

Deploying in Microsoft Azure

- Prerequisites and Guidelines, on page 1
- Deploying Nexus Dashboard in Azure, on page 6

Prerequisites and Guidelines



Note Only the Nexus Dashboard Orchestrator service can be deployed on a cloud-hosted form factor.

Before you proceed with deploying the Nexus Dashboard cluster in Microsoft Azure, you must:

• Ensure that the Azure form factor supports your scale and services requirements.

Scale and services support and co-hosting vary based on the cluster form factor. You can use the Nexus Dashboard Capacity Planning tool to verify that the cloud form factor satisfies your deployment requirements.

- Review and complete the general prerequisites described in the Deployment Overview.
- Review and complete any additional prerequisites described in the *Release Notes* for the services you plan to deploy.
- Have appropriate access privileges for your Azure account and subscription.
- Have created a resource group for your Nexus Dashboard cluster resources.



Note The resource group must be empty and not contain any existing objects. Resource groups with existing objects cannot be used for Nexus Dashboard deployment.

To create a resource group:

- In the Azure portal, navigate to **All Resources** > **Resource Groups**.
- Click +Add to create a new resource group.
- In the **Create a resource group** screen, provide the name of the subscription you will use for your Nexus Dashboard cluster, the name for the resource group (for example, nd-cluster), and the region.

- Ensure that the CPU family used for the Nexus Dashboard VMs supports AVX instruction set.
- Create an SSH key pair.

A key pair consists of a private key and a public key, you will be asked to provide the public key when creating the Nexus Dashboard nodes.



Note

You will need to use the same machine where you create the public key for a one-time login into each node to enable general SSH login during cluster deployment procedure.

Creating SSH keys is described in Generating an SSH Key Pair in Linux or MacOS, on page 2 and Generating an SSH Key Pair in Windows, on page 3 sections below.

Generating an SSH Key Pair in Linux or MacOS

These procedures describe how to generate an SSH public and private key pair in Linux or MacOS. For instructions on generate an SSH public and private key pair in Windows, see Generating an SSH Key Pair in Windows, on page 3.

Procedure

Step 1 On your Linux virtual machine or Mac, create a public and private key pair using ssh-keygen, directing the output to a file.

```
# ssh-keygen -f filename
```

For example:

ssh-keygen -f azure_key

Output similar to the following appears. Press the Enter key without entering any text when you are asked to enter a passphrase (leave the field empty so that there is no passphrase).

```
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in azure_key.
Your public key has been saved in azure_key.pub.
The key fingerprint is:
SHA256:gTsQIIAadjgNsgcguifIloh4XGpVWMdcXVV6U0dyBNs
```

Step 2 Locate the public and private key files that you saved.

1s

Two files should be displayed, where:

- The file with the .pub suffix contains the public key information
- The file with the same name, but with no suffix, contains the private key information

For example, if you directed the output to a file named azure key, you should see the following output:

ls
azure_key
azure_key.pub

In this case:

- The azure key.pub file contains the public key information
- The azure key file contains the private key information
- **Step 3** Open the public key file and copy the public key information from that file, without the username@hostname information at the end.
 - **Note** The private key file is not used in the installation process. However, you might need it for other reasons, such as logging into your Nexus Dashboard nodes through SSH.

Generating an SSH Key Pair in Windows

These procedures describe how to generate an SSH public and private key pair in Windows. For instructions on generate an SSH public and private key pair in Linux, see Generating an SSH Key Pair in Linux or MacOS, on page 2.

Procedure

 Step 1
 Download and install the PuTTY Key Generator (puttygen): https://www.puttygen.com/download-putty

Step 2Run the PuTTY Key Generator by navigating to Windows > Start Menu > All Programs > PuTTY > PuTTYgen.You will see a window for the PuTTY Key Generator on your screen.

