PHILIPS INTELLISPACE

AN EDGENEXUS ADC DEPLOYMENT GUIDE

EDGENEXUS

Contents

Document Properties

Document Number: 2.0.10.12.23.09.10

Document Creation Date: September 27, 2023

Document Last Edited: October 12, 2023

Document Author: Jay Savoor

Document Last Edited by:

Document Referral: EdgeADC - Version All Versions

Document Disclaimer

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

Copyrights

Trademarks

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

Edgenexus Support

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

About Philips Intellispace

The Philips IntelliSpace medical imaging system is a revolutionary advancement in the domain of healthcare and medical imaging, designed to foster enhanced patient care through its integrative, versatile, and comprehensive imaging solutions.

At its core, the IntelliSpace system amalgamates high-quality imaging acquisition with meticulous analytical tools, offering clinicians nuanced insights into patient anatomy and pathology. This amalgamation is pivotal in creating accurate diagnostic pathways and individualized treatment plans, crucial for addressing a myriad of health conditions, ranging from oncological to cardiovascular and neurodegenerative diseases.

One of the distinguishing features of Philips IntelliSpace is its interoperability, offering seamless integration with a variety of imaging modalities like MRI, CT, PET, and ultrasound. This extensive compatibility provides a consolidated view of patient information, enabling healthcare professionals to make informed decisions quickly, thereby escalating the overall efficiency and productivity within a clinical setting.

The IntelliSpace system employs advanced algorithms and machine learning tools to facilitate the automatic segmentation, annotation, and quantification of medical images. These capabilities empower physicians to explore intricate anatomical structures and abnormalities with unparalleled precision and clarity, significantly reducing the time consumed in image analysis and interpretation.

Moreover, Philips has profoundly recognized the critical importance of workflow efficiency in medical imaging. Consequently, the IntelliSpace system features an intuitive, user-friendly interface that is designed to mitigate complexities and facilitate effortless navigation through vast datasets and diverse imaging modalities. The enhanced user experience undoubtedly contributes to expeditious diagnostic processes, allowing clinicians to allocate more time to patient interaction and care.

Beyond the immediate medical realm, the impact of IntelliSpace extends to research and education. The system's cutting-edge analytical tools and diverse imaging modalities serve as fertile grounds for medical research, aiding in the development of novel therapeutic strategies and interventions. Furthermore, the detailed and high-quality images generated through IntelliSpace are invaluable resources for medical training and education, cultivating an enriched learning environment for medical students and trainees.

A significant aspect of the IntelliSpace medical imaging system is its emphasis on patient-centered care. The system prioritizes the protection of patient data through robust security measures, ensuring confidentiality and compliance with healthcare regulations. Additionally, the amalgamation of patient images and medical histories into a singular, accessible platform accentuates a holistic view of patient health, promoting personalized and efficient care strategies.

The flexibility and scalability of the IntelliSpace system are also noteworthy. The system can be tailored to meet the unique demands and workflow of individual healthcare settings, regardless of their size or specialization. This adaptability ensures that the benefits of IntelliSpace can be experienced broadly across the healthcare spectrum, including hospitals, clinics, and research institutions.

Recommendations and Prerequisites

To successfully load balance using the EdgeADC, we recommend the following:

- The ADC is deployed as a pair of appliances in either a virtualization technology, installing it as a virtualized appliance or as a hardware appliance in approved server hardware.
- When external users access the network via the Internet, we recommend that the ADC pair is deployed in the DMZ and the traffic rerouted through the firewall to the LAN zone.
- The ADC's operate in a high-availability (HA) mode when placed in pairs and provide you the level of redundancy and resilience required for mission-critical systems.

The ADC is fully capable of load-balancing your Philips Intellispace, and this guide explains how to set this up.

Prerequisites for supporting Philips Intellispace

As usual, it is assumed that the person who is installing and configuring the ADC is familiar with the terminology used within this document and networking in general. We strongly suggest that both the network technician and Philips Intellispace administrator work in tandem when setting up the load balancing and that this is first done for a sandbox environment before replicating to the production environment.

Further, it is also recommended you follow the below requirements, which are regarded as the minimum:

- The latest ADC firmware should be used
- The Philips Intellispace system should be installed and operational.
- The initial ADC configuration should be done against the Philips Intellispace sandbox deployment.
- DNS entries for both internal and external access should be configured and working.
- The ADC should be reachable using a web browser and the management IP.

