



Azure Deployment Guide Eli-v6.4.84

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	3
2	Guide layout	4
3	Storage accounts	5
3.1	Creating a storage account	5
3.2	Containers	9
4	Uploading a VHD	11
5	Image creation	15
6	Virtual machine creation	22
6.1	Creation menu	22
6.1.1	1 - Basics	22
6.1.2	2 - Disks	24
6.1.2.1	3 - Networking	25
6.1.2.2	Public IP address	26
6.1.2.3	Network Security Group	27
6.1.2.4	Diagnostics	31
6.1.3	4 - Summary	32
6.1.4	SSH key generation (Optional)	34
6.1.4.1	Linux	34
6.1.4.2	Windows	35
7	Route tables	39
7.1	Network interface	47
8	Accessing the GUI	51
9	Troubleshooting	54
9.1	Deployment Problems	54

10 Useful Links

55

Appendix A Network security

56

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.

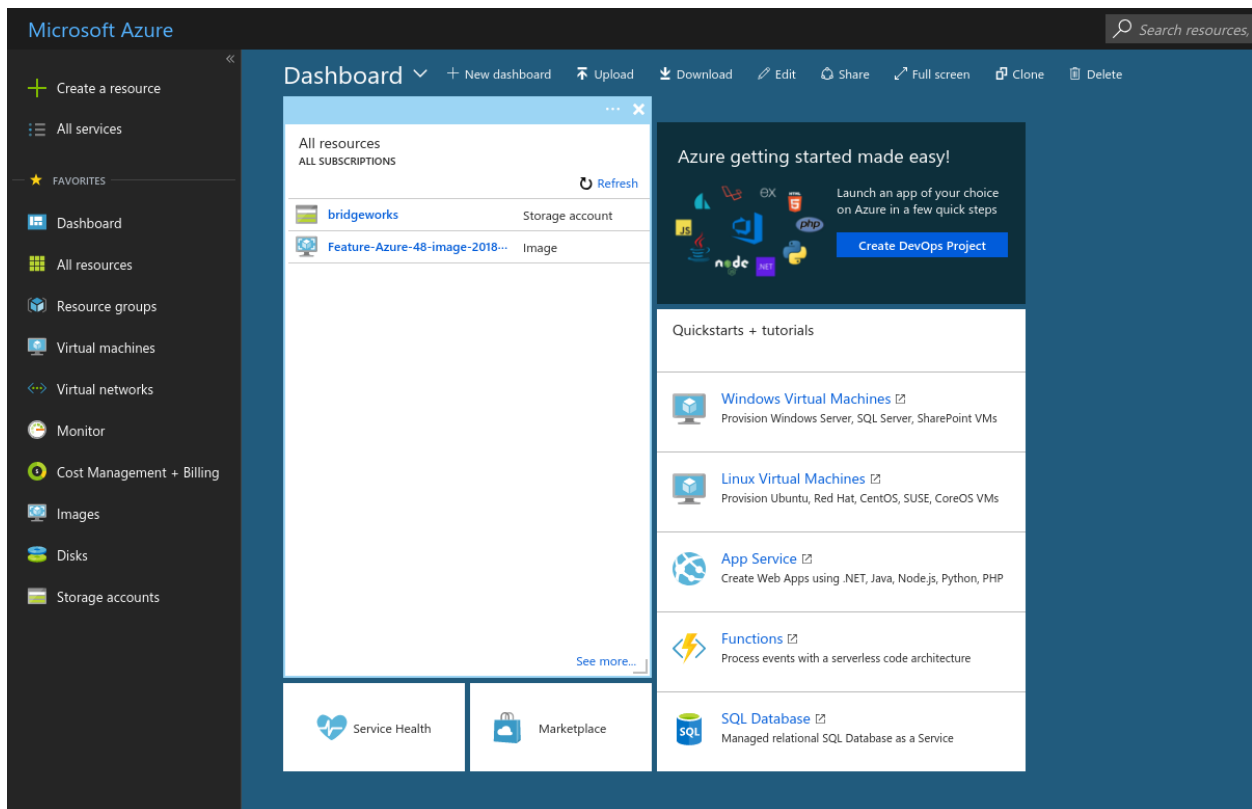
Archive Rarely accessed data. Very low storage cost, high access cost. To read archived data it must be “rehydrated” to Hot or Cool storage; this can take up to 15 hours.

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

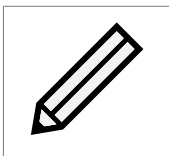
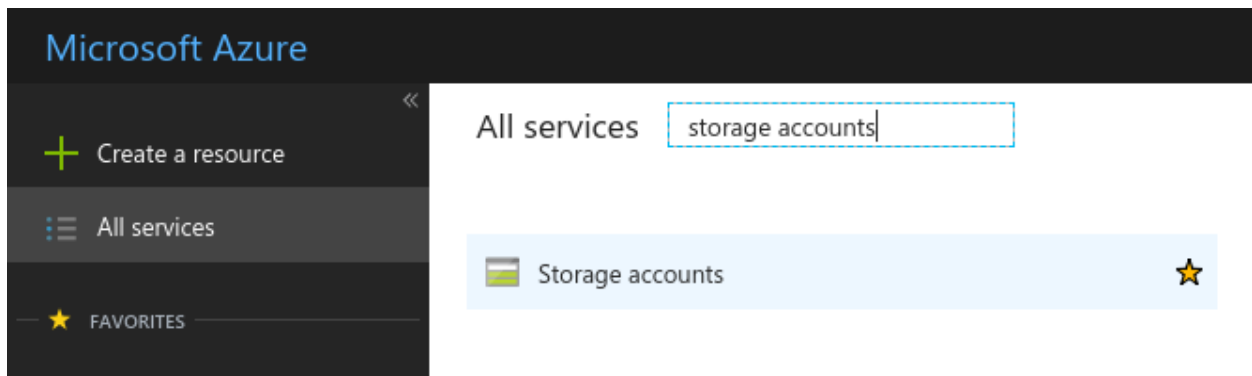
To create a storage account, first log in to your Azure account through the Azure portal.

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.

[All services](#) >


Storage accounts ...


Bridgeworks R&D (orlop.co.uk)


[+ Create](#)  [Manage view](#)   [Refresh](#)  [Export to CSV](#)  [Open query](#) |  [Assign tags](#)  [Delete](#)

Filter for any field...

Subscription == all

Resource group == all 

Location == all 

 Add f

Showing 1 to 4 of 4 records.

<input type="checkbox"/> Name 	Type 
<input type="checkbox"/>  bridgeworks	Storage account
<input type="checkbox"/>  csb10032001b4804110	Storage account
<input type="checkbox"/>  imagesnortheu	Storage 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.

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 *

Resource group * [Create new](#)

Instance details

If you need to create a legacy storage account type, please click [here](#).

Storage account name ⓘ *

Region ⓘ *

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

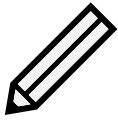
Redundancy ⓘ *

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.

The screenshot displays the Azure portal interface for a storage account. The breadcrumb navigation at the top reads 'Home > Storage accounts > exampledeploymentstorage'. The main header shows 'Storage accounts' with 'Bridgeworks R&D' and 'exampledeploymentstorage' with 'Storage account'. The left sidebar contains a list of storage accounts: 'bridgeworks', 'bridgeworkspayguksouth', 'csa0087678461a4x4c7exb71', and 'exampledeploymentstorage' (which is selected and highlighted in blue). The main content area is divided into three sections: a search bar, a navigation menu, and a details panel. The navigation menu includes 'Overview' (selected), 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', and 'Storage Explorer (preview)'. Below this is a 'SETTINGS' section with 'Access keys', 'Configuration', 'Encryption', and 'Shared access signature'. The details panel on the right shows 'Resource_group (change) example_deployment_group', 'Status' (Primary: Available, Secondary: Available), 'Location' (UK South, UK West), 'Subscription (change) Microsoft Partner Network', 'Subscription ID' (00876784-61a4-4c7e-b717-0c70d57233da), and 'Tags (change)'. A 'Services' section at the bottom right highlights 'Blobs' as 'REST-based object storage for unstructured data' with links for 'Configure CORS rules', 'Setup custom domain', and 'View metrics'.

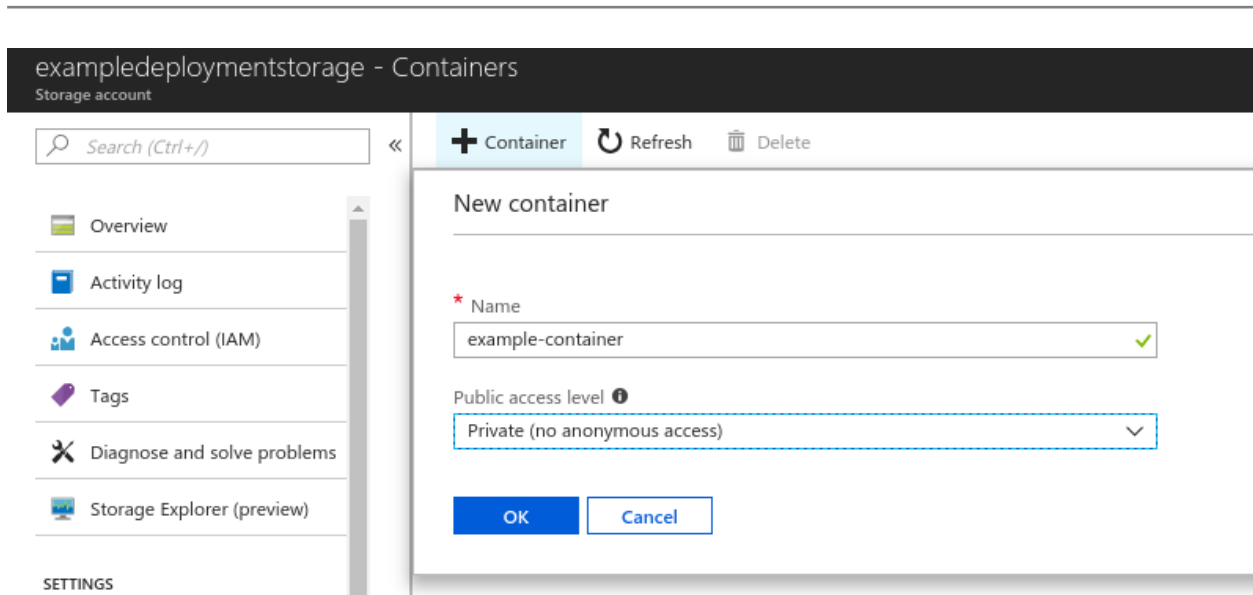
3.2 Containers

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

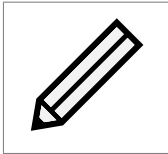
Navigate to the *Storage account* section and left click on your account. In the example, the storage container is labelled *exampledeploymentstorage*.

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*.

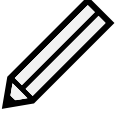


Note: In this example the *Public access level* drop-down is set to *Private*; this is the preferred setting.

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.

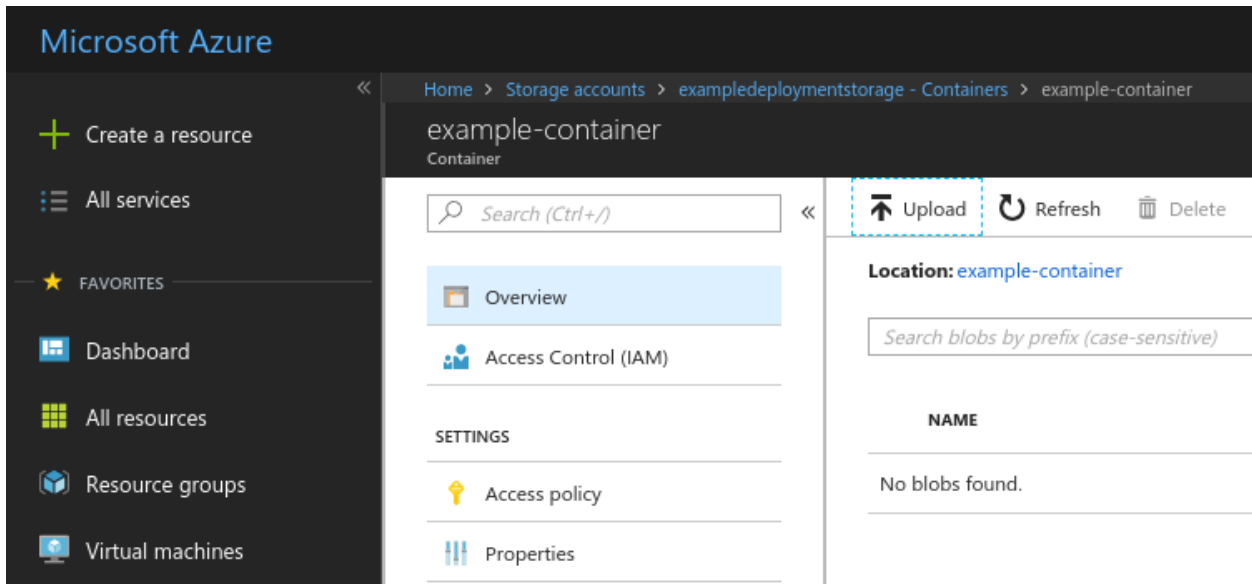
You will need to have access to the unzipped VHD file from the provided Bridgeworks ZIP file.



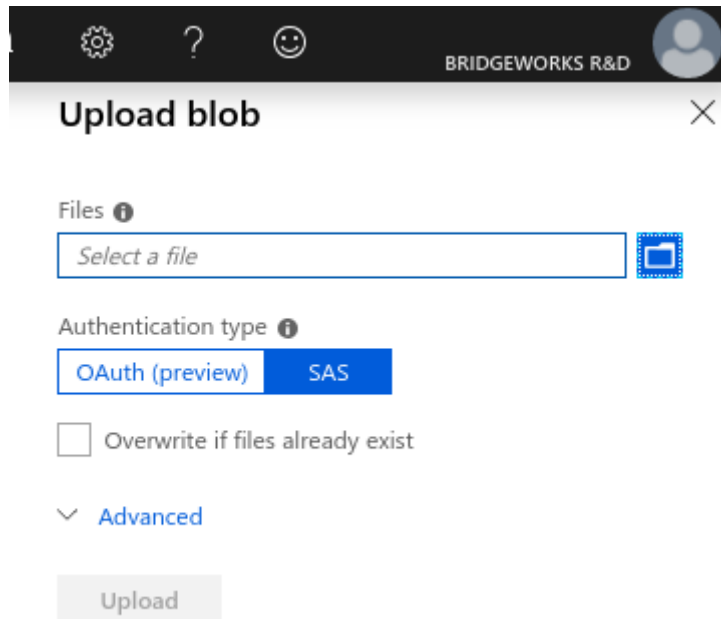
Note: When uploading the VHD, be aware of the region the VHD is being uploaded to. The easiest method is to upload it to the same region it will be deployed in.

