



EdgeADC

GUÍA DE ADMINISTRACIÓN

Contenido

Propiedades del documento	7
Descargo de responsabilidad del documento.....	7
Derechos de autor	7
Marcas comerciales	7
Soporte de Edgenexus.....	7
Instalación del EdgeADC.....	8
VMware ESXi.....	8
Instalación de la interfaz VMXNET3	8
Microsoft Hyper-V	9
Citrix XenServer.....	11
Configuración del primer arranque	12
Primer arranque - Detalles de la red manual.....	12
Primer arranque - DHCP exitoso.....	12
Primer arranque - El DHCP falla	12
Cambio de la dirección IP de gestión	13
Cambio de la máscara de subred para eth0.....	13
Asignación de una puerta de enlace por defecto.....	13
Comprobación del valor de la puerta de enlace predeterminada.....	13
Acceso a la interfaz web	13
Tabla de referencia de comandos	14
Iniciar la consola web del CAD	16
Credenciales de inicio de sesión por defecto	16
El tablero principal	17
Servicios.....	18
Servicios IP.....	18
Servicios virtuales.....	18
Servidores reales.....	25
Cambios en el servidor real para el retorno del servidor directo.....	38
Configuración necesaria del servidor de contenidos.....	38
Cambios en el servidor real - Modo de puerta de enlace	39
Configuración necesaria del servidor de contenidos.....	40
Ejemplo de brazo único	40
Ejemplo de brazo doble.....	40
Biblioteca.....	41
Complementos.....	41
Aplicaciones	41
Comprar un complemento	41

Desplegar una aplicación	42
Autenticación	43
Configuración de la autenticación - Un flujo de trabajo	43
Servidores de autenticación	43
Reglas de autenticación.....	44
Inicio de sesión único	45
Formularios	45
Caché	46
flightPATH.....	49
Monitores de servidores reales	56
Detalles	56
Ejemplos de Real Server Monitor	59
Certificados SSL	61
¿Qué hace el CAD con el certificado SSL?	61
Crear certificado	61
Gestionar el certificado.....	63
Importar un certificado.....	66
Importación de varios certificados	67
Widgets.....	68
Ver	75
Tablero de mandos.....	75
Uso del panel de control	75
Historia	77
Visualización de datos gráficos.....	77
Registros.....	78
Descargar los registros del W3C	79
Estadísticas	79
Compresión.....	79
Golpes y conexiones	80
Caché.....	81
Persistencia de la sesión	81
Hardware.....	82
Estado	82
Detalles del servicio virtual	82
Sistema	85
Agrupación.....	85
Papel.....	85
Ajustes	88

Gestión.....	88
Cambiar la prioridad de un CAD.....	89
Fecha y hora.....	90
Fecha y hora manual.....	90
Sincronizar fecha y hora (UTC).....	90
Eventos por correo electrónico.....	91
Dirección.....	91
Servidor de correo (SMTP).....	92
Notificaciones y alertas.....	92
Advertencias.....	93
Historia del sistema.....	93
Recoger datos.....	94
Mantenimiento.....	94
Licencia.....	94
Detalles de la licencia.....	95
Instalaciones.....	96
Instale la licencia.....	96
Registro.....	96
Detalles del registro del W3C.....	96
Servidor Syslog.....	98
Servidor Syslog remoto.....	98
Almacenamiento remoto de registros.....	99
Borrar archivos de registro.....	101
Red.....	101
Configuración básica.....	101
Detalles del adaptador.....	102
Interfaces.....	103
Vinculación.....	103
Ruta estática.....	105
Detalles de la ruta estática.....	105
Configuración avanzada de la red.....	105
SNAT.....	106
Potencia.....	107
Seguridad.....	107
SNMP.....	109
Configuración de SNMP.....	109
MIB SNMP.....	109
Descarga de MIB.....	109

ADC OID	109
Gráficos históricos.....	110
Usuarios y registros de auditoría.....	111
Usuarios	111
Registro de auditoría.....	113
Avanzado	114
Configuración.....	114
Descarga de una configuración	114
Carga de una configuración.....	114
Ajustes globales.....	115
Temporizador de la caché del host.....	115
Drenaje.....	115
SSL	115
Autenticación.....	115
Protocolo.....	116
Servidor demasiado ocupado	116
Reenviado Para.....	116
Configuración de la compresión HTTP	117
Exclusiones de la compresión global.....	119
Cookies de persistencia.....	119
Software.....	119
Detalles de la actualización del software	120
Descarga desde la nube.....	120
Cargar el software en el ALB.....	121
Aplicar el software almacenado en el ALB.....	121
Solución de problemas.....	122
Archivos de apoyo.....	122
Rastrear	122
Ping.....	123
Captura	124
Ayuda	125
Sobre nosotros.....	125
Referencia	125
Qué es un jetPACK	126
Descarga de un jetPACK	126
Microsoft Exchange.....	126
Microsoft Lync 2010/2013.....	128
Servicios web	128

Escritorio remoto de Microsoft	128
DICOM - Imagen y Comunicación Digital en Medicina	128
Oracle e-Business Suite	128
VMware Horizon View	128
Ajustes globales.....	128
Opciones de cifrado	128
flightPATHs.....	129
Aplicar un jetPACK	129
Creación de un jetPACK.....	129
Introducción a flightPATH	133
¿Qué es flightPATH?	133
¿Qué puede hacer flightPATH?	133
Condición.....	133
Ejemplo	136
Evaluación	136
Acción.....	139
Acción	139
Objetivo	139
Datos.....	139
Usos comunes	141
Cortafuegos y seguridad de las aplicaciones.....	141
Características	141
Reglas preestablecidas.....	142
Extensión HTML.....	142
Índice.....	142
Cerrar carpetas	142
Oculte el CGI-BBIN:	143
Araña de troncos.....	143
Forzar HTTPS	143
Corriente de los medios de comunicación:	144
Cambiar HTTP por HTTPS.....	144
Tarjetas de crédito en blanco	144
Caducidad del contenido	145
Tipo de Servidor de Falsificación.....	145
Cortafuegos de aplicaciones web (edgeWAF)	148
Ejecución del WAF.....	148
Ejemplo de arquitectura	149
WAF utilizando la dirección IP externa	149

WAF utilizando la dirección IP interna	149
Acceso a su complemento WAF	150
Actualización de las normas.....	151
Equilibrio global de la carga del servidor (edgeGSLB)	153
Introducción	153
Resiliencia y recuperación de desastres.....	153
Equilibrio de carga y geolocalización	153
Consideraciones comerciales.....	153
Visión general del sistema de nombres de dominio	153
El DNS consta de tres componentes clave:.....	153
A continuación se explica una transacción típica de DNS:.....	153
Caché.....	154
Tiempo de vivir	154
Visión general de GSLB.....	154
Configuración del GSLB.....	154
Ubicaciones personalizadas.....	160
Redes privadas	160
Cómo funciona	160
¿Cómo configuramos este aspecto en el GSLB?	161
Flujo de tráfico.....	163
Soporte técnico	164

Propiedades del documento

Número de documento: 2.0.6.16.21.18.06

Fecha de creación del documento: 30 de abril de 2021

Documento editado por última vez: June 16, 2021

Autor del documento: Jay Savoor

Documento editado por última vez por:

Remisión de documentos: EdgeADC - Versión 4.2.7.1895

Descargo de responsabilidad del documento

Las capturas de pantalla y los gráficos de este manual pueden diferir ligeramente de su producto debido a las diferencias en la versión de su producto. Edgenexus asegura que realiza todos los esfuerzos razonables para garantizar que la información de este documento sea completa y precisa. Edgenexus no asume ninguna responsabilidad por cualquier error. Edgenexus realizará cambios y correcciones a la información de este documento en futuras versiones cuando sea necesario.

Derechos de autor

2021 Todos los derechos reservados.

La información contenida en este documento está sujeta a cambios sin previo aviso y no representa un compromiso por parte del fabricante. Ninguna parte de esta guía puede ser reproducida o transmitida en cualquier forma o medio, electrónico o mecánico, incluyendo fotocopias y grabaciones, para cualquier propósito, sin el permiso expreso por escrito del fabricante. Las marcas registradas son propiedad de sus respectivos dueños. Se ha hecho todo lo posible para que esta guía sea lo más completa y precisa posible, pero no se ofrece ninguna garantía de idoneidad. Los autores y el editor no tendrán ninguna responsabilidad ante ninguna persona o entidad por las pérdidas o daños derivados del uso de la información contenida en esta guía.

Marcas comerciales

El logotipo de Edgenexus, Edgenexus, EdgeADC, EdgeWAF, EdgeGSLB, EdgeDNS son marcas comerciales o marcas registradas de Edgenexus Limited. Todas las demás marcas comerciales son propiedad de sus respectivos propietarios y son reconocidas.

Soporte de Edgenexus

Si tiene alguna pregunta técnica sobre este producto, por favor, plantee un ticket de soporte en: support@edgenexus.io

Instalación del EdgeADC

El producto EdgeADC (denominado ADC a partir de ahora) está disponible para su instalación mediante varios métodos. Cada objetivo de plataforma requiere su instalador, y todos ellos están a su disposición.

Estos son los distintos modelos de instalación disponibles.

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

El tamaño de la máquina virtual que utilizará para alojar el ADC depende del escenario del caso de uso y del rendimiento de los datos.

VMware ESXi

El ADC está disponible para su instalación en VMware ESXi son 5.x y superiores.

- Descargue el último paquete OVA de instalación de la ADC utilizando el enlace correspondiente que se proporciona con el correo electrónico de descarga.
- Una vez descargado, descomprímalo en un directorio adecuado de su host ESXi o SAN.
- En su cliente vSphere, seleccione Archivo: Desplegar plantilla OVA/OVF.
- Busque y seleccione la ubicación donde ha guardado sus archivos; elija el archivo OVF y haga clic en **SIGUIENTE**
- El servidor ESX solicita el nombre del dispositivo. Escriba un nombre adecuado y pulse **SIGUIENTE**
- Seleccione el almacén de datos desde el que se ejecutará su dispositivo ADC.
- Seleccione un almacén de datos con suficiente espacio y haga clic en **SIGUIENTE**
- A continuación, se le informará sobre el producto; haga clic en **SIGUIENTE**
- Haga clic en **SIGUIENTE**.
- Una vez que haya copiado los archivos en el almacén de datos, podrá instalar el dispositivo virtual.

Inicie su cliente vSphere para ver el nuevo dispositivo virtual ADC.

- Haga clic con el botón derecho del ratón en la VA y vaya a Encendido > Encendido
- Su VA arrancará entonces, y la pantalla de arranque del CAD se mostrará en la consola.

```
Checking for management interface ..... [ OK ]
Management interface: eth0  MAC: 88:8c:29:85:2e:1a

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

Instalación de la interfaz VMXNET3

El controlador VMXnet3 es compatible, pero tendrá que hacer cambios en la configuración de la NIC primero.

Nota - NO actualice el VMware-tools

Habilitación de la interfaz VMXNET3 en una VA recién importada (nunca iniciada)

1. Borrar ambos NICs de la VM
2. Actualice el hardware de la VM - - Haga clic con el botón derecho del ratón en la VA de la lista y seleccione Actualizar el hardware virtual (no inicie una instalación o actualización de las herramientas de VMware, **sólo** realice la actualización del hardware)
3. Añada dos NIC y selecciónelos para que sean VMXNET3
4. Inicie la VA utilizando el método estándar. Funcionará con el VMXNET3

Habilitación de la interfaz VMXNET3 en una VA ya en funcionamiento

1. Detener la VM (comando de apagado CLI o apagado GUI)
2. Obtenga las direcciones MAC de ambos NIC (**¡recuerde el orden de los NIC en la lista!**)
3. Borrar ambos NICs de la VM
4. Actualice el hardware de la VM (no inicie una instalación o actualización de las herramientas VMware, **sólo** realice la actualización del hardware)
5. Añada dos NIC y seleccione que sean VMXNET3
6. Establezca las direcciones MAC para los nuevos NIC de acuerdo con el paso 2
7. Reiniciar la VA

Apoyamos VMware ESXi como plataforma de producción. Para fines de evaluación, puede utilizar VMware Workstation y Player.

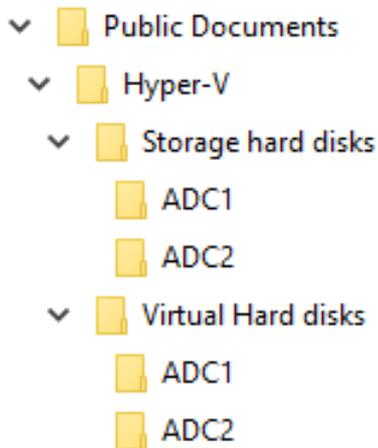
Consulte la sección [CONFIGURACION DEL PRIMER ARRANQUE](#) para seguir adelante.

Microsoft Hyper-V

El dispositivo Edgenexus ADC Virtual puede instalarse fácilmente dentro de un marco de virtualización Microsoft Hyper-V. Esta guía asume que ha especificado y configurado correctamente su sistema Hyper-V y los recursos del sistema para acomodar el ADC y su arquitectura de equilibrio de carga.

Tenga en cuenta que cada aparato requiere una dirección MAC única.

- Extraiga el archivo ADC-VA descargado compatible con Hyper-V a su máquina o servidor local.
- Abra Hyper-V Manager.
- Cree una nueva carpeta para contener el "disco duro virtual" del ADC VA y otra nueva carpeta para contener el "disco duro de almacenamiento", por ejemplo, C:\Users\Public\Documents\Hyper-V\Discos duros virtuales\ADC1 y C:\Users\Public\Documents\Hyper-V\Discos duros de almacenamiento\ADC1
- **Nota:** Es necesario crear nuevas subcarpetas específicas del ADC para los discos duros virtuales y los discos duros de almacenamiento para cada instalación de instancia virtual del ADC, como se muestra a continuación:



- Copie el archivo .vhd de EdgeADC extraído en la carpeta 'Disco duro de almacenamiento' creada anteriormente.
- En su cliente Hyper-V Manager, haga clic con el botón derecho en el servidor y seleccione "Importar máquina virtual"
- Vaya a la carpeta que contiene el archivo de imagen del CAD VA extraído anteriormente
- Seleccione la máquina virtual - resalte la máquina virtual a importar y haga clic en Siguiente
- Seleccione la máquina virtual - resalte la máquina virtual a importar y haga clic en Siguiente
- Elija el tipo de importación - seleccione **"Copiar la máquina virtual (crear un nuevo ID único)"** haga clic en siguiente
- Elija las carpetas para los archivos de la máquina virtual: el destino puede dejarse como el predeterminado de Hyper-V o puede elegir una ubicación diferente
- Localice los discos duros virtuales - busque y seleccione la carpeta de discos duros virtuales creada anteriormente y haga clic en siguiente
- Elija las carpetas para almacenar los discos duros virtuales - busque y seleccione la carpeta de discos duros de almacenamiento creada anteriormente y haga clic en siguiente
- Verifique que los detalles de la ventana de resumen del asistente de importación son correctos y haga clic en Finalizar
- Haga clic con el botón derecho del ratón en la máquina virtual **ADC** recién importada y seleccione Iniciar

NOTA: SEGUN [HTTP://SUPPORT.MICROSOFT.COM/KB/2956569](http://support.microsoft.com/kb/2956569) DEBE IGNORAR EL MENSAJE DE ESTADO "DEGRADADO (SE REQUIERE LA ACTUALIZACION DE LOS SERVICIOS DE INTEGRACION)", QUE PUEDE APARECER COMO SE INDICA A CONTINUACION DESPUES DE INICIAR LA AV. NO SE REQUIERE NINGUNA ACCIÓN Y EL SERVICIO NO ESTÁ DEGRADADO

- Mientras la VM se está inicializando, puede hacer clic con el botón derecho del ratón en la entrada de la VM y seleccionar Conectar... Entonces se le presentará la consola del 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 vez configuradas las propiedades de la red, la VA se reiniciará y presentará el inicio de sesión en la consola de la VA.

Consulte la sección [CONFIGURACION DEL PRIMER ARRANQUE](#) para seguir adelante.

Citrix XenServer

El dispositivo ADC Virtual se puede instalar en Citrix XenServer.

- Extraiga el archivo ADC OVA ALB-VA a su máquina o servidor local.
- Abra el Cliente Citrix XenCenter.
- En su cliente XenCenter, seleccione "**Archivo: Importar**".
- Busque y seleccione el archivo **OVA** y haga clic en "**Abrir siguiente**".
- Seleccione la ubicación de creación de la VM cuando se le pregunte.
- Elija qué XenServer desea instalar y haga clic en "**NEXT**".
- Seleccione el repositorio de almacenamiento (SR) para la colocación del disco virtual cuando se le pregunte.
- Seleccione un SR con suficiente espacio y haga clic en "**NEXT**".
- Asigne sus interfaces de red virtuales. Ambas interfaces dirán Eth0; sin embargo, observe que la interfaz inferior es Eth1.
- Seleccione la red de destino para cada interfaz y haga clic en **SIGUIENTE**
- **NO** marque la opción "Usar la corrección del sistema operativo".
- Pulse "**NEXT**"
- Elija la interfaz de red que se utilizará para la transferencia temporal VM.
- Elija la interfaz de gestión, normalmente la red 0, y deje la configuración de red en DHCP. Tenga en cuenta que debe asignar los detalles de la dirección IP estática si no tiene un servidor DHCP que funcione para la transferencia. Si no lo hace, la importación dirá que se está conectando continuamente y que ha fallado. Haga clic en "**NEXT**".
- Revise toda la información y compruebe los ajustes correctos entonces. Haga clic en "**FINALIZAR**".
- Su VM comenzará a transferir el disco virtual "ADC ADC" y, una vez completado, se mostrará bajo su XenServer.
- Dentro de su cliente XenCenter, ahora podrá ver la nueva máquina virtual. Haga clic con el botón derecho en la VA y haga clic en "**START**".
- Su VM arrancará entonces y se mostrará la pantalla de arranque del CAD.

```
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 vez configurado, se presenta la entrada al VA.

Consulte la sección [CONFIGURACION DEL PRIMER ARRANQUE](#) para seguir adelante.

Configuración del primer arranque

En el primer arranque, el CAD VA muestra la siguiente pantalla solicitando la configuración para las operaciones de producción.

```
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
```

Primer arranque - Detalles de la red manual

En el primer arranque, dispondrá de 10 segundos para interrumpir la asignación automática de datos IP a través de DHCP

Para interrumpir este proceso, haga clic en la ventana de la consola y pulse cualquier tecla. A continuación, puede introducir manualmente los siguientes datos.

- Dirección IP
- Máscara de subred
- Puerta de enlace
- Servidor DNS

Estos cambios son persistentes y sobrevivirán a un reinicio y no necesitan ser configurados de nuevo en la VA.

Primer arranque - DHCP exitoso

Si no interrumpe el proceso de asignación de red, su ADC contactará con un servidor DHCP después de un tiempo de espera para obtener sus datos de red. Si el contacto es exitoso, entonces a su máquina se le asignará la siguiente información.

- Dirección IP
- Máscara de subred
- Pasarela por defecto
- Servidor DNS

Le aconsejamos que no utilice la VA del CAD utilizando una dirección DHCP a menos que esa dirección IP se vincule permanentemente a la dirección MAC de la VA dentro del servidor DHCP. Aconsejamos utilizar siempre una **DIRECCIÓN IP FIJA** cuando utilice la VA. Siga los pasos indicados en [CAMBIO DE LA DIRECCION IP DE GESTION](#) y en las secciones posteriores hasta completar la configuración de la red.

Primer arranque - El DHCP falla

Si no tiene un servidor DHCP o la conexión falla, se asignará la dirección IP 192.168.100.100. La dirección IP se incrementará en '1' hasta que la VA encuentre una dirección IP libre. Igualmente, la VA comprobará si la dirección IP está actualmente en uso, y si es así, se incrementará de nuevo y volverá a comprobarlo.

Cambio de la dirección IP de gestión

Puede cambiar la dirección IP de la VA en cualquier momento utilizando el comando **set greenside=n.n.n.n**, como se muestra a continuación.

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

Cambio de la máscara de subred para eth0

Las interfaces de red utilizan el prefijo 'eth'; la dirección de red base se llama eth0. La máscara de subred o máscara de red puede cambiarse mediante el comando **set mask eth0 n.n.n.n**. Puede ver un ejemplo a continuación.

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

Asignación de una puerta de enlace por defecto

La VA necesita una puerta de enlace por defecto para sus operaciones. Para establecer la puerta de enlace por defecto, utilice el comando **route add default gw n.n.n.n** como se muestra en el ejemplo siguiente.

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

Comprobación del valor de la puerta de enlace predeterminada

Para comprobar si la puerta de enlace por defecto está añadida y es correcta, utilice el comando **route**. Este comando mostrará las rutas de red y el valor de la puerta de enlace por defecto. Vea el ejemplo siguiente.

```
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
```

Ahora puede acceder a la interfaz gráfica de usuario (GUI) para configurar el ADC para su uso en producción o en evaluación.

Acceso a la interfaz web

Puede utilizar cualquier navegador de Internet con Javascript para configurar, supervisar y poner en funcionamiento el ADC.

En el campo de la URL del navegador, escriba **HTTPS://{Dirección IP}** o **HTTPS://{FQDN}**

El CAD, por defecto, utiliza un certificado SSL autofirmado. Puede cambiar el CAD para que utilice el certificado SSL de su elección.

Una vez que su navegador llegue al CAD, le mostrará la pantalla de inicio de sesión. Las credenciales predeterminadas de fábrica para el CAD son:

Nombre de usuario por defecto = **admin** / Contraseña por defecto = **jetnexus**

Tabla de referencia de comandos

Comando	Parámetro1	Parámetro2	Descripción	Ejemplo
fecha			Muestra la fecha y la hora configuradas actualmente	mar 3 de septiembre 13:00 UTC 2013
valores predeterminados			Asigne los ajustes por defecto de su aparato	
salir			Cerrar la sesión de la interfaz de línea de comandos	
ayuda			Muestra todos los comandos válidos	
ifconfig	[en blanco]		Ver la configuración de la interfaz para todas las interfaces	ifconfig
	eth0		Ver la configuración de la interfaz de eth0 solamente	ifconfig eth0
machineid			Este comando proporcionará el machineid utilizado para licenciar el ADC ADC	EF4-3A35-F79
deje de			Cerrar la sesión de la interfaz de línea de comandos	
reiniciar			Finalice todas las conexiones y reinicie el ADC ADC	reiniciar
reiniciar			Reiniciar los servicios virtuales del CAD	
ruta	[en blanco]		Ver la tabla de enrutamiento	ruta
	añadir	gw por defecto	Añada la dirección IP de la puerta de enlace por defecto	route add default gw 192.168.100.254
set	greenside		Establezca la dirección IP de gestión para el CAD	set greenside=192.168.101.1
	máscara		Establezca la máscara de subred para una interfaz. Los nombres de las interfaces son eth0, eth1....	set mask eth0 255.255.255.0
mostrar			Muestra los ajustes de configuración global	
apagado			Termine todas las conexiones y apague el ADC	
estado			Muestra las estadísticas de datos actuales	

top		Ver la información del proceso, como la CPU y la memoria	
ver registro	mensajes	Muestra los mensajes syslog en bruto	Ver los mensajes de registro

Tenga en cuenta que los comandos no distinguen entre mayúsculas y minúsculas. No hay historial de comandos.

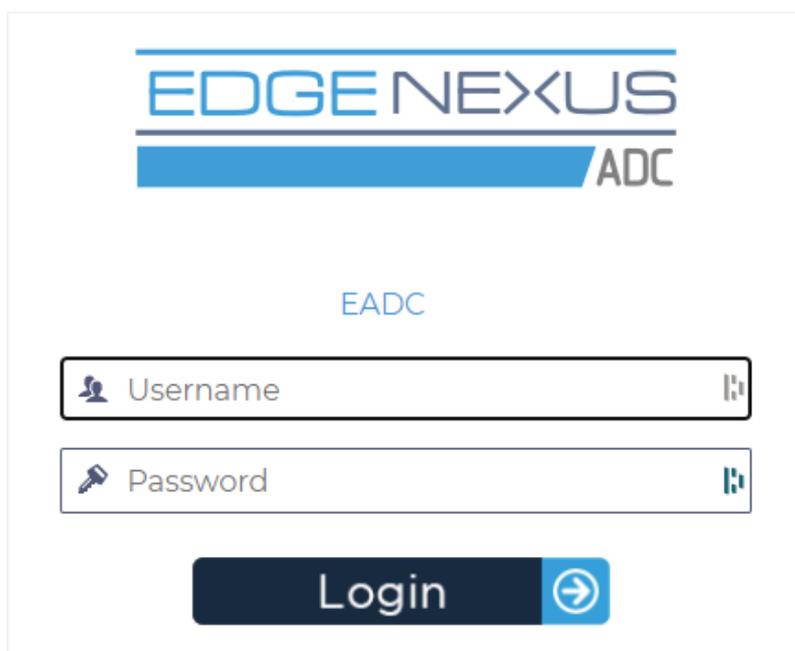
Iniciar la consola web del CAD

Todas las operaciones en el CAD (también denominado ADC) se configuran y realizan mediante la consola web. Se accede a la consola web mediante cualquier navegador con Javascript.

Para iniciar la consola web del ADC, introduzca la URL o la dirección IP del ADC en el campo URL. Utilizaremos el ejemplo de `adc.empresa.com` como ejemplo:

`https://adc.company.com`

Cuando se lanza, la consola web del ADC es como se muestra a continuación, permitiéndole iniciar sesión como usuario administrador.



The screenshot shows the login interface for EdgeNexus ADC. At the top, the logo 'EDGE NEXUS' is displayed in blue, with 'ADC' in a smaller font to the right. Below the logo, the text 'EADC' is centered. There are two input fields: the first is labeled 'Username' and has a user icon on the left; the second is labeled 'Password' and has a key icon on the left. Below these fields is a dark blue 'Login' button with a white right-pointing arrow icon.

Credenciales de inicio de sesión por defecto

Las credenciales de acceso por defecto son:

- Nombre de usuario: admin
- Contraseña: jetnexus

Puede cambiar esto en cualquier momento utilizando las capacidades de configuración de usuarios que se encuentran en *Sistema > Usuarios*.

Una vez que haya iniciado la sesión con éxito, aparecerá el panel principal del CAD.

El tablero principal

La imagen siguiente ilustra el aspecto del tablero principal o "página de inicio" del CAD. Es posible que hagamos algunos cambios de vez en cuando por motivos de mejora, pero todas las funciones se mantendrán.

The screenshot displays the EdgeADC main dashboard. At the top, there is a navigation bar with the 'EDGE NEXUS' logo, a search bar, and buttons for 'GUI Status', 'Home', 'Help', and a user profile 'admin'. Below this is a 'NAVIGATION' sidebar with options like 'Services', 'App Store', 'IP-Services', 'Library', 'View', 'System', 'Advanced', and 'Help'. The main content area is divided into two sections: 'Virtual Services' and 'Real Servers'.

Virtual Services Section:

- Buttons: Copy Service, Add Service, Remove Service
- Table with columns: Primary, VIP, VS, Enabled, IP Address, SubNet Mask / Prefix, Port, Service Name, Service Type.
- Table Row 1: [Icon], [Green], [Green], [Checked], 192.168.1.222, 255.255.255.0, 80, TEST WEB RR, HTTP

Real Servers Section:

- Buttons: Copy Server, Add Server, Remove Server
- Group Name: Server Group
- Table with columns: Status, Activity, Address, Port, Weight, Calculated Weight, Notes, ID.
- Table Row 1: [Green], Online, 192.168.1.200, 80, 100, 100, Site 1, [ID]
- Table Row 2: [Green], Online, 192.168.1.201, 80, 100, 100, Site 2, [ID]

Para ser lo más concisos posible, supondremos que esta primera introducción a las secciones de la pantalla le hará conocer suficientemente las diferentes secciones del área de configuración del ADC, por lo que no las describiremos en detalle a medida que avancemos, sino que nos centraremos en los elementos de configuración.

Yendo de izquierda a derecha, primero tenemos la Navegación. La sección de Navegación consiste en las diferentes áreas dentro del CAD. Cuando haga clic en una opción concreta dentro de la Navegación, se mostrará la sección correspondiente en la parte derecha de la pantalla. También puede ver la sección de configuración elegida con pestañas en la parte superior de la pantalla, junto al logotipo del producto. Las pestañas permiten una navegación más rápida a las áreas preutilizadas de la configuración del CAD.

Servicios

La sección de servicios del CAD tiene varias áreas dentro de ella. Cuando haga clic en el elemento de servicios, éste se ampliará para mostrar las opciones disponibles.

Servicios IP

La sección de servicios IP del CAD le permite añadir, eliminar y configurar los distintos servicios IP virtuales que necesita para su caso de uso particular. Los ajustes y las opciones se dividen en las siguientes secciones. Estas secciones se encuentran en la parte derecha de la pantalla de la aplicación.

Servicios virtuales

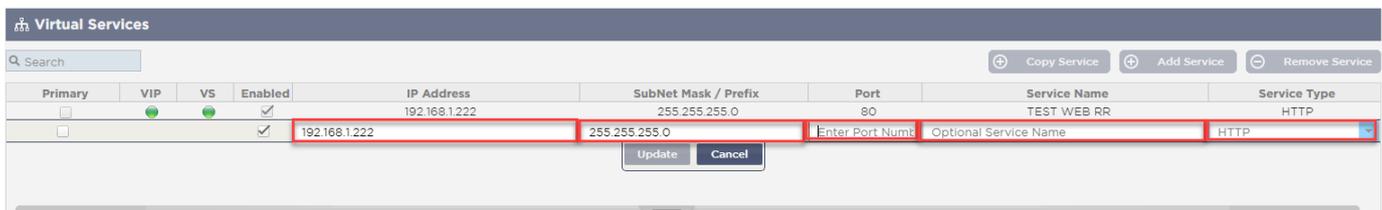
Un Servicio Virtual combina una IP Virtual (VIP) y un puerto TCP/UDP en el que el ADC escucha. El tráfico que llega a la IP del Servicio Virtual se redirige a uno de los Servidores Reales asociados a ese servicio. La dirección IP del Servicio Virtual no puede ser la misma que la dirección de gestión del CAD, es decir, eth0, eth1, etc.

El ADC determina cómo se redistribuye el tráfico a los servidores en función de una política de equilibrio de carga establecida en la pestaña Básica de la sección Servidores reales.

Creación de un nuevo servicio virtual utilizando un nuevo VIP



- Haga clic en el botón Añadir servicio virtual, como se ha indicado anteriormente.



- A continuación, entrará en el modo de **edición de filas**.
- Rellene los cuatro campos resaltados para proceder, y luego haga clic en el botón de actualización.

Utilice la tecla TAB para navegar por los campos.

Campo	Descripción
Dirección IP	Introduzca una nueva dirección IP virtual para que sea el punto de entrada de destino para acceder al Servidor Real. Esta IP es a la que apuntarán los usuarios o las aplicaciones para acceder a la aplicación con equilibrio de carga.
Máscara/Prefijo de subred	Este campo es para la máscara de subred correspondiente a la red en la que se encuentra el CAD
Puerto	El puerto de entrada utilizado cuando se accede al VIP. Este valor no tiene que ser necesariamente el mismo que el del Servidor Real si utiliza el Proxy Inverso.
Nombre del servicio	El nombre del servicio es una representación textual del propósito del VIP. Es opcional, pero le recomendamos que lo proporcione para mayor claridad.
Tipo de servicio	Hay muchos tipos de servicio disponibles para que usted los seleccione. Los tipos de servicio de capa 4 no pueden utilizar la tecnología flightPATH.

Ahora puede pulsar el botón Actualizar para guardar esta sección y saltar automáticamente a la sección Servidor Real que se detalla a continuación:

Campo	Descripción
Actividad	El campo Actividad puede utilizarse para mostrar y cambiar el estado del servidor real con equilibrio de carga. En línea - Denota que el servidor está activo y recibiendo peticiones de carga equilibrada Fuera de línea - El servidor está fuera de línea y no recibe peticiones Drenaje - El servidor se ha colocado en modo de drenaje para que la persistencia se pueda vaciar y el servidor pase a un estado fuera de línea sin afectar a los usuarios. Standby - El servidor ha sido puesto en estado de espera
Dirección IP	Este valor es la dirección IP del Servidor Real. Debe ser precisa y no debe ser una dirección DHCP.
Puerto	El puerto de acceso en el Real Server. Cuando se utiliza un proxy inverso, éste puede ser diferente del Puerto de entrada especificado en el VIP.
Ponderación	Este ajuste suele ser configurado automáticamente por el CAD. Puede modificarlo si desea cambiar la ponderación de la prioridad.

- Haga clic en el botón Actualizar o pulse Intro para guardar los cambios

- La luz de estado se pondrá primero en gris, seguida de verde si la comprobación del estado del servidor tiene éxito. Se volverá Roja si el Monitor del Servidor Real falla.
- Un servidor que tiene una luz de estado roja no será equilibrado en la carga.

Ejemplo de un servicio virtual completado

The screenshot shows two sections of the management interface. The top section, 'Virtual Services', contains a table with one entry:

Primary	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.1.222	255.255.255.0	80	TEST WEB RR	HTTP

The bottom section, 'Real Servers', shows a table with two entries:

Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
<input checked="" type="checkbox"/>	Online	192.168.1.200	80	100	100	Site 1	
<input checked="" type="checkbox"/>	Online	192.168.1.201	80	100	100	Site 2	

Crear un nuevo servicio virtual utilizando un VIP existente

- Resalte un servicio virtual que desee copiar
- Haga clic en Añadir servicio virtual para entrar en el modo de edición de filas

The screenshot shows the 'Virtual Services' interface with the 'TEST WEB RR' service selected. The 'Add Service' button is active, and the 'Update' and 'Cancel' buttons are visible below the table row.

Primary	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.1.222	255.255.255.0	80	TEST WEB RR	HTTP

- La dirección IP y la máscara de subred se copian automáticamente
- Introduzca el número de puerto de su servicio
- Introduzca un nombre de servicio opcional
- Seleccione un tipo de servicio
- Ahora puede pulsar el botón de actualización para guardar esta sección y saltar automáticamente a la sección del servidor real que aparece a continuación

The screenshot shows the 'Real Servers' interface with a new server entry being added. The 'Add Server' button is active, and the 'Update' and 'Cancel' buttons are visible below the table row.

Status	Activity	IP Address	Port	Weight	Calculated Weight	Notes
<input type="checkbox"/>	Online			100	100	

- Deje la opción de Actividad del servidor como Online - esto significa que se equilibrará la carga si pasa el monitor de salud por defecto de TCP Connect. Esta configuración puede cambiarse posteriormente si es necesario.
- Introduzca una dirección IP del Servidor Real
- Introduzca un número de puerto para el servidor real
- Introduzca un nombre opcional para el Servidor Real
- Haga clic en Actualizar para guardar los cambios
- La luz de estado se pondrá primero en gris y luego en verde si la comprobación del estado del servidor tiene éxito. Se volverá Roja si el Monitor del Servidor Real falla.
- Un servidor que tiene una luz de estado roja no se equilibrará la carga

Cambiar la dirección IP de un servicio virtual

Puede cambiar la dirección IP de un servicio virtual o VIP existente en cualquier momento.

- Resalte el Servicio Virtual cuya dirección IP desea cambiar

Primary	VIP Status	Service Status	Enabled	IP Address	SubNet Mask	Port	Service Name	Service Type
<input type="checkbox"/>			<input checked="" type="checkbox"/>	192.168.1.248	255.255.255.0	80	VIP1	HTTP
<input type="checkbox"/>			<input checked="" type="checkbox"/>	192.168.1.251	255.255.255.0	80	VS2	HTTP
<input type="checkbox"/>			<input checked="" type="checkbox"/>	192.168.1.253	255.255.255.0	80	VIP2	HTTP

- Haga doble clic en el campo de la dirección IP para ese servicio

Primary	VIP Status	Service Status	Enabled	IP Address	SubNet Mask	Port	Service Name	Service Type
<input type="checkbox"/>			<input checked="" type="checkbox"/>	192.168.1.248	255.255.255.0	80	VIP1	HTTP
<input type="checkbox"/>			<input checked="" type="checkbox"/>	192.168.1.251	255.255.255.0	80	VS2	HTTP
<input type="checkbox"/>			<input checked="" type="checkbox"/>	192.168.1.254	255.255.255.0	80	VIP2	HTTP

- Cambie la dirección IP por la que desea utilizar
- Pulse el botón Actualizar para guardar los cambios.

Primary	VIP Status	Service Status	Enabled	IP Address	SubNet Mask	Port	Service Name	Service Type
<input type="checkbox"/>			<input checked="" type="checkbox"/>	192.168.1.248	255.255.255.0	80	VIP1	HTTP
<input type="checkbox"/>			<input checked="" type="checkbox"/>	192.168.1.251	255.255.255.0	80	VS2	HTTP
<input type="checkbox"/>			<input checked="" type="checkbox"/>	192.168.1.254	255.255.255.0	80	VIP2	HTTP

Nota: El cambio de la dirección IP de un servicio virtual cambiará la dirección IP de todos los servicios asociados al VIP

Creación de un nuevo servicio virtual mediante el servicio de copia

- El botón Copiar Servicio copiará un servicio completo, incluyendo todos los Servidores Reales, los ajustes básicos, los ajustes avanzados y las reglas flightPATH asociadas a él
- Resalte el servicio que desea duplicar y haga clic en Copiar servicio
- El editor de filas aparecerá con el cursor parpadeante en la columna Dirección IP
- Debe cambiar la dirección IP para que sea única, o si desea mantener la dirección IP, debe editar el Puerto para que sea único para esa dirección IP

No olvide editar cada pestaña si cambia una configuración como la política de equilibrio de carga, el monitor de Real Server o elimina una regla flightPATH.

Filtrar los datos mostrados

Buscar un término específico

El cuadro de búsqueda le permite buscar en la tabla utilizando cualquier valor, como los octetos de la dirección IP o el nombre del servicio.

Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port
Stand-alone			<input checked="" type="checkbox"/>	10.4.8.191	255.255.255.0	80
			<input checked="" type="checkbox"/>	10.4.8.191	255.255.255.0	81
			<input checked="" type="checkbox"/>	10.4.8.191	255.255.255.0	82
			<input checked="" type="checkbox"/>	10.4.8.191	255.255.255.0	443

El ejemplo anterior muestra el resultado de la búsqueda de una dirección IP específica de 10.4.8.191.

Selección de la visibilidad de la columna

También puede seleccionar las columnas que desea mostrar en el tablero.

Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
	Online	192.168.1.200	80	<input checked="" type="checkbox"/>	100	Site 1	
	Online	192.168.1.201	80	<input checked="" type="checkbox"/>	100	Site 2	

- Mueva el ratón sobre cualquiera de las columnas
- Verá que aparece una pequeña flecha en el lado derecho de la columna
- Al hacer clic en las casillas de verificación, se seleccionan las columnas que desea ver en el tablero.

Comprensión de las columnas de servicios virtuales

Primario/Modo

La columna Primaria/Modo indica el rol de alta disponibilidad seleccionado para el VIP actual. Utilice las opciones disponibles en Sistema > Clustering para configurar esta opción.

Clustering

Role

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

Opción	Descripción
Cluster	El clúster es el papel por defecto del ADC en la instalación, y la columna Principal/Modo indicará el modo en el que se está ejecutando actualmente. Cuando

	tenga un par de ADC en HA en su centro de datos, uno de ellos mostrará Activo y el otro Pasivo
Manual	El rol Manual permite que el par ADC funcione en modo Activo-Activo para diferentes direcciones IP Virtuales. En estos casos, la columna Primaria contendrá una casilla junto a cada IP Virtual única que se puede marcar para Activo o dejar sin marcar para Pasivo.
Stand-Alone	El ADC está actuando como dispositivo autónomo y no está en modo de Alta Disponibilidad. Como tal, la columna Primaria indicará Stand-alone.

VIP

Esta columna proporciona información visual sobre el estado de cada servicio virtual. Los indicadores están codificados por colores y son los siguientes:

LED	Significado
	En línea
	Failover-Standby. Este servicio virtual es hot-standby
	Indica que un "secundario" está esperando a un "primario".
	El servicio necesita atención. Esta indicación puede ser el resultado de que un Servidor Real haya fallado en una comprobación del monitor de salud o haya sido cambiado manualmente a Desconectado. El tráfico seguirá fluyendo pero con una capacidad reducida del Servidor Real
	Fuera de línea. Los servidores de contenido son inalcanzables, o no hay servidores de contenido habilitados
	Encontrar el estado
	IPs virtuales no licenciadas o excedidas

Activado

El valor por defecto de esta opción es Activado, y la casilla de verificación aparece marcada. Puede desactivar el servicio virtual haciendo doble clic en la línea, desmarcando la casilla de verificación y haciendo clic en el botón Actualizar.

Dirección IP

Añada su dirección IPv4 en notación decimal con puntos o una dirección IPv6. Este valor es la dirección IP virtual (VIP) de su servicio. Ejemplo IPv4 "192.168.1.100". Ejemplo Ipv6 "2001:0db8:85a3:0000:0000:8a2e:0370:7334"

Máscara/Prefijo de subred

Añada su máscara de subred en notación decimal con puntos. Ejemplo: "255.255.255.0". O para IPv6, añade su prefijo. Para más información sobre IPv6, consulte

[HTTPS://EN.WIKIPEDIA.ORG/WIKI/IPV6_ADDRESS](https://en.wikipedia.org/wiki/IPv6_address)

Puerto

Añada el número de puerto asociado a su servicio. El puerto puede ser un número de puerto TCP o UDP. Ejemplo TCP "80" para el tráfico web y TCP "443" para el tráfico web seguro.

Nombre del servicio

Añada un nombre amigable para identificar su servicio. Ejemplo: "Servidores web de producción".

Tipo de servicio

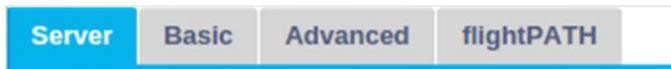
Tenga en cuenta que con todos los tipos de servicio de "Capa 4", el ADC no interactuará ni modificará el flujo de datos, por lo que flightPATH no está disponible con los tipos de servicio de Capa 4. Los servicios de capa 4 simplemente equilibran el tráfico según la política de equilibrio de carga:

Tipo de servicio	Puerto/Protocolo	Capa de servicio	Comentario
TCP de capa 4	Cualquier puerto TCP	Capa 4	El ADC no alterará ninguna información en el flujo de datos y realizará un equilibrio de carga estándar del tráfico de acuerdo con la política de equilibrio de carga
UDP de capa 4	Cualquier puerto UDP	Capa 4	Al igual que con el TCP de capa 4, el ADC no alterará ninguna información en el flujo de datos y realizará un equilibrio de carga estándar del tráfico según la política de equilibrio de carga
Capa 4 TCP/UDP	Cualquier puerto TCP o UDP	Capa 4	Es ideal si su servicio tiene un protocolo primario como el UDP, pero se retrocederá a TCP. El ADC no alterará ninguna información en el flujo de datos y realizará un equilibrio de carga estándar del tráfico de acuerdo con la política de equilibrio de carga
DNS	!!!		
HTTP	Protocolo HTTP o HTTPS	Capa 7	El CAD puede interactuar, manipular y modificar el flujo de datos utilizando flightPATH.
FTP	Protocolo de transferencia de archivos	Capa 7	Utilizar conexiones de control y de datos separadas entre el cliente y el servidor
SMTP	Protocolo simple de transferencia de correo	Capa 4	Utilizar cuando se equilibra la carga de los servidores de correo
POP3	Protocolo de la oficina de correos	Capa 4	Utilizar cuando se equilibra la carga de los servidores de correo
IMAP	Protocolo de acceso a mensajes de Internet	Capa 4	Utilizar cuando se equilibra la carga de los servidores de correo
RDP	Protocolo de escritorio remoto	Capa 4	Utilizar cuando se equilibra la carga de los servidores de Terminal Services
RPC	Llamada a procedimiento remoto	Capa 4	Utilizar cuando se equilibra la carga de los sistemas que utilizan llamadas RPC
RPC/ADS	RPC estática de Exchange 2010 para el servicio de libreta de direcciones	Capa 4	Utilizar cuando se equilibra la carga de los servidores Exchange

RPC/CA/PF	RPC estático de Exchange 2010 para el acceso de los clientes y las carpetas públicas	Capa 4	Utilizar cuando se equilibra la carga de los servidores Exchange
DICOM	Imagen digital y comunicaciones en medicina	Capa 4	Se utiliza cuando se equilibra la carga de los servidores que utilizan protocolos DICOM

Servidores reales

Hay varias pestañas en la sección de Servidores Reales del tablero: Servidor, Básico, Avanzado y FlightPATH.



Servidor

La pestaña Servidores contiene las definiciones de los servidores reales emparejados con el Servicio Virtual actualmente seleccionado. Es necesario añadir al menos un servidor a la sección de Servidores Reales.

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

Añadir servidor

- Seleccione el VIP apropiado que haya definido previamente.
- Haga clic en Añadir servidor
- Aparecerá una nueva fila con el cursor parpadeando en la columna Dirección IP

Online	<input type="text"/>	<input type="text"/>	100	100	
		Update		Cancel	

- Introduzca la dirección IPv4 de su servidor en notación decimal con puntos. El servidor real puede estar en la misma red que su servicio virtual, en cualquier red local directamente conectada o en cualquier red que su ADC pueda enrutar. Ejemplo: "10.1.1.1".
- Vaya a la columna Puerto e introduzca el número de puerto TCP/UDP de su servidor. El número de puerto puede ser el mismo que el del Servicio Virtual u otro número de puerto para la Conectividad de Proxy Inverso. El ADC traducirá automáticamente a este número.
- Vaya a la sección de Notas para añadir cualquier detalle relevante para el servidor. Ejemplo: "Servidor Web IIS 1"

Nombre del grupo



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

Cuando haya añadido los servidores que componen el conjunto de carga equilibrada, también puede adjuntarles un Nombre de grupo. Una vez que haya editado este campo, el contenido se guarda sin necesidad de pulsar el botón Actualizar.

