HA Cloud Connector – for Azure

Installation & Configuration Guide

SOFTWARE VERSION

2.X.X

Document Properties

Document Number: 2.0.8.9.24.11.08

Document Creation Date: 1 August 2024

Document Last Edited: 9 August 2024

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 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

© 2024 All rights reserved.

Information in this document is subject to change without prior notice and does not represent a commitment on the manufacturer's part. No part of this guide may be reproduced or transmitted in any form or means, electronic or mechanical, including photocopying and recording, for any purpose, without the express written permission of the manufacturer. Registered trademarks are properties of their respective owners. Every effort is made to make this guide as complete and accurate as possible, but no warranty of fitness is implied. The authors and the publisher shall have neither responsibility nor liability to any person or entity for loss or damages arising from using the information contained in this guide.

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

Table of Contents

Document Properties 1
Document Disclaimer 1
Copyrights 1
Trademarks 1
Edgenexus Support 1
What is the HA Cloud Connector? 4
Why is HACC needed? 4
How does it work? 4
Prerequisites and Architecture 5
Important 5
Prerequisites 5
Architecture 6
Understanding the Logic Flow 7
Microsoft Azure 8
Important - Using Tags 9
Preparing Azure for HACC 10
Creating the App registration 10
Creating a Resource Group 11
Access Control (IAM) and Roles 12
Creating the ADC Virtual Machines 15
Configuring the Virtual Machine 18
Networking 18
Adding a Subnet 19
Attach a Network Interface to new Subnet 20
Creating IP Addresses for Accessing 21
Creating a Public IP Address 21
Creating Private IP Addresses 23
Important Information Required to Deploy HACC 25
Checklist 25
Information required to proceed 25
Configuring the EdgeADC 26
Configuring the ADC networking 26
Defining the Virtual Services 27
Creating the Monitoring VIPs 28
Simple App Monitoring 28

© 2024 Edgenexus Limited

Cross ADC Monitoring....28
Installing the HA Cloud Connector....30
Deploying the HA Cloud Connector....30
Making the App Operational....30
Configuring the HA Cloud Connector for Azure....32
Logging onto the HA Cloud Connector Console....32
The Cloud Connector Main Page....33
Defining Cloud Connections....33
Defining Destinations for HA....36
Defining Services to be Monitored....37
Testing the HA Cloud Connector for Azure....38
The Failback Setting....39
Enabled Mode....39
Disabled Mode....39
Force Failover by Service....40
Force Failover by Destination....40
Other Settings....41
Changing the password....41
Dark Mode....42
Full-Screen Mode....42
Technical Support....43
Contacting Support....44

© 2024 Edgenexus Limited

What is the HA Cloud Connector?

Designed especially for use with an Edgenexus EdgeADC pair within Cloud environments such as Microsoft Azure, or Amazon AWS, the HA Cloud Connector (HACC) monitors the ADC and Applications for availability. It communicates with the cloud system API to move elastic, or floating IPs to the secondary failover ADC, or vice versa, and ensure continuous availability.

Why is HACC needed?

Normally, within LAN environments you do not need to have something like HACC. In a LAN we can create any IP within our IP segment, address it, and utilise it when we need to. This is not the case within Cloud environments, as they are compartmentalised and highly restricted in terms of users being able to do what every they wish.

This means that setting up load balancers in HA pairs is extremely complex and requires the use of the cloud providers' own load balancer to distribute the floating IP.

HACC has been designed and built to alleviate this issue allowing users to have HA pairs of load balancers without the use of the cloud provider load balancer as an IP address distributor.

How does it work?

The HACC works by utilising a special monitoring Virtual Service, whose job is to monitor, not just the connection to the Real Servers but also the active ADC through its HA passive partner, and work with Cloud provider's API to move the floating IP to the passive ADC, and thus enact the failover.

Important:

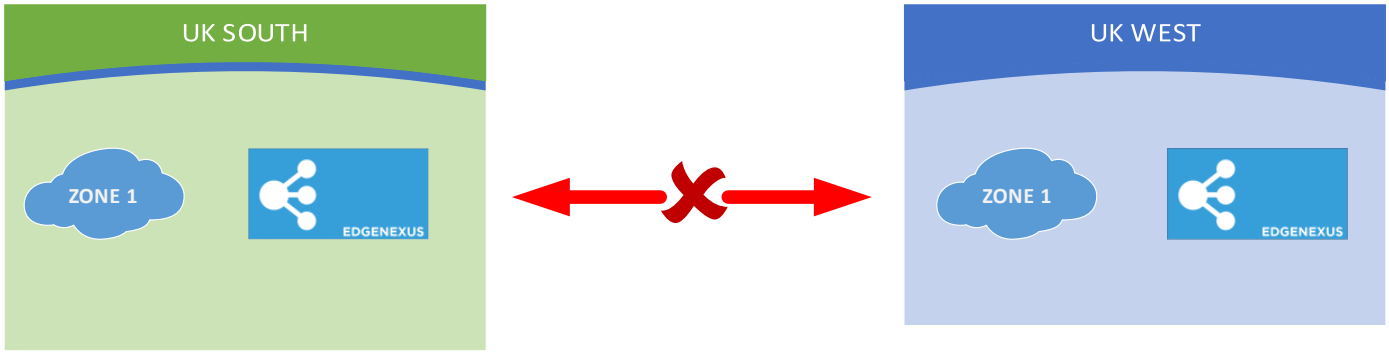
It must be noted that you can only form an ADC pairing for floating IP switching within a region. You can have the ADCs located in different zones, but the network must be contiguous.

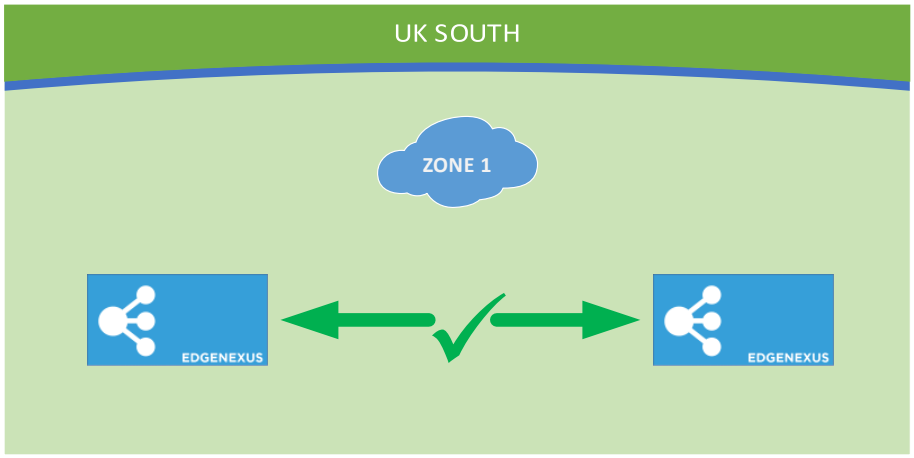
© 2024 Edgenexus Limited

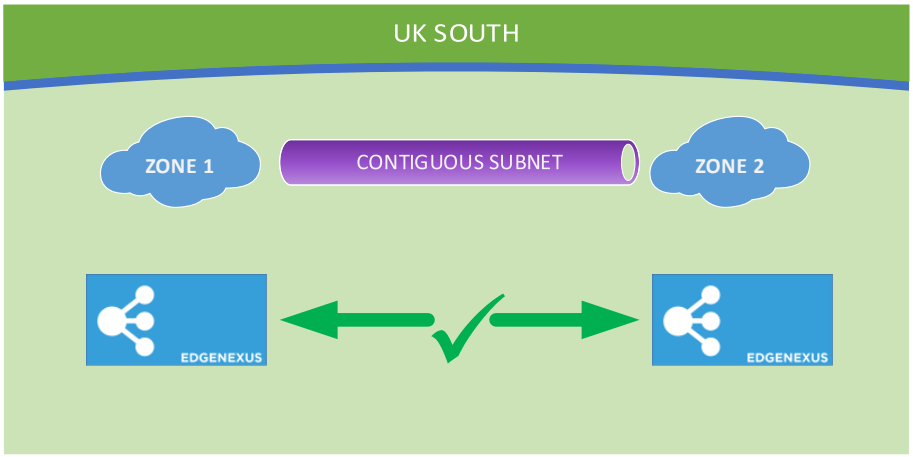
Prerequisites and Architecture

Important

The HACC App and functionality is designed to work within the same Cloud region. It cannot operate across regions. You can however use it across two zones, if there is a contiguous network linking the two zones.







Prerequisites

To use the HACC, you need to fulfil certain prerequisites.

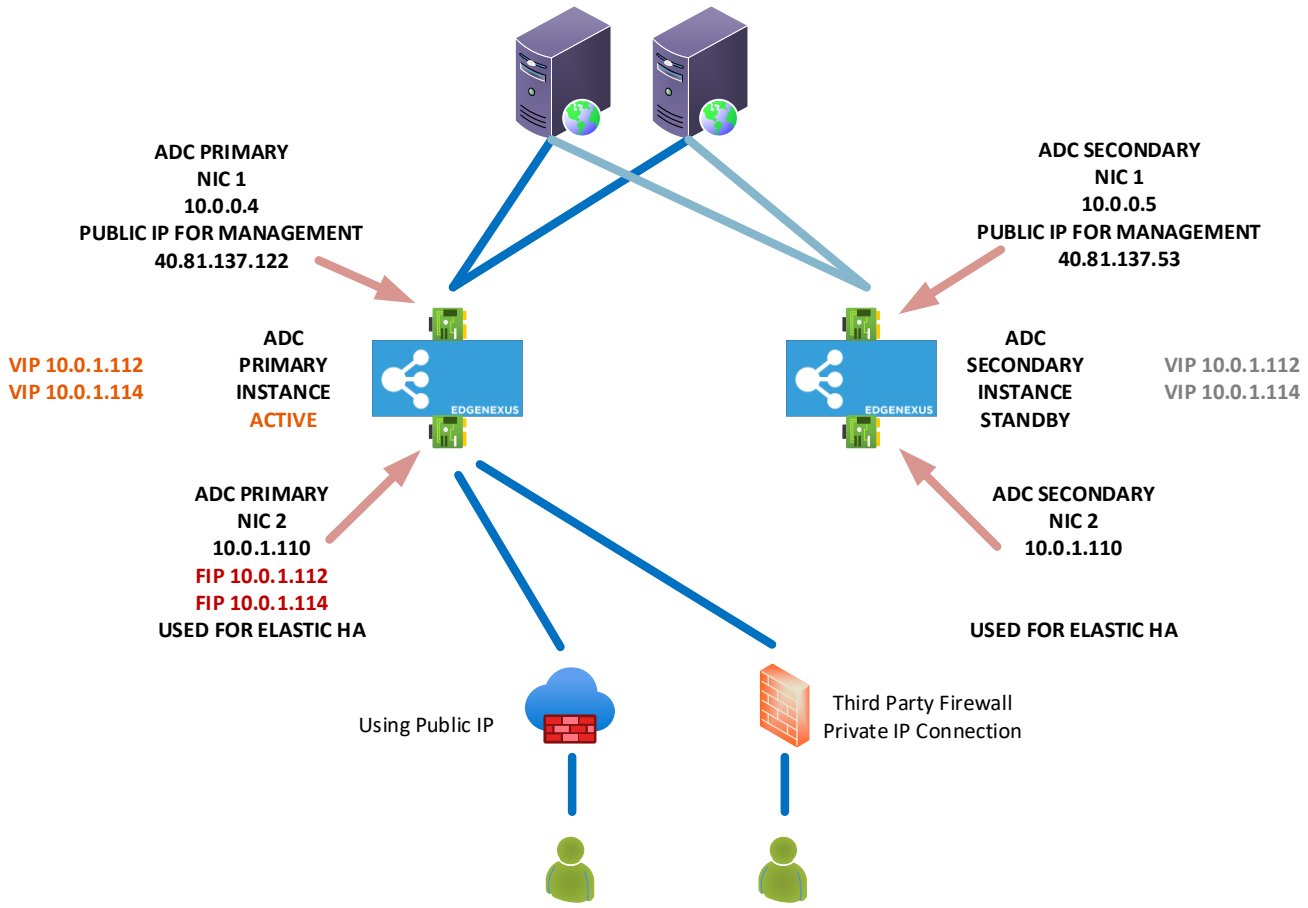
1. You must have TWO Edgenexus ADCs configured and running within the Cloud region.
2. The VIP/VS configurations, except for the IP address of the Monitoring Service should be replicated.
3. The ADCs must be configured as stand-alone devices.

© 2024 Edgenexus Limited

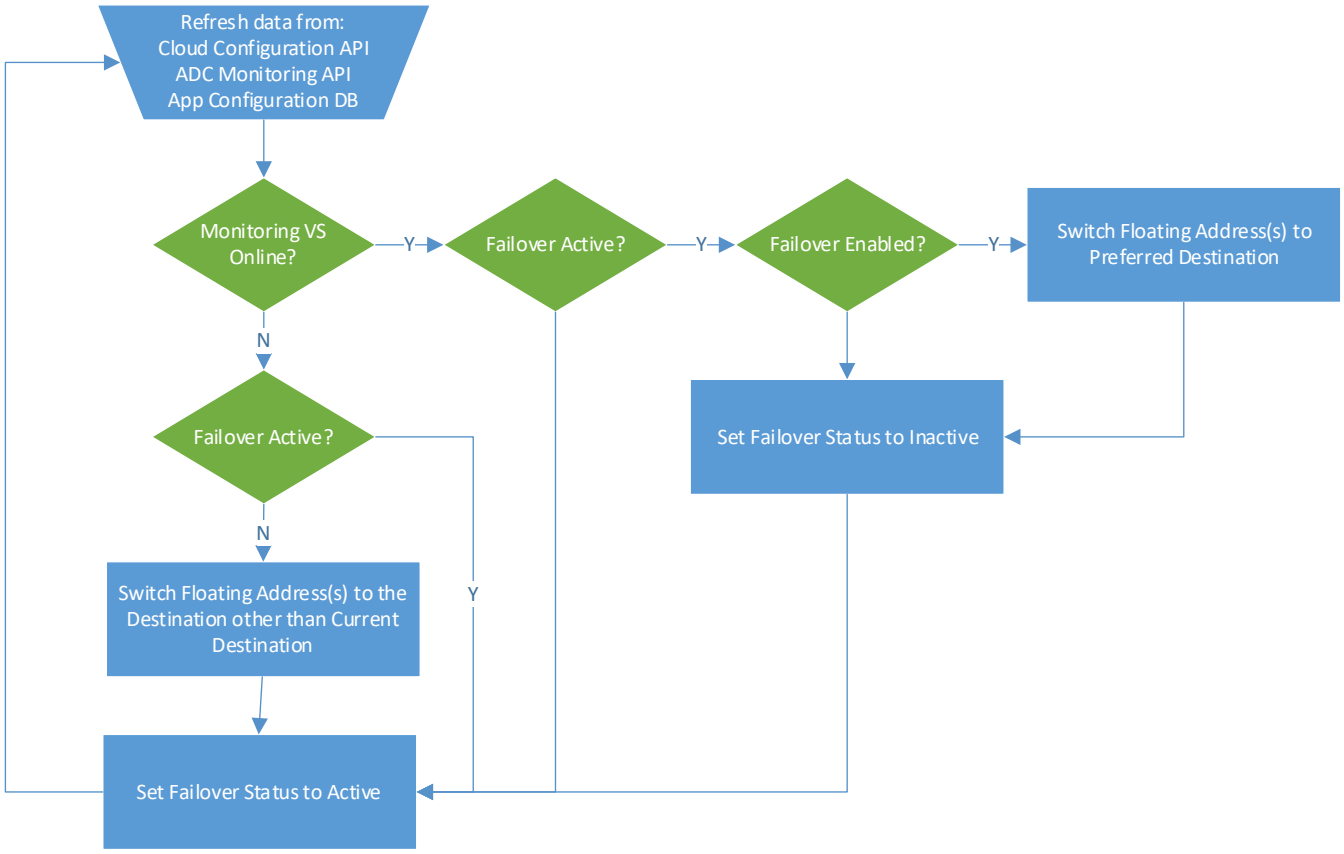
4. You require TWO network interfaces. Let's call them NIC-1 (eth0) and NIC-2 (eth1).
5. NIC-1 on each ADC must have a Cloud Public IP and is used to handle ADC management. If you are accessing it from an internal Cloud resource for security purposes, then you do not need to have the Public IP and can use the Private IP for management access.
6. Associate the floating IP with NIC-2 on ADC 1.
   The floating IP can be a Public IP linked to NIC-2, or several Private IP addresses also linked to NIC-2, or both – you will need to define HACC Services for each floating IP.
   The HA Cloud Connector App uses this and will switch this automatically to NIC-2 on ADC2 when required.

Architecture

Below is our sample architecture.



Understanding the Logic Flow



© 2024 Edgenexus Limited

Microsoft Azure

© 2024 Edgenexus Limited

Important - Using Tags

We strongly advise that you define each element you configure, with a TAG or name.

This makes it easier to select the right elements when configuring the HA Cloud Connector, and the lack of tags not only makes it more difficult, but also may lead to incorrect operation of the product leading to increased support.

For example, we have named our VMs JS-HACC-VM1-UKS-Z1. This allows us to easily see that JS has created a HACC VM number 1, in the UK South region's Zone 1.

Similarly, we also name our NICs. For example, HACC-VM1-NIC2.

© 2024 Edgenexus Limited

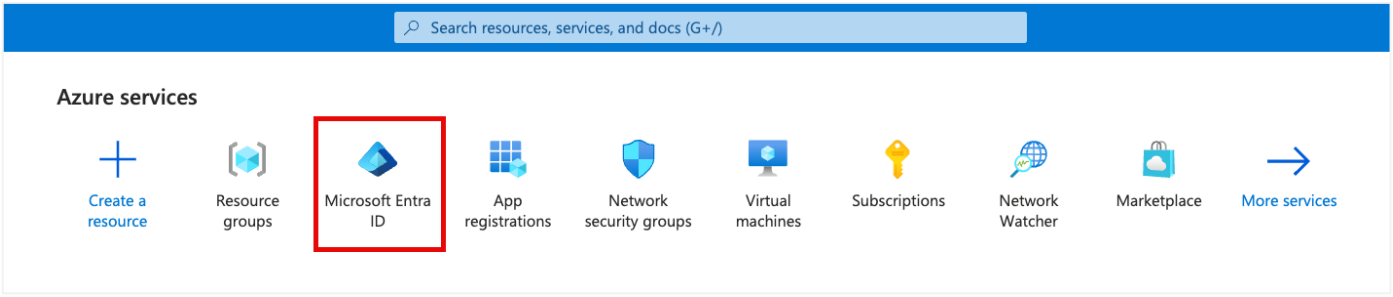
Preparing Azure for HACC

To create the Azure environment for use with HA Cloud Connector, you will need to follow the stages below.

