EDGE
NEXUS

EdgeADC

EdgeADC Administration Guide

Contents

Document Properties

Document Number: 2.0.11.17.21.14.11

Document Creation Date: April 30, 2021

Document Last Edited: November 17, 2021

Document Author: Jay Savoor

Document Last Edited by:

Document Referral: EdgeADC - Version 4.2.8.1909

Document Disclaimer

This manual's screenshots and graphics may differ slightly from your product due to differences in product release. Edgenexus ensures that they make every reasonable effort to ensure that the information in this document is complete and accurate. Edgenexus assumes no liability for any errors. Edgenexus makes changes and corrections to the information in this document in future releases when the need arises.

Copyrights

Trademarks

The Edgenexus logo, Edgenexus, EdgeADC, EdgeWAF, EdgeGSLB, EdgeDNS are all trademarks or registered trademarks of Edgenexus Limited. All other trademarks are the properties of their respective owners and are acknowledged.

Edgenexus Support

If you have any technical questions regarding this product, please raise a support ticket at: support@edgenexus.io

Installing the EdgeADC

The EdgeADC (referred to as ADC) product is available for installation using several methods. Each platform target requires its installer, and these are all available to you.

These are the various installation models available.

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

The sizing of the virtual machine you will use to host the ADC depends on the use case scenario and the data throughput.

VMware ESXi

ADC is available for installation on VMware ESXi are 5.x and above.

- Download the latest installation OVA package of ADC using the appropriate link provided with the download email.
- Once downloaded, please unzip in a suitable directory on your ESXi host or SAN.
- In your vSphere client, select File: Deploy OVA/OVF Template.
- Browse and select the location where you have saved your files; choose the OVF file and click **NEXT**
- The ESX server requests the appliance name. Type a suitable name and click **NEXT**
- Select the datastore from where your ADC appliance will run.
- Select a datastore with enough space and click **NEXT**
- You then will be told information about the product; click **NEXT**
- Click **NEXT.**
- Once you have copied the files to the datastore, you can install the virtual appliance.

Launch your vSphere client to see the new ADC virtual appliance.

- Right-click on the VA and go to Power > Power-On
- Your VA will then boot, and the ADC boot screen will show on the console.

```
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

_
```

Installing the VMXNET3 Interface

The VMXnet3 driver is supported, but you will need to make changes to the NIC settings first.

Note – Do NOT upgrade the VMware-tools

Enabling the VMXNET3 interface on a freshly imported VA (never started)

1. Delete both NICs from the VM

2. Upgrade the VM hardware – -Right-click on the VA in the list and select Upgrade Virtual Hardware (do not start a VMware tools installation or update, **only** perform the hardware upgrade)
3. Add two NICs and selected them to be VMXNET3
4. Start the VA using the standard method. It will work with the VMXNET3

Enabling VMXNET3 interface on an already running VA

1. Stop the VM (CLI shutdown command or GUI power-off)
2. Get the MAC addresses of both NICs (remember the order of the NICs in the list!)
3. Delete both NICs from the VM
4. Upgrade the VM hardware (do not start a VMware tools installation or update, **only** perform the hardware upgrade)
5. Add two NICs and select them to be VMXNET3
6. Set the MAC addresses for the new NICs accordingly to step 2
7. Restart the VA

We support VMware ESXi as the production platform. For evaluation purposes, you can use VMware Workstation and Player.

Please refer to the section **FIRST BOOT CONFIGURATION** to proceed further.

Microsoft Hyper-V

The Edgenexus ADC Virtual appliance can be easily installed within a Microsoft Hyper-V virtualization framework. This guide assumes you have correctly specified and configured your Hyper-V system and system resources to accommodate the ADC and its load balancing architecture.

Note each appliance requires a unique MAC address.

- Extract the downloaded Hyper-V compatible ADC-VA file to your local machine or server.
- Open Hyper-V Manager.
- Create a new folder to contain the ADC VA 'Virtual hard disk' and another new folder to contain the 'Storage hard disk,' e.g., C:\Users\Public\Documents\Hyper-V\Virtual hard disks\ADC1 and C:\Users\Public\Documents\Hyper-V\Storage hard disks\ADC1
- **Note**: New ADC specific subfolders for the Virtual hard disks\ and Storage hard disks\ need to be created for each virtual ADC instance installation, as shown below:

- Public Documents
  - Hyper-V
    - Storage hard disks
      - ADC1
      - ADC2
    - Virtual Hard disks
      - ADC1
      - ADC2
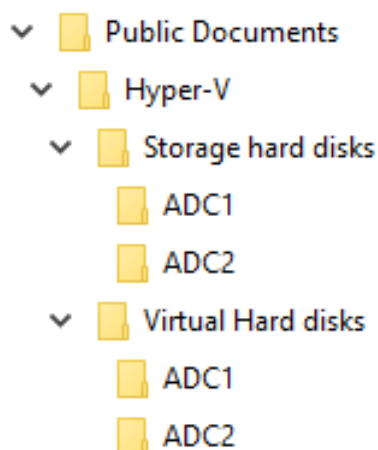
- Copy the extracted EdgeADC .vhd file to the 'Storage hard disk' folder created above.
- In your Hyper-V Manager client, right-click on the server and select "Import Virtual Machine"
- Browse to the folder containing the downloaded ADC VA image file extracted earlier
- Select Virtual Machine - highlight the virtual machine to import and click Next
- Select Virtual Machine - highlight the virtual machine to import and click Next
- Choose Import Type - select "**Copy the virtual machine (create a new unique ID)**" click next

- Choose Folders for Virtual Machine Files - the Destination can be left as the Hyper-V default or you can choose to select a different location
- Locate Virtual Hard Disks – browse to and select the virtual hard disks folder created above and click next
- Choose Folders to Store Virtual Hard Disks – browse to and select the Storage hard disks folder created previously and click next
- Verify the details in the Completing Import Wizard Summary window are correct and click Finish
- Right-click on the newly imported **ADC** virtual machine and select Start

NOTE: AS PER HTTP://SUPPORT.MICROSOFT.COM/KB/2956569 YOU SHOULD IGNORE THE "DEGRADED (INTEGRATION SERVICES UPGRADE REQUIRED)" STATUS MESSAGE, WHICH MAY BE DISPLAYED AS BELOW AFTER THE VA IS STARTED. NO ACTION IS REQUIRED, AND THE SERVICE IS NOT DEGRADED

- While the VM is initializing, you can right-click on the VM entry and select Connect…You will then be presented with the EdgeADC console.

- Once you configure the network properties, the VA will reboot and present the logon to the VA console.

Please refer to the section **FIRST BOOT CONFIGURATION** to proceed further.

Citrix XenServer

The ADC Virtual appliance is installable on Citrix XenServer.

- Extract the ADC OVA ALB-VA file to your local machine or server.
- Open Citrix XenCenter Client.
- In your XenCenter client, select **"File: Import."**
- Browse to, and select the **OVA** file, then click **"Open Next."**
- Select the VM creation location when asked.
- Choose which XenServer you wish to install and click **"NEXT."**
- Select the storage repository (SR) for virtual disk placement when asked.
- Select an SR with enough space and click **"NEXT."**
- Map your virtual network interfaces. Both interfaces will say Eth0; however, note that the bottom interface is Eth1.
- Select the target network for each interface and click **NEXT**
- **DO NOT** tick the "Use Operating System Fixup."
- Click **"NEXT"**
- Choose the network interface to use for the temporary transfer VM.
- Choose the Management interface, usually Network 0, and leave the network settings on DHCP. Please be aware that you must assign static IP address details if you do not have a working DHCP server for the transfer. Failure to do this will result in the import saying Connecting continuously then failed. Click **"NEXT"**
- Review all the information and check the correct settings then. Click **"FINISH."**
- Your VM will begin transferring virtual disk "ADC ADC" and, once complete, will show under your XenServer.
- Within your XenCenter client, you will now be able to see the new virtual machine.
  Right-click on the VA and click "**START**."
- Your VM will then boot, and the ADC boot screen will show.

- Once configured, the logon to the VA presents itself.

Please refer to the section **FIRST BOOT CONFIGURATION** to proceed further.

Nutanix AHV

The following section shows how to install the EdgeADC onto a Nutanix AHV platform.

Requirements and Versions

This guide is relevant for EdgeADC 4.2.6 and above.

All versions of the Nutanix hypervisor are compatible, but the certification has been performed on Nutanix version 5.10.9.

- The first step is to log into Nutanix Prism Central.

Uploading the EdgeADC Image

- Navigate to Virtual Infrastructure > Images
- Click the Add Image button
- Select the EdgeADC image file you have downloaded and click the Open button to upload the image.
- Enter a name for the image in the Image Description field.
- Select an appropriate category
- Select the image and click the right-arrow key
- Select All Images and click Save.

Creating the VM

- Navigate to Virtual Infrastructure > VMs
- Click the Create VM button
- Enter a name for the VM, the number of CPUs you wish to have, and the number of cores you want to allocate to the VM.
- Then scroll down in the dialog and enter the amount of memory you wish to allocate to the VM. You can start with 4GB and increase this depending on usage.

Adding the Disk

- Next, click the Add New Disk link
- Select the Clone from Image Service option within the Operation drop-down.
- Select the EdgeADC image you have added and click the Add button.
- Select the disk to be the bootable disk.

Adding the NIC, Network & Affinity

- Next, click the Add New NIC button. You will need to have two NICS.
- Select the Network and click the Add button
- Click the Set Affinity button
- Select the Nutanix hosts on which the VM is allowed to run, then click the Save button.

- Verify the settings you have made and click the Save button

Powering on the VM
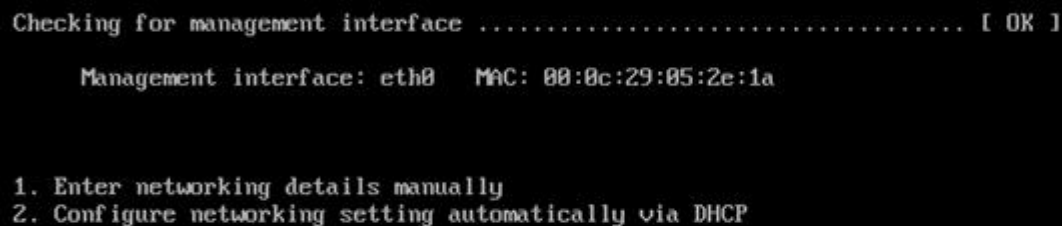
- From the list of VMs, click the VM name you just created
- Click the Power On button for the VM
- Once the VM has powered on, click the Launch Console button

Configuring the EdgeADC Networking

- Follow the instructions in the section First Boot Environment.
- The EdgeADC is now ready for use, and you will be able to access its GUI using your browser and the Management IP address.

First Boot Configuration

On first boot, the ADC VA displays the following screen requesting configuration for production operations.

```
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


_
```

First Boot – Manual Network Details

On first boot, you will have 10 seconds to interrupt the automatic assignment of IP details via DHCP

To interrupt this process, click into the console window and press any key. You can then enter the following details manually.

- IP Address
- Subnet Mask
- Gateway
- DNS Server

These changes are persistent and will survive a reboot and don't need to be configured again on the VA.

First Boot – DHCP successful

If you do not interrupt the network assignment process, your ADC will contact a DHCP server after a timeout to obtain its network details. If contact is successful, then your machine will be assigned the following information.

- IP Address
- Subnet Mask
- Default Gateway
- DNS Server

We advise that you do not operate the ADC VA using a DHCP address unless that IP address links permanently to the MAC address of the VA within the DHCP server. We always advise using a **FIXED IP ADDRESS** when using the VA. Follow the steps in **CHANGING THE MANAGEMENT IP ADDRESS** and subsequent sections until you have completed the network configuration.

First Boot – DHCP Fails

If you do not have a DHCP server or the connection fails, the IP Address 192.168.100.100 will be assigned. The IP address will increment by '1' until the VA finds a free IP address. Equally, the VA will check to see if the IP address is currently in use, and if so, will increment again and recheck.

Changing the Management IP Address

You can change the IP address of the VA at any time using the command **set greenside=n.n.n.n,** as shown below.

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

Changing the Subnet Mask for eth0

The network interfaces use the prefix 'eth'; the base network address is called eth0. The subnet mask or netmask can be changed using the command **set mask eth0 n.n.n.n**. You can see an example below.

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

Assigning a Default Gateway

The VA needs a default gateway for its operations. To set the default gateway, use the command **route add default gw n.n.n.n** as shown in the example below.

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

Checking the Default Gateway value

To check if the default gateway is added and is correct, use the command **route**. This command will display the network routes and default gateway value. See the example below.

```
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
```

You can now access the Graphical User Interface (GUI) to configure the ADC for production or evaluation usage.

Accessing the web interface

You can use any Internet browser with Javascript to configure, monitor, and deploy the ADC into operational use.

In the browser URL field, type either **HTTPS://{IP ADDRESS} or HTTPS://{FQDN}**

The ADC, by default, uses a self-signed SSL certificate. You can change the ADC to use the SSL certificate of your own choice.

Once your browser reaches the ADC, it will show you the login screen. The factory default credentials for the ADC are:

Default Username = **admin** / Default Password = **jetnexus**

Command Reference Table

Command	Parameter1	Parameter2	Description	Example
date			Shows the configured date and time currently configured	Tue Sept 3 13:00 UTC 2013
defaults			Assign the factory default settings for your appliance	
exit			Log out of the command line interface	
help			Displays all valid commands	
ifconfig	[blank]		View the interface configuration for all interfaces	ifconfig
	eth0		View the interface configuration of eth0 only	ifconfig eth0
machineid			This command will provide the machineid used to licence the ADC ADC	EF4-3A35-F79
quit			Log out of the command line interface	
reboot			Terminate all connections and reboot the ADC ADC	reboot
restart			Restart the ADC ADC virtual services	
route	[blank]		View the routing table	route
	add	default gw	Add the default gateway IP address	route add default gw 192.168.100.254
set	greenside		Set the management IP address for ADC	set greenside=192.168.101.1
	mask		Set the subnet mask for an interface. Interface names are eth0, eth1….	set mask eth0 255.255.255.0
show			Displays the global configuration settings	
shutdown			Terminate all connections and power-off the ADC ADC	
status			Displays the current data statistics	
top			View the process information such as CPU and Memory	
viewlog	messages		Displays the raw syslog messages	View log messages

Please note: Commands are not case sensitive. There is no command history.
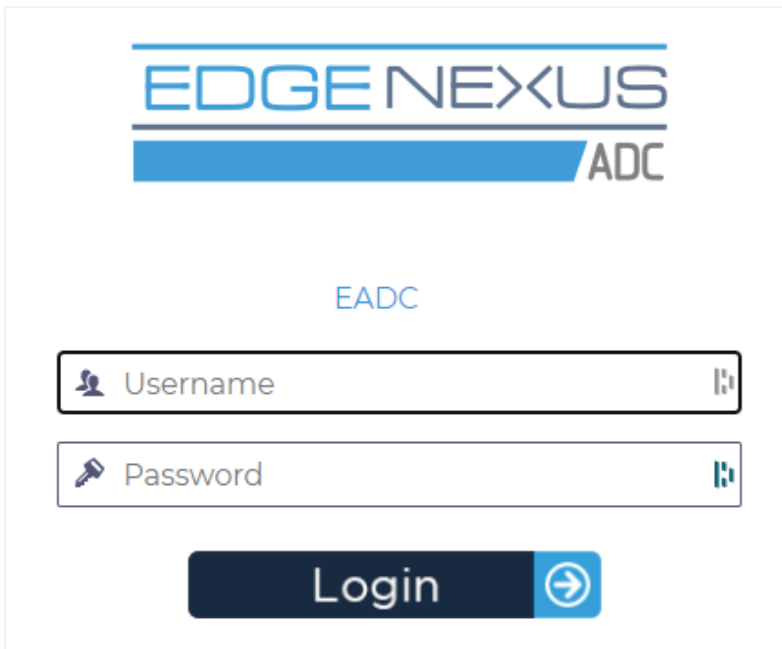
Launching the ADC Web Console

All operations on the ADC (also referred to as ADC) are configured and performed using the web console. The web console is accessed using any browser with Javascript.

To launch the ADC web console, enter the URL or IP address of the ADC into the URL field. We will use the example of adc.company.com as an example:

https://adc.company.com

When launched, the web console of the ADC is as shown below, allowing you to log in as the admin user.

Default Login Credentials

The default login credentials are:

- Username: admin
- Password: jetnexus

You can change this at any time using the user configuration capabilities located at *System > Users.*

Once you successfully log in, the main dashboard of the ADC displays.

The Main Dashboard

The image below illustrates how the main dashboard or 'home page' of the ADC looks. We may make some changes from time to time due to improvement reasons, but all functions will remain.

To be as concise as possible, we will assume that this first introduction to the screen sections will prove sufficiently aware of the different sections to the ADC configuration area, so we will not describe them in detail as we advance but rather focus on the configurational elements.

Going from left to right, we first have Navigation. The Navigation section consists of the different areas within ADC. When you click on a particular choice within Navigation, this will display the corresponding section on the right side of the screen. You can also see the chosen configuration section tabbed at the top of the screen, adjacent to the product logo. The tabs enable faster navigation to pre-used areas of the ADC configuration.

Services

The services section of the ADC has several areas within it. When you click on the Service item, this will expand to show the available choices.

IP Services

The IP Services section of the ADC allows you to add, delete and configure the various virtual IP services you need for your particular use case. The settings and options fall into the sections below. These sections are on the right side of the application screen.

Virtual Services

A Virtual Service combines a Virtual IP (VIP) and a TCP/UDP port on which the ADC listens. Traffic arriving at the Virtual Service IP is redirected to one of the Real Servers associated with that service. The Virtual Service IP address cannot be the same as the management address of the ADC. i.e. eth0, eth1 etc…

The ADC determines how the traffic is re-distributed to the Servers based on a load balancing policy set within the Basic tab in the Real Servers section.

Creating a new Virtual Service using a new VIP

- Click the Add Virtual Service button as indicated above.

- You will then enter the **edit row** mode.
- Complete the four highlighted fields to proceed, and then click the update button.

Please use the TAB key to navigate through the fields.

Field	Description
IP Address	Enter a new Virtual IP address to be the target entry point for accessing the Real Server. This IP is where users or applications will point to access the load-balanced application.
Subnet Mask/Prefix	This field is for the subnet mask relevant to the network on which the ADC sits
Port	The entry port used when accessing the VIP. This value does not necessarily need to be the same as the Real Server if you use Reverse Proxy.
Service Name	The service name is a textual representation of the VIP's purpose. It is optional, but we recommend you provide this for clarity.
Service Type	There are many different Service Types available for you to select. Layer 4 service types cannot use flightPATH technology.

You can now press the Update button to save this section and jump automatically to the Real Server section detailed below:

Field	Description
Activity	The Activity field can be used to show and change the status of the load-balanced real server. Online – Denotes that the server is active and receiving load-balanced requests Offline – The server is offline and is not receiving requests Drain – The server has been placed in drain mode so that persistence can flush and the server moved to an offline state without affecting users. Standby – The server has been placed in a standby state
IP Address	This value is the IP address of the Real Server. It must be accurate and should not be a DHCP address.
Port	The target Port of access on the Real Server. When using a reverse proxy, this can be different from the entry Port specified on the VIP.
Weighting	This setting usually is automatically configured by the ADC. You can change this if you wish to change the priority weighting.

- Click the Update button or press Enter to save your changes
- The Status light will first turn Grey, followed by Green should the Server Health Check succeed. It will turn Red if the Real Server Monitor fails.
- A server that has a red status light will not be load balanced.

Example of a completed Virtual service

Create a new Virtual Service using an existing VIP

- Highlight a Virtual Service you wish to copy
- Click Add Virtual Service to enter row edit mode

- The IP Address and Subnet Mask copies across automatically
- Enter the Port Number for your service
- Enter an optional Service Name
- Select a Service Type
- You can now press the Update button to save this section and jump automatically to the Real Server section below

- Leave the server Activity option as Online – this means it will be load balanced if it passes the default health monitor of TCP Connect. This setting can be changed later if required.
- Enter an IP address of the Real Server
- Enter a Port Number for the Real Server
- Enter an optional name for the Real Server
- Click Update to save your changes
- The Status light will first turn Grey, then Green if the Server Health Check succeeds. It will turn Red if the Real Server Monitor fails.
- A server that has a Red Status light will not be load balanced

Changing the IP Address of a Virtual Service

You can change the IP address of an existing Virtual Service or VIP at any time.

- Highlight the Virtual Service whose IP address you wish to change

- Double click the IP address field for that service

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

Update   Cancel

- Change the IP address to the one you wish to use
- Click the Update button to save the changes.

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

Note: Changing the IP address of a Virtual Service will change the IP address of all services associated with the VIP

Creating a new Virtual Service using Copy Service

- The Copy Service button will copy an entire service, including all the Real Servers, basic settings, advanced settings, and flightPATH rules associated with it
- Highlight the service you wish to duplicate and click Copy Service
- The row editor will appear with the blinking cursor on the IP Address column
- You must change the IP address to be unique, or if you wish to keep the IP address, you must edit the Port so it is unique to that IP address

Don't forget to edit each tab if you change a setting such as a load balancing policy, the Real Server monitor, or remove a flightPATH rule.

Filtering displayed data

Searching for a specific term

The Search box allows you to search the table using any value, such as the octets of the IP address or name of the service.

🔲 IP-Services	⊕ Dashboard ✕					

🔲 Virtual Services

⊕ Copy Service   🔍 10.4.8.191

Mode	VIP	VS	Enabled	IP Address	SubNet Mask / Prefix	Port
Stand-alone	🟢	🟢	☑	10.4.8.191	255.255.255.0	80
		🟢	☑	10.4.8.191	255.255.255.0	81
		🟠	☑	10.4.8.191	255.255.255.0	82
		🟢	☑	10.4.8.191	255.255.255.0	443

The example above shows the result of searching for a specific IP address of 10.4.8.191.

Selecting column visibility

You can also select the columns that you wish to display in the dashboard.

- Move the mouse over any one of the columns
- You will see a small arrow appear on the right side of the column
- Clicking the checkboxes selects the columns you wish to see in the dashboard.

Understanding the Virtual Services columns

Primary/Mode

The Primary/Mode column indicates the high availability role selected for the current VIP. Use the options available in System > Clustering to configure this option.

Option	Description
Cluster	Cluster is the default role for the ADC at installation, and the Primary/Mode column will indicate the mode it is currently running in. When you have an HA pair of ADC appliances in your datacentre, one of them will show Active and the other Passive
Manual	The Manual role allows the ADC pair to run in Active-Active mode for different Virtual IP addresses. In such cases, the Primary column will contain a box next to each unique Virtual IP that is tickable for Active or left un-ticked for Passive.
Stand-Alone	The ADC is acting as a stand-alone device and is not in High Availability mode. As such, the Primary column will state Stand-alone.

VIP

This column provides visual feedback on the status of each Virtual Service. The indicators are color-coded and are as follows:

LED	Meaning
●	Online
●	Failover-Standby. This virtual service is hot-standby
●	Indicates a "secondary" is holding off for a "primary."
●	Service Needs attention. This indication may result from a Real Server failing a health monitor check or has been changed manually to Offline. Traffic will continue to flow but with reduced Real Server capacity
●	Offline. Content servers are unreachable, or no content servers enabled
●	Finding status

●	Not licensed or licensed Virtual IPs exceeded

Enabled

The default for this option is Enabled, and the checkbox shows as ticked. You can disable the Virtual Service by double-clicking the line, unticking the checkbox, and then clicking the Update button.

IP Address

Add your IPv4 address in decimal dotted notation or an IPv6 address. This value is the Virtual IP address (VIP) for your service. Example IPv4 "192.168.1.100". Example Ipv6 "2001:0db8:85a3:0000:0000:8a2e:0370:7334"

Subnet Mask/Prefix

Add your subnet mask in decimal dotted notation. Example "255.255.255.0". Or for IPv6, add in your Prefix. For more information about IPv6, please see **HTTPS://EN.WIKIPEDIA.ORG/WIKI/IPV6_ADDRESS**

Port

Add the port number associated with your service. The port can be a TCP or UDP port number. Example TCP "80" for Web Traffic and TCP "443" for Secured Web Traffic.

Service Name

Add in a friendly name to identify your service. Example "Production Web Servers."

Service Type

Please note that with all "Layer 4" service types, the ADC will not interact or modify the data stream, so flightPATH is unavailable with Layer 4 service types. Layer 4 services simply load balance the traffic according to the load balancing policy:

Service Type	Port/Protocol	Service Layer	Comment
Layer 4 TCP	Any TCP port	Layer 4	The ADC will not alter any information in the data stream and will perform standard load balancing the traffic according to the load balancing policy
Layer 4 UDP	Any UDP port	Layer 4	As with Layer 4 TCP, the ADC will not alter any information in the data stream and will perform standard load balancing the traffic according to the load balancing policy
Layer 4 TCP/UDP	Any TCP or UDP port	Layer 4	It is ideal if your service has a primary protocol such as UDP but will fall back to TCP. The ADC will not alter any information in the data stream and will perform standard load balancing the traffic according to the load balancing policy
DNS	TCP/UDP	Layer 4	Used to load balance DNS servers.
HTTP	HTTP or HTTPS protocol	Layer 7	The ADC can interact, manipulate and modify the data stream using flightPATH.
FTP	File Transfer Protocol Protocol	Layer 7	Using separate control and data connections between client and server
SMTP	Simple Mail Transfer Protocol	Layer 4	Use when load balancing mail servers

POP3	Post Office Protocol	Layer 4	Use when load balancing mail servers
IMAP	Internet Message Access Protocol	Layer 4	Use when load balancing mail servers
RDP	Remote Desktop Protocol	Layer 4	Use when load balancing Terminal Services servers
RPC	Remote Procedure Call	Layer 4	Use when load balancing systems using RPC calls
RPC/ADS	Exchange 2010 Static RPC for Address Book Service	Layer 4	Use when load balancing Exchange servers
RPC/CA/PF	Exchange 2010 Static RPC for Client Access & Public Folders	Layer 4	Use when load balancing Exchange servers
DICOM	Digital Imaging and Communications in Medicine	Layer 4	Use when load balancing servers using DICOM protocols

Real Servers

There are several tabs in the Real Servers section of the dashboard: Server, Basic, Advanced, and flightPATH.
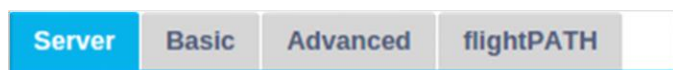
Server

The Server tab holds the definitions of the real back-end servers paired to the Virtual Service currently selected. You are required to add at least one server to the Real Servers section.

Add Server

- Select the appropriate VIP that you have previously defined.
- Click Add Server
- A new row will appear with the cursor blinking on the IP Address column

- Enter the IPv4 address of your server in dotted decimal notation. The Real Server can be on the same network as your Virtual Service, any directly attached local network, or any network that your ADC can route. Example "10.1.1.1".
- Tab to the Port column and enter the TCP/UDP port number for your server. The port number can be the same as the Virtual Service port number or another port number for Reverse Proxy Connectivity. The ADC will automatically translate to this number.
- Tab to the Notes section to add in any relevant detail for the server. Example: "IIS Web Server 1"

Group Name

When you have added in the servers comprising the load-balanced set, you can also attach a Group Name. Once you have edited this field, the contents save without the need to press the Update button.

Real Server Status Lights

You can see the status of a Real Server by the light color in the Status column. See below:

LED	Meaning
●	Connected
◯	Not Monitored
●	Draining
●	Offline
●	Standby
●	Not Connected
●	Finding Status
●	Not licensed or licensed Real Servers exceeded

Activity

You can change the Activity of a Real Server at any time by using the dropdown menu. To do this, double-click on a Real Server row to place it into edit mode.

Option	Description

Online	All Real Servers assigned Online will receive traffic according to the load balancing policy set within the Basic tab.
Drain	All Real Servers assigned as Drain will continue to serve existing connections but will not accept any new connections. The Status light will flash green/blue while the drain is in process. Once the existing connections have closed naturally, the Real Servers will go offline, and the Status light will be solid blue. You can also view these connections by navigating to the Navigation > Monitor > Status section.
Offline	All Real Servers set as Offline will immediately be taken offline and will not receive any traffic.
Standby	All Real Servers set as Standby will remain offline until **ALL** the Online group servers fail their Server Health Monitor checks. Traffic is received by the Standby group as per the load balancing policy when this happens. If one server in the Online group passes the Server Health Monitor check, this Online server will receive all the traffic, and the Standby group will stop receiving traffic.

IP Address

This field is the IP address for your Real Server. Example "192.168.1.200".

Port

TCP or UDP port number that the Real Server is listening on for the service. Example "80" for Web Traffic.

Weight

This column will become editable when there is an appropriate Load Balancing Policy specified.

 The default weight for a Real Server is 100, and you can enter values from 1-100. A value of 100 means maximum load, and 1 means minimum load.

An example for three servers may look something like this:

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

If we consider the load balancing policy is set to Least Connections, and there are 200 total client connections;

- Server 1 will get 100 concurrent connections
- Server 2 will get 50 concurrent connections
- Server 3 will get 50 concurrent connections

If we were to use Round Robin as the load balancing method, which rotates requests through the load balanced server set, altering the weights affects how often the servers get chosen as the target.

If we believe the Fastest load balancing policy uses the shortest time taken to GET a response, adjusting the weights alters the bias similarly to Least Connections.

Calculated Weight

The Calculated Weight of each server can be viewed dynamically and is calculated automatically and is not editable. The field shows the actual weighting that ADC is using when considering manual weighting and load balancing policy.

Notes

Enter any particular notes helpful in describing the defined entry to the Notes field. Example "IIS Server1 – London DC".

ID

The ID field is used within the Cookie ID Load balancing Policy. The ID number placed here is used to identify

Basic

Load Balancing Policy

The dropdown list shows you the currently supported load balancing policies available for use. A list of load-balancing policies, together with an explanation, is below.

Option	Description
Fastest	The Fastest load balancing policy automatically calculates the response time for all requests per server smoothed over time. The Calculated Weight column

	contains the automatically calculated value. Manual entry is only possible when using this load balancing policy.
Round Robin	Round Robin is commonly used in firewalls and basic load balancers and is the simplest method. Each Real Server receives a new request in sequence. This method is only proper when you need to load balance requests to servers evenly; an example would be look-up web servers. However, when you need to load balance based on application load or the server load, or even ensure that you use the same server for the session, the Round Robin method is inappropriate.
Least Connections	The load balancer will keep track of the number of current connections to each Real Server. The Real Server with the least amount of connections receives the subsequent new request.
IP Bound Layer 3 Session Affinity/Persistence	In this mode, the client's IP address forms the basis to select which Real Server will receive the request. This action provides persistence. HTTP and Layer 4 protocols can use this mode. This method is helpful for internal networks where the network topology is known, and you can be confident that there are no "super proxies" upstream. With Layer 4 and proxies, all the requests can look as if they are coming from one client, and as such, the load would not be even. With HTTP, the header (X-Forwarder—For) information is used when present to cope with proxies.
IP List Based Layer 3 Session Affinity/Persistence	The connection to the Real Server initiates using "Least connections" then, session affinity is achieved based on the client's IP address. A list is maintained for 2 hours by default, but this can be changed using a jetPACK.
Session Cookie Layer 7 Session Affinity/Persistence	This mode is the most popular persistence method for HTTP load balancing. In this mode, the ADC uses IP list-based load balancing for each first request. It inserts a cookie into the headers of the first HTTP response. After that, the ADC uses the client cookie to route traffic to the same back-end server. This cookie is used for persistence when the client needs to go to the same back-end server each time. The cookie expires once the session is closed.
Persistent Cookie Layer 7 Session Affinity/Persistence	The IP list-based load balancing mode is used for each first request. The ADC inserts a cookie into the headers of the first HTTP response. After that, the ADC uses the client cookie to route traffic to the same back-end server. This cookie is used for persistence when the client must go to the same back-end server each time. The cookie will expire after 2 hours, and the connection will be load balanced according to an IP List Based algorithm. This expiry time is configurable using a jetPACK.
Session Cookie - Classic ASP Session Cookie	Active Server Pages (ASP) is a Microsoft server-side technology. With this option selected, the ADC will maintain session persistence to the same server if an ASP cookie is detected and found in its known cookies list. On detection of a new ASP cookie, it will be load balanced using the Least Connections algorithm.
Session Cookie - ASP.NET Session Cookie	This mode applies to **ASP.net.** With this mode selected, the ADC will maintain session persistence to the same server if an ASP.NET cookie is detected and found in its list of known cookies. On detection of a new ASP cookie, it will be load balanced using the Least Connections algorithm.
Session Cookie - JSP Session Cookie	Java Server Pages (JSP) is an Oracle server-side technology. With this mode selected, the ADC will maintain session persistence to the same server if a JSP cookie is detected and found in its known cookies list. On detection of a new JSP cookie, it will be load balanced using the Least Connections algorithm.
Session Cookie - JAX-WS Session Cookie	Java web services (JAX-WS) is an Oracle server-side technology. With this mode selected, the ADC will maintain session persistence to the same server if a JAX-WS cookie is detected and found in its list of known cookies. On detection of a new JAX-WS cookie, it will load balanced using the Least Connections algorithm.
Session Cookie - PHP Session Cookie	Personal Home Page (PHP) is an open-source server-side technology. With this mode selected, the ADC will maintain session persistence to the same server when a PHP cookie is detected.

