Azure
Deployment Guide
Eli-v6.5.391

Bridgeworks
Unit 1, Aero Centre, Ampress Lane,
Ampress Park, Lymington,
Hampshire SO41 8QF
Tel: +44 (0) 1590 615 444
Email: support@4bridgeworks.com

Table of Contents

1 Requirements for deployment on Azure

In order to deploy your PORTrockIT you will need the VHD file provided to you by Bridgeworks.

The VHD will be made available to you in ZIP format.

You will need to extract the contents of this ZIP file to an accessible location prior to following the rest of this guide.

2 Guide layout

This guide is divided into a series of ordered steps that should be followed through in order. If at any point you run into trouble with a step please refer to the Useful Links section at the end of this document.

It is recommended to print this list of steps out and check off each step as you complete them.

☐ Step 1. Storage accounts

☐ Step 2. Uploading a VHD

☐ Step 3. Image creation

☐ Step 4. Virtual machine creation

☐ Step 5. Route tables

☐ Step 6. Network interface

☐ Step 7. Network security

3 Storage accounts

The following section will deal with the creation and configuration of a storage account. If you already have a configured General Purpose v1 storage account with a container that you wish to use then please proceed to Chapter 4: Uploading a VHD.

A storage account is used to contain any persistent storage.

In this guide, a storage account will be used to store the VHD from which an image will be created.

Microsoft offer multiple types of storage accounts:

Storage (general purpose v1)
This supports: blobs, Azure files, messages, queues, and in-managed disks.

Storage (general purpose v2)
All of general purpose v1, plus all 3 types of blob described below. This solution runs a different pricing model than the v1, and generally results in higher costs for the same resource access as the v1.

Blob storage

Hot Frequently accessed data.

Cool Infrequently accessed data.

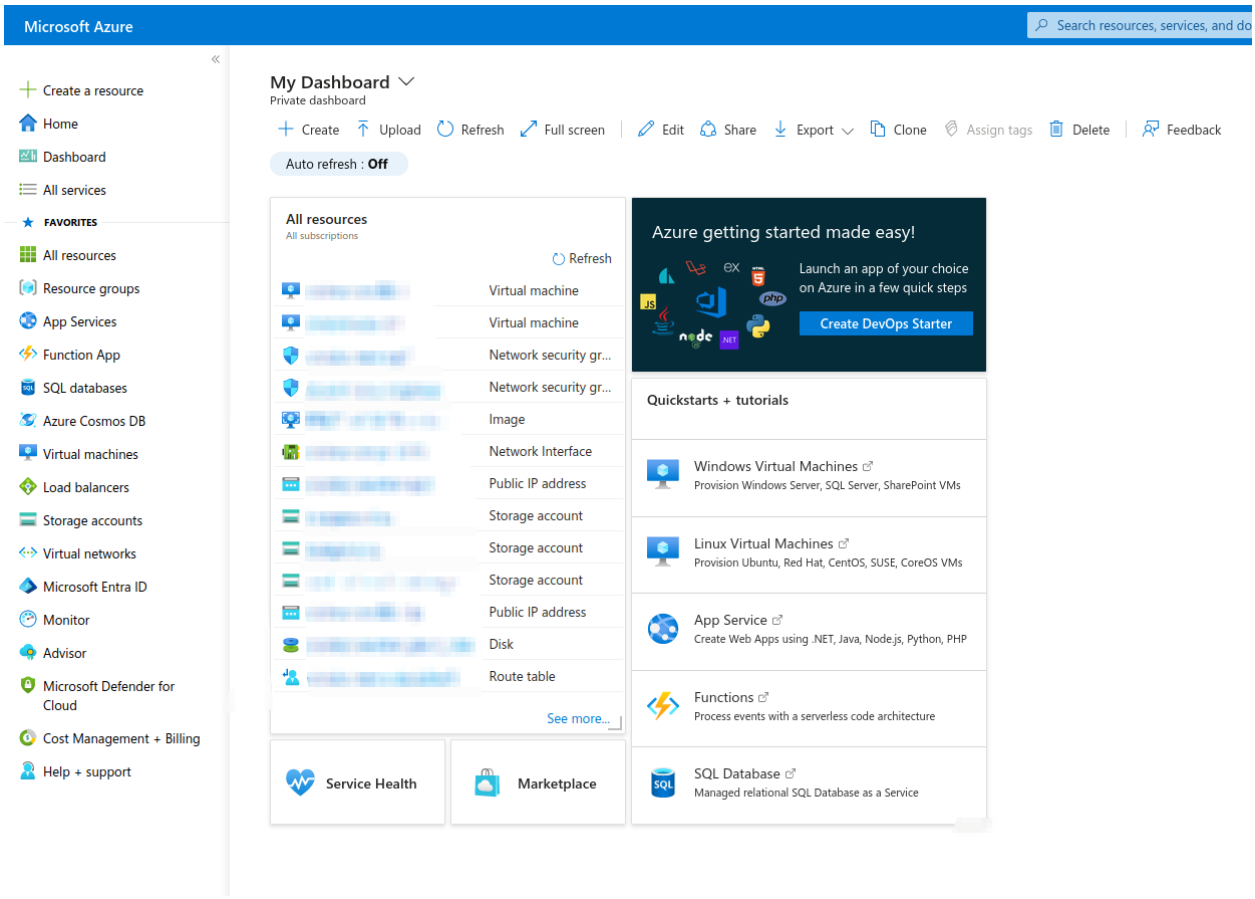
Archive Rarely accessed data. Very low storage cost, high access cost. To read archived data it must be “rehydrated” to Hot or Cool storage; this can take up to 15 hours.

Bridgeworks recommends General Purpose v2 storage for the PORTrockIT. General Purpose v1 is now legacy, and the Blob specific storage does not allow storage of “Page Blobs”, which is the default blob type used for virtual machines.

3.1 Creating a storage account

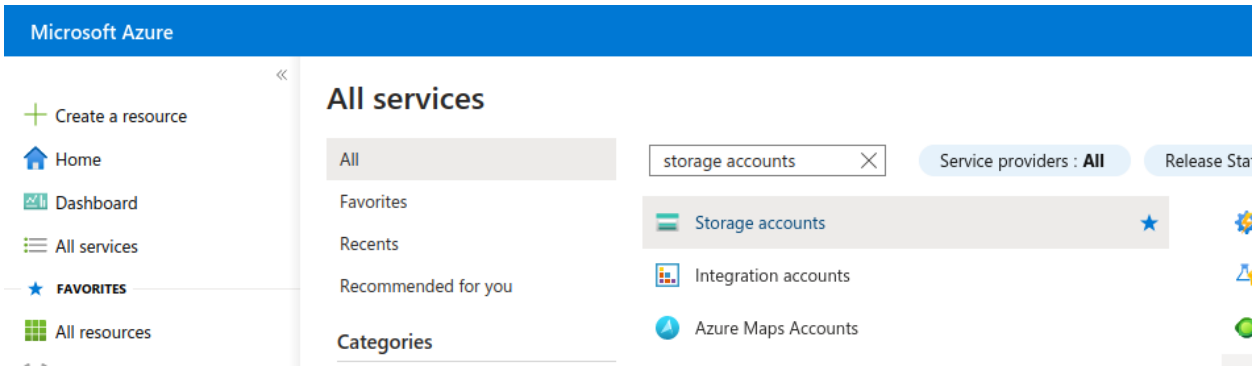
To create a storage account, first log in to your Azure account through the Azure portal.

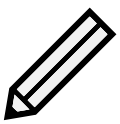
Once logged in, the dashboard should be presented:



On the left panel, navigate to the *Storage accounts* section. This can be achieved by left clicking on *All Services*.

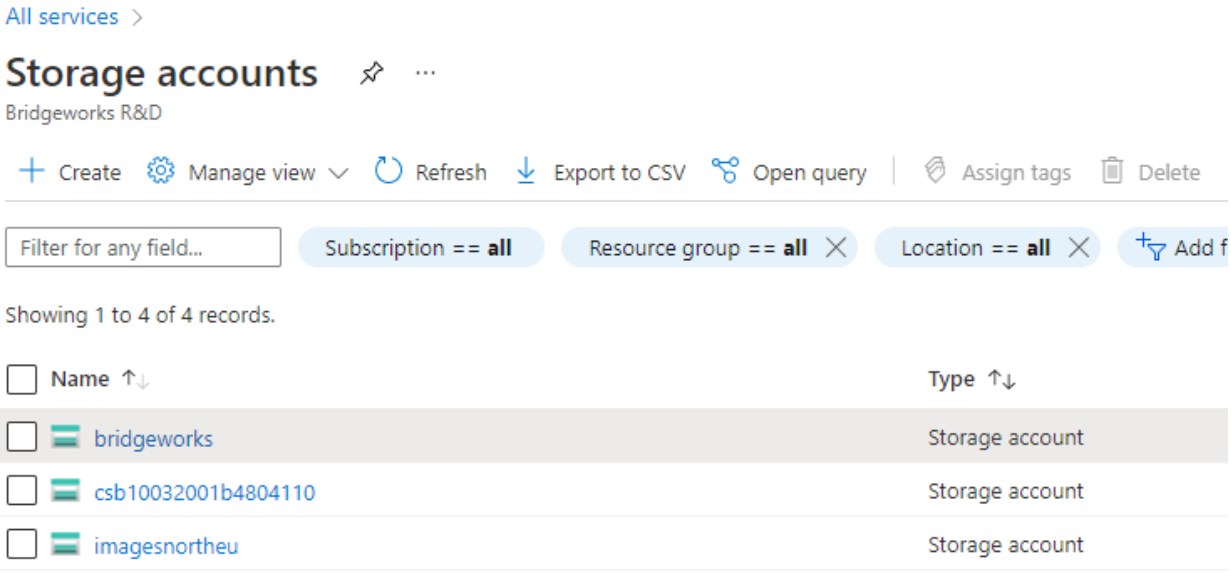
Find the *Storage accounts* section, or enter *Storage accounts* in the *Filter* bar located at the top of the page.





Note: You can add frequently used sections to the left pane of your Azure page by left clicking on the star to the right of your chosen section.

Left click the *Storage accounts*; this will bring up any accounts that are accessible to this Azure account.



In this section, left click the *Create* button at the top of the page. This will bring up a *Create storage account* section. In the image below, the values for this storage account have been filled out.

All services > Storage accounts >

Create a storage account ...

Basics | Advanced | Networking | Data protection | Tags | Review + create

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. Learn more about Azure storage accounts

Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription * Microsoft Partner Network

Resource group * (New) example_deployment_group

Create new

Instance details

If you need to create a legacy storage account type, please click here.

Storage account name * exampledeploymentstorage

Region * (Europe) UK South

Performance *

- (●) **Standard:** Recommended for most scenarios (general-purpose v2 account)
- ( ) **Premium:** Recommended for scenarios that require low latency.

Redundancy * Geo-redundant storage (GRS)

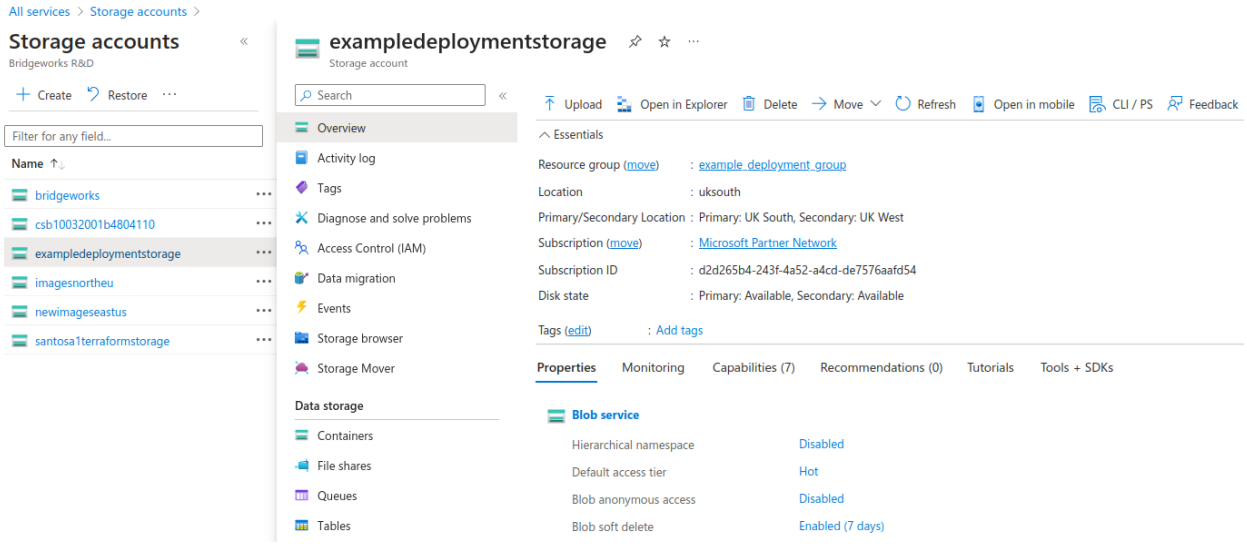
- [x] Make read access to data available in the event of regional unavailability.

Review + create | < Previous | Next : Advanced >

Note:

- The *Replication* entry was left at the default setting. Reduced redundancy settings can be used if desired.
- The *Resource group* is set to *Create new*, but an existing group can be used if you have one set up.
- Ensure that your correct *Subscription* is being used for the billing of this system.

You can now left click the *Review + Create* button to create the storage account. Alternatively, you can configure the storage account further if required. When it has been set up, left click on the storage account to present its overview section.



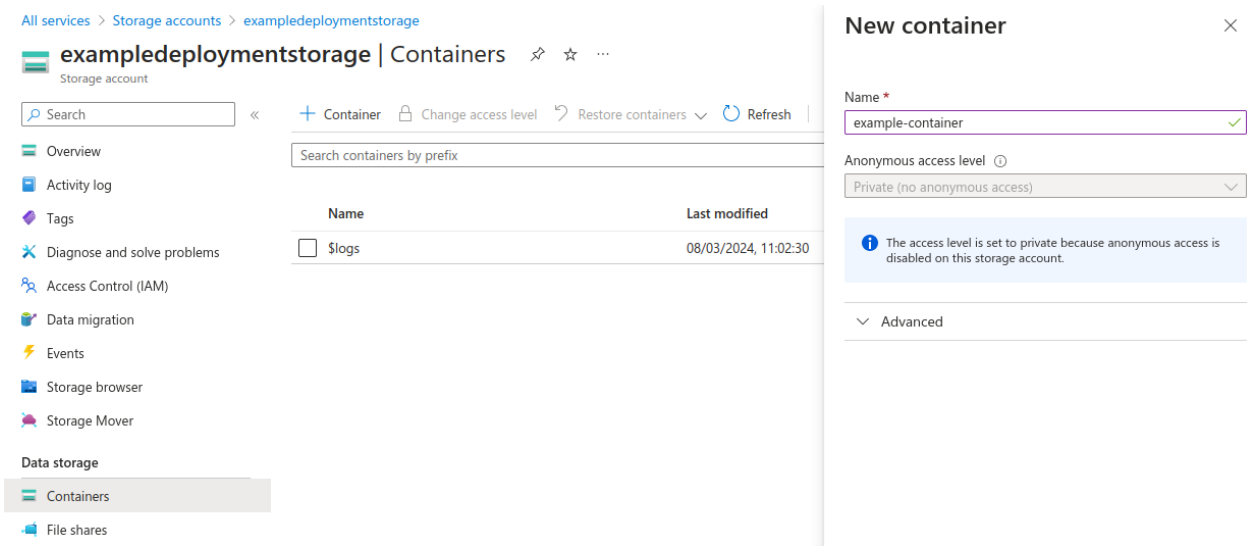
3.2 Containers

To upload data to a storage account on Azure, a container must be added to the storage account in order to hold the data.

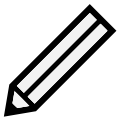
Navigate to the *Storage account* section and left click on your account. In the example, the storage container is labelled *exampledeploymentstorage*.

From the overview for your storage account, left click on the *Blobs* section in the *Blob Service* category.

Then, along the top of the container view, left click on the + *Container* button.



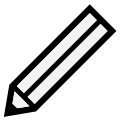
Enter the relevant information and left click *OK*.

	Note: In this example the *Public access level* drop-down is set to *Private*; this is the preferred setting.

4 Uploading a VHD

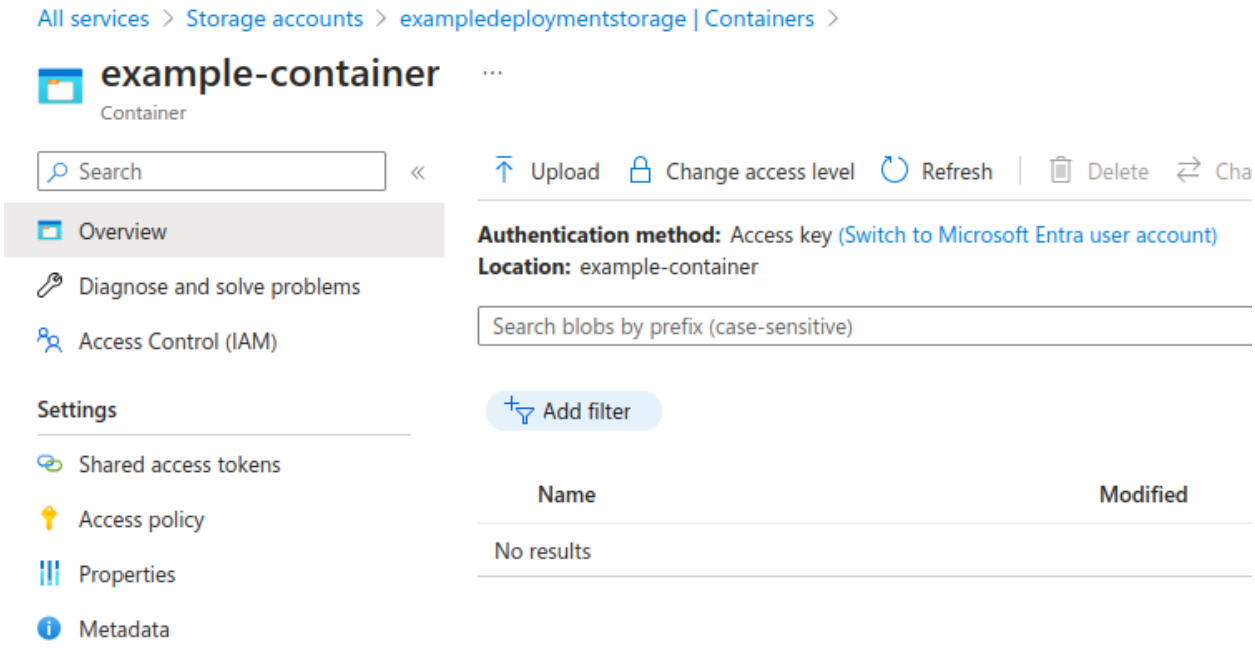
The easiest way to deploy the PORTrockIT as a virtual machine is to upload the provided VHD to a container, create an image from that blob and then create a virtual machine from that image.

You will need to have access to the unzipped VHD file from the provided Bridgeworks ZIP file.

