EDGENEXUS

ALB-X User Guide
Software Version
4.1.4 (Build 1653)

4.1.4

IP Services

The**Setup ---> IP Services** page allows you to add, delete and configure IP Services. The settings are organised into the following sections

Virtual Services

A **Virtual Service** is a combination of a **Virtual IP (VIP)** and a **TCP/UDP** port that the **jetNEXUS ALB-X** will listen on
- Traffic arriving at the **Virtual Service** is directed to one of the **Real Servers** that are associated with that service
- The **Virtual Service** IP address cannot be the same as the management address of the jetNEXUS ALB-X. i.e. eth0, eth1 etc...
- The **jetNEXUS ALB-X** determines how the traffic is distributed to the **Real Servers** based on a load balancing policy set within the **Basic** tab

Create a new Virtual Service using a new VIP

- Click **Add Virtual Service**. You will then enter row edit mode. The 4 boxes highlighted in red must be completed before you can update

- The **IP Address** box should contain a blinking cursor so just start typing your Virtual IP address and then **TAB** to the next box
- Enter the **Subnet Mask** and **TAB** to the next box
- Enter the **Port Number** for your service and **TAB** to the next box
- Enter an optional **Service Name** and **TAB** to the next box
- Use the down arrows on your keyboard or select a **Service Type** using your mouse
- You can now press the **Update** button to save this section and jump automatically to the **Real Server** section below

- Leave the server in the **Online Activity -** this means it will be load balanced if it passes the default health monitor of **TCP Connect**
- Enter an **IP address** for the real server and **TAB** to the next box
- Enter a **Port Number** for the real server and **TAB** to the next box
- Enter an optional name for the **Real Server**
- Click **Update** or press **Enter** to save your changes
- The **Status** light will first turn Grey then **Green Server Heath 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

Example of a completed Virtual Service with 2 Real Servers

Create a new Virtual Service using the same VIP

- Highlight a **Virtual Service** with the IP address you wish to copy
- Click **Add Virtual Service** to enter row edit mode

- The **IP Address** and **Subnet Mask** will be copied automatically
- Enter the **Port Number** for your service and **TAB** to the next box
- Enter an optional **Service Name** and **TAB** to the next box
- Use the down arrows on your keyboard or select a **Service Type** using your mouse
- You can now press the **Update** button to save this section and jump automatically to the **Real Server** section below

- Leave the server in the **Online Activity -** this means it will be load balanced if it passes the default health monitor of **TCP Connect** which can be changed later
- Enter an **IP address** of the real server and **TAB** to the next box
- Enter a **Port Number** for the real server and **TAB** to the next box
- 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 your **Virtual Services**

- Highlight a service with the IP address you would like to change

Primary	VIP Status	Service St...	Enabled	IP Address	SubNet Mask	Port	Service Name	Service Type
Active	●	●	☑	192.168.1.1	255.255.255.0	80	Service 1	Layer 4 TCP
		●	☑	192.168.1.1	255.255.255.0	81	Service 2	Layer 4 TCP
		●	☑	192.168.1.1	255.255.255.0	82	Service 3	Layer 4 TCP

- Double Click into the **IP address** column
- Change the **IP address** and click **Update**
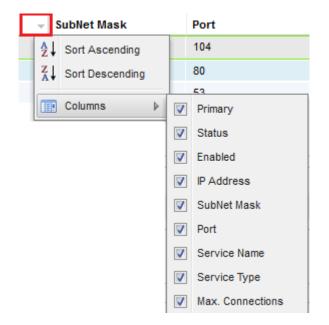
Primary	VIP Status	Service St...	Enabled	IP Address	SubNet Mask	Port	Service Name	Service Type	
Active	🟢	🟢	☑	192.168.1.1	255.255.255.0	80	Service 1	Layer 4 TCP	
		🟢	☑	192.168.1.1	255.255.255.0	81	Service 2	Layer 4 TCP	
			☑	192.168.1.2	255.255.255.0	82	Service 3	Layer 4 TCP	▼

↻ Update   ⊖ Cancel

- This will change the IP address of ALL **Virtual Services** associated with this VIP

Primary	VIP Status	Service St...	Enabled	IP Address	SubNet Mask	Port	Service Name	Service Type
Active	🟢	🟢	☑	192.168.1.2	255.255.255.0	80	Service 1	Layer 4 TCP
		🟢	☑	192.168.1.2	255.255.255.0	81	Service 2	Layer 4 TCP
		🟢	☑	192.168.1.2	255.255.255.0	82	Service 3	Layer 4 TCP

Filtering and Sorting

To the far right of each column is small down arrow (see the red box below). Clicking on this will reveal an extra submenu that allows you to "Sort Ascending", "Sort Descending" and "Columns". Add and remove the tick to show/hide the columns listed below.

▼	**SubNet Mask**	**Port**
A↓ Sort Ascending		104
Z↓ Sort Descending		80
		53
▦ Columns ▶	☑ Primary	
	☑ Status	
	☑ Enabled	
	☑ IP Address	
	☑ SubNet Mask	
	☑ Port	
	☑ Service Name	
	☑ Service Type	
	☑ Max. Connections	

Primary

The **Primary** column contains different information depending on the high availability role that has been selected from the **Cluster** page High Availability Role

1. **Cluster**
   - **This is the default role for a new ALB-X and as such the Primary column will indicate whether the ALB-X is either Active or Passive**
2. **Manual**
   - **In this role the ALB-X can be Active Active for different Virtual IP addresses and as such the Primary column will contain a box next to each unique Virtual IP that can be ticked for Active or left un-ticked for Passive**
3. **Stand-Alone**
   - The **ALB-X** is acting alone and is not in **High Availability** mode and as such the **Primary column** will say **Stand-alone**

VIP Status - This will provide visual feedback for the status of the Virtual IP address and all asociated virtual services

- Online
- Failover-Standby. This virtual service is hot-standby
- Indicates a "secondary" is holding off for a "primary"
- Offline. Content servers are unreachable or no content servers enabled
- Finding status
- Not licensed or licensed Virtual IPs exceeded

Service Status - This will provide visual feedback for the status of each individual virtual service

- Online
- Failover-Standby. This virtual service is hot-standby
- Indicates a "secondary" is holding off for a "primary"
- Service Needs attention. This may be the result of 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. Content servers are unreachable or no content servers enabled
- Finding status
- Not licensed or licensed Virtual IPs exceeded

Enabled

By default the box is ticked to enable the **Virtual Service**. Double click on the row to edit and remove the tick to disable the **Virtual Service**

IP Address

Add in your IPv4 address in decimal dotted notation. This is the Virtual IP address for your service. Example "192.168.1.100"

Subnet Mask

Add in your subnet mask in decimal dotted notation. Example "255.255.255.0"

Port

Add in the port number associated with your service. This may be TCP or UDP port number. Example "80" for 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, edgeNEXUS will not interact or modify the data stream so flightPATH will not work with these service types. It will simply load balance the traffic according to the load balancing policy

Layer 4 TCP:
Any TCP port (Layer 4). edgeNEXUS will not alter any information in the data stream and will simply load balance the traffic according to the load balancing policy

Layer 4 UDP:

Any UDP port (Layer 4) This will change the connectivity to **Basic** and is only available in this mode. edgeNEXUS will not alter any information in the data stream and will simply load balance the traffic according to the load balancing policy

Layer TCP/UDP:

Any TCP or UDP port (Layer 4) This will change the connectivity to **Basic** and is only available in this mode. This is ideal if your service has a primary protocol such as UDP but will fall back to TCP

HTTP:

HTTP(s) Protocol (Layer 7)**.** jetNEXUS ALB-X has the ability to 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)

POP3:

Post Office Protocol (Layer 4)

IMAP:

Internet Message Access Protocol (Layer 4)

RDP:

Remote Desktop Protocol (Layer 4)

RPC:

Remote Procedure Call (Layer 4)

RPC/ADS:

Exchange 2010 Static RPC for Address Book Service (Layer 4)

RPC/CA/PF:

Exchange 2010 Static RPC for Client Access & Public Folders (Layer 4)

DICOM:

Digital Imaging and Communications in Medicine (Layer 4)

Max. Connections

This limits the number of simultaneous real server connections and can be set per service. For example if you set this to 1000 and have two real servers then the jetNEXUS ALB-X will limit 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 in this case. Leave this blank for unlimited connections. This will depend on your system resources.

Real Servers

The **Server** tab contains the **Real Server** details associated with the highlighted **Virtual Service**. You will be prompted to add at least one **Real Server** when setting up a **Virtual Service**.

Add a new Real Server to a Virtual Service

1. Click **Add Server**
2. A new row will appear with the cursor blinking on the IP Address column

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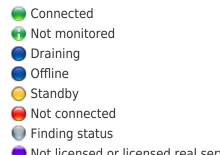
1. Enter the IPv4 address of your server in dotted decimal notation. The **Real Server** can be on the same network as your **Virtual Service**, any directly attached local network or any network that your edgeNEXUS can route to. Example "10.1.1.1".
2. Tab to the **Port** column and enter the TCP/UDP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

Real Server Details

Group Name:

- This is the name you can associate with a particular group of servers. For Example "Exchange 2010 CAS Array"
- This name will be automatically saved once edited
- In this version of software there is no additional functionality, however in future releases we will include the ability to add or link server groups once they have been configured

Real Server Status Lights

- 🟢 Connected
- 🟢 Not monitored
- 🔵 Draining
- 🔵 Offline
- 🟡 Standby
- 🔴 Not connected
- ⚪ Finding status
- 🟣 Not licensed or licensed real servers exceeded

Activity

If you wish to change the **Activity** of a **Real Sever**, click on a row to highlight then click again to enter row edit mode. You can now select an **Activity** from the drop down menu

Online:

    All **Real Servers** assigned as **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 🔵 whilst draining. Once the existing connections have closed naturally the **Real Servers** will be taken offline and the **Status** light will be solid blue 🔵. You can also view these connections on the **Navigation--Monitor--Status** page

Offline:

    All **Real Servers** assigned as **Offline** will immediately be taken offline and will not receive any traffic

Standby:

    All **Real Servers** assigned as **Standby** will remain offline until **ALL** of the **Online** group fail their **Server Health Montior**, at which point members of the **Standby** group will be sent traffic according to the load balancing policy. If one of the **Online** group passes the **Server Health Monitor** this **Online** server will receive all of the traffic and the **Standby** group will be no longer receive traffic.

IP Address

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

Port

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

Notes

Add in some useful notes about the particular server. Example "IIS Server1 - London DC".

Basic

Load Balancing Policy

Select from the drop down list how you would like the traffic to be load balanced. **Round Robin:**
This is the simplest method. Each **Real Server** receives a new request in sequence. This method is useful to load balance evenly however it does not take in to account how busy each server is and can add to the burden of busy servers.

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 will be sent the next new request.