PuTTY Key Generator			?	×
ile Key Conversions Help Key No key.				
Actions Generate a public/private key pair			Counts	
			Generate	
Load an existing private key file			Load	
Load an existing private key file Save the generated key		Save public key	Load Save private key	
Load an existing private key file Save the generated key Parameters		Save public key	Load Save private key	
Load an existing private key file Save the generated key Parameters Type of key to generate:	OECDSA	Save public key	Load Save private key	

Step 3 Click Generate.

A screen appears, asking you to move the mouse over the blank area to generate a public key.

Step 4 Move your cursor around the blank area to generate random characters for a public key.

e Key	Conversions	Help						
Key								
Please g	enerate some rand	domness t	by moving t	he mouse	e over the bla	ank area.		
Actions								
Actions Generat	e a public/private k	key pair				Ge	enerate	
Actions Generat Load an	e a public/private k existing private ke	key pair y file				Ge	enerate Load	
Actions Generat Load an	e a public/private k existing private ke	key pair y file		Cause		Ge	enerate Load	
Actions Generat Load an Save the	e a public/private k existing private ke e generated key	key pair y file		Save p	ublic key	Ge	enerate Load private ke	ey .
Actions Generat Load an Save the Paramet	e a public/private k existing private ke e generated key ers	key pair y file		Save p	ublic key	Ge Save	enerate Load private ke	ey -
Actions Generat Load an Save the Paramet Type of © RSA	e a public/private k existing private ke e generated key ers key to generate: DSA	key pair y file) ECDS	Save p	ublic key	Ga	enerate Load private ke	ey SA)

Step 5 Save the public key.

- a) Navigate to a folder on your laptop where you want to save the public key file and create a text file for this public key.
- b) Copy the information in the PuTTY Key Generator.

Copy the public key information in the window, with these inclusions and exclusions:

- Including the ssh-rsa text at the beginning of the public key.
- Excluding the following text string at the end:
 - == rsa-key-<date-stamp>

Truncate the key so that it does not include the **== rsa-key-<date-stamp>** text string at the end.

Note In the next set of procedures, you will paste the public key information into the Azure ARM template. If the form does not accept the key in this format, add == back to the end of the key, as this format is required in some regions.

If the key is not in the correct format, the Nexus Dashboard will not complete its installation.

Name	PuTTY Key Gener	ator		? ×
azure_key.ppk	File Key Conversion	ons Help		
 zure_key.ppk zure_key.pub putty.exe puttygen.exe 	Key <u>Public key for pasting</u> AAAAB3NzaC tyc2E WMkMWIOLEN+N +HMwd3dbic7Bqc1 WeAwsIgabag2AW Key fingerprint:	a into OpenSSH autho AAAABJQAAAQEAIQ WFKinKNjoNVGgow3 ecAy172Pvo2 yW22 V4CAGsyACWT9H8Qv sshrsa 2048 48:de	rized_keys file: 507UF0d3ks:MV0GAWYr FeYY+ ISENo/AymwWxvRAJUkY WXbaCYFhNVs2X7TFrGA vae:5c16.ce.b3/3d/e8/23:	TexKox4UACLZV AJS&xPKchYuTy IOAY77Xtx:035XIA 76:61:54:46:41:01
	Key gomment: rsa-key-20190708			
	Key passphrase: Confirm passphrase:			
	Actions			
	Generate a public/pri	ivate key pair		Generate
	Load an existing prive	ate key file		Load
	Save the generated i	key	Save pyblic key	Save private key
	Parameters Type of key to gener	ate:) <u>D</u> SA 〇 <u>B</u> enerated key:	CDSA () ED25519	O SSH- <u>1</u> (RSA) 2048

c) Paste the information in the public key text file that you created in 5.a, on page 5 and save the file, giving it a unique file name.

This public key text file will now contain a key that is on a single line of text. You will need the information in this public key text file in the next set of procedures.