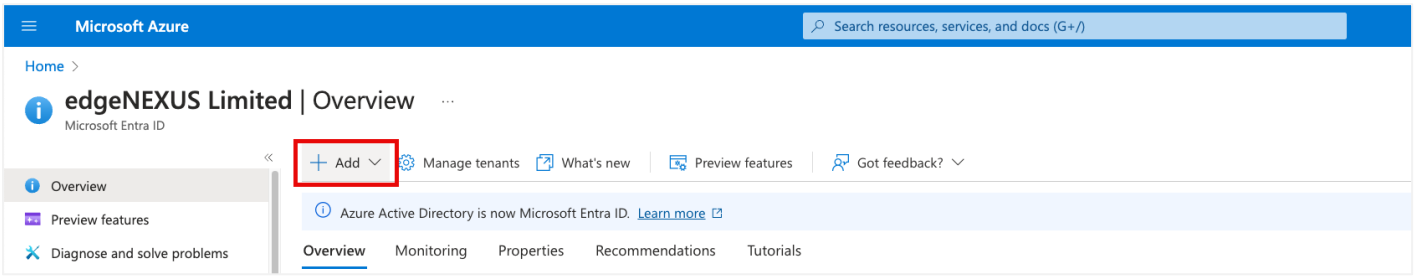
Creating the App registration

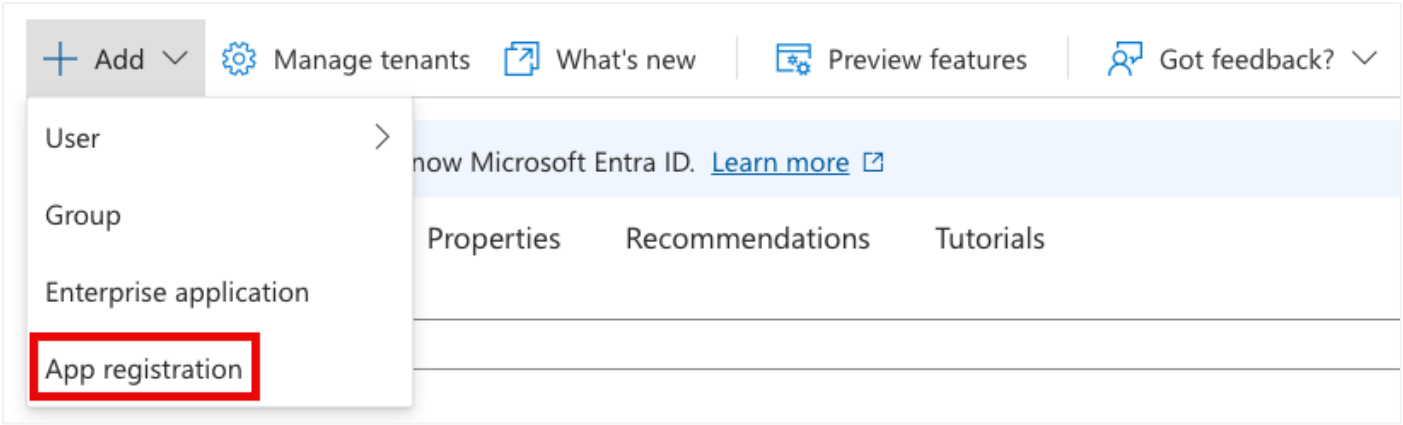
In order to use an App to communicate with Azure's API, you are required to first register it. This process is called App Registration.

- Log into the Azure portal.
- Navigate to Microsoft Entra ID. You can find this by typing Entra ID into the search field at the top, or clicking the icon if it is already visible.

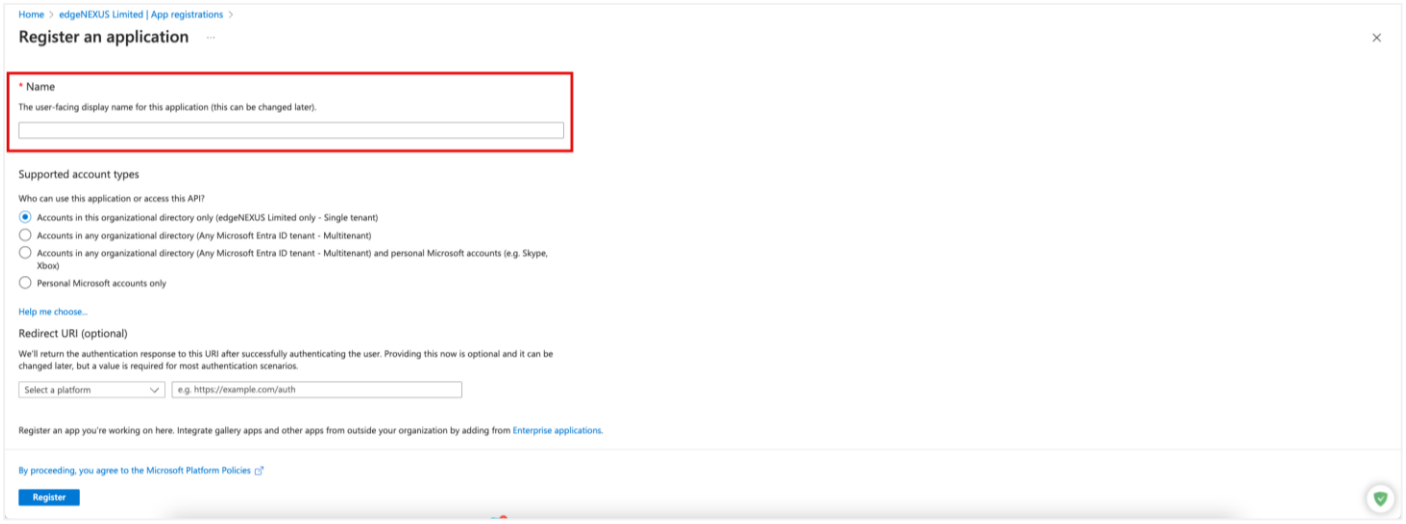


On the next screen (shown below) you need to click the small arrow next to the Add button (highlighted), and choose App registration.



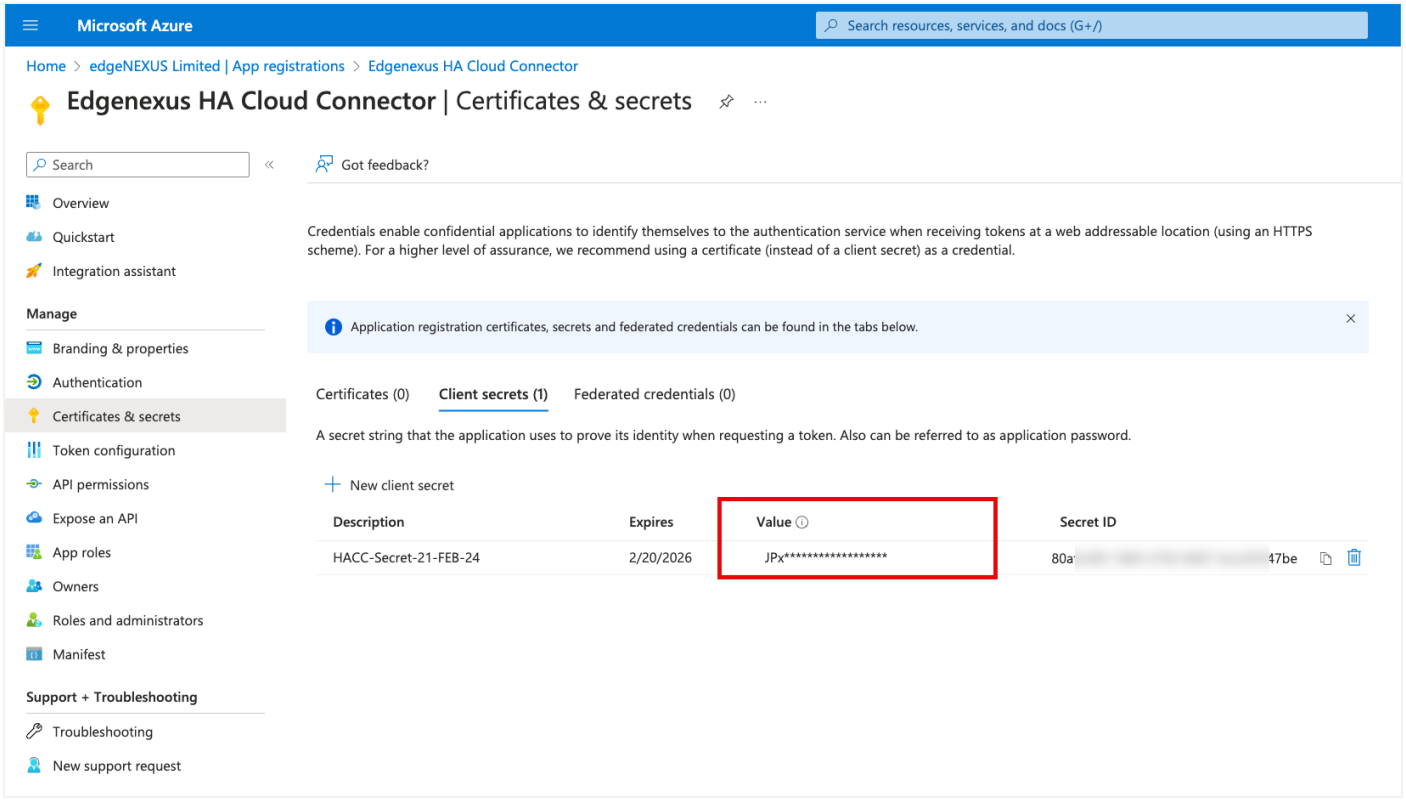


The following screen will display a form that is very easy to fill in.



Provide a name for the application and click Register. We have used the AppName of Edgenexus HA Cloud Connector, but you can use anything that suits you.

On the next screen, you will see the Certificates & Secrets for the Application.



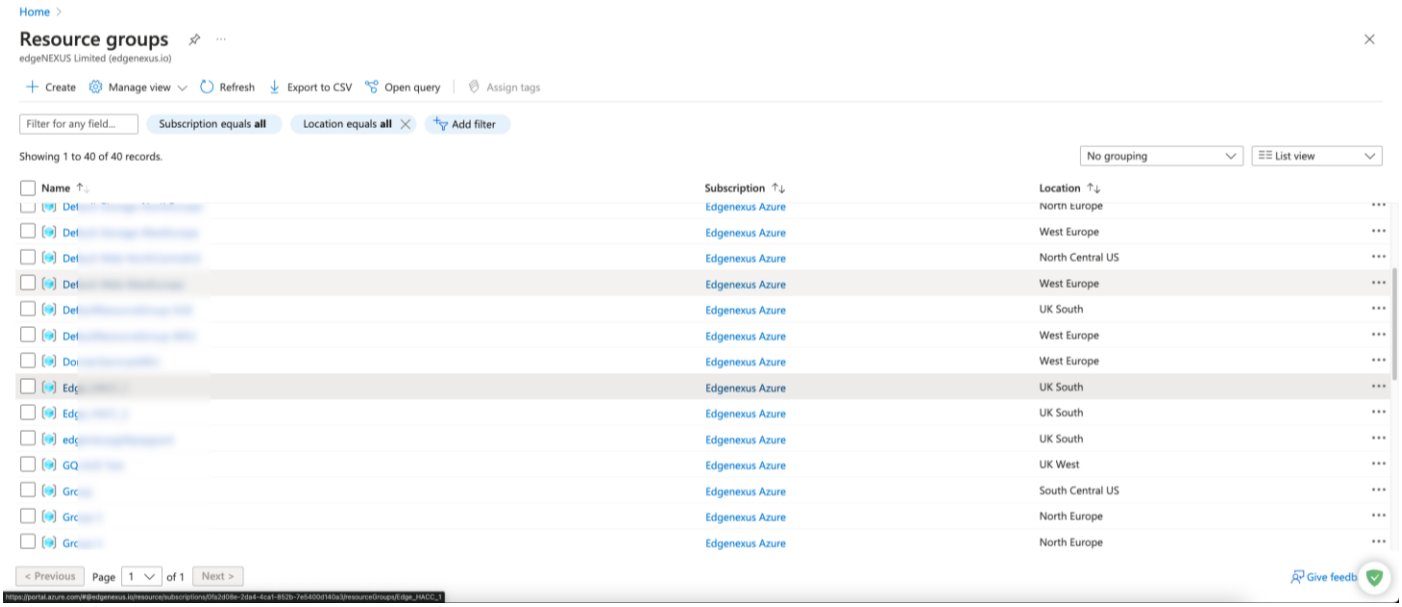
NOTE: It is very important that you make a note of the content in the VALUE field. This is also referred to as the Client Secret and is required within the HACC application.

This concludes the App Registration section.

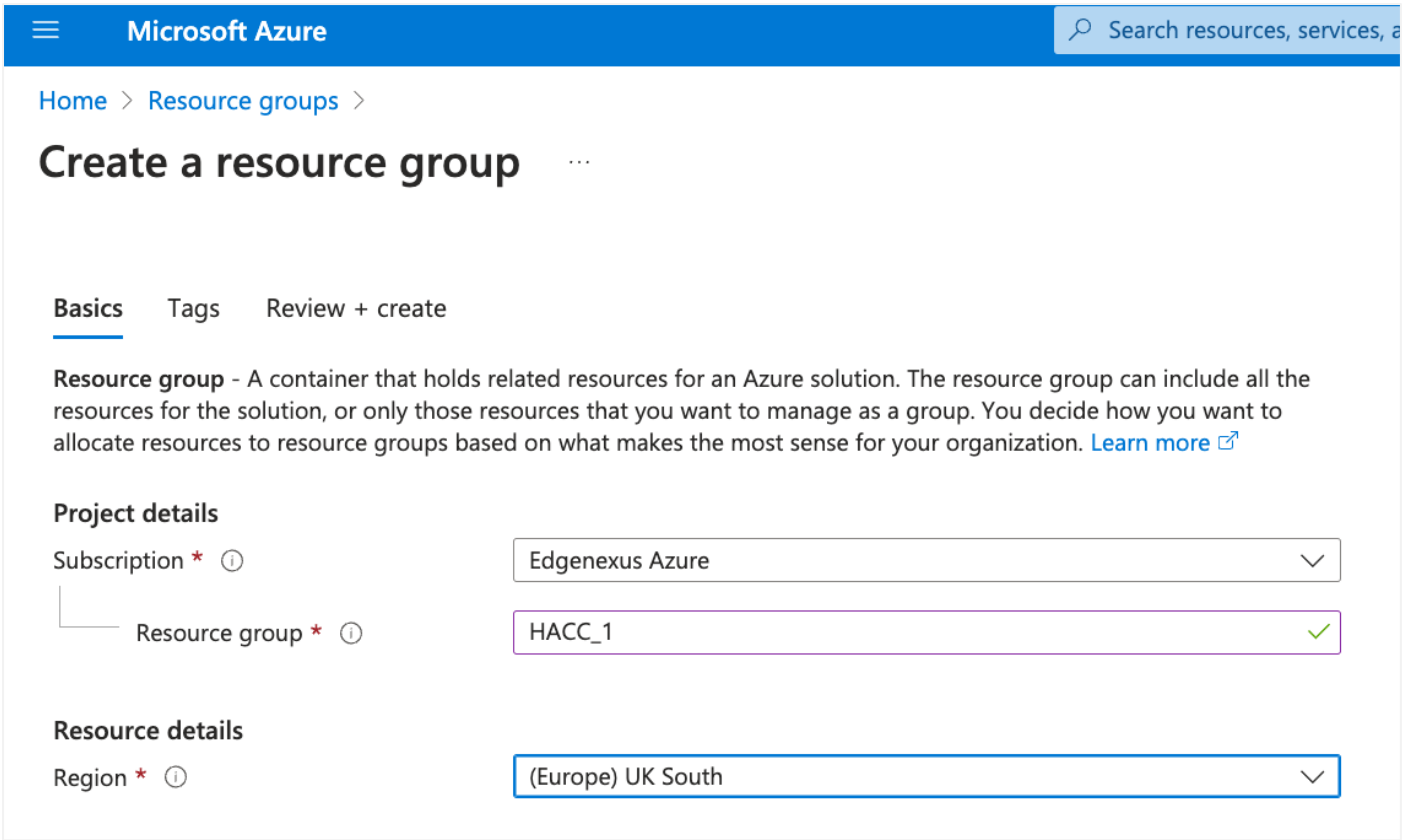
Creating a Resource Group

We advise you to create two Resource Groups for holding the two ADCs and their respective assets. In our case, we have created two Resource Groups called HACC_1 and HACC_2.

To create a Resource Group, type resource group in the search bar. This will show you the icon for the Resource Group section. Click this and go to the Resource Group section.



Click Create located at the top left.



Fill in the details and create the Resource Group. Do this for both groups.

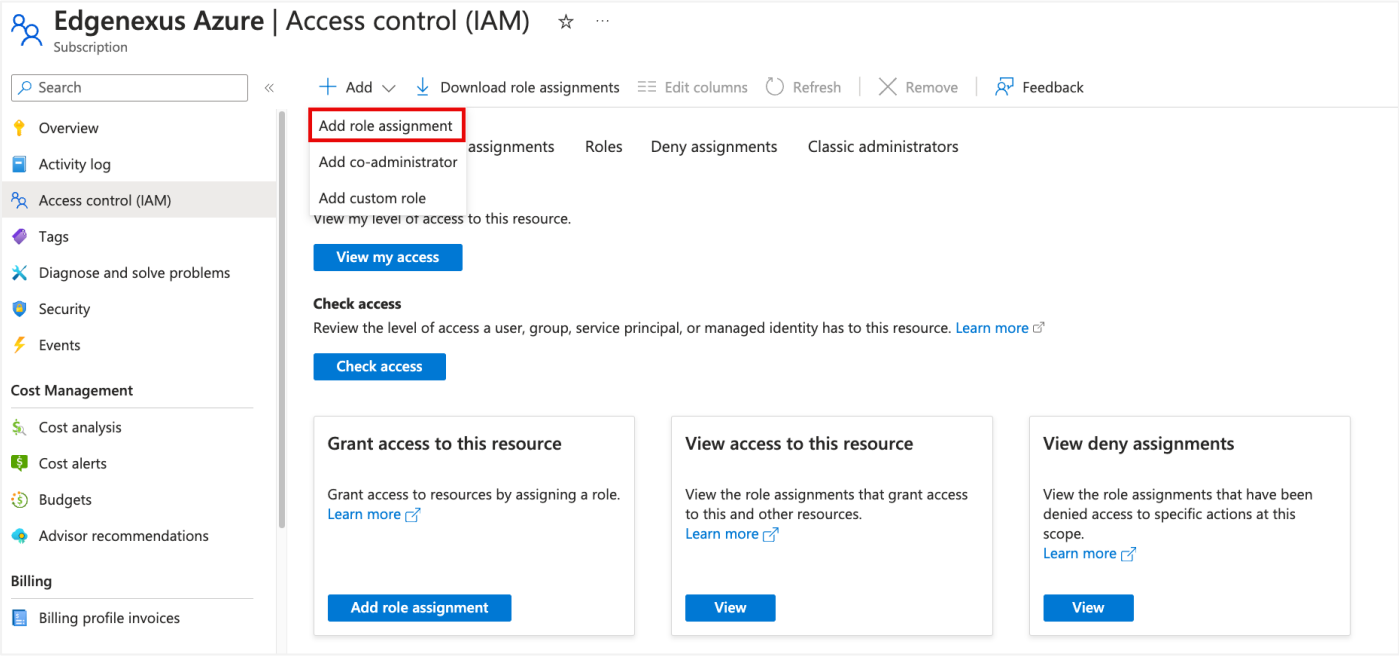
Access Control (IAM) and Roles

The next stage is to set the IAM roles in order for the HACC app to communicate and control aspects of the Azure infrastructure.

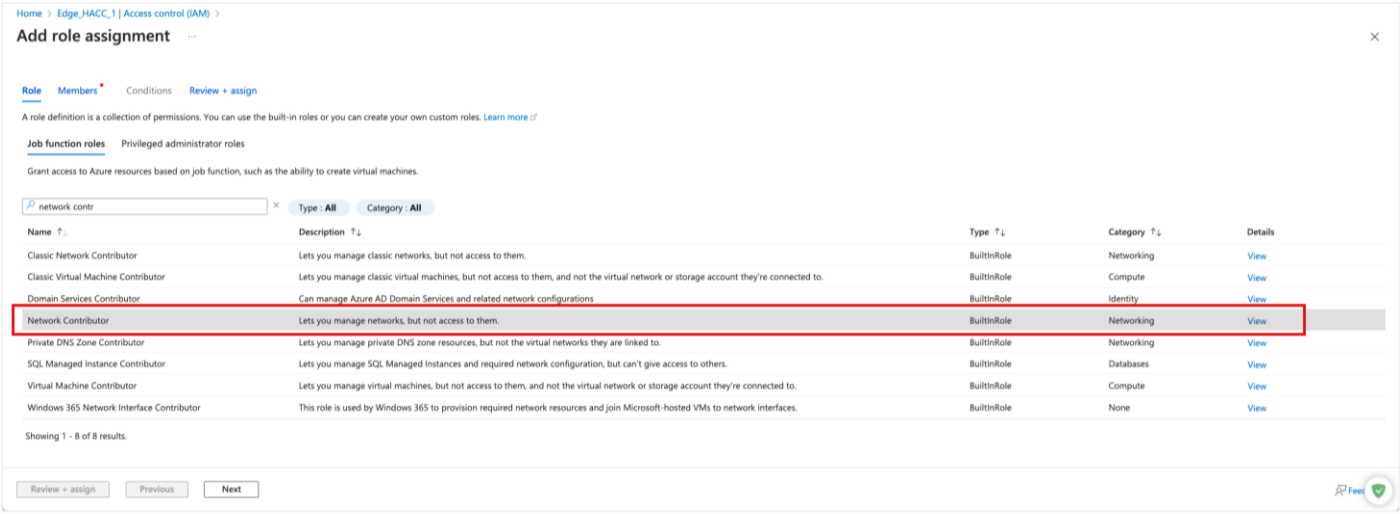
To do this you need to first access the Subscriptions. We will be creating roles called:

- Network Contributor and
- Virtual Machine Contributor.