Session Cookie - RDP Cookie Persistence	This load balancing method uses the Microsoft-created RDP Cookie based on username/domain to provide persistence to a server. The advantage of this method means maintaining a connection to a server is possible even if the IP address of the client changes.
Cookie-ID Based	A new method very much like "PhpCookieBased" and other load-balancing methods, but using CookieIDBased and cookie RegEx h=[^;]+ This method will use the value set in the Real Server's notes field "ID=X;" as the cookie value to identify the server. This, therefore, means it is a similar methodology as CookieListBased but uses a different cookie name and stores a unique cookie value, not the scrambled IP, but the ID from the Real Server (read in at load-time.) The Default value is CookieIDName="h"; however, if there is an override value in the virtual server's advanced settings configuration, use this instead. **NOTE**: We overwrite the cookie expression above to replace h= with the new value if this value is set. The last bit is that if an unknown cookie value arrives and matches one of the Real Server IDs, it should select that server; otherwise, use the next method (delegate.)
Shared IP List Based	This service type is only available when the Connectivity Mode is set to Gateway or Direct Server Return. It has been primarily added for support with VMware load balancing.

Server Monitoring

Your ADC contains six standard Real Server Monitoring methods listed below.
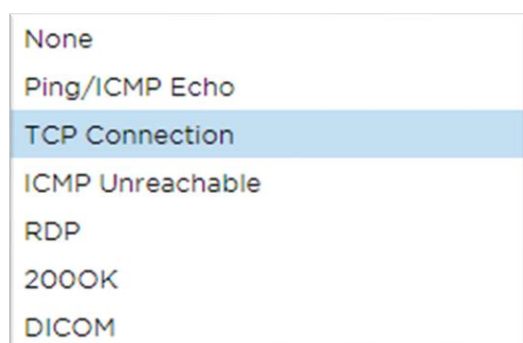
Choose the monitoring method you wish to apply to the Virtual Service (VIP).

It is essential to choose the right monitor for the service. For example, if the Real Server is an RDP server, a 200OK monitor is not relevant. If you are unsure which monitor to choose, the default TCP Connection is an excellent place to start.

You can choose multiple monitors by clicking each monitor you wish to apply to the service in turn. The selected monitors execute in the order you select them; hence start with monitors of the lower layers first. For example, setting monitors Ping/ICMP Echo, TCP Connection, and 200OK will display in the Dashboard Events like the image below:

We can see that Layer 3 Ping and Layer 4 TCP Connect has succeeded if we look at the top line, but Layer 7 200OK has failed. These monitoring results provide enough information to indicate that routing

is OK and there is a service running on the relevant port, but the website is not responding correctly to the page requested. It's now time to look at the webserver and the Library > Real Server Monitor section to see the details of the failing monitor.

Option	Description
None	In this mode, the Real Server is not monitored and is always up and running correctly. The None setting is helpful for situations where monitoring upsets a server and for services that should not join in the fail-over action of the ADC. It is a route to host unreliable or legacy systems that are not primary to H/A operations. Use this monitoring method with any service type.
Ping/ICMP Echo	In this mode, the ADC sends an ICMP echo request to the IP of the content server. If a valid echo response is received, the ADC deems the Real Server up and running, and traffic throughput to the server continues. It will also keep the service available on a H/A pair. This monitoring method is usable with any service type.
TCP Connection	A TCP connection is made to the Real Server and immediately broken without sending any data in this mode. If the connection succeeds, the ADC deems the Real Server to be up and running. This monitoring method is usable with any service type, and UDP services are currently not appropriate for TCP Connection monitoring.
ICMP Unreachable	The ADC will send a UDP health check to the server and mark the Real Server as unavailable if it receives an ICMP port unreachable message. This method can be helpful when you need to check if a UDP service port is available on a server, such as DNS port 53.
RDP	In this mode, a TCP connection initializes as explained in the ICMP Unreachable method. After the connection initializes, a Layer 7 RDP connection is requested. If the link is confirmed, the ADC deems the Real Server to be up and running. This monitoring method is usable with any Microsoft terminal server.
200 OK	In this method, a TCP connection initializes to the Real Server. After the connection succeeds, the ADC sends the Real Server an HTTP request. An HTTP response is waited for and checked for the "200 OK" response code. The ADC deems the Real Server up and running if the "200 OK" response code is received. If the ADC does not receive a "200 OK" response code for any reason, including timeouts, failure to connect, and other reasons, the ADC marks the Real Server unavailable. This monitoring method is only valid for use with HTTP and accelerated HTTP service types. If a Layer 4 Service type is used for an HTTP server, it is useable if SSL is not in use on the Real Server or handled appropriately by the "Content SSL" facility.
DICOM	A TCP connection initializes to the Real Server in DICOM mode, and an Echoscu "Associate Request" is made to the Real Server on connection. A conversation that includes an "Associate Accept" from the content server, a transfer of a small amount of data followed by a "Release Request," then "Release Response" successfully concludes the monitor. If the monitor does not complete successfully, then the Real Server is regarded as down for any reason.
User Defined	Any monitor configured in the Real Server Monitoring section will appear in the list.

Caching Strategy

By default, the Caching Strategy is disabled and set as Off. If your service type is HTTP, then you can apply two types of Caching Strategy.

Off

By Host

By Virtual Service

Please refer to the Configure Cache page to configure detailed cache settings. Note that when caching is applied to a VIP with the Accelerated "HTTP" service type, compressed objects are not cached.

Option	Description
By Host	Caching per host is based on application per hostname. A separate Cache will exist for each domain/hostname. This mode is ideal for web servers that can serve multiple websites depending on the domain.
By Virtual Service	Caching per virtual service is available when you choose this option. Only one Cache will exist for all domain/hostnames that pass through the virtual service. This option is a specialist setting for use with multiple clones of a single site.

Acceleration

Option	Description
Off	Turn compression off for the Virtual Service
Compression	When selected, this option turns on the compression for the selected Virtual Service. The ADC dynamically compresses the data stream to the client upon request. This process only applies to objects that contain the content-encoding: gzip header. Example content includes HTML, CSS, or Javascript. You can also exclude certain content types using the Global Exclusions section.

Note: If the object is cacheable, the ADC will store a compressed version and serve this statically (from memory) until the content expires and is re-validated.

Virtual Service SSL Certificate (Encryption between Client and the ADC)

By default, the setting is No SSL. If your service type is "HTTP" or "Layer4 TCP", you can select a certificate from the dropdown to apply to the Virtual Service. Certificates that have been created or imported will appear in this list. You may highlight multiple certificates to apply to a service. This operation will automatically enable the SNI extension to allow a certificate based on the "Domain Name" requested by the client.

Server Name Indication
This option is an extension to the TLS networking protocol using which the client indicates what hostname it is attempting to connect to at the start of the handshaking process. This setting allows the ADC to present multiple certificates on the same virtual IP address and TCP port.

Option	Description
No SSL	Traffic from the source to the ADC is not encrypted.
All	Loads all available certificates for use
Default	This option results in applying a locally created certificate called "Default" to the browser side of the channel. Use this option to test SSL when one hasn't been created or imported.
AnyUseCert	Use any certificate present on the ADC that the user has uploaded or generated

Real Server SSL Certificate (Encryption between the ADC and Real Server)

The default setting for this option is No SSL. If your server requires an encrypted connection, this value must be anything other than No SSL. Certificates that have been created or imported will appear in this list.

Option	Description
No SSL	Traffic from the ADC to the Real Server is not encrypted. The selection of a certificate on the browser side means "No SSL" can be chosen client-side to provide what is known as "SSL Offload."
Any	The ADC acts as a client and will accept any certificate the Real Server presents. Traffic from the ADC to the Real Server is encrypted when this option is selected. Use the "Any" option when a certificate is specified on the Virtual Service side, providing what is known as "SSL Bridging" or "SSL Re-Encryption."
SNI	The ADC acts as a client and will accept any certificate the Real Server presents. Traffic from the ADC to the Real Server is encrypted if this is selected. Use the "Any" option when a certificate is specified on the Virtual Service side, providing what is known as "SSL Bridging" or "SSL Re-Encryption." Choose this option to enable SNI on the server-side.
AnyUseCert	Any certificates that you have generated or imported into the ADC appear here.

Advanced

Connectivity

Your Virtual Service is configurable with different types of connectivity. Please select the connectivity mode to apply to the service.

Option	Description
Reverse Proxy	Reverse Proxy is the default value and works at Layer7 with compression and caching. And at Layer4 without caching or compression. In this mode, your ADC acts as a reverse proxy and becomes the source address seen by the Real Servers.
Direct Server Return	Direct Server Return or DSR as it's widely known (DR – Direct Routing in some circles) allows the server behind the load balancer to respond directly to the client bypassing the ADC on the response. DSR is only suitable for use with Layer 4 load balancing. Therefore, Caching and Compression are not available with this option chosen. **This mode can only be used with TCP, UDP, and TCP/UDP service types.**

	Layer 7 load balancing does not work with this DSR. Also, there is no persistence support other than IP List Based. SSL/TLS load balancing with this method is not ideal as Source IP persistence support is the only type available. DSR also requires Real Server changes to be done. Please refer to the Real Server Changes section.
Gateway	Gateway mode allows you to route all traffic through the ADC, allowing the Real Servers to be routed via the ADC to other networks via the ADC virtual machines or hardware interfaces. Using the device as a gateway device for Real Servers is ideal when running in multi-interface mode. Layer 7 load balancing with this method does not work as there is no persistence support other than IP List Based. This method requires that the Real Server sets its default gateway to the ADC's local interface address (eth0, eth1, etc.). Please refer to the Real Server Changes section. ***Please note that Gateway mode does not support failover in a cluster environment.***

Cipher Options

You can set ciphers on a per-service level, and it is only relevant for services with SSL/TLS enabled. The ADC performs automatic choice of the cipher, and you can add different ciphers using jetPACKS. On adding the appropriate jetPACK, you can set the Cipher options per service. The benefit of this is that you can create several services with varying levels of security. Be aware that older clients are not compatible with newer ciphers, and to reduce the number of clients, the more secure the service.

Client SSL Renegotiation

Tick this box if you wish to allow client-initiated SSL renegotiation. Disable client SSL renegotiation to prevent any possible DDOS attacks against the SSL Layer by un-ticking this option.

Client SSL Resumption

Tick this box if you wish to enable SSL Resumption Server sessions added to the session cache. When a client proposes re-use of a session, the server will try to reuse the session if found. If Resumption is un-checked, no session caching for the client or server takes place.

SNI Default Certificate

During an SSL connection with the Client-side SNI enabled, if the requested domain does not match any of the certificates assigned to the service, the ADC will present the SNI Default Certificate. The default setting for this is None which would effectively drop the connection should there be no exact match. Choose any of the certificates installed from the dropdown to present should an exact SSL certificate match fail.

Security Log

'On' is the default value and is on a per-service basis, enabling the service of logging authentication information to the W3C logs. Clicking the Cog icon will take you to the System > Logging page, where you can check the settings of the W3C logging.

Connection Timeout

The default connection timeout is 600 seconds or 10 minutes. This setting will adjust the time for the connection to timeout out upon no activity. Reduce this for short-lived stateless web traffic, which is typically 90s or less. Increase this figure for stateful connections such as RDP to something like 7200 seconds (2 hours) or more, depending on your infrastructure. The RDP timeout example means that if a user has a period of inactivity of 2 hours or less, the connections will remain open.

Monitoring Settings

These settings relate to the Real Server Monitors in the Basic tab. There are global entries in the configuration to count the number of successful or failed monitors before a server's status is marked online or failed.

Interval

The interval is the time in seconds between monitors. The default interval is 1second. While 1s is acceptable for most applications, it may be beneficial to increase this for others or during testing.

Monitoring Timeout

The timeout value is when the ADC will wait for a server to respond to a connection request. The default value is 2s. Increase this value for busy servers.

Monitoring In Count

The default value for this setting is 2. The value of 2 indicates that the Real Server must pass two successful health monitor checks before it comes online. Increasing this figure will increase the probability that the server can serve traffic but will take longer to come into service depending on the interval. Decreasing this value will bring your server into service sooner.

Monitoring Out Count

The default value for this setting is 3, meaning that the Real Server monitor must fail three times before the ADC will stop sending traffic to the server, and it is marked RED and Unreachable. Increasing this figure will result in better and more reliable service at the expense of the time it takes the ADC to stop sending traffic to this server.

Switch To Offline On Failure

When this is checked, the Real Servers that fail their health check are placed offline and can only be set online manually.

Max. Connections

Limits the number of simultaneous Real Server connections and is set per service. For example, if you configure this to 1000 and have two Real Servers, the ADC limits **each** Real Server to 1000 concurrent connections. You may also choose to present a "Server too busy" page once this limit is reached on all servers, helping users understand why any non-response or delay has occurred. Leave this blank for unlimited connections. What you set here depends on your system resources.

flightPATH
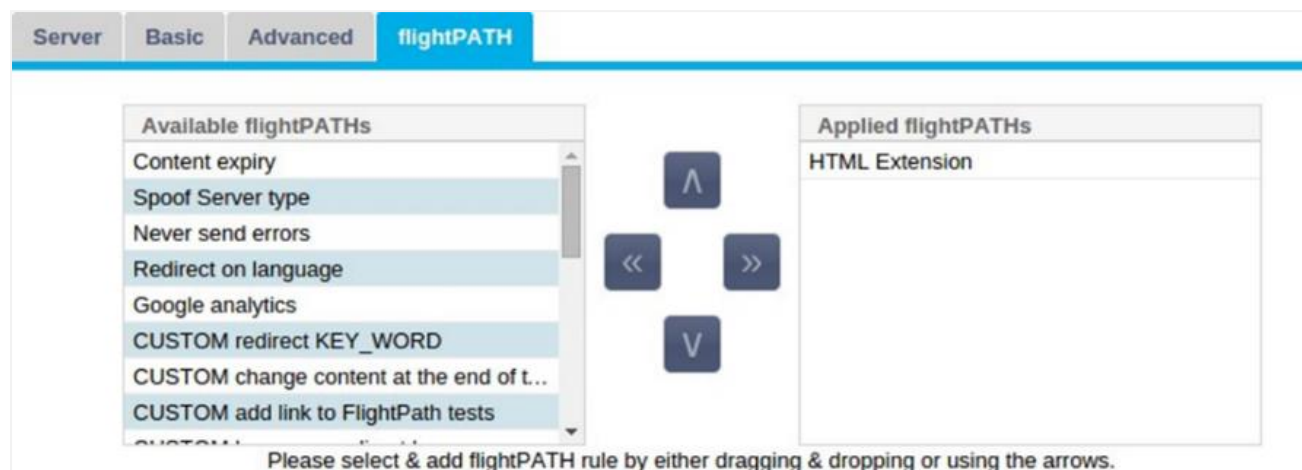
flightPATH is a system designed by Edgenexus and exclusively available within the ADC. Unlike other vendors' rules-based engines, flightPATH does not operate through a command line or script entry console. Instead, it uses a GUI to select the different parameters, conditions, and actions to perform to achieve what they need. These features make flightPATH extremely powerful and allow network administrators to manipulate HTTPS traffic in highly effective ways.

flightPATH is only available for use with HTTPS connections, and this section is not visible when the Virtual Service Type is not HTTP.

You can see from the image above; there is a list of available rules on the left and the rules applied to the virtual service on the right.

Add an available rule by dragging and dropping the rule from the left side to the right or highlighting a rule and clicking the right arrow to move it to the right side.

The order for execution is essential and starts with the top rule executed first. To change the order of execution, highlight the rule and move up and down using the arrows.

To remove a rule, drag and drop it back to the rule inventory on the left or highlight the rule and click the left arrow.

You can add, remove and edit flightPATH rules in the Configure flightPATH section of this guide.

Real Server Changes for Direct Server Return

Direct Server Return or DSR as it's widely known (DR – Direct Routing in some circles) allows the server behind the ADC to respond directly to the client, bypassing the ADC on the response. DSR is only suitable for use with Layer 4 load balancing. Caching and Compression are not available when enabled.

Layer 7 load balancing with this method will not work as there is no persistence support other than source IP. SSL/TLS load balancing with this method is not ideal as there is only source IP persistence support.

How it Works

- Client sends a request to the jetNEXUS ALB-X
- Request received by edgeNEXUS
- Request routed to content servers
- Response sent directly to client without passing through edgeNEXUS
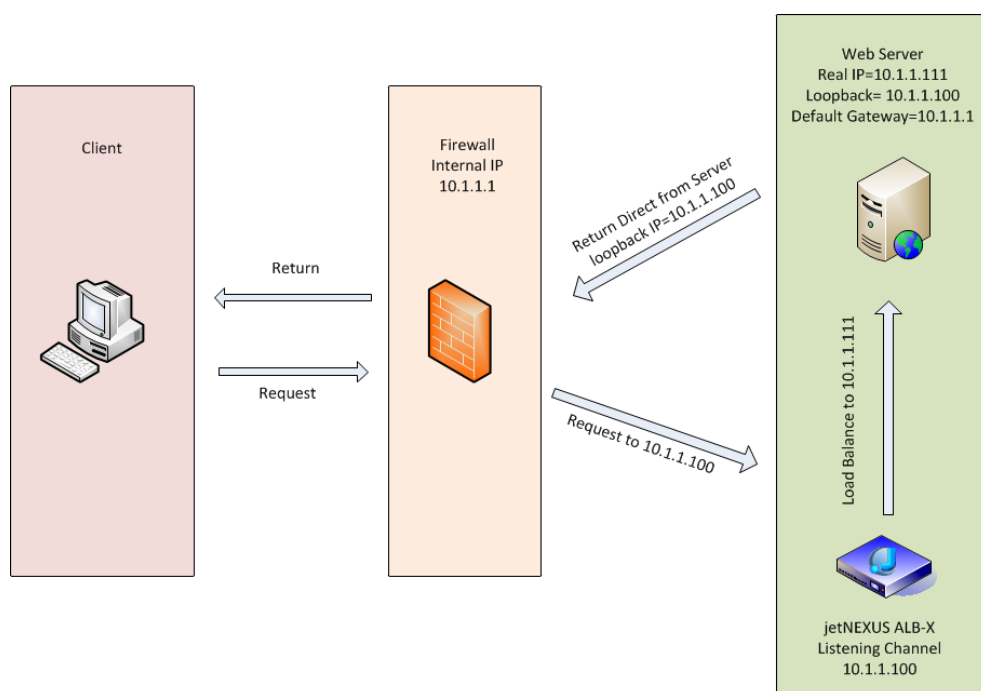
Required Content Server Configuration

General

- The content server default gateway should be configured as normal. (Not via the ADC)

- The content server and the load balancer must be in the same subnet

Windows

- The content server needs to have a loopback or Alias configure
  with the IP address of the Channel or VIP
  - Network metric must be 254 to prevent response to ARP requests
  - Add a loopback adapter in Windows Server 2012 – <u>Click here</u>
  - Add a loopback adapter in Windows Server 2003/2008 – <u>Click here</u>
- Run the following in a command prompt for each network interface you have configured on the Windows Real Servers

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

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

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

Linux

- Add a permanent loopback interface
- Edit "/etc/sysconfig/network-scripts"

ifcfg-lo:1
DEVICE=lo:1
IPADDR=x.x.x.x
NETMASK=255.255.255.255
BROADCAST=x.x.x.x
ONBOOT=yes

- Edit "/etc/sysctl.conf"

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

- Run "sysctl – p"

Real Server Changes – Gateway Mode

Gateway mode allows you to route all traffic through the ADC, and this allows traffic originating from the content servers to be routed via the ADC to other networks via the interfaces on the ADC unit. Using the device as a gateway device for content servers should be used when running in multi-interface mode.

How it works

- The client sends a request to the jetNEXUS ALB-X
- A request is received by edgeNEXUS
- Request sent to content servers
- Response sent to edgeNEXUS
- ADC routes the response to the client

Required Content Server Configuration

- Single Arm Mode – one interface is utilized, but the service VIP and the Real Servers must be on different subnets.

- Dual Arm Mode – two interfaces are utilized, but the service VIP and real servers must be on different subnets.
- In each case, Single and Dual Arm, the Real Servers need to configure their default gateway to the ADC interface address on the relevant subnet.

Single Arm example
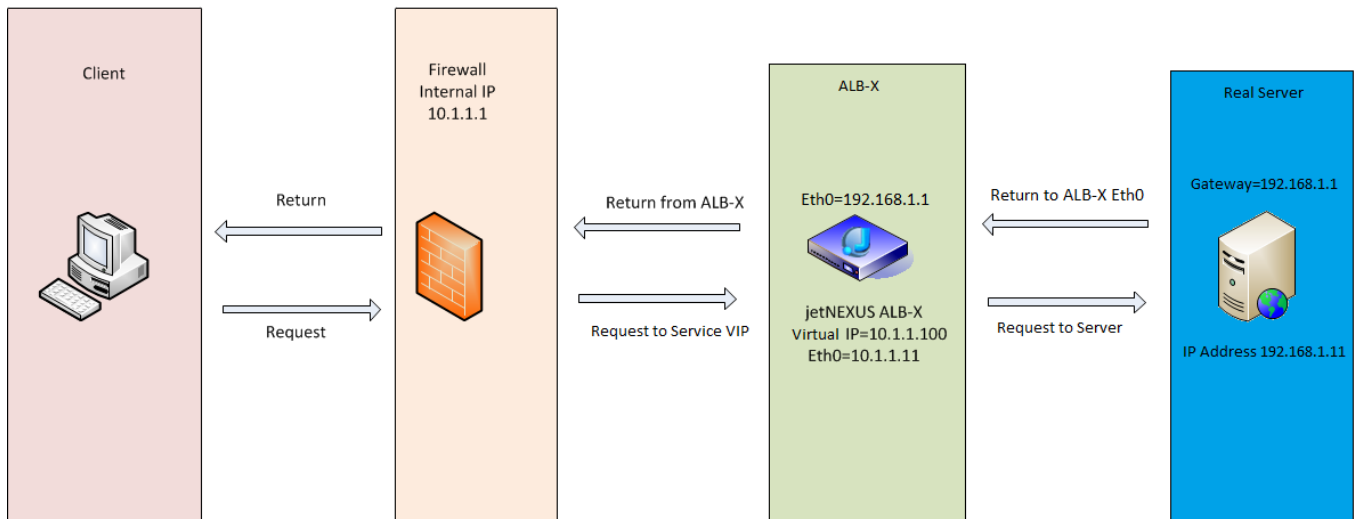
Dual Arm example
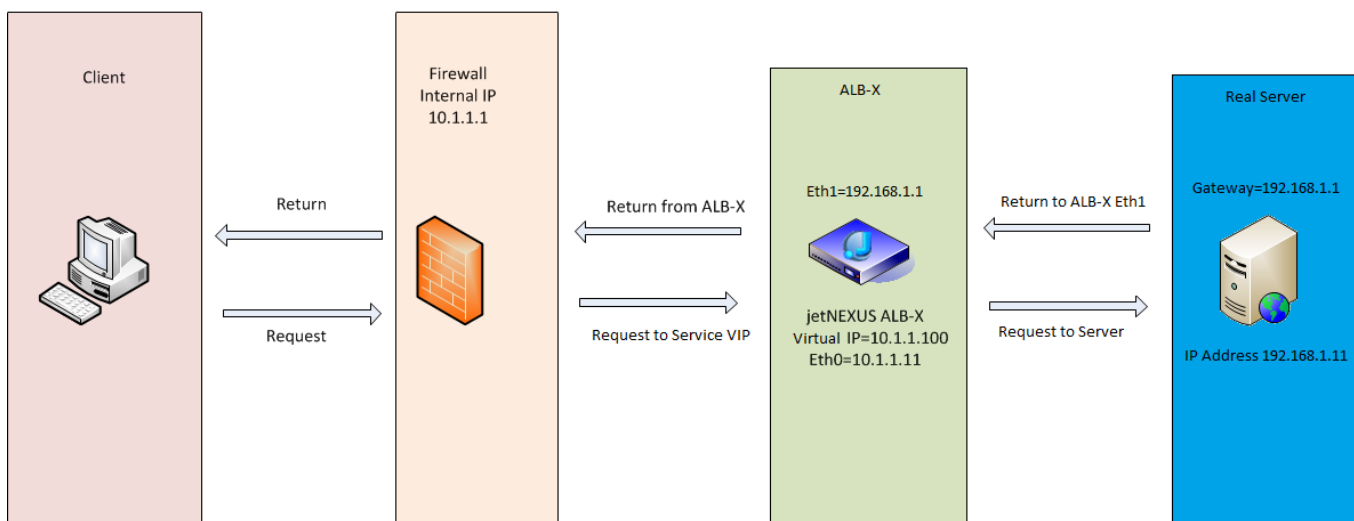
Library

Add-Ons

Add-ons are Docker-based containers that can run in an isolated mode within the ADC. Examples of add-ons could be an application firewall or even a micro instance of the ADC itself.

Apps

The Apps section within Add-Ons details the Apps that you have purchased, downloaded, and deployed.

If there are no Apps present, this section will display a message prompting you to proceed to the Apps section and download and deploy an App.

Once you deploy an App, it will appear in the Apps area.
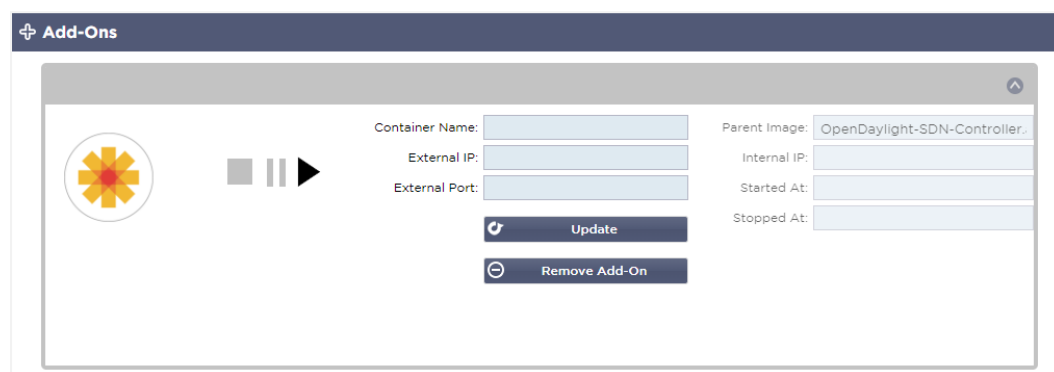
Purchasing an Add-on

To purchase an App, you need to register at the App Store. The purchase is made using the ADC itself. You will find

Navigate to the Library > Apps page of the ADC dashboard.

Here you can select the App you wish to download and then install.

If you are doing this from the ADC dashboard, please only select 1 item. You may own multiple ADC sets, and applications need associating to the ADC on which they deploy.

If you access the App Store via your desktop and browser, you can download as many as you wish. For example, four instances of the WAF or GSLB. They will appear in your ADC's Purchased Apps area so you can download them.

The Apps associate to the ADC's you own and have registered.

When you elect to download an App, you will be asked for the Machine ID, following which the App is encrypted and linked to the ADC Machine ID.

The links to the App Store are:

- Add-Ons: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/ADD-ONS/**
- Health Monitors: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/SERVER-HEALTH-MONITORS/**
- jetPACKS: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/JETPACKS/**
- Feature Packs: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/EDGENEXUS-FEATURE-PACK/**
- flightPATH Rules: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/FLIGHTPATH/**
- Software Updates: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/EDGENEXUS-SOFTWARE-UPDATE/**

Deploying an App

Once downloaded to the ADC, the App will be moved to the Downloaded Apps section and deployed onto the ADC using the Deploy button. This process takes some time depending on the resources available for the ADC. Once deployed, it will appear in the Downloaded Apps section.

Authentication

The Library > Authentication page allows you to set up authentication servers and create authentication rules with options for client-side Basic or Forms and server-side NTLM or BASIC.

Setting up Authentication – A Workflow

Please carry out the following steps as a minimum to apply Authentication to your service.

1. Create an Authentication Server.

2. Create an Authentication Rule that uses an Authentication Server.
3. Create a flightPATH rule that uses an Authentication Rule.
4. Apply the flightPATH rule to a Service

Authentication Servers

To set up a working authentication method, we must first set up an authentication server.

- Click the Add Server button.
- This action will produce a blank row ready for completion.

Option	Description
Name	Give your server a name for identification purposes – this name is used in the rules
Description	Add a description
Authentication Method	Choose an authentication method LDAP – basic LDAP with usernames and passwords sent in clear text to the LDAP server. LDAP-MD5 – basic LDAP with username in clear text and password MD5 hashed for increased security. LDAPS – LDAP over SSL. Sends the password in clear text within an encrypted tunnel between the ADC and LDAP server. LDAPS-MD5 – LDAP over SSL. The password is MD5 hashed for added security within an encrypted tunnel between the ADC and the LDAP server
Domain	Add in the domain name for the LDAP server.
Server Address	Add the IP address or hostname of the authentication server LDAP – IPv4 address or hostname. LDAP-MD5 – hostname only (IPv4 address will not work) LDAPS – IPv4 address or hostname. LDAPS-MD5 – hostname only (IPv4 address will not work).
Port	Use port 389 for LDAP and port 636 for LDAPS by default. No need to add the port number for LDAP and LDAPS. When other methods become available, you will be able to configure them here
Search Conditions	Search conditions must conform to RFC 4515. Example: (MemberOf=CN=Phone- VPN,CN=Users,DC=mycompany,DC=local).
Search Base	This value is the starting point for the search in the LDAP database. Example *dc=mycompany,dc=local*
Login Format	Use the login format you need. Username – with this format chosen, you need only enter the username. Any user and domain information entered by the user is deleted, and the domain information from the server is used. Username and Domain – The user must enter the whole domain and username syntax. Example: *mycompany\gchristie OR someone@mycompany*. The domain information entered at the server level is ignored. Blank – the ADC will accept anything the user inputs and send it on to the authentication server. This option is used when using MD5.
Passphrase	This option is not used in this version.
Dead Time	Not used in this version

Authentication Rules

The next stage is to create the authentication rules for use with the server definition.

