Using the Cloud Service Manager

VMware NSX Cloud services

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

https://docs.vmware.com/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Overview of the Cloud Service Manager 1

Cloud Service Manager (CSM) is a management endpoint that handles public cloud-specific constructs.

You can perform the following tasks in CSM:

- Add an AWS Account: You must add at least one AWS account in CSM to be able to use NSX for VMs in your compute VPC. You can add multiple AWS accounts. After the successful addition of AWS account(s), the VPC(s) and EC2 Instances (workload VMs) hosted in your AWS account(s) become available in CSM.
- Deploy/Undeploy NSX Cloud Gateway (CGW) on compute VPCs: You can deploy one or two (for High Availability) CGW per VPC. You can also undeploy CGW from CSM.
- Quarantine VPCs: You can enable or disable Quarantine Policy on VPCs.
- Switch between Grid and Card view: The cards display an overview of your inventory. The grid displays more details. Click the icons to switch between the view types.

CSM provides a holistic view of all your AWS accounts that you have connected with NSX Cloud by presenting your VPC inventory in different ways:

- You can view the number of regions you are operating in.
- You can view the number of VPCs per region.
- You can view the number of EC2 instances per VPC.

There are four sections under Cross-Cloud.

Accounts

Lists all the AWS accounts you have added to CSM. Each card represents an AWS account. You can see the summary on the card.

The colors for the circles mean the following:

- Green: indicates the number of NSX-managed instances that are running without any errors.
- Red: indicates the number of NSX-managed instances that have errors in them. If you click on the particular instance that has errors, you can see the error codes listed when you click on the red-colored arrow.
- Grey: indicates the number of instances that are not managed by NSX.

Regions

You can filter the Regions-view by AWS Account. Each AWS account may have multiple regions. Each region has VPCs and Instances. If you have deployed any CGW in any of your VPCs, you can see them here.

VPCs

You can filter the VPC inventory by Account and Region.

- Each card represents one VPC. You can have one or two (for HA) CGWs deployed on each VPC. You can view CGW status through the colored up/down arrow.
  - Green-colored upward arrow indicates CGW is up.
  - Orange-colored downward arrow indicates the primary (active) CGW is up but the secondary (standby) CGW is down.
  - Red-colored downward arrow indicates both -- the active as well as standby -- CGWs are down.
- A summary of the VPC displays on the VPC card. You can view more details for each VPC by switching to the grid view.
- Click on Action to access the following:
  - Edit Quarantine: Set it to on or off. See Manage Quarantine Policy for details.
  - Deploy/Undeploy NSX Cloud Gateway. See Step 3: Deploy the Public Cloud Gateway (CGW) on the AWS Compute VPC.

Instances

You can filter the instances inventory by Account, Region, and VPC.

Each card represents an EC2 Instance (VM) and displays a summary.

For details on the instance, click on the card or switch to grid view.

Enable CSM to access your AWS Inventory

2

Your AWS account contains one or more compute VPCs that you want to manage using NSX. To bring your inventory into NSX Cloud, you need to start by adding your AWS account in CSM.

This is a three-step process:

- Step 1 (In NSX Cloud): Add your AWS account using the ARN information generated by the JSON template provided by NSX Cloud.
- Step 2 (In your AWS account): Create or select a VPC in the selected deployment region, with specific configurations.
- Step 3 (In NSX Cloud): Deploy the NSX Public Cloud Gateway (PCG) in the VPC configured for NSX Cloud.

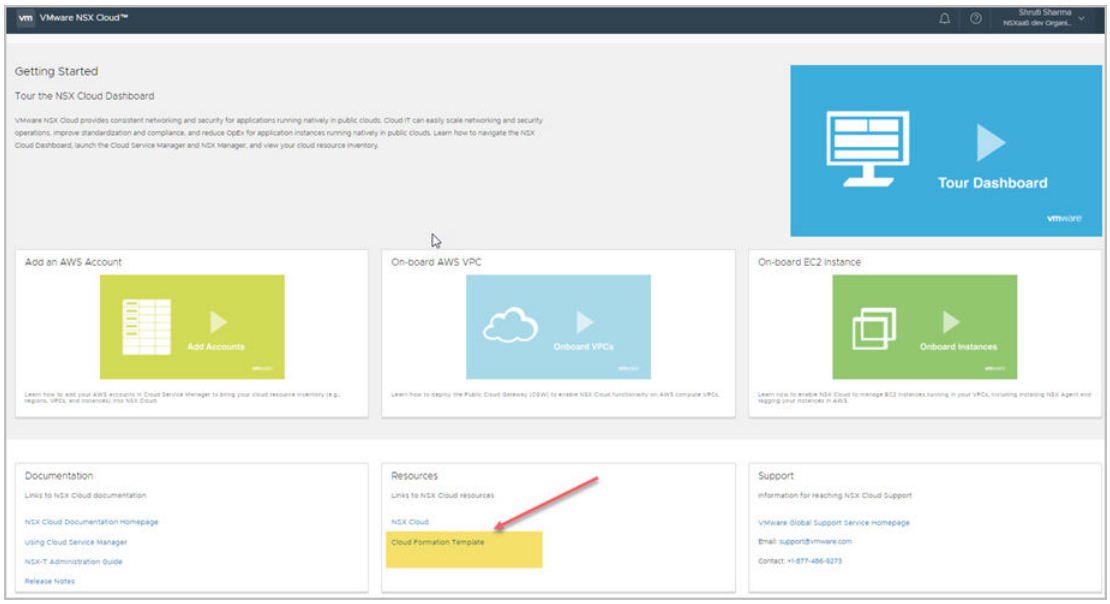
This chapter includes the following topics:

Step 1: Add AWS Account

Add your AWS account using the ARN information generated by the JSON template provided by NSX Cloud.

Procedure

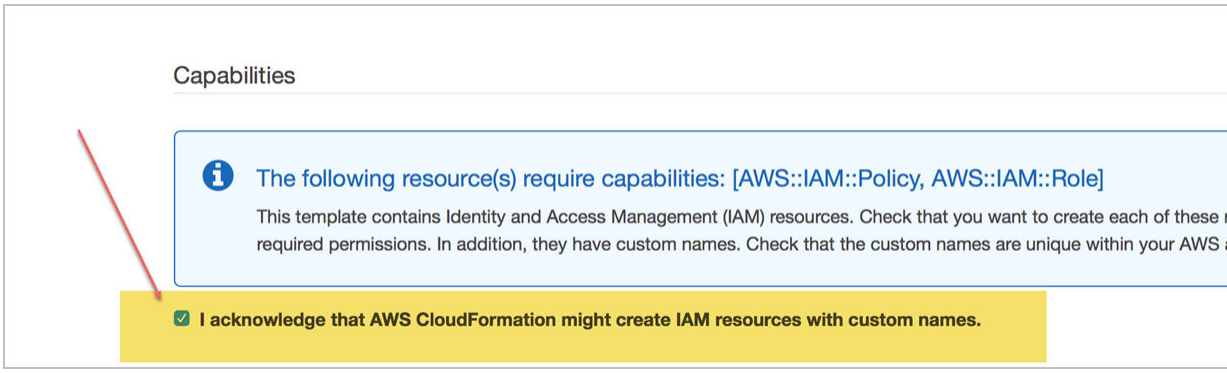
1 In NSX Cloud: From the NSX Cloud dashboard, copy the JSON template URL from the Resources tile.



2 Switch to your AWS account to do the following:

a Create a new Stack in the CloudFormation service.

b Select the checkbox on the Review screen acknowledging that AWS might create IAM resources with custom names.



c Click **Create**. The NSX Cloud JSON template creates three identifiers that are needed to add this account in CSM. This process takes some time to finish.

d Click on the Outputs tab when the creation process completes.

e Make a note of the values for `IAMRoleARN`, `ExternalID`, and `GatewayRoleName`.

Note You have the option to use your AWS account's Access Key and Secret Key for adding it into CSM, but it is not recommended because of security concerns.

3 Switch to CSM to do the following:

a Click **Cross-Cloud** > **Accounts** > **(+) Add AWS Account**.

b Enter the following details on this screen:

Option	Description
Account Name	Provide a descriptive name for this AWS VPC
IAM Role ARN	Use the value generated from the AWS Stack
External ID	Use the value generated from the AWS Stack
Gateway Role Name	Use the value generated from the AWS Stack

c Click **Save**.

The AWS account gets added in CSM.

In the VPCs tab of CSM, you can view all the VPCs in your AWS account.

In the Instances tab of CSM, you can view the EC2 Instances in this VPC.

What to do next

"Step 2: Configure your AWS Compute VPC," on page 9

Step 2: Configure your AWS Compute VPC

Your AWS compute VPC needs specific configurations for NSX Cloud.

You can use the CloudFormation template linked from the NSX Cloud Dashboard's Resources tile, to create a compute VPC with all the basic settings required for NSX Cloud. The CloudFormation template creates the following:

- six subnets for supporting PCG with High Availability
- an Internet gateway (IGW)
- a private and a public route table
- subnet association with route tables
- DNS resolution and DNS hostnames enabled.

The following steps provide information on these configurations and how you can set them yourself in AWS.

Procedure

1 Assuming your VPC uses a /16 network, for each gateway that needs to be deployed, set up three subnets.

Important If using High Availability, set up three additional subnets in a different Availability Zone.

