

Deploying in Amazon Web Services

- Prerequisites and guidelines for deploying the Nexus Dashboard cluster in Amazon Web Services, on page 1
- Deploying Nexus Dashboard in AWS, on page 3

Prerequisites and guidelines for deploying the Nexus Dashboard cluster in Amazon Web Services

Before you proceed with deploying the Nexus Dashboard cluster in Amazon Web Services (AWS), you must:

• Ensure that the AWS 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 AWS account.

You must be able to launch multiple instances of Elastic Compute Cloud (m5.2xlarge) to host the Nexus Dashboard cluster.

- Ensure that the CPU family used for the Nexus Dashboard VMs supports AVX instruction set.
- Have at least 6 AWS Elastic IP addresses.

A typical Nexus Dashboard deployment consists of 3 nodes with each node requiring 2 AWS Elastic IP addresses for the management and data networks.

By default, your AWS account has lower elastic IP limit, so you may need to request an increase. To request IP limit increase:

- 1. In your AWS console, navigate to Computer > EC2.
- In the EC2 Dashboard, click Network & Security > Elastic IPs and note how many Elastic IPs are already being used.
- 3. In the EC2 Dashboard, click Limits and note the maximum number of EC2-VPC Elastic IPs allowed.

Subtract the number of IPs already being used from the limit to get. Then if necessary, click **Request limit increase** to request additional Elastic IPs.

• Create a Virtual Private Cloud (VPC).

A VPC is an isolated portion of the AWS cloud for AWS objects, such as Amazon EC2 instances. To create a VPC:

- 1. In your AWS console, navigate to Networking & Content Delivery Tools > VPC.
- 2. In the VPC Dashboard, click Your VPCs and choose Create VPC. Then provide the Name Tag and IPv4 CIDR block.

The CIDR block is a range of IPv4 addresses for your VPC and must be in the /16 to /24 range. For example, 10.9.0.0/16.

• Create an Internet Gateway and attach it to the VPC.

Internet Gateway is a virtual router that allows a VPC to connect to the Internet. To create an Internet Gateway:

- In the VPC Dashboard, click Internet Gateways and choose Create internet gateway. Then provide the Name Tag.
- In the Internet Gateways screen, select the Internet Gateway you created, then choose Actions > Attach to VPC. Finally, from the Available VPCs dropdown, select the VPC you created and click Attach internet gateway.
- · Create a routes table.

Routes table is used for connecting the subnets within your VPC and Internet Gateway to your Nexus Dashboard cluster. To create a routes table:

- In the VPC Dashboard, click Route Tables, choose the Routes tab, and click Edit routes.
- In the Edit routes screen, click Add route and create a 0.0.0.0/0 destination. From the Target dropdown, select Internet Gateway and choose the gateway you created. Finally, click Save routes.
- · Create a key pair.

A key pair consists of a private key and a public key, which are used as security credentials to verify your identity when connecting to an EC2 instance. To create a key pair:

- Navigate to All services > Compute > EC2.
- In the EC2 Dashboard, click Network & Security > Key Pairs. Then click Create Key Pairs.
- Provide a name for your key pair, select the pem file format, and click Create key pair.

This will download the .pem private key file to your system. Move the file to a safe location, you will need to use it the first time you log in to an EC2 instance's console.



Note By default only PEM-based login is enabled for each node. To be able to SSH into the nodes using a password, as required by the GUI setup wizard, you will need to explicitly enable password-based logins by logging in to each node using the generated key and running the required command as described in the setup section below.

Deploying Nexus Dashboard in AWS

This section describes how to deploy Cisco Nexus Dashboard cluster in Amazon Web Services (AWS).

Before you begin

 Ensure that you meet the requirements and guidelines described in Prerequisites and guidelines for deploying the Nexus Dashboard cluster in Amazon Web Services, on page 1.

