Microsoft Azure

EdgeADC Deployment Guide

Document Properties

Document Number: 2.0.3.31.25.12.03

Document Creation Date: 5 August 2021

Document Last Edited: 31 March 2025

Document Author: Jay Savoor

Document Last Edited by:

Document Disclaimer

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

Copyrights

Trademarks

Edgenexus logo, Edgenexus, EdgeADC, EdgeWAF, EdgeGSLB, EdgeDNS are all Edgenexus Limited's trademarks. 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

This document covers the initialisation of the EdgeADC in the Microsoft Azure environment.

Licensing Methodologies in Azure

There are two methods of licensing the EdgeADC in Azure.

Azure Timed License

This method of licensing and deployment uses Azure's time-based licensing and charging. You will be charged for the use of the EdgeADC on an hourly basis. There are several sizes of EdgeADC to choose from when using this licensing model.

- 500 Mbps – allows a maximum throughput of 500 Mbps.
- 1 Gbps – allows a maximum throughput of 1 Gbps.
- 3 Gbps – allows a maximum throughput of 3 Gbps.
- 10 Gbps – allows a maximum throughput of 10 Gbps.
- Unlimited – allows an unlimited throughput with no maximum.

Bring-Your-Own-License (BYOL)

The BYOL license version of the product allows you to purchase licenses from your reseller partner and utilise them in the Azure deployed EdgeADC. This highly flexible method means you can use this license in any environment should you wish to move from the Azure system at a future date. It also allows the use of both perpetual and SaaS licenses available from Edgenexus. The license can be one of the following types:

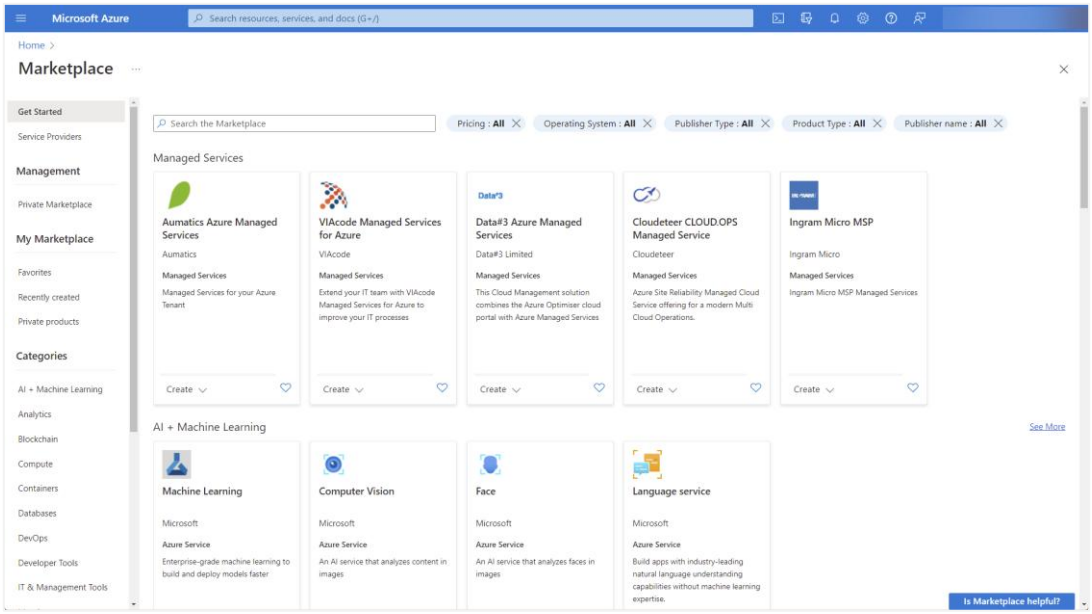
- Perpetual
  - 300 Mbps – allows a maximum throughput of 300 Mbps.
  - 1 Gbps – allows a maximum throughput of 1 Gbps.
  - 3 Gbps – allows a maximum throughput of 3 Gbps.
  - 6 Gbps – allows a maximum throughput of 6 Gbps.
  - Unlimited – allows an unlimited throughput with no maximum.
- SaaS Annual Contract
  - 300 Mbps – allows a maximum throughput of 300 Mbps.
  - 1 Gbps – allows a maximum throughput of 1 Gbps.
  - 3 Gbps – allows a maximum throughput of 3 Gbps.
  - 6 Gbps – allows a maximum throughput of 6 Gbps.
  - Unlimited – allows an unlimited throughput with no maximum.

The license is installed using the EdgeADC's interface located in *System* > *Licensing*.

Deploying the EdgeADC Azure Appliance

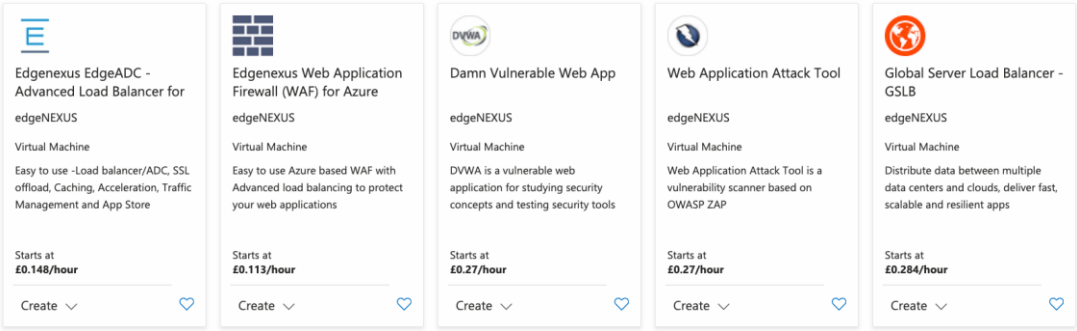
Please follow the steps below to deploy the EdgeADC on Azure.