Layer 3 Session Affinity/Persistence:
IP Bound:
In this situation the client's IP address is used to select which back end server will receive the request. This provides persistence. It can be used with HTTP or layer 4 protocols. This method is useful 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, X-Forwarded-For information is used, if present, to cope with proxies.

IP List Based:
The initial connection to the **Real Server** is made using "Least connections" then session affinity is achieved based on Clients IP. A list is maintained for 2 hours by default but this can be changed using a jetPACK

Layer 7 Session Affinity/Persistence:
ALB Session Cookie:
This is the one of the most popular persistence method for HTTP. In this situation, IP list based load balancing is used for each first request. A cookie is inserted into the headers of the first http response. Thereafter, jetNEXUS ALB-X uses the client cookie to route traffic to the same back end server. Again this is used for persistence, when the client must go to the same back end server each time. The cookie will expire after the session is closed.

ALB Persistent Cookie: In this situation, IP list based load balancing is used for each first request. A cookie is inserted into the headers of the first http response. Thereafter, jetNEXUS ALB-X uses the client cookie to route traffic to the same

back end server. Again this 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 IP List Based algorithm This is a configurable time that can be changed using a jetPACK.

Session Cookie:

    Classic ASP Session Cookie:
    Active Server Pages (ASP) is a Microsoft server-side technology. With this option selected the ALB-X will maintain session persistence to the same server if an ASP cookie is detected and is found in its list of known cookies. If a new ASP cookie is detected then it will be load balanced using the least connections algorithm.

    ASP.NET Session Cookie: ASP.NET is a Microsoft server-side technology. With this option selected the ALB-X will maintain session persistence to the same server if an ASP.NET cookie is detected and is found in its list of known cookies. If a new ASP.NET cookie is detected then it will be load balanced using the least connections algorithm.

    JSP Session Cookie: Java Server Pages (JSP) is an Oracle server-side technology. With this option selected the ALB-X will maintain session persistence to the same server if a JSP cookie is detected and is found in its list of known cookies. If a new JSP cookie is detected then it will be load balanced using the least connections algorithm.

    JAX-WS Session Cookie: Java web services (JAX-WS) is an Oracle server-side technology. With this option selected the ALB-X will maintain session persistence to the same server if a JAX-WS cookie is detected and is found in its list of known cookies. If a new JAX-WS cookie is detected then it will be load balanced using the least connections algorithm.

    PHP Session Cookie: Personal Home Page (PHP) is an open source server-side technology. With this option selected the ALB-X will maintain session persistence to the same server if a PHP cookie is detected.

Server Monitoring

Your jetNEXUS ALB-X contains six standard **Real Server Monitoring** methods listed below. Choose one to apply to the **Virtual Service**. Please make sure that you apply a relevant monitor to the **Virtual Service**. If the **Real Server** is an RDP server then a 200 OK monitor is not relevant. If you are unsure which monitor to choose, the default **TCP Connect** is a good place to start.

None:

In this mode, the content server is not monitored at all and is assumed to be always up and running correctly. This is useful for situations where monitoring upsets a server and for services that should not join in the fail-over action of ALB-X. It can be viewed as a way of hosting unreliable or legacy systems that are not core to H/A operation. This monitoring method can be used with any service type.

Ping/ICMP Echo:

In this mode, ALB-X sends an ICMP echo request to the IP of the content server. If a valid echo response is received, the content server is deemed to be up and running and traffic will be sent to it. It will also then keep the service available on an H/A pair. This monitoring method can be used with any service type

TCP Connection:

In this mode, a TCP connection is made to the content server and immediately broken without sending any data. If the connection succeeds, the content server is deemed to be up and running. This monitoring method can be used with any TCP service type. UDP services are the only ones currently not appropriate for TCP Connection monitoring

RDP:

In this mode, a TCP connection is made as above, but after the connection is made a layer 7 RDP connection is requested. If the connection is confirmed the content server is deemed to be up and running. This monitoring method can be used with Microsoft terminal servers

200 OK:

In this mode, a TCP connection is made to the content server as above, but after connection is made, a brief HTTP request is made to the content server. A HTTP response is waited for and it is checked for the "200 OK" response code. If the "200 OK" response code is received, the content server is deemed to be up and running. If, for any reason, the "200 OK" response code is not received, including timeouts, failure to connect, etc, then the content server is regarded as

down. This monitoring method can only really be used with HTTP and Accelerate HTTP service types, although 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 content server, or is handled appropriately by the "Content SSL" facility

DICOM:

In this mode, a TCP connection is made to the content server as above, but after a connection is made, an Echoscu "Associate Request" is made to the content server. 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 for any reason the monitor does not complete successfully then the content server is regarded as down

User Defined:

Any monitor configured in the Real Server Monitoring section will appear in the list

Caching Strategy

By default the caching strategy is set to Off. If your channel service type is HTTP then you can apply two types of caching strategy. Please refer to the Configure Cache page to configure detailed cache settings. Note that when caching is applied to a channel with service type "Accelerate HTTP", objects that are compressed will not be cached.

By Host:

Caching is applied on a per host name basis. A separate Cache will exist for each domain/host name. Ideal for web servers that can serve multiple websites depending on the domain.

By Virtual Service:

Caching is applied per virtual service. Only one Cache will exist for all domain/host names that pass through the virtual service. This is a specialist setting for use with multiple clones of a single site.

Acceleration

Off:

Turn compression off for the Virtual Service

Compression:

Turn compression on for the Virtual Service. Traffic from the ALB-X to the client will be dynamically compressed upon request. This only applies to objects that contain the content-encoding: gzip header. Example html css or javascript. You can also exclude certain content types from the Global Exclusions section. Note: If the object is cachable we will store a compressed version and serve this statically (from memory) until the content expires and it is revalidated.

Virtual Service SSL Certificate (Encryption between Client and ALB-X)

By default this is set to No SSL. If your service type is "HTTP" or "Layer4 TCP" you can select a certificate from the drop down box to apply to the Virtual Service. Certificates that have been created or imported will appear in this list

No SSL:

Traffic from the browser to the ALB-X will not be encrypted

Default:

A locally created certificate called "Default" is applied to the browser side of the channel. This can be used to test SSL when one hasn't been created or imported

UserCertificate1:

A locally created, imported or signed certificate is applied to the client side of the Virtual Service

Real Server SSL Certificate (Encryption between ALB-X and Real Server)

By default this is set to No SSL. If your server requires an encrypted connection then this must be set to anything other than No SSL. Certificates that have been created or imported will appear in this list.

No SSL:

Traffic from the ALB-X to the content server will not be encrypted. If a certificate has been selected - on the browser side, "No SSL" can be selected client-side to provide what is known as "SSL Offload".

UserCertificate1:

Traffic from the ALB-X to the content server will be encrypted provided the named certificate is presented by the real server. If a certificate has been selected - on the Virtual Service side, "UserCertificate1" can be selected to provide what is known as "SSL Bridging" or "SSL Re-Encryption".

Any:

The ALB-X acts as a client and will accept any certificate the content server presents. Traffic from the ALB-X to the content server will be encrypted if this is selected. If a certificate has been selected - on the Virtual Service side, "Any" can be selected to provide what is known as "SSL Bridging" or "SSL Re-Encryption".

Advanced

Connectivity

Your Virtual Service can be configured with four different types of connectivity. Please select one to apply to the channel.

Reverse Proxy:

This is the default setting for jetNEXUS ALB-X and works at layer7 with compression and caching and also at layer4 without caching and compression. In this mode your jetNEXUS ALB-X acts as a reverse proxy and becomes the source address seen on the content 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 edgeNEXUS on the response. DSR is suitable for using with Layer 4 load balancing only. Therefore Caching and Compression are not available when enabled.
Layer 7 load balancing with this method will not work therefore there is no persistence support other than IP List Based. SSL/TLS load balancing with this method is not ideal as there is only source IP persistence support. This method requires content server changes. Please refer to the real server changes section.

Transparency:

Transparency is suitable for Service Type Layer 4 load balancing only. Caching and Compression are not available when transparency is enabled. Transparency is used when you need the source address of the client making the request and X-Forwarded-For techniques are not sufficient. Layer 7 load balancing with this method will not work therefore there is no persistence support other than IP List Based. This method requires content server changes. Please refer to the real server changes section.

Gateway:

Gateway mode allows you to route all traffic through the jetNEXUS, this allows traffic from the content servers to be routed via the edgeNEXUS to other networks via the interfaces on the edgeNEXUS unit. Using the device as a gateway

device for content servers should be used when running in multi interface mode. Layer 7 load balancing with this method will not work therefore there is no persistence support other than IP List Based. This method requires that the content server sets its default gateway to the local interface address (eth0, eth1, etc....) of the jetNEXUS ALB-X. Please refer to the real server changes section.

Basic:

Basic mode is a very low latency low CPU mode that will provide simple load balancing. The load balancing policy is restricted to Round Robin or if you require session persistence IP List Based. This mode is only available with the 64bit platform which is available from here.

Enable Connection Pooling

When this is ticked the ALB-X maintains connections to the content server so they can be reused when future requests to the real servers are requested. This is a great way to reduce the number connections open on the real servers. This setting is only valid for Service Type "HTTP" and should be used for stateless web connections only.

Connection Pool Size

Set the number of connections to maintain

Connection Timeout

The default setting for this 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. This means that if a user has a period of inactivity of 2 hours or less the connections will still remain open.

Monitoring Settings

These settings are tied 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 is allowed online or marked as failed.

Interval

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

Monitoring Timeout

The timeout value is the amount of time the ALB-X will wait for a server to respond to a connection request. The default value is 2s. This value may need to be increased for busy servers.

Monitoring In Count

The default value for this setting is 2. This means that the real server has to pass two successful health monitors before it will be brought online. Increasing this figure will increases the probability the server is capable of serving 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. This means that the real server monitor has to fail 3 times before the ALB-X will stop sending traffic to the server and it is marked RED and "Unreachable". Increase this figure will result is a more reliable service at

the expense of the time it takes the ALB-X to stop sending traffic to this server.

Cipher Options

As of software version 4.1.1 you can now set the ciphers per service. This is only relevant for services with SSL/TLS enabled. The default cipher will be chosen automatically. You can add different ciphers using jetPACKS available at the following URL Once the jetPACK's have been added you will be able to set the Cipher options per service. The benefit of this is that you can create a number of services with varying levels of security. Be aware that older clients are not compatible with newer ciphers and so you will be reducing the number of clients the more secure the service.

Cipher Options: Defaults

Defaults
Anti Beast
Strong Ciphers

flightPATH

Destination | Actions | **flightPATH**

- flightPATH rules are designed to manipulate HTTP(s) traffic. As such, the option for flightPATH is only visible if for Service Type "HTTP"
- The list of available rules is on the left and the current rules applied to the virtual service are on the right
- To add a new rule drag and drop the rule into position or highlight a rule and click the right arrow
- The order for execution is important and will start with the top rule being executed fist. To change the order highlight a rule and use the arrows to move up or down the list.
- To remove a rule simply drag and drop it back to the rule inventory or highlight the rule and click the left arrow
- You can add, remove and edit flightPATH rules in the Configure flightPATH section.