Note Do not save the public key using the **Save public key** option in the PuTTY Key Generator. Doing so saves the key in a format that has multiple lines of text, which is not compatible with the Nexus Dashboard deployment process.

Step 6 Save the private key.

a) Click Save private key.

A screen appears, asking if you want to save the file without a passphrase. Click Yes on this screen.

b) Navigate to a folder on your laptop and save the private key file, giving it a unique file name.

Note

The private key file is not used in the installation process. However, you might need it for other reasons, such as logging into your Nexus Dashboard nodes through SSH.

Deploying Nexus Dashboard in Azure

This section describes how to deploy Cisco Nexus Dashboard cluster in Microsoft Azure.

Before you begin

• Ensure that you meet the requirements and guidelines described in Prerequisites and Guidelines, on page 1.

Procedure

Step 1	Su a) b)	bscribe to Cisc Log into your In the search You will be re	o Nexus Dashboard product in Azure Marketplace. Azure account and browse to https://azuremarketplace.microsoft.com field, type Cisco Nexus Dashboard and select the option that is presented. e-directed to the Nexus Dashboard Azure Marketplace page.		
	c) Click Get it now.d) In the Select a plan dropdown, select the version and click Create.				
Step 2	Pro a) b) c) d)	ovide Basic inf From the Sub From the Res Guidelines, o From the Reg In the Passwo	ormation. Scription dropdown, select the subscription you want to use for this. ource group dropdown, select the resource group you created for this as part of Prerequisites and n page 1. gion dropdown, select the region where the template will be deployed. ord and Confirm Password fields, provide the admin password for the nodes.		
		This passwor GUI's admin	d will be used for the Nexus Dashboard's rescue-user login, as well as the initial password for the user.		
		Note	You must provide the same password for all nodes or the cluster creation will fail.		
	e) f)	In the SSH pr Guidelines, o	ablic key field, paste the public key from the key pair you generated as part of the Prerequisites and n page 1 section.		
Step 3	Pr	ovide ND Setti	ngs information.		
	a) b) c)	Provide the C In the Image In the Virtua	 Suster Name. Version dropdown, verify that the correct version is selected. I Network Name field, provide the name for a VNET that will be created for your cluster. 		

The VNET must not already exist and will be created for you during deployment. If you provide an already existing VNET, the deployment cannot proceed.

d) In the Subnet Address Prefix field, provide a subnet within the VNET.

The subnet must be a /24 subnet and it must be different from the default VNET subnet you defined when creating the VNET.

e) In the **External Subnets** field, provide the external network allowed to access the cluster.

For example, 0.0.0/0 to be able to access the cluster from anywhere.

- f) Click Next to proceed to the next screen.
- **Step 4** In the **Review + create** page, review information and click **Create** to deploy the cluster.
- **Step 5** Wait for the deployment to complete, then start the VMs.
- **Step 6** Note down all nodes' public IP addresses.

After all instances are deployed, navigate to the Azure console, select each VM, and note down all nodes' public IP addresses. You will provide this information to the GUI bootstrap wizard in the following steps.

Also note which is the "first" node, which will be indicated by the node's VM name vm-node1-<cluster-name>. You will use this node's public IP address to complete cluster configuration.

 Step 7
 Open your browser and navigate to https://<first-node-public-ip> to open the GUI.

 Note
 You must use the public IP address of the first node (vm-node1-<cluster-name>) or cluster configuration cannot be completed.

The rest of the configuration workflow takes place from the first node's GUI. You do not need to log in to or configure the other two nodes directly.



Enter the password you provided for the first node and click Login

Step 8

Provide the **Cluster Details**.