- Management subnet: This subnet is used for NSX management of CGW. The recommended range is /24.
- Uplink subnet: This subnet is used for North-South internet traffic. The recommended range is /24.
- Downlink subnet: This subnet encompasses the workload VM's IP address range, and should be sized accordingly. Bear in mind that you may need to incorporate additional interfaces on the workload VMs for debugging purposes.

Note Label the subnets appropriately, for example, **`management-subnet`**, **`uplink-subnet`**, **`downlink-subnet`**,because you will need to select the subnets when deploying PCG on this VPC.

2 Ensure you have an Internet gateway (IGW) that is attached to this VPC.

3 Ensure the routing table for the VPC has the **Destination** set to **`0.0.0.0/0`** and the **Target** is the IGW attached to the VPC.

4 Ensure you have DNS resolution and DNS hostnames enabled for this VPC.

What to do next

"Step 3: Deploy the Public Cloud Gateway on the AWS Compute VPC," on page 10

Step 3: Deploy the Public Cloud Gateway on the AWS Compute VPC

Deploy the NSX Public Cloud Gateway (PCG) on the AWS compute VPC.

When you deploy PCG, you are able to establish North-South connection. AWS Security Groups are created as part of the process of deploying PCG. See Chapter 5, "Manage Quarantine Policy," on page 23 for more information.

Note It is recommended that your AWS IAM policies include deny statements preventing users from modifying gateway resources to PCG.

Procedure

1 From the CSM dashboard, select **Cross-Cloud > AWS > `<AWS_account_name>`**

2 Select an AWS region name, for example, us-west. The AWS region must be the same where you created the compute VPC.

3 From the VPC section, select the compute VPC configured for NSX Cloud.

4 Click **Deploy Gateways**.

5 Complete the general gateway details:

Option	Description
PEM File	Select one of your PEM files from the drop-down menu. This file must be in the same region where NSX Cloud was deployed and where you created your compute VPC. This uniquely identifies your AWS account.
Quarantine Policy on the Associated VPC	The default selection is Enabled. This is recommended for greenfield deployments. If you already have VMs launched in your VPC, disable the Quarantine policy. See Chapter 5, "Manage Quarantine Policy," on page 23

6 Click **Next**.

7 Complete the High Availability gateway details.

Option	Description
Enable HA for Public Cloud Gateway	The recommended setting is Enable, that sets up a High Availability Active/Standby pair to avoid an unscheduled downtime.
Primary gateway settings	Select an Availability Zone such as us-west-1a, from the drop-down menu as the primary gateway for HA. Assign the uplink, downlink, and management subnets from the drop-down menu.
Secondary gateway settings	Select another Availability Zone such as us-west-1b, from the drop-down menu as the secondary gateway for HA. The secondary gateway is used when the primary gateway fails. Assign the uplink, downlink, and management subnets from the drop-down menu.

Click **Deploy**.

8 Monitor the status of the primary (and secondary, if you selected it) PCG deployment. This process can take 10-12 minutes.

9 Click **Finish** when PCG is successfully deployed.

Click the Gateways link on the VPC. the primary and secondary gateway names appear. The status of the compute VPC appears as **NSX Managed**.

See "Undeploying PCG," on page 34 for instructions and prerequisites for undeploying a PCG.

Behind the Scenes: after adding AWS account and deploying PCG

Essential NSX entities are created and configured in your AWS account and in NSX Manager after the three-step process of enabling CSM to access your AWS inventory.

NSX Manager Configurations

The following configurations are automatically made in NSX Manager:

- Edge Node named **Cloud Gateway** is created.
- Cloud Gateway is added to Edge Cluster.
- Cloud Gateway is registered as a Transport Node with two Transport Zones created.
- Two default logical switches are created.
- One tier-0 logical router is created.
- An IP Discovery Profile is created. This is to be used for overlay logical switches.

- A DHCP Profile is created. This is to be used for DHCP servers.

Verify these configurations in NSX Manager:

1 From the NSX Cloud dashboard, click **NSX Manager**.

2 Browse to **Fabric > Nodes > Edge**. Cloud Gateway should be listed as an Edge Node.

3 Verify that Deployment Status, Manager Connection and Controller Connection are connected (status shows **Up** with a green dot).

4 Browse to **Fabric > Nodes > Edge Clusters** to verify that the Edge Cluster and PCG were added as part of this cluster.

5 Browse to **Fabric > Nodes > Transport Nodes** to verify that PCG is registered as a Transport Node and is connected to two Transport Zones that were auto-created while deploying PCG:

   a Traffic type VLAN -- this connects to gateway uplink

   b Traffic type Overlay -- this is for logical networking

6 Verify whether the logical switches and the tier-0 logical router have been created and the logical router added to the Edge Cluster.

