
EDGE
NEXUS

EdgeADC

Guida all'amministrazione di EdgeADC

VERSIONE SOFTWARE

5.0.0

Contenuti

Proprietà del documento.....	12
Dichiarazione di non responsabilità del documento.....	12
Diritti d'autore.....	12
Marchi di fabbrica.....	12
Supporto Edgenexus.....	12
Introduzione.....	13
Lo scopo di questo documento	13
A chi è destinato questo documento?	13
Bilanciamento del carico 101	14
Che cos'è un Load Balancer o ADC?	15
Spiegazione dei VIP e dei servizi virtuali (VS).....	16
Che cos'è un tipo di servizio di bilanciamento del carico?	18
L'inizio del viaggio	20
Scaricare l'EdgeADC.....	21
Installazione	22
Installazione dell'EdgeADC.....	23
Installazione su VMware ESXi	23
Installazione dell'interfaccia VMXNET3	24
Installazione su Microsoft Hyper-V	24
Installazione su Citrix XenServer	26
Installazione su KVM.....	26
Requisiti e versioni	26
Installazione su Nutanix AHV	29
Requisiti e versioni	29
Installazione su ProxMox	30
Caricamento dell'OVA su ProxMox.....	31
Configurazione del primo avvio.....	33
Primo avvio - Dettagli di rete manuali.....	33
Primo avvio - DHCP riuscito.....	33
Primo avvio - DHCP fallisce	33
Modifica dell'indirizzo IP di gestione.....	34
Modifica della maschera di sottorete per eth0	34
Assegnazione di un gateway predefinito	34
Verifica del valore del gateway predefinito	34
Accesso all'interfaccia web	34
Tabella di riferimento dei comandi	35

La Console Web.....	36
Avvio della Console Web ADC	37
Credenziali di accesso predefinite.....	37
Utilizzo di un servizio di autenticazione esterno	37
Il cruscotto principale.....	38
Servizi	39
Servizi IP.....	40
Servizi virtuali.....	40
Creazione di un nuovo servizio virtuale utilizzando un nuovo VIP	40
Esempio di servizio virtuale completato	41
Come utilizzare Monitor End Point.....	42
Creazione di servizi secondari virtuali	42
Modifica dell'indirizzo IP di un servizio virtuale	43
Creare un nuovo servizio virtuale utilizzando Copy Service	43
Filtrare i dati visualizzati	44
Ricerca di un termine specifico	44
Selezione della visibilità delle colonne	44
Informazioni sulle colonne dei servizi virtuali.....	44
Primario/Modalità.....	44
VIP	44
Abilitato	45
Indirizzo IP.....	45
Maschera di sottorete/Prefisso	45
Porto.....	45
Nome del servizio.....	45
Tipo di servizio	45
Server reali	46
Server.....	46
Base.....	49
Avanzato	55
voloPATH	60
Modifiche al server reale per il ritorno al server diretto.....	61
Configurazione del server dei contenuti richiesta	61
Generale	61
Finestre	61
Linux.....	62
Modifiche al server reale - Modalità gateway.....	63
Configurazione del server dei contenuti richiesta	63

Esempio di braccio singolo	63
Esempio di braccio doppio.....	64
Biblioteca.....	65
Componenti aggiuntivi	66
Applicazioni	67
Il filtro.....	67
Applicazioni scaricate	67
App acquistata.....	67
Distribuire	68
Scarica l'applicazione	68
Cancellare	68
Autenticazione	69
Impostazione dell'autenticazione - Un flusso di lavoro	69
Server di autenticazione.....	69
Opzioni per LDAP, LDAP-MD5, LSAPS, LDAPS-MD5, Radius e SAML	69
Opzioni per l'autenticazione SAML	70
Regni KDC.....	72
Regole di autenticazione.....	72
Moduli	73
Cache.....	76
Impostazioni globali della cache	76
Applicare la regola della cache	77
Creare una regola della cache	77
voloPATH	79
Dettagli	79
Aggiunta di una nuova regola flightPATH.....	79
Condizione	80
Valutazione.....	83
Azione	84
Uno scenario di regole flightPATH.....	86
Applicazione della regola flightPATH	87
Monitor di server reali	89
Tipi di monitor per server reali	89
Dettagli	93
Esempi di Real Server Monitor	94
Certificati SSL.....	98
Cosa fa l'ADC con il certificato SSL?.....	98
Il gestore della configurazione SSL.....	98

L'area di elencazione dei certificati	98
I pulsanti di azione e le aree di configurazione	99
Panoramica	100
Crea richiesta	100
Rinominare	102
Cancellare	102
Installazione/Segnalazione	103
Rinnovare	103
Convalida del certificato.....	104
Aggiunta di intermedi.....	105
Riordino	105
Importazione/Esportazione	107
Backup e ripristino	107
Backup	107
Ripristino	107
Widget	109
Widget configurati	109
Widget disponibili	109
Il widget Eventi	109
Il widget Grafici di sistema	110
Widget dell'interfaccia.....	111
Widget di stato.....	111
Widget di grafica del traffico	111
Vista	114
Cruscotto	115
Utilizzo del cruscotto	115
Il menu dei widget.....	115
Pulsante Pausa dati in tempo reale	115
Pulsante del cruscotto predefinito	115
Ridimensionamento, minimizzazione, riordino e rimozione dei widget.....	116
La storia	117
Visualizzazione dei dati grafici	117
Registri	119
Registri W3C	119
Registro di sistema	119
Statistiche.....	120
Compressione.....	120
Compressione dei contenuti fino ad oggi	120

Compressione complessiva ad oggi	120
Totale ingressi/uscite	120
Colpi e connessioni	120
Numero complessivo di visite conteggiate	121
Connessioni totali	121
Connessioni di picco	121
Caching	121
Dalla Cache	121
Da Server	121
Contenuto della cache	121
Buffer dell'applicazione	122
Persistenza della sessione	122
Totale sessioni correnti	122
% Utilizzato (di max)	122
Nuova sessione questo min	122
Riconvalidare questo min	122
Sessioni scadute questo min	122
Hardware	122
Utilizzo del disco	123
Utilizzo della memoria	123
Utilizzo della CPU	123
Stato	124
Dettagli del servizio virtuale	124
Colonna VIP	124
Colonna Stato VS	124
Nome	124
Servizio virtuale (VIP)	124
Colpo/Sec	125
Cache%	125
Compressione%	125
Stato RS (Server remoto)	125
Server reale	125
Note	125
Conns (Connessioni)	125
Dati	125
Req/Sec (Richieste al secondo)	125
Sistema	126
Raggruppamento	127

Ruolo	127
Cluster.....	127
Ruolo manuale	129
Ruolo autonomo	129
Impostazioni.....	130
Latenza di failover (ms)	130
Messaggistica in Failover	130
Gestione	130
Aggiunta di un ADC al cluster	131
Aggiunta manuale di un ADC al cluster	131
Rimozione di un membro del cluster.....	132
Modifica della priorità di un ADC.....	132
Data e ora.....	134
Data e ora manuali.....	134
Fuso orario	134
Impostare data e ora	134
Sincronizzare data e ora (UTC).....	134
URL del server temporale.....	135
Aggiornamento a [hh:mm]	135
Periodo di aggiornamento [ore]:.....	135
NTP Tipo:	135
Eventi via e-mail	136
Indirizzo	136
Inviare agli eventi via e-mail agli indirizzi e-mail.....	136
Indirizzo e-mail di ritorno:.....	136
Server di posta (SMTP).....	136
Indirizzo dell'host.....	136
Porto.....	136
Timeout di invio	136
Utilizzare l'autenticazione	137
Sicurezza	137
Nome account del server principale.....	137
Password del server di posta.....	137
Notifiche e avvisi.....	137
Avviso di servizio IP.....	137
Avviso di servizio virtuale.....	137
Avviso di server reale	137
voloPATH	137

Raggruppare le notifiche.....	137
Descrizione della posta di gruppo.....	138
Intervallo di invio del gruppo.....	138
Avvertenze e descrizioni degli eventi attivate in Mail.....	138
Spazio su disco.....	138
Avvisa se lo spazio libero è inferiore a.....	138
Scadenza della licenza.....	138
La storia.....	139
Raccogliere i dati.....	139
Abilitazione.....	139
Raccogliere dati ogni.....	139
Manutenzione.....	139
Aggiornamento più recente.....	139
ADC aziendali HP.....	139
Backup.....	139
Cancellare.....	140
Ripristino.....	140
Licenza.....	141
Dettagli della licenza.....	141
ID licenza.....	141
ID macchina.....	141
Rilasciato a.....	141
Persona di contatto.....	141
Data di emissione.....	141
Nome.....	142
Strutture.....	142
Installare la licenza.....	142
Informazioni sul servizio di licenza.....	143
Registrazione.....	144
Dettagli di registrazione W3C.....	144
Livelli di registrazione W3C.....	144
Includere la registrazione W3C.....	145
Includere informazioni sulla sicurezza.....	145
Server Syslog.....	145
Server Syslog remoto.....	146
Archiviazione remota dei registri.....	146
Riepilogo del campo.....	146
Cancellare i file di registro.....	148

Rete.....	149
Gestione delle interfacce di rete virtuali in un ambiente virtuale	149
Considerazioni chiave	149
Passi consigliati per la configurazione dell'host	149
Scenario di esempio	149
Evitare il vMotion frequente per le appliance critiche.....	150
Perché il vMotion frequente non è consigliato.....	150
Raccomandazioni per la gestione delle apparecchiature critiche	150
Impostazione di base	151
Nome ALB.....	151
Gateway IPv4.....	151
Gateway IPv6.....	151
Server DNS 1 e Server DNS 2.....	151
Dettagli sull'adattatore.....	151
Interfacce	152
Legame.....	153
Creazione di un profilo di legame	153
Modalità di legame	154
Percorso statico	154
Aggiunta di una rotta statica	154
Dettagli della rotta statica	155
Impostazioni di rete avanzate.....	155
Che cos'è Nagle?	155
Server Nagle	155
Cliente Nagle.....	155
SNAT	155
Potenza	157
Riavvio.....	157
Riavvio.....	157
Spegnimento.....	157
Sicurezza	158
SSH	158
Servizio di autenticazione	158
Console web	159
API REST	159
Documentazione per l'API REST.....	159
SNMP.....	161
Impostazioni SNMP	161

MIB SNMP	161
Scarica la MIB	161
OID ADC	161
Grafici storici.....	162
Utenti e registri di audit.....	163
Utenti	163
Aggiungi utente	163
Tipo di utente.....	164
Rimozione di un utente	164
Modifica di un utente	165
Registro di controllo	165
Avanzato	166
Configurazione	167
Scaricare una configurazione	167
Caricamento di una configurazione	167
Caricare un JetPACK	167
Impostazioni globali	168
App Store Download Proxy	168
URL proxy HTTP	168
Nome utente del proxy HTTP	168
Password del proxy HTTP	168
Timer cache host	168
Drenaggio	169
SSL.....	169
Autenticazione	170
Impostazione Failover.....	170
Protocollo	171
Server troppo occupato.....	171
Inoltrata per.....	171
Uscita inoltrata.....	171
Intestazione Forwarded-For.....	171
Registrazione avanzata per IIS - Registrazione personalizzata	172
Modifiche di Apache HTTPd.conf	172
Impostazioni di compressione HTTP	173
Esclusioni della compressione globale	174
Cookie di persistenza.....	174
Reset timeout UDP	175
Software	176

Dettagli sull'aggiornamento del software	176
Scaricare da Cloud	176
Software di caricamento.....	177
Caricamento delle applicazioni	177
Aggiornamenti software/firmware	177
Applicare il software memorizzato sull'ADC	177
Risoluzione dei problemi.....	179
File di supporto	179
Traccia.....	179
Ping	180
Cattura.....	181
Aiuto	182
Chi siamo.....	182
Riferimento	182
I pacchetti JetPACK.....	183
I jetPACK Edgenexus	184
Scaricare un jetPACK	184
Microsoft Exchange	184
Microsoft Lync 2010/2013.....	185
Servizi web.....	185
Microsoft Remote Desktop	185
DICOM - Digital Imaging and Communication in Medicine (Immagini e comunicazioni digitali in medicina).....	186
Oracle e-Business Suite	186
VMware Horizon View	186
Impostazioni globali	186
Cifrari e jetPACK di cifratura	186
Cifrari forti.....	186
Anti-Bestia.....	186
No SSLv3	186
No SSLv3 no TLSv1 No RC4	186
NO_TLSv1.1.....	187
Abilitare i cifrari TLS-1.0-1.1	187
Esempio di cifratura jetPACK.....	187
Applicazione di un jetPACK.....	187
Creazione di un jetPACK.....	188
voloPATH	191
Introduzione a flightPATH.....	192

Che cos'è flightPATH?	192
Cosa può fare flightPATH?.....	192
Condizione	192
Partita	193
Controllo	194
Esempio	195
Valutazione	195
Azione.....	197
Azione	197
Obiettivo	198
Dati.....	198
Usi comuni	199
Firewall e sicurezza delle applicazioni	199
Caratteristiche	200
Regole precostituite	200
Estensione HTML.....	200
Indice.html.....	200
Chiudere le cartelle.....	201
Nascondere CGI-BBIN:	201
Ragno di tronchi	201
Forza HTTPS	202
Flusso mediatico:.....	202
Passare da HTTP a HTTPS	202
Carte di credito vuote	203
Scadenza dei contenuti	203
Tipo di server spoof.....	203
SAML e Entra ID.....	206
Impostazione dell'applicazione di autenticazione Entra ID in Microsoft Entra.....	207
Assistenza tecnica.....	210

Proprietà del documento

Numero documento: 2.0.3.19.25.12.03

Data di creazione del documento: 19 March 2025

Ultimo documento modificato: 19 March 2025

Autore del documento: Jay Savoor

Documento Modificato da:

Documento: EdgeADC - Versione 5.0.0

Dichiarazione di non responsabilità del documento

Le schermate e la grafica di questo manuale possono differire leggermente dal prodotto in uso a causa delle differenze tra le versioni del prodotto. Edgenexus assicura di aver compiuto ogni ragionevole sforzo per garantire la completezza e l'accuratezza delle informazioni contenute nel presente documento. Edgenexus non si assume alcuna responsabilità per eventuali errori. Edgenexus apporta modifiche e correzioni alle informazioni contenute in questo documento nelle versioni future, quando se ne presenta la necessità.

Diritti d'autore

© 2025 Tutti i diritti riservati.

Le informazioni contenute in questo documento sono soggette a modifiche senza preavviso e non rappresentano un impegno da parte del produttore. Nessuna parte di questa guida può essere riprodotta o trasmessa in qualsiasi forma o mezzo, elettronico o meccanico, comprese fotocopie e registrazioni, per qualsiasi scopo, senza l'espressa autorizzazione scritta del produttore. I marchi registrati appartengono ai rispettivi proprietari. È stato fatto ogni sforzo per rendere questa guida il più completa e accurata possibile, ma non è implicita alcuna garanzia di idoneità. Gli autori e l'editore non hanno alcuna responsabilità nei confronti di persone o enti per perdite o danni derivanti dall'uso delle informazioni contenute in questa guida.

Marchi di fabbrica

Il logo Edgenexus, Edgenexus, EdgeADC, EdgeWAF, EdgeGSLB, EdgeDNS sono tutti marchi o marchi registrati di Edgenexus Limited. Tutti gli altri marchi sono di proprietà dei rispettivi titolari e sono riconosciuti.

Supporto Edgenexus

In caso di domande tecniche relative a questo prodotto, si prega di inviare un ticket di assistenza a: support@edgenexus.io

Introduzione

State leggendo questa guida perché intendete implementare l'EdgeADC Edgenexus e bilanciare il carico delle vostre applicazioni basate su server in modo efficiente ed economico.

L'EdgeADC è costruito attorno a un motore altamente sicuro che offre elevata scalabilità, sicurezza, alte prestazioni e un'interfaccia di gestione molto semplice da usare. Questi fattori garantiscono che l'implementazione del sistema offra il miglior costo di proprietà possibile.

Lo scopo di questo documento

Questo documento è stato redatto per consentire all'utente di amministrare l'EdgeADC utilizzando la sua semplice interfaccia basata sul Web. Le funzioni e le relative configurazioni sono descritte in dettaglio e ci auguriamo che ciò sia sufficiente per configurare l'EdgeADC in base alle vostre esigenze.

A chi è destinato questo documento?

Questo documento si rivolge a persone con conoscenze di rete, in particolare di protocolli, applicazioni e server.

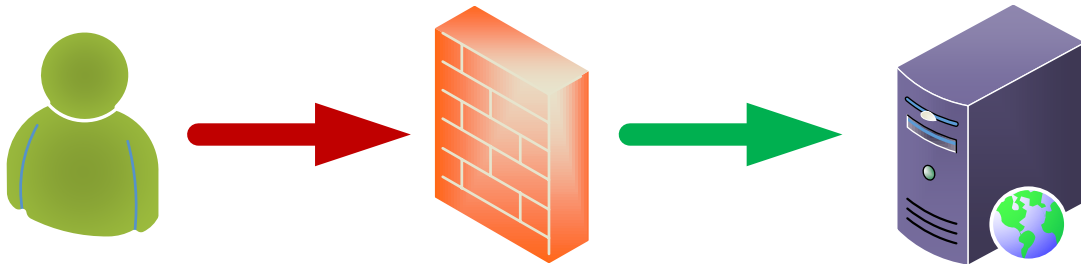
Bilanciamento del carico 101

Che cos'è un Load Balancer o ADC?

I bilanciatori di carico si sono evoluti in modo massiccio e hanno un'intelligenza molto maggiore nei loro motori rispetto al passato. Oggi vengono spesso chiamati application delivery controller o ADC.

Prima di capire che cos'è un bilanciatore di carico o un ADC, dobbiamo riconoscere i problemi degli informatici e degli utenti. Facciamo un esempio.

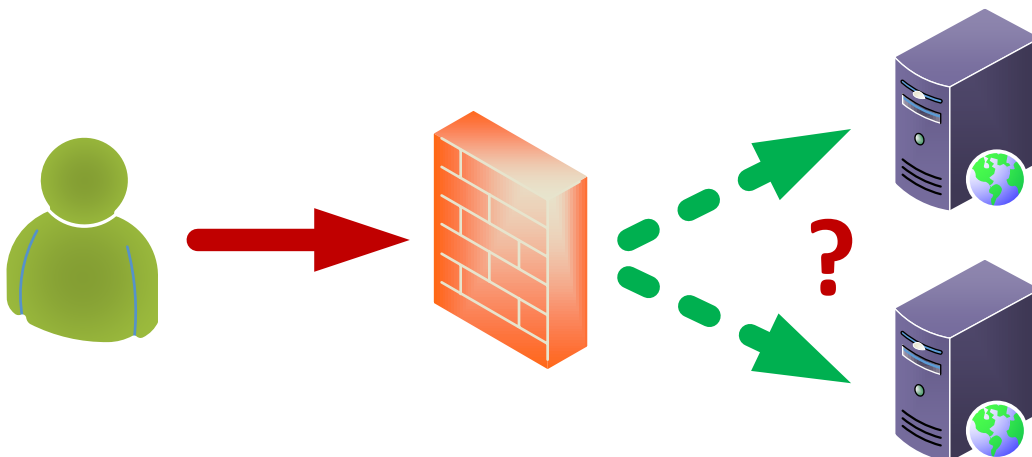
- Un'azienda ha un'applicazione Web che sta pubblicando su Internet. L'applicazione è ospitata su un singolo server Web, mentre i dati risiedono su un server di database separato.



User Client

Application Servers

- Questo server utilizza l'indirizzo IP 1.2.3.4 come esempio.
- Il numero di client che accedono all'applicazione aumenta regolarmente e alcuni hanno notato che le prestazioni dell'applicazione stanno diminuendo.
- L'analisi del server mostra che il traffico che colpisce il server è aumentato in modo massiccio e continua a salire.
- Si decide quindi di aggiungere un altro server per ospitare l'applicazione.
- Il nuovo secondo server utilizza l'indirizzo IP 1.2.3.5.
- Il problema è come indirizzare il client al server nuovo e a quello attuale per condividere il carico e garantire che la sessione dell'utente sia mantenuta sul primo server collegato.



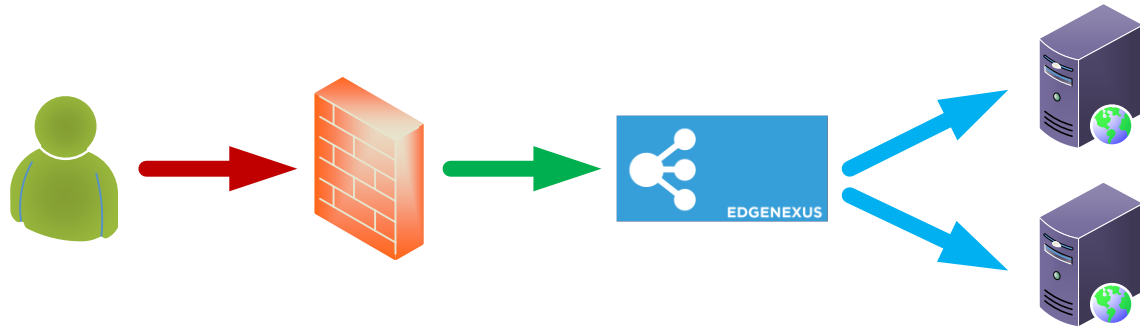
User Client

Application Servers

- La risposta è un bilanciatore di carico o ADC.

Ora la soluzione.

- Posizioniamo un ADC davanti ai due application server.



User Client

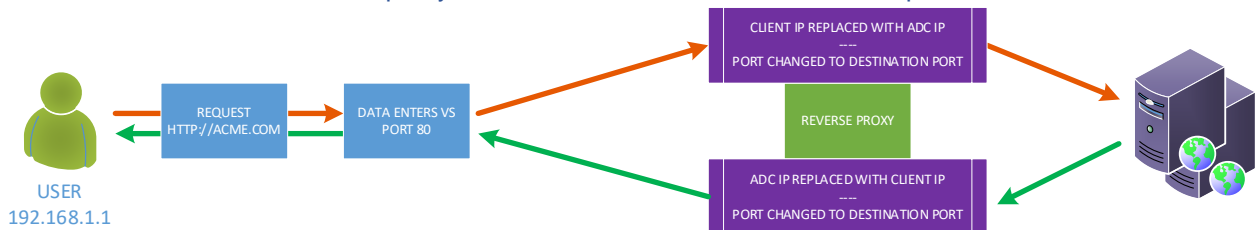
ADC

Application Servers

- L'ADC avrà un IP rivolto all'esterno di 1.2.3.6 e il firewall reindirizzerà NAT le richieste a questo indirizzo invece che al precedente 1.2.3.4.
- L'IP dell'ADC che riceve le richieste è chiamato VIP e la configurazione è chiamata Virtual Service.
- L'ADC riceve le richieste dagli utenti client e le inoltra ai server reali utilizzando politiche di bilanciamento del carico e monitorando lo stato di salute dei server applicativi per garantirne l'efficienza.



- L'ADC bilancia il traffico verso i server in base alla politica di bilanciamento del carico in uso, alla natura del carico e allo stato dei server applicativi.
- Il traffico proveniente dai server viene rinvio al client attraverso l'ADC nella direzione opposta.
- A causa della natura del reverse proxy, il server e il client sono anonimi l'uno per l'altro.



- La tecnologia reverse proxy garantisce un livello di sicurezza ottimale.

Spiegazione dei VIP e dei servizi virtuali (VS)

Un VIP è, in sostanza, un indirizzo IP definito per l'uso sull'EdgeADC e consente agli utenti di accedere ai servizi ad esso collegati. Questo è più o meno ciò che è un VIP. Per il funzionamento dell'EdgeADC, non è necessario che il VIP si trovi nella stessa subnet dei server reali e questa metodologia di traduzione degli indirizzi di rete rende la tecnologia molto sicura per gli hacker che tentano di accedere ai server interni.

Nota: L'indirizzo IP del VIP non può essere lo stesso utilizzato per l'IP di gestione.

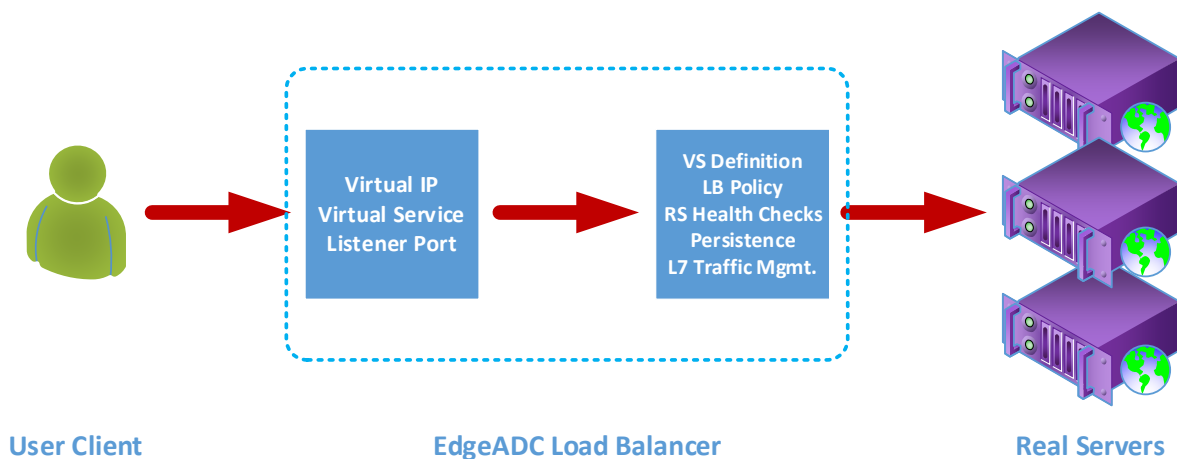
I servizi virtuali costituiscono il nucleo delle tecnologie di proxying e load-balancing di EdgeADC. L'IP virtuale è l'indirizzo attraverso il quale il VS viene pubblicizzato alla rete e al mondo, in ascolto del traffico e delle richieste dei clienti che desiderano utilizzare le applicazioni che serve.

Quando i client raggiungono il VS, quest'ultimo è configurato per eseguire numerose azioni sul traffico, tra cui, a titolo esemplificativo, le seguenti:

- Proxy della connessione del cliente
- Vengono eseguite funzioni specifiche come la compressione, l'accelerazione, il bilanciamento del carico, l'ispezione del traffico, ecc.
- Inoltrare le richieste del client ai server di destinazione definiti nelle politiche di bilanciamento del carico del servizio virtuale.

Si può pensare che il VS sia sposato con un indirizzo IP (VIP) su cui l'EdgeADC è in ascolto in preparazione delle richieste di dati. Quando vengono effettuate configurazioni TCP o HTTP standard, il client si connette al VIP e l'EdgeADC elabora la richiesta in base alla definizione che costituisce il VS. A questo punto, l'EdgeADC invia il traffico ai Real Server specificati.

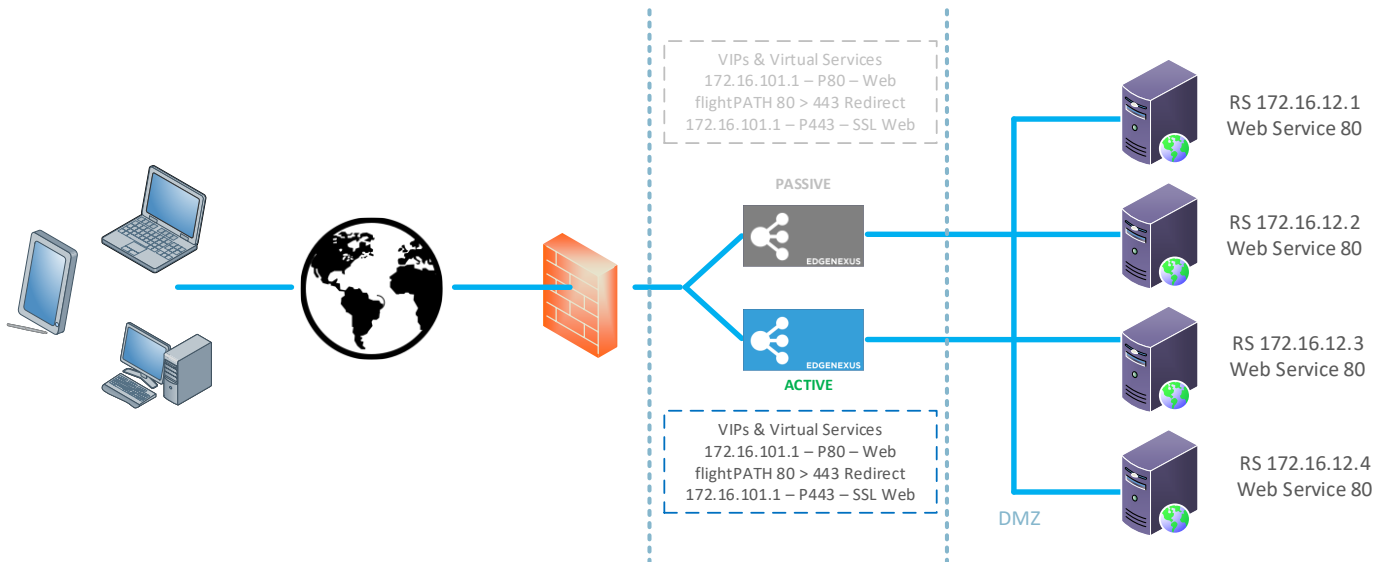
Il VS riceve la connessione e i dati in una configurazione tipica e quindi termina o proxy utilizzando il motore di reverse proxy all'interno dell'EdgeADC. L'EdgeADC procede quindi all'apertura di una nuova connessione ai Real Server e all'invio dei dati. Quando i server reali rispondono alla richiesta, l'EdgeADC invia la risposta al client utilizzando un percorso inverso simile, a seconda delle impostazioni effettuate nell'opzione Connettività della scheda Bilanciamento del carico dei server reali.



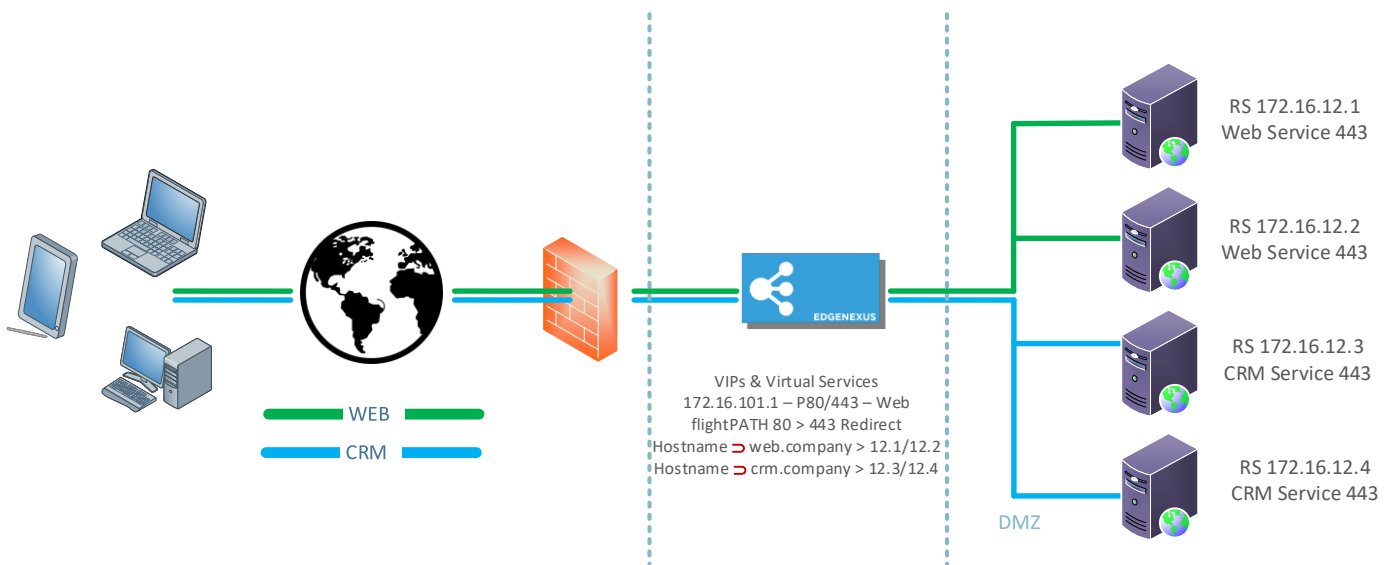
La definizione di un servizio virtuale comprende un singolo indirizzo IP (VIP) e un insieme di porte che servono come punti di ingresso a diversi servizi, utilizzando una varietà di protocolli.

Ad esempio, è necessario bilanciare il carico di una serie di server web per garantire la resilienza. Supponiamo che l'accesso a questi sistemi avvenga tramite comunicazioni protette HTTPS, utilizzando <https://myweb.company.com>.

Se si osserva la definizione di una configurazione di questo tipo, essa comprende un singolo VIP con due voci, una per la porta 80 e l'altra per la porta 443. Il VIP per la porta 80 avrà una regola flightPATH collegata che forzerà la conversione del traffico in HTTPS. La seconda voce per la porta 443 invierà il traffico ai server reali definiti sotto di essa. Allo stesso modo, si possono avere altri servizi sotto lo stesso VIP per bilanciare il traffico verso i server di posta o altri server applicativi.



Con ADC meno funzionali, i servizi che utilizzano le stesse porte avrebbero bisogno di VIP diversi, ma l'ADC e il suo sistema flightPATH consentono di utilizzare un singolo VIP con più servizi che utilizzano le stesse porte. Pertanto, è possibile avere due applicazioni, entrambe accessibili tramite la porta 443 con nomi di host diversi, utilizzando un unico VIP. Un esempio è illustrato di seguito.



I sistemi EdgeADC sono estremamente flessibili e consentono di definire configurazioni molto complesse e funzionali.

Che cos'è un tipo di servizio di bilanciamento del carico?

I tipi di servizio di bilanciamento del carico consistono in algoritmi e metodologie utilizzati per distribuire in modo intelligente o bilanciare il traffico tra pool di server. Il metodo e l'algoritmo che l'ADC mette a disposizione dipendono dal tipo di servizio o dall'applicazione utilizzata sui server da bilanciare, nonché dallo stato della rete e dei server in uso. Va notato che il tipo di servizio di bilanciamento del carico che si sceglie di utilizzare dipende anche dal livello di traffico inviato attraverso l'ADC. Pertanto, quando il traffico o il carico sono bassi, i tipi di servizio di bilanciamento del carico possono essere semplici. Ma quando i carichi sono maggiori, potrebbe essere necessario scegliere tipi più complessi per ottenere una distribuzione più efficiente del carico sui server back-end.

Nell'EdgeADC sono disponibili i seguenti tipi di servizio di bilanciamento del carico.

DICOM	STRATO 4 UDP	RPC
FTP	LIVELLO 4 TCP/UDP	RPC/ADS
HTTP(S)	DNS	RPC/CA/PF
IMAP	POP3	SMTP
STRATO 4 TCP	PSR	GSLB

L'inizio del viaggio

Scaricare l'EdgeADC

Prima di procedere all'installazione, è necessario scaricare l'EdgeADC adatto al proprio ambiente.

Forniamo edizioni per la maggior parte degli ambienti virtualizzati e un'edizione ISO per l'installazione diretta su hardware bare-metal.

Il primo passo consiste nel compilare il modulo di valutazione che si trova sul sito web di Edgenexus, all'indirizzo <https://www.edgenexus.io/products/load-balancer/free-trial/>.

The screenshot shows the Edgenexus website interface. At the top, there is a navigation menu with links: Why Edgenexus?, Try, Products, Solutions, Applications, Resources, and Support. The main content area has a blue background with white paper airplanes. The headline reads "The Easy choice for Load balancing" with the subtext "Fast, Scalable and Secure Applications". A "Why Edgenexus?" button is visible. On the right, there is a "Request a Free Trial" form with the following fields: First name, Last name, Email*, and Company name. Below the form is a reCAPTCHA widget and a red "Submit" button. At the bottom, there are logos for Exchange, SharePoint, Microsoft Dynamics, ORACLE, Skype for Business, and VMware Horizon View. The footer text says "Your Load Balancing Experts" with a chat icon on the right.

La procedura è semplice e, dopo aver compilato e inviato il modulo, si accede alla pagina di download, dove è possibile selezionare l'immagine corretta per il proprio ambiente.

Le edizioni di EdgeADC sono disponibili per i seguenti sistemi di virtualizzazione:

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

Si può anche scegliere di fare un test nel cloud utilizzando le edizioni del marketplace Microsoft Azure o Amazon AWS.

Se si sceglie di scaricare il software per un'installazione on-premise, si riceverà EdgeADC con una licenza di prova incorporata di 14 giorni. Si consiglia di contattare sales@edgenexus.io e richiedere una chiave di licenza di 30 giorni con tutte le funzionalità abilitate.

Installazione

Installazione di EdgeADC

L'EdgeADC (ADC) è disponibile per l'installazione su diverse piattaforme, ognuna delle quali richiede il proprio programma di installazione, che viene reso disponibile una volta effettuata la registrazione per il download.

Questi sono i vari modelli di installazione disponibili.

- VMware ESXi
- KVM
- Citrix Xen
- Nutanix AHV
- Microsoft Hyper-V
- Oracle VM
- Proxmox (Utilizzare OVA)
- ISO per hardware BareMetal

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

Installazione su VMware ESXi

L'ADC è supportato per l'installazione su VMware ESXi 5.x e successivi.

- Scaricare l'ultimo pacchetto OVA di installazione di ADC utilizzando il link appropriato fornito con l'e-mail di download.
- Una volta scaricato, decomprimere in una directory appropriata sull'host ESXi o sulla SAN.
- Nel client vSphere, selezionare File: Deploy OVA/OVF Template.
- Sfogliare e selezionare il percorso in cui sono stati salvati i file; scegliere il file OVF e fare clic su **NEXT**.
- Il server ESX richiede il nome dell'appliance. Digitare un nome adatto e fare clic su **AVANTI**
- Selezionare il datastore da cui verrà eseguita l'appliance ADC.
- Selezionate un datastore con spazio sufficiente e fate clic su **NEXT**.
- A questo punto vi verranno fornite informazioni sul prodotto; fate clic su **NEXT**.
- Fare clic su **AVANTI**.
- Una volta copiati i file sul datastore, è possibile installare il dispositivo virtuale.

Avviare il client vSphere per visualizzare il nuovo dispositivo virtuale ADC.

- Fare clic con il tasto destro del mouse sul VA e scegliere Alimentazione > Accensione
- Il VA si avvia e sulla console viene visualizzata la schermata di avvio dell'ADC.

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

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

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

Installazione dell'interfaccia VMXNET3

Il driver VMXnet3 è supportato, ma è necessario modificare prima le impostazioni della NIC.

Nota - *NON aggiornare VMware-tools*

Abilitazione dell'interfaccia VMXNET3 su una VA appena importata (mai avviata)

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

Abilitazione dell'interfaccia VMXNET3 su una VA già in esecuzione

1. Arresto della macchina virtuale (comando di spegnimento CLI o spegnimento GUI)
2. Ottenete gli indirizzi MAC di entrambe le NIC (**ricordate l'ordine delle NIC nell'elenco**).
3. Eliminare entrambe le NIC dalla macchina virtuale
4. Aggiornare l'hardware della macchina virtuale (non avviare l'installazione o l'aggiornamento degli strumenti VMware, ma eseguire **solo** l'aggiornamento dell'hardware).
5. Aggiungere due NIC e selezionarle come VMXNET3.
6. Impostare gli indirizzi MAC delle nuove NIC come indicato al punto 2.
7. Riavviare il VA

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

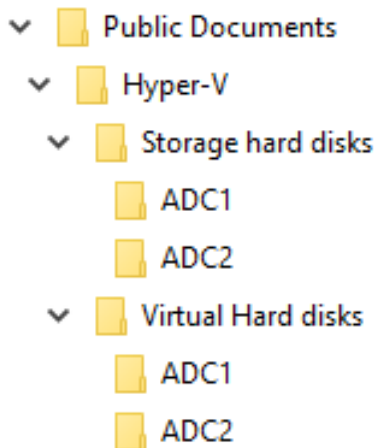
Per procedere ulteriormente, consultare la sezione **CONFIGURAZIONE DEL PRIMO AVVIO**.

Installazione su Microsoft Hyper-V

L'appliance Edgenexus ADC Virtual può essere facilmente installata all'interno di una struttura di virtualizzazione Microsoft Hyper-V. Questa guida presuppone che il sistema Hyper-V e le risorse di sistema siano stati correttamente specificati e configurati per ospitare l'ADC e la sua architettura di bilanciamento del carico.

Si noti che ogni dispositivo richiede un indirizzo MAC univoco.

- Estrarre il file ADC-VA compatibile con Hyper-V scaricato sul computer o sul server locale.
- Aprire Hyper-V Manager.
- Creare una nuova cartella per contenere il "disco rigido virtuale" di ADC VA e un'altra nuova cartella per contenere il "disco rigido di archiviazione", ad esempio C:\Users\Public\Documents\Hyper-V\Virtual hard disks\ADC1 e C:\Users\Public\Documents\Hyper-V\Storage hard disks\ADC1
- **Nota:** Per ogni installazione di istanza ADC virtuale è necessario creare nuove sottocartelle specifiche per ADC per i dischi rigidi virtuali e i dischi rigidi di archiviazione, come mostrato di seguito:



- Copiare il file EdgeADC .vhd estratto nella cartella "Storage hard disk" creata in precedenza.
- Nel client Hyper-V Manager, fare clic con il tasto destro del mouse sul server e selezionare "Importa macchina virtuale".
- Sfolgiare la cartella che contiene il file immagine ADC VA scaricato ed estratto in precedenza
- Selezionare la macchina virtuale: evidenziare la macchina virtuale da importare e fare clic su Avanti.
- Selezionare la macchina virtuale: evidenziare la macchina virtuale da importare e fare clic su Avanti.
- Scegliere Tipo di importazione - selezionare "**Copia della macchina virtuale (creare un nuovo ID univoco)**".
- Scegliere le cartelle per i file della macchina virtuale: la destinazione può essere lasciata come quella predefinita di Hyper-V o si può scegliere di selezionare una posizione diversa.
- Individuare i dischi rigidi virtuali: sfogliare e selezionare la cartella dei dischi rigidi virtuali creata in precedenza e fare clic su Avanti.
- Scegliere Cartelle per archiviare i dischi rigidi virtuali: sfogliare e selezionare la cartella Dischi rigidi di archiviazione creata in precedenza e fare clic su Avanti.
- Verificare che i dettagli nella finestra Riepilogo importazione guidata siano corretti e fare clic su Fine.
- Fare clic con il tasto destro del mouse sulla macchina virtuale **ADC** appena importata e selezionare Avvia.

NOTA: COME INDICATO IN [HTTP://SUPPORT.MICROSOFT.COM/KB/2956569](http://support.microsoft.com/kb/2956569), È NECESSARIO IGNORARE IL MESSAGGIO DI STATO "DEGRADED (INTEGRATION SERVICES UPGRADE REQUIRED)", CHE POTREBBE ESSERE VISUALIZZATO COME DI SEGUITO DOPO L'AVVIO DI VA. NON È RICHIESTA ALCUNA AZIONE E IL SERVIZIO NON È DEGRADATO.

- Durante l'inizializzazione della macchina virtuale, è possibile fare clic con il pulsante destro del mouse sulla voce VM e selezionare Connetti... Verrà quindi visualizzata la console EdgeADC.

```
Checking for management interface ..... [ OK ]  
  
Management interface: eth0  MAC: 00:0c:29:05:2e:1a  
  
1. Enter networking details manually  
2. Configure networking setting automatically via DHCP
```

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

Per procedere ulteriormente, consultare la sezione **CONFIGURAZIONE DEL PRIMO AVVIO**.

Installazione su Citrix XenServer

Il dispositivo ADC Virtual è installabile su Citrix XenServer.

- Estrarre il file ADC OVA ALB-VA sul computer o sul server locale.
- Aprite Citrix XenCenter Client.
- Nel client XenCenter, selezionare "**File: Importa**".
- Cercare e selezionare il file **OVA**, quindi fare clic su "**Open Next**".
- Selezionare la posizione di creazione della macchina virtuale quando viene richiesto.
- Scegliere quale XenServer si desidera installare e fare clic su "**NEXT**".
- Quando viene richiesto, selezionare il repository di archiviazione (SR) per il posizionamento del disco virtuale.
- Selezionare un SR con spazio sufficiente e fare clic su "**NEXT**".
- Mappare le interfacce di rete virtuali. Entrambe le interfacce avranno la dicitura Eth0; tuttavia, si noti che l'interfaccia inferiore è Eth1.
- Selezionare la rete di destinazione per ciascuna interfaccia e fare clic su **AVANTI**.
- **NON** selezionare l'opzione "Usa correzione del sistema operativo".
- Fare clic su "**AVANTI**".
- Scegliere l'interfaccia di rete da utilizzare per il trasferimento temporaneo VM.
- Scegliere l'interfaccia di gestione, di solito Rete 0, e lasciare le impostazioni di rete su DHCP. Tenere presente che è necessario assegnare indirizzi IP statici se non si dispone di un server DHCP funzionante per il trasferimento. Se non si esegue questa operazione, l'importazione risulterà continuamente in connessione e poi fallita. Fare clic su "**AVANTI**".
- Esaminare tutte le informazioni e verificare le impostazioni corrette. Fare clic su "**FINISH**".
- La macchina virtuale inizierà a trasferire il disco virtuale "ADC" e, una volta completato, verrà visualizzata sotto il proprio XenServer.
- Nel client XenCenter sarà ora possibile vedere la nuova macchina virtuale. Fare clic con il pulsante destro del mouse sulla VA e fare clic su "**START**".
- La macchina virtuale si avvia e viene visualizzata la schermata di avvio dell'ADC.

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

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

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

- Una volta configurato, si presenta l'accesso al VA.

Per procedere ulteriormente, consultare la sezione [CONFIGURAZIONE DEL PRIMO AVVIO](#).

Installazione su KVM

La sezione seguente mostra come installare l'EdgeADC su una piattaforma KVM. La piattaforma KVM utilizzata per questo esercizio funzionava su un sistema operativo CentOS v8 con Cockpit e la virtualizzazione installati.

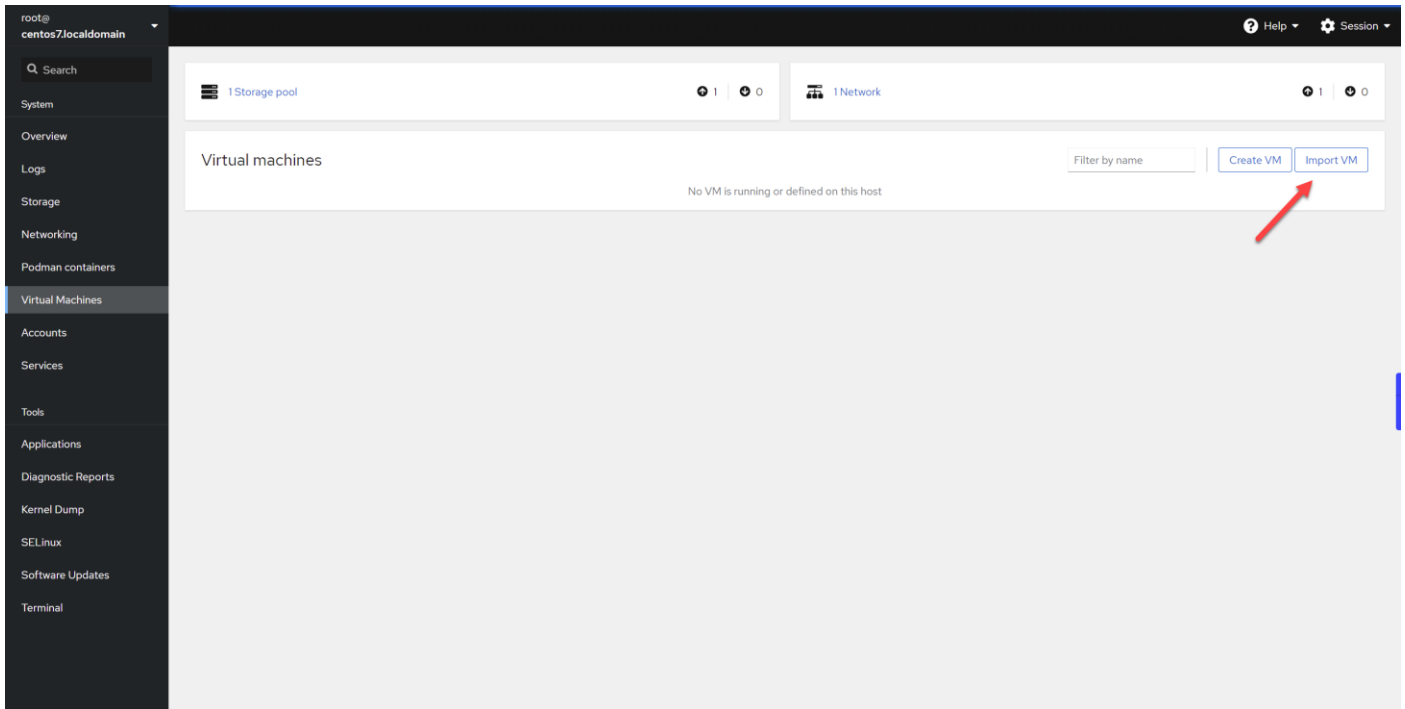
Requisiti e versioni

Questa guida è rilevante per EdgeADC 4.2.6 e versioni successive.

Le indicazioni riportate di seguito non riguardano l'installazione di KVM o il suo collegamento in rete.

Si presume che il dispositivo virtuale KVM sia stato scaricato e memorizzato sull'host in una posizione accessibile.

- Il primo passo è accedere alla console Cockpit.



- Fare clic su Importa VM
- Nella prima finestra di dialogo è necessario specificare i dettagli per l'importazione del dispositivo virtuale. Vedere l'immagine sottostante per il contenuto dei campi. È necessario specificare Red Hat Enterprise 6.0 come sistema operativo.

Import a virtual machine

Name: EdgeADC

Disk image: /home/Edgenexus-ADC-6.8-64-KVM.1140-1909-7567-bam1727.qcow2

Operating system: Red Hat Enterprise Linux 6.0 (Santiago)

Memory: 4 GiB
Up to 7.5 GiB available on the host

Immediately start VM:

Import Cancel

- Assicurarsi che l'opzione "Avvia immediatamente la macchina virtuale" sia deselezionata.

- Una volta compilati i dati, fare clic sul pulsante Importa.
- La fase successiva consiste nello specificare l'allocazione della vCPU e della memoria che si desidera utilizzare.

Overview

General		Hypervisor details	
State	Shut off	Emulated machine	pc-i440fx-rhel7.6.0
Memory	4 MiB edit	Firmware	BIOS
vCPUs	1 edit		
CPU type	host edit		
Boot order	disk edit		
Autostart	<input type="checkbox"/> Run when host boots		

- Per allocare la memoria, viene visualizzata una finestra di dialogo simile a quella riportata di seguito.

EdgeADC memory adjustment

Current allocation: 4 GiB

Maximum allocation: 4 GiB

- Per allocare la vCPU, viene visualizzata una finestra di dialogo simile a quella riportata di seguito.

EdgeADC vCPU details ✕

vCPU count ⓘ	<input type="text" value="4"/>	Sockets ⓘ	<input type="text" value="1"/>
vCPU maximum ⓘ	<input type="text" value="4"/>	Cores per socket	<input type="text" value="2"/>
		Threads per core	<input type="text" value="2"/>

- Le scelte che abbiamo fatto sono solo esempi, ma sono fattibili, a meno che non si utilizzi un throughput elevato con la ricrittografia SSL, nel qual caso sarà necessario regolare di conseguenza la sezione Hardware in Visualizza > Statistiche.

▲ Hardware	
Disk Usage	40%
Memory Usage	11.6%(894.7MB of 7689.6MB)
CPU Usage	16.0%

- Ora è stato installato un ADC funzionante in KVM. Vedere l'immagine sottostante.

Overview

General	Hypervisor details	
State	Running	Emulated machine pc-i440fx-rhel7.6.0
Memory	4 GiB edit	Firmware BIOS
vCPUs	4 edit	
CPU type	custom (Cooperlake) edit	
Boot order	disk edit	
Autostart	<input type="checkbox"/> Run when host boots	

Usage

Memory	583.4 / 4096 MB
CPU	6% of 4 vCPUs

Console

VNC console Expand ↗

Send key

```

Welcome to Edgenexus ADC
Copyright (c) 2002-2021 Edgenexus Ltd. All Rights Reserved.

Using Intel AES Hardware Acceleration

GUI address is https://192.168.159.100:443
After login, type "help" for a list of commands.

jetnexus login:

```

Disks

Device	Used	Capacity	Bus	Access	Source	
disk	14 GiB	25 GiB	virtio	Writeable	File /home/Edgenexus-ADC-6.8-64-KVM.1140-1909-7567-bam1727.qcow2	<input type="button" value="Remove"/> <input type="button" value="Edit"/>

Networks

Type	Model type	MAC address	IP address	Source	State	
network	virtio	52:54:00:60:83:65	Unknown	default	up	<input type="button" value="Delete"/> <input type="button" value="Unplug"/> <input type="button" value="Edit"/>

Installazione su Nutanix AHV

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

Requisiti e versioni

Questa guida è rilevante per EdgeADC 4.2.6 e versioni successive.

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

- Il primo passo consiste nell'accedere a Nutanix Prism Central.

Caricamento dell'immagine EdgeADC

- Navigare in Infrastruttura virtuale > Immagini
- Fare clic sul pulsante Aggiungi immagine
- Selezionare il file immagine EdgeADC scaricato e fare clic sul pulsante Apri per caricare l'immagine.
- Inserire un nome per l'immagine nel campo Descrizione immagine.
- Selezionare una categoria appropriata
- Selezionare l'immagine e fare clic sul tasto freccia a destra.
- Selezionare Tutte le immagini e fare clic su Salva.