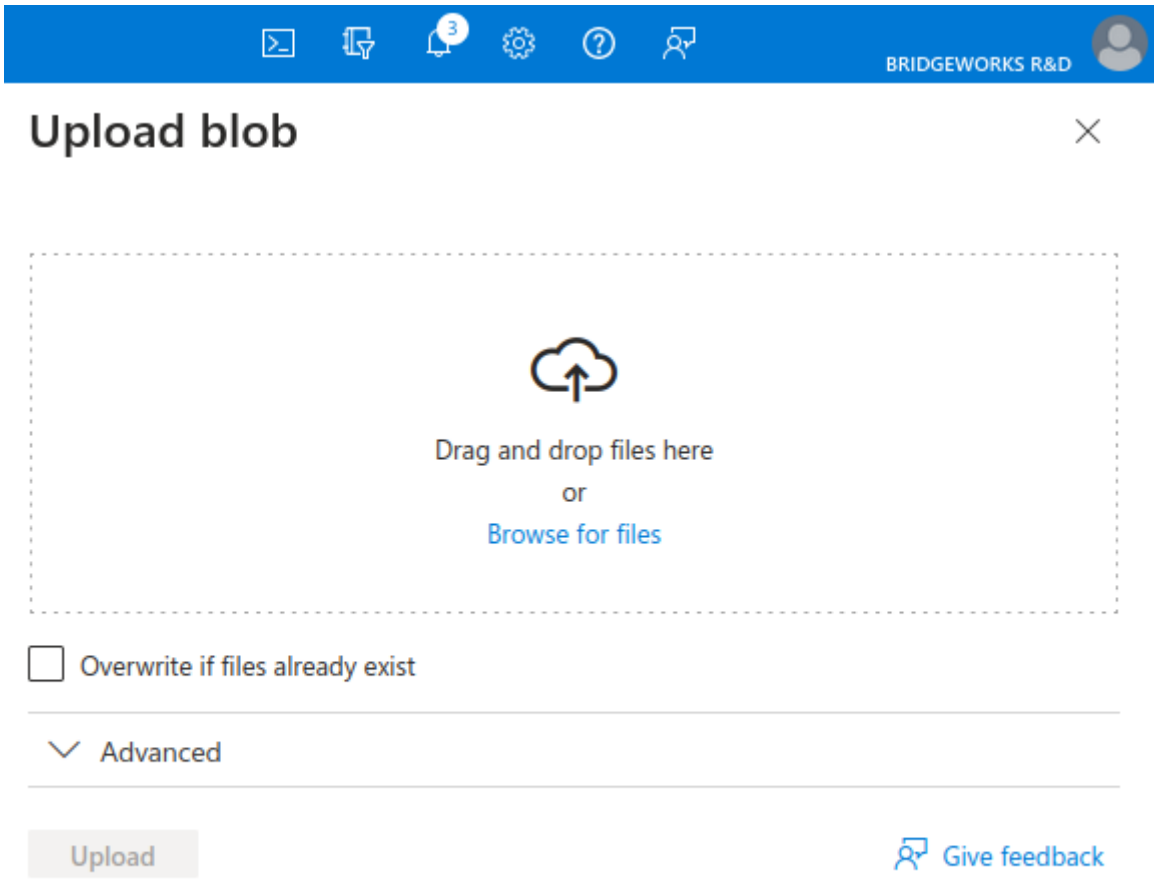
	Note: When uploading the VHD, be aware of the region the VHD is being uploaded to. The easiest method is to upload it to the same region it will be deployed in.

Navigate to the container you intend to use. In the ongoing example the container is the *example-container* located in the *exampledeploymentstorage* storage account.

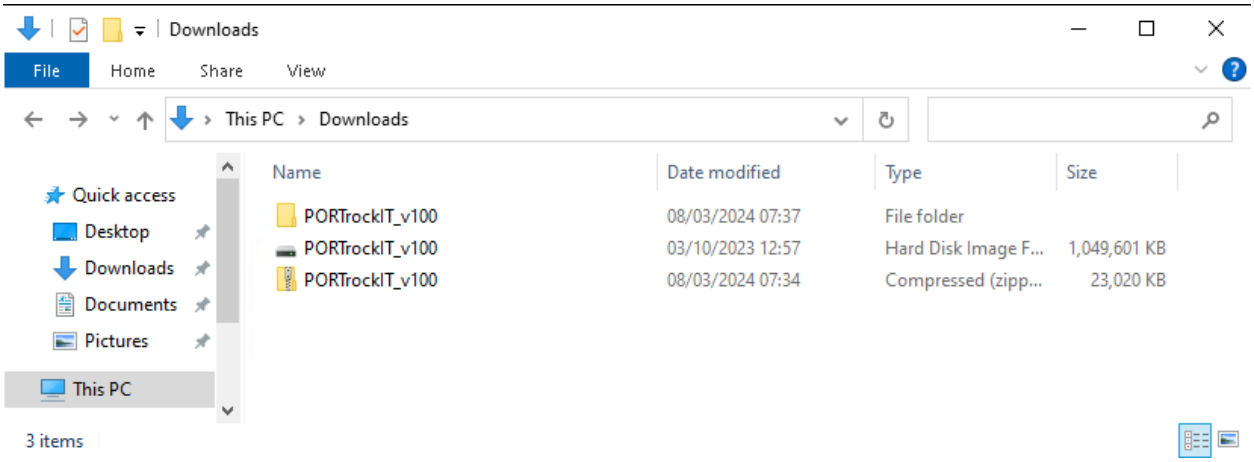
Currently the example container has no contents. Left click the *Upload* icon near the top of the page.



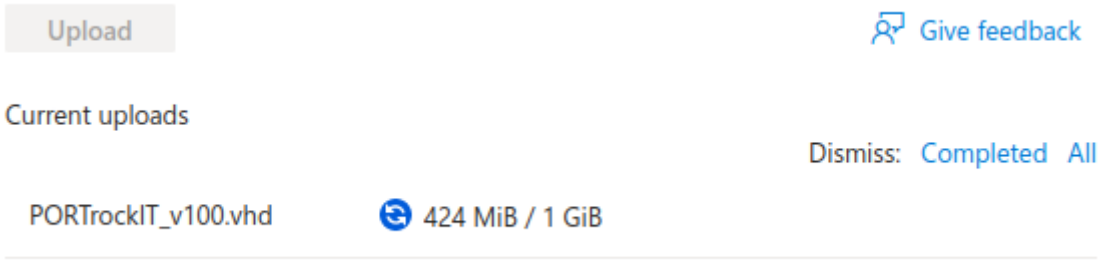
On the right of the page an options menu will appear.



From here, left click on the folder icon to bring up your file explorer. Navigate to the folder containing the VHD file you extracted from the provided PORTrockIT ZIP file.



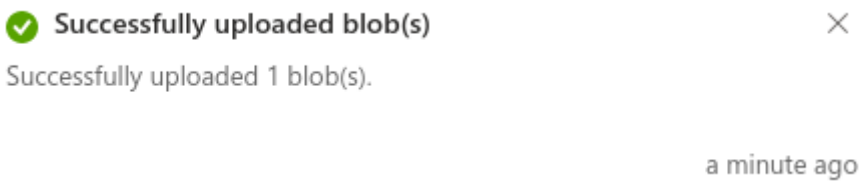
Select the *.vhd* file and left click *Open*, then click the *Upload* button.



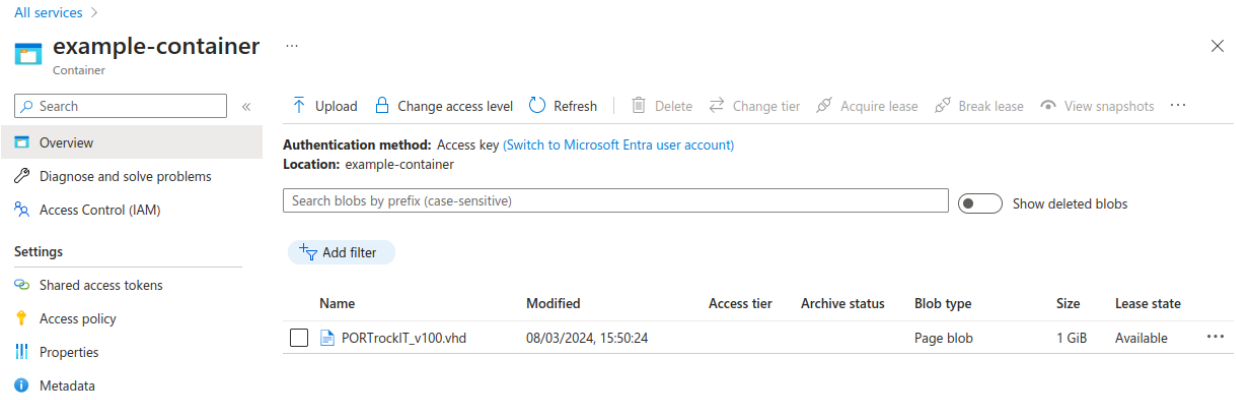
The upload will begin in your current view.

	Note: The screenshot above may show less menu entries than you have; these are found by left clicking on *Advanced*. For this example these settings were not changed from the default.

Leave the upload to complete.



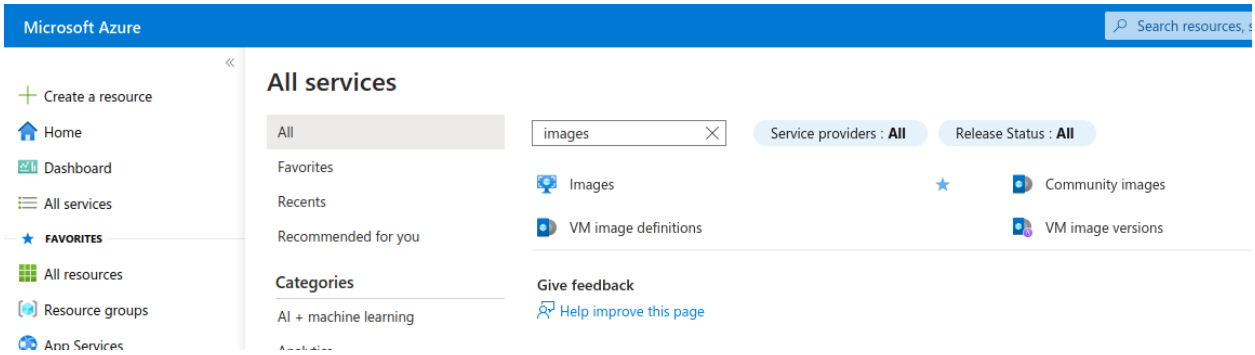
At this stage you should see the newly added file. If not then you may need to refresh the view by left clicking the *Refresh* button.



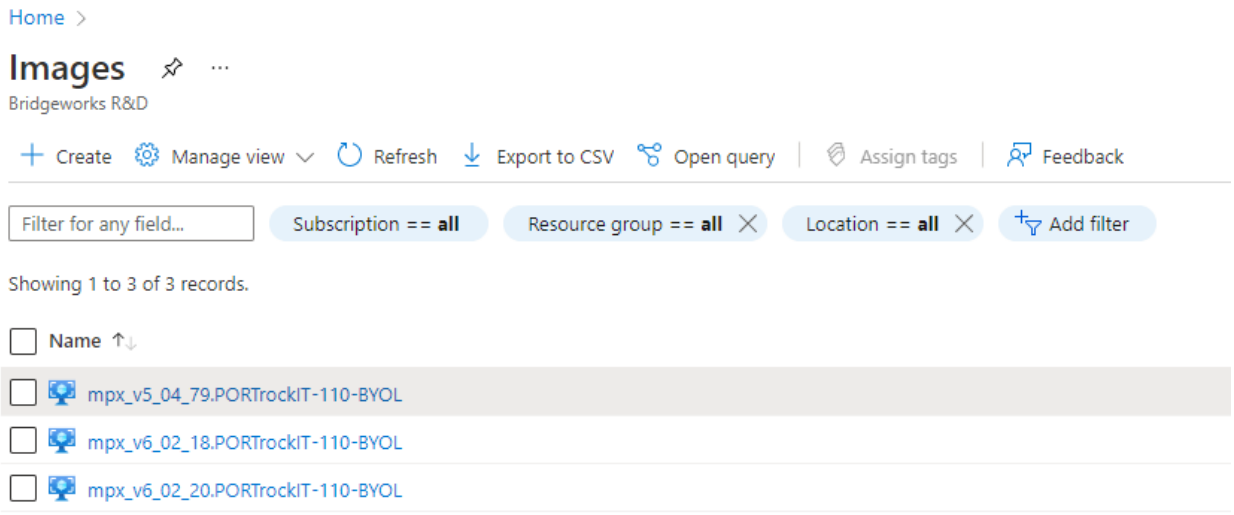
5 Image creation

To deploy a PORTrockIT virtual machine you need to generate an *Image* using the provided VHD that should now be located in a container in a storage account that you have access to.

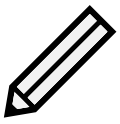
Navigate to the *Images* section. This can be achieved by finding the entry in the *All services* option on the left side of the page.



In the *Images* section, you will be presented with any images available to your account. In this example several have been generated.



From this view, left click the *Create* button. Fill out the information in the new menu that appears. In this example the image is being attached to the *example_deployment_group* which was created while setting up a new storage account.

	Note: It is important that the *OS Type* is set to *Linux*.

Home >

Create an image ...

Basics | Tags | Review + create

Create a managed image that can be used to deploy virtual machines and virtual machine scale sets. The image contains a list of managed blobs and metadata necessary for creating virtual machines. Learn more

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Microsoft Partner Network

Resource group * : example_deployment_group

Create new

Instance details

Name * : example_deployment_image

Region * : (Europe) UK South

Zone resiliency : ☐

OS disk

OS type * : ○ Windows ◉ Linux

VM generation * : ◉ Gen 1 ○ Gen 2

Storage blob * :

Browse

Account type * : Standard HDD

Host caching * : Read/write

Encryption

You can encrypt the OS and data disks with a platform-managed or customer-managed key. Learn more

Encryption type * : (Default) Encryption at-rest with a platform-managed key

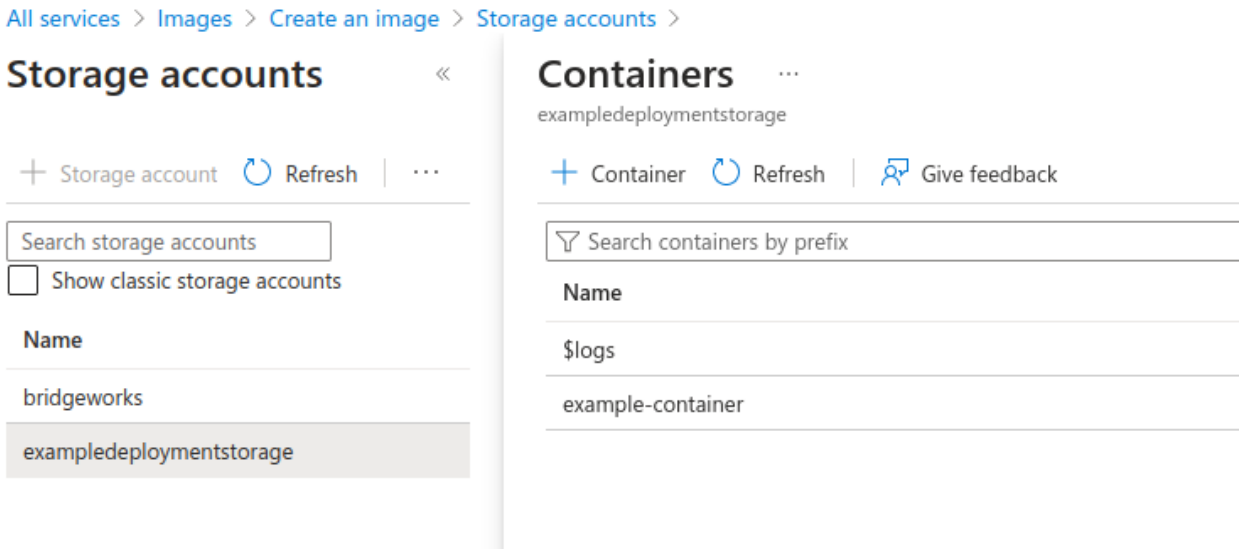
Data disk

+ Add data disk

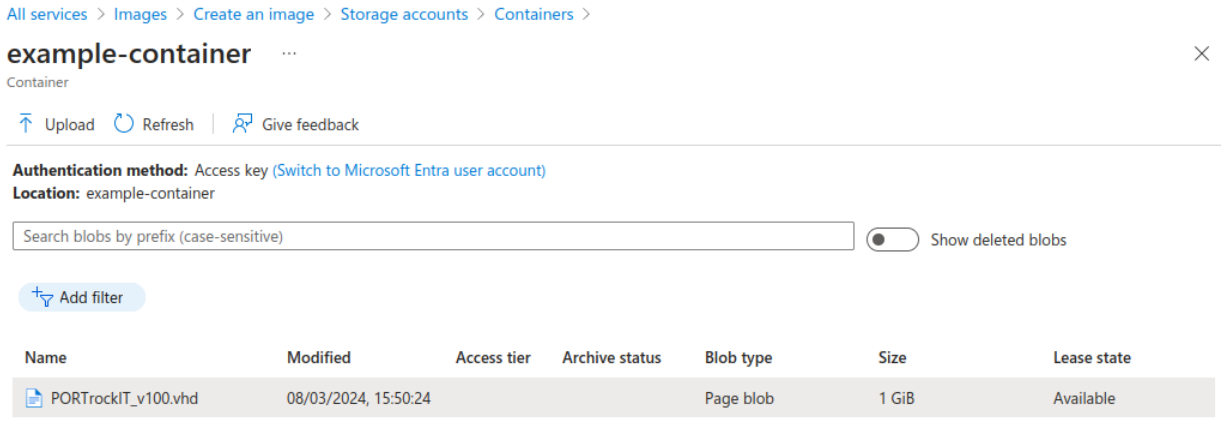
Review + create | < Previous | Next : Tags >

Left click the *Browse* button for the *Storage blob* entry. The page will display the storage account section.

Left click on the storage account you placed the VHD file into.



Left click on the container that the VHD was placed into.



You are now presented with all the data in that container. Left click on the VHD file you uploaded from the provided ZIP file.

Home >

Create an image ...

Basics Tags Review + create

Create a managed image that can be used to deploy virtual machines and virtual machine scale sets. The image contains a list of managed blobs and metadata necessary for creating virtual machines. Learn more

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Microsoft Partner Network

Resource group * : example_deployment_group

Create new

Instance details

Name * : example_deployment_image

Region * : (Europe) UK South

Zone resiliency : ☐

OS disk

OS type * : ○ Windows ◉ Linux

VM generation * : ◉ Gen 1 ○ Gen 2

Storage blob * : https://exampledeploymentstorage.blob.core.windows.net/example-contain...

Browse

Account type * : Standard HDD

Host caching * : Read/write

Encryption

You can encrypt the OS and data disks with a platform-managed or customer-managed key. Learn more

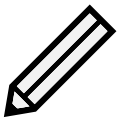
Encryption type * : (Default) Encryption at-rest with a platform-managed key

Data disk

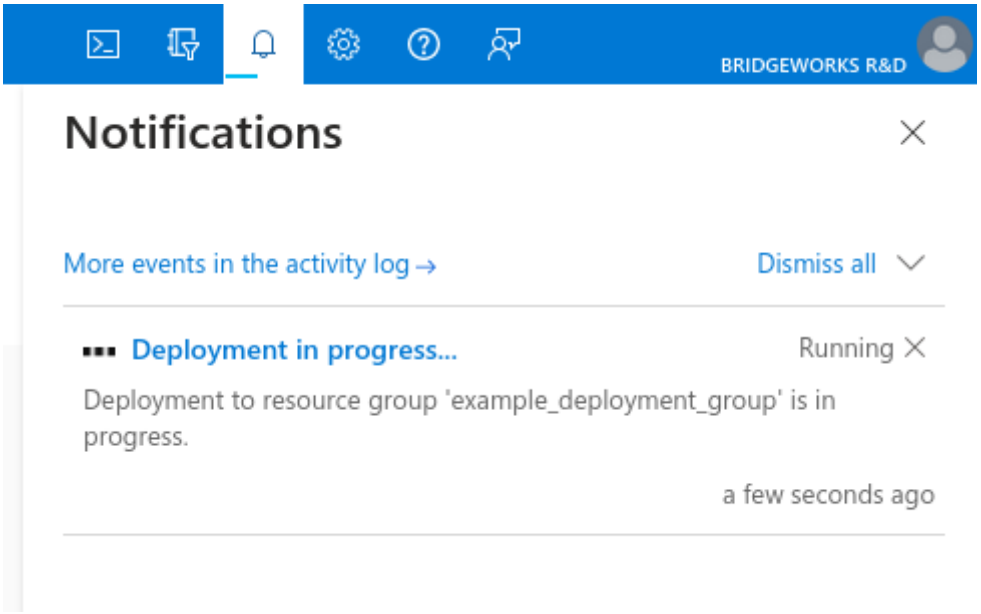
+ Add data disk

Review + create < Previous Next : Tags >

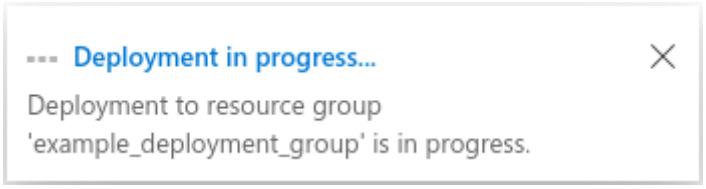
When the settings have been entered, left click the *Create* button at the bottom of the menu.

