth0 n.n.n.n.** Può 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, usi il comando **route add default gw n.n.n.n** come mostrato nell'esempio sottostante.

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

## Controllo del valore del gateway predefinito

Per controllare se il gateway predefinito è stato aggiunto ed è corretto, usi il comando **route**. Questo comando mostrerà i percorsi di rete e il valore del gateway predefinito. Veda 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 può accedere all'interfaccia grafica utente (GUI) per configurare l'ADC per la produzione o l'uso di valutazione.

## Accesso all'interfaccia web

Può usare qualsiasi browser Internet con Javascript per configurare, monitorare e mettere in funzione l'ADC.

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

L'ADC, per default, usa un certificato SSL autofirmato. Può cambiare l'ADC per usare un certificato SSL di sua scelta.

Una volta che il suo browser raggiunge l'ADC, le mostrerà la schermata di login. Le credenziali predefinite di fabbrica 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 sett 13:00 UTC 2013 |
| defaults | | | Assegni le impostazioni predefinite di fabbrica per il suo apparecchio | |
| exit | | | Esca dall'interfaccia della linea di comando | |
| aiutare | | | Visualizza tutti i comandi validi | |
| seconfig | [vuoto] | | Visualizzare la configurazione dell'interfaccia per tutte le interfacce | seconfig |
| | eth0 | | Visualizzi solo la configurazione dell'interfaccia di eth0 | ifconfig eth0 |
| machineid | | | Questo comando fornirà il machineid usato per abilitare l'ADC ADC | EF4-3A35-F79 |
| quit | | | Esca dall'interfaccia della linea di comando | |
| reboot | | | Terminare tutte le connessioni e riavviare l'ADC ADC | reboot |
| riavviare | | | Riavviare i servizi virtuali ADC ADC | |
| percorso | [vuoto] | | Visualizzare la tabella di routing | percorso |
| | aggiungere | gw predefinito | Aggiunga l'indirizzo IP del gateway predefinito | route add default gw 192.168.100.254 |
| set | 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.... | imposta maschera eth0 255.255.255.0 |
| mostra | | | Visualizza le impostazioni di configurazione globale | |
| spegnimento | | | Terminare tutte le connessioni e spegnere l'ADC ADC | |
| status | | | Visualizza le statistiche dei dati correnti | |
| top | | | Visualizzi le informazioni sul processo come CPU e Memoria | |
| viewlog | messaggi | | Visualizza i messaggi syslog grezzi | Visualizzare i messaggi di log |

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

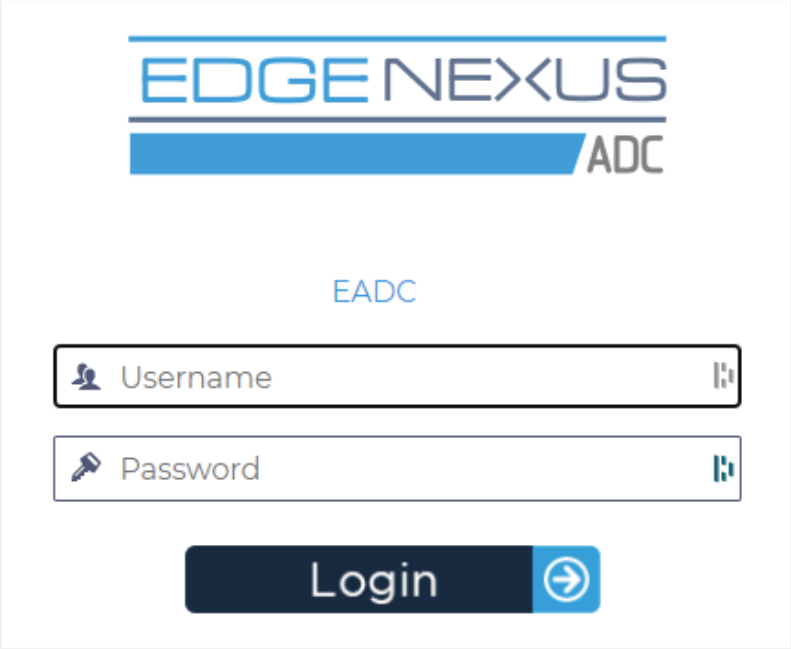
# Lanciare la console web ADC

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

Per lanciare la console web ADC, inserisca 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 qui sotto, e permette di accedere come utente amministratore.




## Credenziali di accesso predefinite

Le credenziali di accesso predefinite sono:

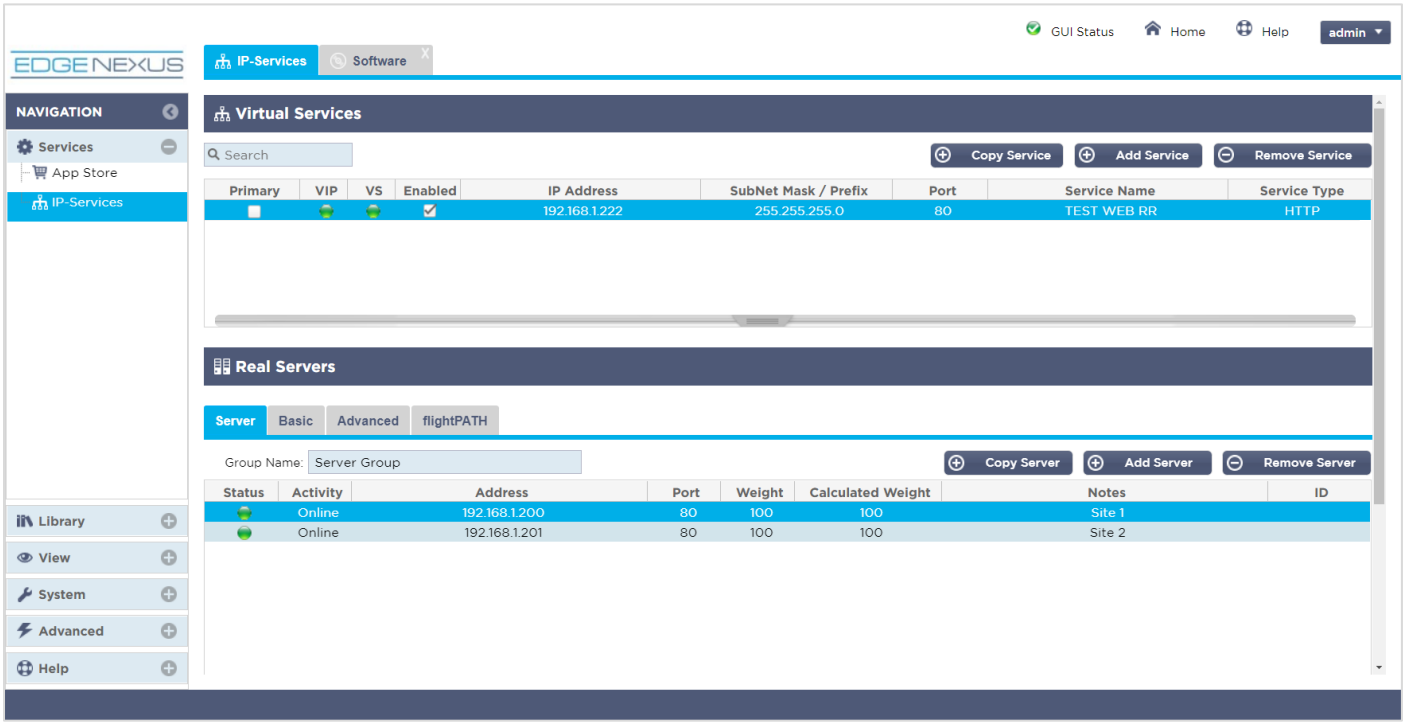
- Nome utente: admin
- Password: jetnexus

Può cambiarlo in qualsiasi momento usando le funzionalità di configurazione utente situate in *Sistema* > *Utenti.*

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

# Il cruscotto principale

L'immagine sottostante illustra come appare il cruscotto principale o 'home page' dell'ADC. Potremmo fare qualche cambiamento 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 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 clicca su una scelta particolare all'interno di Navigazione, questa visualizzerà la sezione corrispondente sul lato destro dello schermo. Può anche vedere la sezione di configurazione scelta a schede nella parte superiore dello schermo, adiacente al logo del prodotto. Le schede permettono una navigazione più veloce verso aree preutilizzate della configurazione dell'ADC.

# Servizi

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

## Servizi IP

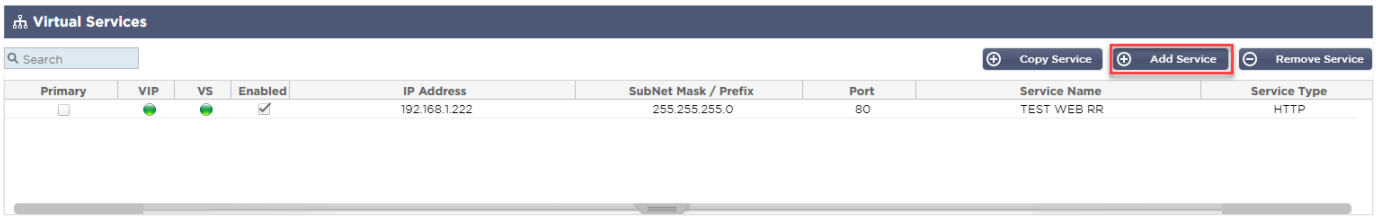
La sezione Servizi IP dell'ADC le permette di aggiungere, cancellare e configurare i vari servizi IP virtuali di cui ha bisogno per il suo particolare caso d'uso. Le impostazioni e le opzioni rientrano nelle sezioni seguenti. Queste sezioni si trovano sul lato destro dello schermo dell'applicazione.

### Servizi virtuali

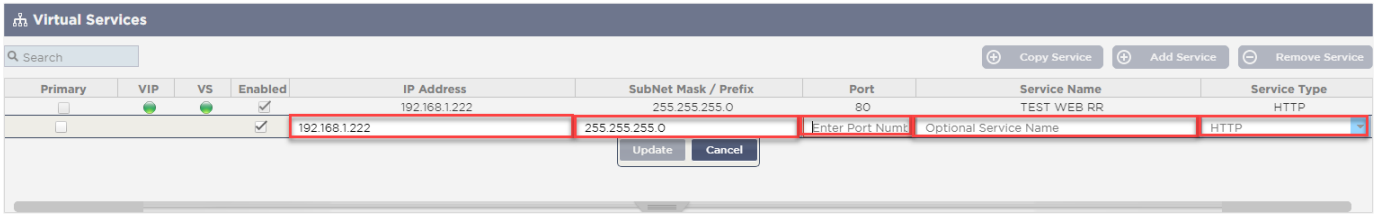
Un Servizio Virtuale combina un IP Virtuale (VIP) e una porta TCP/UDP su cui l'ADC ascolta. Il traffico che arriva all'IP del Servizio Virtuale viene reindirizzato ad uno dei Real Server associati a quel servizio. L'indirizzo IP del Servizio Virtuale non può essere lo stesso dell'indirizzo di gestione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

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

#### Creare un nuovo servizio virtuale usando un nuovo VIP




- Clicchi il pulsante Add Virtual Service come indicato sopra.

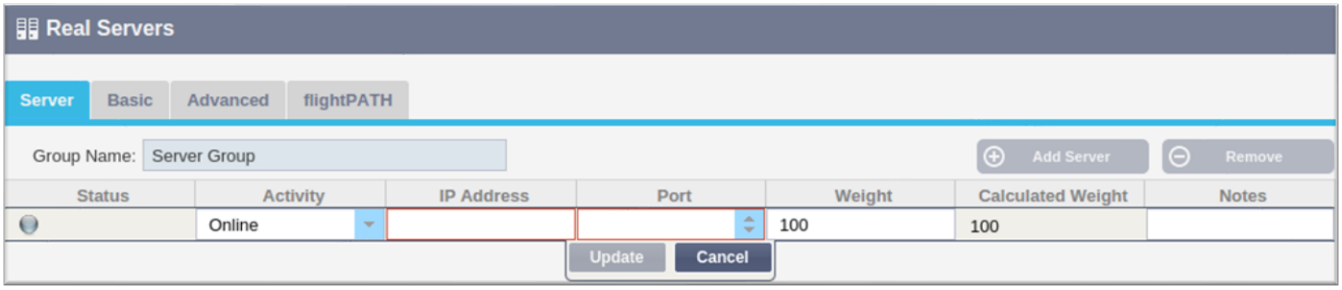



- Entrerà quindi nella modalità di **modifica della riga.**
- Completi i quattro campi evidenziati per procedere e poi clicchi sul pulsante aggiorna.

Usi il tasto TAB per navigare attraverso i campi.

| Campo | Descrizione |
|---|---|
| Indirizzo IP | Inserisca un nuovo indirizzo IP Virtuale che sia il punto d'ingresso di destinazione per accedere al Real Server. Questo IP è dove gli utenti o le applicazioni punteranno per accedere all'applicazione con bilanciamento del carico. |
| Maschera/Prefisso di sottorete | Questo campo è per la subnet mask relativa alla rete su cui si trova l'ADC |
| Porto | La porta d'ingresso usata quando si accede al VIP. Questo valore non deve necessariamente essere lo stesso del Real Server se usa Reverse Proxy. |
| Nome del servizio | Il nome del servizio è una rappresentazione testuale dello scopo del VIP. È opzionale, ma le consigliamo di fornirlo per chiarezza. |
| Tipo di servizio | Ci sono molti tipi di servizio diversi che può scegliere. I tipi di servizio Layer 4 non possono usare la tecnologia flightPATH. |

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

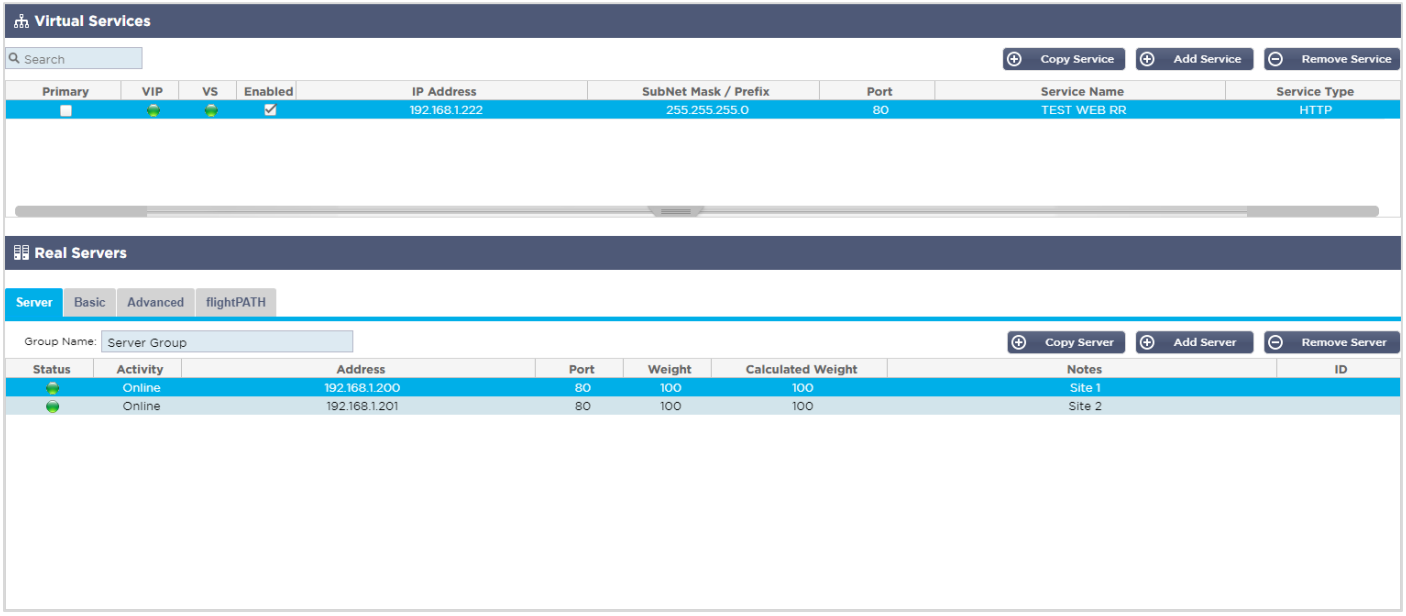



| Campo | Descrizione |
|---|---|
| Attività | Il campo Attività può essere usato per mostrare e cambiare lo stato del server reale con bilanciamento del carico.<br>Online - Denota che il server è attivo e riceve richieste con bilanciamento del carico<br>Offline - Il server è offline e non riceve richieste<br>Drain - Il server è stato messo in modalità drain in modo che la persistenza possa essere lavata e il server spostato in uno stato offline senza influenzare gli utenti.<br>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 usa un reverse proxy, questo può essere diverso dalla Porta d'ingresso specificata sul VIP. |
| Ponderazione | Questa impostazione di solito viene configurata automaticamente dall'ADC. Può cambiarla se vuole cambiare la ponderazione della priorità. |

- Clicchi il pulsante Update o prema Enter per salvare le sue modifiche

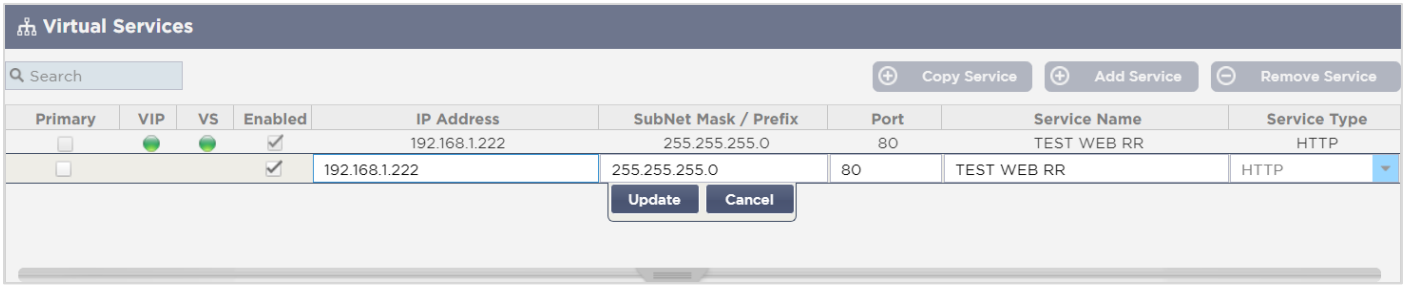
- La luce di stato diventerà prima grigia, seguita da verde se la verifica dello stato di salute del server ha successo. Diventerà Rossa se il Real Server Monitor fallisce.
- Un server che ha una luce di stato rossa non sarà bilanciato nel carico.

## Esempio di un servizio virtuale completato

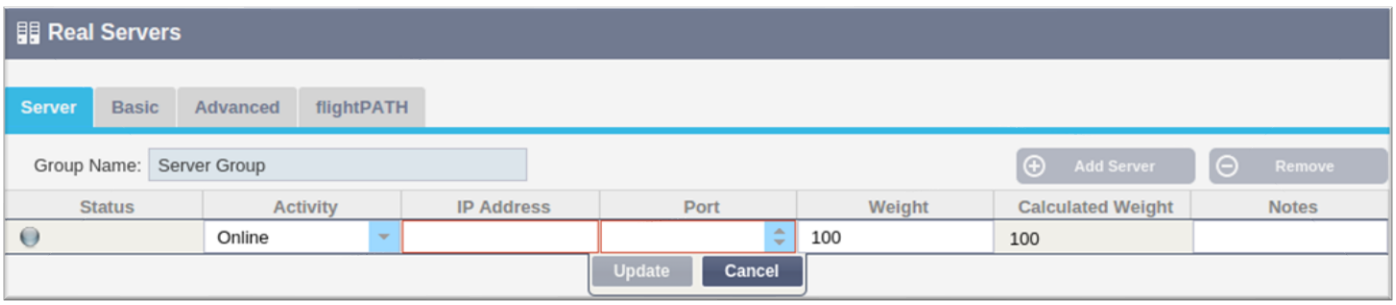



## Creare un nuovo servizio virtuale usando un VIP esistente

- Evidenzi un Servizio Virtuale che desidera copiare
- Clicchi su Add Virtual Service per entrare nella modalità di modifica delle righe




- L'indirizzo IP e la maschera di sottorete si copiano automaticamente
- Inserisca il numero di porta per il suo servizio
- Inserisca un nome di servizio opzionale
- Selezioni un tipo di servizio
- Ora può premere il pulsante Update per salvare questa sezione e saltare automaticamente alla sezione Real Server qui sotto

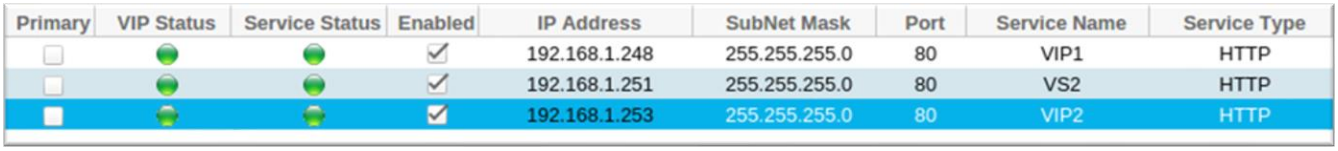


- Lasci l'opzione Attività del server come Online - questo significa che verrà bilanciato il carico se supera il monitor di salute predefinito di TCP Connect. Questa impostazione può essere cambiata in seguito, se necessario.
- Inserisca un indirizzo IP del Real Server
- Inserisca un numero di porta per il Real Server
- Inserisca un nome opzionale per il Real Server
- Clicchi su Update per salvare le sue modifiche
- La luce di stato diventerà prima grigia e poi 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 nel carico

## Cambiare l'indirizzo IP di un servizio virtuale

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

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




- Doppio clic sul campo dell'indirizzo IP per quel servizio


- Cambi l'indirizzo IP con quello che vuole usare
- Clicchi il pulsante Update per salvare le modifiche.


*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

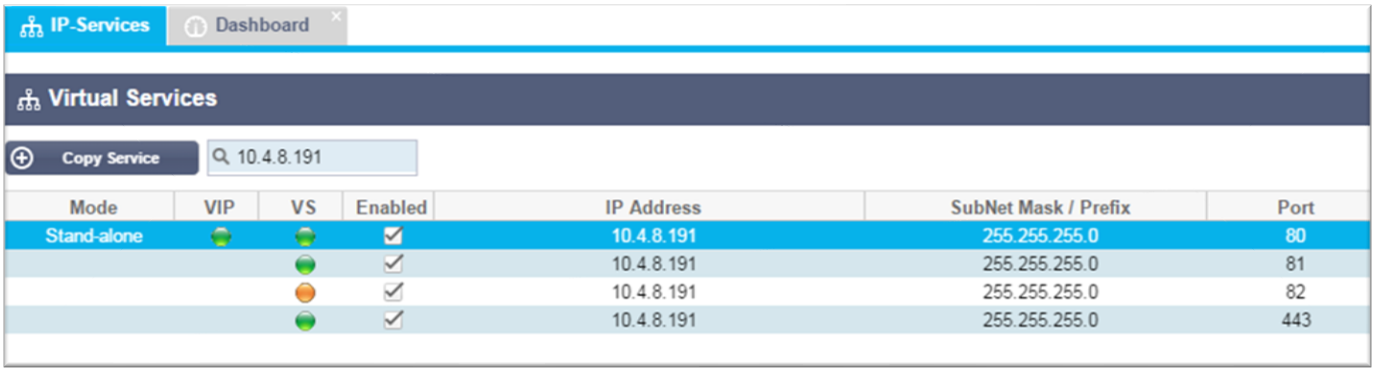
- Il pulsante Copy Service copierà un intero servizio, inclusi tutti i Real Server, le impostazioni di base, le impostazioni avanzate e le regole flightPATH associate
- Evidenzi il servizio che vuole duplicare e clicchi su Copy Service
- L'editor di riga apparirà con il cursore lampeggiante sulla colonna Indirizzo IP
- Deve cambiare l'indirizzo IP in modo che sia unico, o se vuole mantenere l'indirizzo IP, deve modificare la Porta in modo che sia unica per quell'indirizzo IP

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

## Filtrare i dati visualizzati

### *Ricerca di un termine specifico*

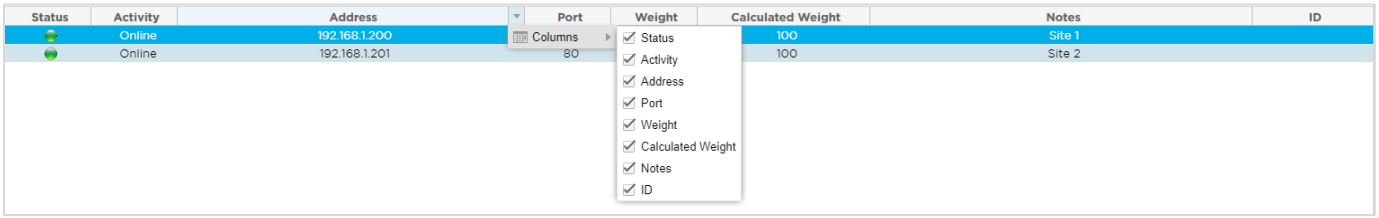
La casella Ricerca le permette di cercare nella tabella usando qualsiasi valore, come gli ottetti dell'indirizzo IP o il nome del servizio.




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

### *Selezione della visibilità delle colonne*

Può anche selezionare le colonne che desidera visualizzare nel dashboard.

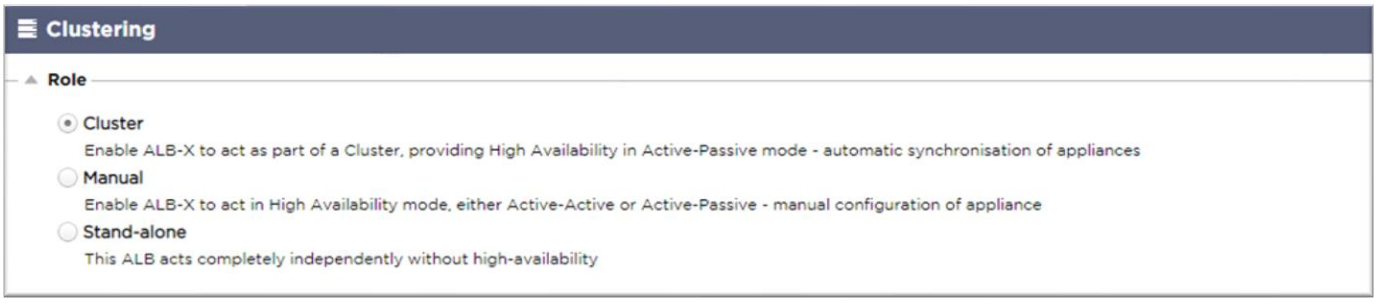



- Sposti il mouse su una qualsiasi delle colonne
- Vedrà apparire una piccola freccia sul lato destro della colonna
- Cliccando sulle caselle di controllo seleziona le colonne che vuole vedere nel dashboard.

## Comprendere 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 al momento dell'installazione e la colonna Primary/Mode indicherà la modalità in cui è attualmente in funzione. Quando ha una coppia HA di apparecchi ADC nel suo datacenter, uno di essi mostrerà Attivo e l'altro Passivo |

| | |
|---|---|
| Manuale | Il ruolo Manuale permette alla coppia ADC di funzionare in modalità Attivo-Attivo per diversi indirizzi IP Virtuali. In questi casi, la colonna Primary conterrà una casella accanto a ciascun IP Virtuale unico che può essere spuntata per Active o lasciata non spuntata per Passive. |
| Stand-Alone | L'ADC sta agendo come 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". |
| ● | Servizio Necessita 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 licenziati o licenziati superati |

### *Abilitato*

L'impostazione predefinita per questa opzione è Enabled e la casella di controllo appare spuntata. Può disattivare il Servizio Virtuale facendo doppio clic sulla linea, deselezionando la casella di controllo e poi cliccando sul pulsante Aggiorna.

### *Indirizzo IP*

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

### *Maschera/Prefisso di sottorete*

Aggiunga la sua subnet mask in notazione decimale punteggiata. Esempio "255.255.255.0". O per IPv6, aggiunga il suo prefisso. Per maggiori informazioni su IPv6, veda **HTTPS://EN.WIKIPEDIA.ORG/WIKI/IPV6_ADDRESS**

### *Porto*

Aggiunga il numero di porta associato al suo 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*

Aggiunga un nome amichevole per identificare il suo servizio. Esempio "Production Web Servers".

### *Tipo di servizio*

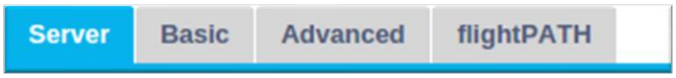
Si noti che con tutti i tipi di servizio "Layer 4", l'ADC non interagisce o modifica il flusso di dati, quindi flightPATH non è disponibile con i tipi di servizio Layer 4. I servizi Layer 4 semplicemente bilanciano il traffico secondo la politica di bilanciamento del carico:

| Tipo di servizio | Porta/Protocollo | Livello di servizio | Commento |
|---|---|---|---|
| Layer 4 TCP | Qualsiasi porta TCP | Livello 4 | L'ADC non altera nessuna 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 per il Layer 4 TCP, l'ADC non altera nessuna 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 suo servizio ha un protocollo primario come UDP ma ricade 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 | !!! | | |
| HTTP | Protocollo HTTP o HTTPS | Strato 7 | L'ADC può interagire, manipolare e modificare il flusso di dati usando flightPATH. |
| FTP | Protocollo di Trasferimento File Protocollo | Strato 7 | Usare connessioni di controllo e dati separate tra client e server |
| SMTP | Protocollo semplice di trasferimento della posta | Livello 4 | Da usare per bilanciare il carico dei server di posta |
| POP3 | Protocollo dell'ufficio postale | Livello 4 | Da usare per bilanciare il carico dei server di posta |
| IMAP | Protocollo di accesso ai messaggi Internet | Livello 4 | Da usare per bilanciare il carico dei server di posta |
| RDP | Protocollo di Desktop Remoto | Livello 4 | Da usare per bilanciare il carico dei server Terminal Services |
| RPC | Chiamata di procedura remota | Livello 4 | Usare quando si equilibrano i sistemi di bilanciamento del carico usando chiamate RPC |
| RPC/ADS | Exchange 2010 RPC statico per il servizio di rubrica | Livello 4 | Da usare per bilanciare il carico dei server Exchange |
| RPC/CA/PF | Exchange 2010 RPC statico per accesso al cliente e cartelle pubbliche | Livello 4 | Da usare per bilanciare il carico dei server Exchange |

| | | | |
|---|---|---|---|
| DICOM | Imaging digitale e comunicazioni in medicina | Livello 4 | Da usare per bilanciare il carico dei server che usano i protocolli DICOM |

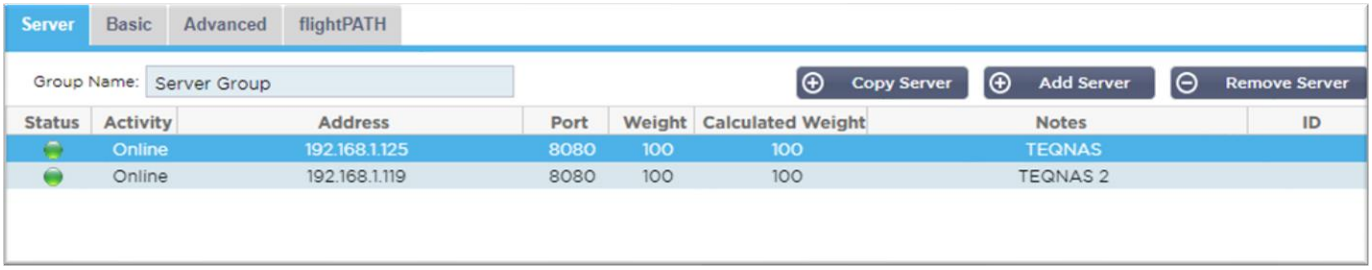
## Server reali

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



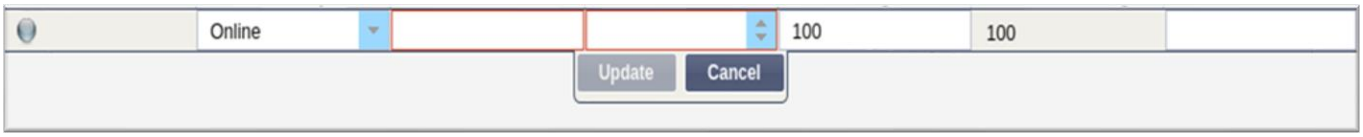

### Server

La scheda Server contiene le definizioni dei server back-end reali abbinati al Servizio Virtuale attualmente selezionato. Deve aggiungere almeno un server alla sezione Real Servers.



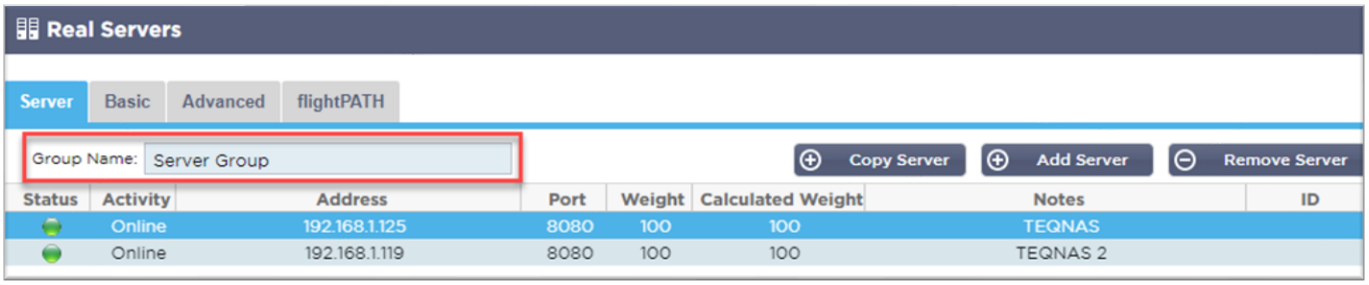

#### *Aggiungere un server*

- Selezioni il VIP appropriato che ha precedentemente definito.
- Clicchi su Add Server
- Apparirà una nuova riga con il cursore lampeggiante sulla colonna Indirizzo IP




- Inserisca l'indirizzo IPv4 del suo server in notazione decimale punteggiata. Il Real Server può trovarsi sulla stessa rete del suo Servizio Virtuale, su qualsiasi rete locale collegata direttamente o su qualsiasi rete che il suo ADC può instradare. Esempio "10.1.1.1".
- Tab alla colonna Port e inserisca il numero di porta TCP/UDP per il suo 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 a questo numero.
- Tab alla sezione Note per aggiungere qualsiasi dettaglio rilevante per il server. Esempio: "IIS Web Server 1"

#### *Nome del gruppo*



Quando ha aggiunto i server che compongono l'insieme bilanciato, può anche attribuire loro un Nome Gruppo. Una volta modificato questo campo, il contenuto si salva senza bisogno di premere il pulsante Update.

### *Luci di stato del server reale*

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

| LED | Significato |
|---|---|
| ● | Collegato |
| ◎ | Non monitorato |
| ● | Drenaggio |
| ● | Offline |
| ● | Standby |
| ● | Non collegato |
| ● | Stato di ritrovamento |
| ● | Server reali non licenziati o con licenza superata |

### *Attività*

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


| Opzione | Descrizione |
|---|---|
| Online | Tutti i Real Server assegnati Online riceveranno il traffico secondo la politica di bilanciamento del carico impostata nella scheda Basic. |
| Drenaggio | 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 Status sarà blu fissa. Può 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 rimangono offline fino a quando **TUTTI** i server del gruppo Online non falliscono 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 supera il controllo Server Health Monitor, questo server Online riceverà tutto il traffico e il gruppo Standby smetterà di ricevere traffico. |

### Indirizzo IP

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

### *Porto*

Numero di porta TCP o UDP su cui il Real Server è in ascolto per il servizio. Esempio "80" per il traffico web.

### *Peso*

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

Il peso predefinito per un Real Server è 100 e può 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 contemporanee
- Il server 2 riceverà 50 connessioni contemporanee
- Il server 3 riceverà 50 connessioni contemporanee

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

Se crediamo che la politica di bilanciamento del carico più veloce usi il tempo più breve impiegato per ottenere una risposta, l'aggiustamento 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 il peso effettivo che ADC sta usando quando considera la ponderazione manuale e la politica di bilanciamento del carico.

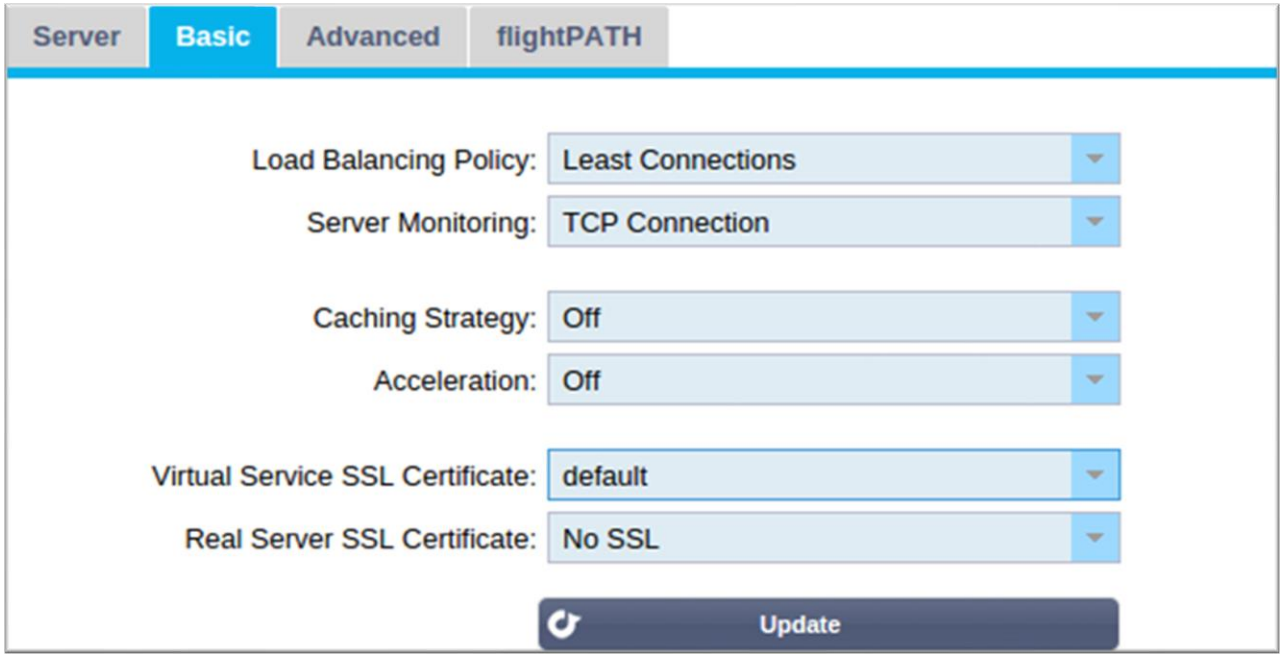
### *Note*

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

### *ID*

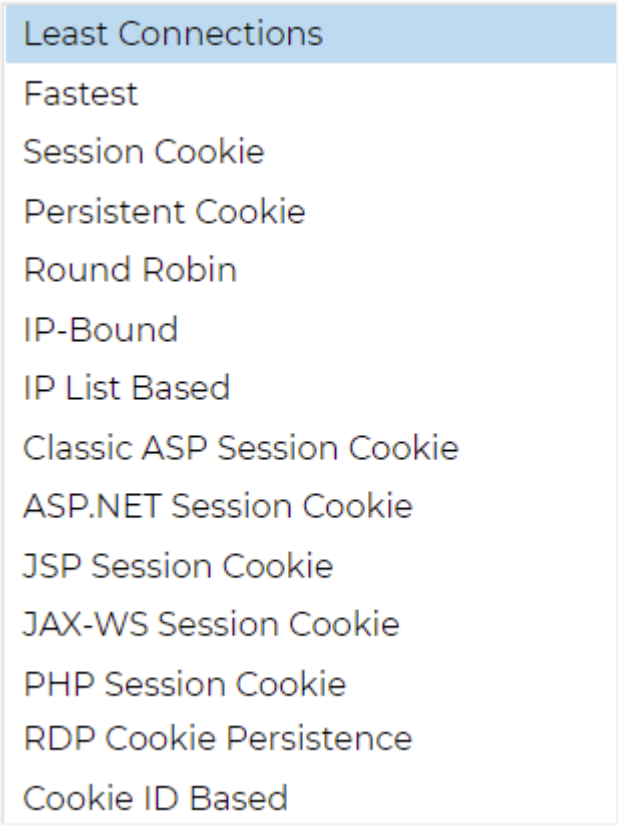
Il campo ID viene usato all'interno della politica di bilanciamento del carico di ID dei cookie. Il numero ID inserito qui è usato per identificare

## Basic




### *Politica di bilanciamento del carico*

L'elenco a discesa le 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.



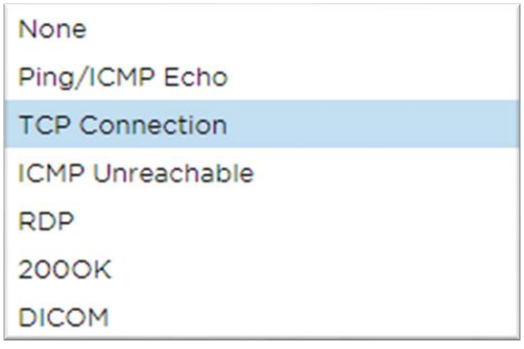

| Opzione | Descrizione |
|---|---|
| Più veloce | La politica di bilanciamento del carico più veloce calcola automaticamente il tempo di risposta per tutte le richieste per server livellato nel tempo. La |

| | |
|---|---|
| | 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 adatto solo quando ha bisogno di bilanciare il carico di richieste ai server in modo uniforme; un esempio sarebbero i server web di ricerca. Tuttavia, quando ha bisogno di bilanciare il carico in base al carico dell'applicazione o al carico del server, o anche assicurarsi di usare lo stesso server per la sessione, il metodo Round Robin è inappropriato. |
| Meno connessioni | Il bilanciatore di carico tiene traccia del numero di connessioni correnti a ciascun Real Server. Il Real Server con il minor numero di connessioni riceve la nuova richiesta successiva. |
| Affinità/Persistenza di sessione di livello 3 - IP Bound | In questa modalità, l'indirizzo IP del cliente costituisce la base per selezionare quale Real Server riceverà la richiesta. Questa azione fornisce persistenza. I protocolli HTTP e Layer 4 possono usare questo modo. 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 Layer 4 e proxy, tutte le richieste possono sembrare provenire da un solo cliente e quindi il carico non sarebbe uniforme. Con HTTP, l'informazione dell'intestazione (X-Forwarder-For) viene usata quando presente per far fronte ai proxy. |
| Affinità/Persistenza di sessione Layer 3 - Basato su lista IP | La connessione al Real Server inizia usando "Least connections" quindi, l'affinità di sessione si ottiene in base all'indirizzo IP del cliente. Una lista viene mantenuta per 2 ore di default, ma questo può essere cambiato usando un jetPACK. |
| Layer 7 Session Affinity/Persistence - Session Cookie | Questa modalità è il metodo di persistenza più popolare per il bilanciamento del carico HTTP. In questa modalità, l'ADC usa il bilanciamento del carico basato su liste IP per ogni prima richiesta. Inserisce un cookie nelle intestazioni della prima risposta HTTP. In seguito, l'ADC usa il cookie del cliente per instradare il traffico allo stesso server back-end. Questo cookie viene usato per la persistenza quando il cliente ha bisogno di andare ogni volta allo stesso server back-end. Il cookie scade una volta chiusa la sessione. |
| Layer 7 Session Affinity/Persistence - Cookie persistente | La modalità di bilanciamento del carico basata su liste IP viene usata per ogni prima richiesta. L'ADC inserisce un cookie nelle intestazioni della prima risposta HTTP. In seguito, l'ADC usa il cookie del cliente per instradare il traffico allo stesso server back-end. Questo cookie viene usato per la persistenza quando il cliente deve andare ogni volta allo stesso server back-end. Il cookie scade dopo 2 ore e la connessione viene bilanciata secondo un algoritmo IP List Based. Questo tempo di scadenza è configurabile usando un jetPACK. |
| Cookie di sessione - Cookie di sessione ASP classico | Active Server Pages (ASP) è una tecnologia lato server di Microsoft. Con questa opzione selezionata, l'ADC manterrà la persistenza della sessione allo stesso server se un cookie ASP viene rilevato e trovato nella sua lista di cookie conosciuti. Al rilevamento di un nuovo cookie ASP, verrà bilanciato il carico usando l'algoritmo Least Connections. |
| Cookie di sessione - ASP.NET Session Cookie | Questa modalità si applica a **ASP.net.** Con questa modalità selezionata, l'ADC manterrà la persistenza della sessione allo stesso server se un cookie ASP.NET viene rilevato e trovato nella sua lista di cookie |

| | |
|---|---|
| | conosciuti. Al rilevamento di un nuovo cookie ASP, verrà bilanciato il carico usando 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 allo stesso server se un cookie JSP viene rilevato e trovato nella sua lista di cookie conosciuti. Al rilevamento di un nuovo cookie JSP, verrà bilanciato il carico usando l'algoritmo Least Connections. |
| Cookie di sessione - JAX-WS Session Cookie | 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, verrà bilanciato il carico usando 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 usa il Cookie RDP creato da Microsoft basato su nome utente/dominio per fornire persistenza ad un server. Il vantaggio di questo metodo è che è possibile mantenere una connessione ad un server anche se l'indirizzo IP del cliente cambia. |
| Basato su cookie-ID | Un nuovo metodo molto simile a "PhpCookieBased" e altri metodi di bilanciamento del carico, ma usando CookieIDBased e cookie RegEx h=[^;]+<br><br>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).<br><br>Il valore predefinito è CookieIDName="h"; tuttavia, se c'è un valore di override nella configurazione delle impostazioni avanzate del server virtuale, usi invece questo. **NOTA**: se questo valore è impostato, sovrascriviamo l'espressione cookie di cui sopra per sostituire h= con il nuovo valore.<br><br>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.) |

### *Monitoraggio del server*

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



Scelga il metodo di monitoraggio che desidera 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 è sicuro di quale monitor scegliere, il predefinito TCP Connection è un ottimo punto di partenza.