Creazione della macchina virtuale

- Navigare in Infrastruttura virtuale > Macchine virtuali
- Fare clic sul pulsante Crea macchina virtuale
- Immettere un nome per la macchina virtuale, il numero di CPU che si desidera avere e il numero di core che si desidera assegnare alla macchina virtuale.
- Quindi scorrere la finestra di dialogo verso il basso e inserire la quantità di memoria che si desidera allocare alla macchina virtuale. Si può iniziare con 4 GB e aumentare in base all'utilizzo.

Aggiunta del disco

- Quindi, fare clic sul collegamento Aggiungi nuovo disco
- Selezionare l'opzione Clona da servizio immagine nel menu a discesa Operazione.
- Selezionare l'immagine EdgeADC aggiunta e fare clic sul pulsante Aggiungi.
- Selezionate il disco da avviare.

Aggiunta di NIC, rete e affinità

- Quindi, fare clic sul pulsante Aggiungi nuova NIC. È necessario disporre di due NICS.
- Selezionare la rete e fare clic sul pulsante Aggiungi
- Fare clic sul pulsante Imposta affinità
- Selezionare gli host Nutanix su cui la macchina virtuale può essere eseguita, quindi fare clic sul pulsante Salva.
- Verificare le impostazioni effettuate e fare clic sul pulsante Salva.

Accensione della macchina virtuale

- Dall'elenco delle macchine virtuali, fare clic sul nome della macchina virtuale appena creata.
- Fare clic sul pulsante di accensione della macchina virtuale
- Una volta accesa la macchina virtuale, fare clic sul pulsante Avvia console.

Configurazione della rete EdgeADC

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

Installazione su ProxMox

L'installazione su ProxMox è semplice, ma richiede un paio di passaggi aggiuntivi.

Utilizzeremo la versione OVA di VMWare per l'installazione. Si tratta di un processo in più fasi che richiede la conoscenza dei comandi di shell di ProxMox. Tuttavia, abbiamo reso le istruzioni il più semplici possibile

da seguire. Partendo dal presupposto che l'utente conosce ProxMox, non approfondiremo le caratteristiche di ProxMox.

Caricamento dell'OVA su ProxMox

Poiché stiamo usando una versione OVA, dovremo prima caricare l'OVA su ProxMox.

- Accedere alla console ProxMox
- Creare una cartella chiamata OVA_Import.
- A questo punto è necessario utilizzare un client SFTP come WinSCP (Windows) o CyberDuck (Mac) per trasferire il file OVA.
- Una volta trasferito il file, lo si vedrà nella cartella creata.
- Digitare il seguente comando per estrarre il contenuto del file OVA.
- `Tar xvf {nome file}`. Vedere l'esempio seguente.

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

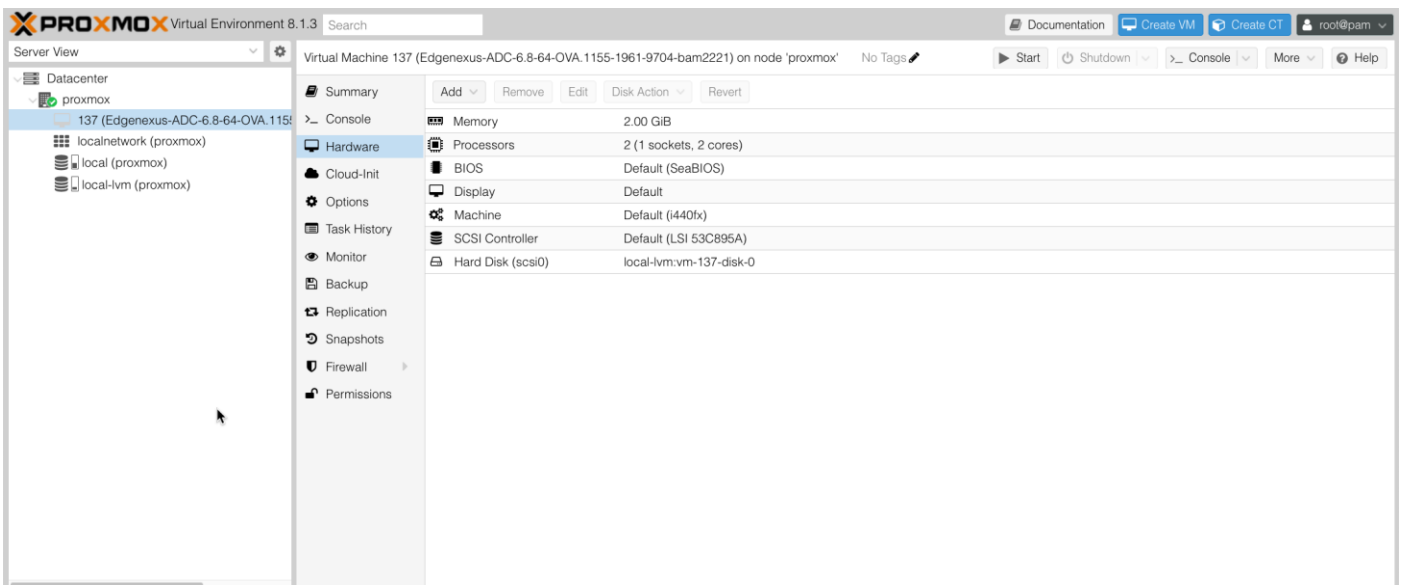
- Una volta estratto, si dovrebbe vedere qualcosa di simile all'esempio seguente.

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

- Ci sono tre file. I file `.ovf` e `.mf` sono la configurazione. Il file `.vmdk` è il disco virtuale che contiene l'ADC.
- Il passo successivo è importare il VMDK in ProxMox e creare la macchina virtuale.
- Digitare il seguente comando per creare la macchina virtuale utilizzando i file di configurazione.

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

- In questo esempio, abbiamo dato un ID di 100, ma questo potrebbe essere diverso per la vostra installazione se avete già macchine virtuali create in ProxMox. È possibile determinare l'ID successivo avviando il processo di creazione di macchine virtuali in ProxMox, oppure scegliendo un numero superiore a 100 che sia tranquillamente non raggiungibile.
- La macchina virtuale è stata creata.



- Il passo successivo consiste nell'aggiungere un'interfaccia di rete alla macchina virtuale.
- Fare clic su Hardware nel pannello di destra.
- Fare clic su Aggiungi e scegliere un'interfaccia di rete.

The screenshot shows a configuration window titled "Add: Network Device". It contains the following fields and options:

- Bridge:** vmbr0
- Model:** VMware vmxnet3
- VLAN Tag:** no VLAN
- MAC address:** auto
- Firewall:**
- Disconnect:**
- Rate limit (MB/s):** unlimited
- MTU:** 1500 (1 = bridge MTU)
- Multiqueue:** (empty)

At the bottom, there is a "Help" button, an "Advanced" checkbox which is checked, and a blue "Add" button.

- Configurarlo come mostra l'immagine qui sopra. È importante scegliere il modello VMware vmxnet3.
- Una volta configurato, fare clic su Aggiungi.
- È possibile aggiungere altri adattatori di rete in base alle proprie esigenze.
- A questo punto è possibile avviare la macchina virtuale e procedere con le istruzioni del capitolo Configurazione del primo avvio.

Configurazione del primo avvio

Al primo avvio, l'ADC (di seguito indicato anche come VA) visualizza la seguente schermata che richiede la configurazione per le operazioni di produzione.

```
Checking for management interface ..... [ OK ]
Management interface: eth0  MAC: 00:0c:29:05:2e:1a

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

Primo avvio - Dettagli di rete manuali

Al primo avvio, si hanno 10 secondi per interrompere l'assegnazione automatica dei dati IP tramite DHCP.

Per interrompere questo processo, fare clic nella finestra della console e premere un tasto qualsiasi. È quindi possibile inserire manualmente i seguenti dati.

- Indirizzo IP
- Maschera di sottorete
- Porta d'ingresso
- Server DNS

Queste modifiche sono persistenti e sopravvivono a un riavvio e non devono essere configurate nuovamente sul VA.

Primo avvio - DHCP riuscito

Se non si interrompe il processo di assegnazione della rete, l'ADC contatterà un server DHCP dopo un timeout per ottenere i dettagli della rete. Se il contatto ha esito positivo, alla macchina vengono assegnate le seguenti informazioni.

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

Si consiglia di utilizzare l'ADC con un indirizzo DHCP solo se tale indirizzo IP è collegato in modo permanente all'indirizzo MAC dell'ADC nel server DHCP. Si consiglia sempre di utilizzare un **INDIRIZZO IP FISSO** quando si utilizzano le appliance virtuali. Seguire i passaggi di [MODIFICA DELL'INDIRIZZO IP DI GESTIONE](#) e delle sezioni successive fino al completamento della configurazione di rete.

Primo avvio - DHCP fallisce

Se non si dispone di un server DHCP o se la connessione fallisce, verrà assegnato l'indirizzo IP 192.168.100.100.

L'indirizzo IP aumenterà di '1' finché il VA non troverà un indirizzo IP libero. Allo stesso modo, la VA verificherà se l'indirizzo IP è attualmente in uso e, in tal caso, effettuerà un nuovo incremento e ricontrollerà.

Modifica dell'indirizzo IP di gestione

È possibile modificare l'indirizzo IP del VA in qualsiasi momento utilizzando il comando **set greenside=n.n.n.n**, come mostrato di seguito.

```
set greenside={indirizzo IP}
```

Modifica della maschera di sottorete per eth0

Le interfacce di rete utilizzano il prefisso "eth"; l'indirizzo di rete di base è chiamato eth0. La maschera di sottorete o netmask può essere modificata con il comando **set mask [NIC] [MASK]**. Di seguito è riportato un esempio.

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

Assegnazione di un gateway predefinito

Il VA ha bisogno di un gateway predefinito per le sue operazioni. Per impostare il gateway predefinito, utilizzare il comando **route add default gw [GATEWAY IP]** come mostrato nell'esempio seguente.

```
route add default gw {indirizzo IP}
```

Verifica del valore del Gateway predefinito

Per verificare se il gateway predefinito è stato aggiunto ed è corretto, utilizzare il comando **route**. Questo comando visualizza i percorsi di rete e il valore del gateway predefinito. Vedere l'esempio seguente.

```
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
```

È ora possibile accedere all'interfaccia grafica utente (GUI) per configurare l'ADC per l'uso in produzione o per la valutazione.

Accesso all'interfaccia web

È possibile utilizzare qualsiasi browser Internet con JavaScript per configurare, monitorare e rendere operativo l'ADC.

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

Per impostazione predefinita, l'ADC utilizza un certificato SSL autofirmato. È possibile modificare l'ADC per utilizzare un certificato SSL di propria scelta.

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

Username: admin / Pwd: jetnexus

Tabella di riferimento dei comandi

Comando	Parametro1	Parametro2	Descrizione	Esempio
data			Mostra la data e l'ora configurate al momento.	Mar Sept 3 13:00 UTC 2013
valori predefiniti			Assegnare le impostazioni di fabbrica dell'apparecchio	
uscita			Uscire dall'interfaccia della riga di comando	
Aiuto			Visualizza tutti i comandi validi	
ifconfig	[vuoto]		Visualizzare la configurazione dell'interfaccia per tutte le interfacce	ifconfig
	eth0		Visualizzare la configurazione dell'interfaccia solo di eth0	ifconfig eth0
macchinaid			Questo comando fornirà il machineid utilizzato per la licenza dell'ADC ADC	EF4-3A35-F79
abbandonare			Uscire dall'interfaccia della riga di comando	
riavvio			Terminare tutti i collegamenti e riavviare l'ADC ADC	riavvio
riavvio			Riavviare i servizi virtuali ADC ADC	
percorso	[vuoto]		Visualizzare la tabella di routing	percorso
	aggiungere	gw predefinito	Aggiungere l'indirizzo IP del gateway predefinito	percorso aggiungere default gw 192.168.100.254
set	greenside		Impostare l'indirizzo IP di gestione per l'ADC	impostare greenside=192.168.101.1
	maschera		Imposta la maschera di sottorete 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 tutti i collegamenti e spegnere l'ADC ADC	
stato			Visualizza le statistiche dei dati correnti	
top			Visualizzare le informazioni sul processo, come CPU e memoria	
viewlog	messaggi		Visualizza i messaggi syslog non elaborati	Visualizzare i messaggi di log

Nota bene: i comandi non sono sensibili alle maiuscole e alle minuscole. Non esiste una cronologia dei comandi.

La Console Web

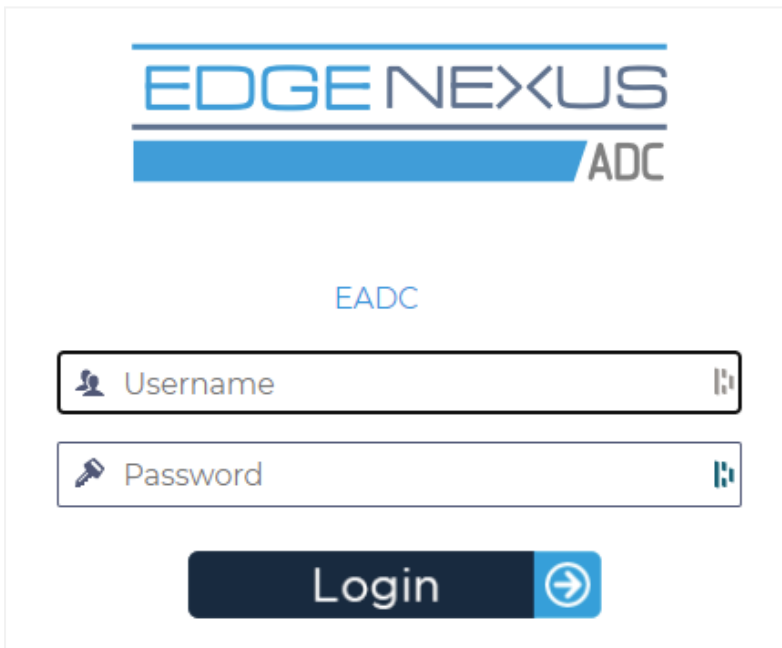
Avvio della Console Web ADC

Tutte le operazioni sull'ADC vengono configurate ed eseguite tramite la console web. Si accede alla console web con qualsiasi browser dotato di JavaScript.

Per avviare la console web dell'ADC, inserire l'URL o l'indirizzo IP dell'ADC nel campo URL. Utilizzeremo l'esempio di `adc.company.com` come esempio:

`https://adc.company.com`

Una volta avviata, la console web dell'ADC si presenta come mostrato di seguito, consentendo di accedere come utente amministratore.



Credenziali di accesso predefinite

Le credenziali di accesso predefinite sono:

Username: admin / Pwd: jetnexus

È possibile modificare questa impostazione in qualsiasi momento utilizzando la configurazione degli utenti che si trova in *Sistema > Utenti*.

Una volta effettuato l'accesso, viene visualizzato il cruscotto principale dell'ADC.

Utilizzo di un servizio di autenticazione esterno

Se si desidera utilizzare un servizio di autenticazione esterno, è possibile farlo configurando un Server di autenticazione e un Servizio di autenticazione.

Per informazioni al riguardo, consultare [Autenticazione](#) e [Servizio di autenticazione](#)

Il cruscotto principale

L'immagine sottostante illustra l'aspetto del cruscotto principale o "home page" dell'ADC. Potremmo occasionalmente apportare alcune modifiche per migliorare l'aspetto, ma tutte le funzioni rimarranno invariate.

The screenshot displays the EdgeNexus main dashboard. At the top, there is a navigation bar with 'EDGE NEXUS' on the left and 'GUI Status', 'Home', 'Help', and 'admin' on the right. Below this, a 'NAVIGATION' sidebar on the left contains 'Services', 'App Store', and 'IP-Services'. The main content area is titled 'Virtual Services' and includes a search bar and buttons for 'Copy Service', 'Add Service', and 'Remove Service'. A table lists virtual services with columns for Mode, VIP, VS, Enab..., IP Address, SubNet Mask / Prefix, Port, Service Name, and Service Type. Below this is the 'Real Servers' section, which has tabs for 'Server', 'Basic', 'Advanced', and 'flightPATH'. It features a search bar and buttons for 'Copy Server', 'Add Server', and 'Remove Server'. A table lists real servers with columns for Status, Activity, Address, Port, Weight, Calculated Weight, Notes, and ID. At the bottom of the dashboard, a status bar indicates '[Timed licence 14 days left]'.

Mode	VIP	VS	Enab...	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active			<input checked="" type="checkbox"/>	10.0.0.130	255.255.255.0	80	Web Sites	HTTP(S)

Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
●	Online	10.0.0.20	80	100	50		
●	Online	10.0.0.21	80	100	100		
●	Online	10.0.0.22	80	100	100		

La sezione Navigazione sul lato sinistro consente di navigare nelle varie aree delle funzionalità dell'ADC. Per impostazione predefinita, è selezionata la sezione Servizi e si apre la sottosezione Servizi IP, indicata dalla scheda situata sopra la sezione Servizi virtuali. Questa scheda è fissa e viene sempre visualizzata.

Facendo clic su una sezione all'interno della Navigazione, la sezione viene espansa e il suo contenuto viene rivelato. Facendo clic su un'opzione all'interno di una sezione, si aprirà il contenuto della sezione sul lato destro e una scheda sarà posizionata in alto per consentire un passaggio rapido.

Le diverse sezioni di navigazione sono spiegate in dettaglio nei capitoli successivi.

Servizi

Servizi IP

La sezione Servizi IP dell'ADC consente di aggiungere, eliminare e configurare i vari servizi IP virtuali necessari per il caso d'uso specifico. Le impostazioni e le opzioni sono suddivise nelle sezioni seguenti. Queste sezioni si trovano sul lato destro della schermata dell'applicazione.

Servizi virtuali

Un servizio virtuale combina un IP virtuale, o VIP, e una porta TCP/UDP su cui l'ADC è in ascolto. Il traffico che arriva all'IP virtuale viene reindirizzato a uno dei server reali associati a quel servizio. L'indirizzo IP virtuale non può essere lo stesso dell'indirizzo di gestione dell'ADC, cioè eth0, eth1 ecc...

L'ADC determina il modo in cui il traffico viene ridistribuito ai server in base a un criterio di bilanciamento del carico impostato nella scheda Basic della sezione Real Servers.

Creazione di un nuovo servizio virtuale utilizzando un nuovo VIP

Mode	VIP	VS	Enab...	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	10.0.0.130	255.255.255.0	80	Web Sites	HTTP(S)

- Fare clic sul pulsante Aggiungi servizio virtuale come indicato sopra.

The screenshot shows the 'Virtual Services' configuration page. At the top, there are buttons for 'Copy Service', 'Add Service', and 'Remove Service'. Below is a table with the following data:

Mode	VIP	VS	Enab...	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	10.0.0.130	255.255.255.0	80	Web Sites	HTTP(S)

Below the table, there are 'Update' and 'Cancel' buttons.

Si accede quindi alla modalità di **modifica della riga**.

- Completare i quattro campi evidenziati per procedere, quindi fare clic sul pulsante di aggiornamento.

Utilizzare il tasto TAB per navigare tra i campi.

Campo	Descrizione
Indirizzo IP	Inserite un nuovo indirizzo IP virtuale come punto di ingresso per l'accesso al Real Server. Questo IP è il punto in cui gli utenti o le applicazioni punteranno per accedere all'applicazione bilanciata.
Maschera di sottorete/Prefisso	Questo campo contiene la maschera di sottorete relativa alla rete su cui si trova l'ADC.
Porto	La porta di ingresso utilizzata per accedere al VIP. Questo valore non deve necessariamente essere lo stesso del Real Server se si utilizza il Reverse Proxy.
Nome del servizio	Il nome del servizio è una rappresentazione testuale dello scopo del VIP. È facoltativo, ma si consiglia di fornirlo per chiarezza. Si noti che questo campo viene utilizzato per altri scopi specifici quando si utilizza GSLB.
Tipo di servizio	Sono disponibili diversi tipi di servizio da selezionare. I tipi di servizio Layer 4 non possono utilizzare la tecnologia flightPATH.

A questo punto è possibile premere il pulsante Aggiorna per salvare questa sezione e passare automaticamente alla sezione Real Server descritta di seguito:

Real Servers											
Server											
Basic											
Advanced											
flightPATH											
Group Name: Server Group						Copy Server		Add Server		Remove Server	
Status	Activity	Address	Port	Weight	Cal. Weight	Monitor End Point	Notes	ID			
●	Online	10.0.0.20	80	100	100	Self		WEB1			
●	Online	10.0.0.21	80	100	100	Self		WEB1			
●	Online	10.0.0.22	80	100	100	Self		WEB1			

Campo	Descrizione
Attività	<p>Il campo Attività può essere utilizzato per mostrare e modificare lo stato del server reale con bilanciamento del carico.</p> <p>Online - Indica che il server è attivo e riceve richieste bilanciate.</p> <p>Offline - Il server è offline e non riceve richieste.</p> <p>Drain - Il server è stato posto in modalità drain, in modo che la persistenza possa essere scaricata e il server spostato in uno stato offline senza influenzare gli utenti.</p> <p>Standby - Il server è stato posto in stato di standby.</p>
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 dell'accesso sul Real Server. Quando si utilizza un reverse proxy, questa può essere diversa dalla porta di ingresso specificata sul VIP.
Ponderazione	Questa impostazione viene solitamente configurata automaticamente dall'ADC. È possibile modificarla se si desidera cambiare la ponderazione della priorità.
Cal. Peso	Se si lascia la ponderazione al valore predefinito, l'ADC calcolerà automaticamente la ponderazione in base ai tempi di risposta.
Monitoraggio del punto finale	Il valore predefinito è "Self". Tuttavia, è possibile modificarlo in un valore di Porta o Indirizzo IP:Porta. Il campo viene utilizzato per monitorare un punto finale diverso e determinare se il traffico deve essere passato al Servizio virtuale. Vedere Come utilizzare Monitor End Point .

- Fare clic sul pulsante **Aggiorna** o premere **Invio** per salvare le modifiche.
- La spia di stato diventerà prima grigia e poi verde se la verifica dello stato di salute del server ha successo. Diventerà rossa se il Monitoraggio del server reale non riesce.
- Un server con una spia di stato rossa non viene bilanciato.

Esempio di servizio virtuale completato

Virtual Services										
Search										
Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type		
Active	●	●	✓	10.0.0.142	255.255.255.0	443		HTTP(S)		
Active	●	●	✓	10.0.0.142	255.255.255.0	80		HTTP(S)		
Active	●	●	✓	10.0.0.143	255.255.255.0	443		HTTP(S)		

Real Servers											
Server											
Basic											
Advanced											
flightPATH											
Group Name: Server Group						Copy Server		Add Server		Remove Server	
Status	Activity	Address	Port	Weight	Cal. Weight	Monitor End Point	Notes	ID			
●	Online	10.0.0.20	80	100	100	Self	Web1	web1			
●	Online	10.0.0.21	80	100	100	Self	Web2	web2			
●	Online	10.0.0.22	80	100	100	Self	Web3	web3			

Come utilizzare Monitor End Point

Esempio 1

Prendiamo l'esempio di un'infrastruttura che comprende due server web bilanciati che forniscono un'applicazione web all'utente finale. L'applicazione web è collegata a un server di database nel back-end. L'accesso al server di database si interrompe, ma i server dell'applicazione web rimangono in funzione. Gli utenti cercano di utilizzare l'applicazione web e ricevono errori.

La soluzione è utilizzare Monitor End Point.

The screenshot shows two parts of the configuration interface. The top part, 'Virtual Services', shows a table with two active services. The bottom part, 'Real Servers', shows a table with three servers: two online and one in standby mode.

Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active	●	●	☑	10.0.0.142	255.255.255.0	443		HTTP(S)
Active	●	●	☑	10.0.0.142	255.255.255.0	80		HTTP(S)
Active	●	●	☑	10.0.0.143	255.255.255.0	443		HTTP(S)

Status	Activity	Address	Port	Weight	Cal. Weight	Monitor End Point	Notes	ID
●	Online	10.0.0.20	80	100	100	10.0.0.111:4033	Web1	web1
●	Online	10.0.0.21	80	100	100	10.0.0.111:4033	Web2	web2
●	Standby	10.0.0.22	80	100	100	Self	Web3	web3

- L'esempio mostra due server Web, 10.0.0.20 e 10.0.0.21, insieme a un terzo server Web 10.0.0.22. Il server 10.0.0.22 è stato messo in modalità standby.
- I due server Web attivi sono stati configurati con un valore di Monitoring End Point pari a 10.0.0.111:4033, che è l'indirizzo IP e la porta di connessione del server del database.
- Nel caso in cui la connessione al server di database dovesse cadere, i due server attivi saranno messi in modalità offline e il server di standby sarà online, servendo una pagina web che potrebbe informare il cliente che i sistemi sono in manutenzione.

Esempio 2

Un altro esempio di utilizzo di Monitor End Point si ha quando si effettua il bilanciamento del carico dei server di protocollo UDP, come ad esempio Always-On-VPN. Come è noto, le porte UDP non sono monitorate in modo affidabile e quindi è necessario monitorare una porta TCP.

L'uso di Monitor End Point ci permette di fare proprio questo. La porta principale utilizzata dai server Always-on-VPN sarà la 53/udp, ma voi monitorerete ad esempio la 8433/tcp. In questo caso, è sufficiente inserire il valore della porta nel campo Monitor End Point.

Creazione di servizi secondari virtuali

È inoltre possibile avere servizi virtuali secondari nei casi in cui sia necessario bilanciare il carico utilizzando porte diverse sullo stesso VIP. Ad esempio, è possibile che l'accesso ai server avvenga tramite lo stesso IP virtuale sulle porte 80, 8088 e 443, per cui sarà necessario creare dei servizi sub-virtuali.

- Evidenziare il servizio virtuale che si desidera copiare.
- Fare clic su **Aggiungi servizio virtuale** per accedere alla modalità di modifica della riga.

The screenshot shows the 'Virtual Services' configuration interface. A service is highlighted in blue, showing its configuration details.

Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active	●	●	☑	10.0.0.130	255.255.255.0	80	Web Sites	HTTP(S)
		●	☑	10.0.0.130	255.255.255.0	443	Web Sites 443	HTTP(S)

- L'indirizzo IP e la maschera di sottorete vengono copiati automaticamente.
- Immettere il numero di porta del servizio.
- Inserire un nome di servizio opzionale
- Selezionare un tipo di servizio.
- A questo punto è possibile premere il pulsante Aggiorna per salvare questa sezione e passare automaticamente alla sezione Real Server, riportata di seguito.

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

- Lasciare l'opzione Attività del server come Online: ciò significa che verrà bilanciato il carico se supera il monitoraggio predefinito dello stato di salute di TCP Connect. Questa impostazione può essere modificata in seguito, se necessario.
- Inserire un indirizzo IP per il Real Server
- Inserire un numero di porta per il Real Server
- Inserire un nome opzionale per il Real Server nel campo Note. Ricordate che questo campo note viene utilizzato per altri scopi specifici, come ad esempio nelle variabili flightPATH, ecc.
- Fare clic su Aggiorna per salvare le modifiche.
- La spia di stato diventa prima grigia e poi verde se il Real Server Monitor ha successo. Diventa rossa se il Real Server Monitor fallisce.
- Un server con una spia di stato rossa non viene bilanciato.

Modifica dell'indirizzo IP di un servizio virtuale

È possibile modificare l'indirizzo IP di un servizio virtuale o di un VIP esistente in qualsiasi momento.

- Evidenziare il servizio virtuale di cui si desidera modificare l'indirizzo IP.
- Fare clic sul campo dell'indirizzo IP di quel servizio per renderlo modificabile.

Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Active	Green	Green	✓	10.0.0.130		80	Web Sites	HTTP(S)
Passive		Green	✓	10.0.0.131	255.255.255.0	443	Web Sites 443	HTTP(S)

- Modificare l'indirizzo IP con quello che si desidera utilizzare
- Fare clic sul pulsante Aggiorna per salvare le modifiche.

Nota: la modifica dell'indirizzo IP di un servizio virtuale comporta la modifica dell'indirizzo IP di tutti i servizi associati al VIP.

Creare un nuovo servizio virtuale utilizzando Copy Service

- Il pulsante Copia servizio copia un intero servizio, compresi tutti i Real Server, le impostazioni di base, le impostazioni avanzate e le regole flightPATH ad esso associate.
- Evidenziare il servizio che si desidera duplicare e fare clic su Copia servizio.
- Viene visualizzato l'editor delle righe con il cursore lampeggiante sulla colonna Indirizzo IP.

- È necessario modificare l'indirizzo IP in modo che sia unico o, se si desidera mantenere l'indirizzo IP, è necessario modificare la Porta in modo che sia unica per quell'indirizzo IP.

Ricordarsi di modificare ogni scheda se si cambia un'impostazione, ad esempio un criterio di bilanciamento del carico, il monitor Real Server o si rimuove una regola flightPATH.

Filtrare i dati visualizzati

Ricerca di un termine specifico

La casella Cerca consente di cercare nella tabella utilizzando qualsiasi valore, ad esempio gli ottetti dell'indirizzo IP o il nome del servizio.

Selezione della visibilità delle colonne

È inoltre possibile selezionare le colonne che si desidera visualizzare nel dashboard.

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

Columns

- Status
- Activity
- Address
- Port
- Weight
- Calculated Weight
- Notes
- ID

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

Informazioni sulle colonne dei servizi virtuali

Primario/Modalità

La colonna Modalità indica il ruolo di alta disponibilità selezionato per il VIP corrente. Per le modalità, vedere Sistema > Clustering > Ruoli.

Opzione	Descrizione
Attivo	In modalità Cluster, il valore di questo campo è Attivo. Quando si dispone di una coppia HA di appliance ADC nel datacenter, una di esse mostrerà Attivo e l'altra Passivo. Se l'appliance corrente
Passivo	Quando l'ADC agisce come membro secondario di un cluster, nella colonna Modalità è indicato Passivo.
Manuale	Il ruolo Manuale consente alla coppia di ADC di funzionare in modalità Attiva-Attiva per diversi indirizzi IP virtuali. In questi casi, la colonna Primary conterrà una casella accanto a ciascun IP virtuale unico, selezionabile per Attivo o lasciata deselezionata per Passivo.
Stand-Alone	L'ADC opera come dispositivo autonomo e non è in modalità High Availability. Pertanto, la colonna Primary indicherà Stand-alone.

VIP

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

LED	Significato
	In linea
	Failover-Standby. Questo servizio virtuale è in hot-standby

●	Indica che un "secondario" sta aspettando un "primario".
●	Servizio Necessita di attenzione. Questa indicazione può derivare dal fatto che un Real Server non ha superato un controllo di salute o è stato modificato manualmente in Offline. Il traffico continuerà a scorrere, ma con una capacità ridotta del Real Server.
●	Offline. I server dei contenuti non sono raggiungibili o non è abilitato alcun server dei contenuti.
●	Stato di ritrovamento
●	IP virtuali non licenziati o licenziati superati

Abilitato

L'impostazione predefinita per questa opzione è Attivato e la casella di controllo viene visualizzata come selezionata. È possibile disattivare il Servizio virtuale facendo doppio clic sulla riga, deselegionando la casella di controllo e facendo quindi clic sul pulsante Aggiorna.

Indirizzo IP

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

Maschera di sottorete/Prefisso

Aggiungere la maschera di sottorete in notazione decimale punteggiata. Esempio "255.255.255.0". Si può anche utilizzare il valore della sottorete, ad esempio /24, oppure, per IPv6, aggiungere il prefisso. Per ulteriori informazioni su IPv6, consultare [HTTPS://EN.WIKIPEDIA.ORG/WIKI/IPV6_ADDRESS](https://en.wikipedia.org/wiki/IPv6_address)

Porto

Aggiungere il numero di porta associato al servizio. La porta può essere un numero di porta TCP o UDP. Ad esempio TCP "80" per il traffico Web e TCP "443" per il traffico Web protetto. È anche possibile specificare un intervallo di valori, ad esempio 80-87.

Attualmente non è possibile utilizzare valori separati da virgole per specificare valori di porta non contigui.

Nome del servizio

Aggiungete un nome amichevole per identificare il vostro servizio. Esempio: "Server Web di produzione". Questo campo viene utilizzato anche quando si utilizza GSLB.

Tipo di servizio

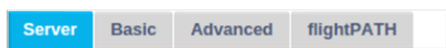
Si noti che con tutti i tipi di servizio "Layer 4", l'ADC non interagirà né modificherà il flusso di dati, pertanto flightPATH non è disponibile con i tipi di servizio Layer 4. I servizi Layer 4 si limitano a bilanciare il traffico in base alla politica di bilanciamento del carico:

Tipo di servizio	Porta/protocollo	Livello di servizio	Commento
Layer 4 TCP	Qualsiasi porta TCP	Strato 4	L'ADC non altera alcuna informazione nel flusso di dati ed esegue il bilanciamento standard del traffico in base alla politica di bilanciamento del carico.
Livello 4 UDP	Qualsiasi porta UDP	Strato 4	Come per il Layer 4 TCP, l'ADC non altera alcuna informazione nel flusso di dati ed esegue il bilanciamento del carico

			standard del traffico in base alla politica di bilanciamento del carico.
Livello 4 TCP/UDP	Qualsiasi porta TCP o UDP	Strato 4	È l'ideale se il servizio ha un protocollo primario come UDP, ma che ricade su TCP. L'ADC non altera alcuna informazione nel flusso di dati ed esegue il bilanciamento standard del traffico in base alla politica di bilanciamento del carico.
DNS	TCP/UDP	Strato 4	Utilizzato per bilanciare il carico dei server DNS.
HTTP(S)	Protocollo HTTP o HTTPS	Strato 7	L'ADC può interagire, manipolare e modificare il flusso di dati utilizzando flightPATH.
FTP	Protocollo di trasferimento file	Strato 7	Utilizzo di connessioni di controllo e di dati separate tra client e server
SMTP	Protocollo di trasferimento della posta semplice	Strato 4	Da utilizzare per il bilanciamento del carico dei server di posta
POP3	Protocollo dell'ufficio postale	Strato 4	Da utilizzare per il bilanciamento del carico dei server di posta
IMAP	Protocollo di accesso ai messaggi Internet	Strato 4	Da utilizzare per il bilanciamento del carico dei server di posta
PSR	Protocollo desktop remoto	Strato 4	Da utilizzare per il bilanciamento del carico dei server di Terminal Services
RPC	Chiamata di procedura remota	Strato 4	Da utilizzare per il bilanciamento del carico dei sistemi che utilizzano chiamate RPC.
RPC/ADS	RPC statico di Exchange 2010 per il servizio di rubrica	Strato 4	Da utilizzare per il bilanciamento del carico dei server Exchange
RPC/CA/PF	Exchange 2010 RPC statico per accesso client e cartelle pubbliche	Strato 4	Da utilizzare per il bilanciamento del carico dei server Exchange
DICOM	Imaging digitale e comunicazione in medicina	Strato 4	Da utilizzare per il bilanciamento del carico dei server che utilizzano i protocolli DICOM.

Server reali

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



Server

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

Status	Activity	Address	Port	Weight	Calculated Weight	Monitor End Point	Notes	ID
+	Online	10.0.020	80	100	100	Self		
+	Online	10.0.021	80	100	100	Self		
+	Online	10.0.022	80	100	100	Self		

Aggiungi server

- Selezionare il VIP appropriato definito in precedenza.
- Fare clic su Aggiungi server
- Viene visualizzata una nuova riga con il cursore lampeggiante sulla colonna Indirizzo IP.
- Inserire l'indirizzo IPv4 del server in notazione decimale punteggiata. Il server reale può trovarsi sulla stessa rete del servizio virtuale, su qualsiasi rete locale collegata direttamente o su qualsiasi rete che l'ADC può instradare. Esempio "10.1.1.1".
- Passare alla colonna Porta e inserire il numero di porta TCP/UDP del 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 proxy inversa. L'ADC tradurrà automaticamente questo numero.
- Passare alla sezione Note per aggiungere qualsiasi dettaglio rilevante per il server. Esempio: "IIS Web Server 1"

Nome del gruppo

Status	Activity	Address	Port	Weight	Calculated Weight	Monitor End Point	Notes	ID
Online	Online	10.0.020	80	100	100	Self		
Online	Online	10.0.021	80	100	100	Self		
Online	Online	10.0.022	80	100	100	Self		

Una volta aggiunti i server che compongono il set di bilanciamento del carico, è possibile aggiungere anche il nome del gruppo. Una volta modificato questo campo, il contenuto viene salvato senza dover premere il pulsante Aggiorna.

Spie di stato del server reale

Lo stato di un Real Server è visibile dal colore della luce nella colonna Stato. Vedere sotto:

LED	Significato
●	Collegato
●	Non monitorato
●	Drenaggio
●	Non in linea
●	Standby
●	Non collegato
●	Stato della ricerca
●	Server reali non autorizzati o con licenza superata

Attività

È possibile modificare l'attività di un Real Server in qualsiasi momento utilizzando il menu a discesa. A tale scopo, fare doppio clic su una riga del Real Server per portarla in modalità di modifica.

Opzione	Descrizione
In linea	Tutti i Real Server assegnati online riceveranno il traffico in base alla politica di bilanciamento del carico impostata nella scheda Base.
Drenaggio	Tutti i Real Server assegnati come Drain continueranno a servire le connessioni esistenti, ma non accetteranno nuove connessioni. La spia di stato lampeggia in verde/blu mentre è in corso il drenaggio. Una volta che le connessioni esistenti di si sono chiuse naturalmente, i Real Server andranno offline e l'indicatore di stato sarà blu fisso. È possibile visualizzare queste connessioni anche navigando nella sezione Navigazione > Monitor > Stato. Il comportamento di scarico può essere modificato nella scheda Impostazioni avanzate.
Non in linea	Tutti i Real Server impostati come Offline saranno immediatamente messi offline e non riceveranno alcun traffico.
Standby	Tutti i server reali impostati come Standby rimarranno offline fino a quando TUTTI i server del gruppo Online non supereranno i controlli di Server Health Monitor. In questo caso, il traffico viene ricevuto dal gruppo Standby in base alla politica di bilanciamento del carico. Se un server del gruppo Online supera il controllo dello stato di salute del server, questo server Online riceverà tutto il traffico e il gruppo Standby smetterà di riceverlo.

Indirizzo IP

Questo campo è l'indirizzo IP del 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 viene specificato un criterio di bilanciamento del carico appropriato.

Il peso predefinito per un Real Server è 100, ma è possibile inserire valori da 1 a 100. Un valore di 100 significa carico massimo, mentre 1 significa carico minimo. Un valore di 100 significa carico massimo e 1 significa carico minimo.

Un esempio per tre server può essere simile a questo:

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

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

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

Se si utilizza Round Robin come metodo di bilanciamento del carico, che fa ruotare le richieste attraverso l'insieme dei server bilanciati, la modifica dei pesi influisce sulla frequenza con cui i server vengono scelti come destinazione.

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

Peso calcolato

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

Monitoraggio del punto finale

Questa funzione consente di specificare particolari endpoint da monitorare e quindi di determinare lo stato di salute della voce Real Server. È possibile lasciare il valore predefinito di "Self", che si affida ai monitor del Real Server specificati per il Virtual Service. In alternativa, è possibile specificare un indirizzo IP, una porta o un indirizzo IP:porta per monitorare un altro endpoint della rete. Ad esempio, un server di database da cui dipendono i servizi.

Note

Inserire nel campo Note qualsiasi nota utile a descrivere la voce definita. Esempio "IIS Server1 - London DC". Questo campo può essere utilizzato per esigenze specifiche nell'ambito delle regole flightPATH e GSLB.

ID

Questa impostazione ha una serie di utilizzi.

Persistenza

Il valore può essere usato insieme al metodo di persistenza basato sull'ID del cookie. Questo metodo è molto simile alla persistenza basata sulla sessione di PHP, ma utilizza una nuova tecnica chiamata Cookie ID Based e cookie RegEx `h=[^:;]+`. Il metodo di persistenza basato sull'ID del cookie utilizza il valore del campo ID per generare un cookie.

flightPATH Uso

È inoltre possibile utilizzare il valore di questo campo per indirizzare il traffico, ecc.

Base

Server
Basic
Advanced
flightPATH

Load Balancing Policy:	Least Connections	▼
Server Monitoring:	TCP Connection	▼
Caching Strategy:	Off	▼
Acceleration:	Compression	▼
Virtual Service SSL Certificate:	No SSL	▼
Real Server SSL Certificate:	No SSL	▼

↻ Update

Politica di bilanciamento del carico

L'elenco a discesa mostra i criteri di bilanciamento del carico attualmente supportati e disponibili per l'uso. Di seguito è riportato un elenco dei criteri di bilanciamento del carico, corredato da una spiegazione.

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

Opzione	Descrizione
Connessioni minime	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.
Il più veloce	Il criterio di bilanciamento del carico più veloce calcola automaticamente il tempo di risposta di tutte le richieste per server, livellato nel tempo. La colonna Peso calcolato contiene il valore calcolato automaticamente. L'inserimento manuale è possibile solo quando si utilizza questo criterio di bilanciamento del carico.
Cookie persistente	Layer 7 Affinità/persistenza della sessione La modalità di bilanciamento del carico basata sull'elenco IP viene utilizzata per ogni prima richiesta. L'ADC inserisce un cookie nelle intestazioni della prima risposta HTTP. Successivamente, l'ADC utilizza il cookie del client per instradare il traffico verso lo stesso server back-end. Questo cookie viene utilizzato per la persistenza quando il client deve andare ogni volta allo stesso server back-end. Il cookie scade dopo 2 ore e la connessione viene bilanciata in base a un algoritmo basato su un elenco di IP. Questo tempo di scadenza è configurabile tramite jetPACK.
Round Robin	Round Robin è comunemente utilizzato nei firewall e nei bilanciatori di carico di base ed è il metodo più semplice. Ogni server reale riceve una nuova richiesta in sequenza. Questo metodo è adatto solo quando è necessario bilanciare il carico delle richieste ai server in modo uniforme; un esempio potrebbe essere quello dei server web di ricerca. Tuttavia, quando è necessario bilanciare il carico in base al carico dell'applicazione o al carico del server, o anche per garantire l'utilizzo dello stesso server per la sessione, il metodo Round Robin è inappropriato.
IP Bound	Cookie di Affinità/Persistenza di sessione di livello 3. In questa modalità, l'indirizzo IP del client costituisce la base per selezionare il Real Server che riceverà la richiesta. Questa azione garantisce la persistenza. I protocolli HTTP e Layer 4 possono utilizzare questa modalità. Questo metodo è utile per le reti interne in cui la topologia della rete è nota e si può essere sicuri che non ci siano "super proxy" a monte. Con il Layer 4 e i proxy, tutte le richieste possono sembrare provenienti da un unico client e quindi il carico non sarebbe uniforme. Con HTTP, le informazioni dell'intestazione (X-Forwarder-For) vengono utilizzate quando sono presenti per far fronte ai proxy.
Elenco IP	La connessione al Real Server inizia utilizzando "Least connections", quindi l'affinità di sessione è ottenuta in base all'indirizzo IP del client. Per impostazione predefinita, l'elenco viene mantenuto per 2 ore, ma può essere modificato con un jetPACK.
Elenco IP condiviso basato su	Questo tipo di servizio è disponibile solo quando la modalità di connettività è impostata su Ritorno diretto al server. È stato aggiunto principalmente per il supporto del bilanciamento del carico VMware.

Cookie persistente	<p>Layer 7 Affinità/persistenza della sessione</p> <p>La modalità di bilanciamento del carico basata sull'elenco IP viene utilizzata per ogni prima richiesta. L'ADC inserisce un cookie nelle intestazioni della prima risposta HTTP. Successivamente, l'ADC utilizza il cookie del client per instradare il traffico verso lo stesso server back-end. Questo cookie viene utilizzato per la persistenza quando il client deve andare ogni volta allo stesso server back-end. Il cookie scade dopo 2 ore e la connessione viene bilanciata in base a un algoritmo basato su un elenco di IP. Questo tempo di scadenza è configurabile tramite jetPACK.</p>
Cookie di sessione ASP classico	<p>Active Server Pages (ASP) è una tecnologia lato server di Microsoft. Con questa opzione selezionata, l'ADC manterrà la persistenza della sessione sullo stesso server se un cookie ASP viene rilevato e trovato nell'elenco dei cookie conosciuti. Quando viene rilevato un nuovo cookie ASP, il carico viene bilanciato utilizzando l'algoritmo Least Connections.</p>
Cookie di sessione ASP.NET	<p>Questa modalità si applica ad ASP.net. Con questa modalità selezionata, l'ADC manterrà la persistenza della sessione sullo stesso server se un cookie ASP.NET viene rilevato e trovato nel suo elenco di cookie conosciuti. Quando viene rilevato un nuovo cookie ASP, il carico viene bilanciato utilizzando l'algoritmo Least Connections.</p>
Cookie di sessione JSP	<p>Java Server Pages (JSP) è una tecnologia lato server di Oracle. Con questa modalità selezionata, l'ADC manterrà la persistenza della sessione sullo stesso server se un cookie JSP viene rilevato e trovato nell'elenco dei cookie conosciuti. Quando viene rilevato un nuovo cookie JSP, il carico viene bilanciato utilizzando l'algoritmo Least Connections.</p>
Cookie di sessione JAX-WS	<p>I servizi web Java (JAX-WS) sono una tecnologia lato server di Oracle. Con questa modalità selezionata, l'ADC manterrà la persistenza della sessione sullo stesso server se un cookie JAX-WS viene rilevato e trovato nel suo elenco di cookie conosciuti. Quando viene rilevato un nuovo cookie JAX-WS, il carico viene bilanciato utilizzando l'algoritmo Least Connections.</p>
Cookie di sessione PHP	<p>Personal Home Page (PHP) è una tecnologia open-source sul lato server. Selezionando questa modalità, l'ADC manterrà la persistenza della sessione sullo stesso server quando viene rilevato un cookie PHP.</p>
Persistenza dei cookie RDP	<p>Questo metodo di bilanciamento del carico utilizza il cookie RDP creato da Microsoft e basato su nome utente/dominio per fornire persistenza a un server. Il vantaggio di questo metodo è che la connessione al server può essere mantenuta anche se l'indirizzo IP del client cambia.</p>
Basato su cookie-ID	<p>Un nuovo metodo molto simile a "PhpCookieBased" e ad altri metodi di bilanciamento del carico, ma che utilizza CookieIDBased e cookie RegEx <code>h=[^;]+</code></p> <p>Questo metodo utilizzerà il valore impostato nel campo note del Real Server "ID=X;" come valore del cookie per identificare il server. Si tratta quindi di una metodologia simile a CookieListBased, ma utilizza un nome di cookie diverso e memorizza un valore di cookie univoco, non l'IP criptato, ma l'ID del server reale (letto al momento del caricamento).</p> <p>Il valore predefinito è <code>CookieIDName="h"</code>; tuttavia, se esiste un valore di override nella configurazione delle impostazioni avanzate del server virtuale, utilizzare questo valore. NOTA: se questo valore è impostato, sovrascriviamo l'espressione del cookie di cui sopra per sostituire <code>h=</code> con il nuovo valore.</p> <p>L'ultimo punto è che se arriva un valore di cookie sconosciuto che corrisponde a uno degli ID del server reale, si deve selezionare quel server; altrimenti, si usa il metodo successivo (delegare).</p>

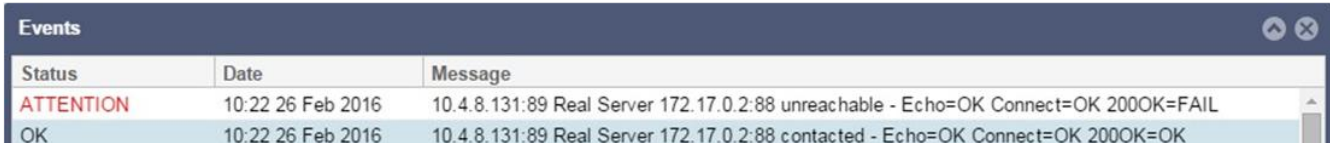
Monitoraggio del server

L'ADC contiene diversi metodi di monitoraggio del Real Server predefiniti.

Scegliere il metodo di monitoraggio che si desidera applicare al servizio virtuale (VIP)

È essenziale scegliere il monitor giusto per il servizio. Ad esempio, se il Real Server è un server RDP, il monitor 200OK non è rilevante. Allo stesso modo, anche la scelta di Connessione TCP e 200OK non ha senso, poiché è necessaria una connessione TCP funzionante per far funzionare 200OK. Se non si è sicuri di quale monitor scegliere, quello predefinito TCP Connection è un ottimo punto di partenza

È possibile scegliere più monitor facendo clic su ciascun monitor che si desidera applicare al servizio. I monitor selezionati vengono eseguiti nell'ordine in cui sono stati selezionati; quindi si con i monitor dei livelli inferiori. Ad esempio, impostando i monitor Ping/ICMP Echo, TCP Connection e 200OK, gli eventi della dashboard verranno visualizzati come nell'immagine seguente:



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

Se osserviamo la riga superiore, possiamo notare che il Layer 3 Ping e il Layer 4 TCP Connect hanno avuto successo, ma il Layer 7 200OK è fallito. Questi risultati del monitoraggio forniscono informazioni sufficienti per indicare che il routing è corretto e che c'è un servizio in esecuzione sulla porta pertinente, ma sito web non risponde correttamente alla pagina richiesta. È ora il momento di esaminare il webserver e la sezione Libreria > Monitor del server reale per vedere i dettagli del monitor fallito.

Opzione	Descrizione
Nessuno	In questa modalità, il Real Server non viene monitorato ed è sempre attivo e funzionante correttamente. L'impostazione Nessuno è utile per le situazioni in cui il monitoraggio disturba un server e per i servizi che non dovrebbero partecipare all'azione di fail-over dell'ADC. È un modo per ospitare sistemi inaffidabili o legacy che non sono primari per le operazioni H/A. Utilizzare questo metodo di monitoraggio con qualsiasi tipo di servizio.
Eco Ping/ICMP	In questa modalità, l'ADC invia una richiesta di echo ICMP all'IP del server di contenuti. Se viene ricevuta una risposta echo valida, l'ADC considera il Real Server attivo e funzionante e il traffico verso il server continua. Inoltre, manterrà il servizio disponibile su una coppia H/A. Questo metodo di monitoraggio è utilizzabile con qualsiasi tipo di servizio.
Connessione TCP	In questa modalità, viene stabilita una connessione TCP al Real Server, che viene immediatamente interrotta senza inviare alcun dato. 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; attualmente i servizi UDP non sono adatti al monitoraggio della connessione TCP.
ICMP non raggiungibile	L'ADC invia un controllo dello stato di salute UDP al server e contrassegna il Real Server come non disponibile se riceve un messaggio ICMP di porta non raggiungibile. Questo metodo può essere utile quando è necessario verificare se una porta di servizio UDP è disponibile su un server, come la porta 53 del DNS.
PSR	In questa modalità, una connessione TCP viene inizializzata 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 considera il Real Server funzionante. 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, viene inizializzata una connessione TCP al Real Server. Dopo che la connessione è riuscita, l'ADC invia al Real Server una richiesta HTTP. Si attende una risposta HTTP e si controlla il codice di risposta "200 OK". L'ADC considera il Real Server attivo e funzionante se riceve il codice di risposta "200 OK". Se l'ADC non riceve un codice di risposta "200 OK" per qualsiasi motivo, compresi i timeout, la mancata

	connessione e altri motivi, l'ADC considera il Real Server non disponibile. Questo metodo di monitoraggio è valido solo per i tipi di servizio HTTP e HTTP accelerato. Se si utilizza un tipo di servizio Layer 4 per un server HTTP, è possibile utilizzarlo se SSL non è in uso sul Real Server o è gestito in modo appropriato dalla funzione "Content SSL".
DICOM	Viene inizializzata una connessione TCP al Real Server in modalità DICOM e al momento della connessione viene effettuata una "Richiesta di associazione" di Echoscu al Real Server. Una conversazione che include un "Associate Accept" dal server dei contenuti, un trasferimento di una piccola quantità di dati seguito da un "Release Request" e da un "Release Response" conclude con successo il monitor. Se il monitoraggio non si conclude con successo, il Real Server viene considerato inattivo per qualsiasi motivo.
Definito dall'utente	Qualsiasi monitor configurato nella sezione Monitoraggio del server reale apparirà nell'elenco.

Strategia di caching

Per impostazione predefinita, la Strategia di caching è disattivata e impostata su Off. Se il tipo di servizio è HTTP, è possibile applicare due tipi di strategia di caching.

Per configurare le impostazioni dettagliate della cache, consultare la pagina Configura cache. Si noti che quando la cache viene applicata a un VIP con il tipo di servizio "HTTP" accelerato, gli oggetti compressi non vengono memorizzati nella cache.

Opzione	Descrizione
Da parte di Host	La cache per host si basa sull'applicazione per nome di host. Per ogni dominio/nome host esiste una cache separata. Questa modalità è ideale per i server web che possono servire più siti web a seconda del dominio.
Per Servizio Virtuale	La cache per servizio virtuale è disponibile quando si sceglie questa opzione. Esisterà una sola cache per tutti i domini/nomi di host che passano attraverso il servizio virtuale. Questa opzione è un'impostazione specializzata per l'uso con più cloni di un singolo sito.

Accelerazione

Opzione	Descrizione
Spento	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 client su richiesta. Questo processo si applica solo agli oggetti che contengono l'intestazione content-encoding: gzip. Un esempio di contenuto è HTML, CSS o JavaScript. È inoltre possibile escludere alcuni tipi di contenuto utilizzando la sezione Esclusioni globali.

Nota: Se l'oggetto è memorizzabile nella cache, l'ADC memorizzerà una versione compressa e la servirà staticamente (dalla memoria) finché il contenuto non scade e viene riconvalidato.

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

L'impostazione predefinita è Nessun SSL. Se il tipo di servizio è "HTTP", è possibile selezionare un certificato dall'elenco a discesa da applicare al servizio virtuale. I certificati creati o importati appariranno in questo elenco.

È anche possibile evidenziare più certificati da applicare a un servizio. Questa operazione abilita automaticamente l'estensione SNI a consentire un certificato basato sul "Nome di dominio" richiesto dal client.

Virtual Service SSL Certificate: 

No SSL
All
default
AnyUseCert

Opzione	Descrizione
No SSL	Il traffico dalla sorgente all'ADC non è crittografato.
Tutti	Carica tutti i certificati disponibili per l'uso
Predefinito	Questa opzione comporta l'applicazione di un certificato creato localmente chiamato "Default" al lato browser del canale. Utilizzare questa opzione per testare l'SSL quando non è stato creato o importato.

Certificato SSL del Real Server (crittografia tra l'ADC e il Real Server)

L'impostazione predefinita per questa opzione è No SSL. Se il server richiede una connessione crittografata, questo valore deve essere diverso da Nessun SSL. I certificati creati o importati appariranno in questo elenco.

No SSL
Any
SNI
default

Opzione	Descrizione
No SSL	Il traffico dall'ADC al Real Server non è criptato. La selezione di un certificato sul lato browser significa che "No SSL" può essere scelto sul lato client per fornire il cosiddetto "SSL Offload".
Qualsiasi	L'ADC agisce come client e accetta qualsiasi certificato presentato dal Real Server. Il traffico dall'ADC al Real Server è crittografato quando si seleziona questa opzione. Utilizzare l'opzione "Qualsiasi" quando viene specificato un certificato sul lato del servizio virtuale, per ottenere il cosiddetto "SSL Bridging" o "SSL Re-Encryption".
SNI	SNI, o Server Name Indication, è un'estensione del protocollo di rete TLS che consente al client di indicare il nome dell'host a cui sta tentando di connettersi all'inizio del processo di handshaking . Questa impostazione consente all'ADC di presentare più certificati sullo stesso indirizzo IP virtuale e sulla stessa porta TCP.
Predefinito	I certificati autofirmati generati appaiono qui.

Avanzato

Real Servers

Server Basic Advanced flightPATH

Connectivity: Reverse Proxy	Connection Timeout (sec): 600
Cipher Options: Defaults	Persistence Timeout (sec):
Client SSL Renegotiation: <input checked="" type="checkbox"/>	Monitoring Interval (sec): 10
Client SSL Resumption: <input checked="" type="checkbox"/>	Monitoring Timeout (sec): 2
SNI Default Certificate: None	Monitoring In Count: 2
Client Proxy Header: None	Monitoring Out Count: 3
Server Proxy Header: None	Monitoring KCD Realm: None
Real Server Source Address: Base IP	Drain Behaviour: Persistence Driven
Security Log: On	Switch To Offline On Failure: <input type="checkbox"/>
Max. Connections (Per Real Server): 	

Update

Connettività

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

Opzione	Descrizione
Proxy inverso	Reverse Proxy è il valore predefinito e utilizza la compressione e la cache quando viene usato con il Layer 7. Al livello 4, il reverse proxy funziona senza cache o compressione. In questa modalità, l'ADC agisce come reverse proxy e diventa l'indirizzo sorgente visto dai Real Server.
Ritorno diretto del server	<p>Il Direct Server Return o DSR, noto anche come DR - Direct Routing, consente al server dietro il bilanciatore di carico di rispondere direttamente al client, bypassando l'ADC sulla risposta. Il DSR è adatto solo per l'uso con il bilanciamento del carico di livello 4. Pertanto, la cache e la compressione non sono disponibili con il DSR. Pertanto, la cache e la compressione non sono disponibili con questa opzione.</p> <p>Questa modalità può essere utilizzata solo con i tipi di servizio TCP, UDP e TCP/UDP. I criteri di persistenza del bilanciamento del carico sono inoltre limitati a Connessioni minime, Elenco IP condiviso, Round Robin e Elenco IP.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p>Least Connection</p> <p>Shared IP List Based</p> <p style="background-color: #2980b9; color: white; padding: 2px;">Round Robin</p> <p>IP List Based</p> </div> <p>L'utilizzo di DSR richiede anche l'esecuzione di modifiche al Real Server. Consultare la sezione Modifiche al Real Server.</p>
NAT	<p>Per impostazione predefinita, l'ADC utilizza l'indirizzo IP dell'ADC come indirizzo IP di origine e i Real Server inviano la risposta all'ADC per restituirla al Cliente. Questo va bene in quasi tutte le circostanze, ma ci sono scenari in cui il Real Server ha bisogno di vedere l'indirizzo IP di origine del Client e non dell'ADC.</p> <p>Quando si applica la modalità NAT, l'ADC riceve la richiesta in entrata e la invia al Real Server dopo aver modificato l'indirizzo IP di origine in quello del Virtual Service (indirizzo VIP).</p> <p>Questa modalità può essere utilizzata solo con i seguenti criteri di bilanciamento del carico:</p>

	<div data-bbox="395 181 810 293" style="border: 1px solid #ccc; padding: 5px;"> Least Connection Round Robin IP List Based </div>
Porta d'ingresso	<p>La modalità gateway consente di instradare tutto il traffico attraverso l'ADC, permettendo ai Real Server di essere instradati attraverso l'ADC verso altre reti tramite i servizi virtuali o le interfacce hardware dell'ADC. L'uso del dispositivo come gateway per i Real Server è ideale quando si opera in modalità multi-interfaccia.</p> <p>I criteri di persistenza del bilanciamento del carico sono inoltre limitati a Connessioni minime, Elenco IP condiviso, Round Robin e Elenco IP.</p> <div data-bbox="395 533 754 663" style="border: 1px solid #ccc; padding: 5px;"> Least Connection Shared IP List Based Round Robin IP List Based </div> <p>Questo metodo richiede che il Real Server imposti il suo gateway predefinito sull'indirizzo dell'interfaccia locale dell'ADC (eth0, eth1, ecc.). Consultare la sezione Modifiche del Real Server.</p> <p>Si noti che la modalità Gateway non supporta il failover in un ambiente cluster.</p>

Opzioni di cifratura

I cifrari costituiscono la base della crittografia SSL e sono estremamente importanti per il successo e la sicurezza della distribuzione di contenuti e applicazioni web.

L'ADC contiene un set integrato di cifrari predefiniti, che comprende i più aggiornati e sicuri disponibili per l'uso.

In alcuni casi, l'utente desidera annunciare la disponibilità di un particolare insieme di cifrari; l'ADC consente di creare tali cifrari tramite i jetPACK scritti dall'utente. I jetPACK scritti dagli utenti possono essere importati nell'ADC tramite Configurazione > Software, quindi resi disponibili per la scelta tramite il menu Opzioni cifratura.

Le opzioni di cifratura sono specifiche per ogni VIP e garantiscono un'elevata flessibilità e sicurezza.

Per ulteriori informazioni sulle opzioni di cifratura, vedere: *Cipher*

Rinegoziazione SSL del client

Selezionare questa casella se si desidera consentire la rinegoziazione SSL avviata dal client. Disattivare la rinegoziazione SSL del client per prevenire eventuali attacchi DDOS contro il livello SSL, deselegando questa opzione.

Ripresa SSL del cliente

Spuntare questa casella se si desidera abilitare le sessioni SSL Resumption Server aggiunte alla cache di sessione. Quando un client propone il riutilizzo di una sessione, il server cercherà di riutilizzare la sessione, se trovata. Se la casella Ripresa è deselegata, non viene eseguita la cache di sessione per il client o il server.

Certificato predefinito SNI

Durante una connessione SSL con l'SNI lato client abilitato, se il dominio richiesto non corrisponde a nessuno dei certificati assegnati al servizio, l'ADC presenterà il certificato predefinito SNI. L'impostazione predefinita è Nessuno, che di fatto interrompe la connessione se non c'è una corrispondenza esatta. Scegliere uno qualsiasi dei certificati installati dall'elenco a discesa da presentare nel caso in cui non ci sia una corrispondenza esatta con il certificato SSL.

Il protocollo proxy

Il protocollo Proxy è stato progettato per consentire ai proxy di rete di inoltrare le informazioni sulla connessione del client (come l'indirizzo IP di origine e il numero di porta) al server ricevente. Questo protocollo è particolarmente utile negli scenari in cui l'indirizzo IP effettivo dell'utente finale deve essere conservato mentre il traffico viene instradato attraverso un bilanciatore di carico o un reverse proxy. Aiuta a mantenere l'IP di origine del client per scopi di registrazione, statistica o sicurezza, migliorando la capacità di prendere decisioni informate basate sulla vera origine del traffico.

Intestazione proxy del client

L'intestazione Client Proxy si riferisce a un'intestazione aggiunta alla richiesta del client dall'ADC, che incapsula le informazioni di connessione originali (come l'indirizzo IP e la porta del client). Questo è fondamentale negli ambienti in cui l'ADC funge da proxy e il server ha bisogno di conoscere i dettagli originali del client per scopi quali la registrazione, la valutazione della sicurezza e il mantenimento del comportamento specifico del client. L'intestazione Client Proxy garantisce che, nonostante il ruolo di intermediario dell'ADC, il server possa identificare con precisione e interagire con i dati di connessione originali del client.

Le opzioni includono:

Opzione	Descrizione
Nessuno	Quando non c'è un'intestazione Proxy o non è supportata dal tipo di servizio corrente.
Rimuovere	Rimuove l'intestazione Proxy dal pacchetto TCP.
In avanti	Inoltra l'intestazione Proxy al server

Intestazione proxy del server

Esistono due versioni di Server Proxy Headers: Versione 1 e Versione 2.

Opzione	Descrizione
Versione 1	<ul style="list-style-type: none"> • Formato basato sul testo, facile da implementare e da debuggare. • Fornisce informazioni di base sulla connessione del client, tra cui IP di origine, IP di destinazione, porta di origine e porta di destinazione. • La linea di protocollo viene aggiunta all'inizio della connessione TCP, rendendola leggibile all'uomo ma leggermente meno efficiente in termini di prestazioni rispetto ai formati binari.
Versione 2	<ul style="list-style-type: none"> • Formato binario, progettato per migliorare le prestazioni e l'efficienza. • Estende le informazioni che possono essere trasmesse sulla connessione, supportando dati aggiuntivi come la famiglia di indirizzi e le informazioni specifiche del protocollo. • Garantisce una migliore compatibilità con i moderni protocolli e funzionalità di rete, compreso il supporto per IPv6 e i protocolli di trasporto oltre il TCP.

Le opzioni Intestazione proxy del client e Intestazione proxy del server sono disponibili solo per i tipi di servizio HTTP Layer 4 e Layer 7.

Indirizzo sorgente del server reale

Questa impostazione funziona insieme a Reverse Proxy e ai servizi Layer 4 TCP, Layer 4 UDP o HTTP(S). L'impostazione offre tre opzioni tra cui scegliere.

Opzione	Descrizione
IP di base (predefinito)	Utilizza l'indirizzo eth0 o IP di base dell'ADC come IP di origine della richiesta.
IP virtuale	Utilizza l'IP virtuale del servizio.
<indirizzo IP>	Consente di specificare un indirizzo IP che fa parte dell'ADC. Potrebbe trattarsi di un'interfaccia di rete diversa o di un VIP diverso.

Registro di sicurezza

'On' è il valore predefinito e si basa su una base per servizio, abilitando il servizio di registrazione delle informazioni di autenticazione nei log W3C. Facendo clic sull'icona dell'ingranaggio si accede alla pagina Sistema > Registrazione, dove è possibile controllare le impostazioni della registrazione W3C.

Massimo. Connessioni

Limita il numero di connessioni simultanee al Real Server ed è impostato per ogni servizio. Ad esempio, se si configura questo limite a 1000 e si hanno due Real Server, l'ADC limita **ogni** Real Server a 1000 connessioni simultanee. Si può anche scegliere di presentare una pagina "Server troppo occupato" una volta raggiunto questo limite su tutti i server, aiutando gli utenti a capire il motivo di una mancata risposta o di un ritardo. Lasciare vuoto questo campo per avere connessioni illimitate. L'impostazione dipende dalle risorse del sistema.

Timeout della connessione

Il timeout predefinito della connessione è di 600 secondi o 10 minuti. Questa impostazione regola il tempo di timeout della connessione in caso di assenza di attività. Ridurre questo valore per il traffico web stateless di breve durata, che in genere è di 90 minuti o meno. Aumentare questo valore per le connessioni statiche, come RDP, fino a 7200 secondi (2 ore) o più, a seconda dell'infrastruttura. L'esempio del timeout RDP significa che se un utente ha un periodo di inattività di 2 ore o meno, le connessioni rimarranno aperte.

Timeout di persistenza

L'impostazione del timeout di persistenza nei bilanciatori di carico specifica la durata per cui un bilanciatore di carico mantiene le informazioni di sessione per un client. Ciò garantisce che le richieste successive dello stesso client siano dirette allo stesso server backend, promuovendo la coerenza della sessione e la comunicazione statica. Una volta trascorso il periodo di timeout specificato senza ulteriori attività del client, le informazioni di sessione vengono scartate e le nuove richieste possono essere indirizzate a un server diverso.

Intervallo di monitoraggio

L'intervallo è il tempo in secondi tra i monitor. L'intervallo predefinito è di 1 secondo. Sebbene 1 secondo sia 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 il tempo in cui l'ADC attende che il server risponda a una richiesta di connessione. Il valore predefinito è 2s. Aumentare 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 prima di essere online. Aumentando questo valore si aumenta 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 del Real Server deve fallire tre volte prima che l'ADC smetta di inviare traffico al server, che viene contrassegnato come ROSSO e irraggiungibile. Aumentando questo valore si otterrà un servizio migliore e più affidabile, a scapito del tempo necessario all'ADC per interrompere l'invio di traffico a questo server.

Monitoraggio del regno KCD

Questa impostazione consente di abilitare il monitoraggio del Kerberos Constrained Delegation Realm impostato nelle definizioni di Kerberos. Vedere Autenticazione > Kerberos.

Comportamento di scarico

Quando un Real Server viene messo in modalità Drain, è sempre meglio poter controllare il comportamento del traffico che gli viene inviato. Il menu Comportamento di scarico consente di selezionare il comportamento del traffico per ogni servizio virtuale. Le opzioni sono:

Opzione	Descrizione
Persistenza guidata	Questa è la selezione predefinita. Ogni volta che l'utente visita la sessione di persistenza, questa viene estesa. Con un utilizzo di 24 ore, è possibile che lo scarico non avvenga mai. Tuttavia, se il numero di connessioni al server reale raggiunge lo 0, il drenaggio termina, le sessioni di persistenza vengono eliminate e tutti i visitatori vengono ribilanciati alla prossima connessione.
Migrare i visitatori	Sessione persistente ignorata alla nuova connessione (comportamento precedente al 2022) Le nuove connessioni TCP (che facciano parte o meno di una sessione esistente) vengono sempre effettuate a un server reale online. Se la sessione di persistenza era a un server reale in esaurimento, viene sovrascritta. Il servizio virtuale ignorerà di fatto la persistenza delle nuove connessioni, che saranno bilanciate su un nuovo server.
Sessioni di pensionamento	Sessioni persistenti non estese. Le connessioni degli utenti in arrivo vengono assegnate al server desiderato, ma la loro sessione di persistenza non viene estesa. Pertanto, una volta superata la durata della sessione di persistenza, saranno trattate come nuove connessioni e spostate su un altro server.

Passa alla modalità offline in caso di guasto

Quando questa opzione è selezionata, i Real Server che non superano il controllo dello stato di salute vengono messi offline e possono essere rimessi in linea solo manualmente.

voloPATH

flightPATH è una tecnologia di gestione del traffico progettata da Edgenexus e disponibile esclusivamente all'interno dell'ADC. A differenza dei motori basati su regole di altri fornitori, flightPATH non opera attraverso una riga di comando o una console di immissione di script. Utilizza invece un'interfaccia grafica per selezionare i diversi parametri, le condizioni e le azioni da eseguire per raggiungere gli obiettivi desiderati. Queste caratteristiche rendono flightPATH estremamente potente e consentono agli amministratori di rete di manipolare il traffico HTTPS in modo estremamente efficace.

flightPATH è disponibile solo per le connessioni HTTPS e questa sezione non è visibile quando il tipo di servizio virtuale non è HTTP.

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

Applicare una regola disponibile trascinandola dal lato sinistro a quello destro, oppure evidenziando una regola e facendo clic sulla freccia destra per spostarla sul lato destro.

L'ordine di esecuzione è essenziale e inizia con la regola superiore eseguita per prima. Per modificare l'ordine di esecuzione, evidenziare la regola e spostarsi verso l'alto e verso il basso utilizzando le frecce.

È importante capire che le regole del flightPATH in questa sezione dell'ADC funzionano su base booleana **OR**, mentre le condizioni e le azioni nell'area di definizione del flightPATH funzionano su base **AND**.

Per rimuovere una regola, trascinarla e rilasciarla nell'inventario delle regole a sinistra oppure evidenziarla e fare clic sulla freccia a sinistra.

È possibile aggiungere, rimuovere e modificare le regole flightPATH nella sezione Configurazione di flightPATH di questa guida.

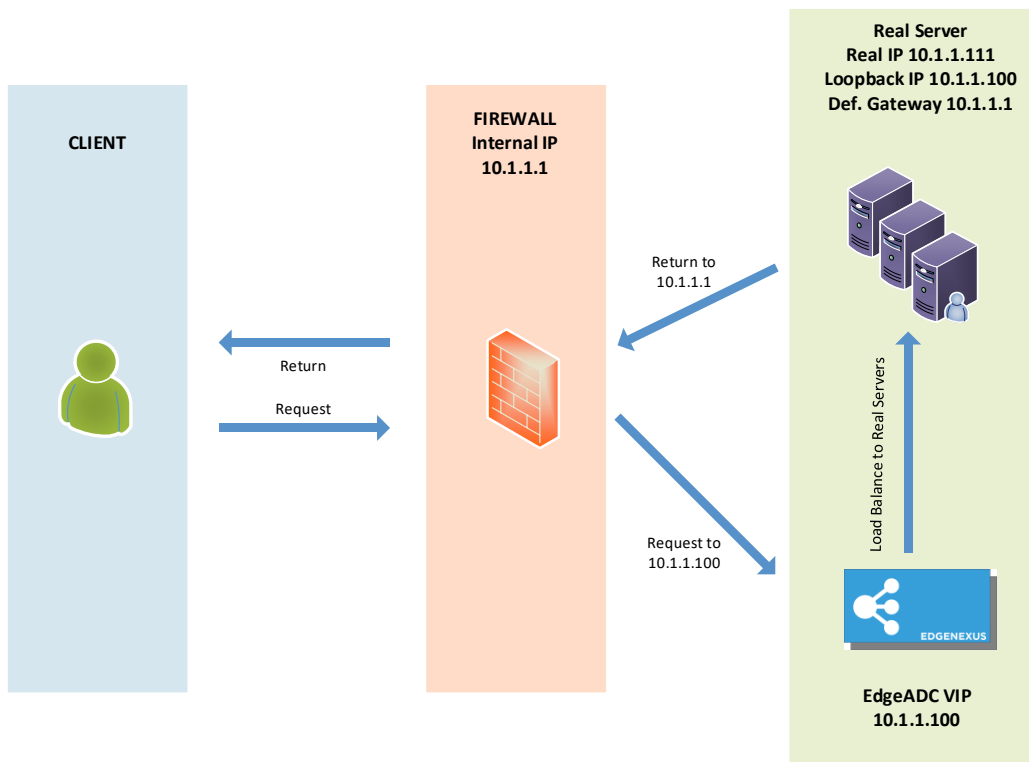
Modifiche al server reale per il ritorno al server diretto

Il Direct Server Return o DSR, come è noto (DR - Direct Routing in alcuni ambienti), consente al server dietro l'ADC di rispondere direttamente al client, bypassando l'ADC nella risposta. DSR è adatto solo per l'uso con il bilanciamento del carico di livello 4. La cache e la compressione non sono disponibili quando sono abilitate.

Il bilanciamento del carico Layer 7 con questo metodo non funziona perché non esiste un supporto di persistenza diverso dall'IP di origine. Il bilanciamento del carico SSL/TLS con questo metodo non è ideale, poiché esiste solo il supporto della persistenza dell'IP di origine.

Come funziona

- Il client invia una richiesta all'EdgeADC VIP
- Richiesta ricevuta da EdgeADC
- Richiesta inoltrata ai server dei contenuti
- Risposta inviata direttamente al client senza passare da EdgeADC



Configurazione del server dei contenuti richiesta

Generale

- Il gateway predefinito del content server deve essere configurato normalmente. (non tramite l'ADC)
- Il server dei contenuti e il bilanciatore di carico devono trovarsi nella stessa sottorete.

Finestre

- Il server dei contenuti 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 - [Fare clic qui](#)
 - Aggiungere un adattatore di loopback in Windows Server 2003/2008 - [Fare clic qui](#)

- Eseguire quanto segue in un prompt dei comandi per ogni interfaccia di rete configurata sui server Windows Real