In the Cluster Details screen of the Cluster Bringup wizard, provide the following information:

راب، Nexus Dashboard cisco					2
OverviewManage	Cluster Bringup Answer some questions, select the se	rvices you want to enable and have Nexus Da	shboard ready to use in a few minutes.		
⊙ Analyze Ĵ₀ Admin	 Configuration Node Details Deployment Mode Summary 	Configuration Provide the cluster name and configure the Nexus Dashboard Cluster Name • r nd-cluster Diseable IPv6 DNS DNS Provider IP Address • 171.70.168.183 Add DNS Provider DNS Search Domain Add DNS Search Domain	DNS, NTP and Proxy to set up Nexus Da	ashboard and bring up the user int	erface
	e	NTP NTP Authentication NTP Host T7.168.38.65 Add NTP Host Name/IP Address	Key ID	Preferred true	^ / @
	9	Proxy Ignore Hosts Add Ignore Host Proxy Server * Authentication required for proxy			Skip Proxy A
	h	Advanced Settings App Network * () [172.17.0.1/16 Service Network * () [10.80.0.0/16 App Network IPv6 () [2000::/108 Service Network IPv6 () [3000::/108)))		

a) Provide the Cluster Name for this Nexus Dashboard cluster.

The cluster name must follow the RFC-1123 requirements.

- b) (Optional) If you want to enable IPv6 functionality for the cluster, check the Enable IPv6 checkbox.
- c) Click +Add DNS Provider to add one or more DNS servers.

After you've entered the information, click the checkmark icon to save it.

d) (Optional) Click +Add DNS Search Domain to add a search domain.

After you've entered the information, click the checkmark icon to save it.

e) (Optional) If you want to enable NTP server authentication, enable the **NTP Authentication** checkbox and click **Add NTP Key**.

In the additional fields, provide the following information:

- **NTP Key** a cryptographic key that is used to authenticate the NTP traffic between the Nexus Dashboard and the NTP server(s). You will define the NTP servers in the following step, and multiple NTP servers can use the same NTP key.
- **Key ID** each NTP key must be assigned a unique key ID, which is used to identify the appropriate key to use when verifying the NTP packet.
- Auth Type this release supports MD5, SHA, and AES128CMAC authentication types.
- Choose whether this key is Trusted. Untrusted keys cannot be used for NTP authentication.
- **Note** After you've entered the information, click the checkmark icon to save it.

For the complete list of NTP authentication requirements and guidelines, see Prerequisites and Guidelines.

f) Click +Add NTP Host Name/IP Address to add one or more NTP servers.

In the additional fields, provide the following information:

- NTP Host you must provide an IP address; fully qualified domain name (FQDN) are not supported.
- **Key ID** if you want to enable NTP authentication for this server, provide the key ID of the NTP key you defined in the previous step.

If NTP authentication is disabled, this field is grayed out.

• Choose whether this NTP server is **Preferred**.

After you've entered the information, click the checkmark icon to save it.

Note If the node into which you are logged in is configured with only an IPv4 address, but you have checked **Enable IPv6** in a previous step and provided an IPv6 address for an NTP server, you will get the following validation error:

NTP Host*	Key ID	Preferred		
2001:420:28e:202a:5054:ff:fe6f:b3f6		true	/	
Add NTP Host Name/IP Address				

 $\underline{\mathbb{A}}$ Could not validate one or more hosts Can not reach NTP on Management Network

This is because the node does not have an IPv6 address yet (you will provide it in the next step) and is unable to connect to an IPv6 address of the NTP server.

In this case, simply finish providing the other required information as described in the following steps and click **Next** to proceed to the next screen where you will provide IPv6 addresses for the nodes.

If you want to provide additional NTP servers, click +Add NTP Host again and repeat this substep.

g) Provide a Proxy Server, then click Validate it.

For clusters that do not have direct connectivity to Cisco cloud, we recommend configuring a proxy server to establish the connectivity. This allows you to mitigate risk from exposure to non-conformant hardware and software in your fabrics.

You can also choose to provide one or more IP addresses communication with which should skip proxy by clicking +Add Ignore Host.