The first step is to access your Azure Portal and the Azure Marketplace. You should see something similar to the image below.



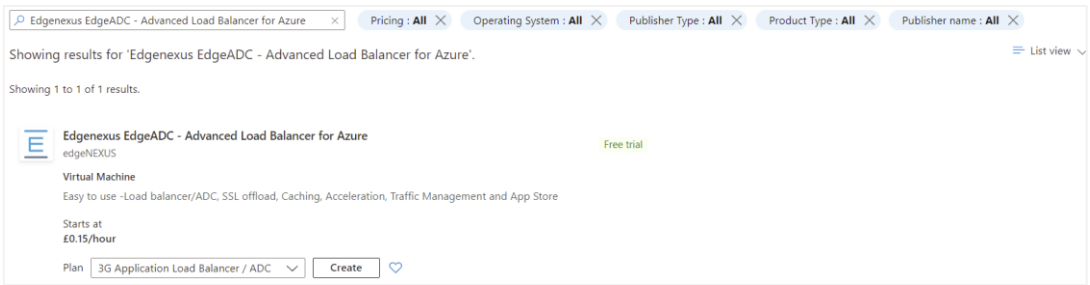
Finding and selecting the product

Search for Edgenexus and select the option: Edgenexus EdgeADC – Advanced Load Balancer for Azure.

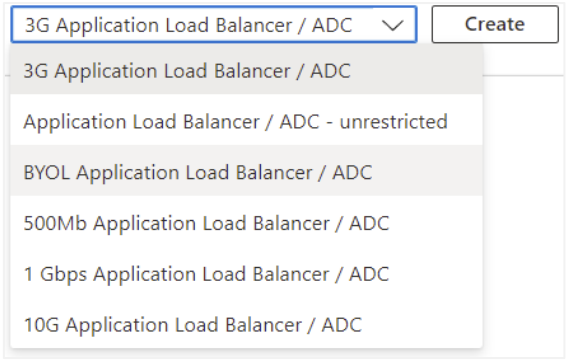


Selecting the right plan

The next screen you will see will be the EdgeADC product page and its different plan selections. The BYOL plan allows you to rent the virtual machine from Azure, and purchase the license from us.



The drop-down menu allows you to select the license type from the options available within the Plan menu and click the Create button to initialise the creation of the appliance.

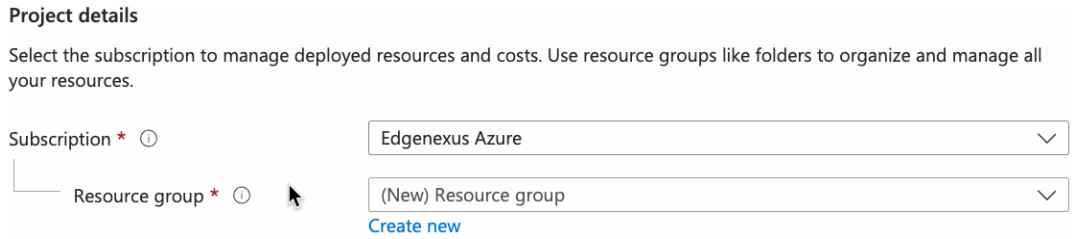


Once you have selected the plan you need, click the Create button.

Basic Configuration

You will be taken to the next series of settings, starting with the Basic section within the Create a Virtual Machine section.

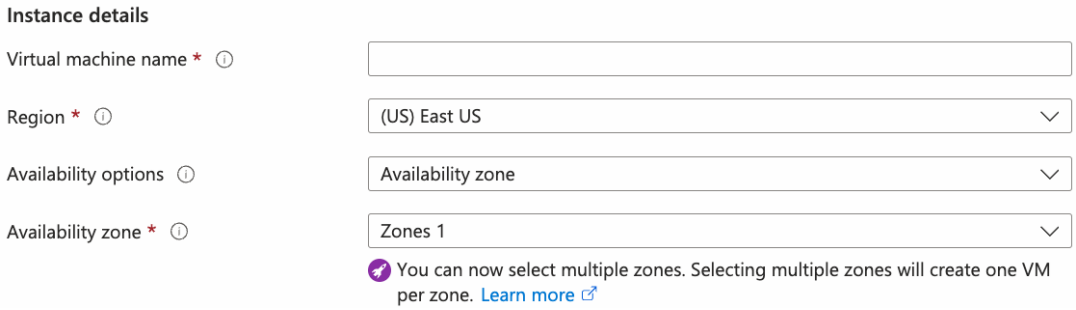
Project details



This section requires you to select the Resource Group. The Subscription section should already be pre-populated for you.

Instance details

Next is the are the details of the Instance. The first section of this deals with the name, location, availability options and the Azure zones the machines will be available within.