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

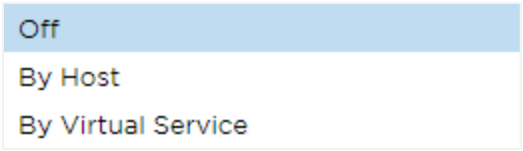

Possiamo vedere che Layer 3 Ping e Layer 4 TCP Connect sono riusciti se guardiamo la linea superiore, ma Layer 7 200OK non è riuscito. Questi risultati di monitoraggio forniscono abbastanza informazioni per indicare che il routing è OK e c'è un servizio in esecuzione sulla porta pertinente, ma il sito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

| 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 situazioni in cui il monitoraggio sconvolge un server e per 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. Usi questo metodo di monitoraggio con qualsiasi tipo di servizio. |
| Eco di ping/ICMP | In questa modalità, l'ADC invia una richiesta ICMP echo all'IP del content server. Se si riceve 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 | In questa modalità, viene effettuata una connessione TCP al Real Server e immediatamente interrotta senza inviare dati. 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. I servizi UDP sono gli unici attualmente non adatti al monitoraggio della connessione TCP. |
| ICMP Irraggiungibile | L'ADC invierà un controllo di salute UDP al server e segnerà il Real Server come non disponibile se riceve un messaggio ICMP port unreachable. Questo metodo può essere utile quando deve 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 si inizializza una connessione TCP al Real Server. Dopo che la connessione riesce, l'ADC invia al Real Server una richiesta HTTP. Si attende una risposta HTTP e si controlla il codice di risposta "200 OK". Se viene ricevuto il codice di risposta "200 OK", l'ADC ritiene che il Real Server sia attivo e funzionante. Se l'ADC non riceve un codice di risposta "200 OK" per qualsiasi |

| | |
|---|---|
| | motivo, compresi timeout, mancata connessione e altri motivi, l'ADC segna il Real Server non disponibile. Questo metodo di monitoraggio è valido solo per i tipi di servizio HTTP e HTTP accelerato. Se un tipo di servizio Layer 4 è in uso per un server HTTP, è utilizzabile se SSL non è in uso sul Real Server o è 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 su connessione. Una conversazione che include una "Associate Accept" dal content server, un trasferimento di una piccola quantità di dati seguito da una "Release Request", quindi una "Release Response" conclude con successo il monitor. Se, per qualsiasi motivo, il monitor non si conclude con successo, il Real Server viene considerato inattivo. |
| Definito dall'utente | Qualsiasi monitor configurato nella sezione Monitoraggio del server reale apparirà nell'elenco. |

### *Strategia di caching*

Per default, la Strategia di Caching è disabilitata e impostata come Off. Se il suo tipo di servizio è HTTP, allora può applicare due tipi di Caching Strategy.




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

| Opzione | Descrizione |
|---|---|
| Per ospite | La cache per host si basa sull'applicazione per hostname. Esisterà una cache separata 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 sceglie questa opzione. Esisterà solo una Cache per tutti i domini/nomi di host che passano attraverso il servizio virtuale. Questa opzione è un'impostazione specialistica da usare con cloni multipli di un singolo sito. |

### *Accelerazione*

| Opzione | Descrizione |
|---|---|
| Off | Disattivare la compressione per il servizio virtuale |
| Compressione | Se selezionata, questa opzione attiva la compressione per il servizio virtuale selezionato. L'ADC comprime dinamicamente il flusso di dati al cliente 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. Può anche escludere certi tipi di contenuto usando la sezione Global Exclusions. |

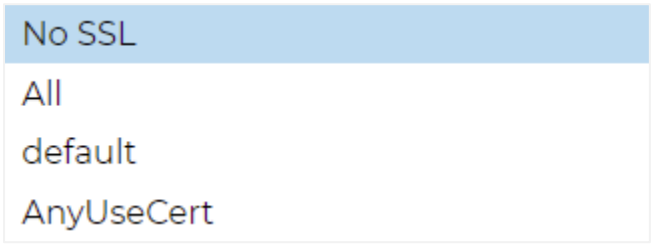
Nota: se l'oggetto è cacheable, l'ADC memorizza una versione compressa e la serve staticamente (dalla memoria) finché il contenuto non scade e viene riconvalidato.

### *Certificato SSL del servizio virtuale (crittografia tra il cliente e l'ADC)*

Per impostazione predefinita, l'impostazione è No SSL. Se il suo tipo di servizio è "HTTP" o "Layer4 TCP", può selezionare un certificato dal menu a tendina da applicare al servizio virtuale. I certificati che sono stati creati o importati appariranno in questo elenco. Può evidenziare più certificati da applicare ad un servizio. Questa operazione abiliterà automaticamente l'estensione SNI per consentire un certificato in base al "Domain Name" richiesto dal cliente.

#### Indicazione del nome del server

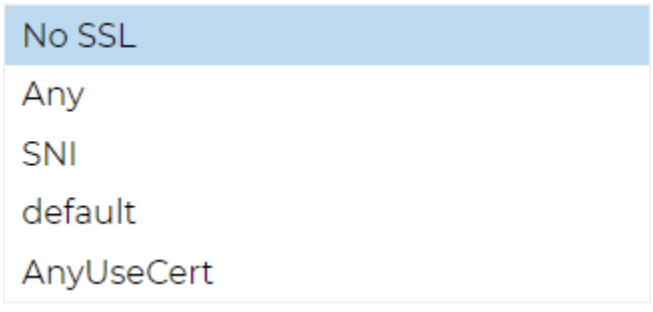
Questa opzione è un'estensione del protocollo di rete TLS con cui il cliente indica a quale hostname sta tentando di connettersi all'inizio del processo di handshaking. Questa impostazione permette all'ADC di presentare più certificati sullo stesso indirizzo IP virtuale e porta TCP.




| Opzione | Descrizione |
|---|---|
| No SSL | Il traffico dalla fonte 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 browser del canale. Usi questa opzione per testare SSL quando non ne è stato creato o importato uno. |
| AnyUseCert | Utilizzi qualsiasi certificato presente sull'ADC che l'utente ha caricato o generato |

### *Certificato SSL di Real Server (Crittografia tra ADC e Real Server)*

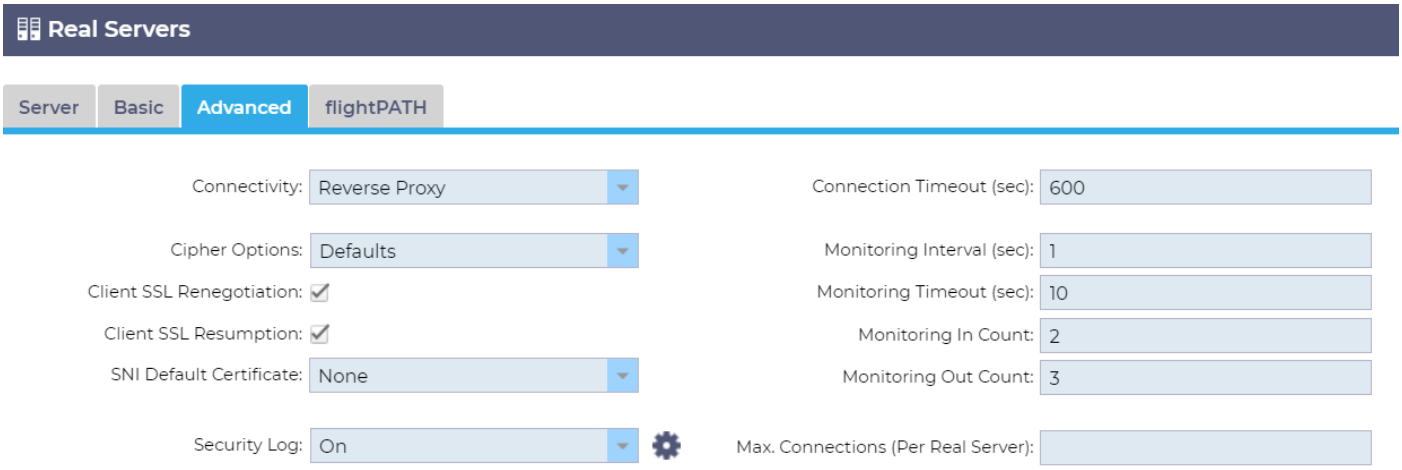
L'impostazione predefinita per questa opzione è No SSL. Se il suo server richiede una connessione criptata, questo valore deve essere diverso da No SSL. I certificati che sono stati creati o importati appariranno in questa lista.




| 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 accetterà qualsiasi certificato presentato dal Real Server. Il traffico dall'ADC al Real Server è criptato quando questa opzione è selezionata. Utilizzi l'opzione "Any" quando viene specificato un certificato sul lato |

| | |
|---|---|
| | Virtual Service, 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. Utilizzi l'opzione "Any" quando viene specificato un certificato sul lato Virtual Service, fornendo ciò che è noto come "SSL Bridging" o "SSL Re-Encryption". Scelga questa opzione per abilitare SNI sul lato server. |
| AnyUseCert | Tutti i certificati che ha generato o importato nell'ADC appaiono qui. |

## Advanced




### *Connettività*

Il suo Servizio Virtuale è configurabile con quattro 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 suo ADC agisce come 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 cliente bypassando l'ADC sulla risposta. DSR è adatto solo per l'uso con bilanciamento del carico a livello 4. Pertanto, Caching e Compressione non sono disponibili con questa opzione scelta.<br>Il bilanciamento del carico a livello 7 non funziona con questo DSR. Inoltre, non c'è supporto di persistenza diverso da IP List Based. Il bilanciamento del carico SSL/TLS con questo metodo non è l'ideale poiché il supporto di persistenza Source IP è l'unico tipo disponibile. DSR richiede anche modifiche al Real Server. Faccia riferimento alla sezione Modifiche al Real Server. |
| Gateway | La modalità gateway le permette di instradare tutto il traffico attraverso l'ADC, permettendo al traffico dai Real Server di essere instradato tramite l'ADC verso altre reti attraverso le macchine virtuali ADC o le interfacce hardware. L'uso del dispositivo come gateway per i Real Server è ideale quando funziona in modalità multi-interfaccia.<br>Il bilanciamento del carico a livello 7 con questo metodo non funziona in quanto non c'è un supporto di persistenza diverso da IP List Based. Questo metodo richiede che il Real Server imposti il suo gateway predefinito all'indirizzo |

dell'interfaccia locale (eth0, eth1, ecc.) dell'ADC. Faccia riferimento alla sezione Modifiche del Real Server.
***Noti che la modalità Gateway non supporta il failover in un ambiente cluster.***

### *Opzioni di cifratura*

Può 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 e lei può aggiungere diversi cifrari usando i jetPACK. Aggiungendo il jetPACK appropriato, può impostare le opzioni Cipher per servizio. Il vantaggio è che può creare diversi servizi con diversi livelli di sicurezza. Tenga presente che i client più vecchi non sono compatibili con i cifrari più recenti per ridurre il numero di client più il servizio è sicuro.

### *Rinegoziazione SSL del cliente*

Spunti questa casella se desidera permettere la rinegoziazione SSL avviata dal cliente. Disabiliti la rinegoziazione SSL del client per prevenire possibili attacchi DDOS contro il livello SSL deselezionando questa opzione.

### *Ripresa SSL del cliente*

Selezioni questa casella se desidera abilitare le sessioni del server di riassunzione SSL aggiunte alla cache di sessione. Quando un cliente propone il riutilizzo di una sessione, il server cercherà di riutilizzare la sessione se trovata. Se Resumption è deselezionato, non avviene alcun caching di sessione per il client o il server.

### *Certificato predefinito SNI*

Durante una connessione SSL con SNI lato cliente 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 Nessuno, che in effetti farebbe cadere la connessione se non ci fosse una corrispondenza esatta. Scelga uno qualsiasi dei certificati installati dal menu a tendina da presentare nel caso in cui non ci sia una corrispondenza esatta del certificato SSL.

### *Registro di sicurezza*

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

### *Timeout della connessione*

Il timeout di connessione predefinito è di 600 secondi o 10 minuti. Questa impostazione regola il tempo di timeout della connessione in assenza di attività. Lo riduca per il traffico web senza stato di breve durata, che in genere è di 90s o meno. Aumenti questa cifra per connessioni statiche come RDP a qualcosa come 7200 secondi (2 ore) o più, a seconda della sua infrastruttura. L'esempio del timeout RDP significa che se un utente ha un periodo di inattività di 2 ore o meno, le connessioni rimangono 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 1secondo. 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 ad una richiesta di connessione. Il valore predefinito è 2s. Aumenti questo valore per i server occupati.

### *Monitoraggio nel conteggio*

Il valore predefinito per questa impostazione è 2. Il valore 2 indica che il Real Server deve superare due controlli di monitoraggio dello stato di salute con successo prima di entrare in servizio. 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 di Real Server deve fallire tre volte prima che l'ADC smetta di inviare traffico al server e questo venga marcato ROSSO e Irraggiungibile. Aumentando questo valore si otterrà un servizio migliore e più affidabile a scapito del tempo necessario all'ADC per smettere di inviare traffico a questo server.

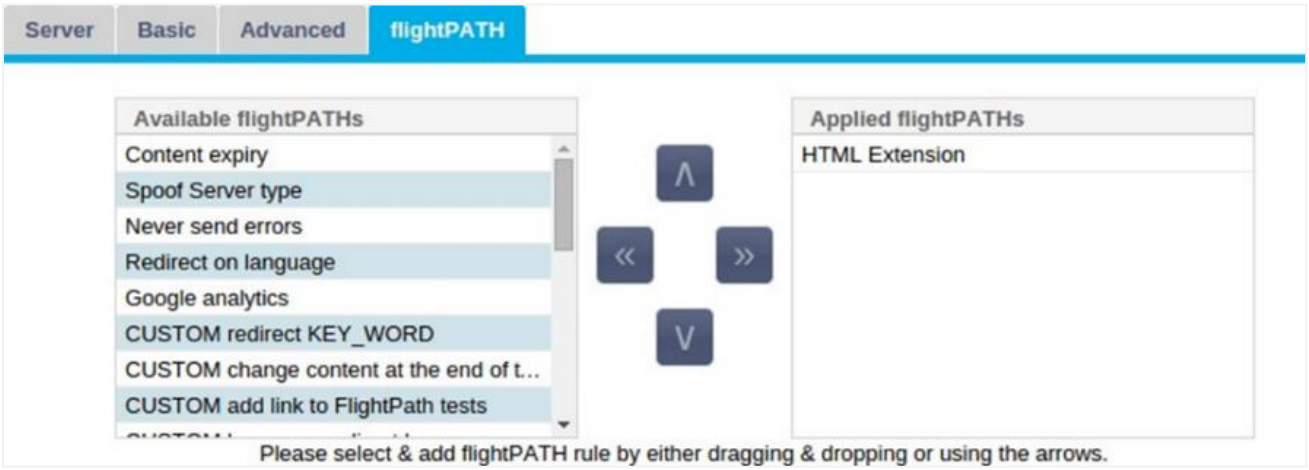
### *Passa a Offline in caso di guasto*

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

### *Max. Connessioni*

Limita il numero di connessioni Real Server simultanee e viene impostato per servizio. Per esempio, se lo configura a 1000 e ha due Real Server, l'ADC limita **ogni** Real Server a 1000 connessioni simultanee. Può 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. Lasci in bianco per connessioni illimitate. Quello che imposta qui dipende dalle risorse del suo 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 venditori, flightPATH non opera attraverso una linea di comando o una console di inserimento di script. Utilizza invece 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.

Come può vedere dall'immagine qui sopra, a sinistra c'è un elenco di regole disponibili e a destra le regole applicate al servizio virtuale.

Aggiunga una regola disponibile trascinandola dal lato sinistro a quello destro o evidenziando una regola e cliccando la 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, evidenzi la regola e si sposti su e giù usando le frecce.

Per rimuovere una regola, la trascini nell'inventario delle regole a sinistra o evidenzi la regola e clicchi sulla freccia sinistra.

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

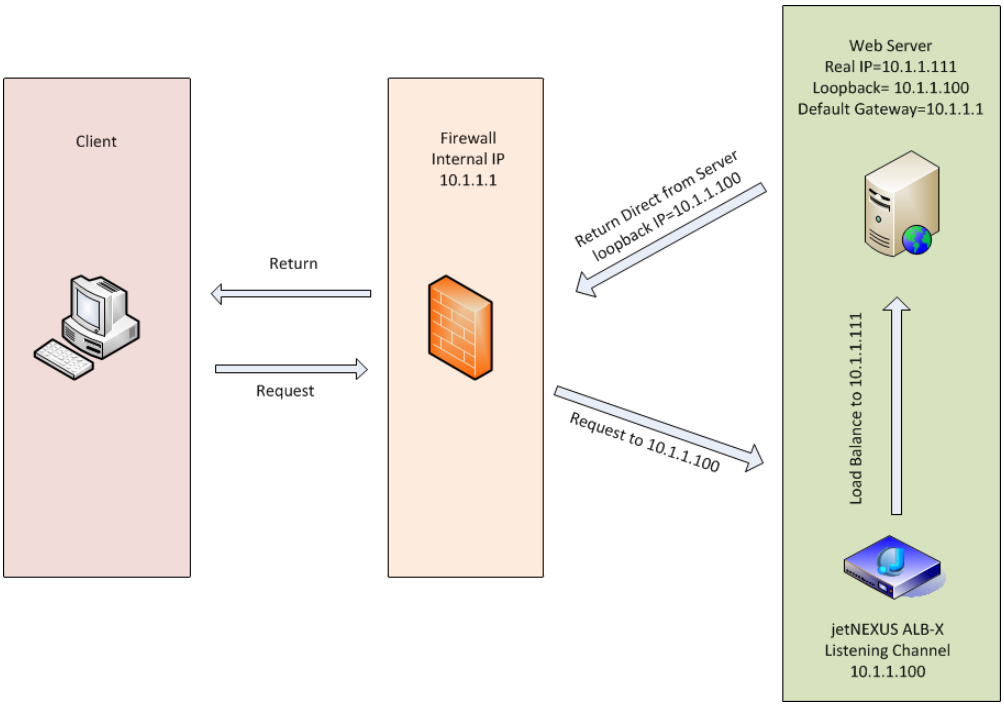
## Modifiche al server reale per il ritorno del server diretto

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 cliente, bypassando l'ADC sulla risposta. DSR è adatto solo per l'uso con bilanciamento del carico a livello 4. Caching e compressione non sono disponibili se abilitati.

Il bilanciamento del carico Layer 7 con questo metodo non funziona 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 di 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 per edgeNEXUS



## Configurazione del server dei contenuti richiesta

### 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
- Esegua quanto segue in un prompt dei comandi per ogni interfaccia di rete che ha configurato sui Windows Real Server

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

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

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

### 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*

- Esegua "sysctl - p"

## Modifiche al server reale - Modalità Gateway

La modalità gateway le permette di instradare tutto il traffico attraverso l'ADC e questo permette al traffico proveniente dai server di contenuto 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 contenuto dovrebbe essere usato quando si lavora in modalità multi-interfaccia.

**Come funziona**

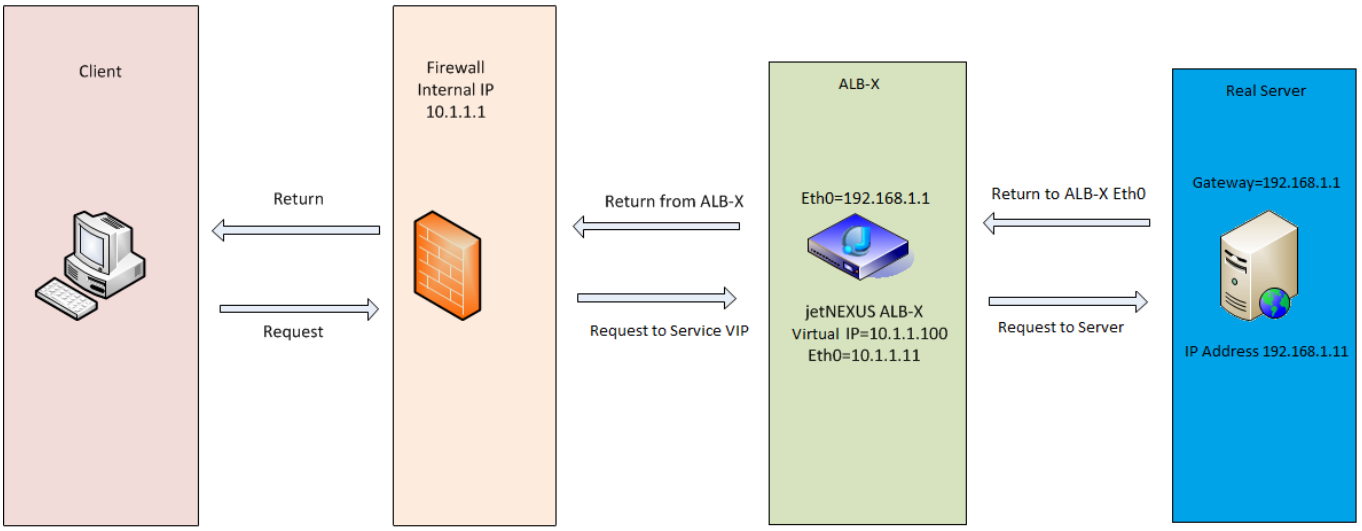
- Il cliente invia una richiesta al jetNEXUS ALB-X
- Una richiesta viene ricevuta da edgeNEXUS
- Richiesta inviata ai server di contenuto

- Risposta inviata a edgeNEXUS
- ADC instrada la risposta al cliente

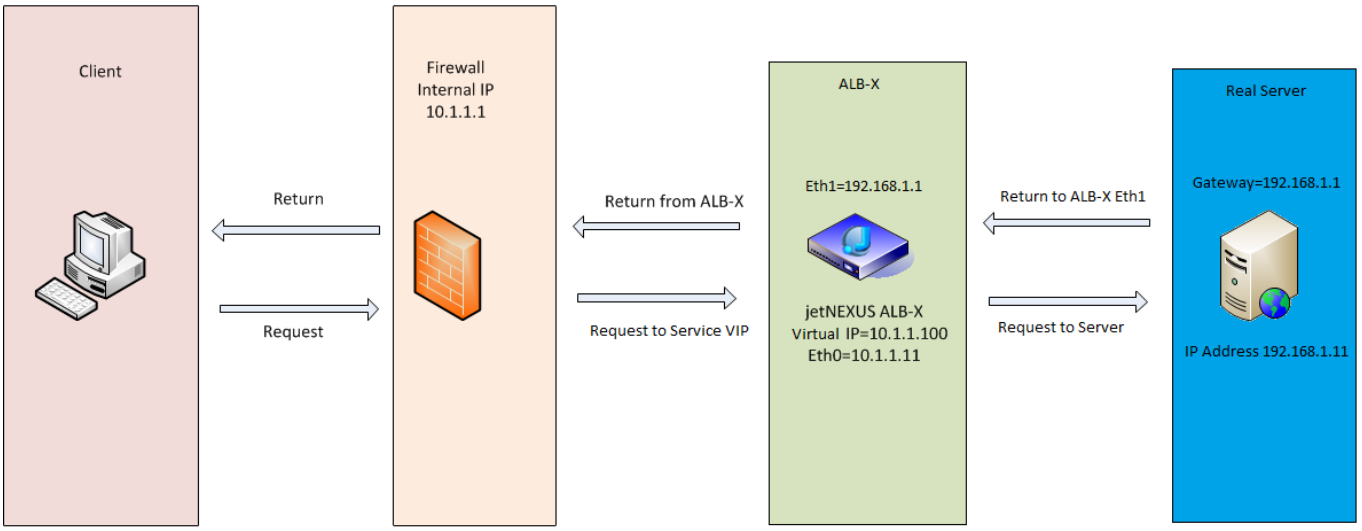
## Configurazione del server dei contenuti richiesta

- Single Arm Mode - si utilizza un'interfaccia, ma il servizio VIP e i Real Server devono trovarsi su sottoreti diverse.
- Dual Arm Mode - si utilizzano due interfacce, ma il servizio VIP e i server reali devono trovarsi su sottoreti diverse.
- In ogni caso, Single e Dual Arm, i Real Server devono configurare il loro gateway predefinito all'indirizzo dell'interfaccia ADC sulla relativa subnet.

## Esempio di braccio singolo




## Esempio di braccio doppio



# Biblioteca

## Add-Ons

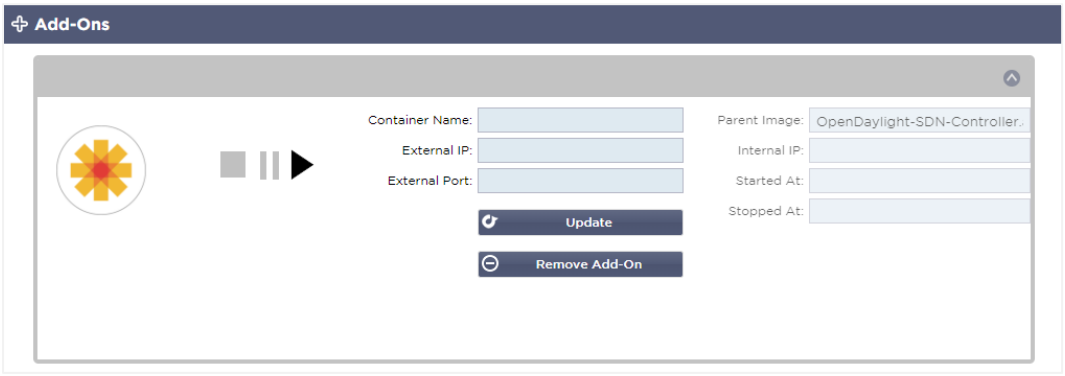
Gli add-on sono contenitori basati su Docker che possono funzionare in modo isolato all'interno dell'ADC. Esempi di add-on potrebbero essere un firewall applicativo o anche una micro istanza dell'ADC stesso.

### Applicazioni

La sezione App all'interno di Add-Ons mostra in dettaglio le App che ha acquistato, scaricato e distribuito.

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

Una volta che ha distribuito un'App, questa apparirà nell'area App.




### Acquisto di un add-on

Per acquistare un'App, deve registrarsi all'App Store. L'acquisto avviene tramite l'ADC stesso. Troverà

Vada alla pagina Library > Apps della dashboard di ADC.

Qui può selezionare l'App che desidera scaricare e poi installare.

Se lo sta facendo dalla dashboard ADC, selezioni solo 1 elemento. Può possedere più set ADC e le applicazioni devono essere associate all'ADC su cui vengono distribuite.

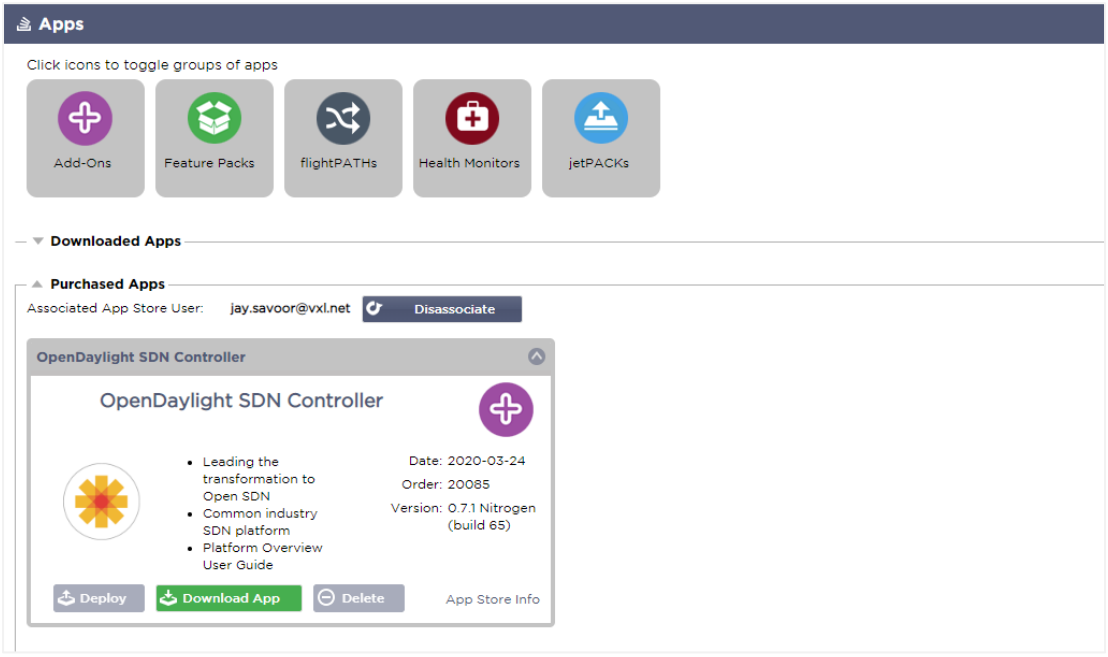
Se accede all'App Store tramite desktop e browser, può scaricarne quante ne vuole. Per esempio, quattro istanze di WAF o GSLB. Appariranno nell'area Purchased Apps del suo ADC, così potrà scaricarle.

Le App si associano agli ADC che possiede e che ha registrato.

Quando sceglie di scaricare un'App, le viene chiesto l'ID macchina, dopodiché l'App viene criptata e collegata all'ID macchina ADC.

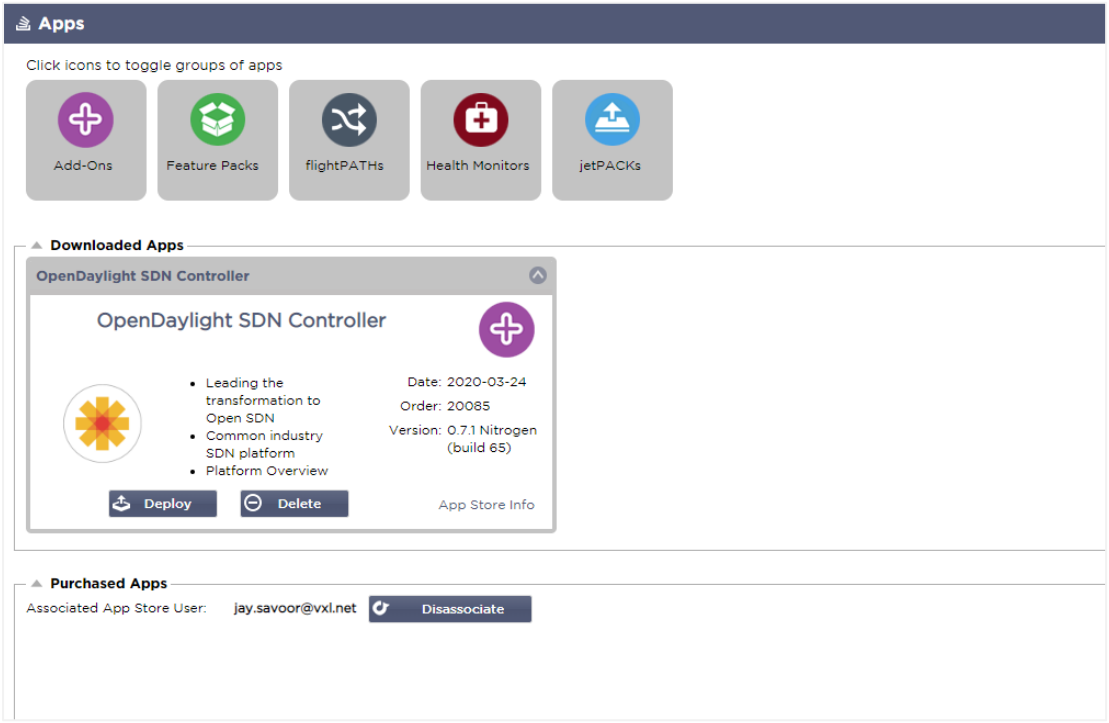
I link all'App Store sono:

- Add-Ons: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/ADD-ON/**
- Monitor di 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 flightPATH: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/FLIGHTPATH/**
- Aggiornamenti software: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/EDGENEXUS-SOFTWARE-UPDATE/**




## Distribuire un'App

Una volta scaricata sull'ADC, l'App verrà 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 le permette di impostare server di autenticazione e creare regole di autenticazione con opzioni per Basic o Forms lato client e NTLM o BASIC lato server.

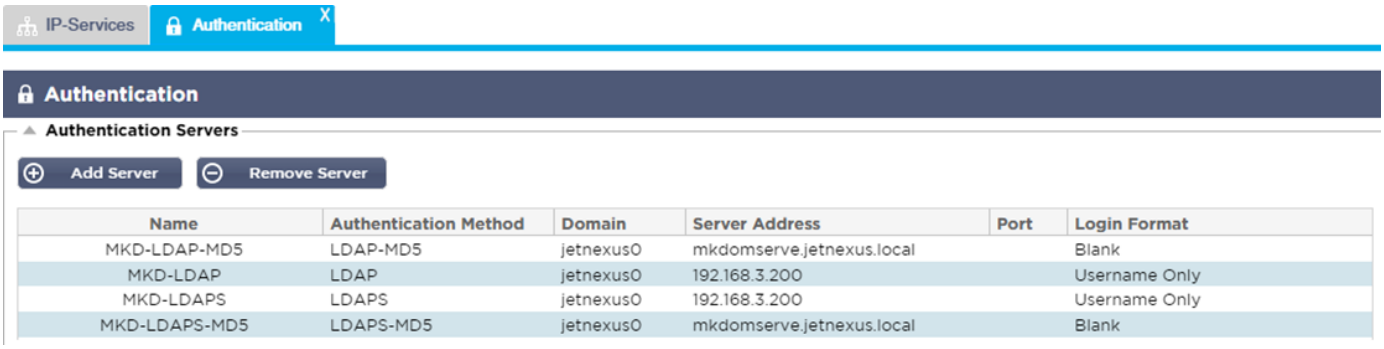
## Impostare l'autenticazione - un flusso di lavoro

Esegua i seguenti passi come minimo per applicare l'Autenticazione al suo servizio.

1. Crei un server di autenticazione.
2. Crei una regola di autenticazione che usi un server di autenticazione.
3. Crei una regola flightPATH che usi una regola di autenticazione.
4. Applica la regola flightPATH a un servizio

## Server di autenticazione

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



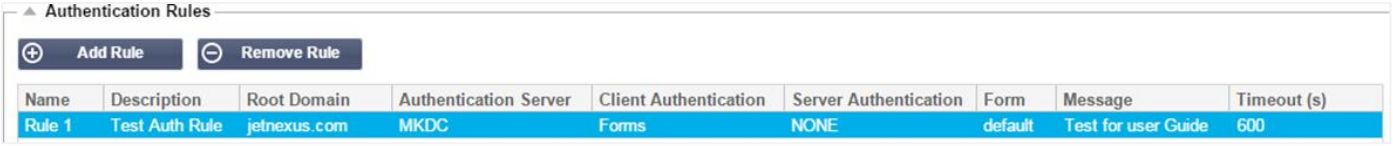

- Clicchi il pulsante Add Server.
- Questa azione produrrà una riga vuota pronta per il completamento.

| Opzione | Descrizione |
|---|---|
| Nome | Dia un nome al suo server per identificarlo - questo nome viene usato nelle regole |
| Descrizione | Aggiunga una descrizione |
| Metodo di autenticazione | Scelga un metodo di autenticazione<br>LDAP - LDAP di base con nomi utente e password inviati in chiaro al server LDAP.<br>LDAP-MD5 - LDAP di base con nome utente in chiaro e password con hash MD5 per una maggiore sicurezza.<br>LDAPS - LDAP su SSL. Invia la password in chiaro all'interno di un tunnel criptato tra l'ADC e il server LDAP.<br>LDAPS-MD5 - LDAP su SSL. La password è sottoposta a hash MD5 per una maggiore sicurezza all'interno di un tunnel criptato tra l'ADC e il server LDAP |
| Dominio | Aggiunga il nome del dominio del server LDAP. |
| Indirizzo del server | Aggiunga l'indirizzo IP o il nome host del server di autenticazione<br>LDAP - Indirizzo IPv4 o hostname.<br>LDAP-MD5 - solo hostname (l'indirizzo IPv4 non funziona)<br>LDAPS - Indirizzo IPv4 o nome host.<br>LDAPS-MD5 - solo hostname (l'indirizzo IPv4 non funziona). |
| Porto | Usa la porta 389 per LDAP e la porta 636 per LDAPS per default. Non è necessario aggiungere il numero di porta per LDAP e LDAPS. Quando saranno disponibili altri metodi, potrà 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). |
| Ricerca Base | Questo valore è il punto di partenza per la ricerca nel database LDAP. Esempio *dc=mycompany,dc=local* |
| Formato di accesso | Usi il formato di login che le serve.<br>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.<br>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.<br>Blank - l'ADC accetterà qualsiasi cosa l'utente inserisca e la invierà al server di autenticazione. Questa opzione si usa quando si usa MD5. |
| Passphrase | Questa opzione non è usata in questa versione. |

| | |
|---|---|
| Tempo morto | Non utilizzato in questa versione |

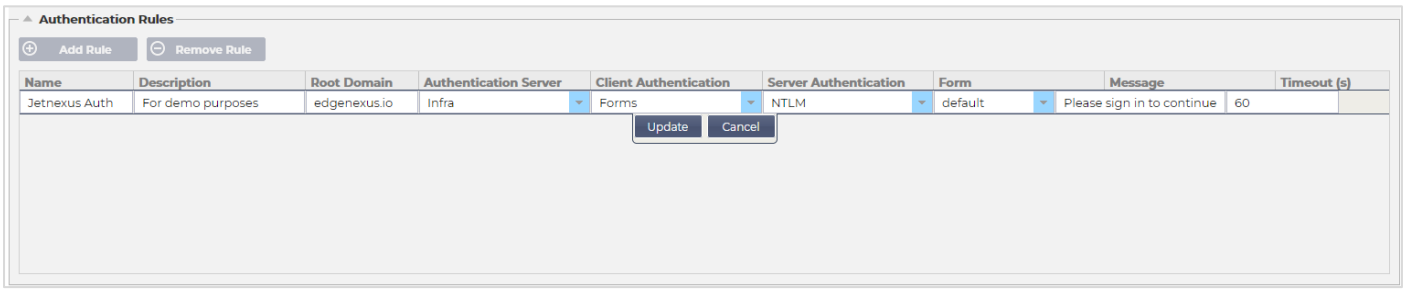
## Regole di autenticazione

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




| Campo | Descrizione |
|---|---|
| Nome | Aggiunga un nome adatto alla sua regola di autenticazione. |
| Descrizione | Aggiunga una descrizione adeguata. |
| Dominio radice | Questo deve essere lasciato vuoto a meno che non abbia bisogno di single-sign-on tra i sottodomini. |
| Server di autenticazione | Questa è una casella a discesa che contiene i server che ha configurato. |
| Autenticazione del cliente: | Scelga il valore adatto alle sue esigenze:<br>Basic (401) - Questo metodo usa il metodo di autenticazione standard 401<br>Forme - questo presenterà all'utente il modulo predefinito ADC. All'interno del modulo può aggiungere un messaggio. Può selezionare un modulo che ha caricato utilizzando la sezione sottostante. |
| Autenticazione del server | Scelga il valore appropriato.<br>Nessuno - se il suo server non ha alcuna autenticazione esistente, selezioni questa impostazione. Questa impostazione significa che può aggiungere capacità di autenticazione ad un server che prima non ne aveva.<br>Basic - se il suo server ha l'autenticazione di base (401) abilitata, allora selezioni BASIC.<br>NTLM - se il suo server ha l'autenticazione NTLM abilitata, allora selezioni NTLM. |
| Modulo | Scelga il valore appropriato<br>Default - Selezionando questa opzione l'ADC userà il suo modulo incorporato.<br>Personalizzato - può aggiungere un modulo da lei progettato e selezionarlo qui. |
| Messaggio | Aggiunga un messaggio personale al modulo. |
| Timeout | Aggiunga un timeout alla regola, dopo il quale l'utente dovrà autenticarsi di nuovo. Noti che l'impostazione Timeout è valida solo per l'autenticazione basata su moduli. |

## Singolo accesso



Se desidera fornire un single sign-on per gli utenti, completi la colonna Root Domain con il suo dominio. In questo esempio abbiamo usato edgenexus.io. Ora possiamo avere più servizi che useranno edgenexus.io come dominio radice 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 usata. Lo stesso utente può poi connettersi a appstore. mycompany.com e sarà autenticato automaticamente dall'ADC. Può impostare il timeout, che forzerà l'autenticazione una volta raggiunto questo periodo di inattività.

## Moduli

Questa sezione le permetterà di caricare un modulo personalizzato.