Field	Description
Name	Add a suitable name for your authentication rule.
Description	Add a suitable description.
Root Domain	This must be left blank unless you need single-sign-on across sub-domains.
Authentication Server	This is a dropdown box containing servers that you have configured.
Client Authentication:	Choose the value appropriate to your needs: Basic (401) – This method uses the standard 401 authentication method Forms – this will present the ADC default form to the user. Within the form, you can add a message. You can select a form that you have uploaded using the section below.
Server Authentication	Choose the appropriate value. None – if your server does not have any existing authentication, select this setting. This setting means that you can add authentication abilities to a server that previously had none. Basic – if your server has basic authentication (401) enabled, then select BASIC. NTLM – if your server has NTLM authentication enabled, then select NTLM.
Form	Choose the appropriate value Default – Selecting this option will result in the ADC using its built-in form. Custom – you can add a form that you have designed and select it here.
Message	Add a personal message to the form.
Timeout	Add a timeout to the rule, after which the user will be required to authenticate again. Note the Timeout setting is only valid for Forms-based authentication.

Single Sign-On

If you wish to provide a single sign-on for users, complete the Root Domain column with your domain. In this example, we have used edgenexus.io. We can now have multiple services that will use edgenexus.io as the root domain, and you will only have to log in once. If we consider the following services:

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

These services can reside on one VIP or can be distributed across 3 VIPs. A user accessing usercentral.mycompany.com for the first time will be presented with a form asking them to log in depending on the authentication rule used. The same user can then connect to appstore.mycompany.com and will be

authenticated automatically by the ADC. You can set the timeout, which will force authentication once this period of inactivity has been reached.

Forms

This section will enable you to upload a custom form.

How to create your custom form

Although the basic form the ADC provides is sufficient for most purposes, there will be occasions where companies wish to present their own identity to the user. You can create your custom form that users will be presented with to fill in in such cases. This form must be in either HTM or HTML format.

Option	Description
Name	form name = loginform action = %JNURL% Method = POST
Username	Syntax: name = "JNUSER"
Password:	name="JNPASS"
Optional Message1:	%JNMESSAGE%
Optional Message2:	%JNAUTHMESSAGE%
Images	If you wish to add an image, then please add it in-line using Base64 encoding.

Example html code of a very basic and simple form

```
<HTML>

<HEAD>

<TITLE>SAMPLE AUTH FORM</TITLE>

</HEAD>

<BODY>

%JNMESSAGE%<br>

<form name="loginform" action="%JNURL%" method="post"> USER: <input type="text" name="JNUSER" size="20" value=""></br>

PASS: <input type="password" name="JNPASS" size="20" value=""></br>

<input type="submit" name="submit" value="OK">

</form>

</BODY>

</HTML>
```

Adding a custom form

Once you have created a custom form, you can add it using the Forms section.

1. Choose a name for your form
2. Browse locally for your form

3. Click Upload

Previewing your custom form

To view the custom form that you have just uploaded, you select it and click Preview. You may also use this section to delete forms that are no longer required.

Cache

The ADC is capable of caching data within its internal memory and periodically flushes this Cache to the ADC's internal storage. The settings that manage this functionality are provided within this section.

Global Cache Settings

Maximum Cache Size (MB)

This value determines the maximum RAM that the Cache can consume. The ADC Cache is an in-memory cache that is also periodically flushed to the storage medium to maintain cache persistence after restarts, reboots, and shutdown operations. This functionality means that the maximum cache size must fit within the memory footprint of the appliance (rather than disk space) and should be no more than half of the available memory.

Desired Cache Size (MB)

This value denotes the optimum RAM to which the Cache will be trimmed. While the maximum cache size represents the absolute upper boundary of the Cache, the desired cache size is intended as the optimum size that the Cache should attempt to attain whenever an automatic or manual check on the cache size is made. The gap between the maximum and desired cache size exists to accommodate the arrival and overlap of new content between periodic checks on cache size to trim expired content. Once again, it may be more effective to accept the default value (30 MB) and periodically review the size of the Cache under "Monitor -> Statistics" for appropriate sizing.

Default Cache Time (D/HH:MM)

The value entered here represents the life of content without an explicit expiry value. The default caching time is the period for which content without a "no-store" directive or explicit expiry time in the traffic header is stored.

The field entry takes the form "D/HH:MM" – so an entry of "1/01:01" (default is 1/00:00) means to store the ADC will hold the content for one day, "01:00" for one hour, and "00:01" for one minute.

Cachable HTTP Response Codes

One of the cached data sets is HTTP responses. The HTTP response codes that are cached are:

- 200 – Standard response for successful HTTP requests
- 203 – Headers are not definitive but are gathered from a local or a 3rd party copy
- 301 – The requested resource has been assigned a new permanent URL
- 304 – Not modified since the last request & locally cached copy should be used instead
- 410 – Resource is no longer available at the server, and no forwarding address is known

This field should be edited with caution as the most common cacheable response codes are already listed.

Cache Checking Time (D/HH:MM)

This setting determines the time interval between cache trim operations.

Cache-Fill Count

This setting is a helper facility to help fill the Cache when a certain number of 304's have been detected.

Apply Cache Rule

This section allows you to apply a cache rule to a domain:

- Add domain manually with the Add Records button. You must use a fully qualified domain name or an IP address in dotted-decimal notation. Example www.mycompany.com or 192.168.3.1:80
- Click the dropdown arrow and choose your domain from the list
- The list will be populated so long as traffic has passed through a virtual service and a caching strategy has been applied to the virtual service
- Choose your cache rule by double-clicking on the Caching Rulebase column and selecting from the list

Create Cache Rule

This section allows you to create several different caching rules that can then be applied to a domain:

- Click Add Records and give your rule a name and description
- You can either type your conditions in manually or use the Add Condition

To add a condition using the Selection Rulebase:

- Choose Include or Exclude
- Choose All JPEG Images
- Click on the + Add symbol
- You will see that 'include *.jpg' has now been added to the conditions
- You can add more conditions. If you choose to do this manually, you need to add each condition on a NEW line. Please note that your rules will display on the same line until you click in the Conditions box then they will show on a separate line

flightPATH

flightPATH is the traffic management technology built into the ADC. flightPATH allows you to inspect HTTP and HTTPS traffic in real-time and perform actions based on conditions.

flightPATH rules must be applied to a VIP when IP objects are used within the rules.

A flightpath rule consists of four elements:

1. Details, where you define the flightPATH Name and Service to which it is attached.
2. Condition(s) that can be defined that cause the rule to be triggered.
3. Evaluation that allows the definition of variables that can be used within Actions
4. Actions that are used to manage what should happen when conditions are met

Details

The details section shows the available flightPATH rules. You can add new flightPATH rules and remove defined ones from this section.

Adding a new flightPATH rule

Field	Description
FlightPATH Name	This field is for the name of the flightPATH rule. The name you provide here appears in and is referenced within other parts of the ADC.
Applied to VS	This column is read-only and shows the VIP to which the flightPATH rule is applied.

Description	Value representing a description provided for readability purposes.

Steps to add a flightPATH rule

1. First, click the Add New button located in the Details section.
2. Enter a name for your rule. Example Auth2
3. Enter a description of your rule
4. Once the rule has been applied to a service, you will see the Applied To column auto-populate with an IP address and port value
5. Don't forget to hit the Update button to save your changes or if you make a mistake, just hit cancel revert to the previous state.

Condition

A flightPATH rule can have any number of conditions. The conditions work on an AND basis allow you to set the condition on which the action is triggered. If you want to use an OR condition, create an additional flightPATH rule and apply it to the VIP in the correct order.

You can also use RegEx by selecting Match RegEx in the Check field and the RegEx value in the Value field. The inclusion of RegEx evaluation extends the capability of flightPATH tremendously.

Creating a new flightPATH condition

Condition

We provide several Conditions as pre-defined within the dropdown and cover all foreseen scenarios. When new Conditions are added, these will be available through Jetpack updates.

Choices available are:

CONDITION	DESCRIPTION	EXAMPLE
<form>	HTML forms are used to pass data to a server	Example "form doesn't have length 0"
GEO Location	Compares the source IP address to the ISO 3166 Country Codes	GEO Location does equal GB, OR GEO Location does equal Germany
Host	Host extracted from the URL	www.mywebsite.com or 192.168.1.1
Language	Language extracted from the language HTTP header	This condition will produce a dropdown with a list of Languages
Method	Dropdown of HTTP methods	Dropdown that includes GET, POST, etc
Origin IP	If upstream proxy supports X-Forwarded-for (XFF) it will use the true Origin address	Client IP. It can also use multiple IPs or subnets.

		10\.1\.2\.* is 10.1.2.0 /24 subnet 10\.1\.2\.3|10\.1\.2\.4 Use | for multiple IP's
Path	Path of the website	/mywebsite/index.asp
POST	POST request method	Check data being uploaded to a website
Query	Name and value of a query, and can either accept the query name or a value also	"Best=jetNEXUS" Where the Match is Best and the Value is edgeNEXUS
Query String	The whole query string after the ? character	
Request Cookie	Name of a cookie requested by a client	MS-WSMAN=afYfn1CDqqCDqUD::
Request Header	Any HTTP Header	Referrer, User-Agent, From, Date
Request Version	The HTTP version	HTTP/1.0 OR HTTP/1.1
Response Body	A user defined string in the response body	Server UP
Response Code	The HTTP code for the response	200 OK, 304 Not Modified
Response Cookie	The name of a cookie sent by the server	MS-WSMAN=afYfn1CDqqCDqUD::
Response Header	Any HTTP Header	Referrer, User-Agent, From, Date
Response Version	The HTTP version sent by the server	HTTP/1.0 OR HTTP/1.1
Source IP	Either the origin IP, proxy server IP, or some other aggregated IP address	Client IP, Proxy IP, Firewall IP. Can also use multiple IP and subnets. You must escape the dots as these are RegEX. Example 10\.1\.2\.3 is 10.1.2.3

Match

The Match field can be either a drop-down or a text value and is definable depending on the value in the Condition field. For example, if the Condition is set to Host, the Match field is not available. If the Condition is set to <form>, the Match field is shown as a text field, and if the Condition is POST, the Match field is presented as a drop-down containing pertinent values.

Choices available are:

MATCH	DESCRIPTION	EXAMPLE
Accept	Content-Types that are acceptable	Accept: text/plain
Accept-Encoding	Acceptable encodings	Accept-Encoding: <compress | gzip | deflate | sdch | identity>
Accept-Language	Acceptable languages for response	Accept-Language: en-US
Accept-Ranges	What partial content range types this server supports	Accept-Ranges: bytes
Authorization	Authentication credentials for HTTP authentication	Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Charge-To	Contains account information for the costs of the application of the method requested	

Content-Encoding	The type of encoding used	Content-Encoding: gzip
Content-Length	The length of the response body in Octets (8-bit bytes)	Content-Length: 348
Content-Type	The mime type of the body of the request (used with POST and PUT requests)	Content-Type: application/x-www-form-urlencoded
Cookie	A HTTP cookie previously sent by the server with Set-Cookie (below)	Cookie: $Version=1; Skin=new;
Date	Date and time at message was originated	Date = "Date" ":" HTTP-date
ETag	An identifier for a specific version of a resource, often a message digest	ETag: "aed6bdb8e090cd1:0"
From	The email address of the user making the request	From: user@example.com
If-Modified-Since	Allows a 304 Not Modified to be returned if the content is unchanged	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Last-Modified	The last modified date for the requested object, in RFC 2822 format	Last-Modified: Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Implementation: Specific headers that may have various effects anywhere along the request-response chain.	Pragma: no-cache
Referrer	Address of the previous web page from which a link to the currently requested page was followed	Referrer: HTTP://www.edgenexus.io
Server	A name for the server	Server: Apache/2.4.1 (Unix)
Set-Cookie	A HTTP cookie	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
User-Agent	The user agent string of the user agent	User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Vary	Tells downstream proxies how to match future request headers to decide whether the cached response can be used rather than requesting a fresh one from the origin server	Vary: User-Agent
X-Powered-By	Specifies the technology (e.g. ASP.NET, PHP, JBoss) supporting the web application	X-Powered-By: PHP/5.4.0

Sense
The Sense field is a drop-down Boolean field and contains either Does or Doesn't choices.

Check
The Check field allows the setting of check values against the Condition.

Choices available are: Contain, End, Equal, Exist, Have Length, Match RegEx, Match List, Start, Exceed Length

CHECK	DESCRIPTION	EXAMPLE
Exist	This does not care for the detail of the condition just that it does/doesn't exist	Host — Does — Exist
Start	The string starts with the Value	Path — Does — Start — /secure
End	The string ends with the Value	Path — Does — End — .jpg

Contain	The string does contain the Value	Request Header — Accept — Does — Contain — image
Equal	The string does Equal the Value	Host — Does — Equal — www.edgenexus.io
Have Length	The string does have a length of the value	Host — Does — Have Length — 16 www.edgenexus.io = TRUE www.edgenexus.com = FALSE
Match RegEx	Enables you to enter a full Perl compatible regular expression	Origin IP — Does — Match Regex — 10\..* | 11\..*

Steps to add a Condition

Adding a new flightPATH Condition is very easy. An example is shown above.

1. Click the Add New button within the Condition area.
2. Choose a condition from the drop-down box. Let's take Host as an example. You can also type into the field, and the ADC will show the value in a drop-down.
3. Choose a Sense. For example, Does
4. Choose a Check. For example, Contain
5. Choose a value. For example, mycompany.com

The above example shows that there are two conditions that both have to be TRUE for the rule to complete

- The first is checking that the requested object is an image
- The second checks whether the host in the URL is www.imagepool.com

Evaluation

The ability to add definable variables is a compelling capability. Regular ADC's offer this capability using scripting or command-line options that are not ideal for anyone. The ADC allows you to define any number of variables using an easy-to-use GUI, as shown and described below.

flightPATH variable definition comprises four entries that need to be made.

- Variable – this is the name of the variable
- Source – a drop-down list of possible source points
- Detail – select values from a drop-down or manually typed.
- Value – the value that the variable holds and can be an alphanumeric value or a RegEx for fine-tuning.

Built-in Variables:

Built-In variables have already been hardcoded, so you do not need to create an evaluation entry for these.

You can use any of the variables listed below in the Action section.

The explanation for each variable is located in the "Condition" table above.

- Method = $method$
- Path = $path$
- Querystring = $querystring$
- Sourceip = $sourceip$
- Response code (text also included "200 OK") = $resp$

- Host = $host$
- Version = $version$
- Clientport = $clientport$
- Clientip = $clientip$
- Geolocation = $geolocation$"

ACTION	TARGET
Action = Redirect 302	Target = HTTPs://$host$/404.html
Action = Log	Target = A client from $sourceip$:$sourceport$ has just made a request $path$ page

Explanation:

- A client accessing page that does not exist would ordinarily be presented with the browser's 404 Error page

- Instead, the user is redirected to the original hostname they used, but the incorrect path is replaced with 404.html

- An entry is added to the Syslog saying, "A client from 154.3.22.14:3454 has just requested the wrong.html page."

Action

The next stage in the process is to add an action associated with the flightPATH rule and condition.

In this example, we want to rewrite the path portion of the URL to reflect the URL typed by the user.

- Click Add New
- Choose Rewrite Path from the Action drop-down menu
- In the Target field, type in $path$/myimages
- Click Update

This action will add /myimages to the path, so the final URL becomes www.imagepool.com/myimages

Applying the flightPATH rule

The application of any flightPATH rule is made within the flightPATH tab of each VIP/VS.

- Navigate to Services > IP Services and choose the VIP to which you wish to assign the flightPATH rule.
- You will see the Real Server list shown below
- Click on the flightPATH tab
- Select the flightPATH rule you have configured or one of the pre-built ones supported. You can select multiple flightPATH rules if required.
- Drag and drop the selected set to the Applied flightPATHs section or click the >> arrow button.
- The rule will be moved to the right side and automatically applied.

Real Server Monitors

When load balancing is set up, it is helpful to monitor the health of the real servers and the applications running on them. For instance, in web servers, you can set up a specific page that you can use to monitor the state or use one of the other monitoring systems the ADC has.

The Library > Real Server Monitors page allows you to add, view and edit custom monitoring. These are Layer 7 server "Health Checks" and select them from the Server Monitoring field within the Basic tab of the Virtual service you define.

Types of Real Server Monitors

There are several Real Server Monitors available, and the table below explains these. You can, of course, write additional monitors using PERL.

Monitoring Method	Description	Example

HTTP 200 OK	A TCP connection is made to the Real Server. After the connection is made, a brief HTTP request is sent to the Real Server. When the response is received, it is checked for the '200 OK' string. If it is present, the server is considered operational. Please note that using this monitor fetches the entire page with contents. This monitoring method can only really be used with HTTP and Accelerated HTTP service types. However, if a Layer 4 Service Type is in use for an HTTP server, it could still be used if SSL is not in use on the Real Server or handled appropriately by the "Content SSL" facility.	**Request**
		GET / HTTP/1.1
		Host: 192.168.159.200
		Accept: */*
		Accept-Language: en-gb
		User-Agent: Edgenexus-ADC/4.0
		Connection: Keep-Alive
		Cache-Control: no-cache
		
		Response
		HTTP/1.1 200 OK
		Content-Type: text/html
		Last-Modified: Wed, 31 Jan 2018 15:08:18 GMT
		Accept-Ranges: bytes
		ETag: "0dd3253a59ad31:0"
		Server: Microsoft-IIS/10.0
		Date: Tue, 13 Jul 2021 15:55:47 GMT
		Content-Length: 1364
		
		\<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
		\<html xmlns="http://www.w3.org/1999/xhtml">
		\<head>
		\<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
		\<title>jetNEXUS\</title>
		\<style type="text/css">
		\<!--
		body {
		    color:#FFFFFF;
		    ...
		\</body>
		\</html>

HTTP 200 Head	A TCP connection is made to the Real Server with the PATH field specifying the location to be checked. The head portion of the response is fetched from the server, with contents discarded. The response is checked for 200 OK. If it is present, the server is considered operational. Please note that using this monitor fetches only the head portion. This monitoring method can only really be used with HTTP and Accelerated HTTP service types. However, if a Layer 4 Service Type is in use for an HTTP server, it could still be used if SSL is not in use on the Real Server or handled appropriately by the "Content SSL" facility.	**Request** HEAD / HTTP/1.1 Host: 192.168.159.200 Accept: */* Accept-Language: en-gb User-Agent: Edgenexus-ADC/4.0 Connection: Keep-Alive Cache-Control: no-cache **Response** HTTP/1.1 200 OK Content-Length: 1364 Content-Type: text/html Last-Modified: Wed, 31 Jan 2018 15:08:18 GMT Accept-Ranges: bytes ETag: "0dd3253a59ad31:0" Server: Microsoft-IIS/10.0 Date: Tue, 13 Jul 2021 15:49:19 GMT
HTTP 200 Options	A TCP connection is made to the Real Server, and an Options request is made.	**Request** OPTIONS / HTTP/1.1 Host: 192.168.159.200 Accept: */*

	The Options are returned and checked for 200 OK content. If the 200 OK content is found, then the server is deemed to be available.	Accept-Language: en-gb User-Agent: Edgenexus-ADC/4.0 Connection: Keep-Alive Cache-Control: no-cache **Response** HTTP/1.1 200 OK Allow: OPTIONS, TRACE, GET, HEAD, POST Server: Microsoft-IIS/10.0 Public: OPTIONS, TRACE, GET, HEAD, POST Date: Tue, 13 Jul 2021 16:23:39 GMT Content-Length: 0
HTTP Head	The HTTP Head monitor allows us to check for a specific value in the Head portion of the HTTP stream. We can enter a Path and Required Response in the appropriate fields and then check for that value in the response. Should the Required Response value be found in the Head, the server is deemed to be up and available. We can also use this on specially protected pages that need a username and password. In this manner, the monitor's result can be deemed to be accurate. For example, providing **/ispagethere.html** and **200 OK** values in the Path and Required Response fields will return a successful result if the server is up, the page is available, and responds to the request. This monitoring method can only really be used with HTTP and Accelerated HTTP service types. However, if a Layer 4 Service Type is in use for an HTTP server, it could still be used if SSL is not in use on the Real Server or handled appropriately by the "Content SSL" facility.	**Request** HEAD /ispagethere.htm HTTP/1.1 Host: 192.168.159.200 Accept: */* Accept-Language: en-gb User-Agent: Edgenexus-ADC/4.0 Connection: Keep-Alive Cache-Control: no-cache **Response** HTTP/1.1 200 OK Content-Length: 1364 Content-Type: text/html Last-Modified: Wed, 31 Jan 2018 15:08:18 GMT Accept-Ranges: bytes ETag: "0dd3253a59ad31:0" Server: Microsoft-IIS/10.0 Date: Wed, 14 Jul 2021 08:28:18 GMT
HTTP Options	The HTTP Options monitor allows you to check for a specific value within the returned Options data. We enter a Path and Required Response in the appropriate fields and then check the response. If the Required Response is found in the Options data, the server is available and running. The Required Response values can be any of the following: OPTIONS, TRACE, GET, HEAD, and POST. For example, providing **/ispagethere.html** and **GET** values in the Path and Required Response fields will return a successful result if the server is up, the page is available, and it responds to the request. This monitoring method can only really be used with HTTP and Accelerated HTTP service types. However, if a Layer 4 Service Type is in use for an HTTP server, it could still be used if SSL is not in use on the Real Server or handled appropriately by the "Content SSL" facility.	**Request** OPTIONS /ispagethere.htm HTTP/1.1 Host: 192.168.159.200 Accept: */* Accept-Language: en-gb User-Agent: Edgenexus-ADC/4.0 Connection: Keep-Alive Cache-Control: no-cache **Response** HTTP/1.1 200 OK Allow: OPTIONS, TRACE, GET, HEAD, POST Server: Microsoft-IIS/10.0 Public: OPTIONS, TRACE, GET, HEAD, POST Date: Wed, 14 Jul 2021 09:47:27 GMT Content-Length: 0

HTTP Response	A connection and HTTP request/response is made to the Real Server and checked as explained in the previous examples. But rather than check for a "200 OK" response code, the HTTP response's header is checked for custom text content. The text can be a full header, part of a header, a line from part of a page, or just one word. For instance, in the example shown to the right, we specified **/ispagethere.htm** as the Path and **Microsoft-IIS** as the Required Response. If the text is found, the Real Server is deemed to be up and running. This monitoring method can only really be used with HTTP and Accelerated HTTP service types. However, if a Layer 4 Service Type is in use for an HTTP server, it could still be used if SSL is not in use on the Real Server or handled appropriately by the "Content SSL" facility.	**Request** GET /ispagethere.htm HTTP/1.1 Host: 192.168.159.200 Accept: */* Accept-Language: en-gb User-Agent: Edgenexus-ADC/4.0 Connection: Keep-Alive Cache-Control: no-cache **Response** HTTP/1.1 200 OK Content-Type: text/html Last-Modified: Wed, 31 Jan 2018 15:08:18 GMT Accept-Ranges: bytes ETag: "0dd3253a59ad31:0" Server: Microsoft-IIS/10.0 Date: Wed, 14 Jul 2021 10:07:13 GMT Content-Length: 1364 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /> <title>jetNEXUS</title> <style type="text/css"> <!-- body { color:#FFFFFF; …
Multi-Port TCP monitor	This method is like the above, except that you can have several different ports. The monitor is deemed successful only if all ports specified in the required content section respond correctly.	Name: Multi-Port Monitor Description: Monitor multiple ports for success Page Location: N/A Required Content: 135,59534,59535
TCP Out of Band	The TCP Out of Band method is like a TCP Connect except that you can specify the port you wish to monitor in the required content column. This port is typically not the same as the traffic port and is used when you want to tie services together	Name: TCP Out of Band Description: Monitor Out of Band/Traffic port Page Location: N/A Required Content: 555
DICOM	We send a DICOM echo using the "Source Calling" AE Title value in the required content column. You can also set the "Destination Called" AE Title value in the Notes section of each server. You can find the Notes column within the IP Services--Virtual Services--Server page.	Name: DICOM Description: L7 health check for DICOM service Monitoring Method: DICOM Page Location: N/A Required Content: AET Value
LDAPS	This new health check is used to check the health and response of an LDAP/AD server.	Name: LDAPS Description: LDAP/AD Server health check Usage parameters are as follows: **Username**: cn=username,cn=users,dc=domainname,dc=local **Password**: DomainUserPassword **Content**: 200OK

SNMP v2	This monitoring method allows you to check for a server availability status using the server's SNMP MIB response. The Require Response value should contain the Community Name.
DNS Server Check	When load balancing DNS Servers, it is helpful to see if the server responds to DNS queries. The monitor can be used as follows: • The Path field is used for the FQDN that you are querying. For example, if you wished to query www.edgenexus.io, then enter this in the Path field. • If you leave this blank, then the monitor will use its default lookup to make the query. • The Required Response field can be left blank, and the monitor will assume that any response is considered valid. Otherwise, you should enter the expected IP in the Required Response field. For example, this may be 101.10.10.100. If the query returns this value, the monitor flags a success; else, it will flag a failure. A success result indicates that the DNS server you are load-balancing is operational.

The Real Server Monitor Page

The Real Server Monitors page is split into three sections.

- Details
- Upload
- Custom Monitors

Details

The Details section is used to add new monitors and to remove any that you do not need. You can also edit an existing monitor by double-clicking on it.

Name

Name of your choice for your monitor.

Description

Textual description for this Monitor, and we recommend that it is best to make it as descriptive as possible.

Monitoring Method

Choose the monitoring method from the drop-down list. Available choices are:

- HTTP 200 OK
- HTTP 200 Head
- HTTP 200 Options
- HTTP Head
- HTTP Options
- HTTP Response
- Multi-Port TCP Monitor

- TCP Out of Band
- DICOM
- SNMP v2
- DNS Server Check
- LDAPS

Page Location

URL Page location for an HTTP monitor. This value can be a relative link such as /folder1/folder2/page1.html. You can also use an absolute link where the website is bound to the hostname.

Required Content

This value contains any content that the monitor needs to detect and utilize. The value represented here will change depending on the monitoring method that is chosen.

Applied to VS

This field is automatically populated with the IP/Port of the Virtual Service to which the monitor is applied. You will not be able to delete any Monitor that has been used with a Virtual Service.

User

Some custom monitors can use this value along with the password field to log into a Real Server.

Password

Some custom monitors can use this value along with the User field to log into a Real Server.

Threshold

The Threshold field is a general integer used in custom monitors where a threshold such as the CPU level is required.

NOTE: Please ensure the response back from the Application server is not a "Chunked" response

Real Server Monitor examples

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			

Upload Monitor

There will be many occasions when users wish to create their own custom monitors and this section allows them to upload them to the ADC.

Custom monitors are written using PERL scripts and have a .pl file extension.

- Give your monitor a name so that you can identify it in the Monitoring Method list

- Browse for the .pl file
- Click Upload New Monitor
- Your file will be uploaded to the correct location and will be visible as a new Monitoring Method.

Custom Monitors

In this section, you can view custom monitors uploaded and remove them if they are no longer needed.

- Click the drop-down box
- Select the name of the custom monitor
- Click Remove
- Your custom monitor will no longer be visible in the Monitoring Method list

Creating a Custom Monitor Perl Script

CAUTION: This section is intended for persons with experience in using and writing in Perl

This section shows you the commands you can use within your Perl script.

The #Monitor-Name: command is the name used for the Perl Script stored on the ADC. If you do not include this line, then your script will not be found!

The following are mandatory:

- #Monitor-Name
- use strict;
- use warning;

The Perl scripts are run in a CHROOTED environment. They often call another application such as WGET or CURL. Sometimes these need to be updated for a specific features, such as SNI.

Dynamic Values

- my $host = $_[0]; - This uses the "Address" from IP Services--Real Server section
- my $port = $_[1]; - This uses the "Port" from IP Services--Real Server section
- my $content = $_[2]; - This uses the "Required Content" value from the Library--Real Server Monitoring section
- my $notes = $_[3]; - This uses the "Notes" column in Real Server section of IP Services
- my $page = $_[4]; - This uses the "Page Location" values from Library--Real Server Monitor section
- my $user = $_[5]; - This uses the "User" value from the Library--Real Server Monitor section
- my $password = $_[6]; - This uses the "Password" value from the Library--Real Server Monitor section

Custom Health Checks have two outcomes

- Successful
  Return Value 1
  Print a success message to Syslog
  Mark the Real Server Online (provided IN COUNT match)
- Unsuccessful
  Return Value 2
  Print a message saying Unsuccessful to Syslog
  Mark the Real Server Offline (provided OUT Count match)

Example of a Custom Health Monitor

```
#Monitor-Name HTTPS_SNI
use strict:
use warnings;
# The monitor name as above is displayed in the drop-down of Available health checks
# There are 6 value passed to this script (see below)
# The script will return the following values
# 1 is the test is successful
# 2 if the test is unsuccessful sub monitor
{
my Shost       = $_[O]; ### Host IP or name
my Sport       = $_[1]; ### Host Port
my Scontent    = $_[2]; ### Content to look for (in the web page and HTTP headers)
my Snotes      = $_[3]; ### Virtual host name
my Spage       = $_[4]; ### The part of the URL after the host address
my Suser       = $_[5]: ### domain/usemame (optional)
my Spassword  = $_[6]; ### password (optional)
my $resolve;
my $auth        =;
if ($port)
{
      $resolve = "$notes:$port:$host":
}
else {
      $resolve = "$notes:$host";
}
if ($user && $password) {
      $auth = "-u $user:$password :
}
my @lines = 'curl -s -i -retry 1 -max-time 1 -k -H "Host:$notes --resolve $resolve $auth HTTPs://${notes}${page} 2>&1';
if(join(""@lines)=~/$content/)
      {
      print "HTTPs://$notes}${page} looking for - $content - Health check successful.\n";
      return(1);
      }
else
      {
      print "HTTPs://${notes}${page} looking for - $content - Health check failed.\n";
      return(2)
      }
}
monitor(@ARGV):
```

NOTE: Custom Monitoring – Use of global variables is not possible. Use local variables only – variables defined inside functions

SSL Certificates

To successfully use Layer 7 load-balancing with servers using encrypted connections using SSL, the ADC must be equipped with the SSL certificates used on the target servers. This requirement is so that the data stream can be decrypted, examined, managed, and then re-encrypted before sending to the target server.

The SSL certificates can range from self-signed certificates that the ADC can generate to the traditional certificates (wildcard included) available from trusted providers. You can also use domain signed certificates that are generated from Active Directory.

What does the ADC do with the SSL Certificate?

The ADC can perform traffic management rules (flightPATH) depending on what the data contains. This management cannot be performed on SSL encrypted data. When the ADC has to inspect the data, it needs first to decrypt it, and for that, it needs to have the SSL certificate used by the server. Once decrypted, the ADC will then be able to examine and perform the flightPATH rules. Following this, the data will be re-encrypted using the SSL certificate and sent onto the final Real Server.

Create Certificate

Although the ADC can use a globally trusted SSL certificate, it can generate a Self-Signed SSL Certificate. The Self-Signed SSL is perfect for internal load balancing requirements. However, your IT policies may require a trusted or domain CA certificate.

How to Create a Local SSL certificate

- Fill in all the details like the example above
- Click on Create Local Certificate
- Once you have clicked this, you can apply the certificate to a **VIRTUAL SERVICE.**

Create a Certificate Request (CSR)

When you need to obtain a globally trusted SSL from an external provider, you will need to generate a CSR to generate the SSL certificate.

Fill in the form as shown above with all relevant data, and then click the Certificate Request button. You will be presented with the popup corresponding to the data you provided.