Clustering

The **Setup---Clustering** page is the home of high availability for your jetNEXUS ALB-X. This page is organised into four sections

Notes on High Availability

- There is **no** requirement for a dedicated cable to maintain high availability heartbeat
- The heartbeat takes place on the same network as the **Virtual Service** that requires high availability
- There is **no** stateful fail-over between ALB-X appliances
- When high availability is enabled on two or more appliances 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 switches of the new **Active** load balancer

Role

jetNEXUS ALB-X can be assigned into three separate roles with regards to high availability

Cluster Role

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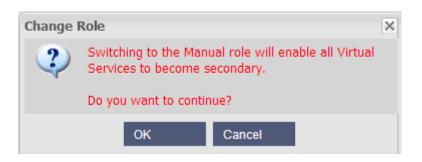
- You cannot remove the last member of the **Cluster** to **Unclaimed Devices,** to remove the last member then please change roles to **Manual** or **Stand-alone**
- The following objects are not synchronised**:**
    - **Manual Date & Time section - (NTP Section is synchronised)**
    - **Cluster Wait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

Failure of Cluster Owner

- When a cluster owner fails one of the remaining members will automatically load balancer traffic
- When the cluster owner returns it will resume load balancing traffic
- If you would like the member load balancing traffic to become the new owner simply highlight the member and click the up arrow so it moves to Priority 1 position
    - If you edit a remaining cluster member and the owner is down it will automatically promote itself to owner without loss of traffic

Changing role from Cluster to Manual

- If you wish to change from **Cluster** to **Manual** after you click on the radio button you will be prompted with the following message

- Click **OK** to change roles
- Please then check your **Virtual Services** and you will see that the **Primary** column now shows an un-ticked box

- This is a safety feature and means that if you have another ALB-X 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 from **Cluster** to **Stand-alone,** after you click on the corresponding radio button you will be prompted with the following message

- Click **OK** to change roles
- Please then check your **Virtual Services** where you should see the **Primary** column change name to **Stand-alone**
- You should also see that all of the **Virtual Services** are disabled (un-ticked) for safety
- Once you are certain that no other ALB-X on the same network has duplicate **Virtual Services** you can enable each one in turn

Manual Role

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

- To make a Virtual IP address "Active" tick the check-box 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 that 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 fail-back to the original **Active** ALB-X

Stand-Alone Role

An ALB-X in the **Stand-alone** role will not communicate with another ALB-X about its services and therefore all Virtual Services will remain status Green and connected. You must ensure that all Virtual Services have unique IP addresses or there will be a

clash on your network.

Settings

In this section you can set the **Wait Time** in milliseconds that a **Passive** ALB-X will wait before taking over the **Virtual Services** after the **Active** ALB-X has failed

We recommend setting this to 10000ms or 10 seconds but you may increase this value to suit your network. If you reduce this to below 3000 you may experience instability in the cluster and your ALB-X may change from **Active** to **Passive** to frequently.

Management

In this section you can add and remove cluster members. You can also change the priority of an ALB-X in the cluster

Add another ALB-X to the cluster

- Before adding an ALB-X to the cluster ensure that all ALB-X have the desired name which can be set in the appliance section

- In the management section you should see your ALB-X as **Priority 1** with **Status** green and its name under the **Cluster Members** column

- All available ALB-X will show up in the **Unclaimed Devices** window within the management section. An **Unclaimed Device** is an ALB-X that has been assigned in the **Cluster Role** but has no **Virtual Services** configured

- Highlight an ALB-X from the left hand **Unclaimed Devices** box and click the right arrow

- Click **OK** to promote your ALB-X to be a memeber of the cluster

-

Your ALB-X should now show as **Priority 2** in the cluster members list

- You can now view the IP Services page on the second box and see the **Virtual Services** have been replicated and the configuration has been synchronised

Removing a Cluster Member

- Highlight the Cluster Member you wish to remove from the cluster
- Click the left arrow
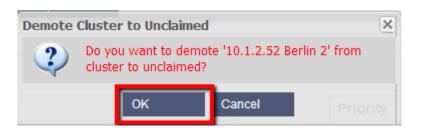
- You will be presented with a confirmation message

- Click **OK** to confirm
- The ALB-X that has been removed will now show up as an **Unclaimed Device** on the remaining cluster member(s)

- You should see on the removed cluster member that it is now the only cluster member

Priority	Status	Cluster Members
1	🟢	10.1.2.52 Berlin 2
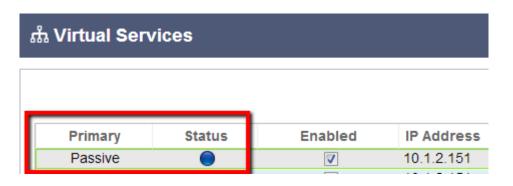
- Please check the **Virtual Services** have been deleted on the removed cluster member

Changing the priority of an ALB-X

- The ALB-X at the top of the **Cluster Members** list is given **Priority 1** and is the **Active** ALB-X for all **Virtual Services**

🖧 Virtual Services

Primary	Status	Enabled	IP Address
Active	🟢	☑	10.1.2.151

- The ALB-X that is second in the list is given **Priority 2** and is the **Passive** ALB-X for all **Virtual Services**

🖧 Virtual Services

Primary	Status	Enabled	IP Address
Passive	🔵	☑	10.1.2.151

- To change which ALB-X is Active simply highlight your ALB-X and click the up arrow until it is at the top of the list

Priority	Status	Cluster Members
1	🟢	10.1.2.51 Berlin 1
2	🟢	10.1.2.52 Berlin 2

Appliance

The **Setup-->Appliance** section allows you view and update the network details of your jetNEXUS ALB-X load balancer. It is organised into the following sections.

Adapter Details

Here you can add, remove and update the adapter settings.

Adapter:

Double click to see the physical adapters installed on your appliance. Choose an adapter from the list

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 ALB-X will set-up a simply policy that will allow connections initiated from this interface to be returned via this interface to the gateway router specified. This allows the ALB-X to be installed in more complex networking environments without the hassle of manually configuring complex policy based routing

Description:

Double click to add a description for your adapter. Example: Public Interface. Note: The ALB-X 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

Appliance

Basic Setup:

ALB Name:

Add in a name for your jetNEXUS ALB-X appliance. Please note that this cannot be changed if there are more than 1 member in the Cluster. Please see Clustering

DNS Server:

Add in the IPv4 address of your DNS server

Advanced Network Setting:

Server Nagle:

Tick the box to enable. This is a means to improve efficiency of TCP/IP networks by reducing the number of packets that need to be sent over the network

Client Nagle:

Tick the box to enable

License

The **Setup-->Licence** page shows the facilities you are able to use. It also provides you with the ability to install a licence. The page is split into two sections.

Licence Details

Issued To:

Name of the company.

Contact Person:

Name of the contact person.

Date Issued:

The date the licence certificate was issued.

Server Ref:

The name of the ALB-X.

Facilities:

ALB:

The core functionality of the ALB-X. This can be "Permanent" or contain a number to indicate how many days the facility has remaining.

SSL:

The ability to decrypt/encrypt traffic. This can be "Permanent" or contain a number to indicate how many days the facility has remaining.

Cache:

The ability to use the jetNEXUS intelligent caching engine for web traffic. This can be "Permanent" or contain a number to indicate how many days the facility has remaining.

flightPATH:

The ability to use the jetNEXUS intelligent traffic manipulation engine. This can be "Permanent" or contain a number to indicate how many days the facility has remaining.

Interfaces:

The maximum number of Virtual IP addresses. This can be "Permanent" or contain a number to indicate how many days the facility has remaining.

Real Servers:

The maximum number of real server IP addresses. This can be "Permanent" or contain a number to indicate how many days the facility has remaining.

Example:

Upload Licence Certificate:

Machine ID:

The machine ID is needed to create your licence certificate. The machine ID is tied to the MAC address of Eth0 for a physical appliance. The Machine ID is tied to the IP address if Eth0 for a virtual appliance. Note, if you change the IP address of Eth0 on a virtual appliance the existing licence will be invalid and your services will stop working. You will still be able to access the web console on https://x.x.x.x:27376.

Upload Certificate:

Once you receive your licence from support@edgenexus.io you can **Browse** for the file. Click **Upload** to apply. You should then see your facilities have updated, please check they are correct. Note you will only be able to upload a licence with the correct Machine ID.

Machine ID: DAF-F739-534

Upload Certificate: [blank]   Browse   > Upload

Paste Licence:

From software version 4.1.1 you can now paste your licence.

1. Open up your licence in a text editor
2. Copy everything
3. Paste into the box
4. Click update to apply
5. The status bar along the bottom should go Green informing you that the licence is uploading
6. In some circumstances you might need to restart the ALB-X to apply

Machine ID: 0025-9073-4BFA

Upload Licence: 002590734BFA   Browse   Upload

Paste Licence:

```
-license-------------------------------------------------------

jetNEXUS ALB Licence
Issued To:                     jetNEXUS
Contact Person:                Gary
Telephone:
Licence Id:                    BFEB144A-12F6-4BF7-A481-8F4EB4E6AB3C

Details
Date Issued:                   25 Mar 2014
Server Ref:                    Tr E4-01

Facilities
  ALB:                         Full Licence
```

↑↓ Update

Licence Support Information

This page contains vital information that will help the jetNEXUS support team in assisting you if you have an issue.

Please click on the [Licence Service Information] to retrieve your Support information similar to below.