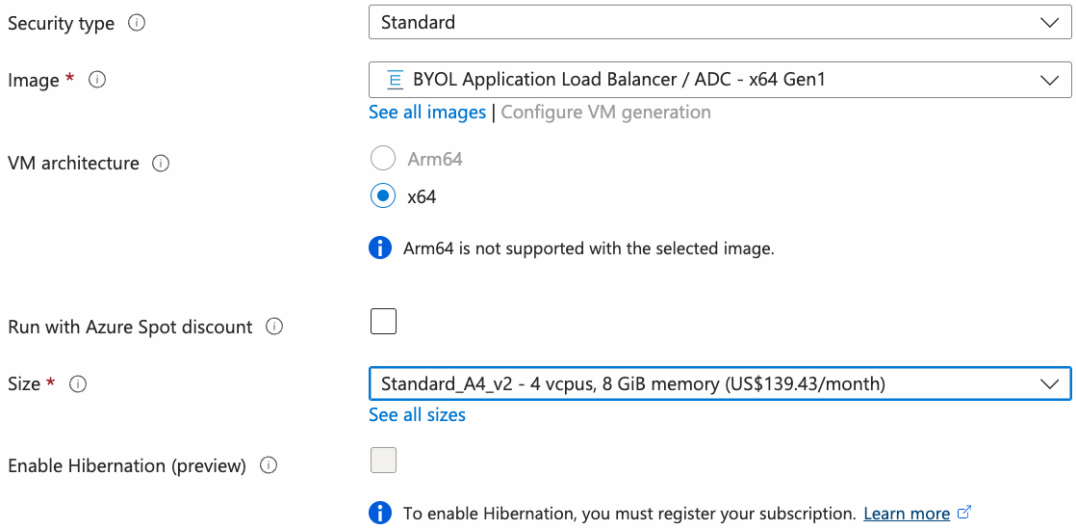


The next section covers the security, image to load and the architecture. Also included is whether you wish to utilise the Azure SpotDiscount, and whether you wish to enable hibernation. Our recommendation is as shown in the image below.

Our suggestion is that:

- Hibernation = Disabled.

- CPU = 4vCPU
- Memory= 8GB or higher
- Local Disk 40GB or higher.



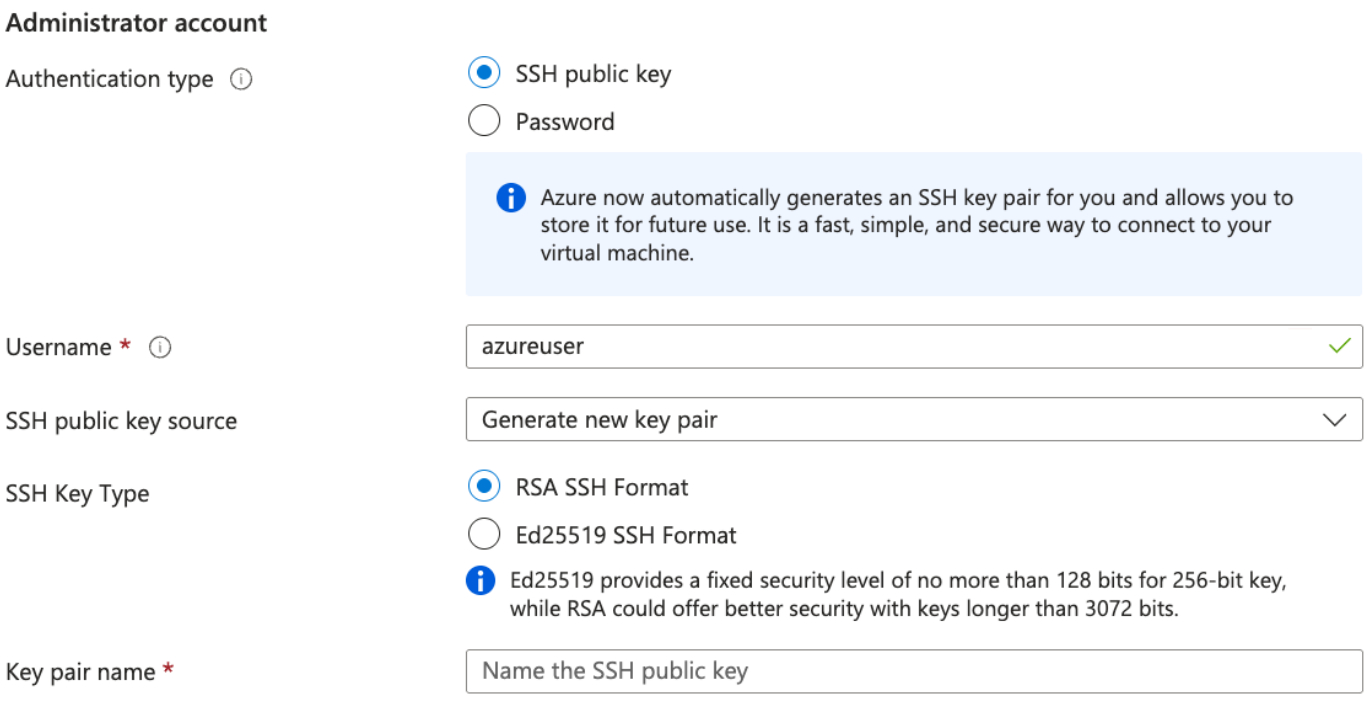
The choice of VM size really depends on the core usage, with CPU affected by SSL Re-encryption etc.

Administrator Account for SSH CLI Login

There are two distinct methods in which Administrator access can be provided to the EdgeADC's VM management interface.

SSH Public Key Method

This is one of the most secure methods of accessing the ADC's command interface.