You will need to cut and paste the contents into a TEXT file and name it with a CSR file extension, for example, *mycert.csr*. This CSR file will then need to be provided to your certificate authority to create the SSL certificate.

Manage Certificate

This sub-section contains various tools to allow management of the SSL certificates you have within the ADC.

Show

There may be times when you wish to look at the details of an installed SSL certificate.

- Select the certificate from the drop-down menu
- Click on the Show button
- The popup shown below will be presented with the details of the certificate.

Installing a Certificate

Once you obtain the certificate from the Trusted Certificate Authority, you will need to match it to the CSR generated and install it within the ADC.

- Select a certificate that you have generated in the steps above. There will be a (Pending) status fixed to the line item. In the example, MyCompanyCertificate is shown in the image above.
- Open the certificate file in a text editor
- Copy the entire contents of the file to the clipboard
- Paste the contents of the signed SSL certificate you received from the trusted authority into the field marked Paste Signed.
- You may also paste in the Intermediates below this, taking care to follow the correct order:
    1. (TOP)   Your Signed Certificate
    2. (2nd From Top)   Intermediate 1
    3. (3rd from Top)   Intermediate 2
    4. (Bottom)   Intermediate 3
    5. Root Certificate Authority   No need to add this as they exist on the client machines.
        (the ADC also contains a root bundle for re-encryption where it acts as a client to a Real Server)
- Click Install
- Once you have installed the certificate, you should see the status (Trusted) next to your certificate

If you have made a mistake or entered the wrong intermediate order, then select the Certificate (Trusted) and add the certificates (including the signed certificate) again in the correct order and click Install

Add Intermediate

It is required on occasion to add intermediate certificates separately. For example, you may have imported a certificate that does not have the intermediates.

- Highlight a Certificate (trusted) or certificate (imported)
- Paste the intermediates one below the other taking care that the intermediate closest to the Certificate authority is pasted last.
- Click Add Intermediate.

If you make a mistake with the order, you can repeat the process and add the intermediates again. This action will only overwrite the previous intermediates.

Delete a Certificate

You can delete a certificate using the Delete button. Once deleted, the certificate will be removed entirely from the ADC and will need to be replaced, then reapplied to the Virtual Services if required again.

Note: Please make sure that the certificate is not attached to an operational VIP before deleting it.

Renew a certificate

The Renew button allows you to obtain a new Certificate Signing Request. This action is required when the certificate is due to expire and needs to be renewed.

- Select a certificate from the drop-down list; you may choose any certificate with the (Pending), (Trusted), or (Imported) status
- Click Renew
- Copy the new CSR details so you can obtain a new certificate

Certificate Details

Certificate Name: MyCompanyCertificate

Certificate Text:
```
-----BEGIN CERTIFICATE REQUEST-----
MIICojCCAYoCAQAwXTELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk5ZMR
EwDwYDVQQH
EwhOZXcgWW9yazESMBAGA1UEChMJTXIDb21wYW55MRowGAYDVQQD
ExF3d3cubXIj
b21wYW55LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCgg
EBAMP8YIOq
D5L6vmbotxHmcnwGORAxzSgqOuQZLOj7h2LCN8Hh0/W8mLEiC+k8iBou
hSna23TJ
B2BrL5xVwIPlSj6RDsAnegpavGUVsdkolu2iu7ujHGvSSAqjSsBBG4Is6ay3fLTI
ZM2ZDslUzjPYK0gW7LStS89bH2ELB/MPf+iILFeQmCGQ2i5pF67sO0PpNM
E7EqXU
MOv/beTQ2Kwf0/awUw2m2RZ2krdgBq/Fw2tzQq+KxS4nHhOsJwIPKBy9u
```

Close

- When you obtain the new certificate, follow the steps detailed in **SHOW**
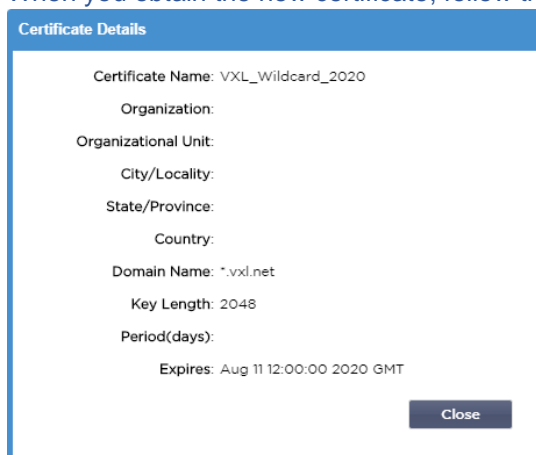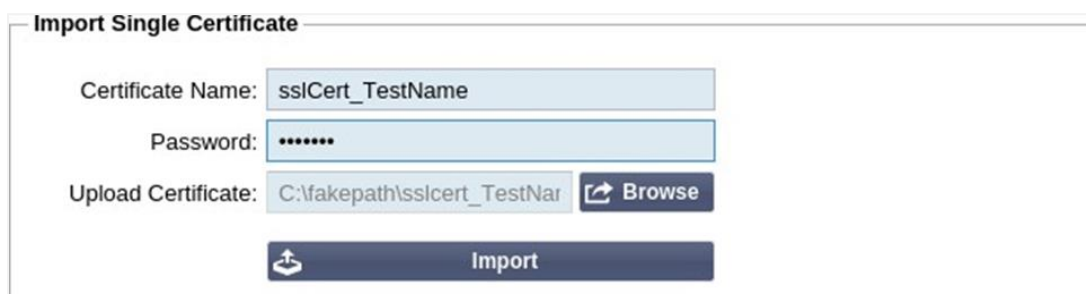
Certificate Details

Certificate Name: VXL_Wildcard_2020
Organization:
Organizational Unit:
City/Locality:
State/Province:
Country:
Domain Name: *.vxl.net
Key Length: 2048
Period(days):
Expires: Aug 11 12:00:00 2020 GMT

Close

-
- **THERE** may be times when you wish to look at the details of an installed SSL certificate.
- Select the certificate from the drop-down menu
- Click on the Show button
- The popup shown below will be presented with the details of the certificate.
- Installing a Certificate.
- The new and renewed certificate will now be installed into the ADC.

Importing a Certificate

In many cases, corporate enterprises will need to use their domain-signed certificates as part of their internal security regimes. The certificates must be in PKCS#12 format, and passwords invariably protect such certificates.

The image below shows the sub-section for importing a single SSL certificate.

- Give your certificate a friendly name. The name identifies it in the drop-down lists used in the ADC. It does not need to be the same as the certificate domain name but must be alphanumeric with no spaces. No special characters other than _ and – are allowed.
- Type the password you used to create the PKCS#12 certificate
- Browse for the {certificate name}.pfx
- Click Import.
- Your certificate will now be in the relevant SSL drop-down menus within the ADC

Importing Multiple Certificates

This section allows you to import a JNBK file that contains multiple certificates. A JNBK file is encrypted and produced by ADC when exporting multiple certificates.

- Browse for your JNBK file – you can create one of these by exporting multiple certificates
- Type the password you used to create the JNBK file
- Click Import.
- Your certificates will now be in the relevant SSL drop-down menus within the ADC

Exporting a Certificate

From time to time, you may wish to export one of the certificates held within the ADC. The ADC has been provided with the capability to do this.

- Click the certificate or certificates you wish to install. You may all click the All option to select all the listed certificates.
- Type a password to protect the exported file. The password must be at least six characters in length. Letters, numbers, and certain symbols can be used. The following characters are **not** acceptable: < > ” ‘ ( ) ; \ | \A3 % &
- Click Export

- Where you are exporting a single certificate, the resulting file will be named sslcert_{certname}.pfx. For example sslcert_Test1Cert.pfx
- In the case of a multi-certificate export, the resulting file will be a JNBK file. The filename will be sslcert__pack.jnbk.

Note: A JNBK file is an encrypted container file produced by the ADC and valid only for import into the ADC

Widgets

The Library > Widgets page allows you to configure various lightweight visual components displayed in your custom dashboard.

Configured Widgets
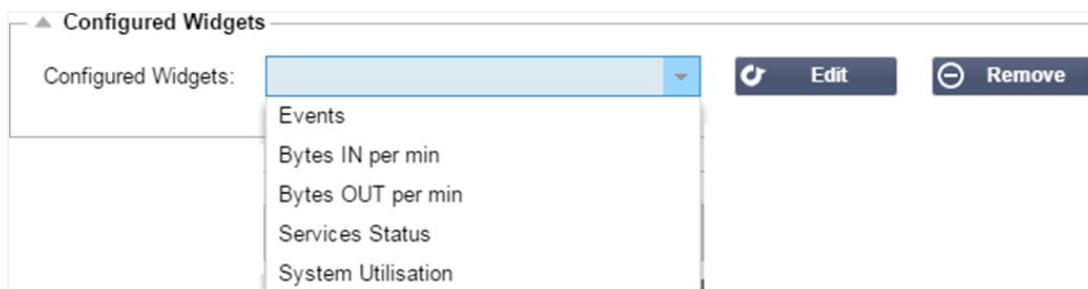
The Configured Widgets section allows you to view, edit or remove any widgets created from the available widgets section.

Available Widgets

There are five different widgets provided within the ADC, and you may configure them to your requirements.

The Events Widget
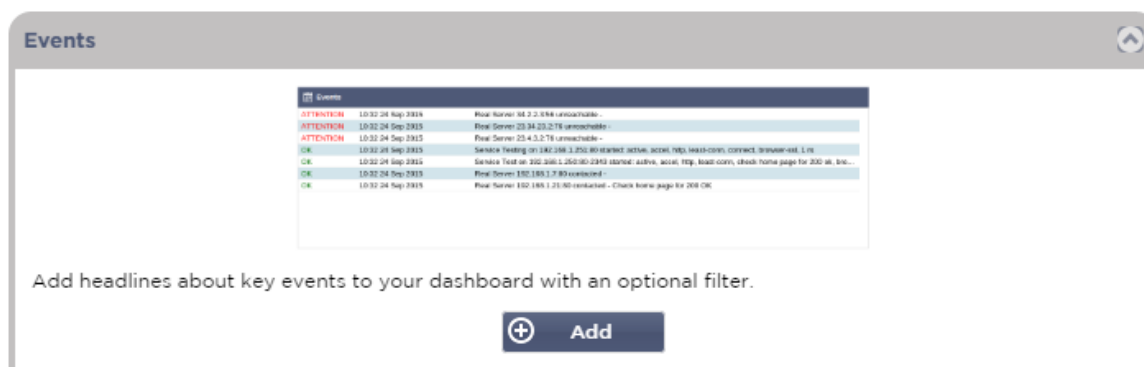
- To add an event to the Events widget, click the Add button.
- Provide a name for your event. In our example, we have added Attention Events as the event name.
- Add a keyword filter. We have also added the filter value of Attention
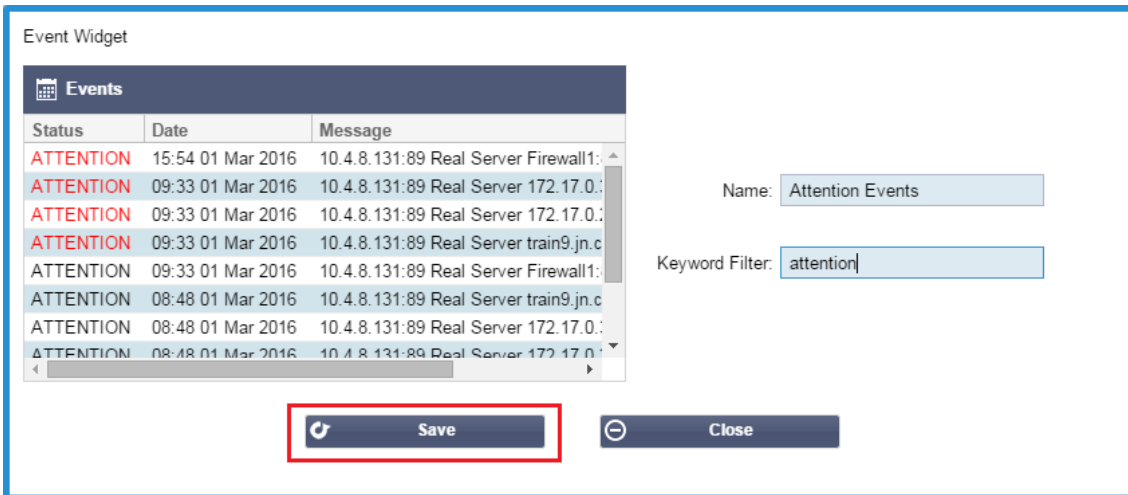
- Click Save, then Close
- You will now see an additional Widget called Attention Events in the Configured Widgets dropdown.
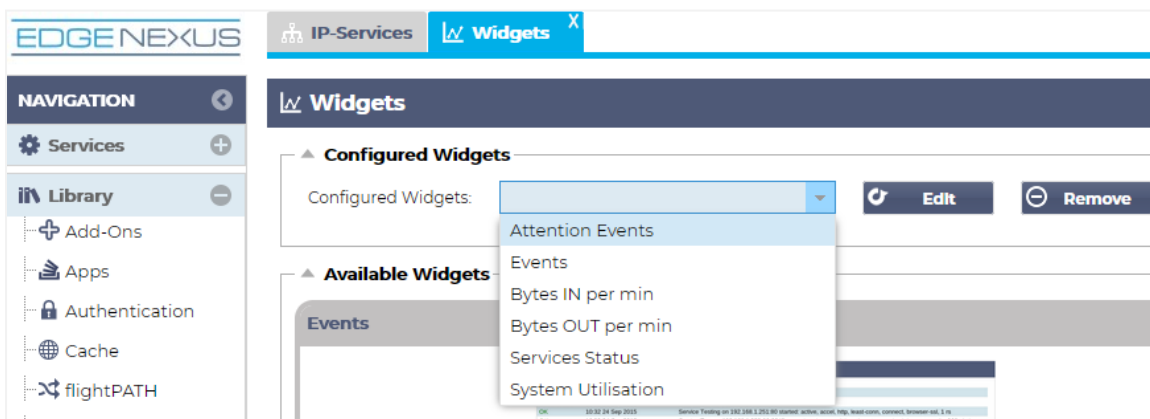
- You can see we have now added this widget in the View > Dashboard section.
- Select the Attention Events widget to display this within the Dashboard. See below.

You can also pause and restart the live data feed by clicking the Pause Live Data button. In addition, you can revert to the default dashboard at any time by clicking the Default Dashboard button.

The System Graphs Widget
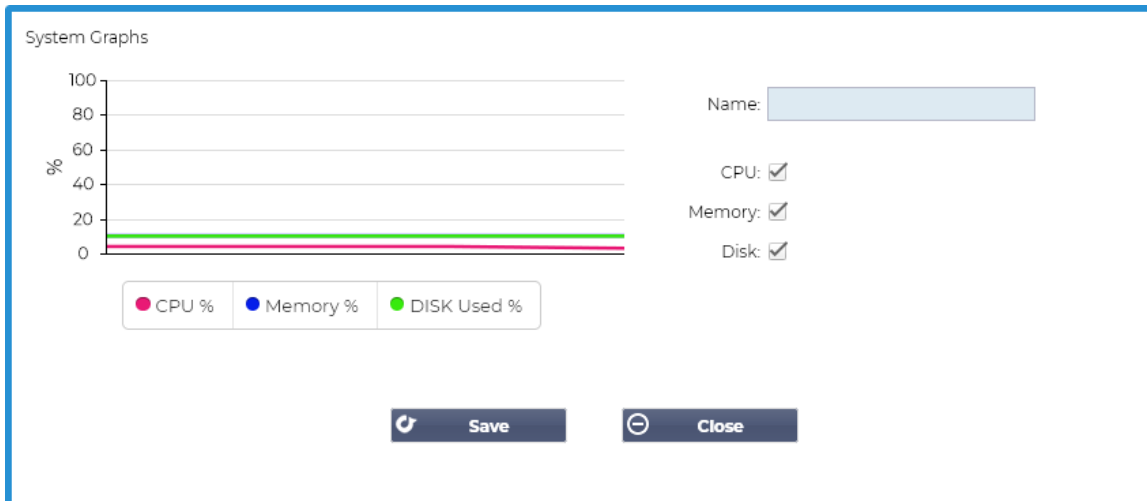
The ADC has a configurable System Graph widget. By clicking the Add button on the widget, you can add the following monitoring graphs to be displayed.

- CPU
- MEMORY
- DISK

Once you have added them, they will be individually available within the Dashboard's widget menu.

Interface Widget

The Interface widget allows you to display the data for the chosen network interface, such as ETH0, ETH1, and so on. The number of available interfaces for addition depends on how many network interfaces you have defined for the virtual appliance or provisioned within the hardware appliance.

Once you have finished, click the Save button, then the Close button.

Select the Widget you just customized from the widget drop-down menu within the Dashboard. You will see a screen like the one below.

Status Widget

The Status widget allows you to see load balancing in action. You can also filter the view to show specific information.

- Click Add.

- Enter a name for the service you wish to monitor
- You can also choose which columns you wish to display in the widget.

- Once you are satisfied, click Save, followed by Close.
- The chosen Status widget will be available in the Dashboard section.

Traffic Graphics Widget

This widget can be configured to show current and historical traffic data per Virtual Services and Real Servers. In addition, you can see overall current and historic data for global traffic

- Click the Add button
- Name your widget.
- Choose a Database from Virtual Services, Real Servers, or System.
- If you choose Virtual Services, you can select a virtual service from the VS/RS drop-down.
- Choose a time frame from the Last drop-down.

- o Minute – last 60s
- o Hour – aggregated data from each minute for the last 60 minutes
- o Day – aggregated data from each hour for the previous 24 hours
- o Week – aggregated data from each day during the previous seven days
- o Month – aggregated data from each week for the last seven days
- o Year – aggregated data from each month during the previous 12 months
- Choose the Data available depending on the database you have chosen
  - o Virtual Services Database
  - o Bytes in
  - o Bytes out
  - o Bytes cached
  - o Compression %
  - o Current Connections
  - o Requests per second
  - o Cache Hits
  - o Cache Hits %
- Real Servers
  - o Bytes in
  - o Bytes out
  - o Current Connections
  - o Request per second
  - o Response time
- System
  - o CPU %
  - o Services CPU
  - o Memory %
  - o Disk Free %
  - o Bytes in
  - o Bytes out
- Chose to show either Average or Peak values
- Once you have chosen all the options, click Save and Close

Example Traffic Graph
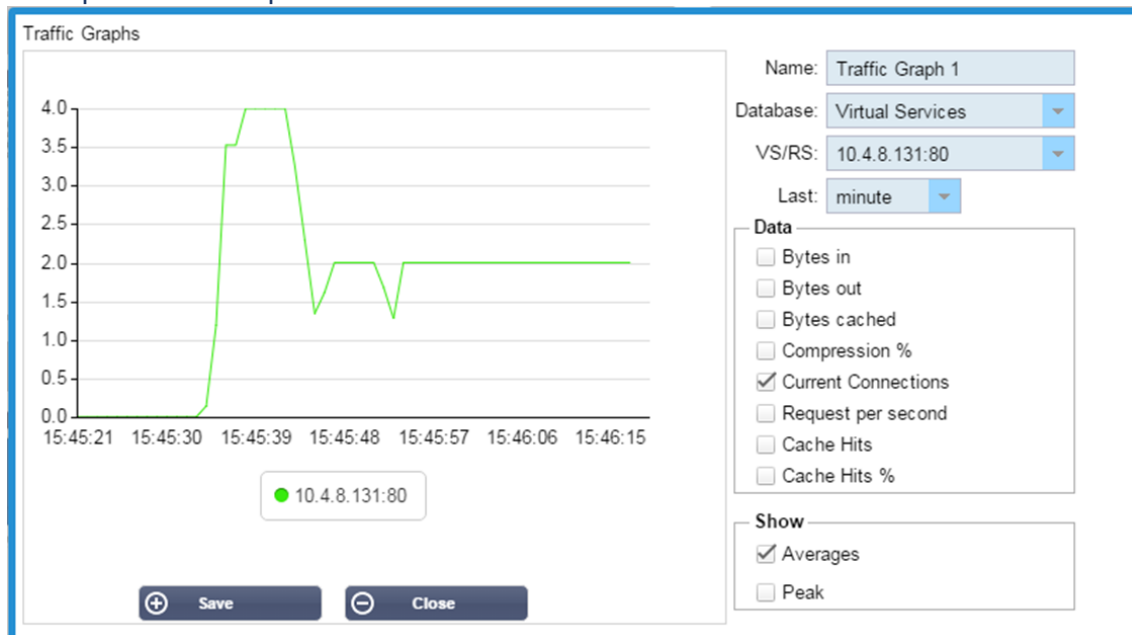
You can now add your Traffic Graph widget to the View > Dashboard.

View

Dashboard

Like all IT systems management interfaces, there are many times when you need to look at performance metrics and data that the ADC is handling. We provide a customizable dashboard for you to do this in an easy and meaningful manner.

The Dashboard is reachable by using the View segment of the navigator panel. When selected, it shows several default widgets and allows you to choose any customized ones that you have defined.
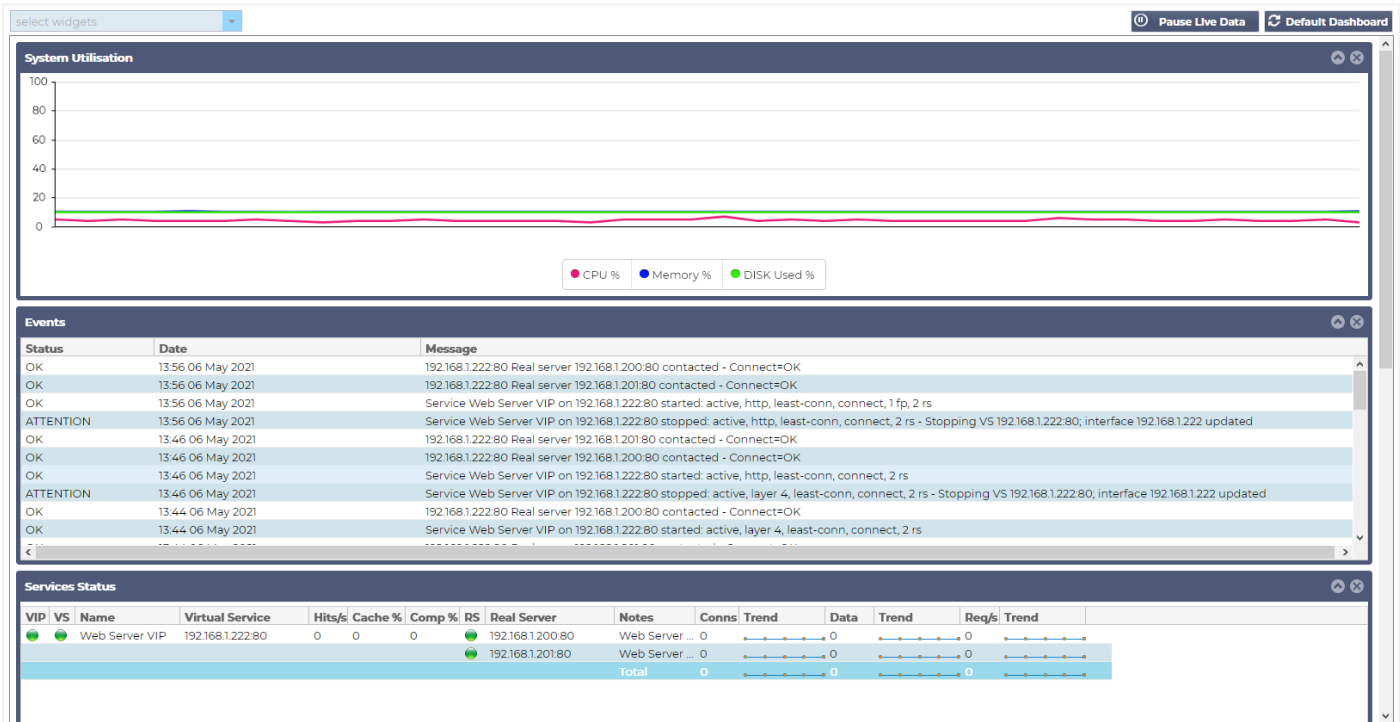
Dashboard Usage

There are four elements to the Dashboard U: The Widgets Menu, the Pause/Play Button, and the Default Dashboard button.

The Widgets Menu

The Widgets menu located at the top left of the dashboard allows you to select and add any standard or customized widgets you have defined. To use this, select the widget from the drop-down.

Pause Live Data Button
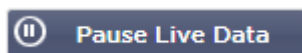
This button allows you to select whether the ADC should update the dashboard in real-time. Once paused, no dashboard widget will be updated, allowing you to examine the content at your leisure. The button changes state to display Play Live Data once a pause is initiated.
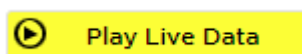
When you have finished, simply click the Play Live Data button to restart the data gathering and update the Dashboard.

Default Dashboard Button
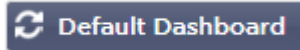
It may come to be that you wish to reset the Dashboard layout to the default. In such a case, press the Default Dashboard button. Once clicked, all changes made to the Dashboard will be lost.

Resizing, minimizing, re-ordering, and removing widgets

Resizing a Widget

You can resize a widget very easily. Click and hold on the widget's title bar and drag it to the left or right side of the Dashboard area. You will see a dotted rectangle that represents the new widget size. Drop the widget into the rectangle and let go of the mouse button. If you wish to drop a resized widget alongside a previously resized widget, you will see the rectangle appear adjacent to the widget you want to drop beside.

Minimizing a Widget

You can minimize widgets at any time by clicking the title bar of the widget. This action will minimize the widget and display only the title bar.

Moving Widget Order

To move a widget, you can drag and drop by click and hold down on the title bar and moving the mouse.

Removing a Widget

You can remove a by clicking the ⊗ icon in the widget title bar.

History

The History option, selectable from the navigator, allows the administrator to examine the historical performance of the ADC. Historical views can be generated for Virtual Services, Real Servers, and System.

It also allows you to see load balancing in action and helps catch any errors or patterns that need investigating. Note that you must enable historical logging in System > History to make use of this feature.

Viewing Graphical Data

Data Set

To view the historical data in graphical format, please proceed as follows:

The first step is to choose the database and period relevant to the information you wish to view. The period that you can select from the Last drop-down is Minute, Hour, Day, Week, Month, and Year.

Database	Description
System	Selecting this database will allow you to see CPU, memory, and disk drive space over time
Virtual Services	Selecting this database will allow you to choose all of the virtual services in the database from when you started logging data. You will see a list of Virtual Services from which you can select one.
Real Services	Selecting this database will allow you to choose all the Real Servers in the database from when you started logging the data. You will see a list of Real Servers from which you can select one.

Download W3C Logs

W3C logging is enabled from the System > Logging section. A W3C log is an access log for Web servers in which text files are generated containing data about each access request, including the source Internet Protocol (IP) address, the HTTP version, the browser type, the referrer page, and the timestamp. W3C logs can become very large depending on the amount of data and the category of logging being recorded.

From the W3C section, you can select the log you need and then view or download it.

View Button

The View button allows you to view the chosen log within the text editor window, such as Notepad.

Download Button

This button allows you to download the log to your local storage for viewing later.

The Cog Icon

Clicking this icon takes you to the W3C Log Settings section located in System > Logging. We will discuss this in detail in the Logging section of the guide.

Statistics

The Statistics section of the ADC is a much-used area by system administrators who want to ensure that the ADC performance is on par with their expectations.

Compression

The whole purpose of the ADC is to monitor data and direct it to Real Servers configured to receive it. The compression feature is provided in the ADC to increase the ADC's performance. There will be times when administrators will wish to test and check the ADC's data compression information; this data provided by the Compression panel within Statistics.

Content Compression to Date

The data shown in this section details the level of compression achieved by the ADC on compressible content. A value of 60-80% is what we would term as typical

Overall Compression to Date

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)

The values provided in this section report how much compression the ADC has achieved on all content. A typical percentage for this depends on how many pre-compressed images are contained in your services. The more the number of images, the smaller the overall compression percentage is likely to be.

Total Input/Output

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

The Total Input/Output figures represent the amount of raw data traversed into and out of the ADC. The unit of measurement will change as the size grows from kbps to Mbps to Gbps.

Hits and Connections

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

The Hits and Connections section contains the overall statistics for hits and transactions that pass through the ADC. So what do hits and connections mean?

- A Hit is defined as a Layer 7 transaction. Typically used for web servers, this is a GET request for an object such as an image.
- A Connection is defined as a Layer 4 TCP connection. Many transactions can occur over 1 TCP connection.

Overall Hits Counted

The figures within this section show the cumulative number of non-cached hits since the last reset. On the right-hand side, the figure will show the current number of hits per second.

Total Connections

The Total Connections value represents the cumulative number of TCP connections since the last reset. The figure in the second column indicates the TCP connections made per second to the ADC. The number in the right-side column is the number of TCP connections per second made to the Real Servers. Example 6/8 connections/sec. We have 6 TCP connections per second to the Virtual Service and 6 TCP connections per second to the Real Servers in the example shown.

Peak Connections

The peak Connections value represents the maximum number of TCP connections made to the ADC. The number on the rightmost column indicates the current number of active TCP connections.

Caching

As you will recall, the ADC is equipped with both compression and caching. This section shows the overall statistics related to caching when applied to a channel. If caching has not been applied to a channel and configured correctly, you will see 0 cache contents.

From Cache

Hits: The first column gives the total number of transactions served from the ADC cache since the last reset. A percentage of the total transactions is also provided.

Bytes: The second column gives the total amount of data in Kilobytes served from the ADC cache. A percentage of total data is also provided.

From Server

Hits: Column 1 gives the total number of transactions served from the Real Servers since the last reset. A percentage of total transactions is also provided.

Bytes: The second column gives the total amount of data in Kilobytes served from the Real Servers. A percentage of total data is also provided.

Cache Contents

Hits: This number gives the total number of objects contained in the ADC cache.

Bytes: The first number gives the overall size in Megabytes of the ADC cached objects. A percentage of the maximum cache size is also provided.

Session Persistence

The Session Persistence section delivers information for several parameters.

Field	Description
Total current sessions	This shows how many persistence sessions are in progress - updated each minute
% Used (of max)	This shows how much usage there is of the total space allowed for session information
New session this min	This shows, within the last minute, how many new persistence sessions were added
Revalidate this min	This shows, within the last minute, how many existing persistence sessions were revalidated by more traffic
Expired sessions this min	This shows, within the last minute, how many existing persistence sessions expired due to no further traffic within the timeout

Hardware

Whether you are using the ADC in a virtual environment or within hardware, this section will provide you with valuable information on the appliance's performance.

Disk Usage

The value provided in column 2 gives the percentage of disk space currently used and includes information on log files and cache data, which is periodically stored on the storage.

Memory Usage

The second column gives the percentage of memory currently used. The more significant number in brackets is the total amount of memory allocated to the ADC. It is recommended that the ADC be allocated a minimum of 2GB of RAM.

CPU Usage

One of the critical values provided is the percentage of CPU currently used by ADC. It is natural for this to fluctuate.

Status

The View > Status page displays the live traffic traversing through the ADC for the virtual Services you have defined. It also shows the number of connections and data to each Real Server so you can experience the load balancing in real-time.

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	

VIP Column

The color of the light indicates the state of the Virtual IP address associated with one or many virtual services.

Status	Description
🟢	Online
🔵	Failover-Standby. This virtual service is hot-standby
🟡	Indicates a "passive" is holding off for an "active"
🔴	Offline. Real servers are unreachable, or no Real Servers are enabled
⚪	Finding status
🟣	Not licensed or licensed Virtual IPs exceeded

VS Status Column

The color of the light indicates the state of the Virtual Service.