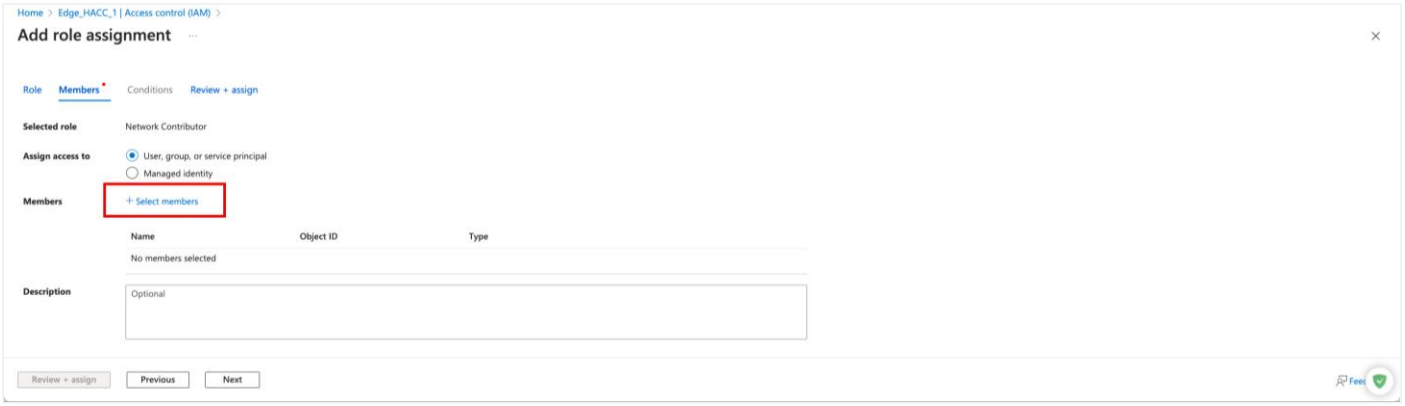
Within the Subscription page, click on the Access Control (IAM) link in the left panel.



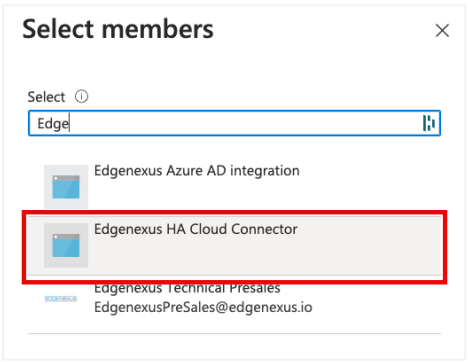
Now click Add Role Assignment as shown above. The screen you will see is one like below. Type Network Contributor in the search box and select the Network Contributor option as shown below.



Now click the +Select Members link as seen below, and then click Next.



You will now see the box shown below on the right side. Select the application you registered. In our case it looks like the image below.



Now repeat the steps above to add the Virtual Machine Contributor role.

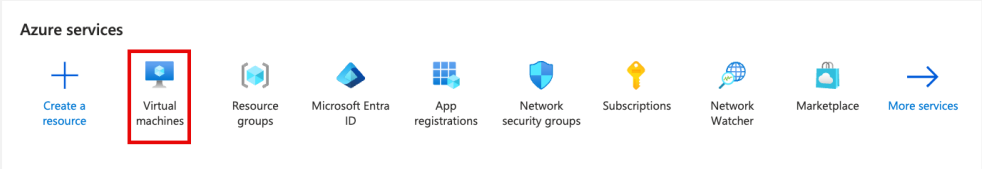
When done, go to the Home page of your portal to proceed to the next steps.

© 2024 Edgenexus Limited

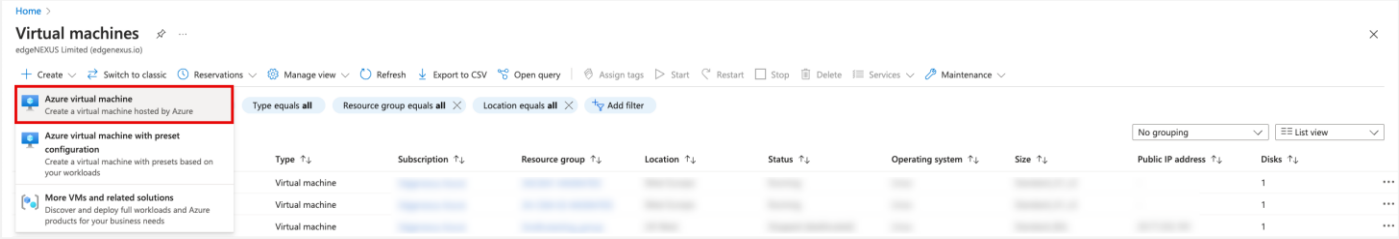
Creating the ADC Virtual Machines

Now comes the main step – creating the EdgeADC virtual machines. We will be creating two virtual machines, both in the same region and zone.

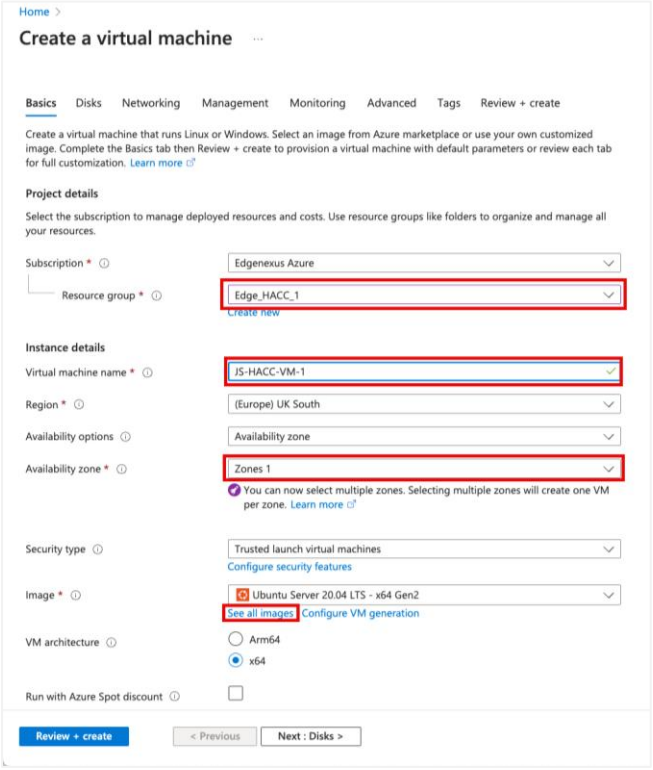
In the main portal, click the Virtual machines icon.



In the next screen click on the Create menu and select Azure virtual machine from the dropdown.



You will now come to the pages where you set up your virtual machine for the EdgeADC.

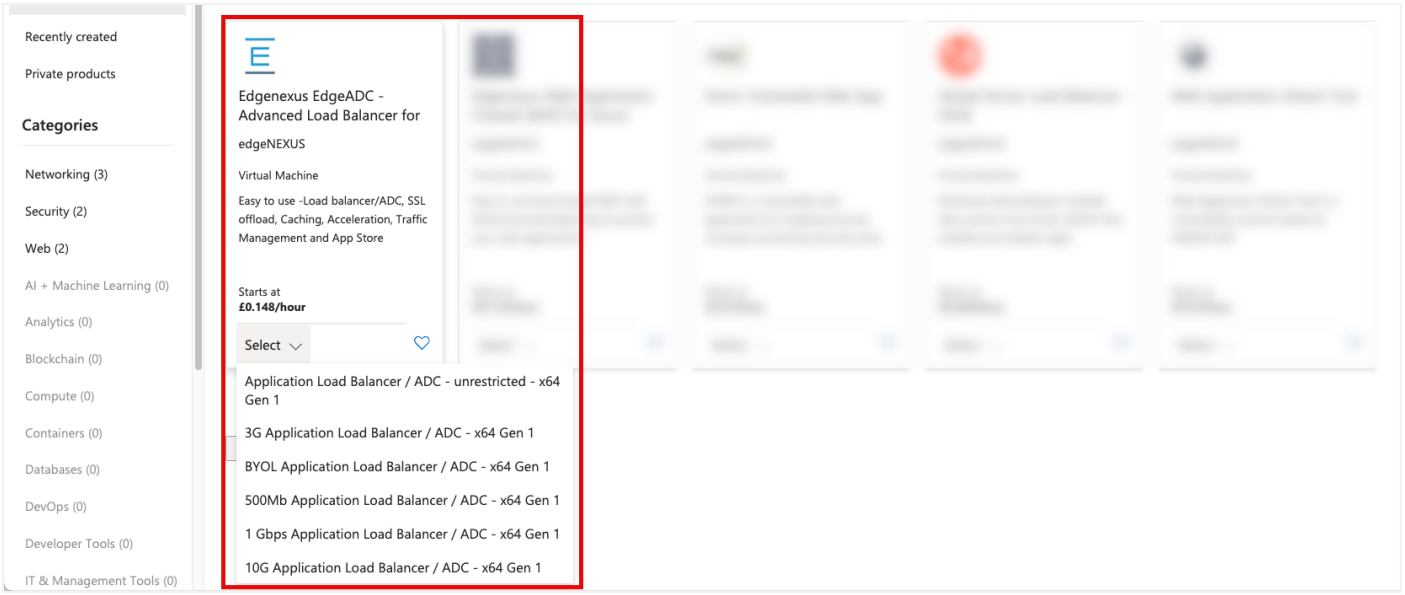


This is the first page of the VM setup. In the image above, we have indicated the fields that need to be selected.

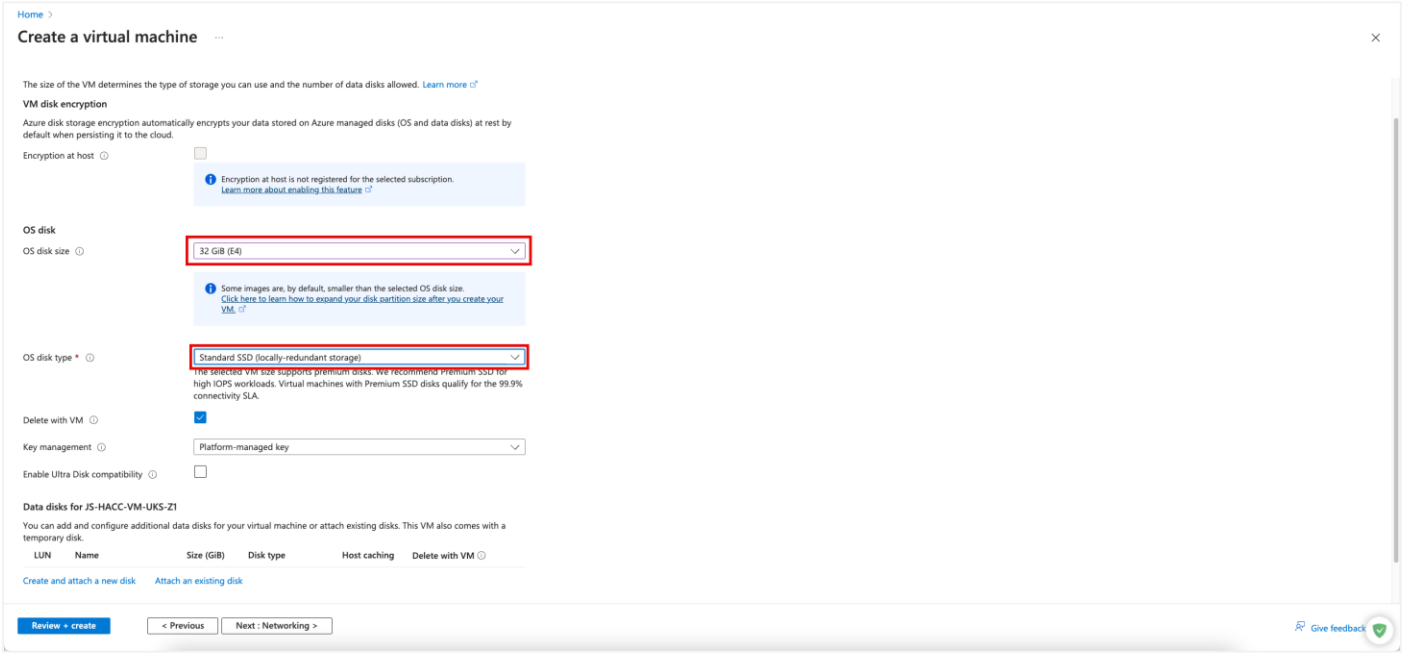
- Select the Resource Group for ADC1 VM
- Give it a VM name of your choice
- Choose the Region and Zone – Need to be in the same region and zone

© 2024 Edgenexus Limited

- Choose Standard as the Security type
- Click the See all images link.
- When the Marketplace comes up, search for Edgenexus

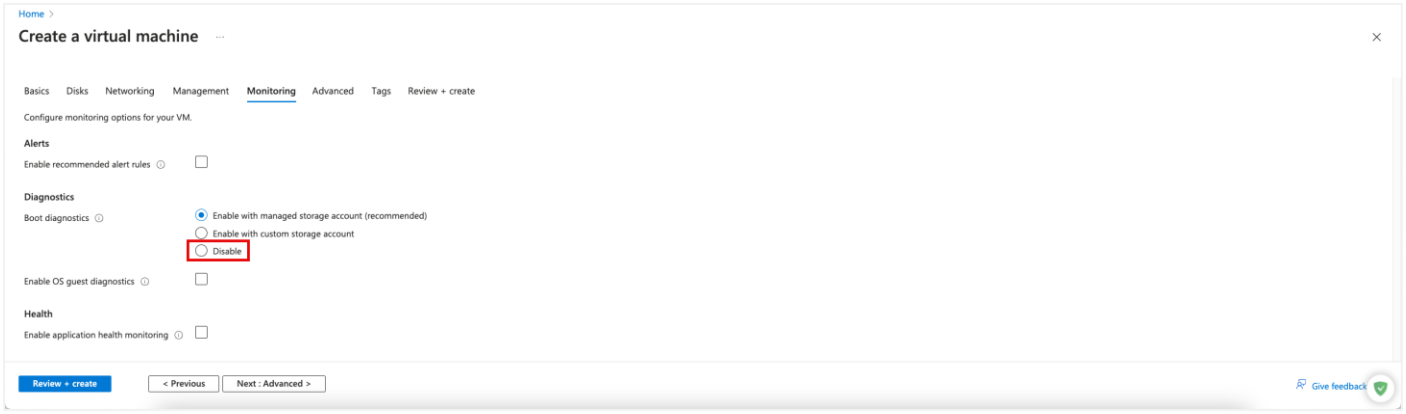


- Choose the type of EdgeADC licensing model you need.
  If you are installing your own license purchased from Edgenexus, choose the BYOL option, otherwise choose one of the times/sized license options.
- You will then be taken back to the virtual machine creation page.
- Click the Next: Disks button.
- On the Disks page we have highlighted the options need changing.



- Choose the Disk size (we recommend 40GB but the nearest is 64GB).
- Choose the OS Disk Type as Standard SSD.
- Click Next: Networking.
- You can skip the Management page unless you wish to use it. Click Next: Monitoring.
- Unless you wish to use Monitoring, we suggest clicking the Disable option.

© 2024 Edgenexus Limited



- Click on the Review & create button as we have no need to do anything on the Advanced page.

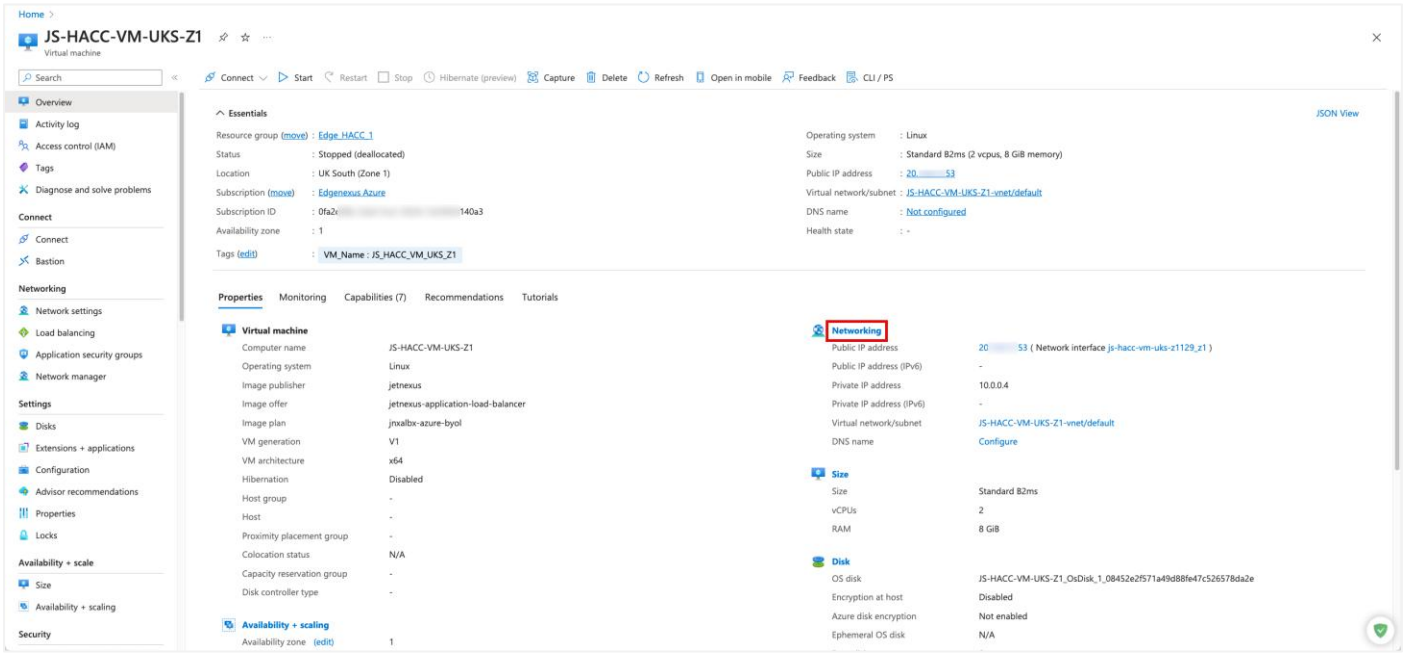
The ADC VM will now be created.

NOTE: These steps will need to be repeated to create the second ADC VM.

Configuring the Virtual Machine

When you have your Virtual machine created, make sure it is in the Off status, as we cannot make the changes we need if it is running.