Luces de estado del servidor real

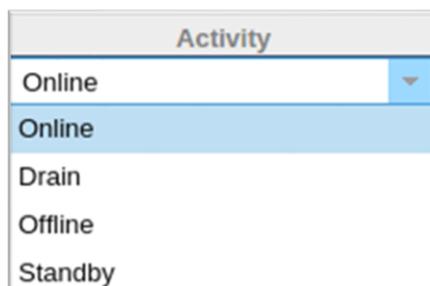
Puede ver el estado de un Servidor Real por el color de la luz en la columna de Estado. Véase más abajo:

LED Significado

- Conectado
- No se controla
- Drenaje
- Fuera de línea
- Standby
- No conectado
- Estado de los hallazgos
- Servidores reales sin licencia o con licencia superada

Actividad

Puede cambiar la actividad de un Servidor Real en cualquier momento utilizando el menú desplegable. Para ello, haga doble clic en una fila del Servidor Real para ponerla en modo de edición.



Opción	Descripción
En línea	Todos los Servidores Reales asignados en línea recibirán el tráfico de acuerdo con la política de equilibrio de carga establecida en la pestaña Básica.
Drenaje	Todos los Servidores Reales asignados como Drenaje continuarán sirviendo a las conexiones existentes pero no aceptarán ninguna conexión nueva. La luz de Estado parpadeará en verde/azul mientras el drenaje esté en proceso. Una vez que las conexiones existentes se hayan cerrado de forma natural, los Servidores Reales se desconectarán y la luz de Estado será de color azul sólido. También puede ver estas conexiones navegando a la sección Navegación > Monitor > Estado.
Fuera de línea	Todos los Servidores Reales configurados como Desconectados serán inmediatamente desconectados y no recibirán ningún tráfico.
Standby	Todos los servidores reales configurados como Standby permanecerán desconectados hasta que TODOS los servidores del grupo Online fallen en sus comprobaciones de Server Health Monitor. El tráfico será recibido por el grupo en espera según la política de equilibrio de carga cuando esto ocurra. Si un servidor del grupo Online pasa la comprobación del Monitor de Salud del Servidor, este servidor Online recibirá todo el tráfico, y el grupo Standby dejará de recibir tráfico.

Dirección IP

Este campo es la dirección IP de su Servidor Real. Ejemplo "192.168.1.200".

Puerto

Número de puerto TCP o UDP en el que el Servidor Real está escuchando para el servicio. Ejemplo "80" para el tráfico web.

Peso

Esta columna será editable cuando haya una política de equilibrio de carga apropiada especificada.

El peso por defecto para un servidor real es 100, y puede introducir valores de 1 a 100. Un valor de 100 significa carga máxima, y 1 significa carga mínima.

Un ejemplo para tres servidores puede ser algo así:

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

Si consideramos que la política de equilibrio de carga está configurada en Conexiones mínimas, y hay un total de 200 conexiones de clientes;

- El servidor 1 recibirá 100 conexiones simultáneas
- El servidor 2 recibirá 50 conexiones simultáneas
- El servidor 3 recibirá 50 conexiones simultáneas

Si utilizáramos Round Robin como método de equilibrio de la carga, que hace rotar las peticiones a través del conjunto de servidores de carga equilibrada, la alteración de los pesos afecta a la frecuencia con la que los servidores son elegidos como objetivo.

Si creemos que la política de equilibrio de carga más rápida utiliza el tiempo más corto que se tarda en OBTENER una respuesta, el ajuste de las ponderaciones altera el sesgo de forma similar al de las conexiones mínimas.

Peso calculado

El peso calculado de cada servidor puede verse dinámicamente y se calcula automáticamente y no es editable. El campo muestra la ponderación real que el CAD está utilizando al considerar la ponderación manual y la política de equilibrio de carga.

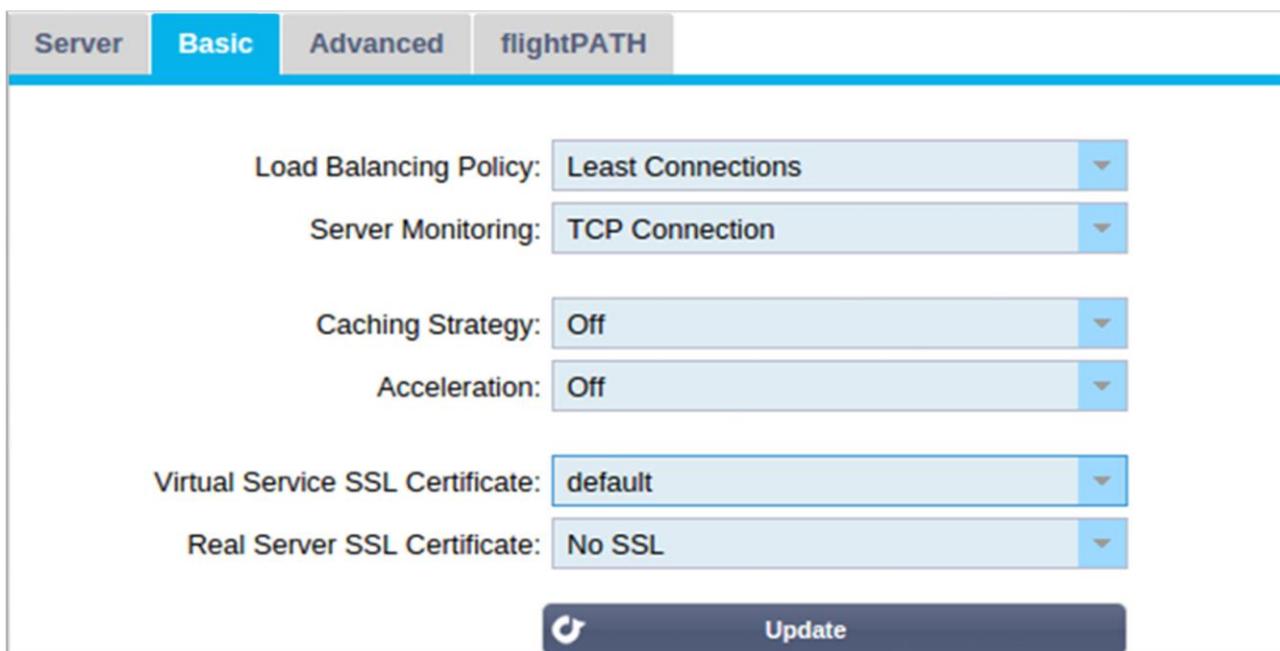
Notas

Introduzca cualquier nota particular que sea útil para describir la entrada definida en el campo Notas. Ejemplo "Servidor IIS1 - DC de Londres".

ID

El campo ID se utiliza dentro de la política de balanceo de carga del ID de la cookie. El número de ID colocado aquí se utiliza para identificar

Básico



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

Política de equilibrio de carga

La lista desplegable le muestra las políticas de equilibrio de carga actualmente soportadas y disponibles para su uso. A continuación encontrará una lista de políticas de equilibrio de carga, junto con una explicación.

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

Opción	Descripción
Más rápido	La política de equilibrio de carga más rápida calcula automáticamente el tiempo de respuesta de todas las solicitudes por servidor suavizado en el tiempo. La columna Peso calculado contiene el valor calculado automáticamente. La introducción manual sólo es posible cuando se utiliza esta política de equilibrio de carga.
Round Robin	El Round Robin se utiliza habitualmente en los cortafuegos y en los equilibradores de carga básicos y es el método más sencillo. Cada servidor real recibe una nueva petición en secuencia. Este método sólo es adecuado cuando se necesita equilibrar la carga de las peticiones a los servidores de manera uniforme; un ejemplo serían los servidores web de búsqueda. Sin embargo, cuando necesita equilibrar la carga en función de la carga de la aplicación o del servidor, o incluso asegurarse de que utiliza el mismo servidor para la sesión, el método Round Robin es inadecuado.
Conexiones mínimas	El equilibrador de carga llevará la cuenta del número de conexiones actuales a cada Servidor Real. El Servidor Real con la menor cantidad de conexiones recibe la nueva solicitud posterior.
Afinidad/Persistencia de la Sesión de Capa 3 - Vinculado a IP	En este modo, la dirección IP del cliente constituye la base para seleccionar qué servidor real recibirá la solicitud. Esta acción proporciona persistencia. Los protocolos HTTP y de capa 4 pueden utilizar este modo. Este método es útil para las redes internas en las que se conoce la topología de la red y se puede confiar en que no hay "superproxies" aguas arriba. Con la capa 4 y los proxies, todas las peticiones pueden parecer que proceden de un solo cliente y, por tanto, la carga no sería uniforme. Con HTTP, la información de la cabecera (X-Forwarder-For) se utiliza cuando está presente para hacer frente a los proxies.

Afinidad/Persistencia de la Sesión de Capa 3 - Basada en la lista de IP	La conexión con el Servidor Real se inicia utilizando "Conexiones mínimas" entonces, la afinidad de la sesión se logra en base a la dirección IP del cliente. Se mantiene una lista durante 2 horas por defecto, pero esto puede cambiarse mediante un jetPACK.
Capa 7 Afinidad/Persistencia de la sesión - Cookie de sesión	Este modo es el método de persistencia más popular para el equilibrio de carga HTTP. En este modo, el ADC utiliza el equilibrio de carga basado en listas de IP para cada primera solicitud. Inserta una cookie en las cabeceras de la primera respuesta HTTP. Después, el ADC utiliza la cookie del cliente para enrutar el tráfico al mismo servidor back-end. Esta cookie se utiliza para la persistencia cuando el cliente necesita ir al mismo servidor back-end cada vez. La cookie expira una vez que se cierra la sesión.
Capa 7 Afinidad/Persistencia de la sesión - Cookie persistente	El modo de equilibrio de carga basado en la lista IP se utiliza para cada primera solicitud. El ADC inserta una cookie en las cabeceras de la primera respuesta HTTP. Después, el ADC utiliza la cookie del cliente para dirigir el tráfico al mismo servidor back-end. Esta cookie se utiliza para la persistencia cuando el cliente debe ir al mismo servidor back-end cada vez. La cookie expirará después de 2 horas, y la conexión se equilibrará en carga según un algoritmo basado en la lista de IP. Este tiempo de expiración es configurable mediante un jetPACK.
Cookie de sesión - Cookie de sesión ASP clásica	Las páginas activas del servidor (ASP) son una tecnología del lado del servidor de Microsoft. Con esta opción seleccionada, el ADC mantendrá la persistencia de la sesión en el mismo servidor si se detecta una cookie ASP y se encuentra en su lista de cookies conocidas. Al detectar una nueva cookie ASP, se equilibrará la carga utilizando el algoritmo de conexiones mínimas.
Cookie de sesión - Cookie de sesión ASP.NET	Este modo se aplica a ASP.net . Con este modo seleccionado, el ADC mantendrá la persistencia de la sesión en el mismo servidor si se detecta una cookie ASP.NET y se encuentra en su lista de cookies conocidas. Al detectar una nueva cookie de ASP, se equilibrará la carga utilizando el algoritmo de conexiones mínimas.
Cookie de sesión - Cookie de sesión JSP	Java Server Pages (JSP) es una tecnología del lado del servidor de Oracle. Con este modo seleccionado, el ADC mantendrá la persistencia de la sesión en el mismo servidor si se detecta una cookie JSP y se encuentra en su lista de cookies conocidas. Al detectar una nueva cookie JSP, se equilibrará la carga utilizando el algoritmo de conexiones mínimas.
Cookie de sesión - Cookie de sesión JAX-WS	Los servicios web de Java (JAX-WS) son una tecnología del lado del servidor de Oracle. Con este modo seleccionado, el ADC mantendrá la persistencia de la sesión en el mismo servidor si se detecta una cookie JAX-WS y se encuentra en su lista de cookies conocidas. Al detectar una nueva cookie JAX-WS, se equilibrará la carga utilizando el algoritmo de conexiones mínimas.
Cookie de sesión - Cookie de sesión PHP	La página personal (PHP) es una tecnología del lado del servidor de código abierto. Con este modo seleccionado, el CAD mantendrá la persistencia de la sesión en el mismo servidor cuando se detecte una cookie de PHP.
Cookie de sesión - Persistencia de la cookie RDP	Este método de equilibrio de carga utiliza la cookie RDP creada por Microsoft y basada en el nombre de usuario/dominio para proporcionar persistencia a un servidor. La ventaja de este método es que el mantenimiento de la conexión a un servidor es posible incluso si la dirección IP del cliente cambia.

Basado en cookies

Un nuevo método muy parecido a "PhpCookieBased" y otros métodos de equilibrio de carga, pero utilizando CookieIDBased y cookie RegEx `h=[^;]+`

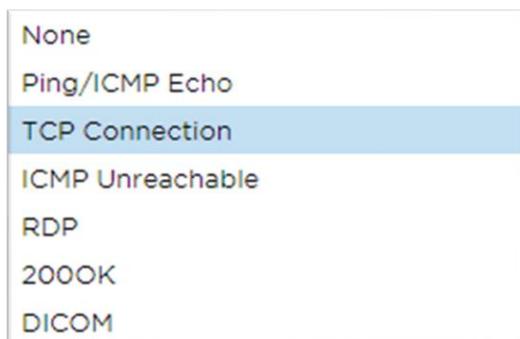
Este método utilizará el valor establecido en el campo de notas del servidor real "ID=X;" como valor de la cookie para identificar el servidor. Esto, por lo tanto, significa que es una metodología similar a CookieListBased pero utiliza un nombre de cookie diferente y almacena un valor de cookie único, no la IP codificada, sino el ID del Servidor Real (leído en el momento de la carga).

El valor por defecto es `CookieIDName="h"`; sin embargo, si existe un valor de anulación en la configuración de los ajustes avanzados del servidor virtual, utilícelo en su lugar. **NOTA:** Si se establece este valor, sobrescribimos la expresión de la cookie anterior para sustituir `h=` por el nuevo valor.

La última parte es que si llega un valor de cookie desconocido y coincide con uno de los ID del servidor real, debe seleccionar ese servidor; de lo contrario, utilice el siguiente método (delegado.)

Monitorización de servidores

Su ADC contiene seis métodos estándar de supervisión de servidores reales que se enumeran a continuación.



Elija el método de supervisión que desea aplicar al servicio virtual (VIP).

Es esencial elegir el monitor adecuado para el servicio. Por ejemplo, si el Servidor Real es un servidor RDP, un monitor 200OK no es relevante. Si no está seguro de qué monitor elegir, la Conexión TCP por defecto es un excelente punto de partida.

Puede elegir varios monitores haciendo clic en cada uno de los monitores que desee aplicar al servicio sucesivamente. Los monitores seleccionados se ejecutan en el orden en que los seleccione; por lo tanto, comience con los monitores de las capas inferiores primero. Por ejemplo, la configuración de los monitores Ping/ICMP Echo, Conexión TCP y 200OK se mostrará en el Panel de Eventos como en la imagen siguiente:

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

Podemos ver que el ping de la capa 3 y la conexión TCP de la capa 4 han tenido éxito si nos fijamos en la línea superior, pero el 200OK de la capa 7 ha fallado. Estos resultados de la monitorización proporcionan suficiente información para indicar que el enrutamiento está bien y que hay un servicio

que se ejecuta en el puerto correspondiente, pero el sitio web no está respondiendo correctamente a la página solicitada. Ahora es el momento de mirar el servidor web y la sección Biblioteca > Monitor del servidor real para ver los detalles del monitor que falla.

Opción	Descripción
Ninguno	En este modo, el Servidor Real no se monitoriza y siempre está funcionando correctamente. El ajuste Ninguno es útil para situaciones en las que la monitorización trastorna un servidor y para servicios que no deben unirse a la acción de conmutación por error del ADC. Es una vía para alojar sistemas poco fiables o heredados que no son primarios para las operaciones del H/A. Utilice este método de monitorización con cualquier tipo de servicio.
Eco Ping/ICMP	En este modo, el CAD envía una solicitud de eco ICMP a la IP del servidor de contenidos. Si se recibe una respuesta eco válida, el ADC considera que el servidor real está en funcionamiento y el tráfico hacia el servidor continúa. También mantendrá el servicio disponible en un par H/A. Este método de monitorización se puede utilizar con cualquier tipo de servicio.
Conexión TCP	En este modo, se establece una conexión TCP con el Servidor Real y se interrumpe inmediatamente sin enviar ningún dato. Si la conexión tiene éxito, el CAD considera que el Servidor Real está en funcionamiento. Este método de monitorización se puede utilizar con cualquier tipo de servicio. Los servicios UDP son los únicos que actualmente no son apropiados para la monitorización de la conexión TCP.
ICMP inalcanzable	El ADC enviará una comprobación de salud UDP al servidor y marcará el Servidor Real como no disponible si recibe un mensaje ICMP de puerto inalcanzable. Este método puede ser útil cuando necesite comprobar si un puerto de servicio UDP está disponible en un servidor, como el puerto DNS 53.
RDP	En este modo, una conexión TCP se inicializa como se explica en el método ICMP Unreachable. Después de que la conexión se inicialice, se solicita una conexión RDP de capa 7. Si se confirma la conexión, el ADC considera que el Servidor Real está en funcionamiento. Este método de monitorización se puede utilizar con cualquier servidor de terminales de Microsoft.
200 OK	En este método, se inicializa una conexión TCP con el Servidor Real. Una vez que la conexión tiene éxito, el CAD envía al Servidor Real una solicitud HTTP. Se espera una respuesta HTTP y se comprueba el código de respuesta "200 OK". Si se recibe el código de respuesta "200 OK", el CAD considera que el Servidor Real está en funcionamiento. Si el CAD no recibe un código de respuesta "200 OK" por cualquier motivo, incluidos los tiempos de espera, los fallos de conexión y otras razones, el CAD marca el Servidor Real como no disponible. Este método de monitorización sólo es válido para su uso con los tipos de servicio HTTP y HTTP acelerado. Si un tipo de servicio de capa 4 está en uso para un servidor HTTP, es utilizable si SSL no está en uso en el Servidor Real o es manejado apropiadamente por la facilidad "Content SSL".
DICOM	Una conexión TCP se inicializa con el Servidor Real en modo DICOM, y se realiza una "Solicitud de Asociación" de Echoscú al Servidor Real en la conexión. Una conversación que incluye una "Associate Accept" del servidor de contenidos, una transferencia de una pequeña cantidad de datos seguida de una "Release Request", y luego una "Release Response" concluye con éxito el monitor. Si, por cualquier motivo, el monitor no concluye con éxito, se considera que el Servidor Real no funciona.
Definido por el usuario	Cualquier monitor configurado en la sección de Monitorización del Servidor Real aparecerá en la lista.

Estrategia de almacenamiento en caché

Por defecto, la Estrategia de Almacenamiento en Caché está desactivada y configurada como Desactivada. Si su tipo de servicio es HTTP, entonces puede aplicar dos tipos de Estrategia de Caché.

Off
By Host
By Virtual Service

Consulte la página Configurar caché para configurar los ajustes detallados de la caché. Tenga en cuenta que cuando el almacenamiento en caché se aplica a un VIP con el tipo de servicio "HTTP" acelerado, los objetos comprimidos no se almacenan en caché.

Opción	Descripción
Por el anfitrión	El almacenamiento en caché por host se basa en la aplicación por nombre de host. Existirá una caché separada para cada dominio/nombre de host. Este modo es ideal para los servidores web que pueden servir varios sitios web en función del dominio.
Por Servicio Virtual	El almacenamiento en caché por servicio virtual está disponible cuando se elige esta opción. Sólo existirá un Caché para todos los dominios/hostnames que pasen por el servicio virtual. Esta opción es una configuración especializada para su uso con múltiples clones de un mismo sitio.

Aceleración

Opción	Descripción
Off	Desactivar la compresión para el servicio virtual
Compresión	Cuando se selecciona, esta opción activa la compresión para el Servicio Virtual seleccionado. El CAD comprime dinámicamente el flujo de datos al cliente cuando lo solicita. Este proceso sólo se aplica a los objetos que contienen la cabecera content-encoding: gzip. Algunos ejemplos de contenido son HTML, CSS o Javascript. También puede excluir ciertos tipos de contenido utilizando la sección de Exclusiones Globales.

Nota: Si el objeto es almacenable en caché, el CAD almacenará una versión comprimida y la servirá estáticamente (desde la memoria) hasta que el contenido caduque y se vuelva a validar.

Certificado SSL de servicio virtual (cifrado entre el cliente y el CAD)

Por defecto, la configuración es Sin SSL. Si su tipo de servicio es "HTTP" o "TCP de capa 4", puede seleccionar un certificado del desplegable para aplicarlo al servicio virtual. Los certificados que se hayan creado o importado aparecerán en esta lista. Puede resaltar varios certificados para aplicarlos a un servicio. Esta operación habilitará automáticamente la extensión SNI para permitir un certificado basado en el "Nombre de dominio" solicitado por el cliente.

Indicación del nombre del servidor

Esta opción es una extensión del protocolo de red TLS mediante la cual el cliente indica a qué nombre de host intenta conectarse al inicio del proceso de handshaking. Este ajuste permite al ADC presentar varios certificados en la misma dirección IP virtual y puerto TCP.

No SSL
All
default
AnyUseCert

Opción	Descripción
Sin SSL	El tráfico de la fuente al ADC no está encriptado.
Todo	Carga todos los certificados disponibles para su uso
Por defecto	Esta opción hace que se aplique un certificado creado localmente llamado "Default" al lado del navegador del canal. Utilice esta opción para probar el SSL cuando no se haya creado o importado uno.
AnyUseCert	Utilizar cualquier certificado presente en el CAD que el usuario haya cargado o generado

Certificado SSL del Servidor Real (Encriptación entre el CAD y el Servidor Real)

El valor por defecto de esta opción es Sin SSL. Si su servidor requiere una conexión encriptada, este valor debe ser cualquier cosa que no sea Sin SSL. Los certificados que se hayan creado o importado aparecerán en esta lista.

No SSL
Any
SNI
default
AnyUseCert

Opción	Descripción
Sin SSL	El tráfico desde el CAD al Servidor Real no está encriptado. La selección de un certificado en el lado del navegador significa que "No SSL" puede ser elegido en el lado del cliente para proporcionar lo que se conoce como "SSL Offload".
Cualquier	El CAD actúa como cliente y aceptará cualquier certificado que el Servidor Real presente. El tráfico del ADC al Servidor Real se encripta cuando se selecciona esta opción. Utilice la opción "Cualquiera" cuando se especifique un certificado en el lado del Servicio Virtual, proporcionando lo que se conoce como "Puente SSL" o "Reencriptación SSL".
SNI	El CAD actúa como cliente y aceptará cualquier certificado que el Servidor Real presente. El tráfico del ADC al Servidor Real se encripta si se selecciona esta opción. Utilice la opción "Cualquiera" cuando se especifique un certificado en el lado del Servicio Virtual, proporcionando lo que se conoce como "Puente SSL" o "Reencriptación SSL". Elija esta opción para habilitar el SNI en el lado del servidor.
AnyUseCert	Aquí aparecen los certificados que haya generado o importado en el CAD.

Avanzado

Real Servers

Server

Basic

Advanced

flightPATH

Connectivity:	Reverse Proxy	Connection Timeout (sec):	600
Cipher Options:	Defaults	Monitoring Interval (sec):	1
Client SSL Renegotiation:	<input checked="" type="checkbox"/>	Monitoring Timeout (sec):	10
Client SSL Resumption:	<input checked="" type="checkbox"/>	Monitoring In Count:	2
SNI Default Certificate:	None	Monitoring Out Count:	3
Security Log:	On	Max. Connections (Per Real Server):	

Conectividad

Su servicio virtual se puede configurar con cuatro tipos diferentes de conectividad. Seleccione el modo de conectividad que desea aplicar al servicio.

Opción	Descripción
Proxy inverso	El Proxy Inverso es el valor por defecto y funciona en la Capa7 con compresión y caché. Y en la Capa4 sin caché ni compresión. En este modo, su ADC actúa como proxy inverso y se convierte en la dirección de origen que ven los servidores reales.
Retorno directo del servidor	El Retorno Directo al Servidor o DSR, como es ampliamente conocido (DR - Enrutamiento Directo en algunos círculos) permite que el servidor detrás del equilibrador de carga responda directamente al cliente saltándose el ADC en la respuesta. DSR sólo es adecuado para su uso con el equilibrador de carga de capa 4. Por lo tanto, el almacenamiento en caché y la compresión no están disponibles con esta opción elegida. El equilibrio de carga de capa 7 no funciona con este DSR. Además, no hay soporte de persistencia que no sea el basado en la lista de IP. El equilibrio de carga SSL/TLS con este método no es ideal ya que el soporte de persistencia de IP de origen es el único tipo disponible. El DSR también requiere que se realicen cambios en el Servidor Real. Por favor, consulte la sección de Cambios en el Servidor Real.
Puerta de enlace	El modo de puerta de enlace le permite enrutar todo el tráfico a través del ADC, permitiendo que el tráfico de los Servidores Reales sea enrutado a través del ADC a otras redes mediante las máquinas virtuales del ADC o las interfaces de hardware. El uso del dispositivo como puerta de enlace para los Servidores Reales es ideal cuando se ejecuta en modo multi-interfaz. El equilibrio de carga de la capa 7 con este método no funciona ya que no hay soporte de persistencia más que el basado en la lista IP. Este método requiere que el Servidor Real establezca su puerta de enlace por defecto en la dirección de la interfaz local (eth0, eth1, etc.) del CAD. Consulte la sección de cambios del Servidor Real. Tenga en cuenta que el modo Gateway no admite la conmutación por error en un entorno de clúster.

Opciones de cifrado

Puede establecer cifrados a nivel de cada servicio, y sólo es relevante para los servicios con SSL/TLS activado. El ADC realiza la elección automática del cifrado, y usted puede añadir diferentes cifrados

mediante jetPACKS. Al añadir el jetPACK apropiado, puede establecer las opciones de cifrado por servicio. La ventaja de esto es que puede crear varios servicios con diferentes niveles de seguridad. Tenga en cuenta que los clientes más antiguos no son compatibles con los cifrados más nuevos para reducir el número de clientes cuanto más seguro sea el servicio.

Renegociación SSL del cliente

Marque esta casilla si desea permitir la renegociación SSL iniciada por el cliente. Desactive la renegociación SSL iniciada por el cliente para evitar posibles ataques DDOS contra la capa SSL desmarcando esta opción.

Reanudación del SSL del cliente

Marque esta casilla si desea habilitar las sesiones del servidor de reutilización SSL añadidas a la caché de sesiones. Cuando un cliente propone la reutilización de una sesión, el servidor intentará reutilizar la sesión si la encuentra. Si la reanudación está desmarcada, no se produce ningún almacenamiento en caché de la sesión para el cliente o el servidor.

Certificado por defecto SNI

Durante una conexión SSL con la SNI del lado del cliente activada, si el dominio solicitado no coincide con ninguno de los certificados asignados al servicio, el ADC presentará el certificado predeterminado de la SNI. El ajuste por defecto para esto es Ninguno, lo que haría que la conexión se cayera en caso de que no hubiera una coincidencia exacta. Elija cualquiera de los certificados instalados en el desplegable para presentarlo en caso de que falle una coincidencia exacta del certificado SSL.

Registro de seguridad

'Activado' es el valor por defecto y es en base a cada servicio, habilitando el servicio de registro de información de autenticación a los registros del W3C. Si hace clic en el icono del engranaje, accederá a la página Sistema > Registro, donde podrá comprobar la configuración del registro del W3C.

Tiempo de espera de la conexión

El tiempo de espera de la conexión por defecto es de 600 segundos o 10 minutos. Esta configuración ajustará el tiempo de espera de la conexión cuando no haya actividad. Reduzca esta cifra para el tráfico web sin estado de corta duración, que suele ser de 90 o menos. Aumente esta cifra para las conexiones con estado, como el RDP, a algo así como 7200 segundos (2 horas) o más, dependiendo de su infraestructura. El ejemplo del tiempo de espera del RDP significa que si un usuario tiene un periodo de inactividad de 2 horas o menos, las conexiones permanecerán abiertas.

Configuración de la monitorización

Estos ajustes están relacionados con los monitores del servidor real en la pestaña básica. Hay entradas globales en la configuración para contar el número de monitores exitosos o fallidos antes de que el estado de un servidor se marque como conectado o fallido.

Intervalo

El intervalo es el tiempo en segundos entre monitores. El intervalo por defecto es de 1 segundo. Aunque 1s es aceptable para la mayoría de las aplicaciones, puede ser beneficioso aumentarlo para otras o durante las pruebas.

Tiempo de espera de monitorización

El valor del tiempo de espera es el tiempo que el ADC esperará a que un servidor responda a una solicitud de conexión. El valor por defecto es de 2s. Aumente este valor para servidores ocupados.

Seguimiento en el recuento

El valor por defecto de este ajuste es 2. El valor de 2 indica que el Servidor Real debe pasar dos comprobaciones exitosas del monitor de salud antes de entrar en servicio. Si se aumenta esta cifra, aumentará la probabilidad de que el servidor pueda servir tráfico, pero tardará más en entrar en servicio en función del intervalo. Disminuir este valor hará que el servidor entre en servicio antes.

Control del recuento de salidas

El valor por defecto de este ajuste es 3, lo que significa que el monitor del Servidor Real debe fallar tres veces antes de que el ADC deje de enviar tráfico al servidor, y se marque como ROJO e Inalcanzable. Si se aumenta esta cifra se obtendrá un servicio mejor y más fiable a costa del tiempo que tarda el CAD en dejar de enviar tráfico a este servidor.

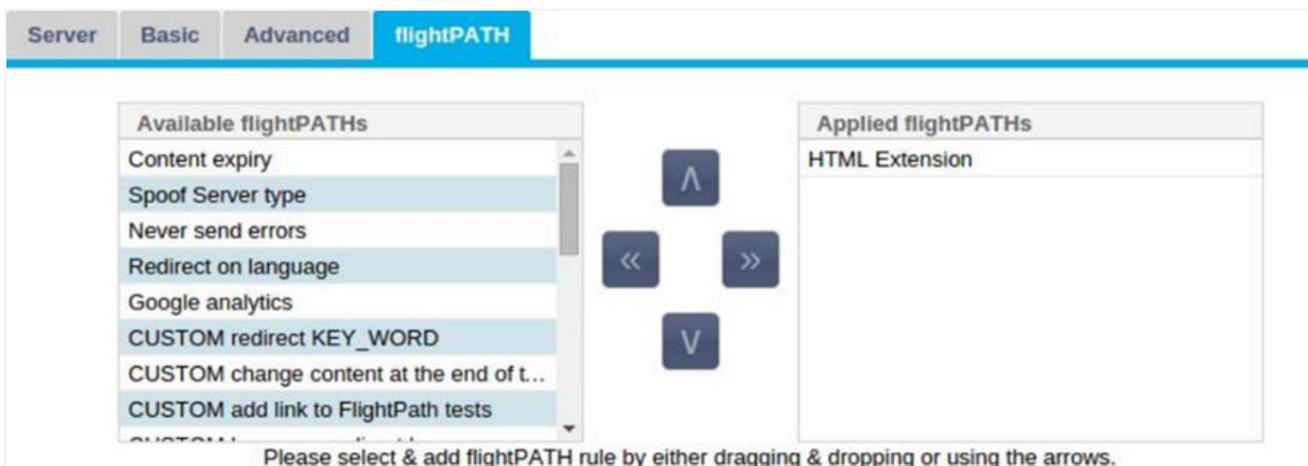
Cambiar a offline en caso de fallo

Cuando esto está marcado, los Servidores Reales que fallan en su chequeo de salud son puestos fuera de línea y sólo pueden ser puestos en línea manualmente.

Max. Conexiones

Limita el número de conexiones simultáneas del Servidor Real y se configura por servicio. Por ejemplo, si lo configura en 1000 y tiene dos Servidores Reales, el ADC limita **cada Servidor Real** a 1000 conexiones simultáneas. También puede optar por presentar una página de "Servidor demasiado ocupado" una vez que se alcance este límite en todos los servidores, ayudando a los usuarios a entender por qué se ha producido una falta de respuesta o un retraso. Deje esto en blanco para conexiones ilimitadas. Lo que establezca aquí depende de los recursos de su sistema.

flightPATH



flightPATH es un sistema diseñado por Edgenexus y disponible exclusivamente en el CAD. A diferencia de los motores basados en reglas de otros proveedores, flightPATH no funciona a través de una línea de comandos o una consola de entrada de scripts. En su lugar, utiliza una interfaz gráfica de usuario para seleccionar los diferentes parámetros, condiciones y acciones a realizar para conseguir lo que necesitan. Estas características hacen que flightPATH sea extremadamente potente y permite a los administradores de la red manipular el tráfico HTTPS de forma muy eficaz.

flightPATH sólo está disponible para su uso con conexiones HTTPS, y esta sección no es visible cuando el tipo de servicio virtual no es HTTP.

Puede ver en la imagen de arriba; hay una lista de reglas disponibles a la izquierda y las reglas aplicadas al servicio virtual a la derecha.

Añada una regla disponible arrastrando y soltando la regla del lado izquierdo al derecho o resaltando una regla y haciendo clic en la flecha derecha para moverla al lado derecho.

El orden de ejecución es esencial y comienza con la regla superior ejecutada primero. Para cambiar el orden de ejecución, resalte la regla y muévase hacia arriba y hacia abajo con las flechas.

Para eliminar una regla, arrástrala y suéltela de nuevo en el inventario de reglas de la izquierda o resalte la regla y haga clic en la flecha de la izquierda.

Puede añadir, eliminar y editar reglas flightPATH en la sección Configurar flightPATH de esta guía.

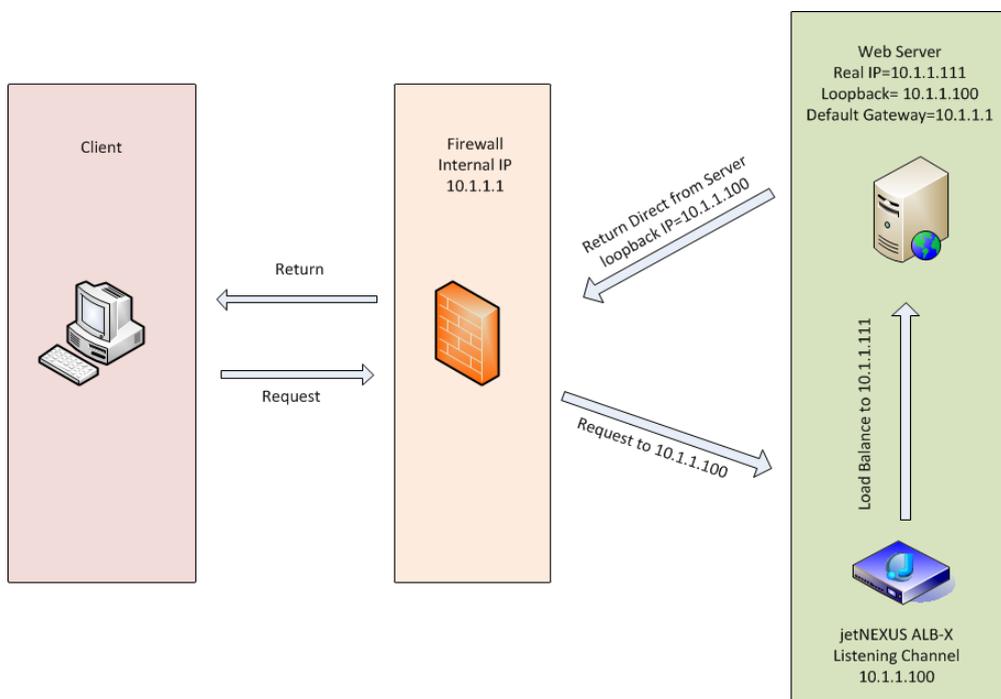
Cambios en el servidor real para el retorno del servidor directo

El Retorno Directo al Servidor o DSR, como es ampliamente conocido (DR - Enrutamiento Directo en algunos círculos) permite que el servidor detrás del ADC responda directamente al cliente, saltándose el ADC en la respuesta. El DSR sólo es adecuado para su uso con el equilibrio de carga de capa 4. El caché y la compresión no están disponibles cuando se activan.

El equilibrio de carga de la capa 7 con este método no funcionará ya que no hay soporte de persistencia más que la IP de origen. El equilibrio de carga SSL/TLS con este método no es ideal ya que sólo hay soporte de persistencia de la IP de origen.

Cómo funciona

- El cliente envía una solicitud al jetNEXUS ALB-X
- Solicitud recibida por edgeNEXUS
- Petición dirigida a los servidores de contenido
- Respuesta enviada directamente al cliente sin pasar por edgeNEXUS



Configuración necesaria del servidor de contenidos

General

- La puerta de enlace por defecto del servidor de contenidos debe configurarse de forma normal. (No a través del CAD)
- El servidor de contenidos y el equilibrador de carga deben estar en la misma subred

Windows

- El servidor de contenidos necesita tener un loopback o Alias configurado con la dirección IP del Canal o VIP
 - La métrica de la red debe ser 254 para evitar la respuesta a las solicitudes ARP
 - Añadir un adaptador de bucle de retorno en Windows Server 2012 - [Haga clic aquí](#)
 - Añadir un adaptador de bucle de retorno en Windows Server 2003/2008 - [Haga clic aquí](#)
- Ejecute lo siguiente en un símbolo del sistema para cada interfaz de red que haya configurado en los servidores Windows Real

```
netsh interface ipv4 set interface "Nombre de la interfaz de red de Windows"
weakhostreceive=enable
```

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

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

Linux

- Añadir una interfaz de bucle invertido permanente
- Edite "/etc/sysconfig/network-scripts"

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

- Edite "/etc/sysctl.conf"

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

- Ejecute "sysctl - p"

Cambios en el servidor real - Modo de puerta de enlace

El modo de pasarela le permite enrutar todo el tráfico a través del ADC, y esto permite que el tráfico que se origina en los servidores de contenido se enrute a través del ADC a otras redes mediante las interfaces de la unidad ADC. El uso del dispositivo como puerta de enlace para los servidores de contenido debe utilizarse cuando se ejecuta en el modo de múltiples interfaces.

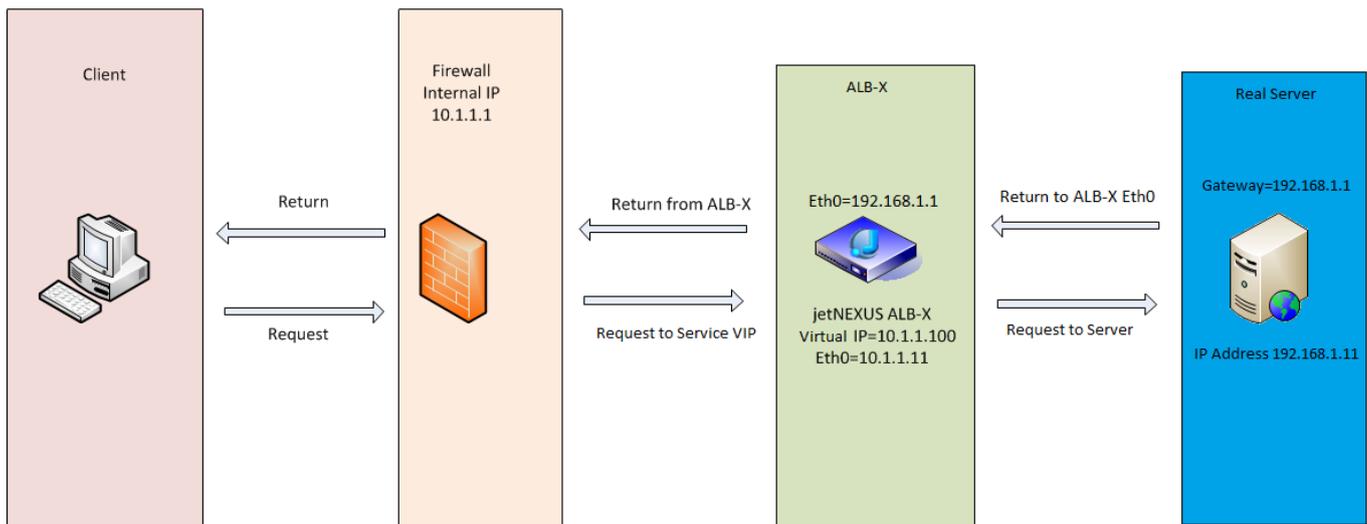
Cómo funciona

- El cliente envía una solicitud al jetNEXUS ALB-X
- El edgeNEXUS recibe una solicitud
- Solicitud enviada a los servidores de contenido
- Respuesta enviada a edgeNEXUS
- El CAD dirige la respuesta al cliente

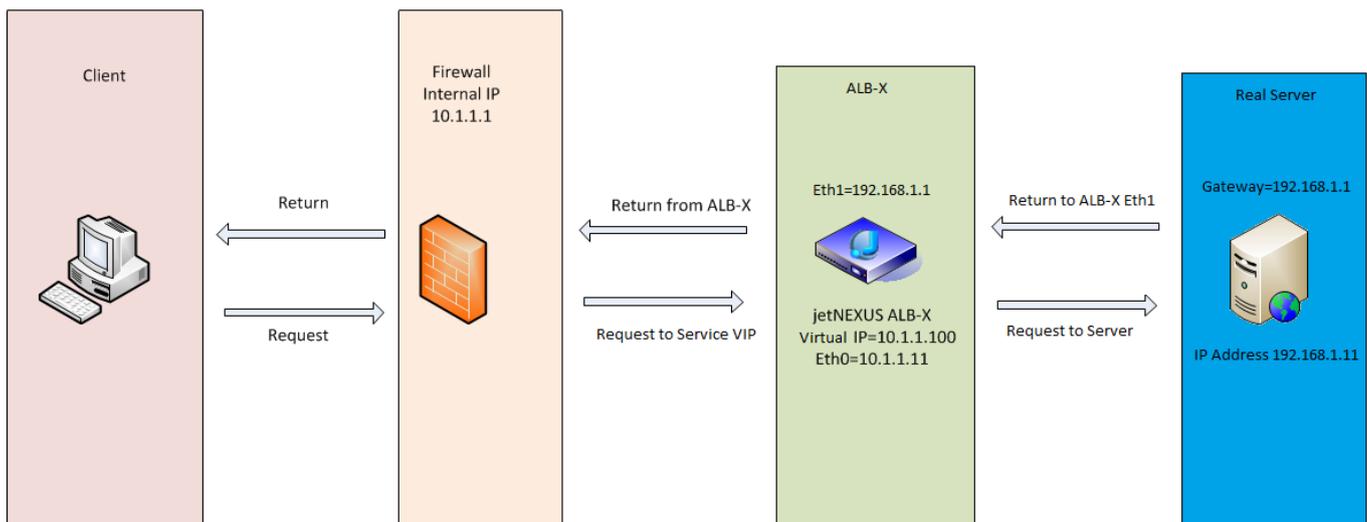
Configuración necesaria del servidor de contenidos

- Modo de brazo único: se utiliza una interfaz, pero el servicio VIP y los servidores reales deben estar en subredes diferentes.
- Modo de doble brazo: se utilizan dos interfaces, pero el servicio VIP y los servidores reales deben estar en subredes diferentes.
- En cada caso, de brazo simple y doble, los servidores reales deben configurar su puerta de enlace por defecto a la dirección de la interfaz del CAD en la subred correspondiente.

Ejemplo de brazo único



Ejemplo de brazo doble



Biblioteca

Complementos

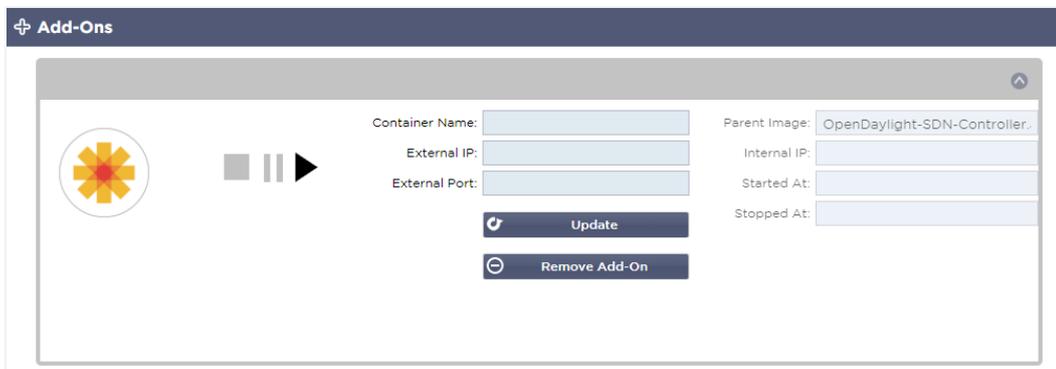
Los complementos son contenedores basados en Docker que pueden ejecutarse en modo aislado dentro del ADC. Ejemplos de complementos podrían ser un cortafuegos de aplicaciones o incluso una microinstancia del propio ADC.

Aplicaciones

La sección de aplicaciones dentro de los complementos detalla las aplicaciones que ha comprado, descargado e implementado.

Si no hay aplicaciones presentes, esta sección mostrará un mensaje que le pedirá que pase a la sección de aplicaciones y descargue e implemente una aplicación.

Una vez que despliegue una aplicación, ésta aparecerá en el área de aplicaciones.



Comprar un complemento

Para comprar una aplicación, es necesario registrarse en la App Store. La compra se realiza a través del propio CAD. Encontrará

Vaya a la página Biblioteca > Aplicaciones del tablero de mandos del CAD.

Aquí puede seleccionar la aplicación que desea descargar y luego instalarla.

Si lo hace desde el panel de control del CAD, seleccione sólo un elemento. Puede poseer varios conjuntos de ADC, y las aplicaciones deben asociarse al ADC en el que se despliegan.

Si accede a la App Store a través del escritorio y el navegador, puede descargar tantas como desee. Por ejemplo, cuatro instancias del WAF o del GSLB. Aparecerán en el área de aplicaciones compradas de su CAD para que pueda descargarlas.