The proxy server must have the following URLs enabled:

```
dcappcenter.cisco.com
svc.intersight.com
svc.ucs-connect.com
svc-static1.intersight.com
svc-static1.ucs-connect.com
```

If you want to skip proxy configuration, click Skip Proxy.

- h) (Optional) If your proxy server required authentication, enable **Authentication required for Proxy**, provide the login credentials, then click **Validate**.
- i) (Optional) Expand the Advanced Settings category and change the settings if required.

Under advanced settings, you can configure the following:

Provide custom App Network and Service Network.

The application overlay network defines the address space used by the application's services running in the Nexus Dashboard. The field is pre-populated with the default 172.17.0.1/16 value.

The services network is an internal network used by the Nexus Dashboard and its processes. The field is pre-populated with the default 100.80.0.0/16 value.

If you have checked the **Enable IPv6** option earlier, you can also define the IPv6 subnets for the App and Service networks.

Application and Services networks are described in the Prerequisites and Guidelines section earlier in this document.

- j) Click Next to continue.
- **Step 9** In the **Node Details** screen, provide the node's information.
 - a) Click the Edit button next to the first node.
 - b) Provide the node's Name.

The **Management Network** and **Data Network** information will be already populated from the VNET subnet you have configured before deploying the cluster.

The cluster creates six subnets from the given VNET, from which the data and management networks will be allocated for the cluster's three nodes.

c) Leave IPv6 addresses and VLAN fields blank.

Cloud Nexus Dashboard clusters do not support these options.

- d) Click **Save** to save the changes.
- **Step 10** Click Add Node to add the second node to the cluster.

The Node Details window opens.

a) Provide the node's Name.

b) In the **Credentials** section, provide the node's **Public IP Address** and the password you provided during template deployment, then click **Verify**.

The IP address and password are used to pull that node's **Management Network** and **Data Network** information, which will be populated in the fields below.

c) Ensure that you select Primary for the node type.

Only 3-node clusters are supported for cloud deployments, so all nodes must be Primary.

- d) Click Save to save the changes.
- **Step 11** Repeat the previous step to add the 3rd node.
- Step 12 In the Node Details page, click Next to continue.

Step 13 Choose the **Deployment Mode** for the cluster.

a) Choose the services you want to enable.

Prior to release 3.1(1), you had to download and install individual services after the initial cluster deployment was completed. Now you can choose to enable the services during the initial installation.

Note Cloud deployments support the Orchestrator service, so you must not select any other deployment modes.

cisco Nexus Dashboard		1
 Urefree Nexus Dashboard Overview Manage Analyze Amin 	Custor Bringuzation Configuration Configuration	tion through telemetry and smart
		Back

 b) Click Add Persistent Service IPs/Pools to provide one or more persistent IPs required by Insights or Fabric Controller services.

For more information about persistent IPs, see the Prerequisites and Guidelines section.

- c) Click Next to proceed.
- **Step 14** In the **Summary** screen, review and verify the configuration information, click **Save**, and click **Continue** to confirm the correct deployment mode and proceed with building the cluster.

During the node bootstrap and cluster bring-up, the overall progress as well as each node's individual progress will be displayed in the UI. If you do not see the bootstrap progress advance, manually refresh the page in your browser to update the status.

It may take up to 30 minutes for the cluster to form and all the services to start. When cluster configuration is complete, the page will reload to the Nexus Dashboard GUI.

Step 15 Verify that the cluster is healthy.

It may take up to 30 minutes for the cluster to form and all the services to start.