Important Do not delete any of the NSX-created entities.

AWS Configurations

In the AWS Compute VPC, the following is configured after PCG is deployed:

- A set of Security Groups (SG) are created in AWS that allow NSX Cloud to apply the Quarantine policy when it is enabled for a VPC.
  - The "gw" SGs are applied to the respective PCG interfaces.

    Table 2-1. AWS Security Groups created by NSX Cloud for CGW Interfaces

AWS Security Group name	Full Name
gw-mgmt-sg	Gateway Management Security Group
gw-uplink-sg	Gateway Uplink Security Group
gw-vtep-sg	Gateway Downlink Security Group

  - The "vm" SGs are applied to workload VMs. If the Quarantine Policy is enabled, the SG assignment for all interfaces for any VMs belonging to this VPC is managed by NSX Cloud.

    Table 2-2. AWS Security Groups created by NSX Cloud for Workload VMs

AWS Security Group name	Full Name
default	Default Security Group
vm-underlay-sg	VM Non-Overlay Security Group
vm-overlay-sg	VM Overlay Security Group
vm-override-sg	VM Override Security Group
vm-outbound-bypass-sg	VM Outbound Bypass Security Group
vm-inbound-bypass-sg	VM Inbound Bypass Security Group

    Note NSX Cloud provides the minimum required access for using NSX. To allow any other access beyond that, add a custom SG in addition to the appropriate SG assigned by NSX Cloud.

See Chapter 5, "Manage Quarantine Policy," on page 23 for more details.

- In the AWS VPC, a new Type A Record Set is added with the name `nsx-gw.vmware.local`. The IP address mapped to this record matches the Management IP address of PCG. This is assigned by AWS using DHCP and will differ for each VPC.
- A secondary IP for the uplink interface for PCG is created. An AWS Elastic IP is associated with this secondary IP address. This configuration is for SNAT.

Set Up the NSX Overlay Network 3

This chapter includes the following topics:

Attach a DHCP server to the Overlay Logical Switch

You must attach a DHCP server to the overlay logical switch before the DHCP server can process DHCP requests from VMs connected to the switch.

Note Use the auto-created DHCP profile for the DHCP server.

Procedure

1 From the NSX Cloud dashboard, click **NSX Manager**.

NSX Manager opens in the current browser window.

2 Select **Switching > Switches** from the navigation panel.

3 Click the overlay logical switch created by NSX Cloud.

4 Click **Actions > Attach DHCP Server**.

Example: Reference

See Attach a DHCP Server to a Logical Switch in the *NSX-T Administration Guide*.

Associate the Tier-0 Router with the Overlay Logical Switch

A tier-0 router and two logical switches are created by NSX Cloud after you deploy CGW. You need to connect the tier-0 router with the overlay logical switch from the NSX Manager.

Procedure

1 From the NSX Cloud dashboard, click **NSX Manager**.

NSX Manager opens in the current browser window.

2 Select **Routing** from the navigation panel.

3 Select the tier-0 router.

4 From the **Configuration** tab, add a new logical router port.

5 Type a name for the port, such as `uplink`.

6 Select the **Uplink** type.

7 Select the appropriate Transport Node labeled like **PublicCloudGatewayxxxxx**

8 Select the overlay logical switch with a name like **DefaultSwitch-Overlay-<vpc-name>**.

9 Select an IP address from the DHCP range for this logical switch.

A new uplink port is added for the tier-0 router.

Example: Reference

See Connect a Tier-0 Logical Router to a VLAN Logical Switch in the *NSX-T Administration Guide*.

Prepare your VMs for NSX 4

NSX Public Cloud Gateway(PCG) can connect your compute VPC with NSX after you install the NSX agent on VMs and tag these VMs appropriately in AWS. Currently the supported Operating Systems are: Windows 2012 Server R2 and Ubuntu 14.04.05.

This is a two-step process.

1 Install the NSX Agent on your Windows or Linux VM.

2 Tag the VM in AWS with the `nsx:network` key with the appropriate value for your overlay or underlay (non-overlay) VM.

Requirements and Recommendations

- Before launching a workload VM, make sure it is connected to the downlink subnet of PCG. If the VM is already on a specific subnet, make sure the downlink subnet is attached to it.
- It is recommended to use a jump host to access your workload VM. A jump host is a VM in your compute VPC that has a public IP address and provides a secure way of accessing other VMs in the VPC. Set up a jump host VM for each of the supported Operating Systems.
- If you have the Quarantine Policy enabled for your compute VPC, before installing the NSX agent, assign the `vm-override-sg` security group to the VM to ensure that NSX Cloud does not quarantine this VM by auto-assigning the `default` security group to the VM. See Chapter 5, "Manage Quarantine Policy," on page 23 for more information.
- If you have Quarantine Policy disabled, NSX Cloud does not apply any security groups to VMs. After installing the agent and tagging the VM as either underlay or overlay, assign the appropriate security group to the VM. See Chapter 5, "Manage Quarantine Policy," on page 23 for more information.
- Workload VM communication with PCG is permitted for essential protocols. For uncommon use cases, for example the use of DNS-UDP, you need to create a DFW permit rule.