Status	Description
●	Online
●	Failover-Standby. This virtual service is hot-standby
●	Indicates a "passive" is holding off for an "active"
●	Service Needs attention. This status indication may result from a Real Server failing a health monitor or has been changed manually to Offline. Traffic will continue to flow but with reduced Real Server capacity.
●	Offline. Real servers are unreachable, or no Real Servers are enabled
●	Finding status
●	Not licensed or licensed Virtual IPs exceeded

Name

The name of the Virtual Service

Virtual Service (VIP)

The Virtual IP address and port for the service and the address users or applications will use.

Hit/Sec

Layer 7 transactions per second on the client-side.

Cache%

The figure provided here represents the percentage of objects that have been served from the ADC's RAM Cache.

Compression%

This figure represents the percentage of objects that have been compressed between the client and the ADC.

RS Status (Remote Server)

The table below outlines the meaning of the status of Real Servers linked to the VIP.

Status	Description
●	Connected
●	Not monitored
●	Drain or Offline
●	Standby
●	Not Connected
●	Finding status
●	Not licensed or licensed Virtual IPs exceeded

Real Server

The Real Server IP address and port.

Notes

This value can be any helpful notes to make others understand the purpose of the entry.

Conns (Connections)

Representing the number of connections to each Real Server allows you to see the load balancing in action. Very helpful to verify that your load balancing policy is working correctly.

Data

The value in this column shows the amount of data being sent to each Real Server.

Req/Sec (Requests per second)

The number of requests per second sent to each Real Server.

System

The System segment of the ADC's user interface permits you to access and control all system-wide aspects of the ADC.

Clustering

The ADC can be used as a single stand-alone device, and it will work perfectly well doing that. However, when one considers that the purpose of the ADC is to load balance sets of servers, the need to cluster the ADC itself becomes apparent. The ADC's easily navigable UI design makes the configuration of the clustering system straightforward.

The System > Clustering page is where you will configure the high availability of your ADC appliances. This section is organized into several sections.

Important Note

- There is no requirement for a dedicated cable between the ADC pair to maintain a high availability heartbeat.
- The heartbeat takes place on the same network as the Virtual Service that requires high availability to be put in place.
- There is no stateful fail-over between the ADC appliances.
- When high availability is enabled on two or more ADC's, each box will broadcast via UDP the Virtual Services it is configured to provide.
- High availability fail-over uses unicast messaging and Gratuitous ARP to inform the new Active load balancer switches.

Role

There are three cluster roles available when you configure the ADC for high availability.

Cluster

- By default, a new ADC will power on using the Cluster role. In this role, each cluster member will have the same "working configuration," and as such, only one ADC in the Cluster will be Active at any one time.
- A "working configuration" means all configuration parameters, except items that need to be unique such as the management IP address, ALB Name, network settings, interface details, and so on.
- The ADC in priority 1, the topmost position, of the Cluster Members box is the Cluster Owner and the Active load balancer, while all other ADC's are Passive members.
- You can edit any ADC in the Cluster, and the changes will be synchronized to all Cluster members.
- When you remove an ADC from the Cluster, all Virtual Services will be deleted from that ADC.
- You cannot remove the last member of the Cluster to Unclaimed Devices. To remove the last member, please change the role to Manual or Stand-alone.
- The following objects are not synchronized:
    - Manual Date & Time section – (NTP Section is synchronized)
    - Failover Latency (ms)
    - Hardware section
    - Appliance section
    - Network section

Failure of the Cluster Owner

- When a cluster owner fails, one of the remaining members will automatically take over and carry on load balancing the traffic.
- When the cluster owner returns, it will resume load balancing traffic and take over the owner role.
- Let's assume the Owner has failed, and a Member has taken over the load balancing. If you would like that Member that has taken over load balancing traffic to become the new owner, highlight the member and click the up arrow to move it to the Priority 1 position.
- If you edit one of the remaining cluster members and the owner is down, the edited member will automatically promote itself to the owner without loss of traffic

Changing role from Cluster role to Manual role

- If you wish to change the role from Cluster to Manual, click the radio button next to the Manual role option

- After you click the radio button, you will see the following message:

- Click the OK button

- Check the Virtual Services section. You will find that the Primary column now shows an unticked box.
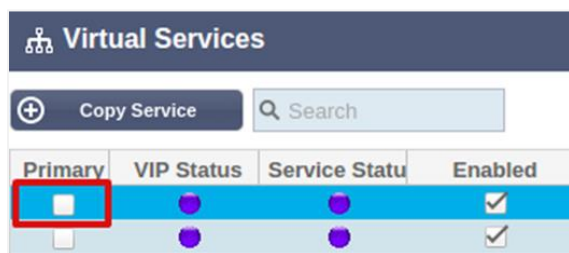
- It is a safety feature and means that if you have another ADC with the same Virtual Services, then there will be no interruption to traffic flow.

Changing role from Cluster to Stand-alone

- If you wish to change the role from Cluster to Stand-alone, click on the radio button next to the Standalone option.
- You will be prompted with the following message:
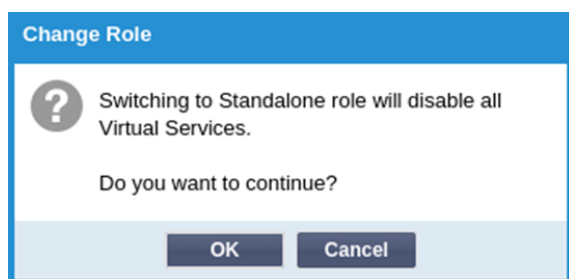
- Click OK to change roles.
- Check your Virtual Services. You will see that the Primary column change name to Stand-alone
- You will also see that all the Virtual Services are disabled (un-ticked) for safety reasons.
- Once you are confident that no other ADC on the same network has duplicate Virtual Services, you can enable each one in turn.

Manual Role

An ADC in the Manual role will work with other ADC's in the Manual role to provide high availability. The main advantage over the Cluster role is the ability to set which ADC is Active for a Virtual IP. The disadvantage is that there is no configuration synchronization between the ADC's. Any changes must be replicated manually on each box via the GUI, or for lots of changes, you can create a jetPACK from one ADC and send this to the other.

- To make a Virtual IP address "Active", tick the checkbox in the primary column (IP Services page)
- To make a Virtual IP address "Passive", leave the check-box blank in the primary column (IP Services page)
- In the event, an Active service fails over to the Passive:
  - If both Primary Columns are ticked, then an election process takes place, and the lowest MAC address will be Active
  - If both are un-ticked, then the same election process takes place. In addition, if both are un-ticked, there is no automatic fallback to the original Active ADC

Stand-alone Role

An ADC in the Stand-alone role will not communicate with any other ADC regarding its services, and therefore all Virtual Services will remain in the Green status and connected. You must ensure that all Virtual Services have unique IP addresses, or there will be a clash on your network.

Settings

In the Settings section, you can set the Failover Latency in milliseconds, the time that a Passive ADC will wait before taking over the Virtual Services after the Active ADC has failed.

We recommend setting this to 10000ms or 10 seconds, but you may decrease or increase this value to suit your network and requirements. Acceptable values fall between 1500ms and 20000ms. If you experience instability in the cluster at a lower latency, you should increase this value.

Management

In this section, you can add and remove cluster members while also changing the priority of an ADC in the cluster. The section consists of two panels and a set of arrow keys in between. The area on the left is the Unclaimed Devices, while the rightmost area is the Cluster itself.

Adding an ADC to the cluster

- Before adding the ADC to the cluster, you must ensure that all the ADC appliances have been provided with a unique name set in the System > Network section.
- You should see the ADC as Priority 1 with Status green and its name under the Cluster Members column in the management section. This ADC is the default primary appliance.
- All the other available ADC's will show up in the Unclaimed Devices window within the management section. An Unclaimed Device is the ADC that has been assigned in the Cluster Role but has no Virtual Services configured.
- Highlight the ADC from the Unclaimed Devices window and click the right arrow button.
- You will now see the following message:

- Click OK to promote the ADC to the cluster.
- Your ADC should now be showing as Priority 2 in the cluster members list.

Removing a cluster member

- Highlight the Cluster Member you wish to remove from the cluster.
- Click the left arrow button.

- You will be presented with a confirmation request.
- Click OK to confirm.
- Your ADC will be removed and be shown on the Unclaimed Devices side.

Changing the priority of an ADC

There may be times when you wish to change the priority of an ADC within the members' list.

- The ADC at the top of the Cluster Members list is given Priority 1 and is the Active ADC for all Virtual Services
- The ADC that is second in the list is given Priority 2 and is the Passive ADC for all Virtual Services
- To change which the ADC is Active simply highlight the ADC and click the up arrow until it is at the top of the list
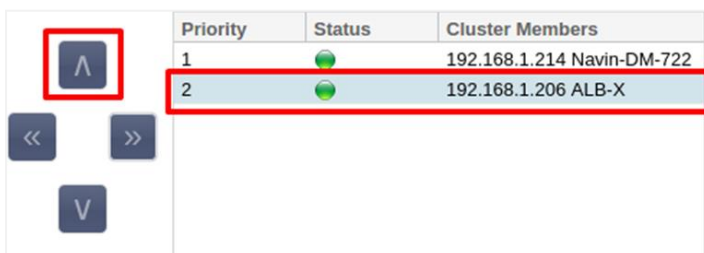
Date and Time

The date and time section allows the setting of the ADC's date/time characteristics, including the timezone in which the ADC is located. Together with the timezone, the date and time play a vital part in the cryptographic processes associated with SSL encryption.

Manual Date and Time

Time Zone

The value you set in this field represents the timezone in which the ADC is located.

- Click on the drop-down box for the Time Zone and start typing your location.
  For example London
- As you begin typing, the ADC will automatically display locations containing the letter L.
- Continue typing 'Lon,' and so on – the locations listed will be narrowed down to ones containing 'Lon.'
- If you are in, say, London, then choose Europe/London to set your location

If the Date and Time is still incorrect after the above change, please change the date manually

Set Date and Time

This setting represents the actual date and time.

- Choose the correct date from the first drop-down or,
  alternatively, you can type the date in the following format DD/MM/YYYY
- Add in the time in the following format hh: mm: ss, for example, 06:00:10 for 6 am and 10 seconds.
- Once you have entered it correctly, please click Update to apply.
- You should then see the new Date and Time in bold characters.

Synchronize Date and Time (UTC)

You can use NTP servers to synchronize your date and time accurately. The NTP servers are located globally, and you may also have your own internal NTP server when your infrastructure has limitations on external access.

Time Server URL

Enter a valid IP address or fully qualified domain name (FQDN) for the NTP server. If the server is a globally located server on the Internet, we recommend using an FQDN.

Update at [hh:mm]

Select the scheduled time at which you would like the ADC to synchronize with the NTP server.

Update Period [hours]:

Select how often you would like synchronization to occur.

NTP Type:

- Public SNTP V4 – This is the current and preferred method when synchronizing with an NTP server. **RFC 5905**
- NTP v1 Over TCP – Legacy NTP version over TCP. **RFC 1059**
- NTP v1 Over UDP – Legacy NTP version over UDP. **RFC 1059**
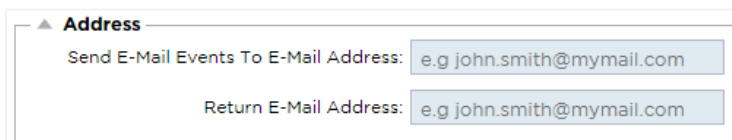
Note: Please note that synchronization is in UTC only. If you wish to set a local time, this can only be done manually. This limitation will be changed in later versions to enable the ability to select a time zone.

Email Events

The ADC is a critical appliance, and like any essential system, it is equipped with the ability to inform the systems administration of any issues that may require attention.

The System > Email Events page allows you to configure an email server connection and send notifications to system admins. The page is organized into the sections below.

Address

Send to Email Events to Email Addresses
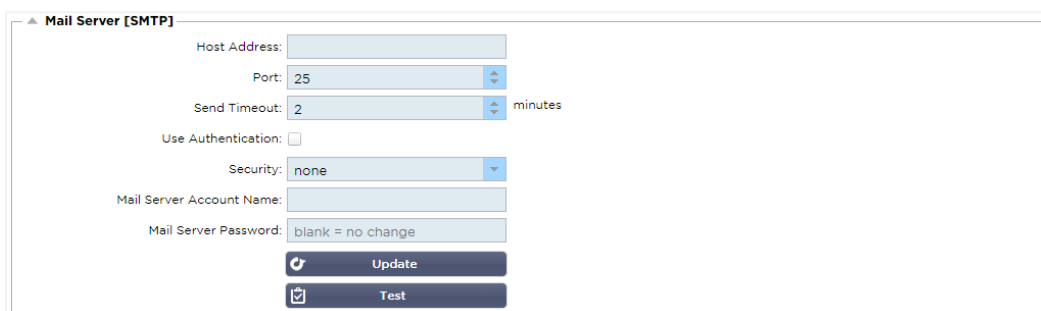
Add a valid email address to send the alerts, notifications, and events to. Example support@domain.com. You can also add multiple email addresses using a comma separator.

Return Email Address:

Add in an email address that will appear in the inbox. Example adc@domain.com.

Mail Server (SMTP)

In this section, you must add the SMTP server details to be used to send the emails. Please ensure that the email address you use for sending is authorized to do so.

Host address

Add in the IP address of your SMTP server.

Port

Add in the Port of your SMTP server. Default Port for SMTP is 25 or 587 if you use SSL.

Send Timeout

Add in an SMTP timeout. The default is set to 2 minutes.

Use Authentication

Tick the box if your SMTP server requires authentication.

Security

- None
- The default setting is none.
- SSL - Use this setting if your SMTP server requires Secure Sockets Layer authentication.
- TLS - Use this setting if your SMTP server requires Transport Layer Security authentication.

Main Server Account Name

Add in the username required for authentication.

Mail Server Password

Add in the password required for authentication.

Notifications and Alerts

There are several types of event notifications that the ADC will send to persons configured to receive them. You can tick and enable the notifications and alerts that should be sent out. Notifications occur when Real Servers are contacted or channels started. Alerts occur when Real Servers cannot be contacted, or channels stop working.

IP Service

The IP Service notice will inform you when any Virtual IP address is online or has stopped working. This action is carried out for all Virtual services that belong to the VIP.

Virtual Service

Informs the recipient a Virtual Service is online or has stopped working.

Real Server

When a Real Sever and Port is connected or is not contactable, the ADC will send the Real Server notice.

flightPATH

This notice is an email sent out when a condition has been met, and there is an action configured instructing the ADC to email the event.

Group Notifications

Tick to group notifications together. With this ticked, all the notifications and alerts will be aggregated into one email.

Group Mail Description

Specify the relevant subject matter for the group notice email.

Group Send interval

Stipulate the amount of time you wish to wait before sending a group notification email. The minimum time is 2 minutes.

Warnings

There are two types of warning emails, and neither should be ignored.

Disk Space

Set the percentage of free disk space before which the warning is sent. When this is reached, you will be emailed.

Licence Expiry

This setting allows you to enable or disable the license expiration warning email sent to the system admin. When this is reached, you will be emailed.

System History

In the System section, there is the System History option, allowing the delivery of historical data for elements such as CPU, memory, requests per second, and other features. Once enabled, you can view the results in graphical form via the View > History page. This page will also allow you to backup or restore your history files to the local ADC.

Collect Data

- To enable the collection of data, please tick the checkbox.
- Next, set the time interval at which you wish the ADC to collect the data. This time value can range between 1-60 seconds.

Maintenance

This section will be greyed out if you have enabled historical logging. Please untick the Enabled checkbox in the Collect Data section and click Update to allow the maintenance of the historical logs.

Backup

Give your backup a descriptive name. Click Backup to backup all the files to the ADC

Delete

Select a backup file from the drop-down list. Click Delete to remove the backup file from the ADC

Restore

Select a previously stored backup file. Click Restore to populate the data from this backup file.

License

The ADC is licensed for use either using one of the following models, which depends on your purchase parameters and customer type.

License Type	Description
Perpetual	You, the customer, have the right to use the ADC and other software in perpetuity. It does not preclude you from having to purchase support to receive assistance and updates.
SaaS	SaaS or Software-as-a-Service means you essentially rent the software on an ongoing or pay-as-you-go basis. In this model, you pay an annual rental for the software. You do not have perpetual rights to use the software.
MSP	Managed Service Providers can offer the ADC as a service and purchase the license on a per-VIP basis, charged and paid annually.

License Details

Each license includes specific details pertinent to the person or organization purchasing it.

License ID

This license ID is directly linked to the Machine ID and other details specific to your purchase and ADC. This information is essential and is required when you wish to retrieve updates and other items from the App Store.

Machine ID

The Machine ID is generated using the eth0 IP address of a virtual ADC appliance and the MAC ID of a hardware-based ADC. If you change the IP address of a virtual ADC appliance, the license will no longer be valid. You will have contact support for assistance. We recommend that your virtual ADC appliance(s) have fixed IP addresses with instructions not to change them. Technical support is available by raising a ticket at HTTPs://edgenexus.io.

Note: You mustn't change the IP address or the MAC ID of your ADC appliances. If you are in a virtualized framework, then please fix the MAC ID and IP Address.

Issued To

This value contains the purchaser's name associated with the ADC's Machine ID.

Contact Person

This value contains the contact person to be contacted at the customer's company associated with the Machine ID

Date Issues

The date on which the license was issued

Name

This value shows the descriptive name for the ADC Appliance that you have provided.

Facilities

The facilities section provides you with information on which functions within the ADC have been licensed for use and the license validity. Also displayed is the throughput that has been licensed for the ADC and the number of Real Servers. This information is dependant on the license you have purchased.

Install License

- Installing a new license is very simple. When you receive your new or replacement license from Edgenexus, it will be sent in the form of a text file. You can open the file and then copy and paste the content into the Paste License field.
- You can also upload it to the ADC if copy/paste is not an option for you.
- Once you have done this, please click the update button
- The license is now installed.

License Service Information

Clicking the License Service Information button will display all the information on the license. This function can be used for sending the details to support personnel.

Logging

The System > Logging page allows you to set the W3C logging levels and specify the remote server to which logs will be automatically exported. The page is organized into the four sections below.

W3C Logging Details

Enabling W3C logging will cause the ADC to start recording a W3C compatible log file. A W3C log is an access log for Web servers in which text files are generated containing data about each access request, including the source Internet Protocol (IP) address, the HTTP version, the browser type, the referrer page, and the time stamp. The format was developed by the World Wide Web Consortium (W3C), an organization that promotes standards for the evolution of the Web. The file is in ASCII text, with space-delimited columns. The file holds comment lines beginning with the # character. One of these comment lines is a line indicating the fields (providing column names) so that data can be mined. There are separate files for HTTP and FTP protocols.

W3C Logging Levels

There are different logging levels available, and depending on the service type, the data provided varies.

The table below describes logging levels for W3C HTTP.

Value	Description
None	W3C logging is off.
Brief	The fields present are: #Fields: time c-ip c-port s-ip method uri x-c-version x-r-version sc-status cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x- round-trip-time cs(User-Agent) x-sc(Content-Type).
Full	This is a more processor-compatible format with separate date and time fields. See the fields summary below for information on what the fields mean. The fields present are: #Fields: date time c-ip c-port cs-username s-ip s-port cs-method cs-uri-stem cs-ur- -query sc-status cs(User-Agent) referer x-c-version x-r-version cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x-roun-trip-time x-sc(Content-Type).
Site	This format is very similar to "Full" but has an additional field. See the summary of the fields below for information on what the fields mean. The fields present are: #Fields: date time x-mil c-ip c-port cs-username s-ip s-port cs-host cs-method cs-uri-stem cs-ur--query sc-status cs(User-Agent) referer x-c-version x-r-version cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x-round--trip-time x-sc(Content-Type).
Diagnostic	This format is filled with all sorts of information relevant to development and support staff. See the fields summary below for information on what the fields mean. The fields present are: #Fields: date time c-ip c-port cs-username s-ip s-port x-xff x-xffcustom cs-host x-r-ip x-r-port cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent) referer x-c-version x-r-version cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x-round-trip-time x-trip-times(new,rcon,rqf,rql,tqf,tql,rsf,rsl,tsf,tsl,dis,log) x-closed-by x- compress-action x-sc(Content-Type) x-cache-action X-finish

The table below describes logging levels for W3C FTP.

Value	Description
Brief	#Fields: date time c-ip c-port s-ip s-port r-ip r-port cs-method cs-param sc-status sc-param sr-method sr-param rs-status rs-param
Full	#Fields: date time c-ip c-port s-ip s-port r-ip r-port cs-method cs-param cs-bytes sc-status sc-param sc-bytes sr-method sr-param sr-bytes rs-status rs-param rs-bytes
Diagnostic	#Fields: date time c-ip c-port s-ip s-port r-ip r-port cs-method cs-param cs-bytes sc-status sc-param sc-bytes sr-method sr-param sr-bytes rs-status rs-param rs-bytes

Include W3C Logging

This option allows you to set what ADC information should be included in the W3C logs.

Value	Description
Client's Network Address and Port	The value shown here displays the actual client IP address along with the port.
Client's Network Address	This option will include and only show the actual client IP address.
Forwarded-For Address and Port	This option will show the details held in the XFF header, including the address and port.
Forwarded-For Address	This option will show the details held in the XFF header, including the address only.

Include Security Information

This menu consists of two options:

Value	Description
On	This setting is global. When set to on, the username will be appended to W3C log when any Virtual Service is using Authentication and has W3C logging enabled.
Off	This will turn off the ability to log the username to the W3C log on a global level.

Syslog Server

This section allows you to set the level of message logging performed to the SYSLOG server. The options available are as follows.

Error
Warning
Notice
Info

Remote Syslog Server

In this section, you can configure two external Syslog servers to send all system logs.

- Add the IP address of your Syslog server
- Add the Port
- Choose whether you wish to use TCP or UDP
- Tick the Enabled checkbox to begin logging
- Click Update

Remote Log Storage

All W3C logs are stored in compressed form onto the ADC every hour. The oldest files will be deleted when 30% of disk space is remaining. Should you wish to export these to a remote server for safekeeping, you can configure this using an SMB share. Please note that the W3C log will not transfer to the remote location until the file has been completed and compressed. As the logs are written every hour, this could take up to two hours in a Virtual Machine appliance and five hours for a hardware appliance.

Col1	Col2
Remote Log Storage	Tick the box to enable remote log storage
IP Address	Specify the IP address of your SMB server. This should be in dotted decimal notation. Example: 10.1.1.23
Share Name	Specify the share name on the SMB server. Example: w3c.
Directory	Specify the directory on the SMB server. Example: /log.
Username	Specify the username for the SMB share.
Password	Specify the password for the SMB share

We will include a test button in future releases to provide some feedback that your settings are correct.
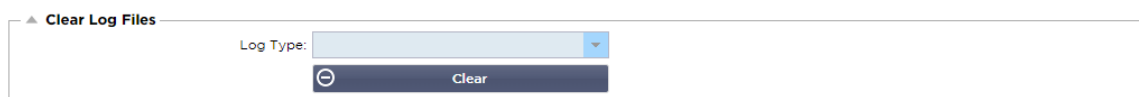
Field Summary

Condition	Description
Date	Not localised = always YYYY-MM-DD (GMT/UTC)
Time	Not localised = HH:MM:SS or HH:MM:SS.ZZZ (GMT/UTC) * Note-unfortunately this has two formats (Site
	has no .ZZZ milliseconds)
x-mil	Site format only = millisecond of time stamp
c-ip	Client IP as best can be derived from network or X-Forwarded-For header
c-port	Client port as best can be derived from network or X-Forwarded-For header
cs-username	Client's user-name request field
s-ip	ALB's listening port
s-port	ALB's listening VIP
x-xff	Value of X-Forwarded-For header

x-xffcustom	Value of configured-named X-Forwarded-For type request header
cs-host	Host name in the request
x-r-ip	IP address of Real Server used
x-r-port	Port of Real Server used
cs-method	HTTP request method * except Brief format
method	* Only brief format uses this name for cs-method
cs-uri-stem	Path of the requested resource * except Brief format
cs-uri-query	Query for the requested resource * except Brief format
uri	* brief format logs a combined path and query-string
sc-status	HTTP response code
cs(User-Agent)	Browser's User-Agent string (as sent by client)
referer	Referring page (as sent by client)
x-c-version	Client's request HTTP version
x-r-version	Content-Server's response HTTP version
cs-bytes	Bytes from client, in the request
sr-bytes	Bytes forwarded to Real Server, in the request
rs-bytes	Bytes from Real Server, in the response
sc-bytes	Bytes sent to client, in the response
x-percent	Compression percentage * = 100 * (1 – output / input) including headers
time-taken	How long the Real Server took in seconds
x-trip-times new pcon	millisecond from connect to posting in "newbie list" millisecond from connect to placing the connection to the Real Server
acon	millisecond from connect to finishing placing the connection to the Real Server
rcon	millisecond from connect to establishing real-server connection
rqf	millisecond from connect to receiving the first byte of request from the client
rql	millisecond from connect to receiving the last byte of request from the client
tqf	millisecond from connect to sending the first byte of request to the Real Server
tql	millisecond from connect to sending the last byte of request to the Real Server
rsf	millisecond from connect to receiving the first byte of response from the Real Server
rsl	millisecond from connect to receiving the last byte of response from the Real Server
tsf	millisecond from connect to sending the first byte of response to the client
tsl	millisecond from connect to sending the last byte of response to the client
dis	millisecond from connect to disconnect (both sides – last one to disconnect)
log	millisecond from connect to this log record usually followed by (Load-balance policy and reasoning)
x-round-trip-time	How long ALB took in seconds
x-closed-by	What action caused the connection to be closed (or kept open)
x-compress-action	How compression was carried out, or prevented
x-sc(Content-Type)	Content-Type of response

x-cache-action	How caching responded, or was prevented
x-finish	Trigger that caused this log row

Clear Log Files
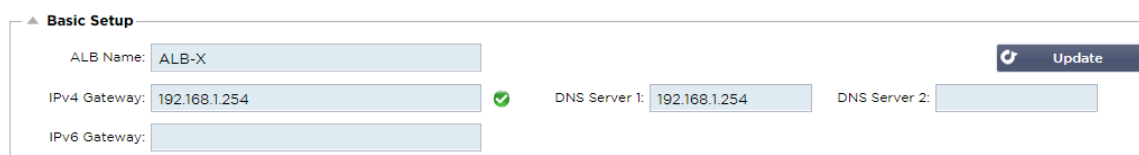
This feature allows you to clear the log files from the ADC. You can select the type of log you wish to delete from the drop-down menu and then click the Clear button.

Network

The Network section within the Library allows the configuration of the ADC's network interfaces and their behavior.

Basic Setup
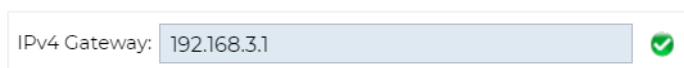
ALB Name

Specify a name for your ADC appliance. Please note that this cannot be changed if there is more than one member in the cluster. Please see the section on Clustering.

IPv4 Gateway

Specify the IPv4 Gateway address. This address will need to be in the same subnet as an existing adapter. If you add in Gateway incorrectly, you will see a White Cross in a red circle. When you add a correct gateway, you will see a green success banner at the bottom of the page and a white tick in a green circle next to the IP address.

IPv6 Gateway

Specify the IPv6 Gateway address. This address will need to be in the same subnet as an existing adapter. If you add in Gateway incorrectly, you will see a White Cross in a red circle. When you add a correct gateway, you will see a green success banner at the bottom of the page and a white tick in a green circle next to the IP address.

DNS Server 1 & DNS Server 2

Add in the IPv4 address of your first and second (optional) DNS server.

Adapter Details

This section of the Network panel shows the network interfaces that are installed in your ADC appliance. You can add and remove adapters as needed.

Column	Description
Adapter	This column displays the physical adapters installed on your appliance. Choose an adapter from the list of available adapters by clicking on it – a double-click will place the listing line into edit mode.
VLAN	Double click to add the VLAN ID for the adapter. A VLAN is a Virtual Local Area Network which creates a distinct broadcast domain. A VLAN has the same attributes as physical LAN but it allows for end stations to be grouped together more easily if they are not on the same network switch
IP Address	Double click to add the IP address associated with the adapter interface. You can add multiple IP addresses to the same interface. This should be an IPv4 32-bit number in quad dotted decimal notation. Example 192.168.101.2
Subnet Mask	Double click to add the subnet mask assigned to the adapter interface. This should be an IPv4 32-bit number in quad dotted decimal notation. Example 255.255.255.0
Gateway	Add a gateway for the interface. When this is added the ADC will set-up a simple policy that will allow connections initiated from this interface to be returned via this interface to the gateway router specified. This allows the ADC to be installed in more complex networking environments without the trouble of manually configuring complex policy based routing.
Description	Double click to add a description for your adapter. Example Public Interface.
	Note: The ADC will automatically name the first interface Green Side, the second interface Red Side and the third interface Side 3 etc.
	Please feel free to change these naming conventions to your own choice.
Web Console	Double click the column then tick the box to assign the interface as the management address for the Graphical User Interface Web Console. Please be very careful when changing the interface that Web Console will listen on. You will need to have the correct routing set up or be in the same subnet as the new interface in order to reach the Web Console after the change. The only way to change this back is to access the command line and issue the set greenside command. This will delete all interfaces except for eth0.

Interfaces

The Interfaces section within the Network panel allows the configuration of certain elements pertaining to the network interface. You can also remove a network interface from the listing by clicking the Remove button. When using a virtual appliance, the interfaces you see here are limited by the underlying virtualization framework.

Column	Description
ETH Type	This value indicates the internal OS reference to the network interface. This field cannot be customized. Values begin with ETH0 and continue in sequence depending on the number of network interfaces.
Status	This graphical indication shows the current status of the network interface. A Green status shows that the interface is connected and up. Other status indicators are shown below. **Adapter UP** Adapter Down Adapter Unplugged Adapter Missing
Speed	By default, this value is set to auto-negotiate the speed. But you can change the network speed of the interface to any value available in the drop-down (10/100/1000/AUTO).
Duplex	The value of this field is customizable, and you can choose between Auto (default), Full-Duplex, and Half-Duplex.
Bonding	You can choose one of the bonding types that you have defined. See the section on Bonding for more details.

Bonding

Many names are used to title network interface bonding: Port Trunking, Channel Bonding, Link Aggregation, NIC teaming, and others. Bonding combines or aggregates multiple network connections into a single channel bonded interface. Bonding allows two or more network interfaces to act as one, increase throughput, and provide redundancy or failover.

The ADC's kernel has a built-in Bonding driver for aggregating multiple physical network interfaces into a single logical interface (for example, aggregating eth0 and eth1 into bond0). For each bonded interface, you can define the mode and the link monitoring options. There are seven different mode options, each providing specific load balancing and fault tolerance characteristics. These are shown in the image below.

NOTE: BONDING CAN ONLY BE CONFIGURED FOR HARDWARE-BASED ADC APPLIANCES.
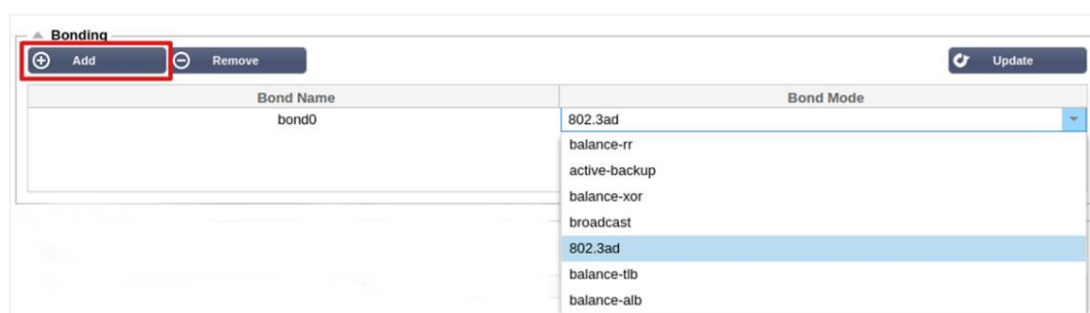
Creating a Bonding profile

- Click on Add button to add a new Bond
- Provide a name for the bonding configuration
- Choose which bonding mode you wish to use

Then from the Interfaces section, select the Bonding mode you wish to use from the Bond drop-down field for the network interface.