	Note: The PORTrockIT does not require a high performance storage type. Therefore, *Standard HDD* can be selected.

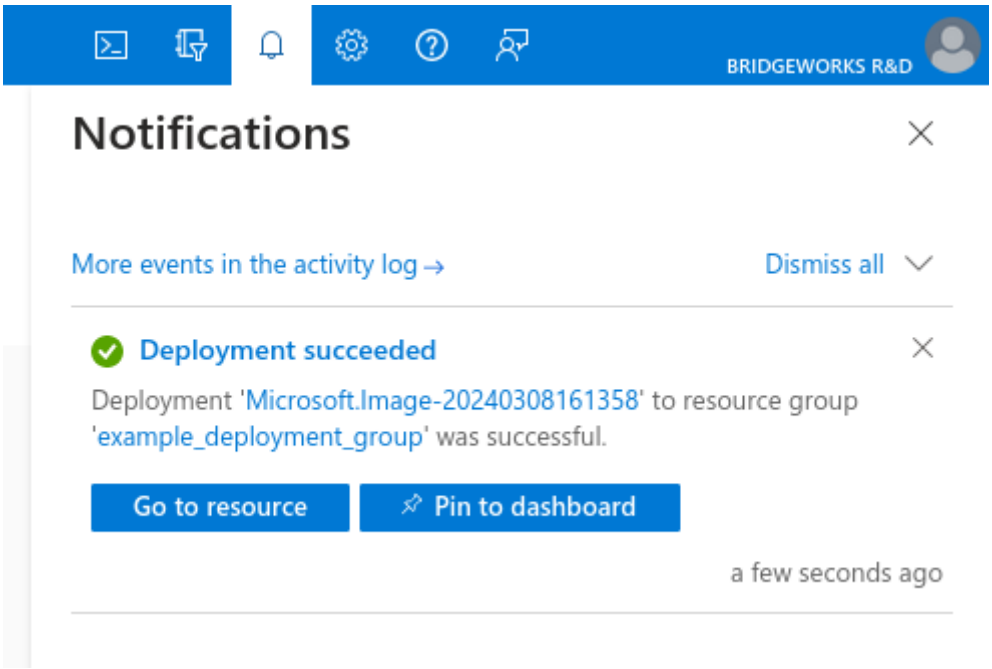
At this stage a notification will appear.



This information can also be found by left clicking on the *Bell* icon at the top of the screen.



Wait for the operation to complete.

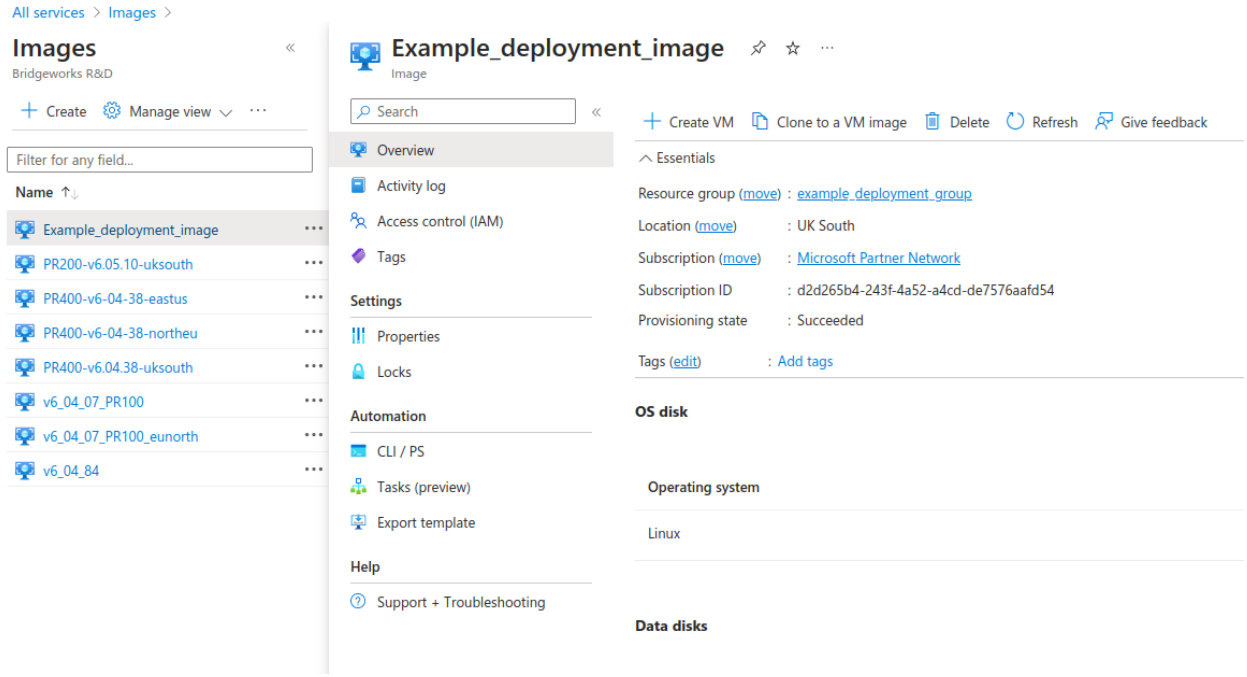


Now *Refresh* the page. Your newly added image should appear.

6 Virtual machine creation

Now that you've created a PORTrockIT image, you can create a virtual machine from it.

Navigate to the *Images* section, then left click on the PORTrockIT's image to get to the overview for that image. In this guide the image is called *example_deployment_image*.



6.1 Basics

Near the top of the page left click the *Create VM* button. This will present you with options for the virtual machine creation. Fill out the options to your liking.

When choosing the size for the virtual machine you will be presented with a large list of available virtual machine sizes. In this example *F8s_v2* is used.

Find the correct size for your PORTrockIT using the tiering table below, and left click to select it.

PORTrockIT tier	Azure machine size
PORTrockIT 100 Series	Standard_F4s_v2
PORTrockIT 200 Series	Standard_F8s_v2
PORTrockIT 400 Series	Standard_F32s_v2

Create a virtual machine ...

Basics | Disks | Networking | Management | Monitoring | Advanced | Tags | Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Microsoft Partner Network

Resource group * : example_deployment_group

Create new

Instance details

Virtual machine name * : example-deployment-vm

Region : (Europe) UK South

Availability options : No infrastructure redundancy required

Security type : Standard

Image * : Example_deployment_image - x64 Gen1

See all images | Configure VM generation

VM architecture : Arm64 / x64

Arm64 is not supported with the selected image.

Run with Azure Spot discount : ☐

Size * : Standard_F4s_v2 - 4 vcpus, 8 GiB memory (£119.79/month)

See all sizes

Enable Hibernation (preview) : ☐

To enable Hibernation, you must register your subscription. Learn more

Administrator account

Authentication type : SSH public key / Password

Azure now automatically generates an SSH key pair for you and allows you to store it for future use. It is a fast, simple, and secure way to connect to your virtual machine.

Username * : azureuser

SSH public key source : Generate new key pair

Key pair name * : example-new-key

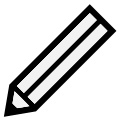
Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * : None / Allow selected ports

Select inbound ports : Select one or more ports

< Previous | Next : Disks > | Review + create

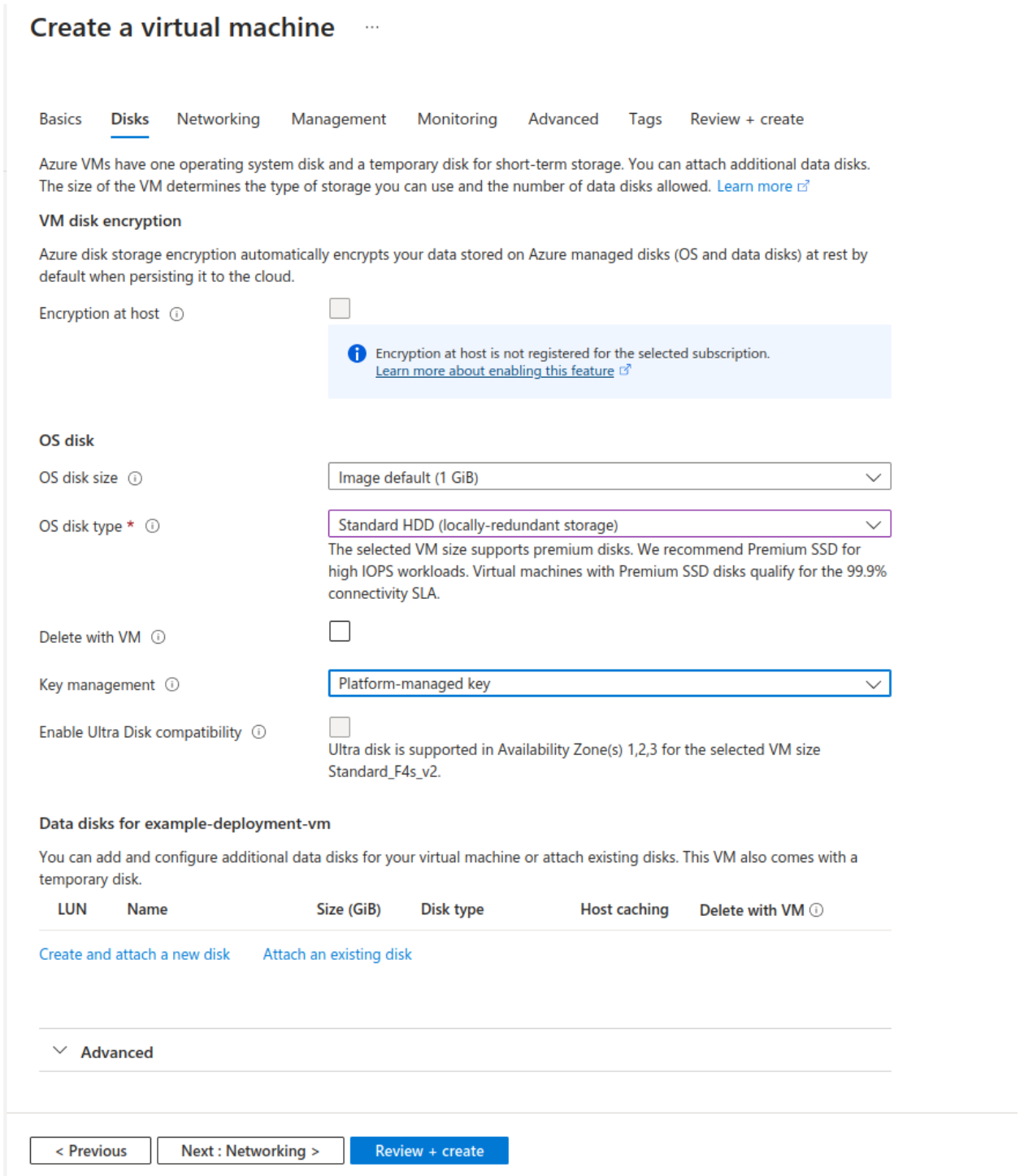


Note: In this instance the PORTrockIT is being set up using an SSH key for access as this is the more secure method. You are able to use a password if preferred. The username entered here will be used when logging into your PORTrockIT.

Left click *Next* to proceed.

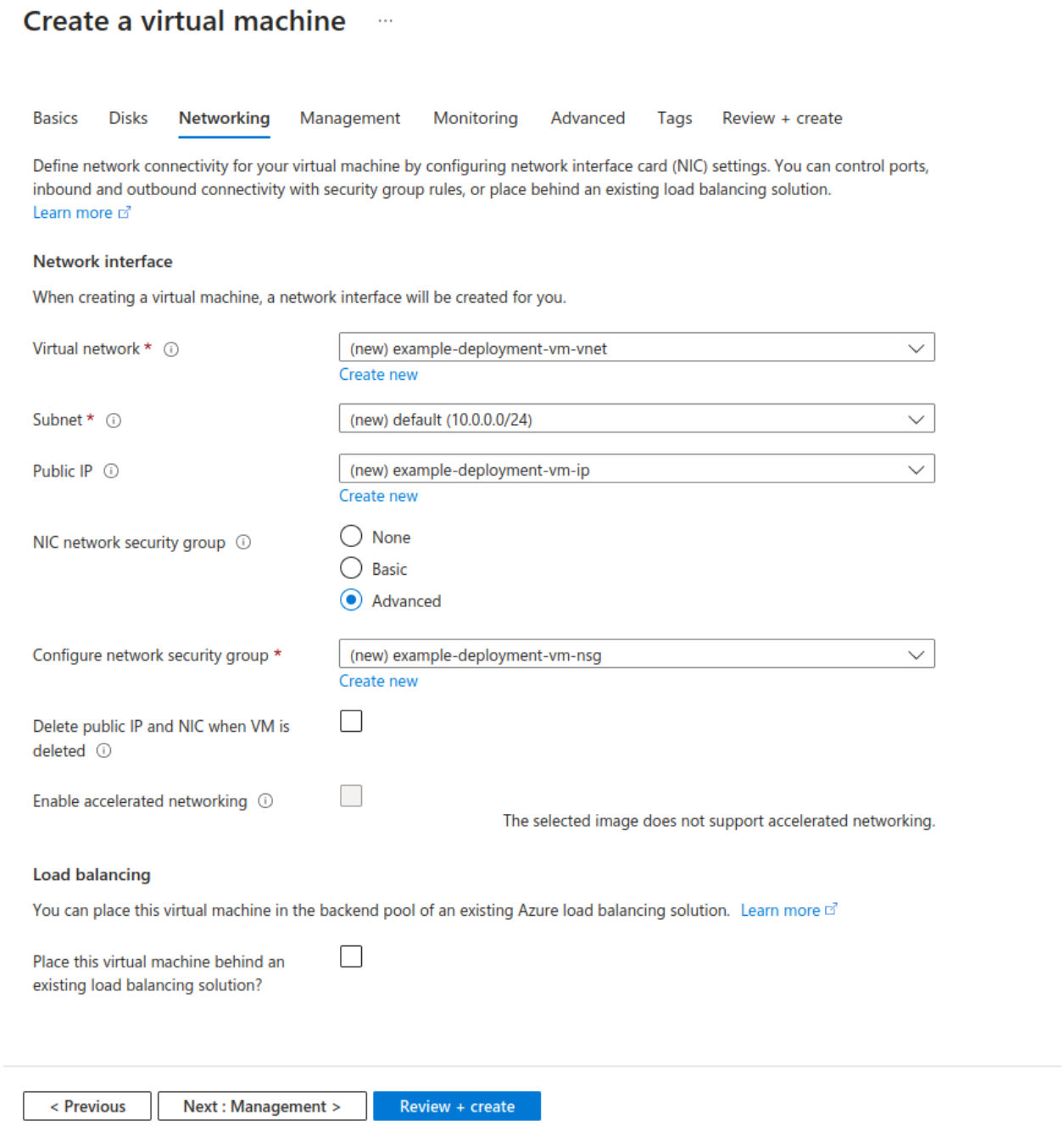
6.2 Disks

Select *Standard HDD* for the Disk Type.You do not need to configure additional data disks to deploy your PORTrockIT.

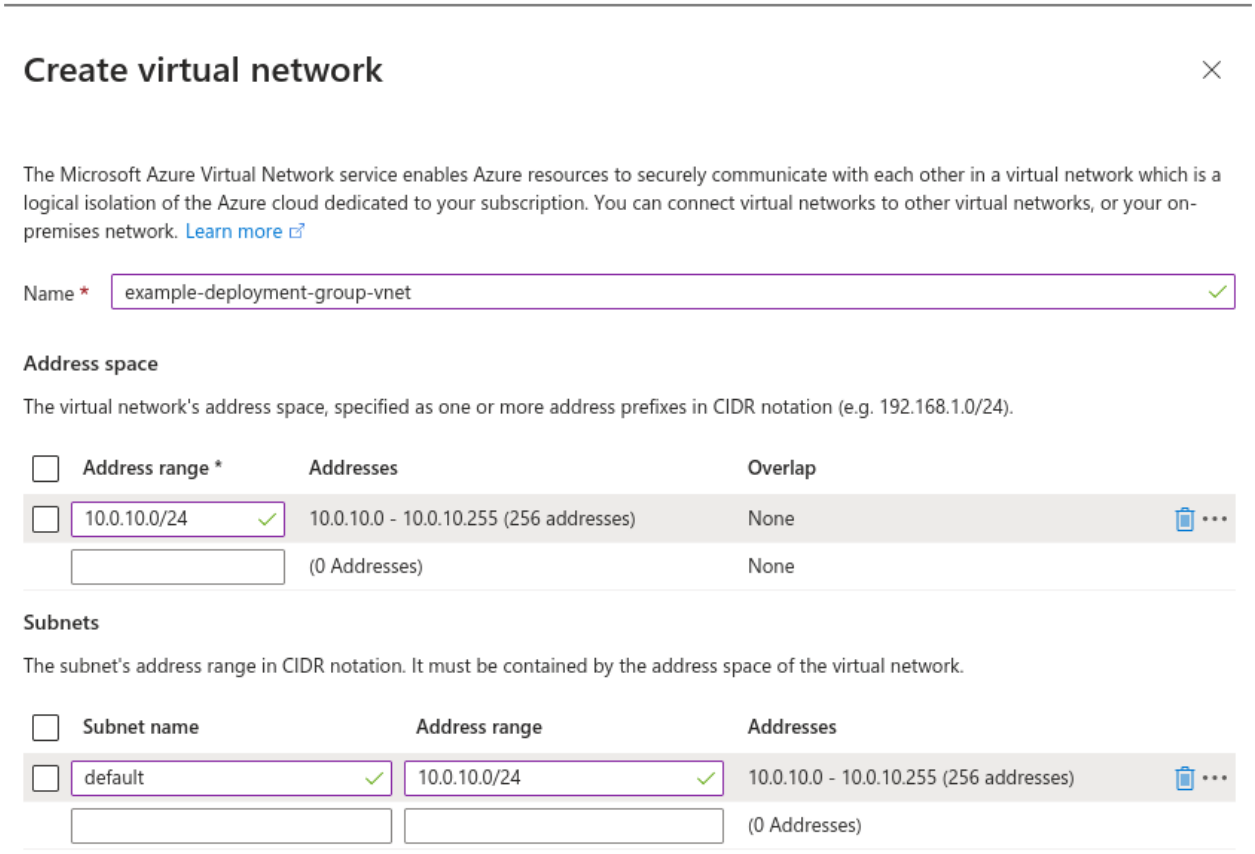


Left click *Next* to proceed.