Networking

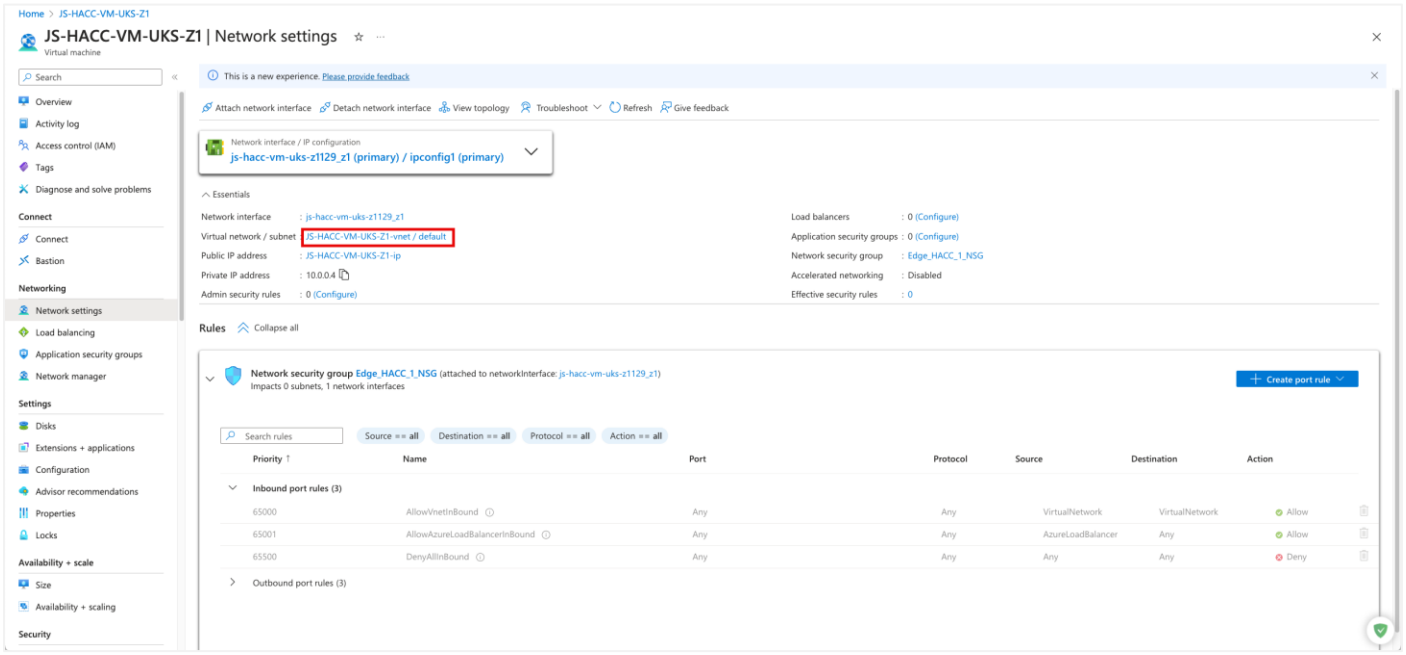


The first stage of configuring the VM for use with HACC is Networking. The first thing we will do is to add a new subnet and an additional network interface (NIC).

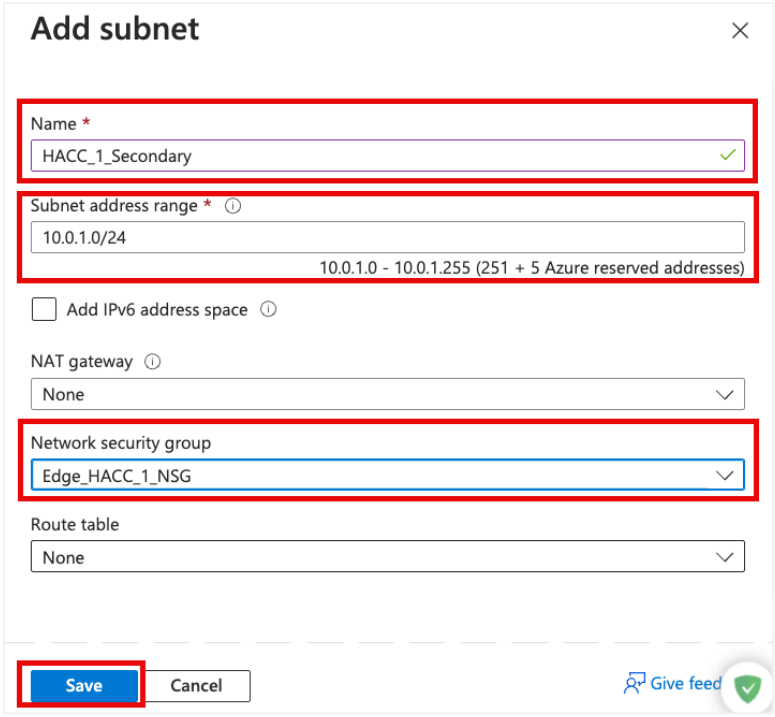
- Click the Networking link highlighted above.
- This will take us to the Networking page.

© 2024 Edgenexus Limited

Adding a Subnet



- Click on the Virtual Network/subnet link highlighted.
- You will now be presented with the Add Subnet page shown below.

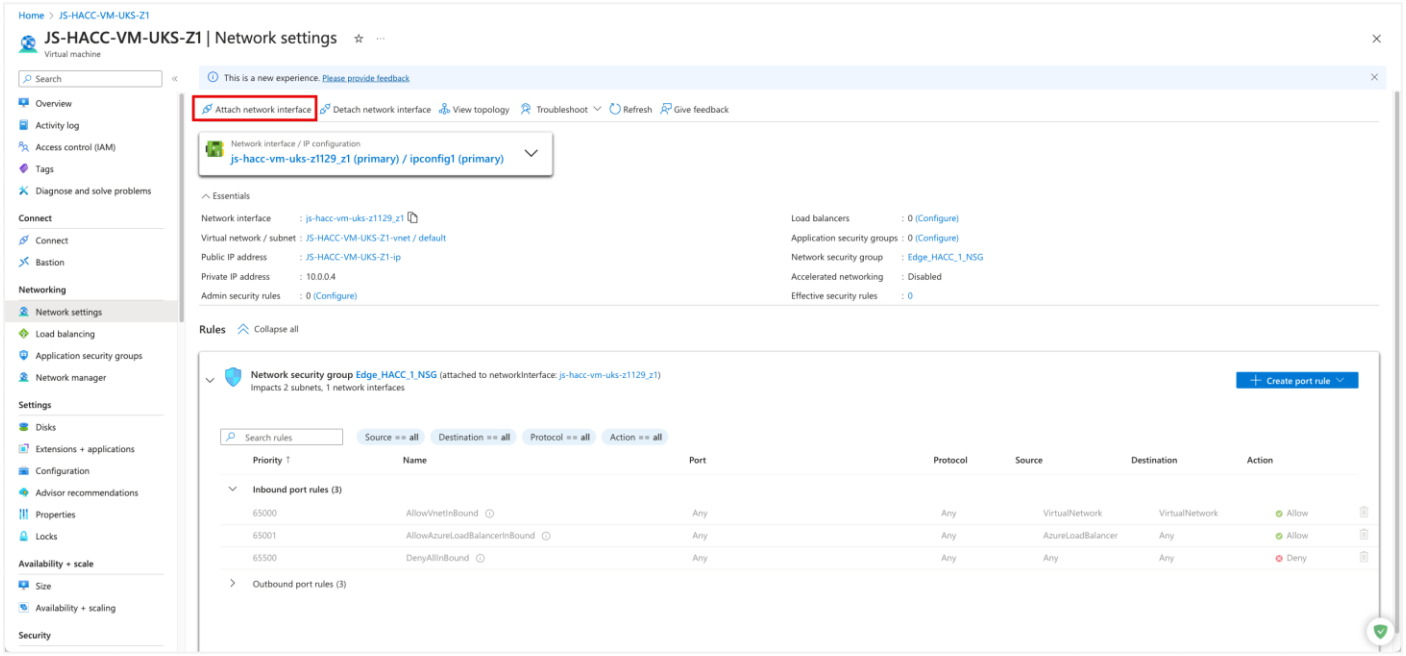


- Fill out the field shown in the image above.
- Remember the subnet should be a new one, and it is this subnet that we will use for the floating IP and user access to the applications.
- Choose the appropriate Network security Group.
- Once done click Save.

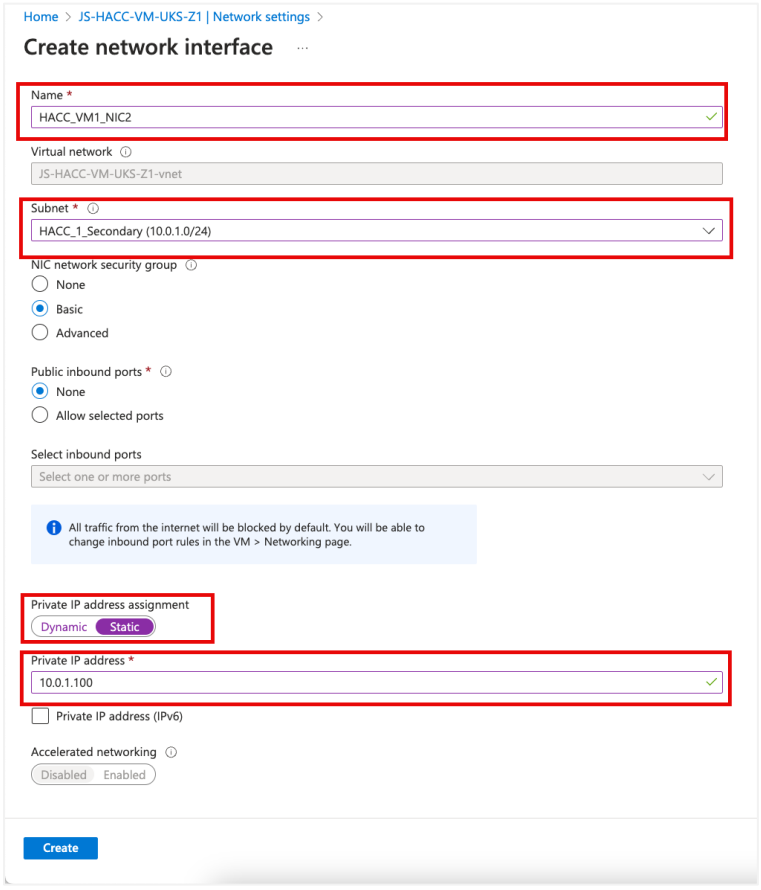
© 2024 Edgenexus Limited

Attach a Network Interface to new Subnet

The next thing to do is to attach a new NIC to the new subnet.



- Click the Attach Network Interface link indicated in the image above.
- Click the Create and attach network interface link below the drop down that appears.
- You will see the following page



- Add a name for the NIC you are creating.
- Choose the new Subnet from the dropdown menu.
- Make it a Static Private IP address.
- Add an IP address making sure it is in the new subnet.
- Click Create.
- This is the BASE IP Address for this network interface.

Creating IP Addresses for Accessing

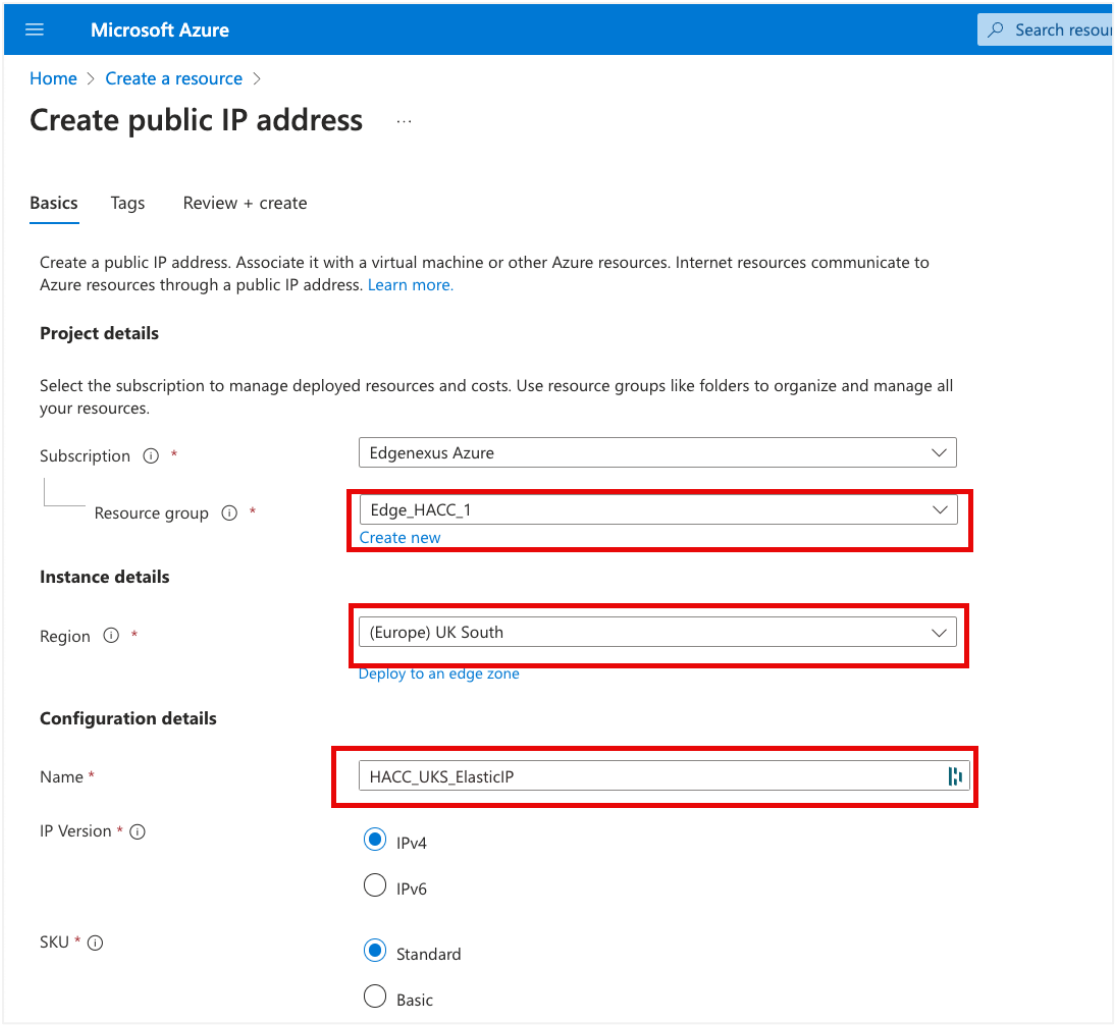
Here, there are two choices.

a. Create a Public IP Address and attach it to the network interface you just created.
or
b. Create multiple Private IP addresses so your other internal resources may connect to, and access the services being provided by the ADC.

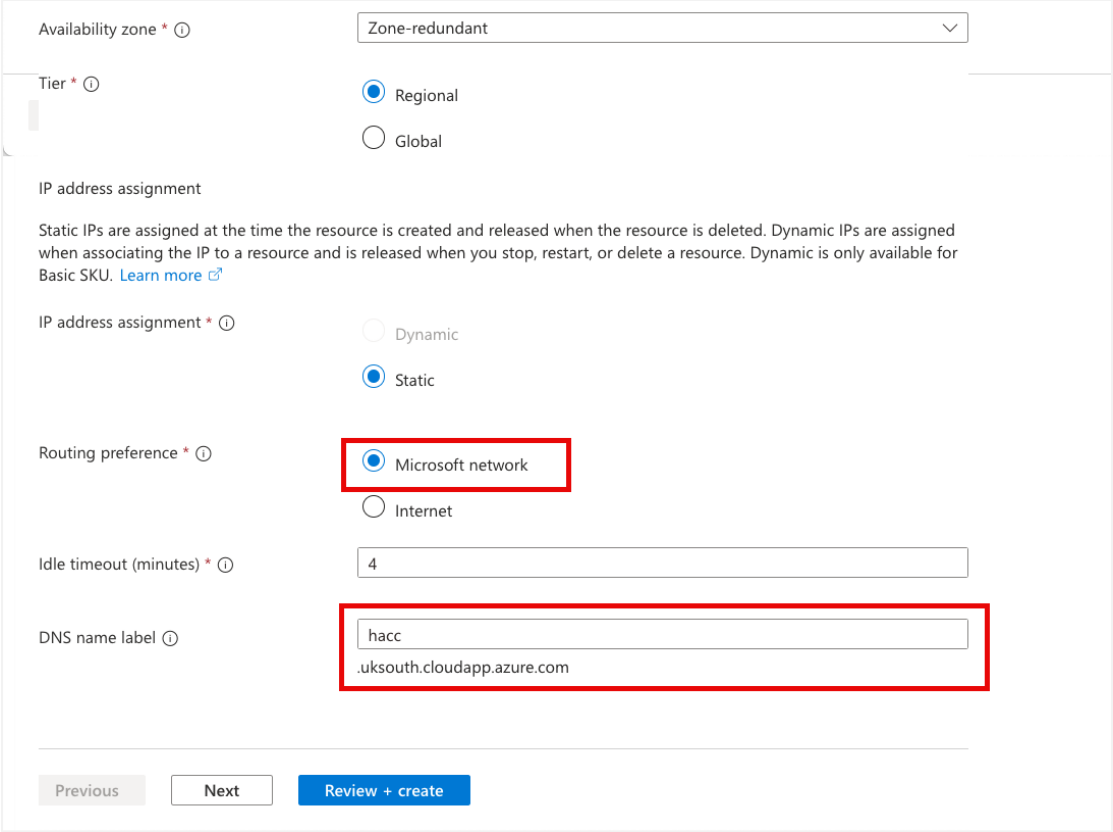
Creating a Public IP Address

The Public IP address that we will create is going to serve as the floating IP Address we will use for high availability.

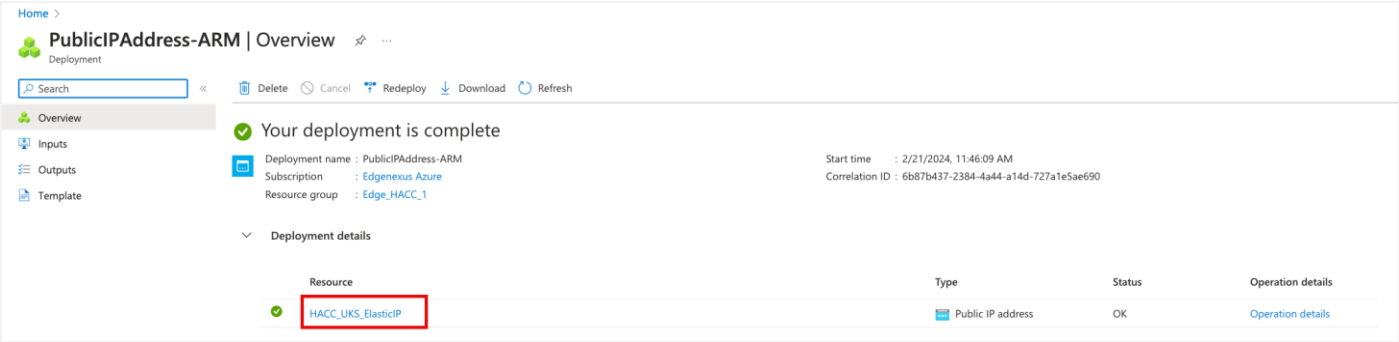
- From the home page of the portal click Create a Resource.
- Select Networking in the left panel or type Public IP Addresses in the search.
- You will see the following page (split into two halves for clarity).



- Choose the Resource Group. We have chosen the group that VM1 was created in.
- Choose the Region.
- Specify a name for this floating IP. Essential that this is be done properly so it is recognizable in the HACC application configuration.
- Choose IP V4 for the IP Version, and Standard for the SKU.



- Leave the Availability Zone as redundant.
- Leave the Tier as Regional.
- Choose Static as the IP address assignment.
- Choose the Routing Preference as Microsoft Network.
- Provide an appropriate DNS name for the floating IP address. We have chosen HACC for convenience, but this may be something more relevant to your deployment.
- Click Review & Create.
- You will see the result looking like the following image.