```
netsh interface ipv4 set interface "nome interfaccia di rete Windows"  
weakhostreceive=enable
```

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

```
netsh interface ipv4 set interface "nome interfaccia loopback di Windows"  
weakhostsendsend=enable
```

Linux

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

```
ifcfg-lo:1
```

```
DISPOSITIVO=lo:1
```

```
IPADDR=x.x.x.x
```

```
NETMASK=255.255.255.255
```

```
BROADCAST=x.x.x.x
```

```
ONBOOT=yes
```

- Modificare "/etc/sysctl.conf".

```
net.ipv4.conf.all.arp_ignore = 1
```

```
net.ipv4.conf.eth0.arp_ignore = 1
```

```
net.ipv4.conf.eth1.arp_ignore = 1
```

```
net.ipv4.conf.all.arp_announce = 2
```

```
net.ipv4.conf.eth0.arp_announce = 2
```

```
net.ipv4.conf.eth1.arp_announce = 2
```

- Eseguire "sysctl - p"

Modifiche al server reale - Modalità gateway

La modalità gateway consente di instradare tutto il traffico attraverso l'ADC, consentendo di instradare il traffico proveniente dai server di contenuti verso altre reti attraverso le interfacce dell'unità ADC. L'uso del dispositivo come gateway per i server di contenuti deve essere utilizzato quando si opera in modalità multi-interfaccia.

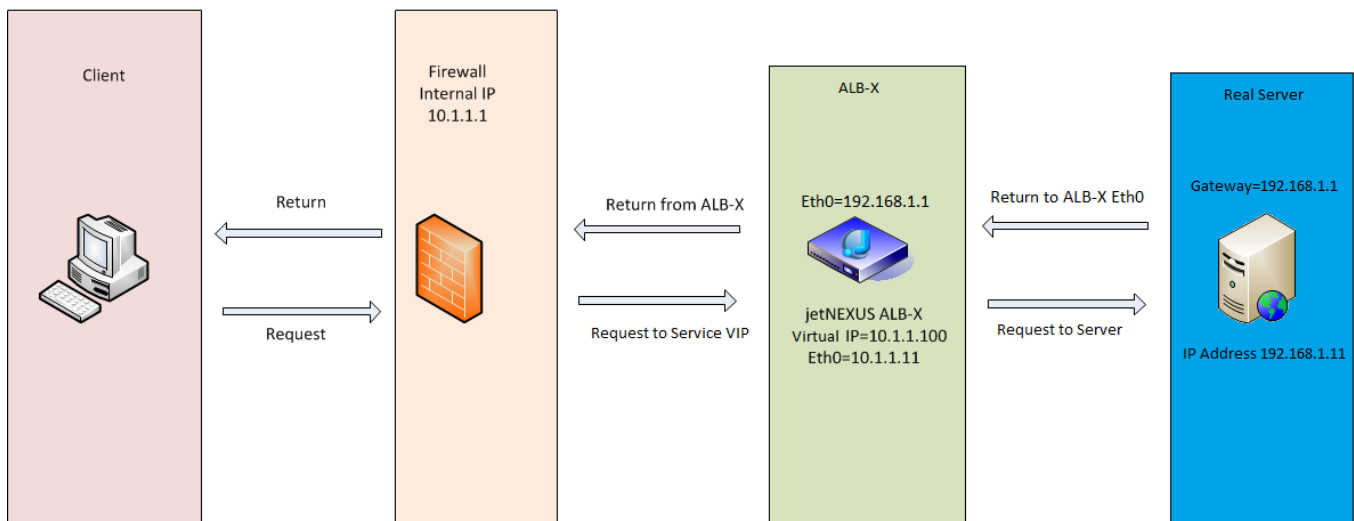
Come funziona

- Il client invia una richiesta all'EdgeADC
- EdgeADC riceve una richiesta
- Richiesta inviata ai server dei contenuti
- Risposta inviata a EdgeADC
- L'ADC inoltra la risposta al client

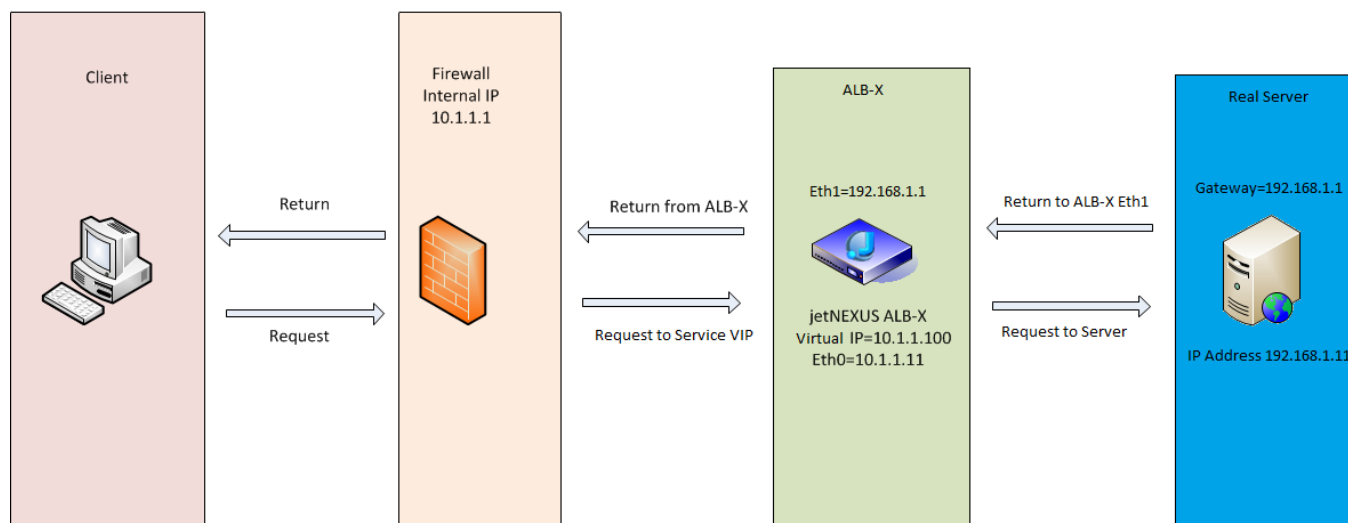
Configurazione del server dei contenuti richiesta

- Modalità a braccio singolo: viene utilizzata un'interfaccia, ma il VIP di servizio e i Real Server devono trovarsi su sottoreti diverse.
- Modalità Dual Arm - vengono utilizzate 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 con l'indirizzo dell'interfaccia ADC sulla relativa subnet.

Esempio di braccio singolo



Esempio di braccio doppio

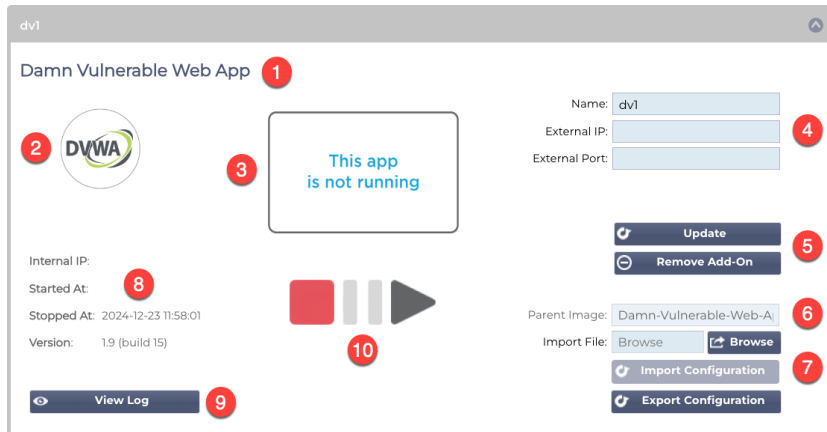


Biblioteca

Componenti aggiuntivi

I componenti aggiuntivi sono applicazioni caricate come contenitori ed eseguite in modalità isolata all'interno dell'ADC. Esempi di componenti aggiuntivi possono essere un firewall applicativo o persino una micro istanza dell'ADC stesso.

Un'applicazione viene distribuita nella sezione Add-Ons utilizzando la pagina App, come descritto in questa guida. Una volta distribuita, l'app appare come segue.



Come si può vedere dall'immagine qui sopra, ci sono diversi elementi che vengono evidenziati.

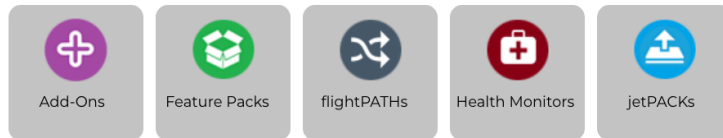
Articolo	Descrizione
1	Titolo dell'applicazione
2	Icona dell'app
3	Visualizzazione dell'applicazione in esecuzione. Se l'app è in esecuzione, viene visualizzata una miniatura dello schermo.
4	Dettagli di accesso: Nome: È un nome interno che si usa per fare riferimento all'applicazione nella sezione Servizi virtuali. Non è possibile fare riferimento a un'app utilizzando il suo indirizzo IP. Solo alfanumerico, senza spazi. IP esterno: è l'indirizzo IP da fornire per l'applicazione. Farà parte della sottorete della vostra rete. Porta esterna: si tratta di un campo importante. È necessario specificare le porte che verranno utilizzate per accedere all'applicazione. Quando si accede al traffico esterno all'applicazione, è necessario specificare la porta utilizzando la seguente notazione: 53/tcp o 53/udp. Inoltre, è necessario specificare la porta dell'interfaccia utente dell'app. Queste sono indicate nel tooltip del campo per ogni app.
5	Pulsante di aggiornamento: Dopo aver compilato i dati specificati in 4, fare clic su questo pulsante per confermare le voci e configurare l'applicazione. Il pulsante Rimuovi Add-On serve a rimuovere l'applicazione dalla sezione Applicazioni. Per rimuovere un'applicazione, assicurarsi che tutti i riferimenti all'applicazione siano stati rimossi prima di tentare la rimozione.
6	L'immagine genitore è un campo informativo e non è utilizzato dall'utente.
7	L'importazione e l'esportazione di una configurazione è importante per mantenere un backup delle impostazioni. Utilizzare questa funzione per eseguire le operazioni di importazione ed esportazione.
8	I dettagli dell'esecuzione forniscono informazioni sull'indirizzo IP dell'API interna, sull'ora di inizio e fine e sul numero di versione dell'applicazione.
9	Questo pulsante consente di scaricare e visualizzare il registro. Viene utilizzato principalmente per aprire un ticket di assistenza.
10	Il funzionamento dell'applicazione avviene tramite questi pulsanti. Rosso=Arresto, Oro=Accensione e Verde=Corso.

Applicazioni

La sezione Applicazioni ha diverse sottosezioni che gestiscono le applicazioni disponibili per l'ADC. Si tratta di Filtro, App scaricate e App acquistate.

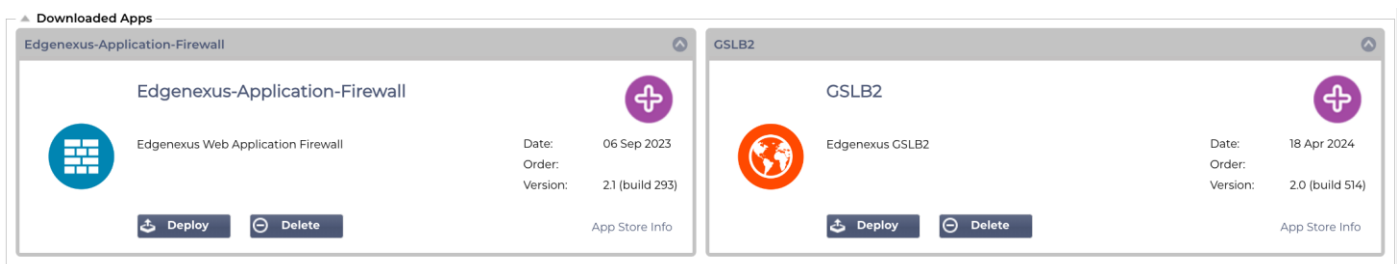
Il filtro

Click icons to toggle groups of apps



Il filtro consente di filtrare le applicazioni/gli strumenti in base al loro tipo.

Applicazioni scaricate

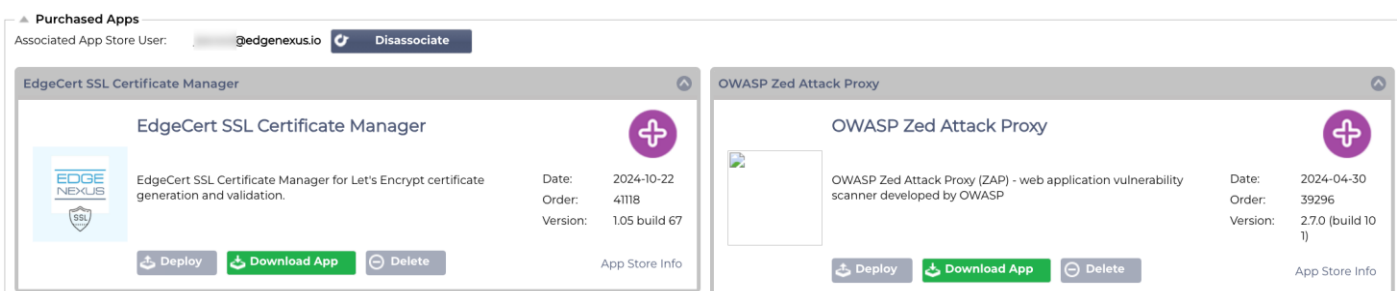


Questa sezione contiene le applicazioni che sono state scaricate sull'ADC. È possibile che siano state scaricate sul desktop locale e successivamente caricate sull'ADC, oppure che siano state scaricate tramite il portale App Store integrato.

Ogni app è dotata di due pulsanti e di dati che indicano il numero di versione e la data di rilascio.

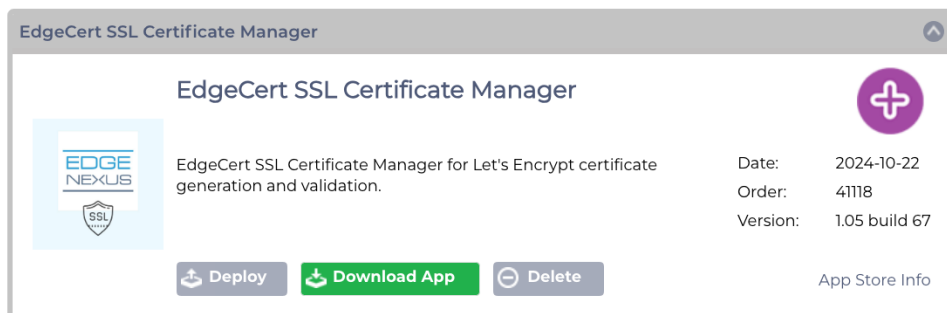
Il pulsante Deploy distribuisce l'applicazione come contenitore protetto, mentre il pulsante Delete elimina l'applicazione dall'ADC.

App acquistata



La prima cosa che si nota è l'Utente App Store associato e il relativo pulsante. È necessario accedere con le credenziali dell'App Store in modo che l'ADC sia associato all'App Store. Sotto di esso si trovano le applicazioni associate al proprio account.

Accedendo all'App Store, direttamente o tramite il portale integrato, è possibile acquistare le applicazioni. Queste sono indicate in questa sezione e possono essere caricate sull'ADC pronte per la distribuzione.



Ogni app ha una serie di pulsanti: Deploy, Download App e Delete. Inoltre, sul lato destro è presente un link App Store Info che porta alla pagina dell'App Store corrispondente e mostra le informazioni sull'addon.

Distribuire

La sezione Applicazioni all'interno di Add-Ons contiene i dettagli delle applicazioni acquistate, scaricate e distribuite. Una volta distribuita, l'applicazione appare nella sezione Scaricati.

Scarica l'applicazione

L'applicazione può essere scaricata dall'App Store facendo clic su questo pulsante.

Cancellare

Se si desidera eliminare un'applicazione che è stata scaricata.

Autenticazione

La pagina Autenticazione della biblioteca> consente di impostare i server di autenticazione e di creare regole di autenticazione.

Impostazione dell'autenticazione - Un flusso di lavoro

Per applicare l'autenticazione al vostro servizio, eseguite almeno i seguenti passaggi.

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

Server di autenticazione

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

La prima fase consiste nel selezionare il metodo di autenticazione necessario.

- Fare clic su Aggiungi server.
- Selezionare il Metodo dal menu a discesa.

The screenshot shows the 'Authentication Servers' configuration interface. At the top, there are 'Add Server' and 'Remove Server' buttons. Below them is a 'Method:' dropdown menu, which is highlighted with a red arrow. To the right of the dropdown are 'Update' and 'Cancel' buttons. Below this is a table with columns: Name, Description, Method, Domain, and Server Address. The table is currently empty.

La funzione Server di autenticazione è dinamica e visualizza solo i campi necessari per il metodo di autenticazione scelto.

- Compilare accuratamente i campi per garantire la corretta connessione ai server.

Opzioni per LDAP, LDAP-MD5, LSAPS, LDAPS-MD5, Radius e SAML

The screenshot shows the 'Authentication Servers' configuration interface with the 'Method' dropdown set to 'LDAP-MD5'. The form fields are as follows:

- Method: LDAP-MD5
- Name: [Text Input]
- Server Address: [Text Input]
- Port: [Dropdown Menu]
- Domain: [Text Input]
- Login Format: Blank
- Description: [Text Input]
- Search Base: [Text Input]
- Search Condition: [Text Input]
- Search User: [Text Input]
- Password: [Text Input]

Below the form are 'Update' and 'Cancel' buttons. At the bottom is a table with columns: Name, Description, Method, Domain, and Server Address. The table is currently empty.

Opzione

Descrizione

Metodo	Scegliere un metodo di autenticazione LDAP - LDAP di base con nomi utente e password inviati in chiaro al server LDAP. LDAP-MD5 - LDAP di base con nome utente in chiaro e password con hash MD5 per una maggiore sicurezza. LDAPS - LDAP su SSL. Invia la password in chiaro all'interno di un tunnel crittografato tra l'ADC e il server LDAP. LDAPS-MD5 - LDAP su SSL. La password viene sottoposta a hash MD5 per una maggiore sicurezza all'interno di un tunnel crittografato tra l'ADC e il server LDAP.
Nome	Assegnate al vostro server un nome a scopo identificativo, che verrà utilizzato in tutte le regole.
Indirizzo del server	Aggiungere l'indirizzo IP o il nome host del server di autenticazione.
Porto	Per LDAP e LDAPS le porte sono impostate a 389 e 636 per impostazione predefinita. Per Radius la porta è generalmente la 1812. Per SAML, le porte sono impostate nell'ADC.
Dominio	Aggiungere il nome del dominio del server LDAP.
Formato di accesso	Utilizzare il formato di login necessario. Nome utente: scegliendo questo formato, è sufficiente inserire il nome utente. Tutte le informazioni sull'utente e sul dominio inserite dall'utente vengono eliminate e vengono utilizzate le informazioni sul dominio del server. Nome utente e dominio - L'utente deve inserire l'intero dominio e la sintassi del nome utente. Esempio: <i>mycompany\jdoe</i> OR <i>jdoe@mycompany</i> . Le informazioni sul dominio inserite a livello di server vengono ignorate. Vuoto - l'ADC accetta qualsiasi dato immesso dall'utente e lo invia al server di autenticazione. Questa opzione viene utilizzata quando si utilizza MD5.
Descrizione	Aggiungere una descrizione
Base di ricerca	Questo valore è il punto di partenza per la ricerca nel database LDAP. Esempio <i>dc=mycompany,dc=local</i>
Condizione di ricerca	Le condizioni di ricerca devono essere conformi a RFC 4515. Esempio: (MemberOf=CN=Phone-VPN,CN=Users,DC=mycompany,DC=local).
Ricerca utente	Eseguire la ricerca di un utente amministratore di dominio all'interno del server di directory.
Password	Password per l'utente amministratore del dominio.
Tempo morto	L'intervallo di tempo dopo il quale un server inattivo viene contrassegnato come nuovamente attivo.

Opzioni per l'autenticazione SAML

IMPORTANTE: quando si imposta l'autenticazione tramite SAML, è necessario creare un'applicazione Enterprise per Entra ID Authentication. Le istruzioni per farlo sono disponibili nel capitolo [Impostazione dell'applicazione di autenticazione Entra ID in Microsoft Entra](#)

▲ Authentication Servers

Method:

Name:

Description:

Identity Provider

IdP Certificate match:

Server Provider

SP Entity ID:

IdP Entity ID:

SP Signing Certificate:

IdP SSO URL:

SP Session Timeout:

IdP Logoff URL:

IdP Certificate:

Name	Description	Method	Domain	Server Address

Opzione	Descrizione
Metodo	Scegliere un metodo di autenticazione LDAP - LDAP di base con nomi utente e password inviati in chiaro al server LDAP. LDAP-MD5 - LDAP di base con nome utente in chiaro e password con hash MD5 per una maggiore sicurezza. LDAPS - LDAP su SSL. Invia la password in chiaro all'interno di un tunnel crittografato tra l'ADC e il server LDAP. LDAPS-MD5 - LDAP su SSL. La password viene sottoposta a hash MD5 per una maggiore sicurezza all'interno di un tunnel crittografato tra l'ADC e il server LDAP.
Nome	Assegnate al vostro server un nome a scopo identificativo, che verrà utilizzato in tutte le regole.
Fornitore di identità	
Corrispondenza del certificato IdP	Per IdP Certificate Match si intende il processo di verifica che il certificato digitale utilizzato da un Identity Provider (IdP) per firmare le asserzioni SAML corrisponda al certificato di cui si fida il Service Provider (SP). Questa convalida garantisce che l'IdP sia legittimo e che le asserzioni che invia siano autentiche e inalterate. L'SP solitamente memorizza il certificato dell'IdP nei suoi metadati e confronta il certificato incorporato nelle asserzioni SAML con quello memorizzato per determinare la corrispondenza.
ID dell'entità IdP	L'IdP Entity ID SAML è un identificativo univoco a livello globale che funge da indirizzo definitivo per un Identity Provider (IdP) all'interno dell'ecosistema Security Assertion Markup Language (SAML). Questo identificatore è tipicamente un URL o un URI che distingue in modo univoco l'IdP da altre entità coinvolte nei processi di autenticazione e autorizzazione basati su SAML. Svolge un ruolo cruciale nello stabilire la fiducia e nel facilitare la comunicazione sicura tra IdP, Service Provider (SP) e utenti.
URL IdP SSO	Un IdP SSO URL, abbreviazione di Single Sign-On URL, è uno specifico endpoint URL fornito da un identity provider (IdP) che funge da gateway di autenticazione per l'avvio di sessioni Single Sign-On (SSO). Quando un utente viene reindirizzato a questo URL, l'IdP gli chiede di autenticarsi utilizzando le proprie credenziali e, una volta avvenuta l'autenticazione, lo reindirizza al service provider (SP) con un'asserzione contenente le informazioni sulla sua identità. Questa asserzione viene poi convalidata dall'SP, consentendo all'utente di accedere alle risorse dell'SP senza dover effettuare una nuova autenticazione.
URL di disconnessione dell'IdP	L'URL di disconnessione dell'IdP SAML è un endpoint specifico dell'Identity Provider (IdP) che avvia e gestisce il processo di disconnessione per le sessioni Single Sign-On (SSO). Quando un utente fa clic sul pulsante di logout di un'applicazione, l'applicazione reindirizza l'utente all'URL di logout dell'IdP. L'IdP invalida quindi la sessione dell'utente su tutti i relying party associati all'autenticazione SSO e invia una risposta di logout all'applicazione, disconnettendo di fatto l'utente da tutte le applicazioni connesse.
Certificato IdP	Un certificato SAML IdP è un certificato digitale X.509 rilasciato da un'autorità fidata a un identity provider (IdP) che partecipa ai protocolli di autenticazione Security Assertion Markup Language (SAML). Questo certificato serve come mezzo sicuro per verificare l'identità dell'IdP e autenticare l'integrità e la riservatezza dei messaggi SAML scambiati tra l'IdP e i service provider (SP). È possibile selezionare il certificato IdP che verrà installato nell'ADC utilizzando il menu a discesa.
Descrizione	Una descrizione per la definizione.
Ricerca utente	Eseguire la ricerca di un utente amministratore del dominio.
Password	Per specificare la password dell'utente admin.
Fornitore di server	
ID entità SP	Un SP Entity ID è un identificatore univoco che funge da indirizzo globale per uno specifico Service Provider (SP) nel contesto del protocollo SAML. Si tratta di un modo standardizzato per identificare un SP ed è tipicamente un URL o un altro URI che individua i metadati SAML del SP, che contengono informazioni critiche come i certificati di crittografia e gli endpoint di autenticazione.

Certificato di firma SP	Un certificato di firma SP SAML è un certificato X.509 utilizzato da un Service Provider (SP) per firmare le risposte SAML, garantendo l'autenticità e l'integrità dei messaggi scambiati tra SP e Identity Provider (IdP) durante l'autenticazione Single Sign-On (SSO). L'SP firma la risposta utilizzando la propria chiave privata e l'IdP verifica la firma utilizzando la chiave pubblica associata al certificato, confermando l'identità del mittente e che il contenuto del messaggio non è stato manomesso.
SP Timeout della sessione	SP Session Timeout si riferisce alla durata massima per la quale la sessione di autenticazione di un utente è considerata valida dal lato del Service Provider (SP) dopo un Single Sign-On (SSO) riuscito attraverso un Identity Provider (IdP). Dopo questo periodo di tempo specificato, l'SP termina la sessione e richiede all'utente una nuova autenticazione per riottenere l'accesso alle risorse protette. Questo meccanismo aiuta a proteggere dagli accessi non autorizzati e garantisce che le sessioni degli utenti non rimangano inattive per lunghi periodi.

Regni KDC

I reami KDC si riferiscono a configurazioni del protocollo di autenticazione Kerberos, in cui ogni reame è essenzialmente un dominio o una rete che opera sotto un singolo Key Distribution Center (KDC). Questa configurazione delinea un gruppo di sistemi che sono gestiti dallo stesso KDC principale, facilitando l'autenticazione sicura e i meccanismi di distribuzione dei ticket in tutta la rete. I reami possono essere gerarchici o non gerarchici, con la possibilità di stabilire relazioni di fiducia tra di essi per un'autenticazione sicura tra i reami.

Status	Name	Description	KDC Server	Username	Password
	My K-Realm	Edgenexus KDC Realm	10.4.17.20	kadmin	*****

L'interfaccia utente fornita dall'ADC, come mostrato nell'immagine qui sopra, consente di definire i reami Kerberos. Queste informazioni possono essere utilizzate nelle regole di autenticazione.

Regole di autenticazione

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

Authentication Rules

Add Rule Remove Rule

Name:

Description:

Root Domain:

Authentication Server:

Client Authentication:

Server Authentication:

Form:

Message:

Timeout (s):

Update Cancel

Name	Description	Root Domain

Campo	Descrizione
Nome	Aggiungere un nome adatto alla regola di autenticazione.
Descrizione	Aggiungere una descrizione adeguata.

Dominio radice	Questo campo deve essere lasciato vuoto, a meno che non si abbia bisogno di un single-sign-on per i sottodomini.
Server di autenticazione	Si tratta di una casella a discesa contenente i server configurati.
Autenticazione del cliente:	Scegliete il valore più adatto alle vostre esigenze: Basic (401) - Questo metodo utilizza il metodo di autenticazione standard 401. Moduli: presenta all'utente il modulo predefinito di ADC. All'interno del modulo è possibile aggiungere un messaggio. È possibile selezionare un modulo caricato utilizzando la sezione sottostante.
Autenticazione del server	Scegliere il valore appropriato. Nessuno - se il server non dispone di alcuna autenticazione, selezionare questa impostazione. Questa impostazione consente di aggiungere capacità di autenticazione a un server che in precedenza non ne aveva. Base - se il server ha abilitato l'autenticazione di base (401), selezionare BASE. NTLM - se il server ha abilitato l'autenticazione NTLM, selezionare NTLM.
Forma	Scegliere il valore appropriato Default - Selezionando questa opzione, l'ADC utilizzerà il suo modulo incorporato. Personalizzato: è possibile aggiungere un modulo progettato da voi e selezionarlo qui.
Messaggio	Aggiungere un messaggio personale al modulo.
Timeout	Aggiungere un timeout alla regola, dopo il quale l'utente dovrà autenticarsi di nuovo. Si noti che l'impostazione Timeout è valida solo per l'autenticazione basata su Forms.

Se si desidera fornire un single sign-on agli utenti, completare il campo Dominio radice con il proprio dominio. In questo esempio, mycompany.com. Ora possiamo avere più servizi che utilizzeranno edgenexus.io come dominio principale e l'utente dovrà accedere una sola volta. Se consideriamo i seguenti servizi:

- [SharePoint.mycompany.com](#)
- [usercentral.mycompany.com](#)
- [App Store.mycompany.com](#)

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

Moduli

▲ Forms

Form Name:

Questa sezione consente di caricare un modulo personalizzato.

Come creare un modulo personalizzato

Sebbene il modulo di base fornito dall'ADC sia sufficiente per la maggior parte degli scopi, in alcuni casi le aziende desiderano presentare all'utente la propria identità. È possibile creare un modulo personalizzato che gli utenti dovranno compilare in questi casi. Questo modulo deve essere in formato HTM o HTML.

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

Esempio di codice html di un modulo molto semplice e basilare