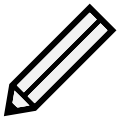
6.3 Networking



In this example a new virtual network is being generated. If you have an existing virtual network containing the endpoints you wish to accelerate then use that one instead. To edit settings for this new virtual network, left click on the *Create new* link beneath the *Virtual network* input box.



In the *Create virtual network* section on the right, fill in the values as required then left click on the *OK* button to continue.

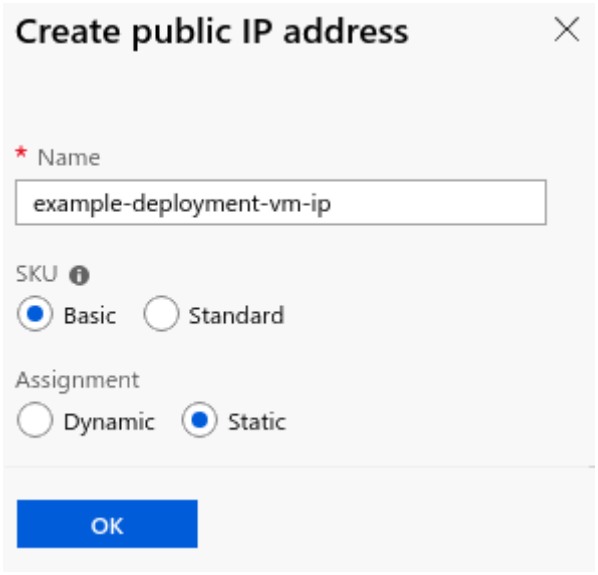


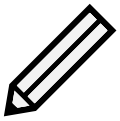
Note: The subnet entry will automatically change when you add the new settings for the new virtual network. If you have attached an existing virtual network then you may need to adjust the subnet manually.

6.3.1 Public IP address

A new public IP address is set to be created by default. To change the IP address settings, left click on the *Create new* link beneath the *IP address* input box.

In this example the *Assignment* setting has been changed. This means that the external IP address of the PORTrockIT won't change like it would with the *Dynamic* setting.



	Note: Setting a *Static* IP address in the *Assignment* is advisable, though there is additional billing with Azure to do so. A dynamic IP address is likely to change every time a deallocated virtual machine is started back up. This would then result in needing to reconnect Nodes, and possibly adjusting firewalls to allow the new public IP address to connect.

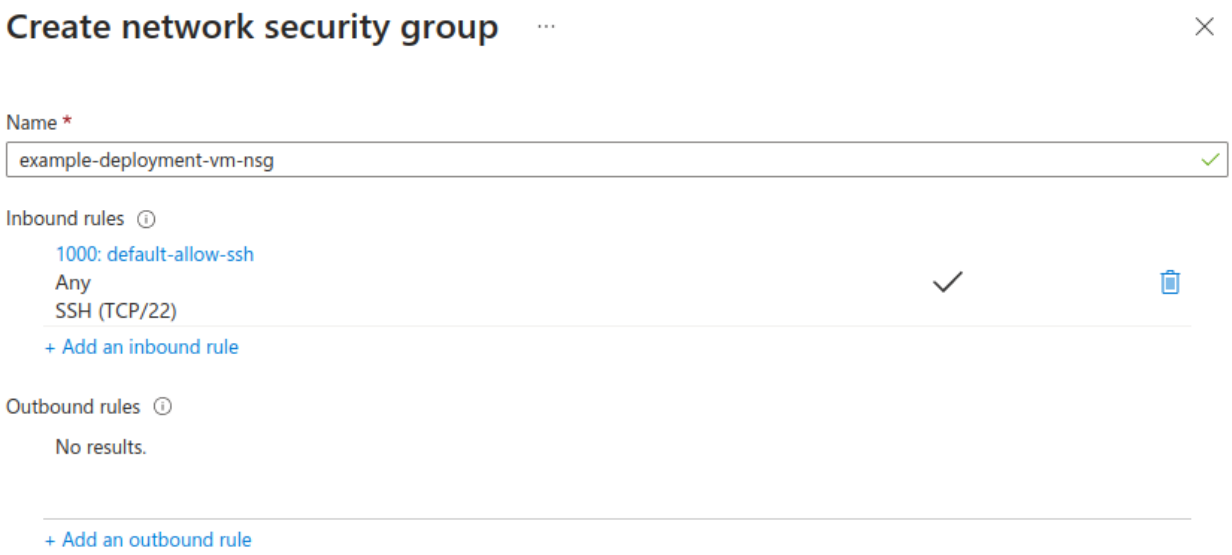
If you have adjusted the settings in the *Create public IP address* panel then left click on the *OK* button in that section.

6.3.2 Network Security Group

The PORTrockIT will require that the *Network Security Group* is set to *Advanced*. This is to allow custom inbound rules for later set up of connections to external Bridgeworks Nodes.

A new network security group will be created by default. If you have an existing group to use, then attach that instead. To edit the settings for the new network security group, left click on the *Create new* link beneath the *Network security group* input box.

In this example setup the connections into the PORTrockIT are going to be restricted to only allow connections from your current IP address.



Left click on *Add an inbound rule* in the *Create network security group* section.

In the right hand menu section enter the information to allow external access from your local machine.

Add inbound security rule

example-deployment-vm-nsg

Source

IP Addresses

Source IP addresses/CIDR ranges *

203.0.113.0/32

Source port ranges *

*

Destination

Any

Service

Custom

Destination port ranges *

*

Protocol

- (•) Any
- ( ) TCP
- ( ) UDP
- ( ) ICMP

Action

- (•) Allow
- ( ) Deny

Priority *

100

Name *

My_Source_IP

Description

Add | Cancel

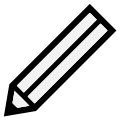
Give feedback

In this example the *Source* drop-down is set to the *IP Addresses* option. The external facing IP address being used to access Azure is entered. The */32* prefix length means only this exact IP address is allowed to connect to this virtual machine.

The *Destination port ranges* entry is also changed. The initial value of *8080* has been removed. Entries have been added for all the entries in the following table. These are the minimum required to access the PORTrockIT and to allow it to connect to an external Node.

Important: These settings only need to be applied to the *Destination port ranges* entry. The *Source port ranges* entry can be left as “*”, which allows the source port to be any number.

Protocol/Port	Description	Recommended Source
TCP 22	SSH, used for accessing the Command Line Interface (CLI).	”My IP”
TCP 80	HTTP, used for accessing the web interface (unencrypted).	”My IP”
TCP 443	HTTPS, used for accessing the web interface (encrypted).	”My IP”
TCP 16665	PORTrockIT main transfer port.	Public facing IP address of the WAN interface of your partner PORTrockIT Node.
UDP 4500	IPsec, used for encrypting PORTrockIT traffic.	Public facing IP address of the WAN interface of your partner PORTrockIT Node.
UDP 500	IPsec used for encrypting PORTrockIT traffic.	Public facing IP address of the WAN interface of your partner PORTrockIT Node.



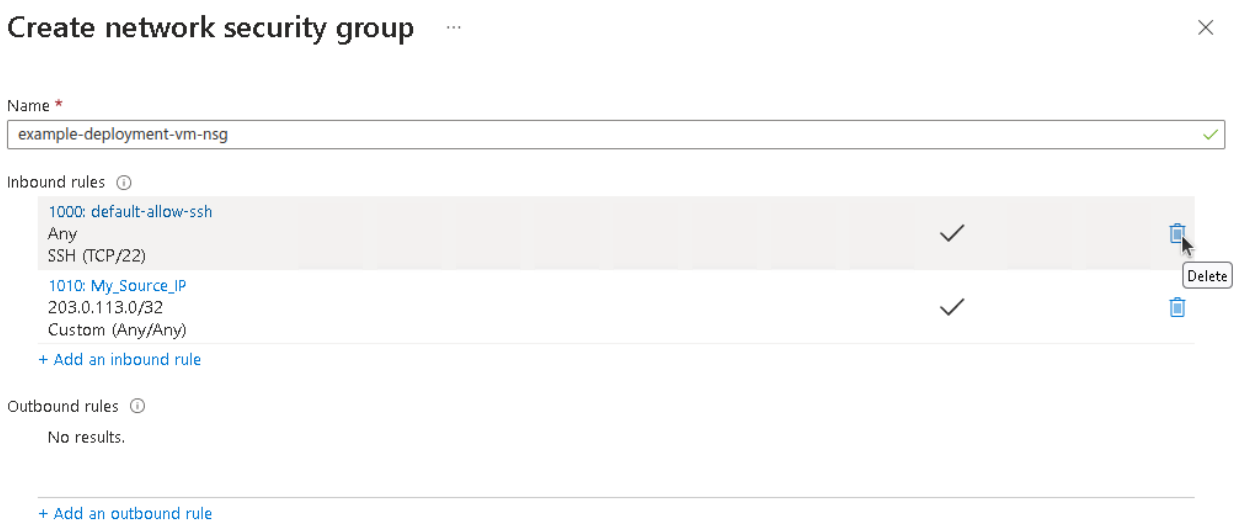
Note: The “*” character can be used to specify that all ports will be available. Use with caution.

All other settings are left in their default state.

Left click on *Add* when you have completed your inbound rule.

Once the rules to allow access to the PORTrockIT have been added the default rule to allow access to TCP port 22 from any IP address can be removed.

Left click on the three dots next to the entry for the rule you wish to remove, then left click on *Remove*.



	Note: The inbound rules will need to be updated if any other IP address will need to access this virtual machine. Inbound rules can be updated in real-time through the Azure platform.

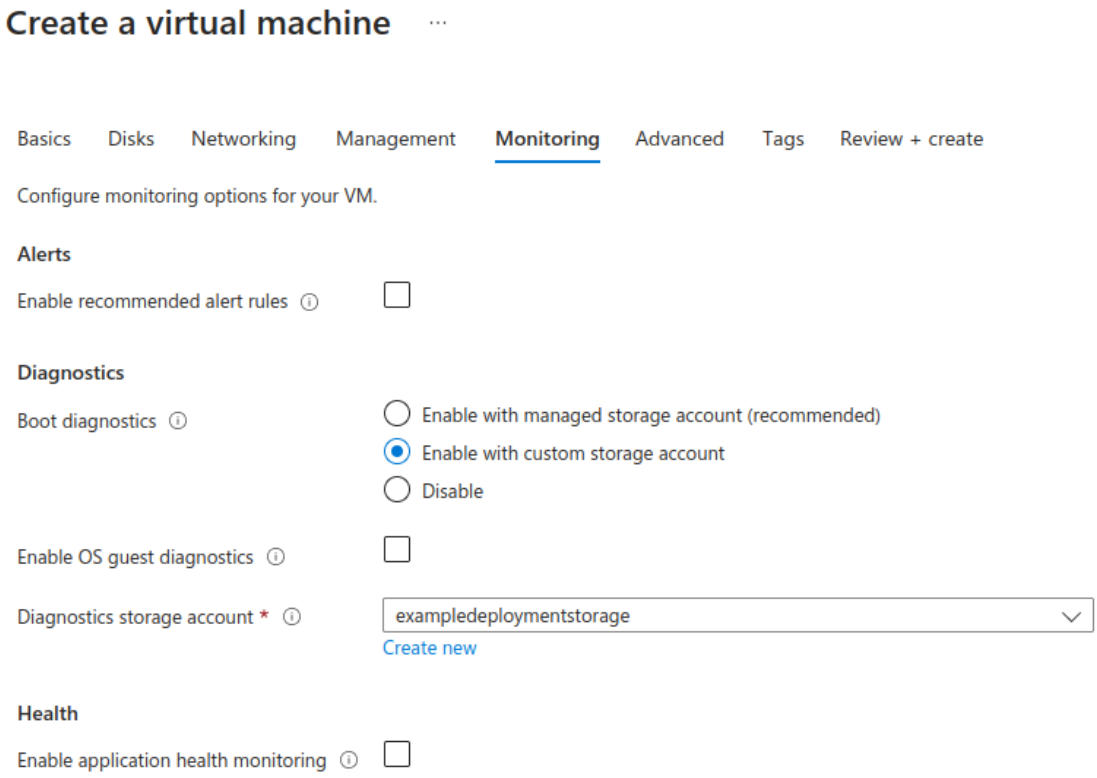
Left click on the *OK* button in the *Create network security group* section once all your inbound rules have been set.

If you do not know the IP address of the partner PORTrockIT Node at this stage, please use Appendix A: Network security to guide you on how to add the security group rules at a later point.

6.3.3 Diagnostics

By default the virtual machine creation will create a new storage account just to store the diagnostics blob for this machine.

In this example the setting has been changed to use the example storage account created earlier. The diagnostics will still create a new container inside that storage account, so it will be distinguishable from the existing data.



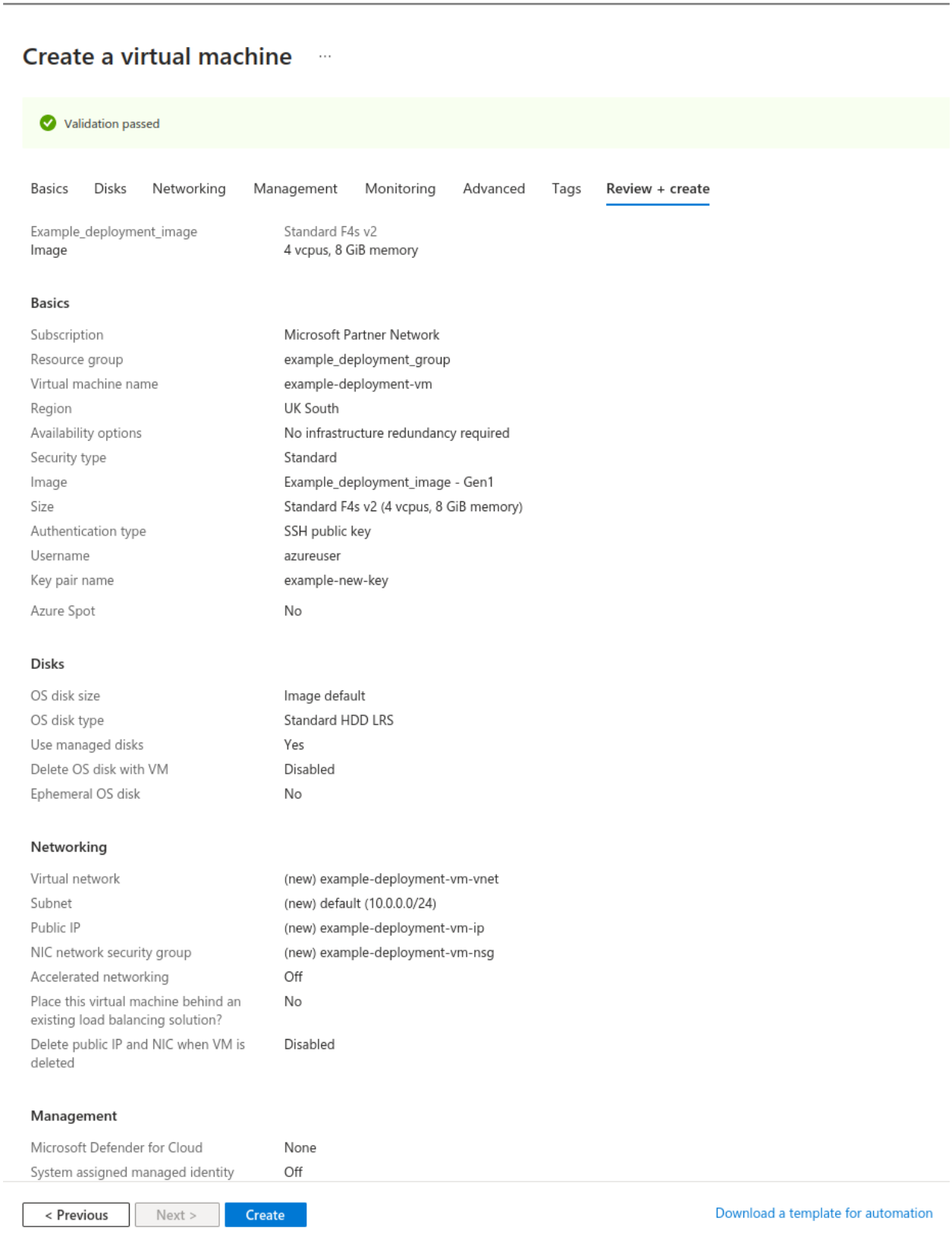
All settings should have been set.

Left click *OK* at the bottom of the *Settings* section to proceed.

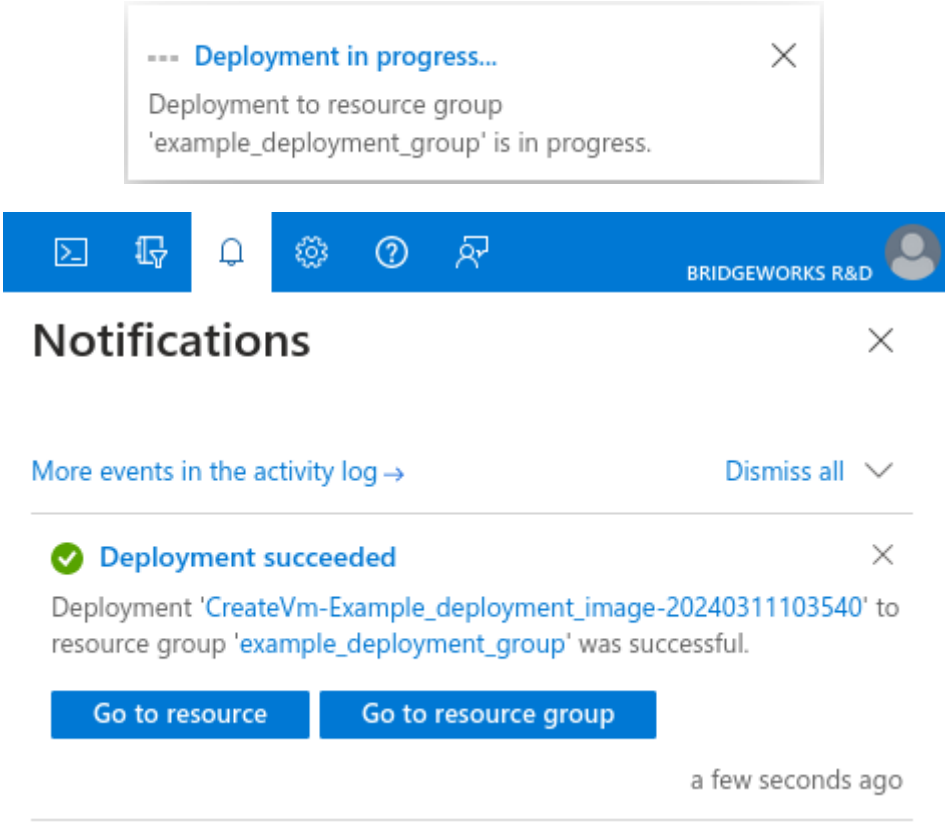
6.4 Summary

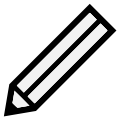
The Azure platform will validate the settings for the virtual machine.

Once this has occurred, left click on *OK* at the bottom to deploy the virtual machine.



A notification will appear.

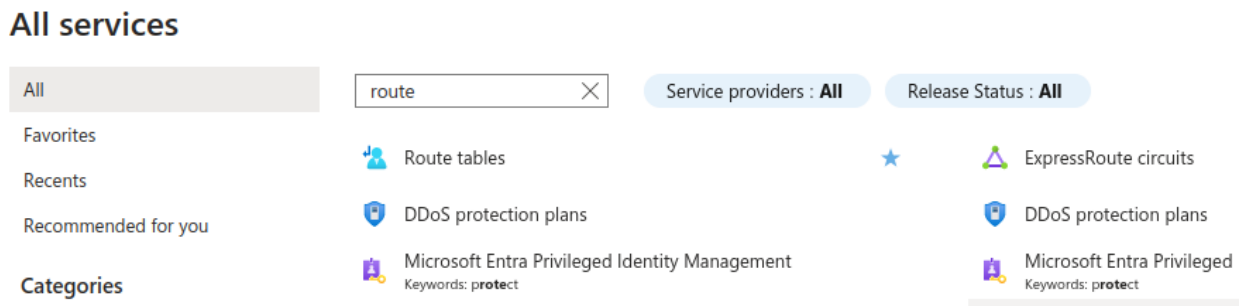


	Note: When this operation completes the virtual machine will be deployed in a running state. If you do not intend to set up the system then it is advisable to power off the virtual machine.