About Overlay VMs

An overlay VM has the following features:

- Has the `nsx:network` tag key with the value of the logical switch assigned to this VM.
- Assigned the `vm-overlay-sg` in AWS, if you have the Quarantine Policy enabled. If not enabled, you must assign this security group to the overlay VM to ensure it is NSX-managed.
- Assigned an IP address from the NSX overlay network.
- See "Remote log in to an Overlay VM," on page 35 for instructions on how to access an overlay VM using SSH or RDP if Quarantine Policy is enabled.

About Underlay VMs

An underlay VM has the following features:

- Gets the `nsx:network` tag key with the value `default`.
- Assigned the `vm-underlay-sg` security group in AWS, if you have the Quarantine Policy enabled. If not enabled, you must assign this security group to the underlay VM to ensure it is NSX-managed.

This chapter includes the following topics:

Install the NSX Agent on your Windows VMs

Install the NSX Agent on your Windows VM. This is the first of two steps required to enable NSX to manage your VMs. Currently, only Windows 2012 Server R2 is supported.

Prerequisites

If you have the Quarantine Policy enabled for your compute VPC, before installing the NSX agent, assign the `vm-override-sg` security group to the VM to ensure that NSX Cloud does not quarantine this VM by auto-assigning the `default` security group to the VM. See Chapter 5, "Manage Quarantine Policy," on page 23 for more information.

Procedure

1 Find the VM's public or private IP address so you can connect to it using RDP (or any other method you prefer):

   a From the CSM dashboard, select **Cross-Cloud** > **AWS** > `<AWS_account_name>`

   b From the VPC section, select `<Compute-VPC-Name>` **Instances**

   c Select a Windows Server 2012 R2 VM.

   d Locate either the public or private IP address of the VM.

   Note If using a jump host, you do not need the public IP address, you can use the private IP address. This is the preferred method of accessing your workload VMs.

2 Download the installation script:

   a Remote log in to the VM using RDP.

   b Download the installation script from
   `http://nsx-gw.vmware.local:8080/factory_default/win63_x64/nsx_install.ps1`

   The default DNS name of PCG is `nsx-gw.vmware.local`. AWS Route 53 maps this name with the primary PCG IP address. The secondary CGW's IP address, if you have one for HA, is also mapped to the same DNS name.

3 Run the installation script: **`\nsx_install.ps1 -downloadPath <path> -operation install`**

   The script uses the interface with the lowest index as the default interface. For a list of all script options and uninstallation instructions, see "NSX Agent Install Script Options for Windows VMs," on page 32.

4 Verify that the required NSX Cloud and Open vSwitch services are running:

- nsx-agent
- nsx-vm-command-relay-agent
- logical-exporter
- ovs-vswitchd
- ovsdb-server
- ovs-l3d

Alternatively, run `sc.exe` in the Windows command prompt to verify that the required services are running:

```
c:\> sc query nsx-agent
```

What to do next

"Apply the nsx:network tag to VMs in AWS," on page 20

Install the NSX Agent on your Linux VMs

Install the NSX Agent on your Linux VM. This is the first of two steps required to enable NSX to manage your VMs. Currently, only Ubuntu 14.04.05 is supported.

Prerequisites

If you have the Quarantine Policy enabled for your compute VPC, before installing the NSX agent, assign the `vm-override-sg` security group to the VM to ensure that NSX Cloud does not quarantine this VM by auto-assigning the `default` security group to the VM. See Chapter 5, "Manage Quarantine Policy," on page 23 for more information.

Important NSX Agent installation on Ubuntu VMs requires internet access for downloading dependencies while installing NSX packages. Make sure your Ubuntu VM has a public IP address.

Procedure

1 Get the VM's IP address so you can log in to it using SSH:

a From the CSM dashboard, select **Cross-Cloud** > **AWS** > `<AWS_account_name>`

b From the VPC section, select `<Compute-VPC-Name>` **Instances**

c Select an Ubuntu VM.

d Locate either the public or private IP address of the VM.

Note If using a jump host, you do not need the public IP address, you can use the private IP address. This is the preferred method of accessing your workload VMs.

2 Download the installation script:

a Remote log in to the VM with root privileges.

b Download the installation script from the PCG: `wget http://nsx-gw.vmware.local:8080/factory_default/trusty_amd64/install_nsx_vm_agent.sh`

The default DNS name of PCG is `nsx-gw.vmware.local`. AWS Route 53 maps this name with the primary PCG's IP address. The secondary PCG's IP address, if you have one for HA, is also mapped to the same DNS name.