You can then send these details with the button on the bottom right hand side [Send Details]

Details

MAC Address:	00:0C:29:41:D3:8E
Current Version:	3.51.1 (Build 1480)
Server Ref:	Demo 1 Web Console
OS Version:	Linux jetnexus 2.6.18-238.19.1.el5 #1 SMP

Licence Configuration:

```
[jetnexusdaemon]
.001Licence="jetNEXUS ALB Licence"
.002Customer="Issued To,jetNEXUS"
.003Contact="Contact Person,support@jetNEXUS.com"
.004Tel="Telephone,"
.005Uuid="Licence Id,5D30E87A-37B0-4CC9-BABF-DFD62D017242"
Customer="jetNEXUS"
.100Details="Details"
MachineID="EF:43:A3:5F:79"
ReleaseCode="076D-EFBF-BFC2-C4E9"
```

System Configuration:

```
[jetnexusdaemon]
AdaptivePollingEnabled=1
AddXForwardedFor=1
AllowCompressedUploads=0
AllowIdentity=0
AlwaysChunk=0
CaptureAdapter="eth1"
CaptureMegs="100"
CapturePackets="99999"
CaptureTime="10"
```

System Log:

```
May 28 08:53:55 jetnexus webconsole[2129]: api: admin: IPS Server: Index=2, FullI:
May 28 08:53:55 jetnexus webconsole[2129]: api: admin: IPS Server: Index=3, FullI:
May 28 08:53:55 jetnexus webconsole[2129]: api: admin: IPS Channel: Enabled=Yes, ons, Data=Layer 4, Protocol=Layer 4,
Cache=Off, Cert=No SSL, ClientCert=No SSL, Desc=POP, Monitoring=None, CSGName=Ser Managed, Servers=[192.168.3.215:110],
flightPATHs=[NNNNNNNNNNNNNNNNNNNNNNNNNNNNNN], B2B=No, AddFP/MoveFP/DelFP[NNN]
May 28 08:53:55 jetnexus jetnexusproxy[17535]: Service on 192.168.101.100:104 sta:
May 28 08:53:55 jetnexus webconsole[2129]: api: admin: IPS Server: Index=2, FullI:
May 28 08:53:55 jetnexus webconsole[2129]: api: admin: IPS Channel: Enabled=Yes, ata=Layer 4, Protocol=Layer 4,
Cache=Off, Cert=No SSL, ClientCert=No SSL, Desc=SMTP, Monitoring=None, CSGName=Se Dsr, Servers=[192.168.3.215:25],
flightPATHs=[NNNNNNNNNNNNNNNNNNNNNNNNNNNNNN], B2B=No, AddFP/MoveFP/DelFP[NNN]
```

Send Details

Network

The **Setup--->Network** configuration page allows you to view and update the routing information on the jetNEXUS ALB-X. The settings are organised in the following sections:

Default Route

Default Gateway:

This is the address of the Firewall or Router that the ALB-X will send traffic to if it does not match any other routes in the routing table. Add the IP address of the Gateway and choose an interface from the drop down box. When you click update, a green tick will appear if the gateway can be reached. A red cross will appear if the gateway cannot be reached.

Static Route

You can manually add routes for specific subnets in this section.

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 reach on that interface. Please make sure you have set up an interface and IP address on the same network as the gateway

Static Route

⊕ Add Route	⊖ Remove Route	⇅ Update

Destination	Gateway	Mask	Adapter	Active
123.123.123.5	10.4.8.1	255.255.255.0	eth1	✓

Details

This section will provide information about all of the routes configured on your ALB-X.

Details

Destination	Gateway	Mask	Flags	Metric	Ref	Use	Adapter
255.255.255.255	0.0.0.0	255.255.255.255	UH	0	0	0	eth0
192.168.101.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
10.10.10.0	10.1.1.2	255.255.255.0	UG	0	0	0	eth1
10.1.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1
169.254.0.0	0.0.0.0	255.255.0.0	U	0	0	0	eth1
0.0.0.0	10.1.1.1	0.0.0.0	UG	0	0	0	eth1

Hardware

The **Setup--->Hardware** configuration page allows you to view and edit the physical interfaces. It also allows you to create a bonded interface. Note that bonding will only work for physical appliances. Bonding should be done on the host Hyper Visor for virtual appliances.
This section is organised in two sections:

Interfaces

The settings on this screen control the network access. The defaults are to fix speed at 100 Mbps and full duplex. This avoids any issue with certain networking devices that have auto-negotiation which re-negotiates too frequently.
The appliance can support speeds from 10 to 1000; for 1000 this should set to auto/auto. If this does not work, set the exact network hardware values.
The speed and duplex setting should only be changed for hardware appliance. Virtual appliances will take their configuration from the underlying hypervisor.

Bonding

Bonding allows you to aggregate multiple ports into a single group, effectively combining the bandwidth into a single connection. Bonding also allows you to create multi-gigabit pipes to transport traffic through the highest traffic areas of your network. Note: this is only relevant for your hardware version of ALB-X. Do not use bonding for the Virtual Appliance.

Bonding Modes

balance-rr:
> Transmits packets in sequential order from the first available slave to the last.

active-backup:
> Has one interface which will be active and the second interface will be in 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 selects the same slave for each destination Mac address.

broadcast:
> Transmits everything on all slave interfaces.

802.3ad:
> Creates aggregation groups that share the same speed and duplex settings. Utilizes all slaves in the active aggregator according to 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. Incoming traffic is received by the current slave. 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.

Configure Bonding

- Click on **Add** button on the bonding section and choose which bonding mode you wish to use

- Assign which interfaces are to be bonded in the interface section. In the example below eth0, eth1 and eth2 are now part of bond0. Whilst Eth0 remains on its own as the management interface

Adapter Status

 - Adapter Up

 - Adapter Down

 - Adapter Unplugged

 - Adapter missing

IP Addressing

Now that you have added your bond you can go to the appliance section to add the IP address and policy routing details

flightPATH

The **Configure--->flightPATH** page allows you to view and update the flightPATH rules on the jetNEXUS ALB-X. The settings are organised in the following sections:

What is flightPATH?

flightPATH is a rule engine developed by edgeNEXUS to intelligently manipulate and route HTTP and HTTPS traffic. It is highly configurable, very powerful and yet very easy to use.

A flightPATH rule has three components:

Condition:
Set multiple criteria to trigger the rule.

Evaluation:
Variables that can be used in the Action.

Action:
The behaviour 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", "Ends With" etc. For more complete control powerful Perl Compatible Regular Expressions can be implemented.
In addition, custom variables can be created and used in the Action enabling many different possibilities.

Details

The details section contains the name and description of all of the flightPATH rules configured on the ALB-X. As you click on a rule the details of the rule will show in the section below.

To add a new flightPATH rule click **Add New** and give your rule a **Name** and **Description** then click **Update** to save this section.

Condition

- New conditions can be added by clicking, **Add New** button.
- Multiple conditions can be used but ALL must be met for the rule to execute.
- To use an OR you would need to create an additional flightPATH rule.
- Each condition contains three elements and a value or not depending on the condition.

Condition:

Select from the drop down list. You can start typing and the option will auto-show, you can now select with arrow keys and tab to the next column

Match:

Select from the drop down list or type your match. Depending on the Condition, the Match maybe blank. For example if the **Condition** is **Request Header** the match might be **User-Agent**

Sense:

Select from the drop down list. There are only two option **Does** and **Doesn't**

Check:

Select from the drop down list. For a simple check use something like **Start**, **End** or **Contain**. If you wish to have more

than one **Check** in the same line then please use **Match Regex**. Example Check = Match RegEx, Value = item1|intem2|item3

Value:

Manually type the value. This may be a text string or a regular expression.

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	his 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=jetNEXUS" 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	an 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

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.jetnexus.com
Have Length	The string does have length of the value	Host -- Does -- Have Length -- 16 www.jetnexus.com = TRUE www.jetnexus.co.uk = FALSE
Match RegEx	This enables you to enter a full Perl compatible regular expression	Origin IP -- Does -- Match Regex -- 10\..* | 11\..*

Example:

- The example below 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

Adding a Variable is a very powerful feature that will allow you to extract data from the request and include this 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.

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.

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	an 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

Example 1:

In the example below we have created a variable called **ignorestart.** It looks at the Path and ignores the first section called **finance** and use the latter part of the path as the contents of the variable.

This method allows the use of regular expression groups to create the variable. The example below only has one group so the value will be the characters contained within the brackets. IF more than one group is used in a regular expression the value will be taken from the last group.

Path = /finance/budgets/alpha/1.html
$ignorestart$ = /budgets/alpha/1.html

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 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

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.

Diagnostics

Tick this box to enable a more detailed trace. This will log additional detail to the syslog and should be used for testing and troubleshooting only as it will increase latency and CPU.

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:

1. HTML Extension:

  Changes all .htm requests to .html.

2. Index.html:

  Force to use index.html in requests to folders.

3. Close Folders:

  Deny requests to folders.

4. Hide CGI-BBIN:

  Hides cgi-bin catalogue in requests to CGI scripts.

5. Log Spider:

  Log spider requests of popular search engines.

6. Force HTTPS:

Force to use HTTPS for certain directory.

7. Media Stream:

Redirects Flash Media Stream to appropriate channel.

8. Swap HTTP to HTTPS:

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

9. Blank out Credit Cards:

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

10. Content Expiry:

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

11. Spoof Server Type:

Get the Server type and change it to something else.

12. Never Send Errors:

Client never gets any errors from your site.

13. Redirect on Language:

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

14. Google Analytics:

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

Real Server Monitoring

The **Configure--->Real Server Monitor** page allows you to add, view and edit custom monitoring. These are layer 7 server "Health-Checks" and once configured will appear in the drop-down list for Server Monitoring.

Details

Name:
Double click on the column to manually add in a name for your monitor.

Description:
Double click on the column to manually add in a description for your monitor.

Monitoring Method:
Double click on the column to choose from the dropdown list.

Page Location:
Double click on the column to manually add in a page location for an HTTP monitor. This can be a relative link such as /folder1/folder2/page1.html. You can also use an absolute link where the web site is bound to the hostname.

Required Content:
Double click on the column to manually add in the required content. This will change depending on the monitoring method.

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

Monitoring Method	Description	Example
HTTP 200 OK	In this mode, a TCP connection is made to the content server as above, but after connection is made, a brief HTTP request is made to the content server. A HTTP response is waited for and it is checked for the "200 OK" response code. If the "200 OK" response code is received, the content server is deemed to be up and running. If, for any reason, the "200 OK" response code is not received, including timeouts, failure to connect, etc. then the content server is regarded as down. This monitoring method can only really be used with HTTP and Accelerate HTTP service types, although 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 content server, or is handled appropriately by the "Content SSL" facility.	**Name:** 200OK **Description** Check production web site **Monitoring Method:** HTTP 200 OK **Page Location:** /main/index.html OR http://www.edgenexus.io/main/index.html **Required Content:** N/A

HTTP Response	In this mode, a connection and HTTP request/response are made/checked for as above, but instead of the "200 OK" response code being checked for, a custom text is searched for in both the HTTP headers, and the body of the HTTP response. The text can be a whole header, part of a header, a line from part of a page, or just one word. If the text is found, the content server is deemed to be up and running. This monitoring method can only really be used with HTTP and Accelerate HTTP service types, although 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 content server, or is handled appropriately by the "Content SSL" facility.	**Name:** Server Up **Description** Check content of page for "Server Up" **Monitoring Method:** HTTP Response **Page Location:** /main/index.html OR http://www.edgenexus.io/main/index.html **Required Content:** Server Up
DICOM	In this mode we send a DICOM echo using the AET value in the Required content column.	**Name:** DICOM **Description** L7 health check for DICOM service **Monitoring Method:** DICOM **Page Location:** N/A **Required Content:** AET Value
TCP Out of Band	This is similar to 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
Multi Port TCP monitor	This is similar to above except that you can have a number of 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

Example

Details

Add Monitor **Remove** **Update**

Name	Description	Monitoring Method	Page Location	Required Content
200OK	Check home page for 200 OK	HTTP 200 OK	/	
DICOM	Monitor DICOM server	DICOM		
L7 HTTP Response	Check content of page for required text	HTTP Response	/doesthispageexist.html	Does this content exist
L4 TCP out of band	Success only if port 55 responds	TCP Out of Band		555
L4 TCP multi-port	Success only if all 3 ports repsond	Multi port TCP monitor		135,59534,59535

Details

Add Monitor **Remove** **Update**

Name	Description	Monitoring Method	Page Location	Required Content
200OK	Check home page for 200 OK	HTTP 200 OK	/	
DICOM	Monitor DICOM server	DICOM		
L7 HTTP Response	Check content of page for required text	HTTP Response	/doesthispageexist.html	Does this content exist
L4 TCP out of band	Success only if port 55 responds	TCP Out of Band		555
L4 TCP multi-port	Success only if all 3 ports repsond	Multi port TCP monitor		135,59534,59535

Users

The **Configure --> Users** page allows you to configure multiple users and assign different roles to each user. It also shows the audit log where you can see changes made by each user.