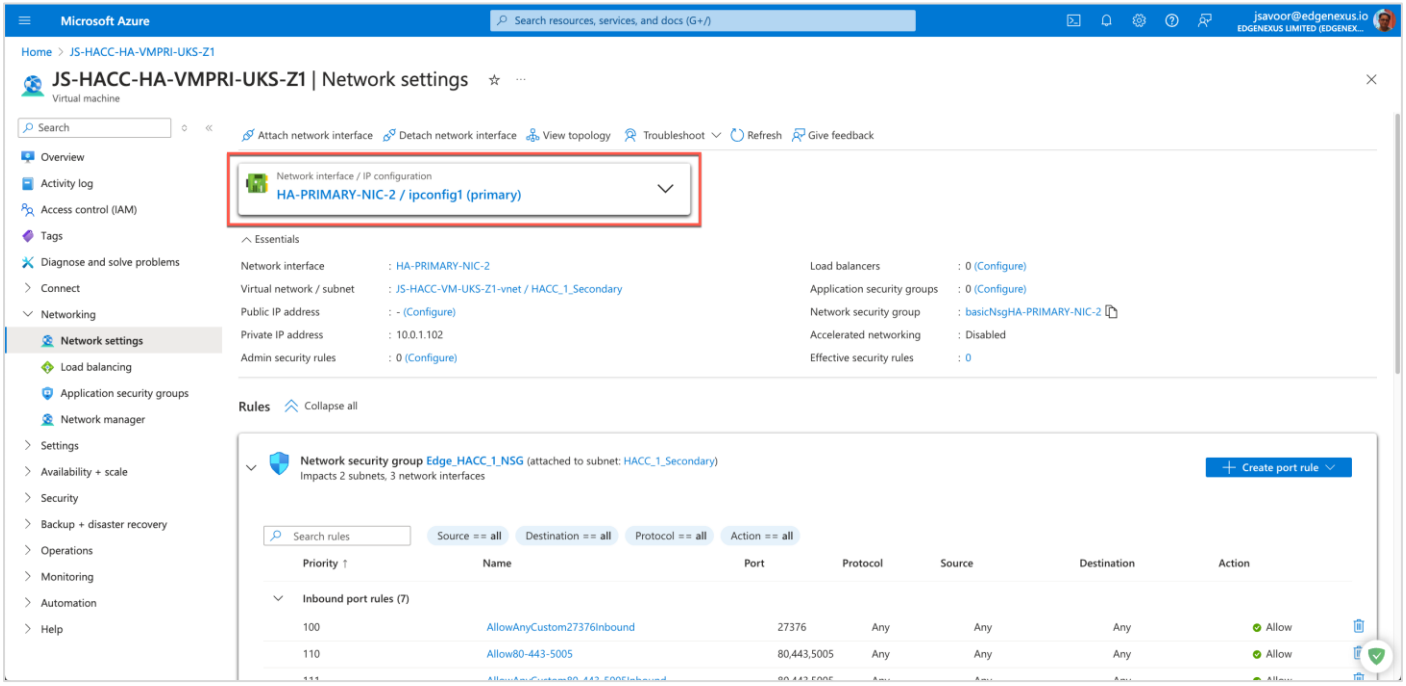


NOTE: You need to associate the Public IP with ADC1-NIC2 initiallty, after which the HACC app will handle this automatically.

Creating Private IP Addresses

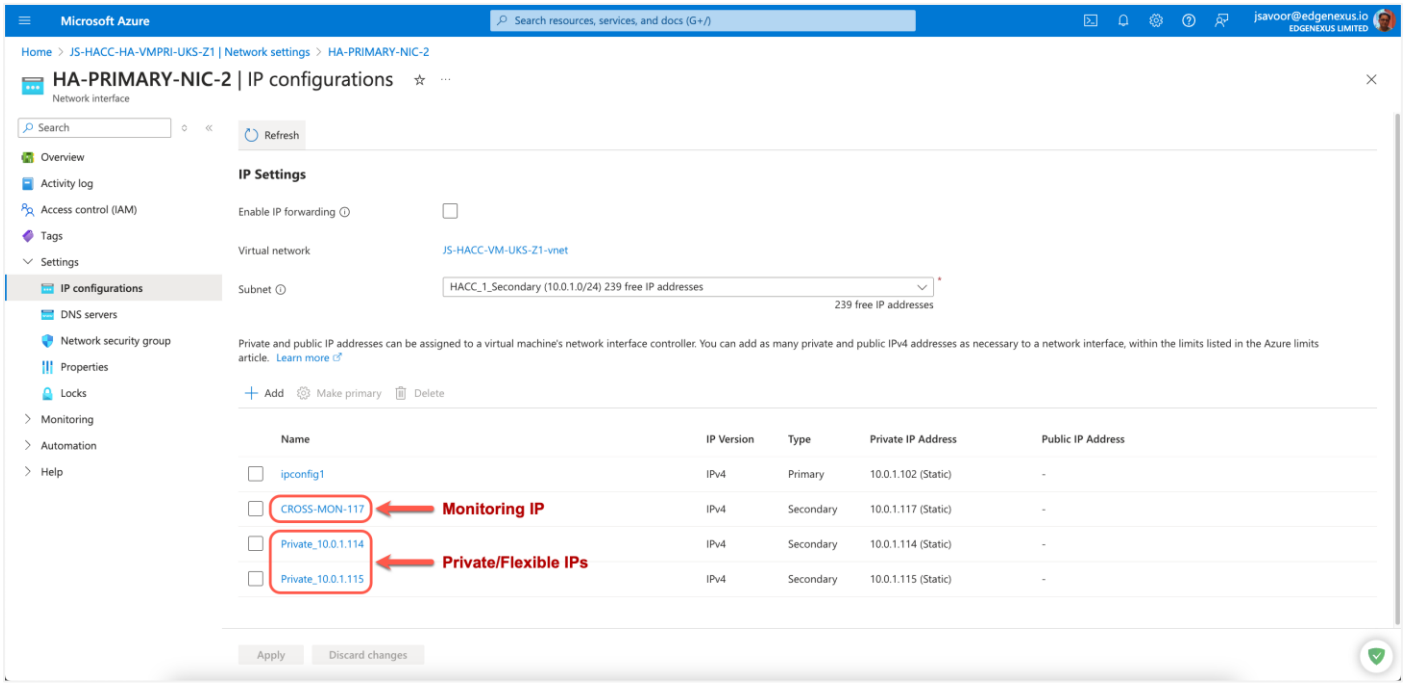
The creation of Private IP addresses is relatively simple.

- We will begin with what we term the Primary ADC.
- In the VM settings, navigate to Networking > Network Settings.
- You will then need to use the Network Interface / IP Configuration menu and select NIC-2. This has been highlighted in the image below.

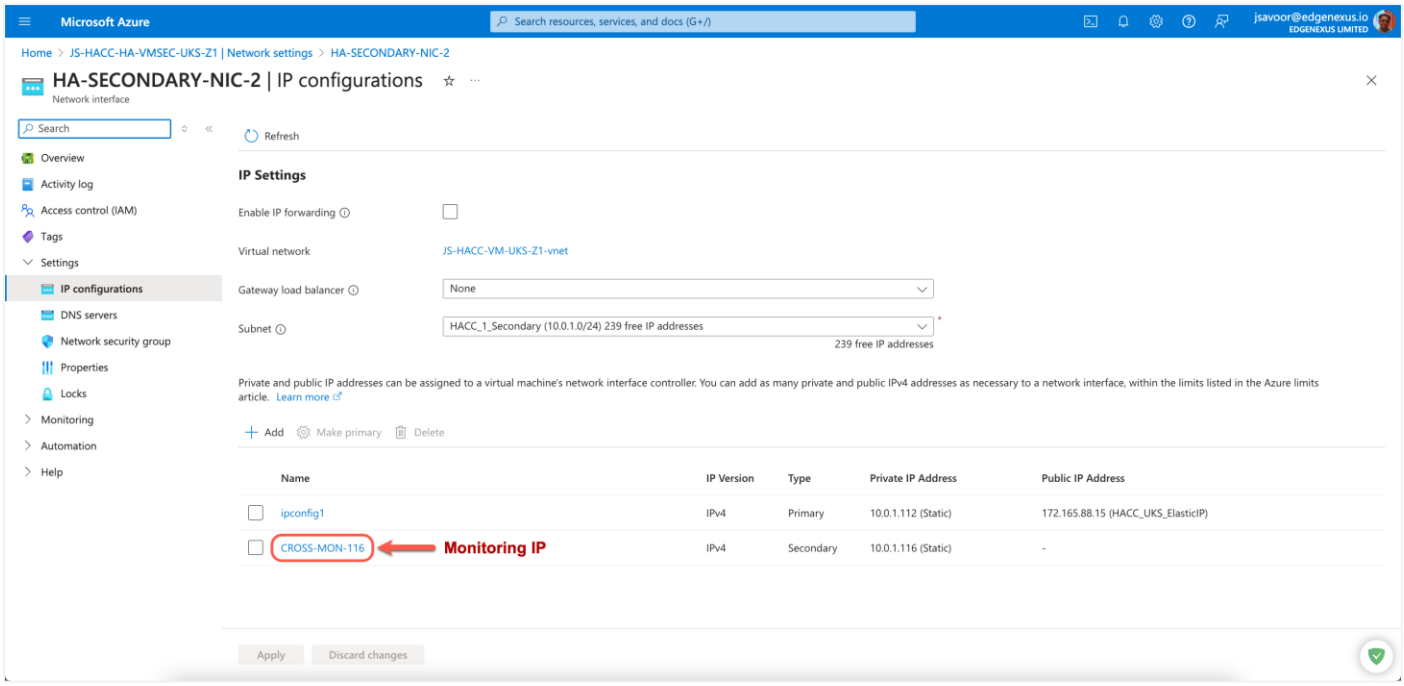


- The option you can see in the image above, *HA-PRIMARY-NIC-2/ipconfig1 (primary)*, is a link. The naming is of course the one we used, and your name for NIC 2 may be different.
- Click the link to proceed and add your IP addresses.
- The next page you will see is IP Configurations.
- Click the Add button highlighted to add an IP address.

© 2024 Edgenexus Limited



- In the Name field highlighted in the right-hand section above, fill in an appropriate name for the Private IP address you are going to create. An example may be something like, Private_10.0.1.114. This name is used as a tag name within the HACC and makes it easier to recognize.
- The next step is to choose the Allocation type. Select Static.
- Then provide a Private IP address within the subnet for the network interface you are going to add it to.
- Click Add.
- The new Private IP will be added to the network interface.
- You can repeat this process for any additional IP addresses you wish to add.
- Perform the steps shown on the Secondary ADC virtual machine. The result should look like this:



Important Information Required to Deploy HACC

We are almost there now and will be ready to deploy the HA Cloud Connector in Azure.

Checklist

1. App Registration
2. Resource Group
3. Access Control IAM Roles
4. Two Virtual Machines with EdgeADC OS Image created
5. Additional subnet added
6. Network Interface attached to new subnet on each ADC
7. Public IP address and any Private IP addresses created

Information required to proceed

a. Azure Subscription ID
b. Directory Tenant ID (found on the HACC App page)
c. Application Client ID (found on the HACC App page)
d. App Secret (Noted down earlier when creating the Application Registration)

NOTE: If you failed to store the App Secret, you will need to delete the App Registration and redo it.

© 2024 Edgenexus Limited

Configuring the EdgeADC

There are several items that need to be configured on the ADC for the HACC app to work.

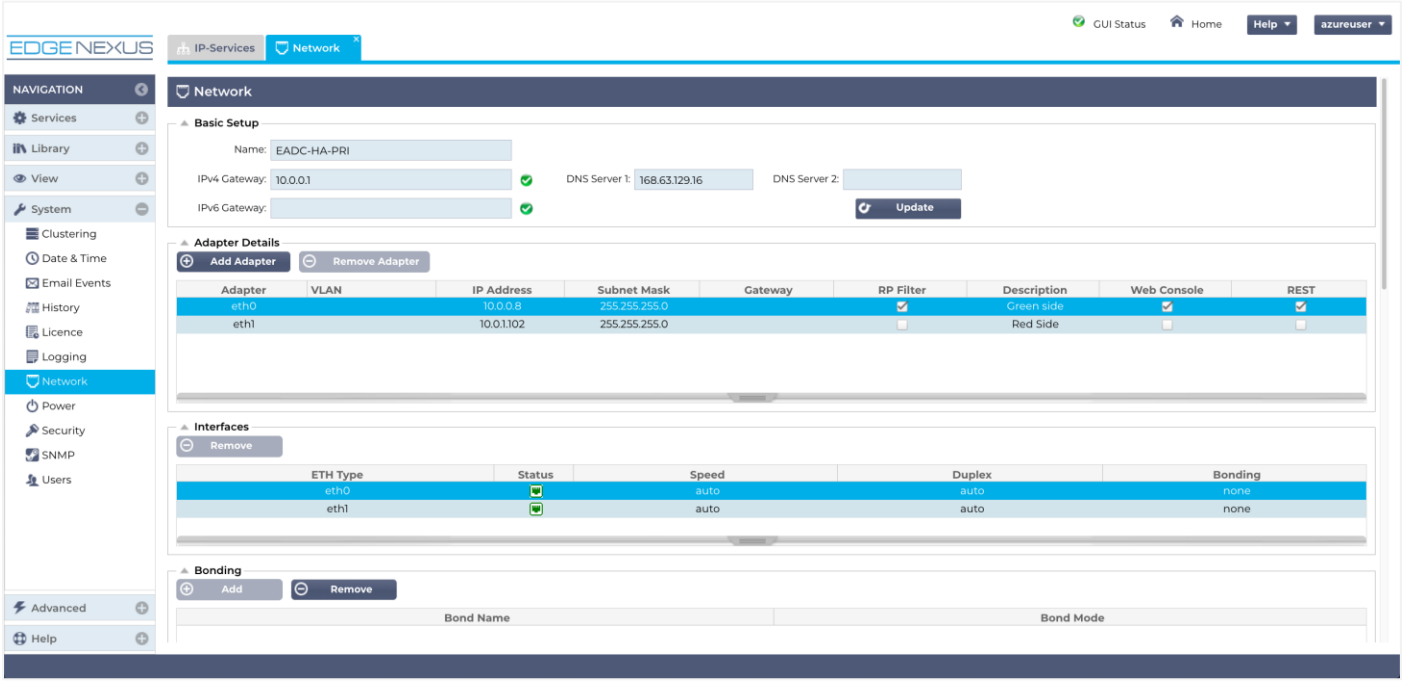
We will also refer to the ADCs and network interfaces as follows:

- Active ADC will be referred to as Preferred
- Passive ADC will be referred to as Secondary
- The eth0 network interface is also referred to as NIC-1
- The eth1 network interface is also referred to as NIC-2

Configuring the ADC networking

By default, when the ADC is created it is populated and configured to use the eth0 network interface. We will need to add the new network interface we created earlier and prepare a virtual service for use.

Below you will find the Networking page of EdgeADC.

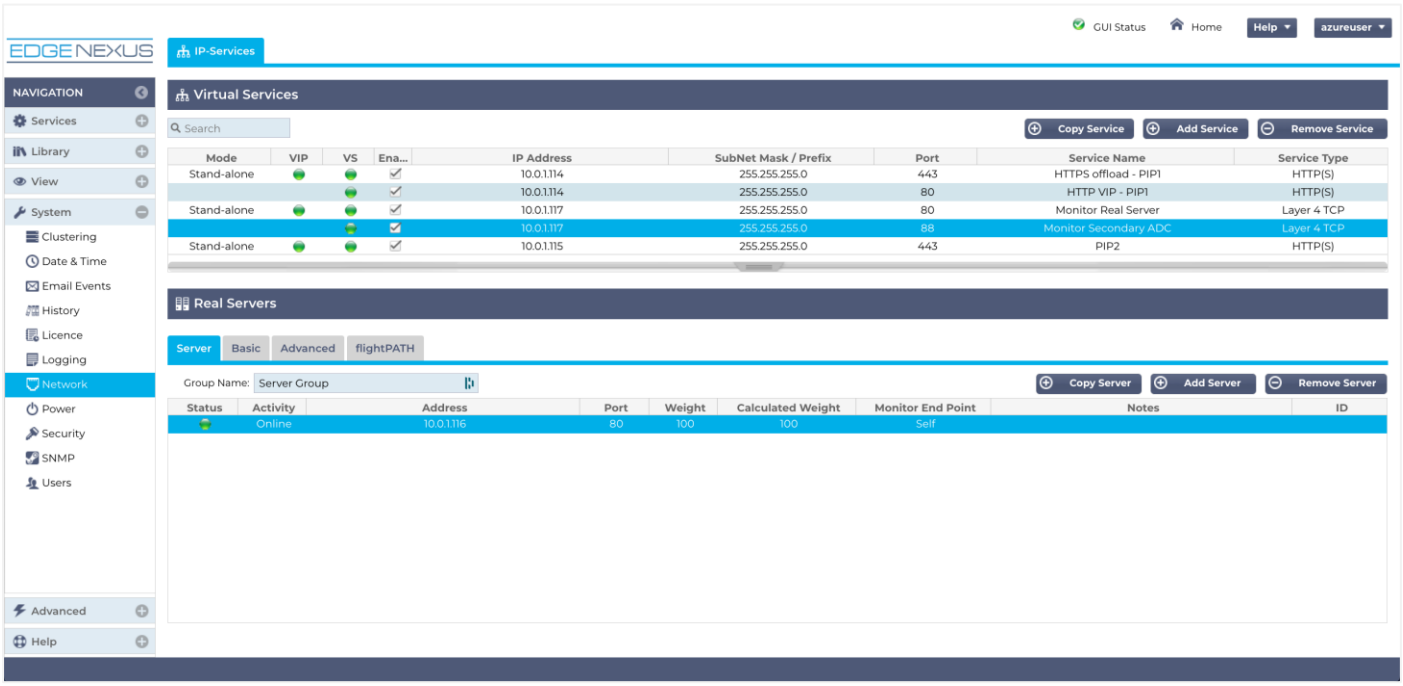


We have already added eth1 as you can see, but the process is extremely simple.

- Click Add Adapter
- You will see a new line placed under eth0 in the Adapter Details section.
- By default, the new line will state eth0, but you can use the dropdown menu to select eth1.
- Once you have done that, you can provide the IP Address that was provided by Azure for this network interface. In our case, its 10.0.1.100.
- Provide the appropriate netmask and the Gateway IP address. The Gateway IP address normally ends with 1 and as you can see it's 10.0.1.1 in our example.
- Click Update and the networking layer of the ADC will restart.
- You will also need to enter the specific Gateway IP address for eth0.
- If the Ethernet interface connects successfully, you will see its icon show Green in the Interfaces section.

© 2024 Edgenexus Limited

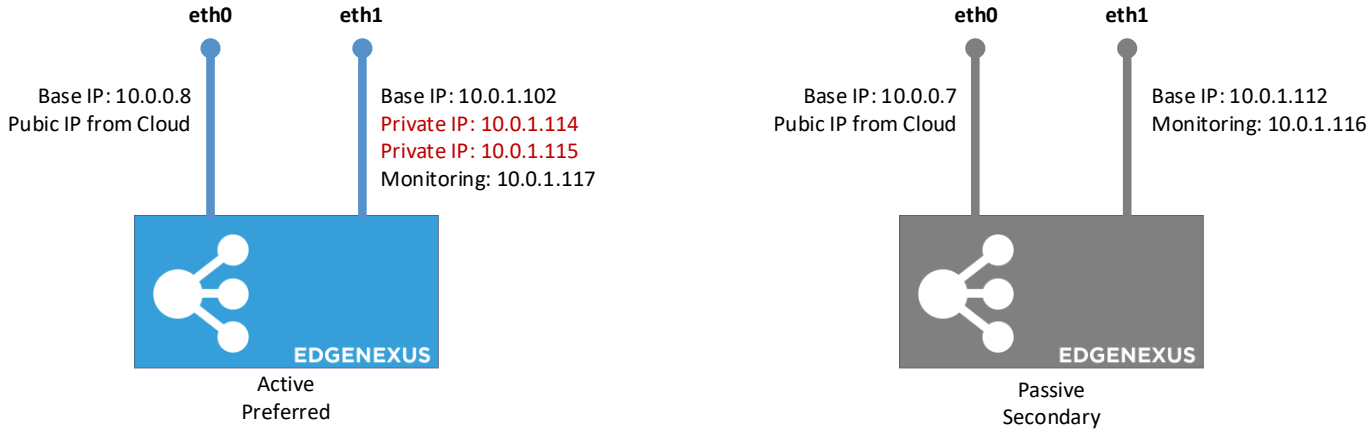
Defining the Virtual Services



In the above image, you can see an example of our configuration. Let's explain what we have there.

Remember, our network interfaces were defined as follows:

- Preferred ADC
  - The eth0 interface uses IP subnet 10.0.0.0/24 and is allocated IP address 10.0.0.8
  - The eth1 interface uses IP subnet 10.0.1.0/24 and is allocated IP address 10.0.1.102
  - Three private IP addresses linked to eth1: 10.0.1.114 and 10.0.1.115
  - One private IP address for the monitoring VIP on eth1: 10.0.1.117
- Secondary ADC
  - The eth0 interface uses IP subnet 10.0.0.0/24 and is allocated IP address 10.0.0.7
  - The eth1 interface uses IP subnet 10.0.1.0/24 and is allocated IP address 10.0.1.112
  - One private IP address for the monitoring VIP on eth1: 10.0.1.116



The two IP addresses you see in red are the ones that will be the flexible IP addresses. As can be seen, they are currently attached to eth1 on ADC Preferred.

© 2024 Edgenexus Limited

Creating the Monitoring VIPs

There are two methods of creating monitoring VIPs, and these have been highlighted below.