Step 1 Subscribe to Cisco Nexus Dashboard product in AWS Marketplace.

a) Log into your AWS account and navigate to the AWS Management Console

The Management Console is available at https://console.aws.amazon.com/.

- b) Navigate to Services > AWS Marketplace Subscriptions.
- c) Click Manage Subscriptions.
- d) Click Discover products.
- e) Search for Cisco Nexus Dashboard and click the result.
- f) In the product page, click Continue to Subscribe.
- g) Click Accept Terms.

It may take a couple of minutes for the subscription to be processed.

- h) Finally click Continue to Configuration.
- **Step 2** Select software options and region.
 - a) From the Fulfillment Option dropdown, select Nexus Dashboard Cloud Deployment
 - b) From the Software Version dropdown, select the version you want to deploy.
 - c) From the **Region** dropdown, select the regions where the template will be deployed.

This must be the same region where you created your VPC.

d) Click Continue to Launch.

The product page appears, which shows a summary of your configuration and enables you to launch the cloud formation template.

Step 3 From the Choose Action, select Launch CloudFormation and click Launch.

The Create stack page appears.

Step 4 Create stack.

- a) In the Prerequisite Prepare template area, select Template is ready.
- b) In the **Specify Template** area, select Amazon S3 URL for the template source. The template will be populated automatically.
- c) Click Next to continue.

The Specify stack details page appears.

Step 5 Specify stack details.

- a) Provide the Stack name.
- b) From the VPC identifier dropdown, select the VPC you created.

For example, vpc-038f83026b6a48e98(10.176.176.0/24).

c) In the ND cluster Subnet block, provide the VPC subnet CIDR block.

Choose a subnet from the VPC CIDR that you defined. You can provide a smaller subnet or use the whole CIDR. The CIDR can be a /24 or /25 subnet and will be segmented to be used across the availability zones.

For example, 10.176.176.0/24.

d) From the Availability Zones dropdown, select one or more available zones.

We recommend you choose 3 availability zones. For regions that support only 2 availability zones, 2nd and 3rd nodes of the cluster will launch in the second availability zone.

e) From the Number of Availability Zones dropdown, select the number of zones you added in the previous substep.

Ensure that the number matches the number of availability zones you selected in the previous substep.

f) Enable Data Interface EIP support.

This field enables external connectivity for the node. External connectivity is required for communication with Cisco ACI fabrics outside AWS.

g) In the Password and Confirm Password fields, provide the password.

This password will be used for the Nexus Dashboard's rescue-user login, as well as the initial password for the GUI's admin user.

Note You must provide the same password for all nodes or the cluster creation will fail.

- h) From the SSH key pair dropdown, select the key pair you created.
- i) In the Access control 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.

- j) Click **Next** to continue.
- **Step 6** In the Advanced options screen, simply click Next.
- **Step 7** In the **Review** screen, verify template configuration and click **Create stack**.
- **Step 8** Wait for the deployment to complete, then start the VMs.

You can view the status of the instance deployment in the **CloudFormation** page, for example CREATE_IN_PROGRESS. You can click the refresh button in the top right corner of the page to update the status.

When the status changes to ${\tt CREATE_COMPLETE},$ you can proceed to the next step.

CloudFormation > Stacks > NDwestus2					
Stacks (1)	C	NDwestus2		Delete Update	Stack actions V Create stack V
Q, Filter by stack name		Stack Info Events Resources Outputs	Parameters Template Change	sets	
Active View nested	< 1 >				
NDwestus2 2021-04-14 17:08:22 UTC-0700	۰	Events (86) Q. Search events			©
		Timestamp	Logical ID	Status	Status reason
		2021-04-14 17:09:30 UTC-0700	NDwestus2	⊘ CREATE_COMPLETE	
		2021-04-14 17:09:27 UTC-0700	NDNode3	⊘ CREATE_COMPLETE	
		2021-04-14 17:09:27 UTC-0700	NDNode1	⊘ CREATE_COMPLETE	-