```
<HTML>
<PAROLA>
<TITOLO>FORMULARIO DI AUTENTICAZIONE DI ESEMPIO</TITOLO>
</HEAD>
<BODY>
%JNMESSAGGIO%<br>
<form name="loginform" action="%JNURL%" method="post"> UTENTE: <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>
```

Aggiunta di un modulo personalizzato

Una volta creato un modulo personalizzato, è possibile aggiungerlo utilizzando la sezione Moduli.

1. Scegliere un nome per il modulo
2. Cercate il vostro modulo a livello locale
3. Fare clic su Carica

Anteprima del modulo personalizzato

Per visualizzare il modulo personalizzato appena caricato, occorre selezionarlo e fare clic su Anteprima. Questa sezione può essere utilizzata anche per eliminare i moduli non più necessari

Nota: quando si utilizzano prodotti per il filtraggio dei cookie, come AdGuard, è possibile che venga visualizzato un messaggio di errore 404. Per evitare che ciò accada, inserire nella whitelist l'indirizzo IP dell'ADC.

Cache

L'ADC è in grado di memorizzare i dati nella sua memoria interna e di migliorare l'erogazione dei servizi web. Le impostazioni che gestiscono questa funzionalità sono riportate in questa sezione.

▲ Global Cache Settings

Maximum Cache Size (MB):	<input type="text" value="50"/>	<input type="button" value="↑"/>	<input type="button" value="↓"/>	
Desired Cache Size (MB):	<input type="text" value="30"/>	<input type="button" value="↑"/>	<input type="button" value="↓"/>	
Default Caching Time (D/HH:MM):	<input type="text" value="1"/>	<input type="button" value="↑"/>	<input type="button" value="↓"/>	<input type="text" value="00:00"/>
Cachable HTTP Response Codes:	<input type="text" value="200 203 301 304 410"/>			
Cache Checking Timer (D/HH:MM):	<input type="text" value="0"/>	<input type="button" value="↑"/>	<input type="button" value="↓"/>	<input type="text" value="03:00"/>
Cache-Fill Count:	<input type="text" value="20"/>	<input type="button" value="↑"/>	<input type="button" value="↓"/>	

Check Cache

Force a check on the cache size

Clear Cache

Remove all items from the cache

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 memoria che viene anche scaricata periodicamente sul supporto di memorizzazione per mantenere la persistenza della cache dopo i riavvii e le operazioni di spegnimento. Questa funzionalità significa che la dimensione massima della cache deve rientrare nell'ingombro della memoria dell'appliance (piuttosto che nello spazio su disco) e non deve superare la metà della memoria disponibile.

Dimensione desiderata della cache (MB)

Questo valore indica la RAM ottimale a cui la Cache verrà 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 deve cercare di raggiungere ogni volta che viene effettuato un controllo automatico o manuale della dimensione della cache. L'intervallo tra la dimensione massima e quella desiderata della cache serve a gestire l'arrivo e la sovrapposizione di nuovi contenuti tra i controlli periodici della dimensione della cache per eliminare i contenuti scaduti. Ancora una volta, può essere più efficace accettare il valore predefinito (30 MB) e controllare periodicamente la dimensione della cache in "Monitor -> Statistiche" per un dimensionamento adeguato.

Tempo di caching predefinito (D/HH:MM)

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

L'immissione del campo assume la forma "D/HH:MM", quindi un'immissione di "1/01:01" (l'impostazione predefinita è 1/00:00) significa che l'ADC conserverà il contenuto per un giorno, "01:00" per un'ora e "00:01" per un minuto.

Codici di risposta HTTP memorizzabili nella cache

Uno dei set di dati memorizzati nella cache è costituito dalle risposte HTTP. I codici di risposta HTTP memorizzati nella cache sono:

- 200 - Risposta standard per le richieste HTTP andate a buon fine
- 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 è stato modificato dall'ultima richiesta e deve essere utilizzata la copia in 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 più comuni codici di risposta memorizzabili nella cache sono già elencati.

Timer controllo 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 viene rilevato un determinato numero di 304.

Applicare la regola della cache

Name	Caching Rulebase
jet.io	Images

Questa sezione consente di applicare una regola di cache a un dominio:

- Aggiungere il dominio manualmente con il pulsante Aggiungi record. È necessario utilizzare un nome di dominio completamente qualificato o un indirizzo IP in notazione dotted-decimale. Esempio `www.mycompany.com` o `192.168.3.1:80`
- Fare clic sulla freccia a discesa e scegliere il 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.
- Scegliere la regola di cache facendo doppio clic sulla colonna Caching Rulebase e selezionando dall'elenco

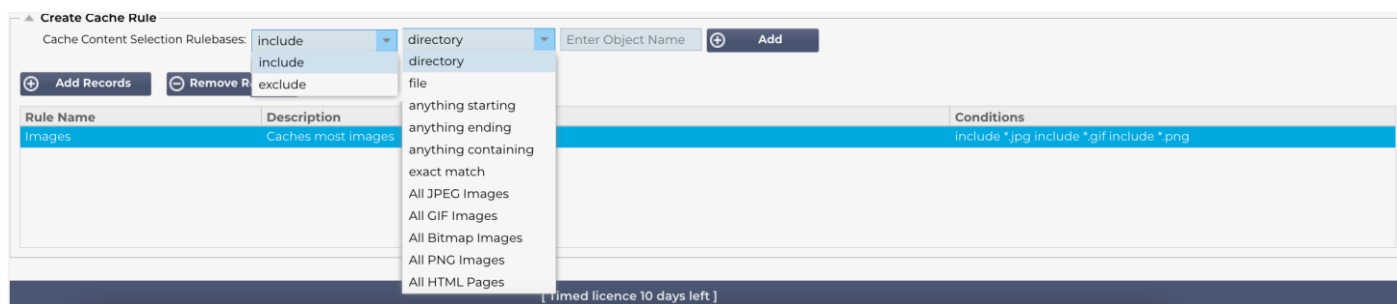
Creare una regola della cache

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

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

- Fare clic su Aggiungi record e assegnare alla regola un nome e una descrizione.
- È possibile digitare manualmente le condizioni o utilizzare il pulsante Aggiungi condizione.

Per aggiungere una condizione usando la base delle regole di selezione:



- Scegliere Includi o Escludi.
- Scegliere un criterio di selezione, ad esempio Tutte le immagini JPEG.
- Cliccare sul simbolo + Aggiungi.
- Si noterà che "include *.jpg" è stato aggiunto alle condizioni.
- È possibile aggiungere altre condizioni. Se si sceglie di farlo manualmente, è necessario aggiungere ogni condizione su una NUOVA riga. Le regole vengono visualizzate sulla stessa riga fino a quando non si fa clic sulla casella Condizioni, quindi vengono visualizzate su una riga separata.

voloPATH

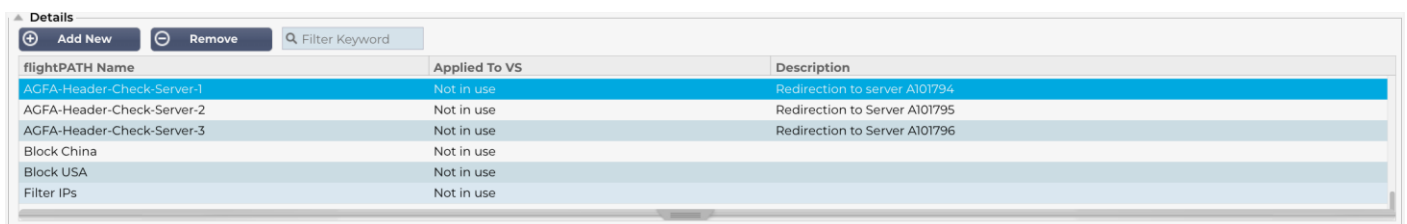
flightPATH è la tecnologia di gestione del traffico integrata nell'ADC e consente di ispezionare il traffico HTTP e HTTPS in tempo reale e di eseguire azioni in base alle condizioni.

Per utilizzare le regole flightPATH, è necessario applicarle a un Servizio virtuale utilizzando la scheda flightPATH nella sezione Server reali.

Una regola di rotta di volo è composta da quattro elementi:

1. Dettagli, dove si definiscono il nome di flightPATH e il servizio a cui è collegato.
2. Condizioni che possono essere definite per attivare la regola.
3. Valutazione che consente la definizione di variabili che possono essere utilizzate all'interno delle Azioni.
4. Azioni utilizzate per gestire ciò che deve accadere quando le condizioni sono soddisfatte.

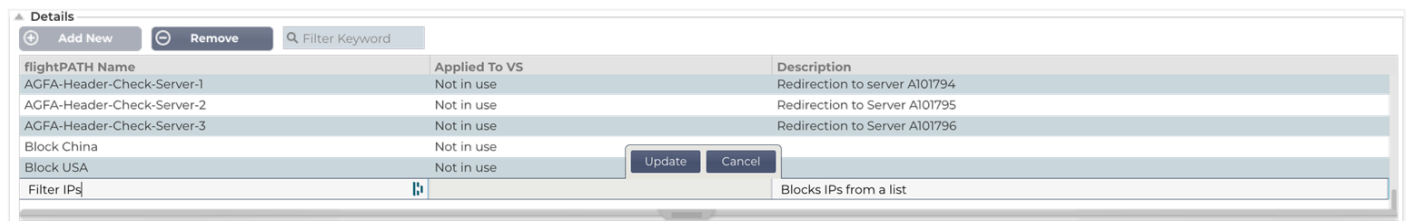
Dettagli



flightPATH Name	Applied To VS	Description
AGFA-Header-Check-Server-1	Not in use	Redirection to server A101794
AGFA-Header-Check-Server-2	Not in use	Redirection to Server A101795
AGFA-Header-Check-Server-3	Not in use	Redirection to Server A101796
Block China	Not in use	
Block USA	Not in use	
Filter IPs	Not in use	

La sezione dei dettagli mostra le regole flightPATH disponibili. In questa sezione è possibile aggiungere nuove regole flightPATH e rimuovere quelle definite.

Aggiunta di una nuova regola flightPATH



flightPATH Name	Applied To VS	Description
AGFA-Header-Check-Server-1	Not in use	Redirection to server A101794
AGFA-Header-Check-Server-2	Not in use	Redirection to Server A101795
AGFA-Header-Check-Server-3	Not in use	Redirection to Server A101796
Block China	Not in use	
Block USA	Not in use	
Filter IPs		Blocks IPs from a list

Campo	Descrizione
Nome FlightPATH	Questo campo contiene il nome della regola flightPATH. Il nome fornito in questo campo viene visualizzato e referenziato in altre parti dell'ADC.
Applicato a VS	Questa colonna è di sola lettura e mostra il VIP a cui è applicata la regola flightPATH.
Descrizione	Valore che rappresenta una descrizione fornita a fini di leggibilità.

Passaggi per aggiungere una regola flightPATH

1. Per prima cosa, fare clic sul pulsante Aggiungi nuovo situato nella sezione Dettagli.
2. Inserire un nome per la regola. Esempio Auth2
3. Inserire una descrizione della regola
4. Una volta che la regola è stata applicata a un servizio, si vedrà la colonna Applicato a popolarsi automaticamente con un indirizzo IP e un valore di porta.
5. Non dimenticate di premere il pulsante Aggiorna per salvare le modifiche o, in caso di errore, di premere Annulla per tornare allo stato precedente.

Condizione

Una regola flightPATH può avere un numero qualsiasi di condizioni. Le condizioni funzionano su base **AND** e consentono di impostare la condizione in base alla quale viene attivata l'azione. Se si desidera utilizzare una condizione **OR**, creare ulteriori regole flightPATH e applicarle al VIP nell'ordine corretto.

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

È anche possibile utilizzare RegEx selezionando Match RegEx nel campo Check e il valore RegEx nel campo Value. L'inclusione della valutazione RegEx estende enormemente le capacità di flightPATH.

Creare una nuova condizione flightPATH

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

Update Cancel

Per prima cosa è necessario selezionare un valore dalla colonna Condizione.

Forniamo diverse condizioni all'interno della tendina e copriamo tutti gli scenari previsti. Quando verranno aggiunte nuove condizioni, queste saranno disponibili tramite gli aggiornamenti di Jetpack.

Le scelte disponibili sono:

CONDIZIONE	DESCRIZIONE	ESEMPIO
<form>	I moduli HTML sono utilizzati per passare i dati al server.	Esempio "Il modulo non ha lunghezza 0".
Posizione GEO	Confronta l'indirizzo IP di origine con i codici paese ISO 3166.	La posizione GEO è uguale a GB, OPPURE la posizione GEO è uguale a Germania
Ospite	Host estratto dall'URL	www.mywebsite.com o 192.168.1.1
Lingua	Lingua estratta dall'intestazione HTTP della lingua	Questa condizione produrrà un menu a tendina con un elenco di Lingue
Metodo	Selezione di metodi HTTP	Un menu a tendina che include GET, POST, ecc.
Origine IP	Se il proxy upstream supporta X-Forwarded-for (XFF), utilizzerà l'indirizzo di origine reale.	IP del client. Può anche utilizzare più IP o sottoreti. 10\.\1\.\2\.* è la sottorete 10.1.2.0 /24 10\.\1\.\2\.[3 4] Utilizzare per più IP
Percorso	Percorso del sito web	/il mio sito/index.asp
POSTA	Metodo di richiesta POST	Controllare i dati caricati su un sito web
Interrogazione	Nome e valore di una query, che può accettare il nome della query o un valore.	"Best=jetNEXUS" Dove la corrispondenza è Best e il valore è edgeNEXUS
Stringa di query	L'intera stringa di query dopo il carattere ?	

Richiesta di cookie	Nome di un cookie richiesto da un client	MS-WSMAN=afYfn1CDqqCDqUD::
Intestazione della richiesta	Qualsiasi intestazione HTTP	Referrer, User-Agent, Da, Data
Versione richiesta	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 della risposta	200 OK, 304 Non modificato
Risposta Cookie	Il nome di un cookie inviato dal server	MS-WSMAN=afYfn1CDqqCDqUD::
Intestazione della risposta	Qualsiasi intestazione HTTP	Referrer, User-Agent, Da, Data
Versione di risposta	La versione HTTP inviata dal server	HTTP/1.0 O HTTP/1.1
Fonte IP	L'IP di origine, l'IP del server proxy o un altro indirizzo IP aggregato.	IP client, IP proxy, IP firewall. Può anche utilizzare più IP e sottoreti. È necessario sfuggire ai punti, poiché si tratta di RegEX. Esempio 10\1\2\3 è 10.1.2.3

Partita

Il campo Partita può essere un menu a tendina o un valore di testo ed è definibile in base al valore del campo Condizione. Ad esempio, se la Condizione è impostata su Host, il campo Partita non è disponibile. Se la Condizione è impostata su <form>, il campo Corrispondenza viene visualizzato come un campo di testo e se la Condizione è POST, il campo Corrispondenza viene presentato come un menu a tendina contenente i valori pertinenti.

Le scelte disponibili sono:

PARTITA	DESCRIZIONE	ESEMPIO
Accettare	Tipi di contenuto accettabili	Accetta: testo/plain
Accetta codifica	Codifiche accettabili	Accept-Encoding: <compress gzip deflate sdch identity>.
Lingua accettata	Lingue accettabili per la risposta	Lingua di accettazione: en-US
Campi di accettazione	Quali sono i tipi di intervallo di contenuto parziale supportati da questo server	Campi di accettazione: byte
Autorizzazione	Credenziali di autenticazione per l'autenticazione HTTP	Autorizzazione: Basic QWxhZGRpbjpvGVuIHNlc2FtZQ==
Addebito a	Contiene informazioni sui costi dell'applicazione del metodo richiesto.	
Codifica del contenuto	Il tipo di codifica utilizzato	Contenuto-Codifica: gzip
Lunghezza del contenuto	La lunghezza del corpo della risposta in ottetti (byte a 8 bit).	Lunghezza del contenuto: 348
Tipo di contenuto	Il tipo di mime del corpo della richiesta (usato con le richieste POST e PUT)	Tipo di contenuto: application/x-www-form-urlencoded

Biscotto	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-data
ETag	Un identificatore per una versione specifica di una risorsa, spesso un message digest.	ETag: "aed6bdb8e090cd1:0".
Da	L'indirizzo e-mail dell'utente che effettua la richiesta	Da: user@example.com
Se-Modificato-Da	Consente di restituire un 304 Not Modified se il contenuto è invariato.	Se-Modificato-Da: Sat, 29 Oct 1994 19:43:31 GMT
Ultima modifica	La data dell'ultima modifica dell'oggetto richiesto, nel formato RFC 2822.	Ultima modifica: 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
Referente	Indirizzo della pagina web precedente da cui è stato seguito un link alla pagina attualmente richiesta	Referente: HTTP://www.edgenexus.io
Server	Un nome per il server	Server: Apache/2.4.1 (Unix)
Imposta-conservazione	Un cookie HTTP	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
Agente utente	La stringa dell'agente utente dell'utente	User-Agent: Mozilla/5.0 (compatibile; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Variare	Indica ai proxy a valle come confrontare le intestazioni delle richieste future per decidere se la risposta nella cache può essere utilizzata piuttosto che richiederne una nuova dal server di 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 Senso è un campo booleano a discesa e contiene le opzioni Fa o Non.

Controllo

Il campo Controllo consente di impostare i valori di controllo rispetto alla Condizione.

Le scelte disponibili sono: Contiene, Fine, Uguale, Esiste, Ha Lunghezza, Corrisponde a RegEx, Corrisponde a Elenco, Inizia, Supera Lunghezza


CONTROLLO	DESCRIZIONE	ESEMPIO
Esistere	Non si preoccupa dei dettagli della condizione, ma solo del fatto che esiste/non esiste.	Host> Does> Exist
Inizio	La stringa inizia con il valore	Percorso> Fa> Inizia /sicuro>
Fine	La stringa termina con il valore	Percorso> Does> End - .jpg
Contenere	La stringa contiene il valore	Intestazione della richiesta> Accept> Does> Contain> image
Pari	La stringa equivale al valore	Host> Does> Equal> www.edgenexus.io

Avere lunghezza	La stringa ha una lunghezza pari al valore	Host> Does> Have Length> 16 www.edgenexus.io = VERO www.edgenexus.com = FALSO
Corrispondenza di RegEx	Consente di inserire un'espressione regolare completa compatibile con Perl.	L'IP di origine> corrisponde a> Regex
Elenco partite	Consente di confrontare il valore con un elenco di valori. Questo è utile quando ci sono, ad esempio, indirizzi IP specifici che devono essere confrontati. I valori sono separati da virgole (,) o da pip ().	IP di origine> Fa > Elenco partite > 10.10.10.1, 10.10.10.2, 10.10.10.3 ecc.
Superare la lunghezza	Consente di verificare se il valore supera la lunghezza specificata.	Percorso > Fa > Supera la lunghezza > 200

Passi per aggiungere una condizione

L'aggiunta di una nuova condizione flightPATH è molto semplice. Un esempio è mostrato qui sopra.

1. Fare clic sul pulsante Aggiungi nuovo nell'area delle condizioni.
2. Scegliere una condizione dalla casella a discesa. Prendiamo ad esempio Host. È possibile anche digitare nel campo e l'ADC mostrerà il valore in un menu a tendina.
3. Scegliere un senso. Ad esempio, Fa
4. Scegliere un controllo. Ad esempio, Contiene
5. Scegliere un valore. Ad esempio, mycompany.com



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

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

- Il primo è verificare che l'oggetto richiesto sia un'immagine
- La seconda verifica se l'host nell'URL è www.imagepool.com

Valutazione

La possibilità di aggiungere variabili definibili è una funzionalità interessante. Altri ADC offrono questa funzionalità utilizzando opzioni di scripting o della riga di comando che non sono ideali per chiunque. L'EdgeADC consente di definire un numero qualsiasi di variabili mediante un'interfaccia grafica di facile utilizzo, come illustrato e descritto di seguito.

La definizione della variabile flightPATH comprende quattro voci da inserire.

- Variabile - è il nome della variabile
- Sorgente: un elenco a discesa di possibili punti di origine.
- Dettaglio: selezionare i valori da un menu a tendina o digitarli manualmente.
- Valore - il valore che la variabile contiene e che può essere un valore alfanumerico o una RegEx per la messa a punto.

Variabili incorporate:

Le variabili incorporate sono già state codificate, quindi non è necessario creare una voce di valutazione per queste.

È possibile utilizzare una qualsiasi delle variabili elencate di seguito nella sezione Azione.

- \$sourceip\$ - L'indirizzo IP di origine della richiesta.
- \$sourceport\$ - La porta sorgente che è stata utilizzata
- \$clientip\$ - L'indirizzo IP del client
- \$clientport\$ - La porta utilizzata dal client
- \$host\$ - L'host indicato nella richiesta
- \$metodo\$ - Il metodo utilizzato: GET, POST ecc.
- \$path\$ - Il percorso specificato nella richiesta
- \$querystring\$ - La querystring utilizzata nella richiesta
- \$version\$ - La versione della richiesta HTTP nel REQUEST (al momento sono ammesse solo 1 e 1.1).
- \$resp\$ - La risposta del server, ad esempio 200OK, 404 ecc.
- \$geolocation\$ - La posizione GEO da cui proviene la richiesta.

AZIONE	OBIETTIVO
Azione = Reindirizzamento 302	Destinazione = HTTPs://\$host\$/404.html
Azione = Registro	Target = Un client da \$sourceip\$: \$sourceport\$ ha appena effettuato una richiesta \$path\$ page

Spiegazione:

- Un cliente che accede a una pagina inesistente verrebbe normalmente presentato con la pagina di errore 404 del browser.
- L'utente viene invece reindirizzato all'hostname originale utilizzato, ma il percorso errato viene sostituito con 404.html.
- Al Syslog viene aggiunta una voce che dice: "Un client 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.

▲ Action

+ Add New
 - Remove

Action	Target	Data
Rewrite Path	\$path\$!	

In questo esempio, si vuole riscrivere la parte di percorso dell'URL per riflettere l'URL digitato dall'utente.

- Fare clic su Aggiungi nuovo
- Scegliere Riscrittura del percorso dal menu a discesa Azione.
- Nel campo Target, digitate \$path\$/myimages
- Fare clic su Aggiorna

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

Azione	Descrizione	Esempio
--------	-------------	---------

Aggiungi cookie di richiesta	Aggiungere il cookie di richiesta dettagliato nella sezione Target con il valore nella sezione Dati	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Aggiungere l'intestazione della richiesta	Aggiungere un'intestazione di richiesta di tipo Target con valore nella sezione Data	Obiettivo= Accetta Dati= image/png
Aggiungi cookie di risposta	Aggiungere il cookie di risposta dettagliato nella sezione Target con il valore nella sezione Data.	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Aggiungere l'intestazione della risposta	Aggiungere l'intestazione della richiesta dettagliata nella sezione Target con il valore nella sezione Data.	Obiettivo= Cache-Control Data= max-age=8888888
Corpo Sostituire tutto	Cercare nel corpo della risposta e sostituire tutte le istanze	Target= http:// (stringa di ricerca) Data= https:// (stringa di sostituzione)
Corpo Sostituire prima	Cercare nel corpo della risposta e sostituire solo la prima istanza	Target= http:// (stringa di ricerca) Data= https:// (stringa di sostituzione)
Corpo Sostituire per ultimo	Cerca nel corpo della risposta e sostituisce solo l'ultima istanza	Target= http:// (stringa di ricerca) Data= https:// (stringa di sostituzione)
Goccia	In questo modo si interrompe la connessione	Obiettivo= N/A Dati= N/A
e-mail	Invia un'e-mail all'indirizzo configurato in Eventi e-mail. È possibile utilizzare una variabile come indirizzo o come messaggio.	Target= "flightPATH ha inviato un'email a questo evento" Data= N/A
Evento di registro	In questo modo viene registrato un evento nel registro di sistema	Target= "flightPATH ha registrato questo dato nel syslog" Data= N/A
Reindirizzamento 301	In questo modo si otterrà un reindirizzamento permanente	Obiettivo= http://www.edgenexus.io Dati= N/A
Reindirizzamento 302	In questo modo si otterrà un reindirizzamento temporaneo	Obiettivo= http://www.edgenexus.io Dati= N/A
Rimuovere il cookie di richiesta	Rimuovere il cookie di richiesta dettagliato nella sezione Target	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii

Rimuovere l'intestazione della richiesta	Rimuovere l'intestazione della richiesta dettagliata nella sezione Target	Destinazione=Server Dati=N/A
Rimuovere la risposta	Rimuovere il cookie di risposta descritto nella sezione Target Cookie	Obiettivo=jnAccel
Rimuovere la risposta	Rimuovere l'intestazione della risposta descritta nella sezione Intestazione del target	Obiettivo= Etag Dati= N/A
Sostituire il cookie di richiesta	Sostituire il cookie di richiesta dettagliato nella sezione Target con il valore della sezione Data.	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Sostituire l'intestazione della richiesta	Sostituire l'intestazione della richiesta nella destinazione con il valore dei dati.	Obiettivo= Connessione Dati= keep-alive
Sostituire la	Sostituire il cookie di risposta dettagliato nella sezione Target con il valore della sezione Dati Cookie	Target=jnAccel=afYfn1CDqqCDqCVii Date=MSWSMAN=afYfn1CDqCDqCVii
Sostituire la risposta	Sostituire l'intestazione della risposta dettagliata nella sezione Target con il valore della sezione Dati Intestazione	Destinatario= Dati del server= Non sono disponibili per motivi di sicurezza
Riscrivere il percorso	Ciò consente di reindirizzare la richiesta a un nuovo URL in base alla condizione	Target= /test/path/index.html\$querystring\$ Data= N/A
Utilizzare un server sicuro	Selezionare il server sicuro o il servizio virtuale da utilizzare	Target=192.168.101:443 Data=N/A
Utilizzare il	Selezionare il server o il servizio virtuale da utilizzare	Obiettivo= 192.168.101:80 Dati= N/A
Crittografia del cookie	In questo modo i cookie vengono crittografati in 3DES e poi codificati in base64.	Target= Inserire il nome del cookie da crittografare, si può usare * come jolly alla fine Data= Inserire una frase di accesso per la crittografia

Uno scenario di regole flightPATH

Un cliente ha un sito di e-commerce e ha problemi con i cookie bloccati dalle ultime versioni di un browser.

Il cliente rintraccia i problemi e scopre che la causa principale è la mancanza di un'etichettatura "sicura" e "same-site" per i cookie in questione.

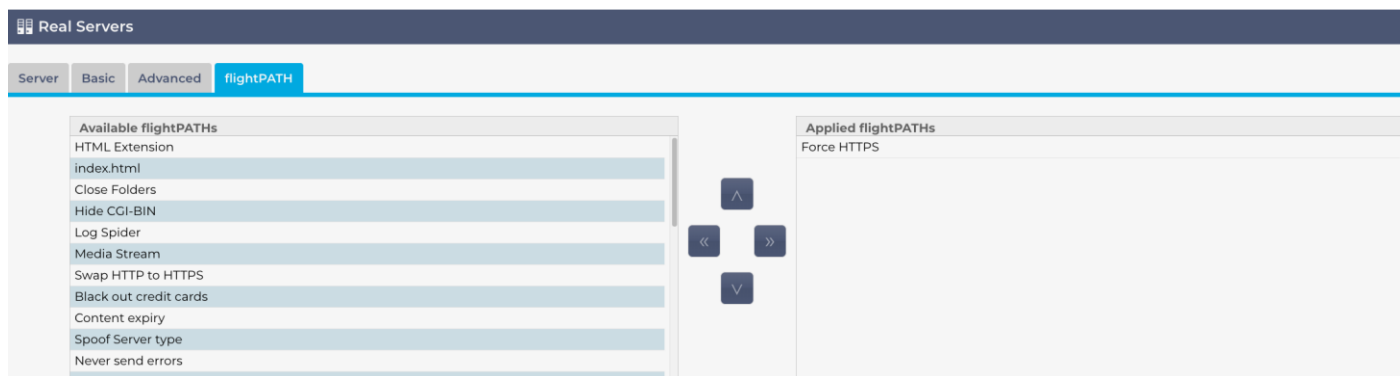
Vediamo come flightPATH può aiutare.

- Abbiamo un cookie di nome 'wp_woocommerce_session_97929973749972642'.
- Il nome del cookie è "wp_woocommerce_session_" con un valore ID univoco casuale di "97929973749972642" generato dal sistema di e-commerce.
- I tag "same-site" e "secure" sembrano essere vuoti, quindi il cookie è bloccato dalle nuove restrizioni di sicurezza del browser.
- Per evitare che ciò accada, si possono creare le seguenti regole flightPATH.
- **flightPATH Regola per l'ID di sessione**
 - **Condizione:**
Lasciare in bianco
 - **Valutazione:**
Variabile = \$variabile_1\$
Fonte = Cookie di risposta
Dettaglio = wp_woocommerce_session_*
 - Azione
Azione = Sostituire il cookie di risposta
Target = wp_woocommerce_session_*
Dati = \$variabile_1\$
- **regola flightPATH per i tag**
 - **Condizione:**
Condizione = Cookie di risposta
Partita = woocommerce_cart_hash
Senso = Esiste
Controllo = Esiste
Valore = Lasciare vuoto
 - **Valutazione:**
Variabile = \$variabile_2\$
Fonte = Cookie di risposta
Dettaglio = woocommerce_cart_hash
Valore = Lasciare vuoto
 - **Azione:**
Azione = Sostituire il cookie di risposta
Destinazione = woocommerce_cart_hash
Dati = \$variabile_2\$,StessoSito=Nessuno,Sicuro

Ora si applicano le regole ai servizi virtuali che le richiedono.

Applicazione della regola flightPATH

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



- Passare a Servizi > Servizi IP e scegliere il VIP a cui assegnare la regola flightPATH.
- Verrà visualizzato l'elenco dei Real Server mostrato di seguito
- Fare clic sulla scheda flightPATH
- Selezionare la regola flightPATH configurata o una di quelle precostituite supportate. Se necessario, è possibile selezionare più regole flightPATH.
- Trascinare e rilasciare il set selezionato nella sezione Applied flightPATHs o fare clic sul pulsante freccia >>.
- La regola verrà spostata sul lato destro e applicata automaticamente.

Monitor di server reali

Monitoring

▲ Details

⊕ Add Monitor ⊖ Remove

Name	Description	Monitoring Method	Applied To VS
200OK	Check home page for 200 OK	HTTP 200 OK	Not in use
DICOM	Monitor DICOM server	DICOM	Not in use
Check Page Returns	Check a page returns Success	HTTP Response	Not in use

Name: User Name:

Description: Password:

Monitoring Method: Threshold:

Page Location: SSL/TLS:

Required Content:

⊕ Update ⊖ Cancel

Il monitoraggio dei server reali è importante in uno scenario di bilanciamento del carico per rilevare e rispondere ai problemi dei server, garantire una distribuzione equilibrata del carico, ottimizzare l'utilizzo delle risorse, dare priorità ai servizi critici e identificare e risolvere le vulnerabilità del software.

La pagina Library> Real Server Monitors consente di aggiungere, visualizzare e modificare il monitoraggio personalizzato. Si tratta di "Controlli di salute" del server Layer 7 e si selezionano dal campo Monitoraggio del server nella scheda Base del servizio virtuale definito.

Tipi di monitor per server reali

Sono disponibili diversi monitor di Real Server, illustrati nella tabella seguente. Naturalmente, è possibile scrivere altri monitor utilizzando PERL.

Metodo di monitoraggio	Descrizione	Esempio
HTTP 200 OK	<p>Viene stabilita una connessione TCP al Real Server. Dopo la connessione, viene inviata una breve richiesta HTTP al Real Server. Quando viene ricevuta la risposta, viene controllata la presenza della stringa "200 OK". Se è presente, il server è considerato operativo.</p> <p>Si noti che utilizzando questo monitor viene recuperata l'intera pagina con i contenuti. Questo metodo di monitoraggio può essere utilizzato solo con i tipi di servizio HTTP e HTTP accelerato. Tuttavia, se un tipo di servizio Layer 4 è in uso per un server HTTP, può essere utilizzato se SSL non è in uso sul Real Server o è gestito in modo appropriato dalla funzione "Content SSL".</p>	<p>Richiesta GET / HTTP/1.1 Host: 192.168.159.200 Accettare: */* Lingua di accettazione: en-gb User-Agent: Edgenexus-ADC/4.0 Connessione: Keep-Alive Cache-Control: no-cache</p> <p>Risposta HTTP/1.1 200 OK Tipo di contenuto: text/html Ultima modifica: Wed, 31 Jan 2018 15:08:18 GMT Campi di accettazione: byte ETag: "Odd3253a59ad31:0" Server: Microsoft-IIS/10.0 Data: Tue, 13 Jul 2021 15:55:47 GMT Lunghezza del contenuto: 1364</p> <pre><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head></pre>

		<pre><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /> <titolo>jetNEXUS</titolo> <style type="text/css"> <!-- corpo { colore:#FFFFFF; ... }> </body> </html>.</pre>
HTTP 200 Testa	<p>Viene stabilita una connessione TCP al Real Server con il campo PATH che specifica la posizione da controllare.</p> <p>La parte di testa della risposta viene recuperata dal server, mentre il contenuto viene scartato. La risposta viene controllata per verificare la presenza di 200 OK. Se è presente, il server è considerato operativo.</p> <p>Si noti che utilizzando questo monitor viene recuperata solo la parte della testa.</p> <p>Questo metodo di monitoraggio può essere utilizzato solo con i tipi di servizio HTTP e HTTP accelerato. Tuttavia, se un tipo di servizio Layer 4 è in uso per un server HTTP, può essere utilizzato se SSL non è in uso sul Real Server o è gestito in modo appropriato dalla funzione "Content SSL".</p>	<p>Richiesta TESTA / HTTP/1.1 Host: 192.168.159.200 Accettare: /* Lingua di accettazione: en-gb User-Agent: Edgenexus-ADC/4.0 Connessione: Keep-Alive Cache-Control: no-cache</p> <p>Risposta HTTP/1.1 200 OK Lunghezza del contenuto: 1364 Tipo di contenuto: text/html Ultima modifica: Wed, 31 Jan 2018 15:08:18 GMT Campi di accettazione: byte ETag: "0dd3253a59ad31:0" Server: Microsoft-IIS/10.0 Data: Tue, 13 Jul 2021 15:49:19 GMT</p>
Opzioni HTTP 200	<p>Viene stabilita una connessione TCP al Real Server e viene effettuata una richiesta di opzioni.</p> <p>Le opzioni vengono restituite e controllate per verificare la presenza di contenuti 200 OK.</p> <p>Se viene trovato il contenuto 200 OK, il server è considerato disponibile.</p>	<p>Richiesta OPZIONI / HTTP/1.1 Host: 192.168.159.200 Accettare: /* Lingua di accettazione: en-gb User-Agent: Edgenexus-ADC/4.0 Connessione: Keep-Alive Cache-Control: no-cache</p> <p>Risposta HTTP/1.1 200 OK Consenti: OPZIONI, TRACE, GET, HEAD, POST Server: Microsoft-IIS/10.0 Pubblico: OPZIONI, TRACE, GET, HEAD, POST Data: Tue, 13 Jul 2021 16:23:39 GMT Lunghezza del contenuto: 0</p>
Testa HTTP	<p>Il monitor HTTP Head consente di verificare la presenza di un valore specifico nella parte Head del flusso HTTP. È possibile inserire un percorso e una risposta richiesta nei campi appropriati e quindi verificare la presenza di tale valore nella risposta.</p> <p>Se il valore Required Response viene trovato nell'Head, il server è considerato attivo e disponibile.</p> <p>Possiamo utilizzarlo anche su pagine appositamente protette che richiedono un nome utente e una password. In questo modo, il risultato del monitor può essere considerato accurato.</p> <p>Ad esempio, fornendo /ispagethere.html e i valori 200 OK nei campi Percorso e Risposta richiesta, si otterrà un risultato positivo se il</p>	<p>Richiesta TESTA /ispagethere.htm HTTP/1.1 Host: 192.168.159.200 Accettare: /* Lingua di accettazione: en-gb User-Agent: Edgenexus-ADC/4.0 Connessione: Keep-Alive Cache-Control: no-cache</p> <p>Risposta HTTP/1.1 200 OK Lunghezza del contenuto: 1364 Tipo di contenuto: text/html Ultima modifica: Wed, 31 Jan 2018 15:08:18 GMT Campi di accettazione: byte ETag: "0dd3253a59ad31:0" Server: Microsoft-IIS/10.0</p>

	<p>server è attivo, la pagina è disponibile e risponde alla richiesta.</p> <p>Questo metodo di monitoraggio può essere utilizzato solo con i tipi di servizio HTTP e HTTP accelerato. Tuttavia, se un tipo di servizio Layer 4 è in uso per un server HTTP, può essere utilizzato se SSL non è in uso sul Real Server o è gestito in modo appropriato dalla funzione "Content SSL".</p>	Data: Wed, 14 Jul 2021 08:28:18 GMT
Opzioni HTTP	<p>Il monitor delle opzioni HTTP consente di verificare la presenza di un valore specifico nei dati delle opzioni restituiti.</p> <p>Si inserisce un Percorso e una Risposta richiesta nei campi appropriati e si controlla la risposta.</p> <p>Se la Risposta richiesta viene trovata nei dati delle Opzioni, il server è disponibile e funzionante.</p> <p>I valori della risposta richiesta possono essere i seguenti: OPTIONS, TRACE, GET, HEAD e POST.</p> <p>Ad esempio, fornendo i valori /ispagethere.html e GET nei campi Percorso e Risposta richiesta, si otterrà un risultato positivo se il server è attivo, la pagina è disponibile e risponde alla richiesta.</p> <p>Questo metodo di monitoraggio può essere utilizzato solo con i tipi di servizio HTTP e HTTP accelerato. Tuttavia, se un tipo di servizio Layer 4 è in uso per un server HTTP, può essere utilizzato se SSL non è in uso sul Real Server o è gestito in modo appropriato dalla funzione "Content SSL".</p>	<p>Richiesta OPZIONI /ispagethere.htm HTTP/1.1 Host: 192.168.159.200 Accettare: /* Lingua di accettazione: en-gb User-Agent: Edgenexus-ADC/4.0 Connessione: Keep-Alive Cache-Control: no-cache</p> <p>Risposta HTTP/1.1 200 OK Consenti: OPZIONI, TRACE, GET, HEAD, POST Server: Microsoft-IIS/10.0 Pubblico: OPZIONI, TRACE, GET, HEAD, POST Data: Wed, 14 Jul 2021 09:47:27 GMT Lunghezza del contenuto: 0</p>
Risposta HTTP	<p>Si effettua una connessione e una richiesta/risposta HTTP al Real Server e si controlla come spiegato negli esempi precedenti.</p> <p>Tuttavia, anziché verificare la presenza di un codice di risposta "200 OK", l'intestazione della risposta HTTP viene controllata per il contenuto di testo personalizzato. Il testo può essere un'intestazione completa, parte di un'intestazione, una riga di una parte della pagina o una sola parola.</p> <p>Ad esempio, nell'esempio mostrato a destra, abbiamo specificato /ispagethere.htm come percorso e Microsoft-IIS come risposta richiesta.</p> <p>Se il testo viene trovato, il Real Server è considerato funzionante.</p> <p>Questo metodo di monitoraggio può essere utilizzato solo con i tipi di servizio HTTP e HTTP accelerato.</p> <p>Tuttavia, se un tipo di servizio Layer 4 è in uso per un server HTTP, può essere ancora utilizzato se SSL non è in uso sul Real Server o se è gestito in modo appropriato dalla funzione "Content SSL".</p>	<p>Richiesta GET /ispagethere.htm HTTP/1.1 Host: 192.168.159.200 Accettare: /* Lingua di accettazione: en-gb User-Agent: Edgenexus-ADC/4.0 Connessione: Keep-Alive Cache-Control: no-cache</p> <p>Risposta HTTP/1.1 200 OK Tipo di contenuto: text/html Ultima modifica: Wed, 31 Jan 2018 15:08:18 GMT Campi di accettazione: byte ETag: "0dd3253a59ad31:0" Server: Microsoft-IIS/10.0 Data: Wed, 14 Jul 2021 10:07:13 GMT Lunghezza del contenuto: 1364</p> <pre><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /> <titolo>jetNEXUS</titolo> <style type="text/css"></pre>

		<!-- corpo { colore:#FFFFFF; ... }
Monitor TCP multi-porta	Questo metodo è simile a quello precedente, tranne per il fatto che si possono avere diverse porte. Il monitor è considerato riuscito solo se tutte le porte specificate nella sezione del contenuto richiesto rispondono correttamente.	Nome: Monitor multi-porta Descrizione: Monitoraggio di più porte per il successo Posizione della pagina: N/A Contenuto richiesto: 135,59534,59535
TCP Fuori banda	Il metodo TCP Out of Band è simile a TCP Connect, tranne per il fatto che si può specificare la porta che si desidera monitorare nella colonna Contenuto richiesto. Questa porta in genere non corrisponde alla porta del traffico e viene utilizzata quando si desidera collegare i servizi tra loro.	Nome: TCP Fuori Banda Descrizione: Monitoraggio della porta fuori banda/traffico Posizione della pagina: N/A Contenuto richiesto: 555
DICOM	Si invia un'eco DICOM utilizzando il valore "Source Calling" AE Title nella colonna del contenuto richiesto. È inoltre possibile impostare il valore del titolo AE "Destinazione chiamata" nella sezione Note di ciascun server. La colonna Note si trova all'interno del menu Servizi IP. -Pagina Servizi virtuali - Server.	Nome: DICOM Descrizione: Controllo dello stato di salute L7 per il servizio DICOM Metodo di monitoraggio: DICOM Posizione della pagina: N/A Contenuto richiesto: Valore AET
LDAPS	Questo nuovo controllo dello stato di salute viene utilizzato per verificare lo stato di salute e la risposta di un server LDAP/AD.	Nome: LDAPS Descrizione: Controllo dello stato di salute del server LDAP/AD I parametri di utilizzo sono i seguenti: Nome utente: cn=nome utente, cn=utenti, dc=nome del dominio, dc=locale Password: DomainUserPassword Contenuto: 200OK
SNMP v2	Questo metodo di monitoraggio consente di verificare lo stato di disponibilità di un server utilizzando la risposta MIB SNMP del server. Il valore Require Response deve contenere il nome della comunità.	
Controllo del server DNS	Durante il bilanciamento del carico dei server DNS, è utile verificare se il server risponde alle query DNS. Il monitor può essere utilizzato come segue: <ul style="list-style-type: none"> • Il campo Percorso è utilizzato per l'FQDN che si sta interrogando. Ad esempio, se si desidera interrogare www.edgenexus.io, inserire questo valore nel campo Percorso. • Se si lascia vuoto questo campo, il monitor utilizzerà la ricerca predefinita per effettuare la query. • Il campo Risposta richiesta può essere lasciato vuoto e il monitor considererà valida qualsiasi risposta. Altrimenti, è necessario inserire l'IP previsto nel campo Risposta richiesta. Ad esempio, può essere 101.10.10.100. Se la query restituisce questo valore, il monitor segnala un successo, altrimenti segnala un fallimento. Un risultato positivo indica che il server DNS che si sta bilanciando è operativo.	

La pagina Monitor del server reale è suddivisa in tre sezioni.

Dettagli

La sezione Dettagli consente di aggiungere nuovi monitor e di rimuovere quelli non necessari. È anche possibile modificare un monitor esistente facendo doppio clic su di esso.

Name	Description	Monitoring Method	Applied To VS
200OK	Check home page for 200 OK	HTTP 200 OK	Not in use
DICOM	Monitor DICOM server	DICOM	Not in use

Name: 200OK
 Description: Check home page for 200 OK
 Monitoring Method: HTTP 200 OK
 Page Location: /
 Required Content: What must be seen within the page
 User Name: User name if the page is a secured
 Password: Password if the page is a secured p
 Threshold: Passed to custom monitors where :
 Update Cancel

Nome

Nome a scelta per il monitor.

Descrizione

Descrizione testuale per questo Monitor; si consiglia di renderla il più descrittiva possibile.

Metodo di monitoraggio

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

- HTTP 200 OK
- HTTP 200 Testa
- Opzioni HTTP 200
- Testa HTTP
- Opzioni HTTP
- Risposta HTTP
- Monitoraggio TCP multi-porta
- TCP Fuori banda
- DICOM
- SNMP v2
- Controllo del server DNS
- LDAPS

Posizione della pagina

URL Posizione della pagina per un monitor HTTP. Questo valore può essere un link relativo, come /cartella1/cartella2/pagina1.html. È anche possibile utilizzare un collegamento assoluto in cui il sito web è legato al nome dell'host.

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 sarà possibile eliminare un monitor utilizzato con un servizio virtuale.

Utente

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

Password

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

Soglia

Il campo Soglia è un numero intero generale utilizzato nei monitor personalizzati in cui è richiesta una soglia come il livello della CPU.

NOTA: Assicurarsi che la risposta del server applicazioni non sia una risposta "Chunked".

SSL/TLS

Questo campo consente di forzare l'uso o meno di SSL. Le impostazioni sono le seguenti:

- On - Questo forzerà l'SSL
- Off - Disattiva l'SSL
- Auto - Lascia lo stato attuale

Esempi di Real Server Monitor

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

Monitoraggio del caricamento

In molte occasioni gli utenti desiderano creare i propri monitor personalizzati e questa sezione consente di caricarli sull'ADC.

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

Upload Monitor

Monitor Name:

- Assegnare un nome al monitor per poterlo identificare nell'elenco Metodo di monitoraggio.
- Cercare il file .pl
- Fare clic su Carica nuovo monitor
- Il file verrà caricato nella posizione corretta e sarà visibile come nuovo Metodo di monitoraggio.

Monitor personalizzati

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

The screenshot shows a web interface titled "Upload Monitor". It contains a form with the following elements:

- A label "Monitor Name:" followed by a text input field containing the text "Test".
- A file path input field containing "C:\fakepath\test.pl" and a "Browse" button to the right.
- A large "Upload New Monitor" button at the bottom, which includes a small icon of a document with an upward arrow.

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

Creazione di uno script Perl di monitoraggio personalizzato

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

Questa sezione mostra i comandi che si possono utilizzare all'interno di uno script Perl.

Il comando `#Nome-Monitor:` è il nome utilizzato per lo script Perl memorizzato nell'ADC. Se non si include questa riga, lo script non verrà trovato!

I seguenti sono obbligatori:

- `#Nome` del monitor
- utilizzare in modo rigoroso;
- avviso di utilizzo;

Gli script Perl vengono eseguiti in un ambiente CHROOTED. Spesso chiamano un'altra applicazione, come WGET o CURL. A volte queste applicazioni devono essere aggiornate per funzioni specifiche, come SNI.

Valori dinamici

- `my $host = $_[0]; ### IP o nome dell'host (proviene dai dettagli di RS o da OOB, se usato)`
- `my $port = $_[1]; ### Porta host (proviene dai dettagli di RS o OOB, se usato)`
- `my $content = $_[2]; ### Contenuto richiesto dalle impostazioni del monitor (ciò che deve essere visualizzato nella risposta)`
- `my $notes = $_[3]; ### note dai dettagli della RS nei servizi IP (da usare per personalizzare ogni monitor RS in modo univoco)`
- `my $page = $_[4]; ### posizione della pagina nelle impostazioni del monitor`
- `my $user = $_[5]; ### nome utente dalle impostazioni del monitor`
- `my $password = $_[6]; ### password dalle impostazioni del monitor`
- `my $threshold = $_[7]; ### parametro di soglia dalle impostazioni del monitor`
- `my $rsaddr = $_[8]; ### RS IP (diverso da _[0] se il monitoraggio è fuori banda)`
- `my $rsport = $_[9]; ### porta RS (diversa da _[1] se il monitoraggio è fuori banda)`
- `my $timeout = $_[10]; ### monitorare il timeout dei contatti in secondi da Servizi IP > Real Server > Avanzate > Monitoraggio timeout`

I controlli sanitari personalizzati hanno due esiti

- Successo
Valore di ritorno 1
Stampa un messaggio di successo su Syslog
Contrassegnare il server reale online (a condizione che IN COUNT corrisponda)
- Non riuscito
Valore di ritorno 2

Stampa un messaggio di insuccesso su Syslog

Contrassegnare il Real Server Offline (a condizione che il conteggio OUT corrisponda)

Esempio di monitor sanitario personalizzato

```
#Nome del monitor HTTPS_SNI
utilizzare in modo rigoroso:
avvertenze per l'uso;
# Il nome del monitor viene visualizzato nel menu a tendina dei controlli sanitari disponibili.
# Ci sono 6 valori passati a questo script (vedi sotto)
# Lo script restituirà i seguenti valori
# 1 se il test ha avuto successo
# 2 se il test non ha successo sub monitor
{
mio Shost      = $_[0]; ### IP o nome dell'host
my Sport      = $_[1]; ### Porta Host
mio Scontento = $_[2]; ### Contenuto da cercare (nella pagina web e nelle intestazioni HTTP)
il mio Snote   = $_[3]; ### Nome dell'host virtuale
mio Spage     = $_[4]; ### La parte dell'URL dopo l'indirizzo dell'host
mio Suser     = $_[5]; ### dominio/nome utente (opzionale)
la mia Spassword = $_[6]; ### password (opzionale)
my $resolve;
il mio $auth  =;
se ($porta)
{
    $resolve = "$note:$porta:$host";
}
else {
    $resolve = "$note:$host";
}
se ($user && $password) {
    $auth = "-u $user:$password :
}
my @lines = 'curl -s -i -retry 1 -max-time 1 -k -H "Host:$note --resolve $resolve $auth HTTPS://${note}${page} 2>&1';
if(join("@lines")!=$content)
{
    print "HTTPS://$note${page} in cerca di - $content - Controllo salute riuscito.\n";
    ritorno(1);
}
altro
{
    print "HTTPS://$note${page} in cerca di - $content - Controllo salute fallito.\n";
    ritorno(2)
}
}
```

monitor(@ARGV):

NOTA:

Monitoraggio personalizzato - L'uso di variabili globali non è possibile. Utilizzare solo variabili locali, ovvero variabili definite all'interno di funzioni.

Uso di RegEx - Tutte le espressioni regolari devono utilizzare una sintassi compatibile con Perl.

Certificati SSL

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

I certificati SSL possono spaziare dai certificati autofirmati che l'ADC può generare ai certificati tradizionali (con caratteri jolly inclusi) disponibili presso fornitori affidabili. È anche possibile utilizzare certificati firmati dal dominio, generati da Active Directory.

Cosa fa l'ADC con il certificato SSL?

L'ADC può eseguire regole di gestione del traffico (flightPATH) in base al contenuto dei dati. Questa gestione non può essere eseguita sui dati criptati SSL. Quando l'ADC deve ispezionare i dati, deve prima decifrarli e per questo deve disporre del certificato SSL utilizzato dal server. Una volta decifrati, l'ADC sarà in grado di esaminare ed eseguire le regole flightPATH. In seguito, i dati verranno nuovamente crittografati utilizzando il certificato SSL e inviati al Real Server finale.

Il gestore della configurazione SSL

A partire dalla versione 196X è disponibile un metodo nuovo e più semplice per configurare e gestire i certificati SSL e le richieste di certificati.

The screenshot displays the 'SSL Certificates' management interface. At the top, there is a header 'SSL Certificates' and a sub-header 'Current Certificates'. Below this is a table with the following columns: Certificate Name, Expiry Date, Expires In, and Status/Type. The table lists several certificates, including CRM-01, NewWeb-1, NewWeb-2, No SSL, OldWeb-1, OldWeb-2, OldWeb-3, and WebServer-CRM-1. Below the table, there are several action buttons: Overview, Create Request, Rename, Delete, Sign / Install, Renew, Validate, Intermediates, Reorder, and Import/Export. Below the buttons, there is a section titled 'SSL CERTIFICATES & CSR MANAGEMENT' with a brief description of the tool's functionality. At the bottom, there is a 'Current Certificate Status' table showing the count of certificates for each status: Imported (1), Pending-renewal (5), and SelfSigned (1).

Certificate Name	Expiry Date	Expires In	Status/Type
CRM-01	Jan 1, 2025	286	Imported
NewWeb-1	Nov 14, 2024	238	Imported
NewWeb-2	Nov 14, 2024	238	Imported
No SSL	Nov 14, 2024	238	
OldWeb-1	Feb 29, 2024	Expired	Imported
OldWeb-2	Feb 29, 2024	Expired	Pending-renewal
OldWeb-3	Feb 29, 2024	Expired	SelfSigned
WebServer-CRM-1	Mar 31, 2024	10	Imported

Status	Count
Imported	1
Pending-renewal	5
SelfSigned	1

SSL Configuration Manager è composto da tre sezioni principali.

L'area di elencazione dei certificati






This screenshot is identical to the one above, showing the 'Current Certificates' table and the 'Current Certificate Status' table.

La parte superiore del Manager mostra i certificati SSL disponibili per l'uso o in attesa di attivazione da parte di un'autorità affidabile.

I certificati vengono visualizzati in un display a quattro colonne, che mostra il nome del certificato, la data di scadenza, il termine di scadenza (numero di giorni alla scadenza) e lo stato/tipo del certificato.

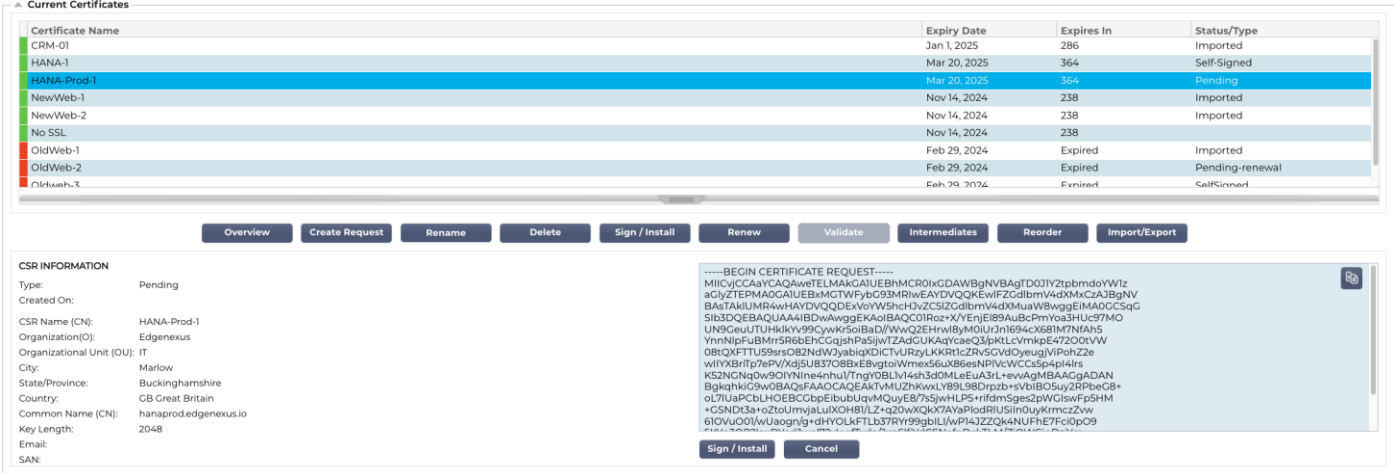
Codici colore

Come si può vedere, ogni riga mostra un certificato insieme a un blocco codificato a colori. Di seguito è riportata una tabella che mostra i diversi blocchi codificati a colori e il loro significato.

Codice colore	Significato
	Il certificato è in corso di validità e ha più di 60 giorni prima della scadenza.
	Il certificato scadrà tra meno di 30 giorni
	Il certificato ha una durata compresa tra 30 e 60 giorni
	Il certificato sta per scadere con <1 giorno rimanente
	Il certificato è scaduto

Display informativo del certificato/CSR

Facendo clic su un certificato o su una CSR, le informazioni relative vengono visualizzate nel pannello inferiore. Vedere l'immagine sottostante.



Current Certificates

Certificate Name	Expiry Date	Expires In	Status/Type
CRM-01	Jan 1, 2025	286	Imported
HANA-1	Mar 20, 2025	364	Self-Signed
HANA-Prod-1	Mar 20, 2025	364	Pending
NewWeb-1	Nov 14, 2024	238	Imported
NewWeb-2	Nov 14, 2024	238	Imported
No SSL	Nov 14, 2024	238	Imported
OldWeb-1	Feb 29, 2024	Expired	Imported
OldWeb-2	Feb 29, 2024	Expired	Pending-renewal
OldWeb-3	Feb 29, 2024	Expired	SelfSigned

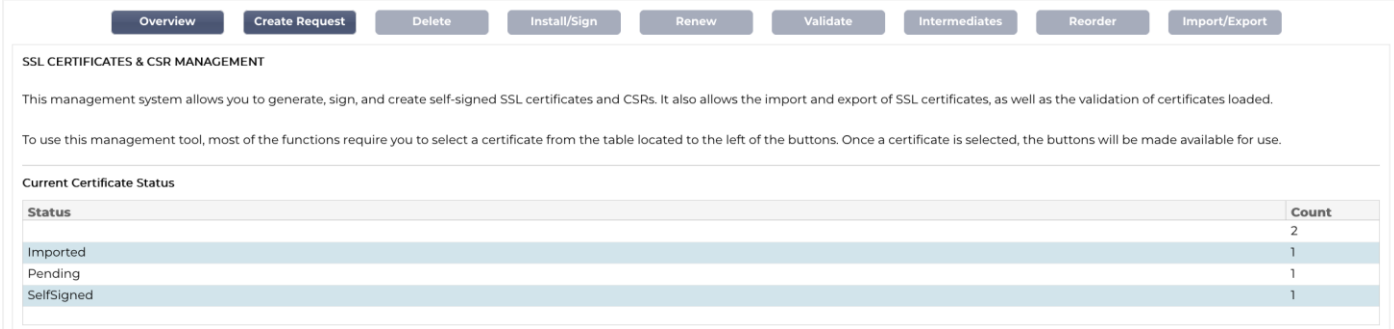
CSR INFORMATION

Type: Pending
 Created On:
 CSR Name (CN): HANA-Prod-1
 Organization(O): Edgenexus
 Organizational Unit (OU): IT
 City: Marlow
 State/Province: Buckinghamshire
 Country: GB Great Britain
 Common Name (CN): hanaprodedgenexusio
 Key Length: 2048
 Email:
 SAN:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICyCCAaYCAQAwETELMAkGAIUEBHMCR0iGDAWBgNVBAgTD0JlY2pmdoYW1z
aGlyZTEPMADGAIUEBxMGTWVjYjY3bG93MRwwEAYDQKwFZcdlBmV4dXNkMzA3BjNV
BAstAklMRwwHAYDQKwFZcdlBmV4dXNkMzA3BjNVBAstAklMRwwHAYDQKwFZcdlBmV4dXNkMzA3BjNV
Sib3DQEBAAUA4IBDwAwggEKAAoIBAQC01Roz+XVEnjEIB9AUBcPmYoa3HUC97MO
UN9GeuTUHkikV99CywK75oiBaDjWwQZEhrw8yM0UjJn1694cx681M7NfAH5
YmNlPpUBMfM5R6bEHCqjshPaSjwZAdGUkAqYcaE33jpkLEvMkpe4720DlVW
0BQKFTLUS9snc82NdWjyabiqDlCTVURzYkKrtlc2RSCVdQeyuGjVfahZze
wIYXBrItp7ePvXjd5U83708BxE8vgtolWmex56uX86esNPVWCcs5p4p14rs
K5ZNGnqDw90IYNne4nhUjTngY0BLV14sh3dOMLeEuA3rL+evAgMBAACgADAN
BqkqhkC9w08BAQ2FAAQCAQEAkVWU2hwxkLY8L58Dppb+VvIB05uZRPbeGB+
oL7UaPcblHOEBCCbpElubUqMQuyE8/75SjwHLPs+rfdmSges2pWGISwFp5HM
+GSNDI3a+oZtoUmyjaLulXOH8l/LZ+q20wXqK7AyaPlodRIUSin0uyKrmczZw
6lOVu00lWUaognlg+dhYOLkFTLb37Ry99gblLwPI4JZQk4NUFH7FolOp09
-----
```

Sign / Install Cancel

I pulsanti di azione e le aree di configurazione



SSL CERTIFICATES & CSR MANAGEMENT

This management system allows you to generate, sign, and create self-signed SSL certificates and CSRs. It also allows the import and export of SSL certificates, as well as the validation of certificates loaded.