You will need to make sure that you have ONE additional private IP address created and allocated to NIC-2 on each ADC. Provide it an appropriate name such as Monitoring-VIP, as I will refer to it as such below.

Simple App Monitoring

Using this method, we will create a simple monitoring VIP that monitors the availability of a web service on the Real Server.

- In the Virtual services panel, click on Add Service
- Select the Private IP address (Monitoring-VIP) you created.
- Provide a valid netmask and port value.
- In the Description, state Preferred-ADC-MVIP
- Select the appropriate Service Type
- In the Real Servers section provide the IP address to your real server.
- Specify the port
- Click Update.

If all is ok, then you will see the indicators showing as Green.

Repeat this step on the Secondary ADC but name the VIP as Secondary-ADC-MVIP.

The names will help you identify it when creating the Service within the HACC App.

Cross ADC Monitoring

In this method, we will create a VIP that monitors where:

a. The Preferred monitors the reachability to the Secondary
   and
b. The Secondary monitors the reachability to the Preferred

The process is as follows:

- **On Preferred ADC (ADC-1)**
- Select the Private IP address (Monitoring-VIP) you created.
- Provide a valid netmask and port value.
- In the Description, state Monitoring-RS-ADC-1-VIP
- Select the appropriate Service Type
- Click Update
- In the Real Servers section provide the IP address to your real server.
- Specify the port
- Click Update.
- **On Secondary ADC (ADC-2)**
- Select the Private IP address (Monitoring-VIP) you created.
- Provide a valid netmask and port value.
- In the Description, state Monitoring-RS-ADC-2-VIP
- Select the appropriate Service Type
- Click Update
- In the Real Servers section provide the IP address to your real server.
- Specify the port
- Click Update.

© 2024 Edgenexus Limited

- **On Preferred ADC (ADC-1)**
- Highlight the click on the MONITORING-RS-ADC-1-VIP you created
- Click on the Copy Service button in the Virtual Services panel.
- This will make a copy of the VIP
- Click Update
- In the Real Servers section, change the IP address of the Real Server to the IP address of MONITORING-RS-ADC-2-VIP
- Click update
- **On Secondary ADC (ADC-2)**
- Highlight the click on the MONITORING-RS-ADC-2-VIP you created
- Click on the Copy Service button in the Virtual Services panel.
- This will make a copy of the VIP
- Click Update
- In the Real Servers section, change the IP address of the Real Server to the IP address of MONITORING-RS-ADC-1-VIP
- Click update

This effectively ensures that ADC-1 monitors ADC-2, and ADC-2 monitors ADC-1 thereby triggering a failover.

© 2024 Edgenexus Limited

Installing the HA Cloud Connector

Important

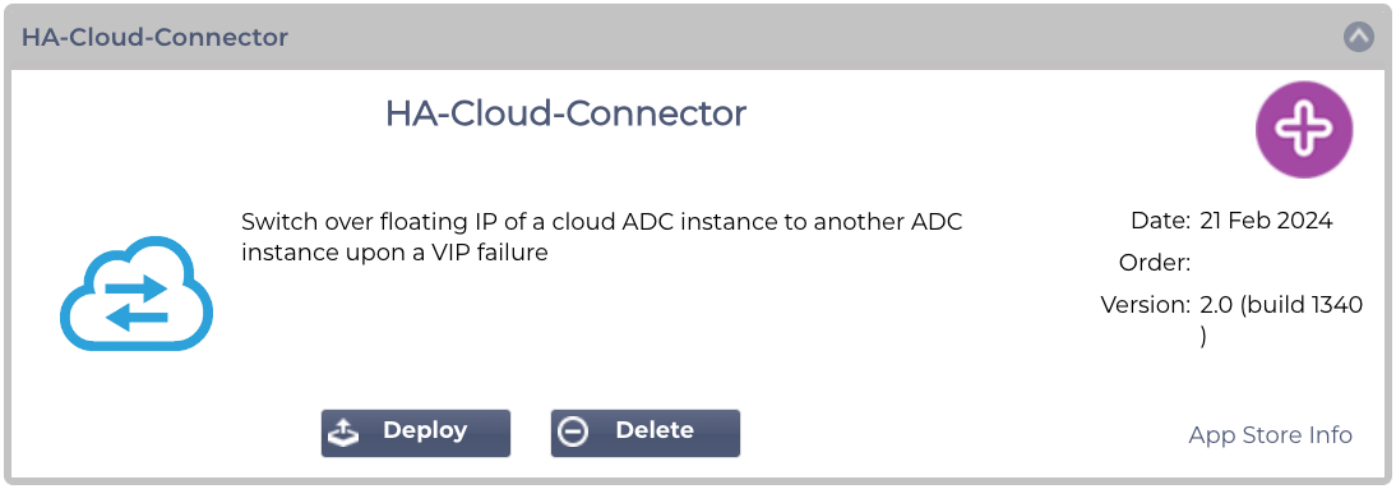
The HA Cloud Connector must be installed and on both ADCs you have in the selected region and zone(s). Each must be configured individually to talk to the Cloud Provider API to switch the floating IP when needed.

Both ADCs must have their cluster role set to Standalone.

Deploying the HA Cloud Connector

This process is very easy, as the HA Cloud Connector (HACC) App is pre-installed into the Cloud version of ADC. So, no need to download anything.

You will find the HACC App under Library > Apps. It looks like the image below.

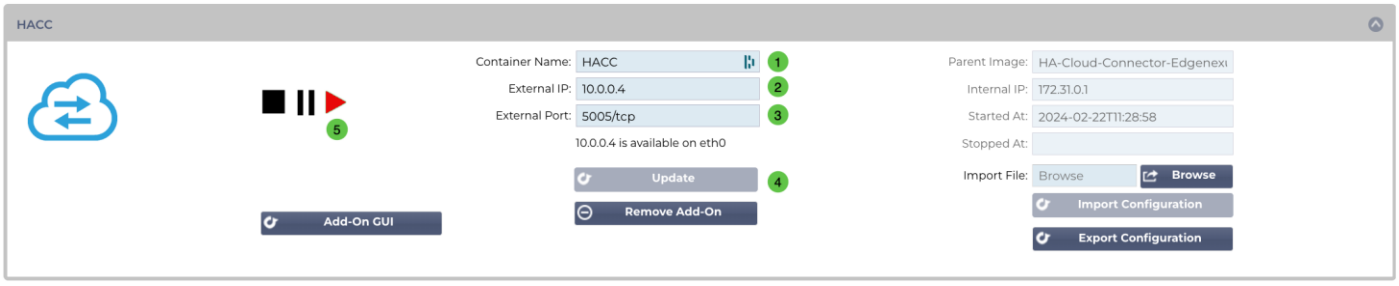


To be able to make the HACC App operational, Click the Deploy button.

Making the App Operational

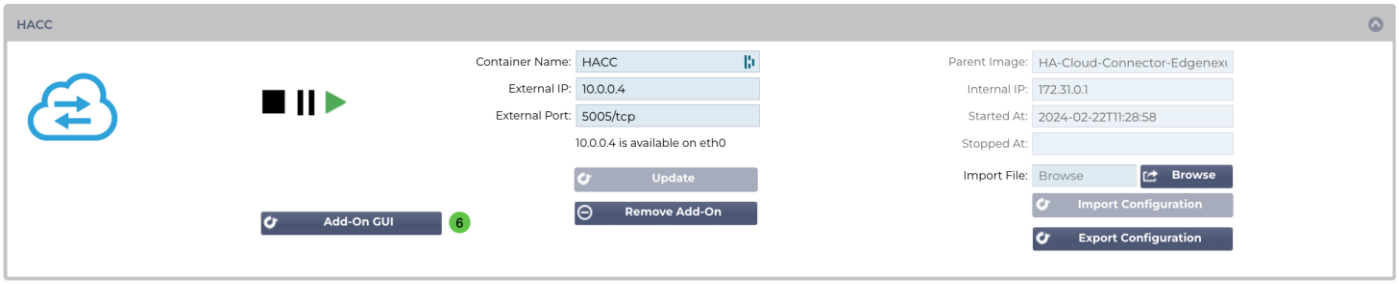
When an App is downloaded and deployed, it is yet to be operational. Normally, the App has to be given an IP address in the same subnet as the EdgeADC and ports through which it needs to be accessible. But in the case of the HACC application, we need to provide it with the IP address of the eth0 network interface.

- Navigate to Library > Add-Ons and locate the HA Cloud Connector App.
- It should look something like the image below.



- Give the Add-On a name 1 – the EdgeADC's internal DNS system uses this to refer to the App when needed.

- Enter the value for the External IP 2. This value should equal the Private IP given to NIC1 of the cloud VM instance.
- Enter a value of **5005/tcp** for the External Port 3.
- Once you have done this, click the Update button 4 to initialize the App.
- Click the PLAY icon 5 above to activate the App into an operational state.
- Once operational, it will look like the following image and be listed in the Services section as an embedded App.



- Note the Add-On GUI 6 button to launch the App GUI and the Pause App and Stop App buttons. Clicking the Add-On GUI button will open the App management screen in another browser tab.

Note: You will need to do this on the HA Cloud Connector on each ADC.

Configuring the HA Cloud Connector for Azure

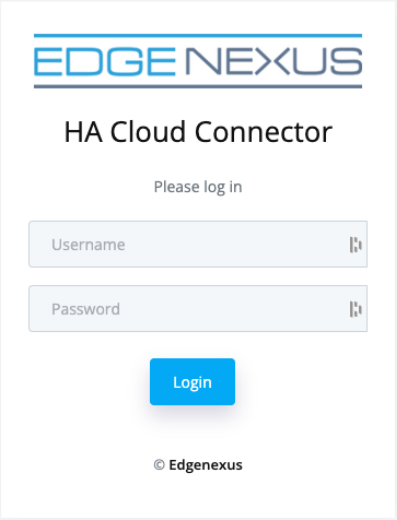
Logging onto the HA Cloud Connector Console

The first step is to log in and access the management console.

To do this, access the Add-ons section of the ADC using the navigation panel. It can be found in the Library section.

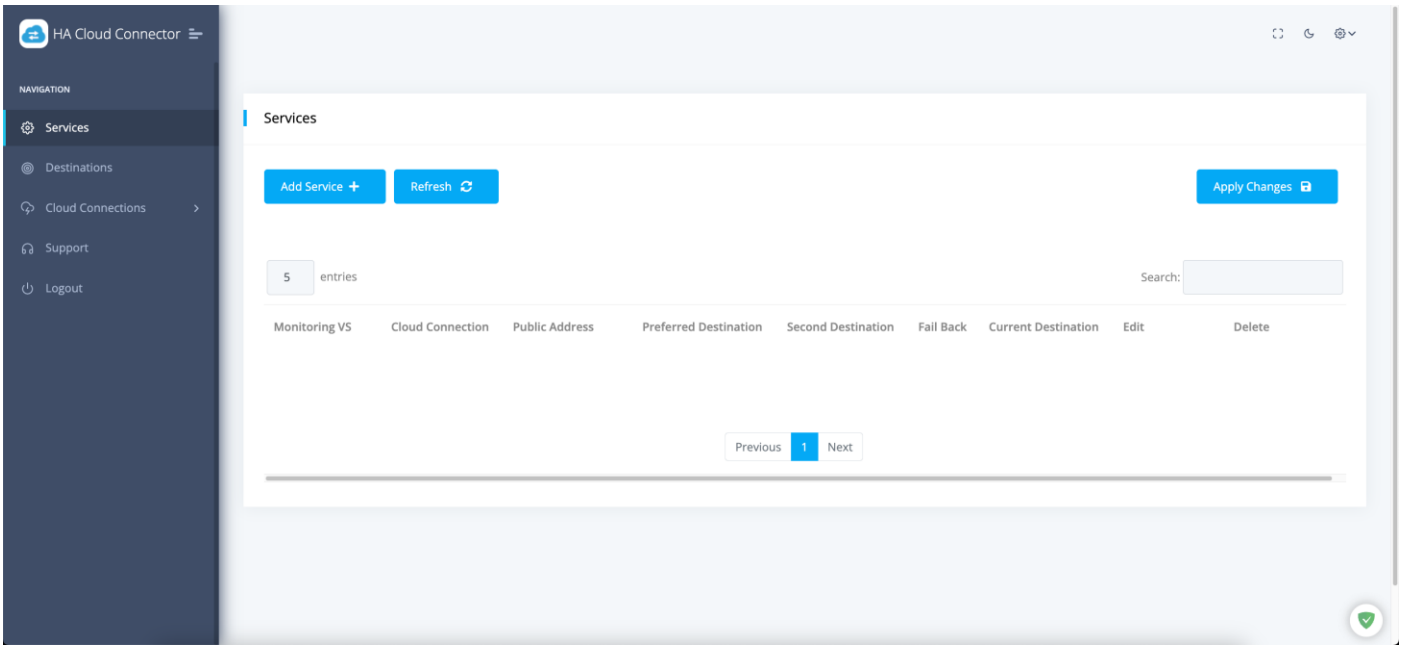
Locate the HA Cloud Connector App that you deployed. If the fields are blank, you have yet to operationalize the App. See the section **Error! Reference source not found.** in the last chapter.

Click the Add-On GUI button to launch the console login page.



The default credentials are **admin/admin** for the username and password. You may change this later within the console if you wish.

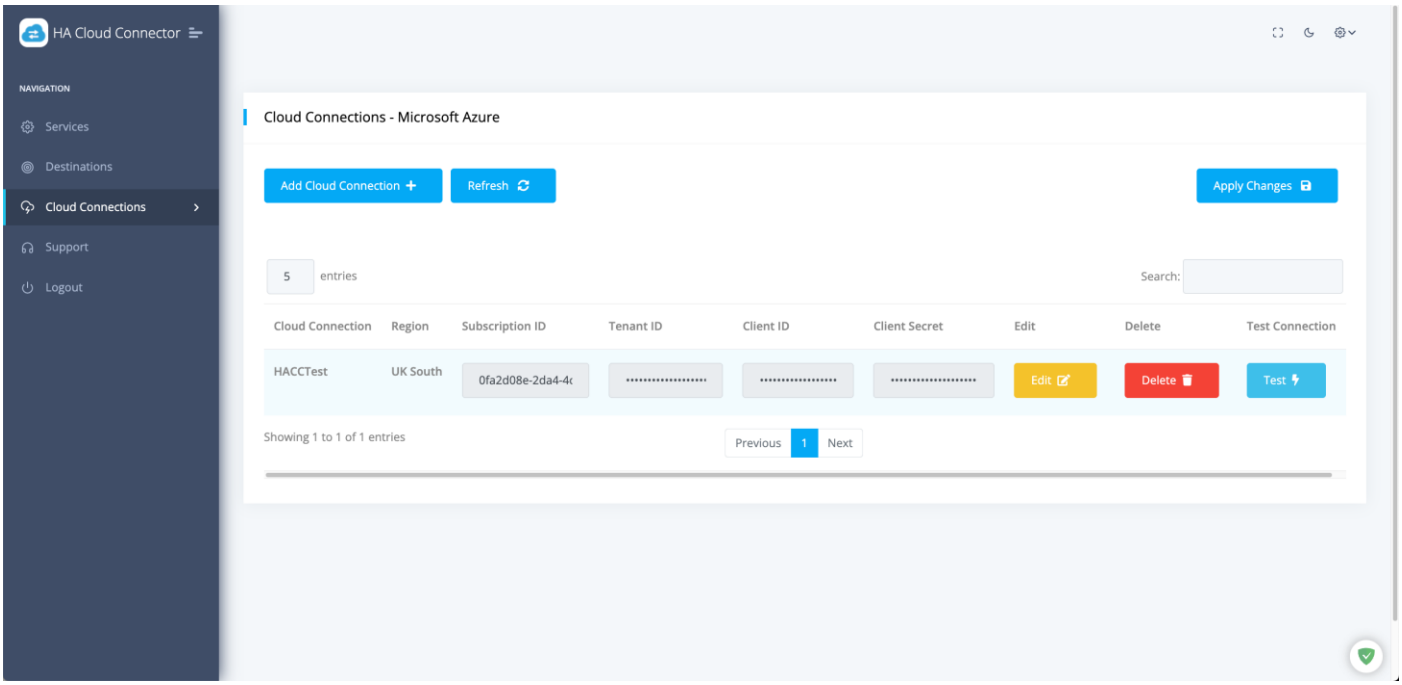
The Cloud Connector Main Page



Once logged into the HA Cloud Connector, you will be presented with the main or Home page. It is from this page that you will perform the configuration of the HA Cloud Connector.

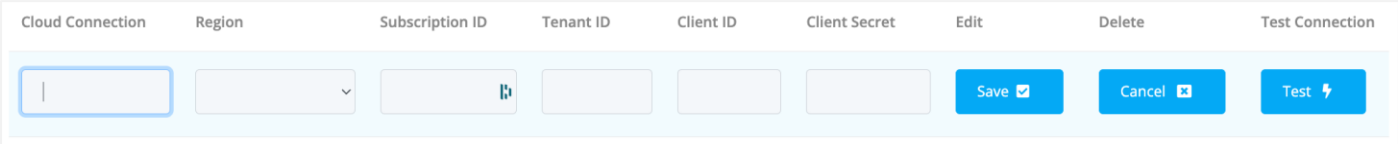
The first step in configuring the HA Cloud Connector is to define the Cloud Connection. The information you provide will give the HA Cloud Connector access to your Cloud environment, particularly the floating IP it will need to manipulate.

Defining Cloud Connections

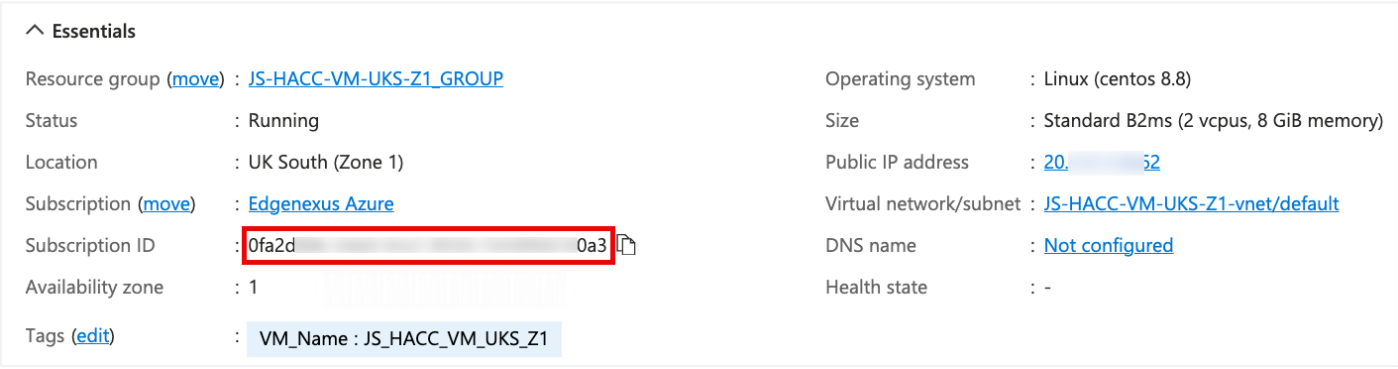


- Click the Cloud Connections option in the Navigation bar on the left of the page and expand it.
- Select Microsoft Azure.
- To add your Cloud Connection, please click the Add Cloud Connection button.