3 If required, change permissions on the installation script to make it executable, and run it:

a **`chmod +x install_nsx_vm_agent.sh`**

b **`sudo ./install_nsx_vm_agent.sh`**

The script uses `eth0` as the default interface. For a list of script options and uninstallation instructions, see "NSX Agent Install Script Options for Linux VMs," on page 33.

What to do next

"Apply the nsx:network tag to VMs in AWS," on page 20

(Optional) Generate AMI

You can generate an AMI of a VM with the NSX agent installed on it.

There are two ways in which you can generate an AMI of a VM with the NSX agent installed on it:

Option 1: You can generate AMIs from a VM that has the NSX agent installed on it but not configured. You can use an install script option to set up this VM for AMI-generation.

Option 2: You can also remove configurations from a VM that has been previously configured, in order to generate AMIs using it.

Procedure

1 By using an install script option while installing the NSX agent on the VM:

a Enter the following command:

- On a Windows VM:

```
.\nsx_install.ps1 -noStart true
```

- On an Ubuntu VM:

```
sudo
./install_nsx_vm_agent.sh --no-start
```

b Go to this VM in AWS and create an AMI.

2 By removing NSX agent configurations from a Windows or Linux VM to enable AMI generation:

a Open the NSX-T CLI: `sudo nsxcli`

b Enter the following commands: `hostname> set debug`

- ```
  hostname> set debug
  hostname> clear nsx-vm-agent state
  ```

c Go to this VM in AWS and create an AMI.

What to do next

Apply the `nsx:network` tag to VMs in AWS

Tag VMs with NSX agent installed on them as either overlay or non-overlay (underlay) in AWS. This is the final step in the two-step process to enable NSX to manage VMs.

Overlay VMs are assigned the overlay NSX-T logical switch ID. Non-overlay VMs are assigned a network by AWS.