Adding a User

- Click [+ Add User] and the screen below will pop up

- Enter a suitable **User Name**:
    - 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

- Enter a suitable strong password

    - 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 with the exception of those in the screen shot below

- Re-enter your strong password

- Tick one or more groups you would like the user to be a member of:

- 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 ALB-X via Secure Shell. This will give access to the command line which has a very limited set of commands available
- API
  - Users in this group will have access to SOAP and REST programmable interface. REST will be avaialbe from Software Version 4.2.1

User Type

 Local User

- ALB-X in Stand-Alone or Manual H/A role will create Local Users only
- By default there is a local user called "admin" that is a member of the admin group. For backwards 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

- ALB-X in Cluster role will create Cluster Users only
- Cluster Users are synchronised across all of the ALB-X 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 then you will not be able to change roles from cluster to manual or stand-alone

 Cluster and Local User

- Any users created whilst in Stand-Alone or Manual role will be copied to the Cluster
- If the ALB-X subsequently leave the Cluster then only Loal Users will remain
- The last configured password for the user will be valid

Removing Users

- 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 last cluster user in the admin group
- You will not be able to delete the admin user for backwards compatibility
- If you remove an ALB-X from the cluster all users except local users will be deleted

Editing Users

- Highlight an existing user
- Click **Edit**

- You may change the users 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

As of software version 4.1.1 jetNEXUS ALB-X logs each change made 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 System LogExample:

Security

The **Configure--->Security** page allows you to change the web console password and enable or disable Secure Shell.

The section is organised below:

Password

Username:
> This is always "admin".

Old Password:
> The default password is "jetnexus".

New Password:
> Enter a new password. The new password must contain numbers and letters only and be of 6 characters or more

Confirm Password:
> Type your new password again, taking care that they match.

SSH

Secure Shell Conn:
> Please tick the box if you wish to gain access to the ALB-X using SSH."Putty" is a great application for this.

SOAP

Enable SOAP Access:

Please tick the box if you wish to control the ALB-X using SOAP API.

SOAP WSDL:

http://**\<IP Address of ALB-X>**:3331/ALBAPI.wsdl

Username:

soap

Password:

jetnexusSOAP

Certificate and Port

GUI SSL Certificate:

Choose a certificate to apply to the management interface. This will automatically be set to "default" which is 1024 local certificate created on the ALB-X.

Any certificate you create or import can be selected here. Once you choose your certificate click update to apply

Secure Port:

The default secure port is 443. You may change this to another port and click update to apply. Your browser will automatically redirect to the new URL. Example: https://10.4.9.51:9090

Configure Logging

The Configure--->Logging page allows you to set the W3C logging levels and specify the remote server export the logs automatically. The page is organised into the two sections below.

Logging Levels

Enabling W3C logging mode will start jetNEXUS ALB-X 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 naming field (providing column names) so that data can be mined.

There are separate files for HTTP and FTP protocols.

HTTP W3C Logging:

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-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-sc(Content-Type).

Site:

This format is very similar to "Full" but has an additional field. See the fields summary 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-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-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

FTP W3C Logging:

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

edgeNEXUS w3c Logging:

Client's Network Address and Port:
This will show the true client IP address along with the port.

Client's Network Address:
This will show the true client IP address only.

Forwarded-For Address and Port:
This will show the details held in the XFF header including the address and port.

Forwarded-For Address:
This will show the details held in the XFF header including the address only.

Show Statistics in edgeNEXUS Headers:

On:
This will add a edgeNEXUS header and include gzip compression statistics. Example: edgeNEXUS: version 3.42.1.1475, 1232/4014 (69%)

Off:
This will turn off statistics within the header but the header will still be present. Example: edgeNEXUS : version 3.42.1.1475, On, [Laptop Demo 1 Primary]

Hidden:
No edgeNEXUS header shown at all.

Remote Log Storage

All W3C logs are stored compressed on the jetNEXUS ALB-X every hour. The oldest files will only be deleted when 30% of disk space is remaining. Should you wish to export these to a remote server for safekeeping you can configure that below using an SMB share. Please note that the W3C log will not transfer to the remote location until after the file has been completed and compressed. As the logs are written every hour this could take up to 2 hours for a Virtual Machine and will be 5 hours behind for a hardware appliance. We will include a test button in future releases to previde some feed back that your settings are correct.

Remote Log Storage:

Tick the box to enable remote log storage.

IP Address:

Add in the IP address of your SMB server. This should be in dotted decimal notation. Example: 10.1.1.23

Share Name:

Add in the share name on the SMB server. Example: w3c.

Directory:

Add in the directory on the SMB server. Example: /log.

Username:

Add in the username for the SMB share.

Password:

Add in the password for the SMB share.

Field Summary

HTTP

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 content server used

x-r-port	Port of content 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 content server, in the request
rs-bytes	Bytes from content-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 content-server took in seconds
x-trip-times	
new	millisecond from connect to posting in "newbie list"
rcon	millisecond from connect to making content-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 content-server
tql	millisecond from connect to sending the last byte of request to the content-server
rsf	millisecond from connect to receiving the first byte of response from the content-server
rsl	millisecond from connect to receiving the last byte of response from the content-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

Email Events

The **Configure-->Email Events** page allows you to configure an email server and send notification about you jetNEXUS ALB-X. The page is organised into the sections below.

Email Address

Send to Email Address:

Add in a valid email address to send the alerts, notifications and events to. Example support@domain.com.

Return Email Address:

Add in an email address that will appear in the inbox. Example ALB1@domain.com.

Mail Sever [SMTP]

Here you can add in the details of the SMTP server to be used to send the emails.

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.

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:

        Default setting is none.

    SSL:

Use this setting if your SMTP server requires Secure Sockets Layer authentication.

TLS:

Use this setting if you 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

Tick the various boxes to enable notifications and events.

Notifications occur when servers are contacted or channels are started. Alerts occur when Servers cannot be contacted or channels stop.

IP Service:

This will inform you when a Virtual IP address is online or stopped. This will include all Virtual Services that belong to that Virtual IP

Virtual Service:

This will inform you when a particular Virtual Service is online or stopped.

Real Server:

This will inform you when a Real Sever and Port is connected or not contactable.

flightPATH

This will email when a condition has been met and the action instructs to email the event**.**

Group Notifications:

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

Group Mail Description:

Add in a relevant subject name.

Group Send interval:

Stipulate the amount of time you wish to wait before sending one group email. Minimum time is 2 minutes.

Warnings

There are two warning emails.

Disk Space:

Set the percentage of free disk space. When this is reached you will be emailed.

Licence Expiry:

The default time remaining before your temporary license will expire is 7 days. When this is reached you will be emailed.

Cache

The **Configure-->Cache** page allows you to configure the cache settings for the ALB-X. The page is organised is in the sections below:

Cache Settings

Maximum Cache Size (MB):

Maximum RAM that the Cache can consume.

The edgeNEXUS Cache is an in-memory cache that is also periodically backed onto hard disk to maintain cache persistence after restarts, reboots and shutdowns. This 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 available memory.

Desired Cache Size(MB):

Optimum RAM that the Cache will be trimmed to.

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 for the purpose of trimming 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):

Life of content without an explicit expiry value.

The default caching time is the period content will be stored in the cache for items that don't have a "no-store" directive, but also have no explicit expiry time in the traffic header.

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

Cachable HTTP Response Codes:

HTTP responses that will be cached:

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):

Interval between cache trim operation

Cache-Fill Count:

This 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. This maybe a fully qualified domain name or an IP address in dotted decimal notation. Example www.jetnexus.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 a number of 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 you 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

SSL Certificates

The **Configure-SSL Certificates** tab contains four sub-pages. They are organised below.

What can edgeNEXUS do with SSL?

jetNEXUS ALB-X has the ability to offload the SSL encryption and decryption work load from your real servers and also becomes the termination point for your SSL certificates. jetNEXUS ALB-X also has the ability to re-encrypt traffic to the real servers for more secure environments.

Create Certificate

To create a local certificate:

- Fill in all the details like the example below
- Click on **Create Local Certificate**
- Once you have clicked this you can apply the certificate to a [Virtual Service](#)

To create a Certificate Request:

- Fill in all the details like the example below except for the Period
- Click on the bottom button called "Create Certificate Request"

Create Certificate Request

- Once you have clicked this, a certificate request will pop-up. Please ensure your browser allows pop-ups
- Copy this information from ----Begin Certificate Request----- to -----End Certificate Request----- and paste into a text file
- This information can now be pasted into the CSR required by your Certificate Authority

```
-----BEGIN CERTIFICATE REQUEST-----
MIICpDCCAYwCAQAwXzELMAkGA1UEBhMCQUUxDTALBgNVBAgTBGFzZGYxDDAKBgNV
BAcTA2FzZjEOMAwGA1UEChMFYWRmYXMxDTALBgNVBAsTBGFzZGYxFDASBgNVBAMT
C2FzZmRhc2QuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA6bVe
nX0a9DxraRCllXX2xKkI/a/IJYHskFLN890ilQrt0tiRbpvI6R9XX5IXS9Y/Gh54
8YLSh3vv4ud6yQO5K+3a1mBathDLrxAdlgjAdfovg7cKLoh3oaahUMsE4pJ3MOol
2AFcJGHi3Z717YjpDZGn1BMSj8MWYkJUzuTBnbsUIcbPOhsh26tUkjwwtGKXZS26
YJq/t+TJe4c7TeLnNRyqb5vnc2jxGFiBUrw8/UyagbDjNixJBrfo36Jru+S3M2jX
6IICgsthXxlgHc5CDd9U+T22jbhwL4LwFGX6nVkTbJb7/QwIdhMG/iRkiYDFdSpL
s/3+8JjqBBs8xXzSdQIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEBAIeM0ApRy5X+
SGhmDCGUZ7oGP6r9b6YQf45kunWbSgBOK1Au/hIYxjvnGyiL1k28awF2H8dlv8FM
PSS82fYSI4LvXjsar41tApmLTztCDIuccJiTDt8ilX/4cNi8mP1xu6S1HyNhpOeX
WOyamCeQAY4EJes7rRWZ1wQLvnkjlDBLRw0T0+vZcewlHuPkpGxO7EuLC/omJnYh
f6CS8863EXgE9fTLDX2MFh/K6w+hnibTiDx9EpOCBxat9NoArJenCOQxzzYf0HRF
sECFgLA85XyGjH3kW7Es5TlD6zom2b5EiCAZeel5yCvzUgvI1MaP+gJvI99fyYg9
Cf4a5whHfMc=
-----END CERTIFICATE REQUEST-----
|
```