### Come creare il suo modulo personalizzato

Anche se il modulo 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. Può creare il suo 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<br>azione = %JNURL%<br>Metodo = POST |
| Nome utente | Sintassi: nome = "JNUSER" |
| Password: | name="JNPASS" |
| Messaggio opzionale1: | %JNMESSAGE% |
| Messaggio opzionale2: | %JNAUTHMESSAGE% |
| Immagini | Se desidera aggiungere un'immagine, la preghiamo di aggiungerla in linea usando la codifica Base64. |

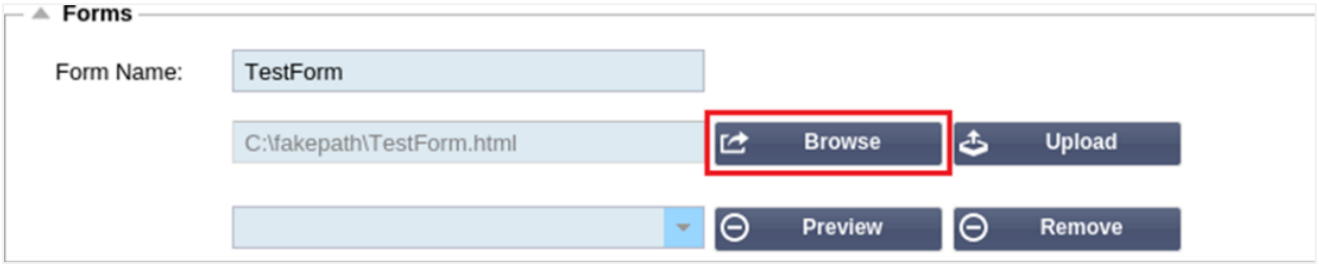
*Esempio di codice html di un modulo molto basico e semplice*

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

</HTML>

### Aggiungere un modulo personalizzato

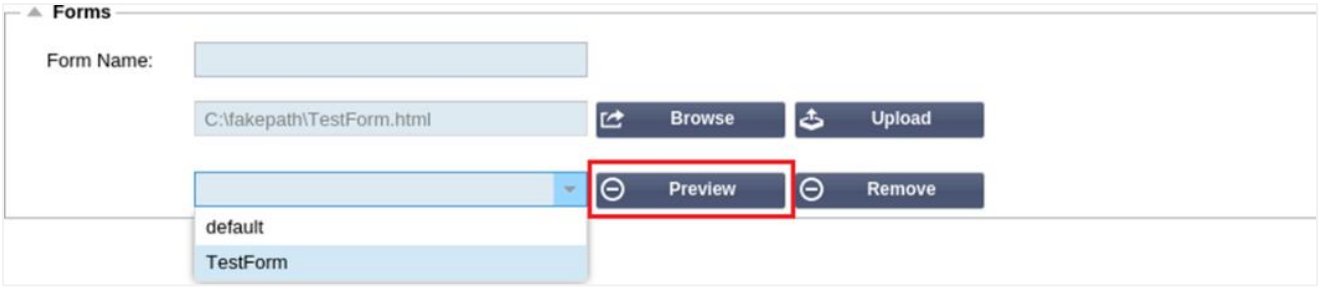
Una volta creato un modulo personalizzato, può aggiungerlo usando la sezione Forme.




1. Scelga un nome per il suo modulo
2. Cerca localmente il suo modulo
3. Clicchi su Upload

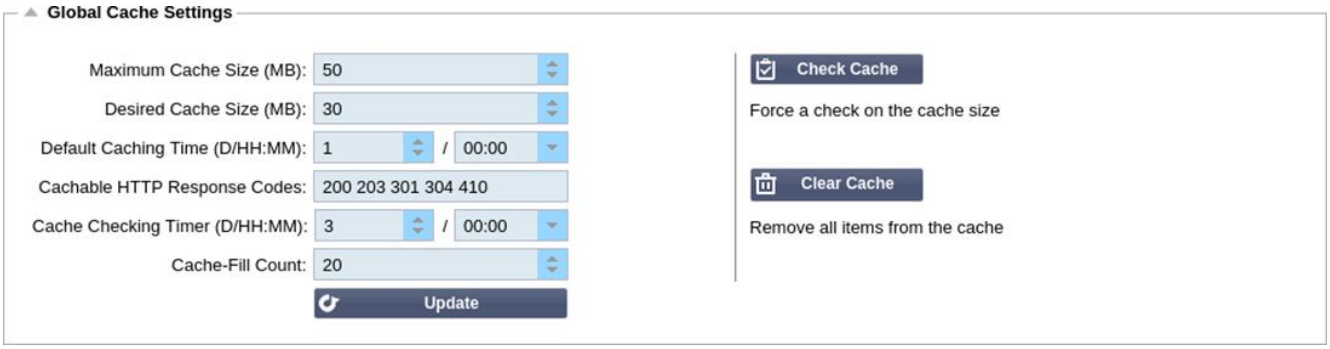
### Anteprima del suo modulo personalizzato

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




## Cache

L'ADC è in grado di cacciare 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 lavata periodicamente sul supporto di memorizzazione per mantenere la persistenza della cache dopo riavvii, riavvii e operazioni di spegnimento. Questa funzionalità significa che

la dimensione massima della cache deve rientrare nell'ingombro di memoria dell'apparecchio (piuttosto che nello spazio su disco) e non deve 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 tentare 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 sulla dimensione della cache per tagliare i contenuti scaduti. Ancora una volta, può essere più efficace accettare il valore predefinito (30 MB) e controllare periodicamente le dimensioni 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 cui viene conservato il contenuto senza una direttiva "no-store" o un tempo di scadenza esplicito nell'intestazione del traffico.

L'inserimento del campo ha la forma "D/HH:MM" - quindi 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 vengono memorizzati 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 dovrebbe invece essere usata una copia nella cache locale
- 410 - La risorsa non è più disponibile sul server e non è noto alcun indirizzo di inoltro

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

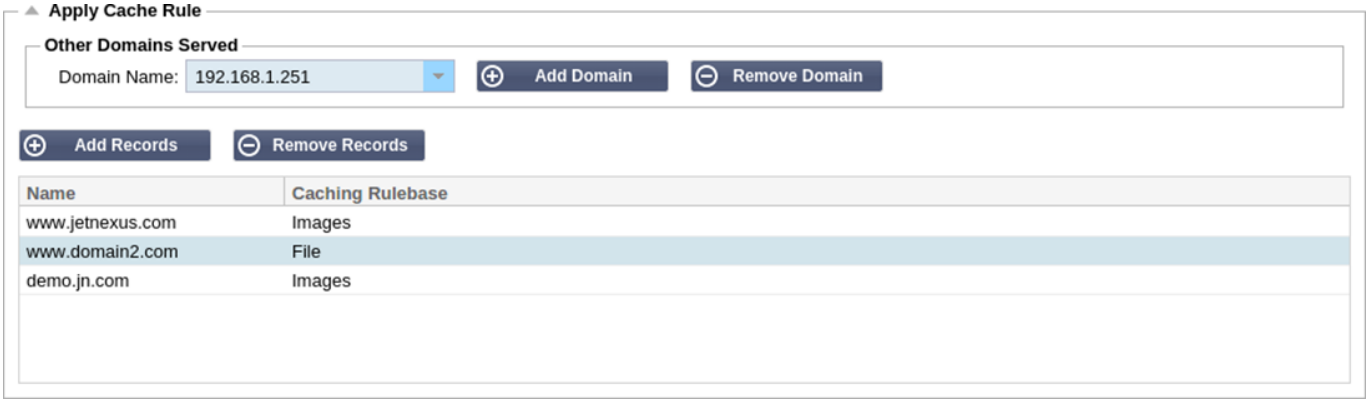
### *Tempo di controllo della cache (D/HH:MM)*

Questa impostazione determina l'intervallo di tempo tra le operazioni di rifinitura 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.

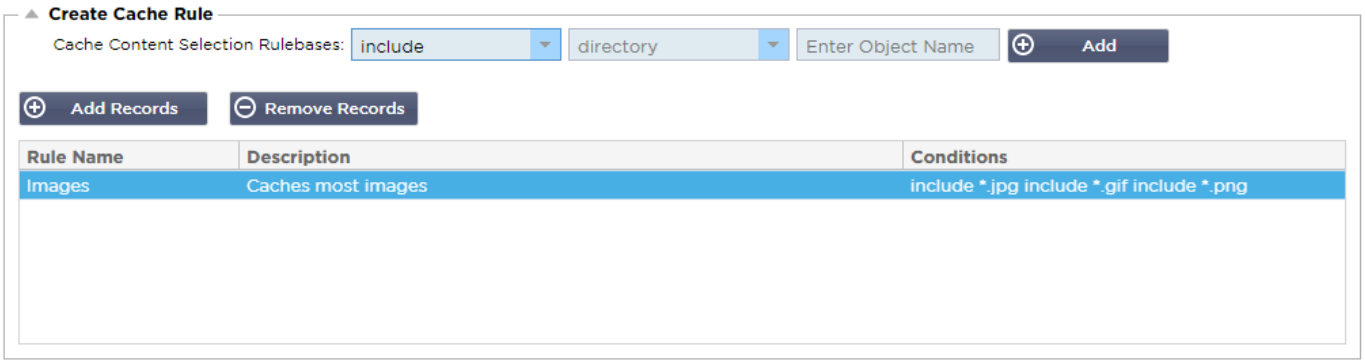
### Applica la regola della cache



Questa sezione le permette di applicare una regola di cache ad un dominio:

- Aggiunga il dominio manualmente con il pulsante Add Records. Deve usare un nome di dominio completamente qualificato o un indirizzo IP in notazione dotted-decimal. Esempio www.mycompany.com o 192.168.3.1:80
- Clicchi sulla freccia a discesa e scelga il suo 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
- Scelga la sua regola di cache facendo doppio clic sulla colonna Caching Rulebase e selezionando dall'elenco

### Creare regola di cache




Questa sezione le permette di creare diverse regole di caching che possono poi essere applicate ad un dominio:

- Clicchi su Add Records e dia alla sua regola un nome e una descrizione
- Può digitare manualmente le sue condizioni o usare la funzione Add Condition

Per aggiungere una condizione usando la Selection Rulebase:

- Scelga Includi o Escludi
- Scelga tutte le immagini JPEG
- Clicchi sul simbolo + Add
- Vedrà che 'include *.jpg' è stato aggiunto alle condizioni
- Può aggiungere più condizioni. Se sceglie di farlo manualmente, deve aggiungere ogni condizione su una riga NUOVA. Noti che le sue regole verranno visualizzate sulla stessa riga finché non clicca nella casella Condizioni, allora verranno visualizzate su una riga separata

## flightPATH

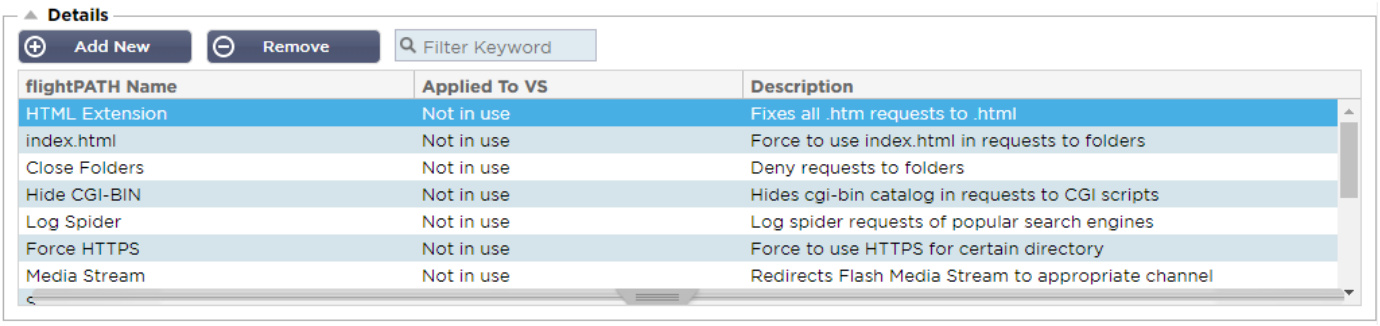
flightPATH è la tecnologia di gestione del traffico incorporata nell'ADC. flightPATH le permette di ispezionare il traffico HTTP e HTTPS in tempo reale ed eseguire azioni in base alle condizioni.

Le regole flightPATH devono essere applicate ad un VIP quando si usano oggetti IP all'interno delle regole.

Una regola del percorso di volo consiste di quattro elementi:

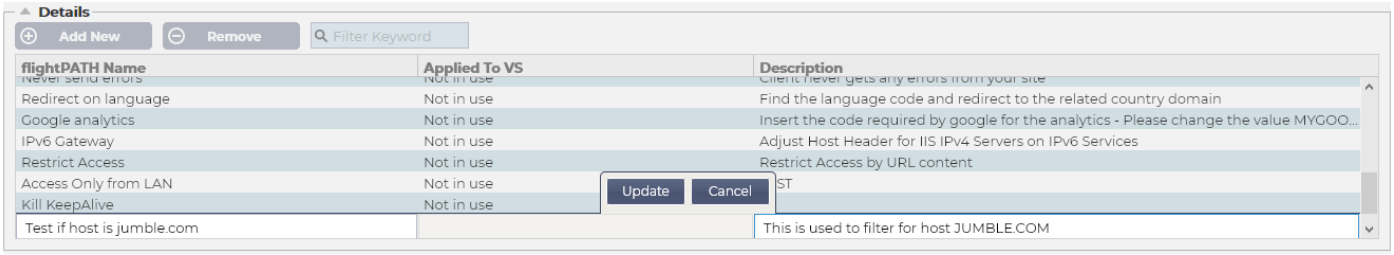
1. Dettagli, dove definisce il nome del flightPATH e il servizio a cui è collegato.
2. Condizioni che possono essere definite che causano l'attivazione della regola.
3. Valutazione che permette la definizione di variabili che possono essere usate all'interno di Azioni
4. Azioni che si usano per gestire ciò che dovrebbe succedere quando si verificano delle condizioni

## Dettagli




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

### *Aggiungere una nuova regola flightPATH*



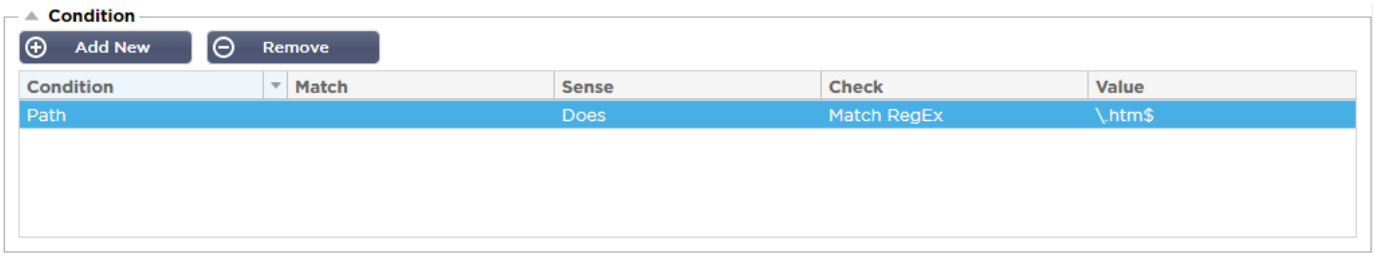

| Campo | Descrizione |
|---|---|
| Nome di FlightPATH | Questo campo è per il nome della regola flightPATH. Il nome che fornisce qui appare e viene referenziato in altre parti dell'ADC. |
| Applicato a VS | Questa colonna è di sola lettura e mostra il VIP a cui viene applicata la regola flightPATH.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

### Passi per aggiungere una regola flightPATH

1. Per prima cosa, clicchi sul pulsante Add New che si trova nella sezione Details.
2. Inserisca un nome per la sua regola. Esempio Auth2
3. Inserisca una descrizione della sua regola
4. Una volta che la regola è stata applicata a un servizio, vedrà la colonna Applied To autopopolarsi con un indirizzo IP e un valore di porta
5. Non dimentichi di premere il pulsante Update per salvare le sue modifiche o, se fa un errore, basta premere cancel per tornare allo stato precedente.

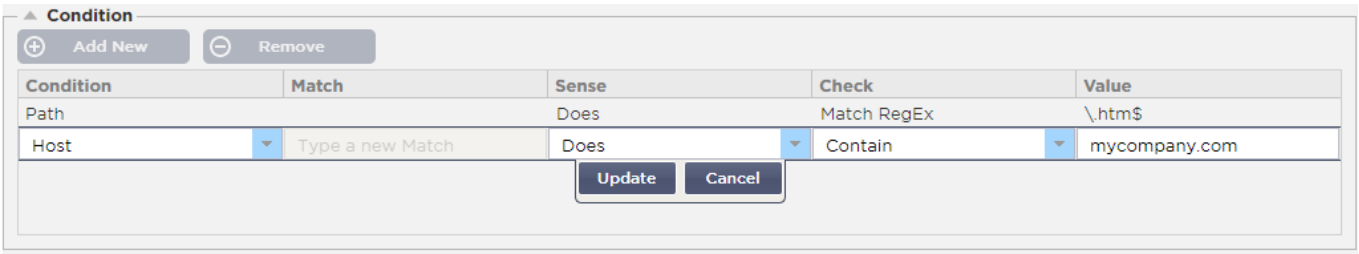
## Condizione

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



Può 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 come predefinite all'interno del dropdown e coprono tutti gli scenari previsti. Quando verranno 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 ad 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 dropdown 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 usare IP multipli o sottoreti. 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 | Controlli 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 della query | L'intera stringa della query dopo il carattere ? | |
| Richiesta 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 di 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 | O l'IP di origine, l'IP del server proxy o qualche altro indirizzo IP aggregato | ClientIP<br>, Proxy IP, Firewall IP. Può anche usare IP multipli e sottoreti. Deve sfuggire ai punti perché sono RegEX. Esempio 10\.1\.2\.3 è 10.1.2.3 |

### Match

Il campo Match può essere un drop-down o 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 viene mostrato come un campo di testo e se la Condizione è POST, il campo Match viene presentato come un drop-down contenente valori pertinenti.

Le scelte disponibili sono:

| MATCH | DESCRIZIONE | ESEMPIO |
|---|---|---|
| Accetta | 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: en-US |
| Accept-Ranges | Quali tipi di intervallo di contenuto parziale supporta questo server | Accettazioni: bytes |
| Autorizzazione | Credenziali di autenticazione per l'autenticazione HTTP | Autorizzazione: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ== |
| Charge-To | Contiene informazioni sul conto dei costi dell'applicazione del metodo richiesto | |
| Content-Encoding | Il tipo di codifica usato | Content-Encoding: gzip |
| Content-Length | La lunghezza del corpo della risposta in ottetti (byte da 8 bit) | Contenuto-Lunghezza: 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 email dell'utente che fa la richiesta | Da: user@example.com |
| If-Modified-Since | 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 | L'ultima data modificata per l'oggetto richiesto, nel formato RFC 2822 | Ultimo-Modificato: Tue, 15 Nov 1994 12:45:26 GMT |
| Pragma | Implementazione: 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 | Referrer: 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 utente | User-Agent: Mozilla/5.0 (compatibile; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0) |
| Vario | Dice ai proxy a valle come abbinare le future intestazioni di richiesta per decidere se<br>la risposta in cache può essere usata piuttosto che richiederne una nuova<br>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 scelte Does o Doesn't.

### Controlli

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 |
|---|---|---|
| Esiste | Questo non si preoccupa del dettaglio della condizione, solo che esiste/non esiste | Host - Does - Exist |
| Iniziare | La stringa inizia con il valore | Path - Does - Start - /secure |
| Fine | La stringa finisce con il valore | Percorso - Fa - Fine - .jpg |
| Contiene | La stringa contiene il valore | Intestazione della richiesta - Accept - Does - Contain - image |

| | | |
|---|---|---|
| Uguale | La stringa equivale al valore | Host - Does - Equal - www.jetnexus.com |
| Abbia Lunghezza | La stringa ha una lunghezza del valore | Host - Does - Have Length - 16www.jetnexus.com = TRUEwww.jetnexus.co.uk = FALSE |
| Corrispondenza RegEx | Le permette di inserire un'espressione regolare completa compatibile con Perl | Origin IP - Does - Match Regex - 10\..* \| 11\..* |

### Passi per aggiungere una condizione

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

1. Clicchi il pulsante Add New nell'area Condition.
2. Scelga una condizione dalla casella a discesa. Prendiamo Host come esempio. Può anche digitare nel campo e l'ADC mostrerà il valore in un drop-down.
3. Scelga un senso. Per esempio, Fa
4. Scelga un controllo. Per esempio, Contiene
5. Scelga un valore. Per esempio, mycompany.com


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

- 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. Gli ADC regolari offrono questa capacità usando opzioni di scripting o di riga di comando che non sono ideali per chiunque. L'ADC le 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 - selezioni i valori da un menu a tendina o li digiti manualmente.
- Valore - il valore che la variabile tiene e può essere un valore alfanumerico o una RegEx per la regolazione fine.

**Variabili incorporate:**

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

Può 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 = Registra | 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.

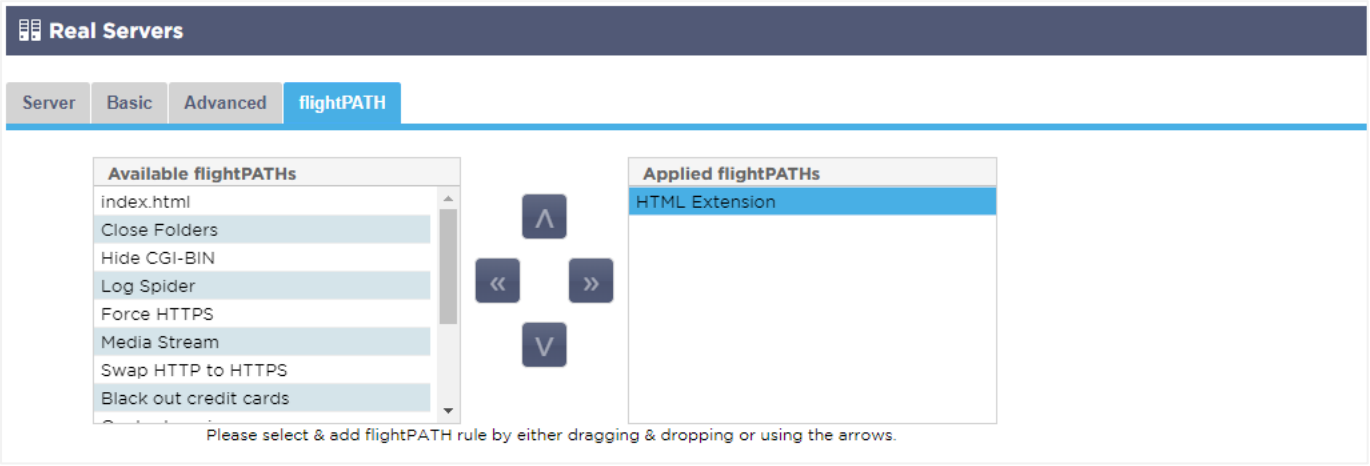

In questo esempio vogliamo riscrivere la porzione di percorso dell'URL per riflettere l'URL digitato dall'utente.

- Clicchi su Aggiungi nuovo
- Scelga Riscrivere percorso dal menu a discesa Azione
- Nel campo Target, digiti $path$/myimages
- Clicchi su Aggiornamento

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

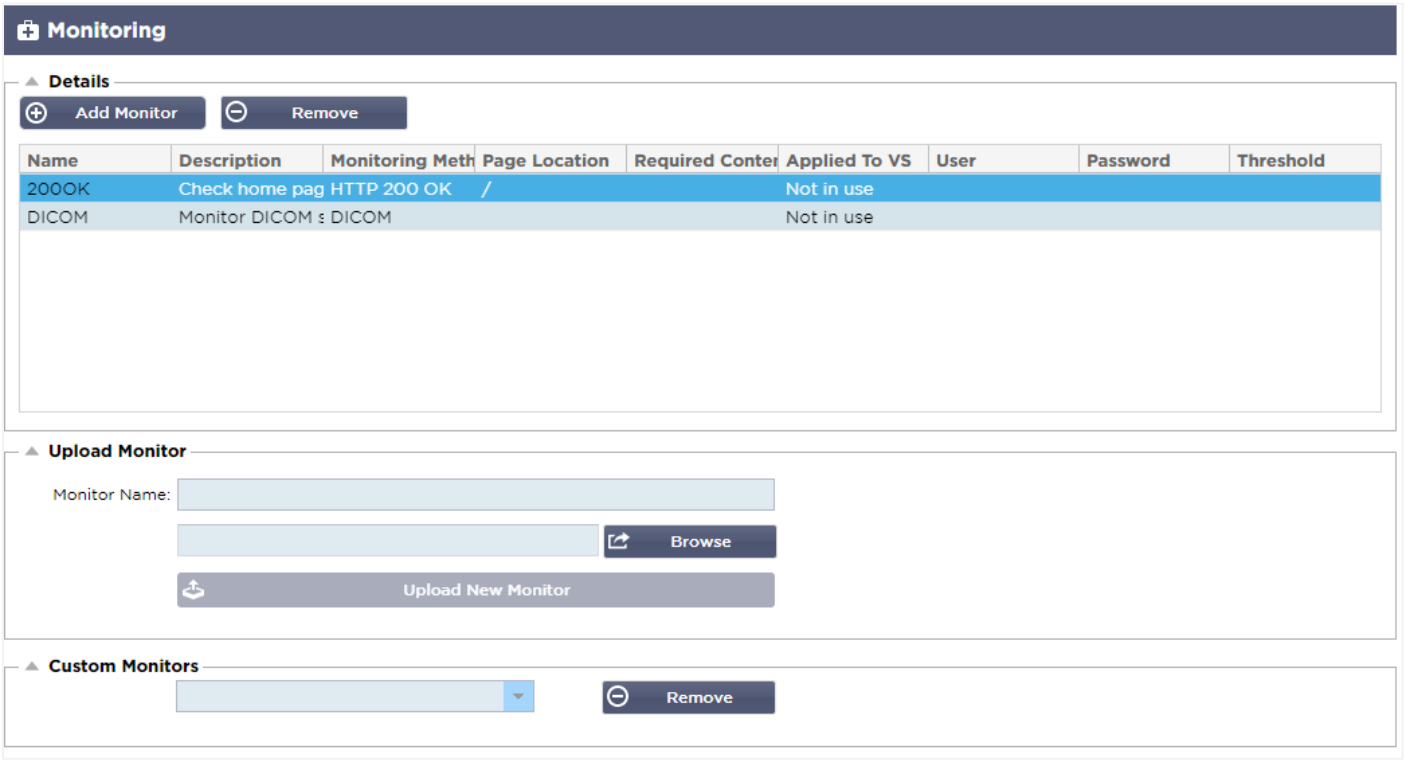
### Applicare la regola flightPATH

L'applicazione di qualsiasi regola di flightPATH avviene nella scheda flightPATH di ogni VIP/VS.




- Vada a Servizi > Servizi IP e scelga il VIP a cui vuole assegnare la regola flightPATH.
- Vedrà l'elenco di Real Server mostrato qui sotto
- Clicchi sulla scheda flightPATH
- Selezioni la regola flightPATH che ha configurato o una di quelle precostituite supportate. Può selezionare più regole flightPATH se necessario.
- Trascini il set selezionato nella sezione Applied flightPATHs o clicchi sul pulsante freccia >>.
- La regola verrà spostata sul lato destro e applicata automaticamente.

## Monitor di server reali




Quando si imposta il bilanciamento del carico, è utile monitorare la salute dei server reali e delle applicazioni che vi girano sopra. Per esempio, nei server web, si può impostare una pagina specifica da usare per monitorare lo stato o usare uno degli altri sistemi di monitoraggio di cui dispone l'ADC.

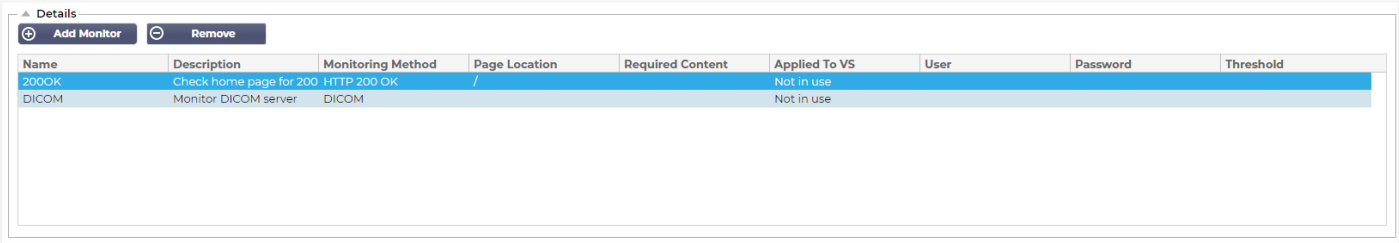
La pagina Library > Real Server Monitors le permette di aggiungere, visualizzare e modificare il monitoraggio personalizzato. Si tratta di "Health Checks" del server Layer 7 e li seleziona dal campo Server Monitoring all'interno della scheda Basic del servizio virtuale che definisce.

La pagina Real Server Monitors è divisa in tre sezioni.

- Dettagli
- Carichi
- Monitor personalizzati

## Dettagli

La sezione Dettagli si usa per aggiungere nuovi monitor e per rimuovere quelli che non le servono. Può anche modificare un monitor esistente facendo doppio clic su di esso.




### Nome

Nome di sua scelta per il suo monitor.

### Descrizione

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

### Metodo di monitoraggio

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

| Metodo di monitoraggio | Descrizione | Esempio |
|---|---|---|
| HTTP 200 OK | Viene effettuata una connessione TCP al Real Server. Dopo aver effettuato la connessione, viene inviata una breve richiesta HTTP al Real Server. Si attende una risposta HTTP dal server e si controlla il codice di risposta "200 OK". Se viene ricevuto il codice di risposta "200 OK", si ritiene che il Real Server sia attivo e funzionante. Se, per qualsiasi motivo, il codice di risposta "200 OK" non viene ricevuto, inclusi timeout o mancata connessione, allora il Real Server viene considerato giù e non disponibile. 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". | Nome: 200OK<br>Descrizione: Controllare il sito web di produzione<br>Metodo di monitoraggio: HTTP 200 OK<br>Posizione della pagina: /main/index.html<br>OR<br>HTTP://www.edgenexus.io/main/index.html<br>Contenuto richiesto: N/A |
| Risposta HTTP | Viene effettuata una connessione e una richiesta/risposta HTTP al Real Server e | Nome: Server Up |

| | | |
|---|---|---|
| | controllata come spiegato nell'esempio precedente. Ma invece di controllare un codice di risposta "200 OK", l'intestazione della risposta HTTP viene controllata per un contenuto di testo personalizzato. Il testo può essere un'intestazione completa, parte di un'intestazione, una riga di una parte della pagina o solo una parola. Se il testo viene trovato, il Real Server viene considerato funzionante. 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". | Descrizione: Controlla il contenuto della pagina per "Server Up. "<br>Metodo di monitoraggio: Risposta HTTP<br>Posizione della pagina: /main/index.html<br>OR<br>HTTP://www.edgenexus.io/main/index.html<br>Contenuto richiesto: Server Up |
| DICOM | Inviamo un eco DICOM usando il valore "Source Calling" AE Title nella colonna del contenuto richiesto. Può anche impostare il valore AE Title "Destinazione Chiamata" nella sezione Note di ogni server. Può trovare la colonna Note all'interno di IP Services-<br>-Servizi virtuali -Pagina del server. | Nome: DICOM<br>Descrizione: Controllo salute L7 per servizio DICOM<br>Metodo di monitoraggio: DICOM<br>Posizione della pagina: N/A<br>Contenuto richiesto: Valore AET |
| TCP Fuori Banda | Il metodo TCP Out of Band è come un TCP Connect, tranne che può specificare la porta che desidera monitorare nella colonna del contenuto richiesto. Questa porta non è tipicamente la stessa della porta del traffico e si usa quando si vogliono legare servizi insieme | Nome: TCP Fuori Banda<br>Descrizione: Monitoraggio della porta Out of Band/Traffic<br>Posizione della pagina: N/A<br>Contenuto richiesto: 555 |
| Monitor TCP multiporta | Questo metodo è come il precedente, tranne che può avere diverse porte. Il monitor è considerato riuscito solo se tutte le porte specificate nella sezione contenuto richiesto rispondono correttamente. | Nome: Monitor Multiporta<br>Descrizione: Monitorare più porte per il successo<br>Posizione della pagina: N/A<br>Contenuto richiesto: 135,59534,59535 |

### Posizione della pagina

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

### Contenuto richiesto

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

### Applicato a VS

Questo campo viene popolato automaticamente con l'IP/Porta del Servizio Virtuale a cui è applicato il monitor. Non potrà cancellare nessun Monitor che è stato usato con un Servizio Virtuale.

### Utente

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

### Password

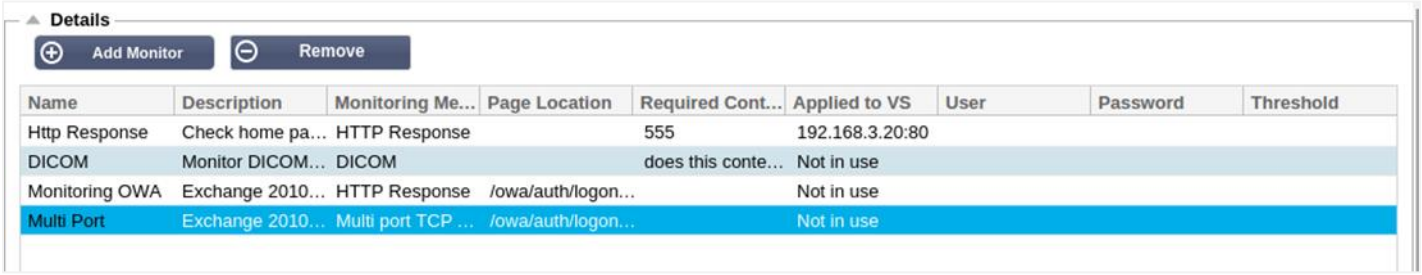
Alcuni monitor personalizzati possono usare questo valore insieme al campo Utente per accedere a un Real Server.

### Soglia

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

*NOTA: si assicuri che la risposta di ritorno dal server delle applicazioni non sia una risposta "Chunked".*

## Esempi di Real Server Monitor




### Monitoraggio dell'upload

Ci saranno molte occasioni in cui gli utenti vorranno creare i loro 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.


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

### Monitor personalizzati

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


- Clicchi sulla casella a discesa

- Selezioni il nome del monitor personalizzato
- Cliccare su Rimuovi
- Il suo 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 le mostra i comandi che può usare all'interno del suo script Perl.

Il comando #Monitor-Name: è il nome usato per lo script Perl memorizzato nell'ADC. Se non include questa linea, il suo script non verrà trovato!

I seguenti sono obbligatori:

- Nome-Monitor.
- utilizzare rigorosamente;
- avvertenza d'uso;

Gli script Perl vengono 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 "Notes" nella sezione Real Server di IP Services
- my $page = $_[4]; - Questo usa i valori "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 (purché OUT Count corrisponda)*

### Esempio di un monitor di salute personalizzato

```
#Nome-Monitor HTTPS_SNI

utilizzare rigorosamente:

avvertenze d'uso;

# Il nome del monitor come sopra viene visualizzato nel drop-down di Controlli sanitari disponibili.

# Ci sono 6 valori passati a questo script (vedi sotto)

# Lo script restituirà i seguenti valori

1 è che il test ha successo.

# 2 se il test non ha successo sub monitor

{
```

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

NOTA: Monitoraggio personalizzato - Non è possibile usare variabili globali. Usa solo variabili locali - variabili definite all'interno di funzioni

## Certificati SSL

Per usare con successo il bilanciamento del carico Layer 7 con server che usano connessioni criptate tramite SSL, l'ADC deve essere dotato dei certificati SSL usati sui server di destinazione. Questo requisito è in modo che il flusso di dati possa essere decrittografato, esaminato, gestito e poi ricrittografato prima dell'invio al server di destinazione.

I certificati SSL possono variare dai certificati autofirmati che l'ADC può generare ai certificati tradizionali (jolly inclusi) disponibili da provider affidabili. Può anche usare certificati firmati dal dominio che vengono generati da Active Directory.

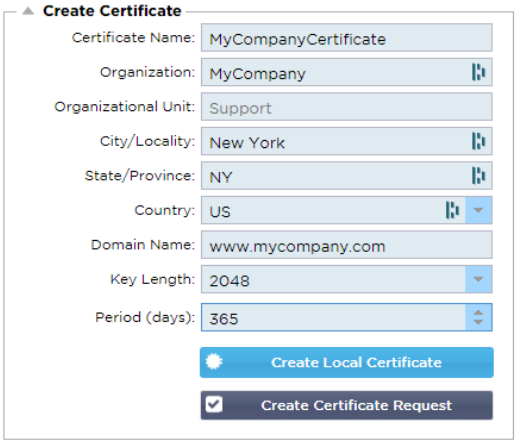
## Cosa fa l'ADC con il Certificato SSL?

L'ADC può eseguire regole di gestione del traffico (flightPATH) a seconda del contenuto dei dati. Questa gestione non può essere eseguita su 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 potrà quindi esaminare ed eseguire le regole di flightPATH. In seguito, i dati verranno nuovamente criptati utilizzando il certificato SSL e inviati al Real Server finale.

## Creare certificato

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

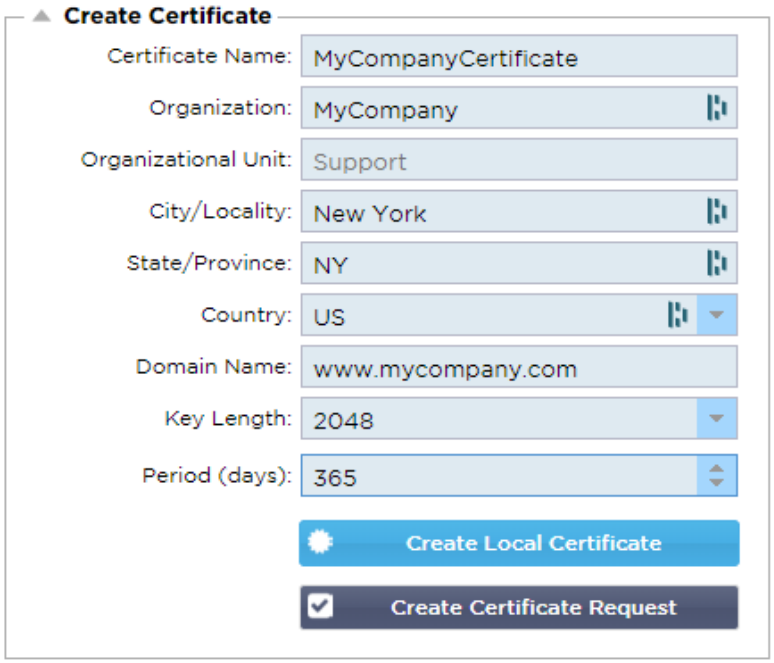
### Come creare un certificato SSL locale




- Compili tutti i dettagli come l'esempio qui sopra
- Clicchi su Crea certificato locale
- Una volta cliccato, può applicare il certificato ad un **SERVIZIO VIRTUALE.**

### Creare una richiesta di certificato (CSR)

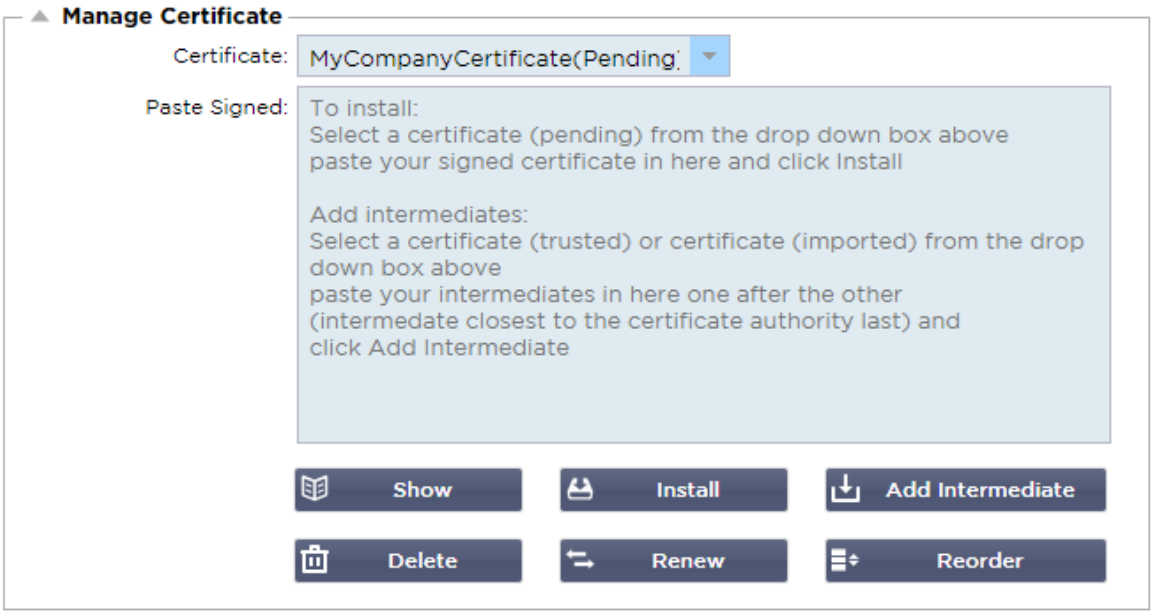
Quando ha bisogno di ottenere un SSL di fiducia globale da un fornitore esterno, dovrà generare una CSR per generare il certificato SSL.




Compili il modulo come mostrato sopra con tutti i dati rilevanti e poi clicchi sul pulsante Certificate Request. Le verrà presentato il popup corrispondente ai dati che ha fornito.

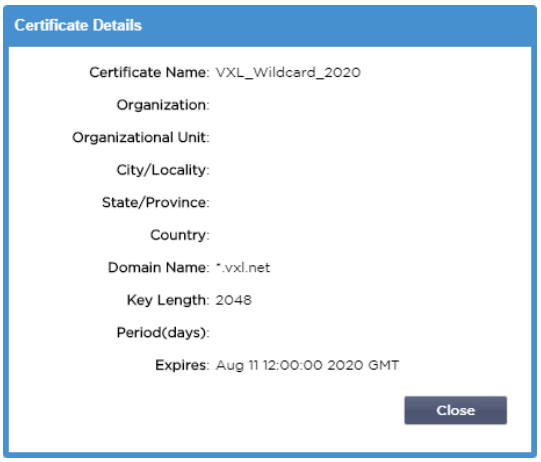

Dovrà tagliare e incollare il contenuto in un file di testo e nominarlo con un'estensione CSR, per esempio, *mycert.csr*. Questo file CSR dovrà poi essere fornito alla sua autorità di certificazione per creare il certificato SSL.

## Gestire il certificato




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

### Mostra

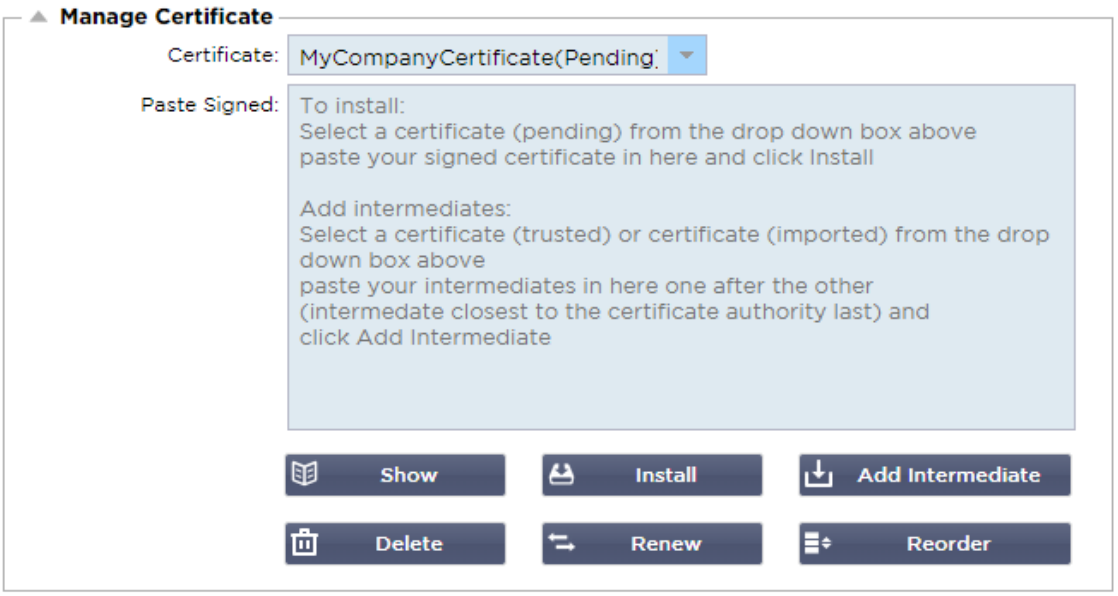



Ci possono essere momenti in cui desidera guardare i dettagli di un certificato SSL installato.