Step 9 Note down all nodes' public IP addresses.

aws Services V			¢	C Search for services, f	leatures, market		-			N. Calif	ornia 1	• Su	pport 1	•
New EC2 Experience		Launch Instance	Connec	ct Actions ~						Q	₫	÷	۰	•
EC2 Dashboard		Q Instance Sta	te : Running	Add filter					0	< <	1 to	3 of 3	> >	i.
Events Tags	4	name	- Na	me	- 1	ni i -	Alarm S	Status	Public DNS (IP	v4)	- IP	v4 Pub	lic IP	
Limits			b ND	1-FirstMaster	ŀ	0	None	7	ec2-52-52-127-1	196.us				
INSTANCES			ND	2-Master	÷		None	20	ec2-184-169-15	c				
Instances a			ND	3-Master	į.	0	None	10	ec2-54-241-237	-45.us				
Instance Types														

- a) After all instances are deployed, navigate to the AWS console's EC2 > Instances page.
- b) Note down which node is labeled as ND1-Master.

You will use this node's public IP address to complete cluster configuration.

c) Note down all nodes' public IP addresses.

You will provide this information to the GUI bootstrap wizard in the following steps.

Step 10 Enable password-based login on all nodes.

By default only PEM-based login is enabled for each node. To be able to SSH into the nodes using a password, as required by the GUI setup wizard, you will need to explicitly enable password-based logins.

- **Note** You must enable password-based login on all nodes before proceeding to cluster bootstrap described in the following steps or you will not be able to complete the cluster configuration.
- a) SSH into one of the instances using its public IP address and the PEM file.

Use the PEM file you created for this as part of Prerequisites and guidelines for deploying the Nexus Dashboard cluster in Amazon Web Services, on page 1.

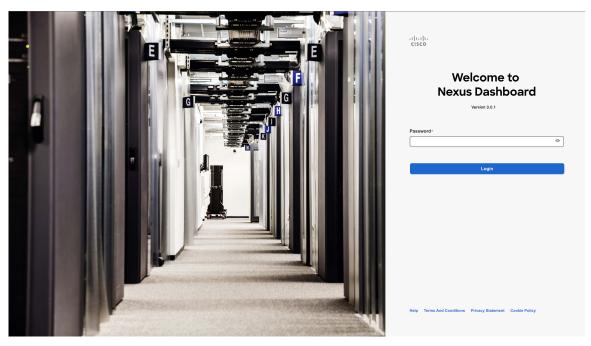
- # ssh -i <pem-file-name>.pem rescue-user@<node-public-ip>
- b) Enable password-based login.

Step 11

On each node, run the following command:

- # acs login-prompt enable
- c) Repeat this step for the other two instances.
- 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 (ND1-Master) 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 12 Provide the **Cluster Details**.

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

cisco Nexus Dashboard					2
Overview	Cluster Bringup				
🖉 Manage	Answer some questions, select th	e services you want to enable and have Nexus I	Dashboard ready to use in a few m	inutes.	
⊙ Analyze ≞o Admin	Configuration Node Details	Configuration Provide the cluster name and configure th Nexus Dashboard Cluster Name *	e DNS, NTP and Proxy to set up No	exus Dashboard and bring up the	user interface
	3 Deployment Mode	b Enable IPv6			
	4 Summary	DNS			^
		DNS Provider IP Address* 171.70.168.183 Add DNS Provider DNS Search Domain Add DNS Search Domain			/ 🗊
		NTP			~
		NTP Host*	Key ID	Preferred	
		171.68.38.65 Add NTP Host Name//P Address		true	/ 1
		Proxy			Skip Proxy 🔨
	•	Ignore Hosts • Add Ignore Host Proxy Server + _ Authentication required for proxy			
		h Advanced Settings			^
		App Network • () 172.17.0.1/16 Service Network • () 100.80.0.0/16 App Network IPv6 () 2000::/108 Service Network IPv6 () 3000::/108			
	\langle				i Ne

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 for all enabled services.