Refer to Installing a certificate to complete the process

Manage Certificates

Install a certificate:

This will allow you to install a certificate from a CSR:
- Select a certificate from the drop-down list that has (pending) tagged on the end
- Paste your signed certificate that you received back from the Certificate Authority at the top

- 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. (ALB-X also contains a root bundle for re-encryption where it acts as a client to a real server)

- Click **Install**
- Once you have installed you should see (Trusted) next to your certificate
- If you have made a mistake or entered the wrong intermediate order then simply select the Certificate(Trusted) and add the certificates (including the signed certificate) again in the correct order and click Install

Add Intermediate:

It is useful on occasion to add in the intermediates separately. For example if you have imported a certificate that does not have 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 last
- Click **Add Intermediate**
- If you make a mistake with the order you can repeat the process and add the intermediates again. This will overwrite the previous intermediates only

Renew a certificate:

This will allow you to obtain a new Certificate Signing Request (CSR) for exisiting certificates

- Select a certificate from the drop-down list, you may choose any certificate (Pending), (Trusted) or (Imported)

- Click **Renew**
- This will provide a new certificate request (**CSR**)
- Once your **CSR** has been signed by your certificate provider, highlight your certificate and click **Install** to update (do not click **Renew** again as this will generate a new CSR)

Show the details of a certificate:

This will enable you to view the details of the certificate selected:

- Select a certificate from the drop-down list.
- Click **Show**
- A pop-up will provide the details of the certificate like the example below

Certificate Details window content:

```
Certificate Details for Test 1 Gary Berlin ...

https://10.4.9.51/config/alb-x/Configure/Certi

        Certificate Name: thursday24th1307
              Organization: jetnexus
     Organizational Unit: testing
              City/Locality: marlow
           State/Province: bucks
                   Country: GB Great Britain
           Domain Name: test.jetnexus.com
               Key Length: 2048
             Period(days):
                   Expires: Aug 23 23:59:59 2014 GMT
```

Drop-down: thursday24th1307(Trusted)

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

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

Buttons: Install | Add Intermediate | Renew | Show | Delete

Delete a certificate:

This will allow you to delete the selected certificate from the ALB-X

- Select a certificate from the drop-down list.
- Click "Delete" at the bottom of the page

Delete

- The certificate is no longer installed on the jetNEXUS ALB-X

Import Certificate

Single Certificate:

This section allows you to import a signed certificate from a trusted Certificate Authority (CA). The signed certificate must be in PKCS#12 format. This container format can contain multiple embedded objects, such as multiple certificates and is usually protected with a password.

Import Single Certificate

Certificate Name: ImportCertTest

Password: ●●●●●●●●●●●●●●

Upload Certificate: C:\fakepath\Exchange2013November2015.pfx   Browse

Import

To import your certificate:

- Give your certificate a friendly name, this is to identify it in the drop down list. It does not need to be the same as the certificate domain name and must alphanumeric only with no spaces
- Type the password you used to create the PKCS#12 container
- Browse for the certificate.pfx
- Click **Import**
- Your certificate will now be in the SSL drop down box for your channel

Multiple Certificates:

This section allows you to import a JNBK file that contains mulitple certificates. A JNBK is an encrypted file produced by jetNEXUS ALB-X when exporting mulitple certificates.

- Browse for your filename.jnbk file - iyou can create one of these by exporting mulitple certificates
- Type the password you used to create the jnbk file
- Click **Import**
- Your certificates will now be in the SSL drop down box for your service

Export Certificate

This section allows you to export any certificates that are installed on the jetNEXUS ALB-X. The certificate will be exported in PKCS#12 container format which will include the private key and intermediate certificates.

- Tick the certificate or certificates you wish to install. You may all tick All to automatically tick all certificates
- Type a password to protect your certificates. This must be at least 6 characters in length. Letters, numbers and certain symbols can be used.
- The following characters can not be accepted < > " ' ( ) ; \ | � % &
- Click **Export**
- Single Certificate: Your certificate will be saved as sslcert_<certificatename>.pfx - Example **sslcert_Test1Cert.pfx**
- Multiple Certificates: Your certificates will we saved as **sslcert_pack.jnbk**

Note: A jnbk file is an encrypted container file produced by jetNEXUS ALB-X. These types of files can only be imported by jetNEXUS ALB-X

Configure History

The **Configure--->History** page allows you enable historical data logging for such things as **CPU, Used Memory, Requests per second** and so on**.** Once you have enabled this you can view the results in graphical form via the **Monitor--> History** page. This page will also allow you to backup or restore your history files to the local ALB-X.

Enable Historical logging

1. Tick the box at the top of the page to enable historical logging.

1. Choose the interval at which data will be logged. This value should be between 1s and 60s
2. Click Update to save these settings
3. Go to Monitor-History to create the graphs from these data points

Maintenance

This section will be greyed out if you have enabled historical logging. To allow the maintenance of the historical logs please untick the Enabled Box and click Update.

Backup

 Give your backup a descriptive name. Click **Backup** to store all files to the jetNEXUS ALB-X

Delete

Select a backup file from the drop down list. Click **Delete** to remove the backup file from your ALB-X

Restore

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

Statistics

The **Monitor-Statistics** page allows you to view information about the traffic flowing through your jetNEXUS ALB-X. The page is split into four sections and organised below.

Total Input/Output

This statistic reports the raw data in and out of the ALB-X. The unit of measurement will change as the size grows from kbps to Mbps to Gbps

Total Input	= 273.6 MB	Input/s	= 13.2Mbps
Total Output	= 1446 MB	Output/s	= 16.4Mbps

Compression

Content Compression to Date

This statistic reports how much compression the jetNEXUS ALB-X has achieved on **compressible** content. A typical percentage for this lies between 60-80%.

Overall Compression to Date

This statistic reports how much compression the jetNEXUS ALB-X has achieved on **all** content. A typical percentage for this depends how many pre-compressed images are contained on your services. The more images the smaller the overall compression percentage is likely to be.

Compression Statistic

Content Compression to Date

Compression	= **64%**		
Throughput Before Compression	= 178.3 kB		
Throughput After Compression	= 62.8 kB		

Overall Compression to Date | | | **Current Values**

Compression	= **2%**		= 0%
Throughput Before Compression	= 5.35 MB		= 0.36 Mbps (data)
Throughput After Compression	= 5.23 MB		= 0.36 Mbps (data)
Throughput From Cache	= **832.1 kB**		= 0.00 Mbps (data)
		Total	= 0.72 Mbps (data)

Hits and Connections

This section contains the overall statistics for hits and transactions.

Hit:
A hit is defined as a layer 7 transaction. Typically for web servers this is a GET for an object such as an image.

Connection:
A connection is defined as a layer 4 TCP connection. Many transactions can occur over 1 TCP connection.

Overall Hits Counted

This is the cumulative number of non-cached hits since last reset. On the right hand side the figure will show the current number of hits per second.

Total Connections

This is the cumulative number of TCP connections since last reset. The first figure on the right hand side you can see the number of TCP connections per second to the ALB-X. The second number is the number of TCP connections per second to the content servers.
Example 6/8 connections/sec - This means we have 6 TCP connections per second to the Virtual Service and 6 TCP connections per second to the real servers.

Peak Connections

This is the maximum number of TCP connections to the jetNEXUS ALB-X. The number on the right hand side gives the current number of active TCP connections.

```
Hits and Connections
Overall Hits Counted    = 297    0 Hits/sec
Total Connection        = 91     0 / 0 connections/sec
Peak Connections        = 76     1 current connections
```

Caching

This section will show the overall statistics in relation to caching when it has been 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 number gives the total number of transactions served from the jetNEXUS ALB-X cache since last reset. A percentage of total transactions is also provided.

Bytes:

The first number gives the total amount of data in KiloBytes served from the jetNEXUS ALB-X cache. A percentage of total data is also provided.

From Server

Hits:

The first number gives the total number of transactions served from the content servers since last reset. A percentage of total transactions is also provided.

Bytes:

The first number gives the total amount of data in KiloBytes served from the content servers. A percentage of total data is also provided.

Cache Contents

Hits:

This number gives the total number of objects contained in the jetNEXUS ALB-X cache.

Bytes:

The first number gives the overall size in MegaBytes of the jetNEXUS ALB-X cached objects. A percentage of the maximum cache size is also provided.

Hardware

This section provides the overall usage stats for the jetNEXUS ALB-X.

Disk Usage

This number gives the percentage of disk space currently used and includes such things as the log files and the cache which is periodically stored on the hard drive.

Memory Usage

This number gives the percentage of memory currently used. The larger number in brackets is the total amount of memory allocated to the ALB-X. It is recommended that this is a minimum of 2GB.

CPU Usage

This number gives the percentage of CPU currently used by jetNEXUS ALB-X. It is natural for this to fluctuate.

Monitor Logging

The **View--->Logging** page allows you to set the W3C logging levels and specify the remote server export the logs automatically.

The page is organised into the two sections below.

Download W3C Log

Once you have configured your W3C logging level you can view or download the log in this section.

The format for each log is:
- Name - w3c
- Year
- Month
- Day
- Hour

1. Highlight the required log.
2. Click **View** for a browser pop-up and the option to open with a text editor.
3. Click **Download** to automatically download to your browser download folder.

Download System Log

The format for each log is:
- Name - sys
- Year
- Month

- Day

1. Highlight the required log.
2. Click **View** for a browser pop-up and the option to open with a text editor.
3. Click **Download** to automatically download to your browser download folder.