- Selezioni il certificato dal menu a discesa
- Clicchi sul pulsante Mostra
- Verrà presentato il popup mostrato qui sotto con i dettagli del certificato.

### Installazione di un certificato

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




- Selezioni un certificato che ha generato nei passi precedenti. Ci sarà uno stato (Pending) fissato alla voce. Nell'esempio, MyCompanyCertificate è mostrato nell'immagine qui sopra.
- Apra il file del certificato in un editor di testo
- Copia l'intero contenuto del file negli appunti
- Incolli il contenuto del certificato SSL firmato che ha ricevuto dall'autorità di fiducia nel campo contrassegnato da Incolla Firmato.
- Può anche incollare gli Intermedi sotto questo, facendo attenzione a seguire l'ordine corretto:
    1. (TOP) Il suo 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 aggiungerlo poiché esistono sulle macchine client.
       (l'ADC contiene anche un bundle radice per la ricodifica dove agisce come client verso un Real Server)
- Clicchi su Installa
- Una volta installato il certificato, dovrebbe vedere lo stato (Trusted) accanto al suo certificato

Se ha commesso un errore o ha inserito un ordine intermedio sbagliato, selezioni il Certificato (Affidabile) e aggiunga nuovamente i certificati (compreso il certificato firmato) nell'ordine corretto e clicchi su Installa

### Aggiungi intermedio

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

- Evidenzi un certificato (fidato) o un certificato (importato)
- Incolla gli intermedi uno sotto l'altro facendo attenzione che l'intermedio più vicino all'autorità di certificazione sia incollato per ultimo.
- Clicchi su Aggiungi intermedio.

Se commette un errore nell'ordine, può ripetere il processo e aggiungere nuovamente gli intermedi. Questa azione sovrascriverà solo gli intermedi precedenti.

## Cancellare un certificato

Può cancellare un certificato usando il pulsante Elimina. Una volta cancellato, il certificato verrà rimosso completamente dall'ADC e dovrà essere sostituito, quindi riapplicato ai Servizi Virtuali se necessario.

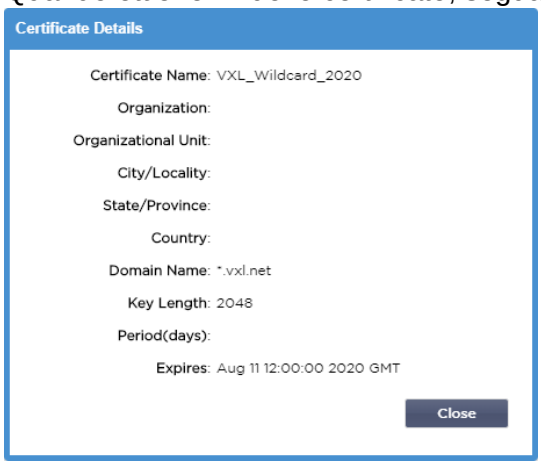
Nota: si assicuri che il certificato non sia collegato ad un VIP operativo prima di cancellarlo.

## Rinnovare un certificato

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

- Selezioni un certificato dall'elenco a discesa; può scegliere qualsiasi certificato con lo stato (Pending), (Trusted) o (Imported)
- Clicchi su Rinnova
- Copi i dettagli della nuova CSR per ottenere un nuovo certificato


- Quando ottiene il nuovo certificato, segua i passi dettagliati in **MOSTRA**




- **CI** possono essere momenti in cui desidera guardare i dettagli di un certificato SSL installato.
- Selezioni il certificato dal menu a discesa
- Clicchi sul pulsante Mostra
- Verrà presentato il popup mostrato qui sotto con 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 aziende 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 sottostante mostra la sottosezione per importare un singolo certificato SSL.


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

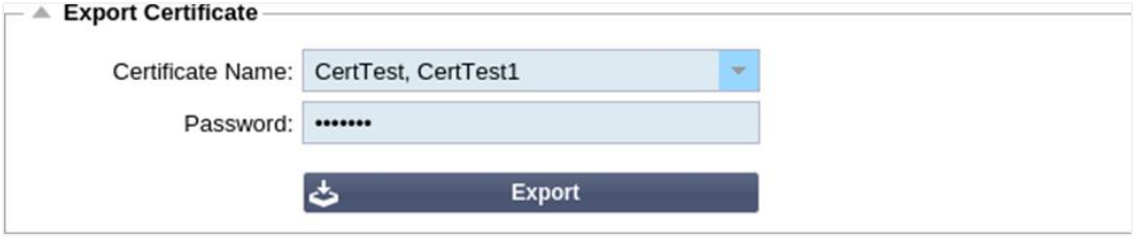
## Importare certificati multipli

Questa sezione le permette di importare un file JNBK che contiene certificati multipli. Un file JNBK viene criptato e prodotto da ADC quando esporta certificati multipli.


- Cerchi il suo file JNBK - può crearne uno esportando più certificati
- Digiti la password che ha usato per creare il file JNBK
- Clicchi su Importa.
- I suoi certificati saranno ora nei relativi menu a discesa SSL all'interno dell'ADC

## Esportare un certificato

Di tanto in tanto potrebbe desiderare di esportare uno dei certificati conservati nell'ADC. L'ADC è stato dotato della capacità di farlo.



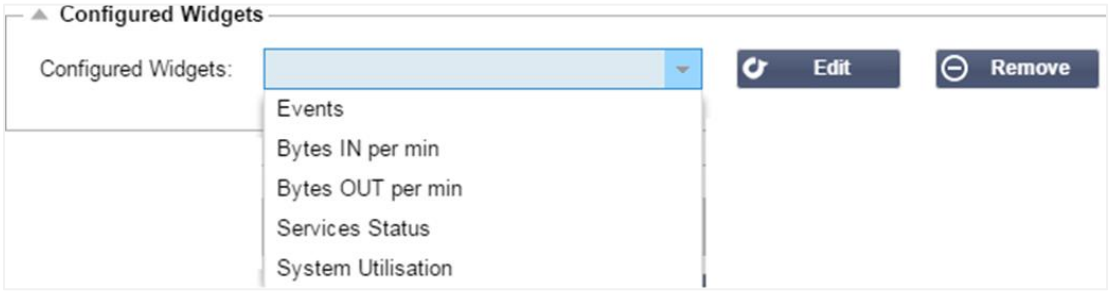
- Clicchi il certificato o i certificati che desidera installare. Può cliccare l'opzione Tutti per selezionare tutti i certificati elencati.
- Digiti una password per proteggere il file esportato. La password deve essere lunga almeno sei caratteri. Si possono usare lettere, numeri e alcuni simboli. I seguenti caratteri **non** sono accettabili: < > " ' ( ) ; \ | \A3 % &
- Clicchi su Esportazione
- Se sta esportando un singolo certificato, il file risultante si chiamerà 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 le permette di configurare vari componenti visivi leggeri visualizzati nella sua dashboard personalizzata.

### Widget configurati

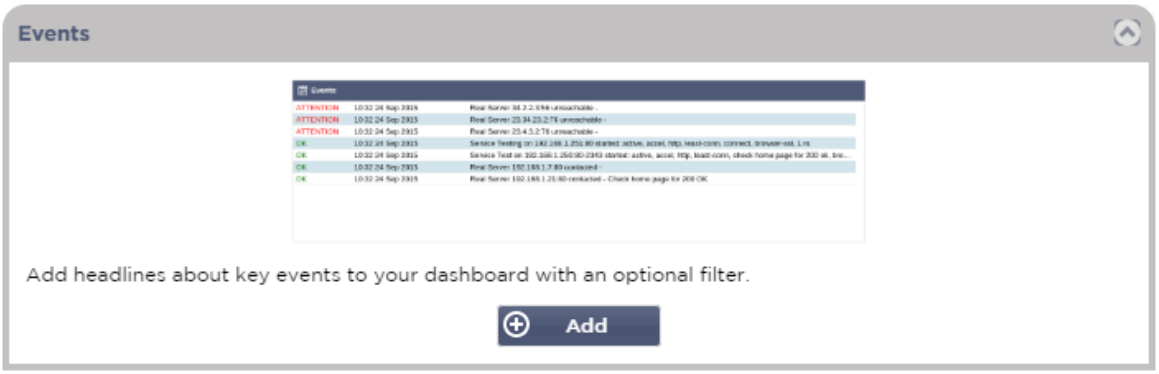



La sezione Configured Widgets le permette di visualizzare, modificare o rimuovere qualsiasi widget creato dalla sezione Available Widgets.

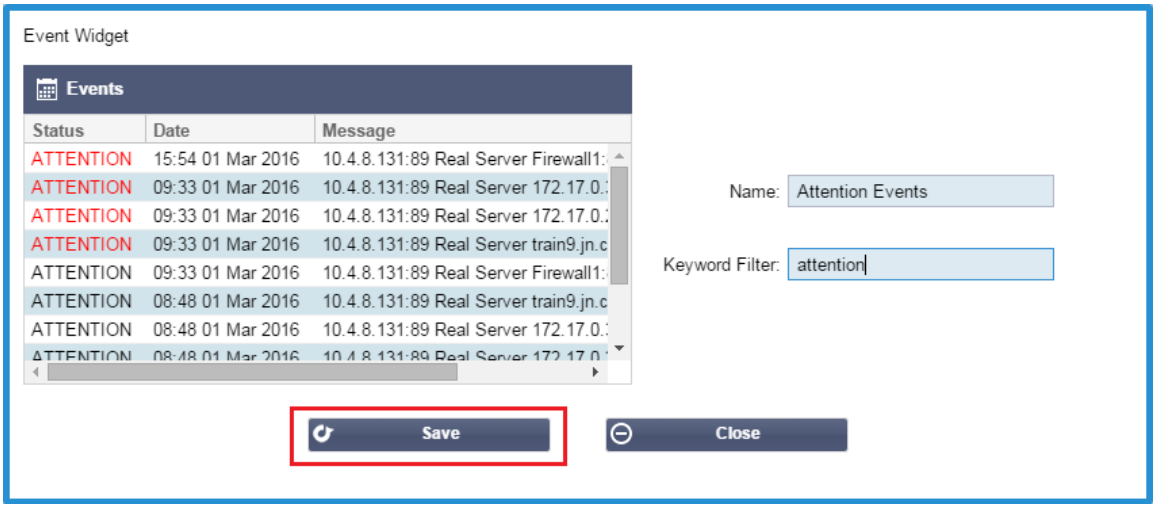
### Widget disponibili

Ci sono cinque diversi widget forniti all'interno dell'ADC e lei può configurarli secondo le sue esigenze.

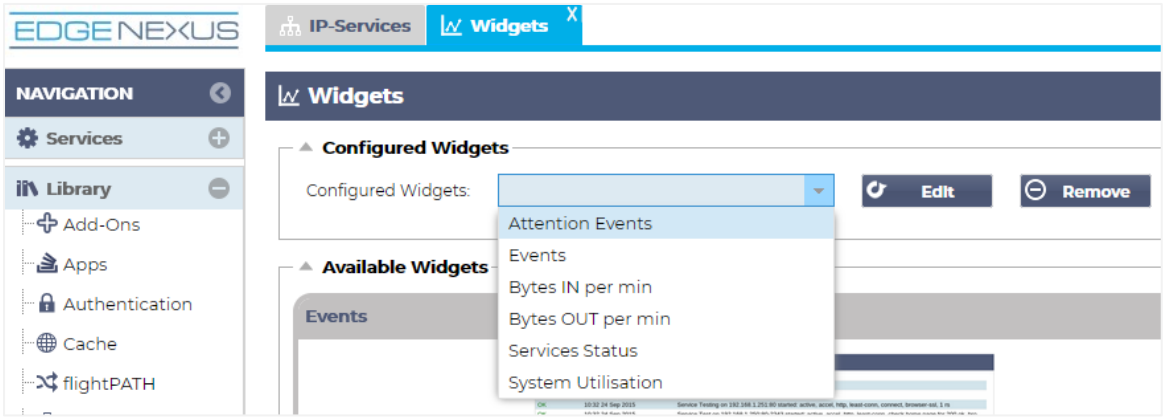
#### *Il widget degli eventi*



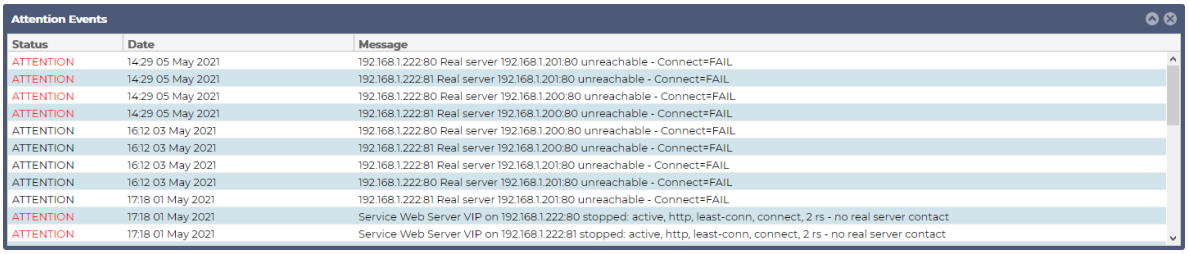

- Per aggiungere un evento al widget Eventi, clicchi sul pulsante Aggiungi.
- Fornisca un nome per il suo evento. Nel nostro esempio abbiamo aggiunto Attention Events come nome dell'evento.
- Aggiungere un filtro per parole chiave. Abbiamo anche aggiunto il valore del filtro di Attenzione




- Clicchi su Salva, poi su Chiudi
- Ora vedrà un widget aggiuntivo chiamato Eventi di Attenzione nel menu a tendina Widget Configurati.

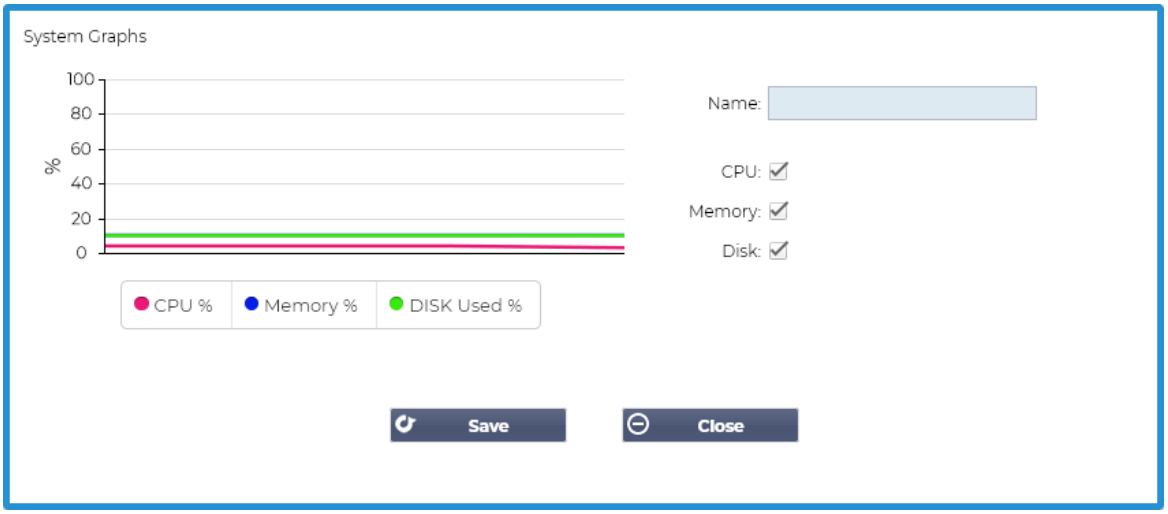



- Può vedere che ora abbiamo aggiunto questo widget nella sezione Vista > Dashboard.
- Selezioni il widget Eventi di Attenzione per visualizzarlo nella Dashboard. Veda sotto.




Può anche mettere in pausa e riavviare il flusso di dati dal vivo cliccando il pulsante Pause Live Data. Inoltre, può tornare alla dashboard predefinita in qualsiasi momento cliccando il pulsante Default Dashboard.

### *Il widget dei grafici di sistema*

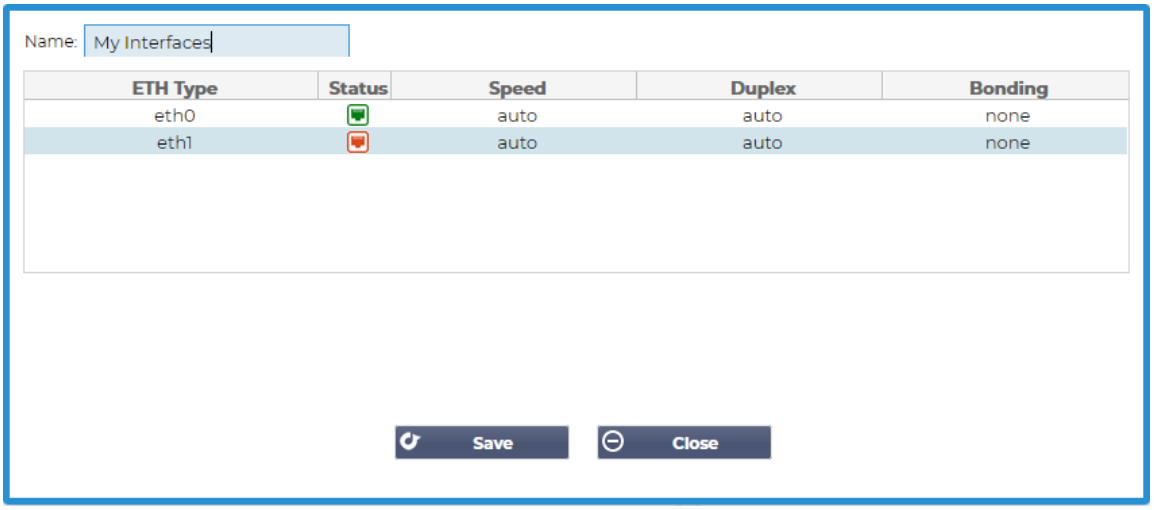



L'ADC ha un widget System Graph configurabile. Cliccando il pulsante Add sul widget, può aggiungere i seguenti grafici di monitoraggio da visualizzare.

- CPU
- MEMORIA
- DISCO

Una volta aggiunti, saranno disponibili individualmente nel menu widget di Dashboard.

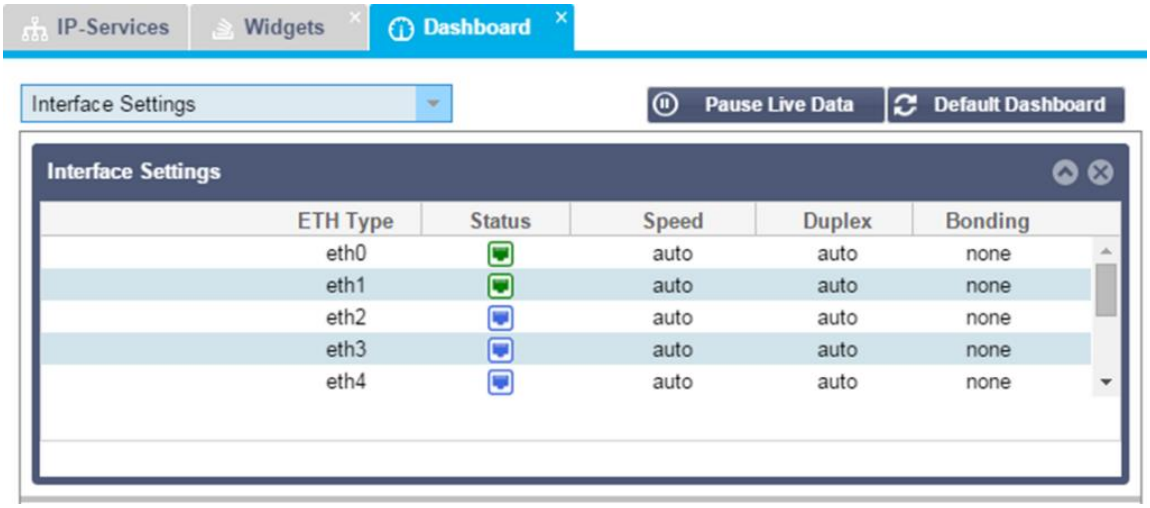
### *Widget dell'interfaccia*




Il widget Interfaccia le 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 da quante interfacce di rete ha definito per l'appliance virtuale o fornito all'interno dell'appliance hardware.

Una volta finito, clicchi sul pulsante Salva e poi su Chiudi.

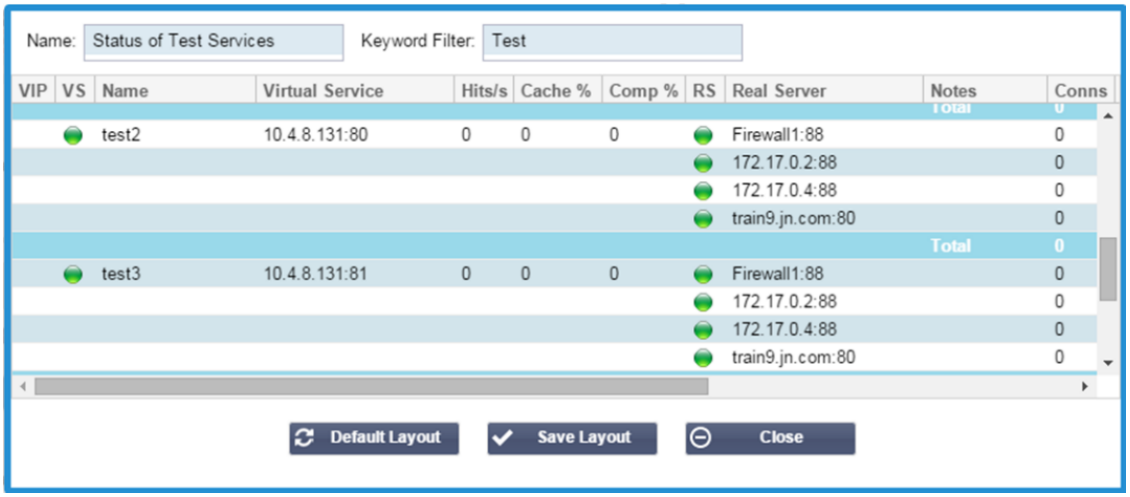
Selezioni il widget che ha appena personalizzato dal menu a discesa dei widget all'interno di Dashboard. Vedrà una schermata come quella sottostante.



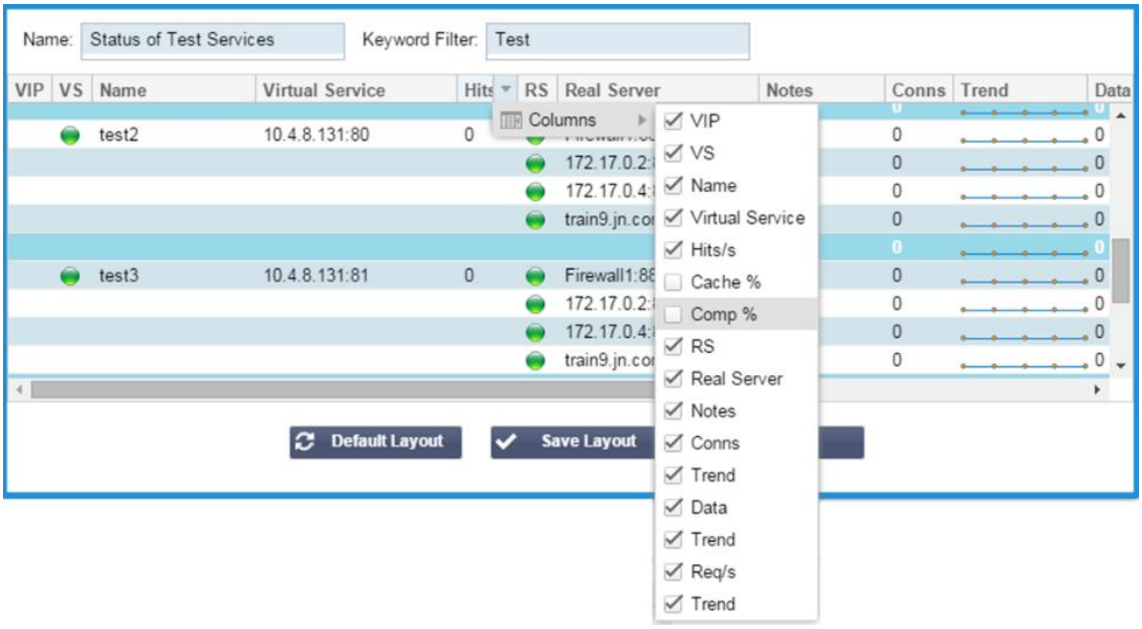

### *Widget di stato*

Il widget Stato le permette di vedere il bilanciamento del carico in azione. Può anche filtrare la vista per mostrare informazioni specifiche.

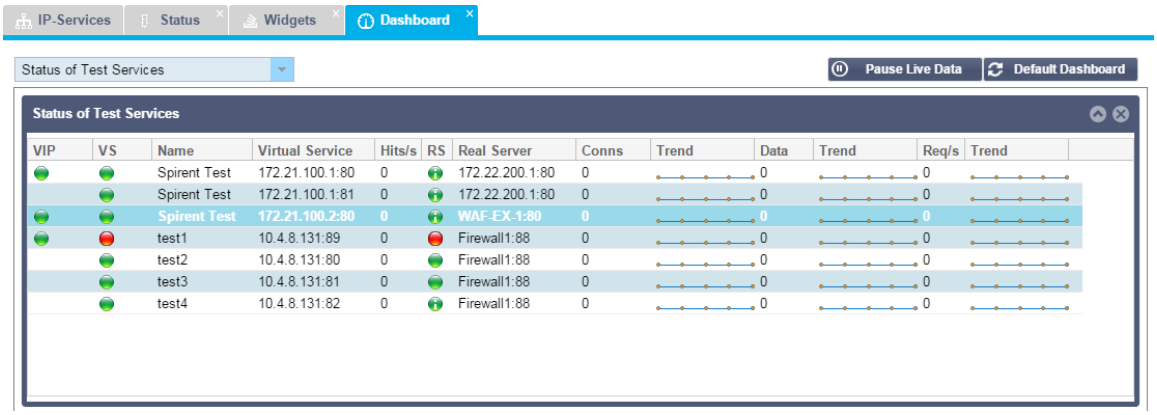
- Clicchi su Aggiungi.




- Inserisca un nome per il servizio che vuole monitorare
- Può anche scegliere quali colonne visualizzare nel widget.

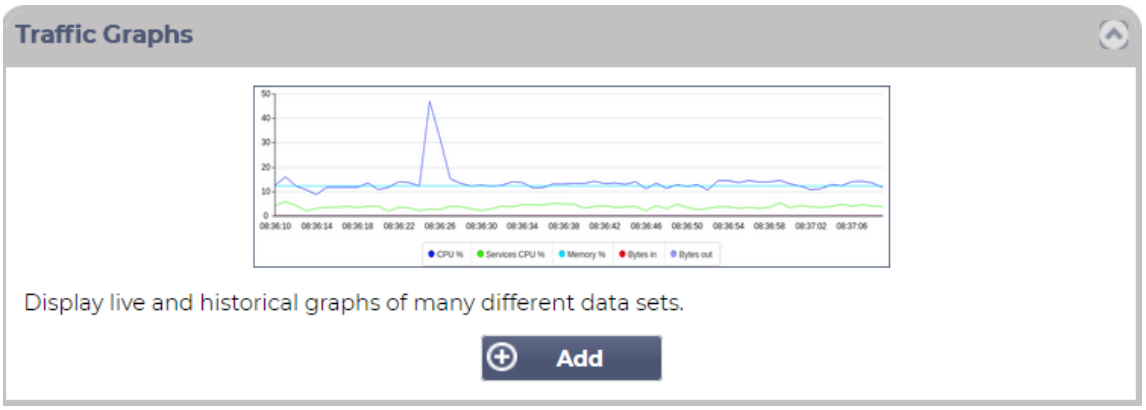



- Una volta soddisfatto, clicchi su Salva, seguito da Chiudi.
- Il widget di stato scelto sarà disponibile nella sezione Dashboard.




## *Widget per la grafica del traffico*

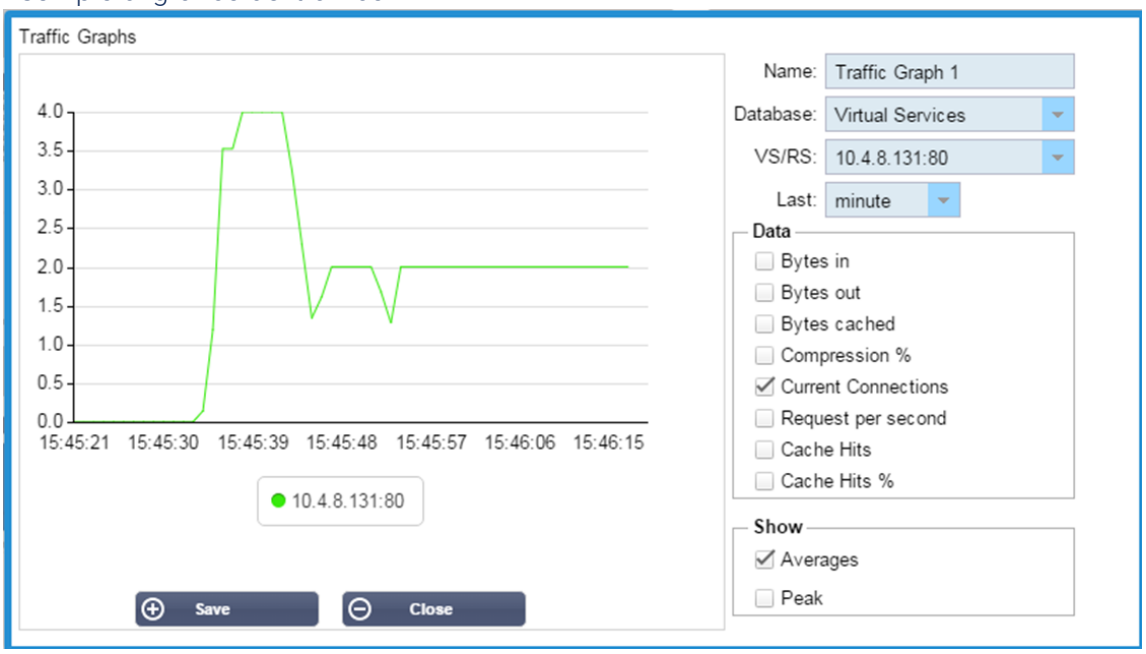
Questo widget può essere configurato per mostrare i dati di traffico attuali e storici per Virtual Services e Real Servers. Inoltre, può vedere i dati complessivi attuali e storici per il traffico globale




- Clicchi il pulsante Aggiungi
- Dia un nome al suo widget.
- Scelga un database da Virtual Services, Real Servers o System.
- Se sceglie Servizi virtuali, può selezionare un servizio virtuale dal menu a tendina VS/RS.

- Scelga 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 da ogni ora per le 24 ore precedenti
  - Settimana - dati aggregati da ogni giorno durante i sette giorni precedenti
  - Mese - dati aggregati di ogni settimana per gli ultimi sette giorni
  - Anno - dati aggregati da ogni mese durante i 12 mesi precedenti
- Scelga i Dati disponibili a seconda della banca dati che ha scelto
  - Banca dati dei servizi virtuali
  - Bytes in
  - Bytes fuori
  - Bytes in cache
  - Compressione %
  - Connessioni attuali
  - Richieste al secondo
  - Cache Hits
  - Cache Hits %
- Server reali
  - Bytes in
  - Bytes fuori
  - Connessioni attuali
  - Richiesta al secondo
  - Tempo di risposta
- Sistema
  - CPU
  - Servizi CPU
  - Memoria
  - Disco Libero %
  - Bytes in
  - Bytes fuori
- Scelga di mostrare i valori medi o di picco
- Una volta scelte tutte le opzioni, clicchi su Salva e chiudi

## Esempio di grafico del traffico



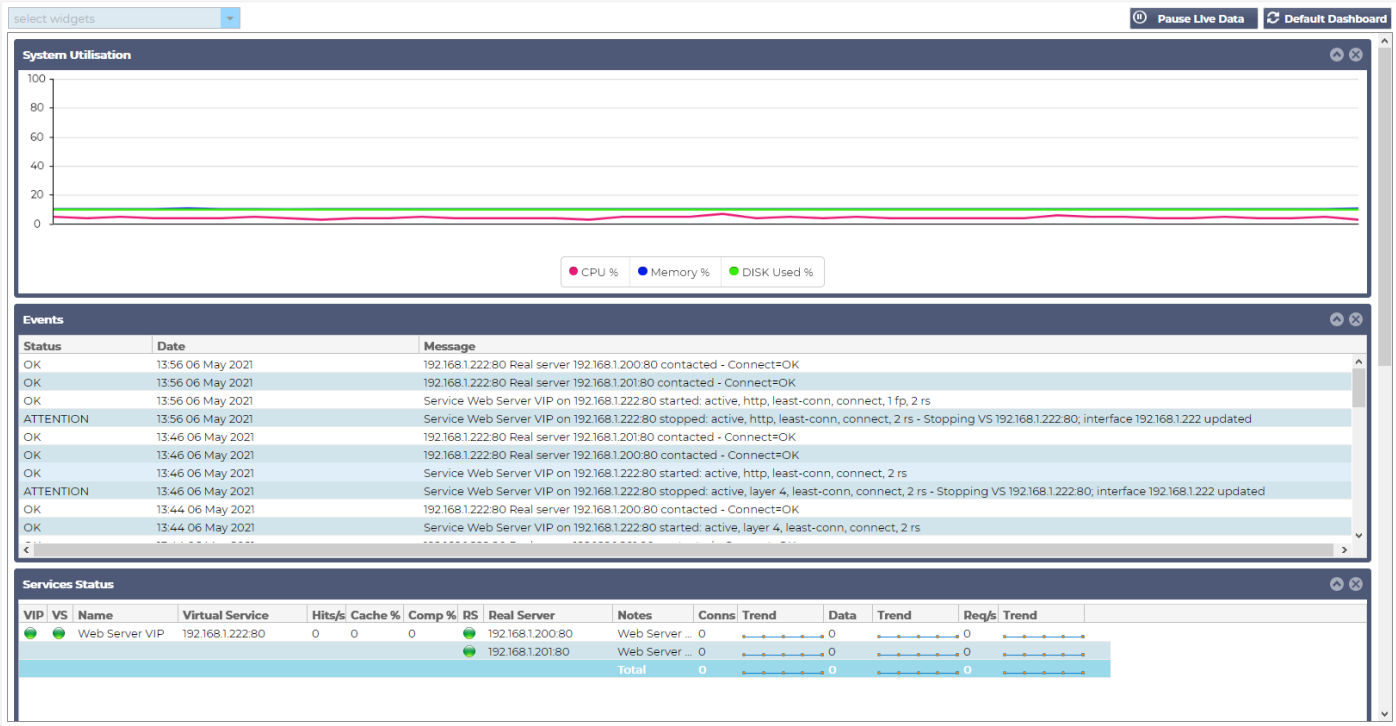
Ora può aggiungere il suo widget Traffic Graph a View > Dashboard.

# Vedere

## Cruscotto

Come tutte le interfacce di gestione dei sistemi IT, ci sono molte volte in cui ha bisogno di guardare le metriche di performance e i dati che l'ADC sta gestendo. Le forniamo una dashboard personalizzabile per farlo in modo facile e significativo.

La Dashboard è raggiungibile usando il segmento View del pannello del navigatore. Quando viene selezionata, mostra diversi widget predefiniti e le permette di scegliere quelli personalizzati che ha definito.



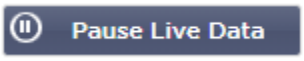

### Uso del cruscotto

Ci sono quattro elementi nella Dashboard U: il Menu Widgets, il Pulsante Pausa/Play e il pulsante Default Dashboard.

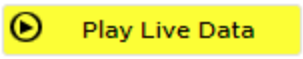
#### Il menu dei widget

Il menu Widget situato in alto a sinistra della dashboard le permette di selezionare ed aggiungere qualsiasi widget standard o personalizzato da lei definito. Per utilizzarlo, selezioni il widget dal menu a tendina.

#### Pulsante Pause Live Data




Questo pulsante le permette di selezionare se l'ADC deve aggiornare la dashboard in tempo reale. Una volta messo in pausa, nessun widget del cruscotto verrà aggiornato, permettendole di esaminare il contenuto a suo piacimento. Il pulsante cambia stato e mostra Play Live Data una volta iniziata la pausa.




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

## Pulsante predefinito del cruscotto


Può capitare che desideri ripristinare il layout di Dashboard ai valori predefiniti. In tal caso, prema il pulsante Default Dashboard. Una volta cliccato, tutte le modifiche apportate alla Dashboard andranno perse.

## Ridimensionare, minimizzare, riordinare e rimuovere i widget


### *Ridimensionare un widget*

Può ridimensionare un widget molto facilmente. Clicchi e tenga premuto sulla barra del titolo del widget e lo trascini sul lato sinistro o destro dell'area Dashboard. Vedrà un rettangolo tratteggiato che rappresenta la nuova dimensione del widget. Faccia cadere il widget nel rettangolo e lasci andare il pulsante del mouse. Se desidera far cadere un widget ridimensionato accanto ad un widget ridimensionato in precedenza, vedrà apparire il rettangolo adiacente al widget che vuole far cadere accanto.

### *Minimizzare un widget*

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

### *Spostamento dell'ordine dei widget*

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

### *Rimozione di un widget*

Può rimuoverne uno cliccando l'⊗icona nella barra del titolo del widget.

# Storia


L'opzione Storia, selezionabile dal navigatore, permette all'amministratore di esaminare la performance storica dell'ADC. Si possono generare viste storiche per Servizi Virtuali, Real Server e Sistema.

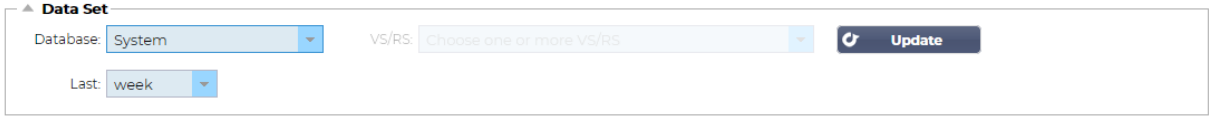
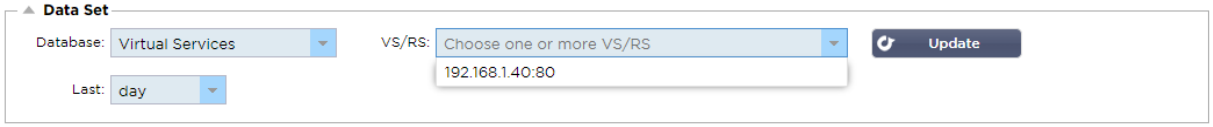
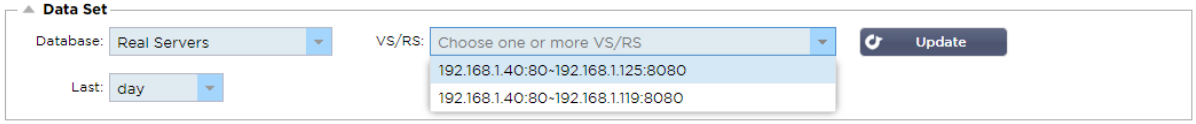
Le permette anche di vedere il bilanciamento del carico in azione e aiuta a cogliere eventuali errori o schemi su cui indagare. Noti che deve abilitare la registrazione storica in Sistema > Cronologia per utilizzare questa funzione.

## Visualizzazione di dati grafici

### Set di dati

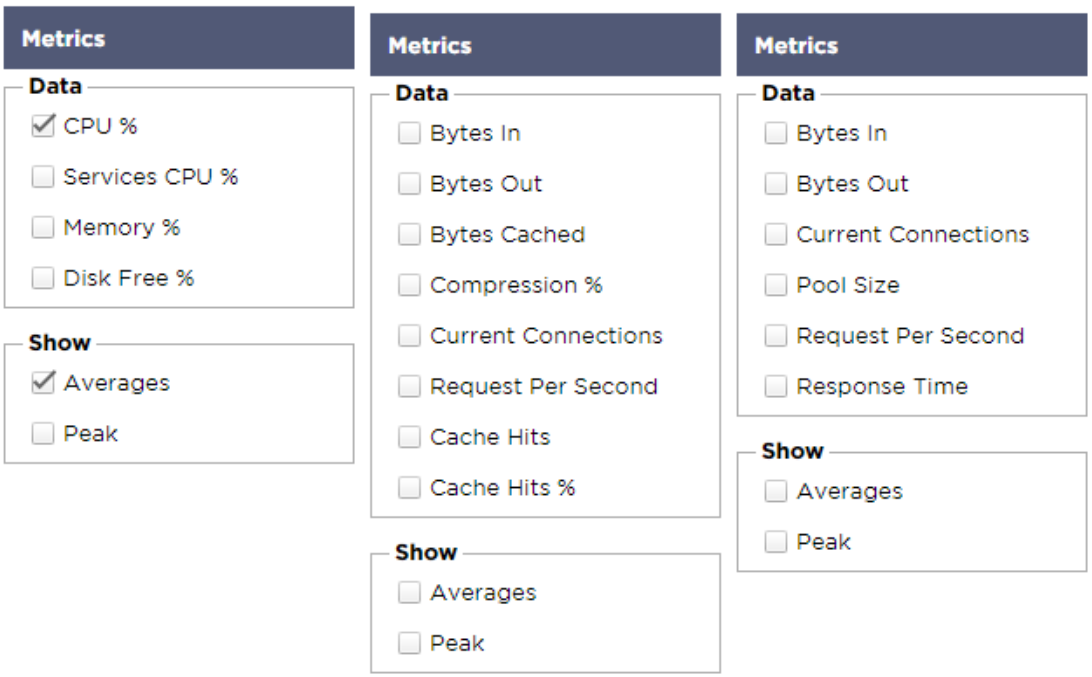
Per visualizzare i dati storici in formato grafico, proceda come segue:

Il primo passo è scegliere il database e il periodo relativo alle informazioni che desidera visualizzare. Il periodo che può selezionare dal menu a tendina Ultimo è Minuto, Ora, Giorno, Settimana, Mese e Anno.