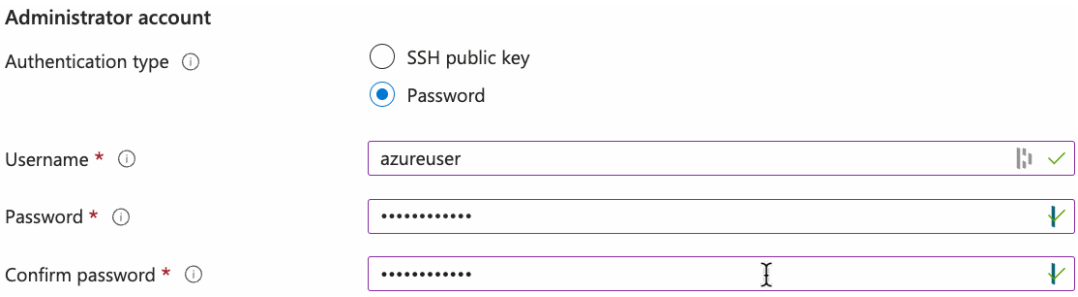


- Select your choice form the SSH Public Key Source menu.
- Provide a name for the Key Pair

IMPORTANT Make a note of the SSH key if you generate a new one. Without this you will not be able to access the command interface.

Password Method

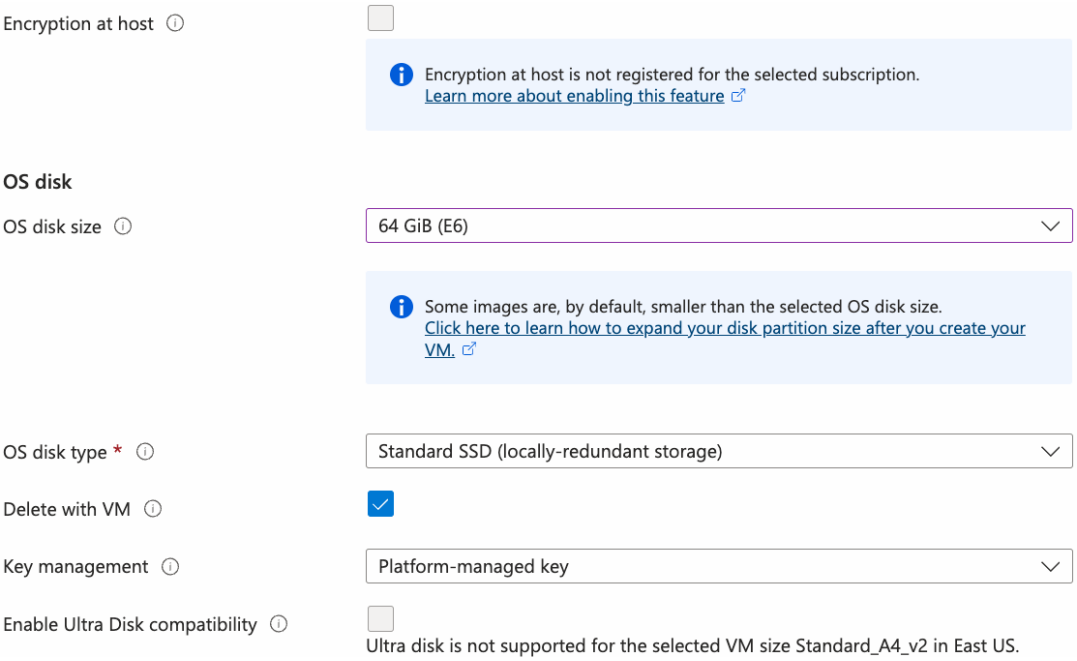
The alternative method is to use the password method.



- Specify the username as **azureuser**.
- Specify a password of your choice that is deemed as secure.

Note: It is important to remember that the admin login name for the EdgeADC in Azure is **admin** and **not** the one for the Command interface.

Disk Configuration



The Disks section of configuration allows you to select what type and size of storage is to be used.

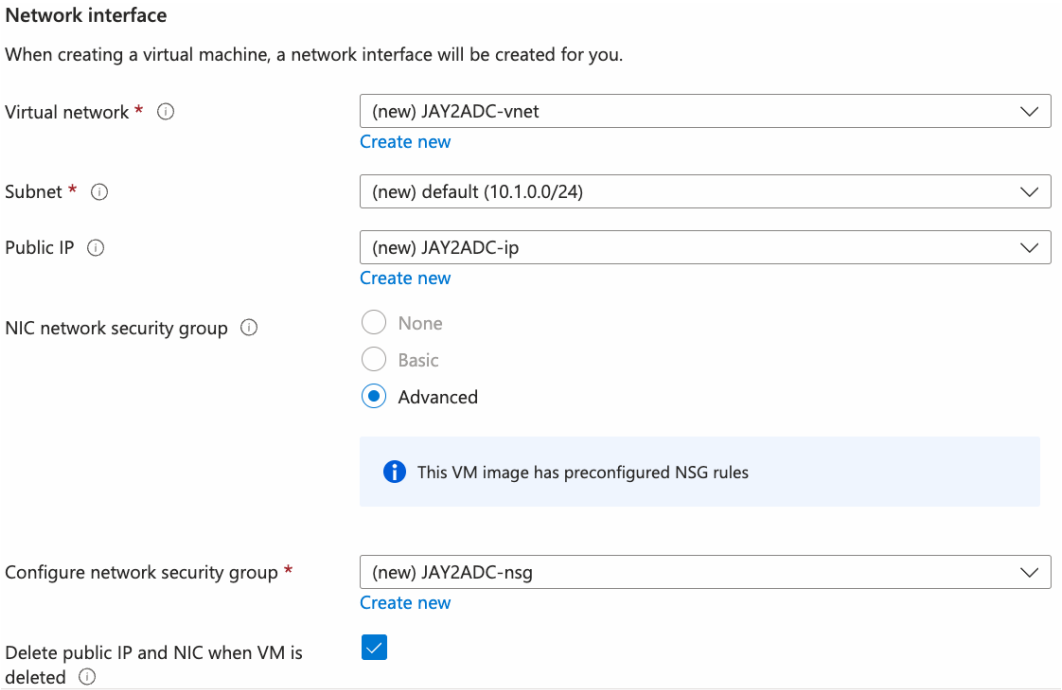
You can choose the size of the OS Disk Size. We have chosen 64 GiB (E6) as ours, but you may choose whichever you wish.