Status

The **Monitor--->Status** page displays the live traffic for your Virtual Services. It also shows the number of connections and data to each real server so you can see the load balancing in action

Virtual Service Details

VIP Status:

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

- 🟢 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:

The colour of the light indicates the state of the Virtual Service:

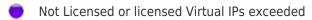- 🟢 Online

- 🔵 Failover-Standby. This virtual service is hot-standby

- 🟡 Indicates a "passive" is holding off for an "active"

🟠 Service Needs attention. This may be the result of 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:

Virtual Service name

Virtual Service:

The virtual ip address and port for the service

Hit/Sec:

Layer 7 transactions per second

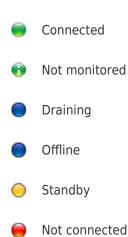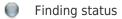# Cache%:

The percentage of objects that have been served from the ALB-X RAM Cache

Compression%:

The percentage of objects that have been compressed between the client and ALB-X

RS Status:

🟢 Connected

🟢 Not monitored

🔵 Draining

🔵 Offline

🟡 Standby

🔴 Not connected

 Finding status

 Not licensed or licensed real servers exeeded

Real Server:

The real server IP address and port

Notes:

Usually the name of the real server or helpful notes about the real server

Conns:

The number of connections to each real server. Here you can see load balancing in action. Very helpful to verify your load balancing policy is working correctly

Data:

The amount of data being sent to each real server

Req/Sec:

The number of requests per second sent to each real server

History

The **Monitor--->History** page displays the historical traffic for your system, virtual services and real services. It is a great way to see load balancing in action and view any errors or patterns over time. Note that you must enable historical logging from the **Configure--> History** page.

How Do I Access My Graphs?

1. Choose a Database:

> **System:**
>> Selecting this database will allow you to see CPU, memory and disk drive space over time
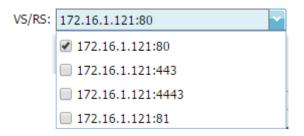>
> **Virtual Services:**
>> Selecting this database will allow you to choose all of the virtual services in the database from the time that you started logging data
>
> **Real Services:**
>> Selecting this database will allow you to choose all the real servers in the database from the time that you started logging the data.

2. Choose VS/RS: Virtual Service or Real Server: Note this will be blank if you choose the system database as it is not relevant

If Virtual Services Database chosen from above. You should now see a list of virtual services. Tick those that you wish to view

If Real Servers Database chosen from above. You should now see a list of real servers. Tick those that you wish to view

3. Choose a time frame:

Last Minute:
> The graph will contain 60 data points, one for each second

Last Hour:
> The graph will contain 60 data points, one for each minute

Last Week:
> The graph will contain 24 data points, one for each hour

Last Month:
> The graph will contain 32 data points one for each day

Last Year:
> The graph will contain 24 data points, two for each month

4. Choose a metric

System:
> CPU % - This will show the maximum/average CPU % over the time period selected Memory % - This will show the maximum/average Memory % over the time period selected Compression % - This will show the maximum/average Compression % over the time period selected

Virtual Services:
> Bytes in - This will show the maximum/average traffic flow in from the server in Bytes over the time period selected Bytes out - This will show the maximum/average traffic flow out to the client in Bytes over the time period selected Bytes cached - This will show the maximum/average size of the cached objects in Bytes over the time period selected Compression % Current Connections Request per second Cache HIts Cache Hits%

Real Servers:
> Bytes in Current Connections: Pool Size Request per second

5. Choose what to Show

Averages:

This will show the average values over the period of time selected

Maximum:

This will show the maximum data values over the period of time selected

The **Services-->Date & Time** page allows you to manually set the Date and Time on your jetNEXUS ALB-X. You can also configure a network time server to synchronise the time on your appliance. The page is organised into the two sections below.

Date & Time

In this section you can view the current Date and Time. This is usually set for Universal Time Zone or UTC but you may change this to your local timezone.

Time Zone:
- Click on the drop down box for the Time Zone and start typing your location.
- Example London
- Start typing L - All location containing the letter L will be displayed
- Continue typing Lon - the above locations will be narrowed down to around 4 locations
- Choose Europe/London to set your location

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

- Add in the date first in the following format DD/MM/YYYY
- Leave a space
- Add in the time in the following format hh:mm:ss
- Once you have set this please click Update to apply.
- You should then see the new Date and Time in bold

Synchronise Date & Time

In this section you can configure a time server to keep the jetNEXUS ALB-X synchronised.Network Time Protocol (NTP) is a networking protocol for clock synchronisation between computer systems over variable-latency networks.

Time Server URL:
Choose the IP address or fully qualified domain name or the NTP server.

Update at [hh:mm]
Select the time that you would like to first access the time server to synchronise.

Update Period [hours]:

      Select how often you would like synchronisation to occur.

NTP Type:

      Public SNTP V4 - This is the current and preferred method when synchronising 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

The example above would synchronise every hour at 7 minutes past the hour with pool.ntp.org. Please not that synchronisation is in UTC only. If you wish to set local time this can only be done manually. This will be changed in later versions to enable the ability to select a time zone.

Ping

The **Services-->Ping** page allows you to troubleshoot your basic network settings. Ping is a utility used to test the reachability of a host.

The page is organised into the section below.

Details

Type in the IP address of the host you wish to test, for example the default gateway using dotted decimal notation. You may have to wait a few seconds for the result but to feedback that you have pressed the "Ping" button it will go grey after pressing

If you have configured a DNS server then you can type in the fully qualified domain name. You can configure a DNS server on the Appliance page. You may have to wait a few seconds for the result but to feedback that you have pressed the "Ping" button it will go grey after pressing

If you have not configured a DNS server or you have configured a DNS server that is not working then you will see the following message

SNMP

The **Services-->SNMP** page allows you to enable the jetNEXUS ALB-X for SNMP agent.
The page is organised into the section below.

SNMP Settings

Simple Network Management Protocol (SNMP) exposes management date in the form of variables on the jetNEXUS ALB-X. These variables can then be queried by third party SNMP managing applications.

- **SNMP v1:**
  RFC-1157
- **SNMP V2c:**
  RFC-1901-1908
- **SNMP v3:**
  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.

JETNEXUS-MIB

Download

JETNEXUS 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 **jetnexusGlobal**　(1.3.6.1.4.1.38370.1.1)
       .2 **jetnexusVirtualServices**　(1.3.6.1.4.1.38370.1.2)
       .3 **jetnexusServers**　(1.3.6.1.4.1.38370.1.3)

      .1 **jetnexusGlobal** (1.3.6.1.4.1.38370.1.1)
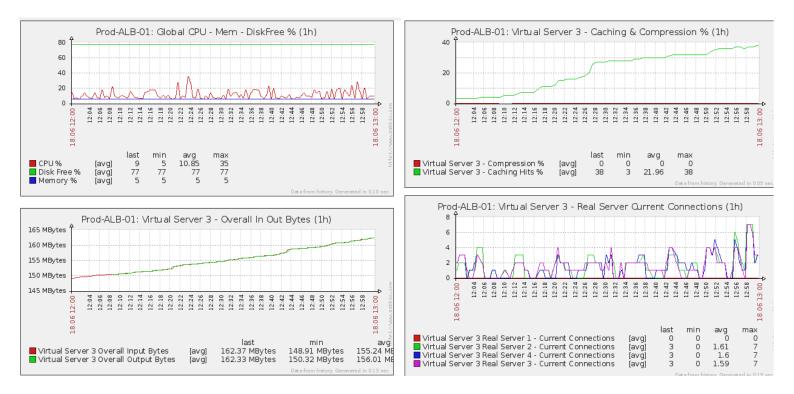
        .1 **jetnexusOverallInputBytes**　(1.3.6.1.4.1.38370.1.1.1.0)
        .2 **jetnexusOverallOutputBytes**　(1.3.6.1.4.1.38370.1.1.2.0)
        .3 **jetnexusCompressedInputBytes**　(1.3.6.1.4.1.38370.1.1.3.0)
        .4 **jetnexusCompressedOutputBytes**　(1.3.6.1.4.1.38370.1.1.4.0)
        .5 **jetnexusVersionInfo**　(1.3.6.1.4.1.38370.1.1.5.0)
        .6 **jetnexusTotalClientConnections**　(1.3.6.1.4.1.38370.1.1.6.0)
        .7 **jetnexusCpuPercent**　(1.3.6.1.4.1.38370.1.1.7.0)
        .8 **jetnexusDiskFreePercent**　(1.3.6.1.4.1.38370.1.1.8.0)
        .9 **jetnexusMemoryPercent**　(1.3.6.1.4.1.38370.1.1.9.0)
        .10 **jetnexusCurrentConnections**　(1.3.6.1.4.1.38370.1.1.10.0)

      .2 **jetnexusVirtualServices**　(1.3.6.1.4.1.38370.1.2)

        .1 **jnvirtualserviceEntry**　(1.3.6.1.4.1.38370.1.2.1)
         .1 **jnvirtualserviceIndexvirtualservice**　(1.3.6.1.4.1.38370.1.2.1.**1**)
         .2 **jnvirtualserviceVSAddrPort**　(1.3.6.1.4.1.38370.1.2.1.**2**)
         .3 **jnvirtualserviceOverallInputBytes**　(1.3.6.1.4.1.38370.1.2.1.**3**)
         .4 **jnvirtualserviceOverallOutputBytes**　(1.3.6.1.4.1.38370.1.2.1.**4**)
         .5 **jnvirtualserviceCacheBytes**　(1.3.6.1.4.1.38370.1.2.1.**5**)
         .6 **jnvirtualserviceCompressionPercent**　(1.3.6.1.4.1.38370.1.2.1.**6**)
         .7 **jnvirtualservicePresentClientConnections**　(1.3.6.1.4.1.38370.1.2.1.**7**)
         .8 **jnvirtualserviceHitCount**　(1.3.6.1.4.1.38370.1.2.1.**8**)
         .9 j**nvirtualserviceCacheHits**　(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 of the edgeNEXUS Custom SNMP MIB is the ability to offload the historical graphing to a management console.

Below are some examples from Zabbix that polls a jetNEXUS ALB-X for various OID values listed above.

Capture

The **Services-->Capture** page allows you capture the information on an individual interface or all interfaces

The page is organised into the section below:

Details

1. Complete each box
2. Click **Generate**
3. Once the capture has run your browser will pop-up and ask you where to save the file. It will be in the format "jetNEXUS.cap.gz"
4. Email this file to support@edgenexus.io
5. You can view the contents using wireshark

Adapter:

Choose your adapter from the drop-down, typically **eth0** or **eth1**. You can also capture all interfaces with "**any**"

Packets:

This is the maximum amount 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

To maintain performance we have limited the download file to 2MB. If you find that this is not enough to capture all the data you require we can increase this figure.

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

Restart

The **Services-->Restart** page allows you to stop and start essential jetNEXUS ALB-X services.
The page is organised into the section below.

Restart

Click the Restart button to quickly stop and start essential jetNEXUS ALB services.

Warning - This will cause a brief break in current connections.

Software Version:4.1.2 (Build 1644)

C Restart

Reboot

The **Services-->Reboot** page allows you to re-initialise all jetNEXUS ALB-X services.

The page is organised into the section below.

Power Off

The **Services-->Power Off** page allows you to shut down the jetNEXUS ALB-X.

The page is organised into the section below.

Power Off

Click the Power off button to completely halt jetNEXUS ALB

Warning - This will suspend your web site and require a hardware power on

Update Software

The **Advanced-->Update Software** page allows you to update the configuration and the firmware of your jetNEXUS ALB-X.