To use this management tool, most of the functions require you to select a certificate from the table located to the left of the buttons. Once a certificate is selected, the buttons will be made available for use.

Current Certificate Status

Status	Count
Imported	2
Pending	1
SelfSigned	1

Sono disponibili diversi pulsanti di azione che entrano in gioco quando si seleziona un certificato nell'elenco.

Panoramica

Current Certificate Status	
Status	Count
Imported	5
Pending	1
Pending-renewal	1
Self-Signed	1
SelfSigned	1

Il pulsante Panoramica visualizza una situazione generale dei certificati nella sezione inferiore. A differenza di altre azioni, il pulsante Panoramica è indipendente e non richiede la selezione di un certificato.

Crea richiesta

Se si desidera creare un certificato autofirmato o un CSR, è necessario fare clic sul pulsante Crea richiesta. Si aprirà un pannello di inserimento comune che consente di fornire tutti i dettagli richiesti.

CREATE SELF-SIGNED CERTIFICATE / CSR

AD Certificate Name (CN): CRM-Server

Organization (O): Jumping Jack Flash Inc

Organizational Unit (OU): IT

City/Locality: New York

State/Province: New York

Country: US United States

Common Name (FQDN): crm.jjf.com

Key Length: 2048

Period (days): 360

Email: flash@jjf.com

Subject Alternative Names: Email www.mysite.com

DNS: www.crm.jjf.com x IP: 10.5.6.7 x Email: admin@jjf.com x

Nome del certificato AD (CN)

È un campo descrittivo utilizzato per visualizzare il nome del certificato nell'ADC. Il campo deve essere specificato come alfanumerico senza spazi.

Organizzazione (O)

Questo campo viene utilizzato per specificare il nome dell'organizzazione che utilizzerà il certificato.

Unità organizzativa (OU)

Normalmente utilizzato per specificare il reparto o l'unità organizzativa, questo campo è facoltativo.

Città/Località

Come suggerisce il nome, gli utenti tendono generalmente a specificare la sede dell'organizzazione.

Stato/Provincia

Specificare in questo campo lo stato, la contea o la provincia.

Paese

Questo campo è obbligatorio e deve essere completato selezionando il Paese in cui verrà utilizzato il certificato. Assicurarsi che le informazioni fornite siano corrette.

Nome comune (FQDN)

Si tratta di un campo critico, utilizzato per specificare il nome di dominio completamente qualificato (FQDN) dei server che devono essere protetti con il certificato. Potrebbe essere qualcosa come `www.edgenexus.io`, o **edgenexus.io**, o anche un carattere jolly ***.edgenexus.io**. È possibile utilizzare anche un indirizzo IP, se si desidera associare il certificato a tale indirizzo.

Lunghezza della chiave

Serve a specificare la lunghezza della chiave di crittografia per il certificato SSL.

Periodo (giorni)

Durata della validità del certificato in giorni. Una volta scaduto il periodo, il certificato diventerà non operativo.

Email

È l'ID e-mail amministrativo utilizzato per il certificato.

Nomi alternativi del soggetto (SAN)

Il Subject Alternative Name (SAN) è un'estensione dei certificati SSL che consente di proteggere più nomi di dominio con un unico certificato. Questa funzione è particolarmente utile per proteggere siti web con più sottodomini o nomi di dominio diversi, consentendo un approccio più snello ed economico alla gestione SSL. Includendo i SAN, un singolo certificato SSL può coprire una varietà di nomi di dominio e sottodomini, eliminando la necessità di certificati individuali per ogni indirizzo web, semplificando così il processo di protezione delle comunicazioni web e garantendo la crittografia dei dati tra domini diversi.

Questo campo è composto da due elementi, un menu a tendina che consente di selezionare il tipo di SAN e un campo di testo per specificare il valore.

L'EdgeADC dispone delle seguenti SAN: DNS, Indirizzo IP, Indirizzo e-mail e URI. È possibile selezionare e specificare più SAN per un certificato o una CSR.

Subject Alternative Names: Email www.mysite.com

DNS: www.crm.jjf.com x IP: 10.5.6.7 x Email: admin@jjf.com x

Le SAN che sono state specificate possono essere rimosse facendo clic sulla **x** rossa situata in ogni valore SAN.

- **DNS** - Il campo DNS Subject Alternate Name (SAN) consente di specificare altri nomi di dominio per i quali il certificato è valido. A differenza del campo Common Name (CN), che consente un solo dominio, il campo SAN può includere più nomi di dominio, offrendo flessibilità e scalabilità nella gestione dei certificati. Questo è particolarmente utile per le organizzazioni che ospitano più servizi su diversi domini e sottodomini, in quanto consente di proteggere le comunicazioni di tutte queste entità con un unico certificato SSL/TLS, semplificando l'amministrazione e migliorando la sicurezza.
- **Indirizzo IP** - Il nome alternativo del soggetto IP (SAN) consente di includere gli indirizzi IP accanto ai nomi di dominio come entità protette dal certificato. Questa funzione è fondamentale per proteggere l'accesso diretto ai servizi tramite gli indirizzi IP, garantendo la possibilità di stabilire connessioni crittografate anche quando si

accede a un server non tramite il suo nome di dominio, ma direttamente tramite il suo indirizzo IP.

Incorporando le SAN IP, le organizzazioni possono migliorare la sicurezza della rete abilitando la crittografia SSL/TLS sia per le comunicazioni basate su dominio che per quelle basate su IP, rendendola versatile per gli ambienti in cui i nomi di dominio potrebbero non essere utilizzati o preferiti per accedere a risorse interne o a servizi specifici.

- **Indirizzo e-mail** - Il Subject Alternative Name (SAN) dell'indirizzo e-mail consente di specificare altri indirizzi e-mail da associare al certificato, oltre al dominio o all'entità principale per cui è stato emesso. Ciò consente al certificato di convalidare l'identità dell'emittente per più indirizzi e-mail, non solo per un singolo dominio o nome comune (CN). È particolarmente utile negli scenari in cui è richiesta una comunicazione e-mail sicura per diversi indirizzi e-mail della stessa organizzazione o entità, garantendo che gli scambi di e-mail crittografate siano autenticati e collegati all'identità dell'emittente verificata dal certificato. Questo rende l'Email Address SAN una funzione chiave per migliorare la sicurezza e l'affidabilità delle comunicazioni e-mail in un contesto crittografato.
- **URI** - La SAN URI (Uniform Resource Identifier) è utilizzata per specificare identità aggiuntive rappresentate da URI per una singola entità garantita dal certificato. A differenza delle voci SAN tradizionali, che in genere includono nomi di dominio (nomi DNS) o indirizzi IP, una SAN URI consente al certificato di associare l'entità a URI specifici, come un URL a una risorsa specifica o un endpoint di servizio. Ciò consente un'identificazione più flessibile e precisa, permettendo di stabilire connessioni sicure con risorse o servizi specifici all'interno di un dominio, anziché limitarsi a proteggere il dominio stesso, migliorando così la granularità e la portata dei certificati SSL/TLS.

Una volta compilato correttamente, si può scegliere di creare una richiesta di firma del certificato (CSR) e inviarla per la firma da parte di un'autorità di certificazione o creare un certificato autofirmato da utilizzare immediatamente.

Il pulsante Annulla annulla l'intera richiesta, mentre il pulsante Ripristina azzera tutti i campi.

Rinominare

Il pulsante Rinomina consente di rinominare i certificati non in uso sui Servizi virtuali.

Per utilizzare questa funzione:

- Fare clic sul certificato che si desidera rinominare e cliccare sul pulsante Rinomina.
- La riga del certificato cambierà e sarà possibile modificarne il nome.

Certificate Name	Expiry Date	Expires In	Status/Type
HANA-1	Mar 20, 2025	364	Self-Signed
HANA-Prod-1	Mar 20, 2025	364	Pending
NewWeb-1	Nov 14, 2024	238	Imported
NewWeb-2	Nov 14, 2024	238	Imported
No SSL	Nov 14, 2024	238	Imported
OldWeb-1	Feb 29, 2024	Expired	Imported
OldWeb-2	Feb 29, 2024	Expired	Pending-renewal
Oldweb-3	Feb 29, 2024	Expired	SelfSigned
WebServer-CRM-1	Mar 31, 2024	9	Imported

Update Cancel

Overview Create Request Rename Delete Sign / Install Renew Validate Intermediates Reorder Import/Export

- Al termine, fare clic sul pulsante Aggiorna.
- È anche possibile fare doppio clic sul certificato per rinominarlo.

Cancellare

Il pulsante Elimina è disponibile solo quando è selezionato un certificato. Quando si fa clic su di esso, viene visualizzato il seguente contenuto

CERTIFICATE/CSR DELETION

You have elected to delete the following SSL certificate:

Certificate/CSR Name: **Web-Server-Certificate**

If you are sure you want to delete, click Delete or to prevent deletion, click Cancel.

Cancel Delete

Nel riquadro inferiore viene visualizzata la richiesta di cancellazione insieme al nome del certificato per il quale è stata richiesta la cancellazione.

Fare clic sul pulsante Elimina in basso a destra del riquadro per procedere all'eliminazione.

Installazione/Segnalazione

SIGN / INSTALL CERTIFICATE

Certificate Name: Web-Server-Certificate

To sign a certificate, please upload the ZIP file provided by your certification authority. This must be an Apache-compliant file.

Upload Certificate:

Alternatively, you can also copy and paste the certificate below. Please take care when doing this and do not miss out any information. Intermediates can also be added below the certificates, and terminated with Root CA.

Certificate Text:

Quando si crea una CSR e si desidera che la richiesta sia firmata da un'Autorità di certificazione (CA), si invia la CSR alla CA. In cambio, la CA invierà il certificato firmato insieme al file della chiave privata e a tutti gli intermediari necessari per il corretto funzionamento del certificato.

È possibile che vi inviino un file ZIP contenente tutti gli elementi richiesti, che può essere caricato utilizzando la parte superiore del pannello di destra.

In alternativa, è possibile costruire il set di certificati in un editor di testo e incollare il contenuto nel campo Testo del certificato nella sezione inferiore del riquadro.

Una volta utilizzato uno dei due metodi, fare clic sul pulsante Firma e poi sul pulsante Applica. Il certificato firmato sarà ora visualizzato nel riquadro di sinistra.

Rinnovare

RENEW CERTIFICATE

You have chosen to **renew** the certificate shown below.

If you'd like to revoke or cancel this request, please click the CSR on the left-side table and select Cancel CSR.

Certificate Name (CN): Web-Server-Certificate

Important
A new CSR has been created for signing, but the original SSL certificate for which renewal was requested is still active. Please ensure you allocate the newly signed certificate to the correct CSR when importing.

Quando un certificato scade oltre i termini di validità, il pulsante Rinnova consente di estendere e rinnovare il certificato. Esistono due tipi di rinnovo.

Certificati autofirmati

I certificati autofirmati, a differenza dei certificati affidabili, non possono essere rinnovati utilizzando un CSR. Il certificato autofirmato viene invece rinnovato presentando una nuova configurazione utilizzando i dati esistenti. L'utente può quindi specificare un nuovo nome per il certificato e un nuovo valore di scadenza per il certificato.

Una volta eseguita questa operazione, il nuovo certificato autofirmato verrà creato e salvato nell'archivio dei certificati. È quindi responsabilità dell'amministratore assicurarsi che i servizi virtuali che utilizzano il certificato siano riconfigurati in tempo.

Certificati firmati affidabili

Quando si tratta di certificati affidabili e firmati da un'autorità di certificazione, si adotta l'uso di CSR.

Quando si fa clic su un certificato in scadenza nel pannello superiore e si fa clic su Rinnova, verrà presentato un nuovo CSR utilizzando i dettagli del certificato corrente. Il CSR può essere scaricato e presentato all'autorità di certificazione per la firma, dopodiché il certificato firmato può essere installato.

Il certificato che era stato chiesto di rinnovare avrà un nuovo stato, Rinnovo. Una volta installato il certificato firmato, vi verrà chiesto di assegnare un nuovo nome al certificato. Questo verrà visualizzato come attendibile. Il certificato originale verrà conservato e tutti i servizi che lo utilizzano dovranno essere configurati per utilizzare il nuovo certificato il prima possibile.

Convalida del certificato

Le parti che compongono un certificato SSL sono numerose ed è essenziale che non solo siano presenti, ma che siano anche nell'ordine corretto. Di seguito sono elencati i motivi per convalidare i certificati SSL ottenuti da organizzazioni terze.

- **Autenticazione:** La convalida garantisce che il certificato provenga da un'autorità affidabile e verifica l'identità del sito web o del server. Questo aiuta a prevenire gli attacchi man-in-the-middle, in cui un aggressore potrebbe intercettare la comunicazione tra un client e un server.
- **Integrità:** Convalidando un certificato SSL, è possibile garantire che il certificato non sia stato manomesso o alterato. Questo è fondamentale per mantenere l'integrità della connessione sicura.
- **Verifica della catena di fiducia:** I certificati SSL sono emessi dalle Autorità di Certificazione (CA). La convalida di un certificato include la verifica che esso si ricolleggi a una CA radice affidabile. Questo processo garantisce che il certificato sia legittimo e affidabile.
- **Stato di revoca:** Durante la convalida, è importante verificare se il certificato SSL è stato revocato dalla CA emittente. Un certificato può essere revocato se è stato emesso per errore, se la chiave privata del sito web è stata compromessa o se il sito non ha più bisogno del certificato. L'importazione di un certificato revocato potrebbe portare a vulnerabilità di sicurezza.
- **Controllo della scadenza:** I certificati SSL sono validi per un periodo specifico. La convalida di un certificato all'importazione include il controllo della data di scadenza per assicurarsi che sia ancora valido. L'uso di un certificato scaduto potrebbe causare vulnerabilità e potrebbe indurre i browser o i client a rifiutare la connessione sicura.
- **Configurazione e compatibilità:** La convalida assicura che la configurazione del certificato sia compatibile con le politiche di sicurezza del client e con i requisiti tecnici del server o dell'applicazione. Ciò include la verifica degli algoritmi utilizzati, dello scopo del certificato e di altri dettagli tecnici.
- **Conformità:** In alcuni settori, le normative possono richiedere la convalida dei certificati SSL per garantire la gestione sicura delle informazioni sensibili. Ciò è particolarmente importante in settori come la finanza, la sanità e l'e-commerce.

Il sistema di gestione SSL dell'ADC consente di convalidare un certificato SSL importato.

- Selezionare un certificato SSL importato.
- Fare clic sul pulsante Convalida.
- I risultati sono visibili nel pannello inferiore, come rappresentato nell'immagine sottostante.

VALIDATE CERTIFICATE		
The validation results are shown below:		
Certificate Name:	EdgeWild	
Test Name	Test Result	Test Status
Certificate file	/jetnexus/etc/sslcert_EdgeWild.pem: CN = *.edgenexus.io error 20 at 0 depth lookup:unable to get local iss	✓
Certificate expires	Certificate expired 114 days ago	✗
Private key check	OK	✓
Public key check	OK	✓

Aggiunta di intermedi

Come già detto, i certificati SSL sono composti da diverse parti, una delle quali è costituita dai certificati intermedi che vanno a comporre la catena completa.

L'SSL Manager dell'ADC consente di aggiungere i certificati intermedi mancanti.

- Fate clic sull'SSL a cui desiderate aggiungere il certificato intermedio.
- Fare clic sul pulsante Intermedi.
- Viene visualizzato un pannello simile all'immagine seguente.

ADD INTERMEDIATES

Certificate selected: EdgeWild

Paste Certificate text here.

Cancel Apply

- Incollare il contenuto del certificato intermedio.
- Fare clic su Applica.

Potrebbe essere necessario modificare l'ordine dei certificati intermedi, in modo che il certificato SSL venga convalidato correttamente. Questo si può fare utilizzando il pulsante Riordina.

Riordino

Affinché un certificato SSL funzioni correttamente, deve essere inserito nell'ordine giusto.

La regola d'oro è che il certificato del mittente deve essere il primo e il certificato radice finale l'ultimo della catena. In genere, questo aspetto è simile alla rappresentazione seguente:

Emittente originale > Intermedio 1 > Radice finale.

La radice finale è un certificato di radice affidabile fornito da un'autorità di certificazione.

In alcuni casi, ci sono diversi certificati intermedi, e anche questi devono essere collocati nella posizione corretta. In sostanza, ogni certificato successivo deve certificare quello che lo precede. Quindi, il risultato potrebbe essere il seguente.

Emittente originale > Intermedio 1 > Radice finale

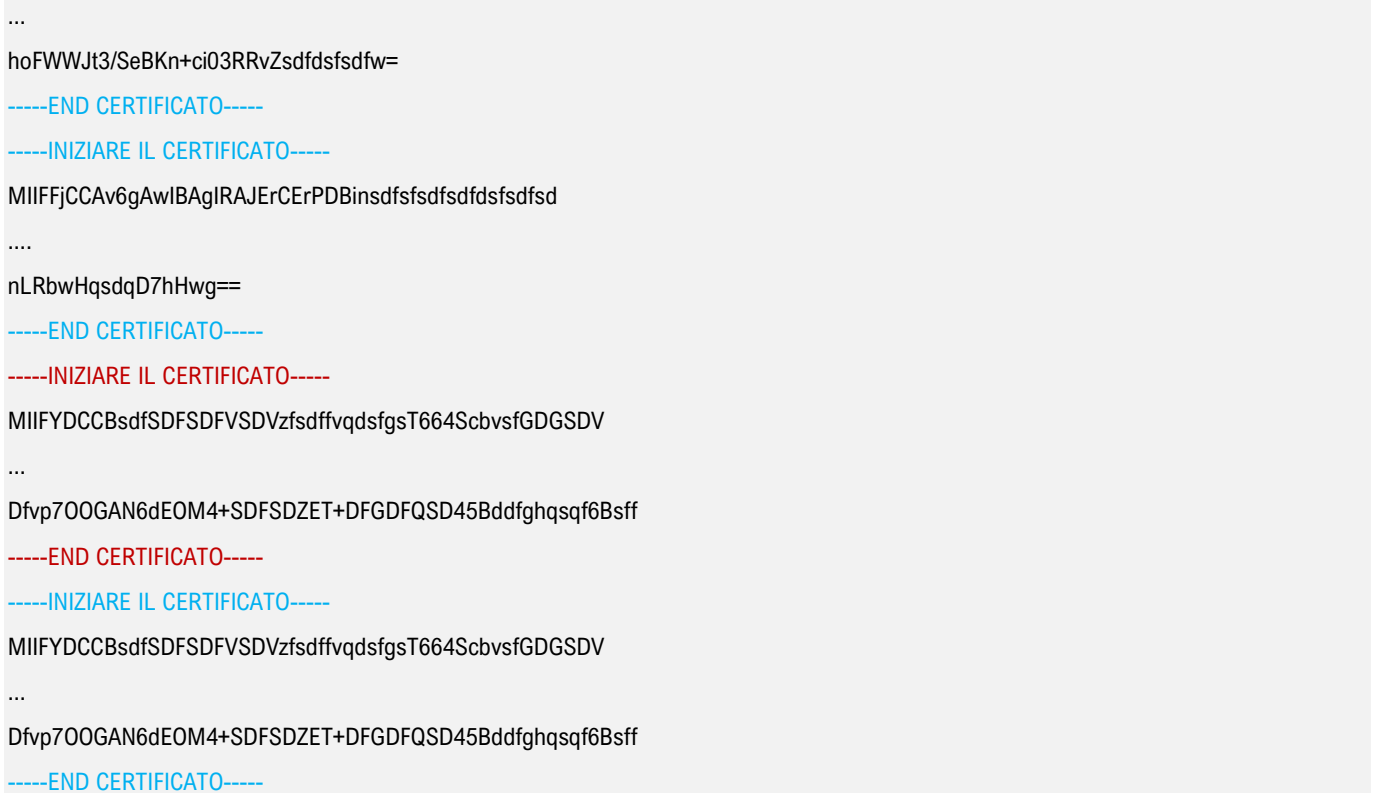
Quando si importa, ad esempio, l'Intermedio 2, questo potrebbe essere collocato alla fine della catena, il che significherebbe che la certificazione non è valida. Da qui la necessità di riordinarla e di collocare l'Intermedio 2 nella sua posizione corretta (in rosso).

Quindi, l'aspetto finale sarebbe il seguente:

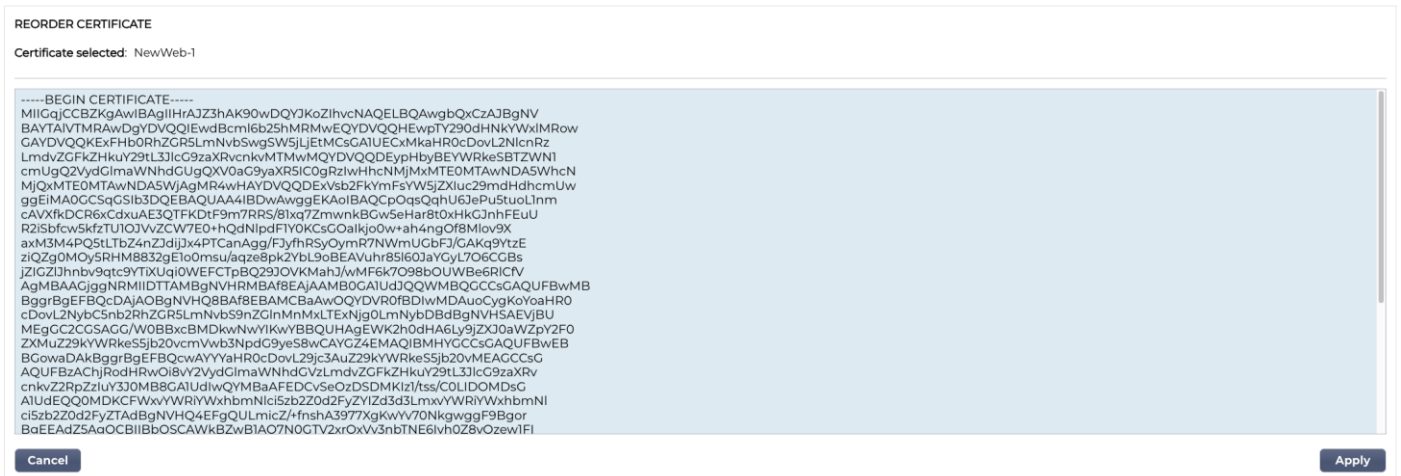
Emittente originale > Intermedio 1 > **Intermedio 2** > Radice finale

-----INIZIARE IL CERTIFICATO-----

MIIFKTCBBGgAwIBAgISA/UUyBj71fucZuvpiLsdfsdfsd



Una volta selezionato un certificato e premuto il pulsante Riordina, la sezione Riordina si presenta come nell'immagine seguente.



Per riordinare le sezioni del certificato, è possibile copiare il testo all'interno della casella, modificare e riordinare il contenuto in un editor di testo e quindi incollarlo nuovamente per sostituire il contenuto esistente. Una volta terminato, fare clic sul pulsante Applica.

Importazione/Esportazione

IMPORT CERTIFICATE

Certificate Name:

Upload Certificate: pfx, .cer, .pem & .der supported

Upload Key File: optional

Password: required for .pfx

EXPORT CERTIFICATE

Certificate Name:

Password:

Ogni volta che si riceve un certificato dal proprio fornitore di certificati SSL, questo si presenta come un file ZIP o un insieme di file. Questi conterranno il certificato SSL, il file della chiave e il root ca, oltre a eventuali file intermedi

È necessario importarli nell'ADC e per questo abbiamo fornito un metodo per importarli.

Esistono diversi formati per i certificati SSL, come CER, DER, PEM e PFX. Alcuni formati richiedono un file KEY da aggiungere alla procedura di importazione. I file PFX richiedono la password per importare il certificato PFX.

Abbiamo anche previsto la possibilità di esportare un certificato dall'ADC, se necessario. Una volta esportato, il file sarà in formato PFX e richiederà quindi una password per la creazione dell'esportazione.

Backup e ripristino

Backup

Backup & Restore

BACKUP ALL SSL, CSR & INTERMEDIATE CERTIFICATES

Filename for Backup:

Certificate Name:

Password:

RESTORE CERTIFICATES, CSRs & INTERMEDIATES FROM BACKUP

Upload Certificate:

Password:

Per eseguire il backup dei certificati nel Certificate Store dell'ADC:

- Aggiungere un nome di file da utilizzare per il backup.
- Utilizzare il menu a discesa per selezionare un singolo certificato o TUTTI per eseguire il backup di tutti i certificati.
- Aggiungere una password
- Fare clic sul pulsante Crea backup.
- Il file creato è un file JNBK crittografato.

IMPORTANTE

Il backup funziona solo con i certificati di fiducia importati.

Ripristino

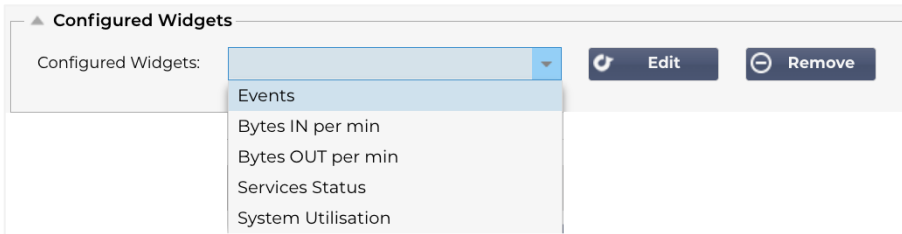
Quando si desidera ripristinare il backup, utilizzare la sezione inferiore della sezione Backup e ripristino.

- Cercare e individuare il file di backup.
- Inserire la password.
- Fare clic sul pulsante Ripristina.
- I certificati presenti nel file di backup verranno ripristinati.

Widget

La pagina Libreria > Widget consente di configurare vari componenti visivi leggeri visualizzati nel dashboard personalizzato.

Widget configurati

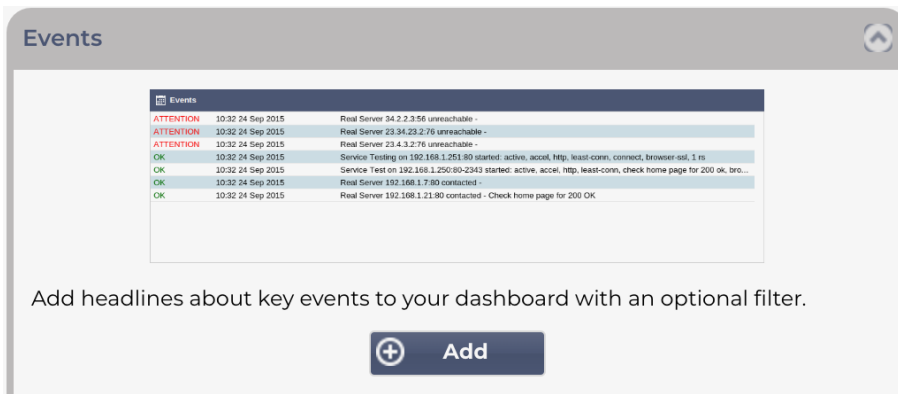


La sezione Widget configurati consente di visualizzare, modificare o rimuovere qualsiasi widget creato dalla sezione Widget disponibili.

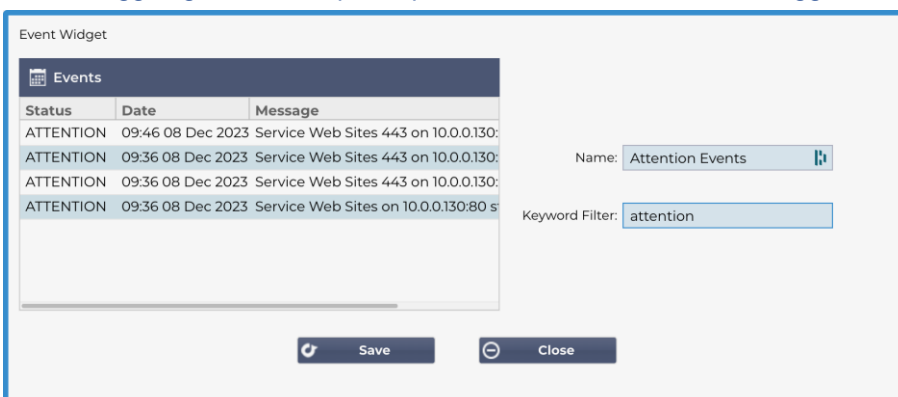
Widget disponibili

L'ADC offre cinque diversi widget, che possono essere configurati in base alle proprie esigenze.

Il widget Eventi

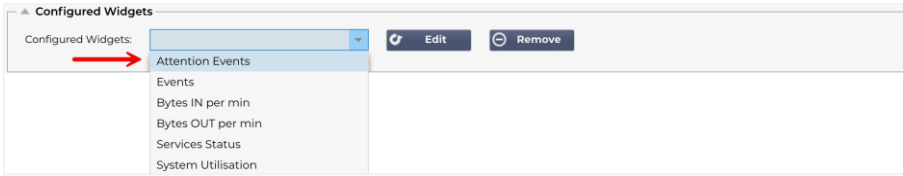


- Per aggiungere un evento al widget Eventi, fare clic sul pulsante Aggiungi.
- Indicare un nome per l'evento. Nel nostro esempio, abbiamo aggiunto Attenzione eventi come nome dell'evento.
- Aggiungere un filtro per le parole chiave. Abbiamo anche aggiunto il valore del filtro Attenzione



- Fare clic su Salva, quindi su Chiudi

- A questo punto, nel menu a tendina dei widget configurati, apparirà un widget aggiuntivo chiamato Eventi di attenzione.

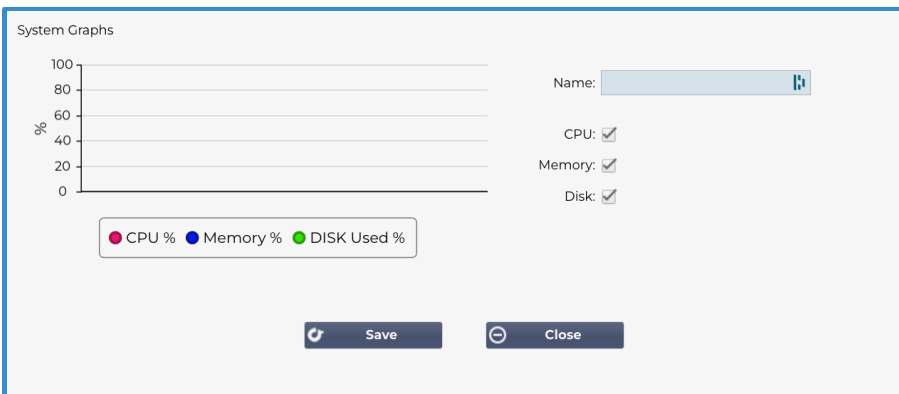


- Si può notare che ora è stato aggiunto questo widget nella sezione Visualizza > Dashboard.
- Selezionare il widget Eventi di attenzione per visualizzarlo nel cruscotto. Vedere sotto.

Status	Date	Message
ATTENTION	14:49 08 Dec 2023	Service on 10.0.0.125:443 stopped: active, accel, http, jsp, 200ok, browser-ssl, 3 rs - stop interface deleted
ATTENTION	10:51 07 Dec 2023	Service on 10.0.0.125:80 stopped: active, accel, http, jsp, 200ok, browser-ssl, 3 rs - Stopping VS 10.0.0.125:80; update interface 10.0.0.125 updated
ATTENTION	10:51 07 Dec 2023	Service on 10.0.0.125:80 stopped: active, accel, http, least-conn, connect, 1 rs - Stopping VS 10.0.0.125:80; update interface 10.0.0.125 updated
ATTENTION	12:12 30 Nov 2023	10.0.0.120:80 Real server myWAF:80 unreachable - Connect=FAIL
ATTENTION	12:09 30 Nov 2023	10.0.0.120:80 Real server myWAF:80 unreachable - Connect=FAIL
ATTENTION	08:53 29 Nov 2023	Service on 10.0.0.125:443 stopped: active, accel, http, least-conn, connect, 3 rs - stop interface deleted
ATTENTION	10:39 23 Nov 2023	Service INGRESS on 10.0.0.120:80 stopped: active, http, least-conn, connect, 1 rs - Stopping VS 10.0.0.120:80; update interface 10.0.0.120 updated
ATTENTION	11:10 22 Nov 2023	Service on 10.0.0.125:443 stopped: active, accel, http, least-conn, connect, browser-ssl, 3 rs - Stopping VS 10.0.0.125:443; update interface 10.0.0.125 updated

È inoltre possibile mettere in pausa e riavviare il flusso di dati in tempo reale facendo clic sul pulsante Pausa dati in tempo reale. Inoltre, è possibile tornare al cruscotto predefinito in qualsiasi momento facendo clic sul pulsante Cruscotto predefinito.

Il widget Grafici di sistema

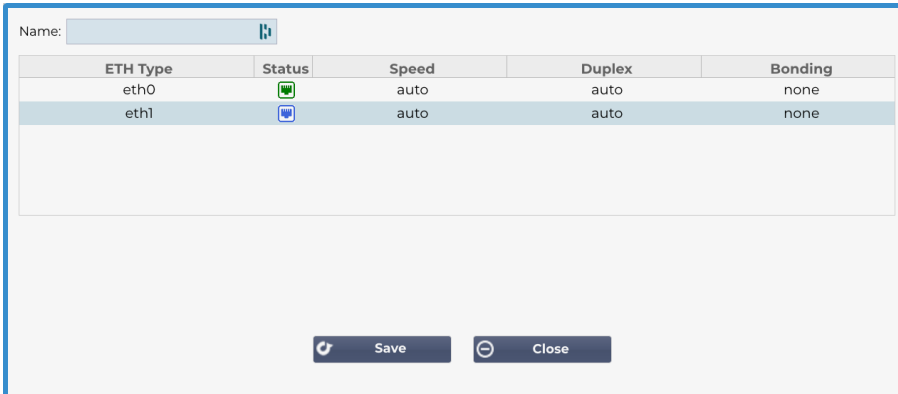


L'ADC dispone di un widget grafico di sistema configurabile. Facendo clic sul pulsante Aggiungi del widget, è possibile aggiungere i seguenti grafici di monitoraggio da visualizzare.

- CPU
- MEMORIA
- DISCO

Una volta aggiunti, saranno disponibili singolarmente nel menu dei widget della Dashboard.

Widget dell'interfaccia



Il widget Interfaccia consente di visualizzare i dati dell'interfaccia di rete scelta, come ETH0, ETH1 e così via. Il numero di interfacce disponibili per l'aggiunta dipende dal numero di interfacce di rete definite per l'appliance virtuale o fornite all'interno dell'appliance hardware.

Al termine, fare clic sul pulsante Salva e poi sul pulsante Chiudi.

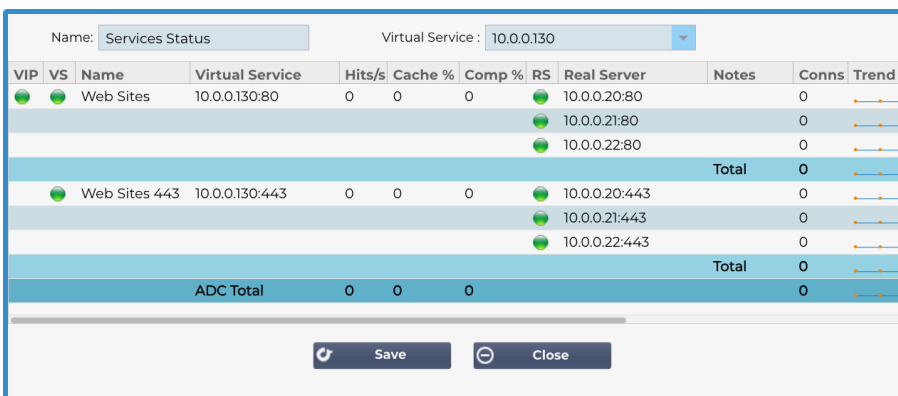
Selezionare il widget appena personalizzato dal menu a discesa dei widget nella Dashboard. Verrà visualizzata una schermata come quella riportata di seguito.



Widget di stato

Il widget Stato consente di vedere il bilanciamento del carico in azione. È anche possibile filtrare la visualizzazione per mostrare informazioni specifiche.

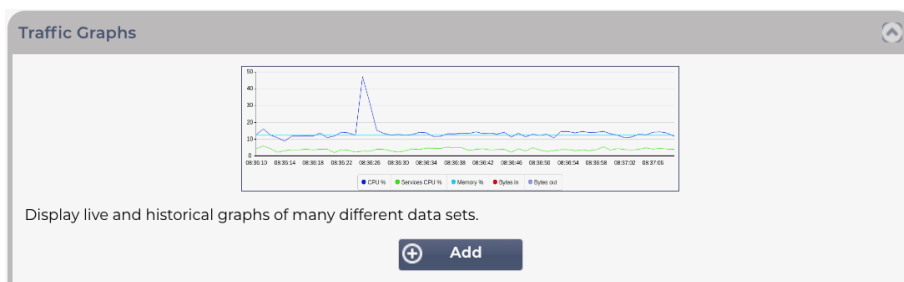
- Fare clic su Aggiungi.



- Inserire un nome per il servizio che si desidera monitorare.
- È inoltre possibile scegliere quali colonne visualizzare nel widget facendo clic sull'intestazione della colonna.
- Una volta soddisfatti, fare clic su Salva e poi su Chiudi.
- Il widget Stato scelto sarà disponibile nella sezione Dashboard.

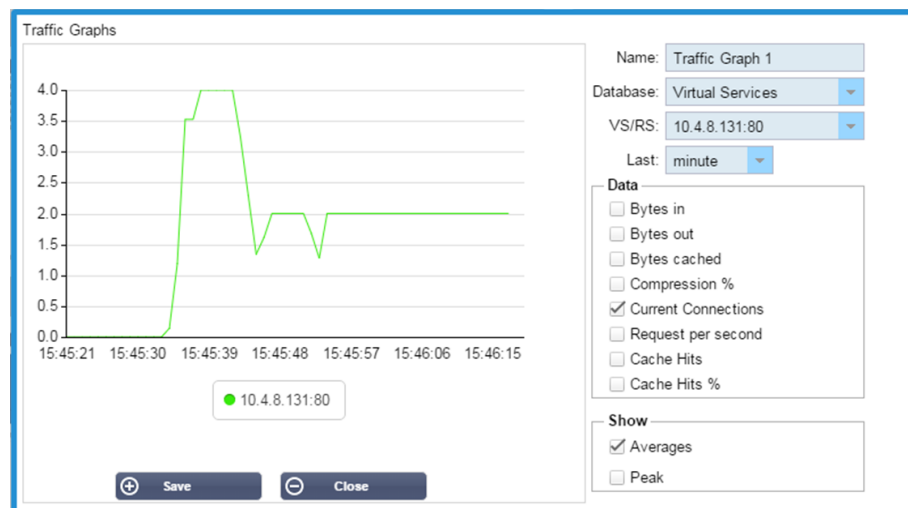
Widget di grafica del traffico

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



- Fare clic sul pulsante Aggiungi
- Date un nome al vostro widget.
- Scegliete un database tra Servizi virtuali, Server reali o Sistema.
- Se si sceglie Servizi virtuali, è possibile selezionare un servizio virtuale dal menu a discesa VS/RS.
- Scegliere un periodo di tempo dal menu a tendina Ultimo.
 - Minuto - ultimi 60 anni
 - Ora - dati aggregati da ogni minuto per gli ultimi 60 minuti
 - Giorno - dati aggregati di ogni ora per le 24 ore precedenti
 - Settimana - dati aggregati di ogni giorno dei sette giorni precedenti
 - Mese - dati aggregati di ogni settimana per gli ultimi sette giorni
 - Anno - dati aggregati di ogni mese nei 12 mesi precedenti
- Scegliere i Dati disponibili in base al database scelto
 - Database dei servizi virtuali
 - Byte in
 - Byte in uscita
 - Byte memorizzati nella cache
 - Compressione %
 - Collegamenti attuali
 - Richieste al secondo
 - Colpi di cache
 - Cache Hits %
- Server reali
 - Byte in
 - Byte in uscita
 - Collegamenti attuali
 - Richiesta al secondo
 - Tempo di risposta
- Sistema
 - CPU %
 - Servizi CPU
 - Memoria %
 - Disco libero %
 - Byte in
 - Byte in uscita
- Scegliere di mostrare i valori medi o di picco
- Una volta scelte tutte le opzioni, fare clic su Salva e chiudi.

Esempio di grafico del traffico



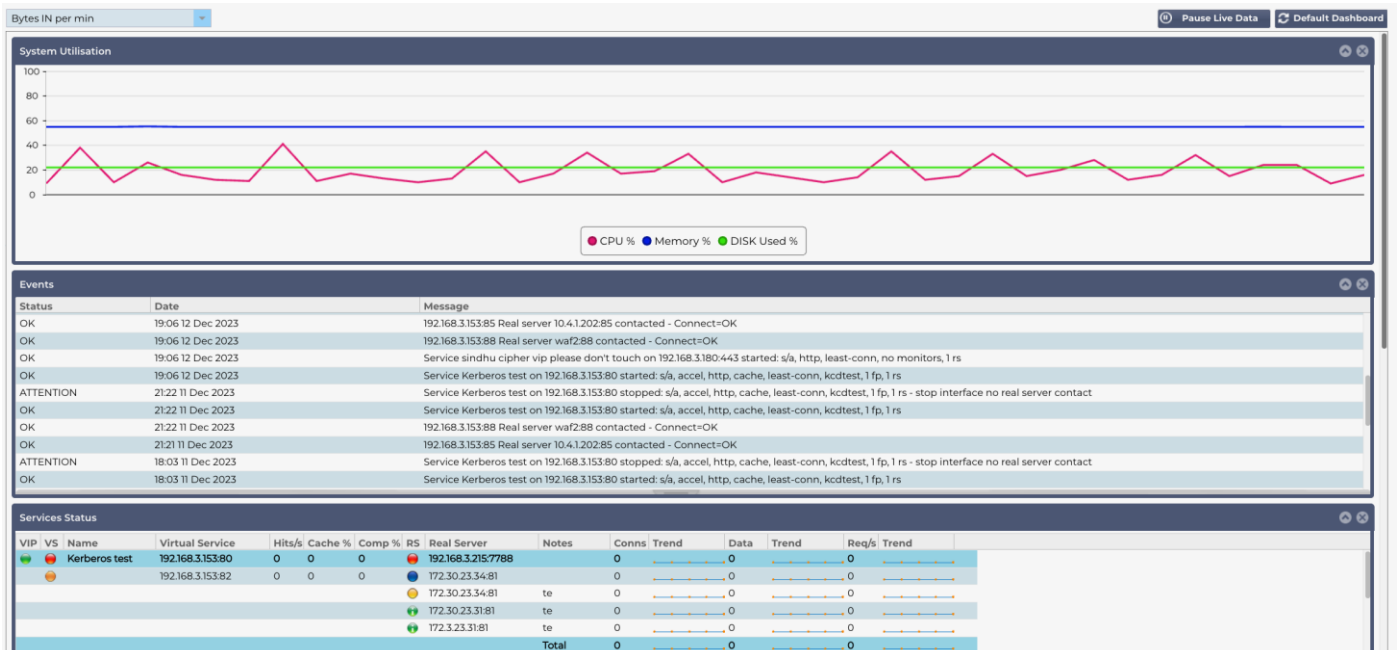
È ora possibile aggiungere il widget del grafico del traffico alla dashboard View> .

Vista

Cruscotto

Come per tutte le interfacce di gestione dei sistemi IT, in molti casi è necessario esaminare le metriche delle prestazioni e i dati gestiti dall'ADC. Noi forniamo un dashboard personalizzabile che vi consente di farlo in modo semplice e significativo.

La Dashboard è raggiungibile tramite il segmento Visualizza del pannello di navigazione. Una volta selezionata, mostra diversi widget predefiniti e consente di scegliere quelli personalizzati definiti dall'utente.



Utilizzo del cruscotto

La Dashboard U è composta da quattro elementi: il menu dei widget, il pulsante Pausa/Play e il pulsante Dashboard predefinito.

Il menu dei widget

Il menu Widget, situato in alto a sinistra del dashboard, consente di selezionare e aggiungere qualsiasi widget standard o personalizzato definito dall'utente. Per utilizzarlo, selezionare il widget dal menu a discesa.

Pulsante Pausa dati in tempo reale

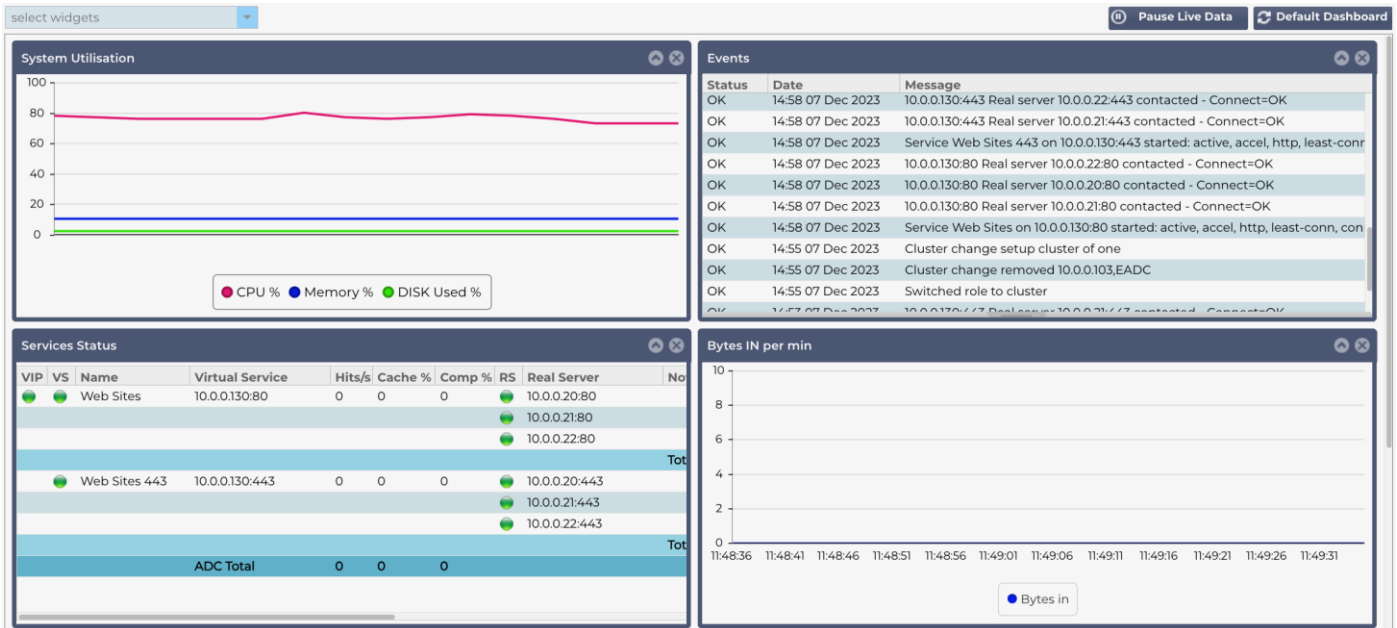
Questo pulsante consente di selezionare se l'ADC deve aggiornare il dashboard in tempo reale. Una volta in pausa, nessun widget del dashboard verrà aggiornato, consentendo all'utente di esaminare il contenuto a proprio piacimento. Il pulsante cambia stato per visualizzare Play Live Data una volta avviata la pausa.

Al termine, è sufficiente fare clic sul pulsante Play Live Data per riavviare la raccolta dei dati e aggiornare il Dashboard.

Pulsante del cruscotto predefinito

È possibile che si desideri ripristinare il layout predefinito del Dashboard. In questo caso, premere il pulsante Cruscotto predefinito. Una volta cliccato, tutte le modifiche apportate al Dashboard andranno perse.

Ridimensionamento, minimizzazione, riordino e rimozione dei widget di



Ridimensionamento di un widget

È possibile ridimensionare un widget molto facilmente. Fare clic e tenere premuto sulla barra del titolo del widget e trascinarlo a sinistra o a destra dell'area del Dashboard. Verrà visualizzato un rettangolo tratteggiato che rappresenta la nuova dimensione del widget. Lasciare cadere il widget nel rettangolo e rilasciare il pulsante del mouse. Se si desidera affiancare un widget ridimensionato a un widget precedentemente ridimensionato, si vedrà apparire il rettangolo adiacente al widget che si desidera affiancare.

Riduzione al minimo di un widget

È possibile ridurre a icona i widget in qualsiasi momento facendo clic sulla barra del titolo del widget. Questa azione riduce a icona il widget e visualizza solo la barra del titolo.

Spostamento dell'ordine dei widget

Per spostare un widget, è possibile trascinarlo facendo clic e tenendo premuto sulla barra del titolo e muovendo il mouse.

Rimozione di un widget

È possibile rimuovere un widget facendo clic sull'icona nella barra del titolo del widget.

La storia



L'opzione Cronologia, selezionabile dal navigatore, consente all'amministratore di esaminare le prestazioni storiche dell'ADC. Le viste storiche possono essere generate per Servizi virtuali, Server reali e Sistema.

Inoltre, consente di vedere il bilanciamento del carico in azione e di individuare eventuali errori o schemi da analizzare. Per utilizzare questa funzione è necessario attivare la registrazione storica in Sistema > Cronologia.

Visualizzazione dei dati grafici

Set di dati

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

Il primo passo è quello di scegliere il database e il periodo di riferimento per le informazioni che si desidera visualizzare. Il periodo che si può selezionare dal menu a tendina Ultimo è Minuti, Ora, Giorno, Settimana, Mese e Anno.

Databas e	Descrizione
Sistema	<p>La selezione di questo database consente di visualizzare la CPU, la memoria e lo spazio su disco nel tempo.</p> 
Servizi virtuali	<p>Selezionando questo database si potranno scegliere tutti i servizi virtuali presenti nel database dal momento in cui si è iniziato a registrare i dati. Verrà visualizzato un elenco di servizi virtuali da cui è possibile selezionarne uno.</p> 
Servizi reali	<p>Selezionando questo database si potranno scegliere tutti i Real Server presenti nel database dal momento in cui si è iniziato a registrare i dati. Verrà visualizzato un elenco di Server reali da cui è possibile selezionarne uno.</p>

▲ **Data Set**

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

Last: day

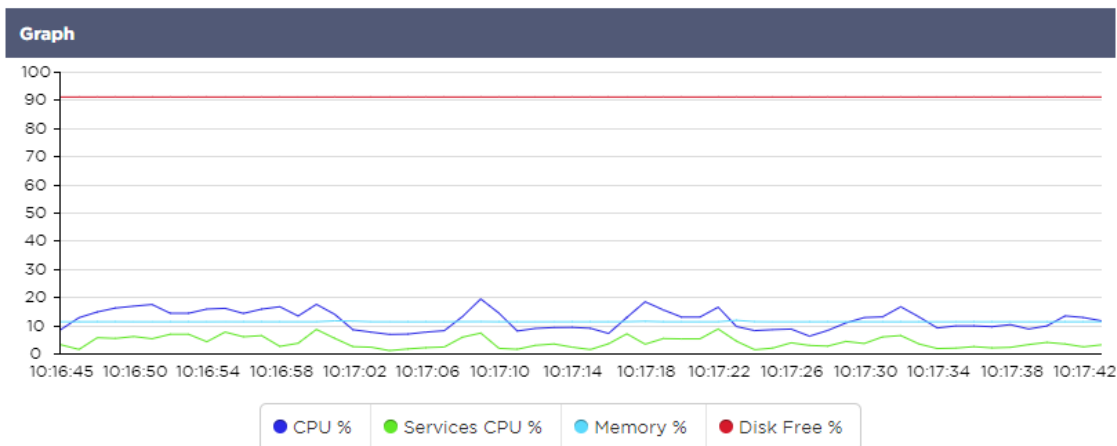
- 192.168.1.40:80-192.168.1.125:8080
- 192.168.1.40:80-192.168.1.119:8080

Metriche

Una volta selezionato il set di dati da utilizzare, è il momento di scegliere le metriche che si desidera visualizzare. L'immagine seguente 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).