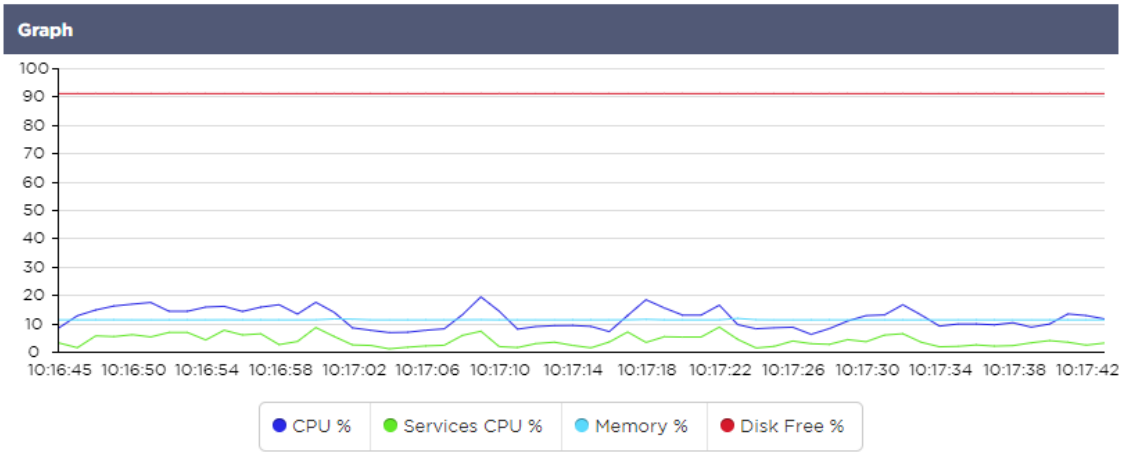
| Database | Descrizione |
|---|---|
| Sistema | Selezionando questo database potrà vedere la CPU, la memoria e lo spazio su disco nel tempo<br>  |
| Servizi virtuali | Selezionando questo database potrà scegliere tutti i servizi virtuali presenti nel database da quando ha iniziato a registrare i dati. Vedrà un elenco di servizi virtuali da cui potrà selezionarne uno.<br>  |
| Servizi reali | Selezionando questo database potrà scegliere tutti i Real Server presenti nel database da quando ha iniziato a registrare i dati. Vedrà un elenco di Real Server da cui potrà selezionarne uno.<br>  |

### Metriche

Una volta selezionato il Data Set che utilizzerà, è il momento di scegliere le metriche che desidera visualizzare. L'immagine sottostante 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).



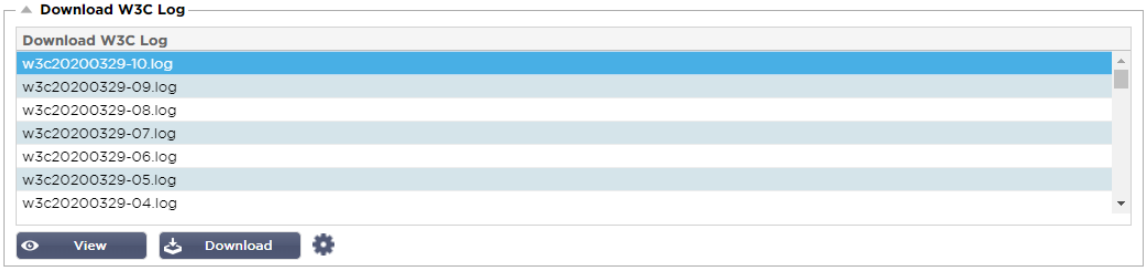

### Grafico di esempio




## Registri

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

## Scarichi i log del W3C




Il log W3C si abilita dalla sezione System > Logging. Un log W3C è un registro di accesso per server web in cui vengono generati file di testo contenenti dati su ogni richiesta di accesso, inclusi 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 log registrata.

Dalla sezione W3C può selezionare il registro di cui ha bisogno e poi visualizzarlo o scaricarlo.

### Visualizza Pulsante

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

### Scarica il pulsante

Questo pulsante le permette di scaricare il registro nella sua memoria locale per visualizzarlo in seguito.

### L'icona dell'ingranaggio

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

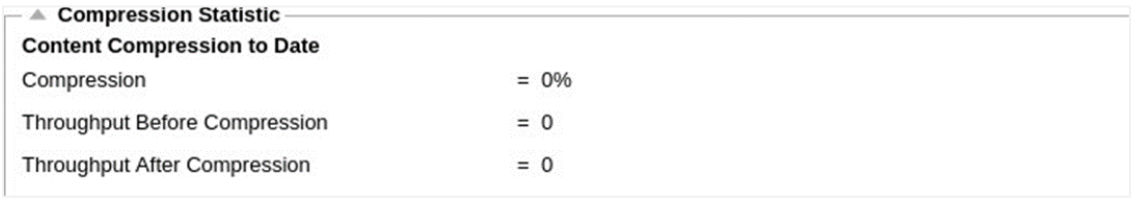
# Statistiche

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

## Compressione

L'intero scopo dell'ADC è 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 del contenuto fino ad oggi




I dati mostrati in questa sezione dettagliano il livello di compressione raggiunto dall'ADC su contenuti comprimibili. 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 dipende da quante immagini precompresse sono contenute nei suoi 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 che entrano ed escono dall'ADC. L'unità di misura cambia al crescere delle dimensioni 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 di hit e transazioni che passano attraverso l'ADC. Quindi cosa significano hit e connessioni?

- Un Hit è definito come una transazione di livello 7. Tipicamente usata per i server web, 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 mostra il numero attuale di hit al secondo.

### Connessioni totali

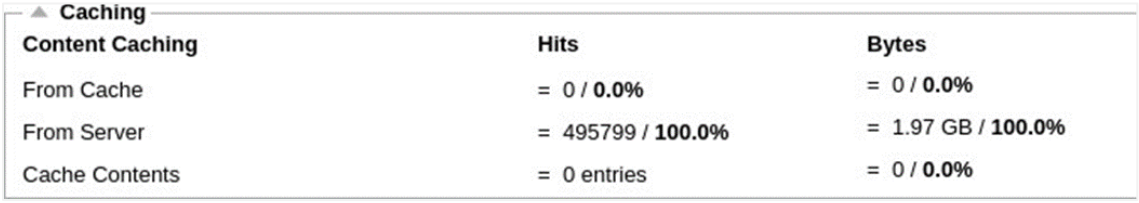
Il valore Total Connections rappresenta il numero cumulativo di connessioni TCP dall'ultimo reset. Il numero nella seconda colonna indica le connessioni TCP fatte al secondo all'ADC. Il numero nella colonna di destra è il numero di connessioni TCP al secondo fatte ai Real Server. Esempio 6/8 connessioni/sec. Nell'esempio mostrato abbiamo 6 connessioni TCP al secondo al Servizio Virtuale e 6 connessioni TCP al secondo ai Real Server.

### Connessioni di picco

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

## Caching

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



**Caching**

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

### Da Cache

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

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

### Dal server

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

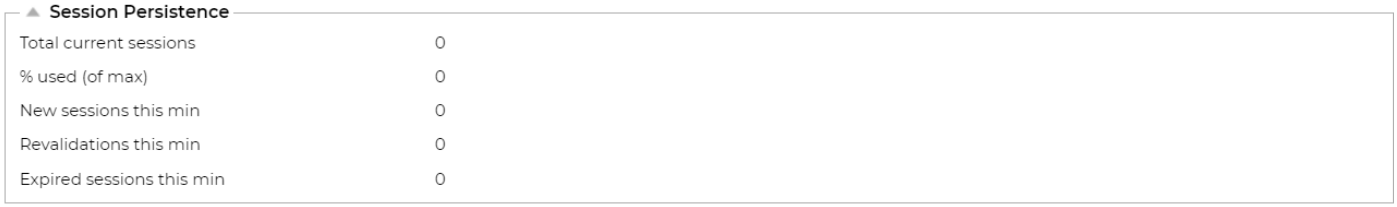
Bytes: La seconda colonna dà la quantità totale di dati in Kilobyte serviti dai Real Server. Viene fornita anche una percentuale dei dati totali.

### 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 fornita anche una percentuale della dimensione massima della cache.

## Persistenza della sessione



**Session Persistence**

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

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 uso c'è dello spazio totale permesso per le informazioni di sessione |
| Nuova sessione questo min | Questo mostra, nell'ultimo minuto, quante nuove sessioni di persistenza sono state aggiunte |
| Rivaluti 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 per mancanza di ulteriore traffico entro il timeout |

### Hardware

Sia che stia usando l'ADC in un ambiente virtuale o all'interno dell'hardware, questa sezione le fornirà informazioni preziose sulla performance 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 usata da ADC. È naturale che questo fluttui.

## Stato

La pagina View > Status mostra il traffico live che attraversa l'ADC per i Servizi virtuali che ha definito. Mostra anche il numero di connessioni e dati per ogni Real Server in modo che lei possa 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 sono irraggiungibili o nessun server reale è abilitato |
| ● | Trovare lo stato |
| ● | IP virtuali non licenziati o licenziati superati |

### Colonna 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". |
| ● | Servizio Necessita 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 sono irraggiungibili o nessun server reale è abilitato |
| ● | Trovare lo stato |
| ● | IP virtuali non licenziati o licenziati superati |

### Nome

Il nome del servizio virtuale

### Servizio Virtuale (VIP)

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

### Hit/Sec

Layer 7 transazioni al secondo sul lato client.

### Cache%

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

### Compressione

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

### Stato RS (Server remoto)

La tabella sottostante 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 licenziati o licenziati 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 a ciascun Real Server le permette di vedere il bilanciamento del carico in azione. Molto utile per verificare che la sua 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 a ciascun Real Server.

# Sistema

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

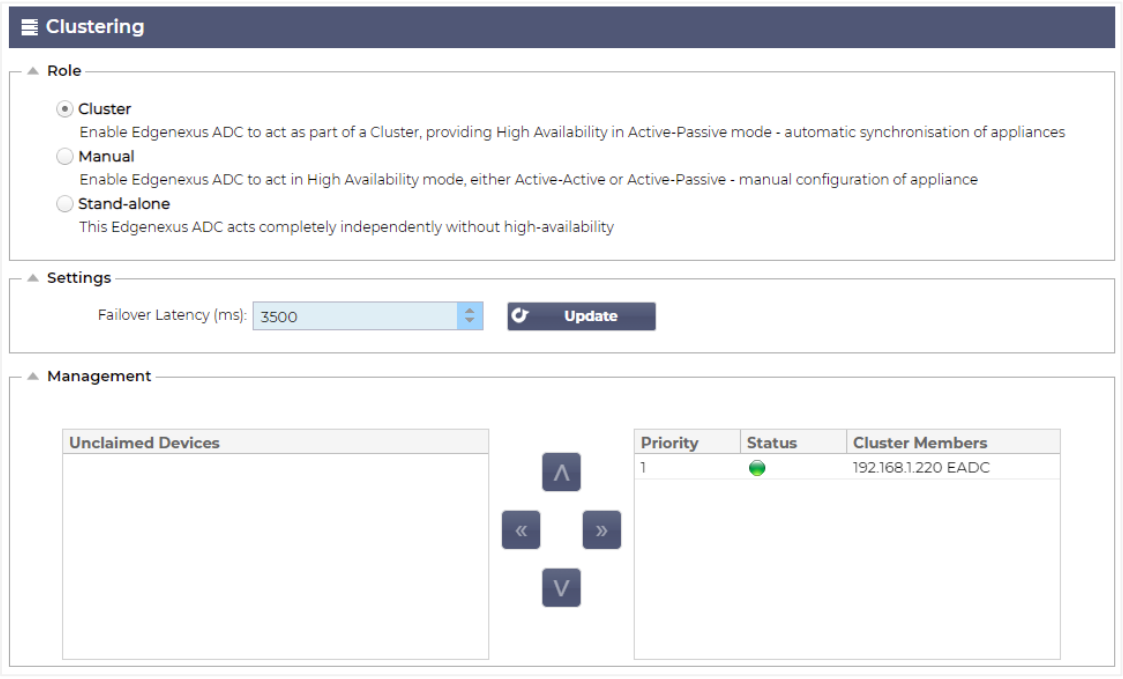
## Clustering

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

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

### Nota importante

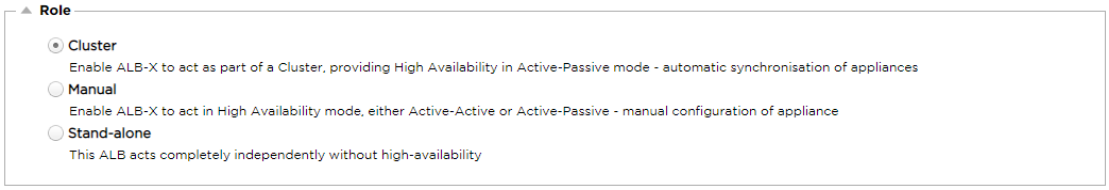
- Non c'è bisogno di un cavo dedicato tra la coppia ADC per mantenere un heartbeat ad alta disponibilità.
- L'heartbeat avviene sulla stessa rete del servizio virtuale che richiede un'alta disponibilità.
- Non c'è uno stateful fail-over tra gli apparecchi ADC.
- Quando l'alta disponibilità è abilitata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




## Ruolo

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

## Cluster



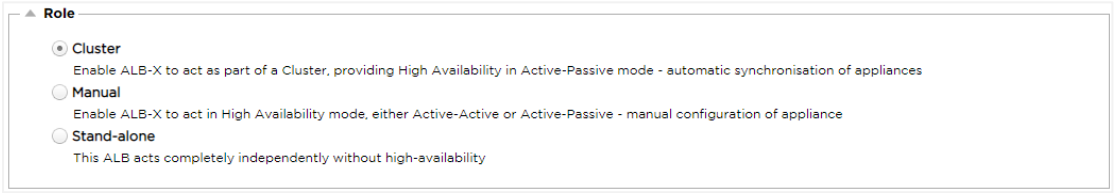

- Per default, un nuovo ADC si accenderà usando il ruolo Cluster. In questo ruolo, ogni membro del cluster avrà la stessa "configurazione di lavoro" e quindi solo un ADC nel cluster sarà attivo in qualsiasi momento.
- Per "configurazione funzionante" si intendono tutti i parametri di configurazione, 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.
- Può modificare qualsiasi ADC nel Cluster e le modifiche saranno sincronizzate a tutti i membri del Cluster.
- Quando rimuove un ADC dal cluster, tutti i servizi virtuali saranno cancellati da quell'ADC.
- Non può rimuovere l'ultimo membro del cluster in Dispositivi non reclamati. Per rimuovere l'ultimo membro, cambi il ruolo in Manuale 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 elettrodomestici
    - Sezione rete

### *Fallimento del proprietario del cluster*

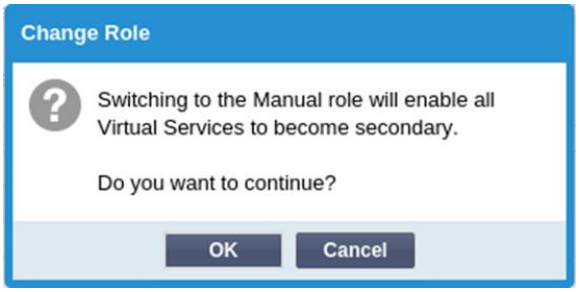
- Quando il proprietario di un cluster fallisce, uno dei membri rimanenti subentra automaticamente e continua a bilanciare il traffico.
- Quando il proprietario del cluster ritorna, riprende il traffico di bilanciamento del carico e assume il ruolo di proprietario.
- Supponiamo che il Proprietario sia fallito e che un membro abbia assunto il bilanciamento del carico. Se vuole che quel membro che ha preso il controllo del traffico di bilanciamento del carico diventi il nuovo proprietario, evidenzi il membro e clicchi sulla freccia in alto per spostarlo nella posizione Priorità 1.
- Se modifica uno dei membri del cluster rimanenti e il proprietario è giù, il membro modificato si promuove automaticamente al proprietario senza perdita di traffico

### *Cambiare ruolo da ruolo Cluster a ruolo Manuale*

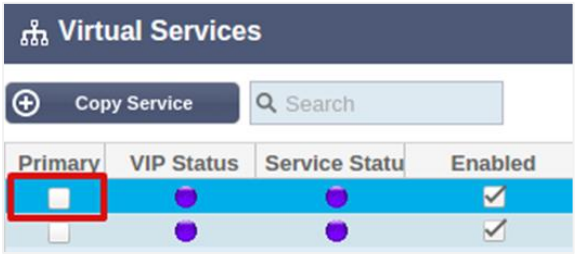
- Se vuole cambiare il ruolo da Cluster a Manuale, clicchi sul pulsante radio accanto all'opzione ruolo Manuale




- Dopo aver cliccato sul pulsante radio, vedrà il seguente messaggio:



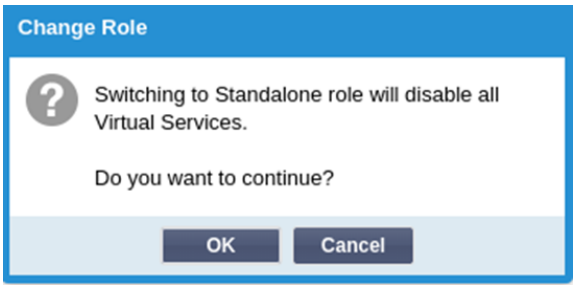

- Clicchi il pulsante OK
- Controlli la sezione Servizi Virtuali. Troverà che la colonna Primary ora mostra una casella non spuntata.




- È una caratteristica di sicurezza e significa che se ha un altro ADC con gli stessi Servizi Virtuali, allora non ci sarà interruzione del flusso di traffico.

### *Cambiare ruolo da Cluster a Stand-alone*

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




- Clicchi su OK per cambiare i ruoli.
- Controlli i suoi Servizi Virtuali. Vedrà che la colonna Primary cambia nome in Stand-alone
- Vedrà anche che tutti i Servizi Virtuali sono disabilitati (non spuntati) per motivi di sicurezza.
- Una volta che è sicuro che nessun altro ADC sulla stessa rete ha duplicato i Servizi Virtuali, può abilitare ciascuno di essi a turno.

### *Ruolo manuale*

Un ADC nel ruolo Manuale lavorerà con altri ADC nel ruolo Manuale 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, si può creare un jetPACK da un ADC e inviarlo all'altro.

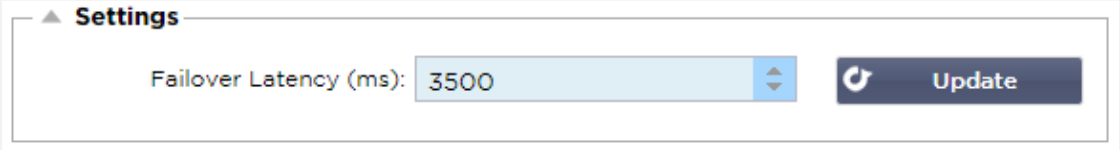
- Per rendere un indirizzo IP Virtuale "Attivo", spunti la casella di controllo nella colonna primaria (pagina Servizi IP).

- Per rendere un indirizzo IP Virtuale "Passivo", lasci 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 nello stato Verde e connessi. Deve assicurarsi che tutti i Servizi Virtuali abbiano indirizzi IP unici, o ci sarà uno scontro nella sua rete.

## Impostazioni

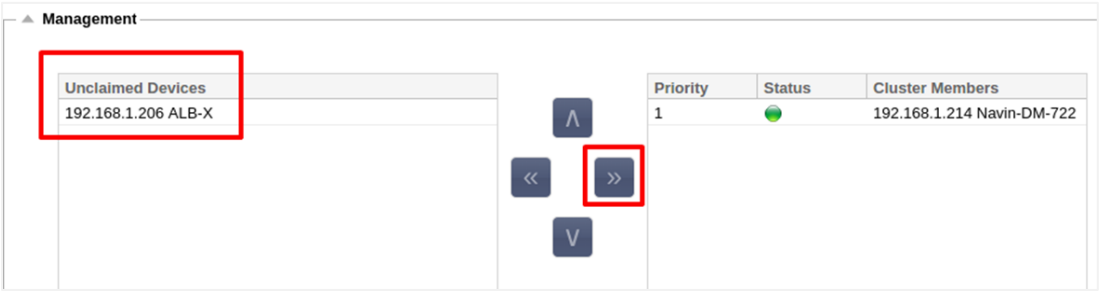



Nella sezione Impostazioni, può impostare la Failover Latency in millisecondi, il tempo che un ADC passivo aspetterà prima di prendere in consegna i servizi virtuali dopo che l'ADC attivo è fallito.

Raccomandiamo di impostarlo a 10000ms o 10 secondi, ma può diminuire o aumentare questo valore per adattarlo alla sua rete e alle sue esigenze. I valori accettabili sono compresi tra 1500ms e 20000ms. Se sperimenta instabilità nel cluster ad una latenza inferiore, dovrebbe aumentare questo valore.

## Gestione

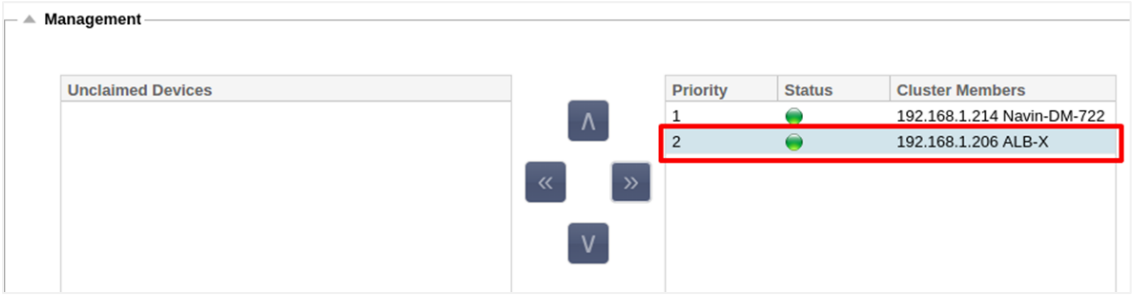
In questa sezione può aggiungere e rimuovere membri del cluster e anche cambiare la priorità di un ADC nel cluster. La sezione consiste di due pannelli e una serie di tasti freccia nel mezzo. L'area a sinistra è quella dei Dispositivi non reclamati, mentre l'area più a destra è il Cluster stesso.




### Aggiungere un ADC al cluster

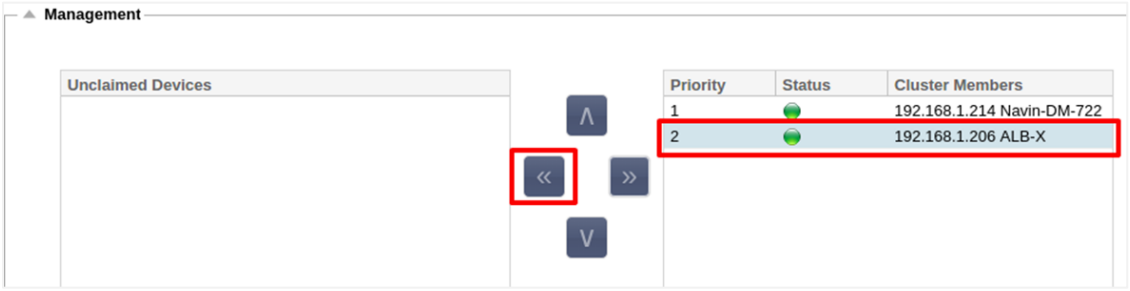
- Prima di aggiungere l'ADC al cluster, deve assicurarsi che tutti gli apparecchi ADC siano stati dotati di un nome unico impostato nella sezione Sistema > Rete.
- Dovrebbe vedere l'ADC come Priorità 1 con Stato verde e il suo nome nella colonna Membri del cluster nella sezione di gestione. Questo ADC 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.
- Evidenzi l'ADC dalla finestra Unclaimed Devices e clicchi sul pulsante freccia destra.
- Ora vedrà il seguente messaggio:


- Clicchi su OK per promuovere l'ADC al cluster.
- Il suo ADC dovrebbe ora apparire come Priorità 2 nell'elenco dei membri del cluster.




## Rimozione di un membro del cluster

- Evidenzi il membro del cluster che vuole rimuovere dal cluster.
- Clicchi il pulsante con la freccia sinistra.




- Le verrà presentata una richiesta di conferma.
- Clicchi su OK per confermare.
- Il suo ADC verrà rimosso e sarà mostrato sul lato Dispositivi non reclamati.

## Cambiare la priorità di un ADC

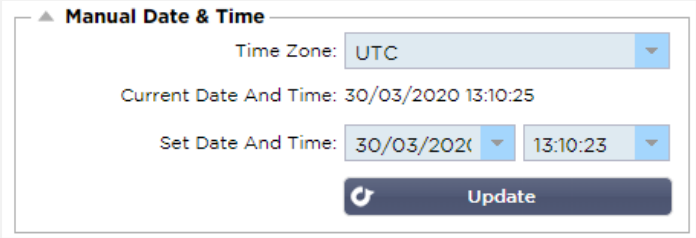
Ci possono essere momenti in cui desidera cambiare la priorità di un ADC nella lista dei membri.

- 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 riceve 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 la freccia su fino a quando è in cima all'elenco

## Data e ora

La sezione data e ora permette di impostare le caratteristiche di data/ora dell'ADC, incluso 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 da lei impostato in questo campo rappresenta il fuso orario in cui si trova l'ADC.

- Clicchi sulla casella a discesa per il fuso orario e inizi a digitare la sua posizione.
  Per esempio Londra
- Quando inizia a digitare, l'ADC visualizzerà automaticamente le posizioni contenenti la lettera L.
- Continui a digitare 'Lon,' e così via - le località elencate si restringeranno a quelle che contengono 'Lon'. ’
- Se si trova, diciamo, a Londra, allora scelga Europa/Londra per impostare la sua posizione

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

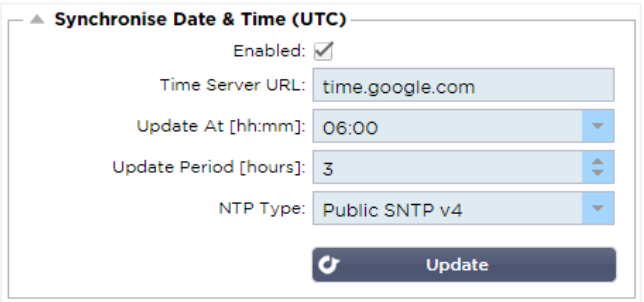
#### Impostare data e ora

Questa impostazione rappresenta la data e l'ora attuali.

- Scelga la data corretta dal primo menù a tendina o,
  in alternativa, può digitare la data nel seguente formato GG/MM/AAAA
- Aggiunga l'ora nel seguente formato hh: mm: ss, per esempio, 06:00:10 per 6 am e 10 secondi.
- Una volta che l'ha inserito correttamente, clicchi su Update per applicare.
- Dovrebbe quindi vedere la nuova Data e Ora in caratteri in grassetto.

### Sincronizzi data e ora (UTC)

Può usare i server NTP per sincronizzare accuratamente data e ora. I server NTP si trovano a livello globale e lei può anche avere un suo server NTP interno quando la sua infrastruttura ha limitazioni sull'accesso esterno.




#### URL del Time Server

Inserisca un indirizzo IP valido o un nome di dominio completamente qualificato (FQDN) per il server NTP. Se il server è un server situato globalmente su Internet, raccomandiamo di usare un FQDN.

### Aggiornamento alle [hh:mm]

Selezioni l'ora programmata alla quale vuole che l'ADC si sincronizzi con il server NTP.

### Periodo di aggiornamento [ore]:

Selezioni la frequenza con cui desidera che la sincronizzazione avvenga.

### Tipo NTP:

- Public SNTP V4 - Questo è il metodo attuale 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**

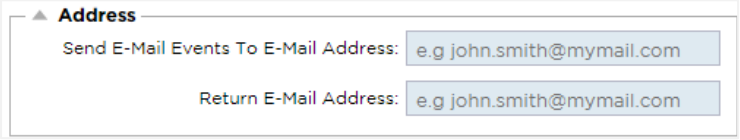
Nota: La preghiamo di notare che la sincronizzazione è solo in UTC. Se desidera impostare un'ora locale, questo può essere fatto solo manualmente. Questa limitazione verrà cambiata nelle versioni successive per consentire la possibilità di selezionare un fuso orario.

## 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 le permette di configurare una connessione al server email e inviare notifiche agli amministratori di sistema. La pagina è organizzata nelle sezioni seguenti.

### Indirizzo




### Inviare ad eventi e-mail a indirizzi e-mail

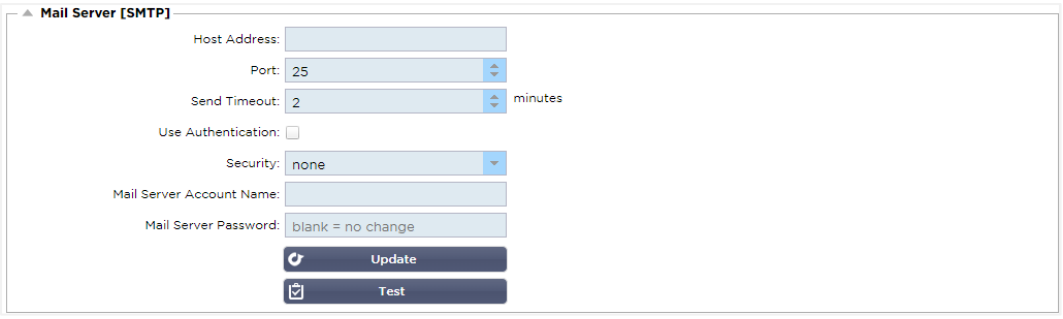
Aggiunga un indirizzo email valido a cui inviare avvisi, notifiche ed eventi. Esempio support@domain.com. Può anche aggiungere più indirizzi email usando un separatore a virgola.

### Indirizzo e-mail di ritorno:

Aggiunga un indirizzo email che apparirà nella posta in arrivo. Esempio adc@domain.com.

### Server di posta (SMTP)

In questa sezione deve aggiungere i dettagli del server SMTP da usare per inviare le email. Si assicuri che l'indirizzo email che usa per l'invio sia autorizzato a farlo.




### Indirizzo dell'host

Aggiunga l'indirizzo IP del suo server SMTP.

### Porto

Aggiunga la porta del suo server SMTP. La porta predefinita per SMTP è 25 o 587 se usa SSL.

### Timeout di invio

Aggiunga un timeout SMTP. Il default è impostato a 2 minuti.

### Usi l'autenticazione

Spunti la casella se il suo server SMTP richiede autenticazione.

### Sicurezza

- Nessuno
- L'impostazione predefinita è nessuno.
- SSL - Usi questa impostazione se il suo server SMTP richiede l'autenticazione Secure Sockets Layer.
- TLS - Usi questa impostazione se il suo server SMTP richiede l'autenticazione Transport Layer Security.

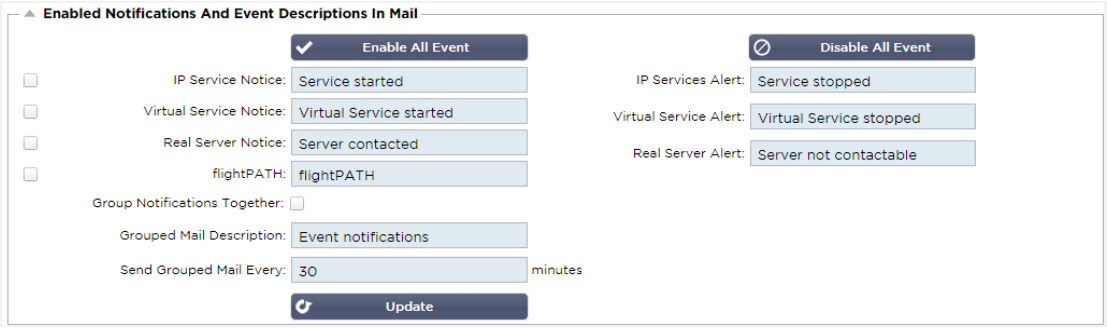
### Nome dell'account del server principale

Aggiunga il nome utente richiesto per l'autenticazione.

### Password del server di posta

Aggiunga 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. Può 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 la informerà 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 Port è connesso o non è contattabile, l'ADC invia un avviso al Real Server.

### flightPATH

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

### Notifiche di gruppo

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

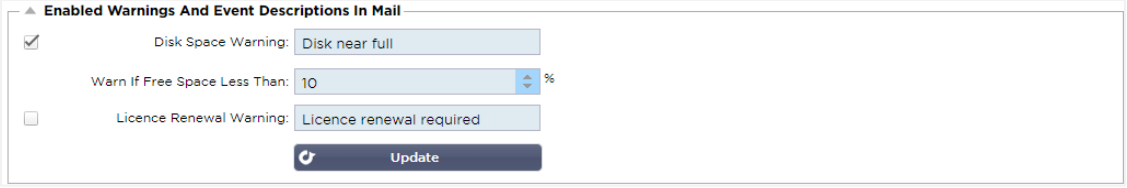
### Descrizione della posta di gruppo

Specifichi l'oggetto rilevante per l'email di avviso del gruppo.

### Intervallo di invio di gruppo

Stabilire la quantità di tempo che desidera attendere prima di inviare un'email 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, le verrà inviata un'email.

### Scadenza della licenza

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

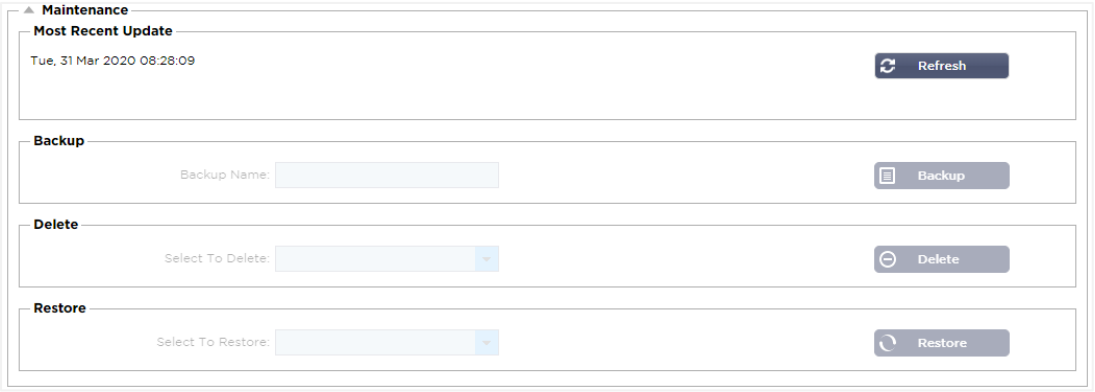
# Storia del sistema

Nella sezione System, c'è l'opzione System History, che permette di fornire dati storici per elementi come CPU, memoria, richieste al secondo e altre caratteristiche. Una volta attivata, può visualizzare i risultati in forma grafica tramite la pagina Visualizza > Cronologia. Questa pagina le permetterà anche di fare un backup o ripristinare i file della cronologia sull'ADC locale.

## Raccogliere dati


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

## Manutenzione




Questa sezione sarà grigia se ha abilitato la registrazione storica. Descriva la casella di controllo Abilitato nella sezione Raccolta dati e clicchi su Aggiorna per permettere il mantenimento dei registri storici.

### Backup

Dia un nome descrittivo al suo backup. Clicchi su Backup per eseguire il backup di tutti i file nell'ADC

### Cancellare

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

### Ripristinare

Selezioni un file di backup precedentemente memorizzato. Clicchi su Ripristina per popolare i dati da questo file di backup.

## Licenza

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

| Tipo di licenza | Descrizione |
|---|---|
| Perpetuo | Lei, il cliente, ha il diritto di usare l'ADC e altri software in perpetuo. Non le impedisce di dover acquistare il supporto per ricevere assistenza e aggiornamenti. |
| SaaS | SaaS o Software-as-a-Service significa che essenzialmente affitta il software su una base continua o pay-as-you-go. In questo modello, paga un affitto annuale per il software. Non ha 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 Macchina e ad altri dettagli specifici del suo acquisto e dell'ADC. Questa informazione è essenziale ed è richiesta quando desidera recuperare aggiornamenti e altri elementi dall'App Store.

### ID macchina

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

Nota: non deve cambiare l'indirizzo IP o il MAC ID dei suoi apparecchi ADC. Se si trova in un quadro virtualizzato, allora corregga 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

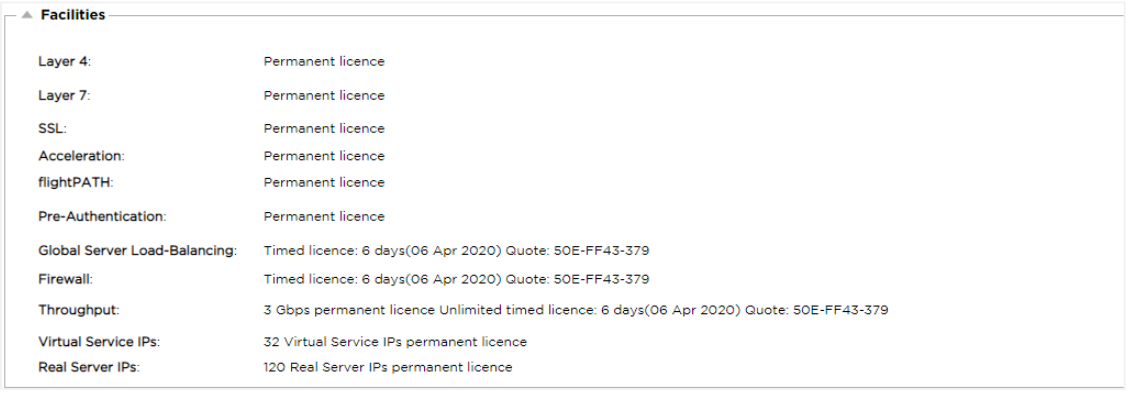
### Problemi di data

La data in cui la licenza è stata rilasciata

### Nome

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

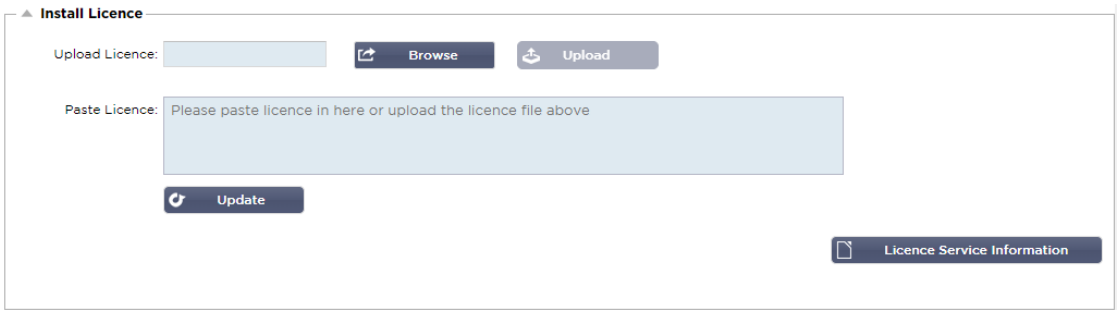
## Strutture




La sezione strutture le 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 ha acquistato.

### Installare licenze




- Installare una nuova licenza è molto semplice. Quando riceve la sua licenza nuova o sostitutiva da Edgenexus, le verrà inviata sotto forma di un file di testo. Può aprire il file e poi copiare e incollare il contenuto nel campo Paste License.
- Può anche caricarlo sull'ADC se il copia/incolla non è un'opzione per lei.
- Una volta fatto questo, clicchi sul pulsante di aggiornamento
- La licenza è ora installata.

#### Informazioni sul servizio di licenza

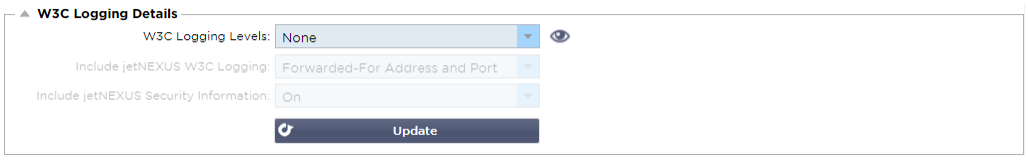
Cliccando il pulsante License Service Information si visualizzano tutte le informazioni sulla licenza. Questa funzione può essere usata per inviare i dettagli al personale di supporto.

## Registrazione

La pagina Sistema > Registrazione le 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 il log W3C l'ADC inizierà a registrare un file di log compatibile con W3C. Un log W3C è un registro di accesso per server Web in cui vengono generati file di testo contenenti dati su ogni richiesta di accesso, inclusi l'indirizzo IP (Internet Protocol) di origine, la versione HTTP, il tipo di browser, la pagina di riferimento e l'indicazione dell'ora. 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 nomi di colonne) in modo che i dati possano essere estratti. Ci sono file separati per i protocolli HTTP e FTP.




#### Livelli di registrazione W3C

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

La tabella seguente descrive i livelli di log 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). |
| Full | Questo è un formato più compatibile con i processori con campi data e ora separati. Veda 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 in più. Veda 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 tipo di informazione rilevante per il personale di sviluppo e supporto. Veda 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 sottostante descrive i livelli di log 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 |
| Full | #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 |

### Includi registrazione W3C

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

| Valore | Descrizione |
|---|---|
| Indirizzo e porta di rete del cliente | Il valore mostrato qui mostra l'effettivo indirizzo IP del cliente insieme alla porta. |
| Indirizzo di rete del cliente | Questa opzione include e mostra solo l'indirizzo IP effettivo del cliente. |
| 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. |

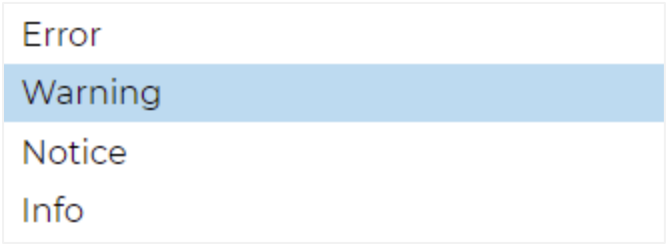
### Includa informazioni sulla sicurezza

Questo menu consiste in due opzioni:

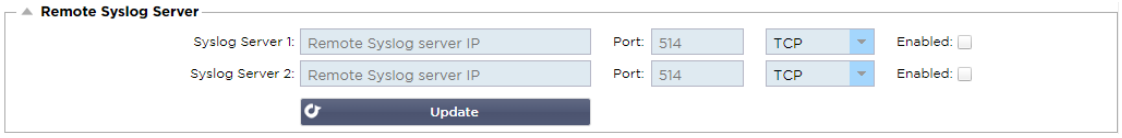
| Valore | Descrizione |
|---|---|
| Su | Questa impostazione è globale. Se impostata su on, il nome utente sarà aggiunto al log W3C quando qualsiasi servizio virtuale usa l'autenticazione e ha il log W3C abilitato. |
| Off | Questo disattiverà la possibilità di registrare il nome utente nel registro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

## Server Syslog


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



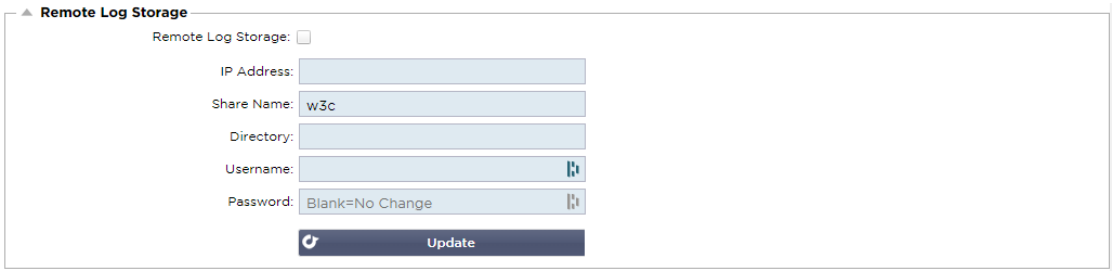

## Server Syslog remoto




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

- Aggiunga l'indirizzo IP del suo server Syslog
- Aggiunga la porta
- Scelga se vuole usare TCP o UDP
- Spunti la casella di controllo Enabled per iniziare la registrazione
- Clicchi su Aggiornamento

## Memorizzazione remota del registro




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

Nelle versioni future includeremo un pulsante di prova per fornire un feedback che le sue impostazioni siano corrette.

| Col1 | Col2 |
|---|---|
| Memorizzazione remota del registro | Spunti la casella per abilitare l'archiviazione remota del registro |
| Indirizzo IP | Specifichi l'indirizzo IP del suo server SMB. Deve essere in notazione decimale punteggiata. Esempio: 10.1.1.23 |
| Condividi Nome | Specificare il nome della condivisione sul server SMB. Esempio: w3c. |
| Directory | Specifichi 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 |

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 di timbro orario |
| c-ip | IP del cliente come meglio può essere derivato dalla rete o dall'intestazione X-Forwarded-For |
| c-port | Porta del cliente come meglio si può ricavare dalla rete o dall'intestazione X-Forwarded-For |
| cs-username | Campo di richiesta del nome utente del cliente |
| s-ip | Porta d'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 configurato |
| cs-host | Nome dell'host nella richiesta |
| x-r-ip | Indirizzo IP del Real Server utilizzato |
| x-r-port | Porta del server reale usata |
| 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 | Query 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 cliente) |
| referer | Pagina di riferimento (come inviata dal cliente) |

| | |
|---|---|
| x-c-version | Richiesta del cliente versione HTTP |
| x-r-version | Risposta di Content-Server Versione HTTP |
| cs-bytes | Bytes dal cliente, nella richiesta |
| sr-bytes | Bytes inoltrati al Real Server, nella richiesta |
| rs-bytes | Bytes da Real Server, nella risposta |
| sc-bytes | Bytes inviati al cliente, 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<br>nuovo<br>pcon | millisecondo dalla connessione all'inserimento nella "newbie list"<br>millisecondo dalla connessione al posizionamento della connessione al Real Server |
| acon | millisecondo dalla connessione al termine della collocazione della connessione al Real Server |
| rcon | millisecondo dalla connessione allo stabilire la connessione real-server |
| rqf | millisecondo dalla connessione alla ricezione del primo byte di richiesta dal cliente |
| rql | millisecondo dalla connessione alla ricezione dell'ultimo byte di richiesta dal cliente |
| 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 cliente |
| tsl | millisecondo dalla connessione all'invio dell'ultimo byte di risposta al cliente |
| dis | millisecondo dalla connessione alla disconnessione (entrambi i lati - l'ultimo a disconnettersi) |
| registro | millisecondo dalla connessione a questo record di registro 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) | Contenuto-Tipo di risposta |
| x-cache-action | Come il caching ha risposto o è stato impedito |
| x-finish | Trigger che ha causato questa riga di registro |

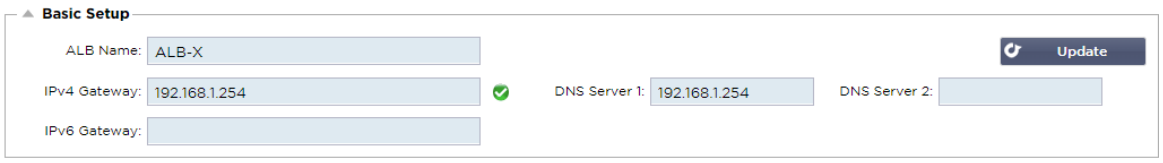
## Cancellare i file di registro

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

## Rete

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

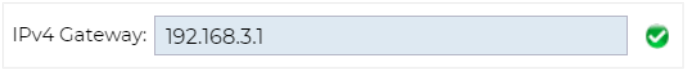
### Impostazione di base




#### Nome ALB

Specifichi un nome per il suo apparecchio ADC. Noti che questo non può essere cambiato se c'è più di un membro nel cluster. Veda la sezione su Clustering.