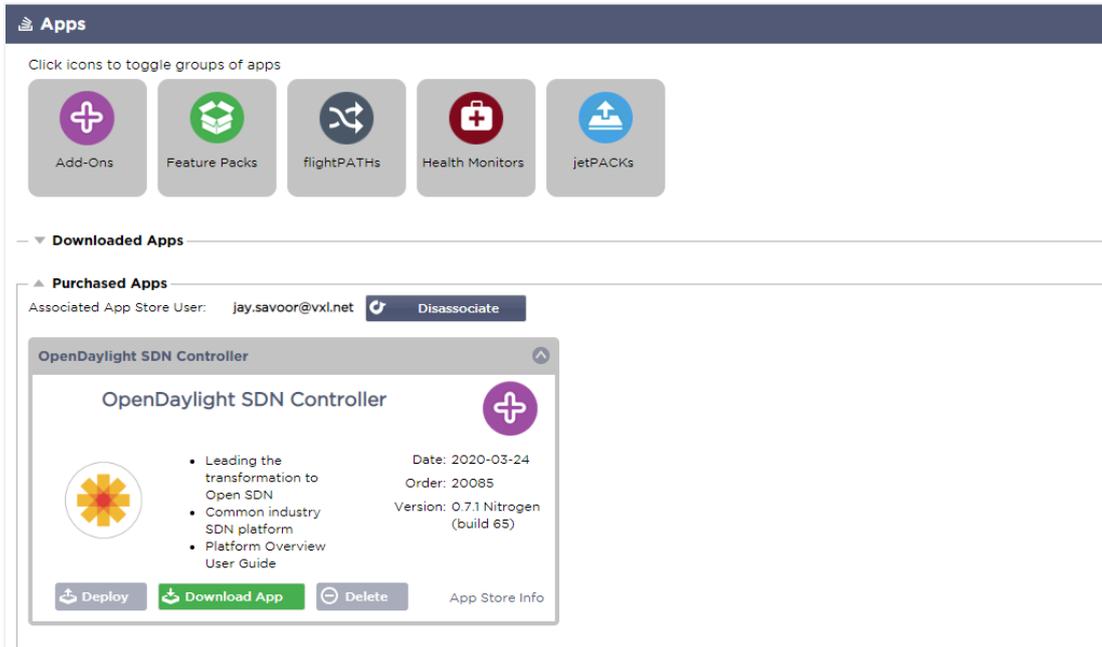
Las Apps se asocian a los CAD que usted posee y ha registrado.

Cuando elija descargar una aplicación, se le pedirá el ID de la máquina, tras lo cual la aplicación se encriptará y se vinculará al ID de la máquina del CAD.

Los enlaces a la App Store son:

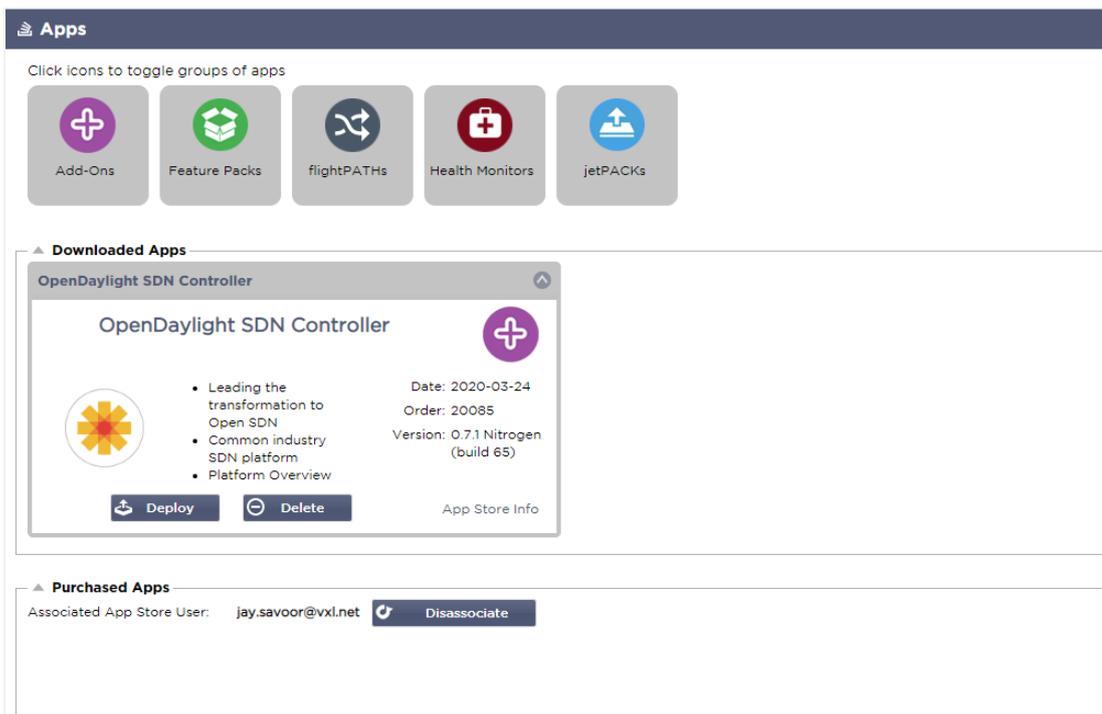
- Complementos: [HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/ADD-ONS/](https://appstore.edgenexus.io/product-category/add-ons/)
- Monitores de salud: [HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/SERVER-HEALTH-MONITORS/](https://appstore.edgenexus.io/product-category/server-health-monitors/)
- jetPACKS: [HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/JETPACKS/](https://appstore.edgenexus.io/product-category/jetpacks/)

- Paquetes de características: [HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/EDGENEXUS-FEATURE-PACK/](https://appstore.edgenexus.io/product-category/edgenexus-feature-pack/)
- Reglas de flightPATH: [HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCTO-CATEGORÍA/FLIGHTPATH/](https://appstore.edgenexus.io/producto-categoría/flightpath/)
- Actualizaciones de software: [HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/EDGENEXUS-SOFTWARE-UPDATE/](https://appstore.edgenexus.io/product-category/edgenexus-software-update/)



Desplegar una aplicación

Una vez descargada en el CAD, la aplicación se trasladará a la sección de aplicaciones descargadas y se desplegará en el CAD mediante el botón de despliegue. Este proceso tarda algún tiempo dependiendo de los recursos disponibles para el CAD. Una vez desplegada, aparecerá en la sección de Aplicaciones Descargadas.



Autenticación

La página Biblioteca > Autenticación le permite configurar servidores de autenticación y crear reglas de autenticación con opciones para Basic o Forms del lado del cliente y NTLM o BASIC del lado del servidor.

Configuración de la autenticación - Un flujo de trabajo

Por favor, lleve a cabo los siguientes pasos como mínimo para aplicar la autenticación a su servicio.

1. Cree un servidor de autenticación.
2. Cree una regla de autenticación que utilice un servidor de autenticación.
3. Cree una regla flightPATH que utilice una regla de autenticación.
4. Aplicar la regla flightPATH a un Servicio

Servidores de autenticación

Para configurar un método de autenticación que funcione, primero debemos configurar un servidor de autenticación.

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

- Haga clic en el botón "Añadir servidor".
- Esta acción producirá una fila en blanco lista para ser completada.

Opción	Descripción
Nombre	Dé a su servidor un nombre para identificarlo - este nombre se utiliza en las reglas
Descripción	Añadir una descripción
Método de autenticación	<p>Elija un método de autenticación</p> <p>LDAP: LDAP básico con nombres de usuario y contraseñas enviados en texto claro al servidor LDAP.</p> <p>LDAP-MD5 - LDAP básico con el nombre de usuario en texto claro y la contraseña con hash MD5 para aumentar la seguridad.</p> <p>LDAPS - LDAP sobre SSL. Envía la contraseña en texto claro dentro de un túnel cifrado entre el ADC y el servidor LDAP.</p> <p>LDAPS-MD5 - LDAP sobre SSL. La contraseña tiene un hash MD5 para mayor seguridad dentro de un túnel encriptado entre el ADC y el servidor LDAP</p>
Dominio	Añada el nombre de dominio para el servidor LDAP.
Dirección del servidor	<p>Añada la dirección IP o el nombre de host del servidor de autenticación</p> <p>LDAP - Dirección IPv4 o nombre de host.</p> <p>LDAP-MD5 - sólo nombre de host (la dirección IPv4 no funcionará)</p> <p>LDAPS - Dirección IPv4 o nombre de host.</p> <p>LDAPS-MD5 - sólo nombre de host (la dirección IPv4 no funcionará).</p>
Puerto	Utilice el puerto 389 para LDAP y el puerto 636 para LDAPS por defecto. No es necesario añadir el número de puerto para LDAP y LDAPS. Cuando estén disponibles otros métodos, podrá configurarlos aquí
Condiciones de búsqueda	Las condiciones de búsqueda deben ajustarse al RFC 4515. Ejemplo: (MemberOf=CN=Phone-VPN,CN=Users,DC=mycompany,DC=local).

Base de búsqueda	Este valor es el punto de partida para la búsqueda en la base de datos LDAP. Ejemplo <i>dc=miempresa,dc=local</i>
Formato de inicio de sesión	Utilice el formato de inicio de sesión que necesite. Nombre de usuario: con este formato elegido, sólo es necesario introducir el nombre de usuario. Cualquier información de usuario y dominio introducida por el usuario se elimina, y se utiliza la información de dominio del servidor. Nombre de usuario y dominio - El usuario debe introducir la sintaxis completa de dominio y nombre de usuario. Ejemplo: <i>miempresa\gchristie</i> O <i>alguien@miempresa</i> . La información del dominio introducida a nivel del servidor se ignora. En blanco: el CAD aceptará todo lo que el usuario introduzca y lo enviará al servidor de autenticación. Esta opción se utiliza cuando se usa MD5.
Frase de paso	Esta opción no se utiliza en esta versión.
Tiempo muerto	No se utiliza en esta versión

Reglas de autenticación

La siguiente etapa consiste en crear las reglas de autenticación para utilizarlas con la definición del servidor.

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

Campo	Descripción
Nombre	Añada un nombre adecuado para su regla de autenticación.
Descripción	Añada una descripción adecuada.
Dominio de la raíz	Debe dejarse en blanco a menos que necesite un inicio de sesión único en todos los subdominios.
Servidor de autenticación	Se trata de un cuadro desplegable que contiene los servidores que ha configurado.
Autenticación de clientes:	Elija el valor adecuado a sus necesidades: Básico (401) - Este método utiliza el método de autenticación estándar 401 Formularios - esto presentará el formulario por defecto del CAD al usuario. Dentro del formulario, puede añadir un mensaje. Puede seleccionar un formulario que haya cargado utilizando la sección siguiente.
Autenticación del servidor	Elija el valor adecuado. Ninguna - si su servidor no tiene ninguna autenticación existente, seleccione esta configuración. Esta configuración significa que puede añadir capacidades de autenticación a un servidor que anteriormente no tenía ninguna. Básico: si su servidor tiene activada la autenticación básica (401), seleccione BÁSICO. NTLM: si su servidor tiene activada la autenticación NTLM, seleccione NTLM.
Formulario	Elija el valor adecuado Por defecto - Al seleccionar esta opción, el CAD utilizará su forma incorporada. Personalizado: puede añadir un formulario que haya diseñado y seleccionarlo aquí.
Mensaje	Añada un mensaje personal al formulario.
Tiempo de espera	Añada un tiempo de espera a la regla, después del cual el usuario deberá autenticarse de nuevo. Tenga en cuenta que la configuración del tiempo de espera sólo es válida para la autenticación basada en formularios.

Inicio de sesión único

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

Si desea proporcionar un inicio de sesión único para los usuarios, complete la columna Dominio raíz con su dominio. En este ejemplo, hemos utilizado edgenexus.io. Ahora podemos tener varios servicios que utilizarán edgenexus.io como dominio raíz, y sólo tendrán que iniciar sesión una vez. Si consideramos los siguientes servicios:

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

Estos servicios pueden residir en una sola VIP o pueden estar distribuidos en 3 VIPs. A un usuario que acceda por primera vez a usercentral. mycompany.com se le presentará un formulario pidiéndole que se identifique en función de la regla de autenticación utilizada. A continuación, el mismo usuario puede conectarse a appstore. mycompany.com y será autenticado automáticamente por el ADC. Puede establecer el tiempo de espera, que forzará la autenticación una vez alcanzado este periodo de inactividad.

Formularios

Esta sección le permitirá cargar un formulario personalizado.

Cómo crear su formulario personalizado

Aunque el formulario básico que proporciona el CAD es suficiente para la mayoría de los propósitos, habrá ocasiones en las que las empresas deseen presentar su propia identidad al usuario. Puede crear su formulario personalizado que se presentará a los usuarios para que lo rellenen en esos casos. Este formulario debe estar en formato HTM o HTML.

Opción	Descripción
Nombre	nombre del formulario = loginform acción = %JNURL% Método = POST
Nombre de usuario	Sintaxis: name = "JNUSER"
Contraseña:	name="JNPASS"
Mensaje opcional1:	%JNMESSAGE%
Mensaje opcional2:	%JNAUTHMESSAGE%.
Imágenes	Si desea añadir una imagen, añádala en línea utilizando la codificación Base64.

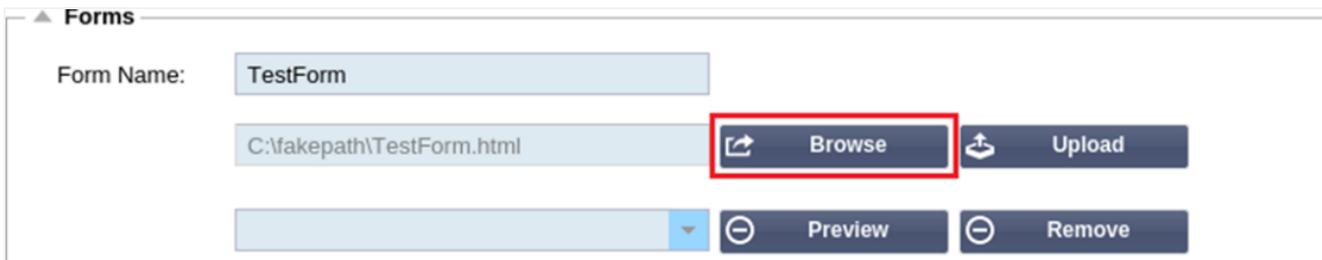
Ejemplo de código html de un formulario muy básico y sencillo

```
<HTML>
<HEAD>
<TÍTULO>FORMULARIO DE AUTENTIFICACIÓN DE EJEMPLO</TÍTULO>
<HEAD>
```

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

Añadir un formulario personalizado

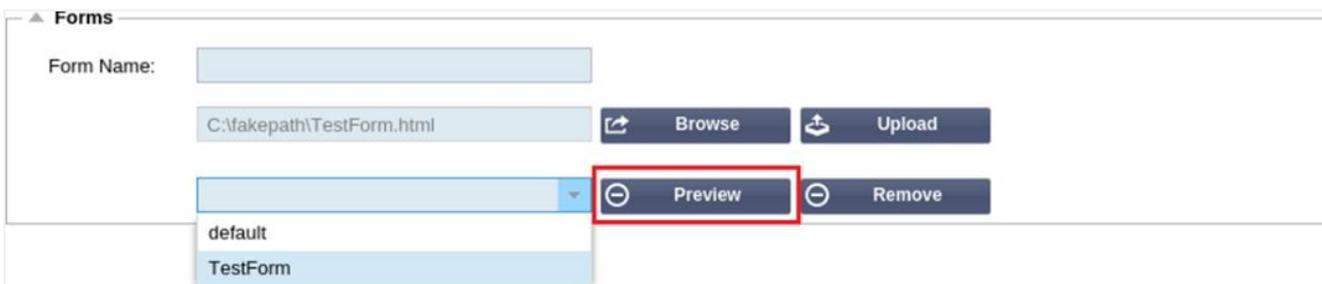
Una vez que haya creado un formulario personalizado, puede añadirlo mediante la sección Formularios.



1. Elija un nombre para su formulario
2. Busque su formulario a nivel local
3. Haga clic en Cargar

Vista previa de su formulario personalizado

Para ver el formulario personalizado que acaba de cargar, lo selecciona y hace clic en Vista previa. También puede utilizar esta sección para eliminar los formularios que ya no sean necesarios.



Caché

El ADC es capaz de almacenar datos en su memoria interna y de vaciar periódicamente esta caché en el almacenamiento interno del ADC. Los ajustes que gestionan esta funcionalidad se proporcionan dentro de esta sección.

▲ Global Cache Settings

Maximum Cache Size (MB):	50
Desired Cache Size (MB):	30
Default Caching Time (D/HH:MM):	1 / 00:00
Cachable HTTP Response Codes:	200 203 301 304 410
Cache Checking Timer (D/HH:MM):	3 / 00:00
Cache-Fill Count:	20

Update

Check Cache
Force a check on the cache size

Clear Cache
Remove all items from the cache

Configuración global de la caché

Tamaño máximo de la caché (MB)

Este valor determina el máximo de RAM que puede consumir la Caché. La caché del ADC es una caché en memoria que también se vacía periódicamente en el medio de almacenamiento para mantener la persistencia de la caché después de los reinicios, reinicios y operaciones de apagado. Esta funcionalidad significa que el tamaño máximo de la caché debe ajustarse a la huella de memoria del aparato (en lugar de al espacio del disco) y no debe ser superior a la mitad de la memoria disponible.

Tamaño de caché deseado (MB)

Este valor denota la RAM óptima a la que se recortará la Caché. Mientras que el tamaño máximo de la caché representa el límite superior absoluto de la caché, el tamaño deseado de la caché se entiende como el tamaño óptimo que la caché debe intentar alcanzar cada vez que se realice una comprobación automática o manual del tamaño de la caché. El espacio entre el tamaño máximo y el deseado de la caché existe para acomodar la llegada y el solapamiento de nuevos contenidos entre las comprobaciones periódicas del tamaño de la caché para recortar los contenidos caducados. Una vez más, puede ser más eficaz aceptar el valor por defecto (30 MB) y revisar periódicamente el tamaño de la Caché en "Monitor -> Estadísticas" para comprobar el tamaño adecuado.

Tiempo de caché por defecto (D/HH:MM)

El valor introducido aquí representa la vida del contenido sin un valor de caducidad explícito. El tiempo de almacenamiento en caché por defecto es el período durante el cual se almacena el contenido sin una directiva "no-store" o un tiempo de caducidad explícito en la cabecera de tráfico.

La entrada del campo adopta la forma "D/HH:MM" - por lo que una entrada de "1/01:01" (por defecto es 1/00:00) significa que para almacenar el ADC mantendrá el contenido durante un día, "01:00" para una hora, y "00:01" para un minuto.

Códigos de respuesta HTTP almacenables en caché

Uno de los conjuntos de datos almacenados en caché son las respuestas HTTP. Los códigos de respuesta HTTP que se almacenan en caché son:

- 200 - Respuesta estándar para solicitudes HTTP exitosas
- 203 - Las cabeceras no son definitivas, sino que se recogen de una copia local o de un tercero
- 301 - Al recurso solicitado se le ha asignado una nueva URL permanente
- 304 - No se ha modificado desde la última solicitud y en su lugar se debe utilizar la copia en caché local
- 410 - El recurso ya no está disponible en el servidor y no se conoce ninguna dirección de reenvío

Este campo debe editarse con precaución, ya que los códigos de respuesta más comunes que se pueden almacenar en caché ya están listados.

Tiempo de comprobación de la caché (D/HH:MM)

Este ajuste determina el intervalo de tiempo entre las operaciones de recorte de la caché.

Recuento de llenado de caché

Este ajuste es una función de ayuda para rellenar la caché cuando se ha detectado un determinado número de 304.

Aplicar la regla de la caché

▲ Apply Cache Rule

Other Domains Served

Domain Name: 192.168.1.251 + Add Domain - Remove Domain

+ Add Records - Remove Records

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

Esta sección le permite aplicar una regla de caché a un dominio:

- Añada el dominio manualmente con el botón Añadir registros. Debe utilizar un nombre de dominio completo o una dirección IP en notación decimal con puntos. Ejemplo www.miempresa.com o 192.168.3.1:80
- Haga clic en la flecha desplegable y elija su dominio de la lista
- La lista se rellenará siempre que el tráfico haya pasado por un servicio virtual y se haya aplicado una estrategia de almacenamiento en caché al servicio virtual
- Elija su regla de caché haciendo doble clic en la columna Base de reglas de caché y seleccionando de la lista

Crear regla de caché

▲ Create Cache Rule

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

+ Add Records - Remove Records

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

Esta sección le permite crear varias reglas de almacenamiento en caché diferentes que pueden aplicarse a un dominio:

- Haga clic en Añadir registros y dé a su regla un nombre y una descripción
- Puede escribir sus condiciones manualmente o utilizar el botón Añadir condición

Para añadir una condición utilizando la base de reglas de selección:

- Elija Incluir o Excluir
- Elegir todas las imágenes JPEG

- Haga clic en el símbolo + Añadir
- Verá que ahora se ha añadido "incluid * .jpg" a las condiciones
- Puede añadir más condiciones. Si decide hacerlo manualmente, deberá añadir cada condición en una línea NUEVA. Tenga en cuenta que sus reglas se mostrarán en la misma línea hasta que haga clic en el cuadro de condiciones, entonces se mostrarán en una línea separada

flightPATH

flightPATH es la tecnología de gestión del tráfico integrada en el ADC. flightPATH le permite inspeccionar el tráfico HTTP y HTTPS en tiempo real y realizar acciones basadas en condiciones.

Las reglas flightPATH deben aplicarse a un VIP cuando se utilizan objetos IP dentro de las reglas.

Una regla de trayectoria de vuelo consta de cuatro elementos:

1. Detalles, donde se define el nombre del flightPATH y el servicio al que se adjunta.
2. Condición(es) que puede(n) ser definida(s) y que hace(n) que la regla se active.
3. Evaluación que permite la definición de variables que pueden ser utilizadas dentro de las Acciones
4. Acciones que se utilizan para gestionar lo que debe ocurrir cuando se cumplen las condiciones

Detalles

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

La sección de detalles muestra las reglas flightPATH disponibles. Puede añadir nuevas reglas flightPATH y eliminar las definidas desde esta sección.

Añadir una nueva regla flightPATH

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

Campo	Descripción
Nombre de FlightPATH	Este campo es para el nombre de la regla flightPATH. El nombre que usted proporciona aquí aparece en y es referenciado dentro de otras partes del CAD.
Aplicado a VS	Esta columna es de sólo lectura y muestra el VIP al que se aplica la regla flightPATH.
Descripción	Valor que representa una descripción proporcionada con fines de legibilidad.

Pasos para añadir una regla flightPATH

1. En primer lugar, haga clic en el botón Añadir nuevo situado en la sección Detalles.
2. Introduzca un nombre para su regla. Ejemplo Auth2

3. Introduzca una descripción de su regla
4. Una vez que la regla se haya aplicado a un servicio, verá que la columna Aplicado a se autocompleta con una dirección IP y un valor de puerto
5. No olvide pulsar el botón Actualizar para guardar los cambios o, si se equivoca, simplemente pulse Cancelar para volver al estado anterior.

Condición

Una regla flightPATH puede tener cualquier número de condiciones. Las condiciones funcionan sobre una base AND, lo que le permite establecer la condición sobre la que se desencadena la acción. Si desea utilizar una condición OR, cree una regla flightPATH adicional y aplíquela al VIP en el orden correcto.

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

También puede utilizar RegEx seleccionando Match RegEx en el campo Check y el valor RegEx en el campo Value. La inclusión de la evaluación RegEx amplía enormemente la capacidad de flightPATH.

Creación de una nueva condición flightPATH

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

Condición

Proporcionamos varias Condiciones como predefinidas dentro del desplegable y cubren todos los escenarios previstos. Cuando se añadan nuevas Condiciones, éstas estarán disponibles a través de las actualizaciones de Jetpack.

Las opciones disponibles son:

CONDICIÓN	DESCRIPCIÓN	EJEMPLO
<form>	Los formularios HTML se utilizan para pasar datos a un servidor	Ejemplo "el formulario no tiene longitud 0"
Ubicación de GEO	Compara la dirección IP de origen con los códigos de país ISO 3166	La ubicación GEO es igual a GB, O la ubicación GEO es igual a Alemania
Anfitrión	Anfitrión extraído de la URL	www.mywebsite.com o 192.168.1.1
Idioma	Idioma extraído de la cabecera HTTP del idioma	Esta condición producirá un desplegable con una lista de idiomas
Método	Despliegue de métodos HTTP	Despliegue que incluye GET, POST, etc.
IP de origen	Si el proxy ascendente admite X-Forwarded-for (XFF), utilizará la verdadera dirección de origen	IP del cliente. También puede utilizar varias IP o subredes. 10\1\2\.* es la subred 10.1.2.0 /24 10\1\2\3 10\1\2\4 Use para múltiples IP's

Ruta	Ruta del sitio web	/mi sitio web/index.asp
POST	Método de solicitud POST	Comprobar los datos que se cargan en un sitio web
Consulta	Nombre y valor de una consulta, y puede aceptar también el nombre de la consulta o un valor	"Best=jetNEXUS" Donde la coincidencia es Best y el valor es edgeNEXUS
Cadena de consulta	Toda la cadena de consulta después del carácter ?	
Solicitar galleta	Nombre de una cookie solicitada por un cliente	MS-WSMAN=afYfn1CDqqUD::
Solicitud de cabecera	Cualquier encabezado HTTP	Referrer, User-Agent, From, Date
Solicitar versión	La versión HTTP	HTTP/1.0 O HTTP/1.1
Órgano de respuesta	Una cadena definida por el usuario en el cuerpo de la respuesta	Servidor UP
Código de respuesta	El código HTTP de la respuesta	200 OK, 304 no modificado
Respuesta Cookie	El nombre de una cookie enviada por el servidor	MS-WSMAN=afYfn1CDqqUD::
Cabecera de respuesta	Cualquier encabezado HTTP	Referrer, User-Agent, From, Date
Versión de la respuesta	La versión HTTP enviada por el servidor	HTTP/1.0 O HTTP/1.1
Fuente IP	Ya sea la IP de origen, la IP del servidor proxy o alguna otra dirección IP agregada	IP del cliente , IP del proxy, IP del cortafuegos. También puede utilizar múltiples IP y subredes. Debe escapar los puntos ya que estos son RegEX. Ejemplo 10\ 1\ 2\ 3 es 10.1.2.3

Partido

El campo Coincidencia puede ser un desplegable o un valor de texto y se define en función del valor del campo Condición. Por ejemplo, si la Condición se establece como Anfitrión, el campo Coincidencia no está disponible. Si la Condición se establece como <form>, el campo Coincidencia se muestra como un campo de texto, y si la Condición es POST, el campo Coincidencia se presenta como un desplegable que contiene los valores pertinentes.

Las opciones disponibles son:

MATCH	DESCRIPCIÓN	EJEMPLO
Acepte	Tipos de contenido aceptables	Aceptar: text/plain
Accept-Encoding	Codificaciones aceptables	Accept-Encoding: <compress gzip deflate sdch identity>
Accept-Language	Idiomas aceptables para la respuesta	Accept-Language: en-US

Accept-Ranges	Qué tipos de rango de contenido parcial soporta este servidor	Accept-Ranges: bytes
Autorización	Credenciales de autenticación para la autenticación HTTP	Autorización: Basic QWxhZGRpbjpvGVuIHNIc2FtZQ==
Cargar a	Contiene información contable de los costes de la aplicación del método solicitado	
Codificación del contenido	El tipo de codificación utilizado	Content-Encoding: gzip
Contenido-Longitud	La longitud del cuerpo de la respuesta en octetos (bytes de 8 bits)	Contenido-Longitud: 348
Tipo de contenido	El tipo mime del cuerpo de la solicitud (utilizado con las solicitudes POST y PUT)	Content-Type: application/x-www-form-urlencoded
Cookie	Una cookie HTTP enviada previamente por el servidor con Set-Cookie (abajo)	Cookie: \$Versión=1; Skin=nuevo;
Fecha	Fecha y hora en que se originó el mensaje	Fecha = "Fecha" ":" HTTP-fecha
ETag	Un identificador para una versión específica de un recurso, a menudo un compendio de mensajes	ETag: "aed6bdb8e090cd1:0"
Desde	La dirección de correo electrónico del usuario que realiza la solicitud	De: user@example.com
Si-Modificado-Desde	Permite que se devuelva un 304 No Modificado si el contenido no se ha modificado	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Última modificación	La última fecha de modificación del objeto solicitado, en formato RFC 2822	Última modificación: Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Implementación: Cabeceras específicas que pueden tener diversos efectos en cualquier punto de la cadena solicitud-respuesta.	Pragma: no-cache
Referente	Dirección de la página web anterior desde la que se siguió un enlace a la página actualmente solicitada	Referente: HTTP://www.edgenexus.io
Servidor	Un nombre para el servidor	Servidor: Apache/2.4.1 (Unix)
Set-Cookie	Una cookie HTTP	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
Usuario-Agente	La cadena del agente de usuario	Usuario-Agente: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Varíe	Indica a los proxies descendentes cómo comparar las futuras cabeceras de las solicitudes para decidir si se puede utilizar la respuesta almacenada en la caché en lugar de solicitar una nueva al servidor de origen	Varía: User-Agent

X-Powered-By	Especifica la tecnología (por ejemplo, ASP.NET, PHP, JBoss) que soporta la aplicación web	X-Powered-By: PHP/5.4.0
--------------	---	-------------------------

Sense

El campo Sentido es un campo booleano desplegable y contiene las opciones Sí o No.

Consulte

El campo Comprobación permite establecer valores de comprobación con respecto a la Condición.

Las opciones disponibles son: Contener, Finalizar, Igualar, Existir, Tener Longitud, Coincidir con RegEx, Coincidir con la Lista, Iniciar, Exceder la Longitud

COMPROBAR	DESCRIPCIÓN	EJEMPLO
Existe	Esto no importa el detalle de la condición sólo que existe/no existe	Anfitrión - Existe
Inicie	La cadena comienza con el valor	Ruta - Hace - Inicio - /secure
Finalizar	La cadena termina con el valor	Ruta - Hace - Fin - .jpg
Contiene	La cadena sí contiene el valor	Encabezado de la solicitud - Aceptar - Contiene - imagen
Equal	La cadena sí es igual al valor	Anfitrión - Hace - Igual - www.jetnexus.com
Tener longitud	La cadena sí tiene una longitud del valor	Anfitrión - Tiene - Longitud - 16www.jetnexus.com = TRUEwww.jetnexus.co.uk = FALSE
RegEx de coincidencia	Le permite introducir una expresión regular completa compatible con Perl	IP de origen - Hace - Coincidir Regex - 10\.* 11\.*

Pasos para añadir una condición

Añadir una nueva condición flightPATH es muy fácil. Un ejemplo se muestra arriba.

1. Haga clic en el botón Añadir nuevo dentro del área de condiciones.
2. Elija una condición en el cuadro desplegable. Tomemos como ejemplo el anfitrión. También puede escribir en el campo y el CAD mostrará el valor en un desplegable.
3. Elija un sentido. Por ejemplo, ¿
4. Elija una marca. Por ejemplo, Contiene
5. Elija un valor. Por ejemplo, miempresa.com

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

El ejemplo anterior muestra que hay dos condiciones que tienen que ser ambas TRUE para que la regla se complete

- La primera es comprobar que el objeto solicitado es una imagen
- El segundo comprueba si el host en la URL es www.imagepool.com

Evaluación

La posibilidad de añadir variables definibles es una capacidad convincente. Los CAD normales ofrecen esta capacidad mediante scripts u opciones de línea de comandos que no son ideales para cualquiera. El CAD le permite definir cualquier número de variables utilizando una interfaz gráfica de usuario fácil de usar, como se muestra y describe a continuación.

La definición de la variable flightPATH comprende cuatro entradas que deben realizarse.

- Variable - es el nombre de la variable
- Fuente: una lista desplegable de posibles puntos de origen
- Detalle: seleccione los valores de un desplegable o introdúzcalos manualmente.
- Valor - el valor que contiene la variable y puede ser un valor alfanumérico o un RegEx para afinar.

Variables incorporadas:

Las variables incorporadas ya han sido codificadas, por lo que no es necesario crear una entrada de evaluación para ellas.

Puede utilizar cualquiera de las variables enumeradas a continuación en la sección Acción.

La explicación de cada variable se encuentra en la tabla "Condición" anterior.

- Método = \$method\$
- Ruta = \$ruta\$
- Cadena de consulta = \$cadena de consulta\$
- Sourceip = \$sourceip\$
- Código de respuesta (el texto también incluye "200 OK") = \$resp\$
- Host = \$host\$
- Versión = \$versión\$
- Puerto del cliente = \$puerto del cliente\$
- Clientip = \$clientip\$
- Geolocalización = \$geolocation\$"

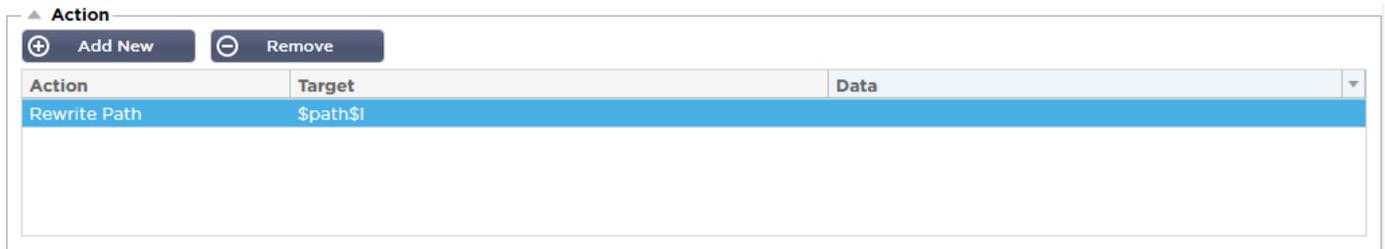
ACCIÓN	OBJETIVO:
Acción = Redirección 302	Objetivo = HTTPs://\$host\$/404.html
Acción = Registro	Objetivo = Un cliente de \$sourceip\$: \$sourceport\$ acaba de realizar una solicitud \$path\$ page

Explicación:

- Un cliente que acceda a una página que no existe, normalmente se encontrará con la página de error 404 del navegador
- En su lugar, el usuario es redirigido al nombre de host original que utilizó, pero la ruta incorrecta es sustituida por 404.html
- Se añade una entrada al Syslog que dice: "Un cliente de 154.3.22.14:3454 acaba de solicitar la página wrong.html".

Acción

La siguiente etapa del proceso es añadir una acción asociada a la regla flightPATH y a la condición.



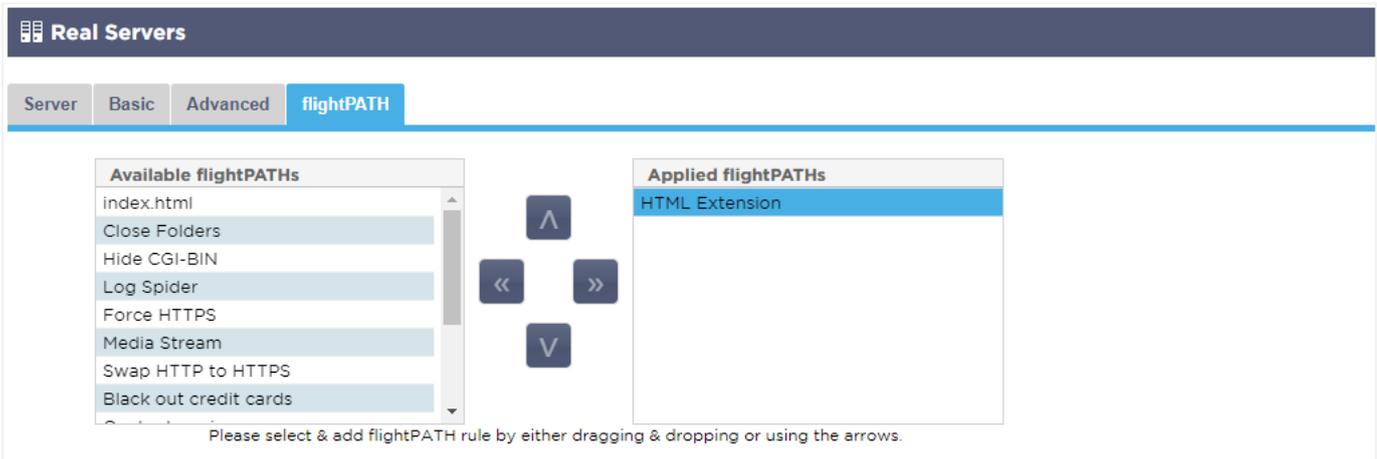
En este ejemplo, queremos reescribir la parte de la ruta de la URL para que refleje la URL escrita por el usuario.

- Haga clic en Añadir nuevo
- Elija Reescribir ruta en el menú desplegable Acción
- En el campo Destino, escriba \$ruta\$/miimágenes
- Haga clic en Actualizar

Esta acción añadirá /myimages a la ruta, por lo que la URL final pasa a ser www.imagepool.com/myimages

Aplicación de la regla flightPATH

La aplicación de cualquier regla flightPATH se realiza dentro de la pestaña flightPATH de cada VIP/VS.



- Vaya a Servicios > Servicios IP y elija la VIP a la que desea asignar la regla flightPATH.
- Verá la lista de servidores reales que se muestra a continuación
- Haga clic en la pestaña flightPATH
- Seleccione la regla flightPATH que haya configurado o una de las preconfiguradas admitidas. Puede seleccionar varias reglas flightPATH si es necesario.
- Arrastre y suelte el conjunto seleccionado a la sección de rutas de vuelo aplicadas o haga clic en el botón de flecha >>.
- La regla se desplazará al lado derecho y se aplicará automáticamente.

Monitores de servidores reales

Monitoring

▲ **Details**

+ Add Monitor
⊖ Remove

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

▲ **Upload Monitor**

Monitor Name:

Browse

Upload New Monitor

▲ **Custom Monitors**

▼

⊖ Remove

Cuando se configura el equilibrio de carga, resulta útil supervisar el estado de los servidores reales y de las aplicaciones que se ejecutan en ellos. Por ejemplo, en los servidores web, se puede configurar una página específica que se puede utilizar para supervisar el estado o utilizar uno de los otros sistemas de supervisión que tiene el CAD.

La página Biblioteca > Monitores del Servidor Real le permite añadir, ver y editar la monitorización personalizada. Se trata de los "Chequeos de Salud" del servidor de la Capa 7 y se seleccionan en el campo Monitorización del Servidor dentro de la pestaña Básica del servicio Virtual que usted defina.

La página de monitores del servidor real está dividida en tres secciones.

- Detalles
- Subir a
- Monitores a medida

Detalles

La sección Detalles se utiliza para añadir nuevos monitores y para eliminar los que no necesite. También puede editar un monitor existente haciendo doble clic sobre él.

Monitoring

▲ **Details**

+ Add Monitor
⊖ Remove

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

Nombre

Nombre de su elección para su monitor.

Descripción

Descripción textual para este Monitor, y recomendamos que sea lo más descriptiva posible.

Método de seguimiento

Elija el método de supervisión en la lista desplegable. Las opciones disponibles son:

Método de seguimiento	Descripción	Ejemplo
HTTP 200 OK	Se establece una conexión TCP con el Servidor Real. Una vez realizada la conexión, se envía una breve solicitud HTTP al Servidor Real. Se espera una respuesta HTTP del servidor y se comprueba el código de respuesta "200 OK". Si se recibe el código de respuesta "200 OK", se considera que el Servidor Real está en funcionamiento. Si, por cualquier motivo, no se recibe el código de respuesta "200 OK", incluidos los tiempos de espera o los fallos de conexión, se considera que el Servidor Real está caído y no disponible. Este método de monitorización sólo puede utilizarse realmente con los tipos de servicio HTTP y HTTP acelerado. Sin embargo, si un tipo de servicio de capa 4 está en uso para un servidor HTTP, podría seguir utilizándose si SSL no está en uso en el Servidor Real o es manejado adecuadamente por la facilidad "Content SSL".	Nombre: 200OK Descripción: Compruebe el sitio web de producción Método de seguimiento: HTTP 200 OK Ubicación de la página: /main/index.html O HTTP://www.edgenexus.io/main/index.html Contenido requerido: N/A
Respuesta HTTP	Se realiza una conexión y una petición/respuesta HTTP al servidor real y se comprueba como se ha explicado en el ejemplo anterior. Pero en lugar de comprobar un código de respuesta "200 OK", se comprueba la cabecera de la respuesta HTTP en busca de contenido de texto personalizado. El texto puede ser una cabecera completa, parte de una cabecera, una línea de una parte de la página o sólo una palabra. Si se encuentra el texto, se considera que el servidor real está en funcionamiento. Este método de supervisión sólo puede utilizarse realmente con los tipos de servicio HTTP y HTTP acelerado. Sin embargo, si un tipo de servicio de capa 4 está en uso para un servidor HTTP, podría seguir utilizándose si SSL no está en uso en el Servidor Real o es manejado adecuadamente por la facilidad "Content SSL".	Nombre: Servidor arriba Descripción: Compruebe el contenido de la página "Servidor arriba." Método de supervisión: Respuesta HTTP Ubicación de la página: /main/index.html O HTTP://www.edgenexus.io/main/index.html Contenido requerido: Servidor arriba
DICOM	Enviamos un eco DICOM utilizando el valor del Título AE "Origen Llamado" en la	Nombre: DICOM

	columna de contenido requerido. También puede establecer el valor del Título AE "Destino Llamado" en la sección de Notas de cada servidor. Puede encontrar la columna Notas dentro de los Servicios IP--Servicios virtuales--Página del servidor.	Descripción: Comprobación de la salud de L7 para el servicio DICOM Método de seguimiento: DICOM Ubicación de la página: N/A Contenido requerido: Valor AET
TCP fuera de banda	El método TCP fuera de banda es como una conexión TCP, salvo que puede especificar el puerto que desea supervisar en la columna de contenido requerido. Este puerto no suele ser el mismo que el puerto de tráfico y se utiliza cuando se quieren unir servicios	Nombre: TCP Fuera de Banda Descripción: Monitorear el puerto fuera de banda/tráfico Ubicación de la página: N/A Contenido requerido: 555
Monitor TCP multipuerto	Este método es como el anterior, salvo que puede tener varios puertos diferentes. El monitor se considera exitoso sólo si todos los puertos especificados en la sección de contenido requerido responden correctamente.	Nombre: Monitor multipuerto Descripción: Monitorear múltiples puertos para el éxito Ubicación de la página: N/A Contenido requerido: 135,59534,59535

Ubicación de la página

URL Ubicación de la página para un monitor HTTP. Este valor puede ser un enlace relativo como /carpeta1/carpeta2/página1.html. También puede utilizar un enlace absoluto en el que la página web esté vinculada al nombre del host.

Contenido requerido

Este valor contiene cualquier contenido que el monitor necesite detectar y utilizar. El valor representado aquí cambiará en función del método de monitorización que se elija.

Aplicado a VS

Este campo se rellena automáticamente con la IP/Puerto del Servicio Virtual al que se aplica el monitor. No podrá eliminar ningún Monitor que haya sido utilizado con un Servicio Virtual.

Usuario

Algunos monitores personalizados pueden utilizar este valor junto con el campo de la contraseña para iniciar sesión en un Servidor Real.

Contraseña

Algunos monitores personalizados pueden utilizar este valor junto con el campo Usuario para entrar en un Servidor Real.

Umbral

El campo Umbral es un entero general que se utiliza en los monitores personalizados en los que se requiere un umbral como el nivel de la CPU.

NOTA: Asegúrese de que la respuesta del servidor de aplicaciones no es una respuesta "Chunked".

Ejemplos de Real Server Monitor

▲ Details

+ Add Monitor - Remove

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

Monitor de carga

Habr  muchas ocasiones en las que los usuarios deseen crear sus propios monitores personalizados y esta secci n les permite cargarlos en el CAD.

Los monitores personalizados se escriben utilizando scripts PERL y tienen una extensi n de archivo .pl.

▲ Upload Monitor

Monitor Name:

- D  un nombre a su monitor para poder identificarlo en la lista de m todos de monitorizaci n
- Busque el archivo .pl
- Haga clic en Cargar nuevo monitor
- Su archivo se cargar  en la ubicaci n correcta y ser  visible como un nuevo M todo de Seguimiento.

Monitores a medida

En esta secci n, puede ver los monitores personalizados cargados y eliminarlos si ya no son necesarios.

▲ Upload Monitor

Monitor Name:

- Haga clic en el cuadro desplegable
- Seleccione el nombre del monitor personalizado
- Haga clic en Eliminar
- Su monitor personalizado ya no ser  visible en la lista de m todos de monitorizaci n

Creaci n de un script Perl de monitorizaci n personalizado

ATENCI N: Esta secci n est  dirigida a personas con experiencia en el uso y la escritura en Perl

Esta secci n le muestra los comandos que puede utilizar dentro de su script Perl.

El comando #NombreDelMonitor: es el nombre que se utiliza para el Script Perl almacenado en el CAD. Si no incluye esta l nea,  su script no ser  encontrado!

Lo siguiente es obligatorio:

- #NombreDelMonitor
- utilice estrictamente;

- advertencia de uso;

Los scripts Perl se ejecutan en un entorno CHROOTED. A menudo llaman a otra aplicación como WGET o CURL. A veces es necesario actualizarlas para una función específica, como SNI.