SYSTEM	VIRTUAL SERVICES	REAL SERVERS
<p>Metrics</p> <p>Data</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> CPU % <input checked="" type="checkbox"/> Services CPU % <input checked="" type="checkbox"/> Memory % <input checked="" type="checkbox"/> Disk Free % <p>Show</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Averages <input type="checkbox"/> Peak 	<p>Metrics</p> <p>Data</p> <ul style="list-style-type: none"> <input type="checkbox"/> Bytes In <input type="checkbox"/> Bytes Out <input type="checkbox"/> Bytes Cached <input type="checkbox"/> Compression % <input type="checkbox"/> Current Connections <input type="checkbox"/> Request Per Second <input type="checkbox"/> Cache Hits <input type="checkbox"/> Cache Hits % <p>Show</p> <ul style="list-style-type: none"> <input type="checkbox"/> Averages <input type="checkbox"/> Peak 	<p>Metrics</p> <p>Data</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> CPU % <input checked="" type="checkbox"/> Services CPU % <input checked="" type="checkbox"/> Memory % <input checked="" type="checkbox"/> Disk Free % <p>Show</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Averages <input type="checkbox"/> Peak

Grafico di esempio



Registri

La pagina Registri della sezione Visualizza consente di visualizzare in anteprima e scaricare i registri W3C e di sistema. La pagina è organizzata in due sezioni, come illustrato di seguito.

Registri W3C



La registrazione W3C si attiva dalla sezione Sistema > Registrazione. Un log W3C è un log di accesso per i server Web in cui vengono generati file di testo contenenti dati su ogni richiesta di accesso, tra cui l'indirizzo del protocollo Internet (IP) di origine, la versione HTTP, il tipo di browser, la pagina di riferimento e il timestamp. I registri W3C possono diventare molto grandi a seconda della quantità di dati e della categoria di registrazione.

Dalla sezione W3C è possibile selezionare il log desiderato e quindi visualizzarlo o scaricarlo.

Visualizza pulsante

Il pulsante Visualizza consente di visualizzare il registro scelto all'interno della finestra di un editor di testo, come ad esempio il Blocco note.

Scarica il pulsante

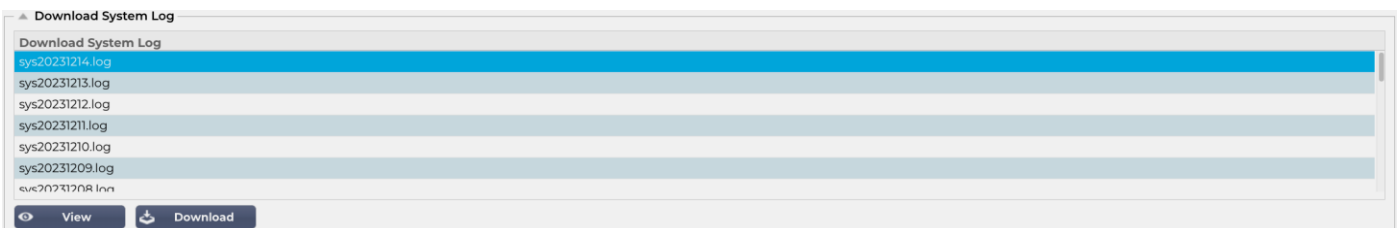
Questo pulsante consente di scaricare il registro nella memoria locale per visualizzarlo successivamente.

Icona Cog

Facendo clic su questa icona si accede alla sezione Impostazioni registro W3C, situata in Sistema > Registrazione. Se ne parlerà in dettaglio nella sezione Registrazione della guida.

Registro di sistema

Il registro di sistema è fondamentale per il debug o l'esame di ciò che accade con l'ADC. È destinato a persone con una certa esperienza all'interno del reparto IT.



Visualizza pulsante

Il pulsante Visualizza consente di visualizzare il registro scelto all'interno della finestra di un editor di testo, come ad esempio il Blocco note.

Scarica il pulsante

Questo pulsante consente di scaricare il registro nella memoria locale per visualizzarlo successivamente.

Statistiche

La sezione Statistiche dell'ADC è un'area molto utilizzata dagli amministratori di sistema che vogliono assicurarsi che le prestazioni dell'ADC siano in linea con le 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 dall'ADC per aumentarne le prestazioni. In alcuni casi gli amministratori desiderano verificare e controllare le informazioni sulla compressione dei dati dell'ADC; questi dati sono forniti dal pannello Compressione all'interno di Statistiche.

Compressione dei contenuti fino ad oggi

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

I dati riportati in questa sezione illustrano il livello di compressione raggiunto dall'ADC sui 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	0	0.00 Mbps (data)
Throughput After Compression	0	0.00 Mbps (data)
Throughput From Cache	0	0.00 Mbps (data)
Total		0.00 Mbps (data)

I valori forniti in questa sezione riportano la percentuale di compressione ottenuta dall'ADC su tutti i contenuti. Una percentuale tipica dipende dal numero di immagini precompresse contenute nei servizi. Maggiore è il numero di immagini, minore sarà probabilmente la percentuale di compressione complessiva.

Totale ingressi/uscite

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

Le cifre relative all'ingresso/uscita totale rappresentano la quantità di dati grezzi trasmessi in entrata e in uscita dall'ADC. L'unità di misura cambia al crescere delle dimensioni, da kbps a Mbps a Gbps.

Colpi e connessioni

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

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

- Un Hit è definito come una transazione di livello 7. Tipicamente utilizzata per i server Web, si tratta di una richiesta GET per un oggetto come un'immagine.

- Una connessione viene definita come una connessione TCP di livello 4. Su una connessione TCP possono avvenire molte transazioni.

Numero complessivo di visite conteggiate

Le cifre di questa sezione mostrano il numero cumulativo di accessi non memorizzati nella cache dall'ultimo reset. Sul lato destro, la figura mostra il numero attuale di accessi al secondo.

Connessioni totali

Il valore Totale connessioni rappresenta il numero cumulativo di connessioni TCP dall'ultimo reset. La cifra nella seconda colonna indica le connessioni TCP effettuate al secondo verso l'ADC. Il numero nella colonna di destra è il numero di connessioni TCP al secondo effettuate ai Real Server. Esempio 6/8 connessioni/sec. Nell'esempio illustrato si hanno 6 connessioni TCP al secondo al servizio virtuale e 6 connessioni TCP al secondo ai server reali.

Connessioni di picco

Il valore di picco delle connessioni 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 si ricorderà, l'ADC è dotato sia di compressione che di caching. Questa sezione mostra le statistiche generali relative alla cache quando viene applicata a un canale. Se la cache non è stata applicata a un canale e configurata correttamente, i contenuti della cache saranno pari a 0.

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

Dalla Cache

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

Byte: La seconda colonna indica la quantità totale di dati in kilobyte serviti dalla cache dell'ADC. Viene fornita anche una percentuale dei dati totali.

Da Server

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

Byte: La seconda colonna indica la quantità totale di dati in kilobyte serviti dai server reali. Viene fornita anche una percentuale dei dati totali.

Contenuto della cache

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

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

Buffer dell'applicazione

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

L'uso dei buffer applicativi in ADC contribuisce a ottimizzare le prestazioni, a migliorare il throughput e a garantire un flusso di dati affidabile ed efficiente tra client e server. Le dimensioni dei buffer, le politiche di gestione e altri parametri sono ottimizzati dall'ADC per regolare con precisione il carico in base ai requisiti specifici delle applicazioni e dell'infrastruttura.

EdgeADC fa il lavoro duro per voi e regola automaticamente i parametri del buffer in base alle esigenze.

Persistenza della sessione

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

La sezione Persistenza della sessione fornisce informazioni su diversi parametri.

Totale sessioni correnti

Mostra quante sessioni di persistenza sono in corso, aggiornate ogni minuto.

% Utilizzato (di max)

Questo mostra l'utilizzo dello spazio totale consentito per le informazioni di sessione.

Nuova sessione questo min

Questo mostra, nell'ultimo minuto, quante nuove sessioni di persistenza sono state aggiunte.

Riconvalidare questo min

Questo mostra, nell'ultimo minuto, quante sessioni di persistenza esistenti sono state riconvalidate da un maggior numero di traffico.

Sessioni scadute questo min

Questo mostra, nell'ultimo minuto, quante sessioni di persistenza esistenti sono scadute a causa dell'assenza di ulteriore traffico entro il timeout.

Hardware

Sia che si utilizzi l'ADC in un ambiente virtuale o nell'hardware, questa sezione fornisce informazioni preziose sulle prestazioni dell'appliance.

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

Utilizzo del disco

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

Utilizzo della memoria

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

Utilizzo della CPU

Uno dei valori critici forniti è la percentuale di CPU attualmente utilizzata dall'ADC. È naturale che questo valore fluttui.

Stato

La pagina Visualizza > Stato visualizza il traffico in tempo reale che attraversa l'ADC per i Servizi virtuali definiti. Mostra anche il numero di connessioni e di dati a ciascun Real Server, in modo da poter sperimentare il bilanciamento del carico in tempo reale.

VIP	VS	Name	Virtual Service	Hits/s	Cache %	Comp %	RS	Real Server	Notes	Conns	Data	Req/s
●	●	Web Sites	10.0.0.130:80	0	0	0	●	10.0.0.20:80		0	0	0
							●	10.0.0.21:80		0	0	0
							●	10.0.0.22:80		0	0	0
								Total		0	0	0
●		Web Sites 443	10.0.0.130:443	0	0	0	●	10.0.0.20:443		0	0	0
							●	10.0.0.21:443		0	0	0
							●	10.0.0.22:443		0	0	0
								Total		0	0	0
			ADC Total	0	0	0				0	0	0

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
●	In linea
●	Failover-Standby. Questo servizio virtuale è in hot-standby
●	Indica che un "passivo" è in attesa di un "attivo".
●	Offline. I server reali non sono raggiungibili o non sono abilitati i server reali.
●	Stato di ritrovamento
●	IP virtuali non licenziati o licenziati superati

Colonna Stato VS

Il colore della luce indica lo stato del servizio virtuale.

Stato	Descrizione
●	In linea
●	Failover-Standby. Questo servizio virtuale è in hot-standby
●	Indica che un "passivo" sta aspettando un "attivo".
●	Servizio Necessita di attenzione. Questa indicazione di stato può derivare dal fallimento di un monitoraggio dello stato di salute di un Real Server o è stata modificata manualmente in Offline. Il traffico continuerà a scorrere, ma con una capacità ridotta del Real Server.
●	Offline. I server reali non sono raggiungibili o non sono abilitati i server reali.
●	Stato di ritrovamento
●	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 gli utenti o le applicazioni utilizzeranno.

Colpo/Sec

Layer 7 transazioni al secondo sul lato client.

Cache%








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

Compressione%

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

Stato RS (Server remoto)

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

Stato	Descrizione
	Collegato
	Non monitorato
	Scarico o non in linea
	Standby
	Non collegato
	Stato di ritrovamento
	IP virtuali non licenziati o licenziati superati

Server reale

Indirizzo IP e porta del Real Server.

Note

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

Conns (Connessioni)

La rappresentazione del numero di connessioni a ciascun Real Server consente di vedere il bilanciamento del carico in azione. È molto utile per verificare che la politica di bilanciamento del carico funzioni correttamente.

Dati

Il valore di questa colonna indica 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

Raggruppamento

L'ADC può essere utilizzato come singolo dispositivo stand-alone e funziona perfettamente. Tuttavia, se si considera che lo scopo dell'ADC è quello di bilanciare il carico di set 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.

Nella pagina Sistema > Clustering si configura l'alta disponibilità delle appliance ADC. Questa sezione è organizzata in diverse sezioni.

Nota importante

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

Clustering

Role

Cluster
Enable Edgenexus ADC to act as part of a Cluster, providing High Availability in Active-Passive mode - automatic synchronisation of appliances

Manual
Enable Edgenexus ADC to act in High Availability mode, either Active-Active or Active-Passive - manual configuration of appliance

Stand-alone
This Edgenexus ADC acts completely independently without high-availability

Settings

Failover Latency (ms):

Failover Messaging:

Management

Unclaimed Devices

Priority	Status	Cluster Members
1	●	10.0.0.103 EADC-103-BETA

IP Address:

Machine Name:

Ruolo

Quando si configura l'ADC per l'alta disponibilità, sono disponibili tre ruoli di cluster.

Cluster

Role

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

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

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

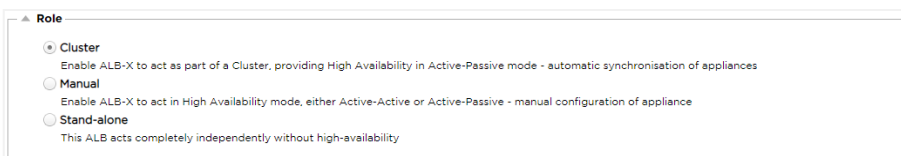
- Per impostazione predefinita, un nuovo ADC si accende utilizzando il ruolo Cluster. In questo ruolo, ogni membro del cluster avrà la stessa "configurazione di lavoro" e, di conseguenza, solo un ADC del cluster sarà attivo in qualsiasi momento.
- Per "configurazione di lavoro" si intendono tutti i parametri di configurazione, ad eccezione degli 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.
- È possibile modificare qualsiasi ADC del cluster e le modifiche saranno sincronizzate con tutti i membri del cluster.
- Quando si rimuove un ADC dal cluster, tutti i servizi virtuali vengono eliminati da quell'ADC.
- Non è possibile rimuovere l'ultimo membro del cluster da Dispositivi non reclamati. Per rimuovere l'ultimo membro, cambiare 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 apparecchi
 - Sezione rete

Fallimento del proprietario del cluster

- Quando il proprietario di un cluster si guasta, uno dei membri rimanenti subentra automaticamente e continua a bilanciare il traffico.
- Quando il proprietario del cluster ritorna, riprende il bilanciamento del traffico e assume il ruolo di proprietario.
- Supponiamo che il proprietario sia fallito e che un membro abbia assunto il bilanciamento del carico. Se si desidera che il membro che ha assunto il bilanciamento del carico diventi il nuovo proprietario, evidenziare il membro e fare clic sulla freccia verso l'alto per spostarlo nella posizione di Priorità 1.
- Se si modifica uno dei membri rimanenti del cluster e il proprietario è inattivo, il membro modificato si promuoverà automaticamente a proprietario senza perdita di traffico.

Cambio di ruolo da ruolo Cluster a ruolo Manuale

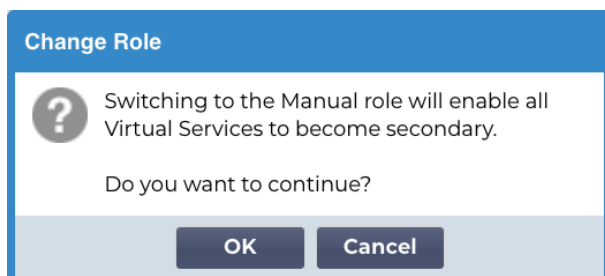
- Se si desidera cambiare il ruolo da Cluster a Manual, fare clic sul pulsante di opzione accanto all'opzione Manual.



▲ Role

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

- Dopo aver fatto clic sul pulsante di opzione, verrà visualizzato il seguente messaggio:



Change Role

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

Do you want to continue?

OK Cancel

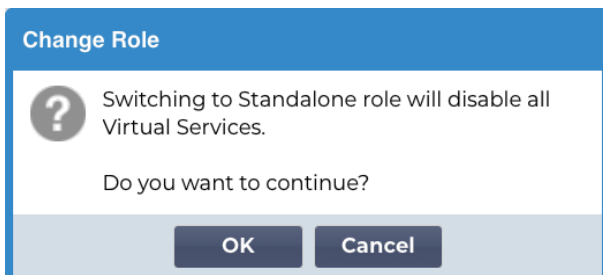
- Fare clic sul pulsante OK
- Controllare la sezione Servizi virtuali. La colonna Primary mostra ora una casella non selezionata.

Virtual Services			
Primary	VIP Status	Service Statu	Enabled
<input type="checkbox"/>	●	●	<input checked="" type="checkbox"/>
<input type="checkbox"/>	●	●	<input checked="" type="checkbox"/>

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

Cambio di ruolo da Cluster a Stand-alone

- Se si desidera cambiare il ruolo da Cluster a Stand-alone, fare clic sul pulsante di opzione accanto all'opzione Standalone.
- Verrà visualizzato il seguente messaggio:



- Fare clic su OK per modificare i ruoli.
- Controllare i Servizi virtuali. Si noterà che la colonna Primary ha cambiato nome in Stand-alone.
- Si noterà inoltre che tutti i Servizi virtuali sono disattivati (non spuntati) per motivi di sicurezza.
- Una volta accertato che nessun altro ADC sulla stessa rete abbia servizi virtuali duplicati, è possibile attivare ciascuno di essi a turno.

Ruolo manuale

Un ADC nel ruolo Manual lavorerà con altri ADC nel ruolo Manual per fornire un'elevata 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. Tutte le modifiche devono essere replicate manualmente su ogni box tramite la GUI oppure, in caso di molte modifiche, è possibile creare un jetPACK da un ADC e inviarlo all'altro.

- Per rendere "attivo" un indirizzo IP virtuale, spuntare la casella di controllo nella colonna primaria (pagina Servizi IP).
- Per rendere un indirizzo IP virtuale "passivo", lasciare vuota la casella di controllo nella colonna primaria (pagina Servizi IP).
- Nel caso in cui un servizio Attivo venga meno per passare al Passivo:
 - Se entrambe le colonne Primary sono spuntate, viene effettuato un processo di elezione e l'indirizzo MAC più basso sarà attivo.
 - Se entrambi sono deselezionati, si svolge lo stesso processo di elezione. Inoltre, se entrambi sono deselezionati, non c'è un ritorno 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 Virtual Services rimarranno nello stato Verde e connessi. È necessario assicurarsi che tutti i servizi virtuali abbiano indirizzi IP univoci, altrimenti si verificherà un conflitto sulla rete.

Impostazioni

▲ **Settings**

Failover Latency (ms):

Failover Messaging:

 **Update**

Latenza di failover (ms)

È possibile impostare la Latenza di Failover in millisecondi. È il tempo di attesa di un ADC passivo prima di assumere il controllo dei servizi virtuali dopo il fallimento dell'ADC attivo.

Si consiglia di impostare questo valore a 10000ms o 10 secondi, ma è possibile diminuirlo o aumentarlo in base alla rete e ai requisiti. I valori accettabili sono compresi tra 1500ms e 20000ms. Se si riscontra instabilità nel cluster con una latenza inferiore, è necessario aumentare questo valore.

Messaggistica in Failover

▲ **Settings**

Failover Latency (ms):

Failover Messaging:

- Broadcast
- Unicast
- Hybrid

Per impostazione predefinita, l'ADC utilizza Broadcast per la messaggistica di failover. Tuttavia, alcune reti bloccano il broadcast e quindi sono disponibili Unicast e Hybrid, un mix di Unicast e Broadcast.

Quando si utilizza la modalità Broadcast predefinita, i dispositivi non reclamati vengono elencati automaticamente e i messaggi broadcast vengono utilizzati per il failover. Se si utilizza la modalità ibrida, i dispositivi non reclamati continueranno a fare pubblicità tramite Broadcast, ma la comunicazione di failover avverrà tramite Unicast. La modalità Unicast non trasmetterà come tale e potrebbe essere necessario inserire manualmente i membri del cluster.

Gestione

In questa sezione è possibile aggiungere e rimuovere membri del cluster e modificare la priorità di un ADC nel cluster. La sezione è composta da due pannelli e da una serie di tasti freccia intermedi. L'area a sinistra è quella dei dispositivi non reclamati, mentre l'area più a destra è il cluster stesso.

▲ Management

Unclaimed Devices
10.0.0.110 EADC-110

Priority	Status	Cluster Members
1	●	10.0.0.103 EADC

⬅
⬆
➡
⬇

Aggiunta di un ADC al cluster

- Prima di aggiungere l'ADC al cluster, è necessario assicurarsi che tutte le appliance ADC abbiano un nome univoco impostato nella sezione Sistema > Rete.
- L'ADC dovrebbe essere visualizzato come Priorità 1 con Stato verde e il suo nome nella colonna Membri del cluster nella sezione di gestione. Questo ADC è l'appliance primaria predefinita.
- Tutti gli altri ADC disponibili appariranno nella finestra Dispositivi non reclamati della sezione di gestione. Un dispositivo non reclamato è un ADC che è stato assegnato al ruolo del cluster, ma non ha servizi virtuali configurati.
- Evidenziare l'ADC dalla finestra Dispositivi non reclamati e fare clic sul pulsante freccia a destra.
- A questo punto viene visualizzato il seguente messaggio:

Promote Unclaimed to Cluster

?

Do you want to promote '10.0.0.110 EADC-110' from unclaimed to cluster?

OK
Cancel

- Fare clic su OK per promuovere l'ADC al cluster.
- L'ADC dovrebbe ora essere visualizzato come priorità 2 nell'elenco dei membri del cluster.

Unclaimed Devices

Priority	Status	Cluster Members
1	●	10.0.0.103 EADC
2	●	10.0.0.110 EADC-110

⬅
⬆
➡
⬇

Aggiunta manuale di un ADC al cluster

Nei sistemi in cui il Broadcast è bloccato, è necessario scegliere la modalità Unicast o Hybrid per aggiungere un ADC al cluster.

▲ Management

Unclaimed Devices

10.0.0.110 EADC-110

▲

◀ ▶

▼

Priority	Status	Cluster Members
1	●	10.0.0.103 EADC-103-BETA

IP Address:

Machine Name:

Add Server

Per aggiungere manualmente un ADC al cluster:

1. Fornire l'indirizzo IP
2. Fornire il nome della macchina, disponibile nella sezione Sistema > Rete.

▲ Basic Setup

Name: EADC-110

IPv4 Gateway: 10.0.0.1 ✓

IPv6 Gateway: ✓

DNS Server 1: 8.8.8.8

DNS Server 2:

Update

3. Fare clic su Aggiungi server

L'ADC verrà quindi aggiunto al cluster.

Se l'ADC che si sta cercando di aggiungere è già presente in un cluster, si riceverà un messaggio di errore.

Rimozione di un membro del cluster

- Evidenziare il membro del cluster che si desidera rimuovere dal cluster.
- Fare clic sul pulsante con la freccia a sinistra.

Unclaimed Devices

▲

◀ ▶

▼

Priority	Status	Cluster Members
1	●	10.0.0.103 EADC
2	●	10.0.0.110 EADC-110

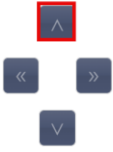
- Verrà presentata una richiesta di conferma.
- Fare clic su OK per confermare.
- L'ADC verrà rimosso e apparirà sul lato Dispositivi non reclamati.



Modifica della priorità di un ADC

Può capitare che si desideri modificare la priorità di un ADC all'interno dell'elenco 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 si trova al secondo posto nell'elenco riceve la priorità 2 ed è l'ADC passivo per tutti i servizi virtuali.
- Per cambiare l'ADC attivo, è sufficiente evidenziarlo e fare clic sulla freccia verso l'alto finché non si trova in cima all'elenco.

Unclaimed Devices

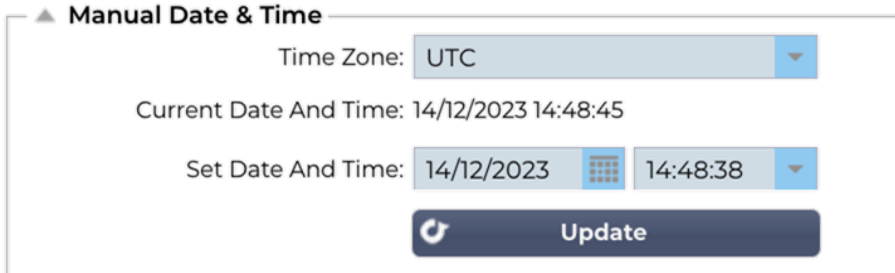


Priority	Status	Cluster Members
1		10.0.0.103 EADC
2		10.0.0.110 EADC-110

Data e ora

La sezione data e ora consente di impostare le caratteristiche di data e ora dell'ADC, compreso il fuso orario in cui si trova l'ADC. Insieme al fuso orario, la data e l'ora svolgono un ruolo fondamentale nei processi crittografici associati alla crittografia SSL.

Data e ora manuali



▲ **Manual Date & Time**

Time Zone: UTC

Current Date And Time: 14/12/2023 14:48:45

Set Date And Time: 14/12/2023 14:48:38

Update

Fuso orario

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

- Fare clic sulla casella a discesa del Fuso orario e iniziare a digitare la propria posizione.
- Ad esempio Londra
- Quando si inizia a digitare, l'ADC visualizzerà automaticamente le posizioni contenenti la lettera L.
- Continuate a digitare "Lon" e così via: le località elencate si restringeranno a quelle contenenti "Lon".
- Se ci si trova, ad esempio, a Londra, scegliere Europa/Londra per impostare la propria posizione.

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

Impostare data e ora

Questa impostazione rappresenta la data e l'ora attuali.

- Scegliere la data corretta dal primo menu a tendina oppure, in alternativa, si può digitare la data nel seguente formato GG/MM/AAAA
- Aggiungere l'ora nel formato hh: mm: ss, ad esempio 06:00:10 per le 6 del mattino e 10 secondi.
- Dopo averla inserita correttamente, fare clic su Aggiorna per applicare.
- La nuova data e ora dovrebbe essere visualizzata in grassetto.

Sincronizzare data e ora (UTC)

È possibile utilizzare i server NTP per sincronizzare con precisione la data e l'ora. I server NTP sono situati in tutto il mondo e si può anche disporre di un proprio server NTP interno quando la propria infrastruttura ha limitazioni di accesso all'esterno.

▲ Synchronise Date & Time (UTC)


Enabled:

Time Server URL:

Update At [hh:mm]: 06:00 ▼

Update Period [hours]: 1 ▲▼

NTP Type: Public SNTP v4 ▼

 Update

URL del server temporale

Inserire un indirizzo IP valido o un nome di dominio completamente qualificato (FQDN) per il server NTP. Se il server è un server situato a livello globale su Internet, si consiglia di utilizzare un FQDN.

Aggiornamento a [hh:mm]

Selezionare l'ora programmata in cui si desidera che l'ADC si sincronizzi con il server NTP.

Periodo di aggiornamento [ore]:

Selezionare la frequenza della sincronizzazione.

NTP Tipo:

- Public SNTP V4 - È il metodo attuale e preferito per la sincronizzazione con un server NTP. [RFC 5905](#)
- NTP v1 Over TCP - Versione NTP legacy su TCP. [RFC 1059](#)
- NTP v1 Over UDP - Versione NTP legacy su UDP. [RFC 1059](#)

Nota: si noti che la sincronizzazione avviene solo in UTC. Se si desidera impostare l'ora locale, è possibile farlo solo manualmente. Questa limitazione sarà modificata nelle versioni successive per consentire la selezione di un fuso orario.

Eventi via e-mail

L'ADC è un dispositivo critico e, come ogni sistema essenziale, è dotato della capacità di informare l'amministratore di sistema di eventuali problemi che richiedono attenzione.

La pagina Sistema > Eventi e-mail consente di configurare una connessione al server e-mail e di inviare notifiche agli amministratori del sistema. La pagina è organizzata nelle sezioni seguenti.

Indirizzo

▲ **Address**

Send E-Mail Events To E-Mail Address:

Return E-Mail Address:

Inviare agli eventi via e-mail agli indirizzi e-mail

Aggiungere un indirizzo e-mail valido a cui inviare gli avvisi, le notifiche e gli eventi. Esempio support@domain.com . È anche possibile aggiungere più indirizzi e-mail utilizzando un separatore di virgole.

Indirizzo e-mail di ritorno:

Aggiungete un indirizzo e-mail che apparirà nella casella di posta. Esempio . adc@domain.com

Server di posta (SMTP)

In questa sezione è necessario aggiungere i dettagli del server SMTP da utilizzare per l'invio delle e-mail. Assicurarsi che l'indirizzo e-mail utilizzato per l'invio sia autorizzato a farlo.

▲ **Mail Server [SMTP]**

Host Address:

Port:

Send Timeout: minutes

Use Authentication:

Security:

Mail Server Account Name:

Mail Server Password:

Indirizzo dell'host

Aggiungere l'FQDN o l'indirizzo IP del server SMTP.

Porto

Aggiungere la porta del server SMTP. La porta predefinita per SMTP è 25 o 587 se si utilizza SSL.

Timeout di invio

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

Utilizzare l'autenticazione

Spuntare la casella se il server SMTP richiede l'autenticazione.

Sicurezza

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

Nome account del server principale

Aggiungere il nome utente necessario per l'autenticazione.

Password del server di posta

Aggiungere la password necessaria per l'autenticazione.

Notifiche e avvisi

Esistono diversi tipi di notifiche di eventi che l'ADC invia alle persone configurate per riceverle. È possibile selezionare e attivare le notifiche e gli avvisi da inviare. 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 Avviso

L'avviso di servizio IP informa l'utente 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 Avviso

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

Avviso sul server reale

Quando un Real Server e una Porta sono connessi o non sono contattabili, l'ADC invia un avviso al Real Server.

voloPATH

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

Notifiche di gruppo Insieme

Selezionare per raggruppare le notifiche. Selezionando questa opzione, tutte le notifiche e gli avvisi verranno aggregati in un'unica e-mail.

Descrizione della posta di gruppo

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


Intervallo di invio del gruppo

Stabilire il tempo di attesa prima di inviare un'e-mail di notifica di gruppo. Il tempo minimo è di 2 minuti. L'impostazione predefinita è di 30 minuti.

Avvertenze abilitate e descrizioni degli eventi in Mail

▲ Enabled Warnings And Event Descriptions In Mail

<input checked="" type="checkbox"/>	Disk Space Warning:	Disk near full
	Warn If Free Space Less Than:	10 %
<input type="checkbox"/>	Licence Renewal Warning:	Licence renewal required

 Update

Esistono due tipi di e-mail di avviso e nessuno dei due deve essere ignorato.

Spazio su disco

Impostare la percentuale di spazio libero su disco prima della quale viene inviato l'avviso. Al raggiungimento di questa percentuale, l'utente riceverà un messaggio di posta elettronica.

Avvisa se lo spazio libero è inferiore a

È possibile impostare un valore percentuale in modo che l'ADC possa inviare un'e-mail di avviso se lo spazio su disco scende al di sotto di questa soglia.

Scadenza della licenza

Questa impostazione consente di attivare o disattivare l'e-mail di avviso di scadenza della licenza inviata all'amministratore del sistema. Quando viene raggiunta questa scadenza, l'utente riceverà un'e-mail.

La storia

Nella sezione Sistema, è presente l'opzione Cronologia del sistema, che consente di fornire dati storici per elementi quali CPU, memoria, richieste al secondo e altre caratteristiche. Una volta attivata, è possibile visualizzare i risultati in forma grafica tramite la pagina Visualizza > Cronologia. Questa pagina consente anche di eseguire il backup o il ripristino dei file di cronologia nell'ADC locale.

Raccogliere i dati

▲ Collect Data

Enabled:

Collect Data Every: 1 Second(s) (1-60)

Update

Abilitazione

Per abilitare la raccolta dei dati, selezionare la casella di controllo.

Raccogliere dati ogni

Quindi, impostare l'intervallo di tempo in cui si desidera che l'ADC raccolga i dati. Questo valore può variare da 1 a 60 secondi.

Manutenzione

▲ Maintenance

Most Recent Update

Fri, 15 Dec 2023 14:45:42

Refresh

Backup

Backup Name:

Backup

Delete

Select To Delete:

Delete

Restore

Select To Restore:

Restore

Aggiornamento più recente

Indica quando sono stati raccolti gli ultimi dati storici dall'ADC.

Questa sezione è grigia se è stata attivata la registrazione storica. Deselezionare la casella di controllo Abilitato nella sezione Raccogli dati e fare clic su Aggiorna per consentire il mantenimento dei registri storici.

ADC aziendali HP

Questa sezione di funzioni è valida solo per gli ADC installati su server HPE ProLiant bare metal e che utilizzano ILO.

Backup

Assegnare al backup un nome descrittivo. Fare clic su Backup per eseguire il backup di tutti i file sull'ADC.

Cancellare

Selezionare un file di backup dall'elenco a discesa. Fare clic su Elimina per rimuovere il file di backup dall'ADC.

Ripristino

Selezionare un file di backup precedentemente memorizzato. Fare clic su Ripristina per inserire i dati da questo file di backup.

Licenza

L'ADC viene concesso in licenza d'uso utilizzando uno dei seguenti modelli, a seconda dei parametri di acquisto e del tipo di cliente.

Tipo di licenza	Descrizione
Perpetuo	Il cliente ha il diritto di utilizzare l'ADC e gli altri software in perpetuo. Ciò non preclude la possibilità di acquistare il supporto per ricevere assistenza e aggiornamenti.
SaaS	SaaS o Software-as-a-Service significa che il software viene essenzialmente noleggiato su base continuativa o pay-as-you-go. In questo modello, si paga un canone annuale per il software. Non si hanno diritti perpetui di utilizzo del software.
MSP	I fornitori di servizi gestiti possono offrire l'ADC come servizio e acquistare la licenza su base individuale, con addebito e pagamento annuale.

Dettagli della licenza

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

Licence Details	
Licence ID:	8090DD7C- DE8D6A1
Machine ID:	F F3
Issued To:	Edgenexus
Contact Person:	Jay Savoor
Date Issued:	06 Dec 2023
Name:	

ID licenza

L'ID di licenza è direttamente collegato all'ID macchina e ad altri dettagli specifici dell'acquisto e dell'apparecchio ADC. Queste informazioni sono essenziali e sono necessarie quando si desidera recuperare aggiornamenti e altri articoli dall'App Store.

ID macchina

L'ID macchina viene generato utilizzando l'indirizzo IP eth0 dell'appliance ADC. Se si cambia l'indirizzo IP del dispositivo ADC, la licenza non sarà più valida. È necessario contattare l'assistenza per ottenere assistenza. Si raccomanda che le appliance ADC abbiano indirizzi IP fissi, con istruzioni al personale IT di non modificarli. L'assistenza tecnica è disponibile tramite un ticket all'indirizzo <https://www.edgenexus.io/support>.

Nota: Non è consentito modificare l'indirizzo IP delle apparecchiature ADC. Se si dispone di un framework virtualizzato, fissare il MAC ID e utilizzare un indirizzo IP statico.

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.

Data Emissione d

La data di rilascio della licenza.

Nome

Questo valore indica il nome descrittivo della periferica ADC fornito in Sistema > Rete.

Strutture

▲ Facilities	
Layer 4:	Permanent licence
Layer 7:	Permanent licence
SSL:	Permanent licence
Acceleration:	Permanent licence
flightPATH:	Permanent licence
Pre-Authentication:	Permanent licence
Global Server Load-Balancing:	Permanent licence
Firewall:	Permanent licence
Throughput:	3 Gbps permanent licence
Virtual Service IPs:	24 Virtual Service IPs permanent licence
Real Server IPs:	64 Real Server IPs permanent licence

La sezione strutture fornisce informazioni su quali funzioni dell'ADC sono state concesse in licenza d'uso e sulla validità della licenza. Vengono inoltre visualizzati il throughput concesso in licenza per l'ADC e il numero di Real Server. Queste informazioni dipendono dalla licenza acquistata.

Installare le licenze e

▲ Install Licence

Upload Licence:

Paste Licence:

- L'installazione di una nuova licenza è molto semplice. Quando si riceve la licenza nuova o sostitutiva da Edgenexus, questa viene inviata sotto forma di file di testo. È possibile aprire il file e copiare e incollare il contenuto nel campo Incolla licenza.
- È anche possibile caricarlo sull'ADC se il copia/incolla non è un'opzione possibile.
- Una volta effettuata questa operazione, fare clic sul pulsante di aggiornamento.

- La licenza è ora installata.

Informazioni sul servizio di licenza

Facendo clic sul pulsante Informazioni sul servizio di licenza vengono visualizzate tutte le informazioni sulla licenza. Questa funzione può essere utilizzata per inviare i dettagli al personale di assistenza.

The screenshot displays the following information:

- MAC Address:** 00:5C:5E:00:00:00
- Current Version:** 4.3.0 (Build 1965) c50631
- Server Ref:** EADC
- OS Version:** Linux jetnexus 2.6.32-754.31.1.el6.x86_64 #1 SMP
- Licence Configuration:**

```
[jetnexusdaemon]
.001Licence="jetNEXUS ALB Licence"
.002Customer="Issued To,Edgenexus"
.003Contact="Contact Person,..."
.004Tel="Telephone,"
.005LicenseID="License ID,[8090D[...] DE8D6A1]"
Customer="Edgenexus"
.100Details="Details"
```
- System Configuration:**

```
[jetnexusdaemon]
AdaptivePollingEnabled=1
AddXForwardedFor=1
AdvancedW3C="HTTP Layer4"
AllowCompressedUploads=0
AllowIdentity=0
AlwaysChunk=0
ApiSessionTimeout="525600"
```
- System Log:**

```
18 Dec 00:28:12 jetnexus software-monitoring:
Stats|HitCount=0|InputBytes=0|OutputBytes=0|CompressedInputBytes=0|CompressedOutputBytes=0|TotalClientConnections=0|TotalServerConnections=0|CurrentConnections=0|MaximumConnections=0|RefusedConnections=0|UploadInputBytes=0|UploadOutputBytes=0|UploadCompressedInputBytes=0|UploadCompressedOutputBytes=0|TotalInputBytes=461,445,645|TotalOutputBytes=378,426,680|Memory=184,552,448|MemoryUsagePercent=10|DiskFreeSpace=19,308,112|DiskFree=98|CPUPercent=3|CPUHostPercent=0|EthernetErrors=0|Runnable=1|Processes=424|Sessions=0|NewSess=0|ExpiredSess=0|RevalidatedSess=0|BLConn=0|BLMax=5,000|BLFill=0|BLAlloc=0|BLRoom=655,360,000|BMCon=0|BMMax=5,000|BMFill=0|BMAlloc=0|BMRoom=30,000,000|BTCon=0|BTMax=10,000|BTFill=0|BTAlloc=0|BTRoom=20,000,000|BSecure=0|CONNECTIONS=5|TIME-WAIT=0|ALLOCSOCK=134|ORPHANSOCK=0|SOCKMEM=0|ESTABLISHED=0|SYN=0|PORTS=21
18 Dec 00:29:02 jetnexus software-monitoring:
```

Registrazione

La pagina Sistema > Registrazione consente di impostare i livelli di registrazione W3C e di specificare il server remoto su cui esportare automaticamente i log. La pagina è organizzata nelle quattro sezioni seguenti.

Dettagli di registrazione W3C

Abilitando la registrazione W3C, l'ADC inizierà a registrare un file di log compatibile W3C. Un log W3C è un log di accesso per i server Web in cui vengono generati file di testo contenenti dati su ogni richiesta di accesso, tra cui l'indirizzo IP (Internet Protocol) di origine, la versione HTTP, il tipo di browser, la pagina di riferimento e l'ora. Il formato è stato sviluppato dal World Wide Web Consortium (W3C), un'organizzazione che promuove gli 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 righe di commento è una riga che indica i campi (fornendo i nomi delle colonne) in modo che i dati possano essere estratti. Esistono 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 precedente descrive i livelli di registrazione per W3C HTTP.

Valore	Descrizione
Nessuno	La registrazione W3C è disattivata.
Breve	I campi presenti sono: #Campi: time c-ip c-port s-ip method uri x-c-version x-r-version sc-status cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x- round-trip-time cs(User-Agent) x-sc(Content-Type).
Completo	Si tratta di un formato più compatibile con i processori, con campi separati per la data e l'ora. Per informazioni sul significato dei campi, vedere il riepilogo dei campi qui sotto. I campi presenti sono: #Campi: date time 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 "Completo", ma presenta un campo aggiuntivo. Per informazioni sul significato dei campi, consultare il riepilogo dei campi riportato di seguito. I campi presenti sono: #Campi: date time x-mil c-ip c-port cs-username s-ip s-port cs-host cs-c-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 informazioni rilevanti per il personale di sviluppo e di supporto. Per informazioni sul significato dei campi, consultare il riepilogo dei campi qui sotto. I campi presenti sono: #Campi: date time c-ip c-port cs-username s-ip s-port x-xff x-xffcustom cs-host x-r-ip x-r-port cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent) referer x-c-version x-r-version cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x-round-trip-time x-trip-times(new,rcon,rqf,rql,tqf,tql,rsf,rsl,tsf,tsl,dis,log) x-closed-by x- compress-action x-sc(Content-Type) x-cache-action X-finish

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

Valore	Descrizione
Breve	#Campi: date time c-ip c-port s-ip s-port r-ip r-port cs-method cs-param sc-status sc-param sr-method sr-param rs-status rs-param
Completo	#Campi: date time 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: date time c-ip c-port s-ip s-port r-ip r-port cs-method cs-param cs-bytes sc-status sc-param sc-bytes sr-method sr-param sr-bytes rs-status rs-param rs-bytes

Includere la registrazione W3C

Questa opzione consente di impostare quali informazioni sull'ADC devono essere incluse nei log W3C.

Valore	Descrizione
Indirizzo e porta di rete del cliente	Il valore mostrato qui visualizza l'indirizzo IP effettivo del client e la porta.
Indirizzo di rete del cliente	Questa opzione include e mostra solo l'indirizzo IP effettivo del client.
Indirizzo e porta inoltrati	Questa opzione mostra i dettagli contenuti nell'intestazione XFF, compresi l'indirizzo e la porta.
Indirizzo di inoltro	Questa opzione mostra i dettagli contenuti nell'intestazione XFF, compreso il solo indirizzo.

Includere informazioni sulla sicurezza

Questo menu è composto da due opzioni:

Valore	Descrizione
Su	Questa impostazione è globale. Se impostata su on, il nome utente verrà aggiunto al log W3C quando un qualsiasi servizio virtuale utilizza l'autenticazione e ha il log W3C abilitato.
Spento	Questo disattiva la possibilità di registrare il nome utente nel registro W3C a livello globale.

Server Syslog

▲ Syslog

Message Level: Warning

Update

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

Error

Warning

Notice

Info

Server Syslog remoto

▲ Remote Syslog Server

Syslog Server 1: Port: Enabled:

Syslog Server 2: Port: Enabled:

In questa sezione è possibile configurare due server Syslog esterni per l'invio di tutti i log di sistema.

- Aggiungere l'indirizzo IP del server Syslog
- Aggiungere la porta
- Scegliere se utilizzare il protocollo TCP o UDP.
- Spuntare la casella di controllo Abilitato per iniziare la registrazione.
- Fare clic su Aggiorna

Archiviazione remota dei registri

▲ Remote Log Storage

Remote Log Storage:

IP Address:

Share Name:

Directory:

Username:

Password:

Tutti i registri W3C vengono memorizzati in forma compressa sull'ADC ogni ora. I file più vecchi vengono eliminati quando rimane il 30% dello spazio su disco. Se si desidera esportare questi file su un server remoto per conservarli, è possibile configurarli utilizzando una condivisione SMB. Si noti che il registro W3C non verrà trasferito alla posizione remota finché il file non sarà stato completato e compresso. Poiché i registri vengono scritti ogni ora, questa operazione potrebbe richiedere fino a due ore in un dispositivo con macchina virtuale e cinque ore per un dispositivo hardware.

Col1	Col2
Archiviazione remota dei registri	Spuntare la casella per abilitare l'archiviazione remota dei registri
Indirizzo IP	Specificare l'indirizzo IP del server SMB. Deve essere in notazione decimale punteggiata. Esempio: 10.1.1.23
Nome della quota	Specificare il nome della condivisione sul server SMB. Esempio: w3c.
Elenco	Specificare la directory sul server SMB. Esempio: /log.
Nome utente	Specificare il nome utente per la condivisione SMB.
Password	Specificare la password per la condivisione SMB

Riepilogo del campo

Condizione	Descrizione
Data	Non localizzato = sempre AAAA-MM-GG (GMT/UTC)
Tempo	Non localizzato = HH:MM:SS o HH:MM:SS.ZZZ (GMT/UTC) * Nota: purtroppo questo ha due formati (Site

	non ha .ZZZ millisecondi)
x-mil	Solo formato sito = millisecondo della marca temporale
c-ip	L'IP del cliente può essere ricavato al meglio dalla rete o dall'intestazione X-Forwarded-For.
porta c	La porta del client può essere ricavata al meglio dalla rete o dall'intestazione X-Forwarded-For.
cs-nome utente	Campo di richiesta del nome utente del cliente
s-ip	Porta di ascolto di ALB
s-port	VIP in ascolto di ALB
x-xff	Valore dell'intestazione X-Forwarded-For
x-xffcustom	Valore dell'intestazione di richiesta di tipo X-Forwarded-For con nome configurato
cs-host	Nome host nella richiesta
x-r-ip	Indirizzo IP del Real Server utilizzato
x-r-port	Porta del server reale utilizzata
cs-metodo	Metodo di richiesta HTTP * tranne il formato Brief
metodo	* Solo il formato breve utilizza questo nome per il metodo cs.
cs-uri-stem	Percorso della risorsa richiesta * tranne il formato Brief
cs-uri-query	Interrogazione della risorsa richiesta * tranne il formato Brief
uri	* Il formato breve registra un percorso combinato con una stringa di interrogazione.
stato sc	Codice di risposta HTTP
cs(User-Agent)	Stringa User-Agent del browser (inviata dal client)
referente	Pagina di riferimento (inviata dal cliente)
x-c-versione	Richiesta del cliente Versione HTTP
x-r-versione	Contenuto-Risposta del server Versione HTTP
cs-byte	Byte dal client, nella richiesta
sr-byte	Byte inoltrati al Real Server, nella richiesta
rs-byte	Byte dal Real Server, nella risposta
sc-byte	Byte inviati al client, nella risposta
x-percentuale	Percentuale di compressione * = $100 * (1 - \text{output} / \text{input})$ comprese le intestazioni
tempo impiegato	Quanto tempo ha impiegato il Real Server in secondi
x-trip-times nuovo pcon	millisecondo dalla connessione alla pubblicazione nella "lista dei nuovi arrivati". millisecondo dalla connessione all'inserimento della connessione al Real Server
acon	millisecondo dalla connessione alla fine della connessione al Real Server
rcon	millisecondo dalla connessione all'instaurazione della connessione al server reale
rqf	millisecondo dalla connessione alla ricezione del primo byte di richiesta dal client
rql	millisecondo dalla connessione alla ricezione dell'ultimo byte di richiesta da parte del client
tqf	millisecondo dalla connessione all'invio del primo byte di richiesta al Real Server
tql	millisecondo dalla connessione all'invio dell'ultimo byte di richiesta al Real Server
rsf	millisecondo dalla connessione alla ricezione del primo byte di risposta dal Real Server
rsl	millisecondo dalla connessione alla ricezione dell'ultimo byte di risposta dal Real Server
tsf	millisecondo dalla connessione all'invio del primo byte di risposta al 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)
log	millisecondo dalla connessione a questo record di log solitamente seguito da (Politica di bilanciamento del carico e ragionamento)
x-round-trip-time	Durata dell'ALB in secondi
x-chiuso da	Quale azione ha causato la chiusura (o il mantenimento) della connessione?
x-azione di compressione	Come la compressione è stata effettuata o evitata
x-sc(Tipo di contenuto)	Tipo di contenuto della risposta
x-cache-action	Come la cache ha risposto o è stata impedita
x-finitura	L'innesco che ha causato questa riga di registro

Cancellare i file di registro

▲ Clear Log Files

Log Type:

Questa funzione consente di cancellare i file di log dall'ADC. È possibile selezionare il tipo di registro da eliminare dal menu a discesa e fare clic sul pulsante Cancella.

Rete

La sezione Rete della Libreria consente di configurare le interfacce di rete dell'ADC e il loro comportamento.

IMPORTANTE

Gestione delle interfacce di rete virtuali in un ambiente virtuale

Quando si distribuiscono le macchine virtuali in un ambiente virtualizzato come ESXi, le interfacce di rete (ad esempio, eth0, eth1) vengono create automaticamente e mappate agli adattatori di rete della configurazione dell'host (ad esempio, Network Adapter 1, Network Adapter 2). Tuttavia, queste mappature potrebbero non essere sempre coerenti a causa delle regole del sistema operativo che legano le interfacce a indirizzi MAC specifici. Questa sezione illustra i passaggi per la gestione delle interfacce di rete sull'host per evitare interruzioni dei servizi quando l'utente non può accedere alla macchina virtuale.

Considerazioni chiave

- Persistenza dell'indirizzo MAC:**
 - Il sistema operativo assegna i nomi delle interfacce (ad esempio, eth0, eth1) in base a regole che associano un nome a un indirizzo MAC specifico.
 - L'eliminazione e la ricreazione di un'interfaccia di rete della macchina virtuale senza riutilizzare l'indirizzo MAC originale può causare una configurazione di rete incoerente o non funzionante.
- Mappature interne in ADC (EdgeOS):**
 - Le interfacce di rete virtuali vengono riconosciute automaticamente dall'ADC (Application Delivery Controller) e mappate internamente.
 - La rimozione di un'interfaccia di rete dall'host della macchina virtuale può lasciare mappature non aggiornate nell'ADC, con potenziali interruzioni dell'accesso alla gestione o ai servizi di rete.

Passi consigliati per la configurazione dell'host

- Prima di rimuovere una NIC:**
 - Registrare l'indirizzo MAC dell'interfaccia che si intende rimuovere. Questo può essere visualizzato nelle impostazioni della macchina virtuale nell'host ESXi.
- Quando si aggiunge una NIC sostitutiva:**
 - Assegnare l'indirizzo MAC registrato in precedenza alla nuova scheda di rete per garantire che le mappature delle interfacce della macchina virtuale rimangano coerenti.
- Prevenire la cancellazione accidentale di NIC critiche:**
 - Identificare quali NIC sono mappate su interfacce ADC critiche (ad esempio, ETH0 (Greenside) per l'accesso alla gestione). Evitate di rimuovere queste NIC se non è assolutamente necessario.
- Verificare la coerenza dell'indirizzo MAC:**
 - Assicurarsi che gli indirizzi MAC assegnati alle interfacce di rete della macchina virtuale corrispondano alla configurazione prevista nell'ADC. Utilizzare gli strumenti dell'host ESXi per confermare questa mappatura.
- Coordinarsi con gli amministratori della macchina virtuale:**
 - Se sono necessarie modifiche che potrebbero influire sulla configurazione interna della macchina virtuale, informare gli amministratori della macchina virtuale per prepararsi a potenziali interruzioni e garantire il mantenimento di mappature corrette.

Scenario di esempio

- Impostazione iniziale:**
 - La macchina virtuale ADC ha due NIC: NIC1 (MAC: 00:11:22:33:44:55) e NIC2 (MAC: 00:11:22:33:44:66).
- Azione:** Rimuovere la NIC1 e aggiungere una nuova NIC (NIC3).
 - Assegnare l'indirizzo MAC originale (00:11:22:33:44:55) alla NIC3 durante la creazione sull'host ESXi.
- Evitare l'impatto:**

- a. Riutilizzando l'indirizzo MAC originale, le mappature interne dell'ADC (ad esempio, ETH0) rimangono coerenti, evitando di interrompere l'accesso alla gestione o ai servizi di rete.

Quando si gestiscono le interfacce di rete in un ambiente virtualizzato, è fondamentale mantenere la coerenza nell'assegnazione degli indirizzi MAC. Se l'accesso alla macchina virtuale non è disponibile, è necessario completare tutte le operazioni necessarie sul lato host per garantire il funzionamento senza interruzioni e prevenire le interruzioni del servizio. Coordinarsi sempre con gli amministratori competenti per affrontare efficacemente i potenziali impatti.

Evitare il vMotion frequente per le appliance critiche

vMotion è una potente funzione di VMware che consente la migrazione live di macchine virtuali (VM) tra host ESXi senza tempi di inattività. Tuttavia, sebbene vMotion sia molto utile per mantenere la flessibilità e la disponibilità dell'infrastruttura, non è consigliabile migrare frequentemente appliance critiche, come i bilanciatori di carico, soprattutto quando gestiscono attivamente un volume elevato di connessioni.

Potrebbero esistere altre tecnologie simili fornite da altri fornitori, ma per questa sezione ci baseremo su VMware.

Perché il vMotion frequente non è consigliato

1. **Interruzioni di sessione:**
 - a. I bilanciatori di carico gestiscono le sessioni attive tra i client e i server backend. Durante un'operazione di vMotion, si verifica un breve periodo in cui lo stato della rete viene reinizializzato, interrompendo potenzialmente queste sessioni.
 - b. L'interruzione può causare cadute di connessione, richiedendo ai client di ristabilire le loro sessioni, il che potrebbe degradare l'esperienza dell'utente.
2. **Latenza e perdita di pacchetti:**
 - a. Il processo di migrazione di una macchina virtuale comporta una pausa temporanea e la sincronizzazione della memoria e dello stato. Per le apparecchiature che gestiscono il traffico in tempo reale, questa pausa può introdurre latenza o addirittura perdita di pacchetti.
 - b. Le applicazioni che si affidano a risposte a bassa latenza possono subire una riduzione delle prestazioni o dei timeout.
3. **Maggiore utilizzo delle risorse:**
 - a. vMotion richiede risorse di CPU, memoria e larghezza di banda di rete per la sincronizzazione dei dati tra gli host di origine e di destinazione.
 - b. Le migrazioni frequenti possono affaticare le risorse dell'infrastruttura, con un potenziale impatto sulle altre macchine virtuali e sui servizi ospitati nello stesso ambiente.
4. **Impatto sulle configurazioni ad alta disponibilità:**
 - a. In ambienti con configurazioni ad alta disponibilità (HA), il vMotion frequente può entrare in conflitto con i meccanismi di failover, causando comportamenti imprevisti o ritardi nelle azioni di failover.
5. **Complessità operativa:**
 - a. Lo spostamento costante di macchine virtuali critiche aumenta la complessità delle configurazioni di rete, comprese le mappature VLAN e le regole del firewall, che possono introdurre errori di configurazione.