Also, you can select the type of drive, and we recommend you choose Standard SSD

Tick the Delete with VM button – this is important if you are testing the ADC and will save unnecessary costs should you delete the VM.

Leave all other values as you see them in the image above.

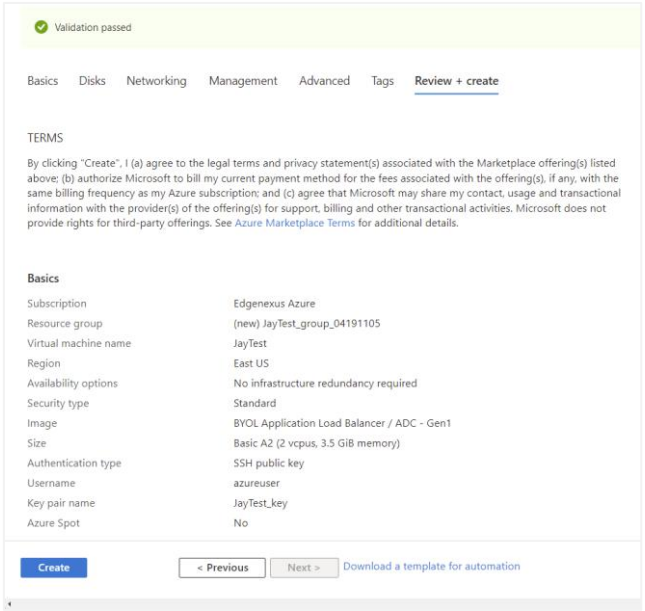
Networking



There is no real need to change anything on this page. The Public IP is the address you will use to access the user interface of the ADC.

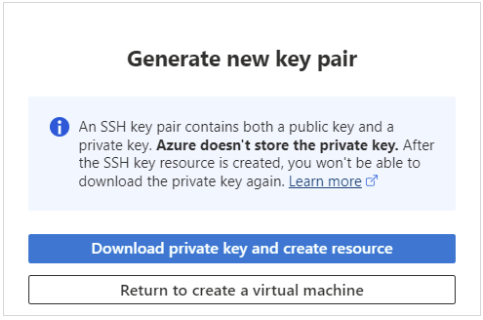
You can skip onto Tags.The final page before the *Review and Create* is *Tags*. If you wish to add tags to your ADC VM, you can do this here.

Finally, you can review and create the ADC in the last Review & Create stage.

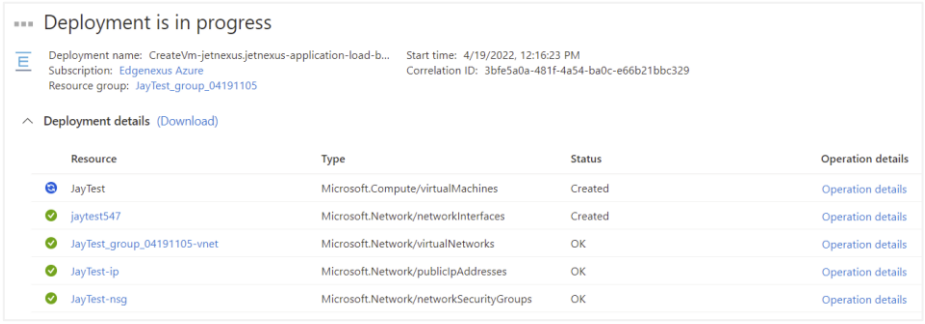


You will then be asked to download and store the Private Key Pair.

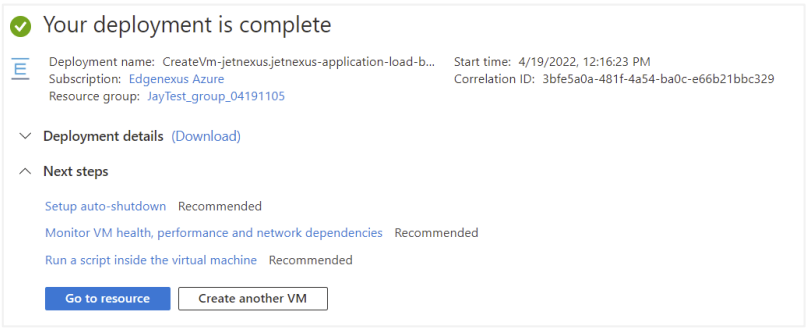
IMPORTANT: The Private Key Pair cannot be recovered and downloaded once the VM is created – keep it safely.



Following the download, you will see something similar to the page below.



Once the deployment is complete, you will see the screen below.



Once deployment has been completed, you can then go to the resource.

To test the ADC and configure it, please use your browser to access the following URL: https://{IP.ADDRESS}:27376.

This will bring up the GUI login. The username and password are:
username: **azureuser**
password: {**password.you.set**}

Note: if you need to add additional network interfaces within the internal network to the EdgeADC, you can do this using the Networking section and add them to the ADC GUI within *System* > *Networking*.