Acronyms used

VIP – Virtual IP
RS – Real Server
ADC – Edgenexus EdgeADC
VS – Virtual Service
RSIP – Real Server IP

Sizing the EdgeADC

The ADC can operate in either physical or virtual deployments. The reverse proxy engine within the ADC is optimized for speed and efficiency. The ADC will use all available threads automatically.

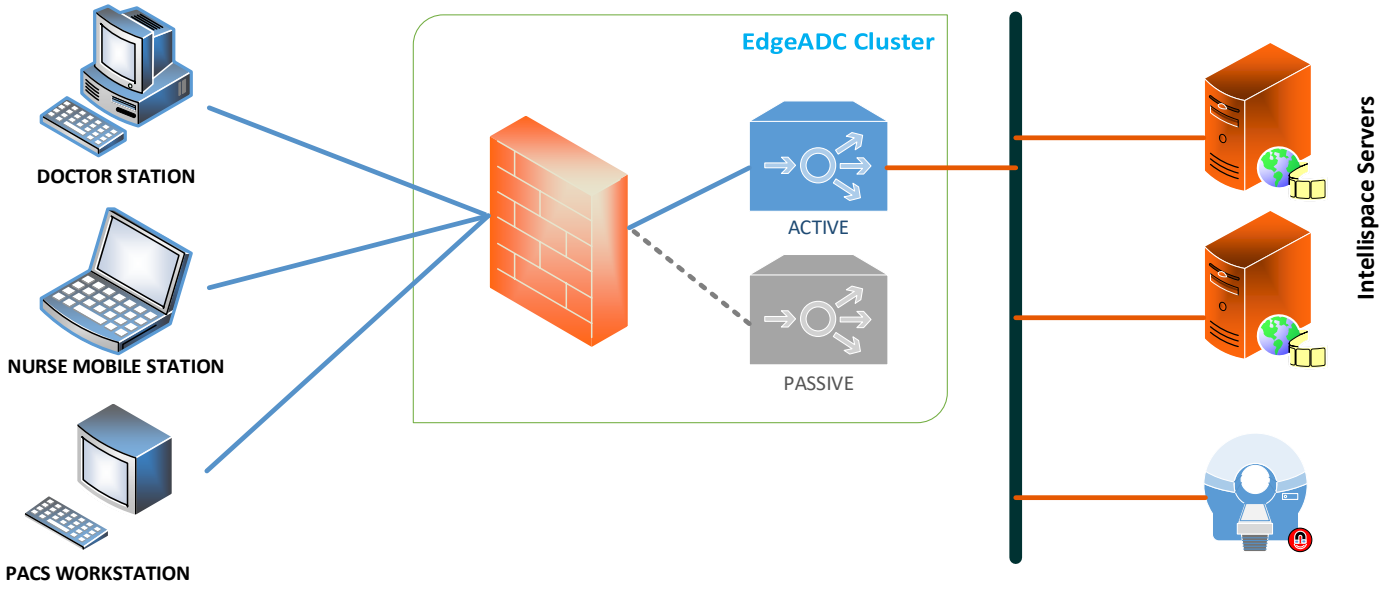
In virtualized environments, we recommend that you set the ADC to 4 vCPU with 8GB RAM, to begin with, and scale up when you need to.

We recommend that you utilize the hardware platforms from our partners in physical environments, with the base system being a quad-core Intel Xeon with 8GB RAM.

In both cases, 50GB of disk storage space should be sufficient.

Deployment Scenarios

Connections to the Philips Intellispace system occur by clients connecting to the VIP or Virtual IP service created on the ADC. The ADC then load-balances the connections to the nodes configured within the ADC and linked to the VIP. An example diagram is shown below.



Virtual Service Methodologies

There are several methods of configuring the ADC for use with Philips Intellispace.

Non-Encrypted Port 80 In this mode, the traffic will enter the ADC using an un-encrypted VIP using port 80. It will then be sent onto the nodes using the same means. Therefore, traffic will not be encrypted when using this mode and is not recommended for best practices. ADC service type Layer 4 TCP is used.

SSL Passthrough In this mode, the traffic enters the ADC on port 443 using SSL. Then, the traffic is sent onto the nodes without inspection. ADC service type Layer 4 TCP is used.