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

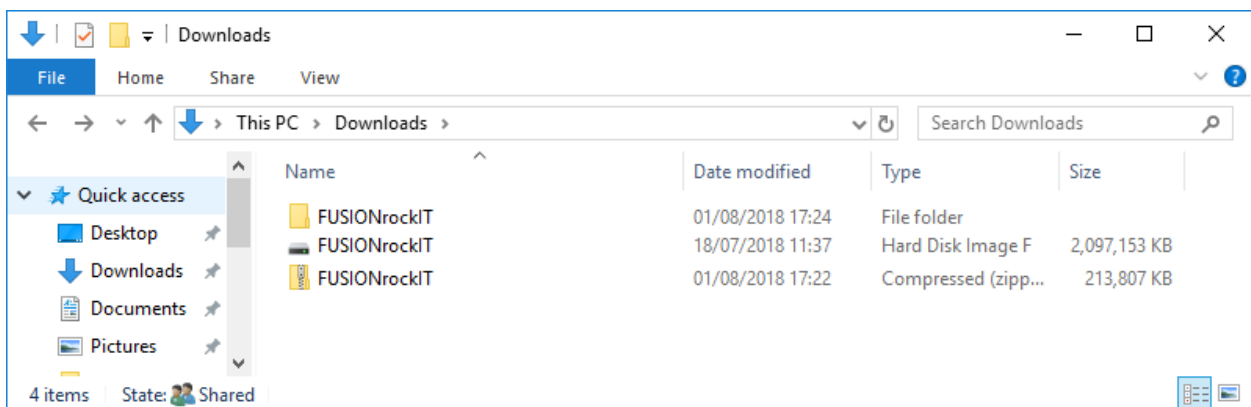
Currently the example container has no contents. Left click the *Upload* icon near the top of the page.



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.

Upload blob

Files ⓘ

Authentication type ⓘ

Overwrite if files already exist

Blob type ⓘ
 ▾

Upload .vhd files as page blobs (recommended)

Block size ⓘ
 ▾

Upload to folder

Current uploads

Dismiss: [Completed](#) [All](#)

FUSIONrockIT.vhd	304 MiB / 1 GiB	...
------------------	-----------------	-----

The upload will begin in your current view.

Note: The screenshot above may show more 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.

Current uploads

Dismiss: [Completed](#) [All](#)

FUSIONrockIT.vhd

✔ 2 GiB / 2 GiB

...

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.

Home > Storage accounts > exampledeploymentstorage - Containers > example-container

example-container
Container

Search (Ctrl+/)

Overview
Access Control (IAM)

SETTINGS
Access policy
Properties

Upload Refresh Delete Acquire lease Break lease View snapshots Create snapshot

Location: example-container

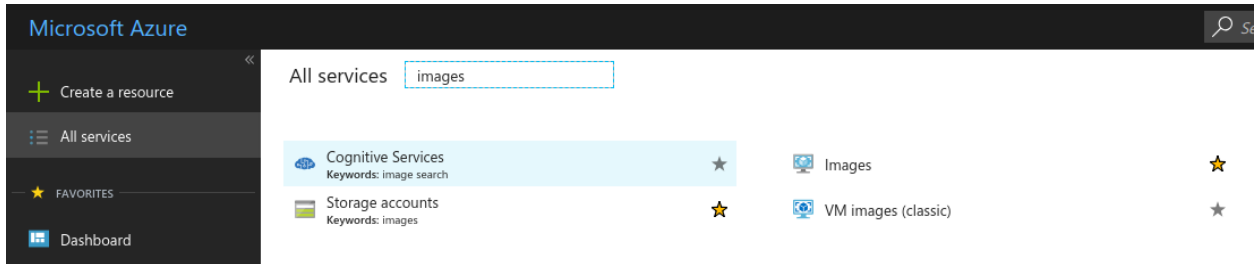
Search blobs by prefix (case-sensitive) Show deleted blobs

NAME	MODIFIED	BLOB TYPE	SIZE	LEASE STATE	
FUSIONrockIT.vhd	18/07/2018, 3:33:23 pm	Page blob	2 GiB	Available	...

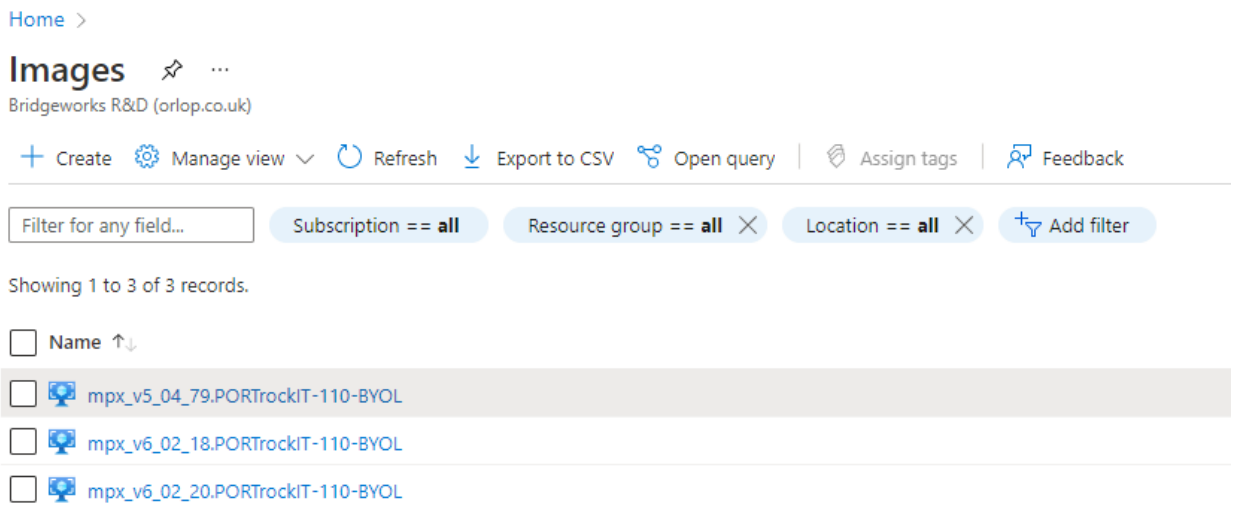
5 Image creation

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. A new menu will appear.

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 * ⓘ

Resource group * ⓘ
[Create new](#)

Instance details

Name *

Region * ⓘ

Zone resiliency ⓘ

OS disk

OS type * ⓘ Windows
 Linux

VM generation * ⓘ Gen 1
 Gen 2

Storage blob * ⓘ
[Browse](#)

Account type * ⓘ

Host caching * ⓘ

Encryption

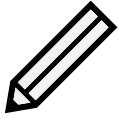
You can encrypt the OS and data disks with a platform-managed or customer-managed key. [Learn more](#)

Encryption type *

Data disk

[+ Add data disk](#)

Fill out the information. 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 * ⓘ ▼

Resource group * ⓘ ▼

[Create new](#)

Instance details

Name * ✓

Region * ⓘ ▼

Zone resiliency ⓘ

OS disk

OS type * ⓘ Windows Linux

VM generation * ⓘ Gen 1 Gen 2

Storage blob * ⓘ [Browse](#)

Account type * ⓘ ▼

Host caching * ⓘ ▼

Encryption

You can encrypt the OS and data disks with a platform-managed or customer-managed key. [Learn more](#)

Encryption type * ▼

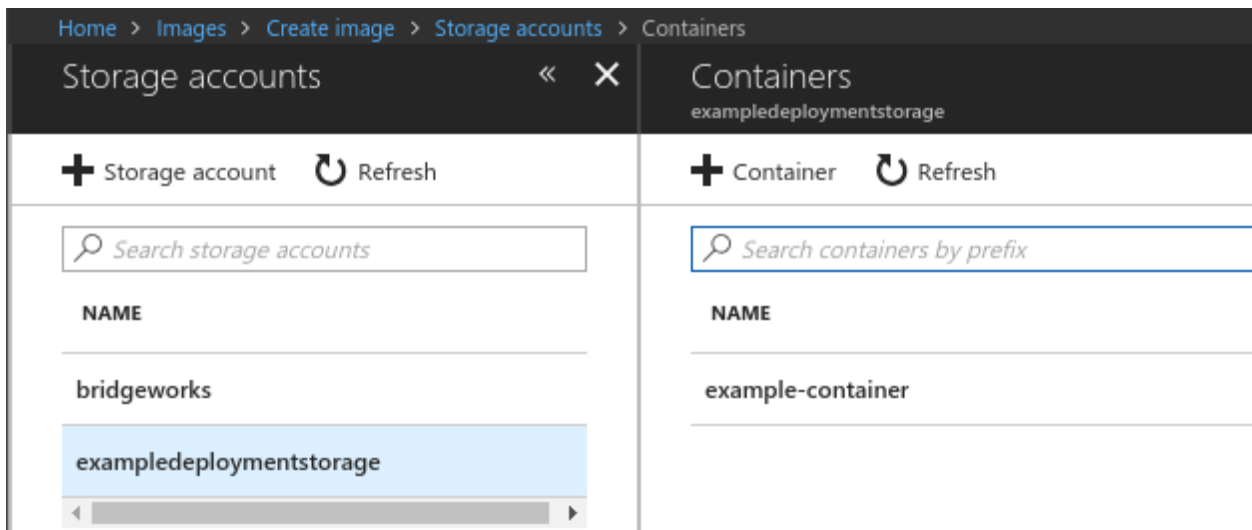
Data disk

[+ Add data disk](#)

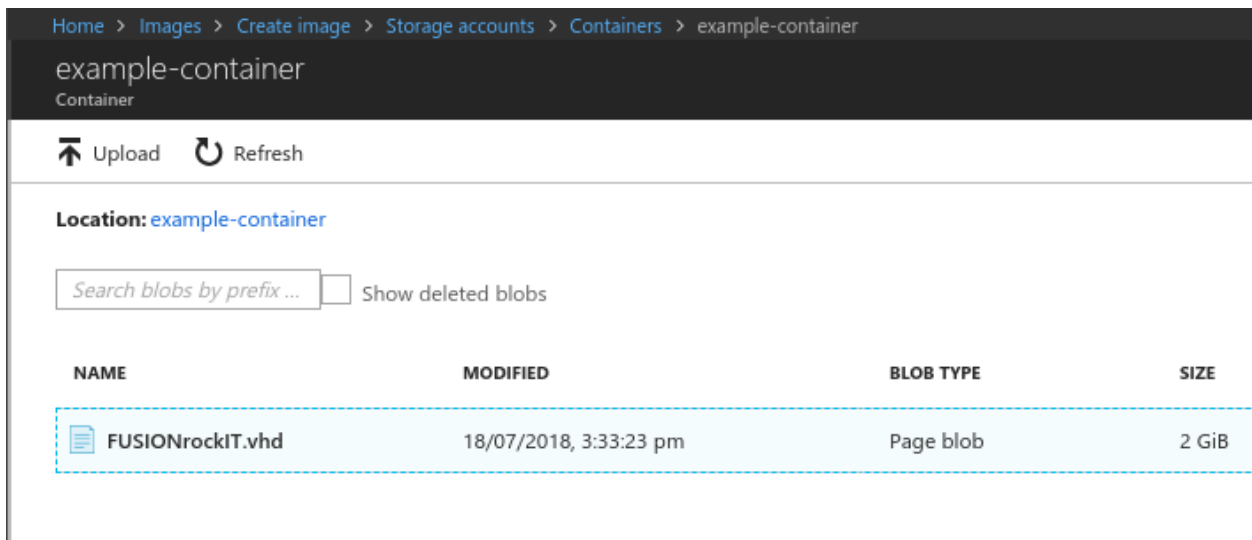
[Review + create](#) [< Previous](#) [Next : Tags >](#)

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.

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 * ⓘ ▼

Resource group * ⓘ ▼

[Create new](#)

Instance details

Name * ✓

Region * ⓘ ▼

Zone resiliency ⓘ

OS disk

OS type * ⓘ Windows
 Linux

VM generation * ⓘ Gen 1
 Gen 2

Storage blob * ⓘ ✓
[Browse](#)

Account type * ⓘ ▼

Host caching * ⓘ ▼

Encryption

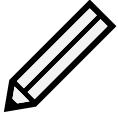
You can encrypt the OS and data disks with a platform-managed or customer-managed key. [Learn more](#)

Encryption type * ▼

Data disk

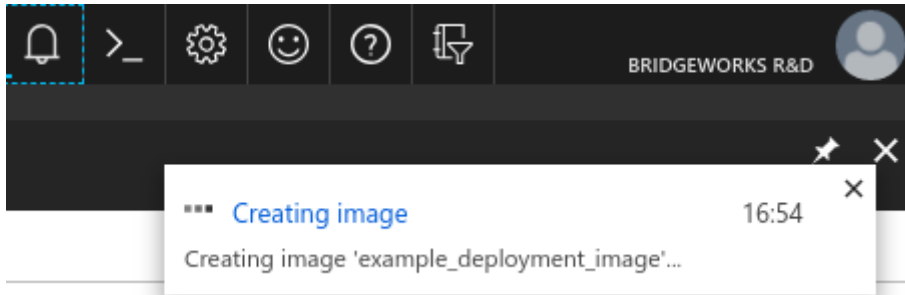
[+ Add data disk](#)

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

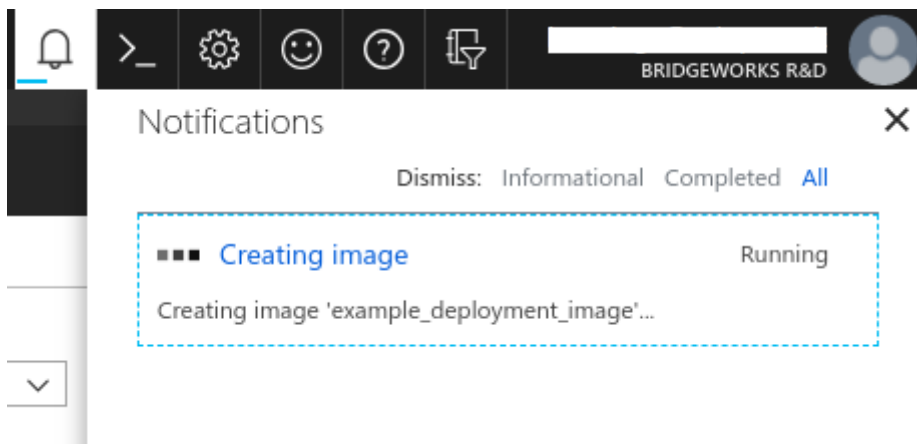


Note: The PORTrockIT does not require a high performance storage type. Therefore, *Standard HDD* can be selected.