#### Gateway IPv4




Specifichi l'indirizzo IPv4 Gateway. Questo indirizzo dovrà trovarsi nella stessa subnet di un adattatore esistente. Se aggiunge Gateway in modo errato, vedrà una croce bianca in un cerchio rosso. Quando aggiunge un gateway corretto, vedrà un banner verde di successo in fondo alla pagina e una spunta bianca in un cerchio verde accanto all'indirizzo IP.

#### Gateway IPv6

Specifichi l'indirizzo IPv6 Gateway. Questo indirizzo dovrà trovarsi nella stessa subnet di un adattatore esistente. Se aggiunge Gateway in modo errato, vedrà una croce bianca in un cerchio rosso. Quando aggiunge un gateway corretto, vedrà un banner verde di successo in fondo alla pagina e una spunta bianca in un cerchio verde accanto all'indirizzo IP.

#### Server DNS 1 & Server DNS 2

Aggiunga l'indirizzo IPv4 del suo primo e secondo server DNS (opzionale).

### Dettagli dell'adattatore

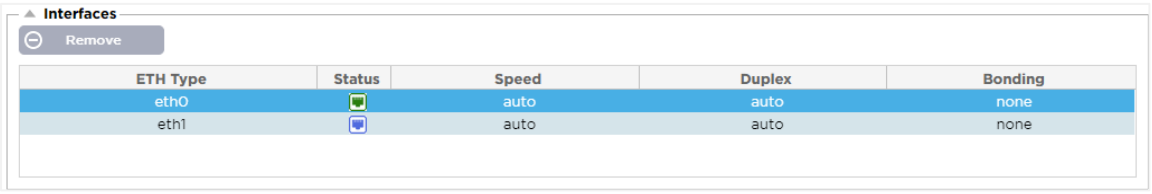
Questa sezione del pannello Rete mostra le interfacce di rete installate nel suo apparecchio ADC. Può aggiungere e rimuovere adattatori secondo necessità.


| Colonna | Descrizione |
|---|---|
| Adattatore | Questa colonna mostra gli adattatori fisici installati sul suo apparecchio. Scelga un adattatore dall'elenco degli adattatori disponibili cliccandoci sopra - un doppio clic porta la riga dell'elenco in modalità modifica. |

| | |
|---|---|
| VLAN | Clicchi due volte 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 di raggruppare più facilmente le stazioni finali se non sono sullo stesso switch di rete |
| Indirizzo IP | Clicchi due volte per aggiungere l'indirizzo IP associato all'interfaccia dell'adattatore. Può aggiungere più indirizzi IP alla stessa interfaccia. Deve essere un numero IPv4 a 32 bit in notazione decimale quadrata. Esempio 192.168.101.2 |
| Maschera di sottorete | Doppio clic per aggiungere la subnet mask assegnata all'interfaccia dell'adattatore. 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 rinviate 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 | Doppio clic per aggiungere una descrizione per il suo adattatore. Esempio di interfaccia pubblica.<br>Nota: l'ADC nominerà automaticamente la prima interfaccia Lato Verde, la seconda interfaccia Lato Rosso e la terza interfaccia Lato 3 ecc.<br>Si senta libero di cambiare queste convenzioni di denominazione a sua scelta. |
| Console web | Faccia doppio clic sulla colonna e spunti la casella per assegnare l'interfaccia come indirizzo di gestione per la Console Web dell'interfaccia utente grafica. Faccia molta attenzione quando cambia l'interfaccia su cui ascolterà Web Console. Dovrà avere il routing corretto impostato o trovarsi nella stessa subnet della nuova interfaccia per raggiungere la Web Console 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 nel pannello Rete permette la configurazione di alcuni elementi relativi all'interfaccia di rete. Può anche rimuovere un'interfaccia di rete dall'elenco cliccando sul pulsante Remove. Quando usa un apparecchio virtuale, le interfacce che vede qui sono limitate dal quadro di virtualizzazione sottostante.



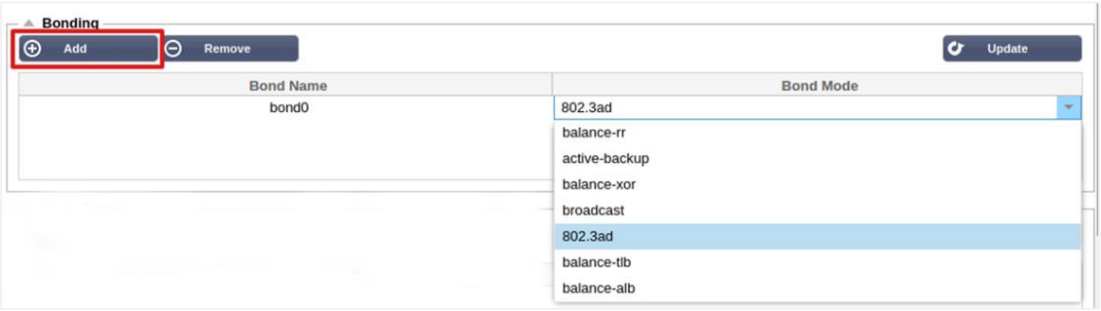
| Colonna | Descrizione |
|---|---|
| Tipo ETH | Questo valore indica il riferimento interno del sistema operativo all'interfaccia di rete. Questo campo non può essere personalizzato. I valori iniziano con ETH0 e continuano in sequenza a seconda del numero di interfacce di rete. |
| Stato | Questa indicazione 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.<br>  **Adattatore UP**<br>  Adattatore giù<br>  Adattatore scollegato<br>  Adattatore mancante |
| Velocità | Per default, questo valore è impostato per auto-negoziare la velocità. Ma può cambiare la velocità di rete dell'interfaccia a qualsiasi valore disponibile nel drop-down (10/100/1000/AUTO). |
| Duplex | Il valore di questo campo è personalizzabile e può scegliere tra Auto (default), Full-Duplex e Half-Duplex. |
| Incollaggio | Può scegliere uno dei tipi di legame che ha definito. Veda la sezione Legami per maggiori dettagli. |

## Incollaggio

Si usano molti nomi per denominare il bonding dell'interfaccia di rete: Port Trunking, Channel Bonding, Link Aggregation, NIC teaming e altri. Il bonding combina o aggrega connessioni di rete multiple in un'unica interfaccia bondata a canale. 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 incorporato per aggregare più interfacce di rete fisiche in una singola interfaccia logica (per esempio, aggregare eth0 e eth1 in bond0). Per ogni interfaccia bondata, può definire la modalità e le opzioni di monitoraggio del collegamento. Ci sono sette diverse opzioni di modalità, ognuna delle quali fornisce caratteristiche specifiche di bilanciamento del carico e tolleranza agli errori. Queste sono mostrate nell'immagine sottostante.

NOTA: IL BONDING PUÒ ESSERE CONFIGURATO SOLO PER APPARECCHI ADC BASATI SU HARDWARE.

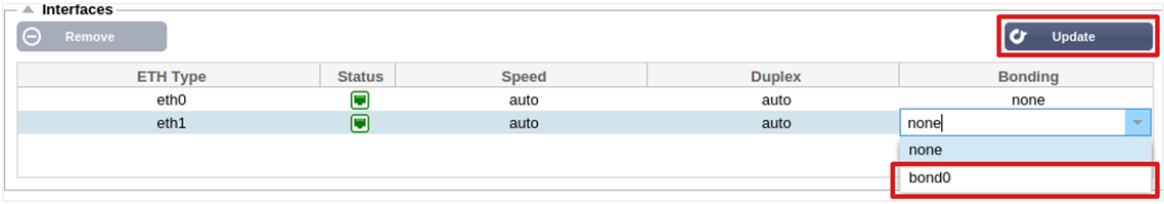



## Creare un profilo di legame

- Clicchi su Aggiungi per aggiungere un nuovo vincolo
- Fornisca un nome per la configurazione di bonding
- Scelga quale modalità di bonding desidera usare

Poi, dalla sezione Interfacce, selezioni il modo Bonding che desidera usare dal campo a discesa Bond per l'interfaccia di rete.

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

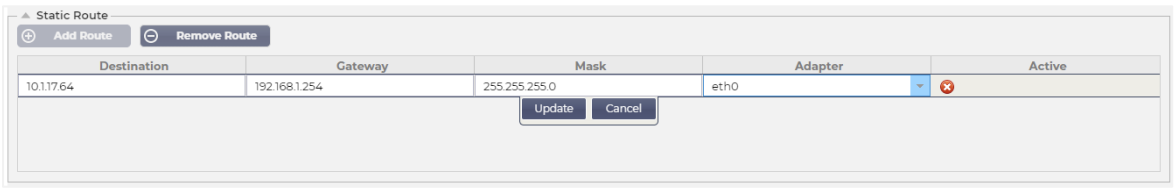



## Modalità di legame

| Modalità di legame | Descrizione |
|---|---|
| balance-rr: | I pacchetti vengono 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: | Questo modo 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: | Il modo bonding di bilanciamento del carico di trasmissione adattivo: Fornisce un channel bonding che non richiede alcun supporto speciale da parte dello switch. Il traffico in uscita viene distribuito in base al 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 assume 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 in ricezione si ottiene tramite 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 che diversi peer usino indirizzi hardware diversi per il server. |

## Rotta statica

Ci saranno momenti in cui avrà bisogno di creare rotte statiche per sottoreti specifiche all'interno della sua rete. L'ADC le offre la possibilità di farlo usando il modulo Static Routes.



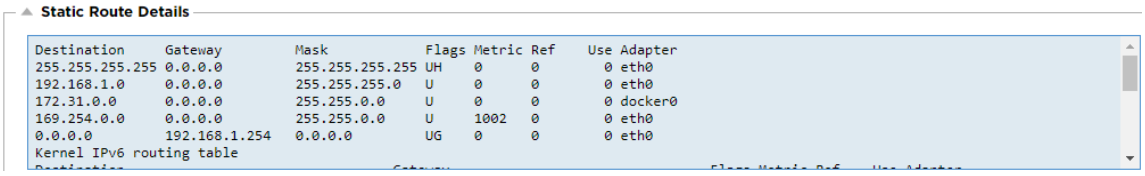
### Aggiungere una rotta statica

- Clicchi sul pulsante Aggiungi rotta
- Compili il campo usando i dettagli nella tabella sottostante come guida.
- Clicchi il pulsante Update quando ha finito.

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

## Dettagli delle rotte statiche

Questa sezione fornisce informazioni su tutti i percorsi configurati 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 da inviare in rete. Vedere l'**ARTICOLO DI WIKIPEDIA SU NAGLE**

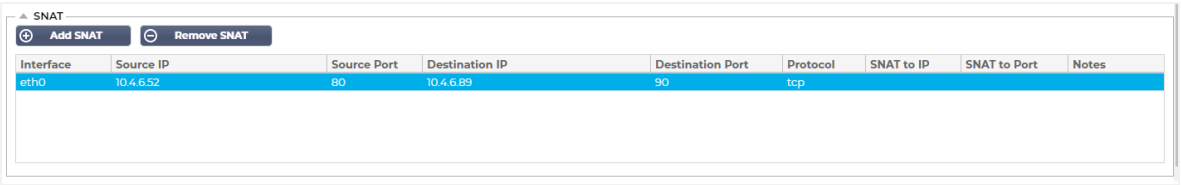
### Server Nagle

Spunti questa casella per attivare 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 in rete. Questa impostazione viene applicata al lato Server della transazione. Bisogna fare attenzione alle impostazioni del server perché Nagle e l'ACK ritardato possono avere un forte impatto sulle prestazioni.

### Cliente Nagle

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

## SN SN SN SNAT _COPY DI _COPY DI




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. Quindi, per esempio, se un endpoint del browser avesse un indirizzo IP di 81.71.61.51, questo sarebbe visibile al VIP.

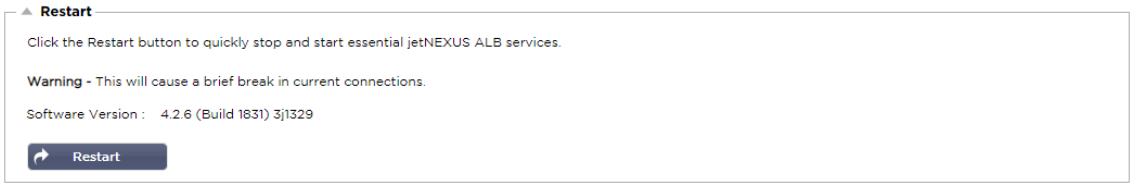
Quando SNAT è in vigore, l'IP di origine originale della richiesta sarà nascosto al VIP, che invece vedrà l'indirizzo IP fornito nella regola SNAT. Pertanto, SNAT può essere usato nei modi di bilanciamento del carico Layer 4 e Layer 7.

| Campo | Descrizione |
|---|---|
| Fonte IP | L'indirizzo IP di origine è opzionale e può essere un indirizzo IP di rete (con /mask) o un indirizzo IP semplice. La maschera può essere una maschera di rete o un numero semplice, 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 una maschera di rete o un numero semplice, specificando il numero di 1 a sinistra della maschera di rete. Così, una maschera di /24 è equivalente a 255.255.255.0. |
| Fonte Porto | La porta di origine è opzionale, può essere un numero singolo, nel qual caso specifica solo quella porta, oppure può includere due punti, che specifica una gamma 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, oppure può includere due punti, che specifica una gamma di porte. Esempi: 80 o 5900:5905. |
| Protocollo | Può scegliere se usare SNAT su un singolo 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 una gamma di indirizzi IP. Esempi: 10.0.0.1 o 10.0.0.1-10.0.0.3. |
| SNAT a Porto | Lo SNAT to Port è opzionale, può essere un numero singolo, nel qual caso specifica solo quella porta, oppure può includere un trattino, che specifica una gamma di porte. Esempi: 80 o 5900-5905. |
| Note | Lo usi per mettere un nome amichevole per ricordarsi perché le regole esistono. Questo è utile anche per il debug nel Syslog. |

## Potenza

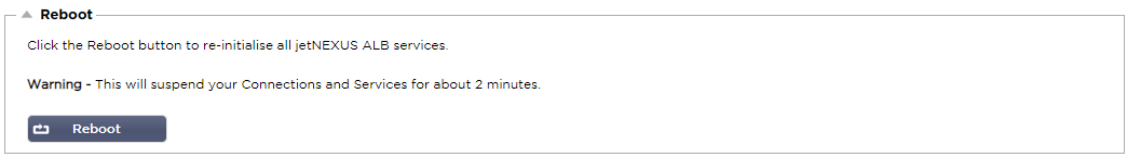
Questa caratteristica del sistema ADC le permette anche di svolgere diversi compiti relativi all'alimentazione sul suo ADC.

### Riavviare



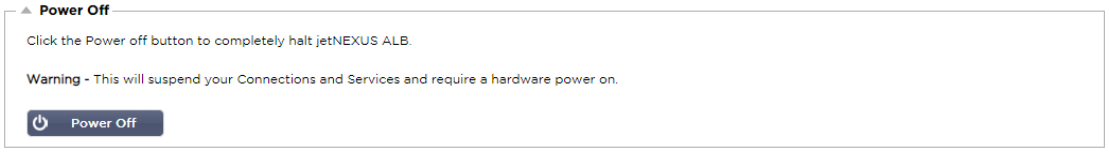

Questa impostazione avvia un riavvio globale di tutti i Servizi e di conseguenza interrompe tutte le connessioni attualmente attive. Tutti i Servizi riprenderanno automaticamente dopo un breve periodo, ma i tempi dipendono da quanti Servizi sono configurati. Verrà visualizzato un pop-up che richiede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

### Reboot




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




Cliccando il pulsante Power Off spegnerà l'ADC. Se si tratta di un apparecchio hardware, dovrà avere accesso fisico al dispositivo per riaccenderlo. Verrà visualizzato un pop-up che chiede conferma dell'azione di spegnimento.

## Sicurezza

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

### SSH


| Opzione | Descrizione |
|---|---|
| Connessione remota Secure Shell | Spunti la casella se desidera accedere all'ADC usando SSH. "Putty" è un'applicazione eccellente per farlo. |

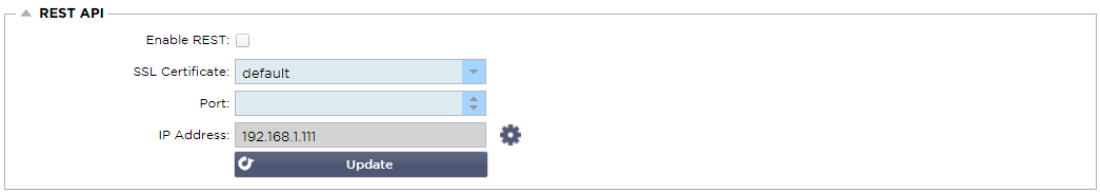
### Console web


Certificato SSL Scelga un certificato dall'elenco a discesa. Il certificato che sceglie sarà usato per proteggere la sua connessione all'interfaccia utente web dell'ADC. Può 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 desidera usare una porta diversa per motivi di sicurezza, può cambiarla qui. |

## API REST

La REST API, conosciuta anche come RESTful API, è un'interfaccia di programmazione di applicazioni conforme allo stile architettonico REST e permette la configurazione dell'ADC o l'estrazione di dati dall'ADC. Il termine REST sta per Representational State Transfer ed è stato creato dall'informatico Roy Fielding.




| Opzione | Descrizione |
|---|---|
| Attiva REST | Spunti questa casella per abilitare l'accesso tramite REST API. Noti che dovrà anche configurare quale adattatore su cui REST è abilitato. Veda la nota sul link Cog qui sotto. |
| Certificato SSL | Scelga 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. Può cliccare sul link Cog per accedere alla pagina Network per cambiare su quale adattatore è abilitato il servizio REST. |
| Collegamento a un ingranaggio | Cliccando su questo link la porterà alla pagina Network dove può 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 ottiene errori nella pagina Swagger è perché hanno un problema nel supportare le stringhe di query*
*Scorra 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*

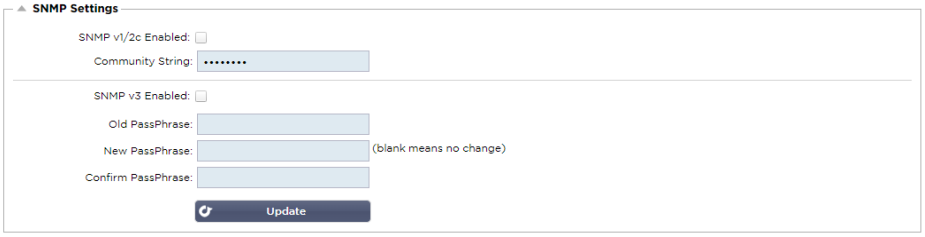
- Comando

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 software di terzi in grado di comunicare con dispositivi dotati di SNMP.

### Impostazioni SNMP




| Opzione | Descrizione |
|---|---|
| SNMP v1 / V2C | Selezioni la casella di controllo per abilitare la MIB V1/V2C.<br>SNMP v1 è conforme a RFC-1157. SNMP V2c è conforme a RFC-1901-1908 |
| SNMP v3 | Spunti la casella di controllo per abilitare la V3 MIB. RFC-3411-3418.<br>Il nome utente per v3 è admin.<br>Esempio:- snmpwalk -v3 -u admin -A jetnexus -l authNoPriv 192.168.1.11 1.3.6.1.4.1.38370 |
| Stringa comunitaria | 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 predefinita 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 identificatori gerarchici di oggetti (OID). Ogni OID può essere letto tramite un'applicazione di gestione SNMP.

### Scaricare MIB

Il MIB può essere scaricato gui:

### 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)

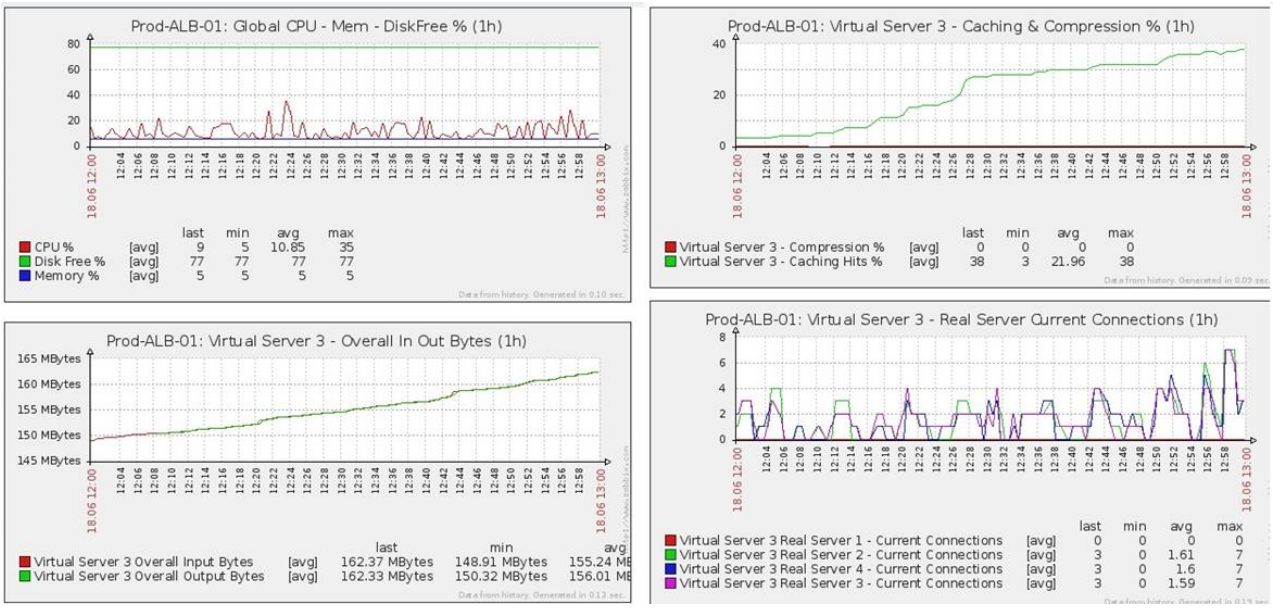
.2 **jetnexusOverallOutputBytes (1**.3.6.1.4.1.38370.1.1.2.0)
.3 **jetnexusCompressedInputBytes (1**.3.6.1.4.1.38370.1.1.3.0)
. 4 **jetnexusCompressedOutputBytes (1**.3.6.1.4.1.38370.1.1.4.0)
. 5 **jetnexusVersionInfo (1**.3.6.1.4.1.38370.1.1.5.0)
.6 **jetnexusTotalClientConnections (1**.3.6.1.4.1.38370.1.1.6.0)
.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 del Custom SNMP MIB dell'ADC è la possibilità di scaricare il grafico storico su una console di gestione di sua scelta. Di seguito alcuni esempi di Zabbix che interrogano un ADC per vari valori OID elencati sopra.



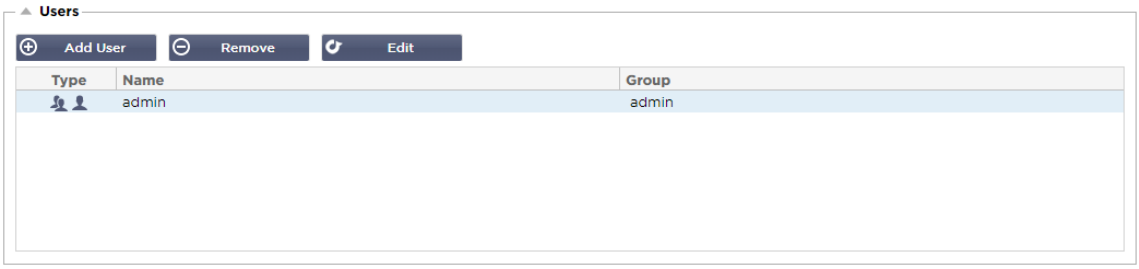

## Utenti e registri di controllo

L'ADC offre 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 ad essi collegato.

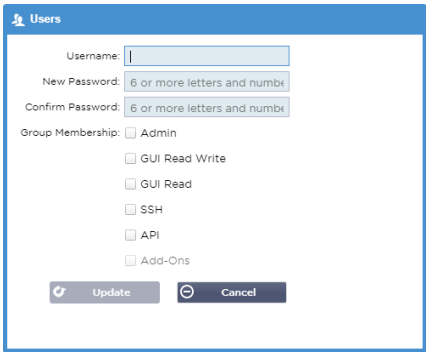
C'è un utente predefinito chiamato **admin** che si usa quando si configura l'ADC per la prima volta. La password predefinita per admin è **jetnexus**.

### Utenti

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




### Aggiungi utente




Clicchi il pulsante Add User mostrato nell'immagine qui sopra per far apparire la finestra di dialogo Add User.

| Parametro | Descrizione/Utilizzo |
|---|---|
| Nome utente | Inserisca un nome utente di sua scelta<br>Il nome utente deve essere conforme a quanto segue:<br>• Numero minimo di caratteri 1<br>• Numero massimo di caratteri 32<br>• Le lettere possono essere maiuscole e minuscole<br>• Si possono usare numeri<br>• I simboli non sono ammessi |
| Password | Inserisca una password **forte** che sia conforme ai seguenti requisiti<br>• Numero minimo di caratteri 6<br>• Numero massimo di caratteri 32<br>• Deve usare almeno una combinazione di lettere e numeri<br>• Le lettere possono essere maiuscole o minuscole<br>• I simboli sono permessi tranne quelli dell'esempio seguente<br>**£**, **%**, **& , < , >** |
| Confermare la password | Confermi nuovamente la password per assicurarsi che sia corretta |
| Membri del gruppo | Spunti il gruppo a cui vuole che l'utente appartenga.<br>• Admin - Questo gruppo può fare tutto<br>• GUI Read Write - Gli utenti di questo gruppo possono accedere alla GUI e fare modifiche tramite la GUI<br>• GUI Read - Gli utenti di questo gruppo possono accedere alla GUI solo per visualizzare informazioni. Non si possono effettuare modifiche<br>• SSH - Gli utenti in 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<br>• 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 default, un** utente locale chiamato "admin" **è membro del gruppo admin. Per compatibilità all'indietro**, **questo utente non può mai essere cancellato**
**Può cambiare la password di questo utente o cancellarlo**, **ma non può cancellare l'ultimo admin locale**

**Utente del cluster**
Il ruolo ADC in Cluster creerà solo utenti Cluster
Gli utenti del cluster sono sincronizzati in tutti gli ADC nel cluster
Qualsiasi modifica a un utente del cluster cambierà su tutti i membri del cluster
Se è collegato come utente del cluster, non potrà cambiare ruolo 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, allora rimarranno solo gli utenti locali
L'ultima password configurata per l'utente sarà valida

### Rimozione di un utente

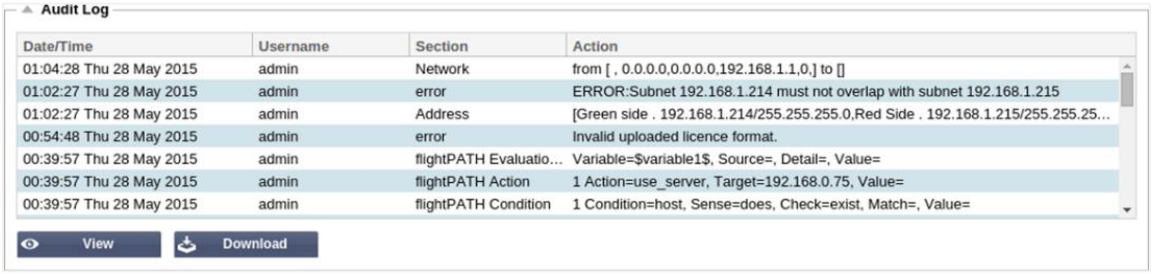
- Evidenziare un utente esistente
- Cliccare su Rimuovi
- Non potrà cancellare l'utente che è attualmente iscritto
- Non potrà rimuovere l'ultimo utente locale nel gruppo admin
- Non potrà rimuovere l'ultimo utente del cluster rimasto nel gruppo admin
- Non potrà cancellare l'utente admin per compatibilità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

### Modifica di un utente

- Evidenziare un utente esistente
- Clicchi su Modifica
- Può cambiare l'appartenenza al gruppo dell'utente spuntando le caselle appropriate e aggiornando
- Può anche cambiare la password di un utente, purché abbia i diritti di amministratore

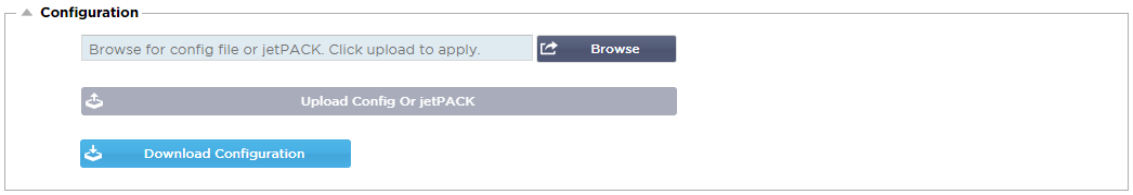
## Registro di controllo

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



# Advanced

## Configurazione




È sempre una buona pratica scaricare e salvare la configurazione dell'ADC una volta che è completamente impostato e funziona come richiesto. Può usare il modulo Configurazione sia per scaricare che per caricare una configurazione.

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

Un file di configurazione è essenzialmente un file basato sul testo e, come tale, può essere modificato da lei 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 attuale dell'ADC, prema il pulsante Download Configuration.
- Apparirà un pop-up che le chiederà di aprire o salvare il file .conf.
- Salvi in una posizione comoda.
- Può aprirlo con qualsiasi editor di testo, come Notepad++.

### Caricamento di una configurazione

- Può caricare un file di configurazione salvato cercando il file .conf salvato.
- Clicchi il pulsante 'Upload Config or Jetpack'.
- L'ADC caricherà e applicherà la configurazione e poi aggiornerà il browser. Se non aggiorna il browser automaticamente, clicchi su refresh del browser.
- Al termine verrà reindirizzato alla pagina Dashboard.

### Carichi 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.
    - Può ottenere un jetPACK dal portale di supporto indicato alla fine di questa guida.
- Cerchi il file jetPACK.txt.
- Clicchi su upload.
- Il browser si aggiornerà automaticamente dopo il caricamento.
- Al termine verrà reindirizzato alla pagina Dashboard.
- L'importazione può richiedere più tempo per distribuzioni più complesse come Microsoft Lync ecc.

## Impostazioni globali

La sezione Impostazioni globali le 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 usato al posto di un indirizzo IP. La cache viene svuotata in caso di fallimento del Real Server. Impostando questo valore a zero si evita che la cache venga lavata. Non esiste un valore massimo per questa impostazione.

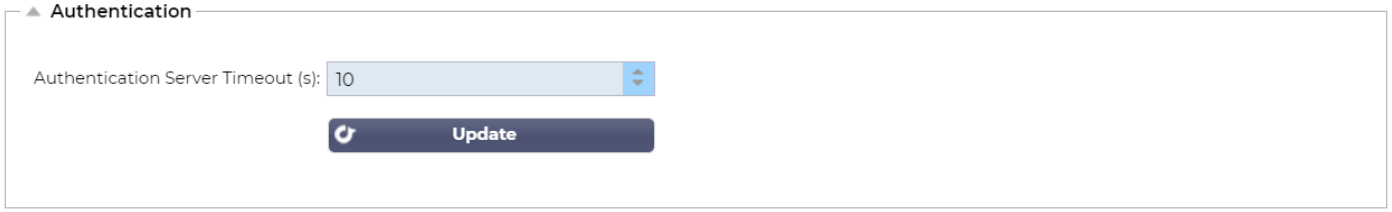
## Drenaggio


La funzione Drain è configurabile per ogni Real Server collegato ad un Servizio Virtuale. Per impostazione predefinita, l'impostazione Drain Clears Persistence è abilitata, permettendo ai server che vengono 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 a seconda delle necessità. La libreria crittografica SSL predefinita usata dall'ADC è di OpenSSL. Se volesse usare una libreria crittografica diversa, questa può essere cambiata qui.

## Autenticazione

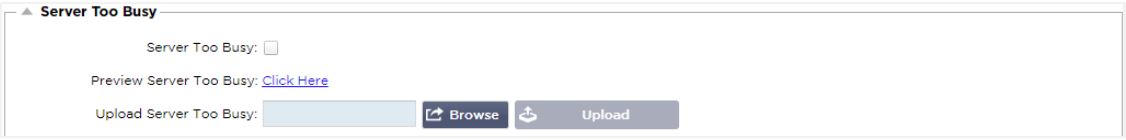



Questo valore imposta il valore di timeout per l'autenticazione, dopo il quale il tentativo di autenticazione sarà considerato fallito.

# Protocollo

La sezione Protocollo si usa per impostare le molte impostazioni avanzate per il protocollo HTTP.

## Server troppo occupato




Supponiamo che lei abbia limitato le connessioni massime ai suoi Real Server; può scegliere di presentare una pagina web amichevole una volta raggiunto questo limite.

- Crei una semplice pagina web con il suo messaggio. Può includere link esterni a oggetti su altri server e siti web. In alternativa, se vuole avere immagini nella sua pagina web, allora usi immagini codificate inline base64
- Cerchi il file HTM(L) della sua pagina web appena creata
- Clicchi su Upload
- Se vuole vedere l'anteprima della pagina, può farlo con il link Clicca qui

## Inoltrato per


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

### Uscita inoltrata

| Opzione | Descrizione |
|---|---|
| Off | ADC non altera l'intestazione Forwarded-For. |
| Aggiunga indirizzo e porta | Questa scelta aggiungerà l'indirizzo IP e la porta, del dispositivo o del cliente collegato all'ADC, all'intestazione Forwarded-For. |
| Aggiunga l'indirizzo | Questa scelta aggiungerà l'indirizzo IP, del dispositivo o del cliente collegato all'ADC, all'intestazione Forwarded-For. |
| Sostituisca 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. |
| Sostituisca l'indirizzo | Questa scelta sostituirà il valore dell'intestazione Forwarded-For con l'indirizzo IP del dispositivo o del cliente collegato all'ADC. |

### Intestazione Forwarded-For

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

### Registrazione avanzata per IIS - Registrazione personalizzata

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

Selezioni Default dall'elenco Source Type dall'elenco Category, selezioni Request Header nella casella Source Name e digiti X-Forwarded-For.

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

### Modifiche di Apache HTTPd.conf

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

Questi cambiamenti sono qui sotto:

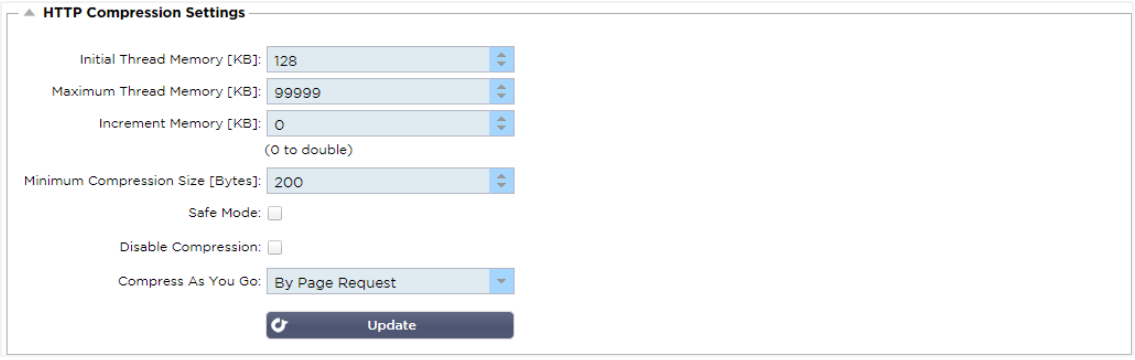
| Tipo | Valore |
|---|---|
| LogFormat: | "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combinato |
| LogFormat: | "%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" proxy SetEnvIf X- Forwarded-For "^.*\\..*\..*\..*" inoltrata |
| CustomLog: | "logs/access_log"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

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

- La riga 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 ad un indirizzo IP, il che va bene in questo caso dato che ci interessa di più se esiste un indirizzo IP nell'intestazione X-Forwarded-For.
- Inoltre, la linea 3 potrebbe essere letta come: "Se esiste un valore X-Forwarded-For, lo usi".
- Le linee 4 e 5 dicono ad Apache quale modello di log usare. Se esiste un valore X-Forwarded-For, usa il modello "proxy", altrimenti usa il modello "combined" per la richiesta. Per leggibilità, le righe 4 e 5 non approfittano della funzione di log rotate logs (piped) di Apache, ma presumiamo che quasi tutti la usino.

Questi cambiamenti porteranno alla registrazione di un indirizzo IP per ogni richiesta.

### Impostazioni di compressione HTTP



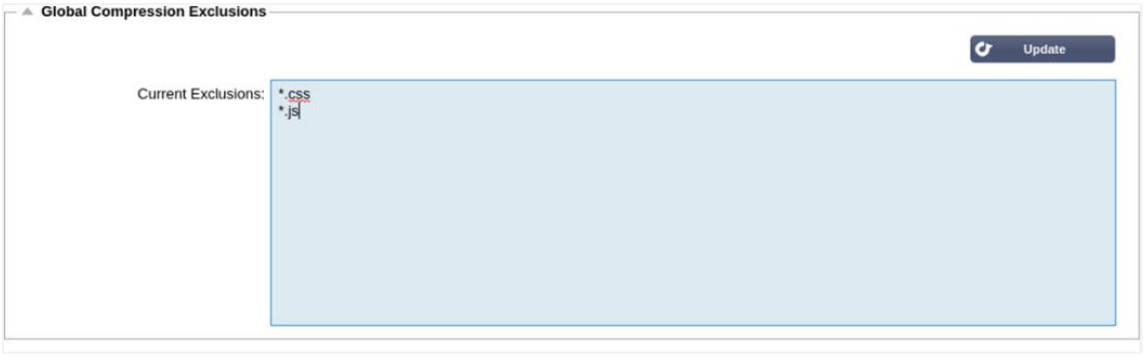

La compressione è una funzione di accelerazione ed è abilitata per ogni servizio nella pagina Servizi IP.

*AVVERTENZA - Faccia molta attenzione quando regola queste impostazioni perché 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 performance più efficiente, questo valore dovrebbe essere impostato ad un valore appena superiore al più grande file HTML non compresso che i server web probabilmente invieranno. |

| | |
|---|---|
| Memoria massima del thread [KB] | Questo valore è la quantità massima di memoria che ADC alloca in una richiesta. Per la massima performance, 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 ne è richiesta una 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 maggioranza delle pagine sono di una dimensione consistente ma ci sono occasionalmente file più grandi. (es. la maggioranza delle pagine è di 128Kb o meno, ma le risposte occasionali sono 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 esempio, 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 al di sotto dei 200 byte non si comprime bene e può persino crescere in dimensioni a causa delle spese generali delle intestazioni di compressione. |
| Modo sicuro | Spunti questa opzione per evitare che ADC applichi la compressione ai fogli di stile di JavaScript. Il motivo è che anche se ADC è consapevole di quali browser individuali possono gestire contenuti compressi, alcuni altri server proxy, anche se dichiarano di essere conformi a 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 usi questa opzione per disabilitare la compressione di questi tipi. Tuttavia, questo ridurrà la quantità complessiva di compressione del contenuto. |
| Disattivare la compressione | Lo spunti per impedire all'ADC di comprimere qualsiasi risposta. |
| Comprima man mano che va avanti | ON - Usa Compress as You Go su questa pagina. Questo comprime ogni blocco di dati ricevuto dal server in un chunk discreto che è completamente decomprimibile.<br>OFF - Non usare Compress as you go su questa pagina.<br>By Page Request - Usa Compress as You Go per richiesta di pagina. |

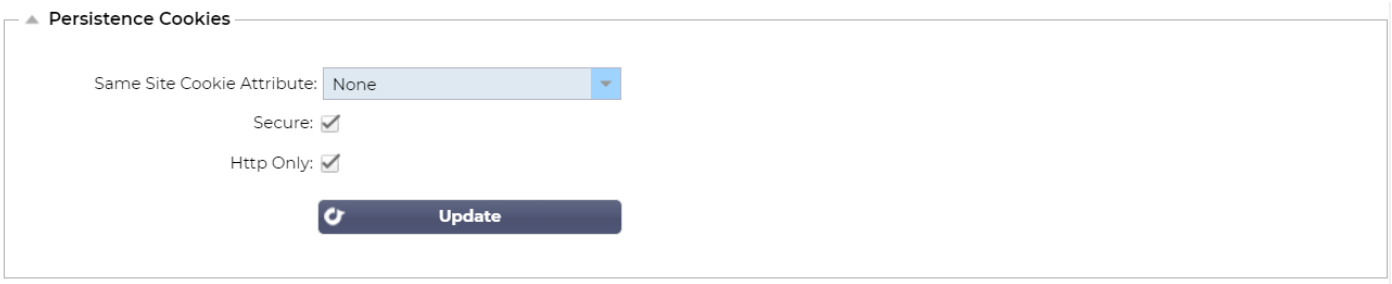
## Esclusioni di compressione globale




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

- Digiti il nome del file individuale.
- Clicchi su aggiornamento.
- Se vuole aggiungere un tipo di file, digiti semplicemente "*.css" per tutti i fogli di stile a cascata da escludere.
- Ogni file o tipo di file deve essere aggiunto ad una nuova riga.