Valores dinámicos

- my \$host = \$_[0]; - Esto utiliza la "Dirección" de la sección Servicios IP--Servidor Real
- my \$port = \$_[1]; - Esto utiliza el "Puerto" de la sección Servicios IP--Servidor Real
- my \$content = \$_[2]; - Esto utiliza el valor "Contenido requerido" de la sección Biblioteca--Monitoreo del servidor real
- my \$notes = \$_[3]; - Esto utiliza la columna "Notas" en la sección de Servidores Reales de Servicios IP
- my \$page = \$_[4]; - Esto utiliza los valores de "Ubicación de la página" de la sección Library--Real Server Monitor
- my \$user = \$_[5]; - Esto utiliza el valor "User" de la sección Library--Real Server Monitor
- my \$contraseña = \$_[6]; - Esto utiliza el valor de "Contraseña" de la sección Biblioteca--Monitorización de Servidores Reales

Los controles de salud personalizados tienen dos resultados

- Exitoso
Valor de retorno 1Imprime un mensaje de éxito a SyslogMarca el servidor real en línea (siempre que coincida con IN COUNT)
- Unsuccessful
Valor de retorno 2Imprime un mensaje diciendo Unsuccessful a SyslogMarque el servidor real fuera de línea (siempre que el recuento OUT coincida)

Ejemplo de monitor de salud personalizado

Nombre del monitor HTTPS_SNI

utilizar estrictamente:

advertencias de uso;

El nombre del monitor como el anterior aparece en el desplegable de Comprobaciones de salud disponibles

Hay 6 valores pasados a este script (ver abajo)

El script devolverá los siguientes valores

1 es que la prueba es exitosa

2 si la prueba no tiene éxito sub monitor

{

my \$host= \$_[0]; ### IP o nombre del host

my \$port= \$_[1]; ### Puerto del host

my \$content= \$_[2]; ### Contenido a buscar (en la página web y en las cabeceras HTTP)

my \$notes= \$_[3]; ### Nombre del host virtual

my \$page= \$_[4]; ### La parte de la URL después de la dirección del host

my \$user= \$_[5]; ### dominio/username (opcional)

my \$password= \$_[6]; ### contraseña (opcional)

mi \$resolución;

my \$auth =;

si (\$puerto)

```

{
    $resolve = "$notas:$puerto:$host":
}
si no {
    $resolve = "$notas:$host";
}
if ($user && $password) {
    $auth = "-u $usuario:$contraseña :
}
my @lines = 'curl -s -i -retry 1 -max-time 1 -k -H "Host:$notes --resolve $resolve $auth HTTPs://${notes}${page} 2>&1';
if(join("@líneas)=~/\$contenido/)
{
    print "HTTPs://$notas}${página} buscando - $contenido - Comprobación de salud con éxito.\n";
    retorno(1);
}
si no
{
    print "HTTPs://$notas}${página} buscando - $contenido - Comprobación de salud fallida.\n";
    retorno(2)
}
}
monitor(@ARGV):

```

NOTA: Monitorización personalizada - El uso de variables globales no es posible. Utilice sólo variables locales - variables definidas dentro de las funciones

Certificados SSL

Para utilizar con éxito el equilibrio de carga de capa 7 con servidores que utilizan conexiones cifradas mediante SSL, el ADC debe estar equipado con los certificados SSL utilizados en los servidores de destino. Este requisito es para que el flujo de datos pueda ser descifrado, examinado, gestionado y luego vuelto a cifrar antes de enviarlo al servidor de destino.

Los certificados SSL pueden ir desde los certificados autofirmados que el ADC puede generar hasta los certificados tradicionales (comodín incluido) disponibles en proveedores de confianza. También puede utilizar certificados firmados por el dominio que se generan desde Active Directory.

¿Qué hace el CAD con el certificado SSL?

El CAD puede realizar reglas de gestión del tráfico (flightPATH) en función de lo que contengan los datos. Esta gestión no puede realizarse sobre los datos encriptados con SSL. Cuando el ADC tiene que inspeccionar los datos, necesita primero descifrarlos y para ello necesita disponer del certificado SSL utilizado por el servidor. Una vez descifrados, el ADC podrá entonces examinar y realizar las reglas flightPATH. A continuación, los datos se volverán a encriptar utilizando el certificado SSL y se enviarán al servidor real final.

Crear certificado

Aunque el ADC puede utilizar un certificado SSL de confianza global, puede generar un certificado SSL autofirmado. El SSL autofirmado es perfecto para los requisitos de equilibrio de carga internos. Sin embargo, es posible que sus políticas de TI requieran un certificado CA de confianza o de dominio.

Cómo crear un certificado SSL local

▲ **Create Certificate**

Certificate Name:	MyCompanyCertificate
Organization:	MyCompany
Organizational Unit:	Support
City/Locality:	New York
State/Province:	NY
Country:	US
Domain Name:	www.mycompany.com
Key Length:	2048
Period (days):	365

Create Local Certificate

Create Certificate Request

- Rellene todos los datos como en el ejemplo anterior
- Haga clic en Crear certificado local
- Una vez que haya pulsado esto, podrá aplicar el certificado a un **SERVICIO VIRTUAL**.

Crear una solicitud de certificado (CSR)

Cuando necesite obtener un SSL de confianza global de un proveedor externo, necesitará generar una CSR para generar el certificado SSL.

▲ **Create Certificate**

Certificate Name:	MyCompanyCertificate
Organization:	MyCompany
Organizational Unit:	Support
City/Locality:	New York
State/Province:	NY
Country:	US
Domain Name:	www.mycompany.com
Key Length:	2048
Period (days):	365

Create Local Certificate

Create Certificate Request

Rellene el formulario tal y como se muestra arriba con todos los datos pertinentes y, a continuación, haga clic en el botón de solicitud de certificado. Se le presentará la ventana emergente correspondiente a los datos que ha proporcionado.