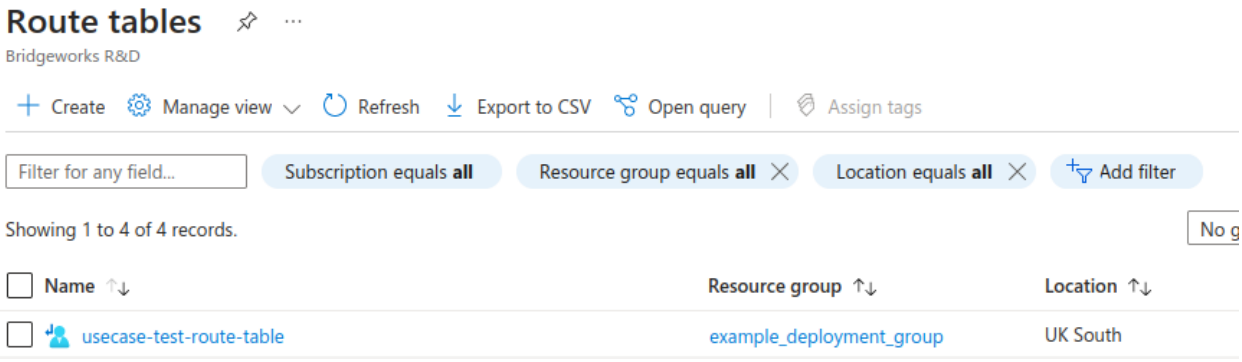
7 Route tables

If you are deploying your PORTrockIT Node and require to run in the “Logical-In-Path” mode, then please follow this section to allow traffic to be passed to the PORTrockIT for acceleration. If you are configuring the PORTrockIT to be used in “Out-of-Path” mode then please proceed to Chapter 8: Accessing the GUI. For help with deciding on modes of operation please consult the Bridgeworks “PORTrockIT Topology Overview” document.

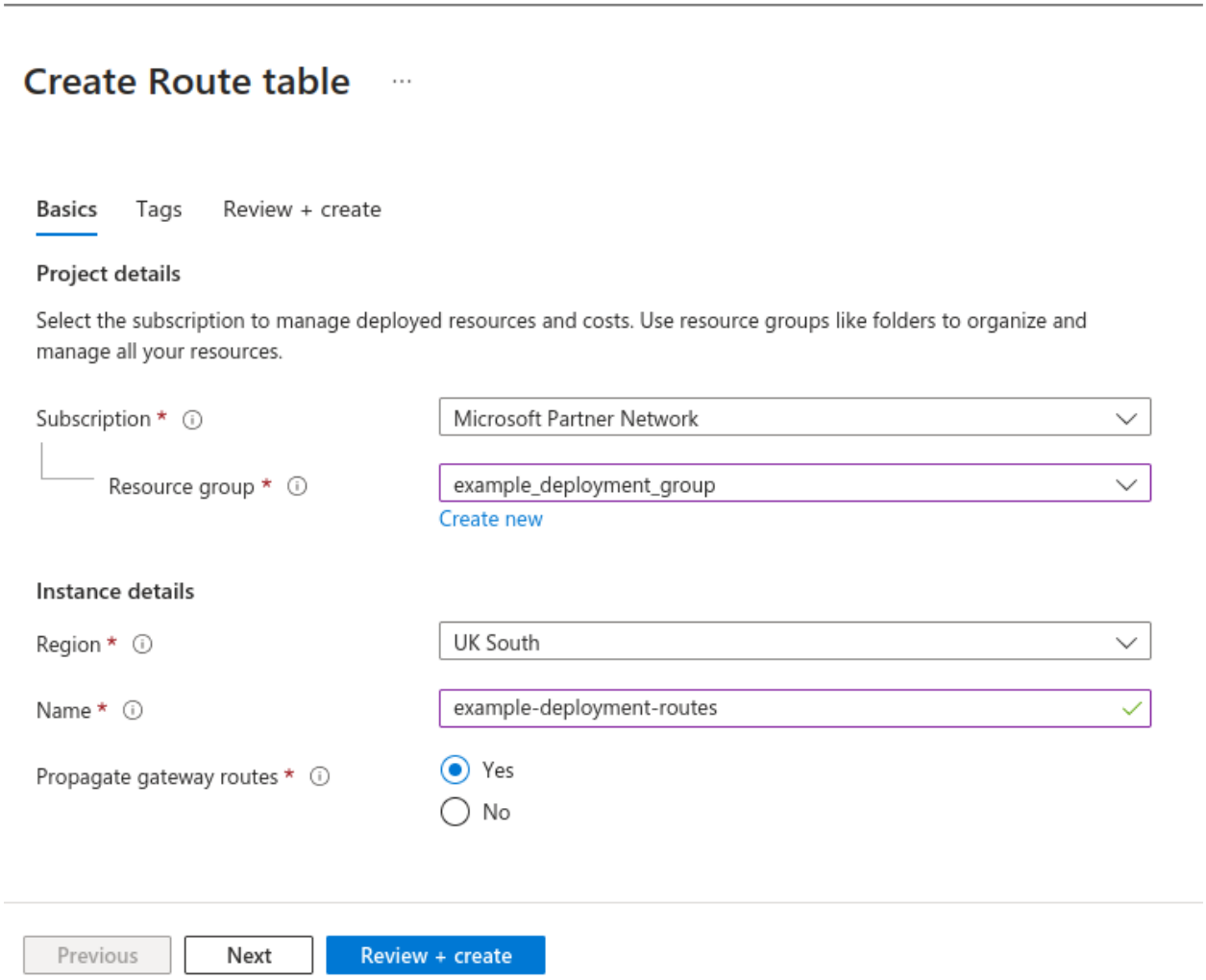
Navigate to the *Route tables* section. This can be achieved by navigating to *All services* on the left side of the page; either look for the *Route tables* link, or type it into the filter.



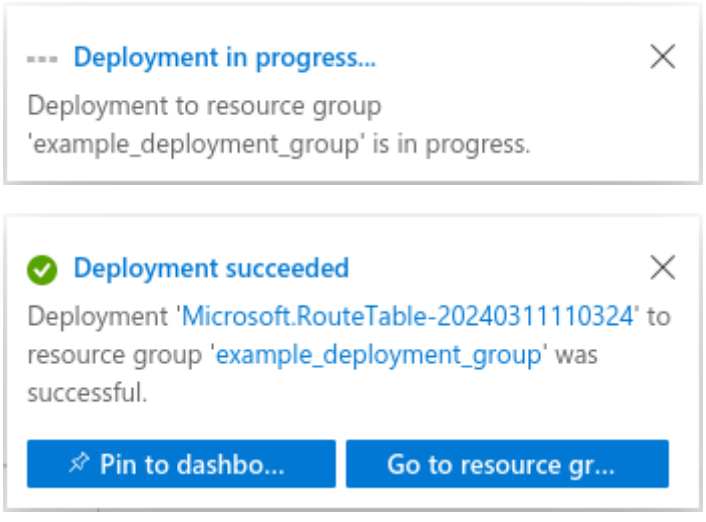
In the *Route tables* section you will be presented with all the route tables that are accessible from this Azure account. Left click the *Create* button near the top of the page.



A *Create route table* section will appear. Fill out the sections with your desired names and location. In this example the route table is set to use the existing resource group created earlier in this guide, and will be in *UK South* as all other resources used in this example are in that region.

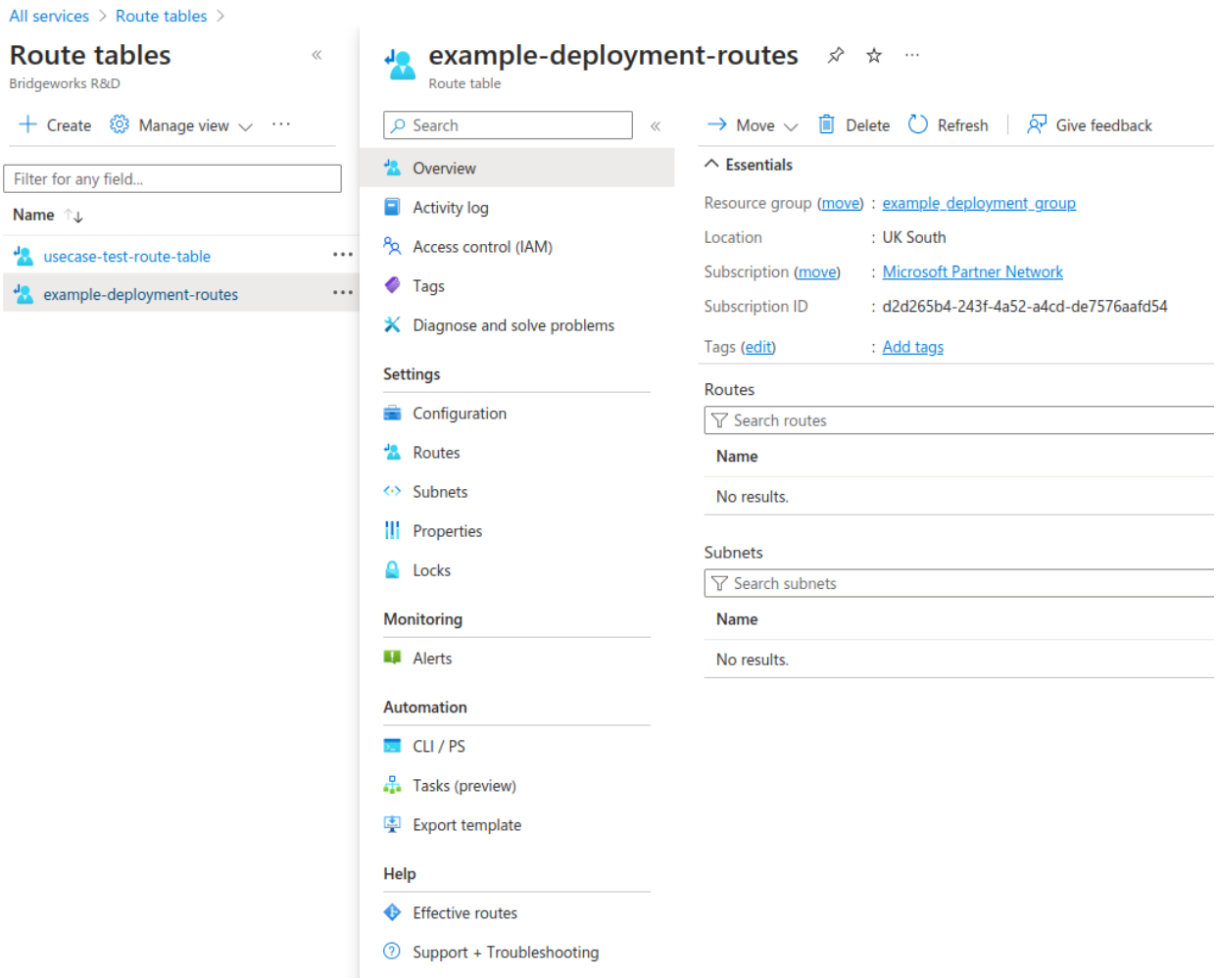


Left click on *Review + Create*, review information and left click on *Create*. At this stage a notification will appear. Wait for the success notification to follow.

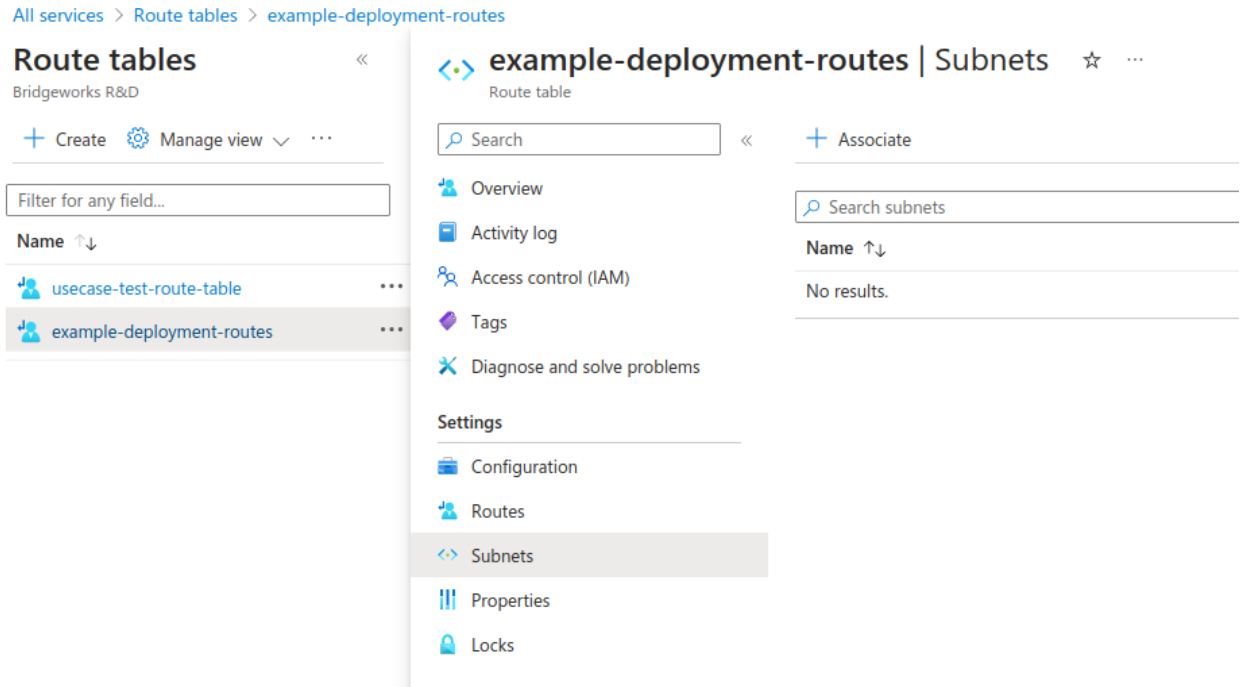


Refresh the *Route tables* section to see your newly added route table.

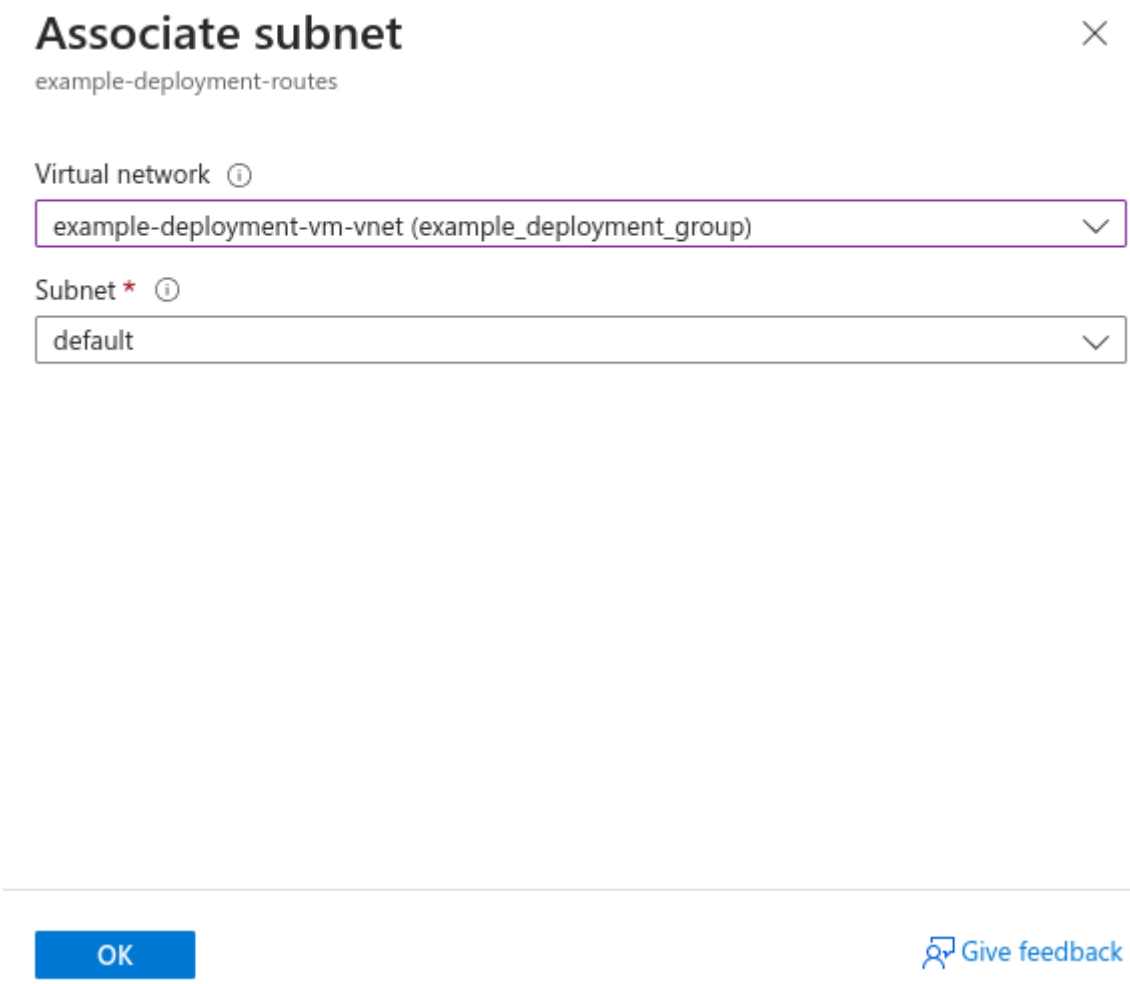
Left click on the route table to see the overview for it.



First you must associate a subnet to this route table. Left click the *Subnets* option in the *Settings* category.

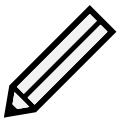


Left click the *Associate* button along the top of the *Subnets* section.

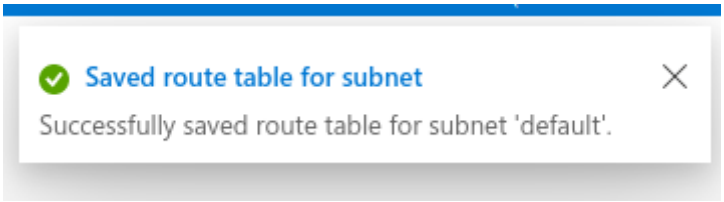


Left click on the *Virtual network* list, and then select the virtual network you are using for your PORTrockIT. Left click on the *Subnet* list and select the subnet your PORTrockIT is using.

Left click on *OK* at the bottom to proceed.

	Note: If you created a new virtual network during the virtual machine creation then there should only be the one subnet. Otherwise you will need to navigate to your virtual machine to find the virtual network and subnet that are being used.

Wait for the notification that the route table has been successfully saved.