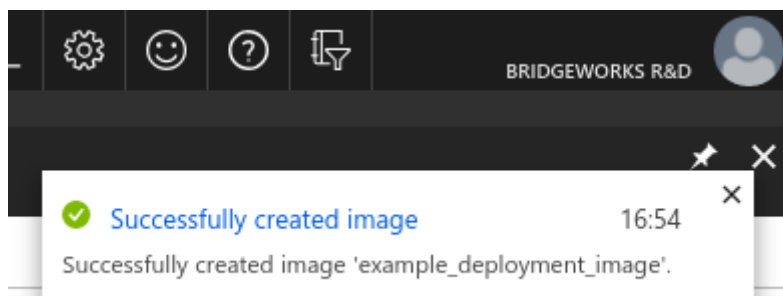
At this stage a notification will appear.



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.

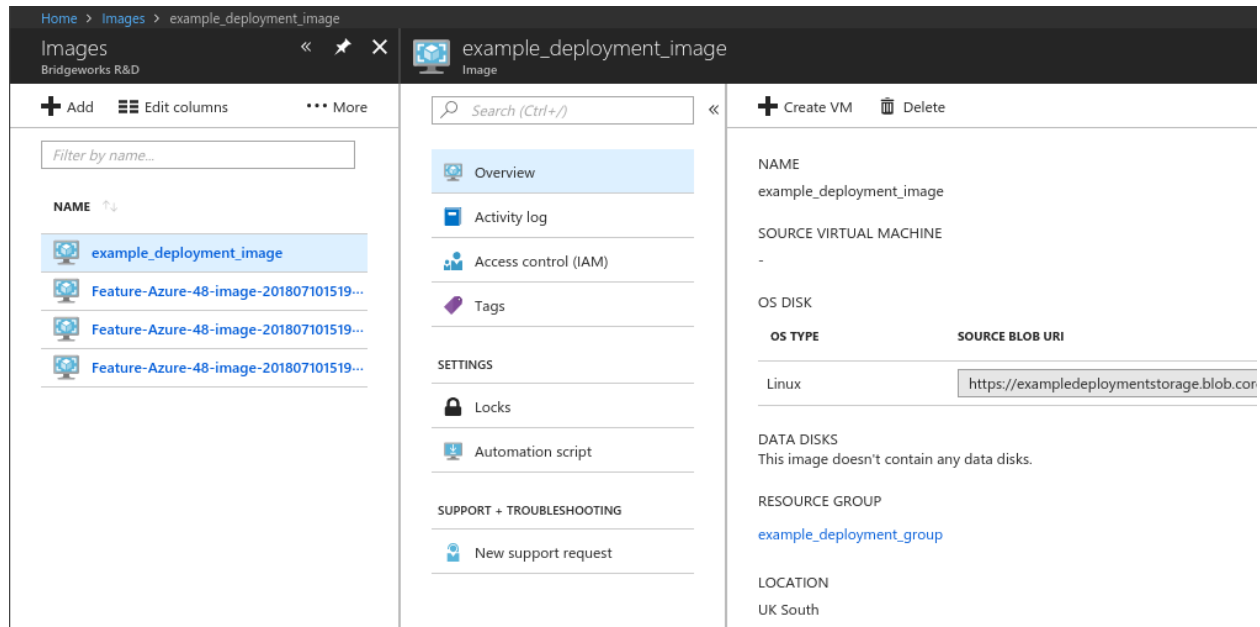


Now *Refresh* the page. Your newly added image should appear.

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 Creation menu

6.1.1 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
- Guest config
- 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.

Looking for classic VMs? [Create VM from Azure Marketplace](#)

PROJECT DETAILS

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

* Subscription ⓘ

* Resource group ⓘ
[Create new](#)

INSTANCE DETAILS

* Virtual machine name ⓘ

* Region ⓘ

Availability options ⓘ

* Image ⓘ
[Browse all images and disks](#)

* Size ⓘ **Standard F8s_v2**
8 vcpus, 16 GB memory
[Change size](#)

ADMINISTRATOR ACCOUNT

Authentication type ⓘ Password SSH public key

* Username ⓘ

* SSH public key ⓘ

INBOUND PORT RULES

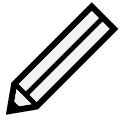
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

* Public inbound ports ⓘ None Allow selected ports

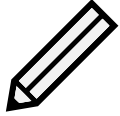
Select inbound ports

i All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

- [Review + create](#)
- [Previous](#)
- [Next : Disks >](#)



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.



Note: Brief guides on generating an SSH key in Linux and Windows are located at the end of this chapter. See Section [6.1.4: SSH key generation \(Optional\)](#).

Left click *Next* to proceed.

6.1.2 2 - Disks

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

Create a virtual machine

[Basics](#) **[Disks](#)** [Networking](#) [Management](#) [Guest config](#) [Tags](#) [Review + create](#)

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

DISK OPTIONS

* OS disk type ⓘ

Standard HDD

The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

DATA DISKS

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	NAME	SIZE (GIB)	DISK TYPE	HOST CACHING
-----	------	------------	-----------	--------------

[Create and attach a new disk](#) [Attach an existing disk](#)

▼ ADVANCED

Review + create

Previous

Next : Networking >

Left click *Next* to proceed.

6.1.2.1 3 - Networking

Create a virtual machine

[Basics](#) [Disks](#) [Networking](#) [Management](#) [Guest config](#) [Tags](#) [Review + create](#)

Configure a new or existing virtual network for your VM as well as how your VM will be accessed on the virtual network. [Learn more](#)

NETWORK INTERFACE

When creating a virtual machine, a network interface will be created for you.

* Virtual network ⓘ	<input type="text" value="(new) example_deployment_group-vnet"/> <input type="button" value="v"/>
	Create new
* Subnet ⓘ	<input type="text" value="default"/> <input type="button" value="v"/>
Public IP ⓘ	<input type="text" value="(new) example-deployment-vm-ip"/> <input type="button" value="v"/>
	Create new
Network security group	<input type="radio"/> Basic <input checked="" type="radio"/> Advanced
Configure network security group	<input type="text" value="(new) example-deployment-vm-nsg"/> <input type="button" value="v"/>
	Create new
Accelerated networking ⓘ	<input type="radio"/> On <input checked="" type="radio"/> Off

The selected image does not support accelerated networking.

[Review + create](#)

[Previous](#)

[Next : Management >](#)

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.

Create virtual network ✕

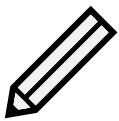
* Name

* Address space
 ✓
10.0.10.0 - 10.0.10.255 (256 addresses)

* Subnet name

* Subnet address range ⓘ
 ✓
10.0.10.0 - 10.0.10.255 (256 addresses)

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.

6.1.2.2 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.

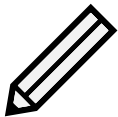
In this example the *Assignment* setting has been changed. This means that the external IP address of the PORTrockIT won't change like it would with the *Dynamic* setting.

Create public IP address ✕

* Name

SKU ⓘ
 Basic Standard

Assignment
 Dynamic Static



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.

6.1.2.3 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.

Create network security g... □ ×

* Name
example-deployment-vm-nsg

Inbound rules ⓘ

1000: default-allow-ssh	✓ ...
Any	
SSH (TCP/22)	

+ Add an inbound rule

Outbound rules ⓘ

No results

+ Add an outbound rule

OK

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

🔧 Basic

* Source ⓘ

IP Addresses
▼

* Source IP addresses/CIDR ranges ⓘ

203.0.113.0/32
✓

* Source port ranges ⓘ

*

* Destination ⓘ

Any
▼

* Destination port ranges ⓘ

*
✓

* Protocol

Any

TCP

UDP

* Action

Allow

Deny

* Priority ⓘ

100

* Name

My_Source_IP
✓


Description

Add


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.

	<p>Important: These settings only need to be applied to the <i>Destination port ranges</i> entry. The <i>Source port ranges</i> entry can be left as "*", which allows the source port to be any number.</p>
---	--

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.

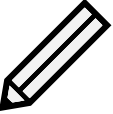
	<p>Note: The "*" character can be used to specify that all ports will be available. Use with caution.</p>
---	---

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.

6.1.2.4 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.

Create a virtual machine

[Basics](#) [Disks](#) [Networking](#) **[Management](#)** [Guest config](#) [Tags](#) [Review + create](#)

Configure monitoring and management options for your VM.

MONITORING

Boot diagnostics ⓘ On Off

OS guest diagnostics ⓘ On Off

* Diagnostics storage account ⓘ

exampledeploymentstorage

[Create new](#)

IDENTITY

System assigned managed identity ⓘ On Off

AUTO-SHUTDOWN

Enable auto-shutdown ⓘ On Off

[Review + create](#)

[Previous](#)

[Next : Guest config >](#)

All settings should have been set.

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

6.1.3 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.

Create a virtual machine

✓ Validation passed

[Basics](#) [Disks](#) [Networking](#) [Management](#) [Guest config](#) [Tags](#) [Review + create](#)

example_deployment_image

Standard F8s_v2

8 vcpus, 16 GB memory

BASICS

Subscription	Microsoft Partner Network
Resource group	example_deployment_group
Virtual machine name	example-deployment-vm
Region	UK South
Availability options	No infrastructure redundancy required
Authentication type	SSH public key
Username	example-username

DISKS

OS disk type	Standard HDD
Use managed disks	Yes

NETWORKING

Virtual network	(new) example_deployment_group-vnet
Subnet	default
Public IP	(new) example-deployment-vm-ip
Network security group	(new) example-deployment-vm-nsg
Accelerated networking	Off

MANAGEMENT

Boot diagnostics	On
OS guest diagnostics	Off

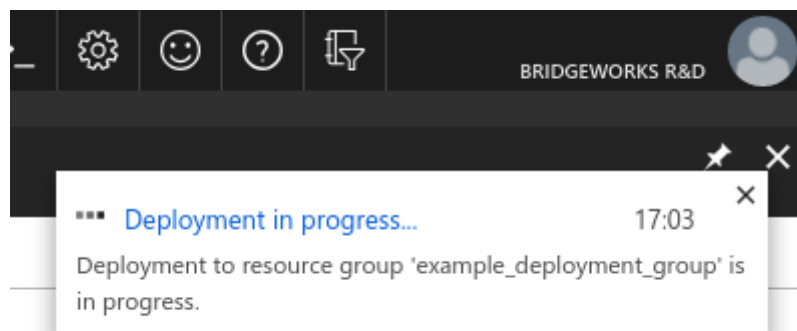
Create

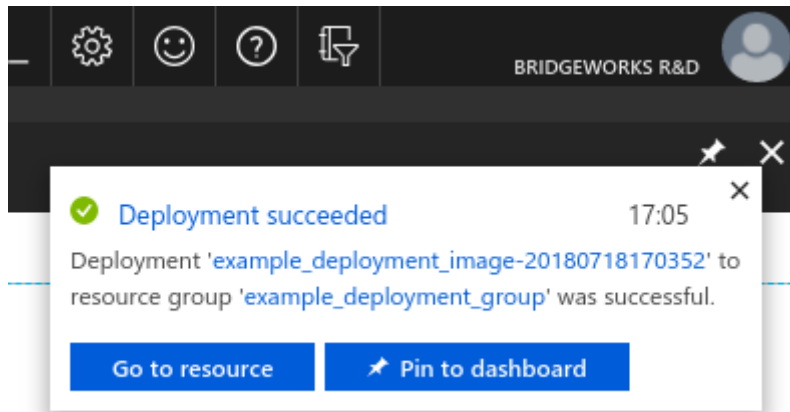
Previous

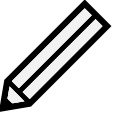
Next

[Download a template for automation](#)

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.

6.1.4 SSH key generation (Optional)

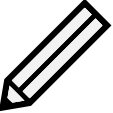
6.1.4.1 Linux

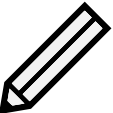
"ssh-keygen" was used to generate the SSH key pair for this guide. This utility is available on any Linux system that has the OpenSSH client installed.

```
$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/h/user/.ssh/id_rsa): /h/user/.ssh/example_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /h/user/.ssh/example_rsa.
Your public key has been saved in /h/user/.ssh/example_rsa.pub.
The key fingerprint is:
SHA256:KPou1E8YZLQkp5uNbzWxtG2u+FwNpMQhMH1YOFbmyU4 user@ubuntu
The key's randomart image is:
+---[RSA 2048]-----+
| ..BBo.+          |
| ==o+* o          |
| .o.oo E .        |
| =.. X o o        |
| +.oo* S o .      |
| .ooo.+ .         |
| .. oo o          |
| .o ..o           |
| o+.o             |
+-----[SHA256]-----+
$ cat ~/.ssh/example_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACyx1TY1B7YrikUmuC3lye94tLEGS+jNgi/MGS1N7X9
38u2t0TirIbhaMfP5iewB9S4aBMForAqcIRB9210+2dU0jLeuMg/vtMi8arDTdgiv5qUSdUZ1W6IXU+B
```

```
Hi0YnsUL/zmcAuk1RJNtqS3qfFx1oWhXD0LmEGkzdVX4I58/pujeNg0yHTS+3ddwFVmHQzwKYUucuHbA  
toGgF+em/Nb49Y3gWgmg2r0sInRAxRUGiABQIDE/yZfk+YyYVTCauW5TOGHXAAHC/k1NVRcQHtQQ8Y1Y  
c9VtCNBKWXIiHbNfWutq11bkhrD7qvh/VNq5Wgv9/zqtNXmhFUGx0hLFXagR user@ubuntu
```

Copy the public key into the *SSH public key* box.