Clustering in Azure

Under normal circumstances it is not possible to cluster ADCs within the Azure network fabric.

Azure's networking fabric does not support Multicast or Broadcast, the latter of which is used by the ADC for detecting and setting up the clustering.

We have added the ability to have clustering capabilities within the latest version of the EdgeADC. So, lets take a look at how the clustering capabilities work.

Important: Both ADCs must be in the same network. In cases where they are going to be in different zones, the network must still spread across and each ADC must be able to communicate with the other.

Azure Regions and Zones

Azure regions and zones are key concepts in the architecture of Microsoft Azure, a cloud computing service.

Azure Regions

- A region in Azure is a geographical location containing at least one data center, but almost certainly multiple.
- These regions are typically far apart and located in different countries or areas within a country to ensure redundancy and high availability.
- Each region is connected through a dedicated regional low-latency network, enhancing the performance and scalability of the services offered.
- When a user deploys a service, an app, or VMs in Azure, they can select a specific region where it will be hosted. Decisions such as this could be influenced by factors like the proximity to the user base, legal or compliance requirements, or the availability of certain Azure services within that region.
- Microsoft ensures that regions are equipped with comprehensive support for all Azure services, but the availability of some services can vary from region to region.

Azure Availability Zones

Within each Azure region, there can be multiple Availability Zones. These are physically separate locations within an Azure region.

- Each Azure zone comprises one or more data centers equipped with the best independent power, cooling, and networking technologies.
- The idea is to protect applications and data from data center failures through redundancy and logical isolation of services.
- Availability Zones are connected through high-speed, private fiber-optic networks.
- By architecting applications across multiple zones, businesses can ensure higher levels of resilience and redundancy. If one zone becomes unavailable due to unforeseen circumstances like natural disasters or system failures, the other zones can continue functioning, minimizing downtime and data loss.

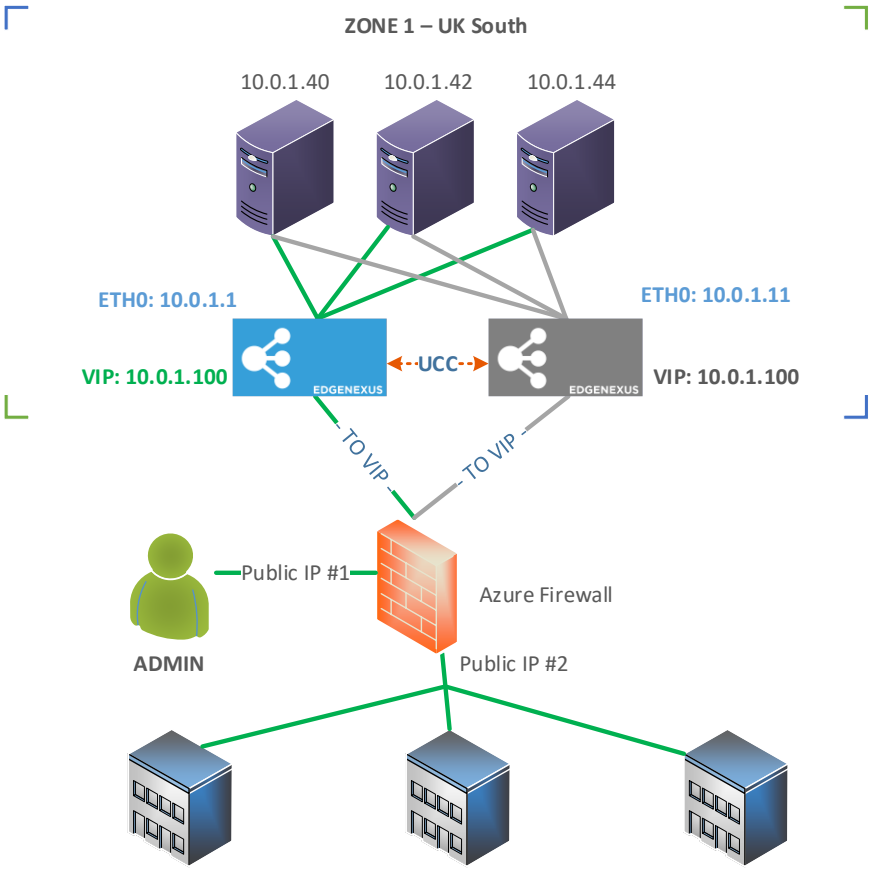
Single Zone Clustering

When you create your application related virtual machines within a zone, you are provided with a set of private IP addresses that you can utilise. It is always best practice to make sure you have enough private IP addresses so you may make use of other technologies within your own network.

When the ADC is deployed within Azure, and more specifically, your private network zone, it will be assigned a public IP address, together with an internal IP address. The public IP address is used by externally located users to access the virtual service on the ADC, while ADCs private address is used as

the Greenside IP (eth0). The internal IP address can also be used for the VIP when application access is required from the Internet, and also for configuration purposes.

When you have two ADCs in cluster within the same zone, they will look something like the diagram below.



In this example, we can see the following:

- The Region is UK South
- The Zone is 1
- There are three (3) real servers
- There are two (2) ADCs
- There are two (2) public IP addresses

Note: Public IP addresses are only required when access to the ADCs, either for management or application access purposes is made across the Internet. When the ADCs are part of an internal private network the public IP addresses are not really applicable.

When the ADCs are created within Azure, they are allocated a single public IP address together with an internal IP address linked to eth0 of the ADC. This public IP address is used to manage the ADC using https://{Public.IP.Address}:27376.