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	/	1
Add NTP Host Name/IP Address				

△ 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 for all enabled services section earlier in this document.

- j) Click Next to continue.
- **Step 13** 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 VPC subnet you have configured before deploying the cluster.

The cluster creates six subnets from the given VPC CIDR, 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 14** 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 15** Repeat the previous step to add the 3rd node.
- Step 16 In the Node Details page, click Next to continue.
- **Step 17** 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.

Nexus Dashboard		٩								
	Cluster Bringup Answer some questions, select the services you want to enable and have Nexus Dashboard ready to use in a few minutes.									
,∞ Manago ⊙ Analyze ∄ ₀ Admin	Answer some questions, seect the services you want to enable and have nexus usanoard ready to use in a ter minutes. Configuration Configur									
	3	Back Next								

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 for all enabled services section.

- c) Click Next to proceed.
- **Step 18** 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.

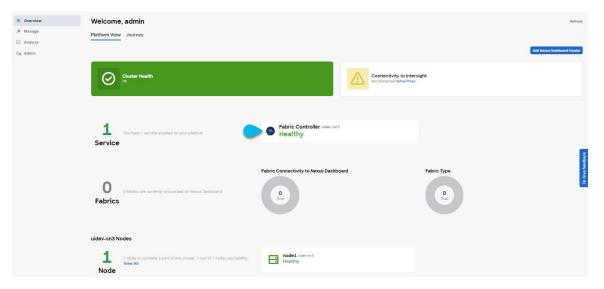
It may take up to 30 minutes for the cluster to form and all the services to start. When cluster configuration is complete, the page will reload to the Nexus Dashboard GUI.

Step 19 Verify that the cluster is healthy.

Depending of the deployment mode, it may take more than 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":

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



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 20 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 fabrics. If you do not plan on on-boarding any NDFC fabrics to your Nexus Dashboard cluster, you can skip this step.

Navigate to one of the nodes' data interface:

Launch Templates ND3-Master H0256683674e6f66c m5.4.starge u Savings Plans ND1-FirstMaster H00368c5983cdcdde3 m5.4.starge u Savings Plans ND2-Master H046135e78c60151 m5.4.starge u Capacity Reservations ND2-Master H046135e78c60151 m5.4.starge u Images AMIs ND2-Master H046135e78c60151 m5.4.starge u Volumes Snapshots Instance: I-000058c5983cdcdde3 Instance: Instance: <td< th=""><th>aws Services V</th><th></th><th>Q 5</th><th>earch for services, features, m</th><th>arketplace products, and docs</th><th>[Option+S]</th><th></th></td<>	aws Services V		Q 5	earch for services, features, m	arketplace products, and docs	[Option+S]	
Instance Types Launch Templates Spot Requests Sot Requests Savings Plans Reserved Instances Dedicated Hosts Capacity Reservations Images AMIs Elastic Block Store Volumes Snapshots Lifecycle Manager Network & Security Security Groups Elastic IPs Placement Groups Reserved Instances tate Instance Type Placement Groups Reserved Instances tate Instance type Finding Private IPs Placement Groups Reserved Instances Secondary private IPs VPC ID Private IPs Secondary private IPs VPC ID Private IPs Secondary private IPs VPC ID Private IPs Cod Balancing Lideout Reserved Instances Cod Balancing Target Groups T	Instances	Launch Instand	Connect	t Actions ~			
Lunch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts Capacity Reservations Instance ID ND1-FirstMaster HO46135678660151 Instance ID ND2-Master HO461356778660151 Instance ID ND2-Master HO461356778660151 Instance ID ND2-Master HO461356778660151 Instance ID ND2-Master HO461356778660151 Instance ID NEtwork Interface eth1 Instance ID Volumes Snapshots Lifecycle Manager Network & Security Security Groups Elastic IPs Placement Groups Key Pairs Network Interfaces Load Balancers Target Groups C C Network Interface Network Interface Network Interface Network Interface Security Groups Elastic IPs Network Interfaces Network Interfaces Network Interfaces Security Groups Load Balancers Target Groups Network Interface Network Interface Network Interface Network Interface Network Interface Security Groups Elastic IPs Network Interfaces Network Interfaces Network Interface Security Groups Elastic IPs Network Interface Security Groups Elastic IPs Network Interface Security Groups Elastic IPs Network Interface Security Groups Elastic Fabric Adapter Disabled Description Network Interface Security Groups Elastic Fabric Adapter Disabled Disabled	Instances a	Q, Filter by tage	s and attributes or sea	arch by keyword			
Spot Requests N03-Master H0025c683c74e9f86c m5.4xlarge u Savings Plans N01-FirstMaster H00a58c5983cdcddo3 m5.4xlarge u Reserved Instances ND2-Master H046135e78cf80151 m5.4xlarge u Dedicated Hosts Capacity Reservations m5.4xlarge u Images AMIs ND2-Master H046135e78cf80151 m5.4xlarge u Volumes Snapshots Instance: I-00a58c5983cdcddda3 Instance: Volumes Volumes vpc-00858d8dob06cce7 Volume Volume: Volume: Volume: Volume: Volume: Vpc-00858d8dob06cce7 Vpc-00858d8db06db6ce7 Vpc-00	Instance Types	name	- Nan	ne	- Instance ID	- Instance Type	- At
Spot Requests D ND1-FirstMaster L00a58c5983cdcdde3 m5.4xlarge u Savings Plans ND2-Master L046135e78bcf80151 m5.4xlarge u Reserved Instances Dedicated Hosts Capacity Reservations m5.4xlarge u Images AMis Instance: I-00a58c5983cdcdde3 m5.4xlarge u Volumes Instance: I-00a58c5983cdcdde3 m5.4xlarge u Volumes Instance: I-00a58c5983cdcdde3 m5.4xlarge u Network & Security Instance ID mstance ID mstance ID mstance ID mstance ID mstance ID mstance ID Attachment Owner 921008781738 modes modes <t< td=""><td>Launch Templates</td><td></td><td>ND3</td><td>I-Master</td><td>i-0025c663e74e9f66c</td><td>m5.4xlarge</td><td>us</td></t<>	Launch Templates		ND3	I-Master	i-0025c663e74e9f66c	m5.4xlarge	us
Savings Plans ND2-Master I-04613567/80:00151 m6.4xdarge u Reserved Instances Dedicated Hosts Capacity Reservations Images I	Spot Requests						us
Reserved Instances Dedicated Hosts Capacity Reservations Images AMIs Elastic Block Store Volumes Snapshots Lifecycle Manager Description Status Checks Instance: Instance ID Instance TPS	Savings Plans						US