	Note: Ensure that you are copying your <i>Public</i> key. Your private key should never be given out. When viewing the string you can tell a private key from a public key. The private key will have the string “ <i>BEGIN RSA PRIVATE KEY</i> ”. The public key generated in this example starts with the more generic “ <i>ssh-rsa</i> ”.
---	--

	Note: You may have noticed that your public key contains your local username at the end. This is a comment, which is not part of the key.
---	---

6.1.4.2 Windows

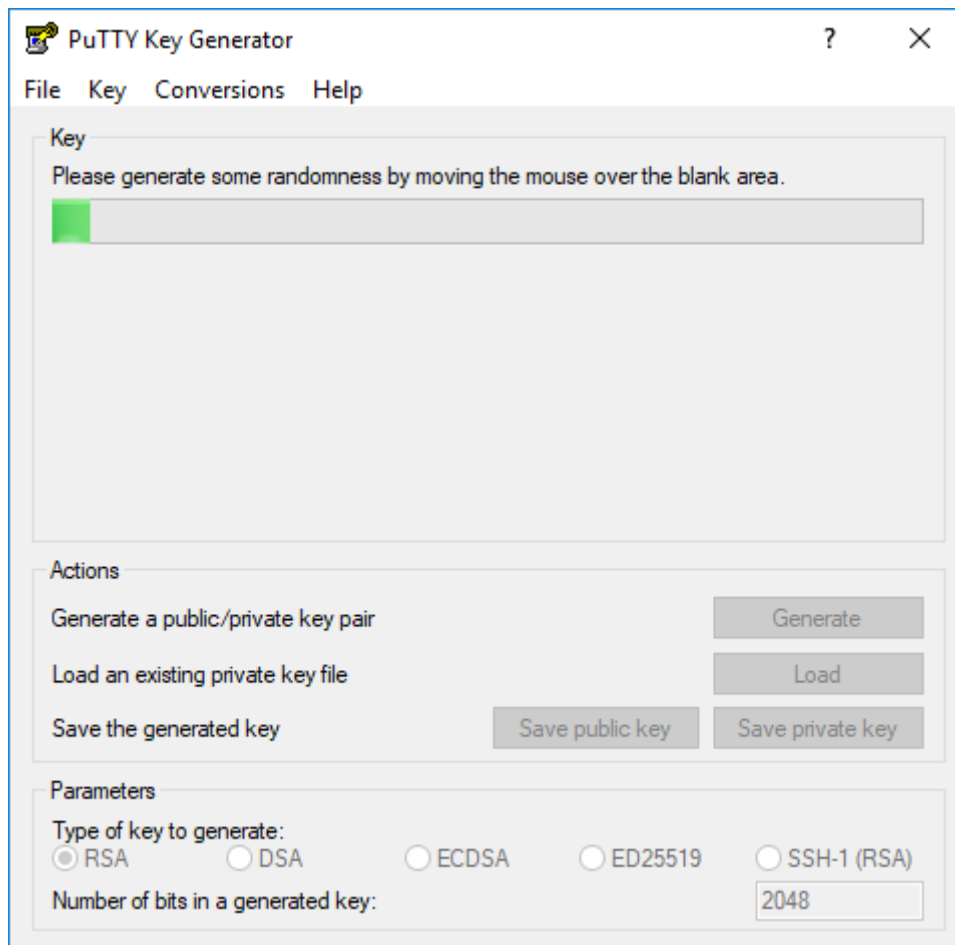
The easiest method to generate an SSH RSA key in Windows is using the *puttygen* utility.

Download the *puttygen* utility from <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>.

	Note: The putty installer will include puttygen. You can download the ZIP file and extract the contents if installation is not possible on your machine.
---	--

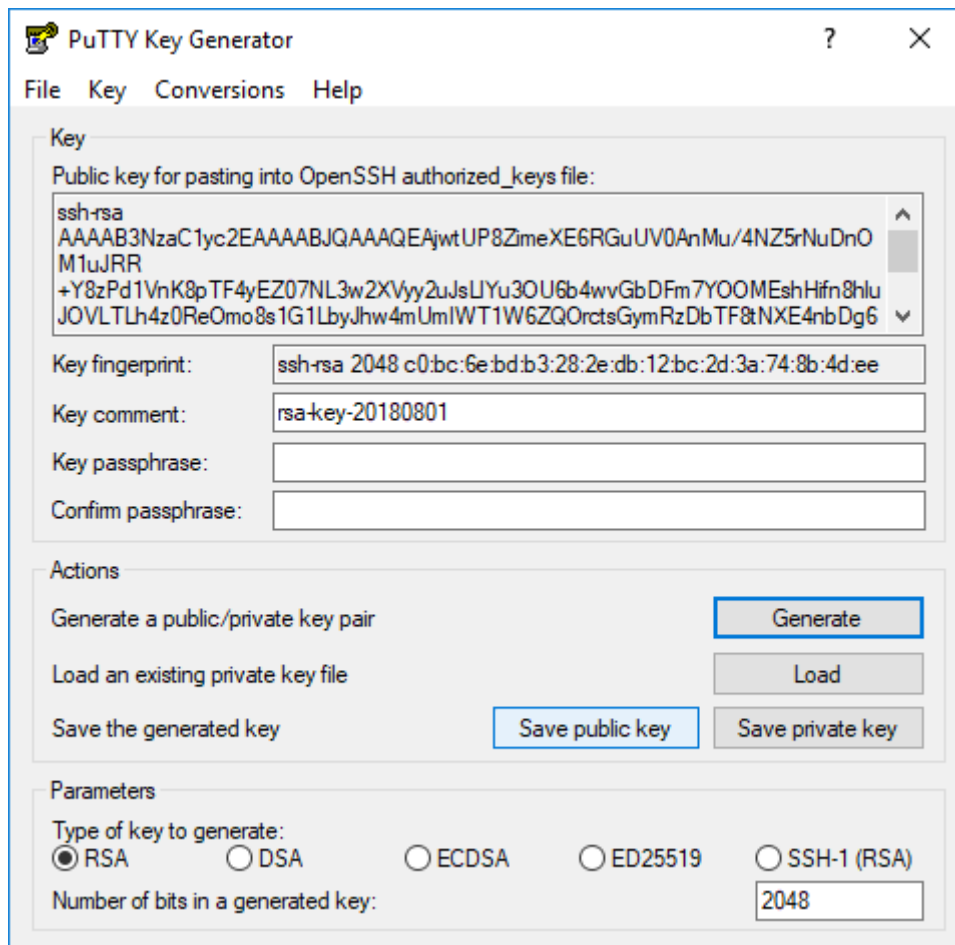
Run *puttygen*. A GUI will be presented.

Left click on *Generate* and follow the on-screen instructions.



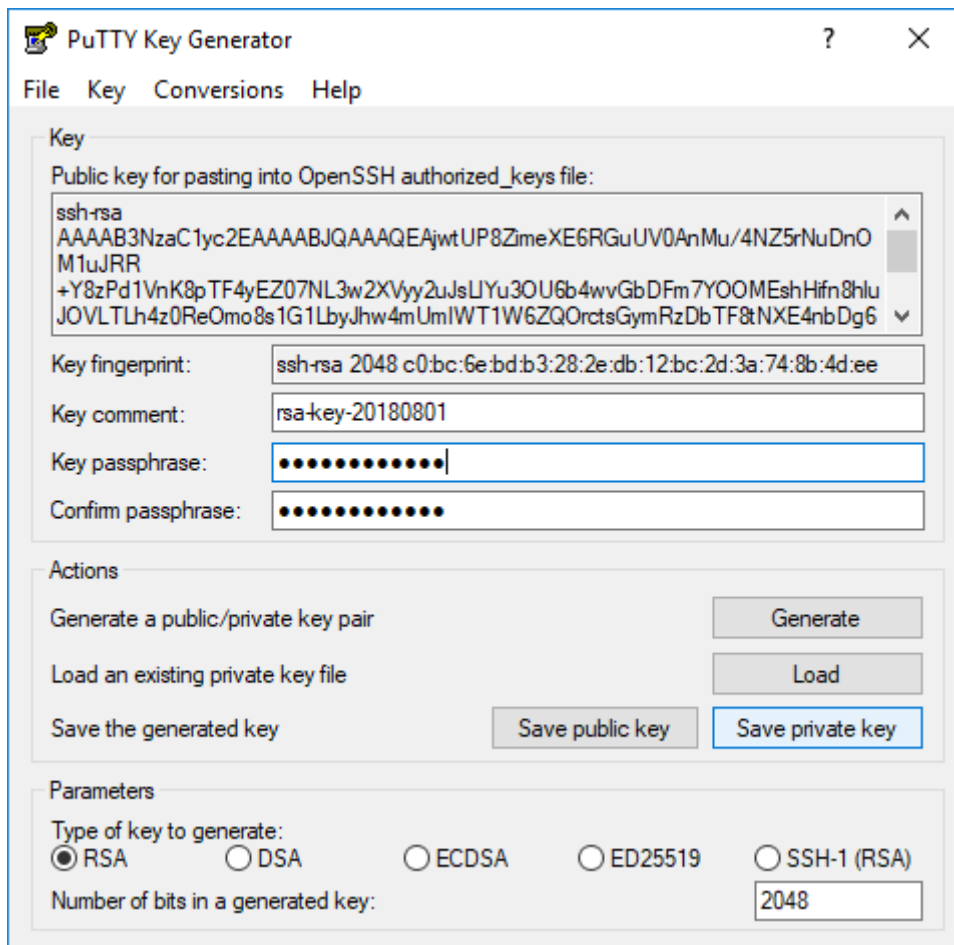
Puttygen will show the public key once it has been generated.

You can safely left click on *Save public key* and save the file somewhere on your system.



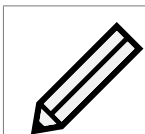
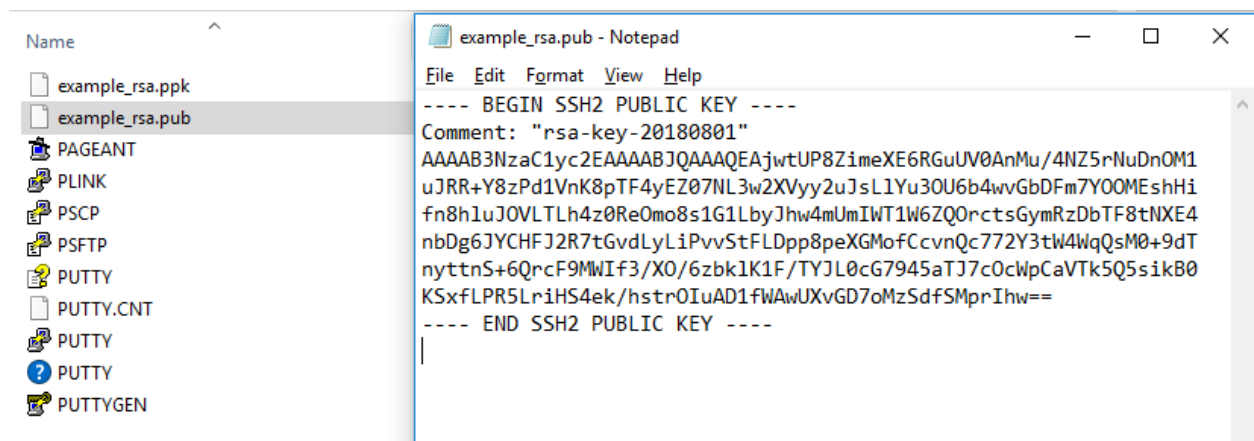
You have to save the private key.

It is recommended that you populate the *Key passphrase* entries to password protect the private key file.



Open the public key with your text editor of choice.

From here you can copy the public key section over to Azure.

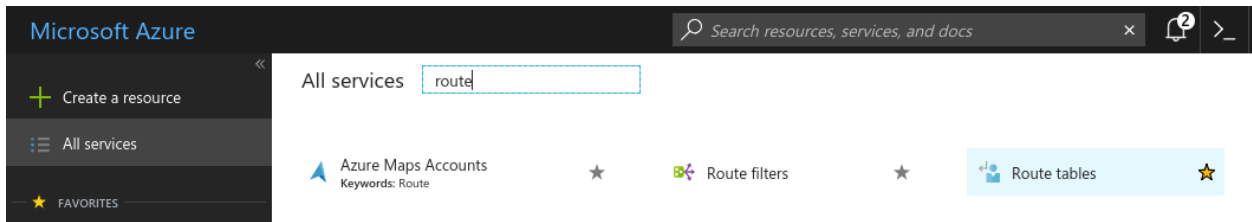


Note: In this example, the public key is the line after the *Comment* double quoted line, up to the `---- END SSH2 PUBLIC KEY ----` line. In this example the public key starts with "AAAAB3Nza" and ends with "Mprihw=="

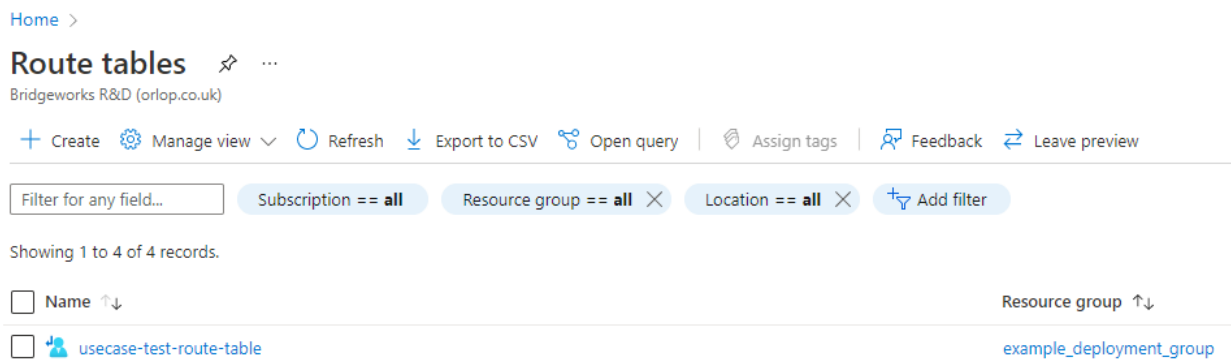
7 Route tables

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.