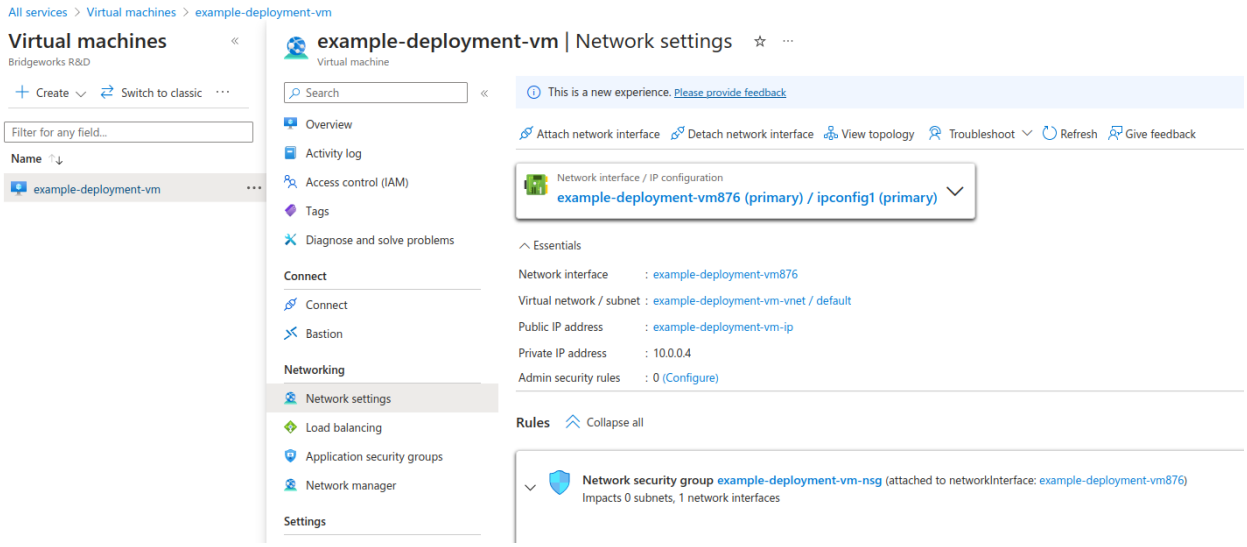


The next step is to add a routing rule for this subnet that will take all traffic destined for the other Node and pass it to the PORTrockIT virtual machine.

To complete this step you need to know the private IP address of the PORTrockIT.

Navigate to the PORTrockIT virtual machine through the *Virtual machines* section, which is accessible from the *All services* section.

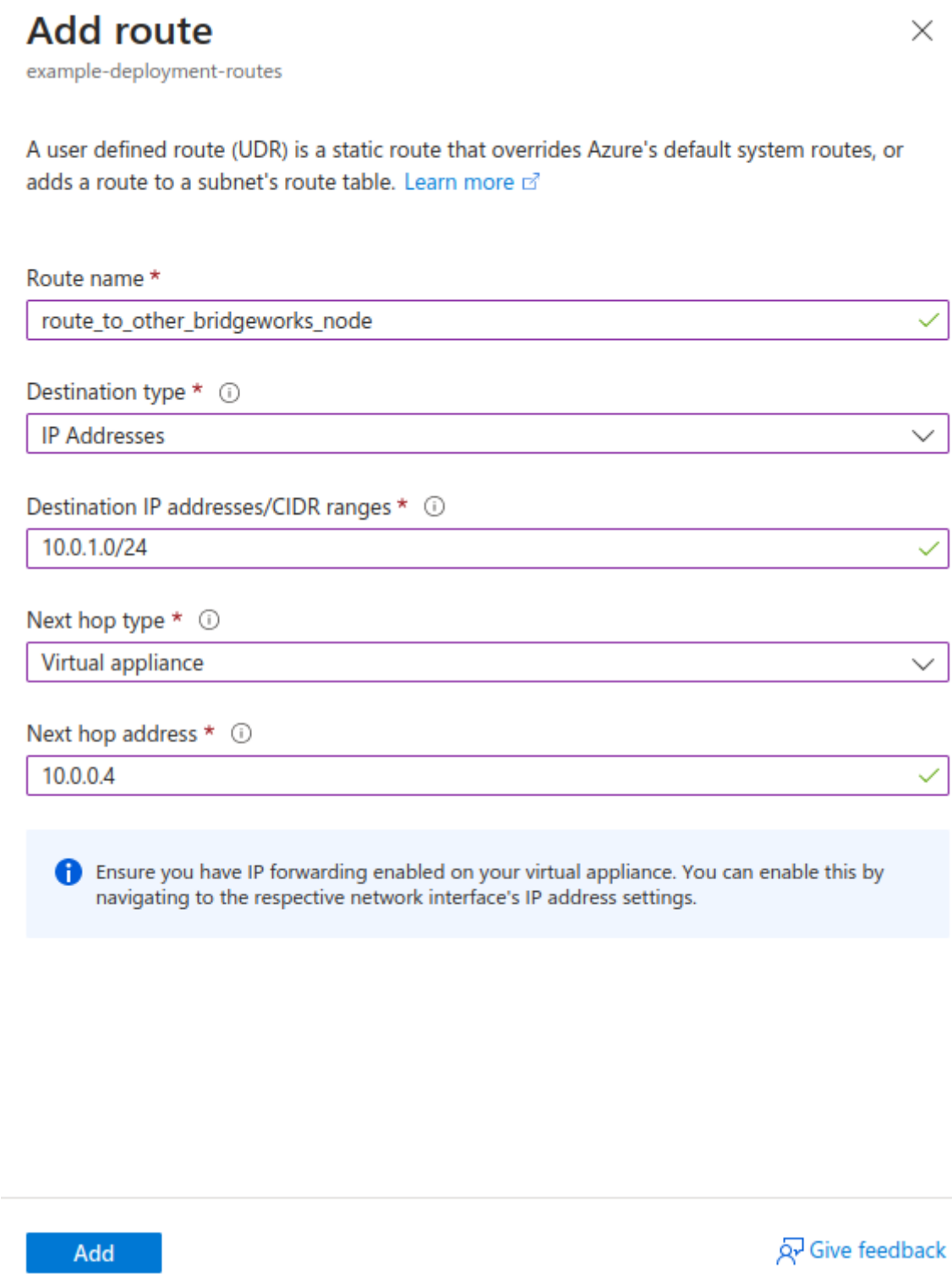
Left click on the PORTrockIT, and then left click the *Networking* section in the *Settings* category. From this view you can see the *Private IP* entry located near the middle of the page.



In this example the private IP of your PORTrockIT virtual machine is *10.0.0.4*; this is the value you need for the route.

In the *Route tables* section, left click the route table you have been setting up, then left click *Routes* in the *Settings* category.

Click *Add* near the top of the *Routes* section. This will clear the screen and present just the *Add route* options.



Enter the information needed to pass network traffic destined for the remote side through the PORTrockIT virtual machine.

In this example:

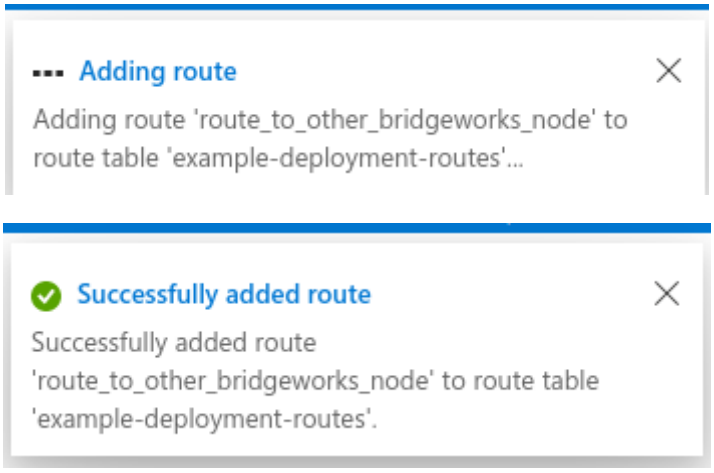
Destination type You want to use the IP Addresses in Azure. The *IP Addresses* selection results in the *Destination IP addresses/CIDR ranges* field appearing.

Destination IP addresses The LAN side of the remote Node. This is the address range for the endpoints you want to be able to connect to through the PORTrockIT connection.

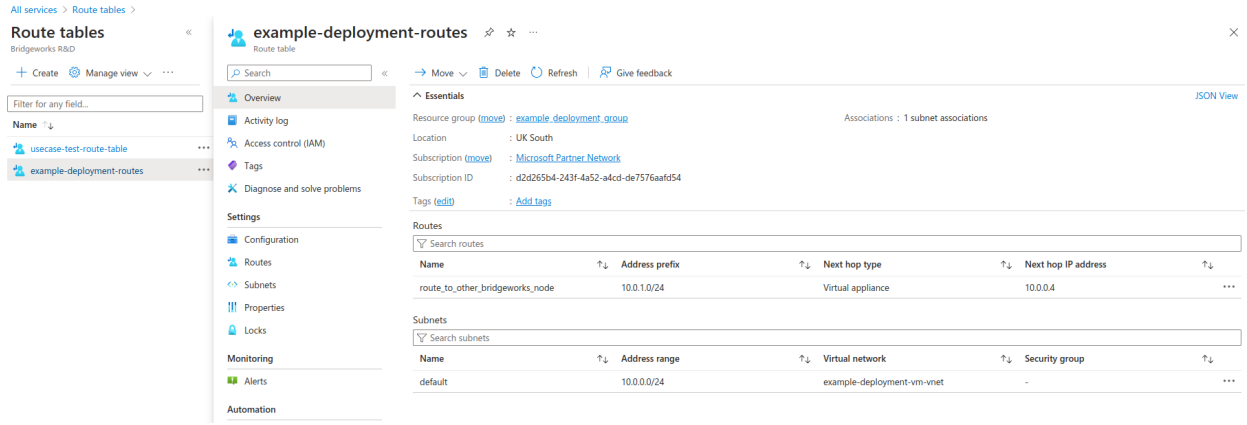
Next hop type You want to use the virtual machine in Azure. The *Virtual Appliance* selection results in the *Next hop address* field appearing.

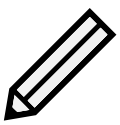
Next hop address The private IP of the PORTrockIT. This is the equivalent of the LAN port on a Node. All network traffic destined for the *Address prefix* IP range will get routed through this IP.

Once all options have been correctly set, left click *OK* to add the route. Wait for the success notification to appear.

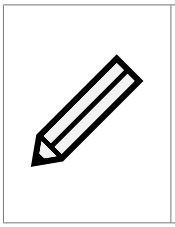


The overview section for your newly set up route table should now show the route to the network address range of the other Node, and the subnet that this routing applies to. In this example the subnet range covers the private IP of the PORTrockIT virtual machine.





Note: The route here will take any network traffic trying to get to any IP on the 10.0.1.0/24 range, and pass it to 10.0.0.4, which is your PORTrockIT. The PORTrockIT will in turn connect to another Node which has a LAN side network running the 10.0.1.0/24 IP range.



Note: The routing rules must cover all the private IP ranges that the PORTrockIT will connect to. In this example if another Node is connected that has an endpoint behind it running an IP of 192.0.2.10, then a new route would need to be added that takes 192.0.2.10/32 (or 192.0.2.0/24 etc.) and passes that through a *Virtual appliance* with a *Next hop address* of 10.0.0.4.

7.1 Network interface

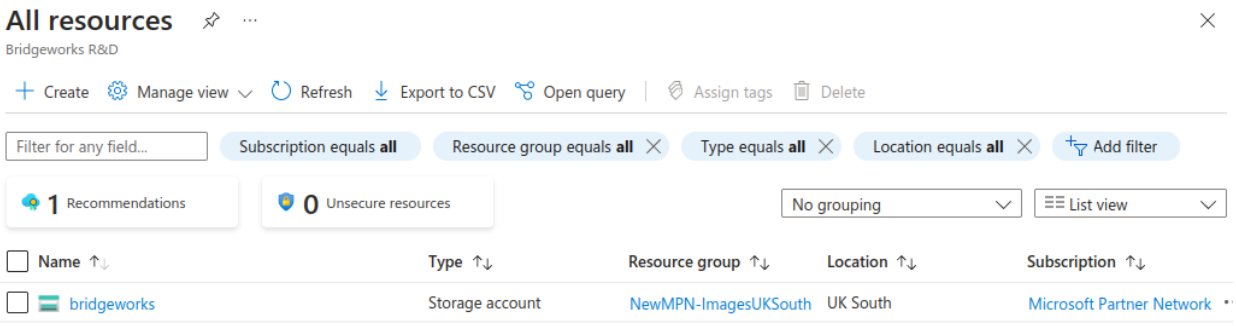
Before this route will work, the network interface on the PORTrockIT Node needs to allow IP forwarding.

When the PORTrockIT virtual machine was deployed, the Azure platform created a network interface for your network connection. See Chapter 6: Virtual machine creation.

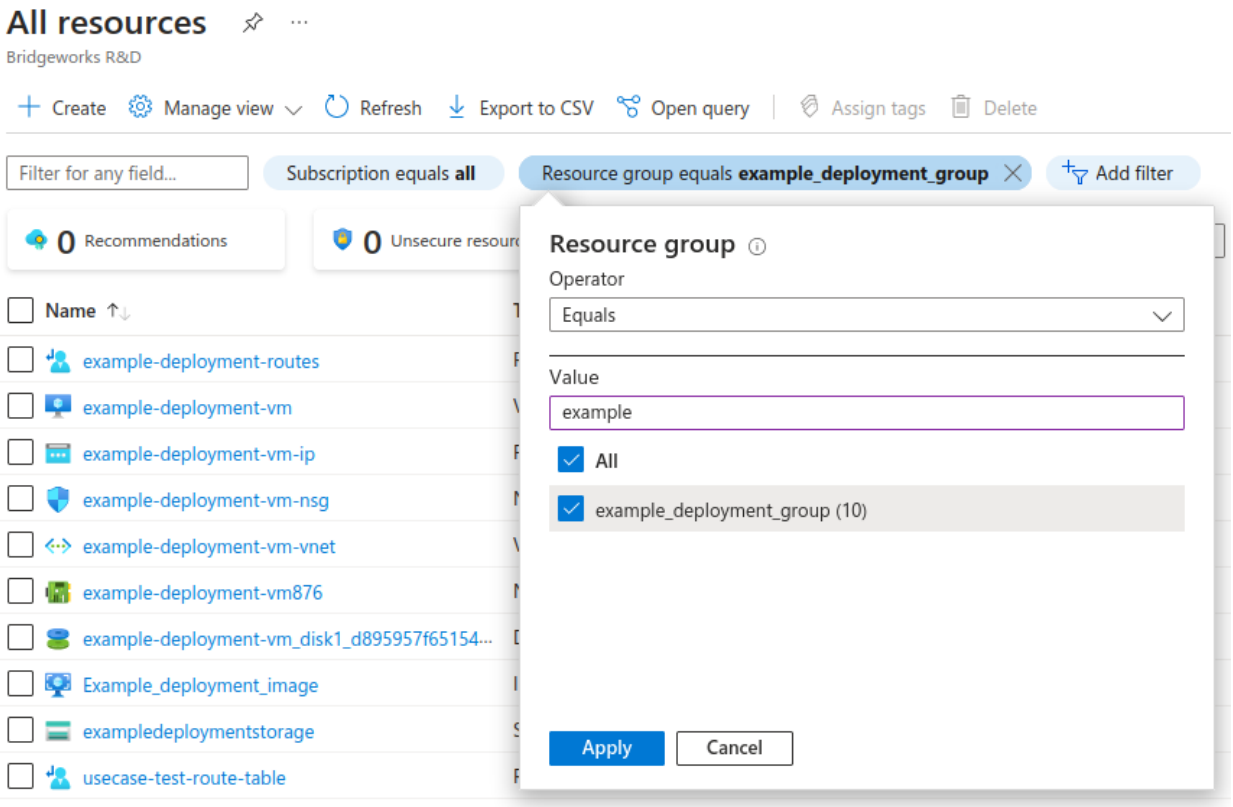
Once you have added a route table and populated it with the route for your Node connection, a dialog box pointed out that you should enable IP forwarding. See Chapter 7: Route tables.

To enable IP forwarding you need to modify settings on the network interface that your PORTrockIT is using.

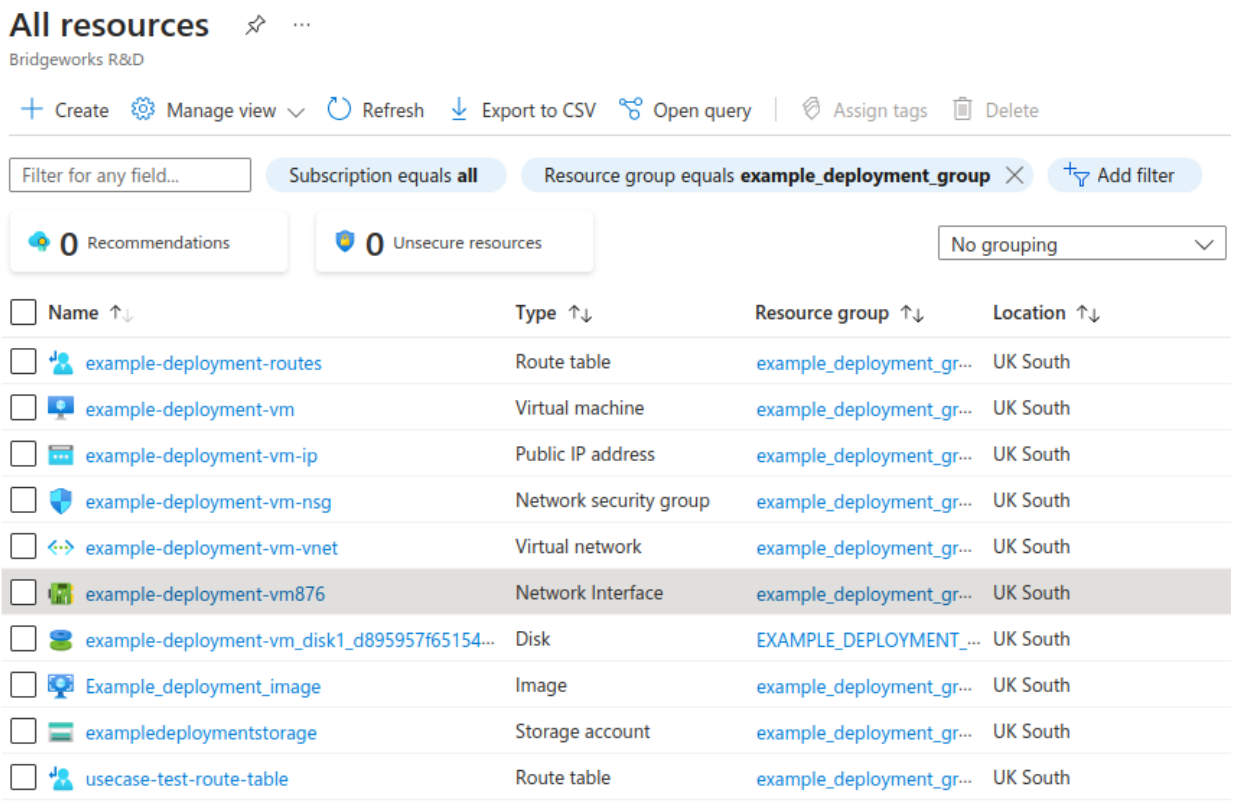
Navigate to *All resources*.



Filter the output to your resource group.

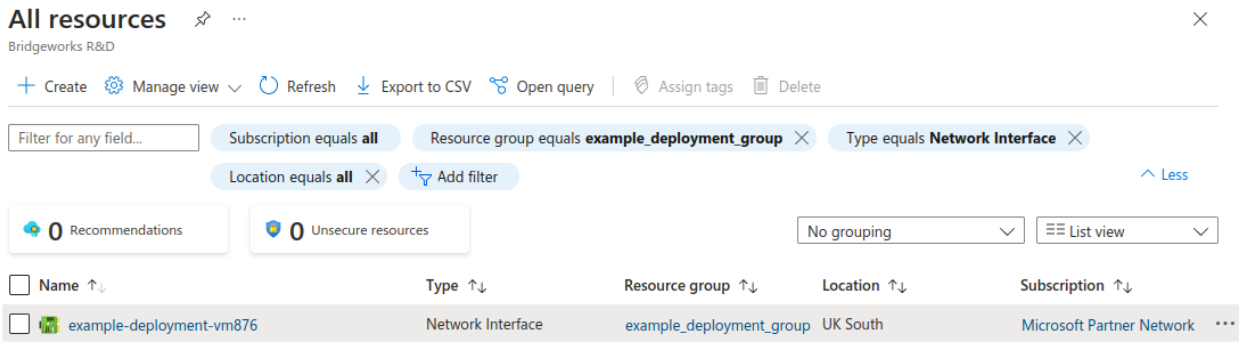


Left click on *Network interface*. In this example it is the only network interface in the resource group and is named *example-deployment-vm876*.