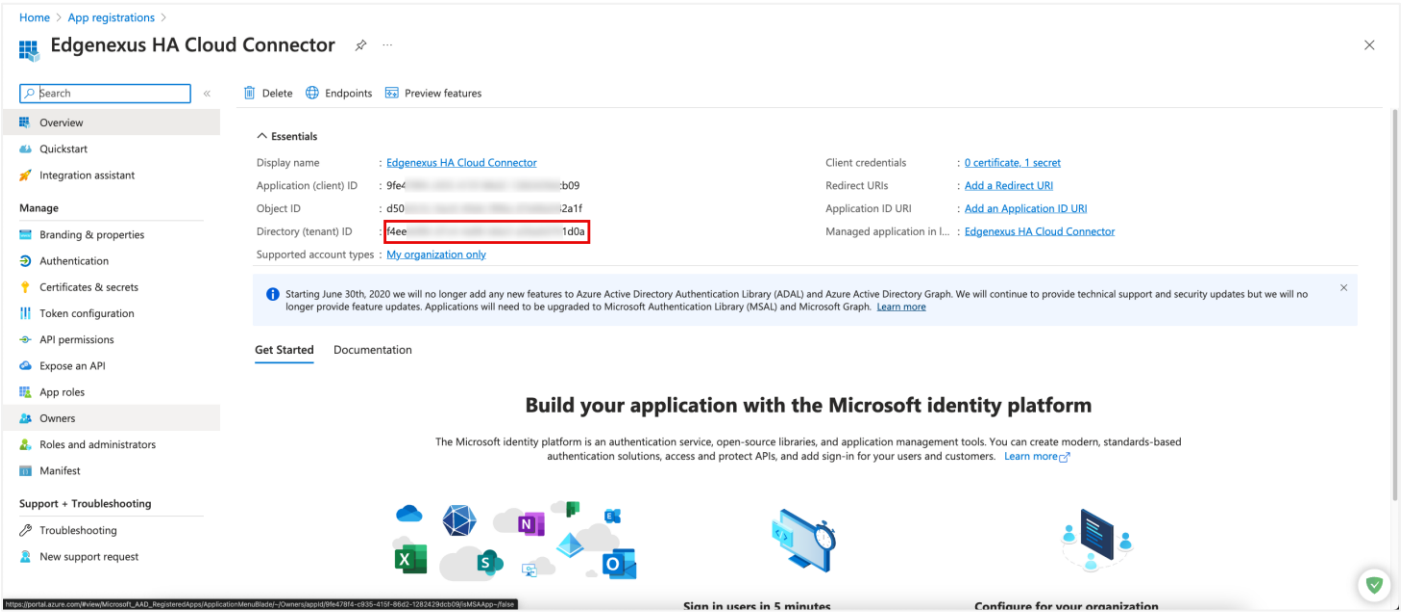
- You will now see a blank field line that you need to fill in.



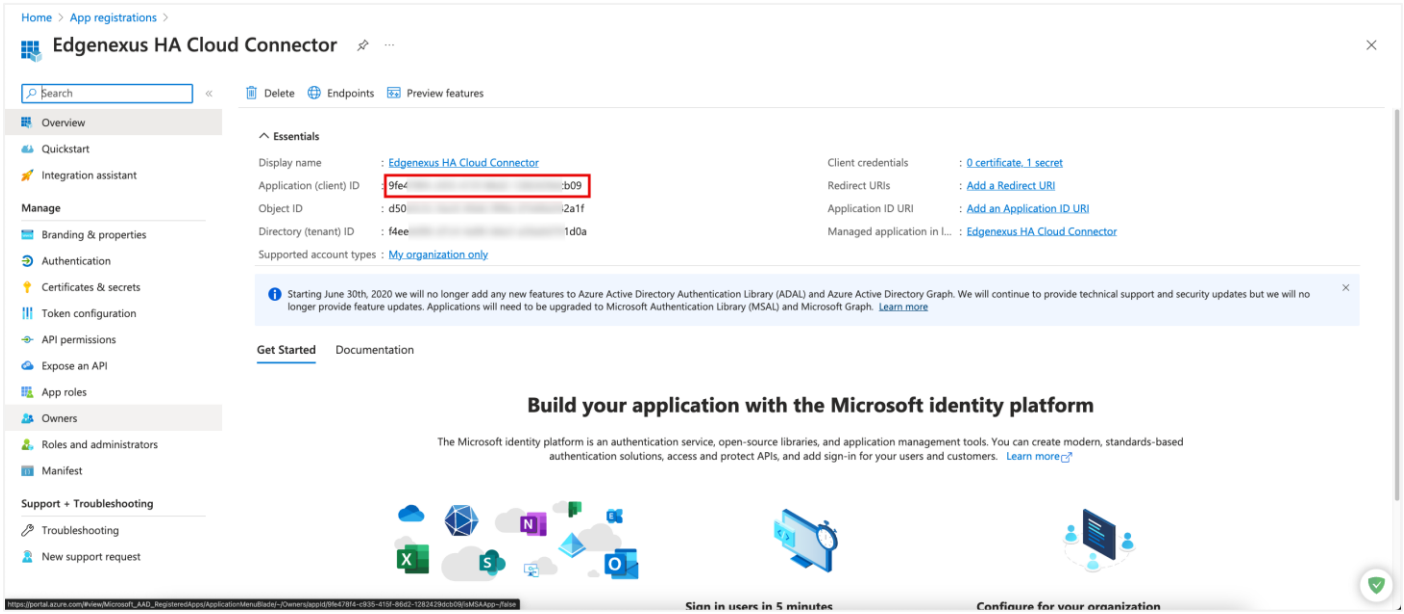
- Add a value for the Cloud Connection name. This can be anything you wish, and in our case we have shown it as HACCTest.
- Add the Azure Region in which your VMs are located.
- Add your Azure Subscription ID. You can find this in your VM Overview page.



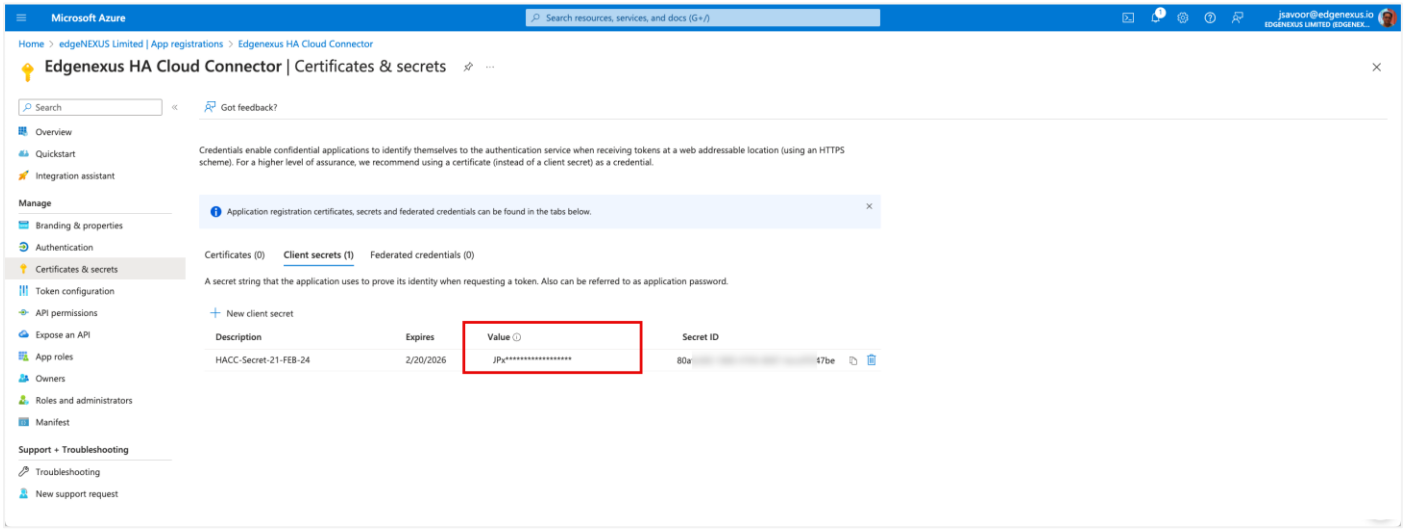
- Next, add the Tenant ID (found in your HACC App Registration overview)



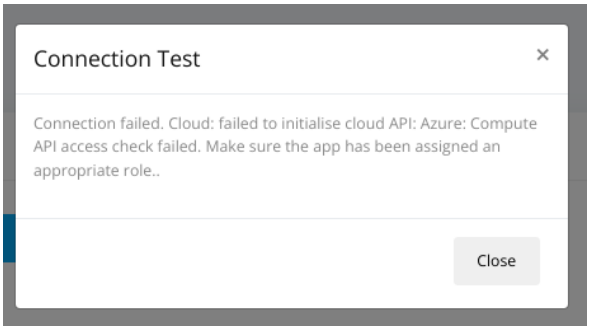
- Next, enter the Client ID (found in your HACC App Registration overview)



- Finally, we have to enter the Client Secret. As you recall, we defined this when creating the App Registration and you should have noted this down.

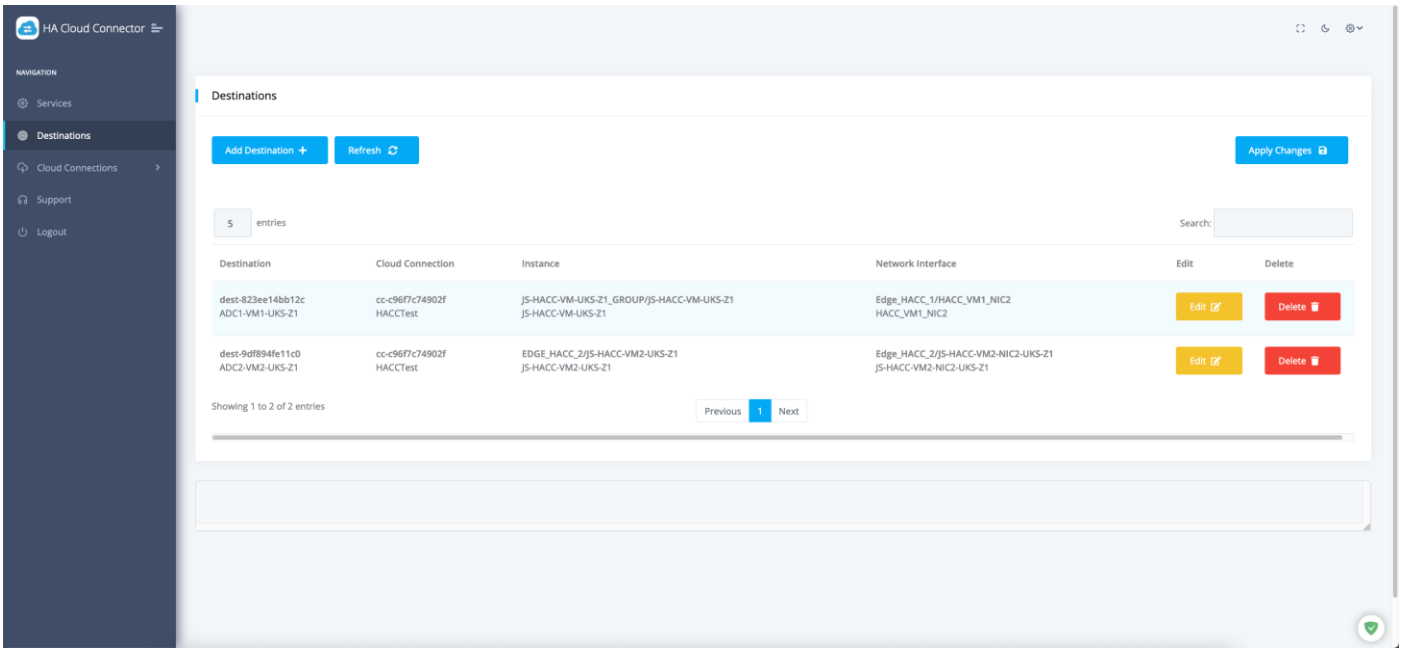


- You finally have to Save and then Apply the changes.
- Next click the Test button to check it works. If an error is shown, check all the settings entered.
- If you see the following error when you perform the test, please check the Role Assignments you defined earlier.

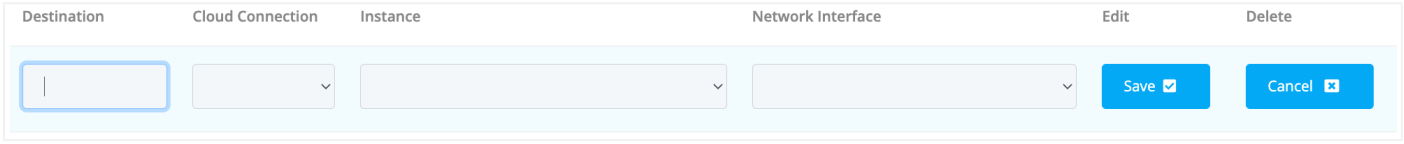


Defining Destinations for HA

The next stage is to add the destinations to which the floating IP will be directed in case of failure of a service or ADC.



- Click Add Destination
- You will be presented with a blank field entry line comprising a number of dropdown menus.



- In the Destination field, enter a descriptive value. We have used ADC1-VM1-UKS-Z1, but you can use whatever you wish.
- Next click the Cloud Connection menu and select the Cloud Connection you defined.
- Next click the Instance dropdown menu and select VM1.
- Next click on the Network Interface field and select NIC2 on VM1.
- Click Save.

For the second definition we will repeat the above steps.

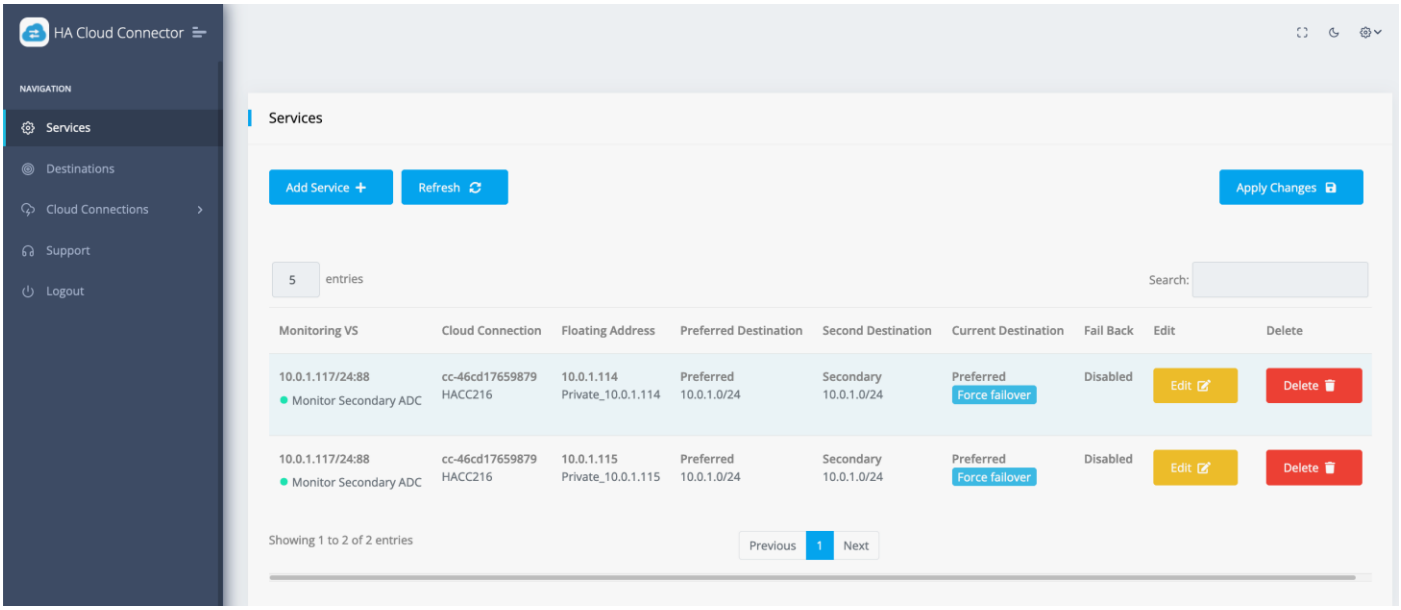
- Click Add Destination
- You will be presented with a blank field entry line comprising a number of dropdown menus.
- In the Destination field, enter a descriptive value. We have used ADC2-VM2-UKS-Z1, but you can use whatever you wish.
- Next click the Cloud Connection menu and select the Cloud Connection you defined.
- Next click the Instance dropdown menu and select VM2.
- Next click on the Network Interface field and select NIC2 on VM2.
- Click Save.

Once you have done, click the Apply Changes button.

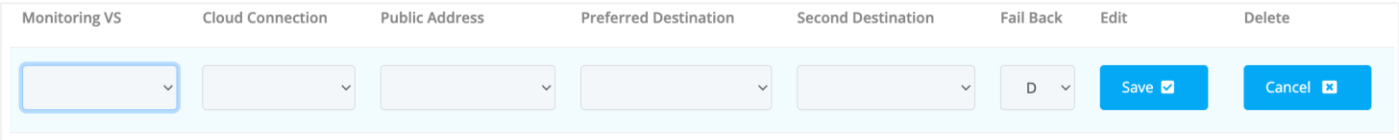
© 2024 Edgenexus Limited

Defining Services to be Monitored

One of the key elements of the HA Cloud Connector is its ability to monitor the virtual services that are running on the ADC. In order to do this, we have defined a monitoring service using the eth0 network interface IP.



- Click Add Service
- A blank field line is presented for entry.



- Click the Monitoring VS menu and select the VIP you defined as the Monitoring VIP. This is the one that used the eth0 IP address of the ADC.
- Select the Cloud Connection.
- Select the floating Public IP address, or the Private IP address you created.
- Select VM1 as the Primary Destination.
- Select VM2 as the Secondary Destination.
- In the Failback field, select Enable if you want to have the HACC App failback to the Primary when the issue has been fixed, or Disable if you would like the connection to be retained on ADC2, making that the Primary.
- Click Save.
- You can add additional Services for each Private IP that requires switching over to ADC 2.
- Click Apply once done.

Repeat these steps within the HACC App on ADC 2.

NOTE: Please make replicate the entries on both Preferred and Secondary ADCs.

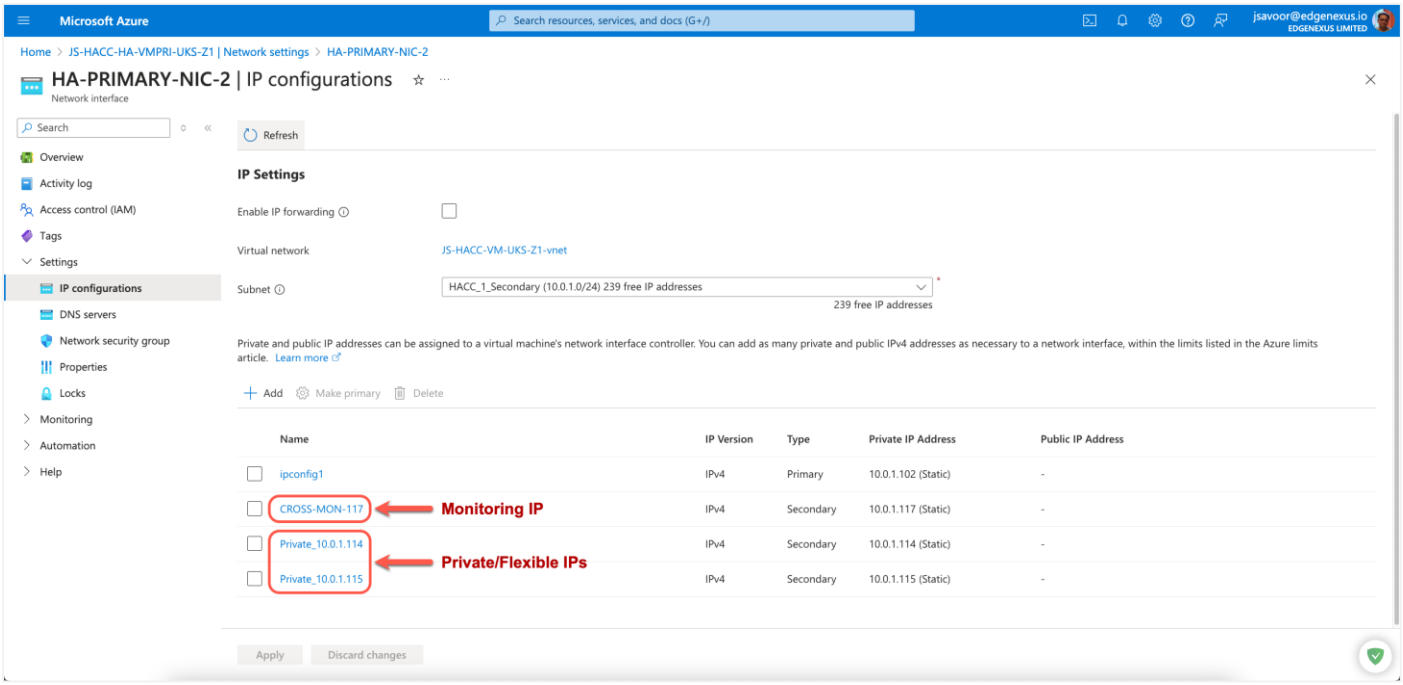
And that is it! HA Cloud Connector has been configured.