After the cluster becomes available, you can access it by browsing to any one of your nodes' management IP addresses. The default password for the admin user is the same as the rescue-user password you chose for the first node. During this time, the UI will display a banner at the top stating "Service Installation is in progress, Nexus Dashboard configuration tasks are currently disabled":

NTP Host*	Key ID	Preferred		
2001:420:28e:202a:5054:ff:fe6f:b3f6		true	/ โ	
+ Add NTP Host Name/IP Address				

△ Could not validate one or more hosts Can not reach NTP on Management Network

After all the cluster is deployed and all services are started, you can check the **Overview** page to ensure the cluster is healthy:

Overview	Welcome, admin Refresh
🖉 Manage	Platform View Journey: Getting Started
O Analyze	Add Nexus Daabboard Cluster
al _o Admin	Overall System Health Ok Cluster Health Ok Cluster Health Ok Connectivity to Intersight Not Connected Setup Intersight
	2 You have 2 services enabled on your platform Fabric Controller Ifev19 Healthy Healthy Healthy
	O sites are currently onboarded on Nexus Dashboard O total Total
	ifav19 Nodes
	6 Nodes are currently a part of this cluster. 6 out of 6 nodes are healthy. View All Nodes →

Alternatively, you can log in to any one node via SSH as the rescue-user using the password you provided during node deployment and using the acs health command to check the status::

• While the cluster is converging, you may see the following outputs:

```
$ acs health
k8s install is in-progress
$ acs health
k8s services not in desired state - [...]
```

```
$ acs health
k8s: Etcd cluster is not ready
```

• When the cluster is up and running, the following output will be displayed:

```
$ acs health
All components are healthy
```

Note In some situations, you might power cycle a node (power it off and then back on) and find it stuck in this stage:

deploy base system services

This is due to an issue with etcd on the node after a reboot of the pND (Physical Nexus Dashboard) cluster.

To resolve the issue, enter the acs reboot clean command on the affected node.

Step 16 Update the nodes' security group with required ports.

This step describes how to update the Nexus Dashboard nodes' instances with the required port configuration for on-boarding Cisco NDFC sites. If you do not plan on on-boarding any NDFC sites to your Nexus Dashboard cluster, you can skip this step.