NOTE You can also create your own logical switch in NSX Manager and assign a DHCP server to it. See instructions in the *NSX-T Administration Guide*.
  ```

You can apply the AWS tag either at the VM-level or the interface-level, but once you decide where to apply the tag, you must use the same level to apply the other tags. For example, if you tagged the interface with the `nsx:network` tag, you cannot apply other tags for this VM at the VM-level, you must choose the interface for any other tag.

The AWS tag's key is `nsx:network`.

For VMs in non-overlay mode, type in `default` (case-sensitive) for the tag value.

For VMs in overlay mode, do the following to find the tag value information:

1 From the CSM dashboard, select **Cross-Cloud > AWS > <AWS_account_name>**

2 From the VPC section, select **<your-compute-VPC> > Logical Switches**

3 Double-click and copy the value in the column **NSX Switch Tag**.

Procedure

1 Log in to the AWS console.

2 In the AWS console, select the VM with the NSX agent installed.

3 Add the tag details for the VM and save your changes.

Option	Description
Key	Enter `nsx:network`
Value	For overlay VMs: Paste the NSX logical switch tag ID you copied from CSM. Example: `c26b5f59-1648-462e-b747-287c72e82a87#OOUeB/I1M+v+zOXFoE4e5+UxCTmlsZpD4z7AQIhiFoG=` For underlay VMs: Type in `default` (case-sensitive).

Important If you have the Quarantine Policy enabled, and you assigned the `vm-override-sg` security group to this VM to prevent it from being quarantined while your prepare it for NSX, remove the `vm-override-sg` security group after applying the tag. NSX Cloud automatically assigns the `vm-overlay-sg` or `vm-underlay-sg` to the VM depending on the tag you applied.

Behind the Scenes: after you prepare your VMs for NSX

Essential NSX-T entities are created and configured automatically after you prepare your VMs for NSX.

The following is the list of these configurations:

- A logical port is created for this VM.
- The VM is assigned an overlay IP address (if you chose to set the mode to overlay).
- The VM is marked as NSX managed.
- The VM is reported as part of the inventory in NSX Manager to achieve, for example, micro-segmentation on logical constructs.
- East-West traffic is enabled for this VM.

Manage Quarantine Policy 5

NSX Cloud uses AWS Security Groups (SG) in conjunction with the VPC's Quarantine Policy for threat detection by quarantining rogue VMs.

For example, if a person with malicious intent forcibly stops the NSX agent on a managed VM, the compromised VM will be quarantined using the `default` SG in AWS. This is only possible for VPCs that have the Quarantine Policy enabled.

You can enable or disable Quarantine Policy for a VPC by right-clicking the VPC and selecting **Edit Quarantine**.

Quarantine Policy Enabled

When Quarantine Policy is enabled:

- The SG assignment for all interfaces for any EC2 Workload Instance (VMs) belonging to this VPC is managed by NSX Cloud. Appropriate Workload VM Security Group(s) are assigned to such interfaces.
  - Un-managed VMs are assigned the `default` SG and are quarantined. This limits the outbound traffic and stops all inbound traffic to such VMs.
  - Un-managed VMs can become NSX-Managed VMs when you install the NSX agent on the VM and tag them in AWS with `nsx:network`. In the default scenario, NSX will assign the `vm-overlay-sg` or `vm-underlay-sg` to allow appropriate inbound/outbound traffic.
  - An NSX-Managed VM can still be assigned the `default` SG and be quarantined if a threat is detected on the VM, for example, if the NSX agent is stopped on the VM.
  - Any manual changes to the security groups will be reverted to the NSX-determined security group(s) within 120 seconds.
  - If you want to move any VM out of quarantine, that is, move it out of the `default` SG, assign the `vm-override-sg` as the only SG to the VM. NSX Cloud does not auto-change the `vm-override-sg` SG and allows SSH and RDP access to the VM. Removing the `vm-override-sg` will again cause the VM security group(s) to revert to the NSX-determined security group(s).

Note When the Quarantine Policy is enabled, assign the `vm-override-sg` to your VMs before installing the NSX agent on them. After you follow the process of installing the NSX agent and tagging the VM in AWS as overlay or underlay, remove the `vm-override-sg` SG from the VM. NSX Cloud will automatically assign the appropriate SG to NSX managed VMs thereafter. This step is necessary because it ensures the VM is not assigned the `default` SG while you are preparing it for NSX.

Quarantine Policy Disabled

When Quarantine Policy is disabled:

- NSX Cloud does not assign any SG to the VMs launched in this VPC. You must assign the appropriate NSX Cloud SG in AWS to VMs to enable NSX Cloud functionality.

  From the AWS console:

- - Assign `vm_overlay_sg` to VMs that you want to manage using the NSX overlay network.
  - Assign `vm_underlay_sg` to VMs for which you want to use the underlay network provided by AWS.
  - Assign `vm_outbound_bypass_sg` and/or `vm_inbound_bypass_sg` to VMs for which you want to enable Distributed Services Routing.

AWS Security Groups

The following AWS Security Groups are created by NSX Cloud at the time of CGW deployment:

Table 5-1. AWS Security Groups created by NSX Cloud for Workload VMs

AWS Security Group name	Full Name
default	Default Security Group
vm-underlay-sg	VM Non-Overlay Security Group
vm-overlay-sg	VM Overlay Security Group