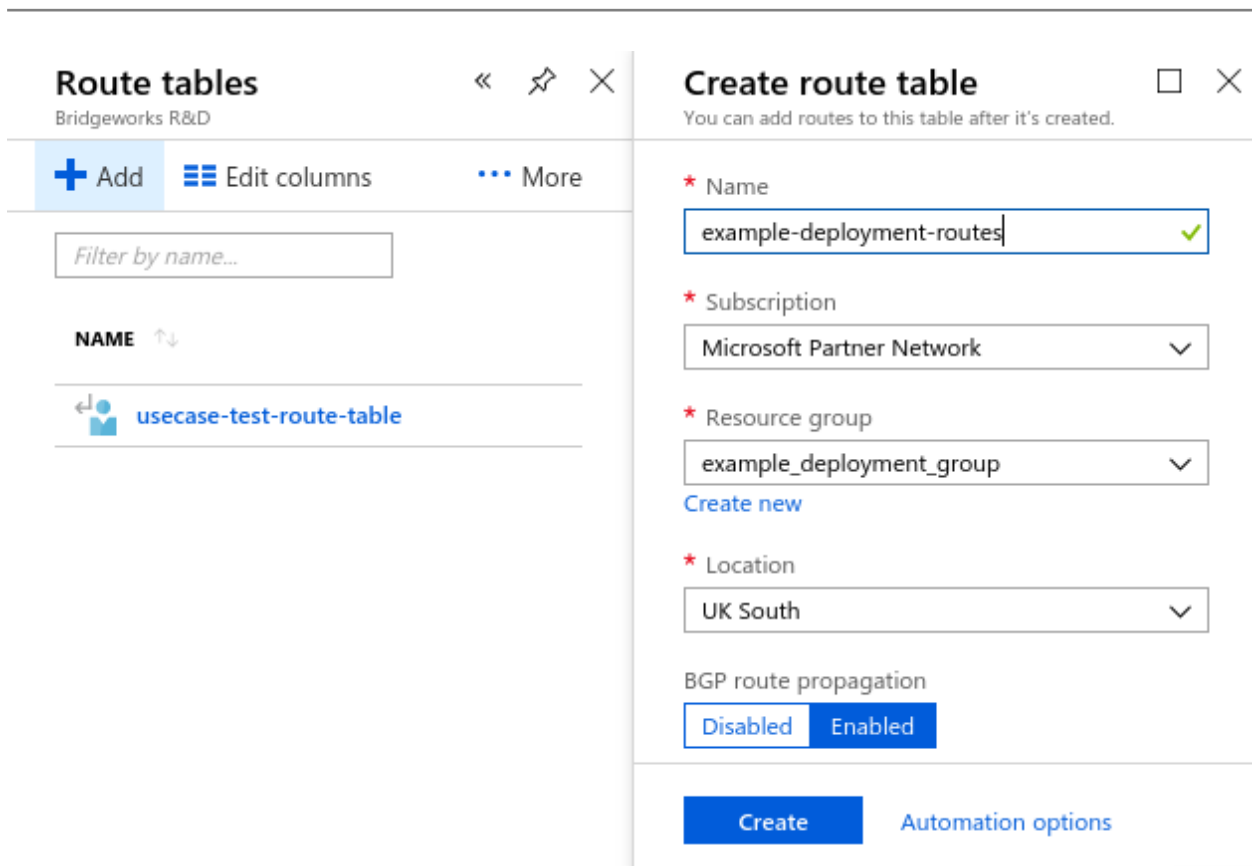
Navigate to the *Route tables* section. This can be achieved by navigating to *All services* on the left side of the page; either look for the *Route tables* link, or type it into the filter.



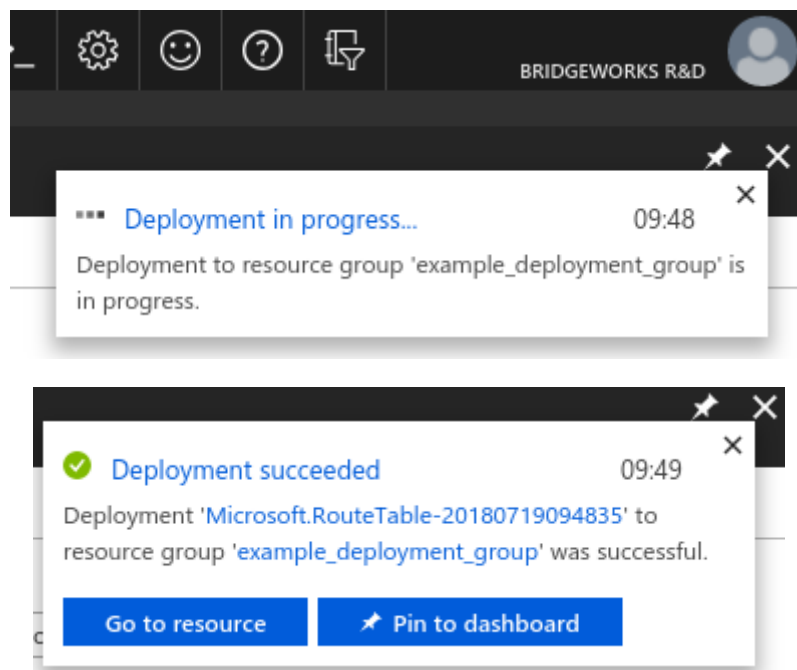
In the *Route tables* section you will be presented with all the route tables that are accessible from this Azure account. Left click the *Create* button near the top of the page.



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 *OK*. 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.

The screenshot displays the Azure portal interface for configuring a route table. The breadcrumb navigation at the top reads: Home > Route tables > example-deployment-routes. The main header shows 'Route tables' with 'Bridgeworks R&D' as the provider, and the specific route table 'example-deployment-routes' is selected.

On the left, there is a list of route tables with a search filter 'Filter by name...'. Two route tables are listed: 'example-deployment-routes' (selected) and 'usecase-test-route-table'.

The central pane contains a search bar 'Search (Ctrl+)' and a navigation menu with the following categories:

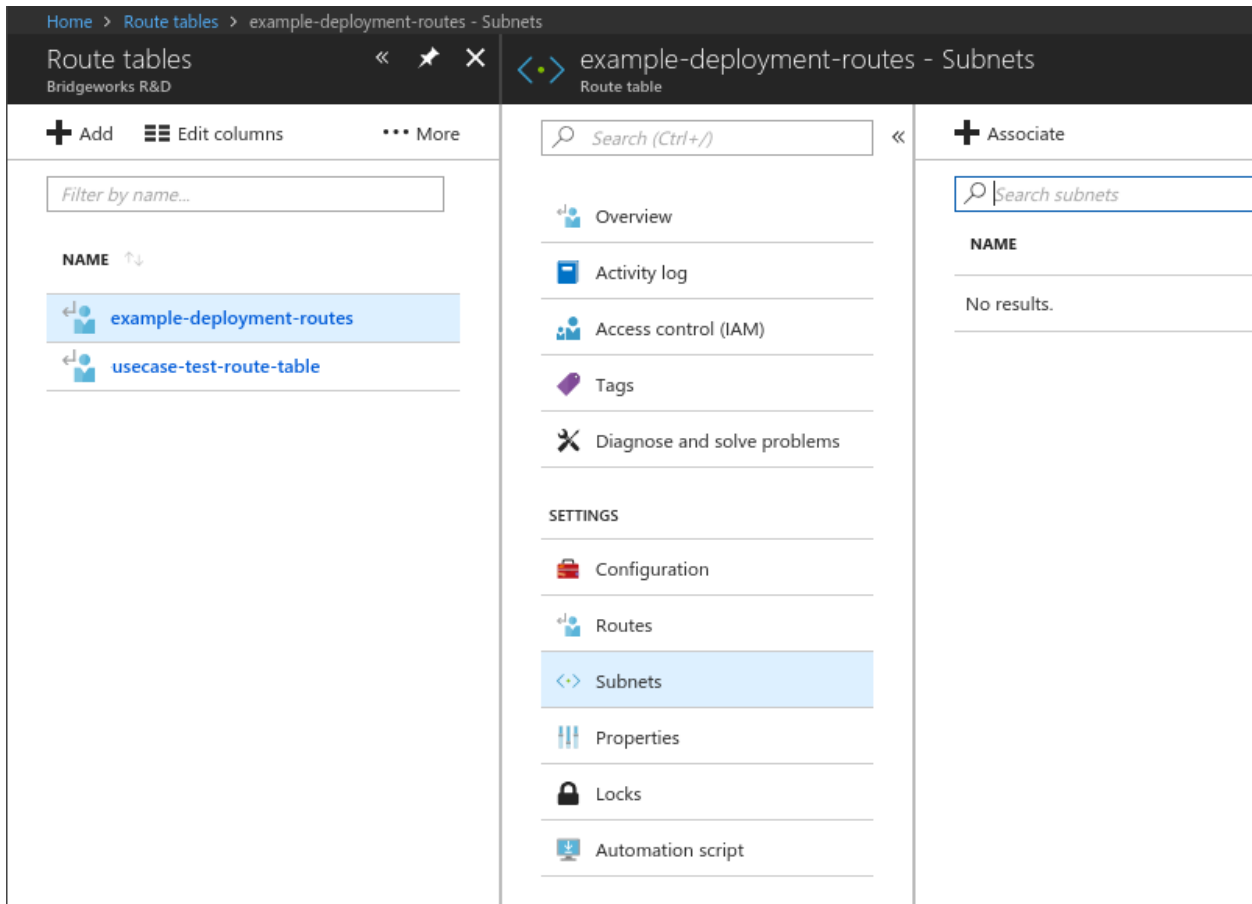
- Overview** (selected): Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems.
- SETTINGS**: Configuration, Routes, Subnets, Properties, Locks, Automation script.
- SUPPORT + TROUBLESHOOTING**

The right-hand pane shows the resource details for 'example-deployment-routes':

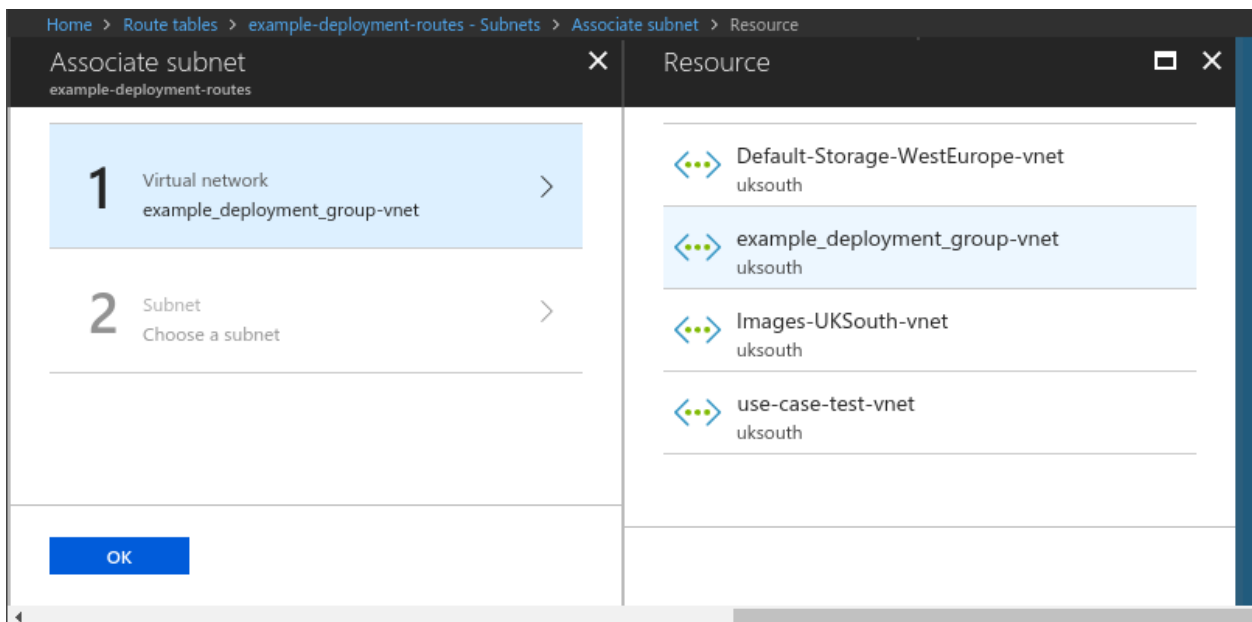
- Resource group**: [example_deployment_group](#) (change)
- Location**: UK South
- Subscription**: [Microsoft Partner Network](#) (change)
- Subscription ID**: 00876784-61a4-4c7e-b717-0c70d57233da
- Tags**: [Tags](#) (change), [Click here to add tags](#)

Below the resource details, there are sections for 'Routes' and 'Subnets', both with search bars and showing 'No results.'.

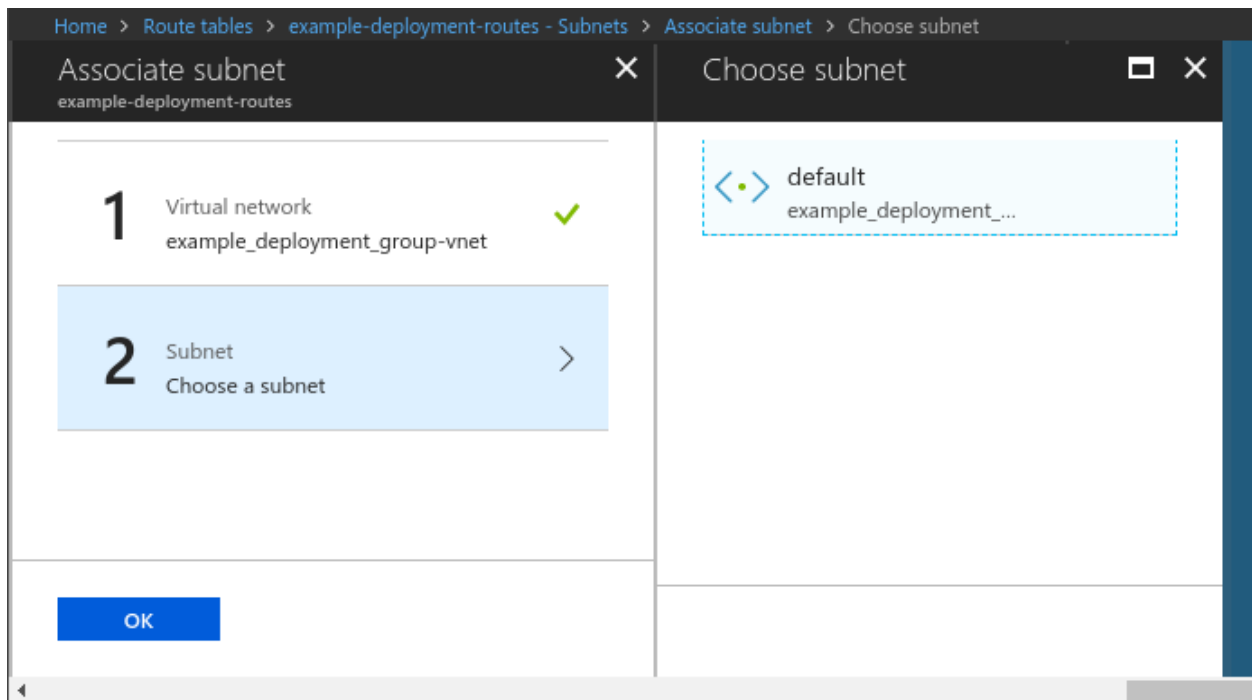
First you must associate a subnet to this route table. Left click the *Subnets* option in the *Settings* category.