Capacity Reservations Capacity Reservations Images AMis Elastic Block Store Volumes Snapshots Ifterycle Manager Description Status Checks Network & Security Security Groups Elastic IPs Placement Groups Finding Private IDs Private IDs Network Interfaces Pattorn Security Groups Elastic IPs Patement Groups Network Interfaces Private IDs Network Interfaces Description Secondary private IPs Network Interfaces Description Virate IDs Instance type Private ID Reservation Network Interfaces VPC ID Pitatorm Network	Reserved Instances			- mustor	101010001000101	no. Andigo	-4
Images AMis Elastic Block Store Volumes Snapshots Lifecycle Manager Description Status Checks Network & Security Security Groups Elastic IPs Placement Groups Kety Pairs Network Interfaces Private IPs Secondary private IPs Public IP Address Source/Dest. Check Security Groups default Elastic Fabric Adapter Disabled	Dedicated Hosts						
AMIS Elastic Block Store Volumes Snapshots Instance: I-00a58c5983odcddo3 Lifecycle Manager Description Status Checks Network & Security Description Status Checks Network & Security Instance tate Instance type Elastic IPs Instance type Instance type Placement Groups Finding Private IPs Network Interfaces Secondary private IPs Polubic IP Address 1.compute.Internal Load Balancers Secondary private IPs Polution Network interface Target Groups Metwork interfaces C Operation Elastic Fabric Adapter Disabled Instance Description	Capacity Reservations						-
AMis Elastic Block Store Volumes Instance: I-00a58c5983cdcddo3 (Snapshots Instance: I-00a58c5983cdcddo3 (Lifecycle Manager Description Network & Security Status Checks Network & Security Instance ID Isstance type Instance type Elastic IPs Instance type Placement Groups Finding Network Interfaces Private IPs Network Interfaces Secondary private IPs Load Balancers Secondary private IPs Target Groups Network interfaces Target Groups Network interfaces							-
Elastic Block Store Volumes Volumes Instance: I-00a58c5983cdcdde3 (Snapshots Instance: I-00a58c5983cdcdde3 (Lifecycle Manager Description Network & Security Status Checks Network & Security Groups Instance ID Elastic IPs Instance type Placement Groups Finding Network Interfaces Private IPs Network Interfaces Secondary private IPs Network Interfaces Security Groups default Elastic Fabric Adapter Disabled	Images						-
Volumes Network Interface eth1 Snapshots Instance: I-00a58c5983cdcddd0 Lifecycle Manager Description Network & Security Description Status Checks Attachment Owner Network & Security Instance ID Security Groups Instance ID Elastic IPs Instance type Placement Groups Finding Private DNS Private DNS Private IPadencing Private IPadencing Load Balancers VPC ID Target Groups Network Interfaces	AMIs						
Snapshots Instance: I-00a58c5983cdcdde3 Lifecycle Manager Description Network & Security Description Status Checks Attachment Owner Vir G ID vpc-005358d8dd0e6ece7 Attachment Owner 921008781738 Security Groups Instance ID Elastic IPs Instance type Placement Groups Finding Private DNS Private DNS Network Interfaces Secondary private IPs Load Balancers VPC ID Platform Network interfaces Code Balancers Platform Target Groups Network interfaces	Elastic Block Store						
Snapshots Instance: I+00a58c5983cdcdde3 Lifecycle Manager Description Network & Security Instance: I Security Groups Instance ID Elastic IPs Instance type Placement Groups Finding Private DNS Private DNS Network Interfaces Secondary private IPs Vec ID Secondary private IPs Load Balancers Vec ID Target Groups Network interfaces	Volumes			Natwork Interface ath			
Lifecycle Manager Instance: F-00ussecsussecueduss in the full of the instance: F-00ussecsussecueduss in the full of the instance: F-00ussecsussecuedus in the full of the instance instance instance instance: F-00ussecsussecuedus instance: F-00ussecsussect instance: F-00ussecsussecs instance: F-00ussecsussecs instance: F-00ussecsussect instance: F-00ussecs instance: F-00ussecsussecs instance: F-00ussecs instance: F-		-					
Network & Security Description Status Checks Attachment Owner 921008781738 Security Groups Instance ID Attachment Owner 921008781738 Elastic IPs Instance state Attachment Status attached Placement Groups Finding Private IP Address 172.35.1.76 Network Interfaces Private IPS Private IPS 1.compute.internal Network Interfaces Private IPS Public IP Address - Load Balancers Platform Platform Security Groups default Target Groups Network Interfaces Platform Elastic Fabric Adapter Disabled		Instance: i-00	a58c5983cdcdde3	l Inte d			