But users cannot access the ADC's load balanced applications through the administrator's public IP. The way forward is to provide a secondary public IP address that NATs to its internal IP address, this being used for the VIP.

In order for clustering to perform and application access to work, we need to have floating an internal IP address for any master VIPs. These are allocated to the VIPs, with any VIP receiving access from across the Internet requiring it's own Public IP address.

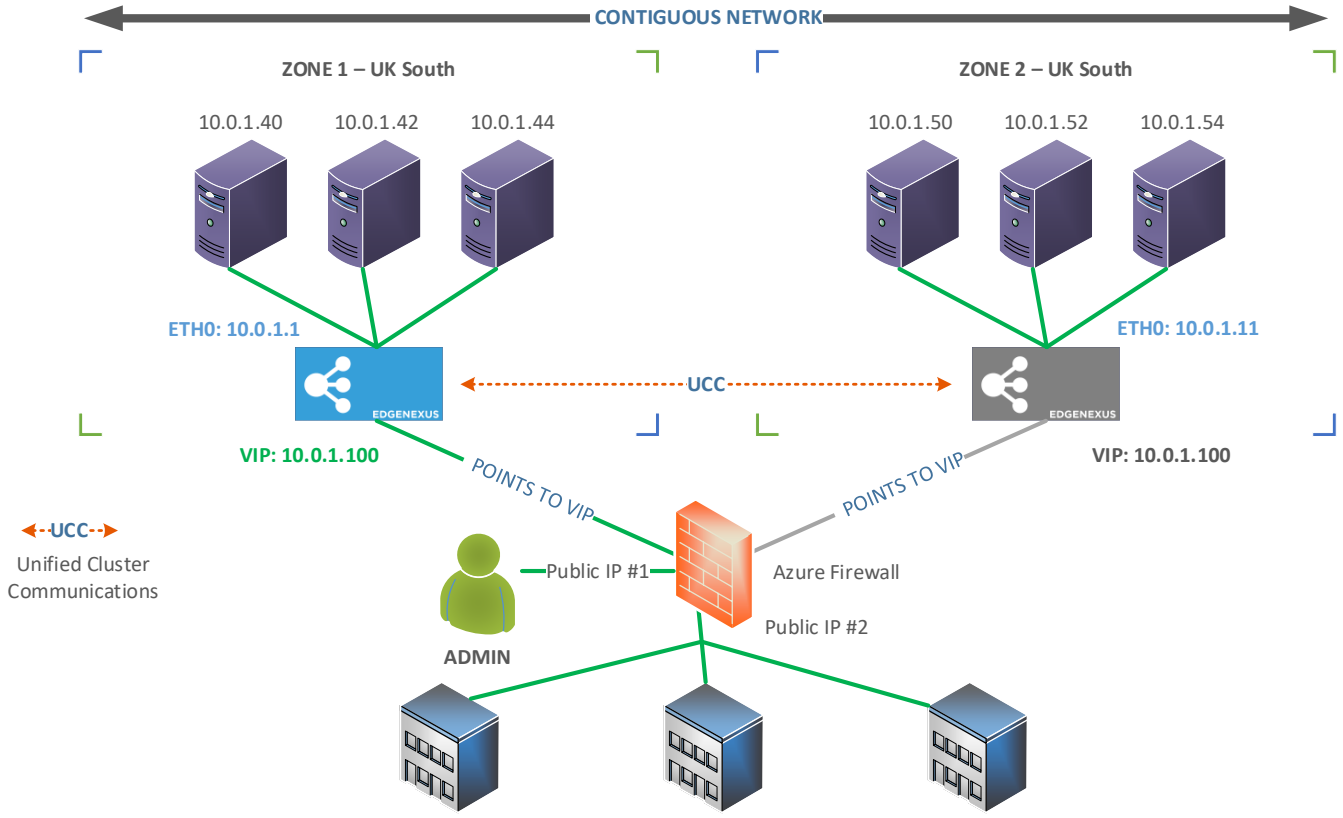
Multi-Zone Spanned Network Clustering

For some customers, Microsoft will provide specific network fabric that stretches across zones within a region. In this way the IP addresses all belong to the same pool, creating what is essentially a single spanning network.

There are a few important aspects when clustering across zones in Azure.

1. The zones must all reside within the same region
2. The network must extend across the zones. This is something that Microsoft can provide through their Azure networking team.

Once these requirements are met, the clustering design would look something like the image below.

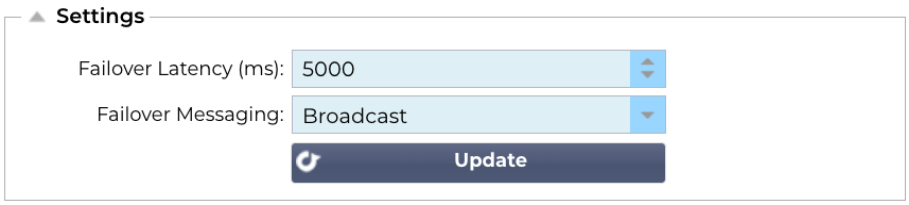


In this diagram, we can see that we have two distinct zones, within the UK South region. Normally, these zones would have their own independent IP ranges available for Azure customers. But for clustering to take place successfully, the zones need to have a contiguous network range spanning them, so the ADC in zone 1 can talk directly to zone 2 thereby enabling clustering.

Setting up Azure Clustering

In order to provide the clustering capability within the Azure system, we have added some additional configuration options within the System > Clustering page.