Newch (tode/) 1 Ad Newch (tode/) Ad Add Add Itel by name Potroal Access control (MA) Dagnose and solve problem String Dagnose and solve problem String Dagnose and solve problem String Doton/secutivy rules Doton/secutivy rules Dagnose and solve problem String Dagnose and solve problem String Dagnose and solve problem String Doton/secutivy rules Doton/secutivy rules Dagnose and solve problem String Dagnose and solve problem String Doton/secutivy rules Doton/secutivy rules Dagnose and solve problem String Doton/secutivy rules Dagnose and solve problem String Doton/secutivy rules Dagnose and solve problem String Doton/secutivy rules Dagnose and solve problem	Dashboard > venkat-nd-rg > nsg-data	s-prod1-2-1-103	2 2 Inbound security	rules		Add inbound security rule	
 Overview Actively logs Filter by name Der was all Source and source of the disk logs Source and source and source	P Search (Cmd+/)	d 🔰 Add 🧠 Hide defa	ult rules 🜔 Refresh 🗎 Delete	Rive feedback			
Activity Log Ac	Overview					Source O Any	
Image: Priority 1: Name 1: Port 1: Protect 1: * Tag: 300 * AlconstandChutter Any Any >> Dagnose and solve problem: 300 * AlconstandChutter Any Any >> Setting: 6000 AlconstandChutter Any Any Pertination ○ Any Any >> Indonal Security rules 6000 AlconstandChutter Any Any Any Secure O Secure O </th <th>Activity log</th> <th>, Filter by name</th> <th>Port =:</th> <th>Protocol == all</th> <th>Source == all</th> <th>5 mm</th> <th></th>	Activity log	, Filter by name	Port =:	Protocol == all	Source == all	5 mm	
• tag: 300 ● Alcon/Databal/Databal/Ary Ary ● Diagnose and solve problems 320 ▲ Dem/Allotatabound Ary Ary Setting: 65000 Alcon/Alcotatabound Ary Ary ● Inbound security rules 65000 Dem/Allotatabound Ary Ary ● Alcon/Datababound Ary Ary Ary ● Alcon/Datababound Ary Ary Service ○ Cutation ○ ● Alcon/Datababound Ary Ary Ary Service ○ Cutation ○ ● Alcon/Datababound Ary Ary Ary Service ○ Cutation ~ ● Alcon/Datababound Ary Ary Ary Cutation ~ Ary ● Subnets • • • • • • • • Alcos •	Access control (IAM)	Priority 1	Name 1	Port 1	Protocol 1+	443	
Diagnose and solve problem 330 ▲ DreyAll/Detainbound Any Any Settings 65000 Allow/AutreficaddBalancetin Any Any I hobound security rules ● 65500 DenyAllinBound Any Outbound security rules ● 65500 DenyAllinBound Any Network interfaces ● 65500 DenyAllinBound Any Network interfaces ● ● ● Outbourd security rules ● ● Sothets ● ● II Properties ● 0 Locks ● ● Monitoring ● 0 I bags ontic settings ● I bags ont settings ●	🔮 Tags	300	AllowDataNDCluster	Any	Any	Destination ()	
string: 65000 Allow/hethibuod Any Any 65001 Allow/Lutt.addBlaineein- Any Any 65000 DenyAllinBound Any Any 65000 Deny Cataon 7 Any Any 65000 Deny Cataon 7 Any Any 65000 Deny Cataon 7 Any Any 65000 Deny 7 Deny 7 Deny 7 Deny 8 Deny 8 Deny 9 Den	Diagnose and solve problems	320	🛕 DenyAliDataInbound	Any	Any	Any	
Atom inbound security rules 0 0 0 </td <td>Settinge</td> <td>65000</td> <td>AllowVnetInBound</td> <td>Any</td> <td>Any</td> <td>Service ①</td> <td></td>	Settinge	65000	AllowVnetInBound	Any	Any	Service ①	
Indiand Security rules ○ Outbourd security rules ○ National security rules ○ Subsets ○ Subsets ○ Locks Monitoring ○ Alerts ○ Dagnostic settings ○ Logis ○ Notional Security rules ○ Solow logis Antomation ○ Locks ○ Locks Notional Security rules ○ Englishing S ○ Locks ○ Solow logis ○ Locks ○ Locks ○ Locks Notional Security rules ○ Solow logis ○ Locks ○ Locks ○ Locks ○ Locks ○ Locks ○ Locks ○ Notional Security rules ○ Locks	takened encoder and	65001	AllowAzureLoadBalancerIn	Any	Any	Custom	
□ Outword Security rules 443 □ □ ○ Nuthood Security rules Protocol ○ Subnets ○ Protocol ○ I Properties ○ TCP ○ Locks ○ UOP Monitoring ○ UOP ◎ Any ○ UOP ◎ Any ○ UOP ○ J Cold ○ UOP ◎ Locks ○ UOP ◎ Any ○ UOP ◎ Locks ○ Locks ◎ Locks ○ Deny ● Locks ○ Deny ● Locks ○ Deny ● Locks ○ Deny ● Description ○ Description ○ Description ○ Description ○ Description ○ Description ◎ Protected ○ Description ◎ Prot_Descevet ○ Description <		65500	DenyAllinBound	Any	Any	Destination port ranges * ()	
Network interfaces Protocol ◇ Subrets Any ② Norterises ○ TCP ③ Locks UDP Monitoring ○ UDP ▲ Aris ○ Norw ◎ Diagnostic settings △ Alow ◎ Locks △ Deny ▲ Kerts ○ Deny ■ Logs → Alow ■ Logs → Anon ■ NSG flow logs → Alow ▲ transion → Deny ▲ Tasks (preview) → Deny ■ Export template Description Support + troubleshooting → Description △ Effective security rules ▲ Description	Outbound security rules					443	