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

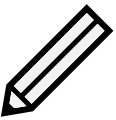


Left click on the *Virtual network* section, and then on the right select the virtual network you are using for your PORTrockIT.

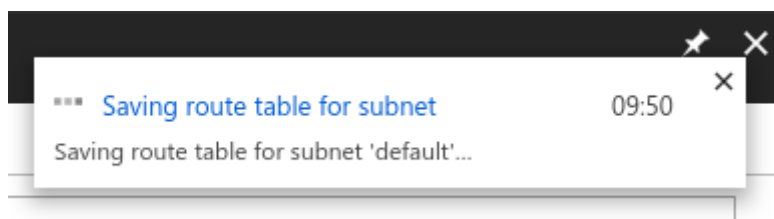


Left click on the *Subnet* section and select the subnet your PORTrockIT is using.

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

	<p>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.</p>
---	---

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

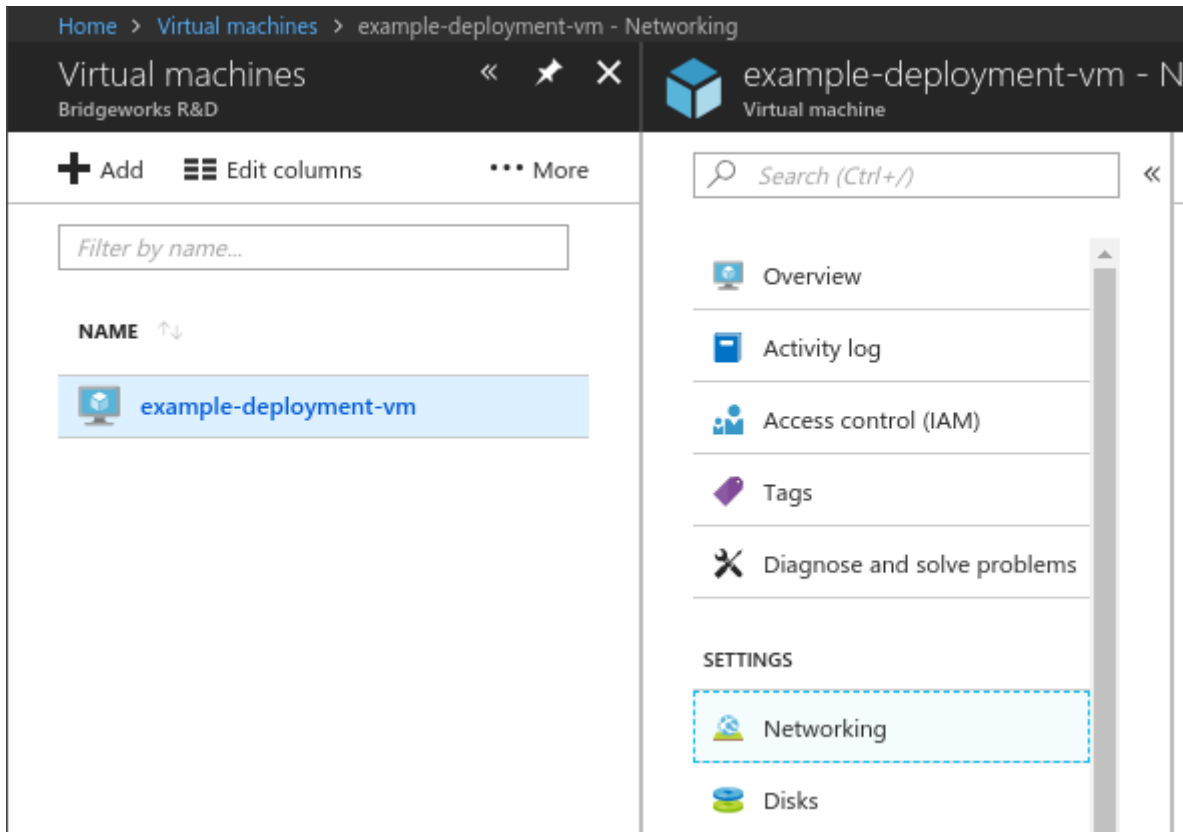


The next step is to add a routing rule for this subnet that will take all traffic destined for the other Node and pass it to the PORTrockIT virtual machine.

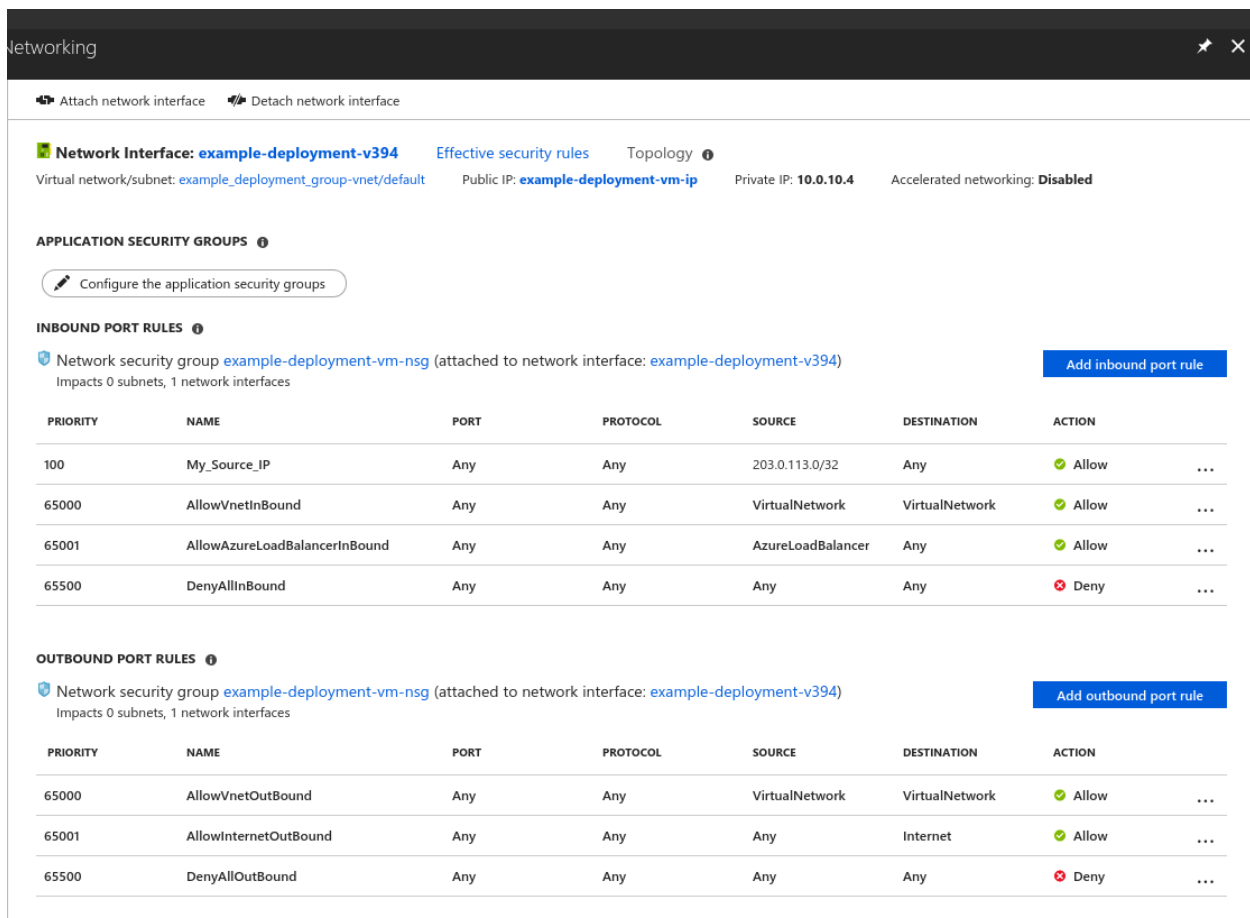
To complete this step you need to know the private IP address of the PORTrockIT.

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 top right of the page.



In this example the private IP of your PORTrockIT virtual machine is *10.0.10.4*; 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.

[All services](#) > [Microsoft.RouteTable-20220104153536](#) > [example-deployment-routes](#) >

Add route ...

example-deployment-routes

Route name *

route_to_other_bridgeworks_node ✓

Address prefix * ⓘ

10.0.11.0/24 ✓

Next hop type ⓘ

Virtual appliance ✓

Next hop address * ⓘ

10.0.10.4 ✓

i Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.

OK

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

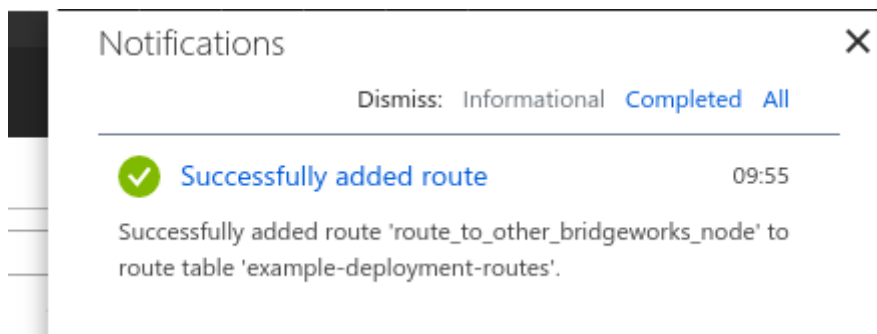
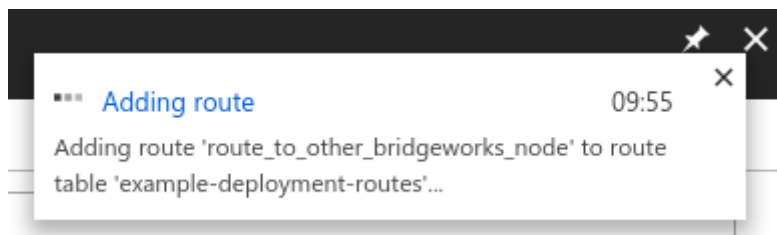
In this example:

Address prefix 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.

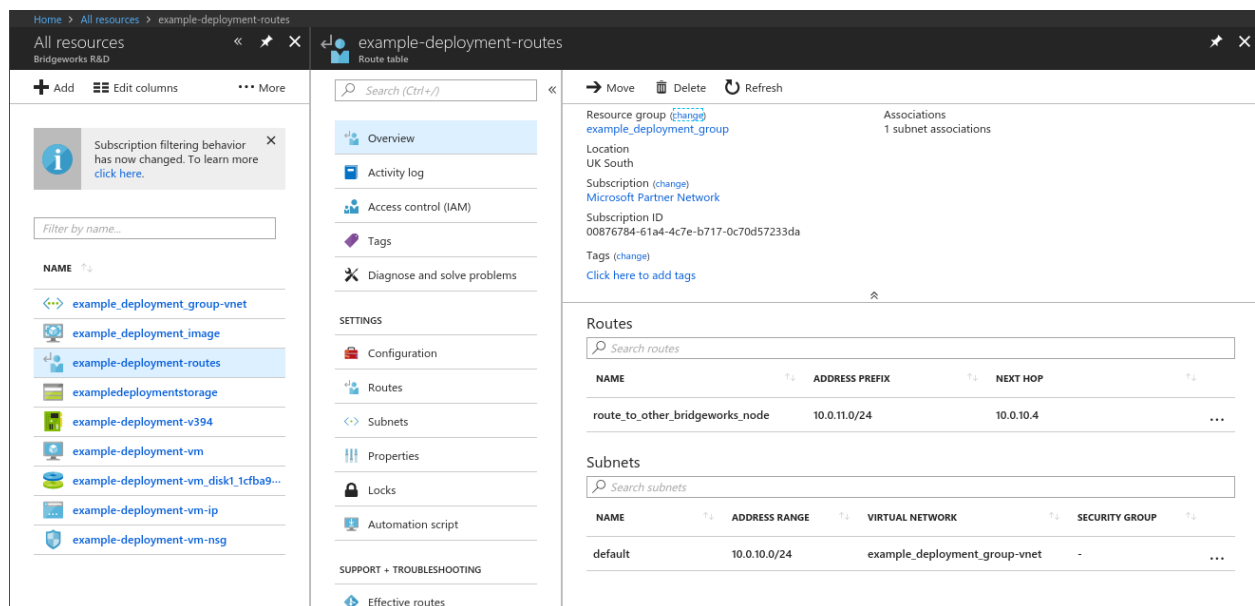
Next hop type You want to use the virtual machine in Azure. The *Virtual Appliance* selection results in the *Next hop address* field appearing.

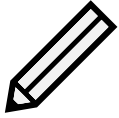
Next hop address The private IP of the PORTrockIT. This is the equivalent of the LAN port on a Node. All network traffic destined for the *Address prefix* IP range will get routed through this IP.

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

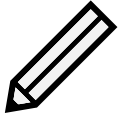


The overview section for your newly set up route table should now show the route to the network address range of the other Node, and the subnet that this routing applies to. In this example the subnet range covers the private IP of the PORTrockIT virtual machine.





Note: The route here will take any network traffic trying to get to any IP on the 10.0.11.0/24 range, and pass it to 10.0.10.4, which is your PORTrockIT. The PORTrockIT will in turn connect to another Node which has a LAN side network running the 10.0.11.0/24 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 10.0.10.4.

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*.