SSL Re-Encrypt In this mode, the SSL traffic is terminated in the ADC and then re-encrypted before passing to the nodes. When this mode is chosen, you will need to have the SSL certificate installed on the nodes and install it in the ADC. This mode is the recommended best practice method for security reasons. ADC service type HTTP is used.

SSL Termination This mode allows SSL traffic to be received by the ADC, which then terminates the SSL encryption internally before passing it to the nodes using unencrypted SSL. This mode may not be the desired choice for security reasons. ADC service type HTTP is used.

You will need to choose the one appropriate to your infrastructure.

Virtual Service Ports for Philips Intellispace

Philips Intellispace utilizes the following ports, and this document will walk you through the configuration of each of them. Please note that this is a guide, and your actual infrastructure may vary from this, so please consult your Philips Intellispace engineering team.

Intellispace Ports

Protocol	Type	Port	Usage
Dicom	TCP	104	Dicom Traffic
Dicom Secure	TCP	2762	Dicom over Secure TLS
DMWL	TCP	8104	Dicom Modality Worklists
DMWL Secure	TCP	10104	Dicom Modality Worklists Secure TLS
QRSCP	TCP	107	Query Retrieve Service Class Provider
QRSCP Secure	TCP	2765	Query Retreive Service Class Provider Secure TLS

Virtual Services

The following are the virtual services required for load balancing Philips Intellispace.

- Log in to the EdgeADC web interface.

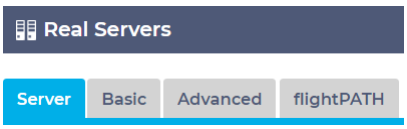
Dicom 104 Virtual Service

- Click **Add Service**
- Add an appropriate value in the **IP address** field. This will be the Virtual IP for the service
- Add the **Netmask** that is appropriate to your infrastructure
- Add **104** in the port field
- Add a suitable description in the Service Name field
- Choose **DICOM** from the Service Type menu
- Click **Update**

The EdgeADC will now create an empty line in the Real Servers section.

- Add the **IP address** of the first Dicom server
- The Port value will automatically be copied over from the VIP configuration. You can change this if needed, causing port forwarding to occur
- Leave the Weight field as is. The EdgeADC will automatically calculate the weight. However, should the servers be disproportionate in terms of specifications, with one server being more powerful and responding to more, or faster, then you will need to manually adjust the Weight values accordingly
- Enter a suitable note in the Note field
- The Cookie ID field is used for Cookie ID Persistence and can be left blank
- Click **Update**

Click the Basic Tab in the Real Servers section.



- Select Load Balancing Policy and choose **IP-List Based**, or other as instructed by the Philips Intellispace team. The Load Balancing Policy is used to select the type of load balancing or, the method of Persistence
- Select **Dicom** from the Server Monitoring menu
- Select **By Virtual Service** in Caching Strategy
- Select **Compression** in the Acceleration menu
- Select **No SSL** in the Virtual Service SSL Certificate menu
- Select **No SSL** in the Real Server SSL Certificate menu
- Click **Update**

Repeat this step for each Real Server. The Status indicator should be green for each of the server entries.

Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
	Online	192.168.159.200	104	100	50	Dicom 1	
	Online	192.168.159.201	104	100	50	Dicom 2	
	Online	192.168.159.202	104	100	50	Dicom 3	

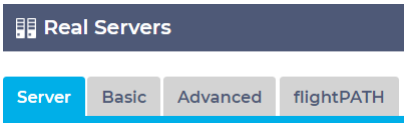
Dicom Secure 2762 Virtual Service

- Click **Add Service**
- Add an appropriate value in the **IP address** field. This will be the Virtual IP for the service
- Add the **Netmask** that is appropriate to your infrastructure
- Add **2762** in the port field
- Add a suitable description in the Service Name field
- Choose **DICOM** from the Service Type menu
- Click **Update**

The EdgeADC will now create an empty line in the Real Servers section.

- Add the **IP address** of the first Dicom server
- The Port value will automatically be copied over from the VIP configuration. You can change this if needed, causing port forwarding to occur
- Leave the Weight field as is. The EdgeADC will automatically calculate the weight. However, should the servers be disproportionate in terms of specifications, with one server being more powerful and responding to more, or faster, then you will need to manually adjust the Weight values accordingly
- Enter a suitable note in the Note field
- The Cookie ID field is used for Cookie ID Persistence and can be left blank
- Click **Update**

Click the Basic Tab in the Real Servers section.