 Subsets Subsets Any TCP TCP Cods UoP CMP Action Action Alow Dispositic settings Action Action Alow Deny Priority * ○ 305 Action Basic Security rules Ner Support Request 	M Network interfaces					Protocol	
II Properties II broperties I cods Monitoring II Aderts I biagnostic settings I biagnostic settings <td>Subnets</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	Subnets						
I Locks UOP Monitoring I CMMP # Aferts Action ID Bagnottic settings O Deny IP Logis Deny IP Logis Priority □ IN SG flow logis 305 Automation Name ¹ /2 IP Tasks (preview) Port, 5080 IP Logis Port, 5080 IP Logis Port, 5080 IP Logis Description IP Effective security rules Image: Security rules	Properties					• TCP	
Monitoring LCMP Image: Adents Action Image: Diagnostic settings Image: Adents Image: Diagnostic settings Denry Image: Diagnostic settings Denry Image: Diagnostic settings Prostry * O Image: Diagnosettingsettings Prostry * O <t< td=""><td>🔒 Locks</td><td></td><td></td><td></td><td></td><td></td><td></td></t<>	🔒 Locks						
Alcina Diagnostic settings Logs NSG flow logs Automation Tasks (preview) Tosts (preview) Export template Support + troubleshooting Effective security rules	Monitoring						
Blagnostic settings Allow Degrostic settings Degrostic settings Degrostic settings Degrostic settings Degrostic settings Degrostic settings Prototy * 0 305 Prototy * 0 305 Prototy * 0 Statis (preview) Prot_0080 Description Description Effective security rules Prot_statis = 0 Prot_statis = 0<td>Alerts</td><td></td><td></td><td></td><td></td><td>Action</td><td></td>	Alerts					Action	
Logi Logi Logi Logi NSG flow logs Automation Automation Export serplate Support + roubleshooting Effective security rules Revesuport Request	Diagnostic settings						
NSG flow logs 305 Automation 305 Attransform 305 Attransform Perclose Attransform Perclose Bis point + troublehooting Description Effective security rules Perclose	Logs					U Delly	
Automation 305 Automation Name At Tasks (preview) Port 8080 If Export template Description Support Fraubleshooting Image: Support Request	NSG flaw loos					Priority * 🔘	
Automation Name ² At Task (preview) Port_6080 If Export template Description Support + roubleshooting Image: Compare the security rules If New Support Request Image: Compare the security rules	inso now logs					305	
trais (preview) t	Automation					Name ⁵ 5	
Export template Export template Export template Effective security rules New Support Request Effective security rules New Support Request Effective security rules E	🚓 Tasks (preview)					Port_8080	
Support + troubleshooting Effective security rules New Support Request	Export template					Description	
Effective security rules New Support Request	Support + troubleshooting						
🖻 New Support Request	Effective security rules						
	R New Support Request						

a) In the Azure portal, navigate to the resource group where you deployed your Nexus Dashboard.

This is the same resource group you selected in Step 2.

b) Select the security group attached to the nodes' data interfaces.

The name of the security group will begin with nsg-data-<region>-....

- c) In the security group's setting navigation bar, select **Inbound security rules**.
- d) Click +Add to add a new inbound security rule, then provide the details to allow inbound communication on port 443.

Provide the following information for the new rule:

- For Source, select Any.
- For Source port ranges, enter 443.
- For **Destination**, select Any.
- For Destination port ranges, enter 443.
- For **Protocol**, choose TCP.
- For Action, choose Allow.
- For Priority, choose a priority between 300 and 320.

For example, 305.

- Provide a Name for the rule.
- e) Click +Add to add a new inbound security rule, then provide the details to allow inbound communication on port 9092.

Repeat the previous substep to add another rule with the following details:

- For Source, select Any.
- For Source port ranges, enter 9092.
- For Destination, select Any.
- For Destination port ranges, enter 9092.
- For **Protocol**, choose TCP.
- For Action, choose Allow.
- For Priority, choose a priority between 300 and 320.

For example, 310.

• Provide a Name for the rule.