The page is organised into the section below.

Configuration

Download or save a configuration file

1. To download the current configuration of the jetNEXUS ALB-X simply press the green **Download Configuration** button.
2. A pop-up will appear asking you to open or save the .conf file.
3. Save to a convenient location.
4. You can open this with any text editor such as Notepad.

Upload a new configuration from a saved .conf file

1. You may upload a saved configuration file by browsing for the saved .conf file.
2. Click Upload.
3. The jetNEXUS ALB-X will apply the config and refresh the browser. If it does not, please click refresh.
4. You will be redirected to the Dashboard page upon completion.

Upload a new jetPACK

1. A jetPACK is a set of updates to the existing configuration.
2. A jetPACK can be as small as changing the TCPTimeout value to a complete application specific deployment such as Microsoft Exchange or Microsoft Lync.
3. You can obtain a jetPACK from support@edgenexus.io.
4. Browse for the jetPACK.txt file.
5. Click upload.
6. The browser will refresh automatically after upload.
7. You will be redirected to the Dashboard page upon completion. This may take longer for more complex deployments such as Lync.

Software

Upgrade the jetNEXUS ALB-X software

1. If your current software version is 4.0.1 (Build 1576) or above you can upgrade using the method below. Please email support@edgenexus.io if you are running a software version below 4.0.1 (Build 1576).
2. You can obtain the latest update version from our FTP server HERE or our DropBox HERE. The file will be in the format ALB-X-Update-64-<version-build>.tar.gz.keyed.
3. Browse for the update file. Do not try to alter this file.
4. Click Upload.
5. The jetNEXUS ALB-X will upload the file and continue to work as normal whilst uploading.
6. Once the file has been uploaded the jetNEXUS ALB-X will reboot to apply the software update.
7. This should take around 5 minutes. Your services will be inaccessible until the software has been applied.

Revert to a previous jetNEXUS ALB-X software version

1. You can revert to a previous version of software.
2. Browse for the file. Please email support@edgenexus.io if you don't have a previous version of software.
3. Click upload.
4. The jetNEXUS ALB-X will upload the file and continue to work as normal whilst uploading.
5. Once the file has been uploaded the jetNEXUS ALB-X will reboot to apply the software update.
6. This should take around 5 minutes. Your services will be inaccessible until the software has been applied.

Software:

Software Version: 4.1.2 (Build 1644)

Browse for software file then click upload to apply.   🔍 Browse

⬆ Upload New Software

HTTP

The **Advanced-->Protocol-->HTTP** page allows you to set advanced settings for HTTP.

The page is organised into the section below.

Server Too Busy

If you have limited the maximum connections to your real servers you can choose to present a friendly web page once this limit has been reached.

1. Create a simple web page with your message. You may include external links to objects on another web server. Alternatively if you want to include images on your web page then use inline base64 encoded images
2. **Browse** for your newly created web page
3. Click **Upload**
4. If you wish to preview the page you can do so with the **Click Here** link

Example of Server Too Busy page

Sorry for the inconvenience but the server is busy

please try again soon

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:

Off:
jetNEXUS ALB-X does not alter the Forwarded-For header.

Add Address and Port:
This will append the IP address and port, of the device or client connected to the jetNEXUS ALB-X, to the Forwarded-For header.

Add Address:
This will append the IP address, of the device or client connected to the jetNEXUS ALB-X, to the Forwarded-For header.

Replace Address and Port:
This will replace the value of the Forwarded-For header with the IP address and port of the device or client connected to jetNEXUS ALB-X.

Replace Address:

> This will replace the value of the Forwarded-For header with the IP address of the device or client connected to jetNEXUS ALB-X.

Forwarded-For Header:

> This is the name given to the Forwarded-For header. Typically this is "X-Forwarded-For" but may be changed for particular environments.

Forwarded For:

Forwarded-For Output: | Add Address and Port | ▾
Forwarded-For Header: | X-Forwarded-For

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

From the Category list, select Default
From the Source Type list, select Request Header
In the Source Name box, type X-Forwarded-For

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

Apache httpd.conf changes

There are several changes you are going to want to make to the default format in order to log the X-Forwarded-For client ip address or the real client ip address if the X-Forwarded-For header does not exist. Those changes are below:

> 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 environment variable.

- The first line is the standard combined log formatted string from the default.
- The second line replaces the %h (remote host) field with the value(s) pulled from the X-Forwarded-For header and sets the name of this log file pattern to "proxy".
- Line 3 is a setting for environment variable "forwarded" that contains a loose regular expression matching an ip address, which is ok in this case since we really care more whether an ip address exists in the X-Forwarded-For header. Explained another way, 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 and X-Forwarded-For value exists, use the "proxy" pattern, else use the "combined" pattern for that request. For readability, lines 4 and 5 do not take advantage of Apache's rotatelogs (piped) logging feature but I assume that it is in use by most everyone.

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

HTTP Compression Settings

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

WARNING - Take extreme care when adjusting these settings as inappropriate settings can adversely affect the performance of jetNEXUS ALB-X

Initial Thread Memory [KB]:
> This is the amount of memory each request received by jetNEXUS ALB-X 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 is the maximum amount of memory that the jetNEXUS ALB-X will allocate on one request. For maximum performance, jetNEXUS ALB-X normally stores and compresses all content in memory. IF an exceptionally large content file exceeding this amount is processed, jetNEXUS ALB-X will write to disk and compress the data there.

Increment Memory [KB]:
> This sets the amount of memory added to the *Initial Thread Memory Allocation* when more is required. The default setting is zero. This means jetNEXUS ALB-X 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 is the size, in bytes, under which the jetNEXUS ALB-X 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 jetNEXUS ALB-X from applying compression to style sheets of JavaScript. The reason for this is that even though jetNEXUS ALB-X 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 jetNEXUS ALB-X 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

Anything added to the current exclusion list will not be compressed.

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

About Us The **Help-->About Us** page will provide the version of software and contact information for edgeNEXUS Solutions Ltd.

Who is jetNEXUS?

- edgeNEXUS provide innovative, market leading solutions for application acceleration, load balancing and application delivery technology
- edgeNEXUS is a successful, profitable and privately owned company with over 10 years' industry experience
- Our product portfolio is accessible to a wide and varied client base, ranging from simple, cost effective point solutions to Enterprise-grade application delivery gateways
- We understand that this technology is

mission critical and as such, maintain a tenacious focus on the quality of our products and technical support

- Via a network of head offices in London, United States and Malaysia, edgeNEXUS continually strives to deliver outstanding support to our partners and customers regardless of location. Our approach to this international presence is: *Global Voice, Local Accent.*

- With a pragmatic attitude to product development, edgeNEXUS aims to include the features that deliver the biggest difference to the end user experience.
  - These features are packaged in a format that is flexible, intuitive and easy to configure.
  - We want to ensure that every interaction we have with our customers and partners is positive

- We love our business and we want this passion to be reflected in our product quality, innovative features and attitude towards support

Contact information

- EMEA

    edgeNEXUS EMEA Head Office,
    Suite 2, Anglers Court,
    33-44 Spittal Street,
    Marlow,
    Buckinghamshire, SL7 1DB, UK.

    Tel: +44 (0) 870 382 5050
    Email: info@edgenexus.io

- US

    edgeNEXUS LLC
    111 West Port Plaza Drive,

Ste 600,
St Louis,
MO 63146, USA

Tel: 800 568 9921

Email: info@edgenexus.io

- ASEAN

edgeNEXUS ASEAN Head Office,
Level 36, Menara Citibank,
165, Jalan Ampang,
50450 Kuala Lumpur,
Malaysia

Tel: +603-21697331

Email: info@edgenexus.io

jetPACK

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

This page is split in to the following sections

Download a jetPACK

Each jetPACK below has been created with a unique Virtual IP address that is 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 own Virtual IP address. In addition each jetPACK has been created with 2 real servers which have the IP address of 127.1.1.1 and 127.2.2.2. Again you can change these in the GUI after upload or beforehand using Notepad++

Right 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 there as an option. If you don't have a licence for flightPATH this jetPACK will still work.	**Global settings:** Service timeout 2 hours **Monitors:** Layer 7 monitor for 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 **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 outlook web app. Layer 4 out of band monitor for client access service **Virtual Service IP:** 1.1.1.2 **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 is needed if your SMTP server needs to see the real ip address of the client.	**Global settings:** Service timeout 2 hours **Monitors:** Layer 7 monitor for outlook web app. Layer 4 out of band monitor for client access service **Virtual Service IP:** 1.1.1.3 **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	The setup add 1 VIP and two services for both HTTP and HTTPS traffic and requires the least amount of CPU	**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 resource than above. You must configure each service as a unique DNS entry Example owa.jetnexus.com, ews.jetnexus.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 and ADS **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 **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 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 and ADS **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
- jetPACK-3.3.3.1-Lync-Reverse-Proxy

Front End
- jetPACK-3.3.3.2-Lync-Front -End

Edge Internal
- jetPACK-3.3.3.3-Lync-Edge-Internal

Edge External
- jetPACK-3.3.3.4-Lync-Edge-External

Web Services

Normal HTTP
- jetPACK-4.4.4.1-Web-HTTP

SSL Offload
- jetPACK-4.4.4.2-Web-SSL-Offload

SSL Re-Encryption
- jetPACK-4.4.4.3-Web-SSL-Re-Encryption

SSL Passthrough
- jetPACK-4.4.4.4-Web-SSL-Passthrough

Microsoft Remote Desktop

- jetPACK-5.5.5.1-Remote-Desktop

DICOM - Digital Imaging and Communications in Medicine

- 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

- jetPACK-8.8.8.1-View-SSL-Offload

Security Servers - SSL Re-Encryption

- jetPACK-8.8.8.2-View-SSL-Re-encryption

Global Settings

- GUI Secure Port 443 - this jetPACK will change you 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 will increase that request to 1 day
- ARP Refresh 10 - during a failover between HA appliances this 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 will increase the size to a maximum of 16MB
- TCP Timeout - 2hrs - this will change the default global TCP timeout to 2 hours

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

Apply a jetPACK

You can apply any jetPACK in any order but be careful not to apply a jetPACK with the same Virtual IP address. This 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

Create a jetPACK

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

- Start by copying the current configuration from your existing ALB-X
  - Advanced
  - Update Software
  - Click the green **Download Current Configuration** button to download the ALB-X.conf file
- Edit this file with Notepad++
- Open up 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 needs to be at the top of the jetPACK or your current configuration will be over written.

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

ContentServerCustomTimer=20000
> This is delay in milliseconds between content server health checks for custom monitors such as DICOM

jnCookieHeader="MS-WSMAN"
> This 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 normally 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 of the details in the IP Services section. Each interface is numbered and contains subinterfaces 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 of the rules. It is important that the numbers match what has been applied to the interface. In the example above we see that flightPATH rule "6" has been applied to the channel so we will include 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=
```