Home > All resources

All resources
Bridgeworks R&D

+ Add Edit columns Refresh Assign tags Delete

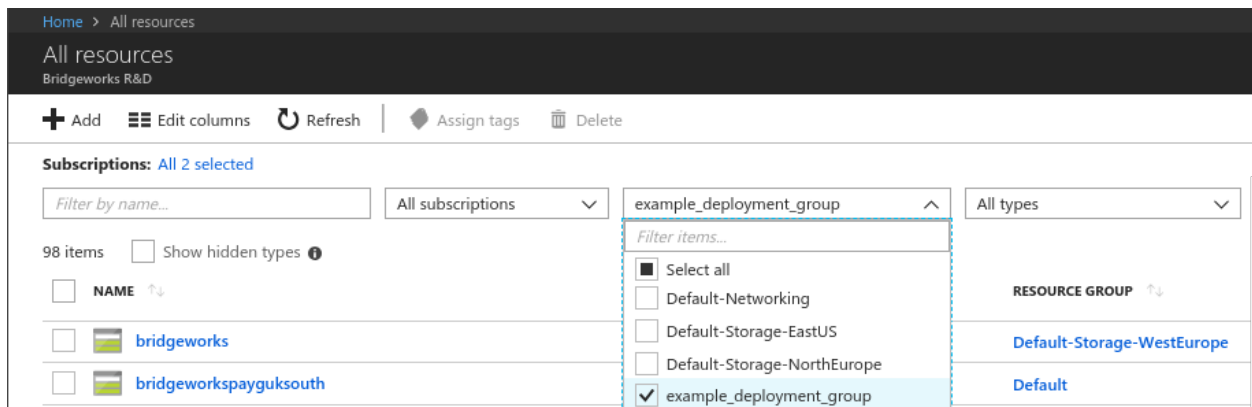
Subscriptions: All 2 selected

Filter by name... All subscriptions All resource groups All types

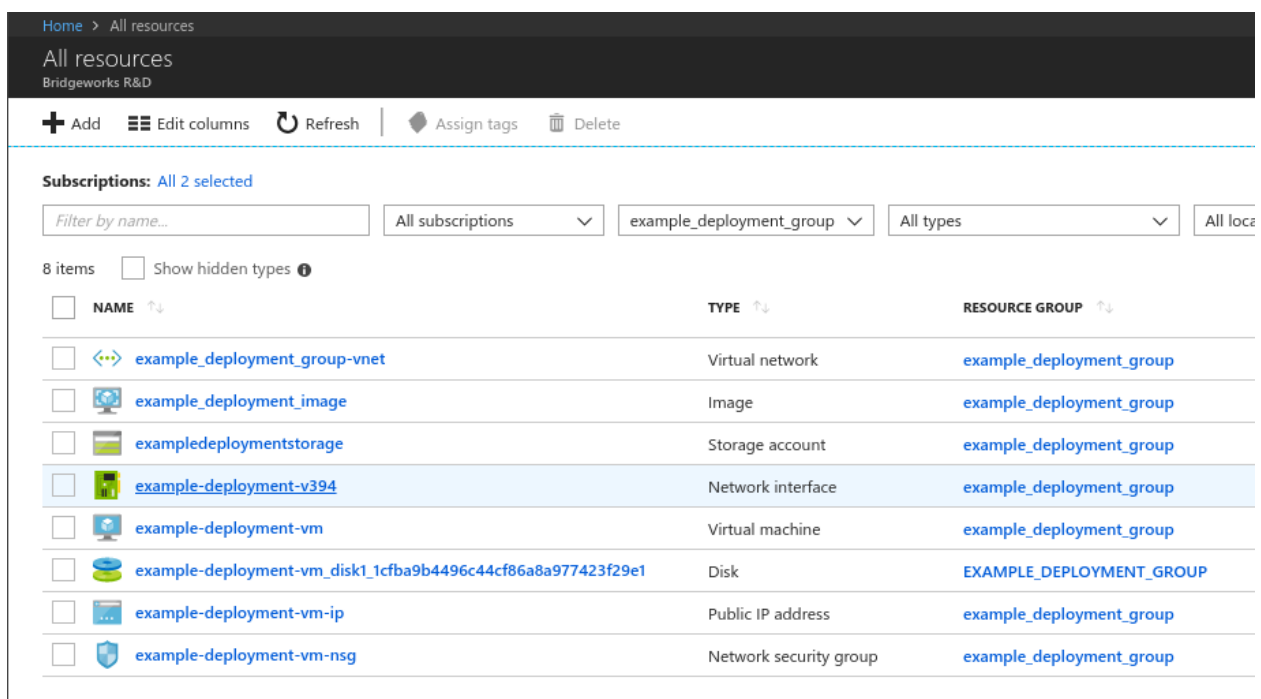
98 items Show hidden types

<input type="checkbox"/>	NAME ↑↓	TYPE ↑↓	RESOURCE GROUP ↑↓
<input type="checkbox"/>	bridgeworks	Storage account	Default-Storage-WestEurope
<input type="checkbox"/>	bridgeworkspayguksouth	Storage account	Default

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-v394*.



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.

Home > All resources

All resources

Bridgeworks R&D


+ Add Edit columns Refresh Assign tags Delete

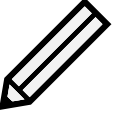
 Subscription filtering behavior has now changed. To learn more [click here](#).

Subscriptions: All 2 selected

Filter by name... All subscriptions example_deployment_group Network interfaces

1 items Show hidden types

NAME	TYPE	RESOURCE GROUP
<input type="checkbox"/>  example-deployment-v394	Network interface	example_deployment_group




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.

Home > All resources > example-deployment-v394

All resources

Bridgeworks R&D

+ Add Edit columns More

 Subscription filtering behavior has now changed. To learn more [click here](#).

Filter by name...

NAME

- [example_deployment_group-vnet](#)
- [example_deployment_image](#)
- [exampledeploymentstorage](#)
- [example-deployment-v394](#)
- [example-deployment-vm](#)
- [example-deployment-vm_disk1_1cfba9...](#)
- [example-deployment-vm-ip](#)
- [example-deployment-vm-nsg](#)

example-deployment-v394
Network interface

Search (Ctrl+*/*)

Move Delete

Overview

- Activity log
- Access control (IAM)
- Tags

SETTINGS

- IP configurations
- DNS servers
- Network security group
- Properties
- Locks
- Automation script

Resource group (change)
[example_deployment_group](#)

Location
UK South

Subscription (change)
[Microsoft Partner Network](#)

Subscription ID
00876784-61a4-4c7e-b717-0c70d57233da

Tags (change)
[Click here to add tags](#)

Private IP address
10.0.10.4

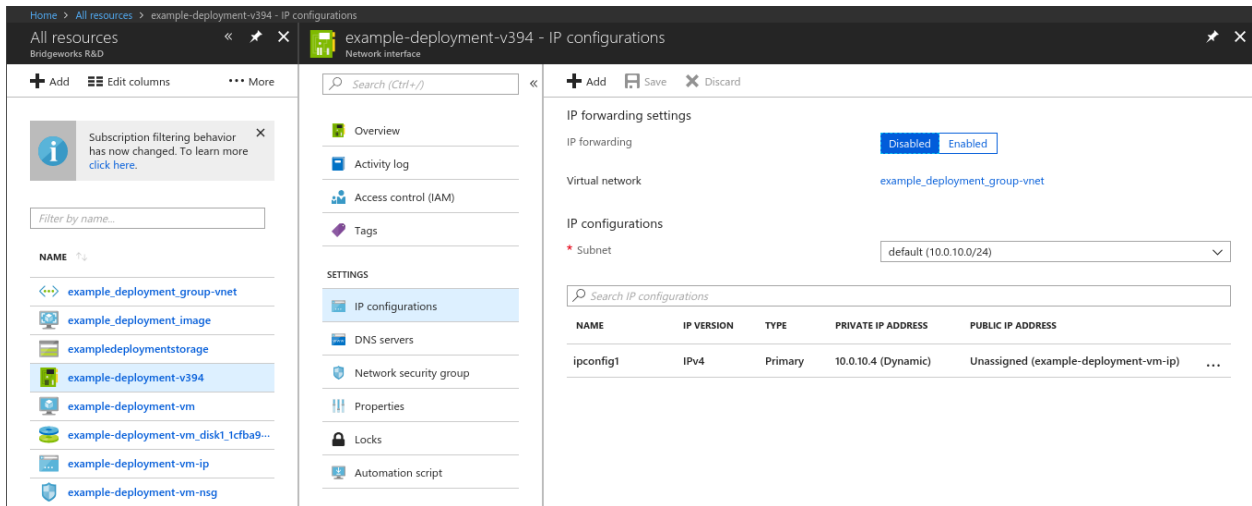
Virtual network/subnet
[example_deployment_group-vnet/default](#)

Public IP address
[example-deployment-vm-ip](#)

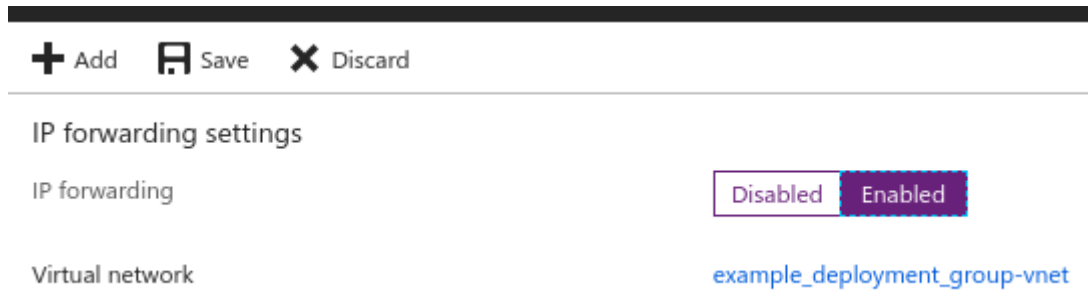
Network security group
[example-deployment-vm-nsg](#)

Attached to
[example-deployment-vm](#)

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

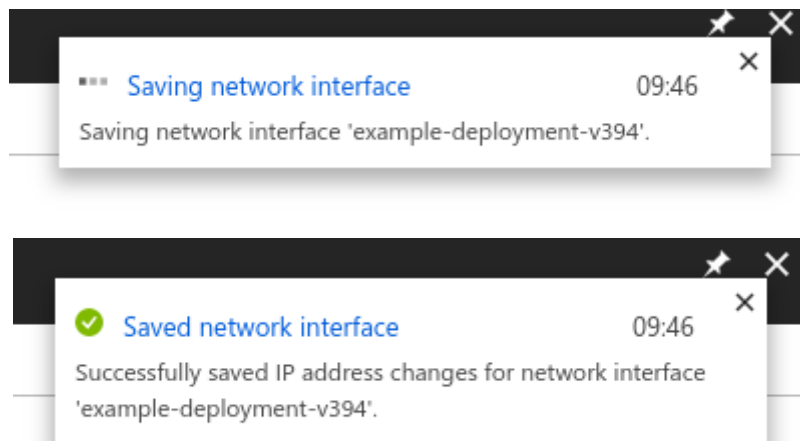


From this view, left click *enabled* on the toggle for *IP forwarding*.



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

Wait for the success notification.

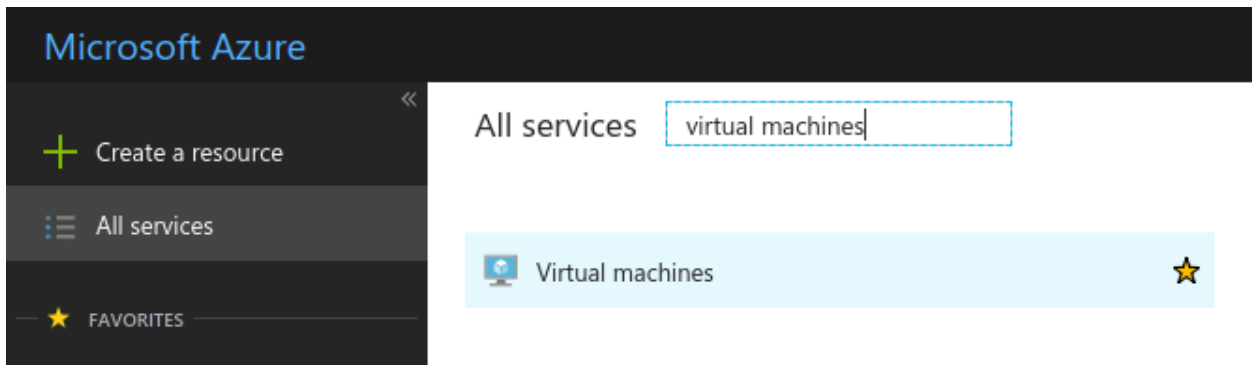


8 Accessing the GUI

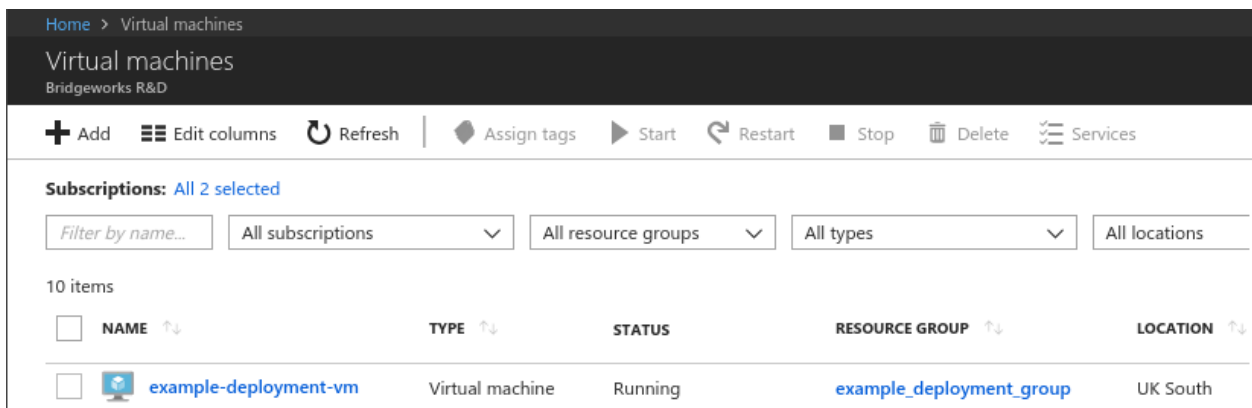
With a PORTrockIT virtual machine running there is now a web GUI available.

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.

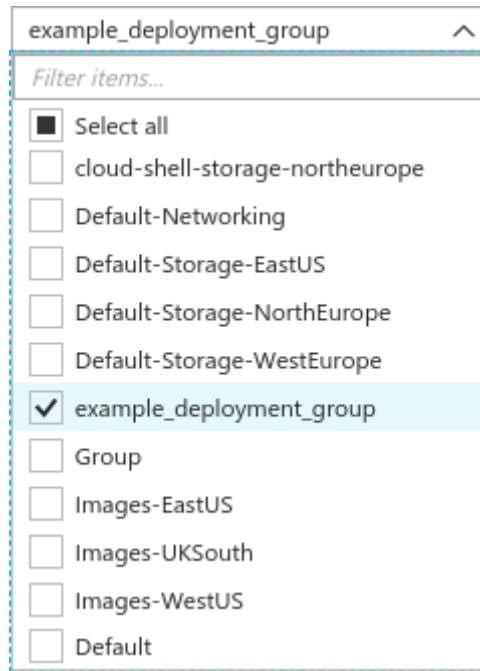


All deployed virtual machines in the account will be displayed in the *Virtual machines* section.