© 2024 Edgenexus Limited

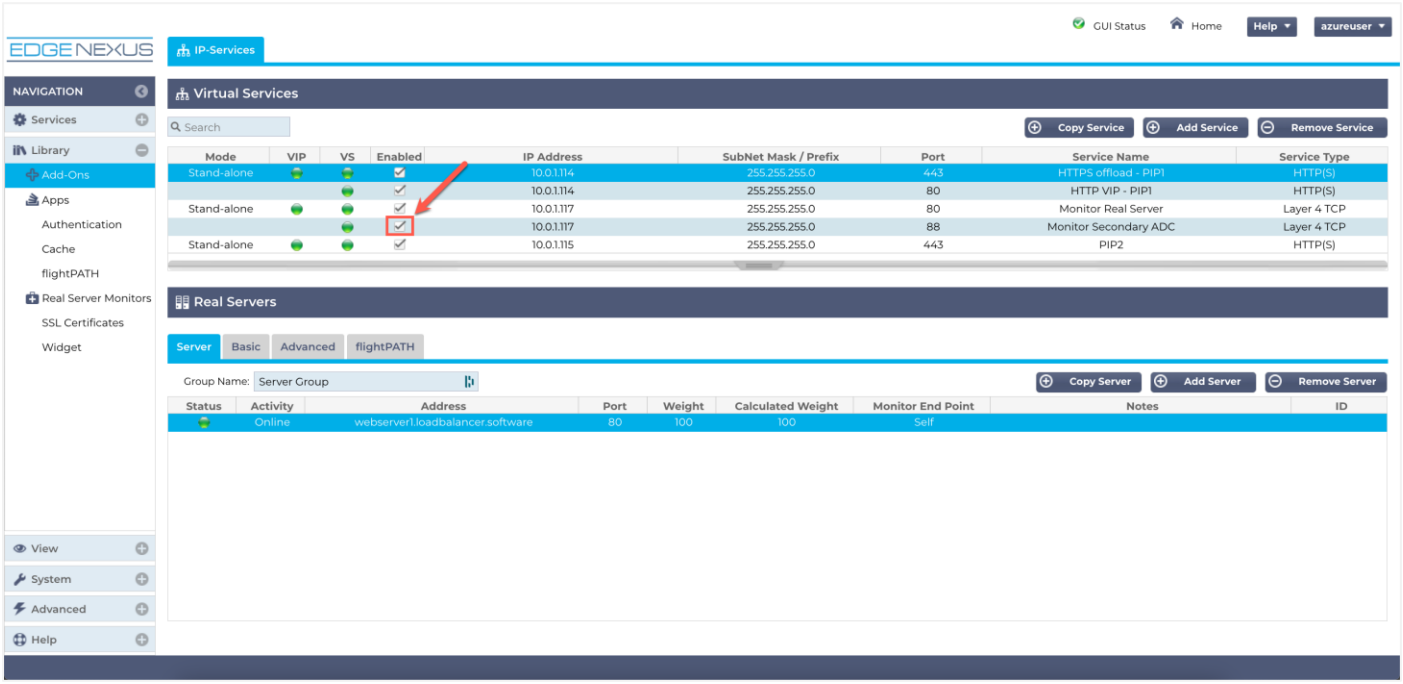
Testing the HA Cloud Connector for Azure

Testing the HA Cloud Connector is very simple. Just follow the procedure below.

1. Navigate to the Network settings page of NIC-2 on the Preferred ADC.



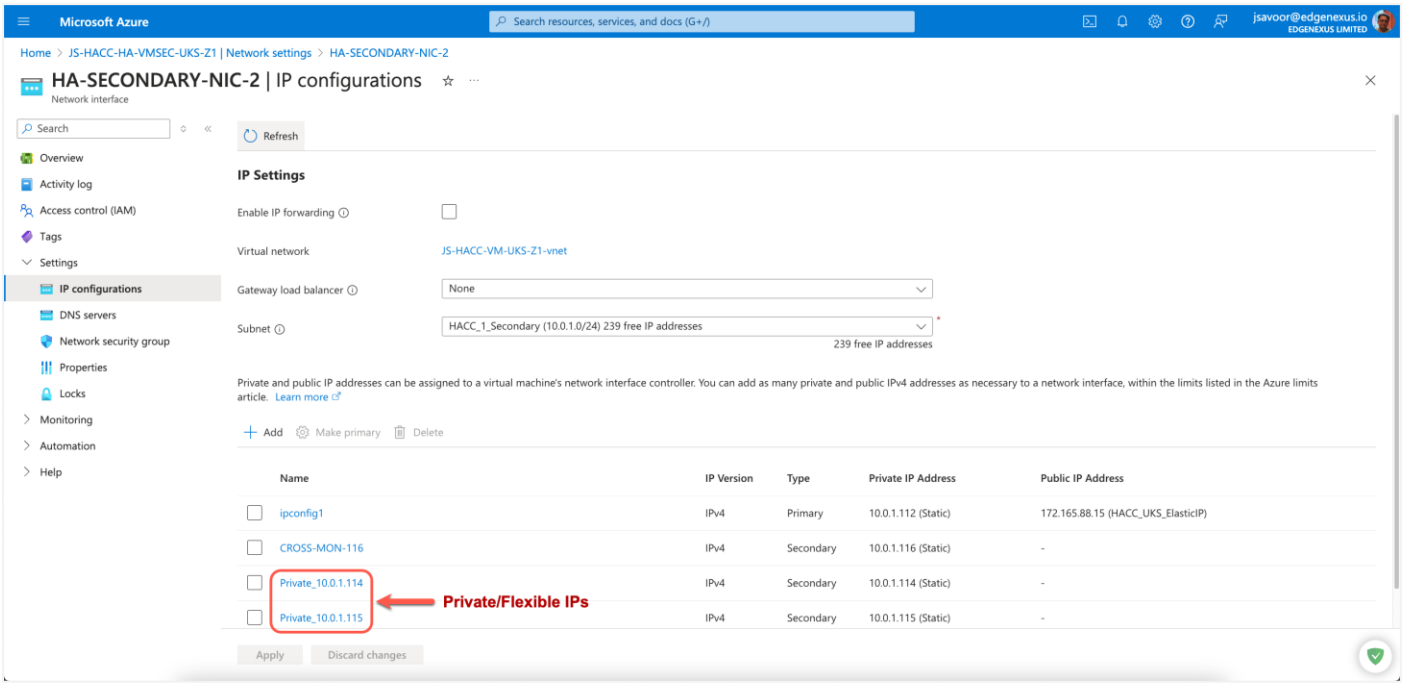
- Note that the IPs are associated with NIC-2 of the Preferred ADC
- Now, go to the IP Services page of Preferred ADC.
- Locate your Monitoring VIP and untick the checkbox.



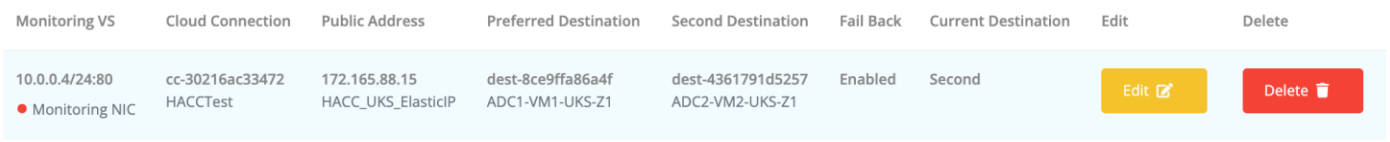
- This makes the service status turn RED as the VIP is no longer communicating with the Real Server.

© 2024 Edgenexus Limited

- Now go to the networking page for **NIC-2** for the Secondary ADC.



- You can also check the Services page in the HACC application.



- Traffic is now going to the Second destination that was our Secondary ADC and has now become the Primary.

The Failback Setting

The Failback setting within the Service definition configures the HACC to do the following:

Enabled Mode

When the Preferred ADC fails, the floating IP(s) are moved to the Secondary ADC.

Once the Preferred is brought online again, the floating IP(s) will be returned to the Preferred from the Secondary.

Disabled Mode

When the Preferred ADC fails, the floating IP(s) are moved to the Secondary ADC.

The Secondary will now be the Preferred ADC.

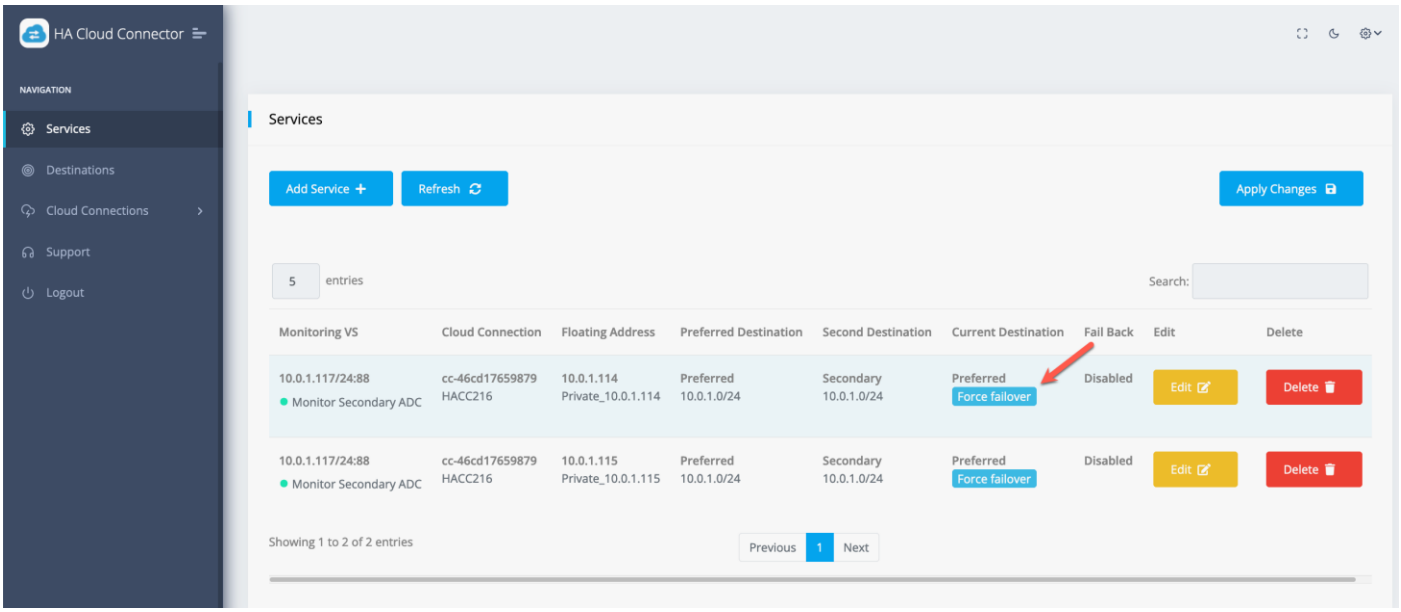
Once the failed ADC is brought online again, the floating IP(s) will remain on the Preferred (ADC2).

Should the Preferred fail at a later time, the floating IP(s) will be moved to the Secondary.

© 2024 Edgenexus Limited

Force Failover by Service

There will be times when you wish to failover the floating IP address, either singly, or in multiples. The Force Failover button allows this to be done.



Clicking the button will force the floating IP address(es) to failover to the partner ADC in a graceful manner.

Force Failover by Destination

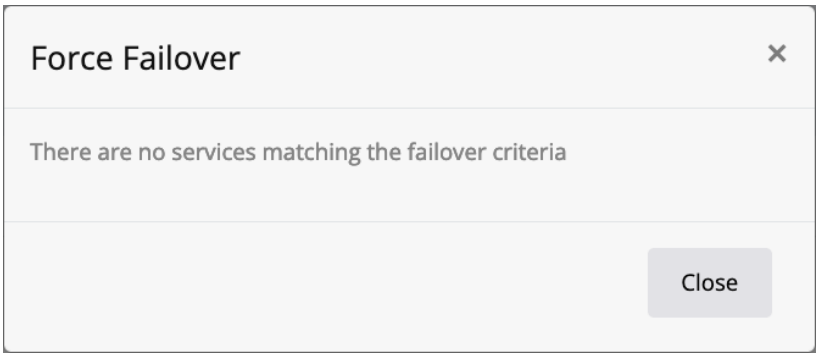
You may also wish to fail over all Services from the Preferred to the Secondary. You may also have many Services that need to be failed over, making it tedious to do it one by one.

To accommodate this, we have provided the Force Failover function on a per Destination basis.

When the Force Failover button is clicked in a Destination table row, all Services which are online and have that Destination within their definition will be switched to the selected Destination. This is particularly useful when you have multiple destinations, with multiple Services. For example:

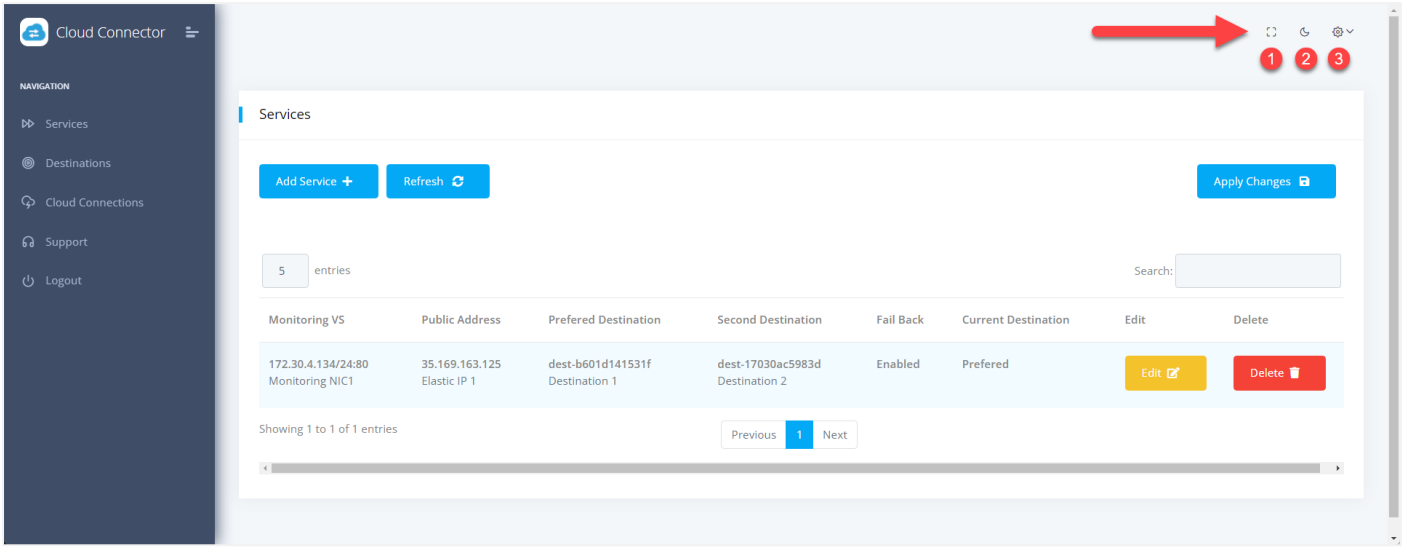
- Service 1: Dest 1 and Dest 2
- Service 2: Dest 1 and Dest 3
- Service 3: Dest 3 and Dest 4

When you click the Force Failover button against an invalid Destination, you will get the following error.



Other Settings

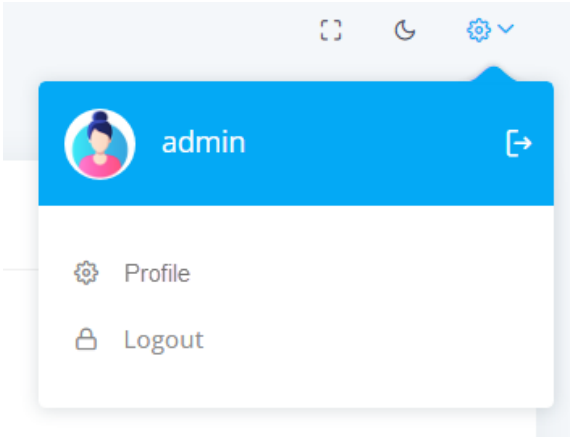
There are a few other settings in the HA Cloud Connector that you may wish to use. These are accessed using one of the icons displayed at the top right of the page.



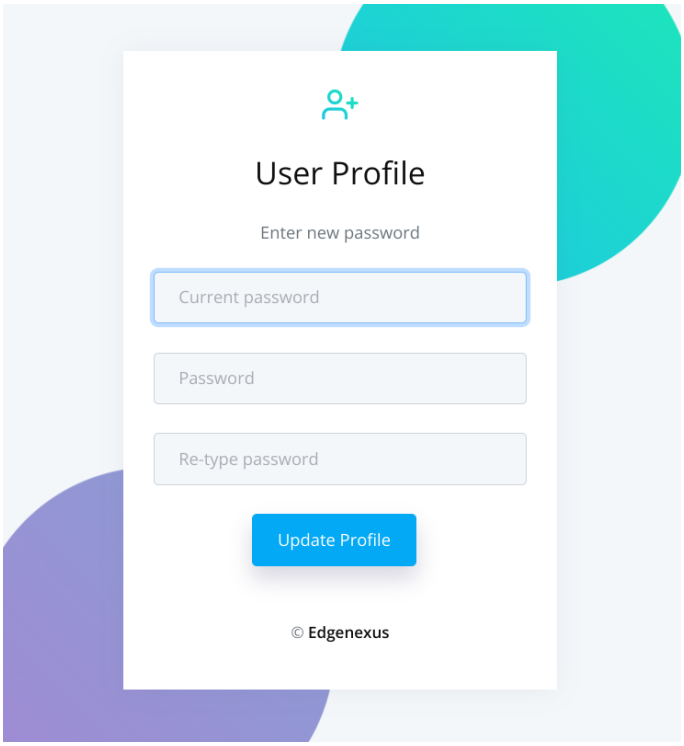
Changing the password

You may change the default password from **admin** to something of your choice.

To do this, click on the icon 3 indicated in the image above to open a menu, from which you must select Profile.



Once selected, you will be shown the form to change your password.



Provide the current password and enter your new password.

Dark Mode

You can display the HA Cloud Connector user interface in either Dark or Light Mode by selecting the icon 2. Clicking the icon alternates the display modes.

Full-Screen Mode

If you wish to display the HA Cloud Connector App on full screen, click the icon 3. The Escape key exits from the full screen display.

Technical Support

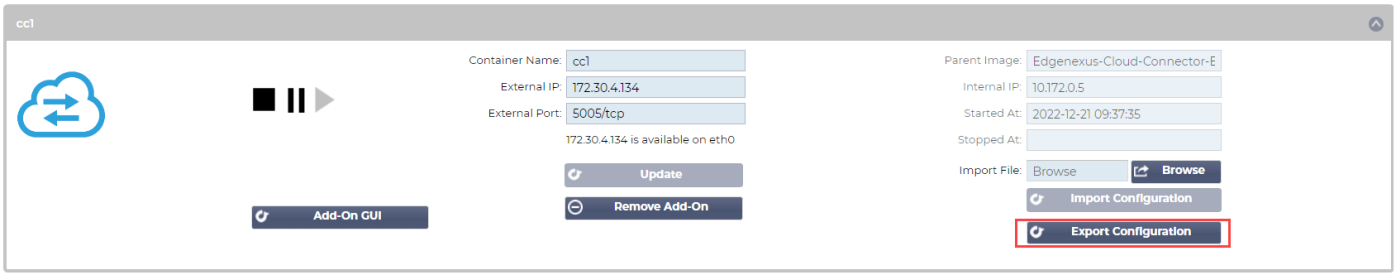
© 2024 Edgenexus Limited

Contacting Support

The HA Cloud Connector App is provided with full email-based support. We always attempt to provide support for free Apps within 4 UK working hours.

Please get in touch with support@edgenexus.io and explain your requirements with a full description. It would also help us greatly if you could provide us with the logs from the ADC and HA Cloud Connector App.

The logs from the ADC that are required are:

1. Support files – found in Advanced > Troubleshooting > Support Files
2. System Logs – found in View > Logs > Download System Logs

The HA Cloud Connector App configuration is located in the ADC and can be found in Add-Ons > App > Export Configuration.