In the example below, eth0, eth1, and eth2 are now part of bond0. While Eth0 remains on its own as the management interface.

Bonding Modes

Bonding Mode	Description
balance-rr:	Packets are sequentially transmitted/received through each interface one by one.
active-backup:	In this mode, one interface will be active, and the second interface will be on standby. This secondary interface only becomes active if the active connection on the first interface fails.
balance-xor:	Transmits based on source MAC address XOR'd with destination MAC address. This option selects the same slave for each destination Mac address.
broadcast:	This mode will transmit all data on all slave interfaces.
802.3ad:	Creates aggregation groups that share the same speed and duplex settings and utilizes all the slaves in the active aggregator following the 802.3ad specification.
balance-tlb:	The Adaptive transmit load balancing bonding mode: Provides channel bonding that does not require any special switch support. The outgoing traffic is distributed according to the current load (computed relative to the speed) on each slave. The current slave receives incoming traffic. If the receiving slave fails, another slave takes over the MAC address of the failed receiving slave.
balance-alb:	The Adaptive load balancing bonding mode: also includes balance-tlb plus receive load balancing (rlb) for IPV4 traffic and does not require any special switch support. The receive load balancing is achieved by ARP negotiation. The bonding driver intercepts the ARP Replies sent by the local system on their way out and overwrites the source hardware address with the unique hardware address of one of the slaves in the bond, such that different peers use different hardware addresses for the server.

Static Route

There will be times when you need to create static routes for specific subnets within your network. The ADC provides you with the ability to do this using the Static Routes module.

Adding a Static Route

- Click the Add Route button
- Fill in the field using the details in the table below as guidance.
- Click the Update button when done.

Field	Description
Destination	Enter the destination network address in decimal dotted notation. Example 123.123.123.5
Gateway	Enter the gateway IPv4 address in decimal dotted notation. Example 10.4.8.1
Mask	Enter the destination subnet mask in decimal dotted notation. Example 255.255.255.0

Adapter	Enter the adapter that the gateway can be reached on. Example eth1.
Active	A green tick box will indicate that the gateway can be reached. A red cross will indicate that the gateway cannot be reached on that interface. Please make sure you have set up an interface and IP address on the same network as the gateway

Static Route Details

This section will provide information about all the routes configured on the ADC.

Advanced Network Settings

What is Nagle?

Nagle's algorithm improves the efficiency of TCP/IP networks by reducing the number of packets that need to be sent over the network. See WIKIPEDIA ARTICLE ON NAGLE

Server Nagle

Tick this box to enable the Server Nagle setting. The Server Nagle is a means of improving the efficiency of TCP/IP networks by reducing the number of packets that need to be sent over the network. This setting is applied to the Server side of the transaction. Care must be taken with the server settings as Nagle and delayed ACK may severely impact performance.

Client Nagle

Tick the box to enable the Client Nagle setting. As above but applied to the Client side of the transaction.

SNAT

SNAT stands for Source Network Address Translation, and different vendors have slight variations in the implementation of SNAT. A simple explanation of the EdgeADC SNAT would be as follows.

Under normal circumstances, inbound requests would be directed to the VIP that would see the source IP of the request. So, for example, if a browser endpoint had an IP address of 81.71.61.51, this would be visible to the VIP.

When SNAT is in force, the original source IP of the request will be hidden from the VIP, and instead, it will see the IP address as provided in the SNAT rule. Thus, SNAT can be used in Layer 4 and Layer 7 load balancing modes.

Field	Description
Source IP	The Source IP address is optional, and it can be either a network IP address (with /mask) or a plain IP address. The mask can be either a network mask or a plain number, specifying the

	number of 1's at the left side of the network mask. Thus, a mask of /24 is equivalent to 255.255.255.0.
Destination IP	The Destination IP address is optional, and it can be either a network IP address (with /mask) or a plain IP address. The mask can be either a network mask or a plain number, specifying the number of 1's at the left side of the network mask. Thus, a mask of /24 is equivalent to 255.255.255.0.
Source Port	The source port is optional, it can be a single number, in which case it specifies only that port, or it can include a colon, which specifies a range of ports. Examples: 80 or 5900:5905.
Destination Port	The destination port is optional, it can be a single number, in which case it specifies only that port, or it can include a colon, which specifies a range of ports. Examples: 80 or 5900:5905.
Protocol	You can choose whether to use SNAT on a single protocol or all the protocols. We suggest being specific to be more precise.
SNAT to IP	SNAT to IP is a mandatory IP address or a range of IP addresses. Examples: 10.0.0.1 or 10.0.0.1-10.0.0.3.
SNAT to Port	The SNAT to Port is optional, it can be a single number, in which case it specifies only that port, or it can include a dash, which specifies a range of ports. Examples: 80 or 5900-5905.
Notes	Use this to put a friendly name to remind yourself why the rules exist. This is also useful for debugging in the Syslog.

Power

This ADC system feature also allows you to conduct several power-related tasks on your ADC.

Restart

This setting initiates a global restart of all Services and consequently breaks all currently active connections. All the Services will automatically resume after a short period, but the timing will depend on how many Services are configured. A pop-up will be displayed requesting confirmation for the restart action.

Reboot

Clicking the Reboot button will power cycle the ADC and automatically bring it back to an active state. A pop-up will be displayed requesting confirmation for the reboot action.

Power Off

Clicking the Power Off button will shut down the ADC. If this is a hardware appliance, you will need physical access to the device to power it back on. A pop-up will be displayed requesting confirmation for the shutdown action.

Security

This section allows you to change the web console password and enable or disable the Secure Shell access. It also allows the enablement of the REST API capability.

SSH

Option	Description
Secure Shell Remote Conn	Please tick the box if you wish to gain access to the ADC using SSH. "Putty" is an excellent application for doing this.

Web Console

SSL Certificate Choose a certificate from the drop-down list. The certificate you choose will be used to secure your connection to the ADC's web user interface. You can create a self-signed certificate within the ADC or import one from the **SSL CERTIFICATES** section.

Option	Description
Secure Port	The default port for the web console is TCP 443. If you wish to use a different port for security reasons, you can change it here.

REST API

The REST API, also known as RESTful API, is an application programming interface that conforms to the REST architectural style and allows configuration of the ADC or data extraction from the ADC. The term REST stood for representational state transfer and was created by computer scientist Roy Fielding.

Option	Description
Enable REST	Tick this box to enable access using the REST API. Note that you will also have to configure which adapter on which REST is enabled. See the note on the Cog link below.
SSL Certificate	Choose a certificate for the REST service. The drop-down will show all the certificates installed on the ADC.
Port	Set the Port for the REST service. It is a good idea to use a port other than 443.
IP Address	This will display the IP address that the REST service is tied to. You can click the Cog link to access the Network page to change which adapter the REST service is enabled on.
Cog Link	Clicking on this link will take you to the Network page where you can configure an adapter for the REST.

Documentation for REST API

Documentation on how to use the REST API is available: **jetAPI | 4.2.3 | jetNEXUS | SwaggerHub**

Note: If you get errors on the Swagger page this is because they have an issue supporting query strings
Scroll past the errors to jetNEXUS REST API

Examples

GUID using CURL:

- Command

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

- will return

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

- Validity
  - GUID is valid for 24 hours

Licence Details

- Command

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

SNMP

The SNMP section allows the configuration of the SNMP MIB residing within the ADC. The MIB can then be queried by third-party software capable of communicating with devices equipped with SNMP.

SNMP Settings

Option	Description
SNMP v1 / V2C	Tick the checkbox to enable the V1/V2C MIB. SNMP v1 conforms with RFC-1157. SNMP V2c conforms with RFC-1901-1908
SNMP v3	Tick the checkbox to enable the V3 MIB. RFC-3411-3418. The username for v3 is admin. Example:- snmpwalk -v3 -u admin -A jetnexus -l authNoPriv 192.168.1.11 1.3.6.1.4.1.38370
Community String	This is the read-only string set on the agent and used by the manager to retrieve the SNMP information. The default community string is jetnexus
PassPhrase	This is the password needed when SNMP v3 is enabled and must be at least 8 characters or more and contain letters Aa-Zz and numbers 0-9 only. The default passphrase is **jetnexus**

SNMP MIB

The information viewable over SNMP is defined by the Management Information Base (MIB). MIB's describe the structure of the management data and use hierarchical object identifiers (OID). Each OID can be read via an SNMP management application.

MIB Download

The MIB can be downloaded [here](#):

ADC OID

ROOT OID

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

Our OIDs

.38370 jetnexusMIB
    .1 **jetnexusData** (1.3.6.1.4.1.38370.1)
        .1 **jetnexusGloba**l (1.3.6.1.4.1.38370.1.1)
        .2 **jetnexusVirtualServices** (1.3.6.1.4.1.38370.1.2)
        .3 **jetnexusServers** (1.3.6.1.4.1.38370.1.3)
            .1 **jetnexusGlobal** (1.3.6.1.4.1.38370.1.1)
                .1 **jetnexusOverallInputBytes** (1.3.6.1.4.1.38370.1.1.1.0)
                .2 **jetnexusOverallOutputBytes** (1.3.6.1.4.1.38370.1.1.2.0)
                .3 **jetnexusCompressedInputBytes** (1.3.6.1.4.1.38370.1.1.3.0)
                .4 jetnexusCompressedOutputBytes (1.3.6.1.4.1.38370.1.1.4.0)
                .5 **jetnexusVersionInfo** (1.3.6.1.4.1.38370.1.1.5.0)
                .6 **jetnexusTotalClientConnections** (1.3.6.1.4.1.38370.1.1.6.0)
                .7 **jetnexusCpuPercent** (1.3.6.1.4.1.38370.1.1.7.0)
                .8 **jetnexusDiskFreePercent** (1.3.6.1.4.1.38370.1.1.8.0)
                .9 **jetnexusMemoryPercent** (1.3.6.1.4.1.38370.1.1.9.0)
                .10 **jetnexusCurrentConnections** (1.3.6.1.4.1.38370.1.1.10.0)

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

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

Historical Graphing

The best use for the ADC's Custom SNMP MIB is the ability to offload the historical graphing to a management console of your choice. Below are some examples from Zabbix that polls an ADC for various OID values listed above.
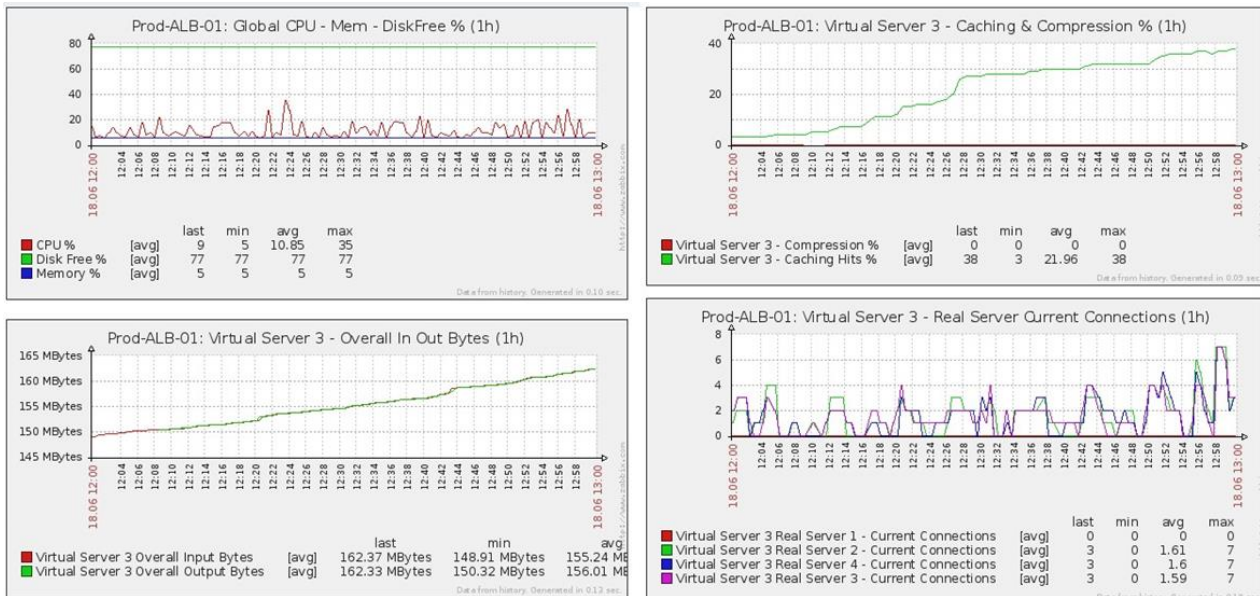
Users and Audit Logs

The ADC provides the ability to have an internal set of users to configure and define what the ADC does. Users defined within the ADC can perform a variety of operations depending on the role attached to them.

There is a default user called **admin** that you use when first configuring the ADC. The default password for admin is **jetnexus**.

Users

The Users section is provided for you to create, edit and remove users from the ADC.
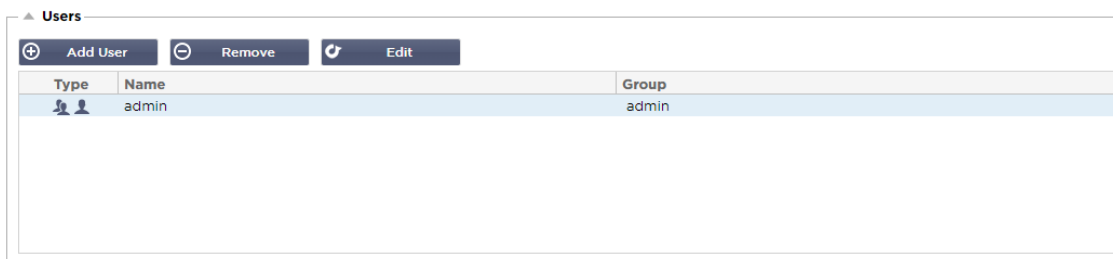
Add User

Click the Add User button shown in the image above to bring up the Add User dialog.

Parameter	Description/Usage
Username	Enter a username of your choice The username must comply with the following: • Minimum number of characters 1 • Maximum number of characters 32 • Letters can be upper and lower case • Numbers may be used • Symbols are not permitted
Password	Enter a **strong** password that conforms with the below requirements • Minimum number of characters 6 • Maximum number of characters 32 • Must use at least a combination of letters and numbers • Letters can be upper or lower case • Symbols are permitted except for those in the example below **£**, **%**, **&**, **<**, **>**
Confirm Password	Confirm the password again to ensure it is correct
Group Membership	Tick the group that you would like the user to belong. • Admin - This group can do everything • GUI Read Write - Users in this group can access the GUI and make changes via the GUI • GUI Read - Users in this group can access the GUI to view information only. No changes can be made • SSH - Users in this group can access the ADC via Secure Shell. This choice will give access to the command line, which has a minimal set of commands available • API - Users in this group will have access to SOAP and REST programmable interface. REST will be available from Software Version 4.2.1

User Type

👤	Local **User** **The ADC in Stand-Alone or Manual H/A role will create Local Users only** **By default,** a local user called "admin" **is a member of the admin group. For backward compatibility**, **this user can never be deleted** **You may change the password of this user or delete it**, **but you cannot delete the last local admin**
👥	**Cluster User** The ADC in Cluster role will create Cluster Users only Cluster Users are synchronized across all the ADCs in the Cluster Any change to a cluster user will change on all members of the cluster If you are logged on as a cluster user, you will not be able to switch roles from Cluster to Manual or Stand-Alone
👥👤	**Cluster and Local User** Any users created while in Stand-Alone or Manual role will be copied to the Cluster If the ADC subsequently leave the Cluster, then only Local Users will remain The last configured password for the user will be valid

Removing a User

• Highlight an existing user
• Click Remove
• You will not be able to delete the user that is currently signed in

- You will not be able to remove the last local user in the admin group
- You will not be able to remove the final remaining cluster user in the admin group
- You will not be able to delete the admin user for backward compatibility
- If you remove the ADC from the cluster, all users except local users will be deleted

Editing a User

- Highlight an existing user
- Click Edit
- You may change the user's group membership by ticking the appropriate boxes and updating
- You may also change the password of a user, provided you have admin rights

Audit Log

The ADC logs changes made to the ADC configuration by individual users. The audit log will provide the last 50 actions carried out by all users. You may also see ALL entries in the **LOGS** section. For example:

Advanced

Configuration
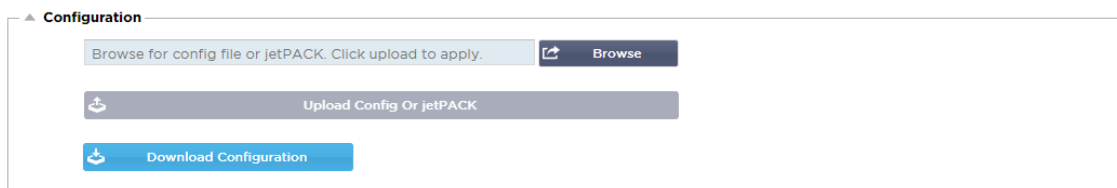
It is always best practice to download and save the configuration of the ADC once it is fully set up and working as required. You can use the Configuration module to both download and upload a configuration.

Jetpacks are configuration files for standard applications and are provided by Edgenexus to simplify your job. These, too, can be uploaded to the ADC using the Configuration module.

A configuration file is essentially a text-based file, and as such, can be edited by you using a text editor such as Notepad++ or VI. Once edited as required, the configuration file can be uploaded into the ADC.

Downloading a configuration

- To download the current configuration of the ADC, press the Download Configuration button.
- A pop-up will appear asking you to open or save the .conf file.
- Save to a convenient location.
- You can open this with any text editor, such as Notepad++.

Uploading a configuration

- You may upload a saved configuration file by browsing for the saved .conf file.
- Click the 'Upload Config or Jetpack' button.
- The ADC will upload and apply the config and then refresh the browser. If it does not refresh the browser automatically, please click refresh on the browser.
- You will be redirected to the Dashboard page upon completion.

Upload a jetPACK

- A jetPACK is a set of configuration updates to the existing configuration.
- A jetPACK can be as small as changing the TCP Timeout value right up to a complete application-specific configuration such as Microsoft Exchange or Microsoft Lync.
  - You can obtain a jetPACK from the support portal shown at the end of this guide.
- Browse for the jetPACK.txt file.
- Click upload.
- The browser will refresh automatically after upload.
- You will be redirected to the Dashboard page upon completion.
- The import may take longer for more complex deployments such as Microsoft Lync etc.

Global Settings

The Global settings section allows you to change various elements, including the SSL cryptographic library.

Host Cache Timer

The Host Cache Timer is a setting that stores the IP Address of a Real Server for a given period when the domain name has been used instead of an IP Address. The cache is flushed upon a Real Server failure. Setting this value to zero will prevent the cache from being flushed. There is no max value for this setting.

Drain

The Drain feature is configurable for each Real Server linked to a Virtual Service. By default, the Drain Clears Persistence setting is enabled, allowing servers that are placed in Drain mode to end sessions gracefully so that they can be taken offline for maintenance.

SSL
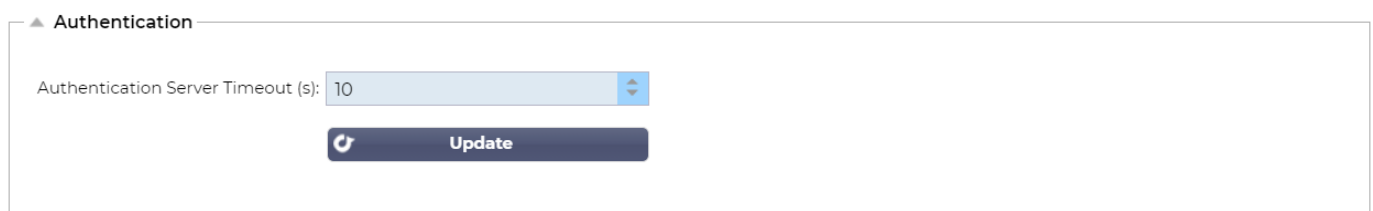
This global setting allows the SSL library to be changed as needed. The default SSL Cryptographic Library used by the ADC is from OpenSSL. If you wanted to use a different crypto library, this could be changed here.

Authentication

This value sets the timeout value for authentication, after which the authentication attempt will have been deemed as failed.

Protocol

The Protocol section is used to set the many advanced settings for the HTTP protocol.

Server too Busy

Suppose you have limited the Max Connections to your Real Servers; you can choose to present a friendly web page once this limit has been reached.

- Create a simple web page with your message. You may include external links to objects on another web servers and sites. Alternatively, if you want to have images on your web page, then use inline base64 encoded images
- Browse for your newly created web page HTM(L) file
- Click Upload
- If you wish to preview the page, you can do so with the Click Here link

Forwarded For

Forwarded For is the de facto standard for identifying the originating IP address of a client connecting to a web server through Layer- 7 load balancers and proxy servers.

Forwarded-For Output

Option	Description
Off	ADC does not alter the Forwarded-For header.
Add Address and Port	This choice will append the IP address and port, of the device or client connected to the ADC, to the Forwarded-For header.
Add Address	This choice will append the IP address, of the device or client connected to the ADC, to the Forwarded-For header.
Replace Address and Port	This choice will replace the value of the Forwarded-For header with the IP address and port of the device or client connected to the ADC.
Replace Address	This choice will replace the value of the Forwarded-For header with the IP address of the device or client connected to ADC.

Forwarded-For Header

This field allows you to specify the name given to the Forwarded-For header. Typically, this is "X-Forwarded-For" but may be changed for some environments.

Advanced Logging for IIS – Custom Logging

You can obtain the X-Forwarded-For information by installing the IIS Advanced logging 64-bit app. Once downloaded, create a Custom Logging Field called X-Forwarded-For with the settings below.

Select Default from the Source Type list from the Category list, select Request Header In the Source Name box, and type X-Forwarded-For.

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

Apache HTTPd.conf changes

You will want to make several changes to the default format to log the X-Forwarded-For client IP address or the actual client IP address if the X-Forwarded-For header does not exist.

Those changes are below:

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

This format takes advantage of Apache's built-in support for conditional logging based upon environmental variables.

- Line 1 is the standard combined log formatted string from the default.
- Line 2 replaces the %h (remote host) field with the value(s) pulled from the X-Forwarded-For header and set the name of this log file pattern to "proxy".
- Line 3 is a setting for the environment variable "forwarded" that contains a loose regular expression matching an IP address, which is ok in this case since we care more whether an IP address exists in the X-Forwarded-For header.
- Also, line 3 could be read as: "If there is an X-Forwarded-For value, use it."
- Lines 4 and 5 tell Apache which log pattern to use. If an X-Forwarded-For value exists, use the "proxy" pattern, else use the "combined" pattern for the request. For readability, lines 4 and 5 do not take advantage of Apache's rotate logs (piped) logging feature, but we assume that almost everyone uses it.

These changes will result in logging an IP address for every request.

HTTP Compression Settings

Compression is an acceleration feature and is enabled for each Service on the IP Services page.

WARNING – Take extreme care when adjusting these settings as inappropriate settings can adversely affect the performance of ADC

Option	Description
Initial Thread Memory [KB]	This value is the amount of memory each request received by ADC may initially allocate. For most efficient performance, this value should be set at a value just in excess of the largest uncompressed HTML file that the web servers are likely to send.
Maximum Thread Memory [KB]	This value is the maximum amount of memory that the ADC will allocate on one request. For maximum performance, ADC normally stores and compresses all

	content in memory. IF an exceptionally large content file exceeding this amount is processed, ADC will write to disk and compress the data there.
Increment Memory [KB]	This value sets the amount of memory added to the Initial Thread Memory Allocation when more is required. The default setting is zero. This means ADC will double the allocation when the data exceeds the current allocation (e.g. 128Kb, then 256Kb, then 512Kb, etc) up to the limit set by Maximum Memory Usage per Thread. This is efficient where the majority of pages are of a consistent size but there are occasional larger files. (e.g. Majority of pages are 128Kb or less, but occasional responses are 1Mb in size.) In the scenario where there are large variable sized files, it is more efficient to set a linear increment of a significant size (e.g. Responses are 2Mb to 10Mb in size, an initial setting of 1Mb with increments of 1Mb would be more efficient.).
Minimum Compression Size [Bytes]	This value is the size, in bytes, under which the ADC will not attempt to compress. This is useful because anything much under 200-bytes does not compress well and may even grow in size due to the overheads of compression headers.
Safe Mode	Tick this option to prevent ADC from applying compression to style sheets of JavaScript. The reason for this is that even though ADC is aware of which individual browsers can handle compressed content, some other proxy servers, even though they claim to be HTTP/1.1 compliant are unable to transport compressed style sheets and JavaScript correctly. If problems are occurring with style sheets or JavaScript through a proxy server, then use this option to disable compression of these types. However, this will reduce the overall amount of compression of content.
Disable Compression	Tick this to stop ADC from compressing any response.
Compress As You Go	ON - Use Compress as You Go on this page. This compresses each block of data received from the server in a discrete chunk that is fully de-compressible. OFF - Do not use Compress As you Go on this page. By Page Request - Use Compress as You Go by page request.

Global Compression Exclusions

Any pages with the added extension in the exclusion list will not be compressed.

- Type in the individual file name.
- Click update.
- If you wish to add a file type, simply type "*.css" for all cascading style sheets to be excluded.
- Each file or file type should be added to a new line.

Persistence Cookies

This setting allows you to specify how Persistence Cookies are handled.

Field	Description
Same Site Cooke Attribute	**None**: All cookies are accessible to scripts **Lax**: Prevents cookies being accessed across sites, but they are stored to become accessible and submitted to the owning site if it is visited **Strict**: prevents any cookie for a different site from being accessed or stored **Off**: returns to the browser's default behavior
Secure	This checkbox, when checked, applies the persistence to secure traffic
HTTP Only	When checked, this allows Persistent Cookes only on HTTP traffic

Software

The Software section allows you to update the configuration and the firmware of your ADC.

Software Upgrade Details

The information in this section will be populated if you have a working Internet connection. If your browser does not have a link to the Internet, this section will be blank. Once connected, you will receive the banner message below.

The section Download from Cloud shown below will be populated with information showing updates available to you under your support plan. You should pay attention to the support Type and Support Expiry date.

Note: We use your browser's internet connection to view what is available from the Edgenexus Cloud. You will only be able to download software updates if the ADC has an internet connection.

To check this:

- Advanced--Troubleshooting--Ping
- IP Address – appstore.edgenexus.io
- Click Ping
- If the result shows "ping: unknown host appstore.edgenexus.io."
- The ADC will NOT be able to download anything from the cloud

Download from Cloud

If your browser is connected to the Internet, you will see details of software available in the cloud.

- Highlight the row you are interested in and click the "Download Selected Software to ALB." button
- The selected software will download to your ALB when clicked, which can be applied in the "Apply Software Stored on ALB" section below.

Note: If the ADC does not have direct internet access, you will receive an error like the below:

Download error, ALB not able to access ADC Cloud Services for file build1734-3236-v4.2.1-Sprint2-update-64.software.alb

Upload software to ALB

Apps Upload

If you have an App file which ends with <apptype>.alb you can use this method to upload it.

- There are five types of App
    - <appname>flightpath.alb
    - <appname>.monitor.alb
    - <appname>.jetpack.alb
    - <appname>.addons.alb
    - <appname>.featurepack.alb
- Once uploaded, each app will be found in the Library>Apps section.
- You must then deploy each App in that section individually.

Software

- If you wish to upload software without applying it, then use the highlighted button.
- The Software File is <softwarename>.software.alb.
- It will then show in the "Software Stored on ALB" section, from where you can apply it at your convenience.

Apply Software stored on 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

This section will show all Software files stored on the ALB and available for deployment. The listing will include updated Web Application Firewall (WAF) signatures.

- Highlight the Software row you are interested in using.
- Click "Apply Software from Selected"
- If this is an ALB Software Update, please be aware that it will upload and then reboot the ALB to apply.
- If the update you are applying is an OWASP signature update, it will apply automatically without rebooting.

Troubleshooting

There are always issues that require troubleshooting to come to a root cause and solution. This section allows you to do that.

Support Files

If you have an issue with the ADC and need to open a support ticket, Technical Support will often request several different files from the ADC appliance. These files have now been aggregated into one single .dat file that can be downloaded via this section.

- Select a time frame from the drop-down: A choice of 3, 7, 14, and All days are available to you.
- Click "Download Support Files"
- A file will be downloaded in the format Support-jetNEXUS-yyymmddhh-NAME.dat
- Raise a support ticket on the support portal, details of which are available at the end of this document.
- Make sure you describe the problem thoroughly and attach the .dat file to the ticket.

Trace

The Trace section will allow you to examine information enabling the debugging of the issue. The information delivered depends on the options you choose from the drop-downs and the tick boxes.

Option	Description
Nodes to Trace	**Your IP**: This will filter the output to use the IP address you are accessing the GUI from (Note do not choose this option for Monitoring as Monitoring will use the ADC interface address) **All IP**: No filter will be applied. It should be noted that on a busy box this will adversely affect performance.
Connections	This checkbox, when ticked, will show you information about the client and server-side connections.
Cache	This checkbox ticked will show you information with regards to cached objects.
Data	When this checkbox is ticked, it will include the raw data bytes handled in and out by the ADC.
flightPATH	Th flightPATH menu allows you to select a particular flightPATH rule to monitor or All flightPATH rules.
Server Monitoring	This checkbox, when ticked, will show the server health monitors active on the ADC and their respective results.
Monitoring Unreachable	When this option is selected, it's very much like Server monitoring in behavior, except it will only show the failed monitors and so acts as a filter for these messages only.
Auto-Stop Records	The default value is 1,000,000 records, after which the Trace facility will automatically stop. This setting is a safety precaution to prevent Trace from accidentally being left on and affecting your ADC performance.
Auto-Stop Duration	The default time is set to 10 minutes, after which the Trace facility will automatically stop. This feature is a safety precaution to prevent Trace from accidentally being left on and affecting the performance of the ADC.
Start	Click this to Start the Trace facility manually.
Stop	Click to manually stop the Trace facility before the automatic record or time is reached.
Download	Although you can see the live viewer on the right-hand side, the information may be displayed too quickly. Instead, you can download the Trace.log to view all the information gathered during the various traces that day. This feature is a filtered list of trace information. If you wish to view previous days' trace information, you can download Syslog for that day but will have to filter manually.
Clear	Clears the trace log

Ping

You can check for network connectivity to servers and other network objects in your infrastructure using the Ping tool.

```
 ┌─ ▲ Ping ──────────────────────────────────────────────────────┐
 │  IP Address: 192.168.1.125                    (◉  Ping )        │
 │                                                                │
 │  Ping Results: PING 192.168.1.125 (192.168.1.125) 56(84) bytes of data.      │
 │               64 bytes from 192.168.1.125: icmp_seq=1 ttl=64 time=0.914 ms   │
 │               64 bytes from 192.168.1.125: icmp_seq=2 ttl=64 time=0.340 ms   │
 │               64 bytes from 192.168.1.125: icmp_seq=3 ttl=64 time=0.362 ms   │
 │               64 bytes from 192.168.1.125: icmp_seq=4 ttl=64 time=0.565 ms   │
 │                                                                │
 │               --- 192.168.1.125 ping statistics ---            │
 │               4 packets transmitted, 4 received, 0% packet loss, time 3002ms │
 │               rtt min/avg/max/mdev = 0.340/0.545/0.914/0.230 ms              │
 │                                                                │
 └────────────────────────────────────────────────────────────────┘
```

Type in the host's IP address you wish to test, for example, the default gateway using dotted decimal notation or an IPv6 address. You may have to wait a few seconds for the result to feedback once you have pressed the "Ping" button.