- Select Load Balancing Policy and choose **IP-List Based**, or other as instructed by the Philips Intellispace team. The Load Balancing Policy is used to select the type of load balancing or, the method of Persistence
- Select **Dicom** from the Server Monitoring menu
- Select **By Virtual Service** in Caching Strategy
- Select **Compression** in the Acceleration menu
- Select **Your SSL*** in the Virtual Service SSL Certificate menu
- Select **Your SSL*** in the Real Server SSL Certificate menu. If you are offloading then please select NO SSL.
- Click **Update**

Repeat this step for each Real Server. The Status indicator should be green for each of the server entries.

** Check the EdgeADC administration guide on how to import an SSL certificate.*

Status	Activity	Address	Port	Weight	Calculated Weight	Notes	ID
	Online	192.168.159.200	2762	100	100	Dicom 1	
	Online	192.168.159.201	2762	100	100	Dicom 2	
	Online	192.168.159.202	2762	100	100	Dicom 3	

Dicom Modality Worklist 8104 Virtual Service

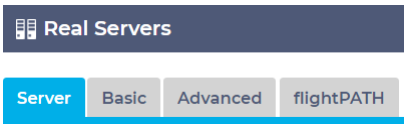
- Click **Add Service**

- Add an appropriate value in the **IP address** field. This will be the Virtual IP for the service
- Add the **Netmask** that is appropriate to your infrastructure
- Add **8104** in the port field
- Add a suitable description in the Service Name field, perhaps DMWL-8104
- Choose **DICOM** from the Service Type menu
- Click **Update**

The EdgeADC will now create an empty line in the Real Servers section.

- Add the **IP address** of the first server
- The Port value will automatically be copied over from the VIP configuration. You can change this if needed, causing port forwarding to occur
- Leave the Weight field as is. The EdgeADC will automatically calculate the weight. However, should the servers be disproportionate in terms of specifications, with one server being more powerful and responding to more, or faster, then you will need to manually adjust the Weight values accordingly
- Enter a suitable note in the Note field
- The Cookie ID field is used for Cookie ID Persistence and can be left blank
- Click **Update**

Click the Basic Tab in the Real Servers section.



- Select Load Balancing Policy and choose **IP-List Based**, or other as instructed by the Philips Intellispace team. The Load Balancing Policy is used to select the type of load balancing or, the method of Persistence
- Select **DICOM** from the Server Monitoring menu
- Select **By Virtual Service** in Caching Strategy
- Select **Compression** in the Acceleration menu
- Select **No SSL** in the Virtual Service SSL Certificate menu
- Select **No SSL** in the Real Server SSL Certificate menu
- Click **Update**

Repeat this step for each Real Server. The Status indicator should be green for each of the server entries.

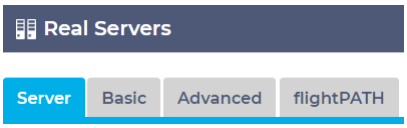
Dicom Modality Worklist Secure 10104 Virtual Service

- Click **Add Service**
- Add an appropriate value in the **IP address** field. This will be the Virtual IP for the service
- Add the **Netmask** that is appropriate to your infrastructure
- Add **10104** in the port field
- Add a suitable description in the Service Name field, perhaps DMWL-Secure-10104
- Choose **DICOM** from the Service Type menu
- Click **Update**

The EdgeADC will now create an empty line in the Real Servers section.

- Add the **IP address** of the first server
- The Port value will automatically be copied over from the VIP configuration. You can change this if needed, causing port forwarding to occur
- Leave the Weight field as is. The EdgeADC will automatically calculate the weight. However, should the servers be disproportionate in terms of specifications, with one server being more powerful and responding to more, or faster, then you will need to manually adjust the Weight values accordingly
- Enter a suitable note in the Note field
- The Cookie ID field is used for Cookie ID Persistence and can be left blank
- Click **Update**

Click the Basic Tab in the Real Servers section.



- Select Load Balancing Policy and choose **IP-List Based**, or other as instructed by the Philips Intellispace team. The Load Balancing Policy is used to select the type of load balancing or, the method of Persistence
- Select **DICOM** from the Server Monitoring menu
- Select **By Virtual Service** in Caching Strategy
- Select **Compression** in the Acceleration menu
- Select **Your SSL*** in the Virtual Service SSL Certificate menu
- Select **Your SSL*** in the Real Server SSL Certificate menu. If you are offloading then please select NO SSL.
- Click **Update**

Repeat this step for each Real Server. The Status indicator should be green for each of the server entries.