Raccomandazioni per la gestione delle apparecchiature critiche

1. **Pianificare le operazioni di vMotion durante le finestre di manutenzione:**
 - a. Programmare le migrazioni durante i periodi di basso traffico per ridurre al minimo l'impatto sulle sessioni attive.
2. **Implementare il clustering del bilanciatore di carico:**
 - a. Utilizzare configurazioni di clustering o ad alta disponibilità per i bilanciatori di carico per garantire la ridondanza. Ciò consente di reindirizzare il traffico su un altro nodo durante le operazioni di vMotion.
3. **Monitoraggio delle risorse infrastrutturali:**
 - a. Assicurarsi che siano disponibili CPU, memoria e larghezza di banda di rete sufficienti prima di avviare il vMotion per evitare la contesa delle risorse.
4. **Ridurre al minimo la frequenza di migrazione:**

- a. Limitare il vMotion delle appliance critiche agli scenari in cui è assolutamente necessario, come la manutenzione dell'host o il ripristino di un guasto.
5. **Test prima della produzione:**
- a. Testate le operazioni di vMotion in un ambiente di staging per comprenderne l'impatto sulle sessioni attive e garantire l'ottimizzazione delle configurazioni.

Sebbene vMotion sia uno strumento prezioso per la gestione delle macchine virtuali, deve essere usato con giudizio per le appliance critiche come i bilanciatori di carico. Migrazioni frequenti possono interrompere i servizi, aumentare la latenza e affaticare le risorse. Pianificando attentamente le operazioni di vMotion e impiegando strategie come il clustering e la pianificazione della manutenzione, è possibile garantire un'erogazione affidabile dei servizi e ridurre al minimo il rischio di interruzioni.

Impostazione di base

Nome ALB

Specificare un nome per l'appliance ADC. Si noti che questo nome non può essere modificato se c'è più di un membro nel cluster. Consultare la sezione Clustering.

Gateway IPv4

Specificare l'indirizzo del gateway IPv4. Questo indirizzo deve essere nella stessa sottorete di un adattatore esistente. Se il gateway è stato aggiunto in modo errato, verrà visualizzata una croce bianca in un cerchio rosso. Quando si aggiunge un gateway corretto, si vedrà un banner verde di successo in fondo alla pagina e un segno di spunta bianco in un cerchio verde accanto all'indirizzo IP.

Gateway IPv6

Specificare l'indirizzo del gateway IPv6. Questo indirizzo deve trovarsi nella stessa sottorete di un adattatore esistente. Se il gateway è stato aggiunto in modo errato, verrà visualizzata una croce bianca in un cerchio rosso. Quando si aggiunge un gateway corretto, si vedrà un banner verde di successo in fondo alla pagina e un segno di spunta bianco in un cerchio verde accanto all'indirizzo IP.

Server DNS 1 e Server DNS 2

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

Dettagli sull'adattatore

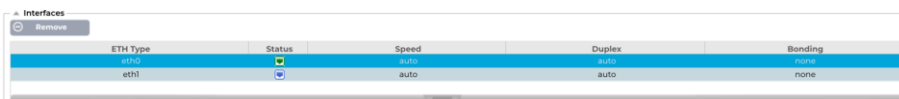
Questa sezione del pannello Rete mostra le interfacce di rete installate nell'appliance ADC. È possibile aggiungere e rimuovere gli adattatori secondo le necessità.

Colonna	Descrizione
Adattatore	In questa colonna sono visualizzati gli adattatori fisici installati sull'appliance. Scegliete un adattatore dall'elenco degli adattatori disponibili facendo clic su di esso - un doppio clic porterà la riga dell'elenco in modalità di modifica.
VLAN	Fare doppio clic per aggiungere l'ID VLAN dell'adattatore. Una VLAN è una rete locale virtuale che crea un dominio di trasmissione distinto. Una VLAN ha gli stessi attributi di una





	LAN fisica, ma consente di raggruppare più facilmente le stazioni finali che non si trovano sullo stesso switch di rete.
Indirizzo IP	Fare doppio clic per aggiungere l'indirizzo IP associato all'interfaccia dell'adattatore. È possibile aggiungere più indirizzi IP alla stessa interfaccia. Si tratta di un numero IPv4 a 32 bit in notazione decimale quadrupla. Esempio 192.168.101.2
Maschera di sottorete	Fare doppio clic per aggiungere la maschera di sottorete assegnata all'interfaccia dell'adattatore. Si tratta di un numero IPv4 a 32 bit in notazione decimale punteggiata. Esempio 255.255.255.0
Porta d'ingresso	Aggiungere un gateway per l'interfaccia. Una volta aggiunto, l'ADC imposterà un semplice criterio che consentirà alle connessioni avviate da questa interfaccia di essere rinviate attraverso questa interfaccia al router gateway specificato. Ciò consente di installare l'ADC in ambienti di rete più complessi, senza dover configurare manualmente criteri di routing complessi.
Descrizione	Fare doppio clic per aggiungere una descrizione all'adattatore. Esempio di interfaccia pubblica. Nota: l'ADC assegnerà automaticamente un nome alla prima interfaccia Lato verde, alla seconda interfaccia Lato rosso e alla terza interfaccia Lato 3, ecc. Sentitevi liberi di cambiare queste convenzioni di denominazione a vostra scelta.
Console web	Fare doppio clic sulla colonna e selezionare la casella per assegnare l'interfaccia come indirizzo di gestione per la Console Web dell'interfaccia grafica. Prestare molta attenzione quando si cambia l'interfaccia su cui la Console Web è in ascolto. Per raggiungere la Console Web dopo la modifica, è necessario aver impostato il routing corretto o trovarsi nella stessa sottorete della nuova interfaccia. L'unico modo per tornare indietro è accedere alla riga di comando e lanciare il comando set greenside. In questo modo si cancellano tutte le interfacce tranne eth0.

Interfacce

La sezione Interfacce del pannello Rete consente di configurare alcuni elementi relativi all'interfaccia di rete. È anche possibile rimuovere un'interfaccia di rete dall'elenco facendo clic sul pulsante Rimuovi. Quando si utilizza un'appliance virtuale, le interfacce visualizzate sono limitate dal framework di virtualizzazione sottostante.



ETH Type	Status	Speed	Duplex	Bonding
eth0	up	auto	auto	none

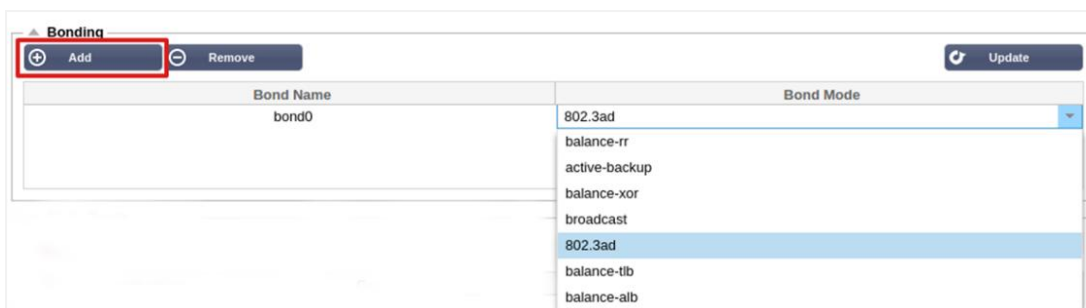
Colonna	Descrizione
Tipo ETH	Questo valore indica il riferimento del sistema operativo interno all'interfaccia di rete. Questo campo non può essere personalizzato. I valori iniziano con ETH0 e proseguono in sequenza a seconda del numero di interfacce di rete.
Stato	Questa indicazione grafica mostra lo stato attuale dell'interfaccia di rete. Lo stato verde indica che l'interfaccia è connessa e attiva. Gli altri indicatori di stato sono riportati di seguito. <div style="display: flex; flex-direction: column; align-items: flex-start; margin-top: 10px;"> <div style="display: flex; align-items: center; margin-bottom: 5px;">  <div style="margin-left: 10px;">Adattatore UP</div> </div> <div style="display: flex; align-items: center; margin-bottom: 5px;">  <div style="margin-left: 10px;">Adattatore giù</div> </div> <div style="display: flex; align-items: center; margin-bottom: 5px;">  <div style="margin-left: 10px;">Adattatore scollegato</div> </div> <div style="display: flex; align-items: center;">  <div style="margin-left: 10px;">Adattatore mancante</div> </div> </div>
Velocità	Per impostazione predefinita, questo valore è impostato per l'auto-negoziamento della velocità. Tuttavia, è possibile modificare la velocità di rete dell'interfaccia con qualsiasi valore disponibile nel menu a discesa (10/100/1000/AUTO).
Duplex	Il valore di questo campo è personalizzabile e si può scegliere tra Auto (default), Full-Duplex e Half-Duplex.
Legame	È possibile scegliere uno dei tipi di legame definiti. Per maggiori dettagli, consultare la sezione Legami.

Legame

Per indicare il bonding delle interfacce di rete si usano molti nomi: Port Trunking, Channel Bonding, Link Aggregation, NIC teaming e altri. Il bonding combina o aggrega più connessioni di rete in un'unica interfaccia channel bonded. Il bonding consente a due o più interfacce di rete di agire come una sola, di aumentare il throughput e di fornire ridondanza o failover.

Il kernel dell'ADC dispone di un driver di bonding integrato per aggregare più interfacce di rete fisiche in una singola interfaccia logica (ad esempio, aggregando eth0 e eth1 in bond0). Per ogni interfaccia bonded, è possibile definire la modalità e le opzioni di monitoraggio del collegamento. Esistono sette diverse opzioni di modalità, ognuna delle quali fornisce caratteristiche specifiche di bilanciamento del carico e tolleranza ai guasti. Queste sono mostrate nell'immagine seguente.

Nota: il bonding può essere configurato solo per le apparecchiature ADC basate su hardware.

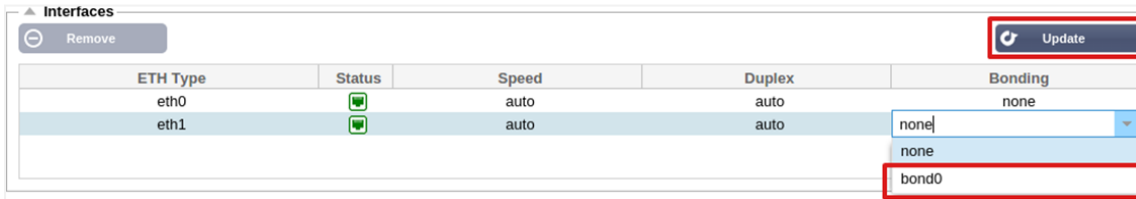


Creazione di un profilo di legame

- Fare clic sul pulsante Aggiungi per aggiungere una nuova obbligazione
- Fornire un nome per la configurazione di bonding
- Scegliere la modalità di bonding che si desidera utilizzare

Quindi, nella sezione Interfacce, selezionare la modalità di bonding che si desidera utilizzare dal campo a discesa Bond per l'interfaccia di rete.

Nell'esempio seguente, eth0, eth1 e eth2 fanno ora parte del bond0. Mentre Eth0 rimane indipendente come interfaccia di gestione.

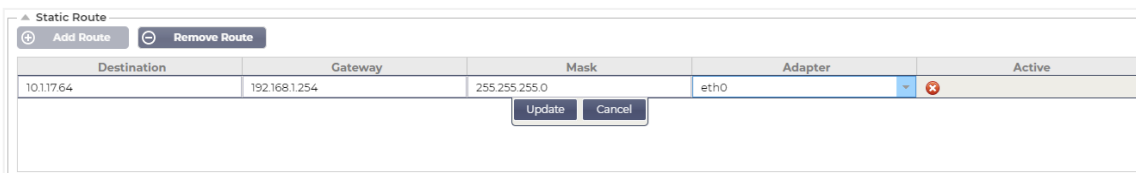


Modalità di legame

Modalità di legame	Descrizione
equilibrio-rr:	I pacchetti vengono trasmessi/ricevuti in sequenza attraverso ogni interfaccia, uno alla volta.
backup attivo:	In questa modalità, un'interfaccia sarà attiva e la seconda sarà in standby. L'interfaccia secondaria diventa attiva solo se la connessione attiva della prima interfaccia si interrompe.
equilibrio-xor:	Trasmette in base all'indirizzo MAC di origine XOR con l'indirizzo MAC di destinazione. Questa opzione seleziona lo stesso slave per ogni indirizzo MAC di destinazione.
trasmissione:	Questa modalità trasmette 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 dell'aggregatore attivo secondo le specifiche 802.3ad.
equilibrio-tlb:	La modalità di bonding con 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 si guasta, un altro slave assume l'indirizzo MAC dello slave ricevente guasto.
equilibrio-alb:	La modalità bonding Adaptive load balancing: comprende anche balance-tlb più receive load balancing (rlb) per il traffico IPV4 e non richiede alcun supporto speciale da parte dello switch. Il bilanciamento del carico in ricezione si ottiene tramite la negoziazione ARP. Il driver di bonding intercetta le risposte ARP inviate dal sistema locale in uscita e sovrascrive l'indirizzo hardware di origine con l'indirizzo hardware univoco di uno degli slave nel bond, in modo che i diversi peer utilizzino indirizzi hardware diversi per il server.

Percorso statico

In alcuni casi è necessario creare rotte statiche per specifiche sottoreti della rete. L'ADC offre la possibilità di farlo utilizzando il modulo Rotte statiche.



Aggiunta di una rotta statica

- Fare clic sul pulsante Aggiungi percorso
- Compilare il campo utilizzando come guida i dati riportati nella tabella sottostante.
- Al termine, fare clic sul pulsante Aggiorna.

Campo	Descrizione
Destinazione	Inserire l'indirizzo di rete di destinazione in notazione decimale punteggiata. Esempio 123.123.123.5
Porta d'ingresso	Inserire l'indirizzo IPv4 del gateway in notazione decimale punteggiata. Esempio 10.4.8.1
Maschera	Inserire la maschera di sottorete di destinazione in notazione decimale punteggiata. Esempio 255.255.255.0
Adattatore	Inserire l'adattatore su cui è possibile raggiungere il gateway. Esempio eth1.
Attivo	Una casella di spunta verde indica che il gateway è raggiungibile. Una croce rossa indica che il gateway non è raggiungibile su quell'interfaccia. Assicurarsi di aver impostato un'interfaccia e un indirizzo IP sulla stessa rete del gateway.

Dettagli della rotta statica

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

▲ Static Route Details

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

Kernel IPv6 routing table

Impostazioni di rete avanzate

▲ Advanced Network Setting

Server Nagle:

Client Nagle:

[Update](#)

Che cos'è Nagle?

L'algoritmo di Nagle, noto anche come algoritmo TCP No Delay, è una tecnica utilizzata nelle comunicazioni di rete per ridurre il numero di pacchetti ritrasmessi a causa di dati fuori ordine. Funziona ritardando l'invio di piccoli pacchetti se non è stato ricevuto alcun riscontro per i pacchetti precedenti. Questo aiuta a garantire che i dati arrivino nell'ordine corretto e riduce il carico sulla rete.

Vedi [l'ARTICOLO DI WIKIPEDIA SU NAGLE](#)

Server Nagle

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

Cliente Nagle

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

SNAT

▲ SNAT

[Add SNAT](#) [Remove SNAT](#)

Interface	Src IP	Src Port	Dest IP	Dest Port	Protocol	SNAT to IP	SNAT to Port	Notes

SNAT è l'acronimo di Source Network Address Translation (traduzione dell'indirizzo di rete di origine) e i diversi fornitori presentano lievi variazioni nell'implementazione di SNAT. Una semplice spiegazione dello SNAT di EdgeADC è la seguente.

In circostanze normali, le richieste in entrata verrebbero dirette al VIP che vedrebbe l'IP di origine della richiesta. Quindi, ad 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 della richiesta sarà nascosto al VIP, che vedrà invece l'indirizzo IP fornito dalla regola SNAT. Pertanto, SNAT può essere utilizzato nelle modalità di bilanciamento del carico di Layer 4 e Layer 7.

Campo	Descrizione
Fonte IP	L'indirizzo IP di origine è facoltativo 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. Pertanto, una maschera di /24 equivale 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. Pertanto, una maschera di /24 equivale a 255.255.255.0.
Fonte Porta	La porta di origine è facoltativa, può essere un numero singolo, nel qual caso specifica solo quella porta, oppure può includere i due punti, per specificare un intervallo di porte. Esempi: 80 o 5900:5905.
Porta di destinazione	La porta di destinazione è facoltativa, può essere un numero singolo, nel qual caso specifica solo quella porta, oppure può includere i due punti, per specificare un intervallo di porte. Esempi: 80 o 5900:5905.
Protocollo	È possibile scegliere se utilizzare SNAT su un singolo protocollo o su tutti i protocolli. Sugeriamo di essere specifici per essere più precisi.
Da SNAT a IP	SNAT to IP è un indirizzo IP obbligatorio o un intervallo di indirizzi IP. Esempi: 10.0.0.1 o 10.0.0.1-10.0.0.3.
Da SNAT a Porta	La porta SNAT to è facoltativa; può essere un numero singolo, nel qual caso specifica solo quella porta, oppure può includere un trattino, che specifica un intervallo di porte. Esempi: 80 o 5900-5905.
Note	Utilizzare questa opzione per assegnare un nome amichevole che ricordi il motivo dell'esistenza delle regole. È utile anche per il debug nel Syslog.

Potenza

Questa funzione del sistema ADC consente inoltre di eseguire diverse operazioni relative all'alimentazione dell'ADC.


Riavvio

▲ **Restart**

Click the Restart button to quickly stop and start essential jetNEXUS ALB services.

Warning - This will cause a brief break in current connections.

Software Version : 4.2.6 (Build 1831) 3j1329

 Restart


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 dal numero di servizi configurati. Verrà visualizzato un pop-up che richiede la conferma dell'azione di riavvio.

Riavvio

▲ **Reboot**

Click the Reboot button to re-initialise all jetNEXUS ALB services.

Warning - This will suspend your Connections and Services for about 2 minutes.

 Reboot

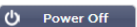
Facendo clic sul pulsante Riavvia, l'ADC viene spento e riportato automaticamente allo stato attivo. Viene visualizzato un pop-up che richiede la conferma dell'azione di riavvio.

Spegnimento

▲ **Power Off**

Click the Power off button to completely halt jetNEXUS ALB.

Warning - This will suspend your Connections and Services and require a hardware power on.

 Power Off

Facendo clic sul pulsante Spegnimento si spegne l'ADC. Se si tratta di un dispositivo hardware, è necessario accedere fisicamente al dispositivo per riaccenderlo. Verrà visualizzato un pop-up che richiede la conferma dell'azione di spegnimento.

Sicurezza

Questa sezione consente di modificare la password della console Web e di attivare o disattivare l'accesso Secure Shell. Consente inoltre di abilitare la funzionalità REST API.

SSH

▲ SSH
Secure Shell Remote Conn:

Opzione	Descrizione
Connessione remota Secure Shell	Spuntare la casella se si desidera accedere all'ADC utilizzando SSH. "Putty è un'applicazione eccellente per questo scopo.

Servizio di autenticazione

▲ Authentication Service


Authentication Mode: Remote Then Local ▼

Authentication Source: ▼

ALB GUI Admin Groups:

ALB GUI Read/Write Groups:

ALB GUI Read-Only Groups:

 Update

Nella maggior parte delle organizzazioni, l'accesso all'interfaccia di gestione dell'ADC deve avvenire tramite i servizi di autenticazione dell'azienda.

Per questi scenari, abbiamo messo a disposizione la funzione Authentication Service descritta qui. Questa funzione funziona con i servizi di directory locali e con servizi esterni come SAML.

Opzione	Descrizione
Modalità di autenticazione	Solo locale: questa è la modalità predefinita e utilizza il database locale dell'ADC, ad esempio per l'utente admin. Remoto e poi Locale: L'ADC tenterà di convalidare l'utente rispetto al server di autenticazione remoto specificato nel campo Origine di autenticazione. In caso di esito negativo, utilizzerà il database locale come fonte di convalida.
Fonte di autenticazione	Questo menu a discesa consente di selezionare uno dei server di autenticazione definiti in Libreria > Autenticazione.
Gruppi di amministrazione della GUI ALB	Specificare i gruppi di amministratori consentiti.
Gruppi di lettura/scrittura della GUI ALB	Specificare i gruppi di lettura/scrittura consentiti
Gruppi di sola lettura dell'interfaccia grafica ALB	Specificare i gruppi di sola lettura consentiti.

Console web

Certificato SSL Scegliere un certificato dall'elenco a discesa. Il certificato scelto verrà utilizzato per proteggere la connessione all'interfaccia utente web dell'ADC. È possibile 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 si desidera utilizzare una porta diversa per motivi di sicurezza, è possibile modificarla qui.

API REST

L'API REST, nota anche come API RESTful, è un'interfaccia di programmazione di applicazioni conforme allo stile architettonico REST che consente 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
Abilitare REST	Selezionare questa casella per abilitare l'accesso tramite l'API REST. Si noti che è necessario configurare anche l'adattatore su cui è abilitato REST. Vedere la nota sul link Cog qui sotto.
Certificato SSL	Scegliere 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 buona norma utilizzare una porta diversa da 443.
Indirizzo IP	Questo visualizzerà l'indirizzo IP a cui è legato il servizio REST. È possibile fare clic sul collegamento Cog per accedere alla pagina Rete e modificare l'adattatore su cui è abilitato il servizio REST.
Collegamento a pignone	Facendo clic su questo link si accede alla pagina Rete, dove è possibile configurare un adattatore per REST.

Documentazione per l'API REST

La documentazione su come utilizzare l'API REST è disponibile: [jetAPI | 4.2.3](#) | [jetNEXUS](#) | [SwaggerHub](#)

Nota: se si riscontrano errori nella pagina Swagger, ciò è dovuto a un problema di supporto delle stringhe di query.

Scorrere oltre gli errori per accedere all'API REST di jetNEXUS

Esempi

GUID utilizzando 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
 - Il GUID è valido per 24 ore

Dettagli sulla licenza

- Comando

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

SNMP

La sezione SNMP consente di configurare la MIB SNMP che risiede nell'ADC. La MIB può essere interrogata da software di terze parti in grado di comunicare con dispositivi dotati di SNMP.

Impostazioni SNMP

Opzione	Descrizione
SNMP v1 / V2C	Selezionare la casella di controllo per abilitare la MIB V1/V2C. SNMP v1 è conforme a RFC-1157. SNMP V2c è conforme a RFC-1901-1908.
SNMP v3	Spuntare la casella di controllo per abilitare il MIB V3. RFC-3411-3418. Il nome utente per la V3 è admin. Esempio: - snmpwalk -v3 -u admin -A jetnexus -l authNoPriv 192.168.1.11 1.3.6.1.4.1.38370
Stringa comunitaria	È la stringa di sola lettura impostata sull'agente e utilizzata dal manager per recuperare le informazioni SNMP. La stringa di comunità predefinita è jetnexus
Frase di passaggio	È la password necessaria quando è abilitato SNMP v3 e deve essere composta da 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 utilizzano identificatori gerarchici di oggetti (OID). Ogni OID può essere letto tramite un'applicazione di gestione SNMP.

Scarica la MIB

Il MIB può essere scaricato [qui](#):

OID ADC

OID DI RADICE

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

I nostri OID

```
.38370 jetnexusMIB
.1 jetnexusData (1.3.6.1.4.1.38370.1)
.1 jetnexusGlobal (1.3.6.1.4.1.38370.1.1)
.2 jetnexusVirtualServices (1.3.6.1.4.1.38370.1.2)
.3 jetnexusServers (1.3.6.1.4.1.38370.1.3)
.1 jetnexusGlobal (1.3.6.1.4.1.38370.1.1)
.1 jetnexusOverallInputBytes (1.3.6.1.4.1.38370.1.1.1.0)
.2 jetnexusOverallOutputBytes (1.3.6.1.4.1.38370.1.1.2.0)
.3 jetnexusCompressedInputBytes (1.3.6.1.4.1.38370.1.1.3.0)
.4 jetnexusCompressedOutputBytes (1.3.6.1.4.1.38370.1.1.4.0)
.5 jetnexusVersionInfo (1.3.6.1.4.1.38370.1.1.5.0)
```

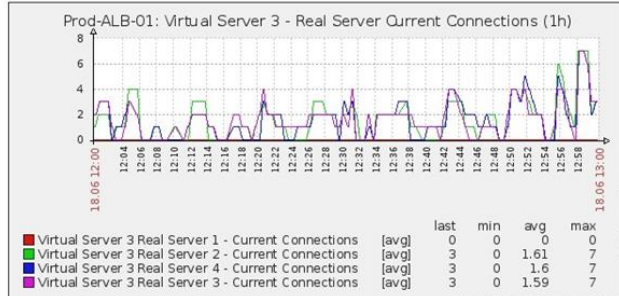
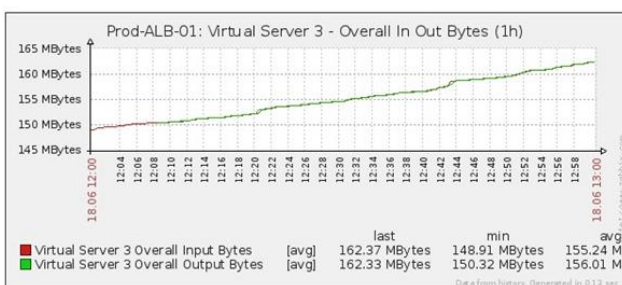
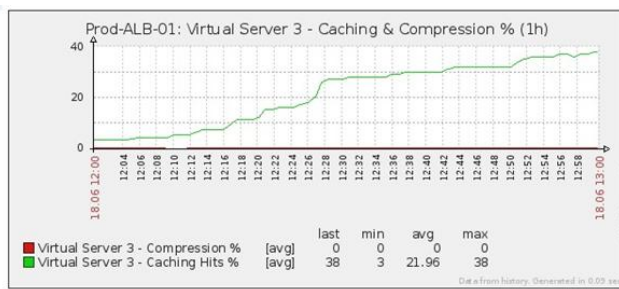
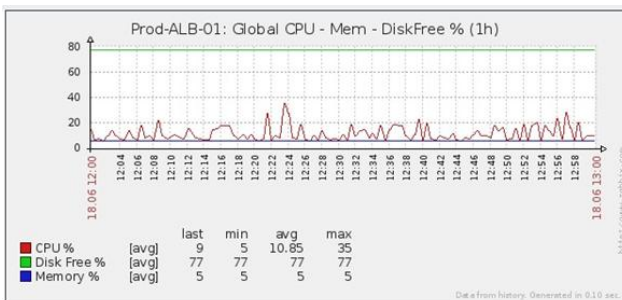
- .6 jetnexusTotalClientConnections (1.3.6.1.4.1.38370.1.1.6.0)
- .7 jetnexusCpuPercent (1.3.6.1.4.1.38370.1.1.7.0)
- .8 jetnexusDiskFreePercent (1.3.6.1.4.1.38370.1.1.8.0)
- .9 jetnexusMemoryPercent (1.3.6.1.4.1.38370.1.1.9.0)
- .10 jetnexusCurrentConnections (1.3.6.1.4.1.38370.1.1.10.0)

- .2 jetnexusVirtualServices (1.3.6.1.4.1.38370.1.2)
 - .1 jnvirtualserviceEntry (1.3.6.1.4.1.38370.1.2.1)
 - .1 jnvirtualserviceIndexvirtualservice (1.3.6.1.4.1.38370.1.2.1.1)
 - .2 jnvirtualserviceVSAddrPort (1.3.6.1.4.1.38370.1.2.1.2)
 - .3 jnvirtualserviceOverallInputBytes (1.3.6.1.4.1.38370.1.2.1.3)
 - .4 jnvirtualserviceOverallOutputBytes (1.3.6.1.4.1.38370.1.2.1.4)
 - .5 jnvirtualserviceCacheBytes (1.3.6.1.4.1.38370.1.2.1.5)
 - .6 jnvirtualserviceCompressionPercent (1.3.6.1.4.1.38370.1.2.1.6)
 - .7 jnvirtualservicePresentClientConnections (1.3.6.1.4.1.38370.1.2.1.7)
 - .8 jnvirtualserviceHitCount (1.3.6.1.4.1.38370.1.2.1.8)
 - .9 jnvirtualserviceCacheHits (1.3.6.1.4.1.38370.1.2.1.9)
 - .10 jnvirtualserviceCacheHitsPercent (1.3.6.1.4.1.38370.1.2.1.10)
 - .11 jnvirtualserviceVSStatus (1.3.6.1.4.1.38370.1.2.1.11)

- .3 jetnexusRealServers (1.3.6.1.4.1.38370.1.3)
 - .1 jnrealserverEntry (1.3.6.1.4.1.38370.1.3.1)
 - .1 jnrealserverIndexVirtualService (1.3.6.1.4.1.38370.1.3.1.1)
 - .2 jnrealserverIndexRealServer (1.3.6.1.4.1.38370.1.3.1.2)
 - .3 jnrealserverChAddrPort (1.3.6.1.4.1.38370.1.3.1.3)
 - .4 jnrealserverCSAddrPort (1.3.6.1.4.1.38370.1.3.1.4)
 - .5 jnrealserverOverallInputBytes (1.3.6.1.4.1.38370.1.3.1.5)
 - .6 jnrealserverOverallOutputBytes (1.3.6.1.4.1.38370.1.3.1.6)
 - .7 jnrealserverCompressionPercent (1.3.6.1.4.1.38370.1.3.1.7)
 - .8 jnrealserverPresentClientConnections (1.3.6.1.4.1.38370.1.3.1.8)
 - .9 jnrealserverPoolUsage (1.3.6.1.4.1.38370.1.3.1.9)
 - .10 jnrealserverHitCount (1.3.6.1.4.1.38370.1.3.1.10)
 - .11 jnrealserverRSStatus (1.3.6.1.4.1.38370.1.3.1.11)

Grafici storici

L'uso migliore della MIB SNMP personalizzata dell'ADC è la possibilità di scaricare i grafici storici su una console di gestione a scelta. Di seguito sono riportati alcuni esempi di Zabbix che eseguono il polling di un ADC per i vari valori OID sopra elencati.



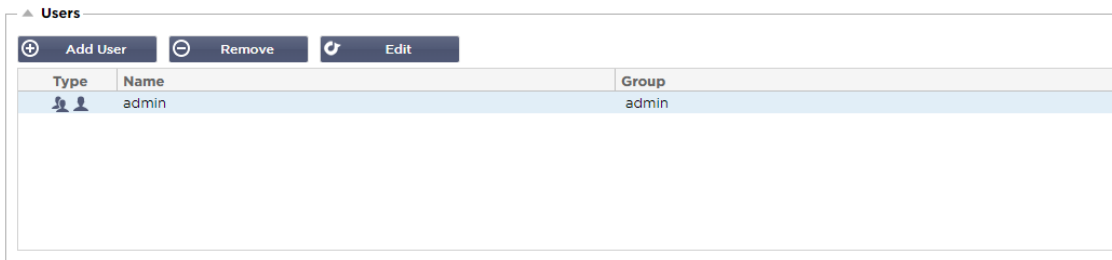
Utenti e registri di audit

L'ADC offre la possibilità di avere un insieme di utenti interni per configurare e definire le attività dell'ADC. Gli utenti definiti all'interno dell'ADC possono eseguire una serie di operazioni a seconda del ruolo loro assegnato.

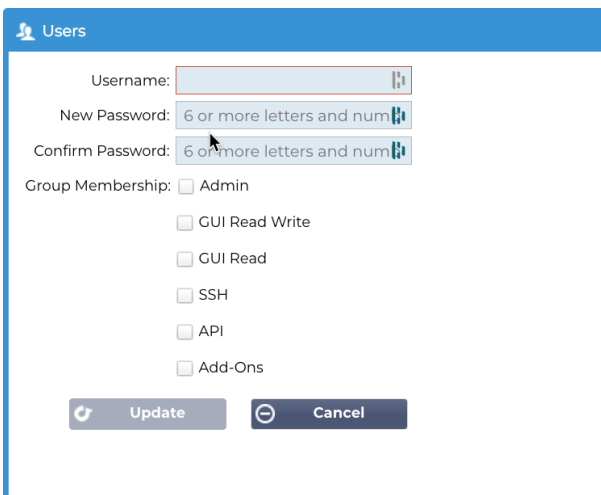
Esiste un utente predefinito, chiamato **admin**, che viene utilizzato alla prima configurazione dell'ADC. La password predefinita di admin è **jetnexus**.

Utenti

La sezione Utenti consente di creare, modificare e rimuovere gli utenti dall'ADC.



Aggiungi utente



The screenshot shows a dialog box titled "Users" with a blue header. It contains the following fields and options:




- Username:
- New Password: (6 or more letters and num)
- Confirm Password: (6 or more letters and num)
- Group Membership: Admin
- GUI Read Write
- GUI Read
- SSH
- API
- Add-Ons

At the bottom, there are two buttons: "Update" (with a refresh icon) and "Cancel" (with a minus icon).

Fare clic sul pulsante Aggiungi utente mostrato nell'immagine precedente per visualizzare la finestra di dialogo Aggiungi utente.

Parametro	Descrizione/Utilizzo
Nome utente	Inserire un nome utente a scelta. Il nome utente deve essere conforme a quanto segue: <ul style="list-style-type: none"> • Numero minimo di caratteri 1 • Numero massimo di caratteri 32 • Le lettere possono essere maiuscole e minuscole. • È possibile utilizzare i numeri. • Non sono ammessi simboli
Password	Immettere una password forte , conforme ai requisiti indicati di seguito. <ul style="list-style-type: none"> • Numero minimo di caratteri 6 • Numero massimo di caratteri 32 • Deve utilizzare almeno una combinazione di lettere e numeri. • Le lettere possono essere maiuscole o minuscole. • I simboli sono consentiti, tranne quelli dell'esempio seguente £, %, &, <, >
Conferma la password	Confermare nuovamente la password per verificare che sia corretta
Membri del gruppo	Selezionare il gruppo a cui si desidera che l'utente appartenga. <ul style="list-style-type: none"> • Admin - Questo gruppo può fare tutto. • GUI Read Write - Gli utenti di questo gruppo possono accedere alla GUI e apportare modifiche tramite la GUI. • GUI Read - Gli utenti di questo gruppo possono accedere alla GUI solo per visualizzare le informazioni. Non è possibile apportare modifiche. • SSH - Gli utenti di questo gruppo possono accedere all'ADC tramite Secure Shell. Questa scelta consente di accedere alla riga di comando, che dispone di una serie minima di comandi. • API - Gli utenti di questo gruppo avranno accesso all'interfaccia programmabile SOAP e REST. REST sarà disponibile a partire dalla versione software 4.2.1. • Add-On - L'autorizzazione è concessa per accedere alle configurazioni Add-On.

Tipo di utente

	<p>Utente locale</p> <p>L'ADC nel ruolo Stand-Alone o Manual H/A creerà solo utenti locali. Per impostazione predefinita, un utente locale chiamato "admin" è membro del gruppo admin. Per compatibilità, questo utente non può mai essere cancellato. È possibile modificare la password di questo utente o , ma non è possibile eliminare l'ultimo amministratore locale.</p>
	<p>Utente del cluster</p> <p>Il ruolo ADC in cluster creerà solo utenti del cluster. Gli utenti del cluster sono sincronizzati tra tutti gli ADC del cluster. Qualsiasi modifica apportata a un utente del cluster verrà applicata a tutti i membri del cluster. Se si è connessi come utente del cluster, non sarà possibile cambiare ruolo da Cluster a Manuale o Stand-Alone.</p>
	<p>Cluster e utente locale</p> <p>Tutti gli utenti creati nel ruolo Stand-Alone o Manuale saranno copiati nel Cluster. Se l'ADC lascia successivamente il cluster, rimarranno solo gli Utenti locali. L'ultima password configurata per l'utente sarà valida.</p>

Rimozione di un utente

- Evidenziare un utente esistente.

- Fare clic su Rimuovi.
- Non sarà possibile eliminare l'utente che ha effettuato l'accesso.
- Non sarà possibile rimuovere l'ultimo utente locale del gruppo di amministrazione.
- Non sarà possibile rimuovere l'ultimo utente del cluster rimasto nel gruppo di amministratori.
- Non sarà possibile eliminare l'utente amministratore per compatibilità con il passato.
- Se si rimuove l'ADC dal cluster, tutti gli utenti, tranne quelli locali, verranno eliminati.

Modifica di un utente

- Evidenziare un utente esistente.
- Fare clic su Modifica
- È possibile modificare l'appartenenza al gruppo dell'utente selezionando le caselle appropriate e aggiornando.
- È inoltre possibile modificare la password di un utente, a condizione che si disponga dei diritti di amministratore.

Registro di controllo

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

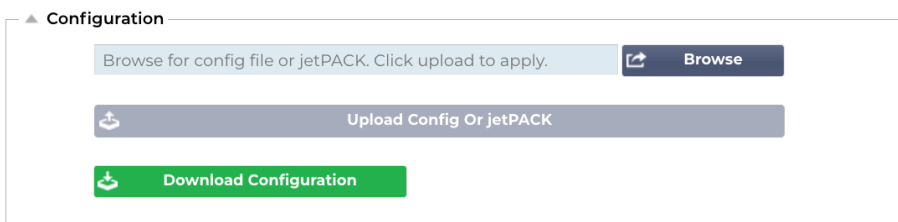
▲ Audit Log

Date/Time	Username	Section	Action
09:49:01 Fri 15 Dec 2023	admin	warning	Passwords must have 6 or more characters
09:49:01 Fri 15 Dec 2023	admin	import certificate [Jet2]	
09:48:15 Fri 15 Dec 2023	admin	error	Failed to create local certificate
09:48:14 Fri 15 Dec 2023	admin	Cert	Create
15:17:44 Thu 14 Dec 2023	admin	IP Services	Deleted: virtual service: :
15:17:44 Thu 14 Dec 2023	admin	IP Services	Deleted: virtual service: (Web Sites 443)
15:17:40 Thu 14 Dec 2023	admin	IP Services	Deleted: virtual service: 10.0.0.130:80 (Web Sites)

View Download

Avanzato

Configurazione



È sempre consigliabile scaricare e salvare la configurazione dell'ADC una volta che è stato completamente impostato e funziona come richiesto. È possibile utilizzare il modulo Configurazione per scaricare e caricare una configurazione.

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

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

ATTENZIONE:

La modifica del file di configurazione dell'EdgeADC è destinata esclusivamente a esperti qualificati. Se decidete di modificare voi stessi il file di configurazione e si verifica un problema tecnico, l'assistenza tecnica Edgenexus non sarà più in grado di supportare il prodotto.

Scaricare una configurazione

- Per scaricare la configurazione corrente dell'ADC, premere il pulsante Scarica configurazione.
- Verrà visualizzato un pop-up che chiede di aprire o salvare il file .conf.
- Salvare in una posizione comoda.
- È possibile aprirlo con qualsiasi editor di testo, come Notepad++.

Caricamento di una configurazione

- È possibile caricare un file di configurazione salvato cercando il file .conf salvato.
- Fare clic sul pulsante "Carica configurazione o Jetpack".
- L'ADC caricherà e applicherà la configurazione, quindi aggiornerà il browser. Se il browser non si aggiorna automaticamente, fare clic su aggiorna sul browser.
- Al termine, si verrà reindirizzati alla pagina Dashboard.

Critica: è fondamentale non tentare di copiare la configurazione da un ADC a un altro senza aver prima consultato l'assistenza Edgenexus. Ciò potrebbe rendere il vostro ADC irrecuperabile.

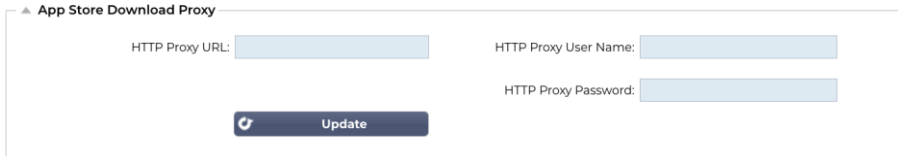
Caricare un JetPACK

- Un JetPACK è un insieme di aggiornamenti della configurazione esistente.
- Un JetPACK può essere di dimensioni ridotte, come la modifica del valore di timeout TCP, fino a una configurazione completa specifica per un'applicazione come Microsoft Exchange o Microsoft Lync.
 - È possibile ottenere un JetPACK dal portale di assistenza indicato alla fine di questa guida.
- Cercate il file jetPACK.txt.
- Fare clic su Carica.
- Il browser si aggiorna automaticamente dopo il caricamento.
- Al termine, si verrà reindirizzati alla pagina Dashboard.
- L'importazione può richiedere più tempo per le distribuzioni più complesse, come Microsoft Lync, ecc.

Impostazioni globali

La sezione Impostazioni globali consente di modificare vari elementi, tra cui la libreria crittografica SSL.

App Store Download Proxy




▲ App Store Download Proxy

HTTP Proxy URL:

HTTP Proxy User Name:

HTTP Proxy Password:

 Update

Le reti protette generalmente non consentono l'accesso a Internet, a meno che i dati non vengano inviati tramite i server proxy dell'organizzazione. L'EdgeADC è un dispositivo perimetrale e deve poter accedere ai server Edgenexus per verificare la validità del supporto e per accedere all'App Store per scaricare aggiornamenti e applicazioni.

URL proxy HTTP

Questo campo serve a specificare il nome host o l'indirizzo IP del server proxy.


Nome utente del proxy HTTP

Inserire il nome utente utilizzato specificamente per autorizzare i dispositivi e gli utenti che utilizzano il server proxy.

Password del proxy HTTP

Il nome utente specificato in Nome utente proxy HTTP sarà un nome protetto. È necessario inserire la password associata in questo campo.

Timer cache host



▲ HostCache Timer

HostCache Timer (s):

 Update

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 dell'indirizzo IP. La cache viene cancellata in caso di guasto del Real Server. Impostando questo valore a zero, la cache non viene cancellata. Non esiste un valore massimo per questa impostazione.

Drenaggio

▲ Drain

Default Drain Behaviour: Migrate Visitors

Update

Quando un Real Server viene messo in modalità Drain, è sempre meglio poter controllare il comportamento del traffico che gli viene inviato. Il menu Comportamento di scarico consente di selezionare il comportamento del traffico per ogni servizio virtuale. Le opzioni sono:

Opzione	Descrizione
Persistenza guidata	Questa è la selezione predefinita. Ogni volta che l'utente visita la sessione di persistenza, questa viene estesa. Con un utilizzo di 24 ore, è possibile che lo scarico non avvenga mai. Tuttavia, se il numero di connessioni al server reale raggiunge lo 0, il drenaggio termina, le sessioni di persistenza vengono eliminate e tutti i visitatori vengono ribilanciati alla prossima connessione.
Migrare i visitatori	Sessione persistente ignorata alla nuova connessione (comportamento precedente al 2022) Le nuove connessioni TCP (che facciano parte o meno di una sessione esistente) vengono sempre effettuate a un server reale online. Se la sessione di persistenza era a un server reale in esaurimento, viene sovrascritta. Il servizio virtuale ignorerà di fatto la persistenza delle nuove connessioni, che saranno bilanciate su un nuovo server.
Sessioni di pensionamento	Le sessioni persistenti non vengono estese. Le connessioni degli utenti in arrivo vengono assegnate al server desiderato, ma la loro sessione di persistenza non viene estesa. Pertanto, una volta superata la durata della sessione di persistenza, saranno trattate come una nuova connessione e spostate su un altro server.

SSL

▲ SSL

SSL Cryptographic Library: Open SSL

Update

Questa impostazione globale consente di modificare la libreria SSL in base alle esigenze. La libreria crittografica SSL predefinita utilizzata dall'ADC è OpenSSL. Se si desidera utilizzare una libreria crittografica diversa, è possibile modificarla qui.

Autenticazione

▲ **Authentication**

Authentication Server Timeout (s):

Update

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

Impostazione Failover

▲ **Failover Setting**

VIP Failover Behaviour :

Update

Quando viene creato un insieme di ADC in cluster, esistono ora due metodi per specificare il modo in cui un Virtual Service subirà il fail over.

Opzione	Descrizione
Qualsiasi servizio	Quando si sceglie questa opzione, il guasto di un qualsiasi servizio all'interno del VIP causerà il fallimento dell'intero VIP con i suoi servizi virtuali sul partner del cluster. Ad esempio, si può avere un VIP 10.0.100.101, con servizi virtuali che utilizzano ciascuno la porta 443, 8080, 4399, 2020, ecc. In caso di guasto di uno di questi sottoservizi, l'intero VIP subirà un fail over.
Tutti i servizi	Se si sceglie questa opzione, in caso di guasto di uno o più sottoservizi, il VIP rimarrà sul membro del cluster corrente. Il VIP verrà trasferito al partner del cluster solo se tutti i servizi si guastano. Questo è utile quando si desidera disabilitare un particolare servizio, ma non si vuole che il VIP venga sostituito.

Protocollo

La sezione Protocollo è utilizzata per impostare le numerose impostazioni avanzate del protocollo HTTP.

Server troppo occupato

Supponiamo che abbiate limitato il numero massimo di connessioni ai vostri Real Server; potete scegliere di presentare una pagina web amichevole una volta raggiunto questo limite.

- Create una semplice pagina web con il vostro messaggio. È possibile includere collegamenti esterni a oggetti su altri server e siti Web. In alternativa, se si desidera avere immagini nella pagina web, utilizzare immagini inline codificate in base64.
- Cercare il file HTM(L) della pagina web appena creata.
- Fare clic su Carica
- Se si desidera visualizzare un'anteprima della pagina, è possibile farlo con il link [Clicca qui](#).

Inoltrata per

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

Uscita inoltrata

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

Intestazione Forwarded-For

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

Registrazione avanzata per IIS - Registrazione personalizzata

È possibile ottenere le informazioni X-Forwarded-For installando l'applicazione IIS Advanced logging 64-bit. Una volta scaricata, creare un campo di registrazione personalizzato chiamato X-Forwarded-For con le impostazioni riportate di seguito.

Selezionare Default dall'elenco Tipo di origine dall'elenco Categoria, selezionare Intestazione richiesta nella casella Nome origine e digitare X-Forwarded-For.

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

Modifiche al file HTTPd.conf di Apache

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

Le modifiche sono riportate di seguito:

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 "^\.\.\.\." forwarded
CustomLog:	"logs/access_log" combinato env=!forwarded
CustomLog:	"logs/access_log" proxy env=forwarded

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

- La riga 1 è la stringa formattata del log combinato standard di default.
- La riga 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 riga 3 è un'impostazione per la variabile d'ambiente "forwarded" che contiene un'espressione regolare libera che corrisponde a un indirizzo IP, il che va bene in questo caso poiché ci interessa di più se un indirizzo IP esiste nell'intestazione X-Forwarded-For.
- Inoltre, la riga 3 potrebbe essere letta come: "Se esiste un valore X-Forwarded-For, usarlo".
- Le righe 4 e 5 indicano ad Apache quale modello di log utilizzare. Se esiste un valore X-Forwarded-For, utilizzare lo schema "proxy", altrimenti utilizzare lo schema "combinato" per la richiesta. Per motivi di leggibilità, le righe 4 e 5 non sfruttano la funzione di log rotate (piped) di Apache, ma si presume che quasi tutti la utilizzino.

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

Impostazioni di compressione HTTP

▲ HTTP Compression Settings

Initial Thread Memory [KB]:

Maximum Thread Memory [KB]:


Increment Memory [KB]:
(0 to double)

Minimum Compression Size [Bytes]:

Safe Mode:

Disable Compression:

Compress As You Go:

 **Update**

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

AVVERTENZA - Prestare la massima attenzione quando si regolano queste impostazioni, in quanto impostazioni inadeguate possono influire negativamente sulle 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 ottenere prestazioni più efficienti, questo valore dovrebbe essere impostato a un valore appena superiore al più grande file HTML non compresso che i server web possono inviare.
Memoria massima del thread [KB]	Questo valore è la quantità massima di memoria che l'ADC alloca per una richiesta. Per ottenere le massime prestazioni, l'ADC normalmente memorizza e comprime tutto il contenuto in memoria. Se viene elaborato un file di contenuto eccezionalmente grande che supera questa quantità, l'ADC scriverà su disco e comprimerà i dati.
Memoria di incremento [KB]	Questo valore imposta la quantità di memoria aggiunta all'allocazione iniziale della memoria del thread quando è richiesta una quantità maggiore. L'impostazione predefinita è zero. Ciò significa che ADC raddoppierà l'allocazione quando i dati superano l'allocazione corrente (ad esempio 128Kb, poi 256Kb, poi 512Kb, ecc.) fino al limite fissato da Utilizzo massimo della memoria per thread. Questo è efficiente quando la maggior parte delle pagine ha una dimensione costante, ma occasionalmente ci sono file più grandi. (ad esempio, la maggior parte delle pagine è di 128Kb o meno, ma le risposte occasionali sono di 1Mb). Nello scenario in cui ci sono file di dimensioni variabili, è più efficiente impostare un incremento lineare di una dimensione significativa (ad esempio, se le risposte hanno dimensioni comprese tra 2 e 10 Mb, sarebbe più efficiente un'impostazione iniziale di 1 Mb con incrementi di 1 Mb).
Dimensione minima di compressione [Byte]	Questo valore è la dimensione, in byte, al di sotto della quale l'ADC non tenterà di comprimere. È utile perché tutto ciò che è inferiore a 200 byte non viene compresso bene e può persino crescere di dimensioni a causa delle spese generali delle intestazioni di compressione.
Modalità provvisoria	Selezionare questa opzione per evitare che ADC applichi la compressione ai fogli di stile e a JavaScript. Il motivo è che, anche se ADC è a conoscenza di quali browser possono gestire contenuti compressi, alcuni 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, utilizzare questa opzione per

	disabilitare la compressione di questi tipi di contenuti. Tuttavia, questo ridurrà la quantità complessiva di compressione dei contenuti.
Disattivare la compressione	Selezionare questa opzione per impedire all'ADC di comprimere qualsiasi risposta.
Comprimere man mano che si procede	ON - Utilizza Compress as You Go in questa pagina. In questo modo, ogni blocco di dati ricevuto dal server viene compresso in una porzione discreta, completamente decomprimibile. OFF - Non utilizzare Compress as you Go in questa pagina. Per richiesta di pagina - Usa Comprimi come vai per richiesta di pagina.

Esclusioni della compressione globale

Tutte le pagine con l'estensione aggiunta nell'elenco di esclusione non verranno compresse.

- Digitare il nome del singolo file.
- Fare clic su Aggiorna.
- Se si desidera aggiungere un tipo di file, è sufficiente digitare "*.css" per escludere tutti i fogli di stile a cascata.
- Ogni file o tipo di file deve essere aggiunto a una nuova riga.

Cookie di persistenza


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

Campo	Descrizione
Stesso sito Attributo Cooke	Nessuno: Tutti i cookie sono accessibili agli script Lassista: Impedisce l'accesso ai cookie da un sito all'altro, ma i cookie vengono memorizzati per diventare accessibili e inviati al sito proprietario se viene visitato. Strict: impedisce l'accesso o la memorizzazione di qualsiasi cookie per un sito diverso. Off: ripristina il comportamento predefinito del browser
Sicuro	Questa casella di controllo, se selezionata, applica la persistenza al traffico protetto.
Solo HTTP	Se si seleziona questa opzione, si consente l'uso di Cookies persistenti solo per il traffico HTTP.

Reset timeout UDP

▲ UDP Timeout Reset

UDP Timeout Reset On :

 **Update**

Il reset del timeout UDP è un meccanismo utilizzato nelle comunicazioni di rete in cui il timeout relativo a una sessione UDP (User Datagram Protocol) viene riavviato. Il reset contribuisce a mantenere attiva la sessione, garantendo un flusso di dati continuo senza interruzioni.

Opzione	Descrizione
Entrambi	Azzerà il timeout UDP sia sul server che sul client.
Server	Azzerà il timeout UDP sul server.
Cliente	Azzerà il timeout UDP sul client.

Software

La sezione Software consente di aggiornare la configurazione e il firmware dell'ADC.

Dettagli sull'aggiornamento del software

Le informazioni contenute in questa sezione saranno compilate se si dispone di una connessione Internet funzionante. Se il browser non dispone di un collegamento a Internet, questa sezione sarà vuota. Una volta connessi, si riceverà il messaggio del banner sottostante.

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

La sezione Download from Cloud mostrata di seguito sarà popolata di informazioni che mostrano gli aggiornamenti disponibili nell'ambito del vostro piano di assistenza. È necessario prestare attenzione al tipo di supporto e alla data di scadenza del supporto.

Nota: per visualizzare le informazioni disponibili su Edgenexus Cloud, utilizziamo la connessione Internet del browser. Sarà possibile scaricare gli aggiornamenti software solo se l'ADC dispone di una connessione a Internet.

Per verificarlo:

- Avanzate--Risoluzione dei problemi--Ping
- Indirizzo IP - App Store.edgenexus.io
- Fare clic su Ping
- Se il risultato mostra "ping: host sconosciuto App Store.edgenexus.io".
- L'ADC NON sarà in grado di scaricare nulla dal cloud.