Network & Security Attachment Owner Security Groups Security Groups Instance ID Attachment Status attached Elastic IPs Instance state Mon Sep 13 11:53:14 GMT-700 2021 Placement Groups Finding Key Pairs Private DNS Network Interfaces Private IPs Load Balancers Platform Target Groups Network Interfaces	Lifecycle Manager	Description	Status Checks				
Security Groups Instance ID Attachment Time Mon Sep 13 11:53:14 GMT-700 2021 Elastic IPs Instance type Delete on Terminate false Placement Groups Finding Private IP Address 172:35:1.76 Key Pairs Private DNS Private DNS nemotic IP Address Network Interfaces Private IPs Public IP Address - Load Balancers Platform Secondary private IPs Security Groups default Target Groups Network interfaces Platform Elastic Fabric Adapter Disabled	Network & Security						
Elastic IPs Instance state Delete on Terminate false Placement Groups Instance type Private IP Address 172.35.1.76 Very Pairs Private DNS Private DNS Incompute.internal Network Interfaces Private IPs Public IP Address - Load Balancers Platform Secondary private IPs Security Groups default Load Balancers Platform Elastic Fabric Adapter Disabled	Security Groups					121	
Placement Groups Finding Private IP Address 172.35.1.76 Placement Groups Finding Private IDNS Ip-172-35-1-76.us-west- Key Pairs Private IDNS I.compute.internal Network Interfaces Private IPs Public IP Address - Load Balancers Secondary private IPs Security Groups ND 1 data network interface Target Groups Network interfaces Platform Elastic Fabric Adapter	Elastic IPs						
Key Pairs Private DNS Private DNS Name ip-172-35-1-76.us-west- Network Interfaces Private IPs 1.compute.Internal Load Balancing Secondary private IPs Public IP Address - Load Balancers Platform Secondary private IPs ND 1 data network Interface Load Balancers Platform Security Groups default Target Groups Network Interfaces Elastic Fabric Adapter Disabled	Placement Groups		and a state of the local	Private IP Address	172.35.1.76		
Network Interfaces Private IPs Public IP Address - Load Balancing Secondary private IPs Source/Dest. Check true Load Balancers VPC ID Description ND 1 data network interface Target Groups Network interfaces C eth1				Private DNS Name			
Network interfaces Source/Dest. Check true V Load Balancing VPC ID Description ND 1 data network interface Load Balancers Platform Security Groups default Target Groups Network interfaces Disabled			Private IPs	Public IP Address			
Load Balancing VPC ID Description ND1 data network interface Load Balancers Platform Security Groups default Target Groups Network interfaces Elastic Fabric Adapter Disabled	Network Interfaces				true		
Load Balancers Platform Target Groups Network interfaces eth1	Load Balancing	Sec		Description	ND 1 data network interface		
Target Groups Network interfaces eth1	Load Balancers			The second second second second second			
	Target Groups		Network interfaces		Disabled		
Auto Scaling Source/dest: cneck True	Auto Scalina			eth1 True			

- a) In the AWS console, navigate to Instances.
- b) Select one of the Nexus Dashboard instances.

You will make changes to the default security group, so you only need to select one of the nodes.

- c) Click the data interface (eth1).
- d) Click the Interface ID.

The Network Interface properties page opens.

e) In the Network Interface page, click default in the Security groups column of the interface.

Add the new rules:

- a) In the default security group's page, select the Inbound rules tab.
- b) Click Edit inbound rules.
- c) In the **Edit inbound rules** page, click **Add rule** 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 Type, select Custom TCP.
- For **Port range**, enter 443.
- For **Source**, provide the IP addresses of the NDFC controllers which you plan to onboard to your Nexus Dashboard.
- d) Still in the **Edit inbound rules** page, click **Add rule** to add another inbound security rule, then provide the details to allow inbound communication on port 9092.

Provide the following information for the new rule:

- For Type, select Custom TCP.
- For Port range, enter 9092.
- For **Source**, provide the IP addresses of the NDFC controllers which you plan to onboard to your Nexus Dashboard.

I