Certificate Details

Certificate Name: MyCompanyCertificate

Certificate Text:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICojCCAYoCAQAwXTElMAkGA1UEBhMCVVMxCzAJBgNVBAGTAk5ZMR
EwDwYDVQQH
EwhOZXcgWW9yazESMBAGA1UEChMJTXIDb21wYW55MR0wGAYDVQQD
ExF3d3cubXlj
b21wYW55LmNvbTCCASlwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCgg
EBAMP8YIOq
D5L6vmbotxHmcnwGORAxzSgqOuQZLOj7h2LCN8Hh0/W8mLEiC+k8iBou
hSna23TJ
B2BrL5xVwIPISj6RDsAnegpavGUVsdkolu2iu7ujHGvSSAqjSsBBG4Is6ay3fLTI
ZM2ZDsIUzjPYK0gW7LStS89bH2ELB/MPf+iILFeQmCGQ2i5pF67sOOPpNM
E7EqXU
MOv/beTQ2Kwf0/awUw2m2RZ2krdgBq/Fw2tzQq+KxS4nHhOsJwIPKBy9u
```

[Close](#)

Deberá cortar y pegar el contenido en un archivo de TEXTO y nombrarlo con una extensión de archivo CSR, por ejemplo, *mycert.csr*. Este archivo CSR tendrá que ser proporcionado a su autoridad de certificación para crear el certificado SSL.

Gestionar el certificado

▲ Manage Certificate

Certificate: MyCompanyCertificate(Pending) ▼

Paste Signed:

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

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

[Show](#)

[Install](#)

[Add Intermediate](#)

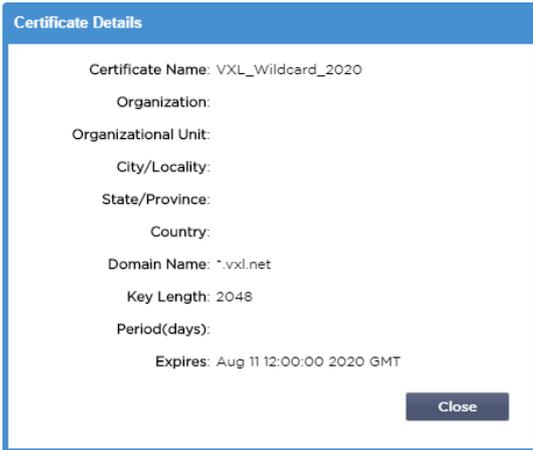
[Delete](#)

[Renew](#)

[Reorder](#)

Esta sub-sección contiene varias herramientas que permiten la gestión de los certificados SSL que tiene dentro del ADC.

Mostrar

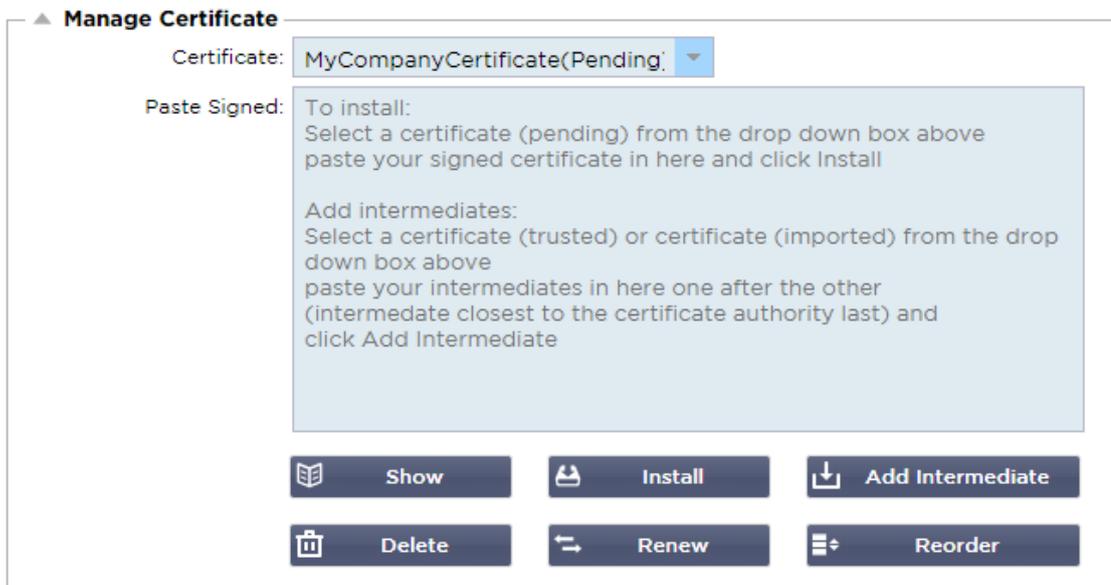


Puede haber ocasiones en las que desee mirar los detalles de un certificado SSL instalado.

- Seleccione el certificado en el menú desplegable
- Haga clic en el botón Mostrar
- Se presentará la ventana emergente que se muestra a continuación con los detalles del certificado.

Instalación de un certificado

Una vez que obtenga el certificado de la Autoridad Certificadora de Confianza, tendrá que compararlo con la CSR generada e instalarlo dentro del ADC.



- Seleccione un certificado que haya generado en los pasos anteriores. Habrá un estado (Pendiente) fijado a la partida. En el ejemplo, el certificado de MiEmpresa se muestra en la imagen superior.
- Abra el archivo del certificado en un editor de texto
- Copiar todo el contenido del archivo en el portapapeles
- Pegue el contenido del certificado SSL firmado que recibió de la autoridad de confianza en el campo marcado como Paste Signed.
- También puede pegar los intermedios debajo de esto, teniendo cuidado de seguir el orden correcto:
 1. (TOP) Su certificado firmado
 2. (2º desde arriba) Intermedio 1
 3. (3ª desde arriba) Intermedio 2
 4. (Abajo) Intermedio 3

5. Autoridad de certificación raíz No es necesario añadir esto ya que existen en las máquinas cliente.
(el ADC también contiene un paquete raíz para la recodificación en el que actúa como cliente de un servidor real)

- Haga clic en Instalar
- Una vez que haya instalado el certificado, debería ver el estado (Trusted) junto a su certificado

Si se ha equivocado o ha introducido un orden intermedio erróneo, seleccione el certificado (de confianza) y añada de nuevo los certificados (incluido el certificado firmado) en el orden correcto y haga clic en Instalar

Añadir intermedio

En ocasiones es necesario añadir los certificados intermedios por separado. Por ejemplo, puede haber importado un certificado que no tenga los intermedios.

- Resalte un certificado (de confianza) o un certificado (importado)
- Pegue los intermedios uno debajo de otro teniendo cuidado de que el intermedio más cercano a la autoridad de certificación se pegue en último lugar.
- Haga clic en "Añadir intermedio".

Si se equivoca en el orden, puede repetir el proceso y añadir los intermedios de nuevo. Esta acción sólo sobrescribirá los intermedios anteriores.

Borrar un certificado

Puede eliminar un certificado utilizando el botón Eliminar. Una vez borrado, el certificado se eliminará por completo del CAD y tendrá que ser sustituido, para luego volver a aplicarlo a los servicios virtuales si se requiere de nuevo.

Nota: Asegúrese de que el certificado no está unido a una VIP operativa antes de borrarlo.

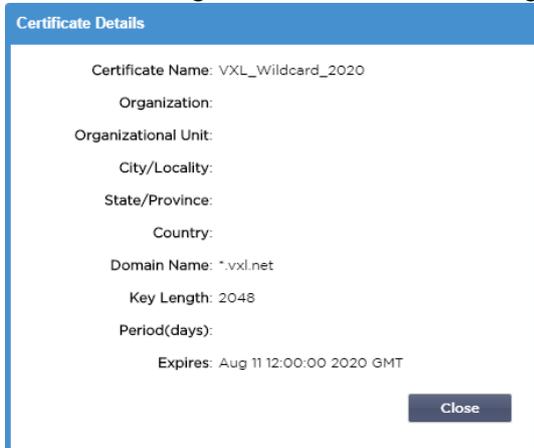
Renovar un certificado

El botón Renovar le permite obtener una nueva solicitud de firma de certificado. Esta acción es necesaria cuando el certificado está a punto de caducar y necesita ser renovado.

- Seleccione un certificado de la lista desplegable; puede elegir cualquier certificado con el estado (Pendiente), (De confianza) o (Importado)
- Haga clic en Renovar
- Copie los detalles de la nueva CSR para poder obtener un nuevo certificado



- Cuando obtenga el nuevo certificado, siga los pasos detallados en [MOSTRAR](#)



- Puede haber ocasiones en las que desee mirar los detalles de un certificado SSL instalado.
- Seleccione el certificado en el menú desplegable
- Haga clic en el botón Mostrar
- Se presentará la ventana emergente que se muestra a continuación con los detalles del certificado.
- Instalación de un certificado.
- El certificado nuevo y renovado se instalará ahora en el CAD.

Importar un certificado

En muchos casos, las empresas corporativas necesitarán utilizar sus certificados firmados por el dominio como parte de sus regímenes de seguridad internos. Los certificados deben estar en formato PKCS#12, y las contraseñas protegen invariablemente dichos certificados.

La imagen siguiente muestra la subsección para importar un solo certificado SSL.

- Asigne a su certificado un nombre amigable. Este nombre lo identifica en las listas desplegables utilizadas en el CAD. No es necesario que sea el mismo que el nombre de dominio del certificado, pero debe ser alfanumérico y sin espacios. No se permiten caracteres especiales distintos de _ y -.
- Escriba la contraseña que utilizó para crear el certificado PKCS#12
- Busque el {nombre del certificado}.pfx
- Haga clic en Importar.
- Su certificado estará ahora en los menús desplegables de SSL correspondientes dentro del CAD

Importación de varios certificados

Esta sección le permite importar un archivo JNBK que contenga múltiples certificados. Un archivo JNBK es encriptado y producido por el CAD cuando se exportan múltiples certificados.

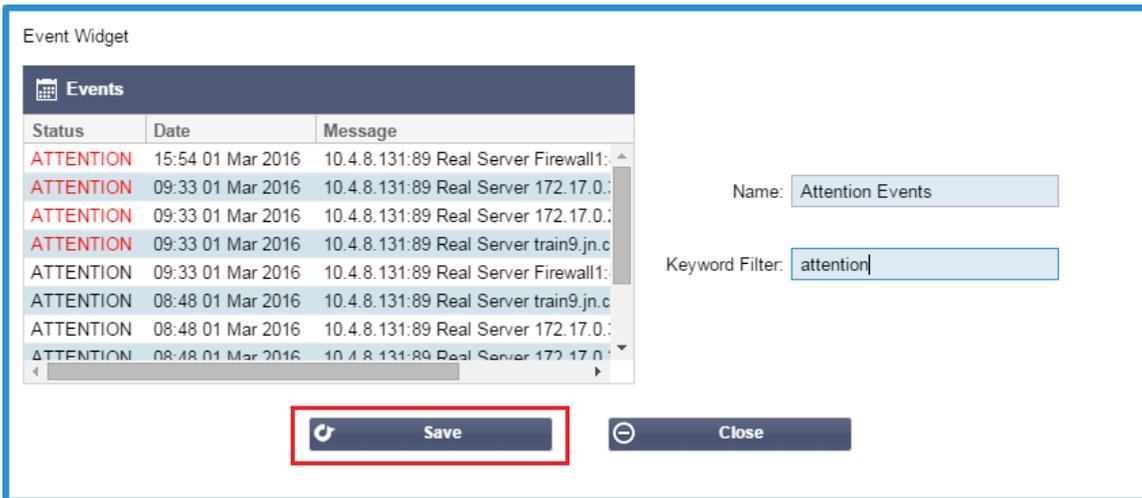
- Busque su archivo JNBK - puede crear uno de ellos exportando varios certificados
- Escriba la contraseña que utilizó para crear el archivo JNBK
- Haga clic en Importar.
- Sus certificados estarán ahora en los menús desplegables de SSL correspondientes dentro del CAD

Exportar un certificado

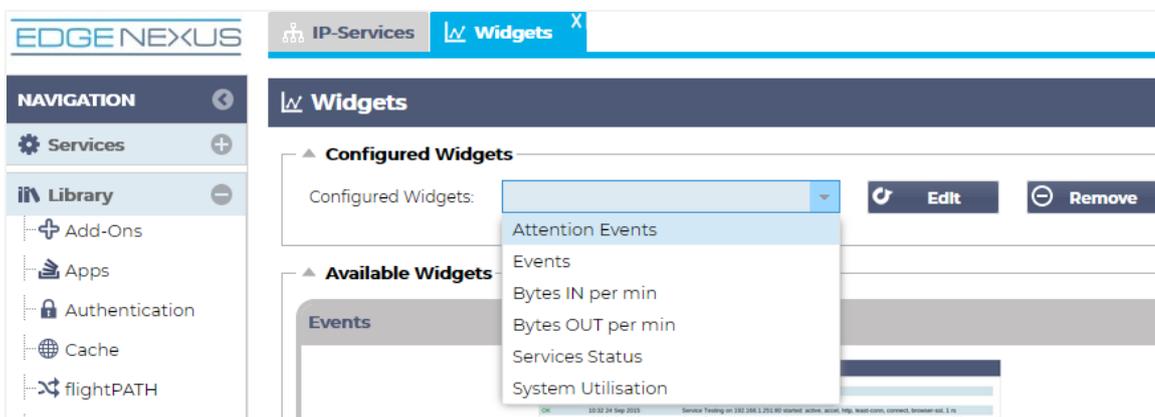
De vez en cuando, es posible que desee exportar uno de los certificados que tiene el CAD. El CAD ha sido dotado de la capacidad de hacerlo.

- Haga clic en el certificado o certificados que desee instalar. Puede hacer clic en la opción Todos para seleccionar todos los certificados de la lista.
- Escriba una contraseña para proteger el archivo exportado. La contraseña debe tener al menos seis caracteres. Se pueden utilizar letras, números y algunos símbolos. Los siguientes caracteres **no** son aceptables: < > " ' () ; \ | \A3 % &
- Haga clic en Exportar
- Si exporta un solo certificado, el archivo resultante se llamará sslcert_{certname}.pfx. Por ejemplo sslcert_Test1Cert.pfx
- En el caso de una exportación de varios certificados, el archivo resultante será un archivo JNBK. El nombre del archivo será sslcert__pack.jnbk.

Nota: Un archivo JNBK es un archivo contenedor encriptado producido por el CAD y válido sólo para la importación en el CAD



- Haga clic en Guardar y luego en Cerrar
- Ahora verá un Widget adicional llamado Eventos de Atención en el desplegable de Widgets Configurados.

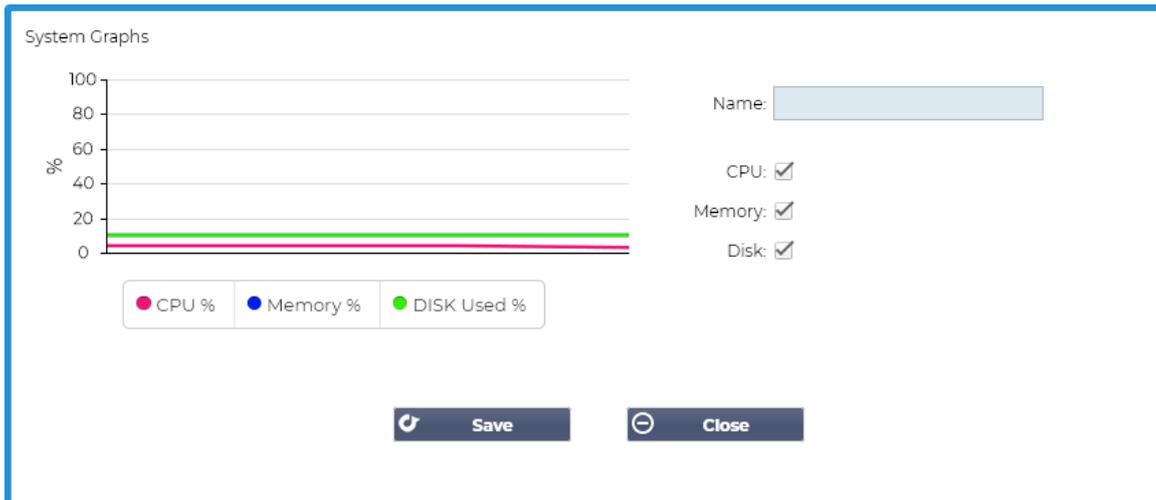


- Puede ver que ahora hemos añadido este widget en la sección Vista > Tablero.
- Seleccione el widget de Eventos de Atención para mostrarlo dentro del Tablero. Véase más abajo.

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

También puede pausar y reiniciar la alimentación de datos en directo haciendo clic en el botón Pausar datos en directo. Además, puede volver al cuadro de mandos por defecto en cualquier momento haciendo clic en el botón Cuadro de mandos por defecto.

El widget de gráficos del sistema



El CAD dispone de un widget configurable de gráficos del sistema. Haciendo clic en el botón Añadir del widget, puede añadir los siguientes gráficos de monitorización para que se muestren.

- CPU
- MEMORIA
- DISCO

Una vez que los haya añadido, estarán disponibles individualmente dentro del menú de widgets del Tablero.

Widget de interfaz

Name:

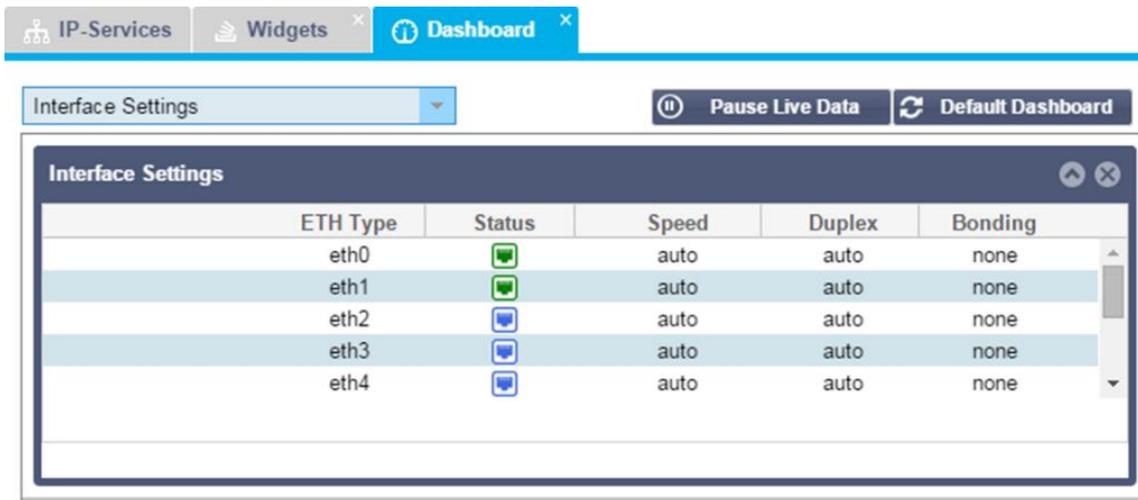
ETH Type	Status	Speed	Duplex	Bonding
eth0		auto	auto	none
eth1		auto	auto	none

Save Close

El widget de interfaz le permite mostrar los datos de la interfaz de red elegida, como ETH0, ETH1, etc. El número de interfaces disponibles para la adición depende de cuántas interfaces de red haya definido para el dispositivo virtual o provisionado dentro del dispositivo de hardware.

Una vez que haya terminado, haga clic en el botón Guardar y luego en el botón Cerrar.

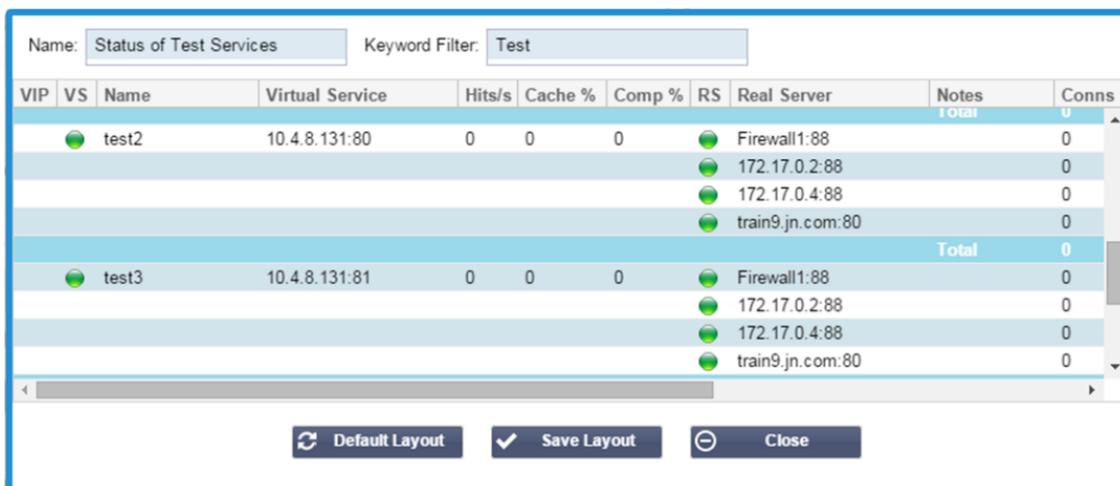
Seleccione el widget que acaba de personalizar en el menú desplegable de widgets dentro del panel de control. Verá una pantalla como la siguiente.



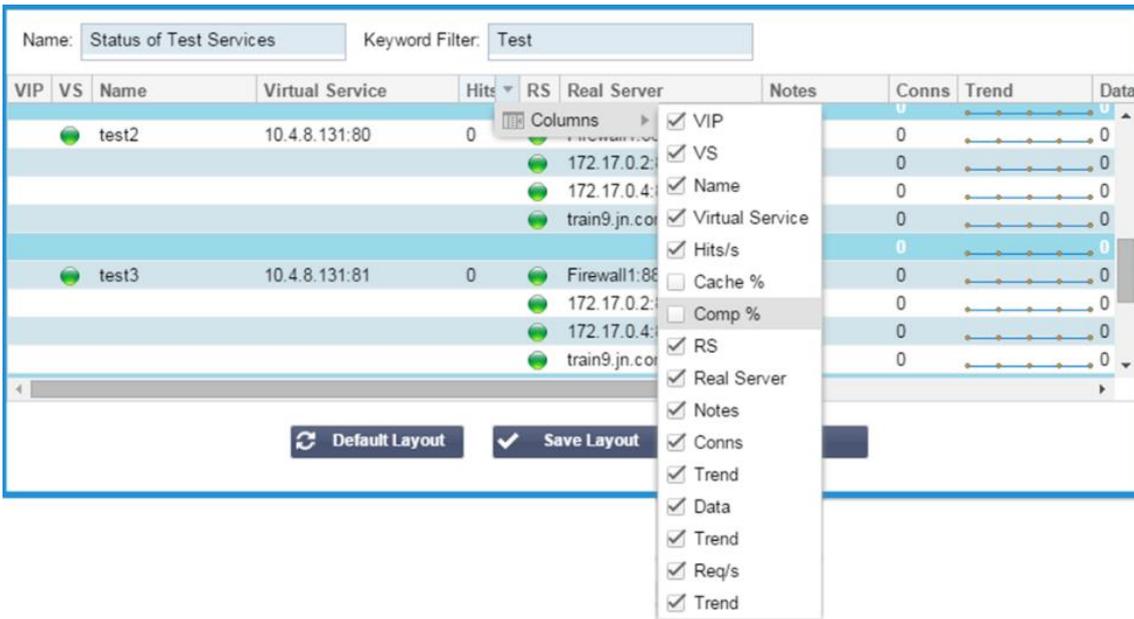
Widget de estado

El widget de estado le permite ver el equilibrio de carga en acción. También puede filtrar la vista para mostrar información específica.

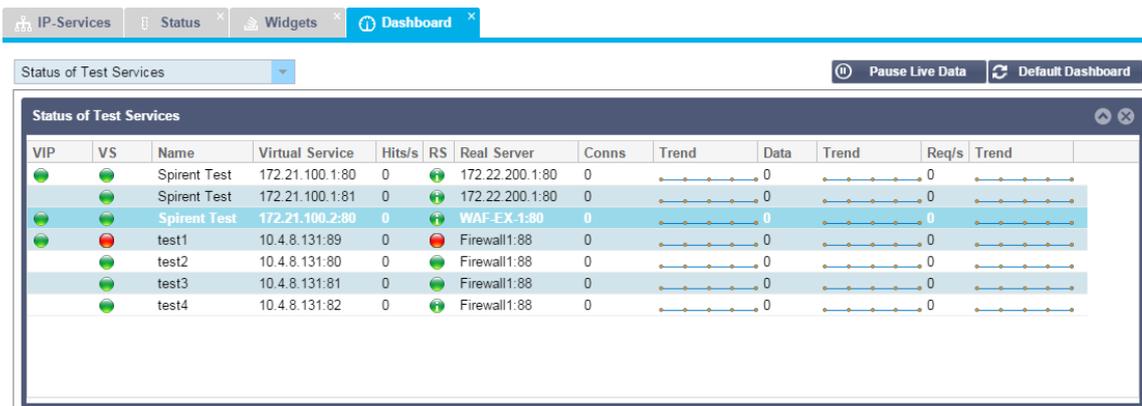
- Haga clic en Añadir.



- Introduzca un nombre para el servicio que desea supervisar
- También puede elegir qué columnas desea mostrar en el widget.

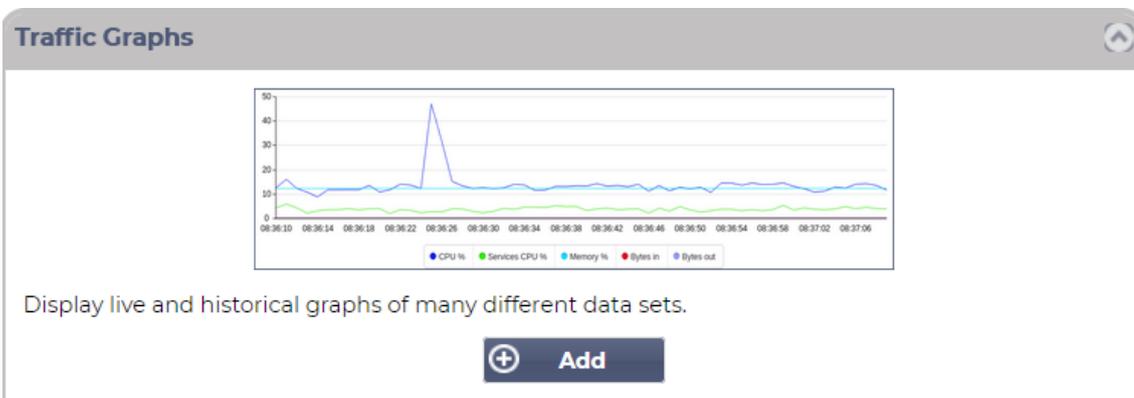


- Una vez que esté satisfecho, haga clic en Guardar, seguido de Cerrar.
- El widget de Estado elegido estará disponible en la sección del Tablero.



Widget de gráficos de tráfico

Este widget puede configurarse para mostrar los datos de tráfico actuales e históricos por Servicios Virtuales y Servidores Reales. Además, puede ver los datos generales actuales e históricos del tráfico global



- Pulse el botón Añadir
- Ponga un nombre a su widget.
- Elija una base de datos entre los servicios virtuales, los servidores reales o el sistema.

- Si elige Servicios Virtuales, puede seleccionar un servicio virtual en el desplegable VS/RS.
- Elija un periodo de tiempo en el desplegable Último.
 - Minuto - últimos 60
 - Hora - datos agregados de cada minuto durante los últimos 60 minutos
 - Día - datos agregados de cada hora para las 24 horas anteriores
 - Semana - datos agregados de cada día durante los siete días anteriores
 - Mes: datos agregados de cada semana de los últimos siete días
 - Año - datos agregados de cada mes durante los 12 meses anteriores
- Elija los datos disponibles en función de la base de datos que haya elegido
 - Base de datos de servicios virtuales
 - Bytes en
 - Bytes fuera
 - Bytes almacenados en caché
 - Compresión
 - Conexiones actuales
 - Solicitudes por segundo
 - Golpes en la caché
 - Porcentaje de aciertos en la caché
- Servidores reales
 - Bytes en
 - Bytes fuera
 - Conexiones actuales
 - Solicitudes por segundo
 - Tiempo de respuesta
- Sistema
 - CPU %
 - Servicios CPU
 - Memoria %
 - Disco Libre %
 - Bytes en
 - Bytes fuera
- Elija si desea mostrar los valores medios o los valores máximos
- Una vez que haya elegido todas las opciones, haga clic en Guardar y Cerrar

Ejemplo de gráfico de tráfico



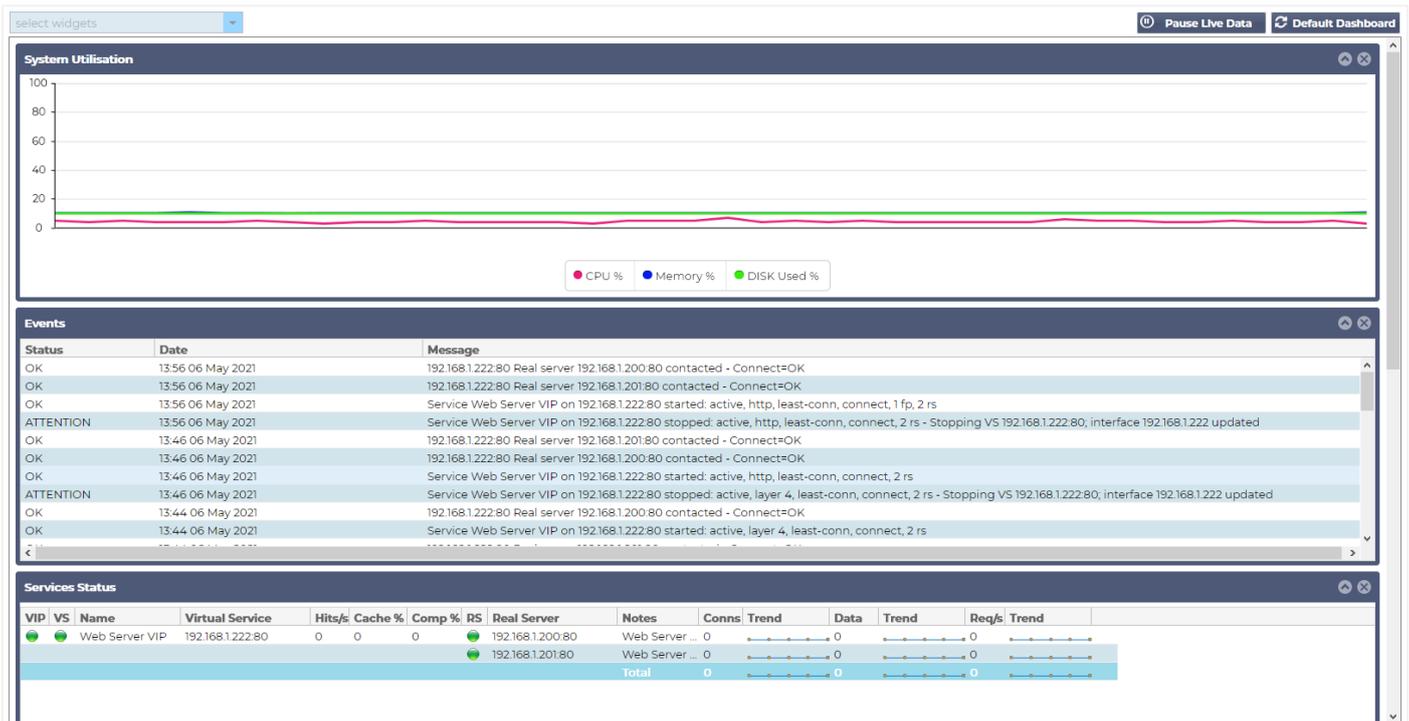
Ahora puede añadir su widget de Gráfico de Tráfico a la Vista > Tablero.

Ver

Tablero de mandos

Al igual que todas las interfaces de gestión de sistemas de TI, hay muchas ocasiones en las que necesita consultar las métricas de rendimiento y los datos que maneja el CAD. Le proporcionamos un panel de control personalizable para que pueda hacerlo de forma fácil y significativa.

Se puede acceder al Tablero de Control utilizando el segmento de Vista del panel del navegador. Cuando se selecciona, muestra varios widgets por defecto y le permite elegir los personalizados que haya definido.



Uso del panel de control

Hay cuatro elementos en el tablero U: el menú de widgets, el botón de pausa/reproducción y el botón de tablero por defecto.

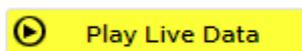
El menú de widgets

El menú de widgets situado en la parte superior izquierda del panel de control le permite seleccionar y añadir cualquier widget estándar o personalizado que haya definido. Para utilizarlo, seleccione el widget en el menú desplegable.

Botón de pausa de datos en vivo



Este botón le permite seleccionar si el CAD debe actualizar el salpicadero en tiempo real. Una vez en pausa, no se actualizará ningún widget del salpicadero, lo que le permitirá examinar el contenido a su antojo. El botón cambia de estado para mostrar Reproducir datos en directo una vez iniciada la pausa.



Cuando haya terminado, sólo tiene que hacer clic en el botón Reproducir datos en directo para reiniciar la recopilación de datos y actualizar el panel.

Botón del tablero por defecto



Puede ocurrir que desee restablecer el diseño del Tablero de Instrumentos por defecto. En tal caso, pulse el botón Tablero de mandos por defecto. Una vez pulsado, se perderán todos los cambios realizados en el Tablero.

Redimensionar, minimizar, reordenar y eliminar widgets



Cambiar el tamaño de un widget

Puede cambiar el tamaño de un widget muy fácilmente. Mantenga pulsada la barra de título del widget y arrástrelo a la izquierda o a la derecha del área del tablero. Verá un rectángulo punteado que representa el nuevo tamaño del widget. Suelte el widget en el rectángulo y suelte el botón del ratón. Si desea soltar un widget redimensionado junto a otro previamente redimensionado, verá que el rectángulo aparece junto al widget que desea soltar.

Minimizar un widget

Puede minimizar los widgets en cualquier momento haciendo clic en la barra de título del widget. Esta acción minimizará el widget y mostrará sólo la barra de título.

Ordenación de los widgets en movimiento

Para mover un widget, puede arrastrar y soltar haciendo clic y manteniendo pulsada la barra de título y moviendo el ratón.

Cómo eliminar un widget

Puede eliminar un widget haciendo clic en el  icono de la barra de título del widget.

Historia



La opción Historial, seleccionable desde el navegador, permite al administrador examinar el rendimiento histórico del ADC. Se pueden generar vistas históricas para los servicios virtuales, los servidores reales y el sistema.

También le permite ver el equilibrio de la carga en acción y ayuda a detectar cualquier error o patrón que deba investigarse. Tenga en cuenta que debe activar el registro histórico en Sistema > Historial para hacer uso de esta función.

Visualización de datos gráficos

Conjunto de datos

Para ver los datos históricos en formato gráfico, proceda como sigue:

El primer paso es elegir la base de datos y el periodo correspondiente a la información que desea ver. El periodo que puede seleccionar en el desplegable Último es Minuto, Hora, Día, Semana, Mes y Año.

Base de datos	Descripción
Sistema	La selección de esta base de datos le permitirá ver el espacio de la CPU, la memoria y la unidad de disco a lo largo del tiempo
Servicios virtuales	Si selecciona esta base de datos, podrá elegir todos los servicios virtuales de la base de datos desde que empezó a registrar datos. Verá una lista de servicios virtuales de la que podrá seleccionar uno.
Servicios reales	La selección de esta base de datos le permitirá elegir todos los Servidores Reales de la base de datos desde que comenzó a registrar los datos. Verá una lista de Servidores Reales de la que podrá seleccionar uno.

▲ Data Set

Database: System VS/RS: Choose one or more VS/RS Update

Last: week

▲ Data Set

Database: Virtual Services VS/RS: Choose one or more VS/RS Update

Last: day

192.168.1.40:80

Data Set

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

Last: day

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

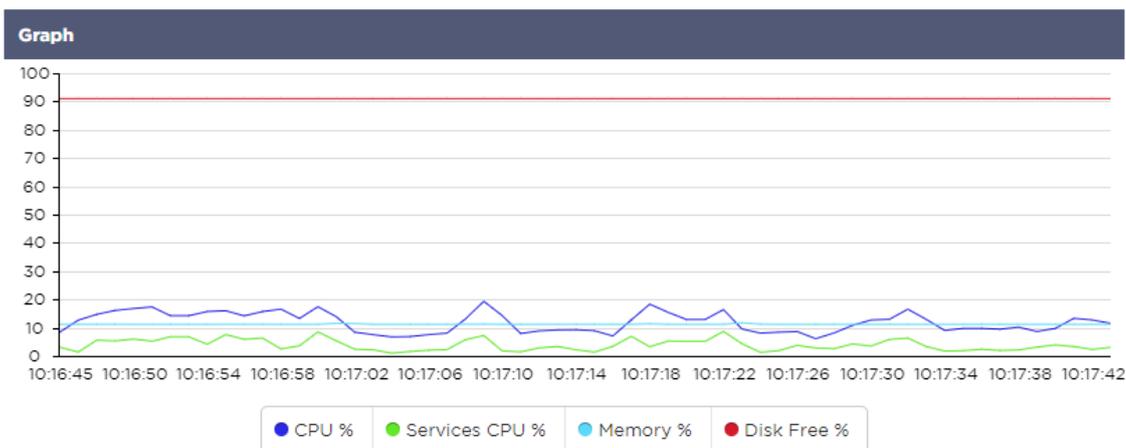
Update

Métrica

Una vez que haya seleccionado el conjunto de datos que va a utilizar, es el momento de elegir las métricas que desea visualizar. La imagen siguiente ilustra las métricas disponibles para su selección por parte del administrador: estas selecciones se corresponden con Sistema, Servicios virtuales y Servidores reales (de izquierda a derecha).

Metrics	Metrics	Metrics
<p>Data</p> <p><input checked="" type="checkbox"/> CPU %</p> <p><input type="checkbox"/> Services CPU %</p> <p><input type="checkbox"/> Memory %</p> <p><input type="checkbox"/> Disk Free %</p> <p>Show</p> <p><input checked="" type="checkbox"/> Averages</p> <p><input type="checkbox"/> Peak</p>	<p>Data</p> <p><input type="checkbox"/> Bytes In</p> <p><input type="checkbox"/> Bytes Out</p> <p><input type="checkbox"/> Bytes Cached</p> <p><input type="checkbox"/> Compression %</p> <p><input type="checkbox"/> Current Connections</p> <p><input type="checkbox"/> Request Per Second</p> <p><input type="checkbox"/> Cache Hits</p> <p><input type="checkbox"/> Cache Hits %</p> <p>Show</p> <p><input type="checkbox"/> Averages</p> <p><input type="checkbox"/> Peak</p>	<p>Data</p> <p><input type="checkbox"/> Bytes In</p> <p><input type="checkbox"/> Bytes Out</p> <p><input type="checkbox"/> Current Connections</p> <p><input type="checkbox"/> Pool Size</p> <p><input type="checkbox"/> Request Per Second</p> <p><input type="checkbox"/> Response Time</p> <p>Show</p> <p><input type="checkbox"/> Averages</p> <p><input type="checkbox"/> Peak</p>

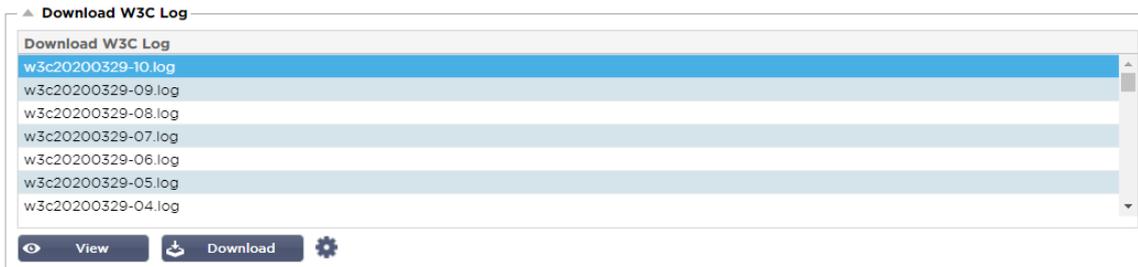
Gráfico de muestra



Registros

La página de Registros dentro de la sección Ver le permite previsualizar y descargar los registros del W3C y del Sistema. La página está organizada en dos secciones, como se detalla a continuación.

Descargar los registros del W3C



El registro W3C se activa desde la sección Sistema > Registro. Un registro W3C es un registro de acceso para servidores web en el que se generan archivos de texto que contienen datos sobre cada solicitud de acceso, incluyendo la dirección de protocolo de Internet (IP) de origen, la versión HTTP, el tipo de navegador, la página de referencia y la marca de tiempo. Los registros del W3C pueden llegar a ser muy grandes, dependiendo de la cantidad de datos y de la categoría de registro que se esté llevando a cabo.

Desde la sección del W3C, puede seleccionar el registro que necesita y luego verlo o descargarlo.

Ver botón

El botón Ver le permite ver el registro elegido dentro de la ventana del editor de texto, como el Bloc de notas.

Botón de descarga

Este botón le permite descargar el registro a su almacenamiento local para verlo más tarde.

El icono del engranaje

Al hacer clic en este icono, accederá a la sección de configuración del registro W3C, situada en Sistema > Registro. Discutiremos esto en detalle en la sección de Registro de la guía.

Estadísticas

La sección de estadísticas del CAD es un área muy utilizada por los administradores de sistemas que quieren asegurarse de que el rendimiento del CAD está a la altura de sus expectativas.

Compresión

El objetivo del CAD es controlar los datos y dirigirlos a los servidores reales configurados para recibirlos. La función de compresión se proporciona en el CAD para aumentar el rendimiento del mismo. Habrá ocasiones en las que los administradores desearán probar y comprobar la información de compresión de datos del CAD; estos datos los proporciona el panel de Compresión dentro de las Estadísticas.

Compresión de contenidos hasta la fecha

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

Los datos que se muestran en esta sección detallan el nivel de compresión alcanzado por el CAD en contenidos comprimibles. Un valor del 60-80% es lo que denominaríamos como típico

Compresión global hasta la fecha

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

Los valores proporcionados en esta sección informan de cuánta compresión ha logrado el CAD en todo el contenido. El porcentaje típico depende del número de imágenes precomprimidas que contengan sus servicios. Cuanto mayor sea el número de imágenes, menor será probablemente el porcentaje de compresión global.

Total de entradas/salidas

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

Las cifras de entrada/salida total representan la cantidad de datos brutos que entran y salen del ADC. La unidad de medida cambiará a medida que el tamaño crezca de kbps a Mbps y a Gbps.

Golpes y conexiones

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

La sección de aciertos y conexiones contiene las estadísticas globales de aciertos y transacciones que pasan por el CAD. ¿Qué significan los accesos y las conexiones?

- Un golpe se define como una transacción de la capa 7. Normalmente se utiliza para los servidores web, se trata de una solicitud GET para un objeto como una imagen.
- Una conexión se define como una conexión TCP de capa 4. En una conexión TCP pueden producirse muchas transacciones.

Total de aciertos contados

Las cifras de esta sección muestran el número acumulado de visitas no almacenadas en caché desde el último reinicio. En la parte derecha, la cifra mostrará el número actual de visitas por segundo.

Conexiones totales

El valor de Conexiones totales representa el número acumulado de conexiones TCP desde el último reinicio. La cifra de la segunda columna indica las conexiones TCP realizadas por segundo al ADC. La cifra de la columna de la derecha es el número de conexiones TCP por segundo realizadas a los servidores reales. Ejemplo 6/8 conexiones/seg. En el ejemplo mostrado tenemos 6 conexiones TCP por segundo al Servicio Virtual y 6 conexiones TCP por segundo a los Servidores Reales.

Conexiones máximas

El valor máximo de Conexiones representa el número máximo de conexiones TCP realizadas al CAD. El número de la columna más a la derecha indica el número actual de conexiones TCP activas.

Caché

Como recordará, el CAD está dotado tanto de compresión como de almacenamiento en caché. Esta sección muestra las estadísticas generales relacionadas con el almacenamiento en caché cuando se aplica a un canal. Si el almacenamiento en caché no se ha aplicado a un canal y se ha configurado correctamente, verá 0 contenidos de caché.

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

De la caché

Golpes: La primera columna da el número total de transacciones servidas desde la caché del CAD desde el último reinicio. También se proporciona un porcentaje del total de transacciones.

Bytes: La segunda columna da la cantidad total de datos en Kilobytes servidos desde la caché del CAD. También se proporciona un porcentaje de los datos totales.

Desde el servidor

Golpes: La columna 1 da el número total de transacciones servidas desde los servidores reales desde el último reinicio. También se proporciona un porcentaje del total de transacciones.

Bytes: La segunda columna da la cantidad total de datos en Kilobytes servidos desde los Servidores Reales. También se proporciona un porcentaje de los datos totales.

Contenido de la caché

Golpes: Este número da el número total de objetos contenidos en la caché del CAD.

Bytes: El primer número da el tamaño global en Megabytes de los objetos almacenados en la caché del CAD. También se proporciona un porcentaje del tamaño máximo de la caché.

Persistencia de la sesión

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

La sección de persistencia de la sesión ofrece información para varios parámetros.

Campo	Descripción
Total de sesiones actuales	Esto muestra cuántas sesiones de persistencia están en curso - se actualiza cada minuto
% Utilizado (del máximo)	Esto muestra el uso del espacio total permitido para la información de la sesión
Nueva sesión este min	Esto muestra, en el último minuto, cuántas nuevas sesiones de persistencia se añadieron
Revalidar este min	Esto muestra, en el último minuto, cuántas sesiones de persistencia existentes fueron revalidadas por más tráfico
Sesiones caducadas este min	Esto muestra, en el último minuto, cuántas sesiones de persistencia existentes expiraron debido a que no hubo más tráfico dentro del tiempo de espera

Hardware

Tanto si utiliza el ADC en un entorno virtual como dentro del hardware, esta sección le proporcionará información valiosa sobre el rendimiento del aparato.

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

Uso del disco

El valor proporcionado en la columna 2 da el porcentaje de espacio en disco utilizado actualmente e incluye información sobre los archivos de registro y los datos de la caché, que se almacenan periódicamente en el almacenamiento.

Uso de la memoria

La segunda columna indica el porcentaje de memoria utilizado actualmente. El número más significativo entre paréntesis es la cantidad total de memoria asignada al CAD. Se recomienda asignar al CAD un mínimo de 2 GB de RAM.

Uso de la CPU

Uno de los valores críticos proporcionados es el porcentaje de la CPU utilizado actualmente por el CAD. Es natural que éste fluctúe.

Estado

La página Ver > Estado muestra el tráfico en directo que atraviesa el ADC para los Servicios virtuales que ha definido. También muestra el número de conexiones y datos de cada Servidor Real para que pueda experimentar el equilibrio de carga en tiempo real.

Detalles del servicio virtual

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

Columna VIP

El color de la luz indica el estado de la dirección IP virtual asociada a uno o varios servicios virtuales.

Estado	Descripción
	En línea
	Failover-Standby. Este servicio virtual es hot-standby
	Indica que un "pasivo" está aguantando para un "activo"
	Fuera de línea. Los servidores reales son inalcanzables, o no hay servidores reales habilitados
	Encontrar el estado
	IPs virtuales no licenciadas o excedidas

Columna de estado VS

El color de la luz indica el estado del servicio virtual.

Estado	Descripción
	En línea
	Failover-Standby. Este servicio virtual es hot-standby
	Indica que un "pasivo" está aguantando para un "activo"
	El servicio necesita atención. Esta indicación de estado puede ser el resultado de que un Servidor Real haya fallado en un control de salud o haya sido cambiado manualmente a Desconectado. El tráfico seguirá fluyendo pero con una capacidad reducida del Servidor Real.
	Fuera de línea. Los servidores reales son inalcanzables, o no hay servidores reales habilitados
	Encontrar el estado
	IPs virtuales no licenciadas o excedidas

Nombre

El nombre del servicio virtual

Servicio virtual (VIP)

La dirección IP virtual y el puerto para el servicio y la dirección que utilizarán los usuarios o las aplicaciones.

Golpe/Sec

Transacciones de capa 7 por segundo en el lado del cliente.

Caché%.

La cifra proporcionada aquí representa el porcentaje de objetos que han sido servidos desde la caché RAM del CAD.

Compresión%.

Esta cifra representa el porcentaje de objetos que han sido comprimidos entre el cliente y el CAD.

Estado de la RS (servidor remoto)

La siguiente tabla resume el significado del estado de los Real Servers vinculados al VIP.

Estado	Descripción
●	Conectado
●	No se controla
●	Drenaje o fuera de línea
●	Standby
●	No conectado
●	Encontrar el estado
●	IPs virtuales no licenciadas o excedidas

Servidor real

La dirección IP y el puerto del servidor real.

Notas

Este valor puede ser cualquier nota útil para que otros entiendan el propósito de la entrada.

Conns (Conexiones)

La representación del número de conexiones a cada servidor real le permite ver el equilibrio de carga en acción. Es muy útil para verificar que su política de equilibrio de carga funciona correctamente.

Datos

El valor de esta columna muestra la cantidad de datos que se envían a cada Servidor Real.

Req/Sec (Solicitudes por segundo)

El número de solicitudes por segundo enviadas a cada Servidor Real.

Sistema

El segmento Sistema de la interfaz de usuario del ADC le permite acceder y controlar todos los aspectos del sistema del ADC.

Agrupación

El ADC puede utilizarse como un único dispositivo autónomo, y funcionará perfectamente haciendo eso. Sin embargo, si se tiene en cuenta que el propósito del ADC es equilibrar la carga de conjuntos de servidores, se hace evidente la necesidad de agrupar el propio ADC. El diseño de la interfaz de usuario del ADC, fácilmente navegable, hace que la configuración del sistema de clustering sea sencilla.

En la página Sistema > Clustering es donde configurará la alta disponibilidad de sus dispositivos ADC. Esta sección está organizada en varios apartados.

Nota importante

- No es necesario un cable dedicado entre el par ADC para mantener un latido de alta disponibilidad.
- El latido del corazón tiene lugar en la misma red que el servicio virtual que requiere alta disponibilidad para ser puesto en marcha.
- No hay conmutación por error de estado entre los aparatos ADC.
- Cuando se habilita la alta disponibilidad en dos o más ADC, cada caja difundirá a través de UDP los servicios virtuales que esté configurada para proporcionar.
- La conmutación por error de alta disponibilidad utiliza la mensajería unicast y el ARP gratuito para informar a los nuevos conmutadores del equilibrador de carga activo.

The screenshot shows the 'Clustering' configuration page. It is divided into three main sections: Role, Settings, and Management.

Role: Three radio buttons are visible:

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

Settings: A 'Failover Latency (ms):' field is set to 3500. An 'Update' button is present to the right.

Management: Contains an 'Unclaimed Devices' table (currently empty), a central navigation area with four directional arrows (up, down, left, right), and a 'Cluster Members' table with the following data:

Priority	Status	Cluster Members
1	●	192.168.1.220 EADC

Papel

Hay tres roles de cluster disponibles cuando se configura el ADC para alta disponibilidad.

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

- Por defecto, un nuevo ADC se encenderá utilizando el rol de Cluster. En este rol, cada miembro del cluster tendrá la misma "configuración de trabajo", y como tal, sólo un ADC del Cluster estará Activo en cualquier momento.
- Una "configuración de trabajo" significa todos los parámetros de configuración, excepto los elementos que deben ser únicos como la dirección IP de gestión, el nombre del ALB, los ajustes de red, los detalles de la interfaz, etc.
- El ADC de prioridad 1, la posición más alta, del cuadro de miembros del clúster es el propietario del clúster y el equilibrador de carga activo, mientras que todos los demás ADC son miembros pasivos.
- Puede editar cualquier CAD del clúster y los cambios se sincronizarán con todos los miembros del clúster.
- Cuando elimine un ADC del clúster, se eliminarán todos los servicios virtuales de ese ADC.
- No puede eliminar el último miembro del Cluster a Dispositivos no reclamados. Para eliminar el último miembro, cambie el rol a Manual o Stand-alone.
- Los siguientes objetos no están sincronizados:
 - Sección manual de fecha y hora - (La sección NTP está sincronizada)
 - Latencia de la conmutación por error (ms)
 - Sección de hardware
 - Sección de electrodomésticos
 - Sección de la red

Fallo del propietario del clúster

- Cuando el propietario de un clúster falla, uno de los miembros restantes tomará automáticamente el relevo y seguirá equilibrando la carga del tráfico.
- Cuando el propietario del clúster regrese, reanudará el tráfico de equilibrio de carga y asumirá el papel de propietario.
- Supongamos que el Propietario ha fallado y que un Miembro ha asumido el equilibrio de carga. Si desea que ese Miembro que ha asumido el tráfico de equilibrio de carga se convierta en el nuevo propietario, resalte el miembro y haga clic en la flecha hacia arriba para moverlo a la posición de Prioridad 1.
- Si edita uno de los miembros restantes del clúster y el propietario está caído, el miembro editado se promoverá automáticamente al propietario sin pérdida de tráfico

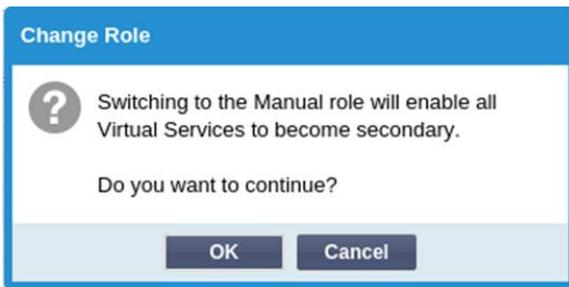
Cambio de rol de Cluster a rol Manual

- Si desea cambiar el rol de Cluster a Manual, haga clic en el botón de radio junto a la opción de rol Manual

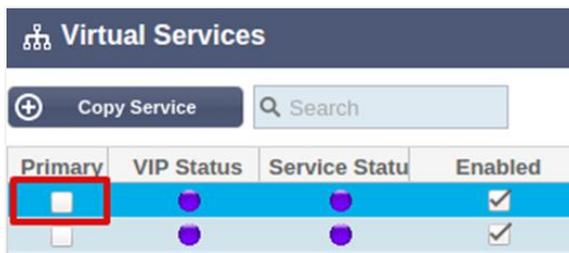
▲ Role

- 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

- Después de hacer clic en el botón de opción, verá el siguiente mensaje:



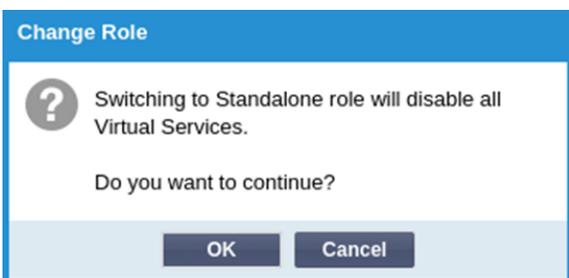
- Pulse el botón OK
- Compruebe la sección de Servicios Virtuales. Verá que la columna Primaria muestra ahora una casilla sin marcar.



- Es una característica de seguridad y significa que si tiene otro CAD con los mismos servicios virtuales, no habrá interrupción del flujo de tráfico.

Cambio de rol de clúster a autónomo

- Si desea cambiar el rol de Cluster a Stand-alone, haga clic en el botón de radio junto a la opción Standalone.
- Se le solicitará el siguiente mensaje:



- Haga clic en Aceptar para cambiar los roles.
- Compruebe sus Servicios Virtuales. Verá que la columna Primaria cambia de nombre a Independiente
- También verá que todos los servicios virtuales están desactivados (sin marcar) por razones de seguridad.
- Una vez que esté seguro de que ningún otro ADC de la misma red tiene servicios virtuales duplicados, puede habilitar cada uno de ellos a su vez.

Rol manual

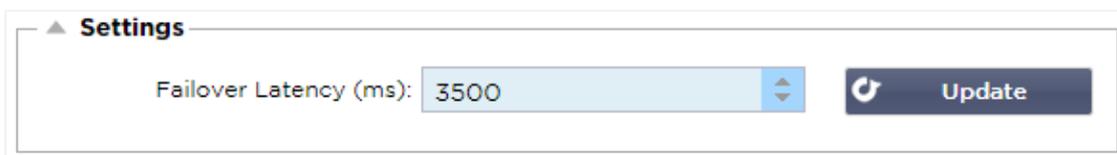
Un CAD en el rol Manual trabajará con otros CAD en el rol Manual para proporcionar alta disponibilidad. La principal ventaja sobre el rol Cluster es la posibilidad de establecer qué ADC es el Activo para una IP Virtual. La desventaja es que no hay sincronización de la configuración entre los CAD. Cualquier cambio debe ser replicado manualmente en cada caja a través de la GUI, o para muchos cambios, puede crear un jetPACK desde un ADC y enviarlo al otro.

- Para hacer que una dirección IP virtual esté "activa", marque la casilla de la columna principal (página de servicios IP)
- Para hacer que una dirección IP virtual sea "pasiva", deje la casilla en blanco en la columna principal (página de servicios IP)
- En el caso de que un servicio Activo falle al Pasivo:
 - Si las dos columnas primarias están marcadas, se produce un proceso de elección y la dirección MAC más baja será la activa
 - Si ambos están desmarcados, se produce el mismo proceso de elección. Además, si ambas están desmarcadas, no hay un retorno automático al CAD activo original

Papel autónomo

Un ADC en el rol de autónomo no se comunicará con ningún otro ADC en lo que respecta a sus servicios, y por lo tanto todos los Servicios Virtuales permanecerán en el estado Verde y conectados. Debe asegurarse de que todos los Servicios Virtuales tienen direcciones IP únicas, o habrá un conflicto en su red.

Ajustes

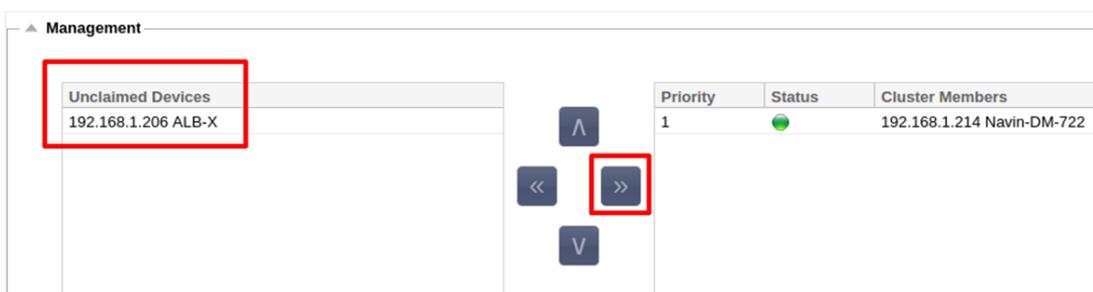


En la sección de configuración, puede establecer la Latencia de conmutación por error en milisegundos, el tiempo que un ADC pasivo esperará antes de hacerse cargo de los servicios virtuales después de que el ADC activo haya fallado.

Recomendamos establecerlo en 10000ms o 10 segundos, pero puede disminuir o aumentar este valor para adaptarlo a su red y a sus necesidades. Los valores aceptables se sitúan entre 1500ms y 20000ms. Si experimenta inestabilidad en el clúster con una latencia más baja, debería aumentar este valor.

Gestión

En esta sección, puede añadir y eliminar miembros del clúster, así como cambiar la prioridad de un ADC en el clúster. La sección consta de dos paneles y un conjunto de flechas entre ellos. El área de la izquierda son los dispositivos no reclamados, mientras que el área de la derecha es el propio clúster.



Añadir un ADC al clúster

- Antes de añadir el ADC al clúster, debe asegurarse de que todos los aparatos ADC han recibido un nombre único establecido en la sección Sistema > Red.
- Debería ver el ADC como prioridad 1 con el estado en verde y su nombre bajo la columna Miembros del clúster en la sección de gestión. Este ADC es el aparato primario por defecto.
- Todos los demás ADCs disponibles aparecerán en la ventana de Dispositivos No Reclamados dentro de la sección de gestión. Un Dispositivo No Reclamado es el ADC que ha sido asignado en el Rol de Cluster pero que no tiene Servicios Virtuales configurados.

- Resalte el ADC de la ventana de dispositivos no reclamados y haga clic en el botón de la flecha derecha.
- Ahora verá el siguiente mensaje:



- Haga clic en Aceptar para promover el CAD al clúster.
- Su ADC debería aparecer ahora como prioridad 2 en la lista de miembros del cluster.



Eliminación de un miembro del clúster

- Resalte el miembro del clúster que desea eliminar del clúster.
- Pulse el botón de la flecha izquierda.



- Se le presentará una solicitud de confirmación.
- Haga clic en OK para confirmar.
- Su CAD será eliminado y se mostrará en el lado de Dispositivos no reclamados.

Cambiar la prioridad de un CAD

Puede haber ocasiones en las que desee cambiar la prioridad de un CAD dentro de la lista de miembros.

- El CAD que encabeza la lista de miembros del clúster recibe la prioridad 1 y es el CAD activo para todos los servicios virtuales
- El ADC que ocupa el segundo lugar en la lista recibe la prioridad 2 y es el ADC pasivo para todos los servicios virtuales
- Para cambiar cuál es el CAD activo simplemente resalte el CAD y haga clic en la flecha hacia arriba hasta que esté en la parte superior de la lista

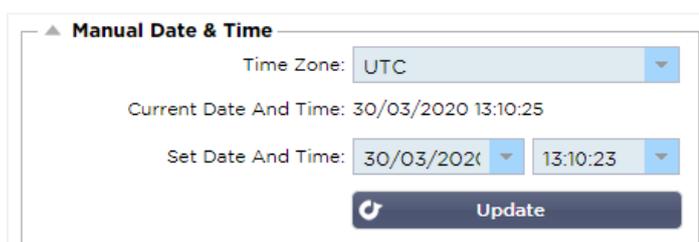


Priority	Status	Cluster Members
1	●	192.168.1.214 Navin-DM-722
2	●	192.168.1.206 ALB-X

Fecha y hora

La sección de fecha y hora permite configurar las características de fecha y hora del CAD, incluyendo la zona horaria en la que se encuentra el CAD. Junto con la zona horaria, la fecha y la hora desempeñan un papel vital en los procesos criptográficos asociados al cifrado SSL.

Fecha y hora manual



Zona horaria

El valor que establezca en este campo representa la zona horaria en la que se encuentra el CAD.

- Haga clic en el cuadro desplegable de la zona horaria y comience a escribir su ubicación. Por ejemplo, Londres
- Cuando empiece a escribir, el CAD mostrará automáticamente las ubicaciones que contengan la letra L.
- Siga escribiendo 'Lon', y así sucesivamente: los lugares de la lista se reducirán a los que contengan 'Lon'.
- Si está en, por ejemplo, Londres, elija Europa/Londres para establecer su ubicación

Si la fecha y la hora siguen siendo incorrectas después del cambio anterior, cambie la fecha manualmente

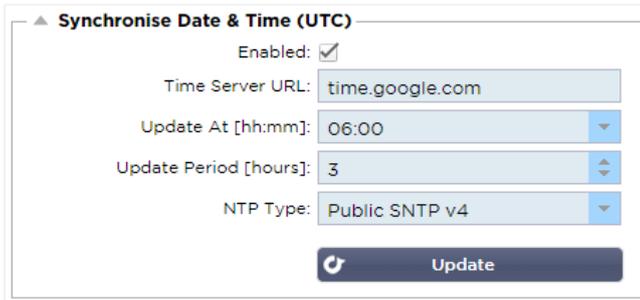
Fijar la fecha y la hora

Este ajuste representa la fecha y la hora reales.

- Elija la fecha correcta en el primer desplegable o, alternativamente, puede escribir la fecha en el siguiente formato DD/MM/AAAA
- Añada la hora en el siguiente formato hh: mm: ss, por ejemplo, 06:00:10 para las 6 de la mañana y 10 segundos.
- Una vez que lo haya introducido correctamente, haga clic en Actualizar para solicitarlo.
- A continuación, debería ver la nueva Fecha y Hora en negrita.

Sincronizar fecha y hora (UTC)

Puede utilizar servidores NTP para sincronizar la fecha y la hora con precisión. Los servidores NTP se encuentran en todo el mundo, y también puede tener su propio servidor NTP interno cuando su infraestructura tenga limitaciones de acceso externo.



▲ Synchronise Date & Time (UTC)

Enabled:

Time Server URL:

Update At [hh:mm]:

Update Period [hours]:

NTP Type:

URL del servidor de tiempo

Introduzca una dirección IP válida o un nombre de dominio completo (FQDN) para el servidor NTP. Si el servidor es un servidor localizado globalmente en Internet, se recomienda utilizar un FQDN.

Actualización a las [hh:mm]

Seleccione la hora programada a la que desea que el ADC se sincronice con el servidor NTP.

Período de actualización [horas]:

Seleccione la frecuencia con la que desea que se produzca la sincronización.

Tipo NTP:

- SNTP público V4 - Este es el método actual y preferido cuando se sincroniza con un servidor NTP. [RFC 5905](#)
- NTP v1 sobre TCP - Versión NTP heredada sobre TCP. [RFC 1059](#)
- NTP v1 sobre UDP - Versión NTP heredada sobre UDP. [RFC 1059](#)

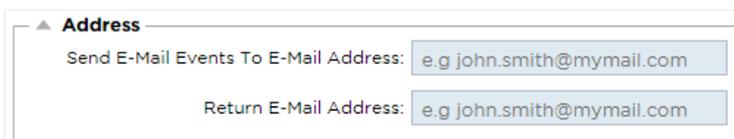
Nota: Tenga en cuenta que la sincronización es sólo en UTC. Si desea establecer una hora local, sólo podrá hacerlo manualmente. Esta limitación se modificará en versiones posteriores para habilitar la posibilidad de seleccionar una zona horaria.

Eventos por correo electrónico

El ADC es un aparato crítico y, como cualquier sistema esencial, está dotado de la capacidad de informar a la administración de sistemas de cualquier problema que pueda requerir atención.

La página Sistema > Eventos de correo electrónico le permite configurar una conexión al servidor de correo electrónico y enviar notificaciones a los administradores del sistema. La página está organizada en las siguientes secciones.

Dirección



▲ Address

Send E-Mail Events To E-Mail Address:

Return E-Mail Address:

Enviar a eventos de correo electrónico a direcciones de correo electrónico

Añada una dirección de correo electrónico válida a la que enviar las alertas, notificaciones y eventos. Ejemplo: support@domain.com. También puede añadir varias direcciones de correo electrónico utilizando un separador de comas.

Dirección de correo electrónico de retorno:

Añada una dirección de correo electrónico que aparecerá en la bandeja de entrada. Ejemplo: adc@domain.com.

Servidor de correo (SMTP)

En esta sección, debe añadir los detalles del servidor SMTP que se utilizará para enviar los correos electrónicos. Asegúrese de que la dirección de correo electrónico que utiliza para el envío está autorizada para ello.

Mail Server [SMTP]

Host Address:

Port: 25

Send Timeout: 2 minutes

Use Authentication:

Security: none

Mail Server Account Name:

Mail Server Password: blank = no change

Update

Test

Dirección del anfitrión

Añada la dirección IP de su servidor SMTP.

Puerto

Añada el puerto de su servidor SMTP. El puerto por defecto para SMTP es el 25 o el 587 si utiliza SSL.

Tiempo de espera de envío

Añada un tiempo de espera SMTP. El valor predeterminado es de 2 minutos.

Utilizar la autenticación

Marque la casilla si su servidor SMTP requiere autenticación.

Seguridad

- Ninguno
- El ajuste por defecto es ninguno.
- SSL - Utilice esta configuración si su servidor SMTP requiere autenticación de capa de sockets seguros.
- TLS - Utilice esta configuración si su servidor SMTP requiere autenticación de Seguridad de la Capa de Transporte.

Nombre de la cuenta del servidor principal

Añada el nombre de usuario necesario para la autenticación.

Contraseña del servidor de correo

Añada la contraseña necesaria para la autenticación.

Notificaciones y alertas

Enabled Notifications And Event Descriptions In Mail

Enable All Event

Disable All Event

IP Service Notice: Service started

Virtual Service Notice: Virtual Service started

Real Server Notice: Server contacted

flightPATH: flightPATH

IP Services Alert: Service stopped

Virtual Service Alert: Virtual Service stopped

Real Server Alert: Server not contactable

Group Notifications Together:

Grouped Mail Description: Event notifications

Send Grouped Mail Every: 30 minutes

Update

Hay varios tipos de notificaciones de eventos que el ADC enviará a las personas configuradas para recibirlos. Puede marcar y habilitar las notificaciones y alertas que deben enviarse. Las notificaciones se producen cuando se contacta con los Servidores Reales o se inician los canales. Las alertas se producen cuando no se puede contactar con los Servidores Reales o los canales dejan de funcionar.

Servicio IP

El aviso de servicio IP le informará cuando alguna dirección IP virtual esté en línea o haya dejado de funcionar. Esta acción se lleva a cabo para todos los servicios virtuales que pertenecen al VIP.

Servicio virtual

Informa al destinatario de que un servicio virtual está en línea o ha dejado de funcionar.

Servidor real

Cuando un servidor real y un puerto se conectan o no son localizables, el CAD enviará el aviso de servidor real.

flightPATH

Este aviso es un correo electrónico que se envía cuando se ha cumplido una condición, y hay una acción configurada que indica al CAD que envíe el evento por correo electrónico.

Notificaciones de grupo

Marque esta opción para agrupar las notificaciones. Si se marca esta opción, todas las notificaciones y alertas se agruparán en un solo correo electrónico.

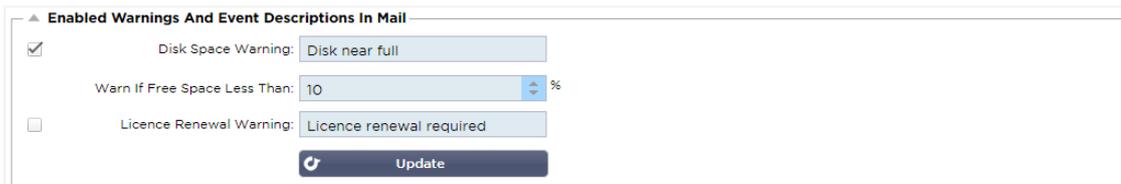
Descripción del correo de grupo

Especifique el asunto pertinente para el correo electrónico de notificación del grupo.

Intervalo de envío del grupo

Especifique el tiempo que desea esperar antes de enviar un correo electrónico de notificación de grupo. El tiempo mínimo es de 2 minutos.

Advertencias



Enabled Warnings And Event Descriptions In Mail

Disk Space Warning: Disk near full

Warn If Free Space Less Than: 10 %

Licence Renewal Warning: Licence renewal required

Update

Hay dos tipos de correos electrónicos de advertencia, y ninguno debe ser ignorado.

Espacio en disco

Establezca el porcentaje de espacio libre en disco antes del cual se enviará el aviso. Cuando se alcance éste, se le enviará un correo electrónico.

Expiración de la licencia

Este ajuste le permite activar o desactivar el correo electrónico de aviso de caducidad de la licencia que se envía al administrador del sistema. Cuando se alcance, se le enviará un correo electrónico.

Historia del sistema

En la sección Sistema, se encuentra la opción Historial del sistema, que permite la entrega de datos históricos para elementos como la CPU, la memoria, las peticiones por segundo y otras características.

Una vez activada, podrá ver los resultados en forma de gráfico a través de la página Ver > Historial. Esta página también le permitirá hacer una copia de seguridad o restaurar los archivos del historial en el CAD local.

Recoger datos

- Para permitir la recogida de datos, marque la casilla.
- A continuación, establezca el intervalo de tiempo en el que desea que el ADC recoja los datos. Este valor de tiempo puede oscilar entre 1-60 segundos.

Mantenimiento

Esta sección aparecerá en gris si ha habilitado el registro histórico. Por favor, desmarque la casilla Habilitado en la sección Recoger datos y haga clic en Actualizar para permitir el mantenimiento de los registros históricos.

Copia de seguridad

Dé a su copia de seguridad un nombre descriptivo. Haga clic en Copia de seguridad para hacer una copia de seguridad de todos los archivos en el CAD

Borrar

Seleccione un archivo de copia de seguridad de la lista desplegable. Haga clic en Borrar para eliminar el archivo de copia de seguridad del CAD.

Restaurar

Seleccione un archivo de copia de seguridad previamente almacenado. Haga clic en Restaurar para rellenar los datos de este archivo de copia de seguridad.

Licencia

La licencia de uso del ADC es de uno de los siguientes modelos, que depende de sus parámetros de compra y del tipo de cliente.

Tipo de licencia	Descripción
Perpetua	Usted, el cliente, tiene derecho a utilizar el CAD y el resto del software a perpetuidad. Ello no impide que tenga que adquirir el soporte para recibir asistencia y actualizaciones.

SaaS	SaaS o Software-as-a-Service significa que usted alquila esencialmente el software sobre una base continua o de pago por uso. En este modelo, usted paga un alquiler anual por el software. No tiene derechos perpetuos para utilizar el software.
MSP	Los proveedores de servicios gestionados pueden ofrecer el ADC como un servicio y adquirir la licencia por VIP, que se cobra y paga anualmente.

Detalles de la licencia

Cada licencia incluye detalles específicos pertinentes a la persona u organización que la adquiere.

▲ Licence Details	
Licence ID:	EA5325D4-4796-48CC-B27E-7382FF02879E
Machine ID:	F43793B-4C5
Issued To:	edgeNEXUS
Contact Person:	Greg Howett
Date Issued:	24 Nov 2020
Name:	Sergey Box

Identificación de la licencia

Este ID de licencia está directamente vinculado al ID de la máquina y a otros detalles específicos de su compra y del CAD. Esta información es esencial y se requiere cuando se desea recuperar las actualizaciones y otros elementos de la App Store.

Identificación de la máquina

El ID de la máquina se genera utilizando la dirección IP eth0 de un dispositivo ADC virtual y el ID MAC de un ADC basado en hardware. Si cambia la dirección IP de un dispositivo ADC virtual, la licencia dejará de ser válida. Tendrá que ponerse en contacto con el servicio de asistencia para obtener ayuda. Le recomendamos que su(s) dispositivo(s) ADC virtual(es) tenga(n) direcciones IP fijas con instrucciones de no cambiarlas. El soporte técnico está disponible levantando un ticket en [HTTPs://edgenexus.io](https://edgenexus.io).

Nota: No debe cambiar la dirección IP ni el MAC ID de sus aparatos ADC. Si está en un marco virtualizado, entonces por favor fije el MAC ID y la dirección IP.

Emitido a

Este valor contiene el nombre del comprador asociado al ID de la máquina del CAD.

Persona de contacto

Este valor contiene la persona de contacto a la que hay que dirigirse en la empresa del cliente asociada al ID de la máquina

Problemas de fechas

La fecha de emisión de la licencia

Nombre

Este valor muestra el nombre descriptivo del dispositivo ADC que usted ha proporcionado.

Instalaciones

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

La sección de instalaciones le proporciona información sobre las funciones del CAD que tienen licencia de uso y la validez de la licencia. También se muestra el rendimiento que se ha licenciado para el ADC y el número de Servidores Reales. Esta información depende de la licencia que haya adquirido.

Instale la licencia

Install Licence

Upload Licence:

Paste Licence:

- La instalación de una nueva licencia es muy sencilla. Cuando reciba su licencia nueva o de sustitución de Edgenexus, ésta se enviará en forma de archivo de texto. Puede abrir el archivo y, a continuación, copiar y pegar el contenido en el campo Pegar licencia.
- También puede subirlo al CAD si copiar/pegar no es una opción para usted.
- Una vez hecho esto, por favor, pulse el botón de actualización
- La licencia ya está instalada.

Información sobre el servicio de licencias

Al hacer clic en el botón de información sobre el servicio de licencias, se mostrará toda la información sobre la licencia. Esta función puede utilizarse para enviar los detalles al personal de soporte.

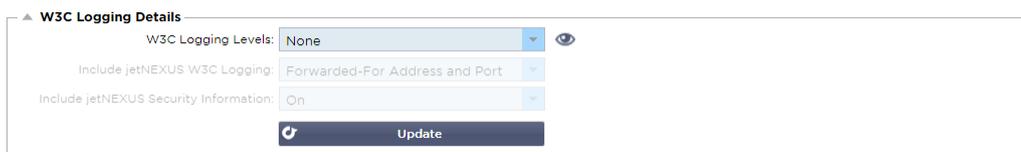
Registro

La página Sistema > Registro le permite establecer los niveles de registro W3C y especificar el servidor remoto al que se exportarán automáticamente los registros. La página está organizada en las cuatro secciones siguientes.

Detalles del registro del W3C

La activación del registro W3C hará que el CAD comience a registrar un archivo de registro compatible con el W3C. Un registro W3C es un registro de acceso para servidores web en el que se generan archivos de texto que contienen datos sobre cada solicitud de acceso, incluyendo la dirección de protocolo de Internet (IP) de origen, la versión HTTP, el tipo de navegador, la página de referencia y la marca de tiempo. El formato fue desarrollado por el Consorcio de la World Wide Web (W3C), una organización que promueve estándares para la evolución de la Web. El archivo está en texto ASCII, con columnas delimitadas por espacios. El archivo contiene líneas de comentario que comienzan con el carácter #. Una de estas líneas

de comentario es una línea que indica los campos (proporcionando los nombres de las columnas) para que los datos puedan ser extraídos. Hay archivos separados para los protocolos HTTP y FTP.



Niveles de registro del W3C

Hay diferentes niveles de registro disponibles y, según el tipo de servicio, los datos proporcionados varían.

La siguiente tabla describe los niveles de registro para W3C HTTP.

Valor	Descripción
Ninguno	El registro del W3C está desactivado.
Breve	Los campos presentes son: #Campos: tiempo c-ip c-puerto s-ip método uri x-c-versión x-r-versión sc-estado cs-bytes sr-bytes rs-bytes sc-bytes x-porcentaje de tiempo tomado x-tiempo de ida y vuelta cs(User-Agent) x-sc(Content-Type).
Completo	Este es un formato más compatible con el procesador, con campos de fecha y hora separados. Consulte el resumen de los campos a continuación para obtener información sobre el significado de los mismos. Los campos presentes son: #Campos: fecha hora c-ip c-puerto cs-nombre-de-usuario s-ip s-puerto cs-método cs-ur- -consulta sc-estado cs(User-Agent) referer x-c-versión x-r-versión cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x-roun-trip-time x-sc(Content-Type).
Sitio	Este formato es muy similar al "Completo" pero tiene un campo adicional. Consulte el resumen de los campos a continuación para obtener información sobre el significado de los mismos. Los campos presentes son: #Campos: fecha hora x-mil c-ip c-puerto cs-nombre-de-usuario s-ip s-puerto cs-host cs-método cs-uri-stem cs-ur--query sc-status cs(User-Agent) referer x-c-versión x-r-versión cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x-round--trip-time x-sc(Content-Type).
Diagnóstico	Este formato está lleno de todo tipo de información relevante para el personal de desarrollo y apoyo. Consulte el resumen de los campos a continuación para obtener información sobre el significado de los mismos. Los campos presentes son: Campos fecha hora c-ip c-puerto cs-nombre de usuario s-ip s-puerto x-xff x-xffcustom cs-host x-r-ip x-r-puerto 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 siguiente tabla describe los niveles de registro para el FTP del W3C.

Valor	Descripción
Breve	#Campos: fecha hora c-ip c-puerto s-ip s-puerto r-ip cs-método cs-param sc-estado sc-param sr-método sr-param rs-estado rs-param
Completo	#Campos: fecha hora c-ip c-puerto s-ip s-puerto r-ip cs-método cs-param cs-bytes sc-estado sc-param sc-bytes sr-método sr-param sr-bytes rs-estado rs-param rs-bytes
Diagnóstico	#Campos: fecha hora c-ip c-puerto s-ip s-puerto r-ip cs-método cs-param cs-bytes sc-estado sc-param sc-bytes sr-método sr-param sr-bytes rs-estado rs-param rs-bytes

Incluir el registro W3C

Esta opción le permite establecer qué información del CAD debe incluirse en los registros del W3C.

Valor	Descripción
Dirección de red y puerto del cliente	El valor mostrado aquí muestra la dirección IP real del cliente junto con el puerto.
Dirección de red del cliente	Esta opción incluirá y sólo mostrará la dirección IP real del cliente.
Dirección y puerto de reenvío	Esta opción mostrará los detalles contenidos en la cabecera XFF, incluyendo la dirección y el puerto.
Dirección de reenvío	Esta opción mostrará los detalles contenidos en la cabecera XFF, incluyendo sólo la dirección.

Incluir información de seguridad

Este menú consta de dos opciones:

Valor	Descripción
En	Este ajuste es global. Si está activado, el nombre de usuario se añadirá al registro W3C cuando cualquier servicio virtual utilice la autenticación y tenga activado el registro W3C.
Off	Esto desactivará la capacidad de registrar el nombre de usuario en el registro del W3C a nivel global.

Servidor Syslog

▲ Syslog

Message Level:

Esta sección le permite establecer el nivel de registro de mensajes que se realiza en el servidor SYSLOG. Las opciones disponibles son las siguientes.

Error

Warning

Notice

Info

Servidor Syslog remoto

▲ Remote Syslog Server

Syslog Server 1: Port: Enabled:

Syslog Server 2: Port: Enabled:

En esta sección, puede configurar dos servidores Syslog externos para enviar todos los registros del sistema.

- Añada la dirección IP de su servidor Syslog
- Añadir el puerto
- Elija si desea utilizar TCP o UDP
- Marque la casilla Habilitado para comenzar el registro
- Haga clic en Actualizar

Almacenamiento remoto de registros

Remote Log Storage:

IP Address:

Share Name:

Directory:

Username:

Password:

Todos los registros del W3C se almacenan en forma comprimida en el CAD cada hora. Los archivos más antiguos se borrarán cuando quede un 30% de espacio en el disco. Si desea exportarlos a un servidor remoto para guardarlos, puede configurarlo utilizando un recurso compartido SMB. Tenga en cuenta que el registro W3C no se transferirá a la ubicación remota hasta que el archivo se haya completado y comprimido. Como los registros se escriben cada hora, esto podría llevar hasta dos horas en un dispositivo de máquina virtual y cinco horas para un dispositivo de hardware.

Incluiremos un botón de prueba en futuras versiones para que pueda comprobar que su configuración es correcta.

Col1	Col2
Almacenamiento remoto de registros	Marque la casilla para activar el almacenamiento remoto de registros
Dirección IP	Especifique la dirección IP de su servidor SMB. Debe estar en notación decimal con puntos. Ejemplo: 10.1.1.23
Comparte el nombre	Especifique el nombre del recurso compartido en el servidor SMB. Ejemplo: w3c.
Directorio	Especifique el directorio en el servidor SMB. Ejemplo: /log.
Nombre de usuario	Especifique el nombre de usuario para el recurso compartido SMB.
Contraseña	Especifique la contraseña para el recurso compartido SMB

Resumen del campo

Condición	Descripción
Fecha	No localizado = siempre AAAA-MM-DD (GMT/UTC)
Tiempo	No localizado = HH:MM:SS o HH:MM:SS.ZZZ (GMT/UTC) * Nota-desgraciadamente esto tiene dos formatos (Sitio no tiene milisegundos .ZZZ)
x-mil	Sólo formato de sitio = milisegundo de sello de tiempo
c-ip	IP del cliente como mejor pueda derivarse de la red o de la cabecera X-Forwarded-For
c-port	Puerto del cliente como mejor se pueda derivar de la red o de la cabecera X-Forwarded-For
cs-nombre de usuario	Campo de solicitud del nombre de usuario del cliente
s-ip	Puerto de escucha del ALB
s-port	VIP de escucha de ALB

x-xff	Valor de la cabecera X-Forwarded-For
x-xffcustom	Valor de la cabecera de solicitud de tipo X-Forwarded-For configurada
cs-host	El nombre del host en la solicitud
x-r-ip	Dirección IP del servidor real utilizado
puerto x-r	Puerto del servidor real utilizado
cs-método	Método de solicitud HTTP * excepto formato breve
método	* Sólo el formato breve utiliza este nombre para el método cs
cs-uri-stem	Ruta del recurso solicitado * excepto formato breve
cs-uri-query	Consulta del recurso solicitado * excepto formato breve
uri	* El formato breve registra una ruta combinada y una cadena de consulta
sc-status	Código de respuesta HTTP
cs(Usuario-Agente)	Cadena User-Agent del navegador (tal como la envía el cliente)
referente	Página de referencia (como la enviada por el cliente)
x-c-versión	Versión HTTP de la solicitud del cliente
x-r-versión	Contenido-Respuesta del servidor Versión HTTP
cs-bytes	Bytes del cliente, en la solicitud
sr-bytes	Bytes reenviados al Servidor Real, en la solicitud
rs-bytes	Bytes del Servidor Real, en la respuesta
sc-bytes	Bytes enviados al cliente, en la respuesta
x-percent	Porcentaje de compresión * = $100 * (1 - salida / entrada)$ incluyendo las cabeceras
tiempo tomado	Cuánto tiempo tardó el Servidor Real en segundos
x-trip-times nuevo pcon	milisegundo desde la conexión hasta la publicación en la "lista de novatos" milisegundo desde la conexión hasta la colocación de la conexión al Servidor Real
acon	milisegundo desde que se conecta hasta que se termina de colocar la conexión con el Servidor Real
rcon	milisegundo desde la conexión hasta el establecimiento de la conexión con el servidor real
rqf	milisegundo desde la conexión hasta la recepción del primer byte de solicitud del cliente
rql	milisegundo desde la conexión hasta la recepción del último byte de solicitud del cliente
tqf	milisegundo desde la conexión hasta el envío del primer byte de solicitud al Servidor Real
tql	milisegundo desde la conexión hasta el envío del último byte de solicitud al Servidor Real
rsf	milisegundo desde la conexión hasta la recepción del primer byte de respuesta del Servidor Real
rsl	milisegundo desde la conexión hasta la recepción del último byte de respuesta del Servidor Real

tsf	milisegundo desde la conexión hasta el envío del primer byte de respuesta al cliente
tsl	milisegundo desde la conexión hasta el envío del último byte de respuesta al cliente
dis	milisegundo desde la conexión hasta la desconexión (ambos lados - el último en desconectarse)
Registrar	milisegundo desde la conexión a este registro normalmente seguido de (Política de equilibrio de carga y razonamiento)
x-round-trip-time	Cuánto tiempo tardó el ALB en segundos
x-closed-by	Qué acción ha provocado el cierre de la conexión (o el mantenimiento de la misma)
x-compress-action	Cómo se llevó a cabo la compresión, o se evitó
x-sc(Tipo de contenido)	Tipo de contenido de la respuesta
x-cache-action	Cómo ha respondido o se ha impedido el almacenamiento en caché
x-finish	Disparador que causó esta fila de registro

Borrar archivos de registro

▲ Clear Log Files

Log Type:

Esta función le permite borrar los archivos de registro del CAD. Puede seleccionar el tipo de registro que desea borrar en el menú desplegable y luego hacer clic en el botón Borrar.

Red

La sección de Red dentro de la Biblioteca permite la configuración de las interfaces de red del CAD y su comportamiento.

Configuración básica

▲ Basic Setup

ALB Name:

IPv4 Gateway: DNS Server 1: DNS Server 2:

IPv6 Gateway:

Nombre del ALB

Especifique un nombre para su dispositivo ADC. Tenga en cuenta que esto no puede cambiarse si hay más de un miembro en el clúster. Por favor, consulte la sección de Clustering.

Pasarela IPv4

IPv4 Gateway:

Especifique la dirección de la puerta de enlace IPv4. Esta dirección deberá estar en la misma subred que un adaptador existente. Si añade la puerta de enlace de forma incorrecta, verá una cruz blanca en un círculo rojo. Cuando añada una puerta de enlace correcta, verá un cartel verde de éxito en la parte inferior de la página y una marca blanca en un círculo verde junto a la dirección IP.

Pasarela IPv6

Especifique la dirección de la pasarela IPv6. Esta dirección deberá estar en la misma subred que un adaptador existente. Si añade la puerta de enlace de forma incorrecta, verá una cruz blanca en un círculo rojo. Cuando añada una puerta de enlace correcta, verá un cartel verde de éxito en la parte inferior de la página y una marca blanca en un círculo verde junto a la dirección IP.

Servidor DNS 1 y Servidor DNS 2

Añada la dirección IPv4 de su primer y segundo servidor DNS (opcional).

Detalles del adaptador

Esta sección del panel Red muestra las interfaces de red que están instaladas en su dispositivo ADC. Puede añadir y eliminar adaptadores según sea necesario.

Adapter	VLAN	IP Address	Subnet Mask	Gateway	RP Filter	Description	Web Console	REST
eth0		192.168.1.111	255.255.255.0		<input checked="" type="checkbox"/>	Green side	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Columna	Descripción
Adaptador	Esta columna muestra los adaptadores físicos instalados en su aparato. Elija un adaptador de la lista de adaptadores disponibles haciendo clic sobre él - un doble clic pondrá la línea del listado en modo de edición.
VLAN	Haga doble clic para añadir el ID de la VLAN para el adaptador. Una VLAN es una red de área local virtual que crea un dominio de difusión distinto. Una VLAN tiene los mismos atributos que una LAN física, pero permite agrupar las estaciones finales con mayor facilidad si no están en el mismo conmutador de red
Dirección IP	Haga doble clic para añadir la dirección IP asociada a la interfaz del adaptador. Puede añadir varias direcciones IP a la misma interfaz. Debe ser un número IPv4 de 32 bits en notación decimal cuadrada. Ejemplo 192.168.101.2
Máscara de subred	Haga doble clic para añadir la máscara de subred asignada a la interfaz del adaptador. Debe ser un número IPv4 de 32 bits en notación decimal cuadrada. Ejemplo 255.255.255.0
Puerta de enlace	Añada una puerta de enlace para la interfaz. Cuando se añada esto, el ADC configurará una política simple que permitirá que las conexiones iniciadas desde esta interfaz sean devueltas a través de esta interfaz al enrutador de la puerta de enlace especificada. Esto permite que el ADC se instale en entornos de red más complejos sin la molestia de configurar manualmente un complejo enrutamiento basado en políticas.
Descripción	Haga doble clic para añadir una descripción para su adaptador. Ejemplo de interfaz pública. Nota: El ADC nombrará automáticamente la primera interfaz Lado Verde, la segunda interfaz Lado Rojo y la tercera interfaz Lado 3, etc. Por favor, siéntase libre de cambiar estas convenciones de nomenclatura a su propia elección.
Consola web	Haga doble clic en la columna y luego marque la casilla para asignar la interfaz como dirección de gestión para la consola web de la interfaz gráfica de usuario. Tenga mucho cuidado al cambiar la interfaz en la que escuchará la Consola Web. Deberá tener configurado el enrutamiento correcto o estar en la misma subred que

la nueva interfaz para poder llegar a la Consola Web después del cambio. La única forma de volver a cambiar esto es acceder a la línea de comandos y emitir el comando `set greenside`. Esto borrará todas las interfaces excepto `eth0`.

Interfaces

La sección de Interfaces dentro del panel de Red permite la configuración de ciertos elementos pertenecientes a la interfaz de red. También puede eliminar una interfaz de red del listado haciendo clic en el botón Eliminar. Cuando se utiliza un dispositivo virtual, las interfaces que se ven aquí están limitadas por el marco de virtualización subyacente.



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

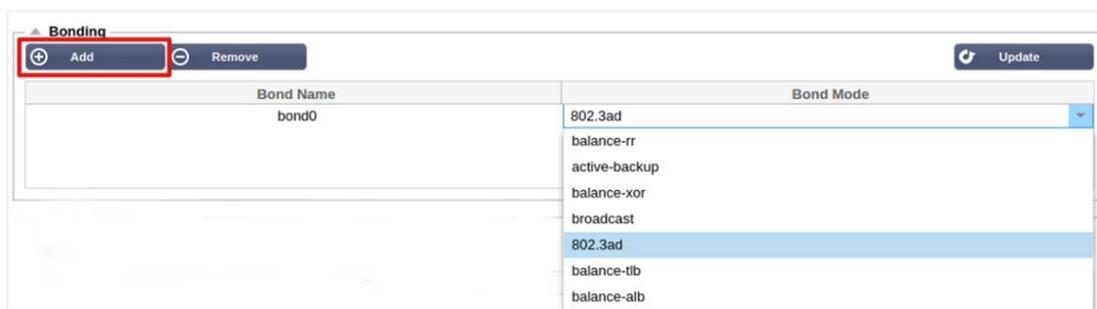
Columna	Descripción
Tipo de ETH	Este valor indica la referencia interna del SO a la interfaz de red. Este campo no se puede personalizar. Los valores comienzan con <code>ETH0</code> y continúan en secuencia dependiendo del número de interfaces de red.
Estado	Esta indicación gráfica muestra el estado actual de la interfaz de red. Un estado verde muestra que la interfaz está conectada y en funcionamiento. A continuación se muestran otros indicadores de estado. <ul style="list-style-type: none">  Adaptador UP  Adaptador de baja  Adaptador desenchufado  Falta el adaptador
Velocidad	Por defecto, este valor está configurado para autonegociar la velocidad. Pero puede cambiar la velocidad de red de la interfaz a cualquier valor disponible en el desplegable (<code>10/100/1000/AUTO</code>).
Dúplex	El valor de este campo es personalizable, y puede elegir entre Auto (por defecto), Full-Duplex y Half-Duplex.
Vinculación	Puede elegir uno de los tipos de enlace que haya definido. Consulte la sección sobre vinculación para obtener más detalles.

Vinculación

Se utilizan muchos nombres para titular la unión de interfaces de red: Port Trunking, Channel Bonding, Link Aggregation, NIC teaming y otros. La vinculación combina o agrega varias conexiones de red en una única interfaz vinculada a un canal. La vinculación permite que dos o más interfaces de red actúen como una sola, aumentando el rendimiento y proporcionando redundancia o conmutación por error.

El núcleo del CAD tiene un controlador de enlace incorporado para agregar varias interfaces de red físicas en una única interfaz lógica (por ejemplo, agregando `eth0` y `eth1` en `bond0`). Para cada interfaz de enlace, puede definir el modo y las opciones de supervisión del enlace. Hay siete opciones de modo diferentes, cada una de las cuales proporciona características específicas de equilibrio de carga y tolerancia a fallos. Éstas se muestran en la imagen siguiente.

NOTA: LA VINCULACIÓN SÓLO PUEDE CONFIGURARSE PARA LOS APARATOS ADC BASADOS EN HARDWARE.

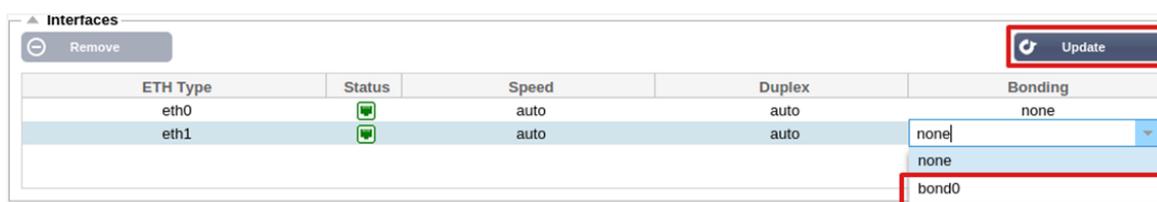


Creación de un perfil de vinculación

- Pulse el botón Añadir para añadir un nuevo bono
- Proporcione un nombre para la configuración de enlace
- Elija el modo de unión que desea utilizar

A continuación, en la sección Interfaces, seleccione el modo de enlace que desea utilizar en el campo desplegable Enlace para la interfaz de red.

En el ejemplo siguiente, eth0, eth1 y eth2 son ahora parte de bond0. Mientras que Eth0 permanece por su cuenta como interfaz de gestión.



Modos de vinculación

Modo de unión	Descripción
balance-rr:	Los paquetes se transmiten/reciben secuencialmente a través de cada interfaz uno por uno.
respaldo activo:	En este modo, una interfaz estará activa y la segunda interfaz estará en espera. Esta interfaz secundaria sólo se activa si falla la conexión activa de la primera interfaz.
balance-xor:	Transmite basándose en la dirección MAC de origen XOR con la dirección MAC de destino. Esta opción selecciona el mismo esclavo para cada dirección MAC de destino.
emitido:	Este modo transmitirá todos los datos en todas las interfaces esclavas.
802.3ad:	Crea grupos de agregación que comparten la misma configuración de velocidad y dúplex y utiliza todos los esclavos del agregador activo siguiendo la especificación 802.3ad.
balance-tlb:	El modo de enlace de equilibrio de carga de transmisión adaptable: Proporciona una unión de canales que no requiere ningún soporte especial del conmutador. El tráfico saliente se distribuye en función de la carga actual (calculada en relación con la velocidad) en cada esclavo. El esclavo actual recibe el tráfico entrante. Si el esclavo receptor falla, otro esclavo toma la dirección MAC del esclavo receptor que ha fallado.
balance-alb:	El modo de enlace de equilibrio de carga adaptable: también incluye balance-tlb más equilibrio de carga de recepción (rlb) para el tráfico IPV4 y no requiere

ningún soporte especial del conmutador. El equilibrio de carga de recepción se consigue mediante la negociación ARP. El controlador de enlace intercepta las respuestas ARP enviadas por el sistema local en su salida y sobrescribe la dirección de hardware de origen con la dirección de hardware única de uno de los esclavos en el enlace, de forma que los diferentes pares utilizan diferentes direcciones de hardware para el servidor.

Ruta estática

Habrà ocasiones en las que necesite crear rutas estáticas para subredes específicas dentro de su red. El CAD le ofrece la posibilidad de hacerlo mediante el módulo de rutas estáticas.

Destination	Gateway	Mask	Adapter	Active
10.117.64	192.168.1.254	255.255.255.0	eth0	

Añadir una ruta estática

- Haga clic en el botón Añadir ruta
- Rellene el campo utilizando los datos de la tabla siguiente como guía.
- Haga clic en el botón Actualizar cuando haya terminado.

Campo	Descripción
Destino	Introduzca la dirección de red de destino en notación decimal con puntos. Ejemplo 123.123.123.5
Puerta de enlace	Introduzca la dirección IPv4 de la pasarela en notación decimal con puntos. Ejemplo 10.4.8.1
Máscara	Introduzca la máscara de subred de destino en notación decimal con puntos. Ejemplo 255.255.255.0
Adaptador	Introduzca el adaptador por el que se puede acceder a la pasarela. Ejemplo eth1.
Activo	Una cruz verde indicará que se puede alcanzar la pasarela. Una cruz roja indicará que no se puede alcanzar la pasarela en esa interfaz. Asegúrese de que ha configurado una interfaz y una dirección IP en la misma red que la pasarela

Detalles de la ruta estática

Esta sección proporcionará información sobre todas las rutas configuradas en el CAD.

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

Configuración avanzada de la red

¿Qué es Nagle?

El algoritmo de Nagle mejora la eficiencia de las redes TCP/IP al reducir el número de paquetes que deben enviarse por la red. Ver [EL ARTÍCULO DE WIKIPEDIA SOBRE NAGLE](#)

Servidor Nagle

Marque esta casilla para activar la configuración del Nagle del servidor. El Nagle del Servidor es un medio para mejorar la eficiencia de las redes TCP/IP reduciendo el número de paquetes que deben enviarse por la red. Este ajuste se aplica al lado del servidor de la transacción. Hay que tener cuidado con los ajustes del servidor, ya que el Nagle y el ACK retardado pueden afectar gravemente al rendimiento.

Cliente Nagle

Marque la casilla para activar la configuración de Nagle del cliente. Como en el caso anterior, pero aplicado al lado del Cliente de la transacción.

SNAT

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

SNAT significa Source Network Address Translation (traducción de direcciones de red de origen), y los diferentes proveedores tienen ligeras variaciones en la implementación de SNAT. Una explicación sencilla del SNAT del EdgeADC sería la siguiente.

En circunstancias normales, las solicitudes entrantes se dirigirían al VIP que vería la IP de origen de la solicitud. Así, por ejemplo, si un punto final del navegador tuviera una dirección IP de 81.71.61.51, ésta sería visible para el VIP.

Cuando SNAT está en vigor, la IP de origen original de la solicitud quedará oculta para el VIP y, en su lugar, verá la dirección IP proporcionada en la regla SNAT. De este modo, SNAT puede utilizarse en los modos de equilibrio de carga de Capa 4 y Capa 7.

Campo	Descripción
Fuente IP	La dirección IP de origen es opcional, y puede ser una dirección IP de red (con /máscara) o una dirección IP simple. La máscara puede ser una máscara de red o un número simple, especificando el número de 1's a la izquierda de la máscara de red. Así, una máscara de /24 equivale a 255.255.255.0.
IP de destino	La dirección IP de destino es opcional, y puede ser una dirección IP de red (con /máscara) o una dirección IP simple. La máscara puede ser una máscara de red o un número plano, especificando el número de 1's a la izquierda de la máscara de red. Así, una máscara de /24 equivale a 255.255.255.0.
Puerto de origen	El puerto de origen es opcional, puede ser un solo número, en cuyo caso especifica sólo ese puerto, o puede incluir dos puntos, que especifica un rango de puertos. Ejemplos: 80 o 5900:5905.
Puerto de destino	El puerto de destino es opcional, puede ser un solo número, en cuyo caso especifica sólo ese puerto, o puede incluir dos puntos, que especifica un rango de puertos. Ejemplos: 80 o 5900:5905.
Protocolo	Puede elegir si desea utilizar SNAT en un solo protocolo o en todos los protocolos. Le sugerimos que sea específico para ser más preciso.
SNAT a IP	SNAT a IP es una dirección IP obligatoria o un rango de direcciones IP. Ejemplos: 10.0.0.1 o 10.0.0.1-10.0.3.
SNAT a Puerto	El puerto SNAT a es opcional, puede ser un solo número, en cuyo caso especifica sólo ese puerto, o puede incluir un guión, que especifica un rango de puertos. Ejemplos: 80 o 5900-5905.

Notas	Utilice esto para poner un nombre amigable que le recuerde por qué existen las reglas. Esto también es útil para la depuración en el Syslog.
-------	--

Potencia

Esta función del sistema de CAD también le permite realizar varias tareas relacionadas con la energía en su CAD.

Reinicie

▲ **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 1631) 3j1329

 Restart

Este ajuste inicia un reinicio global de todos los Servicios y, en consecuencia, interrumpe todas las conexiones actualmente activas. Todos los Servicios se reanudarán automáticamente después de un breve período, pero el tiempo dependerá de cuántos Servicios estén configurados. Aparecerá una ventana emergente solicitando confirmación para la acción de reinicio.

Reiniciar

▲ **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

Al hacer clic en el botón de reinicio, el CAD se apagará y volverá a estar activo automáticamente. Aparecerá una ventana emergente solicitando confirmación para la acción de reinicio.

Apagado

▲ **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

Al hacer clic en el botón de apagado se apagará el ADC. Si se trata de un aparato de hardware, necesitará acceso físico al dispositivo para volver a encenderlo. Aparecerá una ventana emergente solicitando confirmación para la acción de apagado.

Seguridad

Esta sección le permite cambiar la contraseña de la consola web y habilitar o deshabilitar el acceso a Secure Shell. También permite habilitar la capacidad de la API REST.

SSH

▲ **SSH**

Secure Shell Remote Conn:

Opción	Descripción
Conexión remota Secure Shell	Marque la casilla si desea acceder al CAD mediante SSH. "Putty" es una excelente aplicación para hacerlo.

Consola web

Certificado SSL Elija un certificado de la lista desplegable. El certificado que elija se utilizará para asegurar su conexión a la interfaz de usuario web del ADC. Puede crear un certificado autofirmado dentro del ADC o importar uno desde la sección de [CERTIFICADOS SSL](#).

Opción	Descripción
Puerto seguro	El puerto por defecto para la consola web es TCP 443. Si desea utilizar un puerto diferente por razones de seguridad, puede cambiarlo aquí.

API REST

La API REST, también conocida como API RESTful, es una interfaz de programación de aplicaciones que se ajusta al estilo arquitectónico REST y permite configurar el CAD o extraer datos del mismo. El término REST significa transferencia de estado representacional y fue creado por el informático Roy Fielding.

Opción	Descripción
Habilitar REST	Marque esta casilla para habilitar el acceso mediante la API REST. Tenga en cuenta que también tendrá que configurar en qué adaptador se habilita REST. Vea la nota en el enlace de Cog más abajo.
Certificado SSL	Elija un certificado para el servicio REST. El desplegable mostrará todos los certificados instalados en el CAD.
Puerto	Establezca el puerto para el servicio REST. Es una buena idea utilizar un puerto distinto al 443.
Dirección IP	Esto mostrará la dirección IP a la que está vinculado el servicio REST. Puede hacer clic en el enlace Cog para acceder a la página de red y cambiar en qué adaptador está habilitado el servicio REST.
Enlace con el engranaje	Al hacer clic en este enlace, accederá a la página de la red, donde podrá configurar un adaptador para el REST.

Documentación para la API REST

La documentación sobre cómo utilizar la API REST está disponible: [jetAPI | 4.2.3 | jetNEXUS | SwaggerHub](#)

*Nota: Si obtiene errores en la página de Swagger es porque tienen un problema de soporte de cadenas de consulta
Desplácese más allá de los errores hasta la API REST de jetNEXUS*

Ejemplos

GUID utilizando CURL:

- Comando

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

- devolverá

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

- Validez
 - El GUID es válido durante 24 horas

Detalles de la licencia

- Comando