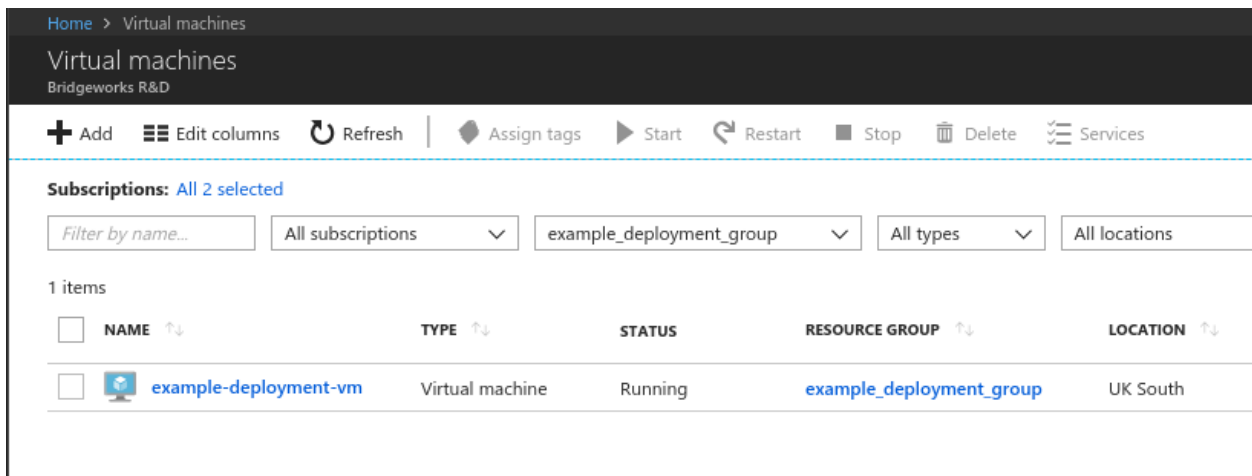


To reduce the list to your intended machine you can use filters. At the top of this list there are drop-down bars to filter the list. In this example the *All resource groups* drop-down will be changed:

- 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.

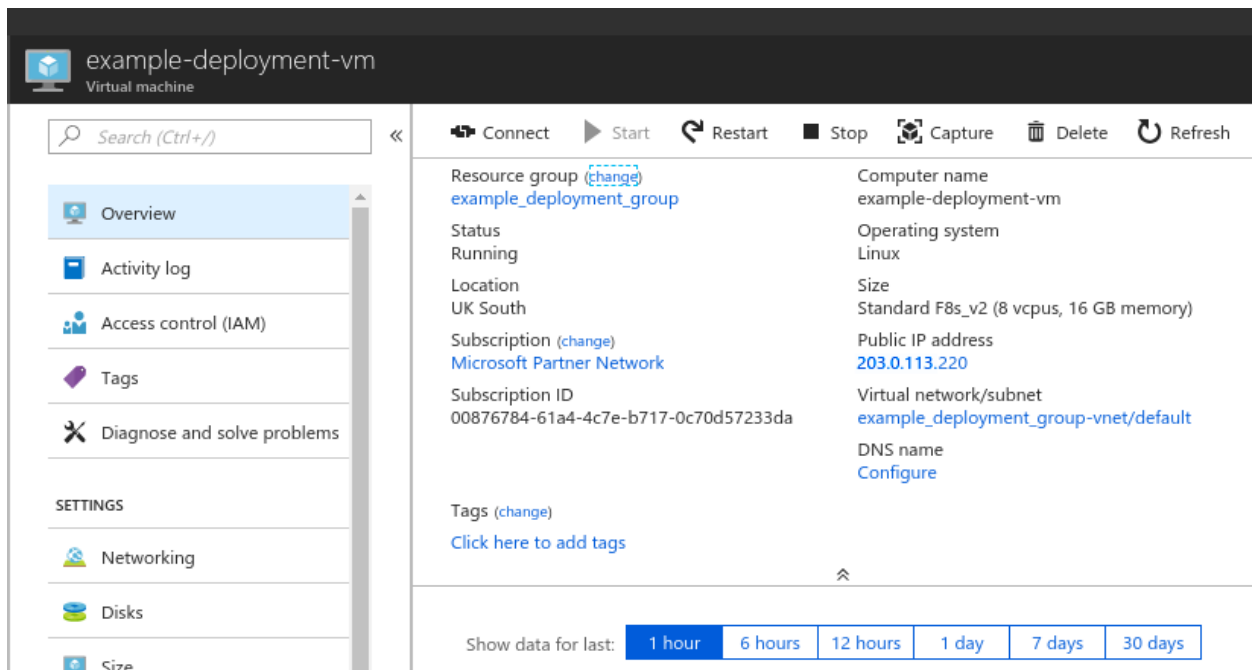


The result will be a filtered list of virtual machines attached to that group.



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

The following section contains links to other guides and FAQs. Support is available through our website: <https://support.4bridgeworks.com/>

The following resources are available online:

- [User Manuals](#)
- [Installation Guides](#)
- [General FAQ](#)
- [AWS FAQ](#)

If your question is not answered in our documentation, please [submit a ticket](#) through our website.

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 6.1.2.3: [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*.

Home > All resources
All resources
Bridgeworks R&D

+ Add Edit columns Refresh Assign tags Delete

Subscriptions: All 2 selected

Filter by name... All subscriptions All resource groups All types

98 items Show hidden types

NAME	TYPE	RESOURCE GROUP
bridgeworks	Storage account	Default-Storage-WestEurope
bridgeworkspayguksouth	Storage account	Default

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

Home > All resources
All resources
Bridgeworks R&D

+ Add Edit columns Refresh Assign tags Delete

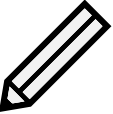
Subscriptions: All 2 selected

Filter by name... All subscriptions example_deployment_group All types

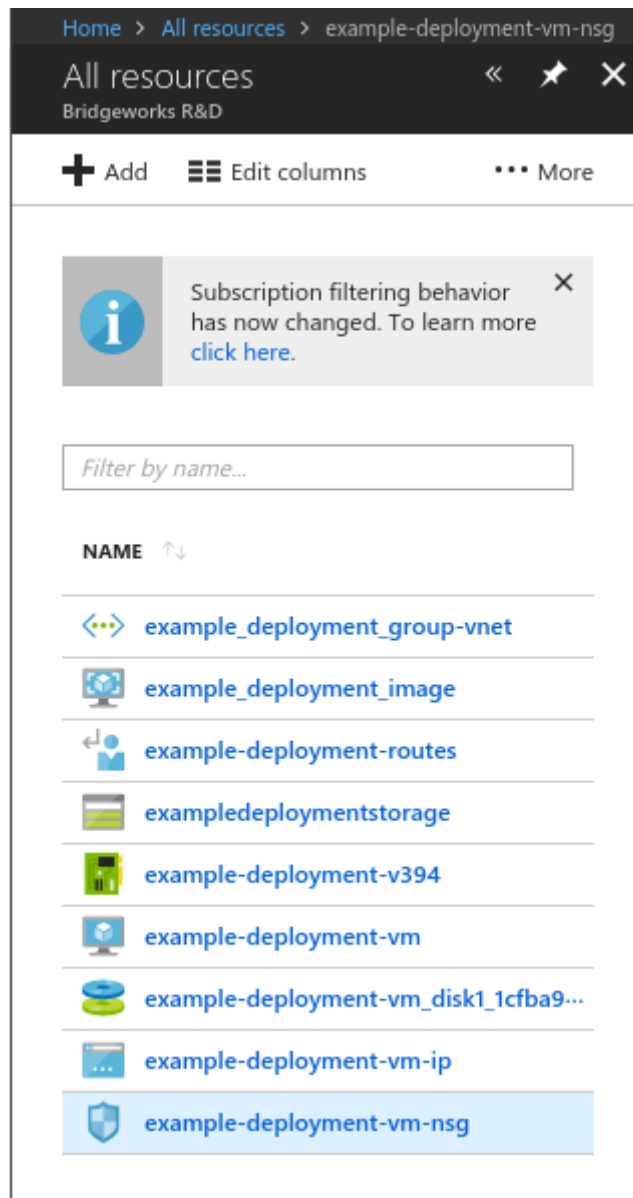
98 items Show hidden types

NAME	TYPE	RESOURCE GROUP
bridgeworks	Storage account	Default-Storage-WestEurope
bridgeworkspayguksouth	Storage account	Default

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.

example-deployment-vm-nsg
Network security group

Search (Ctrl+/) << → Move Delete Refresh

Resource group (change) [example_deployment_group](#) Security rules
1 inbound, 0 outbound
Location UK South Associated with
0 subnets, 1 network interfaces
Subscription (change) [Microsoft Partner Network](#)
Subscription ID 00876784-61a4-4c7e-b717-0c70d57233da
Tags (change) [Click here to add tags](#)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

SETTINGS

Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Automation script

MONITORING

Diagnostics logs

SUPPORT + TROUBLESHOOTING

Effective security rules

Inbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	My_Source_IP	Any	Any	203.0.113.0/32	Any	Allow ...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow ...
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow ...
65500	DenyAllInBound	Any	Any	Any	Any	Deny ...

Outbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow ...
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow ...
65500	DenyAllOutBound	Any	Any	Any	Any	Deny ...

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

example-deployment-vm-nsg - Inbound security rules
Network security group

Search (Ctrl+/) << + Add Default rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	My_Source_IP	Any	Any	203.0.113.0/32	Any	Allow ...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow ...
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow ...
65500	DenyAllInBound	Any	Any	Any	Any	Deny ...

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

SETTINGS

Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Automation script

Left click on *Add*.

BRIDGEWORKS R&D

Add inbound security rule

example-deployment-vm-nsg

Basic

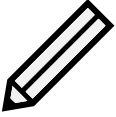
- * Source: IP Addresses
- * Source IP addresses/CIDR ranges: 203.0.113.100/32
- * Source port ranges: *
- * Destination: Any
- * Destination port ranges: *
- * Protocol: Any, TCP, UDP
- * Action: Allow, Deny
- * Priority: 110
- * Name: example_external_bridgeworks_node
- Description: This is the other Bridgeworks Node. All traffic to/from the 10.0.11.0/24 route will actually come through here.

Add

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 6.1.2.3: [Network Security Group](#). This adds the minimum functionality to access the PORTrockIT and connect it to the external Node.

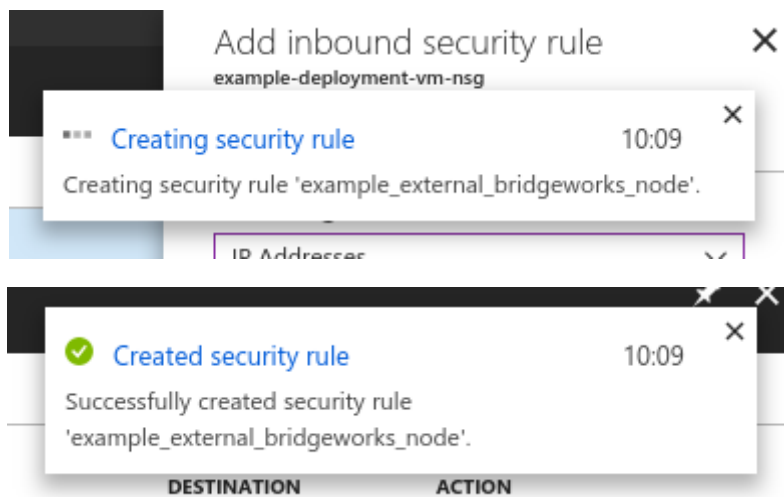


Note: Other services will need their relevant ports added to the list.

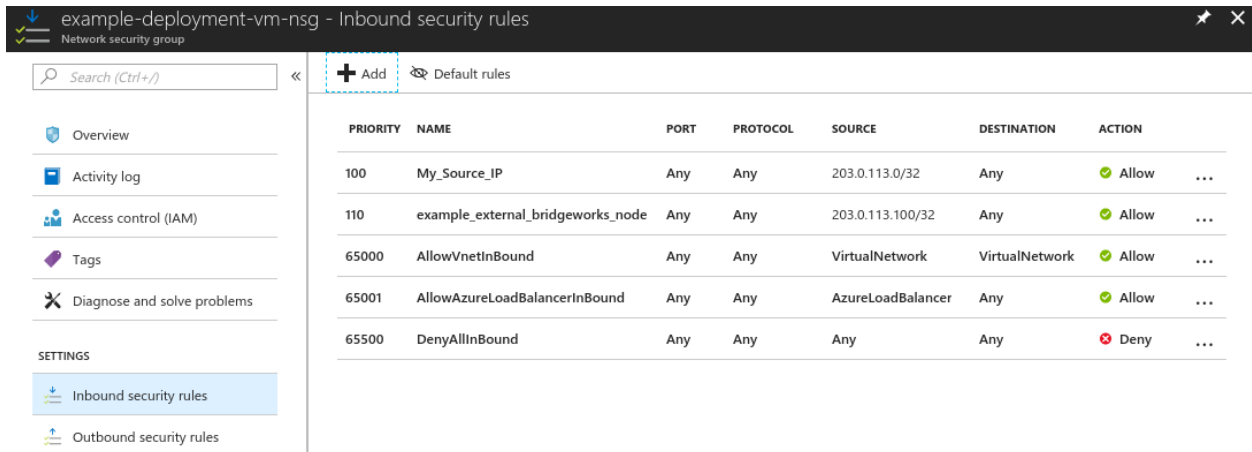
This connection will be the target when your PORTrockIT virtual machine routes network traffic destined for the 10.0.11.0/24 IP address range seen previously in this guide.

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

Wait for the success notification to occur.



The screenshot shows the 'Add inbound security rule' dialog box for the 'example-deployment-vm-nsg' network security group. A notification message indicates 'Creating security rule' for 'example_external_bridgeworks_node'. A second notification message shows 'Created security rule' successfully.



The screenshot displays the 'example-deployment-vm-nsg - Inbound security rules' configuration page. The table below shows the configured rules.

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	My_Source_IP	Any	Any	203.0.113.0/32	Any	Allow
110	example_external_bridgeworks_node	Any	Any	203.0.113.100/32	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

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.