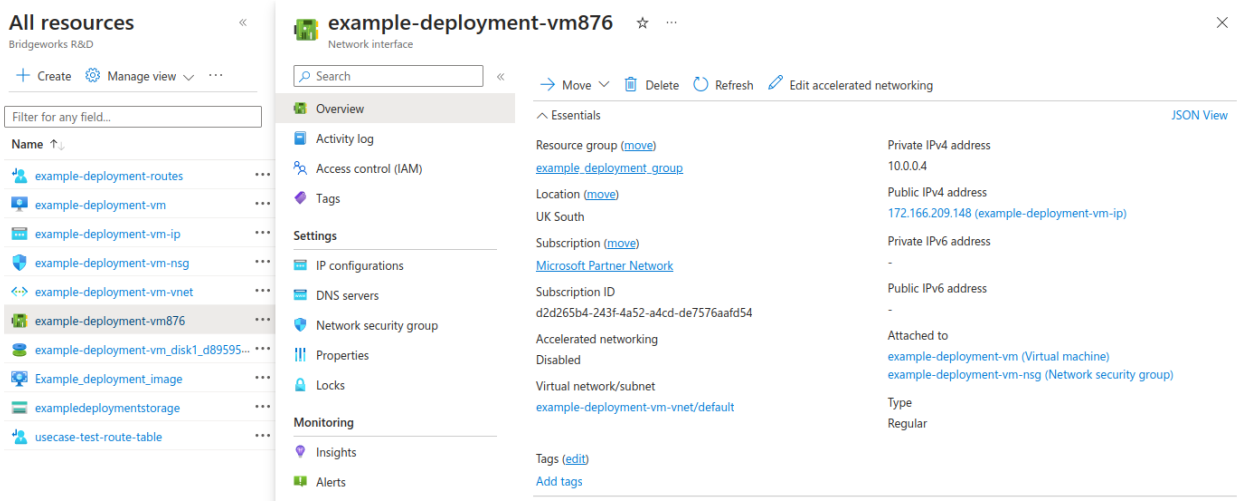


Additionally, you can also filter the results to show only the network interfaces:

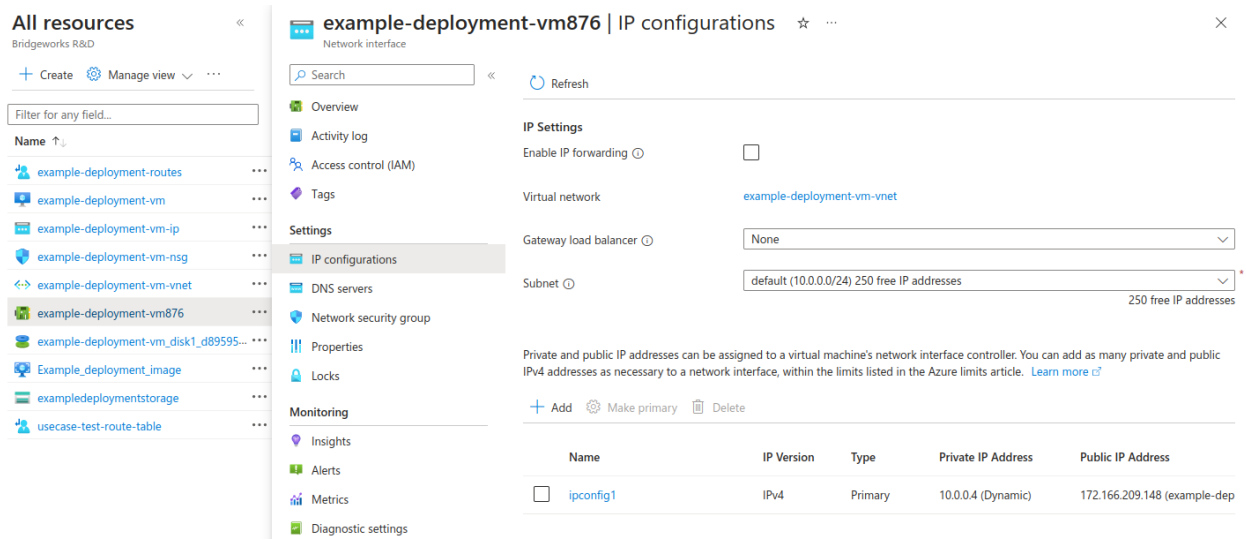
- Select the drop-down labelled *All Types*.
- Deselect the *Select all* box.
- Select the *filter items* bar at the top of the list.
- Type *Network interfaces*.
- Left click the box labelled *Network interfaces*.
- Click out of the drop-down to apply the setting.



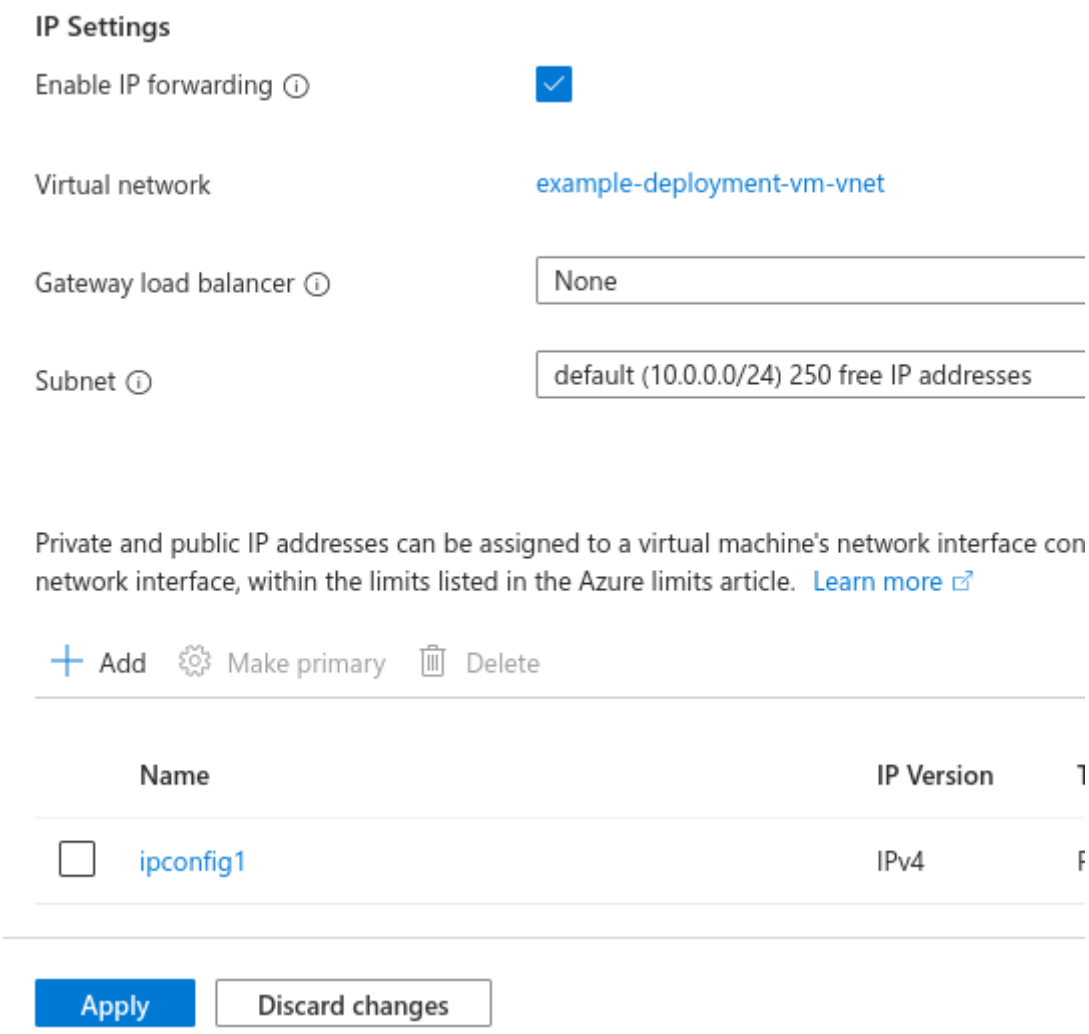
Note: If your group has multiple interfaces then you need to establish which one is connected to your PORTrockIT virtual machine. Left click each network interface and check the overview section; there will be an entry titled *Attached to* from which you can find the network interface attached to your PORTrockIT virtual machine.



In the overview section, left click on the *IP configurations* section in the *Settings* category.

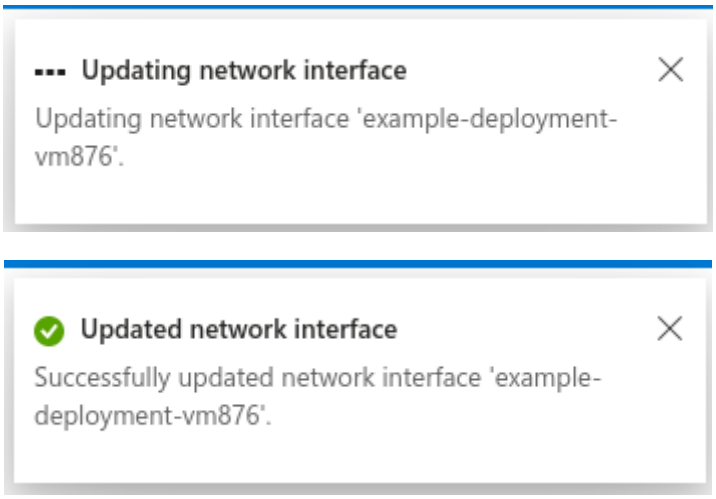


From this view, left click on the toggle for *Enable IP forwarding*.



Left click on *Apply* when you are ready to proceed.

Wait for the success notification.

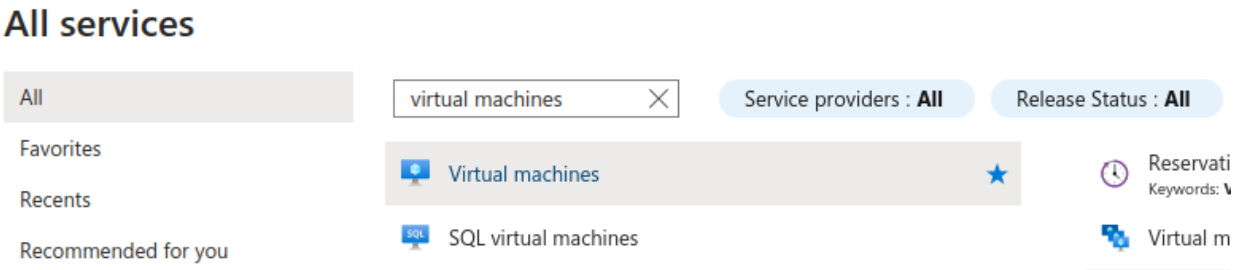

Updating network interface
Updating network interface 'example-deployment-vm876'.
Updated network interface
Successfully updated network interface 'example-deployment-vm876'.

8 Accessing the GUI

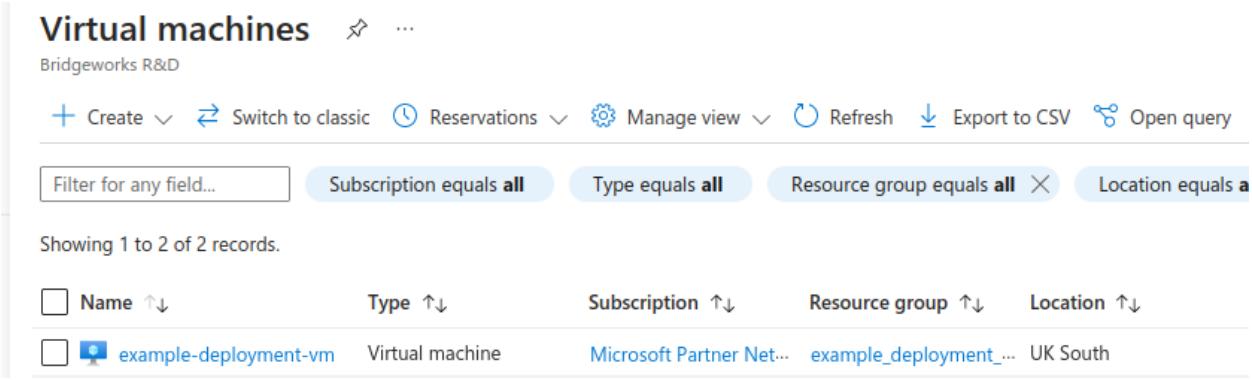
With a PORTrockIT virtual machine running there is now a web GUI available.

To access the GUI you need to know the public IP address for your virtual machine.

Navigate to the virtual machines section. This can be achieved by navigating to *All services* on the left side of the page. In this view either look for *Virtual machines*, or type it into the filter.

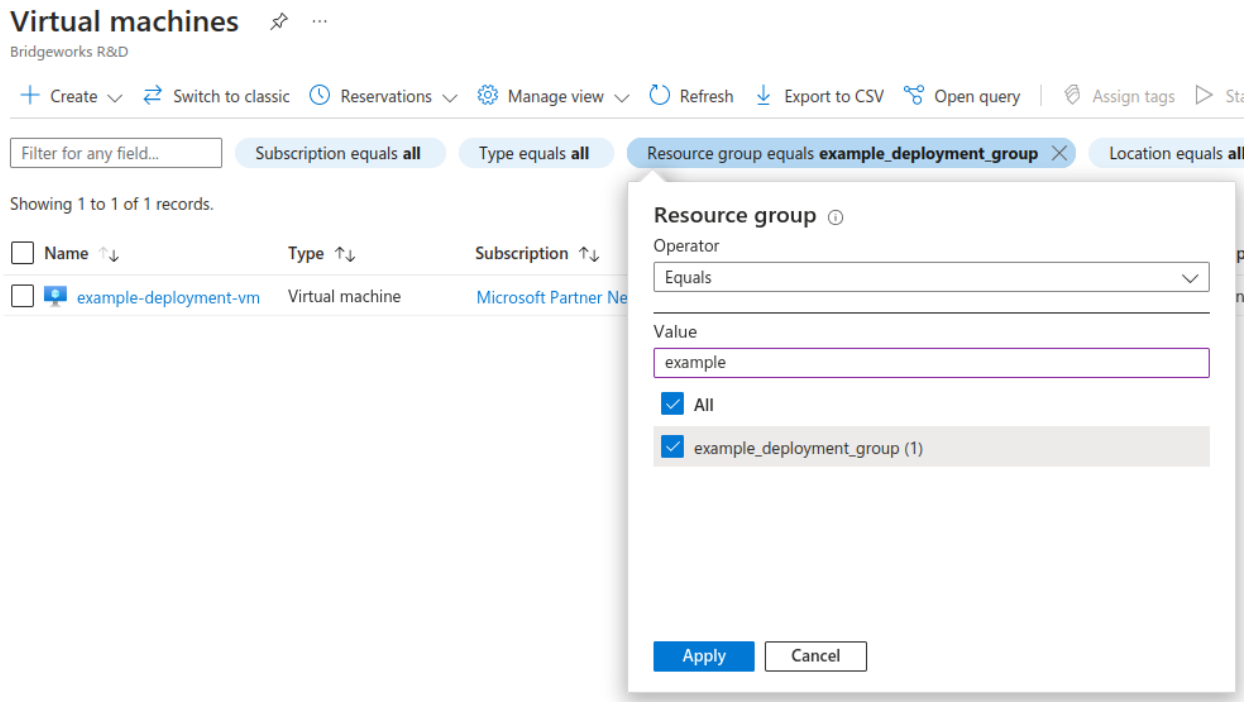


All deployed virtual machines in the account will be displayed in the *Virtual machines* section.

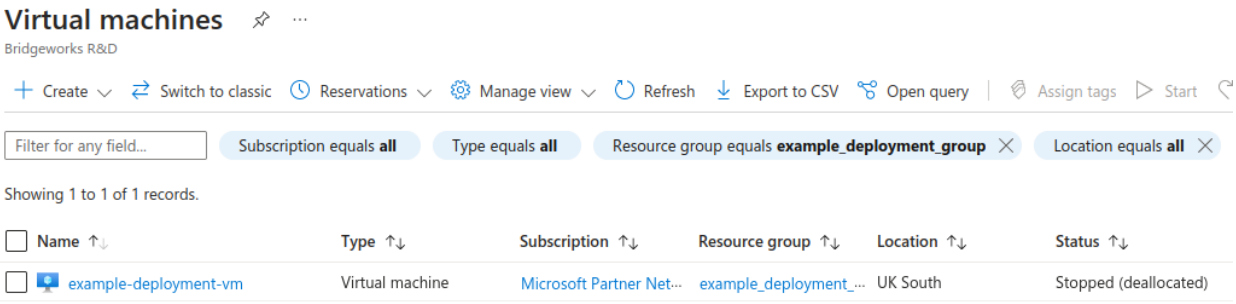


To reduce the list to your intended machine you can use filters. At the top of this list there are drop-down bars to filter the list. In this example the *All resource groups* drop-down will be changed:

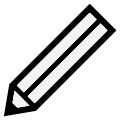
- Left click on *All resource groups* to show the drop-down.
- Left click the ticked *Select all* box to deselect everything.
- Left click on the desired resource group, in this example it is the *example_deployment_group*.
- Left click out from the drop-down to cause the filter to load.

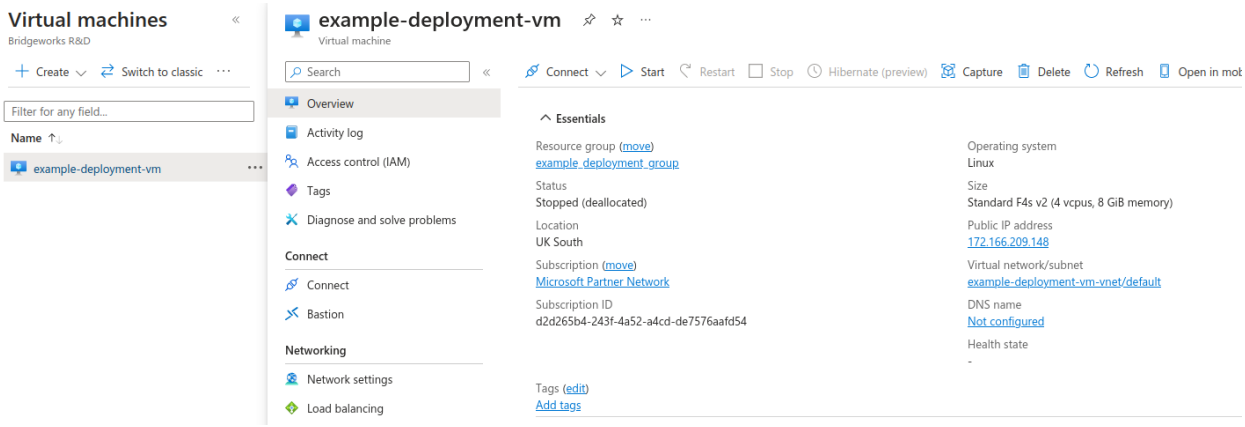


The result will be a filtered list of virtual machines attached to that group.