** Check the EdgeADC administration guide on how to import an SSL certificate.*

QRSCP 107 Virtual Service

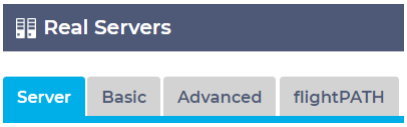
IntelliSpace QRSCP, provided by Philips, is a healthcare informatics solution that functions as a Query Retrieve Service Class Provider within a DICOM network, facilitating the communication, storage, and exchange of medical imaging data between various DICOM-compliant modalities and systems. It essentially acts as a hub in a medical imaging network, allowing different DICOM devices and applications like PACS to query and retrieve medical images and related information efficiently and securely, thus enhancing the interoperability and seamless exchange of medical imaging data within healthcare settings.

- Click **Add Service**
- Add an appropriate value in the **IP address** field. This will be the Virtual IP for the service
- Add the **Netmask** that is appropriate to your infrastructure
- Add **107** in the port field
- Add a suitable description in the Service Name field, perhaps QRSCP-107
- Choose **HTTP** from the Service Type menu
- Click **Update**

The EdgeADC will now create an empty line in the Real Servers section.

- Add the **IP address** of the first server
- The Port value will automatically be copied over from the VIP configuration. You can change this if needed, causing port forwarding to occur
- Leave the Weight field as is. The EdgeADC will automatically calculate the weight. However, should the servers be disproportionate in terms of specifications, with one server being more powerful and responding to more, or faster, then you will need to manually adjust the Weight values accordingly
- Enter a suitable note in the Note field
- The Cookie ID field is used for Cookie ID Persistence and can be left blank
- Click **Update**

Click the Basic Tab in the Real Servers section.



- Select Load Balancing Policy and choose **IP-List Based**, or other as instructed by the Philips Intellispace team. The Load Balancing Policy is used to select the type of load balancing or, the method of Persistence
- Select **Ping** from the Server Monitoring menu
- Select **By Virtual Service** in Caching Strategy
- Select **Compression** in the Acceleration menu
- Select **No SSL** in the Virtual Service SSL Certificate menu
- Select **No SSL** in the Real Server SSL Certificate menu
- Click **Update**

Repeat this step for each Real Server. The Status indicator should be green for each of the server entries.

QRSCP Secure 2765 Virtual Service

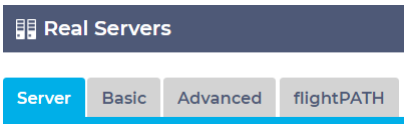
- Click **Add Service**
- Add an appropriate value in the **IP address** field. This will be the Virtual IP for the service
- Add the **Netmask** that is appropriate to your infrastructure
- Add **2765** in the port field
- Add a suitable description in the Service Name field, perhaps QRSCP-Secure-2765
- Choose **HTTP** from the Service Type menu
- Click **Update**

The EdgeADC will now create an empty line in the Real Servers section.

- Add the **IP address** of the first server
- The Port value will automatically be copied over from the VIP configuration. You can change this if needed, causing port forwarding to occur
- Leave the Weight field as is. The EdgeADC will automatically calculate the weight. However, should the servers be disproportionate in terms of specifications, with one server being more powerful and responding to more, or faster, then you will need to manually adjust the Weight values accordingly

- Enter a suitable note in the Note field
- The Cookie ID field is used for Cookie ID Persistence and can be left blank
- Click **Update**

Click the Basic Tab in the Real Servers section.