### Cookie di persistenza



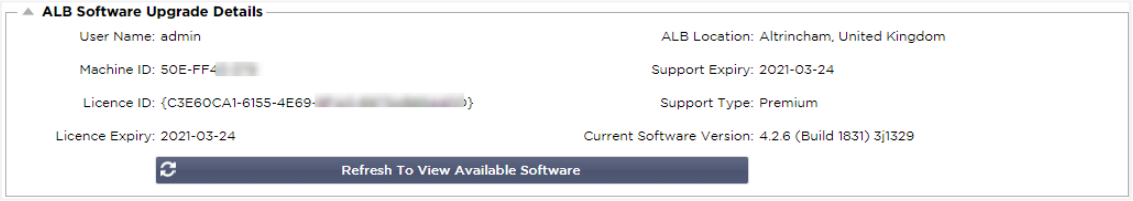

Questa impostazione le permette di specificare come vengono gestiti i Persistence Cookies.

| Campo | Descrizione |
|---|---|
| Stesso sito Attributo Cooke | **Nessuno**: Tutti i cookie sono accessibili agli script<br>**Lassista**: Impedisce che i cookie siano accessibili da un sito all'altro, ma vengono memorizzati per diventare accessibili e presentati al sito proprietario se viene visitato.<br>**Strict**: impedisce l'accesso o la memorizzazione di qualsiasi cookie per un sito diverso<br>**Off**: ritorna al comportamento predefinito del browser |
| Sicuro | Questa casella di controllo, se 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 le permette di aggiornare la configurazione e il firmware del suo ADC.

### Dettagli dell'aggiornamento del software




Le informazioni in questa sezione saranno popolate se ha una connessione Internet funzionante. Se il suo browser non ha un collegamento a Internet, questa sezione sarà vuota. Una volta connesso, riceverà il messaggio del banner sottostante.

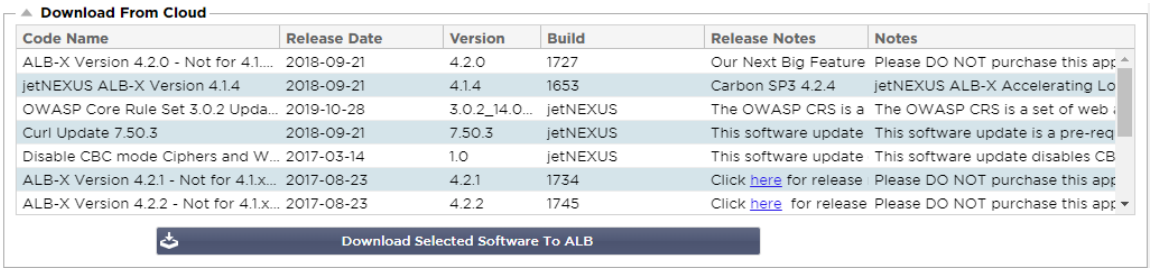

La sezione Download from Cloud mostrata qui sotto sarà popolata con informazioni che mostrano gli aggiornamenti disponibili per lei sotto il suo piano di supporto. Deve prestare attenzione al Tipo di supporto e alla Data di scadenza del supporto.

*Nota: usiamo la connessione internet del suo browser per visualizzare ciò che è disponibile da Edgenexus Cloud. Potrà scaricare gli aggiornamenti del software solo se l'ADC ha una connessione internet.*

Per controllare questo:

- Advanced--Troubleshooting--Ping
- Indirizzo IP - appstore.edgenexus.io
- Clicchi su Ping
- Se il risultato mostra "ping: host sconosciuto appstore.edgenexus.io. "
- L'ADC NON potrà scaricare nulla dal cloud

## Scaricare da Cloud




Se il suo browser è collegato a Internet, vedrà i dettagli del software disponibile nel cloud.

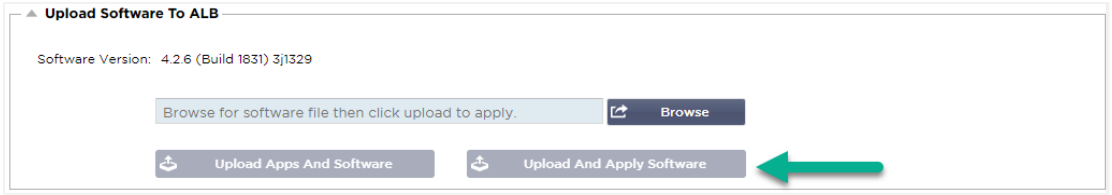
- Evidenzi la riga che le interessa e clicchi su "Download Selected Software to ALB. ".
- Una volta cliccato, il software selezionato verrà scaricato nella sua ALB e potrà essere applicato nella sezione "Apply Software Stored on ALB" qui sotto.

Nota: se l'ADC non ha un accesso diretto a Internet, riceverà un errore come il seguente:

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

## Carichi il software su ALB

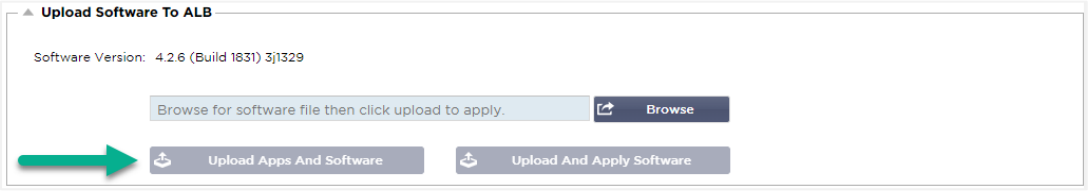
### Caricamento delle applicazioni




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

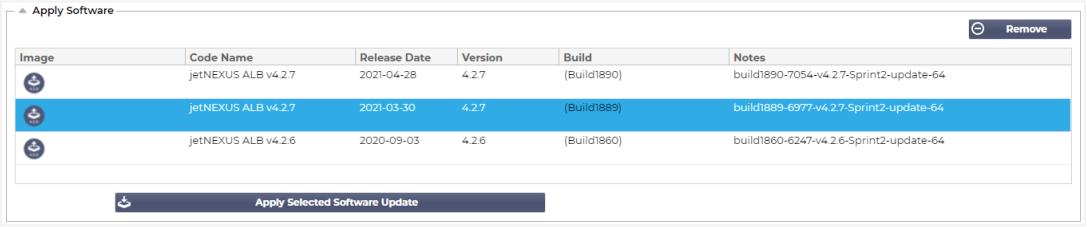
- Ci sono cinque tipi di App
  - <appname>flightpath.alb
  - <appname>.monitor.alb
  - <appname>.jetpack.alb
  - <appname>.addons.alb
  - <appname>.featurepack.alb
- Una volta caricata, ogni app si troverà nella sezione Biblioteca> App.
- Deve poi distribuire ogni App in quella sezione individualmente.

### Software




- Se desidera caricare il software senza applicarlo, allora usi il pulsante evidenziato.
- Il file del software è <nome del software>.software.alb.
- Verrà poi mostrato nella sezione "Software Stored on ALB", da dove potrà applicarlo a suo piacimento.

### Applichi 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.

- Evidenzi la riga Software che le interessa.
- Clicchi su "Applica software da selezionato".
- Se si tratta di un aggiornamento del software dell'ALB, sappia che verrà caricato e poi riavviato l'ALB per essere applicato.
- Se l'aggiornamento che sta applicando è un aggiornamento della firma OWASP, si applicherà automaticamente senza riavviare.

## Risoluzione dei problemi

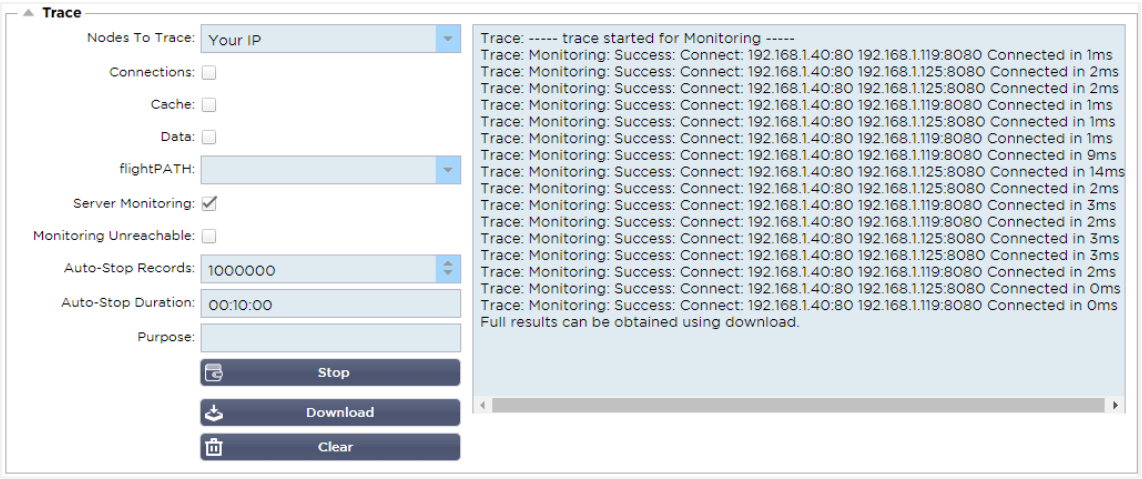
Ci sono sempre problemi che richiedono la risoluzione di problemi per arrivare alla causa principale e alla soluzione. Questa sezione le permette di farlo.

### File di supporto


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

- Selezioni un periodo di tempo dal menu a tendina: Può scegliere tra 3, 7, 14 e Tutti i giorni.
- Clicchi su "Scaricare i file di supporto".
- Verrà scaricato un file nel formato Support-jetNEXUS-yyymmddhh-NAME.dat
- Sollevi un ticket di supporto sul portale di supporto, i cui dettagli sono disponibili alla fine di questo documento.
- Si assicuri di descrivere accuratamente il problema e di allegare il file .dat al biglietto.

## Traccia



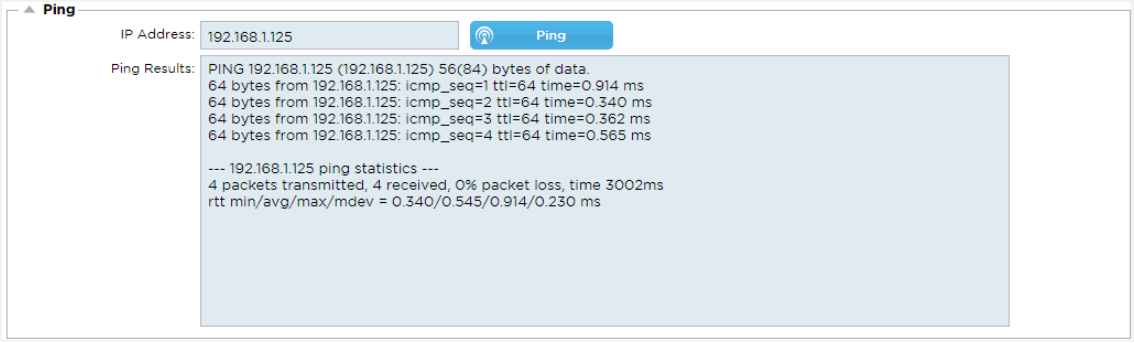

La sezione Trace le permetterà di esaminare informazioni che permettono il debugging del problema. Le informazioni fornite dipendono dalle opzioni che sceglie dai menu a tendina e dalle caselle di spunta.

| Opzione | Descrizione |
|---|---|
| Nodi da rintracciare | **Il tuo IP**: Questo filtrerà l'output per usare l'indirizzo IP da cui stai accedendo alla GUI (Nota: non scegliere questa opzione per il Monitoraggio perché il Monitoraggio userà l'indirizzo dell'interfaccia ADC) **Tutti gli IP**: Non verrà applicato alcun filtro. Va notato che su un box occupato questo influenzerà negativamente le prestazioni. |
| Connessioni | Questa casella di controllo, se spuntata, le mostrerà informazioni sulle connessioni lato client e lato server. |
| Cache | Questa casella spuntata le mostrerà 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 le 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 Irraggiungibile | Quando questa opzione è selezionata, il suo 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. |
| Registri Auto-Stop | Il valore predefinito è 1.000.000 record, dopodiché la funzione Trace si ferma automaticamente. Questa impostazione è una precauzione di sicurezza per evitare che Trace venga lasciato accidentalmente acceso e influenzi le prestazioni dell'ADC. |
| Durata dell'Auto-Stop | Il tempo predefinito è impostato a 10 minuti, dopodiché la funzione Trace si ferma automaticamente. Questa caratteristica è una precauzione di sicurezza per evitare che Trace venga lasciato accidentalmente acceso e influenzi le prestazioni dell'ADC. |
| Iniziare | Clicchi qui per avviare manualmente la funzione Trace. |
| Si fermi | Clicchi per fermare manualmente la funzione Trace prima che venga raggiunto il record automatico o il tempo. |

| | |
|---|---|
| Scarichi | Anche se può vedere il live viewer sul lato destro, le informazioni potrebbero essere visualizzate troppo velocemente. Può invece scaricare il Trace.log per visualizzare tutte le informazioni raccolte durante le varie tracce di quel giorno. Questa funzione è una lista filtrata di informazioni sulle tracce. Se desidera visualizzare le informazioni di traccia dei giorni precedenti, può scaricare Syslog per quel giorno ma dovrà filtrare manualmente. |
| Chiaro | Cancella il registro di tracciamento |

## Ping

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




Digiti l'indirizzo IP dell'host che vuole testare, per esempio il gateway predefinito usando la notazione decimale punteggiata o un indirizzo IPv6. Potrebbe dover aspettare alcuni secondi per il risultato dopo aver premuto il pulsante "Ping".

Se ha configurato un server DNS, allora può digitare il nome di dominio completamente qualificato. Può configurare un server DNS nella sezione **DNS SERVER 1 & DNS SERVER 2.** Potrebbe dover attendere alcuni secondi per il risultato dopo aver premuto il pulsante "Ping".

## Cattura


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

- Completi le opzioni nel modulo
- Clicchi su Genera
- Una volta eseguita la cattura, il suo browser apparirà e le chiederà dove vuole salvare il file. Sarà nel formato "jetNEXUS.cap.gz".
- Sollevi un ticket di supporto sul portale di supporto, i cui dettagli sono disponibili alla fine di questo documento.
- Si assicuri di descrivere accuratamente il problema e di allegare il file al biglietto.
- Può anche visualizzare il contenuto usando Wireshark

| **Opzione** | **Descrizione** |
|---|---|

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

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

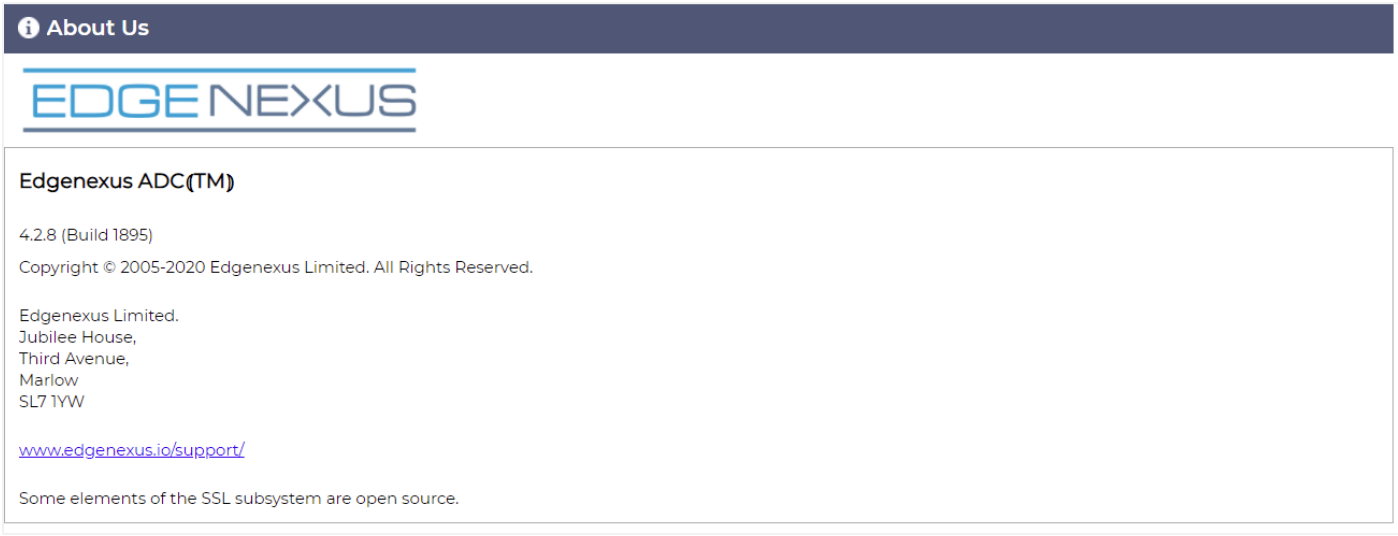
Nota: questo avrà un impatto sulla performance dei siti live. Per aumentare la dimensione di cattura disponibile, applichi un'impostazione globale jetPACK per aumentare la dimensione di cattura.

# Aiuto

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

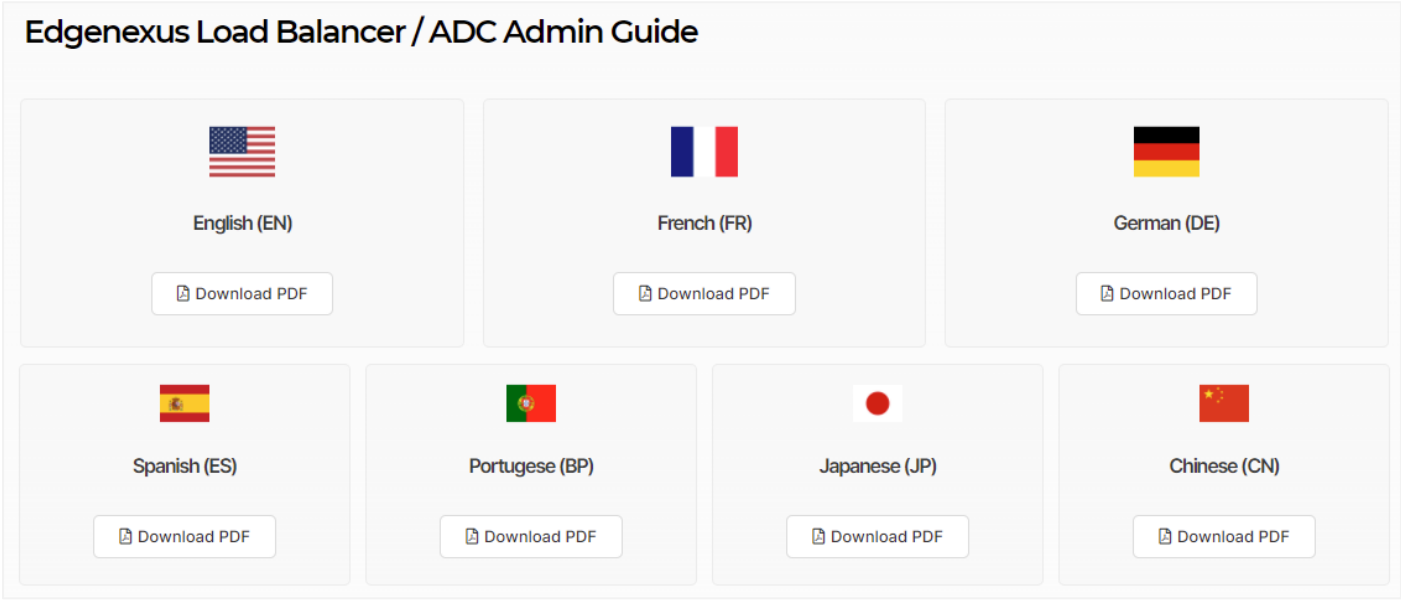
## Informazioni su di noi

Cliccando sull'opzione Chi siamo visualizzerà 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 trova quello che sta cercando, contatti support@edgenexus.io.

# Cos'è un jetPACK

I jetPACK sono un metodo unico per configurare istantaneamente il suo ADC per applicazioni specifiche. Questi modelli facili da usare sono preconfigurati e completamente sintonizzati con tutte le impostazioni specifiche dell'applicazione di cui ha bisogno per godere di un servizio ottimizzato dal suo ADC. Alcuni dei jetPACK usano flightPATH per manipolare il traffico e lei deve avere una licenza flightPATH perché questo elemento funzioni. Per sapere se ha una licenza per flightPATH, faccia riferimento alla pagina **LICENZA.**

## Scaricare un jetPACK

- Ogni jetPACK qui sotto è stato creato con un indirizzo IP Virtuale unico contenuto nel titolo del jetPACK. Per esempio, il primo jetPACK qui sotto ha un indirizzo IP Virtuale di 1.1.1.1
- Può 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 suo 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 può cambiarli nella GUI dopo il caricamento o prima usando Notepad++.
- Clicchi su un link jetPACK qui sotto e salvi il link come file jetPACK-VIP-Application.txt nella posizione scelta

### Microsoft Exchange

| Applicazione | Link per il download | 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. È inclusa una regola flightPATH per reindirizzare il traffico sul servizio HTTP a HTTPS, ma è un'opzione. Se non ha una licenza per flightPATH, questo jetPACK funzionerà comunque. | Impostazioni globali: Timeout di servizio 2 ore<br>Monitor: Monitor di livello 7 per l'applicazione web di Outlook e monitor di livello 4 fuori banda per il servizio di accesso del cliente<br>IP del servizio virtuale: 1.1.1.1<br>Porte di servizio virtuali: 80, 443, 135, 59534, 59535<br>Server reali: 127.1.1.1<br>127.2.2.2<br>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<br>Monitor: Monitor di livello 7 per l'applicazione web di Outlook.<br>Monitor di livello 4 fuori banda per il servizio di accesso al client<br>IP del servizio virtuale: 1.1.1.1<br>Porte di servizio virtuali: 80, 443, 135, 59534, 59535, 25 (reverse proxy)<br>Server reali: 127.1.1.1<br>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 suo server SMTP deve vedere l'indirizzo IP effettivo del cliente. | Impostazioni globali: Timeout di servizio 2 ore<br>Monitor: Monitor di livello 7 per l'applicazione web di Outlook. Monitor di livello 4 fuori banda per il servizio di accesso al client<br>IP del servizio virtuale: 1.1.1.1<br>Porte di servizio virtuali: 80, 443, 135, 59534, 59535, 25 (ritorno diretto al server)<br>Server reali: 127.1.1.1 127.2.2.2<br>flightPATH: aggiunge il reindirizzamento da HTTP a HTTPs |
| Exchange 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.<br>È possibile aggiungere più controlli di salute al VIP per controllare che ognuno dei singoli servizi sia attivo | Impostazioni globali:<br>Monitor: Monitor di livello 7 per OWA, EWS, OA, EAS, ECP, OAB e ADS<br>IP del servizio virtuale: 2.2.2.1<br>Porte di servizio virtuali: 80, 443<br>Server reali: 127.1.1.1 127.2.2.2<br>flightPATH: aggiunge il reindirizzamento da HTTP a HTTPS |
| | jetPACK-2.2.3.1-Exchange-2013-Med-Resource | Questa configurazione usa un indirizzo IP unico per ogni servizio e quindi usa più risorse di quanto sopra. Deve configurare ogni servizio come voce DNS individuale Esempio owa.jetnexus.com, ews.jetnexus.com, ecc. Verrà aggiunto un monitor per ogni servizio e applicato al relativo servizio | Impostazioni globali:<br>Monitor: Monitor di livello 7 per OWA, EWS, OA, EAS, ECP, OAB, ADS, MAPI e PowerShell<br>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<br>Porte di servizio virtuali: 80, 443<br>Server reali: 127.1.1.1 127.2.2.2<br>flightPATH: aggiunge il reindirizzamento da HTTP a HTTPs |
| | jetPACK-2.2.2.3-Exchange2013-HIgh-Resource | Questo jetPACK aggiungerà un indirizzo IP unico e diversi servizi virtuali su porte diverse. flightPATH commuterà quindi il contesto in base al percorso di destinazione al servizio virtuale corretto. Questo | Impostazioni globali:<br>Monitor: Monitor di livello 7 per OWA, EWS, OA, EAS, ECP, OAB, ADS, MAPI e PowerShell<br>IP del servizio virtuale: 2.2.2.3 |

| | | |
|---|---|---|
| | jetPACK richiede la maggior quantità di CPU per eseguire la commutazione di contesto | Porte di servizio virtuali: 80, 443, 1, 2, 3, 4, 5, 6, 7<br>Server reali: 127.1.1.1 127.2.2.2<br>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 day - la GUI le chiederà di inserire la sua password ogni 20 minuti. Questa impostazione aumenterà quella 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
- Capture Size 16MB - la dimensione di cattura predefinita è di 2MB. Questo valore aumenterà la dimensione fino ad un massimo di 16MB

## Opzioni di cifratura

- Strong Ciphers - Questo aggiungerà la possibilità di scegliere "Strong Ciphers" dall'elenco 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 - aggiunga questa intestazione se non esiste e la imposti a "nosniff" - impedisce che il browser faccia automaticamente "MIME-Sniffing".
- X-Frame-Options - aggiunga questa intestazione se non esiste e la imposti su "SAMEORIGIN" - le pagine del suo sito possono essere incluse nei Frames, ma solo su altre pagine all'interno dello stesso sito.
- X-XSS-Protection - aggiunga questa intestazione se non esiste e la imposti a "1; mode=block" - abiliti le protezioni cross-site scripting del browser
- Strict-Transport-Security - aggiunga l'intestazione se non esiste e la imposti a "max-age=31536000 ; includeSubdomains" - assicura che il client debba onorare che tutti i link siano HTTPs:// per la max-age

## Applicare un jetPACK

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

- Vada su Avanzato > Aggiorna software
- Sezione di configurazione
- Caricare una nuova configurazione o jetPACK
- Cerca per jetPACK
- Clicchi su Upload
- Una volta che lo schermo del browser diventa bianco, clicchi su refresh e aspetti che appaia la pagina Dashboard

### Creare un jetPACK

Una delle cose grandiose di jetPACK è che può crearne di sue. Può darsi che lei abbia creato la configurazione perfetta per un'applicazione e voglia usarla per diverse altre scatole in modo indipendente.

- Cominci copiando la configurazione attuale dal suo ALB-X esistente
  - Advanced
  - Aggiornare il software
  - Scaricare la configurazione attuale
- Modifichi questo file con Notepad++
- Apra un nuovo documento txt e lo chiami "yourname-jetPACK1.txt".
- Copia tutte le sezioni rilevanti dal file di configurazione a "yourname-jetPACK1.txt".
- Salvi una volta completato

IMPORTANTE: ogni jetPACK è diviso in diverse sezioni, ma tutti i jetPACK devono avere #!jetpack in cima alla pagina.

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

### Sezione 0:

```
#!jetpack
```

Questa linea deve essere all'inizio del jetPACK, altrimenti la sua configurazione attuale verrà 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 verrà chiusa dopo 10 minuti di inattività

```
ContentServerCustomTimer=20000
```

Questo esempio è il ritardo in millisecondi tra i controlli di salute del content server 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". Questo particolare cambiamento è necessario 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]
Content="Server Up"
Desc="Monitor 1″
Method="CheckResponse"
Name="Health Check- Is Server Up"
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 suo 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="default"

ClientCertificateName="No SSL"

Comprimere=1

ConnectionLimiting=0

DSR=0

DSRProto="tcp"

Enabled=1

LoadBalancePolicy="CookieBased"

MaxConnections=10000

MonitoringPolicy="1″

PassThrough=0

Protocol="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="Forza l'uso di HTTPS per certe directory"
Name="Gary - Force HTTPS"
[jetnexusdaemon-Path-6-Condition-1]
Check="contain"
Condizione="percorso"
Match=
Senso="fa"
Value="/secure/"
[jetnexusdaemon-Path-6-Evaluate-1]
Dettaglio=
Fonte="host"
Valore=
Variabile="$host$"[jetnexusdaemon-Path-6-Function-1]
Action="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.

Sebbene alcuni componenti di flightPATH siano oggetti IP, come Source IP, flightPATH può essere applicato solo ad un **Tipo di Servizio** uguale a HTTP. Se sceglie qualsiasi altro tipo di servizio, la scheda flightPATH in IP Services sarà vuota.

Una regola flightPATH ha tre componenti:

| Opzione | Descrizione |
|---|---|
| Condizione | Impostare criteri multipli per attivare la regola flightPATH. |
| Valutazione | Permette l'uso di variabili che possono essere usate 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, veda questo utile sito https://www.regexbuddy.com/regex.html

Inoltre, si possono creare variabili personalizzate e usarle nell'area **Azione** consentendo molte possibilità diverse.

## Condizione

| Condizione | Descrizione | Esempio |
|---|---|---|
| <form> | I moduli HTML sono usati per passare dati ad 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 dropdown 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 usare IP multipli 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 | Controlli 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=jetNEXUS" Dove la corrispondenza è Best e il valore è edgeNEXUS |
| Stringa della query | L'intera stringa della query dopo il carattere ? | |
| Richiesta 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 di 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<br>, Proxy IP, Firewall IP. Può anche usare IP multipli e sottoreti. Deve<br>evitare i punti perché sono RegEX.<br>Esempio 10\.1\.2\.3 è 10.1.2.3 |

| **Match** | **Descrizione** | **Esempio** |
|---|---|---|
| Accetta | 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: en-US |
| Accept-Ranges | Quali tipi di intervallo di contenuto parziale supporta questo server | Accettazioni: bytes |
| Autorizzazione | Credenziali di autenticazione per l'autenticazione HTTP | Autorizzazione: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ== |
| Charge-To | Contiene informazioni sul conto dei costi dell'applicazione del metodo richiesto | |
| Content-Encoding | Il tipo di codifica usato sui dati. | Content-Encoding: gzip |
| Content-Length | La lunghezza del corpo della risposta in ottetti (byte da 8 bit) | Contenuto-Lunghezza: 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 email dell'utente che fa la richiesta | Da: user@example.com |
| If-Modified-Since | 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 | L'ultima data modificata per l'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 link alla pagina attualmente richiesta | Referrer: 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 utente | User-Agent: Mozilla/5.0 (compatibile; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0) |
| Vario | Dice ai proxy a valle come abbinare le future intestazioni di richiesta per decidere se<br>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 |

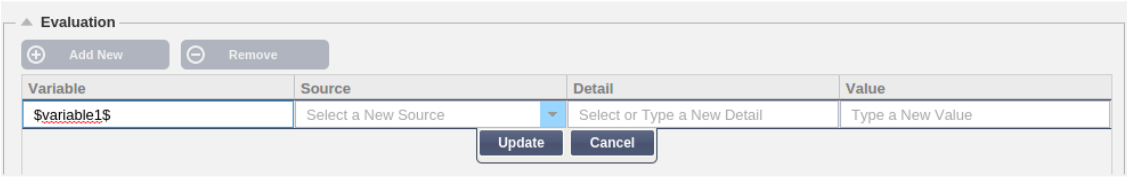
| **Controlli** | **Descrizione** | **Esempio** |
|---|---|---|
| Esiste | Questo non si preoccupa del dettaglio della condizione, solo che esiste/non esiste | Host - Does - Exist |
| Iniziare | La stringa inizia con il valore | Path - Does - Start - /secure |
| Fine | La stringa finisce con il valore | Percorso - Fa - Fine - .jpg |
| Contiene | La stringa contiene il valore | Intestazione della richiesta - Accept - Does - Contain - image |

| | | |
|---|---|---|
| Uguale | La stringa equivale al valore | Host - Does - Equal - www.jetnexus.com |
| Abbia Lunghezza | La stringa ha la lunghezza del valore | Host - Does - Have Length - 16www.jetnexus.com = TRUEwww.jetnexus.co.uk = FALSE |
| Corrispondenza RegEx | Questo le permette di inserire un'espressione regolare completamente compatibile con Perl | Origin IP - Does - Match Regex - 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




Aggiungere una variabile è una caratteristica irresistibile che le permetterà di estrarre dati dalla richiesta e utilizzarli nelle Azioni. Per esempio, potrebbe registrare il nome utente o inviare un'email se c'è un problema di sicurezza.

- Variabile: Deve iniziare e finire con un simbolo $. Per esempio $variabile1$
- Fonte: Selezioni dalla casella a discesa la fonte della variabile
- Dettaglio: Selezionare dalla lista quando pertinente. Se il Source=Request Header, il Details potrebbe essere User-Agent
- Valore: Inserisca 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.
- Può usare una qualsiasi delle variabili elencate qui sotto nella sua 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 = Registra
  - 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 cliente da 154.3.22.14:3454 ha appena fatto una richiesta alla pagina wrong.html".

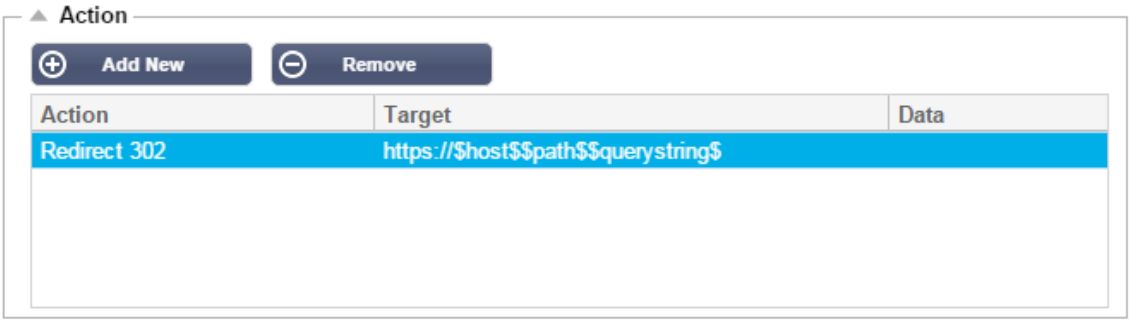
| Fonte | Descrizione | Esempio |
|---|---|---|
| Cookie | Questo è il nome e il valore dell'intestazione del cookie | MS-WSMAN=afYfn1CDqqCDqUD::Dove il nome è MS-WSMAN e il valore è afYfn1CDqCDqUD:: |
| Ospite | Questo è l'hostname estratto dall'URL | www.mywebsite.com o 192.168.1.1 |
| Lingua | Questa è la lingua estratta dall'intestazione HTTP Language | Questa condizione produrrà una discesa con una lista 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 | Controlli i dati che vengono caricati su un sito web |
| Voce di interrogazione | Questo è il nome e il valore di una query. Come tale può accettare il nome della query o un valore anche | "Best=jetNEXUS" Dove la corrispondenza è Best e il valore è edgeNEXUS |
| Stringa della query | Questa è l'intera stringa dopo il carattere ? | HTTP://server/path/programma?query_string |
| Intestazione della richiesta | Può essere qualsiasi intestazione inviata dal cliente | Referrer, User-Agent, From, Date... |
| Intestazione di risposta | 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 |
|---|---|---|
| Accetta | 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: en-US |
| Accept-Ranges | Quali tipi di intervallo di contenuto parziale supporta questo server | Accettazioni: bytes |

| | | |
|---|---|---|
| Autorizzazione | Credenziali di autenticazione per l'autenticazione HTTP | Autorizzazione: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ== |
| Charge-To | Contiene informazioni sul conto dei costi dell'applicazione del metodo richiesto | |
| Content-Encoding | Il tipo di codifica usato sui dati. | Content-Encoding: gzip |
| Content-Length | La lunghezza del corpo della risposta in ottetti (byte da 8 bit) | Contenuto-Lunghezza: 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 email dell'utente che fa la richiesta | Da: user@example.com |
| If-Modified-Since | 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 | L'ultima data modificata per l'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 link alla pagina attualmente richiesta | Referrer: 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 utente | User-Agent: Mozilla/5.0 (compatibile; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0) |
| Vario | 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 vengono attivati una volta che la condizione o le condizioni sono state soddisfatte.




### Azione

Clicchi due volte sulla colonna Azione per visualizzare l'elenco a discesa.

### Obiettivo

Clicchi due volte sulla colonna Target per visualizzare l'elenco a discesa. L'elenco cambierà a seconda dell'Azione.

Può anche digitare manualmente con alcune azioni.

### Dati

Clicchi due volte sulla colonna Dati per aggiungere manualmente i dati che desidera aggiungere o sostituire.

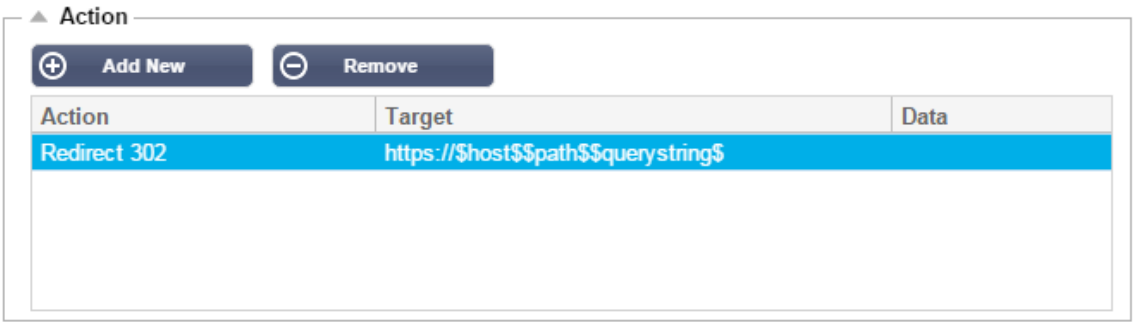
La lista di tutte le azioni è dettagliata qui sotto:

| Azione | Descrizione | Esempio |
|---|---|---|
| Aggiungere il cookie di richiesta | Aggiunga il cookie di richiesta dettagliato nella sezione Target con il valore nella sezione Data | Target= Cookie<br>Dati= MS-WSMAN=afYfn1CDqqCDqCVii |
| Aggiunga l'intestazione della richiesta | Aggiungere un'intestazione di richiesta di tipo Target con valore nella sezione Data | Target= Accetta<br>Data= image/png |
| Aggiunga un cookie di risposta | Aggiunga il Response Cookie dettagliato nella sezione Target con il valore nella sezione Data | Target= Cookie<br>Dati= MS-WSMAN=afYfn1CDqqCDqCVii |
| Aggiunga un'intestazione di risposta | Aggiunga un'intestazione di richiesta dettagliata nella sezione Target con valore nella sezione Data | Target= Cache-Control<br>Dati= max-age=8888888 |
| Corpo Sostituisci Tutto | Cerchi il corpo della risposta e sostituisca tutte le istanze | Target= HTTP:// (Stringa di ricerca)<br>Data= HTTPs:// (stringa di sostituzione) |
| Il corpo si sostituisce prima | Cerchi il corpo della risposta e sostituisca solo la prima istanza | Target= HTTP:// (Stringa di ricerca)<br>Data= HTTPs:// (stringa di sostituzione) |

| | | |
|---|---|---|
| Sostituire il corpo per ultimo | Cerchi il corpo della risposta e sostituisca solo l'ultima istanza | Target= HTTP:// (Stringa di ricerca)<br>Data= HTTPs:// (stringa di sostituzione) |
| Goccia | Questo farà cadere la connessione | Obiettivo= N/A<br>Dati= N/A |
| e-Mail | Invierà un'email all'indirizzo configurato in Eventi email. Può usare una variabile come indirizzo o come messaggio | Target= "flightPATH ha inviato questo evento per e-mail"<br>Dati= N/A |
| Evento di registro | Questo registrerà un evento nel registro di sistema | Target= "flightPATH ha registrato questo nel syslog"<br>Dati= N/A |
| Redirect 301 | Questo emetterà un reindirizzamento permanente | Target= HTTP://www.edgenexus.ioData= N/A |
| Redirect 302 | Questo emetterà un reindirizzamento temporaneo | Target= HTTP://www.edgenexus.ioData= N/A |
| Rimuova il cookie di richiesta | Rimuova il cookie di richiesta dettagliato nella sezione Target | Target= Cookie<br>Dati= MS-WSMAN=afYfn1CDqqCDqCVii |
| Rimuova l'intestazione della richiesta | Rimuova l'intestazione della richiesta dettagliata nella sezione Target | Target=ServerData=N/A |
| Rimuova il cookie di risposta | Rimuova il cookie di risposta dettagliato nella sezione Target | Target=jnAccel |
| Rimuova l'intestazione di risposta | Rimuova l'intestazione di risposta dettagliata nella sezione Target | Target= Etag<br>Dati= N/A |
| Sostituire il cookie della richiesta | Sostituisca il cookie di richiesta dettagliato nella sezione Target con il valore nella sezione Data | Target= Cookie<br>Dati= MS-WSMAN=afYfn1CDqqCDqCVii |
| Sostituisca l'intestazione della richiesta | Sostituisca l'intestazione della richiesta nel Target con il valore Data | Target= Connessione<br>Data= keep-alive |
| Sostituire il cookie di risposta | Sostituisca il cookie di risposta dettagliato nella sezione Target con il valore nella sezione Data | Target=jnAccel=afYfn1CDqqCDqCViiDate=MS-WSMAN=afYfn1CDqqCDqCVii |
| Sostituisca l'intestazione della risposta | Sostituisca l'intestazione di risposta dettagliata nella sezione Target con il valore nella sezione Data | Target= Server<br>Dati= Trattenuti per sicurezza |
| Riscrivere il percorso | Questo le permetterà di reindirizzare la richiesta a un nuovo URL in base alla condizione | Target= /test/path/index.html$querystring$<br>Dati= N/A |
| Usi un server sicuro | Selezioni quale server sicuro o servizio virtuale usare | Target=192.168.101: 443Data=N/A |
| Usi il server | Selezioni quale server o servizio virtuale usare | Target= 192.168.101:80Data= N/A |

| | | |
|---|---|---|
| Criptare il cookie | Questo cifrerà i cookie in 3DES e poi li codificherà in base64 | Target= Inserisca il nome del cookie da criptare, può usare * come carattere jolly alla fineData=<br>Inserisca una frase d'accesso per la criptazione |

Esempio:




L'azione sottostante emetterà un reindirizzamento temporaneo al browser verso un Servizio Virtuale HTTPS sicuro. Userà lo stesso hostname, percorso e querystring della richiesta.

## Usi comuni

### Firewall applicativo e sicurezza

- Blocca gli IP indesiderati
- Forzi 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 cartelle
- 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
- Corregga gli URL non funzionanti
- Log e Email Alert 404 codici di risposta
- Impedire l'accesso/la navigazione nelle directory
- Invii agli spider contenuti diversi

## Regole pre-costruite

### Estensione HTML

Cambia tutte le richieste .htm in .html

**Condizione:**

- Condizione = Percorso

- Senso = Fa
- Check = Match RegEx
- Valore = \x22.htm$

**Valutazione:**

- Vuoto

**Azione:**

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

### Indice.html

Forza ad usare 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

Rifiuta le richieste di cartelle.