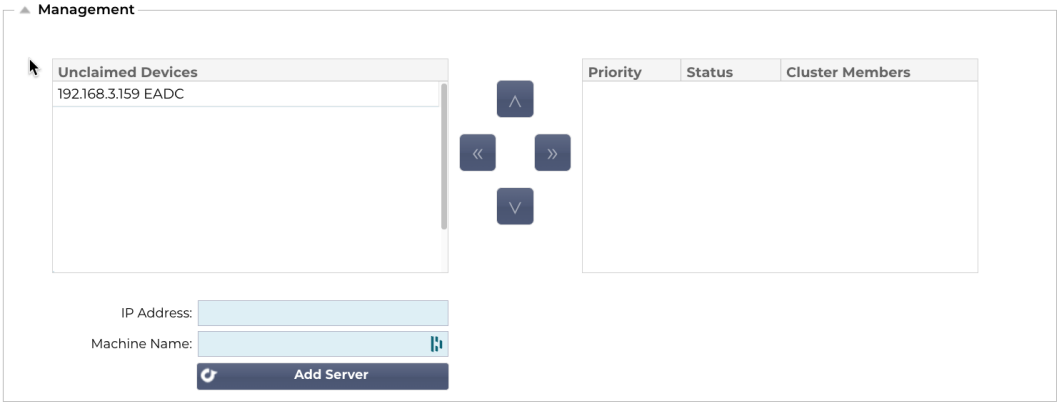
Failover Messaging



Located in the Settings section, the new Failover Messaging menu consists of three options:

Option	Explanation
Broadcast	This is the default setting for the ADC. In this mode, the ADC shows unclaimed devices and uses failover communication using broadcast.
Unicast	This mode does not use broadcast as a means of communicating with other ADC members. When set to this mode, you will need to use the IP Address and Name fields to add the unclaimed ADC to the cluster. This mode is provided for use within Azure.
Mixed	In Mixed mode, the ADC will use broadcast to show unclaimed devices, but use Unicast for failover communications.

IP Address and Name



When the Failover Messaging mode is set to Unicast, you will need to add the prospective cluster member using the IP Address and Name fields.

CRITICAL NOTE: When you enter the IP address and Machine Name, please ensure that you enter the information carefully. The Machine Name is found in System > Networking, and is case sensitive for security purposes. Should you enter an IP address without a Machine Name, or an IP address of something other than an Edgenexus ADC, then it may be accepted temporarily while validation takes place, but will be rejected finally.

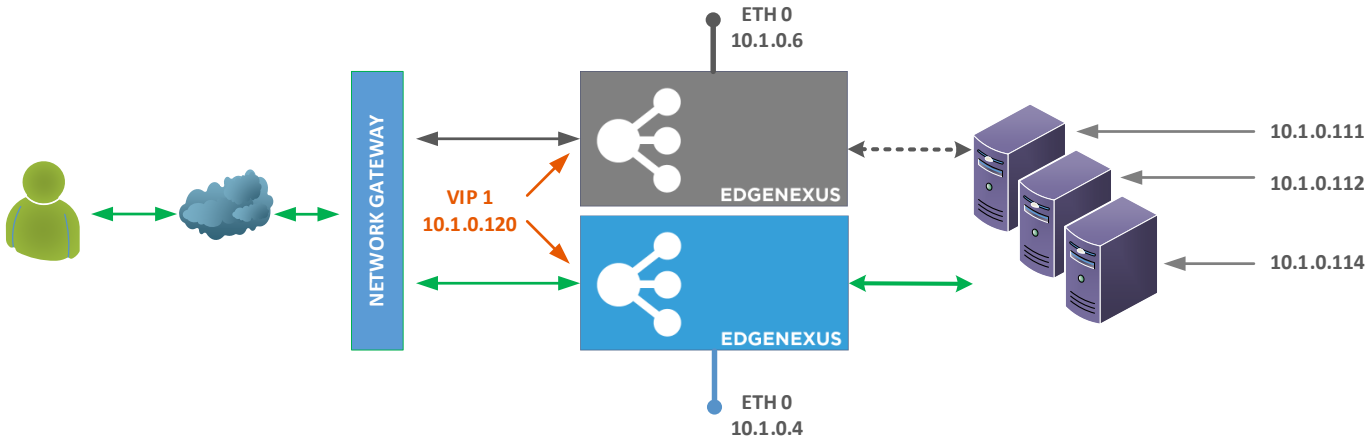
Virtual IP Setup

As can be seen by the diagrams shown earlier in this document, the ETH0 network interfaces have independent internal IP addresses. These IP addresses cannot be used as VIP addresses when you are performing clustering.

So we need to assign an internal Azure IP address for each VIP that we are going to utilise for application load balancing. These internal IP addresses will be from your internal network pool.

You will note that you can only access the VIPs from within the Azure network as they are private IP addresses, and this may well be ok for large organizations that have VPNs or networks that connect to the Azure network.

In such cases, the network may look something like this:



But for customers that wish to connect to the VIP IP addresses through the Internet, via the Azure Firewall using an Azure Public IP address, you will need the assistance of an Azure certified engineer to help set this access up. In such a case, the Azure Public IP Adddress will need to be NAT'd to the VIP address of the ADC.

Technical Support

Pre-Sales Support

If you are evaluating our producs and require support or have any questions you would like to ask, please email presales@edgenexus.io.

After-Sales Support

Should you have any requirement for our technical support, this is available via our website. Please visit our website at www.edgenexus.io/support from where you will be able to access us via email or telephone.