Left click on the virtual machine you wish to access. The overview for that virtual machine will be shown. On the right there should be a *Public IP address*. Note or copy that address.

	Note: Azure has a quick copy. Left click on the copy symbol that appears when hovering the mouse over the entry.



Open a new tab in your browser and enter the IP address taken from the virtual machine overview to access your PORTrockIT.

You will now be presented with the password prompt page.

Follow the on-screen prompts to set the password and log in.

For further guidance on setting up data acceleration and routing, see the *Policy Routed* guide.

9 Troubleshooting

9.1 Deployment Problems

If a virtual machine has problems deploying, there may be communication issues between the Microsoft Azure Linux Agent (WAAgent) and the Azure Fabric Controller (Microsoft Azure Service), causing the PORTrockIT to have a provisioning failure. If this occurs, the virtual machine's state will be unable to progress from *Creating* in the Azure portal. You will also be unable to log into the GUI with the credentials set up during deployment.

The PORTrockIT needs to be rebooted in order for provisioning to be retried. You can do this by either stopping and restarting the Virtual Machine on the Azure portal or by logging into the GUI and rebooting the node.

To access the GUI, follow the on screen prompt to set a temporary password and log in with the username *admin*. You will then have access to the GUI and can reboot the PORTrockIT from the left hand menu.

Once provisioning succeeds, you will be able to access the PORTrockIT using the credentials set up during creation of the virtual machine. If username and password authentication was used when creating the virtual machine, log in with that username and password. If SSH authentication was used, you will need to set a new password using the on screen prompts and log in using the username chosen during creation.

10 Useful Links

Further documentation and support is available through our website: https://support.4bridgeworks.com/

If your question is not answered in our documentation, please submit a ticket: https://support.4bridgeworks.com/contact/

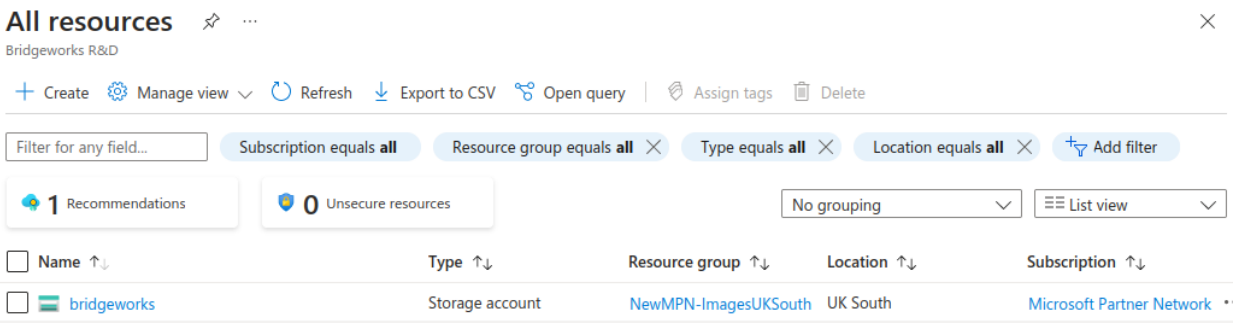
Appendix A: Network security

During virtual machine creation a network security group was created. In this example this group was modified to only allow access from the IP address you are currently connecting to Azure from. See Section 6.3.2: Network Security Group for the initial network security group setup.

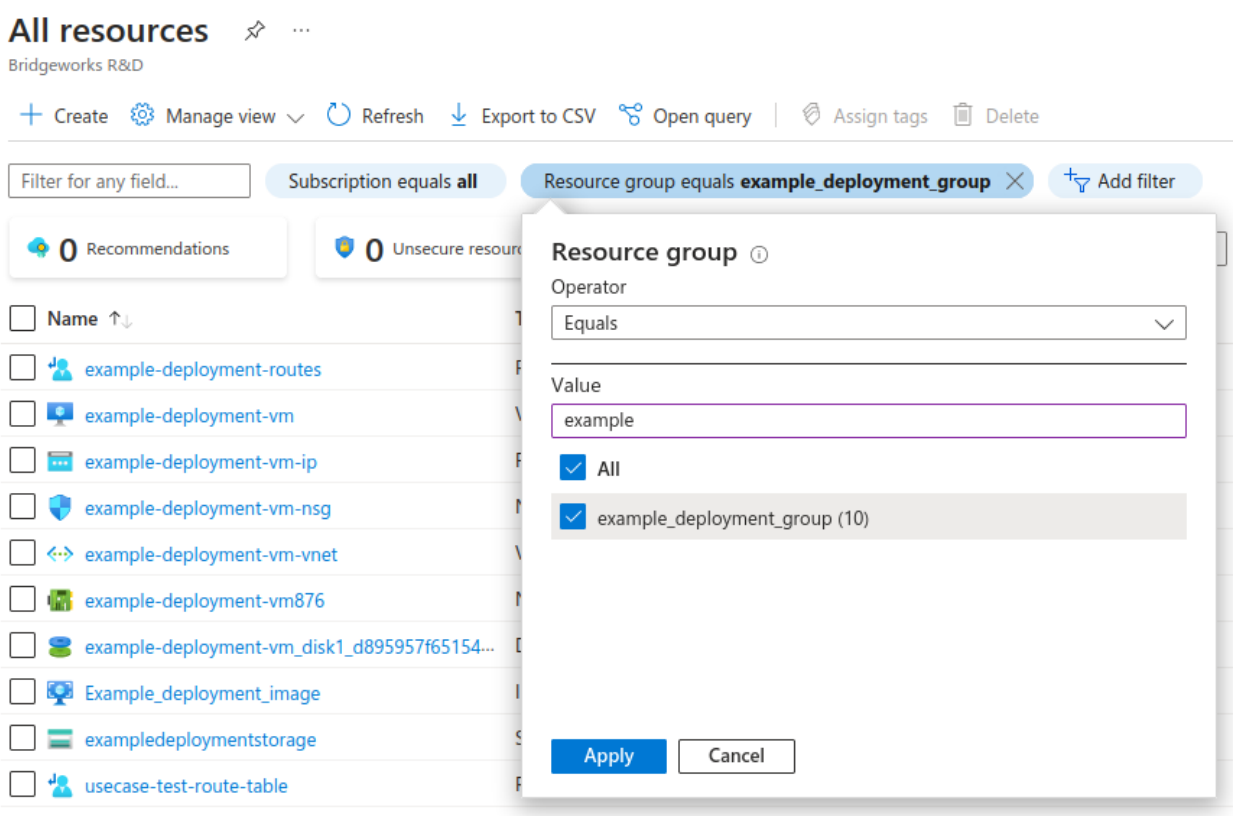
In order to start using a Node connection you need to add another inbound rule to allow the other Node's public IP address.

Navigate to the *Network security group* used by your PORTrockIT virtual machine that has been set up.

This can be achieved by left clicking *All services* on the left of the page and then finding *All resources*.

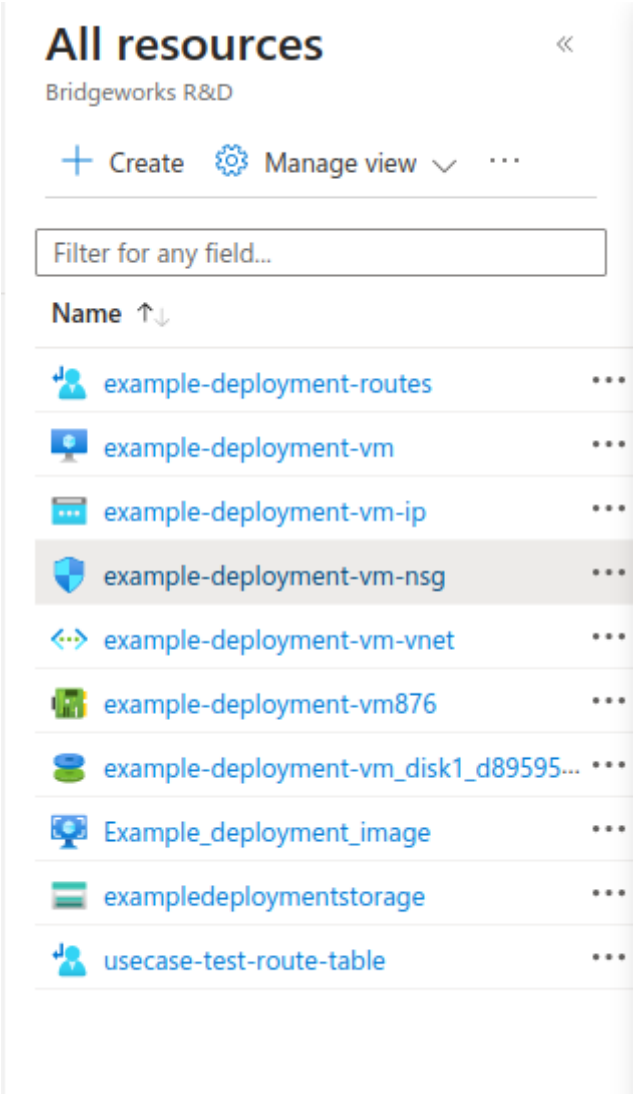


Then filter the *All resource groups* to use the your group.

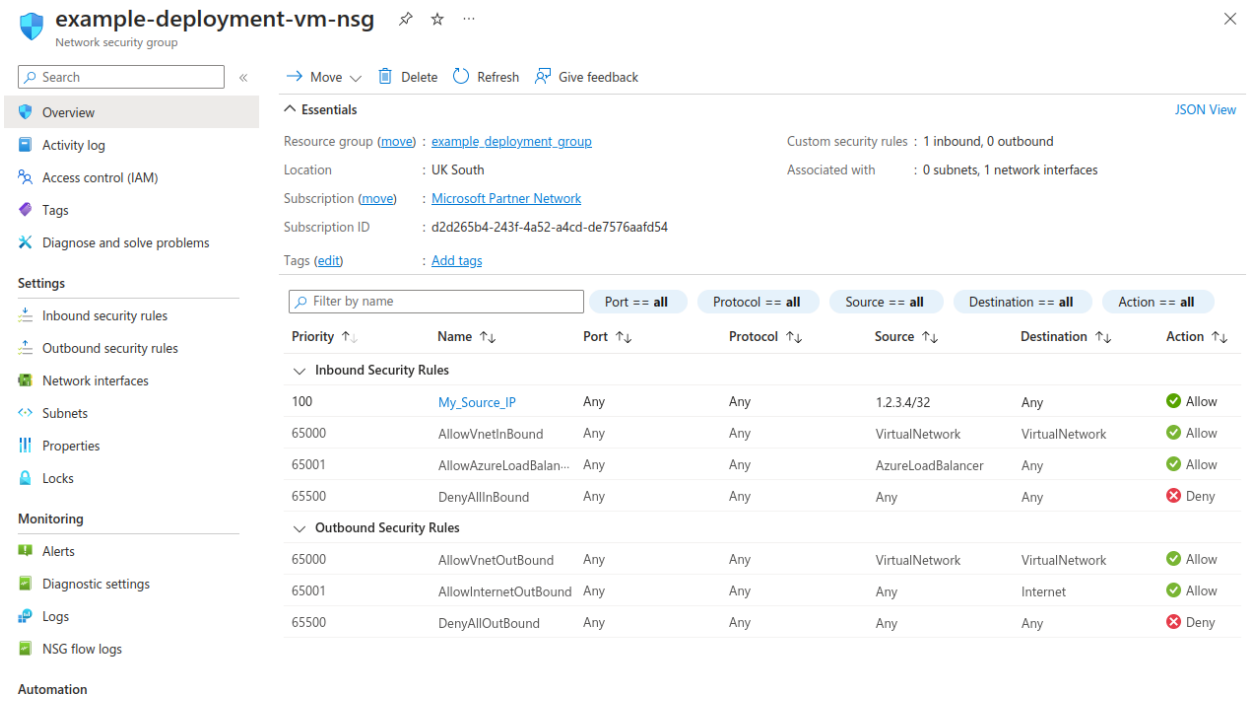


Once in your resource group look for the *Network security group*. In this example it is named *example-deployment-vm-nsg*. Left click on the *Network security group*.

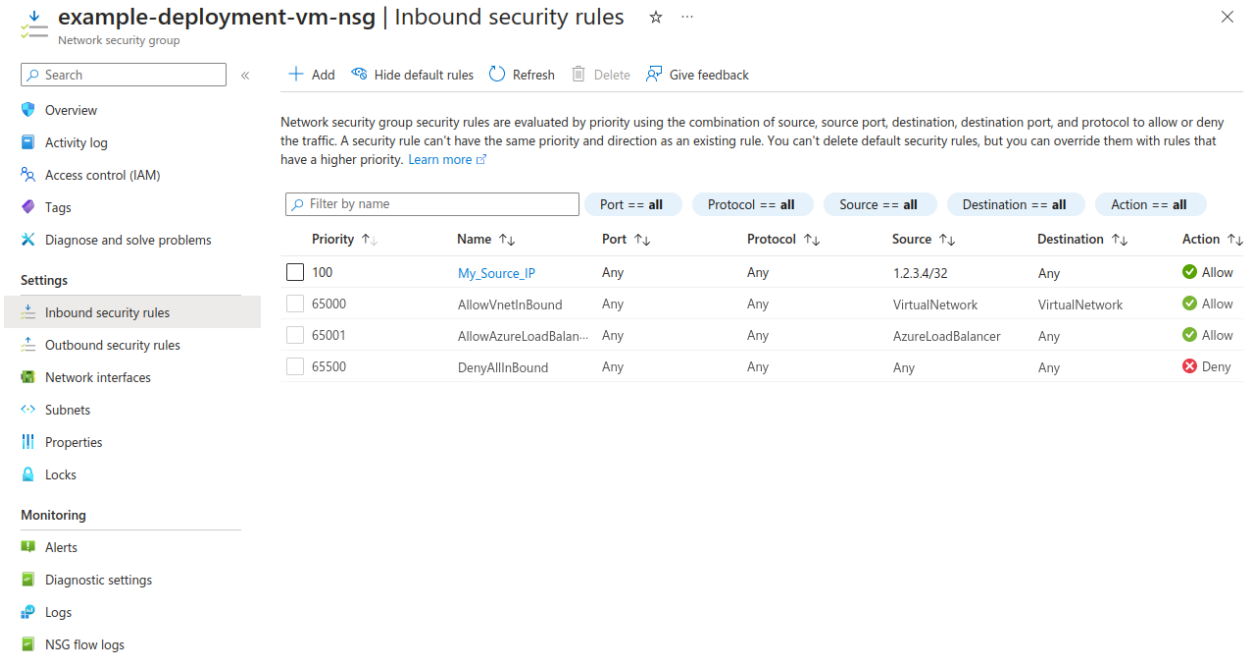
	Note: The filters along the top also allow filtering to *Network security groups* from the *All types* drop-down.



The only custom rule is *My_Source_IP*. This allows your connection to the PORTrockIT.



Left click on the *Inbound security rules* in the *Settings* category.



Left click on *Add*.

Add inbound security rule

example-deployment-vm-nsg

Source

IP Addresses

Source IP addresses/CIDR ranges *

203.0.113.100/32

Source port ranges *

*

Destination

Any

Service

Custom

Destination port ranges *

*

Protocol

- (•) Any
- ( ) TCP
- ( ) UDP
- ( ) ICMP

Action

- (•) Allow
- ( ) Deny

Priority *

110

Name *

example_external_bridgeworks_node

Description

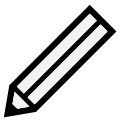
This is the other Bridgeworks Node. All traffic to/from the 10.0.1.0/24 route will actually come through here.

Add | Cancel | Give feedback

Fill out the settings to allow the other Node to connect to this PORTrockIT virtual machine.

In this example, another Bridgeworks PORTrockIT is set up with a public IP address of *203.0.113.100*. The external Node is the only IP address in that range that should be allowed to connect to the Azure one being set up, so a *32* prefix length is used.

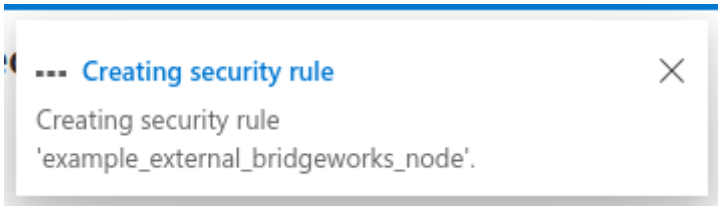
The *Destination port ranges* entry is set according to the table found in Section 6.3.2: Network Security Group. This adds the minimum functionality to access the PORTrockIT and connect it to the external Node.

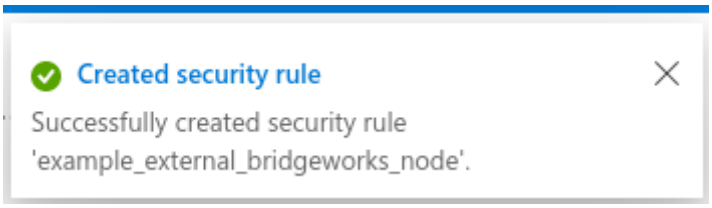
	Note: Other services will need their relevant ports added to the list.

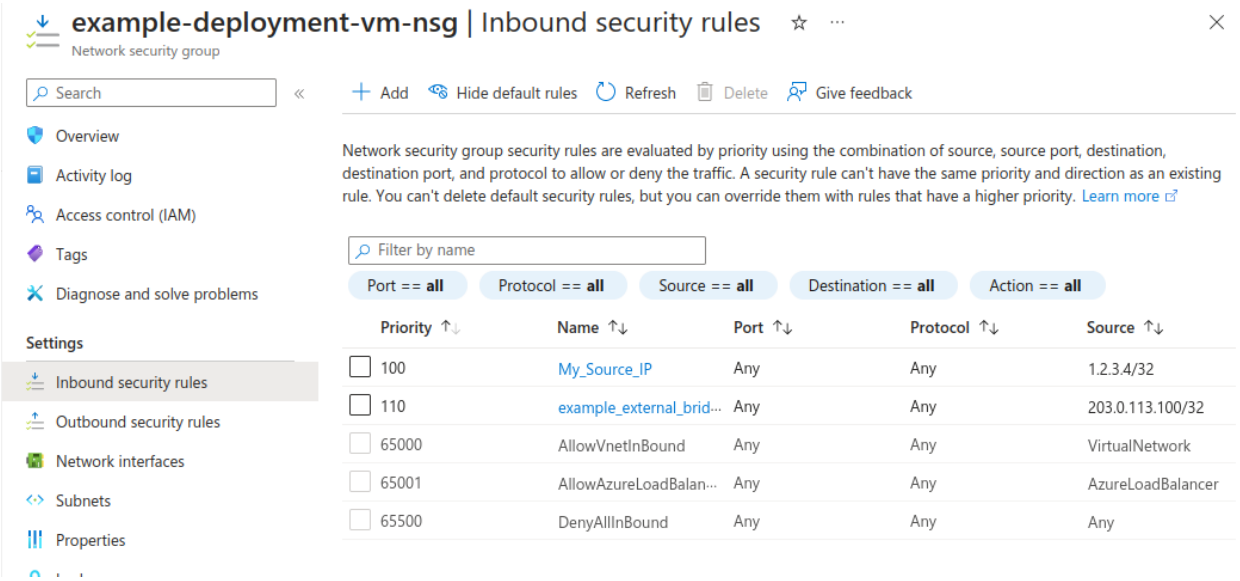
This connection will be the target when your PORTrockIT virtual machine routes network traffic destined for the 10.0.1.0/24 IP address range seen previously in this guide.

Left click *Add* when you are ready to proceed.

Wait for the success notification to occur.







You now have two custom rules; *My_Source_IP* allows you to access the PORTrockIT GUI and

connect to it via SSH from your current connection, and *example_external_bridgeworks_node* allows incoming network traffic from an external Node.