Scaricare da Cloud

Code Name	Release Date	Version	Build	Release Notes	Notes
ALB-X Version 4.2.6	2020-Apr-15	4.2.6	1826	Click here for release notes. This is our latest release 4.2.6. This APP will only w	
ALB-X Version 4.2.4 Safe Rollback	2022-Aug-05	4.2.4	jetNEXUS	Use this safe 1764 roll-back, not s	Use this safe 1764 roll-back, not software stored in
OWASP Core Rule Set 3.14 Update for Edgenexus Ap 2023 Feb-09	2023-Feb-09	3.14_20.01.2023	Edgenexus	The OWASP CRS is a set of web s	The OWASP CRS is a set of web application firew
ADC Version 4.2.10 Software Update	2023-Oct-27	4.2.10	1961	Release notes	EdgeADC version 4.2.10 software update Offline f

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

- Evidenziare la riga interessata e fare clic sul pulsante "Scarica il software selezionato in ALB".
- Quando si fa clic sul software selezionato, questo viene scaricato sulla ALB e può essere applicato nella sezione "Applicare il software memorizzato sulla ALB".

Nota: se l'ADC non dispone di un accesso diretto a Internet, si riceverà un errore come quello riportato di seguito:

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

Se la rete è protetta da un server proxy, consultare App Store Download Proxy

Software di caricamento

▲ Upload Software

Software Version: 4.3.0 (Build 1965) c50631

Browse for software file then click upload to apply.

Caricamento delle applicazioni

▲ Upload Software

Software Version: 4.3.0 (Build 1965) c50631

Browse for software file then click upload to apply.

Se si dispone di un file di app che termina con <appname> .<apptype> .alb, è possibile utilizzare questo metodo per caricarlo.

- Esistono cinque tipi di App
 - <appname>flightpath.alb
 - <appname>.monitor.alb
 - <appname>.jetpack.alb
 - <appname>.addons.alb
 - <appname>.featurepack.alb
- Una volta caricata, ogni applicazione si trova nella sezione Biblioteca>Apps.
- È quindi necessario distribuire singolarmente ogni applicazione di quella sezione.

Software / Aggiornamenti firmware

▲ Upload Software To ALB

Software Version: 4.2.6 (Build 1831) 3j1329

Browse for software file then click upload to apply.

- Se si desidera caricare il software senza applicarlo, utilizzare il pulsante evidenziato.
- Il file software è <nome software>.software.alb.
- Verrà quindi visualizzata nella sezione "Software memorizzato su ALB", da dove sarà possibile applicarla a proprio piacimento.

Applicare il software memorizzato su ADC

▲ Apply Software

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

Questa sezione mostra tutti i file software archiviati nell'ALB e disponibili per la distribuzione. L'elenco includerà le firme aggiornate del Web Application Firewall (WAF).

- Evidenziare la riga del software che si desidera utilizzare.
- Fare clic su "Applica il software dalla selezione".
- Se si tratta di un aggiornamento del software dell'ALB, tenere presente che verrà caricato e poi riavviato l'ALB per essere applicato.
- Se l'aggiornamento che si sta applicando è un aggiornamento della firma OWASP, verrà applicato 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 vi permette di farlo.

File di supporto

▲ **Support Files**

Time Frame: 7 days

Download Support Files

Se si verifica un problema con l'ADC e si deve aprire un ticket di assistenza, il supporto tecnico spesso richiede diversi file dall'appliance ADC. Questi file sono stati ora aggregati in un unico file .dat che può essere scaricato da questa sezione.

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

Traccia

▲ **Trace**

Nodes To Trace: Your IP

Connections:

Cache:

Data:

Authentication:

flightPATH: No flightPATH trace

Server Monitoring:

Monitoring Unreachable:

Auto-Stop Records: 1000000

Auto-Stop Duration: 00:10:00

Purpose:

Start

Download

Clear

Full results can be obtained using download.

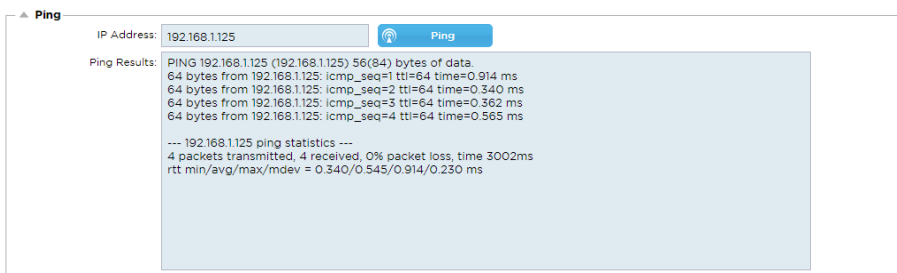
La sezione Trace consente di esaminare le informazioni che permettono il debug del problema. Le informazioni fornite dipendono dalle opzioni scelte dai menu a tendina e dalle caselle di selezione.

Opzione	Descrizione
Nodi da tracciare	Il tuo IP: Filtra l'uscita in modo da utilizzare l'indirizzo IP da cui si accede all'interfaccia grafica (nota: non scegliere questa opzione per il monitoraggio, poiché quest'ultimo utilizzerà l'indirizzo dell'interfaccia ADC). Tutti gli IP: non verrà applicato alcun filtro. Si noti che su un box occupato questa opzione influisce negativamente sulle prestazioni.
Connessioni	Questa casella di controllo, se selezionata, mostra le informazioni sulle connessioni client e server.

Cache	Questa casella di controllo, se spuntata, mostra le informazioni relative agli oggetti memorizzati nella cache.
Dati	Quando questa casella di controllo è selezionata, include i byte di dati grezzi gestiti in entrata e in uscita dall'ADC.
voloPATH	Il menu flightPATH consente di selezionare una particolare regola flightPATH da monitorare o Tutte le regole flightPATH.
Monitoraggio del server	Questa casella di controllo, se selezionata, mostra i monitor di salute del server attivi sull'ADC e i rispettivi risultati.
Monitoraggio non raggiungibile	Quando questa opzione è selezionata, il comportamento è molto simile a quello del monitoraggio del server, tranne che per il fatto che mostra solo i monitor falliti e agisce quindi come un filtro solo per questi messaggi.
Registri di arresto automatico	Il valore predefinito è di 1.000.000 di registrazioni, dopo le quali la funzione Trace si interrompe automaticamente. Questa impostazione è una precauzione di sicurezza per evitare che la funzione Trace rimanga accidentalmente attiva e influisca sulle prestazioni dell'ADC.
Durata dell'arresto automatico	Il tempo predefinito è impostato su 10 minuti, al termine dei quali la funzione Trace si interrompe automaticamente. Questa funzione è una precauzione di sicurezza per evitare che la funzione Trace rimanga accidentalmente attiva e influisca sulle prestazioni dell'ADC.
Inizio	Fare clic su questo pulsante per avviare manualmente la funzione Trace.
Fermarsi	Fare clic per interrompere manualmente la funzione Trace prima che venga raggiunta la registrazione automatica o il tempo.
Scaricare	Sebbene sia possibile visualizzare il live viewer sul lato destro, le informazioni potrebbero essere visualizzate troppo velocemente. È invece possibile scaricare il Trace.log per visualizzare tutte le informazioni raccolte durante le varie tracce del giorno. Questa funzione è un elenco filtrato di informazioni sulle tracce. Se si desidera visualizzare le informazioni di traccia dei giorni precedenti, è possibile scaricare il Syslog di quel giorno, ma si dovrà filtrare manualmente.
Libero	Cancella il registro di traccia

Ping

È possibile verificare la connettività di rete ai server e agli altri oggetti di rete dell'infrastruttura utilizzando lo strumento Ping.



Digitare l'indirizzo IP dell'host che si desidera testare, ad esempio il gateway predefinito utilizzando la notazione decimale punteggiata o un indirizzo IPv6. Potrebbe essere necessario attendere qualche secondo prima che il risultato venga visualizzato dopo aver premuto il pulsante "Ping".

Se è stato configurato un server DNS, è possibile digitare il nome di dominio completamente qualificato. È possibile configurare un server DNS nella sezione [SERVER DNS 1 E SERVER DNS 2](#). Potrebbe essere necessario attendere qualche secondo prima che il risultato venga visualizzato dopo aver premuto il pulsante "Ping".

Cattura


▲ Capture

Adapter:

Packets:

Duration[Sec]:

Address:

 Generate

Per acquisire il traffico di rete, seguire le semplici istruzioni riportate di seguito.

- Completare le opzioni del modulo
- Fare clic su Genera
- Una volta eseguita l'acquisizione, il browser chiederà dove si desidera salvare il file. Il file sarà nel formato "jetNEXUS.cap.gz".
- Creare un ticket di assistenza sul portale di assistenza, i cui dettagli sono disponibili alla fine di questo documento.
- Assicuratevi di descrivere accuratamente il problema e di allegare il file al ticket.
- È inoltre possibile visualizzare i contenuti utilizzando Wireshark

Opzione	Descrizione
Adattatore	Scegliere l'adattatore dal menu a tendina, in genere eth0 o eth1. È anche possibile catturare tutte le interfacce con "any".
Pacchetti	Questo valore rappresenta il numero massimo di pacchetti da catturare. In genere, 99999
Durata	Scegliere un tempo massimo per l'acquisizione. Un tempo tipico è di 15 secondi per i siti ad alto traffico. L'interfaccia grafica sarà inaccessibile durante il periodo di cattura.
Indirizzo	Questo valore filtrerà qualsiasi indirizzo IP inserito nella casella. Lasciare vuoto per non filtrare.

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

Nota: questo avrà un impatto sulle prestazioni dei siti live. Per aumentare le dimensioni di acquisizione disponibili, applicare l'impostazione globale jetPACK per aumentare le dimensioni di acquisizione.

Aiuto

La sezione Aiuto consente di accedere alle informazioni su Edgenexus e alle guide per l'utente e ad altre informazioni utili.

Chi siamo

Facendo clic sull'opzione "Chi siamo" si visualizzano le informazioni su Edgenexus e sulla sua sede aziendale.

Riferimento

L'opzione di riferimento apre la pagina web contenente le guide per l'utente e altri documenti utili. La pagina web può essere trovata anche utilizzando il sito <https://www.edgenexus.io/documentation>.

Se non trovate quello che cercate, contattate [.support@edgenexus.io](mailto:support@edgenexus.io)

I pacchetti JetPACK

Edgenexus jetPACK s

I jetPACK sono un metodo unico per configurare istantaneamente il vostro ADC per applicazioni specifiche. Questi modelli, facili da usare, sono preconfigurati e completamente sintonizzati con tutte le impostazioni specifiche dell'applicazione necessarie per ottenere un servizio ottimizzato dal vostro ADC. Alcuni jetPACK utilizzano flightPATH per manipolare il traffico e per far funzionare questo elemento è necessario disporre di una licenza flightPATH. Per sapere se si dispone di una licenza per flightPATH, consultare la pagina delle [LICENZE](#).

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
- È possibile caricare questo jetPACK così com'è e modificare l'indirizzo IP nella GUI oppure modificare il jetPACK con un editor di testo come Notepad++ e cercare e sostituire 1.1.1.1 con il proprio indirizzo IP virtuale.
- Inoltre, ogni jetPACK è stato creato con 2 Real Server con gli indirizzi IP 127.1.1.1 e 127.2.2.2. Anche in questo caso è possibile modificarli nella GUI dopo l'upload o prima, utilizzando Notepad++.
- Fate clic su un link jetPACK qui sotto e salvate il link come file jetPACK-VIP-Application.txt nella posizione scelta.

Microsoft Exchange

Applicazione	Link per il download	Che cosa fa?	Cosa è incluso?
Scambio 2010	jetPACK-1.1.1.1-Exchange-2010	Questo jetPACK aggiunge le impostazioni di base per il bilanciamento del 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 si dispone di una licenza per flightPATH, questo jetPACK funzionerà comunque.	Impostazioni globali: Timeout servizio 2 ore Monitor: Monitor di livello 7 per l'applicazione web di Outlook e monitor di livello 4 fuori banda per il servizio di accesso ai client. IP del servizio virtuale: 1.1.1.1 Porte di servizio virtuali: 80, 443, 135, 59534, 59535 Server reali: 127.1.1.1 127.2.2.2 flightPATH: aggiunge il reindirizzamento da HTTP a HTTPS
	jetPACK-1.1.1.2-Exchange-2010-SMTP-RP	Come sopra, ma aggiungerà un servizio SMTP sulla porta 25 in connettività reverse proxy. Il server SMTP vedrà l'indirizzo dell'interfaccia ALB-X come IP di origine.	Impostazioni globali: Timeout servizio 2 ore Monitor: Monitor di livello 7 per l'applicazione web di Outlook. Monitor di livello 4 fuori banda per il servizio di accesso al client. IP del servizio virtuale: 1.1.1.1 Porte dei servizi virtuali: 80, 443, 135, 59534, 59535, 25 (reverse proxy) Server reali: 127.1.1.1 127.2.2.2 flightPATH: aggiunge il reindirizzamento da HTTP a HTTPS
	jetPACK-1.1.1.3-Exchange-	Come sopra, ma questo jetPACK configura il servizio SMTP in modo che utilizzi la connettività Direct Server Return. Questo jetPACK è necessario se	Impostazioni globali: Timeout servizio 2 ore Monitor: Monitor di livello 7 per l'applicazione web di Outlook.

	2010-SMTP-DSR	il server SMTP deve vedere l'indirizzo IP effettivo del client.	Monitor di livello 4 fuori banda per il servizio di accesso al client. IP del servizio virtuale: 1.1.1.1 Porte del servizio virtuale: 80, 443, 135, 59534, 59535, 25 (ritorno diretto al server) Server reali: 127.1.1.1 127.2.2.2 flightPATH: aggiunge il reindirizzamento da HTTP a HTTP
Scambio 2013	jetPACK-2.2.2.1-Exchange-2013-Low-Resource	Questa configurazione aggiunge 1 VIP e due servizi per il traffico HTTP e HTTPS e richiede il minor numero di CPU. È possibile aggiungere più controlli sanitari al VIP per verificare che ogni singolo servizio sia attivo.	Impostazioni globali: Monitor: Monitor Layer 7 per OWA, EWS, OA, EAS, ECP, OAB, e ADS IP del servizio virtuale: 2.2.2.1 Porte di servizio virtuali: 80, 443 Server reali: 127.1.1.1 127.2.2.2 flightPATH: aggiunge il reindirizzamento da HTTP a HTTPS
	jetPACK-2.2.3.1-Exchange-2013-Med-Resource	Questa configurazione utilizza un indirizzo IP univoco per ogni servizio e quindi utilizza più risorse rispetto a quelle indicate sopra. È necessario configurare ogni servizio come voce DNS individuale Esempio owa.edgenexus.com, ews.edgenexus.com, ecc. Per ogni servizio verrà aggiunto un monitor che verrà applicato al servizio in questione.	Impostazioni globali: Monitoraggio: Monitoraggio Layer 7 per OWA, EWS, OA, EAS, ECP, OAB, ADS, MAPI e PowerShell IP del servizio virtuale: 2.2.3.1, 2.2.3.2, 2.2.3.3, 2.2.3.4, 2.2.3.5, 2.2.3.6, 2.2.3.7, 2.2.3.8, 2.2.3.9, 2.2.3.10 Porte di servizio virtuali: 80, 443 Server reali: 127.1.1.1 127.2.2.2 flightPATH: aggiunge il reindirizzamento da HTTP a HTTP
	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 verso il servizio virtuale corretto. Questo jetPACK richiede la massima quantità di CPU per eseguire la commutazione di contesto.	Impostazioni globali: Monitoraggio: Monitor Layer 7 per OWA, EWS, OA, EAS, ECP, OAB, ADS, MAPI e PowerShell. IP del servizio virtuale: 2.2.2.3 Porte di servizio virtuali: 80, 443, 1, 2, 3, 4, 5, 6, 7 Server reali: 127.1.1.1 127.2.2.2 flightPATH: aggiunge il reindirizzamento da HTTP a HTTPS

Microsoft Lync 2010/2013

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

Servizi web

HTTP normale	Offload SSL	Crittografia SSL	Passaggio SSL
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 (Immagini e comunicazioni digitali in medicina)

HTTP normale

[jetPACK-6.6.6.1-DICOM](#)

Oracle e-Business Suite

Offload SSL

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

VMware Horizon View

Server di connessione - Offload SSL

[jetPACK-8.8.8.1-View-SSL-Offload](#)

Server di sicurezza - Ricrittografia SSL

[jetPACK-8.8.8.2-Vista-SSL-Re-encryption](#)

Impostazioni globali

- Porta sicura GUI 443 - questo jetPACK cambierà la porta sicura della GUI da 27376 a 443. HTTP://x.x.x.x
- Timeout GUI 1 giorno - la GUI richiede l'immissione della password ogni 20 minuti. Questa impostazione aumenterà tale richiesta a 1 giorno
- ARP Refresh 10 - durante un failover tra dispositivi HA, questa impostazione aumenterà il numero di **ARP gratuiti** per assistere gli switch durante la transizione.
- Dimensione di acquisizione 16MB - la dimensione di acquisizione predefinita è di 2MB. Questo valore aumenterà le dimensioni fino a un massimo di 16MB.

Cipher s e Cipher jetPACKs

L'EdgeADC è dotato di cifrari di serie. Questi cifrari sono abbinati ai rispettivi protocolli TLS, per agevolare gli utenti.

Abbiamo fornito una serie di cifrari aggiuntivi da utilizzare in caso di necessità.

Cifrari forti

Aggiunge la possibilità di scegliere "Cifrari forti" dall'elenco delle opzioni di cifratura:

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

Anti-Bestia

Aggiunge la possibilità di scegliere "Anti-Bestia" dall'elenco delle opzioni di cifratura:

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

No SSLv3

Aggiunge la possibilità di scegliere "No SSLv3" dall'elenco delle opzioni di cifratura:

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

No SSLv3 no TLSv1 No RC4

Aggiunge la possibilità di scegliere "No-TLSv1 No-SSLv3 No-RC4" dall'elenco delle opzioni di cifratura:

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

NO_TLSv1.1

Aggiunge la possibilità di scegliere "NO_TLSv1.1" dall'elenco delle opzioni di cifratura:

```
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
```

Abilitare i cifrari TLS-1.0-1.1

A partire dalla build 4.2.10, il supporto di Cipher per i protocolli TLS1.0 e TLS 1.1 è stato deprecato. Tuttavia, alcuni clienti continuano a utilizzare questi vecchi protocolli per i loro server interni. Il Cipher di seguito aggiunge la possibilità di abilitare TLS v1.0 e TLS v1.1.

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

Esempio di cifratura jetPACK

I cifrari vengono importati nell'ADC utilizzando i jetPACK. Un jetPACK è un semplice file di testo che contiene i parametri riconosciuti dall'ADC. L'esempio seguente mostra un jetPACK che utilizza il Cifrario Enable TLS-1.0-1.1.

```
#aggiornamento
[jetnexusdaemon-cipher-TLS1-0-TLS-1-1]
Cipher="AES128-SHA:AES256-SHA:DES-CBC-SHA:DES-CBC3-SHA:EXP-DES-CBC-SHA:RC4-SHA:RC4-MD5:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:EDH-RSA-DES-CBC-SHA:EDH-RSA-DES-CBC3-SHA:EXP-EDH-RSA-DES-CBC-SHA:EXP-RC2-CBC-MD5:AES128-SHA256:AES256-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-DSS-AES128-SHA256:DHE-DSS-AES256-SHA256:DHE-DSS-AES128-GCM-SHA256:DHE-DSS-AES256-GCM-SHA384:AES:ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM"
Cifra1=""
Cipher2=""
CipherOptions="-NO_TLSv1.0 -NO_TLSv1.1 -NO_TLSv1.2 -NO_TLSv1"
Descrizione=" TLS v1.0 - v1.1 abilitato".
```

- [X-Content-Type-Options](#) - aggiungere questa intestazione se non esiste e impostarla su "nosniff" - impedisce al browser di "MIME-Sniffing" automatico.
- [X-Frame-Options](#) - aggiungete questa intestazione se non esiste e impostatela su "SAMEORIGIN" - le pagine del vostro sito web possono essere incluse nei frame, ma solo in altre pagine dello stesso sito web.
- [X-XSS-Protection](#) - aggiungere questa intestazione se non esiste e impostarla a "1; mode=block" - abilitare le protezioni cross-site scripting del browser
- [Strict-Transport-Security](#) - aggiungere l'intestazione se non esiste e impostarla a "max-age=31536000 ; includeSubdomains" - assicura che il client rispetti il fatto che tutti i collegamenti siano HTTPS:// per il max-age

Applicazione di un jetPACK

È possibile applicare qualsiasi jetPACK in qualsiasi ordine, ma bisogna fare attenzione a non utilizzare un jetPACK con lo stesso indirizzo IP virtuale. Questa azione causerà un indirizzo IP duplicato nella configurazione. Se lo si fa per errore, è possibile modificarlo nella GUI.

- [Spostarsi su Avanzate > Aggiornamento software](#)
- [Sezione Configurazione](#)
- [Caricare una nuova configurazione o jetPACK](#)
- [Sfogliare per jetPACK](#)

- Fare clic su Carica
- Quando lo schermo del browser diventa bianco, fare clic su Aggiorna e attendere che venga visualizzata la pagina Dashboard.

Creazione di un jetPACK

Uno dei vantaggi di jetPACK è la possibilità di crearne di propri. È possibile che abbiate creato la configurazione perfetta per un'applicazione e vogliate utilizzarla per diverse altre scatole in modo indipendente.

- Iniziare copiando la configurazione corrente dall'ALB-X esistente.
 - Avanzato
 - Aggiornamento del software
 - Scarica la configurazione corrente
- Modificare questo file con Notepad++
- Aprite un nuovo documento txt e chiamatelo "yourname-jetPACK1.txt".
- Copiare tutte le sezioni rilevanti del file di configurazione in "yourname-jetPACK1.txt".
- Salvare una volta completato

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

Di seguito sono elencate le sezioni che si consiglia di modificare/copiare.

Sezione 0:

```
#!jetpack
```

Questa riga deve trovarsi all'inizio del jetPACK, altrimenti la 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 modificate 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 viene chiusa dopo 10 minuti di inattività.

```
ContentServerCustomTimer=20000
```

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

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

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

Sezione 2:

```
[jetnexusdaemon-Csm-Rules]
```

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

Esempio:

```
[jetnexusdaemon-Csm-Rules-0]
Contenuto="Server Up"
Desc="Monitor 1"
Metodo="CheckResponse"
Name="Verifica dello stato di salute - Il server è attivo"
Uri="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 comprende sotto-interfacce per ogni canale. Se al canale è stata applicata una regola flightPATH, la sezione contiene anche una sezione Path.

Esempio:

```
[jetnexusdaemon-LocalInterface1]
1.1="443"
1.2="104"
1.3="80"
1.4="81"
Abilitato=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="Senza SSL"
Comprimere=1
ConnectionLimiting=0
DSR=0
DSRProto="tcp"
Abilitato=1
LoadBalancePolicy="CookieBased" (basato sui cookie)
MaxConnections=10000
Politica di monitoraggio="1".
Passaggio=0
Protocollo="Accelerazione HTTP"
ServiceDesc="Server sicuri 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 flightPATH. I numeri devono corrispondere a quelli applicati all'interfaccia. Nell'esempio precedente, si nota che la regola flightPATH "6" è stata applicata al canale.

Esempio:

```
[jetnexusdaemon-Path-6]
Desc="Forza l'uso di HTTPS per determinate directory".
Nome="Gary - Forza HTTPS"
[jetnexusdaemon-Path-6-Condition-1]
Controllare="contenere"
Condizione="percorso"
Partita=
Senso="fa"
Valore="/secure/"
[jetnexusdaemon-Path-6-Evaluate-1]
Dettaglio=
Fonte="host"
Valore=
Variabile="$host$" [jetnexusdaemon-Path-6-Function-1]
Azione="reindirizzare"
Target="HTTPS://$host$$path$$querystring$"
Valore=
```

voloPATH

Introduzione a flightPATH

Che 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 allo stesso tempo molto facile da usare.

Sebbene alcuni componenti di flightPATH siano oggetti IP, come l'IP sorgente, flightPATH può essere applicato solo a un tipo di servizio Layer 7 uguale a HTTP. Se si sceglie un altro tipo di servizio, la scheda flightPATH di IP Services sarà vuota.

Cosa può fare flightPATH?

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

Oltre a utilizzare semplici corrispondenze di stringhe, come ad esempio "Inizia con" e "Finisce con", è possibile implementare un controllo completo utilizzando potenti espressioni regolari (RegEx) compatibili con Perl.

Per ulteriori informazioni su RegEx, consultare questo utile sito

Inoltre, è possibile creare variabili personalizzate nella sezione Valutazione e utilizzarle nell'area Azione, consentendo molte possibilità diverse.

Una regola flightPATH ha tre componenti:

Opzione	Descrizione
Dettagli	Utilizzato per aggiungere o rimuovere un flightPATH e per elencare quelli disponibili.
Condizione	Impostare più criteri per attivare la regola flightPATH.
Valutazione	Consente l'uso di variabili che possono essere utilizzate nell'area Azione.
Azione	Il comportamento una volta che la regola è stata attivata.

Condizione

In questa sezione è possibile specificare cinque parametri individuali applicabili a una condizione. Di seguito sono riportati una descrizione di ciascuna opzione e un esempio.

Condizione	Descrizione	Esempio
<form>	I moduli HTML vengono utilizzati per passare i dati al server.	Esempio "Il modulo non ha lunghezza 0".
Posizione GEO	Confronta l'indirizzo IP di origine con il codice paese ISO 3166.	Posizione GEO uguale a GB OPPURE Posizione GEO 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 una tendina con un elenco di Lingue
Metodo	Si tratta di un elenco a discesa di metodi HTTP	Si tratta di un menu a tendina che include GET, POST ecc.
Origine IP	Se il proxy upstream supporta X-Forwarded-for (XFF), utilizzerà l'indirizzo di origine reale.	IP del cliente. Può anche utilizzare più IP o sottoreti. 10\1\2\.* è la sottorete 10.1.2.0 /24 10\1\2\3 10\1\2\4 Utilizzare per più IP

Percorso	Questo è il percorso del sito web	/il mio sito/index.asp
POSTA	Metodo di richiesta POST	Controllare i dati caricati su un sito web
Interrogazione	Si tratta del nome e del valore di una query, che può accettare il nome della query o anche un valore.	"Best=edgeNEXUS" Dove la corrispondenza è Best e il valore è edgeNEXUS
Stringa di query	L'intera stringa di query dopo il carattere ?	
Richiesta di cookie	È il nome di un cookie richiesto da un client.	MS-WSMAN=afYfn1CDqqCDqUD::
Intestazione della richiesta	Può essere un'intestazione HTTP qualsiasi	Referrer, User-Agent, Da, Data
Versione richiesta	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 della risposta	200 OK, 304 Non modificato
Risposta Cookie	Questo è il nome di un cookie inviato dal server.	MS-WSMAN=afYfn1CDqqCDqUD::
Intestazione della risposta	Può essere un'intestazione HTTP qualsiasi	Referrer, User-Agent, Da, Data
Versione di risposta	La versione HTTP inviata dal server	HTTP/1.0 O HTTP/1.1
Fonte IP	Si tratta dell'IP di origine, dell'IP del server proxy o di un altro indirizzo IP aggregato.	Cliente IP, IP proxy, IP firewall. Può anche utilizzare più IP e sottoreti. È necessario è necessario sfuggire ai punti, in quanto si tratta di RegEX. Esempio 10\1\2\3 è 10.1.2.3

Partita

Il parametro Partita è sensibile al contesto e dipende dal valore del parametro Condizione.

Partita	Descrizione	Esempio
Accettare	Tipi di contenuto accettabili	Accetta: testo/plain
Accetta codifica	Codifiche accettabili	Accept-Encoding: <compress gzip deflate sdch identity>.
Lingua accettata	Lingue accettabili per la risposta	Lingua di accettazione: en-US
Campi di accettazione	Quali sono i tipi di intervallo di contenuto parziale supportati da questo server	Campi di accettazione: byte
Autorizzazione	Credenziali di autenticazione per l'autenticazione HTTP	Autorizzazione: Basic QWxhZGRpbjpvGVulHNlc2FtZQ==
Addebito a	Contiene informazioni sui costi dell'applicazione del metodo richiesto.	
Codifica del contenuto	Il tipo di codifica utilizzata per i dati.	Contenuto-Codifica: gzip
Lunghezza del contenuto	La lunghezza del corpo della risposta in ottetti (byte a 8 bit).	Lunghezza del contenuto: 348

Tipo di contenuto	Il tipo di mime del corpo della richiesta (usato con le richieste POST e PUT)	Tipo di contenuto: application/x-www-form-urlencoded
Biscotto	Un cookie HTTP precedentemente inviato dal server con Set-Cookie (di seguito)	Cookie: \$Version=1; Skin=new;
Data	Data e ora di origine del messaggio	Data = "Data" ":" HTTP-data
ETag	Un identificatore per una versione specifica di una risorsa, spesso un message digest.	ETag: "aed6bdb8e090cd1:0".
Da	L'indirizzo e-mail dell'utente che effettua la richiesta	Da: user@example.com
Se-Modificato-Da	Consente di restituire un 304 Not Modified se il contenuto è invariato.	Se-Modificato-Da: Sat, 29 Oct 1994 19:43:31 GMT
Ultima modifica	La data dell'ultima modifica dell'oggetto richiesto, nel formato RFC 2822.	Ultima modifica: 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
Referente	È l'indirizzo della pagina web precedente da cui è stato seguito il link alla pagina attualmente richiesta.	Referente: HTTP://www.edgenexus.io
Server	Un nome per il server	Server: Apache/2.4.1 (Unix)
Imposta-conservazione	Un cookie HTTP	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
Agente utente	La stringa dell'agente utente dell'utente	User-Agent: Mozilla/5.0 (compatibile; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Variare	Indica ai proxy a valle come confrontare le intestazioni delle richieste future per decidere se la risposta nella cache può essere utilizzata piuttosto che richiederne una nuova dal server di 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

Controllo

Controllo	Descrizione	Esempio
Esistere	Non si preoccupa dei dettagli della condizione, ma solo del fatto che esiste/non esiste.	Host> Does> Exist
Inizio	La stringa inizia con il valore	Percorso> Fa> Inizia /sicuro>
Fine	La stringa termina con il valore	Percorso> Fa> Fine> .jpg
Contenere	La stringa contiene il valore	Intestazione della richiesta> Accept> Does> Contain> Image
Pari	La stringa equivale al valore	Host> Does> Equal> www.edgenexus.io
Avere lunghezza	La stringa ha la lunghezza del valore	Host> Does> Have Length> 16 www.edgenexus.io = VERO www.edgenexus.com = FALSO
Superare la lunghezza	Controlla che il valore non superi la lunghezza specificata.	Percorso > Fa > Supera la lunghezza - 10

Corrispondenza di RegEx	Consente di inserire un'espressione regolare completa compatibile con Perl	IP di origine > > corrisponde al Regex> 10\..* 11\..*
Elenco partite	Consente di fornire un elenco delimitato da PIPE () di valori da controllare.	IP sorgente > Fa > Elenco partite > 10.0.0.1 10.0.0.100 192.178.28.32

Esempio

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

- L'esempio presenta due condizioni ed **ENTRAMBE** devono essere soddisfatte per eseguire l'azione
- Il primo è verificare che l'oggetto richiesto sia un'immagine
- Il secondo è il controllo di un hostname specifico

Valutazione

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

L'aggiunta di una variabile è una funzione interessante che consente di estrarre i dati dalla richiesta e di utilizzarli nelle azioni. Ad esempio, si può registrare il nome utente o inviare un'e-mail in caso di problemi di sicurezza.

- Variabile: Deve iniziare e terminare con il simbolo \$. Per esempio \$variabile1\$
- Fonte: Selezionare dalla casella a discesa la fonte della variabile.
- Dettaglio: Selezionare dall'elenco se pertinente. Se l'origine è l'intestazione della richiesta, i dettagli possono essere User-Agent.
- Valore: Inserire il testo o l'espressione regolare per regolare la variabile.

Variabili incorporate:

- Le variabili incorporate sono già state codificate, quindi non è necessario creare una voce di valutazione per queste.
- È possibile utilizzare una qualsiasi delle variabili elencate di seguito nella propria azione
- La spiegazione di ogni variabile si trova nella tabella "Condizioni" di cui sopra.
 - Metodo = \$metodo\$
 - Percorso = \$percorso\$
 - Querystring = \$querystring\$
 - Sourceip = \$sourceip\$
 - Codice di risposta (testo incluso anche "200 OK") = \$resp\$
 - Host = \$host\$
 - Versione = \$versione\$
 - Porta client = \$porta client\$
 - Clientip = \$clientip\$
 - Geolocalizzazione = \$geolocalizzazione\$".

Esempio di azione:

- Azione = Reindirizzamento 302

- Destinazione = HTTPs://\$host\$/404.html
- Azione = Registro
 - Target = Un client da \$sourceip\$: \$sourceport\$ ha appena effettuato una richiesta \$path\$ page

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 utilizzato, ma il percorso errato viene sostituito con 404.html.
- Al syslog viene aggiunta una voce che dice "Un client da 154.3.22.14:3454 ha appena effettuato una richiesta alla pagina wrong.html".

Fonte	Descrizione	Esempio
Biscotto	Questo è il nome e il valore dell'intestazione del cookie	MS-WSMAN=afYfn1CDqQCDqUD::Dove il nome è MS-WSMAN e il valore è afYfn1CDqQCDqUD::
Ospite	Questo è il nome dell'host estratto dall'URL	www.mywebsite.com o 192.168.1.1
Lingua	Questa è la lingua estratta dall'intestazione HTTP di Language	Questa condizione produrrà una tendina con un elenco di lingue.
Metodo	Si tratta di un elenco a discesa di metodi HTTP	Il menu a tendina comprende GET, POST
Percorso	Questo è il percorso del sito web	/il mio sito/index.html
POSTA	Metodo di richiesta POST	Controllare i dati caricati su un sito web
Voce della query	Si tratta del nome e del 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 di query	Questa è l'intera stringa dopo il carattere ?	HTTP://server/path/programma?query_string
Intestazione della richiesta	Può trattarsi di qualsiasi intestazione inviata dal client	Referrer, User-Agent, From, Date...
Intestazione della risposta	Può trattarsi di qualsiasi intestazione inviata dal server	Referrer, User-Agent, From, Date...
Versione	Questa è la versione HTTP	HTTP/1.0 o HTTP/1.1

Dettaglio	Descrizione	Esempio
Accettare	Tipi di contenuto accettabili	Accetta: testo/plain
Accetta codifica	Codifiche accettabili	Accept-Encoding: <compress gzip deflate sdch identity>.
Lingua accettata	Lingue accettabili per la risposta	Lingua di accettazione: en-US
Campi di accettazione	Quali sono i tipi di intervallo di contenuto parziale supportati da questo server	Campi di accettazione: byte
Autorizzazione	Credenziali di autenticazione per l'autenticazione HTTP	Autorizzazione: Basic QWxhZGRpbjpvGVulHNlc2FtZQ==
Addebito a	Contiene informazioni sui costi dell'applicazione del metodo richiesto.	
Codifica del contenuto	Il tipo di codifica utilizzata per i dati.	Contenuto-Codifica: gzip

Lunghezza del contenuto	La lunghezza del corpo della risposta in ottetti (byte a 8 bit).	Lunghezza del contenuto: 348
Tipo di contenuto	Il tipo di mime del corpo della richiesta (usato con le richieste POST e PUT)	Tipo di contenuto: application/x-www-form-urlencoded
Biscotto	un cookie HTTP precedentemente inviato dal server con Set-Cookie (di seguito)	Cookie: \$Version=1; Skin=new;
Data	Data e ora in cui il messaggio è stato originato	Data = "Data" ":" HTTP-data
ETag	Un identificatore per una versione specifica di una risorsa, spesso un message digest.	ETag: "aed6bdb8e090cd1:0".
Da	L'indirizzo e-mail dell'utente che effettua la richiesta	Da: user@example.com
Se-Modificato-Da	Consente di restituire un 304 Not Modified se il contenuto è invariato.	Se-Modificato-Da: Sat, 29 Oct 1994 19:43:31 GMT
Ultima modifica	La data dell'ultima modifica dell'oggetto richiesto, nel formato RFC 2822.	Ultima modifica: 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
Referente	È l'indirizzo della pagina web precedente da cui è stato seguito il link alla pagina attualmente richiesta.	Referente: HTTP://www.edgenexus.io
Server	Un nome per il server	Server: Apache/2.4.1 (Unix)
Imposta-conservazione	un cookie HTTP	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
Agente utente	La stringa dell'agente utente dell'utente	User-Agent: Mozilla/5.0 (compatibile; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Variare	Indica ai come confrontare le intestazioni delle richieste future per decidere se se la risposta nella cache può essere utilizzata piuttosto che richiederne una nuova dal server di 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 l'attività o le attività che vengono attivate una volta soddisfatte la condizione o le condizioni.

Action		
Action	Target	Data
Authentication	Form login	

Azione

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

Obiettivo

Fare doppio clic sulla colonna Destinazione per visualizzare l'elenco a discesa. L'elenco cambia a seconda dell'Azione.

Si può anche digitare manualmente con alcune azioni.

Dati

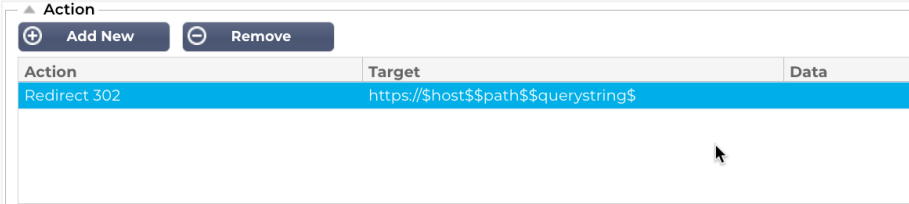
Fare doppio clic sulla colonna Dati per aggiungere manualmente i dati che si desidera aggiungere o sostituire.

L'elenco di tutte le azioni è riportato di seguito:

Azione	Descrizione	Esempio
Aggiungi cookie di richiesta	Aggiungere il cookie di richiesta dettagliato nella sezione Target con il valore nella sezione Dati	Obiettivo= Cookie Dati= MS-WSMAN=afYfn1CDqqCDqCVii
Aggiungere l'intestazione della richiesta	Aggiungere un'intestazione di richiesta di tipo Target con valore nella sezione Data	Obiettivo= Accetta Dati= image/png
Aggiungi cookie di risposta	Aggiungere il cookie di risposta dettagliato nella sezione Target con il valore nella sezione Data.	Obiettivo= Cookie Dati= MS-WSMAN=afYfn1CDqqCDqCVii
Aggiungere l'intestazione della risposta	Aggiungere l'intestazione della richiesta dettagliata nella sezione Target con il valore nella sezione Data.	Obiettivo= Cache-Control Dati= max-age=8888888
Corpo Sostituire tutto	Cercare nel corpo della risposta e sostituire tutte le istanze	Obiettivo= HTTP:// (stringa di ricerca) Dati= HTTPs:// (stringa di sostituzione)
Corpo Sostituire prima	Cercare nel corpo della risposta e sostituire solo la prima istanza	Obiettivo= HTTP:// (stringa di ricerca) Dati= HTTPs:// (stringa di sostituzione)
Corpo Sostituire per ultimo	Cerca nel corpo della risposta e sostituisce solo l'ultima istanza	Obiettivo= HTTP:// (stringa di ricerca) Dati= HTTPs:// (stringa di sostituzione)
Goccia	In questo modo si interrompe la connessione	Obiettivo= N/A Dati= N/A
e-mail	Invia un'e-mail all'indirizzo configurato in Eventi e-mail. È possibile utilizzare una variabile come indirizzo o come messaggio.	Target= "flightPATH ha inviato un'email a questo evento". Dati= N/A
Evento di registro	In questo modo viene registrato un evento nel registro di sistema	Target= "flightPATH ha registrato questo messaggio nel syslog". Dati= N/A
Reindirizzamento 301	In questo modo si otterrà un reindirizzamento permanente	Obiettivo= HTTP://www.edgenexus.io Dati= N/A
Reindirizzamento 302	In questo modo si otterrà un reindirizzamento temporaneo	Obiettivo= HTTP://www.edgenexus.io Dati= N/A
Rimuovere il cookie di richiesta	Rimuovere il cookie di richiesta dettagliato nella sezione Target	Obiettivo= Cookie Dati= MS-WSMAN=afYfn1CDqqCDqCVii
Rimuovere l'intestazione della richiesta	Rimuovere l'intestazione della richiesta dettagliata nella sezione Target	Destinatario=Server Dati=N/A

Rimuovere il cookie di risposta	Rimuovere il cookie di risposta descritto nella sezione Target	Obiettivo=jnAccel
Rimuovere l'intestazione della risposta	Rimuovere l'intestazione della risposta descritta nella sezione Target	Obiettivo= Etag Dati= N/A
Sostituire il cookie di richiesta	Sostituire il cookie di richiesta dettagliato nella sezione Target con il valore della sezione Data.	Obiettivo= Cookie Dati= MS-WSMAN=afYfn1CDqqCDqCVii
Sostituire l'intestazione della richiesta	Sostituire l'intestazione della richiesta nella destinazione con il valore dei dati.	Obiettivo= Connessione Dati= keep-alive
Sostituire il cookie di risposta	Sostituire il cookie di risposta dettagliato nella sezione Target con il valore della sezione Data.	Target=jnAccel=afYfn1CDqqCDqCVii Data=MS-WSMAN=afYfn1CDqqCDqCVii
Sostituire l'intestazione della risposta	Sostituire l'intestazione della risposta dettagliata nella sezione Target con il valore della sezione Data.	Obiettivo= Server Dati= Non sono disponibili per motivi di sicurezza
Riscrivere il percorso	Questo consente di reindirizzare la richiesta a un nuovo URL in base alla condizione	Obiettivo= /test/percorso/index.html\$querystring\$ Dati= N/A
Utilizzare un server sicuro	Selezionare il server sicuro o il servizio virtuale da utilizzare	Target=192.168.101:443 Dati=N/A
Utilizzare il server	Selezionare il server o il servizio virtuale da utilizzare	Obiettivo= 192.168.101:80 Dati= N/A
Crittografia del cookie	In questo modo i cookie vengono crittografati in 3DES e poi codificati in base64.	Target= Inserire il nome del cookie da crittografare, si può usare * come jolly alla fine. Dati= Inserire una frase di accesso per la crittografia.

Esempio:



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

L'azione seguente invia al browser un reindirizzamento temporaneo a un servizio virtuale HTTPS sicuro. Utilizzerà lo stesso hostname, percorso e querystring della richiesta.

Usi comuni

Firewall e sicurezza delle applicazioni

- Bloccare gli IP indesiderati
- Forzare l'utente a utilizzare HTTPS per un contenuto specifico (o per tutti i contenuti)
- Bloccare o reindirizzare gli spider
- Prevenzione e avviso di cross-site scripting
- Prevenzione e segnalazione di SQL injection
- Nascondere la struttura interna delle directory
- Riscrivere i cookie
- Directory sicura per utenti particolari

Caratteristiche

- Reindirizzare gli utenti in base al percorso
- Fornire il Single Sign On su più sistemi
- Segmentare gli utenti in base all'ID utente o al cookie
- Aggiungere intestazioni per l'offload SSL
- Rilevamento della lingua
- Riscrivere la richiesta dell'utente
- Correggere gli URL non funzionanti
- Codici di risposta 404 dei log e degli avvisi e-mail
- Impedire l'accesso alla directory/la navigazione
- Inviare agli spider contenuti diversi

Regole precostituite

Estensione HTML

Cambia tutte le richieste .htm in .html

Condizioni:

- Condizione = Percorso
- Senso = Fa
- Controllo = Corrispondenza con RegEx
- Valore = \.htm\$

Valutazione:

- Vuoto

Azione:

- Azione = Riscrivere il percorso
- Obiettivo = \$percorso\$I

Indice.html

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

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

- Condizione = Ospite
- Senso = Fa
- Controllo = Esistente

Valutazione:

- Vuoto

Azione:

- Azione = Reindirizzamento 302
- Destinazione = HTTP://\$host\$path\$index.html\$querystring\$

Chiudere le cartelle

Negare le richieste di cartelle.

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

- Condizione = questo richiede una riflessione adeguata
- Senso =
- Controllare =

Valutazione:

- Vuoto

Azione:

- Azione =
- Obiettivo =

Nascondere CGI-BBIN:

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

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

- Condizione = Ospite
- Senso = Fa
- Controllo = Corrispondenza con RegEX
- Valore = \.cgi\$

Valutazione:

- Vuoto

Azione:

- Azione = Riscrivere il percorso
- Destinazione = /cgi-bin\$path\$

Ragno di tronchi

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

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

- Condizione = Intestazione della richiesta
- Corrispondenza = Agente utente
- Senso = Fa
- Controllo = Corrispondenza con RegEX
- Valore = Googlebot|Slurp|bingbot|ia_archiver

Valutazione:

- Variabile = \$crawler\$
- Fonte = Intestazione della richiesta
- Dettaglio = Agente utente

Azione:

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

Forza HTTPS

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

Condizioni:

- Condizione = Percorso
- Senso = Fa
- Controllare = Contenere
- Valore = `/secure/`

Valutazione:

- Vuoto

Azione:

- Azione = Reindirizzamento 302
- Destinazione = `HTTP://$host$$$path$$$querystring$`

Flusso mediatico:

Reindirizza il Flash Media Stream al servizio appropriato.

Condizioni:

- Condizione = Percorso
- Senso = Fa
- Controllo = Fine
- Valore = `.flv`

Valutazione:

- Vuoto

Azione:

- Azione = Reindirizzamento 302
- Destinazione = `HTTP://$host$:8080/$path$`

Passare da HTTP a HTTPS

Cambiare qualsiasi `HTTP://` codificato in `HTTPS://`

Condizioni:

- Condizione = Codice di risposta
- Senso = Fa
- Controllo = uguale
- Valore = 200 OK

Valutazione:

- Vuoto

Azione:

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

Carte di credito vuote

Controllate che non ci siano carte di credito nella risposta e, se ne trovate una, cancellatela.

Condizioni:

- Condizione = Codice di risposta
- Senso = Fa
- Controllo = 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 dei contenuti

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

Condizione: si tratta di una condizione generica che fa da collante. Si consiglia di focalizzare questa condizione sulla

- Condizione = Codice di risposta
- Senso = Fa
- Controllo = uguale
- Valore = 200 OK

Valutazione:

- Vuoto

Azione:

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

Tipo di server spoof

Prendere il tipo di server e cambiarlo in qualcosa di diverso.

Condizione: si tratta di una condizione generica che fa da collante. Si consiglia di focalizzare questa condizione sulla

- Condizione = Codice di risposta

- Senso = Fa
- Controllo = uguale
- Valore = 200 OK

Valutazione:

- Vuoto

Azione:

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

Mai inviare errori

Il cliente non riceve mai errori dal vostro sito.

Condizione

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

Valutazione

- Vuoto

Azione

- Azione = Reindirizzamento 302
- Destinazione = HTTP//\$host\$/

Reindirizzamento sulla lingua

Individuare il codice della lingua e reindirizzare al relativo dominio nazionale.

Condizione

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

Valutazione

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

Azione

- Azione = Reindirizzamento 302
- Obiettivo = HTTP//\$host_template\$de\$path\$\$querystring\$

Google Analytics

Inserire il codice richiesto da Google per l'analisi - Cambiare il valore MYGOOGLECODE con il proprio ID Google UA.

Condizione

- Condizione = Codice di risposta
- Senso = Fa
- Controllo = uguale
- Valore = 200 OK

Valutazione

- vuoto

Azione

- Azione = Corpo Sostituisci ultimo
- Obiettivo = </body>
- Dati = <script type='text/javascript'> var _gaq = _gaq || []; _gaq.push(['_setAccount', 'IL MIO CODICE GOOGLE']); _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

Regola 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, pertanto questa regola lo sostituisce con un nome generico.

Condizione

- vuoto

Valutazione

- vuoto

Azione

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

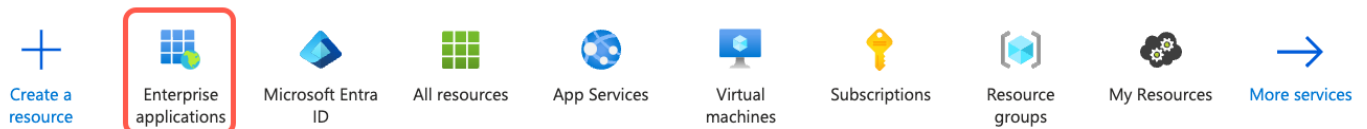
SAML e Entra ID

Impostazione dell'applicazione di autenticazione Entra ID in Microsoft Entra

Affinché l'autenticazione SAML funzioni correttamente, è necessario configurare un'applicazione Enterprise nel portale Microsoft Entra Admin. Si tratta di un'operazione semplice che consente di fornire il certificato di firma necessario per le richieste e i token di autenticazione SAML, nonché i dati XML di configurazione.

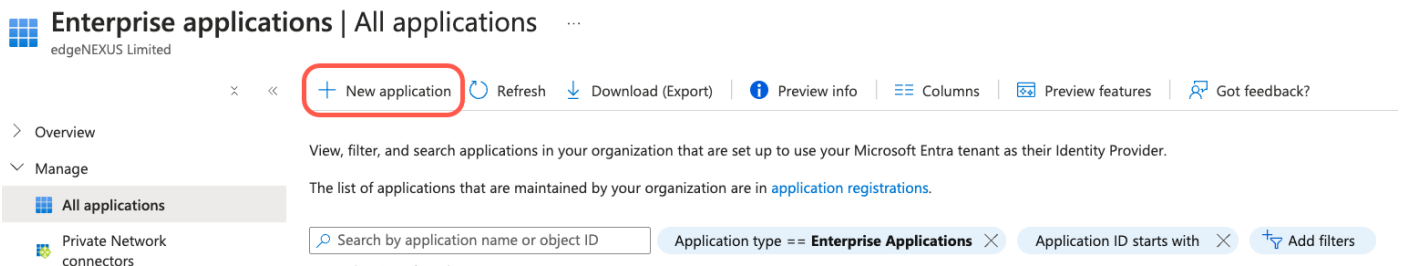
A tale scopo, occorre innanzitutto accedere al portale Microsoft Entra (<https://portal.azure.com>) e assicurarsi di trovarsi nella pagina dei servizi Azure, dove si trova un elenco di icone nella parte superiore della pagina (vedere sotto).

Azure services



- Fare clic su Applicazioni aziendali. Se non riuscite a vedere Applicazioni aziendali nell'elenco delle icone, potete inserire il nome nella barra di ricerca in alto. Verrà visualizzata una pagina come quella mostrata di seguito.

[Home](#) > [Enterprise applications](#)

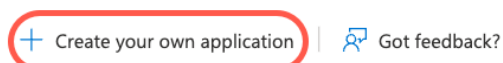


Fare clic su [Nuova applicazione](#)

Nella pagina successiva, fate clic su [Crea la tua applicazione](#).

[Home](#) > [Enterprise applications](#) | [All applications](#) >


Browse Microsoft Entra Gallery



The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning.¹ users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Er described in [this article](#).

- Sul lato destro della pagina si aprirà una sezione intitolata "[Crea la tua applicazione](#)".

Create your own application ×

 Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

What are you looking to do with your application?

- Configure Application Proxy for secure remote access to an on-premises application
- Register an application to integrate with Microsoft Entra ID (App you're developing)
- Integrate any other application you don't find in the gallery (Non-gallery)

- Fornire un nome per l'applicazione, ad esempio "My Entra ID Auth App". È possibile scegliere il nome che si desidera.
- Fare clic sull'opzione *Integrare qualsiasi altra applicazione non presente nella galleria (Non-gallery)*.
- Fare clic sul pulsante *Crea*.

A questo punto si aprirà una pagina simile a quella che segue.

My Entra ID Auth App | Overview ...

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Roles and administrators
 - Users and groups
 - Single sign-on
 - Provisioning
 - Application proxy
 - Self-service
 - Custom security attributes
- Security
- Activity
- Troubleshooting + Support
 - New support request

Properties

ME Name ⓘ
My Entra ID Auth App 🗑️

Application ID ⓘ
f4bf0c51-2fa1-4cdf-8bff... 🗑️

Object ID ⓘ
284d2b8e-1fe5-4554-b7... 🗑️

Getting Started

1. Assign users and groups

Provide specific users and groups access to the applications

[Assign users and groups](#)

2. Set up single sign on

Enable users to sign into their application using their Microsoft Entra credentials

[Get started](#)

3. Provision User Accounts

Automatically create and delete user accounts in the application

[Get started](#)

4. Conditional Access

Secure access to this application with a customizable access policy.

[Create a policy](#)

5. Self service

Enable users to request access to the application using their Microsoft Entra credentials

[Get started](#)

- Fare clic sull'opzione Single Sign-on nella barra di navigazione sinistra.
- Selezionare la casella SAML

Select a single sign-on method [Help me decide](#)

Disabled

Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML

Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.


Password-based

Password storage and replay using a web browser extension or mobile app.

Linked

Link to an application in My Apps and/or Office 365 application launcher.

- Verrà visualizzata una pagina contenente la sezione Configurazione SAML di base.

Basic SAML Configuration		 Edit
Identifier (Entity ID)	Required	
Reply URL (Assertion Consumer Service URL)	Required	
Sign on URL	<i>Optional</i>	
Relay State (Optional)	<i>Optional</i>	
Logout Url (Optional)	<i>Optional</i>	

- Nell'area Configurazione SAML di base compilare:
 - Identificatore (ID dell'entità)
 - URL di risposta (URL del servizio consumatori di asserzioni)
 - URL di accesso
 - URL di logout (opzionale)
- Salvare la configurazione e testare l'applicazione.

Per una guida più dettagliata, è possibile consultare la documentazione [Enable single sign-on for an enterprise application](#) sul sito Microsoft.

Assistenza tecnica

Forniamo assistenza tecnica a tutti i nostri utenti secondo i termini di servizio standard dell'azienda.

L'assistenza tecnica viene fornita se si dispone di un contratto di assistenza e manutenzione attivo per EdgeADC, EdgeWAF o EdgeGSLB.

Per inviare un ticket di assistenza, visitare il sito:

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