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

- Condizione = questo richiede 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
- Target = /cgi-bin$path$

### Ragno di tronchi

Registri 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
- Match = 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 ad usare HTTPS per certe directory. In questo caso se un cliente accede a qualcosa che contiene la directory /secure/ verrà 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/$path$

### Scambi HTTP con HTTPS

Cambi ogni hardcoded HTTP:// in HTTPS://

**Condizione:**

- Condizione = Codice di risposta
- Senso = Fa
- Controllare = Uguale
- Valore = 200 OK

**Valutazione:**

- Vuoto

**Azione:**

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

### Svuotare le carte di credito

Controlli che non ci siano carte di credito nella risposta e se ne trova una, la cancelli.

**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

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

**Condizione:** questa è una condizione generica come catch all. Si raccomanda di concentrare questa condizione sul suo

- Condizione = Codice di risposta
- Senso = Fa
- Controllare = Uguale
- Valore = 200 OK

**Valutazione:**

- Vuoto

**Azione:**

- Azione = Aggiungi intestazione di risposta
- Target = Cache-Control
- Dati = max-age=3600

### Tipo di server spoof

Prenda il tipo di Server e lo cambi in qualcos'altro.

**Condizione:** questa è una condizione generica come catch all. Si raccomanda di concentrare questa condizione sul suo

- Condizione = Codice di risposta
- Senso = Fa
- Controllare = Uguale
- Valore = 200 OK

**Valutazione:**

- Vuoto

**Azione:**

- Azione = Sostituisci intestazione di risposta
- Obiettivo = Server
- Dati = Segreto

**Mai inviare errori**

Il cliente non riceve mai errori dal suo sito.

**Condizione**

- Condizione = Codice di risposta
- Senso = Fa
- Controllare = Contenere

- Valore = 404

**Valutazione**

- Vuoto

**Azione**

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

**Reindirizzamento sulla lingua**

Trovi il codice della lingua e reindirizzi 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**

Inserisca il codice richiesto da Google per l'analitica - Cambi il valore MYGOOGLECODE con il suo Google UA ID.

**Condizione**

- Condizione = Codice di risposta
- Senso = Fa
- Controllare = Uguale
- Valore = 200 OK

**Valutazione**

- vuoto

**Azione**

- Azione = Body Replace Last
- 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 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**

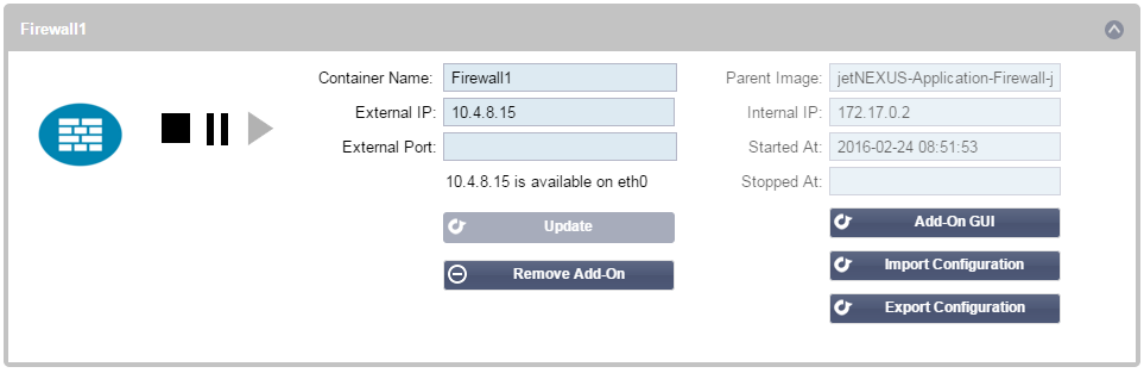
- Azione = Sostituire l'intestazione della richiesta
- Obiettivo = Host
- Dati =ipv4.host.header

# 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 effettuata utilizzando la sezione Apps integrata nell'ADC.

## Esecuzione del WAF

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

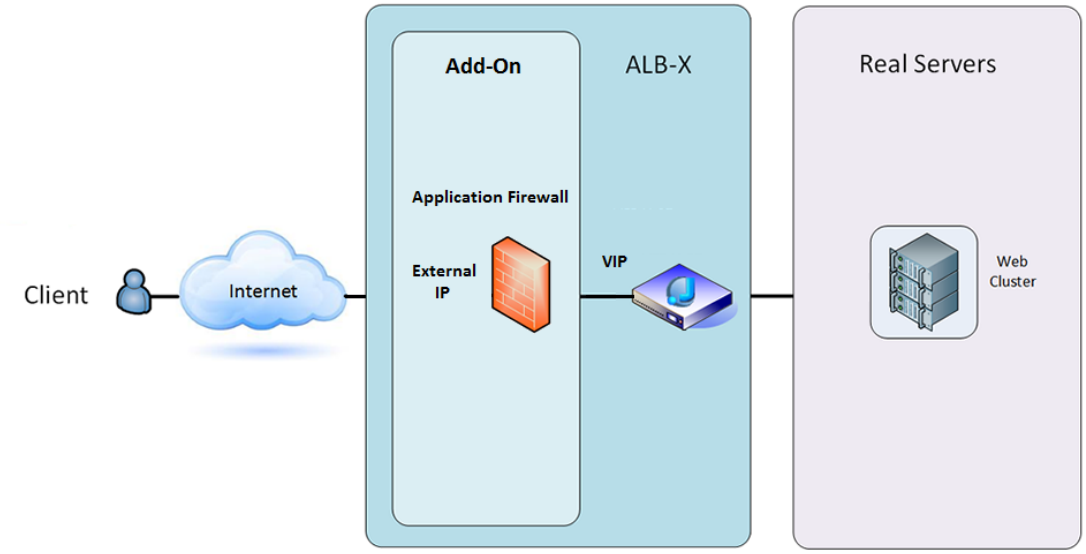



| Opzione | Descrizione |
|---|---|
| Si fermi | Rimarrà in grigio finché non verrà avviata un'istanza Add-On. Prema questo pulsante per fermare l'istanza Docker. |
| Pausa | Questo pulsante mette in pausa l'Add-On. |
| Gioca su | Avvierà l'Add-On con le impostazioni correnti. |
| Nome del contenitore | Dia un nome al suo contenitore per identificarlo dagli altri contenitori. Questo deve essere unico. Può usarlo come nome per un Real Server se lo desidera e si risolverà automaticamente all'indirizzo IP interno dell'istanza |
| IP esterno | Qui può impostare un IP esterno per accedere al suo Add-On. Questo può essere per accedere alla GUI dell'Add-On così come al servizio che gira tramite l'Add-On. Nel caso dell'Add-On Firewall questo è l'indirizzo IP del suo servizio HTTP. Il Firewall può quindi essere configurato per accedere ad un server o ad un VIP ALB-X che contiene più server per il bilanciamento del carico. |
| Porta esterna | Se lo lascia vuoto, tutte le porte saranno inoltrate al suo Firewall. Per limitarlo, aggiunga semplicemente l'elenco di porte separate da virgola. Esempio 80, 443, 88. Noti che l'indirizzo GUI del Firewall sarà **HTTP//[IP esterno]88/waf.** Quindi, lasci l'impostazione External Port vuota o aggiunga la porta 88 per accedere alla GUI se sta limitando la lista di porte. |
| Aggiornamenti | Può aggiornare le impostazioni di un Add-On solo dopo che è stato fermato. Una volta che la sua istanza si è fermata può cambiare il nome del contenitore, l'IP esterno e le impostazioni della porta esterna. |
| Rimuova l'Add-On | Rimuoverà completamente l'Add-On dalla pagina Add-On. Dovrà 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. Potrebbero esserci diverse versioni di un Firewall o addirittura un altro tipo di Add-On completamente, quindi questo aiuterà a distinguerle. Questa sezione è solo a scopo informativo e quindi è grigia. |

| | |
|---|---|
| IP interno | Docker crea automaticamente l'indirizzo IP interno e quindi non può essere modificato. Se ferma l'istanza Docker e la riavvia, verrà emesso un nuovo indirizzo IP interno. Per questo motivo deve usare un indirizzo IP esterno per il suo servizio o usare il nome del contenitore per l'indirizzo del server reale del suo servizio. |
| Iniziato a | Questo indicherà la data e l'ora in cui l'Add-On è stato avviato. Esempio 2016-02-16 155721 |
| Si è 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

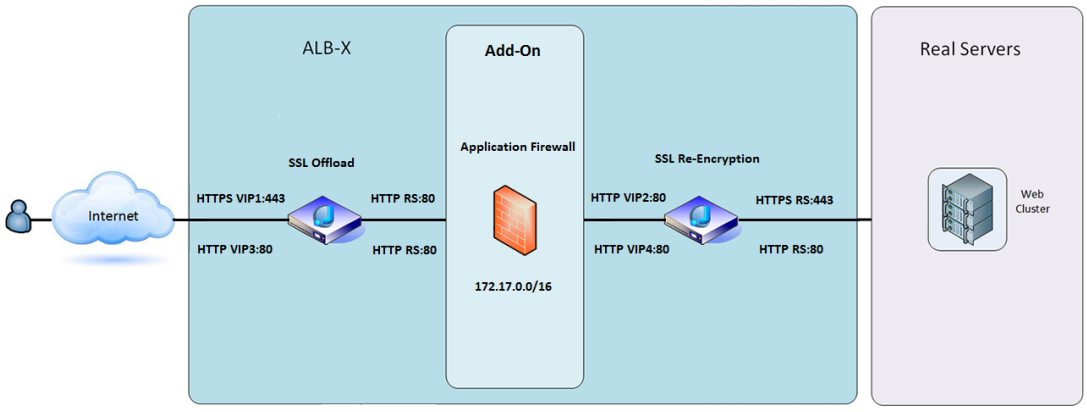



In questa architettura, solo HTTP può essere usato per il suo servizio poiché il Firewall non può ispezionare il traffico HTTPS.

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 suo cluster web.

### WAF usando l'indirizzo IP interno




In questa architettura può specificare HTTP e HTTPS.

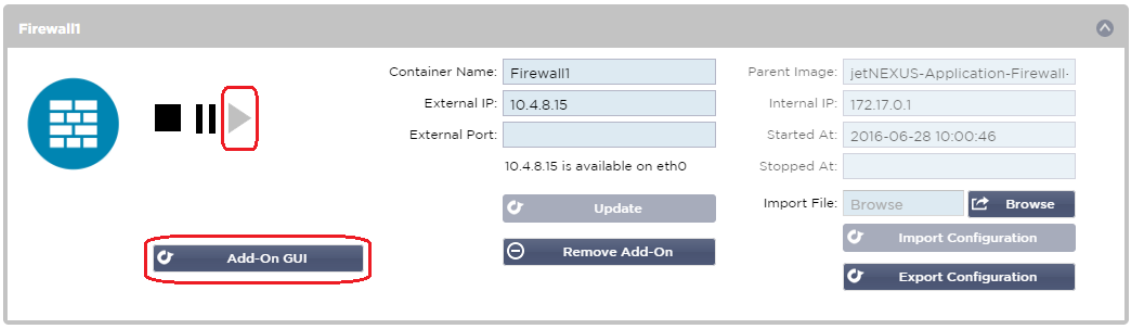
HTTPS può essere end-to-end dove le connessioni dal Client all'ALB-X sono criptate e dall'ALB-X ai Real Server.

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 inoltrato ad un altro VIP che può ricodificare il traffico e bilanciare il carico verso server sicuri o semplicemente bilanciare il carico verso server insicuri su HTTP.

## Accedere al suo componente aggiuntivo WAF

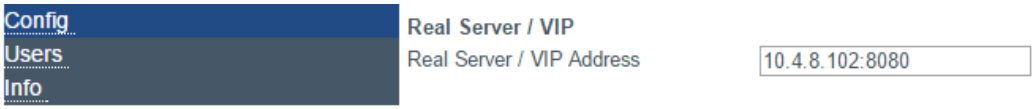
- Compili i dettagli del suo Firewall
- Può limitare le sue porte a ciò che le serve o lasciarlo vuoto per permettere tutte le porte
- Clicchi il pulsante Play
- Apparirà un pulsante GUI Add-On



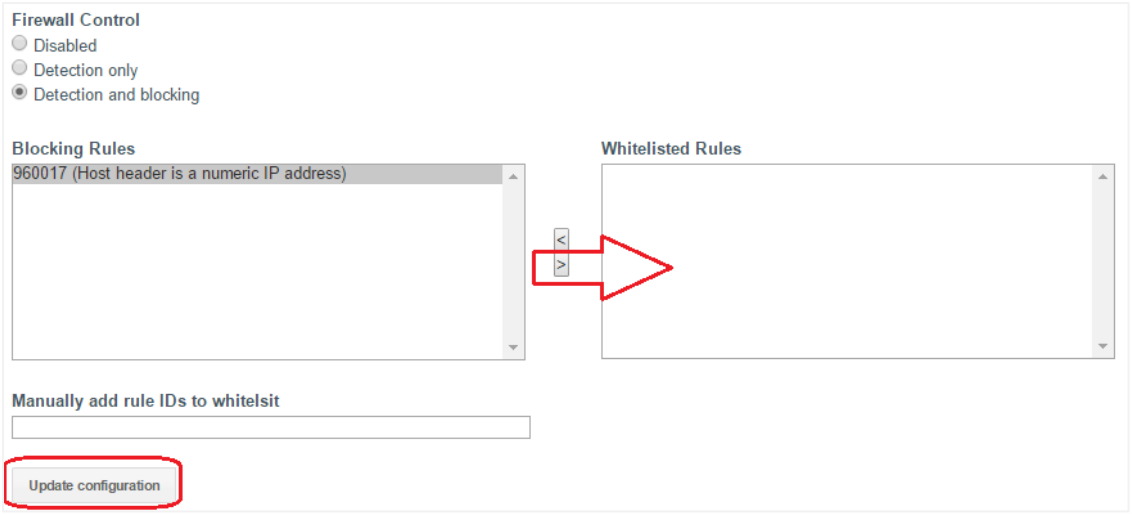

- Cliccando su questo pulsante, si aprirà un browser su HTTP://[IP esterno]:88/waf
- In questo esempio, sarà HTTP://10.4.8.15:88/waf
- Le verrà presentata una finestra di dialogo di login.
- Inserisca le credenziali del suo ADC.
- Una volta completato con successo il login, le verrà presentata la pagina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


- La pagina iniziale mostra una panoramica grafica degli eventi, cioè delle azioni di filtraggio eseguite da Application Firewall.
- Molto probabilmente i grafici saranno vuoti quando aprirà la pagina per la prima volta perché non ci saranno tentativi di accesso attraverso il firewall.

- Può configurare l'indirizzo IP o il nome di dominio del sito web a cui vuole inviare il traffico dopo che il firewall lo ha filtrato.
- Questo può essere cambiato nella sezione Gestione > Config



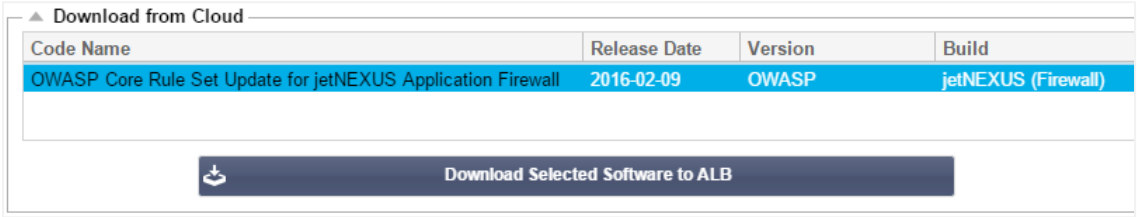

- Il Firewall ispezionerà il traffico e poi lo invierà al Real Sever IP o all'indirizzo VIP qui indicato. Può anche inserire una porta insieme all'indirizzo IP. Se inserisce un indirizzo IP da solo, si presume che la porta sia la porta 80. Clicchi il pulsante "Update Configuration" per salvare questa nuova impostazione.
- Quando il Firewall blocca una risorsa applicativa, 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, sposti la regola di blocco nella sezione Regole Whitelist.



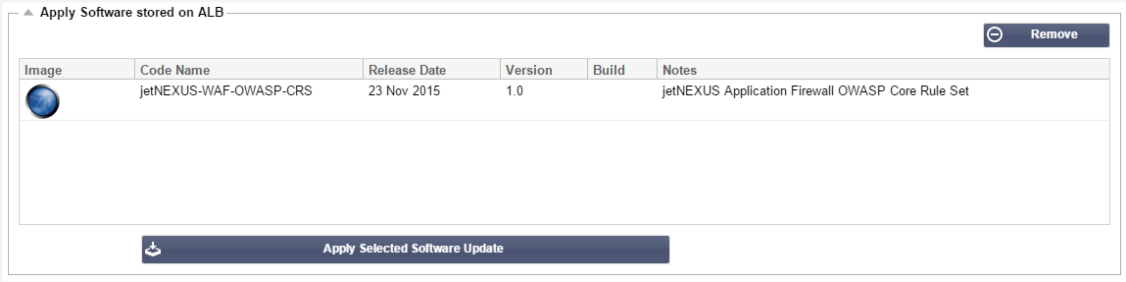

- Prema Update Configuration quando ha trasferito tutte le regole dalla sezione Blocking alla sezione Whitelist.

## Aggiornamento delle regole

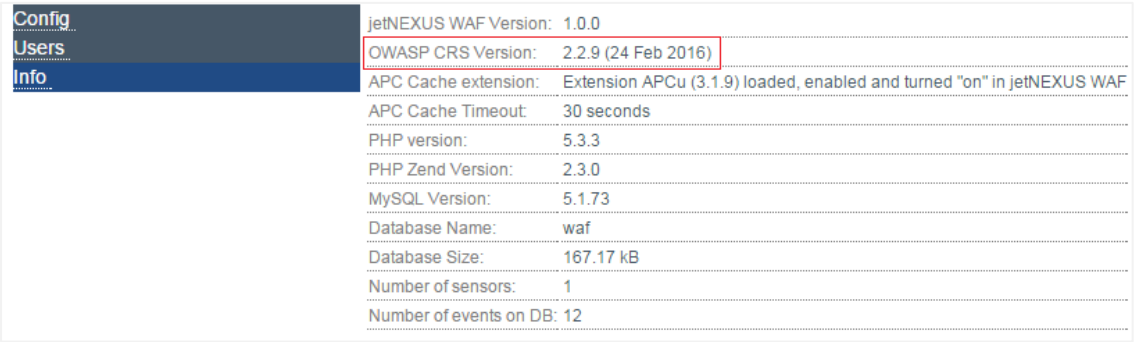
- Le regole di Application Firewall possono essere aggiornate accedendo alla sezione Advanced - Software
- Clicchi su Refresh per visualizzare il pulsante del software disponibile nella sezione Software Upgrade Details
- Viene ora visualizzata una casella aggiuntiva chiamata Download from Cloud
- Controlli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




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




- Evidenzi il jetNEXUS-WAF-OWASP-CRS e clicchi su Apply Selected Software Update e clicchi su Apply
- Il Firewall rileverà automaticamente il set di regole aggiornato, lo caricherà e lo applicherà.
- Gli ID delle regole Whitelisted saranno conservati. Tuttavia, le nuove regole possono iniziare a bloccare risorse di applicazioni valide.
- In questo caso controlli la lista delle Regole di Blocco nella pagina Whitelist.
- Può anche controllare nella sezione Management Info della GUI del Firewall 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), in quanto è usato tipicamente 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 si usa tipicamente nelle seguenti situazioni:

### Resilienza e disaster recovery

Lei ha più data center e desidera gestirli in una situazione Attiva-Passiva in modo che se un data center fallisce, il traffico venga inviato all'altro.

### Bilanciamento del carico e geo-localizzazione

Lei vorrebbe 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 dello stato di salute del data center e la posizione fisica del cliente (in modo da poterlo mandare al data center più vicino), ecc.

### Considerazioni commerciali

Assicurarsi che gli utenti di specifiche località geografiche siano inviati a particolari centri dati. Assicurarsi che vengano serviti (o bloccati) contenuti diversi ad altri utenti, a seconda di vari 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 consiste di 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: è il nameserver a cui il client si collega inizialmente per eseguire la risoluzione DNS.
- Server di nomi autoritativi: Includa i nameserver del Top Level Domain (TLD) e i nameserver di root.

### Una tipica transazione DNS è spiegata di seguito:

- Un utente digita 'example.com' in un browser web e la richiesta viaggia in Internet e viene ricevuta da un resolver DNS ricorsivo.
- Il resolver quindi interroga 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 viene 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 clienti. I resolver e le applicazioni lato client possono avere diverse politiche di caching.

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

### Tempo di vivere

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

## Panoramica di GSLB

GSLB si basa su DNS e usa 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 di 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 utilizza un sottodominio. Il server DNS autoritativo primario non viene sostituito da GSLB ma delega un sottodominio per la risoluzione. Delegare direttamente i nomi o usare i CNAME le permette di controllare cosa viene e non viene gestito da GSLB. In questo caso non deve 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 ad un altro GSLB, evitando che il sito vada giù.

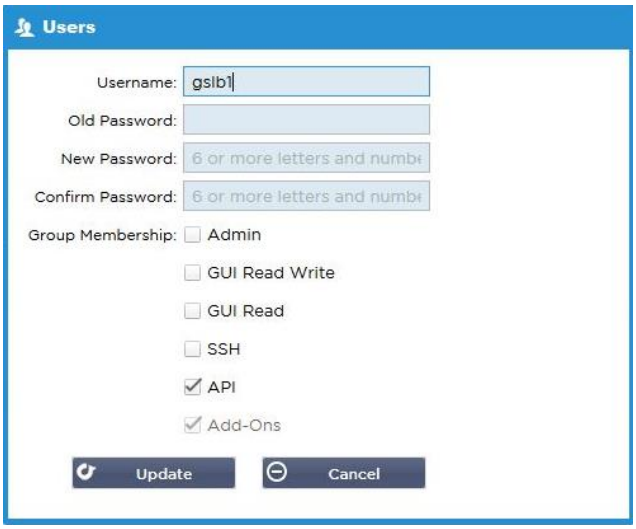
## Configurazione GSLB

Dopo aver scaricato il GSLB Add-On, lo distribuisca visitando la pagina Library > Apps di ADC GUI e cliccando il pulsante "Deploy" come mostrato qui sotto.

Dopo l'installazione, configuri i dettagli di GSLB Add-On, incluso il nome del contenitore, l'IP esterno e le porte esterne nella pagina Library > Add-Ons di ADC GUI come mostrato nella figura sottostante.

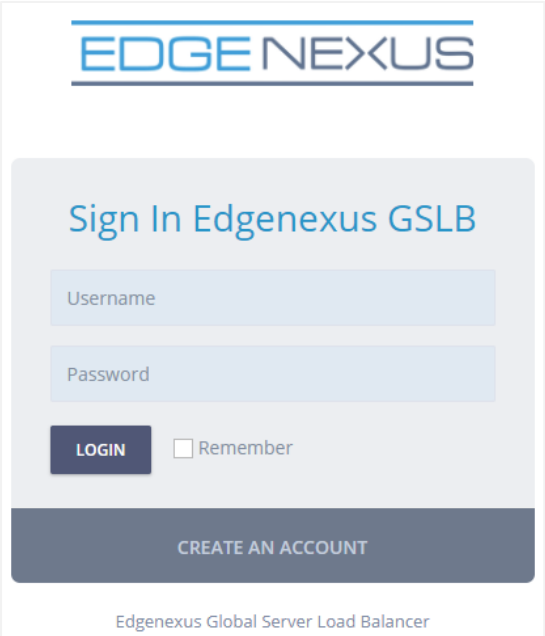
- Container Name è un nome unico di un'istanza di Add-On in esecuzione, ospitata da ADC, si usa per distinguere più Add-On di uno stesso tipo.
- IP esterno è l'IP della sua rete che sarà assegnato a GSLB.
- Deve configurare il GSLB per avere un indirizzo IP esterno se vuole prendere decisioni basate su GEO, perché questo permetterà al GSLB di visualizzare il vero indirizzo IP dei clienti.
- External Ports è la lista delle porte TCP e UDP di GSLB a cui si può accedere da altri host di rete.
- Metta "53/UDP, 53/TCP, 9393/TCP" nella casella di input External Ports per permettere le comunicazioni DNS (53/UDP, 53/TCP) e edgeNEXUS GSLB GUI (9393/TCP).
- Dopo aver configurato i dettagli dell'Add-On, clicchi sul pulsante Update.
- Avvii il GSLB Add-On cliccando il pulsante Run.


- Il passo successivo è permettere all'edgeNEXUS GSLB Add-On di leggere e cambiare la configurazione ADC.
- Visiti la pagina Sistema > Utenti di ADC GUI e modifichi un utente con lo stesso nome del GSLB Add-On che ha distribuito, come mostrato nella figura sottostante.
- Modifichi l'utente "gslb1" e spunti API, poi clicchi su Update - nelle versioni successive del software potrebbe essere già spuntato di default.



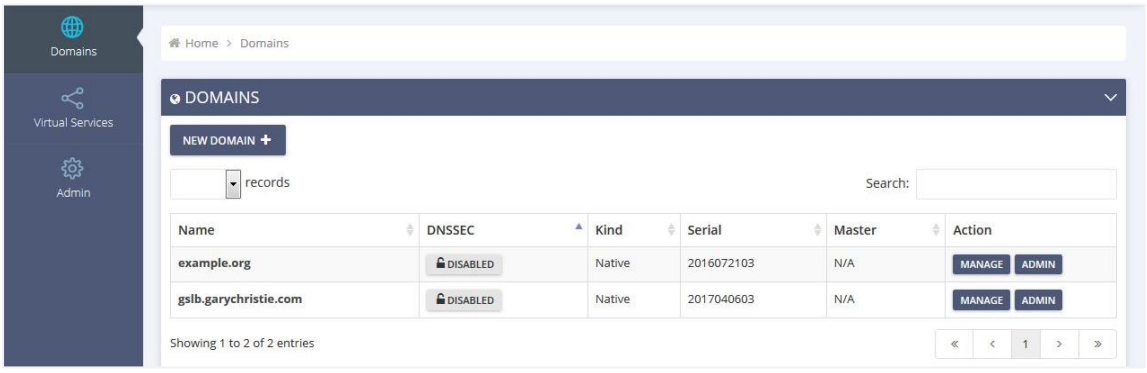

- Il prossimo passo è necessario solo se sta configurando GSLB per scopi di test o valutazione e non vuole modificare i dati delle zone DNS su Internet.
- In questo caso, ordini all'ADC di usare GSLB Add-On come server primario di risoluzione DNS modificando "DNS Server 1 nella pagina Sistema > Rete dell'ADC GUI, come mostrato nella figura sottostante.
- DNS Server 2 può essere configurato generalmente con il suo server DNS locale o uno su Internet, come Google 8.8.8.8.


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



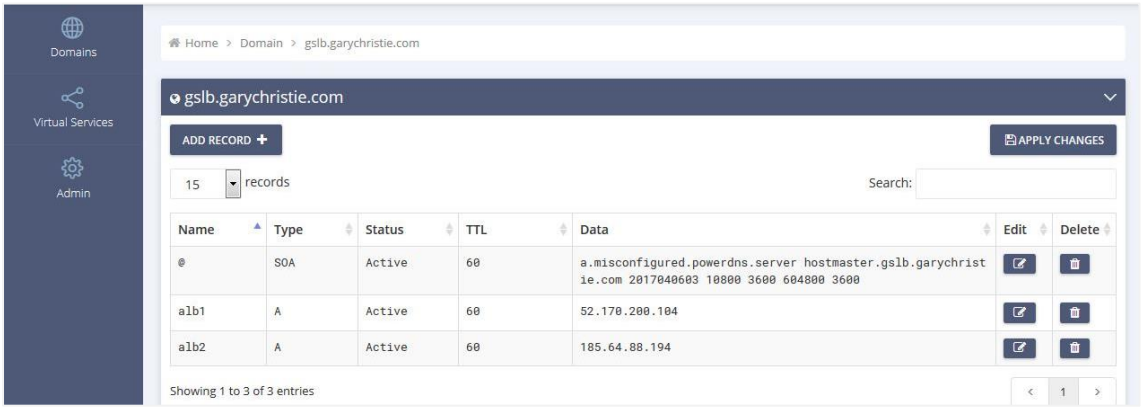

- Il nome utente predefinito è admin e la password predefinita è jetnexus. Non dimentichi di cambiare la password nella pagina Amministratore > Il mio profilo di GSLB GUI.
- Il passo successivo nella sequenza di configurazione è creare una zona DNS nel nameserver PowerDNS, che fa parte di GSLB, rendendolo 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".
- Per dettagli approfonditi sulla configurazione delle zone DNS, veda la **DOCUMENTAZIONE DI POWERDNS NAMESERVER**. Un esempio di zona è mostrato nella Figura 6.

* edgeNEXUS GSLB GUI si basa su un progetto Open Source PowerDNS-Admin.

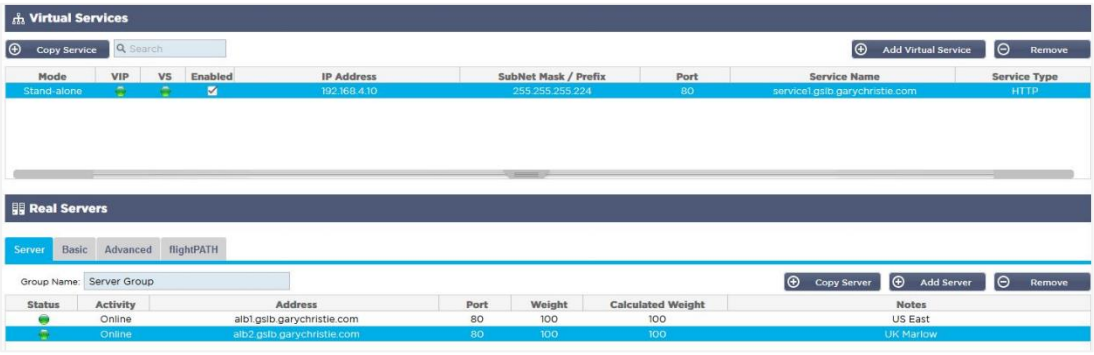



- Dopo aver creato una zona DNS, clicchi sul pulsante Manage e aggiunga hostname al dominio, come mostrato nella figura sottostante.
- Dopo aver modificato qualsiasi record esistente all'interno della GUI GSLB, prema il pulsante Salva.

- Dopo aver completato la creazione dei record di hostname, clicchi sul pulsante Apply Changes. Se non clicca Applica e poi modifica la pagina, perderà le sue modifiche.
- Di seguito abbiamo creato dei record che sono record di indirizzi IPv4.
- Si assicuri di creare un record per tutti i record che desidera far risolvere, compresi i record AAAA per gli indirizzi IPv6.

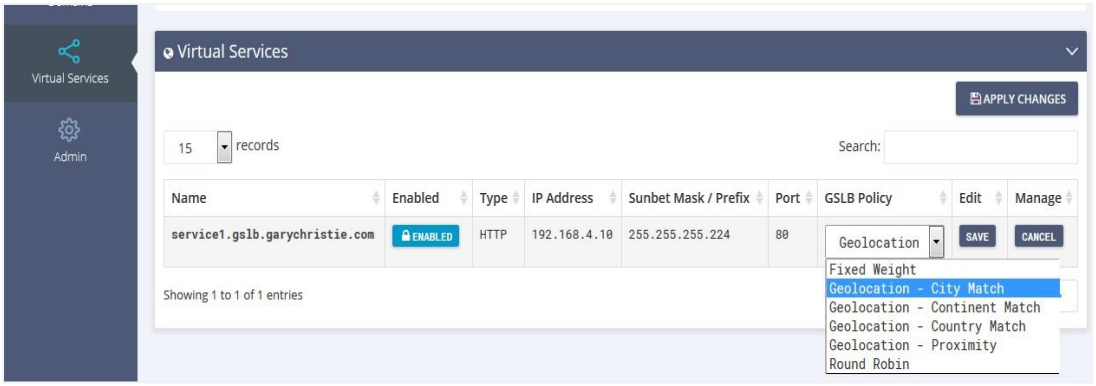



- Ora torniamo alla GUI ADC e definiamo un Servizio Virtuale che corrisponde alla zona DNS che abbiamo appena creato.




- Il servizio virtuale sarà usato 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 usato con qualsiasi tipo di servizio supportato dall'ADC.
- Vada alla pagina Servizi > Servizi IP della GUI ADC e crei un Servizio Virtuale, come mostrato nella figura sottostante.
- Si assicuri di configurare il Service Name con il nome di dominio corretto che desidera usare nel GSLB. GSLB lo leggerà tramite l'API e popolerà automaticamente la sezione Virtual Services nella GUI di GSLB.
- Aggiunga tutti i server nel dominio GSLB sotto la sezione Real Servers dell'immagine sopra.
- Può specificare i server, sia per i loro nomi di dominio che per gli indirizzi IP.
- Se specifica i nomi di dominio, allora userà i record creati sul suo GSLB.
- Può scegliere diversi metodi e parametri di monitoraggio della salute del server nelle schede Basic e Advanced.
- Può 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 in un indirizzo del server Standby.
- Faccia riferimento alla sezione **SERVIZI VIRTUALI** per i dettagli sulla configurazione dei Servizi Virtuali.
- Ora passiamo alla GUI di GSLB.
- Vada alla pagina Servizi virtuali e selezioni una policy GSLB per il dominio dell'API recuperato dalla sezione Servizi virtuali ADC.

- Questo è mostrato nella figura sottostante.




- Il GSLB sostiene le seguenti politiche:

| Politica | Descrizione |
|---|---|
| Peso fisso | 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 seleziona uno di questi server a caso. |
| Round Robin ponderato | Scelga i server uno per uno, in fila. I server che hanno pesi maggiori vengono selezionati più spesso dei server che hanno pesi minori. |
| Geolocalizzazione | Prossimità - sceglie un server che si trova più vicino alla posizione del cliente usando 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 - sceglie un server nella stessa città del cliente. Se non c'è un server nella città del cliente, selezioni un server nel paese del cliente. Se non c'è un server nel paese del cliente, selezioni un server nello stesso continente. Se questo non è possibile, selezioni un server che si trova più vicino alla posizione del cliente usando i dati geografici di latitudine e longitudine. |
| Geolocalizzazione | Corrispondenza paese - sceglie un server nello stesso paese del cliente. Se non c'è un server nello stesso paese, provi con lo stesso continente, poi provi con la località più vicina. |
| Geolocalizzazione | Continent match - sceglie un server nello stesso continente del cliente. Se non c'è un server nello stesso continente, provi la località più vicina. |

- Dopo aver selezionato una GSLB Policy, non dimentichi di cliccare sul pulsante Apply Changes.
- Ora può rivedere e regolare i dettagli del Servizio Virtuale cliccando sul pulsante Gestisci.
- Questo presenterà la pagina mostrata qui sotto.
- Se ha selezionato una delle politiche basate sul peso, potrebbe dover regolare i pesi GSLB del server.
- Se ha selezionato una delle politiche GSLB basate sulla geo-localizzazione, potrebbe dover specificare i dati geografici dei server.
- Se non specifica alcun dato geografico per i server, GSLB userà i dati forniti dal **DATABASE GEOLITE2 DI MAXMIND**.
- Può anche modificare il nome del server, la porta e l'attività in questa pagina.
- Queste modifiche saranno sincronizzate con l'ADC quando cliccherà sul pulsante "Apply Changes".

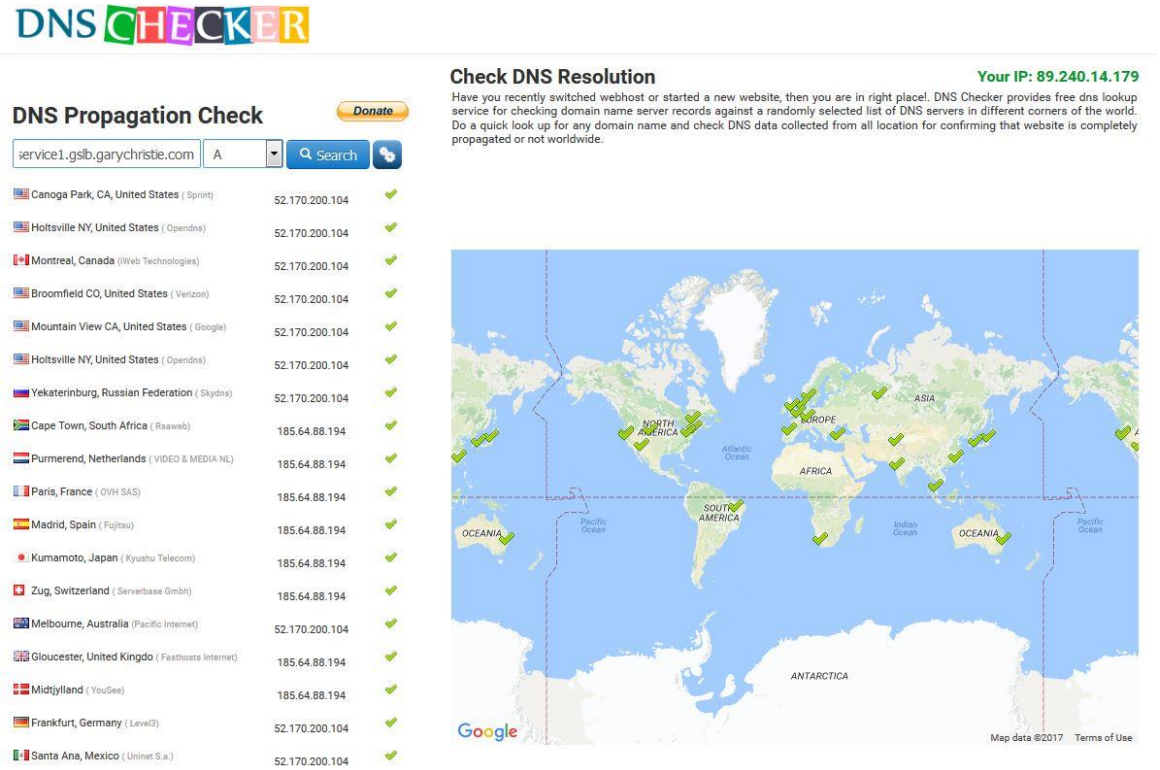

- Un ottimo modo per controllare quali risposte il GSLB rimanda ai clienti è usare NSLOOKUP.
- Se sta usando Windows, il comando è qui sotto.

  NSLOOKUP service1.gslb.garychristie.com 192.168.4.10

- Dove service1.gslb.garychristie.com è il nome di dominio che desidera risolvere.
- Dove 192.168.4.10 è l'indirizzo IP esterno del suo GSLB.
- Per controllare quale indirizzo IP verrà restituito su internet, può usare il server DNS di Google 8.8.8.8.

  Nslookup service1.gslb.garychristie.com 8.8.8.8.

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




## Luoghi personalizzati

### Reti private

La GSLB può anche essere configurata per usare posizioni personalizzate in modo da poterla usare su reti interne "private". Nello scenario di cui sopra, il GSLB determina la posizione del cliente incrociando

l'indirizzo IP pubblico del cliente con un database per determinare la sua posizione. Calcola anche la posizione dell'indirizzo IP del servizio dalla stessa banca dati 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 esiste una banca dati simile per gli indirizzi privati interni conformi a RFC 1918 per gli indirizzi IPv4 e RFC 4193 per gli indirizzi IPv6.

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

## Come funziona

Tipicamente, l'idea alla base dell'uso del nostro GSLB per le reti interne è che gli utenti di indirizzi specifici ricevano 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, sempre che il servizio funzioni correttamente.

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

- Dobbiamo avere almeno due località personalizzate, una per ogni data-center
- Assegni le varie reti private a queste posizioni
- Assegni ogni servizio alla rispettiva sede

## Come configuriamo questo aspetto sul GSLB?

### Aggiunga una posizione per il Centro Dati Nord

- Clicchi su Posizioni personalizzate sul lato sinistro
- Clicchi su Aggiungi posizione
- Nome
  - Nord
- Aggiunga un indirizzo IP privato e una subnet mask per la sua rete Northern. Per questo esercizio, assumeremo che il servizio e gli indirizzi IP del cliente siano nella stessa rete privata
  - 10.1.1.0/24
- Aggiunga il codice del continente
  - UE
- Aggiunga il codice paese
  - UK
- Aggiunga la città
  - Enfield
- Aggiunga la latitudine - ottenuta da google
  - 51.6523
- Aggiunga la longitudine - ottenuta da google
  - 0.0807

Nota, per favore usi il codice corretto che può essere ottenuto da qui

### Aggiunga una posizione per il Centro Dati Sud

- Clicchi su Posizioni personalizzate sul lato sinistro
- Clicchi su Aggiungi posizione
- Nome
  - Sud
- Aggiunga un indirizzo IP privato e una subnet mask per la sua rete Sud. Assumeremo che il servizio e gli indirizzi IP del cliente siano nella stessa rete privata per questo esercizio.

    - 192.168.1.0/24
- Aggiunga il codice del continente
    - UE
- Aggiunga il codice paese
    - UK
- Aggiunga la città
    - Croydon
- Aggiunga la latitudine - ottenuta da google
    - 51.3762
- Aggiunga la longitudine - ottenuta da google
    - 0.0982

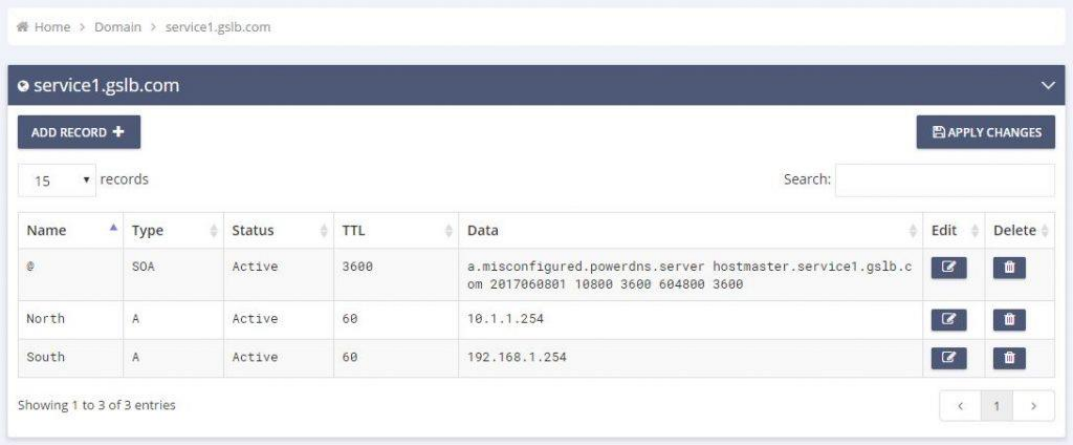
Nota, per favore usi il codice corretto che può essere ottenuto da QUI


### Aggiungere un record A per north.service1.gslb.com

- Clicchi sul dominio service1.gslb.com
- Clicchi su Aggiungi record
- Aggiungere nome
    - Nord
- Tipo
    - A
- Stato
    - Attivo
- TTL
    - 1 minuto
- Indirizzo IP
    - 10.1.1.254 (Notare che si trova nella stessa rete della località Enfield)

### Aggiungere un record A per south.service1.gslb.com

- Clicchi sul dominio service1.gslb.com
- Clicchi su Aggiungi record
- Aggiungere nome
    - Sud
- Tipo
    - A
- Stato
    - Attivo
- TTL
    - 1 minuto
- Indirizzo IP
    - 192.168.1.254 (Notare che è nella stessa rete della località Croydon)




## Flusso di traffico

Esempio 1 - Cliente in un Data-Center 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 a Custom Location 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

- IP cliente 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 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.

Le forniremo tutto il supporto tramite l'assistenza tecnica se ha un contratto di Supporto e Manutenzione attivo per edgeADC, edgeWAF o edgeGSLB.

Per sollevare un ticket di supporto, visiti il sito:

https://www.edgenexus.io/support/