If you have configured a DNS server, then you can type in the fully qualified domain name. You can configure a DNS server in the **DNS SERVER 1 & DNS SERVER 2** section. You may have to wait a few seconds for the result to feedback once you have pressed the "Ping" button.

Capture

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

To capture network traffic, follow the simple instructions below.

- Complete the options in the form
- Click Generate
- Once the capture has run, your browser will pop up and ask you where you wish to save the file. It will be in the format "jetNEXUS.cap.gz"
- Raise a support ticket on the support portal, details of which are available at the end of this document.
- Make sure you describe the problem thoroughly and attach the file to the ticket.
- You can also view the contents using Wireshark

Option	Description
Adapter	Choose your adapter from the drop-down, typically eth0 or eth1. You can also capture all interfaces with "any"
Packets	This value is the maximum number of packets to capture. Typically, 99999
Duration	Choose a maximum time that the capture will run for. A typical time is 15 seconds for high-traffic sites. The GUI will be inaccessible during the capture period
Address	This value will filter on any IP address entered in the box. Leave this blank for no filter.

To maintain performance, we have limited the download file to 10MB. If you find that this is not enough to capture all the data needed, we can increase this figure.

Note: This will have an impact on the performance of live sites. To increase the available capture size, please apply a global setting jetPACK to increase the capture size.

Help

The Help section provides access to the information on Edgenexus and access to the user guides and other helpful information.

About us

Clicking on the About Us option will display information on Edgenexus and its corporate office.

Reference

The reference option will open the page containing user guides and other helpful documents.

If you do not find what it is you are looking for, please contact support@edgenexus.io.

What is a jetPACK

jetPACKs are a unique method of instantly configuring your ADC for specific applications. These easy-to-use templates come pre-configured and fully tuned with all application-specific settings that you need to enjoy optimized service delivery from your ADC. Some of the jetPACKs use flightPATH to manipulate the traffic, and you must have a flightPATH license for this element to work. To find out if you have a license for flightPATH, please refer to the **LICENSE** page.

Downloading a jetPACK

- Each jetPACK below has been created with a unique Virtual IP address contained in the title of the jetPACK. For example, the first jetPACK below has a Virtual IP Address of 1.1.1.1
- You can either upload this jetPACK as is and change the IP address in the GUI or edit the jetPACK with a text editor such as Notepad++ and search and replace 1.1.1.1 with your Virtual IP address.
- In addition, each jetPACK has been created with 2 Real Servers with IP addresses of 127.1.1.1 and 127.2.2.2. Again you can change these in the GUI after upload or beforehand using Notepad++.
- Click on a jetPACK link below and Save Link as a jetPACK-VIP-Application.txt file in your chosen location

Microsoft Exchange

Application	Download link	What does it do?	What's included?
Exchange 2010	jetPACK-1.1.1.1-Exchange-2010	This jetPACK will add the basic settings to load balance Microsoft Exchange 2010. There is a flightPATH rule included to redirect traffic on the HTTP service to HTTPS, but it is an option. If you don't have a license for flightPATH, this jetPACK will still work.	Global settings: Service timeout 2 hours Monitors: Layer 7 monitor for the Outlook web app, and Layer 4 out of band monitor for client access service Virtual Service IP: 1.1.1.1 Virtual Service Ports: 80, 443, 135, 59534, 59535 Real Servers: 127.1.1.1 127.2.2.2 flightPATH: Adds redirect from HTTP to HTTPS
	jetPACK-1.1.1.2-Exchange-2010-SMTP-RP	Same as above, but it will add an SMTP service on port 25 in reverse proxy connectivity. The SMTP server will see the ALB-X interface address as the source IP.	Global settings: Service timeout 2 hours Monitors: Layer 7 monitor for the Outlook web app. Layer 4 out of band monitor for client access service Virtual Service IP: 1.1.1.1 Virtual Service Ports: 80, 443, 135, 59534, 59535, 25 (reverse proxy) Real Servers: 127.1.1.1 127.2.2.2 flightPATH: Adds redirect from HTTP to HTTPS
	jetPACK-1.1.1.3-Exchange-2010-SMTP-DSR	Same as above, except this jetPACK will configure the SMTP service to use Direct Server Return connectivity. This jetPACK is needed if your SMTP server needs to see the actual IP address of the client.	Global settings: Service timeout 2 hours Monitors: Layer 7 monitor for the Outlook web app. Layer 4 out of band monitor for client access service Virtual Service IP: 1.1.1.1 Virtual Service Ports: 80, 443, 135, 59534, 59535, 25 (direct server return) Real Servers: 127.1.1.1 127.2.2.2

			flightPATH: Adds redirect from HTTP to HTTPs
Exchange 2013	jetPACK-2.2.2.1-Exchange-2013-Low-Resource	This setup adds 1 VIP and two services for HTTP and HTTPS traffic and requires the least CPU. It is possible to add multiple health checks to the VIP to check each of the individual services is up	Global settings: Monitors: Layer 7 monitor for OWA, EWS, OA, EAS, ECP, OAB, and ADS Virtual Service IP: 2.2.2.1 Virtual Service Ports: 80, 443 Real Servers: 127.1.1.1 127.2.2.2 flightPATH: Adds redirect from HTTP to HTTPS
	jetPACK-2.2.3.1-Exchange-2013-Med-Resource	This setup uses a unique IP address for each service and therefore uses more resources than above. You must configure each service as an individual DNS entry Example owa.edgenexus.com, ews.edgenexus.com, etc. A monitor for each service will be added and applied to the relevant service	Global settings: Monitors: Layer 7 monitor for OWA, EWS, OA, EAS, ECP, OAB,ADS, MAPI and PowerShell Virtual Service 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 Virtual Service Ports: 80, 443 Real Servers: 127.1.1.1 127.2.2.2 flightPATH: Adds redirect from HTTP to HTTPs
	jetPACK-2.2.2.3-Exchange2013-HIgh-Resource	This jetPACK will add one unique IP address and several virtual services on different ports. flightPATH will then context switch based on the destination path to the correct Virtual Service. This jetPACK requires the most amount of CPU to carry out the context switching	Global settings: Monitors: Layer 7 monitor for OWA, EWS, OA, EAS, ECP, OAB, ADS, MAPI and PowerShell Virtual Service IP: 2.2.2.3 Virtual Service Ports: 80, 443, 1, 2, 3, 4, 5, 6, 7 Real Servers: 127.1.1.1 127.2.2.2 flightPATH: Adds redirect from HTTP to HTTPS

Microsoft Lync 2010/2013

Reverse Proxy	Front End	Edge Internal	Edge External
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

Web Services

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

Microsoft Remote Desktop

Normal
jetPACK-5.5.5.1-Remote-Desktop

DICOM – Digital Imaging and Communication in Medicine

Normal HTTP
jetPACK-6.6.6.1-DICOM

Oracle e-Business Suite

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

VMware Horizon View

Connection Servers – SSL Offload	Security Servers – SSL Re-Encryption
jetPACK-8.8.8.1-View-SSL-Offload	jetPACK-8.8.8.2-View-SSL-Re-encryption

Global settings

- GUI Secure Port 443 – this jetPACK will change your secure GUI port from 27376 to 443. HTTPs://x.x.x.x
- GUI Timeout 1 day – the GUI will request you to input your password every 20 minutes. This setting will increase that request to 1 day
- ARP Refresh 10 – during a failover between HA appliances, this setting will increase the number of **Gratuitous ARP's** to assist the switches during the transition
- Capture Size 16MB – the default capture size is 2MB. This value will increase the size to a maximum of 16MB

Cipher Options

- Strong Ciphers – This will add the ability to choose "Strong Ciphers" from the Cipher options list:
    - Cipher = ALL:RC4+RSA:+RC4:+HIGH:!DES-CBC3-SHA:!SSLv2:!ADH:!EXP:!ADHexport:!MD5
- Anti-Beast – This will add the ability to choose "Anti Beast" from the Cipher Options list:
    - Cipher = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH
- No SSLv3 – This will add the ability to choose "No SSLv3" from the Cipher Options list:
    - Cipher = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
- No SSLv3 no TLSv1 No RC4 – This will add the ability to choose "No-TLSv1 No-SSLv3 No-RC4" from the Cipher Options list:
    - Cipher = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
- NO_TLSv1.1 –This will add the ability to choose "NO_TLSv1.1" from the Cipher Options list:
    - Cipher= ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:
      DH+AES:RSA+AESGCM:RSA+AES:HIGH:!3DES:!aNULL:!MD5:!DSS:!MD5:!aNULL:!EDH:!RC4

flightPATHs

- X-Content-Type-Options – add this header if it doesn't exist and set it to "nosniff" – prevents the browser from automatically "MIME-Sniffing".
- X-Frame-Options – add this header if it doesn't exist and set it to "SAMEORIGIN" – pages on your website can be included in Frames, but only on other pages within the same website.
- X-XSS-Protection – add this header if it doesn't exist and set it to "1; mode=block" – enable browser cross-site scripting protections
- Strict-Transport-Security – add header if it doesn't exist and set it to "max-age=31536000 ; includeSubdomains" – ensures client should honor that all links should be HTTPs:// for the max-age

Applying a jetPACK

You can apply any jetPACK in any order but be careful not to use a jetPACK with the same Virtual IP address. This action will cause a duplicate IP address in the configuration. If you do this by mistake, you can change this in the GUI.

- Navigate to Advanced > Update Software
- Configuration Section
- Upload New Configuration or jetPACK
- Browse for jetPACK

- Click Upload
- Once the browser screen turns white, please click refresh and wait for the Dashboard page to appear

Creating a jetPACK

One of the great things about jetPACK is that you can create your own. It may be that you have created the perfect config for an application and want to use this to several other boxes independently.

- Start by copying the current configuration from your existing ALB-X
  - o Advanced
  - o Update Software
  - o Download Current Configuration
- Edit this file with Notepad++
- Open a new txt document and call it "yourname-jetPACK1.txt"
- Copy all the relevant sections from the config file to "yourname-jetPACK1.txt"
- Save once complete

IMPORTANT: Each jetPACK is split into different sections, but all jetPACKs must have #!jetpack at the top of the page.

The sections that are recommended for editing/copying are listed below.

Section 0:

#!jetpack

This line needs to be at the top of the jetPACK, or your current configuration will be overwritten.

Section1:

[jetnexusdaemon]

This section contains global settings that, once changed, will apply to all services. Some of these settings can be changed from the web console, but others are only available here.

Examples:

ConnectionTimeout=600000

This example is the TCP timeout value in milliseconds. This setting means that a TCP connection will be closed after 10 minutes of inactivity

ContentServerCustomTimer=20000

This example is the delay in milliseconds between content server health checks for custom monitors such as DICOM

jnCookieHeader="MS-WSMAN"

This example will change the name of the cookie header used in persistent load balancing from the default "jnAccel" to "MS-WSMAN". This particular change is needed for Lync 2010/2013 reverse proxy.

Section 2:

[jetnexusdaemon-Csm-Rules]

This section contains the custom server monitoring rules that are typically configured from the web console here.

Example:

[jetnexusdaemon-Csm-Rules-0]
Content="Server Up"
Desc="Monitor 1"
Method="CheckResponse"
Name="Health Check- Is Server Up"

Url="HTTP://demo.jetneus.com/healthcheck/healthcheck.html"

Section 3:

[jetnexusdaemon-LocalInterface]

This section contains all the details in the IP Services section. Each interface is numbered and includes sub-interfaces for each channel. If your channel has a flightPATH rule applied, then it will also contain a Path section too.

Example:

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

This section contains all the flightPATH rules. The numbers must match what has been applied to the interface. In the example above, we see that flightPATH rule "6" has been applied to the channel, including this as an example below.

Example:

[jetnexusdaemon-Path-6]
Desc="Force to use HTTPS for certain directory"
Name="Gary – Force HTTPS"
[jetnexusdaemon-Path-6-Condition-1]
Check="contain"

Condition="path"
Match=
Sense="does"
Value="/secure/"
[jetnexusdaemon-Path-6-Evaluate-1]
Detail=
Source="host"
Value=
Variable="$host$"[jetnexusdaemon-Path-6-Function-1]
Action="redirect"
Target="HTTPs://$host$$path$$querystring$"
Value=

Introduction to flightPATH

What is flightPATH?

flightPATH is an intelligent rules engine developed by Edgenexus to manipulate and route HTTP and HTTPS traffic. It is highly configurable, very powerful, and yet very easy to use.

Although some components of flightPATH are IP objects, such as Source IP, flightPATH can only be applied to a **Service Type** equal to HTTP. If you choose any other service type, then the flightPATH tab in IP Services will be blank.

A flightPATH rule has three components:

Option	Description
Condition	Set multiple criteria to trigger the flightPATH rule.
Evaluation	Allows the use of variables that can be used in the Action area.
Action	The behavior once the rule has triggered.

What can flightPATH do?

flightPATH can be used to modify Incoming and Outgoing HTTP(s) content and requests.

As well as using simple string matches such as "Starts with" and "Ends With" for example, complete control using powerful Perl-compatible Regular Expressions (RegEx) can be implemented.

For more on RegEx, please see this helpful site https://www.regexbuddy.com/regex.html

In addition, custom variables can be created and used in the **Action** area enabling many different possibilities.

Condition

Condition	Description	Example
<form>	HTML forms are used to pass data to a server	Example "form doesn't have length 0"
GEO Location	This compares the source IP address to the ISO 3166 Country Code	GEO Location does equal GB OR GEO Location does equal Germany
Host	This is the host extracted from the URL	www.mywebsite.com or 192.168.1.1
Language	This is the Language extracted from the language HTTP header	This condition will produce a dropdown with a list of Languages
Method	This is a drop down of HTTP methods	This is a drop down that includes GET, POST etc
Origin IP	If upstream proxy supports X-Forwarded-for (XFF) it will use the true Origin address	Client IP. Can also use multiple IP's or subnets. 10\.1\.2\.* is 10.1.2.0 /24 subnet 10\.1\.2\.3|10\.1\.2\.4 Use | for multiple IP's
Path	This is the path of the website	/mywebsite/index.asp
POST	POST request method	Check data being uploaded to a website
Query	This is the name and Value of a Query as such it can either accept the query name or a value also	"Best=edgeNEXUS" Where the Match is Best and the Value is edgeNEXUS
Query String	The whole query string after the ? character	

Request Cookie	This is the name of a cookie requested by a client	MS-WSMAN=afYfn1CDqqCDqUD::
Request Header	This can be any HTTP Header	Referrer, User-Agent, From, Date
Request Version	This is the HTTP version	HTTP/1.0 OR HTTP/1.1
Response Body	A user defined string in the response body	Server UP
Response Code	The HTTP code for the response	200 OK, 304 Not Modified
Response Cookie	This is the name of a cookie sent by the server	MS-WSMAN=afYfn1CDqqCDqUD::
Response Header	This can be any HTTP Header	Referrer, User-Agent, From, Date
Response Version	The HTTP version sent by the server	HTTP/1.0 OR HTTP/1.1
Source IP	This is either the origin IP, proxy server IP or some other aggregated IP address	Client IP, Proxy IP, Firewall IP. Can also use multiple IP's and subnets. You must escape the dots as these are RegEX. Example 10\.1\.2\.3 is 10.1.2.3

Match	Description	Example
Accept	Content-Types that are acceptable	Accept: text/plain
Accept-Encoding	Acceptable encodings	Accept-Encoding: <compress | gzip | deflate | sdch | identity>
Accept-Language	Acceptable languages for response	Accept-Language: en-US
Accept-Ranges	What partial content range types this server supports	Accept-Ranges: bytes
Authorization	Authentication credentials for HTTP authentication	Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Charge-To	Contains account information for the costs of the application of the method requested	
Content-Encoding	The type of encoding used on the data.	Content-Encoding: gzip
Content-Length	The length of the response body in Octets (8-bit bytes)	Content-Length: 348
Content-Type	The mime type of the body of the request (used with POST and PUT requests)	Content-Type: application/x-www-form-urlencoded
Cookie	A HTTP cookie previously sent by the server with Set-Cookie (below)	Cookie: $Version=1; Skin=new;
Date	Date and time at message was originated	Date = "Date" ":" HTTP-date
ETag	An identifier for a specific version of a resource, often a message digest	ETag: "aed6bdb8e090cd1:0"
From	The email address of the user making the request	From: user@example.com

If-Modified-Since	Allows a 304 Not Modified to be returned if the content is unchanged	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Last-Modified	The last modified date for the requested object, in RFC 2822 format	Last-Modified: Tue, 15 Nov 1994 12:45:26 GMT
Pragma	The Implementation-specific headers may have various effects anywhere along the request-response chain.	Pragma: no-cache
Referrer	This is the address of the previous web page from which a link to the currently requested page was followed	Referrer: HTTP://www.edgenexus.io
Server	A name for the server	Server: Apache/2.4.1 (Unix)
Set-Cookie	A HTTP cookie	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
User-Agent	The user agent string of the user agent	User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Vary	Tells downstream proxies how to match future request headers to decide whether the cached response can be used rather than requesting a fresh one from the origin server	Vary: User-Agent
X-Powered-By	Specifies the technology (e.g. ASP.NET, PHP, JBoss) supporting the web application	X-Powered-By: PHP/5.4.0

Check	Description	Example
Exist	This does not care for the detail of the condition just that it does/doesn't exist	Host — Does — Exist
Start	The string starts with the Value	Path — Does — Start — /secure
End	The string ends with the Value	Path — Does — End — .jpg
Contain	The string does contain the Value	Request Header — Accept — Does — Contain — image
Equal	The string does Equal the Value	Host — Does — Equal — www.edgenexus.io
Have Length	The string does have length of the value	Host — Does — Have Length — 16 www.edgenexus.io = TRUE www.edgenexus.com = FALSE
Match RegEx	This enables you to enter a full Perl compatible regular expression	Origin IP — Does — Match Regex — 10\..* | 11\..*

Example

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

- The example has two conditions, and **BOTH** must be met to carry out the action
- The first is checking that the requested object is an image
- The second is checking for a specific hostname

Evaluation

Evaluation			
⊕ Add New ⊖ Remove			
Variable	**Source**	**Detail**	**Value**
$variable1$	Select a New Source ▾	Select or Type a New Detail	Type a New Value
	Update Cancel		

Adding a Variable is a compelling feature that will allow you to extract data from the request and utilize it in the Actions. For example, you could log a user username or send an email if there is a security problem.

- Variable: This must start and end with a $ symbol. For example $variable1$
- Source: Select from the drop-down box the source of the variable
- Detail: Select from the list when relevant. If the Source=Request Header, the Details could be User-Agent
- Value: Enter the text or regular expression to fine-tune the variable.

Built-in Variables:

- Built-In variables have already been hard coded, so you do not need to create an evaluation entry for these.
- You can use any of the variable listed below in your action
- The explanation for each variable is located in the "Condition" table above
  - Method = $method$
  - Path = $path$
  - Querystring = $querystring$
  - Sourceip = $sourceip$
  - Response code (text also included "200 OK") = $resp$
  - Host = $host$
  - Version = $version$
  - Clientport = $clientport$
  - Clientip = $clientip$
  - Geolocation = $geolocation$"

Example Action:

- Action = Redirect 302
  - Target = HTTPs://$host$/404.html
- Action = Log
  - Target = A client from $sourceip$:$sourceport$ has just made a request $path$ page

Explanation:

- A client accessing page that does not exist would ordinarily be presented with a browsers 404 page
- In this instance the user is redirected to the original hostname they used but the wrong path is replaced with 404.html
- An entry is added to the syslog saying "A client from 154.3.22.14:3454 has just made a request to wrong.html page"

Source	Description	Example
Cookie	This is the name and value of the cookie header	MS-WSMAN=afYfn1CDqqCDqUD::Where the name is MS-WSMAN and the value is afYfn1CDqqCDqUD::
Host	This is the hostname extracted from the URL	www.mywebsite.com or 192.168.1.1
Language	This is the language extracted from the Language HTTP header	This condition will produce a dropdown with a list of languages.
Method	This is a drop down of HTTP methods	The dropdown will include GET, POST
Path	This is the path of the website	/mywebsite/index.html

POST	POST request method	Check data being uploaded to a website
Query Item	This is the name and value of a query. As such it can either accept the query name or a value also	"Best=jetNEXUS" Where the Match is Best and the Value is edgeNEXUS
Query String	This is the whole string after the ? character	HTTP://server/path/program?query_string
Request Header	This can be any header sent by the client	Referrer, User-Agent, From, Date…
Response Header	This can be any header sent by the server	Referrer, User-Agent, From, Date…
Version	This is the HTTP version	HTTP/1.0 or HTTP/1.1

Detail	Description	Example
Accept	Content-Types that are acceptable	Accept: text/plain
Accept-Encoding	Acceptable encodings	Accept-Encoding: <compress | gzip | deflate | sdch | identity>
Accept-Language	Acceptable languages for response	Accept-Language: en-US
Accept-Ranges	What partial content range types this server supports	Accept-Ranges: bytes
Authorization	Authentication credentials for HTTP authentication	Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Charge-To	Contains account information for the costs of the application of the method requested	
Content-Encoding	The type of encoding used on the data.	Content-Encoding: gzip
Content-Length	The length of the response body in Octets (8-bit bytes)	Content-Length: 348
Content-Type	The mime type of the body of the request (used with POST and PUT requests)	Content-Type: application/x-www-form-urlencoded
Cookie	a HTTP cookie previously sent by the server with Set-Cookie (below)	Cookie: $Version=1; Skin=new;
Date	Date and time at which the message was originated	Date = "Date" ":" HTTP-date
ETag	An identifier for a specific version of a resource, often a message digest	ETag: "aed6bdb8e090cd1:0"
From	The email address of the user making the request	From: user@example.com
If-Modified-Since	Allows a 304 Not Modified to be returned if content is unchanged	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Last-Modified	The last modified date for the requested object, in RFC 2822 format	Last-Modified: Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Implementation-specific headers that may have various effects anywhere along the request-response chain.	Pragma: no-cache
Referrer	This is the address of the previous web page from which a link to the currently requested page was followed	Referrer: HTTP://www.edgenexus.io

Server	A name for the server	Server: Apache/2.4.1 (Unix)
Set-Cookie	an HTTP cookie	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
User-Agent	The user agent string of the user agent	User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Vary	Tells downstream proxies how to match future request headers to decide whether the cached response can be used rather than requesting a fresh one from the origin server	Vary: User-Agent
X-Powered-By	Specifies the technology (e.g. ASP.NET, PHP, JBoss) supporting the web application	X-Powered-By: PHP/5.4.0

Action

The action is the task or tasks that are enabled once the condition or conditions have been met.

Action

Double click on the Action column to view drop-down list.

Target

Double click on the Target column to view the drop-down list. The list will change depending on the Action.

You may also type manually with some actions.

Data

Double click on the Data column to manually add your data that you wish to add or replace.

The list of all the actions are detailed below:

Action	Description	Example
Add Request Cookie	Add request cookie detailed in the Target section with value in Data section	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Add Request Header	Add a request header of Target type with value in Data section	Target= Accept Data= image/png
Add Response Cookie	Add Response Cookie detailed in the Target section with value in Data section	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Add Response Header	Add request header detailed in the Target section with value in the Data section	Target= Cache-Control Data= max-age=8888888
Body Replace All	Search the Response Body and replace all instances	Target= HTTP:// (Search string) Data= HTTPs:// (Replacement string)

Body Replace First	Search the Response Body and replace first instance only	Target= HTTP:// (Search string) Data= HTTPs:// (Replacement string)
Body Replace Last	Search the Response Body and replace last instance only	Target= HTTP:// (Search string) Data= HTTPs:// (Replacement string)
Drop	This will drop the connection	Target= N/A Data= N/A
e-Mail	Will send an email to the address configured in Email Events. You can use a variable as the address or the message	Target= "flightPATH has emailed this event" Data= N/A
Log Event	This will log an event to the System log	Target= "flightPATH has logged this in syslog" Data= N/A
Redirect 301	This will issue a permanent redirect	Target= HTTP://www.edgenexus.io Data= N/A
Redirect 302	This will issue a temporary redirect	Target= HTTP://www.edgenexus.io Data= N/A
Remove Request Cookie	Remove request cookie detailed in the Target section	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Remove Request Header	Remove request header detailed in the Target section	Target=Server Data=N/A
Remove Response Cookie	Remove response cookie detailed in the Target section	Target=jnAccel
Remove Response Header	Remove the response header detailed in Target section	Target= Etag Data= N/A
Replace Request Cookie	Replace request cookie detailed in the Target section with value in the Data section	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Replace Request Header	Replace request header in the Target with Data value	Target= Connection Data= keep-alive
Replace Response Cookie	Replace the response cookie detailed in Target section with value in Data section	Target=jnAccel=afYfn1CDqqCDqCVii Date=MS-WSMAN=afYfn1CDqqCDqCVii
Replace Response Header	Replace the response header detailed in Target section with value in Data section	Target= Server Data= Withheld for Security
Rewrite Path	This will allow you to redirect the request to new URL based on the condition	Target= /test/path/index.html$querystring$ Data= N/A
Use Secure Server	Select which secure server or virtual service to use	Target=192.168.101:443 Data=N/A
Use Server	Select which server or virtual service to use	Target= 192.168.101:80 Data= N/A
Encrypt Cookie	This will 3DES Encrypt cookies and then base64 encode them	Target= Enter the cookie name to be encrypted, you may use the * as a wild card at the end Data= Enter a pass phrase for the encryption

Example:

The action below will issue a temporary redirect to the browser to a secure HTTPS Virtual Service. It will use the same hostname, path, and querystring as the request.

Common Uses

Application Firewall and Security

- Block unwanted IPs
- Force user to HTTPS for specific (or all) content
- Block or redirect spiders
- Prevent and alert cross-site scripting
- Prevent and alert SQL injection
- Hide internal directory structure
- Rewrite cookies
- Secure directory for particular users

Features

- Redirect users based on path
- Provide Single sign on across multiple systems
- Segment users based on User ID or Cookie
- Add headers for SSL offload
- Language detection
- Rewrite user request
- Fix broken URLs
- Log and Email Alert 404 response codes
- Prevent directory access/ browsing
- Send spiders different content

Pre-Built Rules

HTML Extension

Changes all .htm requests to .html

Condition:

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

Evaluation:

- Blank

Action:

- Action = Rewrite Path
- Target = $path$l

Index.html

Force to use index.html in requests to folders.

Condition: this condition is a general condition that will match most objects

- Condition = Host
- Sense = Does
- Check = Exist

Evaluation:

- Blank

Action:

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

Close Folders

Deny requests to folders.

Condition: this condition is a general condition that will match most objects

- Condition = this need proper thought
- Sense =
- Check =

Evaluation:

- Blank

Action:

- Action =
- Target =

Hide CGI-BBIN:

Hides cgi-bin catalogue in requests to CGI scripts.

Condition: this condition is a general condition that will match most objects

- Condition = Host
- Sense = Does
- Check = Match RegEX
- Value = \.cgi$

Evaluation:

- Blank

Action:

- Action = Rewrite Path
- Target = /cgi-bin$path$

Log Spider

Log spider requests of popular search engines.

Condition: this condition is a general condition that will match most objects

- Condition = Request Header
- Match = User-Agent
- Sense = Does
- Check = Match RegEX
- Value = Googlebot|Slurp|bingbot|ia_archiver

Evaluation:

- Variable = $crawler$
- Source = Request Header
- Detail = User-Agent

Action:

- Action = Log Event
- Target = [$crawler$] $host$$path$$querystring$

Force HTTPS

Force to use HTTPS for certain directory. In this case if a client is accessing anything containing the /secure/ directory then they will be redirected to the HTTPs version of the URL requested.

 Condition:

- Condition = Path
- Sense = Does
- Check = Contain
- Value = /secure/

Evaluation:

- Blank

Action:

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

Media Stream:

Redirects Flash Media Stream to appropriate service.

Condition:

- Condition = Path
- Sense = Does
- Check = End
- Value = .flv

Evaluation:

- Blank

Action:

- Action = Redirect 302

- Target = HTTP://$host$:8080/$path$

Swap HTTP to HTTPS

Change any hardcoded HTTP:// to HTTPS://

Condition:

- Condition = Response Code
- Sense = Does
- Check = Equal
- Value = 200 OK

Evaluation:

- Blank

Action:

- Action = Body Replace All
- Target = HTTP://
- Data = HTTPs://

Blank out Credit Cards

Check that there are no credit cards in the response and if one is found, blank it out.

Condition:

- Condition = Response Code
- Sense = Does
- Check = Equal
- Value = 200 OK

Evaluation:

- Blank

Action:

- Action = Body Replace All
- 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]+
- Data = xxxx-xxxx-xxxx-xxxx

Content Expiry

Add a sensible content expiry date to the page to reduce the number of requests and 304s.

Condition: this is a generic condition as a catch all. It is recommended to focus this condition on your

- Condition = Response Code
- Sense = Does
- Check = Equal
- Value = 200 OK

Evaluation:

- Blank

Action:

- Action = Add Response Header

- Target = Cache-Control
- Data = max-age=3600

Spoof Server Type

Get the Server type and change it to something else.

Condition: this is a generic condition as a catch all. It is recommended to focus this condition on your

- Condition = Response Code
- Sense = Does
- Check = Equal
- Value = 200 OK

Evaluation:

- Blank

Action:

- Action = Replace Response Header
- Target = Server
- Data = Secret

Never Send Errors

Client never gets any errors from your site.

Condition

- Condition = Response Code
- Sense = Does
- Check = Contain
- Value = 404

Evaluation

- Blank

Action

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

Redirect on Language

Find the language code and redirect to the related country domain.

Condition

- Condition = Language
- Sense = Does
- Check = Contain
- Value = German (Standard)

Evaluation

- Variable = $host_template$
- Source = Host
- Value = .*\.

Action

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

Google Analytics

Insert the code required by Google for the analytics – Please change the value MYGOOGLECODE to your Google UA ID.

Condition

- Condition = Response Code
- Sense = Does
- Check = Equal
- Value = 200 OK

Evaluation

- blank

Action

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

IPv6 Gateway

Adjust Host Header for IIS IPv4 Servers on IPv6 Services. IIS IPv4 servers do not like to see an IPV6 address in the host client request so this rule replaces this with a generic name.

Condition

- blank

Evaluation

- blank

Action

- Action = Replace Request Header
- Target = Host
- Data =ipv4.host.header

Web Application Firewall (edgeWAF)

The Web Application Firewall (WAF) is available on request and is licensed on an annual chargeable basis. Installation of the WAF is done using the inbuilt Apps section within the ADC.

Running the WAF

Running in a Docker Container, the WAF needs some network parameters to be set before starting it.