- Select Load Balancing Policy and choose **IP-List Based**, or other as instructed by the Philips Intellispace team. The Load Balancing Policy is used to select the type of load balancing or, the method of Persistence
- Select **Ping** from the Server Monitoring menu
- Select **By Virtual Service** in Caching Strategy
- Select **Compression** in the Acceleration menu
- Select **Your SSL*** in the Virtual Service SSL Certificate menu
- Select **Your SSL*** in the Real Server SSL Certificate menu. If you are offloading then please select NO SSL.
- Click **Update**

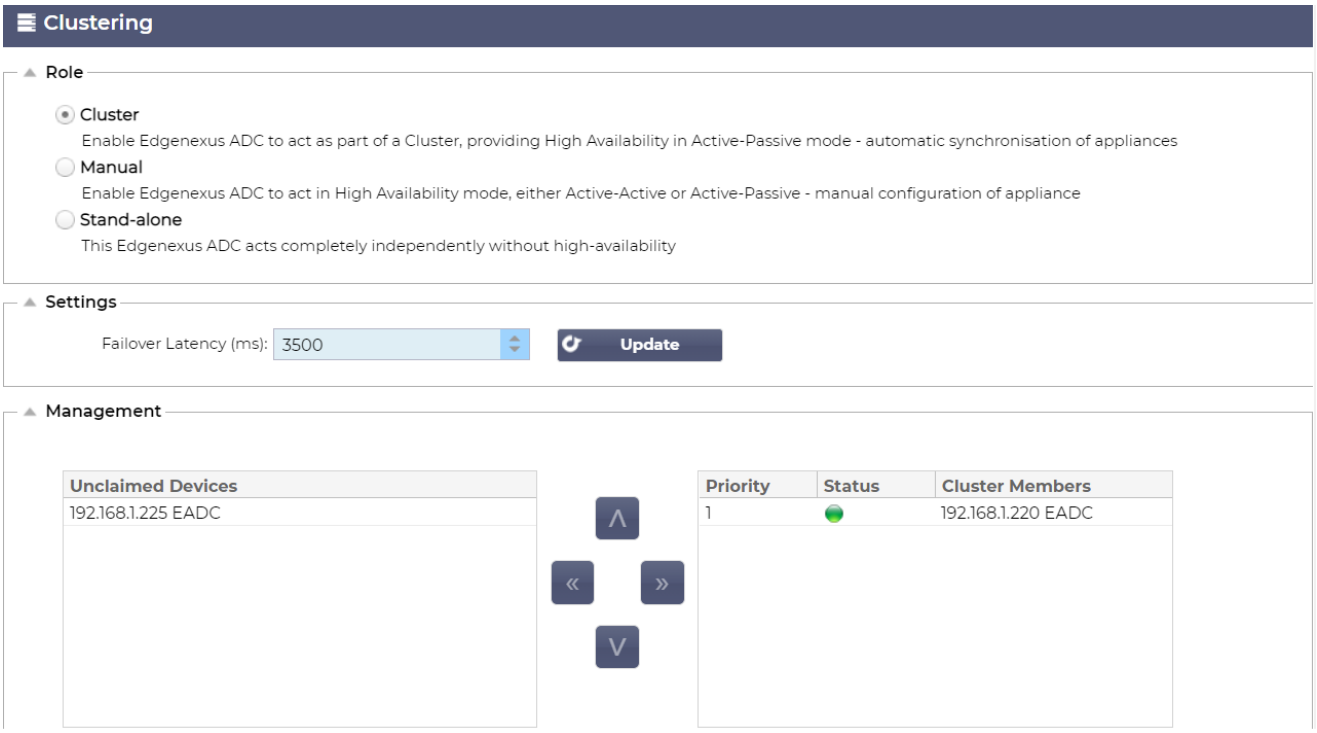
Repeat this step for each Real Server. The Status indicator should be green for each of the server entries.

** Check the EdgeADC administration guide on how to import an SSL certificate.*

Clustering the EdgeADC

The EdgeADC can operate as a stand-alone appliance, and it is incredibly reliable. However, in terms of best practice, we must accept that it is as critical as the servers it is load balancing, and we would therefore recommend placing it in a cluster.

- First, stand up a second EdgeADC in the same subnet as the primary.
- Once you have licensed it logon to your Primary EdgeADC
- Proceed to System > Clustering
- You should see the page as below.



- You will notice that there are two panels within the Management panel. On the left is the Unclaimed panel. On the right is the Cluster showing the cluster members, their priority, and status.
- In between the two panels is a cluster of arrow buttons.
- Click on the EdgeADC that is in the Unclaimed Panel and click the RIGHT arrow button.
- This action moved the unclaimed EdgeADC into the cluster.
- Immediately it is moved across; the Primary will replicate its settings, including VIPs to the secondary. Note that any apps you have added to the Primary will not be replicated to the Secondary – examples are WAF, GSLB, etc.
- After clustering, the Management panel should look like the one below.