```
curl -k https://<resto ip>/GET/39 -GET -b 'GUID=<guid>'
```

SNMP

La sección SNMP permite la configuración de la MIB SNMP que reside en el ADC. La MIB puede entonces ser consultada por software de terceros capaz de comunicarse con dispositivos equipados con SNMP.

Configuración de SNMP

Opción	Descripción
SNMP v1 / V2C	Marque la casilla para activar el MIB V1/V2C. SNMP v1 se ajusta a la RFC-1157. SNMP V2c se ajusta a RFC-1901-1908
SNMP v3	Marque la casilla para habilitar el MIB V3. RFC-3411-3418. El nombre de usuario para v3 es admin. Ejemplo:- snmpwalk -v3 -u admin -A jetnexus -l authNoPriv 192.168.1.11 1.3.6.1.4.1.38370
Cadena comunitaria	Es la cadena de sólo lectura establecida en el agente y utilizada por el gestor para recuperar la información SNMP. La cadena de comunidad por defecto es jetnexus
Frase de paso	Esta es la contraseña que se necesita cuando se habilita el SNMP v3 y debe tener al menos 8 caracteres o más y contener letras Aa-Zz y números 0-9 solamente. La frase de contraseña por defecto es jetnexus

MIB SNMP

La información que se puede ver a través de SNMP está definida por la Base de Información de Gestión (MIB). Las MIB describen la estructura de los datos de gestión y utilizan identificadores de objetos jerárquicos (OID). Cada OID puede leerse a través de una aplicación de gestión SNMP.

Descarga de MIB

El MIB puede descargarse [aquí](#):

ADC OID

ROOT OID

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

Nuestras 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 (1.3.6.1.4.1.38370.1.1.0)

.2 jetnexusOverallOutputBytes (1.3.6.1.4.1.38370.1.2.0)

.3 jetnexusCompressedInputBytes (1.3.6.1.4.1.38370.1.1.3.0)

.4 jetnexusCompressedOutputBytes (1.3.6.1.4.1.38370.1.4.0)

.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 (1.3.6.1.4.1.38370.1.8.0)

.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)

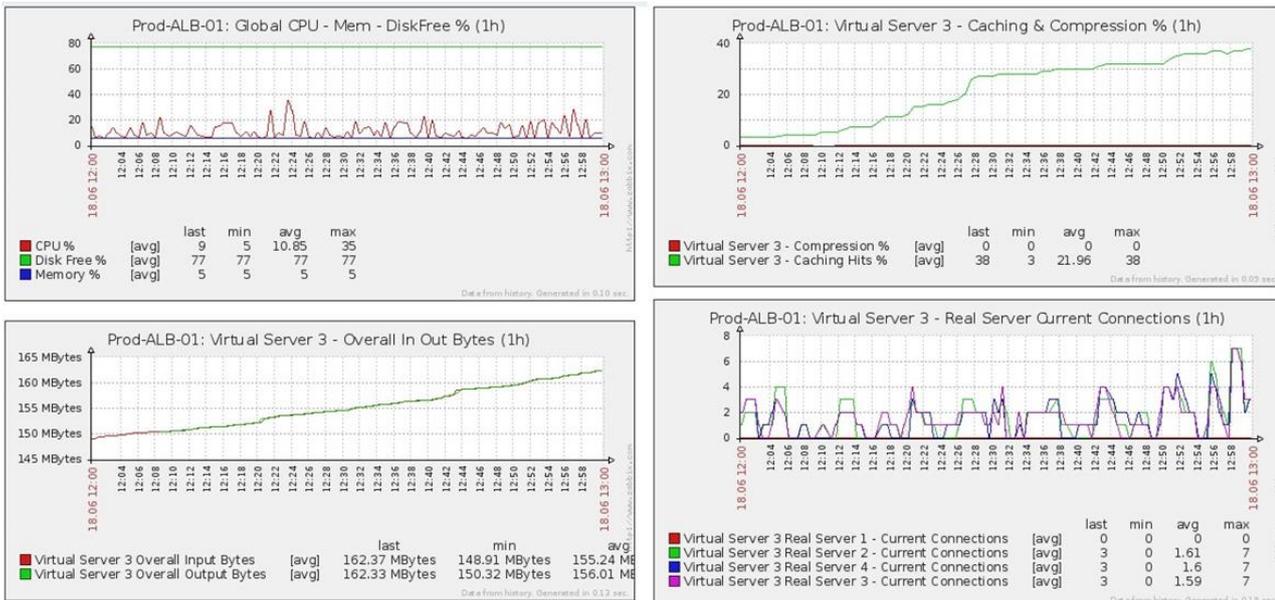
.9 jnrealserverPoolUsage (1.3.6.1.4.1.38370.1.3.1.9)

.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)

Gráficos históricos

El mejor uso de la MIB SNMP personalizada del ADC es la posibilidad de descargar el gráfico histórico a una consola de gestión de su elección. A continuación se muestran algunos ejemplos de Zabbix que sondean un CAD para varios valores OID enumerados anteriormente.



Usuarios y registros de auditoría

El CAD ofrece la posibilidad de tener un conjunto interno de usuarios para configurar y definir lo que hace el CAD. Los usuarios definidos dentro del CAD pueden realizar una serie de operaciones en función del rol que se les asigne.

Hay un usuario por defecto llamado **admin** que se utiliza cuando se configura por primera vez el CAD. La contraseña por defecto para admin es **jetnexus**.

Usuarios

La sección de usuarios le permite crear, editar y eliminar usuarios del CAD.



Añadir usuario

Users

Username:

New Password: 6 or more letters and numbr

Confirm Password: 6 or more letters and numbr

Group Membership: Admin

GUI Read Write
 GUI Read
 SSH
 API
 Add-Ons

Haga clic en el botón Añadir usuario que se muestra en la imagen anterior para que aparezca el cuadro de diálogo Añadir usuario.

Parámetro	Descripción/Uso
Nombre de usuario	<p>Introduzca un nombre de usuario de su elección El nombre de usuario debe cumplir con lo siguiente:</p> <ul style="list-style-type: none"> • Número mínimo de caracteres 1 • Número máximo de caracteres 32 • Las letras pueden ser mayúsculas y minúsculas • Se pueden utilizar números • Los símbolos no están permitidos
Contraseña	<p>Introduzca una contraseña fuerte que se ajuste a los siguientes requisitos</p> <ul style="list-style-type: none"> • Número mínimo de caracteres 6 • Número máximo de caracteres 32 • Debe utilizar al menos una combinación de letras y números • Las letras pueden ser mayúsculas o minúsculas • Los símbolos están permitidos excepto los del ejemplo siguiente £, %, &, <, >
Confirme la contraseña	Confirme de nuevo la contraseña para asegurarse de que es correcta
Afiliación al grupo	<p>Marque el grupo al que desea que pertenezca el usuario.</p> <ul style="list-style-type: none"> • Admin - Este grupo puede hacer todo • GUI Lectura Escritura - Los usuarios de este grupo pueden acceder a la GUI y realizar cambios a través de la misma • Lectura de la interfaz gráfica de usuario - Los usuarios de este grupo pueden acceder a la interfaz gráfica de usuario sólo para ver información. No se pueden realizar cambios • SSH - Los usuarios de este grupo pueden acceder al ADC a través de Secure Shell. Esta elección dará acceso a la línea de comandos, que tiene un conjunto mínimo de comandos disponibles • API - Los usuarios de este grupo tendrán acceso a la interfaz programable SOAP y REST. REST estará disponible a partir de la versión de software 4.2.1

Tipo de usuario



Usuario local

El CAD en rol de H/A autónomo o manual creará sólo usuarios locales
Por defecto, un usuario local llamado "admin" es miembro del grupo admin. Por compatibilidad con el pasado, este usuario nunca puede ser eliminado
Puede cambiar la contraseña de este usuario o borrarla, pero no puede borrar el último admin local



Usuario del clúster

El rol de ADC en Cluster creará sólo usuarios de Cluster
Los usuarios del clúster se sincronizan en todos los CAD del clúster
Cualquier cambio en un usuario del cluster cambiará en todos los miembros del cluster
Si está conectado como usuario del clúster, no podrá cambiar los roles de Clúster a Manual o Stand-Alone



Clúster y usuario local

Todos los usuarios creados mientras están en el rol Stand-Alone o Manual serán copiados al Cluster
Si el ADC abandona posteriormente el clúster, sólo quedarán los usuarios locales
La última contraseña configurada para el usuario será válida

Eliminación de un usuario

- Destacar un usuario existente
- Haga clic en Eliminar
- No podrá eliminar el usuario que está conectado actualmente
- No podrá eliminar el último usuario local del grupo de administradores
- No podrá eliminar el último usuario del clúster que queda en el grupo de administradores
- No podrá eliminar el usuario administrador por compatibilidad con versiones anteriores
- Si elimina el CAD del clúster, se eliminarán todos los usuarios, excepto los locales

Editar un usuario

- Destacar un usuario existente
- Haga clic en Editar
- Puede cambiar la pertenencia al grupo del usuario marcando las casillas correspondientes y actualizando
- También puede cambiar la contraseña de un usuario, siempre que tenga derechos de administrador

Registro de auditoría

El CAD registra los cambios realizados en la configuración del CAD por usuarios individuales. El registro de auditoría proporcionará las últimas 50 acciones realizadas por todos los usuarios. También puede ver TODAS las entradas en la sección de **REGISTROS**. Por ejemplo:

Date/Time	Username	Section	Action
01:04:28 Thu 28 May 2015	admin	Network	from [. 0.0.0.0.0.0.0.192.168.1.1,0] to []
01:02:27 Thu 28 May 2015	admin	error	ERROR:Subnet 192.168.1.214 must not overlap with subnet 192.168.1.215
01:02:27 Thu 28 May 2015	admin	Address	[Green side . 192.168.1.214/255.255.255.0,Red Side . 192.168.1.215/255.255.255.0]
00:54:48 Thu 28 May 2015	admin	error	Invalid uploaded licence format.
00:39:57 Thu 28 May 2015	admin	flightPATH Evaluatio...	Variable=\$variable1\$, Source=, Detail=, Value=
00:39:57 Thu 28 May 2015	admin	flightPATH Action	1 Action=use_server, Target=192.168.0.75, Value=
00:39:57 Thu 28 May 2015	admin	flightPATH Condition	1 Condition=host, Sense=does, Check=exist, Match=, Value=

View Download

Avanzado

Configuración



Siempre es una buena práctica descargar y guardar la configuración del CAD una vez que esté completamente configurado y funcionando como se requiere. Puede utilizar el módulo de configuración tanto para descargar como para cargar una configuración.

Los Jetpacks son archivos de configuración para aplicaciones estándar y son proporcionados por Edgenexus para simplificar su trabajo. Estos también pueden cargarse en el CAD mediante el módulo de configuración.

Un archivo de configuración es esencialmente un archivo basado en texto, y como tal, puede ser editado por usted utilizando un editor de texto como el Bloc de notas++ o VI. Una vez editado como sea necesario, el archivo de configuración puede cargarse en el CAD.

Descarga de una configuración

- Para descargar la configuración actual del CAD, pulse el botón Descargar configuración.
- Aparecerá una ventana emergente que le pedirá que abra o guarde el archivo .conf.
- Guarde en un lugar conveniente.
- Puede abrirlo con cualquier editor de texto, como el Bloc de notas++.

Carga de una configuración

- Puede cargar un archivo de configuración guardado buscando el archivo .conf guardado.
- Haga clic en el botón "Cargar configuración o Jetpack".
- El CAD cargará y aplicará la configuración y luego refrescará el navegador. Si no refresca el navegador automáticamente, por favor, haga clic en refrescar en el navegador.
- Será redirigido a la página del Tablero de Control una vez completado.

Subir un jetPACK

- Un jetPACK es un conjunto de actualizaciones de la configuración existente.
- Un jetPACK puede ser tan pequeño como cambiar el valor de TCP Timeout hasta una configuración completa de una aplicación específica como Microsoft Exchange o Microsoft Lync.
 - Puede obtener un jetPACK en el portal de soporte que se muestra al final de esta guía.
- Busque el archivo jetPACK.txt.
- Haga clic en cargar.
- El navegador se actualizará automáticamente después de la carga.
- Será redirigido a la página del Tablero de Control una vez completado.
- La importación puede tardar más tiempo en el caso de implantaciones más complejas, como Microsoft Lync, etc.

Ajustes globales

La sección de ajustes globales le permite cambiar varios elementos, incluida la biblioteca criptográfica SSL.

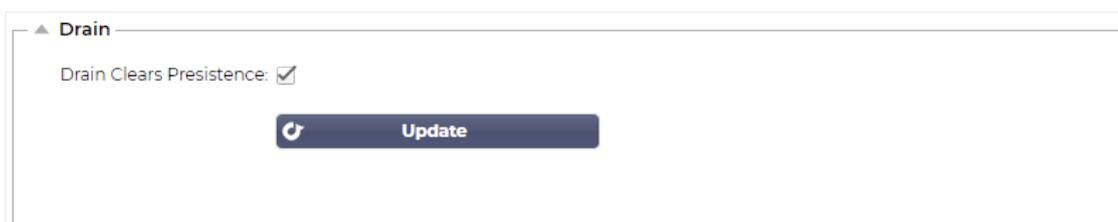
Temporizador de la caché del host



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

El temporizador de la caché del host es un ajuste que almacena la dirección IP de un servidor real durante un periodo determinado cuando se ha utilizado el nombre de dominio en lugar de una dirección IP. La caché se vacía cuando falla el Servidor Real. Si se ajusta este valor a cero, se evitará que la caché se vacíe. No hay un valor máximo para este ajuste.

Drenaje



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

La función Drenaje es configurable para cada Servidor Real vinculado a un Servicio Virtual. Por defecto, la configuración de Drenaje borra la persistencia está activada, lo que permite que los servidores que se colocan en el modo Drenaje terminen las sesiones de forma elegante para que puedan ser desconectados para su mantenimiento.

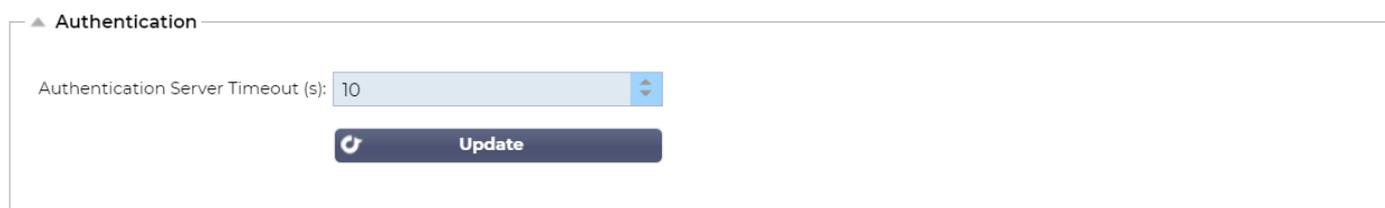
SSL



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

Esta configuración global permite cambiar la biblioteca SSL según sea necesario. La biblioteca criptográfica SSL por defecto utilizada por el ADC es de OpenSSL. Si desea utilizar una biblioteca criptográfica diferente, esto podría cambiarse aquí.

Autenticación



The screenshot shows a configuration panel titled "Authentication". It contains a label "Authentication Server Timeout (s):" followed by a numeric input field with the value "10". Below the input field is a dark blue button with a refresh icon and the text "Update".

Este valor establece el valor de tiempo de espera para la autenticación, después del cual el intento de autenticación se considerará fallido.

Protocolo

La sección Protocolo se utiliza para establecer los numerosos ajustes avanzados del protocolo HTTP.

Servidor demasiado ocupado

Supongamos que ha limitado las conexiones máximas a sus servidores reales; puede optar por presentar una página web amigable una vez que se haya alcanzado este límite.

- Cree una página web sencilla con su mensaje. Puede incluir enlaces externos a objetos de otros servidores y sitios web. Como alternativa, si quiere tener imágenes en su página web, utilice imágenes codificadas en línea en base64
- Busque el archivo HTM(L) de su página web recién creada
- Haga clic en Cargar
- Si desea obtener una vista previa de la página, puede hacerlo con el enlace Haga clic aquí

Reenviado Para

El Forwarded For es el estándar de facto para identificar la dirección IP de origen de un cliente que se conecta a un servidor web a través de los equilibradores de carga de capa 7 y los servidores proxy.

Salida de la red de distribución

Opción	Descripción
Off	El CAD no altera la cabecera Forwarded-For.
Añadir dirección y puerto	Esta opción añadirá la dirección IP y el puerto, del dispositivo o cliente conectado al CAD, a la cabecera Forwarded-For.
Añadir dirección	Esta opción añadirá la dirección IP, del dispositivo o cliente conectado al CAD, a la cabecera Forwarded-For.
Reemplace la dirección y el puerto	Esta opción sustituirá el valor de la cabecera Forwarded-For por la dirección IP y el puerto del dispositivo o cliente conectado al ADC.
Sustituir la dirección	Esta opción sustituirá el valor de la cabecera Forwarded-For por la dirección IP del dispositivo o cliente conectado al CAD.

Encabezado de la transmisión

Este campo le permite especificar el nombre dado a la cabecera Forwarded-For. Normalmente es "X-Forwarded-For", pero puede cambiarse en algunos entornos.

Registro avanzado para IIS - Registro personalizado

Puede obtener la información de X-Forwarded-For instalando la aplicación IIS Advanced logging 64-bit. Una vez descargada, cree un campo de registro personalizado llamado X-Forwarded-For con la configuración que se indica a continuación.

Seleccione Predeterminado en la lista Tipo de fuente en la lista Categoría, seleccione Cabecera de solicitud en el cuadro Nombre de la fuente y escriba X-Forwarded-For.

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

Cambios en Apache HTTPd.conf

Deberá realizar varios cambios en el formato por defecto para registrar la dirección IP del cliente X-Forwarded-For o la dirección IP real del cliente si la cabecera X-Forwarded-For no existe.

Dichos cambios se encuentran a continuación:

Tipo	Valor
Formato de registro:	"%h %l %u %t \ "%r\ " %>s %b \ "%{Referer}i\ \ "%{User-Agent}i"" combinado
Formato de registro:	"%{X-Forwarded-For}i %l %u %t \ "%r\ " %>s %b \ "%{Referer}i\ \ "%{User-Agent}i"" proxy SetEnvIf X- Forwarded-For "\.^\.\.*\N" reenviado
CustomLog:	"logs/access_log" combinado env=!forwarded
CustomLog:	"logs/access_log" proxy env=forwarded

Este formato aprovecha el soporte integrado de Apache para el registro condicional basado en variables de entorno.

- La línea 1 es la cadena estándar de formato de registro combinado de la norma.
- La línea 2 sustituye el campo %h (host remoto) por el valor o valores extraídos de la cabecera X-Forwarded-For y establece el nombre de este patrón de archivo de registro como "proxy".
- La línea 3 es un ajuste para la variable de entorno "forwarded" que contiene una expresión regular suelta que coincide con una dirección IP, lo que está bien en este caso ya que nos importa más si existe una dirección IP en la cabecera X-Forwarded-For.
- Además, la línea 3 podría leerse como "Si existe un valor X-Forwarded-For, utilícelo".
- Las líneas 4 y 5 indican a Apache qué patrón de registro debe utilizar. Si existe un valor X-Forwarded-For, utiliza el patrón "proxy", si no, utiliza el patrón "combinado" para la petición. Para facilitar la lectura, las líneas 4 y 5 no aprovechan la función de registro de rotación de registros (piped) de Apache, pero suponemos que casi todo el mundo la utiliza.

Estos cambios harán que se registre una dirección IP para cada solicitud.

Configuración de la compresión HTTP

HTTP Compression Settings

Initial Thread Memory [KB]: 128

Maximum Thread Memory [KB]: 99999

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

Minimum Compression Size [Bytes]: 200

Safe Mode:

Disable Compression:

Compress As You Go: By Page Request

Update

La compresión es una característica de aceleración y se habilita para cada Servicio en la página de Servicios IP.

ADVERTENCIA - *Tenga mucho cuidado al ajustar estos parámetros, ya que una configuración inadecuada puede afectar negativamente al rendimiento del ADC*

Opción	Descripción
Memoria inicial del hilo [KB]	Este valor es la cantidad de memoria que cada solicitud recibida por el CAD puede asignar inicialmente. Para obtener un rendimiento más eficiente, este valor debe establecerse en un valor apenas superior al mayor archivo HTML sin comprimir que probablemente envíen los servidores web.
Memoria máxima del hilo [KB]	Este valor es la cantidad máxima de memoria que el CAD asignará en una solicitud. Para obtener el máximo rendimiento, el CAD normalmente almacena y comprime todo el contenido en la memoria. Si se procesa un archivo de contenido excepcionalmente grande que supere esta cantidad, el CAD escribirá en el disco y comprimirá allí los datos.
Incremento de la memoria [KB]	Este valor establece la cantidad de memoria que se añade a la asignación de memoria inicial del hilo cuando se necesita más. El valor por defecto es cero. Esto significa que el CAD duplicará la asignación cuando los datos excedan la asignación actual (por ejemplo, 128Kb, luego 256Kb, luego 512Kb, etc) hasta el límite establecido por el Uso Máximo de Memoria por Hilo. Esto es eficiente cuando la mayoría de las páginas son de un tamaño consistente pero hay ocasionalmente archivos más grandes. (Por ejemplo, la mayoría de las páginas son de 128Kb o menos, pero las respuestas ocasionales tienen un tamaño de 1Mb). En el escenario donde hay archivos grandes de tamaño variable, es más eficiente establecer un incremento lineal de un tamaño significativo (por ejemplo, las respuestas tienen un tamaño de 2Mb a 10Mb, un ajuste inicial de 1Mb con incrementos de 1Mb sería más eficiente).
Tamaño mínimo de compresión [Bytes]	Este valor es el tamaño, en bytes, por debajo del cual el CAD no intentará comprimir. Esto es útil porque todo lo que sea muy inferior a 200 bytes no se comprime bien e incluso puede aumentar su tamaño debido a los gastos generales de las cabeceras de compresión.
Modo seguro	Marque esta opción para evitar que el CAD aplique la compresión a las hojas de estilo de JavaScript. El motivo es que, aunque el CAD es consciente de qué navegadores individuales pueden manejar contenido comprimido, algunos otros servidores proxy, aunque afirmen ser compatibles con HTTP/1.1, no pueden transportar correctamente hojas de estilo y JavaScript comprimidos. Si se producen problemas con las hojas de estilo o JavaScript a través de un servidor proxy, utilice esta opción para desactivar la compresión de estos tipos. Sin embargo, esto reducirá la cantidad total de compresión del contenido.
Desactivar la compresión	Marque esta opción para evitar que el CAD comprima cualquier respuesta.
Comprimir a medida que avanza	ON - Utilizar la compresión sobre la marcha en esta página. Esto comprime cada bloque de datos recibido del servidor en un trozo discreto que es totalmente descomprimible. APAGADO - No utilizar Compress As You Go en esta página. Por solicitud de página - Utilizar Compress as You Go por solicitud de página.

Exclusiones de la compresión global

Las páginas con la extensión añadida en la lista de exclusión no se comprimirán.

- Escriba el nombre del archivo individual.
- Haga clic en actualizar.
- Si desea añadir un tipo de archivo, simplemente escriba "*.css" para que se excluyan todas las hojas de estilo en cascada.
- Cada archivo o tipo de archivo debe añadirse a una nueva línea.

Cookies de persistencia

Esta configuración le permite especificar cómo se manejan las cookies de persistencia.

Campo	Descripción
Atributo de Cooke en el mismo sitio	<p>Ninguna: Todas las cookies son accesibles a los scripts</p> <p>Laxo: Evita que se acceda a las cookies a través de los sitios, pero se almacenan para que sean accesibles y se envíen al sitio propietario si se visita</p> <p>Estricto: impide que se acceda o se almacene cualquier cookie de un sitio diferente</p> <p>Desactivado: vuelve al comportamiento por defecto del navegador</p>
Asegure	Esta casilla, cuando está marcada, aplica la persistencia al tráfico seguro
Sólo HTTP	Cuando está marcada, permite las cocinas persistentes sólo en el tráfico HTTP

Software

La sección de software le permite actualizar la configuración y el firmware de su ADC.

Detalles de la actualización del software

ALB Software Upgrade Details

User Name: admin	ALB Location: Altrincham, United Kingdom
Machine ID: 50E-FF4	Support Expiry: 2021-03-24
Licence ID: {C3E60CA1-6155-4E69-...}	Support Type: Premium
Licence Expiry: 2021-03-24	Current Software Version: 4.2.6 (Build 1831) 3j1329

Refresh To View Available Software

La información de esta sección se completará si tiene una conexión a Internet que funcione. Si su navegador no tiene conexión a Internet, esta sección estará en blanco. Una vez conectado, recibirá el mensaje de banner que aparece a continuación.

We have successfully connected to Cloud Services Manager to retrieve your Software Update Details

La sección Descarga desde la nube que se muestra a continuación se llenará con información que muestra las actualizaciones disponibles para usted bajo su plan de soporte. Debe prestar atención al tipo de soporte y a la fecha de caducidad del mismo.

Nota: Utilizamos la conexión a Internet de su navegador para ver lo que está disponible en la nube de Edgenexus. Sólo podrá descargar las actualizaciones de software si el CAD tiene conexión a Internet.

Para comprobarlo:

- Avanzado--Solución de problemas--Ping
- Dirección IP - appstore.edgenexus.io
- Haga clic en Ping
- Si el resultado muestra "ping: host desconocido appstore.edgenexus.io. "
- El CAD NO podrá descargar nada de la nube

Descarga desde la nube

Download From Cloud

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

Download Selected Software To ALB

Si su navegador está conectado a Internet, verá los detalles del software disponible en la nube.

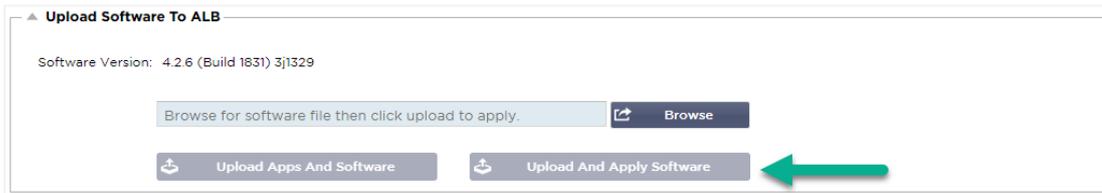
- Resalte la fila que le interesa y haga clic en el botón "Descargar el software seleccionado en el ALB. "
- El software seleccionado se descargará en su ALB al hacer clic, lo que puede aplicarse en la sección "Aplicar el software almacenado en el ALB" más adelante.

Nota: Si el CAD no tiene acceso directo a Internet, recibirá un error como el siguiente:

Error de descarga, ALB no puede acceder a los servicios en la nube de ADC para el archivo build1734-3236-v4.2.1-Sprint2-update-64.software.alb

Cargar el software en el ALB

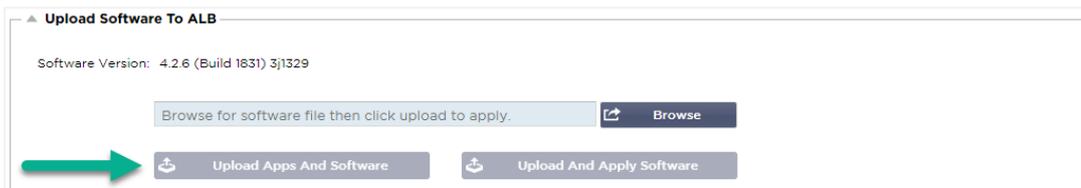
Carga de aplicaciones



Si tiene un archivo de aplicación que termina con <apptype>.alb puede utilizar este método para cargarlo.

- Hay cinco tipos de App
 - <nombre de la aplicación>flightpath.alb
 - <nombre de la aplicación>.monitor.alb
 - <nombre de la aplicación>.jetpack.alb
 - <nombre de la aplicación>.addons.alb
 - <nombre de la aplicación>.featurepack.alb
- Una vez cargada, cada aplicación se encontrará en la sección Biblioteca > Aplicaciones.
- A continuación, deberá desplegar cada aplicación de esa sección de forma individual.

Software



- Si desea cargar el software sin aplicarlo, utilice el botón resaltado.
- El archivo de software es <softwarename>.software.alb.
- A continuación, se mostrará en la sección "Software almacenado en el ALB", desde donde podrá aplicarlo a su conveniencia.

Aplicar el software almacenado en el ALB

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

Esta sección mostrará todos los archivos de software almacenados en el ALB y disponibles para su despliegue. El listado incluirá las firmas actualizadas del Web Application Firewall (WAF).

- Resalte la fila del software que le interesa utilizar.
- Haga clic en "Aplicar el software desde el seleccionado"
- Si se trata de una actualización del software del ALB, tenga en cuenta que se cargará y luego se reiniciará el ALB para aplicarlo.
- Si la actualización que está aplicando es una actualización de la firma OWASP, se aplicará automáticamente sin necesidad de reiniciar.

Solución de problemas

Siempre hay problemas que requieren la resolución de problemas para llegar a la causa raíz y a la solución. Esta sección le permite hacerlo.

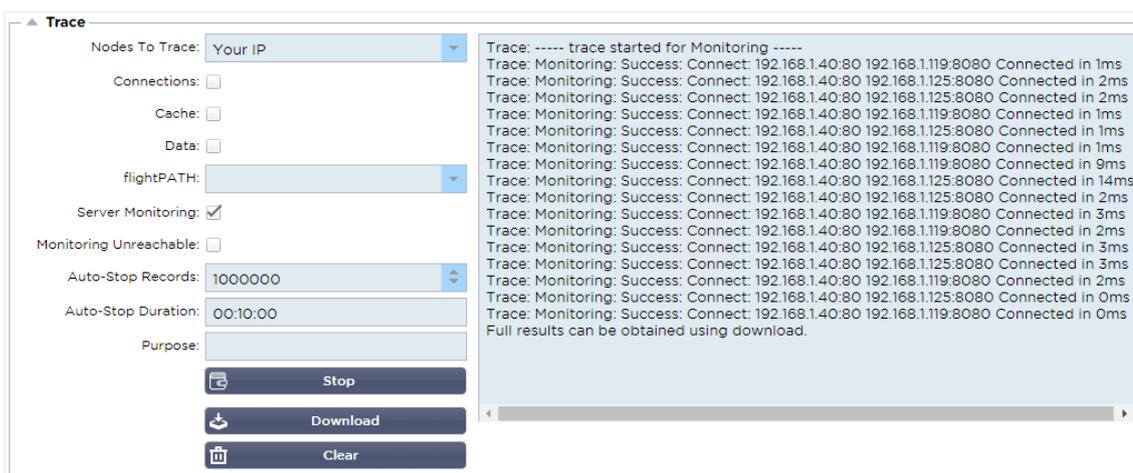
Archivos de apoyo



Si tiene un problema con el ADC y necesita abrir un ticket de asistencia, el servicio de asistencia técnica suele solicitar varios archivos diferentes del aparato ADC. Estos archivos se han agrupado ahora en un único archivo .dat que puede descargarse a través de esta sección.

- Seleccione un periodo de tiempo en el desplegable: Puede elegir entre 3, 7, 14 y Todos los días.
- Haga clic en "Descargar archivos de soporte"
- Se descargará un archivo con el formato Soporte-jetNEXUS-yyymmddhh-NAME.dat
- Levante un ticket de soporte en el portal de soporte, cuyos detalles están disponibles al final de este documento.
- Asegúrese de describir bien el problema y de adjuntar el archivo .dat al ticket.

Rastrear



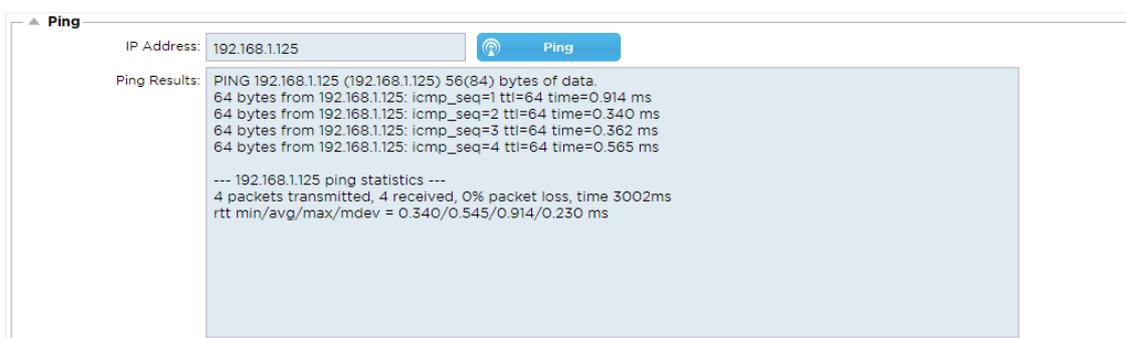
La sección de rastreo le permitirá examinar la información que permite la depuración del problema. La información entregada depende de las opciones que elija en los desplegables y las casillas de verificación.

Opción	Descripción
Nodos a rastrear	Su IP: Esto filtrará la salida para utilizar la dirección IP desde la que está accediendo a la GUI (Tenga en cuenta que no debe elegir esta opción para la monitorización, ya que ésta utilizará la dirección de la interfaz del CAD) Todas las IP: No se aplicará ningún filtro. Hay que tener en cuenta que en una caja ocupada esto afectará negativamente al rendimiento.
Conexiones	Esta casilla, cuando está marcada, le mostrará información sobre las conexiones del lado del cliente y del servidor.
Caché	Esta casilla marcada le mostrará información con respecto a los objetos en caché.

Datos	Cuando esta casilla está marcada, se incluirán los bytes de datos brutos manejados en la entrada y salida por el ADC.
flightPATH	El menú flightPATH le permite seleccionar una regla flightPATH particular para monitorear o Todas las reglas flightPATH.
Monitorización de servidores	Esta casilla, cuando está marcada, mostrará los monitores de salud del servidor activos en el ADC y sus respectivos resultados.
Monitoreo inalcanzable	Cuando se selecciona esta opción, su comportamiento es muy parecido al de la monitorización del servidor, excepto que sólo mostrará los monitores fallidos y, por tanto, actúa como un filtro sólo para estos mensajes.
Registros de parada automática	El valor por defecto es de 1.000.000 de registros, tras lo cual la función de Rastreo se detendrá automáticamente. Este ajuste es una medida de seguridad para evitar que Trace se quede accidentalmente activado y afecte al rendimiento de su CAD.
Duración de la parada automática	El tiempo por defecto está fijado en 10 minutos, después de los cuales la instalación de Trace se detendrá automáticamente. Esta función es una precaución de seguridad para evitar que Trace se quede accidentalmente encendido y afecte al rendimiento del ADC.
Inicie	Haga clic en esta opción para iniciar la instalación de rastreo manualmente.
Detener	Haga clic para detener manualmente la función de rastreo antes de que se alcance el registro automático o la hora.
Descargar	Aunque puede ver el visor en vivo en la parte derecha, la información puede aparecer demasiado rápido. En su lugar, puede descargar el Trace.log para ver toda la información recopilada durante las distintas trazas de ese día. Esta función es una lista filtrada de información de rastreo. Si desea ver la información de rastreo de días anteriores, puede descargar el Syslog de ese día, pero tendrá que filtrarlo manualmente.
Claro	Borra el registro de rastreo

Ping

Puede comprobar la conectividad de la red con los servidores y otros objetos de la red en su infraestructura utilizando la herramienta Ping.



Escriba la dirección IP del host que desea probar, por ejemplo, la puerta de enlace por defecto utilizando la notación decimal con puntos o una dirección IPv6. Es posible que tenga que esperar unos segundos para que el resultado se muestre una vez que haya pulsado el botón "Ping".

Si ha configurado un servidor DNS, puede introducir el nombre de dominio completo. Puede configurar un servidor DNS en la sección **SERVIDOR DNS 1 Y SERVIDOR DNS 2**. Es posible que tenga que esperar unos segundos para que el resultado se muestre una vez que haya pulsado el botón "Ping".

Captura

The screenshot shows a 'Capture' configuration window with the following fields:

- Adapter: any
- Packets: 999999
- Duration[Sec]: 20
- Address: 192.168.1.40

A 'Generate' button is located at the bottom of the form.

Para capturar el tráfico de la red, siga las sencillas instrucciones que aparecen a continuación.

- Complete las opciones del formulario
- Haga clic en Generar
- Una vez ejecutada la captura, su navegador aparecerá y le preguntará dónde desea guardar el archivo. Tendrá el formato "jetNEXUS.cap.gz"
- Levante un ticket de soporte en el portal de soporte, cuyos detalles están disponibles al final de este documento.
- Asegúrese de describir bien el problema y de adjuntar el archivo al ticket.
- También puede ver el contenido utilizando Wireshark

Opción	Descripción
Adaptador	Elija su adaptador en el desplegable, normalmente eth0 o eth1. También puede capturar todas las interfaces con "any"
Paquetes	Este valor es el número máximo de paquetes a capturar. Normalmente, 99999
Duración	Elija el tiempo máximo que durará la captura. Un tiempo típico es de 15 segundos para sitios de alto tráfico. La interfaz gráfica de usuario será inaccesible durante el periodo de captura
Dirección	Este valor filtrará cualquier dirección IP introducida en la casilla. Déjelo en blanco para no filtrar.

Para mantener el rendimiento, hemos limitado el archivo de descarga a 10 MB. Si considera que esto no es suficiente para capturar todos los datos necesarios, podemos aumentar esta cifra.

Nota: Esto tendrá un impacto en el rendimiento de los sitios en vivo. Para aumentar el tamaño de captura disponible, aplique un ajuste global jetPACK para aumentar el tamaño de captura.

Ayuda

La sección de ayuda permite acceder a la información sobre Edgenexus y acceder a las guías de usuario y a otra información útil.

Sobre nosotros

Al hacer clic en la opción "Acerca de nosotros" aparecerá información sobre Edgenexus y su oficina corporativa.

About Us



Edgenexus ADC(TM)

4.2.8 (Build 1895)
Copyright © 2005-2020 Edgenexus Limited. All Rights Reserved.

Edgenexus Limited.
Jubilee House,
Third Avenue,
Marlow
SL7 1YW

www.edgenexus.io/support/

Some elements of the SSL subsystem are open source.

Referencia

La opción de referencia abrirá la página que contiene las guías del usuario y otros documentos útiles.

Edgenexus Load Balancer / ADC Admin Guide

 <p>English (EN)</p> <p>Download PDF</p>	 <p>French (FR)</p> <p>Download PDF</p>	 <p>German (DE)</p> <p>Download PDF</p>	
 <p>Spanish (ES)</p> <p>Download PDF</p>	 <p>Portugese (BP)</p> <p>Download PDF</p>	 <p>Japanese (JP)</p> <p>Download PDF</p>	 <p>Chinese (CN)</p> <p>Download PDF</p>

Si no encuentra lo que busca, póngase en contacto con support@edgenexus.io.

Qué es un jetPACK

Los jetPACKs son un método único para configurar instantáneamente su ADC para aplicaciones específicas. Estas plantillas fáciles de usar vienen preconfiguradas y totalmente ajustadas con todos los parámetros específicos de la aplicación que necesita para disfrutar de una prestación de servicios optimizada de su ADC. Algunos de los jetPACKs utilizan flightPATH para manipular el tráfico, y debe tener una licencia de flightPATH para que este elemento funcione. Para saber si tiene una licencia para flightPATH, consulte la página de [LICENCIAS](#).

Descarga de un jetPACK

- Cada jetPACK de abajo ha sido creado con una dirección IP Virtual única contenida en el título del jetPACK. Por ejemplo, el primer jetPACK de abajo tiene una Dirección IP Virtual de 1.1.1.1
- Puede subir este jetPACK tal cual y cambiar la dirección IP en la GUI o editar el jetPACK con un editor de texto como el Notepad++ y buscar y reemplazar 1.1.1.1 por su dirección IP virtual.
- Además, cada jetPACK ha sido creado con 2 servidores reales con direcciones IP de 127.1.1.1 y 127.2.2.2. De nuevo, puede cambiarlas en la interfaz gráfica de usuario después de la carga o de antemano utilizando el Bloc de notas++.
- Haga clic en un enlace jetPACK de los que aparecen a continuación y guarde el enlace como un archivo jetPACK-VIP-Application.txt en la ubicación que elija

Microsoft Exchange

Aplicación	Enlace de descarga	¿Qué hace?	¿Qué incluye?
Intercambio 2010	jetPACK-1.1.1.1-Exchange-2010	Este jetPACK añadirá la configuración básica para equilibrar la carga de Microsoft Exchange 2010. Hay una regla flightPATH incluida para redirigir el tráfico en el servicio HTTP a HTTPS, pero es una opción. Si no tiene una licencia para flightPATH, este jetPACK seguirá funcionando.	Ajustes globales: Tiempo de espera del servicio 2 horas Monitores: Monitor de capa 7 para la aplicación web de Outlook, y monitor de capa 4 fuera de banda para el servicio de acceso del cliente IP del servicio virtual: 1.1.1.1 Puertos de servicio virtual: 80, 443, 135, 59534, 59535 Servidores reales: 127.1.1.1 127.2.2.2 flightPATH: Añade la redirección de HTTP a HTTPS
	jetPACK-1.1.1.2-Exchange-2010-SMTP-RP	Igual que el anterior, pero añadirá un servicio SMTP en el puerto 25 en conectividad proxy inversa. El servidor SMTP verá la dirección de la interfaz ALB-X como la IP de origen.	Ajustes globales: Tiempo de espera del servicio 2 horas Monitores: Monitor de capa 7 para la aplicación web de Outlook. Monitor de capa 4 fuera de banda para el servicio de acceso del cliente. IP del servicio virtual: 1.1.1.1 Puertos de servicios virtuales: 80, 443, 135, 59534, 59535, 25 (proxy inverso) Servidores reales: 127.1.1.1 127.2.2.2

			flightPATH: Añade la redirección de HTTP a HTTPS
	jetPACK-1.1.1.3-Exchange-2010-SMTP-DSR	Igual que el anterior, excepto que este jetPACK configurará el servicio SMTP para utilizar la conectividad de Retorno Directo al Servidor. Este jetPACK es necesario si su servidor SMTP necesita ver la dirección IP real del cliente.	Ajustes globales: Tiempo de espera del servicio 2 horas Monitores: Monitor de capa 7 para la aplicación web de Outlook. Monitor de capa 4 fuera de banda para el servicio de acceso del cliente. IP del servicio virtual: 1.1.1.1 Puertos de servicios virtuales: 80, 443, 135, 59534, 59535, 25 (retorno directo del servidor) Servidores reales: 127.1.1.1 127.2.2.2 flightPATH: Añade la redirección de HTTP a HTTPS
Intercambio 2013	jetPACK-2.2.2.1-Exchange-2013-Low-Resource	Esta configuración añade 1 VIP y dos servicios para el tráfico HTTP y HTTPS y es la que menos CPU requiere. Es posible añadir múltiples controles de salud al VIP para comprobar que cada uno de los servicios individuales está al día	Ajustes globales: Monitores: Monitor de capa 7 para OWA, EWS, OA, EAS, ECP, OAB y ADS IP del servicio virtual: 2.2.2.1 Puertos de servicio virtuales: 80, 443 Servidores reales: 127.1.1.1 127.2.2.2 flightPATH: Añade la redirección de HTTP a HTTPS
	jetPACK-2.2.3.1-Exchange-2013-Med-Resource	Esta configuración utiliza una dirección IP única para cada servicio y por lo tanto utiliza más recursos que la anterior. Debe configurar cada servicio como una entrada DNS individual Ejemplo owa.jetnexus.com, ews.jetnexus.com, etc. Se añadirá un monitor para cada servicio y se aplicará al servicio correspondiente	Ajustes globales: Monitores: Monitor de capa 7 para OWA, EWS, OA, EAS, ECP, OAB, ADS, MAPI y PowerShell Servicio virtual IP: 2.2.3.1, 2.2.3.2, 2.2.3.3, 2.2.3.4, 2.2.3.5, 2.2.3.6, 2.2.3.7, 2.2.3.8, 2.2.3.9, 2.2.3.10 Puertos de servicio virtuales: 80, 443 Servidores reales: 127.1.1.1 127.2.2.2 flightPATH: Añade la redirección de HTTP a HTTPS
	jetPACK-2.2.2.3-Exchange2013-High-Resource	Este jetPACK añadirá una única dirección IP y varios servicios virtuales en diferentes puertos. flightPATH cambiará entonces de contexto basándose en la ruta de destino al servicio virtual correcto. Este jetPACK requiere la mayor cantidad de CPU para llevar a cabo el cambio de contexto	Ajustes globales: Monitores: Monitor de capa 7 para OWA, EWS, OA, EAS, ECP, OAB, ADS, MAPI y PowerShell IP del servicio virtual: 2.2.2.3 Puertos de servicio virtual: 80, 443, 1, 2, 3, 4, 5, 6, 7 Servidores reales: 127.1.1.1 127.2.2.2

flightPATH: Añade la redirección de HTTP a HTTPS

Microsoft Lync 2010/2013

Proxy inverso	Parte delantera	Borde interno	Borde externo
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

Servicios web

HTTP normal	Descarga de SSL	Reencriptación SSL	Traspaso SSL
jetPACK-4.4.4.1-Web-HTTP	jetPACK-4.4.4.2-Descarga Web-SSL	jetPACK-4.4.4.3-Recodificación Web-SSL	jetPACK-4.4.4.4-Paseo Web-SSL

Escritorio remoto de Microsoft

Normal

[jetPACK-5.5.5.1-Remote-Desktop](#)

DICOM - Imagen y Comunicación Digital en Medicina

HTTP normal

[jetPACK-6.6.6.1-DICOM](#)

Oracle e-Business Suite

Descarga de SSL

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

VMware Horizon View

Servidores de conexión - Descarga de SSL **Servidores de seguridad - Reencriptación SSL**

[jetPACK-8.8.8.1-Ver-SSL-Descarga](#)

[jetPACK-8.8.8.2-Ver-SSL-Re-encryptación](#)

Ajustes globales

- Puerto seguro GUI 443 - este jetPACK cambiará su puerto seguro GUI de 27376 a 443. HTTPs://x.x.x.x
- Tiempo de espera de la GUI 1 día - la GUI le pedirá que introduzca su contraseña cada 20 minutos. Este ajuste aumentará esa solicitud a 1 día
- ARP Refresh 10 - durante una conmutación por error entre aparatos de HA, este ajuste aumentará el número de **ARP gratuitos** para ayudar a los conmutadores durante la transición
- Tamaño de la captura 16MB - el tamaño de la captura por defecto es de 2MB. Este valor aumentará el tamaño hasta un máximo de 16MB

Opciones de cifrado

- Cifrado fuerte - Esto añadirá la posibilidad de elegir "Cifrado fuerte" en la lista de opciones de cifrado:

- Cifrado = ALL:RC4+RSA:+RC4:+HIGH:!DES-CBC3-SHA:!SSLv2:!ADH:!EXP:!ADHexport:!MD5
- Antibestia - Esto añadirá la posibilidad de elegir "Antibestia" en la lista de opciones de cifrado:
 - Cifrado = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH
- No SSLv3 - Esto añadirá la posibilidad de elegir "No SSLv3" en la lista de opciones de cifrado:
 - Cifrado = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
- No SSLv3 no TLSv1 No RC4 - Esto añadirá la posibilidad de elegir "No-TLSv1 No-SSLv3 No-RC4" de la lista de opciones de cifrado:
 - Cifrado = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
- NO_TLSv1.1 -Esto añadirá la posibilidad de elegir "NO_TLSv1.1" en la lista de opciones de cifrado:
 - Cifrado= ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:RSA+AESGCM:RSA+AES:HIGH:!3DES:!aNULL:!MD5:!DSS:!MD5:!aNULL:!EDH:!RC4

flightPATHs

- X-Content-Type-Options - añada esta cabecera si no existe y ajústela a "nosniff" - evita que el navegador haga "MIME-Sniffing" automáticamente.
- X-Frame-Options - añada esta cabecera si no existe y ajústela a "SAMEORIGIN" - las páginas de su sitio web pueden ser incluidas en Frames, pero sólo en otras páginas dentro del mismo sitio web.
- X-XSS-Protection - añada esta cabecera si no existe y configúrela con el valor "1; mode=block" - habilite las protecciones contra scripts cruzados del navegador
- Strict-Transport-Security - añada la cabecera si no existe y la establece como "max-age=31536000 ; includeSubdomains" - asegura que el cliente debe respetar que todos los enlaces sean HTTPS:// para la edad máxima

Aplicar un jetPACK

Puede aplicar cualquier jetPACK en cualquier orden, pero tenga cuidado de no utilizar un jetPACK con la misma dirección IP virtual. Esta acción causará una dirección IP duplicada en la configuración. Si lo hace por error, puede cambiarlo en el GUI.

- Navegue hasta Avanzado > Actualizar software
- Sección de configuración
- Cargar nueva configuración o jetPACK
- Buscar jetPACK
- Haga clic en Cargar
- Una vez que la pantalla del navegador se vuelva blanca, haga clic en actualizar y espere a que aparezca la página del panel de control

Creación de un jetPACK

Una de las grandes cosas de jetPACK es que usted puede crear el suyo propio. Puede ser que haya creado la configuración perfecta para una aplicación y quiera utilizarla en varias otras cajas de forma independiente.

- Comience por copiar la configuración actual de su ALB-X existente
 - Avanzado
 - Actualizar el software
 - Descargar la configuración actual

- Edite este archivo con el Bloc de notas++
- Abra un nuevo documento txt y llámelo "su nombre-jetPACK1.txt"
- Copie todas las secciones relevantes del archivo de configuración en "yourname-jetPACK1.txt"
- Guardar una vez completado

IMPORTANTE: Cada jetPACK está dividido en diferentes secciones, pero todos los jetPACKs deben tener #!jetpack en la parte superior de la página.

A continuación se enumeran las secciones que se recomienda editar/copiar.

Sección 0:

```
#Jetpack
```

Esta línea tiene que estar en la parte superior del jetPACK, o su configuración actual se sobrescribirá.

Sección 1:

```
[jetnexusdaemon]
```

Esta sección contiene ajustes globales que, una vez modificados, se aplicarán a todos los servicios. Algunos de estos ajustes se pueden cambiar desde la consola web, pero otros sólo están disponibles aquí.

Ejemplos:

```
ConnectionTimeout=600000
```

Este ejemplo es el valor del tiempo de espera TCP en milisegundos. Este ajuste significa que una conexión TCP se cerrará después de 10 minutos de inactividad

```
ContentServerCustomTimer=20000
```

Este ejemplo es el retraso en milisegundos entre las comprobaciones de salud del servidor de contenidos para los monitores personalizados como DICOM

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

Este ejemplo cambiará el nombre de la cabecera de la cookie que se utiliza en el equilibrio de carga persistente del valor predeterminado "jnAccel" a "MS-WSMAN". Este cambio en particular es necesario para el proxy inverso de Lync 2010/2013.

Sección 2:

```
[jetnexusdaemon-Csm-Rules]
```

Esta sección contiene las reglas personalizadas de monitorización del servidor que suelen configurarse desde la consola web aquí.

Ejemplo:

```
[jetnexusdaemon-Csm-Rules-0]
```

```
Content="Servidor arriba"
```

```
Desc="Monitor 1"
```

```
Method="CheckResponse"
```

```
Name="Comprobación del estado del servidor"
```

```
Uri="HTTP://demo.jetneus.com/healthcheck/healthcheck.html"
```

Sección 3:

```
[jetnexusdaemon-LocalInterface]
```

Esta sección contiene todos los detalles de la sección de Servicios IP. Cada interfaz está numerada e incluye subinterfaces para cada canal. Si su canal tiene una regla flightPATH aplicada, entonces también contendrá una sección Path.

Ejemplo:

```
[jetnexusdaemon-LocalInterface1]
1.1="443"
1.2="104"
1.3="80"
1.4="81"
Activado=1
Netmask="255.255.255.0"
PrimaryV2="{A28B2C99-1FFC-4A7C-AAD9-A55C32A9E913}"
[jetnexusdaemon-LocalInterface1.1]
1=">,""Grupo Seguro"",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="Sin SSL"
Comprimir=1
ConnectionLimiting=0
DSR=0
DSRProto="tcp"
Activado=1
LoadBalancePolicy="Basado en cookies"
MaxConnections=10000
MonitoringPolicy="1"
PassThrough=0
Protocolo="Acelerar HTTP"
ServiceDesc="Servidores seguros VIP"
SNAT=0
SSL=1
SSLClient=0
SSLInternalPort=27400
[jetnexusdaemon-LocalInterface1.1-Path]
1="6"
Sección 4:
[jetnexusdaemon-Path]
```

Esta sección contiene todas las reglas flightPATH. Los números deben coincidir con lo que se ha aplicado a la interfaz. En el ejemplo anterior, vemos que la regla flightPATH "6" se ha aplicado al canal, incluyéndolo como ejemplo a continuación.

Ejemplo:

```
[jetnexusdaemon-Path-6]
Desc="Forzar el uso de HTTPS para cierto directorio"
Name="Gary - Forzar HTTPS"
[jetnexusdaemon-Path-6-Condition-1]
Check="contener"
Condition="ruta"
Partido=
Sense="hace"
Valor="/seguro/"
[jetnexusdaemon-Path-6-Evaluate-1]
Detalle=
Fuente="host"
Valor=
Variable="$host$" [jetnexusdaemon-Path-6-Function-1]
Acción="redirect"
Target="HTTPS://$host$$path$$querystring$"
Valor=
```

Introducción a flightPATH

¿Qué es flightPATH?

flightPATH es un motor de reglas inteligente desarrollado por Edgenexus para manipular y enrutar el tráfico HTTP y HTTPS. Es altamente configurable, muy potente y a la vez muy fácil de usar.

Aunque algunos componentes de flightPATH son objetos IP, como la IP de origen, flightPATH sólo puede aplicarse a un tipo **de servicio** igual a HTTP. Si elige cualquier otro tipo de servicio, la pestaña flightPATH en Servicios IP estará en blanco.

Una regla flightPATH tiene tres componentes:

Opción	Descripción
Condición	Establezca múltiples criterios para activar la regla flightPATH.
Evaluación	Permite el uso de variables que pueden ser utilizadas en el área de Acción.
Acción	El comportamiento una vez que la regla se ha disparado.

¿Qué puede hacer flightPATH?

flightPATH puede utilizarse para modificar el contenido y las peticiones HTTP entrantes y salientes.

Además de utilizar coincidencias de cadenas sencillas como "Empieza por" y "Termina por", por ejemplo, se puede implementar un control completo mediante potentes expresiones regulares (RegEx) compatibles con Perl.

Para más información sobre RegEx, consulte este útil sitio <https://www.regexbuddy.com/regex.html>

Además, se pueden crear y utilizar variables personalizadas en el área de **Acción**, lo que permite muchas posibilidades diferentes.

Condición

Condición	Descripción	Ejemplo
<form>	Los formularios HTML se utilizan para pasar datos a un servidor	Ejemplo "el formulario no tiene longitud 0"
Ubicación de GEO	Esto compara la dirección IP de origen con el código de país ISO 3166	La ubicación GEO es igual a GB O la ubicación GEO es igual a Alemania
Anfitrión	Este es el host extraído de la URL	www.mywebsite.com o 192.168.1.1
Idioma	Este es el idioma extraído de la cabecera HTTP del idioma	Esta condición producirá un desplegable con una lista de idiomas
Método	Este es un desplegable de métodos HTTP	Se trata de un desplegable que incluye GET, POST, etc.
IP de origen	Si el proxy ascendente admite X-Forwarded-for (XFF), utilizará la verdadera dirección de origen	IP del cliente. También puede utilizar varias IP o subredes. 10\1\2\.* es la subred 10.1.2.0 /2410\1\2\3 10\1\2\4 Use para múltiples IP's
Ruta	Esta es la ruta del sitio web	/mi sitio web/index.asp

EdgeADC - GUÍA DE ADMINISTRACIÓN

POST	Método de solicitud POST	Comprobar los datos que se cargan en un sitio web
Consulta	Es el nombre y el valor de una consulta, por lo que puede aceptar el nombre de la consulta o también un valor	"Best=jetNEXUS" Donde la coincidencia es Best y el valor es edgeNEXUS
Cadena de consulta	Toda la cadena de consulta después del carácter ?	
Solicitar galleta	Es el nombre de una cookie solicitada por un cliente	MS-WSMAN=afYfn1CDqqUD::
Solicitud de cabecera	Esto puede ser cualquier encabezado HTTP	Referrer, User-Agent, From, Date
Solicitar versión	Esta es la versión HTTP	HTTP/1.0 O HTTP/1.1
Órgano de respuesta	Una cadena definida por el usuario en el cuerpo de la respuesta	Servidor UP
Código de respuesta	El código HTTP de la respuesta	200 OK, 304 no modificado
Respuesta Cookie	Este es el nombre de una cookie enviada por el servidor	MS-WSMAN=afYfn1CDqqUD::
Cabecera de respuesta	Esto puede ser cualquier encabezado HTTP	Referrer, User-Agent, From, Date
Versión de la respuesta	La versión HTTP enviada por el servidor	HTTP/1.0 O HTTP/1.1
Fuente IP	Se trata de la IP de origen, la IP del servidor proxy o alguna otra dirección IP agregada	IP del cliente , IP del proxy, IP del cortafuegos. También puede utilizar varias IP y subredes. Debe escapar los puntos ya que estos son RegEX. Ejemplo 10\ 1\ 2\ 3 es 10.1.2.3

Partido	Descripción	Ejemplo
Acepte	Tipos de contenido aceptables	Aceptar: text/plain
Accept-Encoding	Codificaciones aceptables	Accept-Encoding: <compress gzip deflate sdch identity>
Accept-Language	Idiomas aceptables para la respuesta	Accept-Language: en-US
Accept-Ranges	Qué tipos de rango de contenido parcial soporta este servidor	Accept-Ranges: bytes
Autorización	Credenciales de autenticación para la autenticación HTTP	Autorización: Basic QWxhZGRpbjpvGVuIHhlc2FtZQ==
Cargar a	Contiene información contable de los costes de la aplicación del método solicitado	
Codificación del contenido	El tipo de codificación utilizado en los datos.	Content-Encoding: gzip

EdgeADC - GUÍA DE ADMINISTRACIÓN

Contenido-Longitud	La longitud del cuerpo de la respuesta en octetos (bytes de 8 bits)	Contenido-Longitud: 348
Tipo de contenido	El tipo mime del cuerpo de la solicitud (utilizado con las solicitudes POST y PUT)	Content-Type: application/x-www-form-urlencoded
Cookie	Una cookie HTTP enviada previamente por el servidor con Set-Cookie (abajo)	Cookie: \$Versión=1; Skin=nuevo;
Fecha	Fecha y hora en que se originó el mensaje	Fecha = "Fecha" ":" HTTP-fecha
ETag	Un identificador para una versión específica de un recurso, a menudo un compendio de mensajes	ETag: "aed6bdb8e090cd1:0"
Desde	La dirección de correo electrónico del usuario que realiza la solicitud	De: user@example.com
Si-Modificado-Desde	Permite que se devuelva un 304 No Modificado si el contenido no se ha modificado	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Última modificación	La última fecha de modificación del objeto solicitado, en formato RFC 2822	Última modificación: Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Las cabeceras específicas de la implementación pueden tener varios efectos en cualquier punto de la cadena solicitud-respuesta.	Pragma: no-cache
Referente	Es la dirección de la página web anterior desde la que se siguió un enlace a la página actualmente solicitada	Referente: HTTP://www.edgenexus.io
Servidor	Un nombre para el servidor	Servidor: Apache/2.4.1 (Unix)
Set-Cookie	Una cookie HTTP	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
Usuario-Agente	La cadena del agente de usuario	Usuario-Agente: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Varíe	Indica a los proxies descendentes cómo comparar las futuras cabeceras de las solicitudes para decidir si se puede utilizar la respuesta almacenada en la caché en lugar de solicitar una nueva al servidor de origen	Varía: User-Agent
X-Powered-By	Especifica la tecnología (por ejemplo, ASP.NET, PHP, JBoss) que soporta la aplicación web	X-Powered-By: PHP/5.4.0

Consulte	Descripción	Ejemplo
Existe	Esto no importa el detalle de la condición sólo que existe/no existe	Anfitrión - Existe
Inicie	La cadena comienza con el valor	Ruta - Hace - Inicio - /secure
Finalizar	La cadena termina con el valor	Ruta - Hace - Fin - .jpg

Contiene	La cadena sí contiene el valor	Encabezado de la solicitud - Aceptar - Contiene - imagen
Equal	La cadena sí es igual al valor	Anfitrión - Hace - Igual - www.jetnexus.com
Tener longitud	La cadena sí tiene la longitud del valor	Anfitrión - Tiene - Longitud - 16www.jetnexus.com = TRUEwww.jetnexus.co.uk = FALSE
RegEx de coincidencia	Esto le permite introducir una expresión regular completa compatible con Perl	IP de origen - Hace - Coincidir Regex - 10\..* 11\..*

Ejemplo

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

- El ejemplo tiene dos condiciones, y **AMBAS** deben cumplirse para llevar a cabo la acción
- La primera es comprobar que el objeto solicitado es una imagen
- La segunda es la comprobación de un nombre de host específico

Evaluación

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

La adición de una variable es una característica convincente que le permitirá extraer datos de la solicitud y utilizarlos en las acciones. Por ejemplo, podría registrar un nombre de usuario o enviar un correo electrónico si hay un problema de seguridad.

- Variable: Debe comenzar y terminar con el símbolo \$. Por ejemplo \$variable1\$
- Fuente: Seleccione en el cuadro desplegable la fuente de la variable
- Detalle: Seleccione de la lista cuando sea relevante. Si la Fuente=Cabecera de la Solicitud, los Detalles podrían ser Usuario-Agente
- Valor: Introduzca el texto o la expresión regular para afinar la variable.

Variables incorporadas:

- Las variables incorporadas ya han sido codificadas, por lo que no es necesario crear una entrada de evaluación para ellas.
- Puede utilizar cualquiera de las variables enumeradas a continuación en su acción
- La explicación de cada variable se encuentra en la tabla "Condición" anterior
 - Método = \$method\$
 - Ruta = \$ruta\$
 - Cadena de consulta = \$cadena de consulta\$
 - Sourceip = \$sourceip\$
 - Código de respuesta (el texto también incluye "200 OK") = \$resp\$
 - Host = \$host\$
 - Versión = \$versión\$

- Puerto del cliente = \$puerto del cliente\$
- Clientip = \$clientip\$
- Geolocalización = \$geolocation\$"

Ejemplo de acción:

- Acción = Redirección 302
 - Objetivo = HTTPs://\$host\$/404.html
- Acción = Registro
 - Objetivo = Un cliente de \$sourceip\$: \$sourceport\$ acaba de realizar una solicitud \$path\$ page

Explicación:

- Un cliente que acceda a una página que no existe se encontrará normalmente con una página 404 del navegador
- En este caso, el usuario es redirigido al nombre de host original que utilizó, pero la ruta errónea es sustituida por 404.html
- Se añade una entrada al syslog que dice "Un cliente de 154.3.22.14:3454 acaba de hacer una petición a la página wrong.html"

Fuente	Descripción	Ejemplo
Cookie	Este es el nombre y el valor de la cabecera de la cookie	MS-WSMAN=afYfn1CDqqCDqUD::Donde el nombre es MS-WSMAN y el valor es afYfn1CDqqCDqUD::
Anfitrión	Este es el nombre de host extraído de la URL	www.mywebsite.com o 192.168.1.1
Idioma	Este es el idioma extraído de la cabecera HTTP Language	Esta condición producirá un desplegable con una lista de idiomas.
Método	Este es un desplegable de métodos HTTP	El desplegable incluirá GET, POST
Ruta	Esta es la ruta del sitio web	/mi sitio web/index.html
POST	Método de solicitud POST	Comprobar los datos que se cargan en un sitio web
Elemento de consulta	Es el nombre y el valor de una consulta. Como tal, puede aceptar el nombre de la consulta o un valor también	"Best=jetNEXUS" Donde la coincidencia es Best y el valor es edgeNEXUS
Cadena de consulta	Esta es la cadena completa después del carácter ?	HTTP://servidor/ruta/programa?query_string
Solicitud de cabecera	Puede ser cualquier cabecera enviada por el cliente	Referrer, User-Agent, From, Date...
Cabecera de respuesta	Puede ser cualquier cabecera enviada por el servidor	Referrer, User-Agent, From, Date...
Versión	Esta es la versión HTTP	HTTP/1.0 o HTTP/1.1

Detalle	Descripción	Ejemplo
Acepte	Tipos de contenido aceptables	Aceptar: text/plain

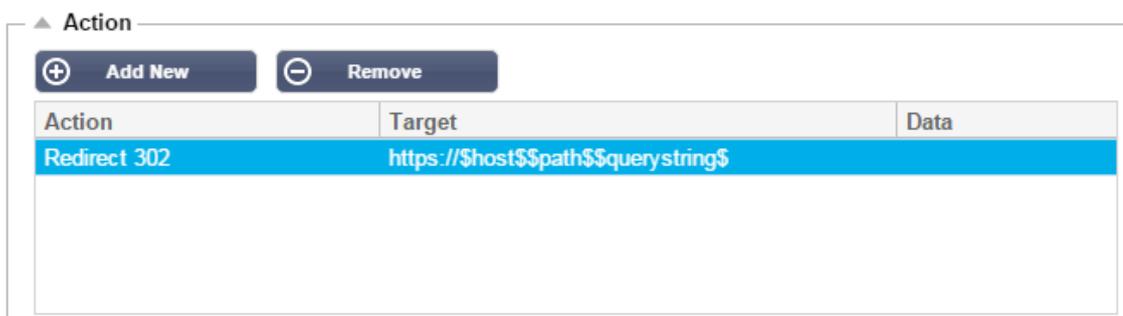
Accept-Encoding	Codificaciones aceptables	Accept-Encoding: <compress gzip deflate sdch identity>
Accept-Language	Idiomas aceptables para la respuesta	Accept-Language: en-US
Accept-Ranges	Qué tipos de rango de contenido parcial soporta este servidor	Accept-Ranges: bytes
Autorización	Credenciales de autenticación para la autenticación HTTP	Autorización: Basic QWxhZGRpbjpvGVuIHhlc2FtZQ==
Cargar a	Contiene información contable de los costes de la aplicación del método solicitado	
Codificación del contenido	El tipo de codificación utilizado en los datos.	Content-Encoding: gzip
Contenido-Longitud	La longitud del cuerpo de la respuesta en octetos (bytes de 8 bits)	Contenido-Longitud: 348
Tipo de contenido	El tipo mime del cuerpo de la solicitud (utilizado con las solicitudes POST y PUT)	Content-Type: application/x-www-form-urlencoded
Cookie	una cookie HTTP enviada previamente por el servidor con Set-Cookie (abajo)	Cookie: \$Versión=1; Skin=nuevo;
Fecha	Fecha y hora en que se originó el mensaje	Fecha = "Fecha" ":" HTTP-fecha
ETag	Un identificador para una versión específica de un recurso, a menudo un compendio de mensajes	ETag: "aed6bdb8e090cd1:0"
Desde	La dirección de correo electrónico del usuario que realiza la solicitud	De: user@example.com
Si-Modificado-Desde	Permite que se devuelva un 304 No Modificado si el contenido no se ha modificado	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Última modificación	La última fecha de modificación del objeto solicitado, en formato RFC 2822	Última modificación: Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Cabeceras específicas de la implementación que pueden tener diversos efectos en cualquier punto de la cadena solicitud-respuesta.	Pragma: no-cache
Referente	Es la dirección de la página web anterior desde la que se siguió un enlace a la página actualmente solicitada	Referente: HTTP://www.edgenexus.io
Servidor	Un nombre para el servidor	Servidor: Apache/2.4.1 (Unix)
Set-Cookie	una cookie HTTP	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
Usuario-Agente	La cadena del agente de usuario	Usuario-Agente: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Varíe	Indica a los proxies downstream	Varía: User-Agent

cómo cotejar las futuras cabeceras de las solicitudes para decidir si se puede utilizar la respuesta en caché en lugar de solicitar una nueva al servidor de origen

X-Powered-By	Especifica la tecnología (por ejemplo, ASP.NET, PHP, JBoss) que soporta la aplicación web	X-Powered-By: PHP/5.4.0
--------------	---	-------------------------

Acción

La acción es la tarea o tareas que se habilitan una vez que se ha cumplido la condición o condiciones.



Acción

Haga doble clic en la columna Acción para ver la lista desplegable.

Objetivo

Haga doble clic en la columna Objetivo para ver la lista desplegable. La lista cambiará en función de la Acción.

También puede escribir manualmente con algunas acciones.

Datos

Haga doble clic en la columna de Datos para añadir manualmente los datos que desee añadir o sustituir.

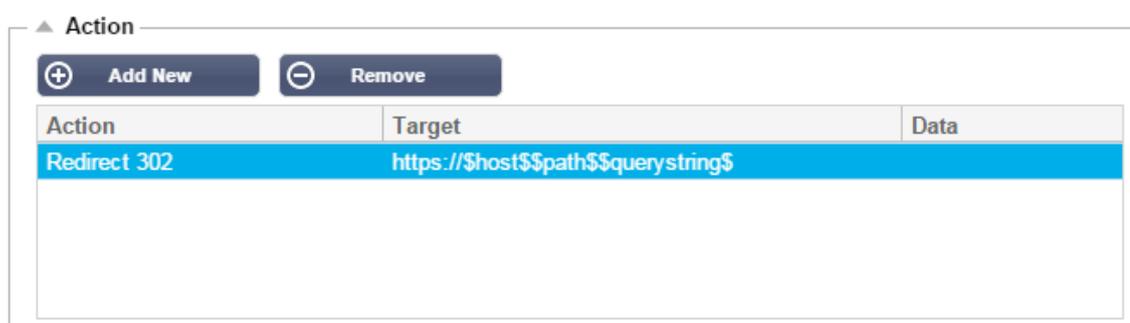
La lista de todas las acciones se detalla a continuación:

Acción	Descripción	Ejemplo
Añadir cookie de solicitud	Añada la cookie de solicitud detallada en la sección Objetivo con valor en la sección Datos	Objetivo= Cookie Datos= MS-WSMAN=afYfn1CDqqCVii
Añadir cabecera de solicitud	Añadir una cabecera de solicitud de tipo Target con valor en la sección Data	Objetivo= Aceptar Datos= imagen/png
Añadir cookie de respuesta	Añada la cookie de respuesta detallada en la sección de destino con el valor en la sección de datos	Objetivo= Cookie Datos= MS-WSMAN=afYfn1CDqqCVii
Añadir cabecera de respuesta	Añada la cabecera de la solicitud detallada en la sección Destino con valor en la sección Datos	Target= Cache-Control Datos= max-age=8888888

Cuerpo Reemplazar todo	Buscar en el cuerpo de la respuesta y reemplazar todas las instancias	Target= HTTP:// (Cadena de búsqueda) Data= HTTPs:// (Cadena de sustitución)
Reemplazar el cuerpo primero	Buscar en el cuerpo de la respuesta y reemplazar sólo la primera instancia	Target= HTTP:// (Cadena de búsqueda) Data= HTTPs:// (Cadena de sustitución)
Cuerpo Reemplazar último	Buscar en el cuerpo de la respuesta y reemplazar sólo la última instancia	Target= HTTP:// (Cadena de búsqueda) Data= HTTPs:// (Cadena de sustitución)
Gota	Esto hará que se pierda la conexión	Objetivo= N/A Datos= N/A
Correo electrónico	Enviar un correo electrónico a la dirección configurada en Eventos de correo electrónico. Puede utilizar una variable como dirección o el mensaje	Target= "flightPATH ha enviado este evento por correo electrónico" Datos= N/A
Evento de registro	Esto registrará un evento en el registro del sistema	Target= "flightPATH ha registrado esto en syslog" Datos= N/A
Redirección 301	Esto emitirá una redirección permanente	Target= HTTP://www.edgenexus.io Data= N/A
Redirección 302	Esto emitirá una redirección temporal	Target= HTTP://www.edgenexus.io Data= N/A
Eliminar la cookie de solicitud	Eliminar la cookie de solicitud detallada en la sección Objetivo	Objetivo= Cookie Datos= MS-WSMAN=afYfn1CDqqCVii
Eliminar la cabecera de la solicitud	Eliminar el encabezado de la solicitud detallado en la sección Objetivo	Target=Datos del servidor=N/A
Eliminar la cookie de respuesta	Eliminar la cookie de respuesta detallada en la sección Objetivo	Target=jnAccel
Eliminar el encabezado de la respuesta	Eliminar la cabecera de respuesta detallada en la sección Objetivo	Objetivo= Etag Datos= N/A
Reemplazar la cookie de solicitud	Sustituya la cookie de solicitud detallada en la sección de destino por el valor de la sección de datos	Objetivo= Cookie Datos= MS-WSMAN=afYfn1CDqqCVii
Sustituir la cabecera de la solicitud	Sustituir la cabecera de la solicitud en el objetivo por el valor de los datos	Objetivo= Conexión Datos= keep-alive
Reemplazar la cookie de respuesta	Reemplace la cookie de respuesta detallada en la sección Target por el valor en la sección Data	Target=jnAccel=afYfn1CDqqCDqCVii Date=MS-WSMAN=afYfn1CDqCDqCVii
Reemplazar el encabezado de la respuesta	Sustituir la cabecera de respuesta detallada en la sección Target por el valor de la sección Data	Objetivo= Servidor Datos= Retenidos por seguridad

Ruta de reescritura	Esto le permitirá redirigir la solicitud a una nueva URL en función de la condición	Target= /test/path/index.html\$querystring\$ Datos= N/A
Utilizar un servidor seguro	Seleccione qué servidor seguro o servicio virtual utilizar	Target=192.168.101: 443Data=N/A
Utilizar el servidor	Seleccione qué servidor o servicio virtual utilizar	Objetivo= 192.168.101:80Datos= N/A
Encriptar la cookie	Esto encriptará las cookies en 3DES y luego las codificará en base64	Target= Introduzca el nombre de la cookie a encriptar, puede utilizar el * como comodín al finalData= Introduzca una frase de paso para la encriptación

Ejemplo:



La acción siguiente emitirá una redirección temporal al navegador hacia un servicio virtual HTTPS seguro. Utilizará el mismo nombre de host, la misma ruta y la misma cadena de consulta que la solicitud.

Usos comunes

Cortafuegos y seguridad de las aplicaciones

- Bloquee las IPs no deseadas
- Forzar al usuario a usar HTTPS para un contenido específico (o todo)
- Bloquear o redirigir las arañas
- Prevenir y alertar sobre el cross-site scripting
- Prevenir y alertar sobre la inyección SQL
- Ocultar la estructura interna de los directorios
- Reescribir cookies
- Directorio seguro para usuarios particulares

Características

- Redirigir a los usuarios en función de la ruta
- Proporcionar un inicio de sesión único en varios sistemas
- Segmentar a los usuarios en función del ID de usuario o de la cookie
- Añadir cabeceras para la descarga de SSL
- Detección de idiomas
- Reescribir la solicitud del usuario
- Arreglar las URLs rotas
- Registro y alerta por correo electrónico de los códigos de respuesta 404
- Impedir el acceso al directorio/la navegación

- Enviar a las arañas un contenido diferente

Reglas preestablecidas

Extensión HTML

Cambia todas las peticiones .htm a .html

Estado:

- Condición = Camino
- Sentido = Hace
- Comprobación = Coincidencia de RegEx
- Valor = \Nde.htm\$

Evaluación:

- En blanco

Acción:

- Acción = Reescribir la ruta
- Objetivo = \$ruta\$

Índice

Forzar el uso de index.html en las peticiones a las carpetas.

Condición: esta condición es una condición general que coincidirá con la mayoría de los objetos

- Condición = Anfitrión
- Sentido = Hace
- Comprobación = Existir

Evaluación:

- En blanco

Acción:

- Acción = Redirección 302
- Objetivo = HTTP://\$host\$\$path\$index.html\$querystring\$

Cerrar carpetas

Denegar las solicitudes de carpetas.

Condición: esta condición es una condición general que coincidirá con la mayoría de los objetos

- Condición = esto necesita una reflexión adecuada
- Sentido =
- Comprobación =

Evaluación:

- En blanco

Acción:

- Acción =
- Objetivo =

Oculte el CGI-BBIN:

Ocultar el catálogo de cgi-bin en las peticiones a los scripts CGI.

Condición: esta condición es una condición general que coincidirá con la mayoría de los objetos

- Condición = Anfitrión
- Sentido = Hace
- Comprobación = Coincidencia de RegEX
- Valor = \\N-.cgi\$

Evaluación:

- En blanco

Acción:

- Acción = Reescribir la ruta
- Objetivo = /cgi-bin\$path\$

Araña de troncos

Registre las peticiones de la araña de los motores de búsqueda más populares.

Condición: esta condición es una condición general que coincidirá con la mayoría de los objetos

- Condición = Cabecera de la solicitud
- Coincidencia = Usuario-Agente
- Sentido = Hace
- Comprobación = Coincidencia de RegEX
- Valor = Googlebot|Slurp|bingbot|ia_archiver

Evaluación:

- Variable = \$crawler\$
- Fuente = Cabecera de la solicitud
- Detalle = Agente-Usuario

Acción:

- Acción = Registro de eventos
- Objetivo = [\$crawler\$] \$host\$\$path\$\$querystring\$

Forzar HTTPS

Forzar el uso de HTTPS para cierto directorio. En este caso, si un cliente accede a cualquier cosa que contenga el directorio /secure/, será redirigido a la versión HTTPS de la URL solicitada.

Estado:

- Condición = Camino
- Sentido = Hace
- Comprobar = Contener
- Valor = /seguro/

Evaluación:

- En blanco

Acción:

- Acción = Redirección 302
- Objetivo = HTTPs://\$host\$\$path\$\$querystring\$

Corriente de los medios de comunicación:

Redirige el Flash Media Stream al servicio apropiado.

Estado:

- Condición = Camino
- Sentido = Hace
- Comprobación = Fin
- Valor = .flv

Evaluación:

- En blanco

Acción:

- Acción = Redirección 302
- Objetivo = HTTP://\$host\$:8080/\$path\$

Cambiar HTTP por HTTPS

Cambie cualquier código duro HTTP:// por HTTPS://

Estado:

- Condición = Código de respuesta
- Sentido = Hace
- Comprobación = Igualdad
- Valor = 200 OK

Evaluación:

- En blanco

Acción:

- Acción = Cuerpo Reemplazar todo
- Objetivo = HTTP://
- Datos = HTTPs://

Tarjetas de crédito en blanco

Compruebe que no hay tarjetas de crédito en la respuesta y, si se encuentra alguna, póngala en blanco.

Estado:

- Condición = Código de respuesta
- Sentido = Hace
- Comprobación = Igualdad

- Valor = 200 OK

Evaluación:

- En blanco

Acción:

- Acción = Cuerpo Reemplazar todo
- 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]+
- Datos = xxxx-xxxx-xxxx-xxxx

Caducidad del contenido

Añada una fecha de caducidad de contenido razonable a la página para reducir el número de peticiones y 304s.

Condición: se trata de una condición genérica a modo de cajón de sastre. Se recomienda centrar esta condición en su

- Condición = Código de respuesta
- Sentido = Hace
- Comprobación = Igualdad
- Valor = 200 OK

Evaluación:

- En blanco

Acción:

- Acción = Añadir cabecera de respuesta
- Objetivo = Cache-Control
- Datos = max-age=3600

Tipo de Servidor de Falsificación

Obtenga el tipo de servidor y cámbielo por otro.

Condición: se trata de una condición genérica a modo de cajón de sastre. Se recomienda centrar esta condición en su

- Condición = Código de respuesta
- Sentido = Hace
- Comprobación = Igualdad
- Valor = 200 OK

Evaluación:

- En blanco

Acción:

- Acción = Reemplazar el encabezado de la respuesta
- Objetivo = Servidor
- Datos = Secreto

Nunca envíe errores

El cliente nunca recibe errores de su sitio.

Condición

- Condición = Código de respuesta
- Sentido = Hace
- Comprobar = Contener
- Valor = 404

Evaluación

- En blanco

Acción

- Acción = Redirección 302
- Objetivo = HTTP//\$host\$/

Redirección sobre la lengua

Encuentre el código del idioma y redirija al dominio del país correspondiente.

Condición

- Condición = Lengua
- Sentido = Hace
- Comprobar = Contener
- Valor = alemán (estándar)

Evaluación

- Variable = \$host_template\$
- Fuente = Anfitrión
- Valor = .*\\N-

Acción

- Acción = Redirección 302
- Objetivo = HTTP//\$host_template\$de\$path\$\$querystring\$

Google Analytics

Inserte el código requerido por Google para la analítica - Por favor, cambie el valor MYGOOGLECODE por su ID de Google UA.

Condición

- Condición = Código de respuesta
- Sentido = Hace
- Comprobación = Igualdad
- Valor = 200 OK

Evaluación

- en blanco

Acción

- Acción = Cuerpo Reemplazar último
- Objetivo = </body>

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

Pasarela IPv6

Ajustar la cabecera del host para los servidores IPv4 de IIS en los servicios IPv6. A los servidores IPv4 de IIS no les gusta ver una dirección IPV6 en la solicitud del cliente del host, por lo que esta regla la sustituye por un nombre genérico.

Condición

- en blanco

Evaluación

- en blanco

Acción

- Acción = Reemplazar la cabecera de la solicitud
- Objetivo = Anfitrión
- Datos = ipv4.host.header

Cortafuegos de aplicaciones web (edgeWAF)

El cortafuegos de aplicaciones web (WAF) está disponible bajo petición y su licencia es de pago anual. La instalación del WAF se realiza mediante la sección de Apps incorporada dentro del CAD.

Ejecución del WAF

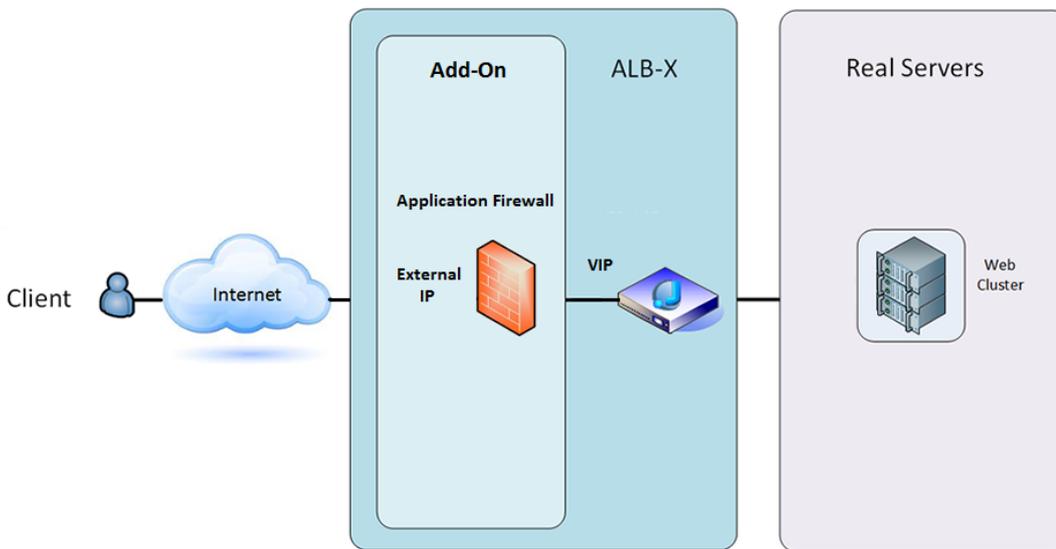
Al ejecutarse en un contenedor Docker, el WAF necesita que se establezcan algunos parámetros de red antes de iniciarlo.

Opción	Descripción
Detener	Aparecerá en gris hasta que se inicie una instancia Docker. Pulse este botón para detener la instancia Docker.
Pausa	Este botón pondrá en pausa el complemento.
Juega a	Iniciará el complemento con la configuración actual.
Nombre del contenedor	Dé a su contenedor un nombre para identificarlo de los demás contenedores. Este debe ser único. Puede utilizarlo como nombre para un servidor real si lo desea y se resolverá automáticamente a la dirección IP interna de la instancia
IP externa	Aquí puede establecer una IP externa para acceder a su Add-On. Esto puede ser para acceder a la GUI del Add-On así como al servicio que se ejecuta a través del Add-On. En el caso del Add-On Firewall esta es la dirección IP de su servicio HTTP. El Cortafuegos puede entonces ser configurado para acceder a un servidor o a un ALB-X VIP que contenga múltiples servidores para el equilibrio de carga.
Puerto externo	Si deja esto en blanco, entonces todos los puertos serán reenviados a su Firewall. Para restringir esto entonces simplemente añada en la lista de puertos separados por comas. Ejemplo 80, 443, 88. Tenga en cuenta que la dirección de la GUI del cortafuegos será HTTP//[IP externa]88/waf . Por lo tanto, deje la configuración del puerto externo en blanco o añada el puerto 88 para acceder a la interfaz gráfica de usuario si está restringiendo la lista de puertos.
Actualización	Sólo puede actualizar la configuración de un complemento una vez que se haya detenido. Una vez que su instancia se ha detenido, puede cambiar el nombre del contenedor, la IP externa y la configuración del puerto externo.
Eliminar el complemento	Eliminará completamente el Add-On de la página de Add-On. Tendrá que ir a la página Biblioteca-Apps para desplegar el Add-On de nuevo.
Imagen de los padres	Indica la imagen Docker a partir de la cual se construye el Add-On. Puede haber varias versiones de un cortafuegos o incluso de otro tipo de complemento por completo, por lo que esto ayudará a distinguirlas. Esta sección es sólo para fines informativos y por lo tanto está en gris.

IP interna	Docker crea automáticamente la dirección IP interna y, por tanto, no puede ser editada. Si detiene la instancia Docker y la reinicia, se emitirá una nueva dirección IP interna. Por esta razón, debe utilizar una dirección IP externa para su servicio o utilizar el nombre del contenedor para la dirección real del servidor de su servicio.
Comenzó en	Esto indicará la fecha y la hora en que se inició el complemento. Ejemplo 2016-02-16 155721
Detenido en	Esto indicará la fecha y la hora en que se detuvo el complemento. Ejemplo 2016-02-24 095839

Ejemplo de arquitectura

WAF utilizando la dirección IP externa

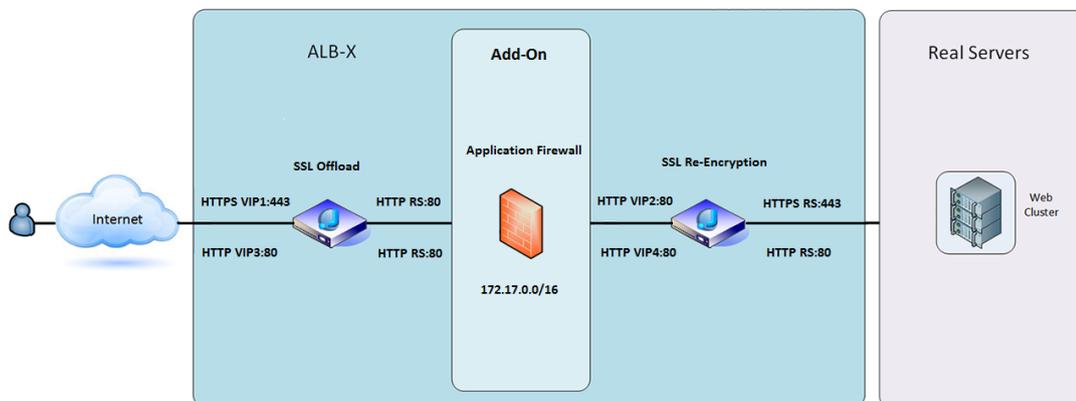


En esta arquitectura, sólo se puede utilizar HTTP para su servicio, ya que el cortafuegos no puede inspeccionar el tráfico HTTPS.

El cortafuegos tendrá que ser configurado para enviar el tráfico al ALB-X VIP.

El ALB-X VIP, a su vez, se configurará para equilibrar la carga del tráfico hacia su clúster web.

WAF utilizando la dirección IP interna



En esta arquitectura, puede especificar HTTP y HTTPS.

HTTPS puede ser de extremo a extremo, donde las conexiones desde el Cliente a ALB-X están encriptadas y desde el ALB-X a los Servidores Reales.

El tráfico desde el ALB-X hacia la dirección IP interna del cortafuegos debe ser descifrado para que pueda ser inspeccionado.

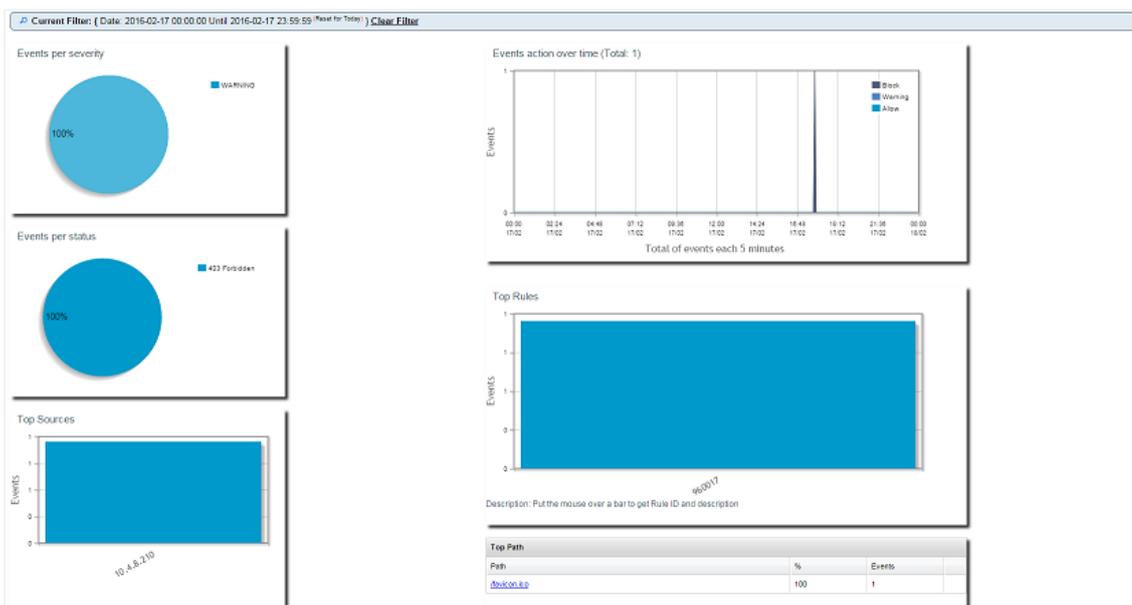
Una vez que el tráfico ha atravesado el cortafuegos, se reenvía a otro VIP que puede volver a cifrar el tráfico y equilibrar la carga hacia servidores seguros o simplemente equilibrar la carga hacia servidores inseguros a través de HTTP.

Acceso a su complemento WAF

- Rellene los datos de su cortafuegos
- Puede restringir los puertos a lo que necesite o dejarlo en blanco para permitir todos los puertos
- Pulse el botón de reproducción
- Aparecerá un botón de la interfaz gráfica de usuario (GUI) de Add-On



- Pulse este botón y se abrirá un navegador en HTTP://[IP externa]:88/waf
- En este ejemplo, será HTTP://10.4.8.15:88/waf
- Se le presentará un diálogo de inicio de sesión.
- Introduzca las credenciales de su CAD.
- Una vez que haya iniciado la sesión con éxito, se le presentará la página de inicio del WAF.

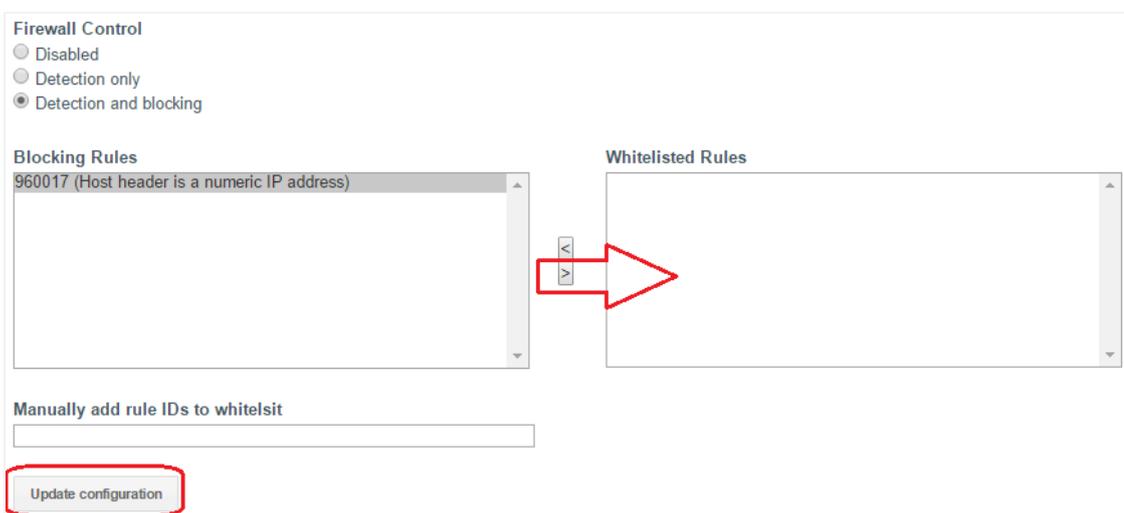


- La página de inicio muestra un resumen gráfico de los eventos, es decir, de las acciones de filtrado realizadas por el cortafuegos de aplicaciones.

- Lo más probable es que los gráficos estén en blanco cuando abra la página por primera vez, ya que no habrá intentos de acceso a través del cortafuegos.
- Puede configurar la dirección IP o el nombre de dominio del sitio web al que desea enviar el tráfico después de que el cortafuegos lo haya filtrado.
- Esto se puede cambiar en la sección de Gestión > Configuración



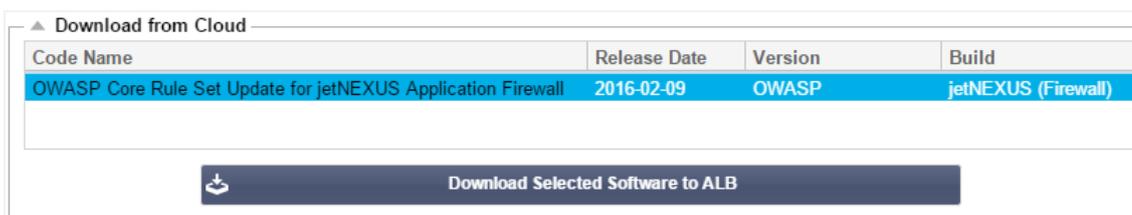
- El cortafuegos inspeccionará el tráfico y luego lo enviará a la dirección IP del servidor real o a la dirección VIP que aparece aquí. También puede introducir un puerto junto con su dirección IP. Si introduce una dirección IP por sí sola, se asumirá que el puerto es el 80. Pulse el botón "Actualizar configuración" para guardar esta nueva configuración.
- Cuando el cortafuegos bloquea un recurso de aplicación, la regla que está bloqueando el tráfico aparecerá en la lista de Reglas de bloqueo de la página de la lista blanca.
- Para evitar que el cortafuegos bloquee el recurso de la aplicación válida, mueva la regla de bloqueo a la sección Reglas de la lista blanca.



- Pulse Actualizar configuración cuando haya transferido todas las reglas de la sección de bloqueo a la sección de lista blanca.

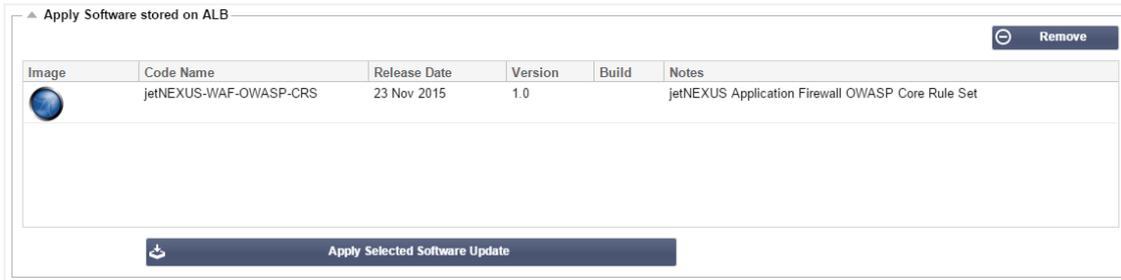
Actualización de las normas

- Las reglas del cortafuegos de aplicaciones se pueden actualizar accediendo a la sección Avanzado - Software
- Haga clic en Actualizar para ver el botón de software disponible en la sección Detalles de la actualización del software
- Ahora aparece una casilla adicional llamada Descarga desde la nube
- Compruebe si hay un conjunto de reglas básicas de OWASP disponible



- Si es así, puede resaltar y hacer clic en Descargar el software seleccionado en ALB-X

- Esta acción descargará el archivo inteligente en el software de aplicación almacenado en el ALB



- Resalte el jetNEXUS-WAF-OWASP-CRS y haga clic en Aplicar la actualización de software seleccionada y haga clic en Aplicar
- El cortafuegos detectará automáticamente el conjunto de reglas actualizado, lo cargará y lo aplicará.
- Los ID de las reglas de la lista blanca se mantendrán. Sin embargo, las nuevas reglas pueden empezar a bloquear recursos de aplicación válidos.
- En este caso, compruebe la lista de reglas de bloqueo en la página de la lista blanca.
- También puede comprobar la sección de información de gestión de la interfaz gráfica de usuario del cortafuegos para ver la versión de OWASP CRS

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

Equilibrio global de la carga del servidor (edgeGSLB)

Introducción

El equilibrio de la carga del servidor global (GSLB) es un término que se utiliza para describir los métodos de distribución del tráfico de red en Internet. El GSLB es diferente del Equilibrio de la Carga del Servidor (SLB) o del Equilibrio de la Carga de la Aplicación (ALB), ya que suele utilizarse para distribuir el tráfico entre varios centros de datos, mientras que un ADC/SLB tradicional se utiliza para distribuir el tráfico dentro de un único centro de datos.

El GSLB se suele utilizar en las siguientes situaciones:

Resiliencia y recuperación de desastres

Tiene varios centros de datos y desea ejecutarlos en una situación Activo-Pasivo, de modo que si un centro de datos falla, el tráfico se enviará al otro.

Equilibrio de carga y geolocalización

Le gustaría distribuir el tráfico entre los centros de datos en una situación Activo-Activo basándose en criterios específicos como el rendimiento del centro de datos, la capacidad del centro de datos, la comprobación de la salud del centro de datos y la ubicación física del cliente (para poder enviarlo a su centro de datos más cercano), etc.

Consideraciones comerciales

Garantizar que los usuarios de determinadas ubicaciones geográficas sean enviados a determinados centros de datos. Garantizar que se sirvan (o bloqueen) contenidos diferentes a otros usuarios, en función de varios criterios como el país en el que se encuentra el cliente, el recurso que solicita, el idioma, etc.

Visión general del sistema de nombres de dominio

El GSLB puede ser complejo, por lo que merece la pena dedicar tiempo a entender cómo funciona el misterioso sistema de servidores de nombres de dominio (DNS).

El DNS consta de tres componentes clave:

- El resolutor de DNS, es decir, el Cliente: el resolutor es responsable de iniciar las consultas que finalmente conducen a una resolución completa del recurso requerido.
- Servidor de nombres: es el servidor de nombres al que se conecta inicialmente el cliente para realizar la resolución DNS.
- Servidores de nombres autorizados: Incluye los servidores de nombres de dominio de nivel superior (TLD) y los servidores de nombres raíz.

A continuación se explica una transacción típica de DNS:

- Un usuario teclea 'ejemplo.com' en un navegador web, y la consulta viaja a Internet y es recibida por un resolver recursivo DNS.
- A continuación, el resolutor consulta un servidor de nombres raíz DNS (.).
- El servidor raíz responde entonces al resolutor con la dirección de un servidor DNS de dominio de primer nivel (TLD) (como .com o .net), que almacena la información de sus dominios. Al buscar ejemplo.com, nuestra petición se dirige al TLD .com.
- El resolutor solicita entonces el TLD .com.
- El servidor del TLD responde entonces con la dirección IP del servidor de nombres del dominio, ejemplo.com.

- Por último, el resolvidor recursivo envía una consulta al servidor de nombres del dominio.
- La dirección IP, por ejemplo.com, se devuelve entonces al resolver desde el servidor de nombres.
- El resolver DNS responde entonces al navegador web con la dirección IP del dominio solicitado inicialmente.
- Una vez que los ocho pasos de la búsqueda DNS han devuelto la dirección IP, por ejemplo.com, el navegador puede solicitar la página web:
- El navegador realiza una petición **HTTP** a la dirección IP.
- El servidor de esa IP devuelve la página web para que sea renderizada en el navegador.

Este proceso puede complicarse aún más:

Caché

Los servidores de nombres que resuelven las respuestas en caché pueden enviar la misma respuesta a muchos clientes. Los resolutores del lado del cliente y las aplicaciones pueden tener diferentes políticas de almacenamiento en caché.

Nota: Para las pruebas, detenemos y desactivamos el Cliente DNS de Windows dentro de la sección de servicios de su sistema operativo. Los nombres DNS seguirán resolviéndose; sin embargo, no almacenará en caché los resultados ni registrará el nombre del ordenador. El administrador de su sistema deberá decidir si ésta es la mejor opción para su entorno, ya que puede afectar a otros servicios.

Tiempo de vivir

El servidor de nombres que resuelve puede ignorar el tiempo de vida (TTL), es decir, el tiempo de caché de la respuesta.

Visión general de GSLB

El GSLB se basa en el DNS y utiliza un mecanismo muy similar al descrito anteriormente.

El CAD puede cambiar la respuesta en función de varios factores que se describen más adelante en la guía. El CAD hace uso de los monitores que comprueban la disponibilidad de los recursos remotos accediendo al propio recurso. Sin embargo, para aplicar cualquier lógica, el sistema debe recibir primero la solicitud DNS.

Hay varios diseños que lo permiten. El primero es aquel en el que el GSLB actúa como servidor de nombres autoritativo.

El segundo diseño es la implementación más común y es similar a la configuración del servidor de nombres autoritativo pero utiliza un subdominio. El servidor DNS primario autoritativo no es sustituido por el GSLB, sino que delega un subdominio para su resolución. La delegación directa de nombres o el uso de CNAMEs le permite controlar lo que es y lo que no es manejado por el GSLB. En este caso, no tiene que dirigir todo el tráfico DNS al GSLB para los sistemas que no requieren GSLB.

Se proporciona redundancia para que si un servidor de nombres (GSLB) falla, entonces el servidor de nombres remoto emite automáticamente otra solicitud a otro GSLB, evitando que el sitio web se caiga.

Configuración del GSLB

Después de descargar el complemento GSLB, despléguelo visitando la página Biblioteca > Aplicaciones de la interfaz gráfica de usuario del CAD y haciendo clic en el botón "Desplegar", como se muestra a continuación.



Tras la instalación, configure los detalles del complemento GSLB, incluyendo el nombre del contenedor, la IP externa y los puertos externos en la página Biblioteca > Complementos de la interfaz gráfica de usuario del CAD, como se muestra en la figura siguiente.

- El nombre del contenedor es un nombre único de una instancia de Add-On en ejecución, alojada por el ADC, se utiliza para distinguir varios Add-Ons de un mismo tipo.
- La IP externa es la IP de su red que se asignará al GSLB.
- Debe configurar el GSLB para que tenga una dirección IP externa si quiere tomar decisiones basadas en el GEO, ya que esto permitirá al GSLB ver la dirección IP real de los clientes.
- Puertos externos es la lista de puertos TCP y UDP de GSLB, a los que se puede acceder desde otros hosts de la red.
- Por favor, ponga "53/UDP, 53/TCP, 9393/TCP" en la casilla de entrada de Puertos Externos para permitir las comunicaciones DNS (53/UDP, 53/TCP) y edgeNEXUS GSLB GUI (9393/TCP).
- Después de configurar los detalles del complemento, haga clic en el botón Actualizar.
- Inicie el complemento GSLB haciendo clic en el botón Ejecutar.



- El siguiente paso es permitir que el complemento edgeNEXUS GSLB lea y cambie la configuración del ADC.
- Por favor, visite la página Sistema > Usuarios de la GUI del CAD y edite un usuario con el mismo nombre que el Add-On GSLB que ha desplegado, como se muestra en la figura siguiente.
- Edite el usuario "gslb1" y marque API, luego haga clic en Actualizar - en versiones posteriores del software puede que ya esté marcada por defecto.

Users

Username:

Old Password:

New Password:

Confirm Password:

Group Membership: Admin
 GUI Read Write
 GUI Read
 SSH
 API
 Add-Ons

- El siguiente paso sólo es necesario si está configurando el GSLB con fines de prueba o evaluación y no quiere modificar ningún dato de la zona DNS en Internet.
- En este caso, instruya al ADC para que utilice el complemento GSLB como su servidor primario de resolución DNS modificando "Servidor DNS 1 en la página Sistema > Red de la interfaz gráfica de usuario del ADC, como se muestra en la figura siguiente.
- El servidor DNS 2 puede configurarse generalmente con su servidor DNS local o con uno de Internet, como Google 8.8.8.8.

Network

Basic Setup

ALB Name:

IPv4 Gateway:

DNS Server 1: DNS Server 2:

IPv6 Gateway:

- Ahora es el momento de entrar en la GUI de GSLB.
- Vaya a la página Biblioteca > Complementos de la interfaz gráfica de usuario del CAD y haga clic en el botón Complementos de la interfaz gráfica de usuario.
- Al hacer clic se abrirá una nueva pestaña del navegador que presenta la página de inicio de sesión de la GUI de GSLB, como se muestra a continuación.

EDGE NEXUS

Sign In Edgenexus GSLB

Username

Password

Remember

Edgenexus Global Server Load Balancer

- El nombre de usuario por defecto es admin, y la contraseña por defecto es jetnexus. Por favor, no olvide cambiar su contraseña en la página Administrador > Mi perfil de la GUI de GSLB.
- El siguiente paso en la secuencia de configuración es crear una zona DNS en el servidor de nombres PowerDNS, que forma parte de GSLB, convirtiéndolo en un servidor de nombres autoritativo para la zona "ejemplo.org" o en una zona de subdominio, como el subdominio "geo.ejemplo.org" mencionado en la sección "Visión general de GSLB basado en DNS" anterior.
- Para obtener detalles en profundidad sobre la configuración de la zona DNS, consulte la [DOCUMENTACIÓN DE POWERDNS NAMESERVER](#). En la figura 6 se muestra una zona de ejemplo.

* La GUI de edgeNEXUS GSLB se basa en un proyecto de código abierto PowerDNS-Admin.



- Después de crear una zona DNS, haga clic en el botón Gestionar y añada nombres de host al dominio, como se muestra en la figura siguiente.
- Después de editar cualquier registro existente dentro de la interfaz gráfica de usuario de GSLB, pulse el botón Guardar.
- Una vez que haya terminado de crear los registros de nombres de host, haga clic en el botón Aplicar cambios. Si no hace clic en Aplicar y luego modifica la página, perderá los cambios.
- A continuación hemos creado registros que son registros de direcciones IPv4.
- Asegúrese de crear un registro para todos los registros que desee que se resuelvan, incluidos los registros AAAA para las direcciones IPv6.



- Ahora, volvamos a la GUI del ADC y definamos un Servicio Virtual que corresponda a la zona DNS que acabamos de crear.

Virtual Services								
Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port	Service Name	Service Type
Stand-alone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.4.10	255.255.255.224	80	service1.gslb.garychristie.com	HTTP

Real Servers							
Status	Activity	Address	Port	Weight	Calculated Weight	Notes	
<input checked="" type="checkbox"/>	Online	alb1.gslb.garychristie.com	80	100	100	US East	
<input checked="" type="checkbox"/>	Online	alb2.gslb.garychristie.com	80	100	100	UK Marlow	

- El servicio virtual se utilizará para la comprobación de la salud de los servidores en el dominio GSLB.
- El GSLB aprovecha el mecanismo de comprobación de la salud del CAD, incluidos los monitores personalizados. Puede utilizarse con cualquiera de los tipos de servicio admitidos por el CAD.
- Vaya a la página Servicios > Servicios IP de la interfaz gráfica de usuario del CAD y cree un servicio virtual, como se muestra en la figura siguiente.
- Asegúrese de configurar el Nombre de Servicio con el nombre de dominio correcto que desea utilizar en el GSLB. El GSLB lo leerá a través de la API y rellenará automáticamente la sección de Servicios Virtuales en la GUI del GSLB.
- Por favor, añada todos los servidores del dominio GSLB en la sección de Servidores Reales de la imagen anterior.
- Puede especificar los servidores, ya sea por sus nombres de dominio o por sus direcciones IP.
- Si especifica los nombres de dominio, entonces utilizará los registros creados en su GSLB.
- Puede elegir diferentes métodos y parámetros de supervisión del estado del servidor en las pestañas Básico y Avanzado.
- Puede establecer la actividad de algunos servidores en Standby para un escenario Activo-Pasivo.
- En este caso, si un servidor "Online" falla en la comprobación de salud y hay un servidor Standby sano, Edgenexus EdgeGSLB resolverá el nombre de dominio a una dirección del servidor Standby.
- Por favor, consulte la sección de **SERVICIOS** Virtuales para obtener detalles sobre la configuración de los Servicios Virtuales.
- Ahora, pasemos a la interfaz gráfica de usuario de GSLB.
- Vaya a la página de servicios virtuales y seleccione una política GSLB para el dominio de la API recuperada de la sección de servicios virtuales del ADC.
- Esto se muestra en la siguiente figura.

Name	Enabled	Type	IP Address	Subnet Mask / Prefix	Port	GSLB Policy	Edit	Manage
service1.gslb.garychristie.com	<input checked="" type="checkbox"/>	HTTP	192.168.4.10	255.255.255.224	80	Geolocation	SAVE	CANCEL

Showing 1 to 1 of 1 entries

- La GSLB apoya las siguientes políticas:

Política	Descripción
----------	-------------

Peso fijo	El GSLB selecciona el servidor con el mayor peso (la ponderación del servidor puede ser asignada por el usuario). En el caso de que varios servidores tengan el peso más alto, el GSLB seleccionará uno de estos servidores al azar.
Round Robin ponderado	Elija los servidores uno a uno, en fila. Los servidores que tienen mayor peso se seleccionan más a menudo que los que tienen menor peso.
Geolocalización	Proximidad: elija un servidor que esté situado lo más cerca posible de la ubicación del cliente utilizando los datos geográficos de latitud y longitud. Se prefieren los servidores del mismo país que el cliente, aunque estén más alejados que los servidores de los países vecinos.
Geolocalización	Coincidencia de ciudad: elija un servidor en la misma ciudad que el cliente. Si no hay ningún servidor en la ciudad del cliente, seleccione un servidor en el país del cliente. Si no hay ningún servidor en el país del cliente, seleccione un servidor en el mismo continente. Si esto no es posible, seleccione un servidor que esté situado lo más cerca posible de la ubicación del cliente utilizando los datos geográficos de latitud y longitud.
Geolocalización	Coincidencia de país: elija un servidor en el mismo país que el cliente. Si no hay ningún servidor en el mismo país, pruebe en el mismo continente y luego en la ubicación más cercana.
Geolocalización	Coincidencia de continente: elija un servidor en el mismo continente que el cliente. Si no hay ningún servidor en el mismo continente, pruebe con la ubicación más cercana.

- Después de haber seleccionado una política GSLB, no olvide hacer clic en el botón Aplicar cambios.
- Ahora puede revisar y ajustar los detalles del Servicio Virtual haciendo clic en el botón Gestionar.
- Esto presentará una página que se muestra a continuación.
- Si ha seleccionado una de las políticas basadas en el peso, es posible que tenga que ajustar los pesos GSLB del servidor.
- Si ha seleccionado una de las políticas GSLB basadas en la geolocalización, es posible que tenga que especificar los datos geográficos de los servidores.
- Si no especifica ningún dato geográfico para los servidores, el GSLB utilizará los datos proporcionados por [LA BASE DE DATOS GEOLITE2 DE MAXMIND](#).
- También puede modificar el nombre del servidor, el puerto y la actividad en esta página.
- Estos cambios se sincronizarán con el CAD cuando pulse el botón "Aplicar cambios".



- Una buena manera de comprobar qué respuestas enviará el GSLB a los clientes es utilizar NSLOOKUP.
- Si está utilizando Windows, el comando es el siguiente.

NSLOOKUP servicio1.gslb.garychristie.com 192.168.4.10

- Donde servicio1.gslb.garychristie.com es el nombre de dominio que desea resolver.
- Donde 192.168.4.10 es la dirección IP externa de su GSLB.
- Para comprobar qué dirección IP se devuelve en Internet, puede utilizar el servidor DNS de google de 8.8.8.8.

Nslookup servicio1.gslb.garychristie.com 8.8.8.8.

- Como alternativa, puede utilizar algo como HTTPs://dnschecker.org. Ejemplo HTTPs://dnschecker.org/#A/service1.gslb.garychristie.com.
- Vea a continuación un ejemplo de los resultados.



DNS Propagation Check

service1.gslb.garychristie.com A Search

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

Check DNS Resolution

Your IP: 89.240.14.179

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

Ubicaciones personalizadas

Redes privadas

El GSLB también puede configurarse para utilizar ubicaciones personalizadas, de modo que pueda utilizarlo en redes "privadas" internas. En el escenario anterior, el GSLB determina la ubicación del cliente cruzando la dirección IP pública del cliente con una base de datos para calcular su ubicación. También calcula la ubicación de la dirección IP del servicio a partir de la misma base de datos, y si la política de equilibrio de carga está configurada como política GEO, devolverá la dirección IP más cercana. Este método funciona perfectamente con las direcciones IP públicas, pero no existe una base de datos de este tipo para las direcciones privadas internas que se ajustan al RFC 1918 para las direcciones IPv4 y al RFC 4193 para las direcciones IPv6.

Consulte la página de Wikipedia que explica el direccionamiento privado

[HTTPS://EN.WIKIPEDIA.ORG/WIKI/PRIVATE_NETWORK](https://en.wikipedia.org/wiki/Private_network)

Cómo funciona

Normalmente, la idea de utilizar nuestro GSLB para las redes internas es que los usuarios de direcciones específicas reciban una respuesta diferente para un servicio dependiendo de la red en la que se encuentren. Así, consideremos dos centros de datos, Norte y Sur, que proporcionan un servicio llamado norte.servicio1.gslb.com y sur.servicio1.gslb.com, respectivamente. Cuando un usuario del centro de datos

del Norte consulta el GSLB, queremos que éste responda con la dirección IP asociada a norte.servicio1.gslb.com siempre que el servicio funcione correctamente. Por otro lado, si un usuario del centro de datos del sur consulta el GSLB, queremos que éste responda con la dirección IP asociada a sur.servicio1.gslb.com de nuevo, siempre que el servicio funcione correctamente.

Entonces, ¿qué tenemos que hacer para que se produzca el escenario anterior?

- Necesitamos tener al menos dos ubicaciones personalizadas, una para cada centro de datos
- Asigne las distintas redes privadas a estas ubicaciones
- Asigne cada servicio a la ubicación respectiva

¿Cómo configuramos este aspecto en el GSLB?

Añadir una ubicación para el Centro de Datos del Norte

- Haga clic en Ubicaciones personalizadas en el lado izquierdo
- Haga clic en Añadir ubicación
- Nombre
 - Norte
- Añada una dirección IP privada y una máscara de subred para su red del Norte. Para este ejercicio, supondremos que el servicio y las direcciones IP del cliente están en la misma red privada
 - 10.1.1.0/24
- Añada el código del continente
 - UE
- Añada el código de país
 - REINO UNIDO
- Añadir ciudad
 - Enfield
- Añadir latitud - obtenida de google
 - 51.6523
- Añadir longitud - obtenida de google
 - 0.0807

Nota, por favor, utilice los códigos correctos que puede obtener de aquí

Añadir una ubicación para el Centro de Datos del Sur

- Haga clic en Ubicaciones personalizadas en el lado izquierdo
- Haga clic en Añadir ubicación
- Nombre
 - Sur
- Añada una dirección IP privada y una máscara de subred para su red Sur. Supondremos que el servicio y las direcciones IP del cliente están en la misma red privada para este ejercicio.
 - 192.168.1.0/24
- Añada el código del continente
 - UE
- Añada el código de país
 - REINO UNIDO
- Añadir ciudad
 - Croydon
- Añadir latitud - obtenida de google
 - 51.3762
- Añadir longitud - obtenida de google
 - 0.0982

Nota, por favor, utilice los códigos correctos que puede obtener de [AQUÍ](#)

Custom Locations

ADD LOCATION + APPLY CHANGES

15 records Search:

Name	IP Address	Subnet Mask / Prefix	Continent	Country	City	Latitude	Longitude	Edit	Delete
North	10.1.1.0	24	EU	UK	Enfield	51.6523	0.0807		
South	192.168.1.0	24	EU	UK	Croydon	51.3762	0.0982		

Showing 1 to 2 of 2 entries < 1 >

Añada un registro A para north.service1.gslb.com

- Haga clic en el dominio service1.gslb.com
- Haga clic en Añadir registro
- Añadir nombre
 - Norte
- Tipo
 - A
- Estado
 - Activo
- TTL
 - 1 minuto
- Dirección IP
 - 10.1.1.254 (Tenga en cuenta que está en la misma red que la localidad de Enfield)

Añada un registro A para south.service1.gslb.com

- Haga clic en el dominio service1.gslb.com
- Haga clic en Añadir registro
- Añadir nombre
 - Sur
- Tipo
 - A
- Estado
 - Activo
- TTL
 - 1 minuto
- Dirección IP
 - 192.168.1.254 (Tenga en cuenta que está en la misma red que la localidad de Croydon)

Home > Domain > service1.gslb.com

service1.gslb.com

ADD RECORD + APPLY CHANGES

15 records Search:

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

Showing 1 to 3 of 3 entries < 1 >

Flujo de tráfico

Ejemplo 1 - Cliente en el Centro de Datos del Norte

- El cliente IP 10.1.1.23 consulta a GSLB para el servicio1.gslb.com
- GSLB busca la dirección IP 10.1.1.23 y la hace coincidir con la ubicación personalizada Enfield 10.1.1.0/24
- GSLB mira sus registros A para el servicio1.gslb.com y coincide con north.service1.gslb.com ya que también está en la red 10.1.1.0/24
- GSLB responde a 10.1.1.23 con la dirección IP 10.1.1.254 para service1.gslb.com

Ejemplo 2 - Cliente en el centro de datos del sur

- El cliente IP 192.168.1.23 consulta a GSLB para el servicio1.gslb.com
- GSLB busca la dirección IP 192.168.1.23 y la hace coincidir con la ubicación personalizada Croydon 192.168.1.0/24
- GSLB mira sus registros A para el servicio1.gslb.com y coincide con south.service1.gslb.com ya que también está en la red 192.168.1.0/24
- GSLB responde a 192.168.1.23 con la dirección IP 192.168.1.254 para service1.gslb.com

Soporte técnico

Proporcionamos soporte técnico a todos nuestros usuarios según las condiciones de servicio estándar de la empresa.

Le proporcionaremos todo el apoyo a través del soporte técnico si tiene un contrato de soporte y mantenimiento activo para el edgeADC, el edgeWAF o el edgeGSLB.

Para elevar un ticket de soporte, por favor visite:

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