Option	Description
Stop	It will be greyed out until an Add-On instance is started. Press this button to Stop the Docker instance.
Pause	This button will pause the Add-On.
Play	It will start the Add-On with the current settings.
Container name	Give your container a name to identify it from the other containers. This must be unique. You may use this as the name for a Real Server if you wish and it will resolve automatically to the Internal IP address of the instance
External IP	Here you can set an External IP to access your Add-On. This may be to access the GUI of the Add-On as well as the service that runs via the Add-On. In the case of the Firewall Add-On this is the IP address of your HTTP service. The Firewall can then be configured to access a server or an ALB-X VIP that contains multiple servers for load balancing.
External Port	If you leave this blank, then all ports will be forwarded to your Firewall. To restrict this then simply add in the comma separated port list. Example 80, 443, 88. Note the Firewall GUI address will be **HTTP//[External IP]88/waf.** So, either leave the External Port setting blank or add in port 88 to access the GUI if you are restricting the port list.
Update	You can only update the settings of an Add-On once it has been stopped. Once your instance has stopped you can change the Container name, External IP and External Port settings.
Remove Add-On	Will completely remove the Add-On from the Add-On page. You will need to go to the Library–Apps page to deploy the Add-On again.
Parent Image	Indicates the Docker image that the Add-On is built from. There might be several versions of a Firewall or indeed another type of Add-On completely so this will help to distinguish between them. This section is for informational purposes only and therefore is greyed out.
Internal IP	Docker automatically creates the internal IP address and, therefore, cannot be edited. If you stop the Docker instance and restart, a new internal IP address will be issued. It is for this reason that you should either use an External IP address for you service or you use the Container Name for the Real Server Address of your service.
Started At	This will state the date and time the Add-On was started. Example 2016-02-16 155721
Stopped At	This will state the date and time the Add-On was stopped. Example 2016-02-24 095839

Example Architecture
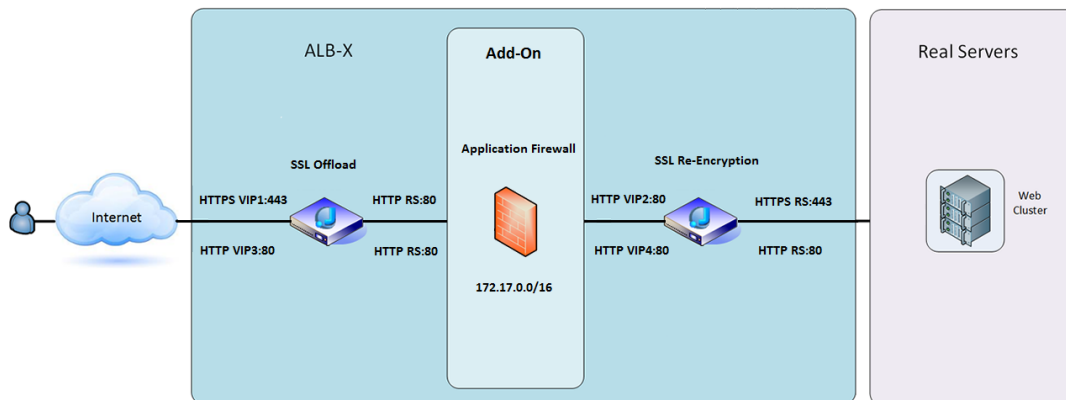
WAF using external IP address
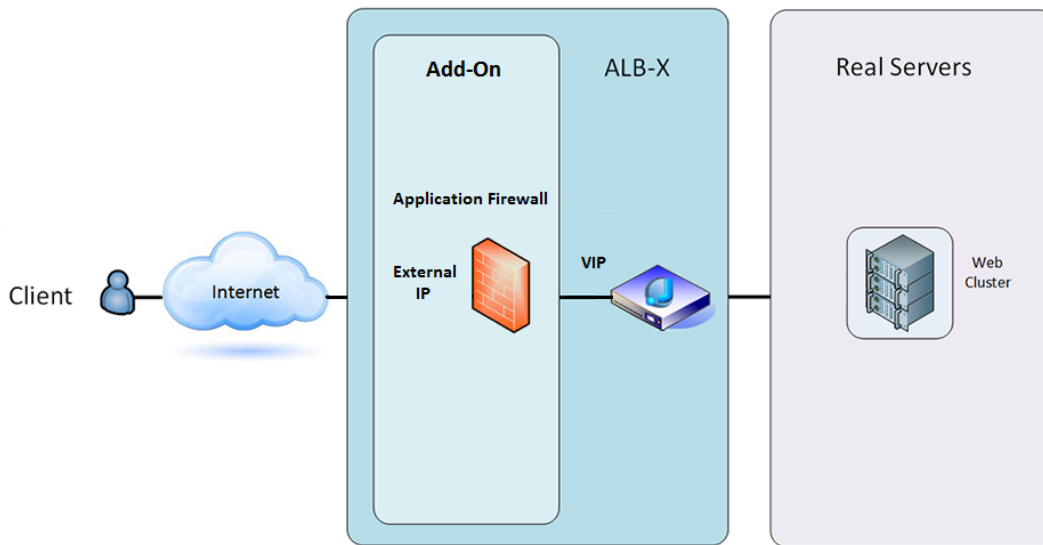
In this architecture, only HTTP can be used for your service as the Firewall cannot inspect HTTPS traffic.

The Firewall will need to be configured to send traffic on to the ALB-X VIP.

The ALB-X VIP, in turn, will be configured to load balance traffic to your web cluster.

WAF using internal IP address

In this architecture, you can specify HTTP and HTTPS.

HTTPS can be end-to-end where the connections from the Client to ALB-X are encrypted and from the ALB-X to the Real Servers.

The traffic from the ALB-X to the internal IP address of the firewall needs to be un-encrypted so that it can be inspected.

Once the traffic has passed through the Firewall, it is then forwarded to another VIP which can then either re-encrypt the traffic and load balance to secure servers or simply load balance to insecure servers over HTTP.

Accessing your WAF add-on

- Fill out the details for your Firewall
- You can either restrict your Ports to what you need or leave it blank to allow all ports

- Click the Play button
- An Add-On GUI button will appear
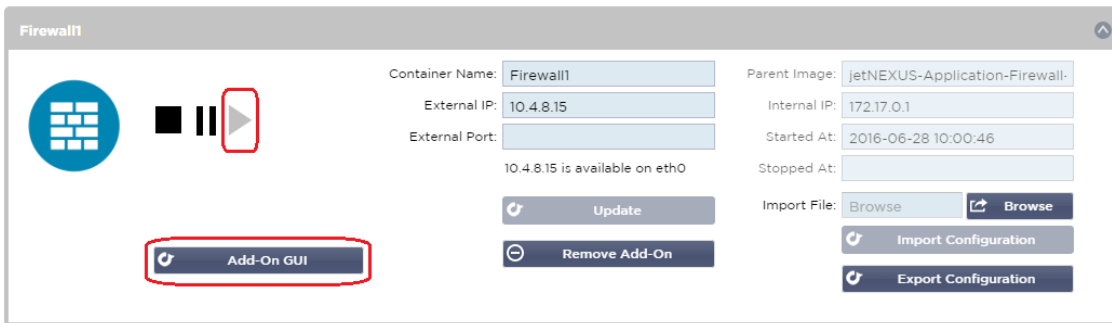
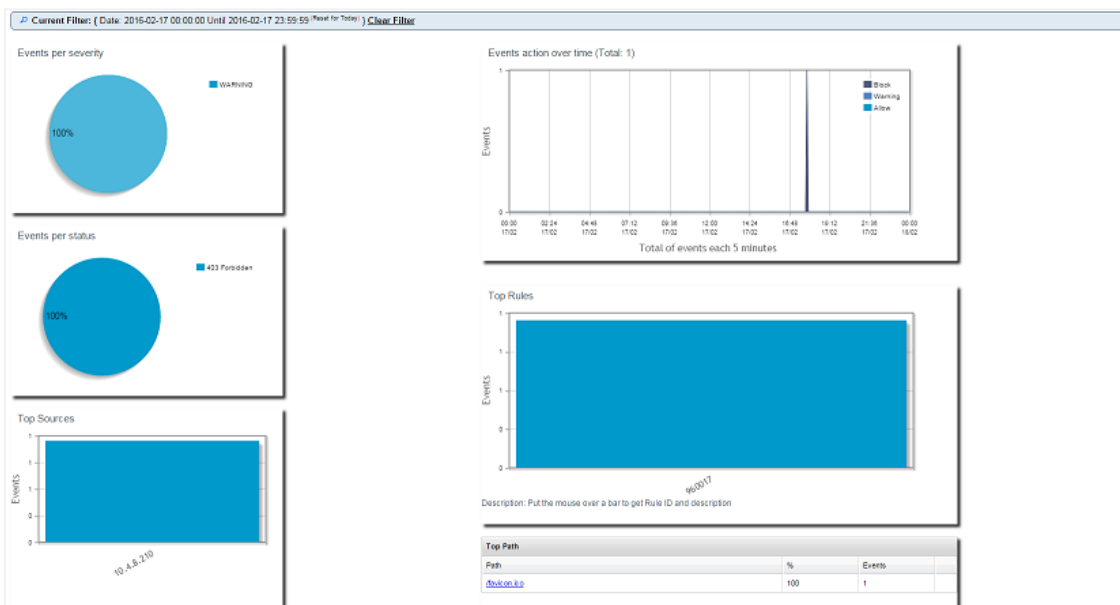- Click on this button, and it will open up a browser on HTTP://[External IP]:88/waf
- In this example, it will be HTTP://10.4.8.15:88/waf
- You will be presented with a login dialog.
- Enter the credentials for your ADC.
- On completion of a successful login, you will be presented with the home page of the WAF.

- The home page displays a graphical overview of the events, i.e., filtering actions performed by the Application Firewall.
- The graphs will most likely be blank when you first open the page as there will be no access attempts through the firewall.
- You can configure the IP address or the website's domain name you would like to send the traffic to after the firewall has filtered it.
- This can be changed in the Management > Config section
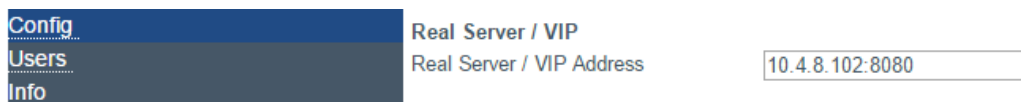
- The Firewall will inspect the traffic and then send it to the Real Sever IP or VIP address here. You may also enter a port along with your IP address. If you enter an IP address on its own, the port will be assumed to be port 80. Click the "Update Configuration" button to save this new setting.
- When the Firewall blocks an application resource, the rule that is blocking traffic will appear in the Blocking Rules list on the Whitelist page.
- To prevent the firewall from blocking the valid application resource, please move the blocking rule to the Whitelist Rules section.

Firewall Control

○ Disabled
○ Detection only
● Detection and blocking

Blocking Rules   **Whitelisted Rules**

960017 (Host header is a numeric IP address)	

Manually add rule IDs to whitelsit

[Update configuration]

- Press Update Configuration when you have transferred all the rules from the Blocking section to the Whitelist section.

Updating Rules

- Application Firewall rules can be updated by accessing the Advanced — Software section
- Click Refresh to view the available software button in the Software Upgrade Details section
- An additional box called Download from Cloud is now displayed
- Check to see if there is an OWASP Core Rule set available

Download from Cloud

Code Name	Release Date	Version	Build
OWASP Core Rule Set Update for jetNEXUS Application Firewall	2016-02-09	OWASP	jetNEXUS (Firewall)

[Download Selected Software to ALB]

- If so, you can highlight and click Download Selected Software to ALB-X
- This action will then download the smart file to the Apply Software stored on ALB

Apply Software stored on ALB

[⊖ Remove]

Image	Code Name	Release Date	Version	Build	Notes
🔵	jetNEXUS-WAF-OWASP-CRS	23 Nov 2015	1.0		jetNEXUS Application Firewall OWASP Core Rule Set

[Apply Selected Software Update]

- Highlight the jetNEXUS-WAF-OWASP-CRS and click Apply Selected Software Update and click Apply
- The Firewall will automatically detect the updated rule set, load, and apply it.
- The IDs of Whitelisted rules will be kept. However, new rules may start blocking valid application resources.
- Please check the Blocking Rules list on the Whitelist page in this case.
- You can also check the Management Info section of the Firewall GUI for the OWASP CRS Version

jetNEXUS WAF Version:	1.0.0
OWASP CRS Version:	2.2.9 (24 Feb 2016)
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

Config
Users
Info

Global Server Load Balancing (edgeGSLB)

Introduction

Global Server Load Balancing (GSLB) is a term used to describe methods for distributing network traffic around the Internet. GSLB is different from Server Load Balancing (SLB) or Application Load Balancing (ALB), as it's typically used to distribute traffic between multiple data centers, whereas a traditional ADC/SLB is used to distribute traffic within a single data center.

GSLB is typically used in the following situations:

Resiliency and disaster recovery

You have multiple data centers, and you wish to run them in an Active-Passive situation so that if one data center fails, traffic will be sent to the other.

Load balancing and geo-location

You would like to distribute traffic between data centers in an Active-Active situation based on specific criteria such as data center performance, data center capability, data center health check, and the client's physical location (so you can send them to their closest data center), etc.

Commercial considerations

Ensure users from specific geographic locations are sent to particular data centers. Ensure different content is served (or blocked) to other users, depending on several criteria such as the country that the client is in, the resource they are requesting, the language, etc.

Domain Name System Overview

GSLB can be complex; thus, it is worth spending the time to understand how the mysterious Domain Name Server (DNS) system works.

DNS consists of three key components:

- The DNS resolver, i.e., the Client: the resolver is responsible for initiating the queries that ultimately lead to a full resolution of the resource required.
- Nameserver: this is the nameserver that the client initially connects to perform DNS resolution.
- Authoritative Name Servers: Include the Top Level Domain (TLD) nameservers and root nameservers.

A typical DNS transaction is explained below:

- A user types 'example.com' into a web browser, and the query travels into the Internet and is received by a DNS recursive resolver.
- The resolver then queries a DNS root nameserver (.).
- The root server then responds to the resolver with the address of a Top-Level Domain (TLD) DNS server (such as .com or .net), which stores the information for its domains. When searching for example.com, our request is pointed toward the .com TLD.
- The resolver then requests the .com TLD.
- The TLD server then responds with the IP address of the domain's nameserver, example.com.
- Lastly, the recursive resolver sends a query to the domain's nameserver.
- The IP address, for example.com, is then returned to the resolver from the nameserver.
- The DNS resolver then responds to the web browser with the IP address of the domain requested initially.
- Once the eight steps of the DNS lookup have returned the IP address, for example.com, the browser can request the web page:
- The browser makes an **HTTP** request to the IP address.
- The server at that IP returns the webpage to be rendered in the browser.

This process can be further complicated:

Caching

Resolving nameservers cache responses can send the same response to many clients. Client-side resolvers and applications may have different caching policies.

Note: For testing, we stop and disable the Windows DNS Client within the services section of your operating system. The DNS names will continue to be resolved; however, it will not cache the results or register the computer's name. Your system administrator will need to decide if this is the best option for your environment, as it may affect other services.

Time To Live

The resolving name server may ignore the Time To Live (TTL) i.e., the caching time for the response.

GSLB Overview

GSLB is based on DNS and uses a very similar mechanism as described above.

The ADC can change the response based on several factors described later in the guide. The ADC makes use of the monitors checking for availability of remote resources by accessing the resource itself. However, to apply any logic, the system must first receive the DNS request.

Several designs allow this. The first is where the GSLB acts as the authoritative nameserver.

The second design is the most common implementation and is similar to the authoritative nameserver configuration but uses a sub-domain. The primary authoritative DNS server is not replaced by GSLB but delegates a sub-domain for resolution. Either directly delegating names or using CNAMEs allows you to control what is and is not handled by the GSLB. In this case, you don't have to route all the DNS traffic to the GSLB for systems that don't require GSLB.

Redundancy is provided so that if one nameserver (GSLB) fails, then the remote nameserver automatically issues another request to another GSLB, preventing the website from going down.

GSLB Configuration

After downloading the GSLB Add-On, please deploy it by visiting the Library > Apps page of the ADC GUI and clicking the "Deploy" button as shown below.
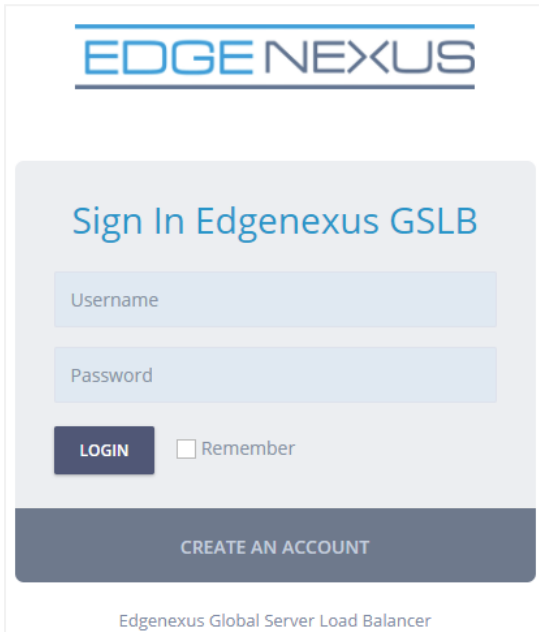

Following installation, please configure GSLB Add-On details, including Container name, External IP and External Ports in the Library > Add-Ons page of the ADC GUI as shown in the figure below.

- Container Name is a unique name of a running Add-On instance, hosted by ADC, it is used to distinguish multiple Add-Ons of a same kind.
- External IP is the IP on your network that will be assigned to GSLB.
- You must configure the GSLB to have an external IP address if you want to make GEO based decisions, as this will enable the GSLB to view the clients real IP address.
- External Ports is the list of TCP and UDP ports of GSLB, which can be accessed from other network hosts.
- Please put "53/UDP, 53/TCP, 9393/TCP" in the External Ports input box to allow DNS (53/UDP, 53/TCP) and edgeNEXUS GSLB GUI communications (9393/TCP).
- After configuring the Add-On details, please click the Update button.
- Start the GSLB Add-On by clicking the Run button.

- The next step is to allow the edgeNEXUS GSLB Add-On to read and change the ADC configuration.
- Please visit the System > Users page of ADC GUI and edit a user with the same name as the GSLB Add-On you have deployed, as shown in the figure below.
- Edit "gslb1" user and tick API, then click Update – in later versions of the software may already be ticked by default.

- The next step is only required if you are configuring GSLB for testing or evaluation purposes and do not want to modify any DNS zone data on the internet.
- In this case, please instruct the ADC to use GSLB Add-On as its primary DNS resolving server by altering "DNS Server 1 in the System > Network page of the ADC GUI, as shown in the figure below.
- DNS Server 2 can be configured generally with your local DNS server or one out on the internet, such as Google 8.8.8.8.

- Now is the time to log in to GSLB GUI.
- Please navigate to the Library > Add-Ons page of the ADC GUI and click the Add-On GUI button.
- Clicking will open a new browser tab that presents the GSLB GUI log-in page, as shown below.

- The default username is admin, and the default password is jetnexus. Please don't forget to change your password on the Administrator > My Profile page of GSLB GUI.
- The next step in the configuration sequence is to create a DNS zone in the PowerDNS nameserver, which is a part of GSLB, making it either an authoritative nameserver for the "example.org" zone or a subdomain zone, such as "geo.example.org" subdomain mentioned in the "DNS-based GSLB Overview" section above.
- For in-depth details on DNS zone configuration, please see the **POWERDNS NAMESERVER DOCUMENTATION**. An example zone is shown in Figure 6.

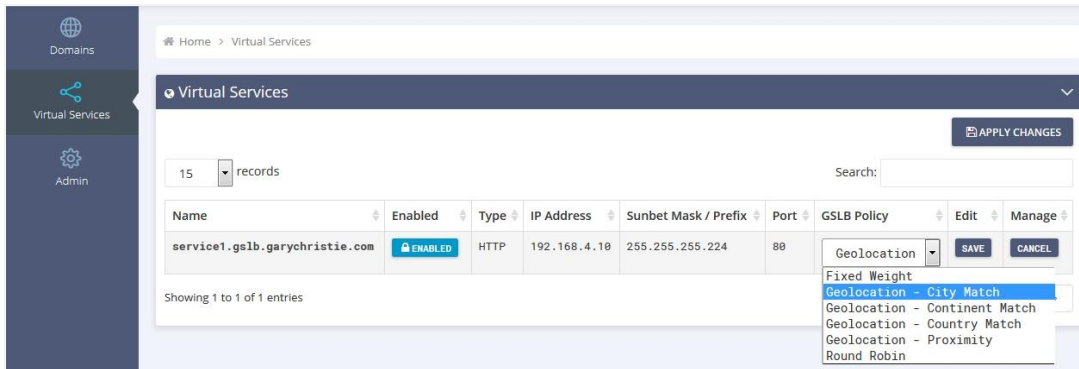* edgeNEXUS GSLB GUI is based on an Open Source project PowerDNS-Admin.

- After creating a DNS zone, please click the Manage button and add hostnames to the domain, as shown in the figure below.
- After you edit any existing records within the GSLB GUI, please press the Save button.
- After you have completed creating hostname records, please click the Apply Changes button. If you don't click Apply and then amend the page, you will lose your changes.
- Below we have created records which are IPv4 address records.
- Please ensure you create a record for all the records you wish to have resolved, including AAAA records for IPv6 addresses.
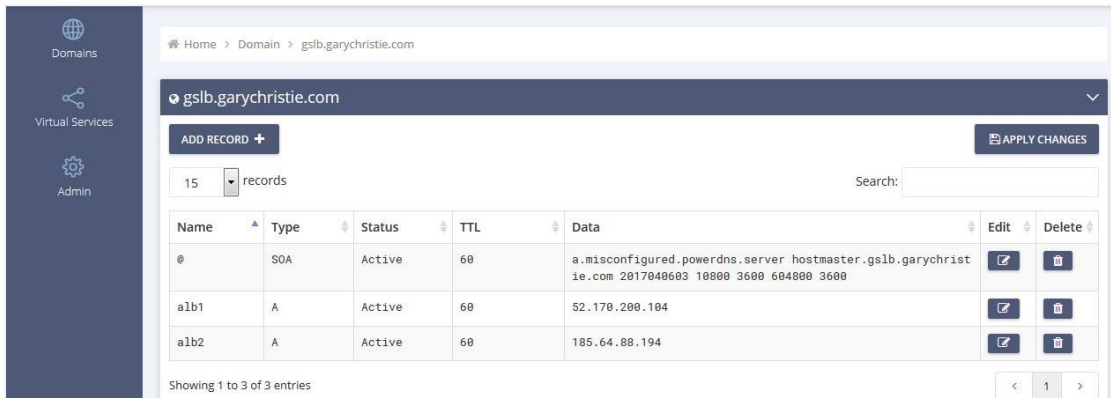
- Now, let's go back to the ADC GUI and define a Virtual Service that corresponds to the DNS zone we have just created.
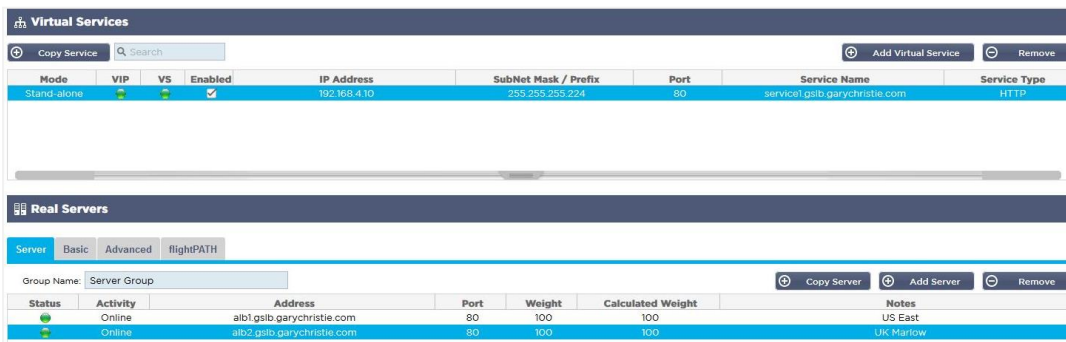
- The Virtual Service will be used for health checking of the servers in the GSLB domain.
- The GSLB leverages the ADC health checking mechanism, including custom monitors. It can be used with any of the Service Types supported by the ADC.
- Please navigate to the Services > IP-Services page of the ADC GUI and create a Virtual Service, as shown in the figure below.
- Be sure to configure the Service Name with the correct domain name you wish to use in the GSLB. The GSLB will read this via the API and automatically populate the Virtual Services section in the GSLB GUI.
- Please add all the servers in the GSLB domain under the Real Servers section of the above image.
- You may specify servers, either by their domain names or IP addresses.
- If you specify the domain names, then it will use the records created on your GSLB.
- You may choose different server health monitoring methods and parameters in the Basic and Advanced tabs.
- You may set the activity of some servers to Standby for an Active-Passive scenario.
- In this case, if an "Online" server fails a health check and there is a healthy Standby server, Edgenexus EdgeGSLB will resolve the domain name to an address of the Standby server.
- Please refer to the **VIRTUAL SERVICES** section for details on configuring Virtual Services.
- Now, let's move to the GSLB GUI.
- Navigate to the Virtual Services page and select a GSLB policy for the API's domain retrieved from the ADC virtual services section.
- This is shown in the figure below.

- The GSLB supports the following policies:

Policy	Description
Fixed Weight	The GSLB selects the server with the highest weight (server weighting can be assigned by the user). In the case where multiple servers have the highest weight, GSLB will select one of these servers at random.
Weighted Round Robin	Choose servers one by one, in a row. Servers that have higher weights are selected more often than servers that have lower weights.
Geolocation	Proximity - choose a server that is located closest to the client's location using geographical latitude and longitude data. Servers in the same country as the client are preferred, even if they are more distant than servers in neighbouring countries.
Geolocation	City match – choose a server in the same city as the client. If there is no server in the client's city, select a server in the client's country. If there is no server in the client's country, select a server in the same continent. If this is not possible, select a server that is located closest to the client's location using geographical latitude and longitude data.
Geolocation	Country match – choose a server in the same country as the client. If there is no server in the same country, try the same continent, then try closest location.
Geolocation	Continent match – choose a server in the same continent as the client. If there is no server in the same continent, try closest location.

- After you have selected a GSLB Policy, please don't forget to click the Apply Changes button.
- Now you may review and adjust the Virtual Service details by clicking the Manage button.
- This will present a page shown below.
- If you have selected one of the weight-based policies, you may need to adjust the server GSLB weights.
- If you have selected one of the geo-location-based GSLB Policies, you may need to specify geographical data for the servers.
- If you don't specify any geographical data for the servers, the GSLB will use the data provided by **MAXMIND'S GEOLITE2 DATABASE**.
- You may also modify the server name, port, and activity on this page.
- These changes will be synced with the ADC when you click the "Apply Changes" button.

- A great way to check what answers the GSLB will send back to the clients is to use NSLOOKUP.
- If you are using Windows, the command is below.

  NSLOOKUP service1.gslb.garychristie.com 192.168.4.10

- Where service1.gslb.garychristie.com is the domain name that you wish to resolve.
- Where 192.168.4.10 is the External IP Address of your GSLB.
- To check what IP address will be returned out on the internet, you can use the google DNS server of 8.8.8.8.

  Nslookup service1.gslb.garychristie.com 8.8.8.8.

- Alternatively, you can use something like HTTPs://dnschecker.org.
  Example HTTPs://dnschecker.org/#A/service1.gslb.garychristie.com.
- See below for an example of the results.

Custom Locations

Private Networks

The GSLB can also be configured to use custom locations so that you can use it on internal "private" networks. In the scenario above, the GSLB determines the client location by cross-referencing the client's public IP address with a database to work out its location. It also works out the service IP address location from the same database, and if the load balancing policy is set to a GEO policy, it will return the closest IP address. This method works perfectly well with public IP addresses, but there is no such database for internal private addresses that conform to RFC 1918 for IPv4 addresses and RFC 4193 for IPv6 addresses.

Please see the Wikipedia page explaining private addressing **HTTPs://en.wikipedia.org/wiki/Private_network**

How it works

Typically, the idea behind using our GSLB for internal networks is so that users from specific addresses will receive a different answer for a service depending on which network they are located in. So, let's consider two data-centers, North and South, providing a service called north.service1.gslb.com and south.service1.gslb.com, respectively. When a user from the Northern data-center queries the GSLB, we want the GSLB to respond with the IP address associated with north.service1.gslb.com provided the

service is working correctly. Alternatively, if a user from the Southern data-center queries the GSLB, we want the GSLB to respond with the IP address associated with south.service1.gslb.com again, providing the service is working correctly.

So, what do we need to do to make the above scenario happen?

- We need to have at least two Custom Locations, one for each data-center
- Assign the various private networks to these locations
- Assign each service to the respective location

How do we configure this look on the GSLB?

Add a location for the Northern Data Center

- Click on Custom Locations on the left-hand side
- Click Add Location
- Name
  - North
- Add a private IP address and subnet mask for your Northern network. For this exercise, we will assume that the service and the client IP addresses are in the same private network
  - 10.1.1.0/24
- Add the Continent code
  - EU
- Add the Country code
  - UK
- Add City
  - Enfield
- Add Latitude – obtained from google
  - 51.6523
- Add Longitude – obtained from google
  - 0.0807

Note, please use the correct code's which can be obtained from here

Add a location for the Southern Data Center

- Click on Custom Locations on the left-hand side
- Click Add Location
- Name
  - South
- Add a private IP address and subnet mask for your Southern network. We will assume that the service and the client IP addresses are in the same private network for this exercise.
  - 192.168.1.0/24
- Add the Continent code
  - EU
- Add the Country code
  - UK
- Add City
  - Croydon
- Add Latitude – obtained from google
  - 51.3762
- Add Longitude – obtained from google
  - 0.0982

Note, please use the correct code's which can be obtained from **HERE**

Add an A record for north.service1.gslb.com

- Click on the domain service1.gslb.com
- Click Add Record
- Add Name
  - North
- Type
  - A
- Status
  - Active
- TTL
  - 1 Minute
- IP Address
  - 10.1.1.254 (Note this is in the same network as the location Enfield)

Add an A record for south.service1.gslb.com

- Click on the domain service1.gslb.com
- Click Add Record
- Add Name
  - South
- Type
  - A
- Status
  - Active
- TTL
  - 1 Minute
- IP Address
  - 192.168.1.254 (Note this is in the same network as the location Croydon)

Traffic Flow

Example 1 – Client in Northern Data-Center

- Client IP 10.1.1.23 queries GSLB for service1.gslb.com
- GSLB looks up the IP address 10.1.1.23 and matches it with Custom Location Enfield 10.1.1.0/24
- GSLB looks at its A records for the service1.gslb.com and matches north.service1.gslb.com as it is also in the network 10.1.1.0/24
- GSLB responds to 10.1.1.23 with the IP address 10.1.1.254 for service1.gslb.com

Example 2 – Client in Southern Data-Center

- Client IP 192.168.1.23 queries GSLB for service1.gslb.com
- GSLB looks up the IP address 192.168.1.23 and matches it with Custom Location Croydon 192.168.1.0/24
- GSLB looks at its A records for the service1.gslb.com and matches south.service1.gslb.com as it is also in the network 192.168.1.0/24
- GSLB responds to 192.168.1.23 with the IP address 192.168.1.254 for service1.gslb.com

- Client IP 10.1.1.23 queries GSLB for service1.gslb.com
- GSLB looks up the IP address 10.1.1.23 and matches it with Custom Location Enfield 10.1.1.0/24
- GSLB looks at its A records for the service1.gslb.com and matches north.service1.gslb.com as it is also in the network 10.1.1.0/24
- GSLB responds to 10.1.1.23 with the IP address 10.1.1.254 for service1.gslb.com

Technical Support

We provide technical support for all our users per the company's standard terms of service.

We will provide all support via technical support if you have an active Support and Maintenance contract for the edgeADC, edgeWAF, or edgeGSLB.

To raise a support ticket, please visit:

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

Technical Support