vm-override-sg	VM Override Security Group
vm-outbound-bypass-sg	VM Outbound Bypass Security Group
vm-inbound-bypass-sg	VM Inbound Bypass Security Group

Recommendations for Brownfield and Greenfield deployments

Brownfield: It is recommend to disable Quarantine Policy if you already have VMs set up in your VPC and you do not plan to have all your existing VMs to be managed by NSX. Disabling the Quarantine Policy ensures that your existing VMs are not automatically quarantined by being moved to the “default” SG in AWS.

Greenfield: For greenfield deployments, it is recommended that you enable Quarantine Policy to allow all threat detection workflows for your VMs to be managed by NSX Cloud.

Using Advanced NSX Cloud Features 6

This chapter includes the following topics:

Enable Syslog Forwarding

NSX Cloud supports syslog forwarding.

You can enable syslog forwarding for Distributed Firewall (DFW) packets on NSX-managed VMs.

Do the following:

Procedure

1 Log in to CGW using the jump host.

2 Type the `nsxcli` command to open NSX-T CLI.

3 Type the command to enable DFW log forwarding:

- `nsx-public-cloud-gateway> set gw-controller vm-log-forwarding enabled`

After this is set, NSX agent DFW packet logs are available under `/var/log/syslog` on CGW.

4 To enable log forwarding per VM, enter the following command:

- `nsx-public-cloud-gateway> set gw-controller vm-log-forwarding enabled <vm-id>`

Access AWS Services in the Underlay Network

AWS Services such as S3, ELB, RDS, have IP addresses that cannot be accessed by NSX-managed VMs in overlay-mode. To overcome this limitation, NSX Cloud provides Distributed Services Routing (DSR).

DSR is a feature that allows services in the overlay network to have direct access to underlay services in AWS. It also allows underlay services to access VMs via the overlay network.

Procedure

1 To enable only outbound access from your VM, do the following:

a Add the `nsx:directroute.[n]` tag to the VM with the CIDR of the service for which you want to enable access.

2 To enable outbound and inbound access from and to your VM, do the following:

   a Add the `nsx:directroute.[n]` tag to the VM with the CIDR of the service for which you want to enable access.

   b Add the `nsx:directinbound` tag to the VM with the value `true` (case-sensitive).

   You can add multiple outbound service prefixes/CIDRs using the `nsx:directroute.[n]` tag. The VM will drop all traffic from IP addresses not listed in the tag value.

   When you enable inbound services to this VM by attaching the `nsx:directinbound` tag, all the outbound services can send traffic to this VM. You cannot choose which services will send inbound traffic to the VM.

Example: DSR example

For example, if you want to enable S3 functionality on your VM in the us-west-2 region, add the following tags:

Table 6-1.

Key	Value
nsx:directroute.0	54.231.160.0/19
nsx:directroute.1	52.218.128.0/17
nsx:directroute.2	52.92.32.0/22

Table 6-2. AWS Tags for DSR

What you need to do...	Use this Tag Key(s)	Use this Tag Value	Behind the Scenes
Allow Outbound Traffic from VM	nsx:directroute.[n]	Provide one of the following: ■ IPv4 CIDR, e.g. 10.10.10.0/24 ■ The string "vpc-cidr-block". This is mapped to the CIDR of the VPC this VM belongs to.	Within about a minute, the VM is added to the AWS security group "`vm-outbound-bypass-sg`", which permits the appropriate outbound traffic.
Allow Inbound and Outbound Traffic to and from this VM	1 nsx:directroute.[n] 2 nsx:directinbound	1 Provide one of the values for outbound traffic. 2 Type in `true` (case-sensitive)	Within about a minute, the VM is added to the AWS Security Group: "`vm-inbound-bypass-sg`".

Enable NAT on NSX-managed VMs

NSX Cloud supports enabling NAT on NSX-managed VMs.

You can enable North-South traffic on VMs in overlay mode using AWS tags.

Procedure

- On the NSX-managed VM for which you want to enable NAT, apply the following AWS tag:

Key	Value
nsx:publicip	`<EIP from, AWS>`, for example, 50.1.2.3

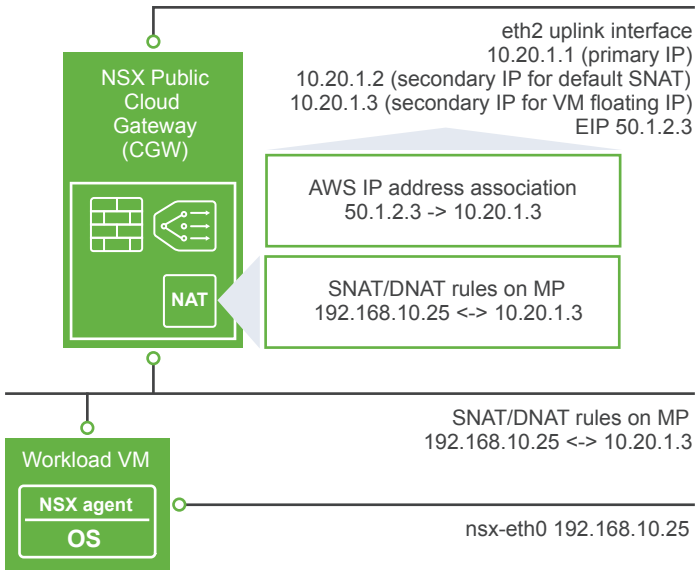
  Make sure the EIP you provide here is free to use. If you assign an EIP that was previously associated with any other instance or private IP, NAT does not work. In that case, unassign the EIP, remove the `nsx:publicip` tag on the VM or interface, and add it again.

After this tag is applied, the following configurations take place behind the scenes:

1. A secondary IP is allocated on the uplink interface of CGW. This IP is associated with the EIP specified in the tag's value.
2. One SNAT rule and one DNAT rule is created in NSX Manager mapping the overlay private IP of this VM with the secondary IP and vice versa. For example:
   - SNAT: 192.168.10.25 -> 10.201.1.3
   - DNAT: 10.20.1.3 -> 192.168.10.25
3. Two levels of NAT takes place.

   For SNAT:
   - From VM's overlay IP to CGW's secondary IP
   - From CGW's secondary IP to EIP in AWS

   For DNAT:
   - From EIP to CGW's secondary IP in AWS
   - From AWS secondary IP to the VM's overlay IP in CGW



Cheat Sheets and Troubleshooting 7

This chapter includes the following topics:

Onboarding Workflows

The workflows that allow NSX to manage workload VMs in your AWS cloud involve several steps to be performed in-tandem in NSX Cloud and AWS. This table depicts them at a glance.

Enabling NSX to Access your AWS Inventory and Manage your VMs

Table 7-1.

Task	NSX Cloud Workflow	AWS Workflow
1. Add your AWS account in CSM. See Chapter 2, "Enable CSM to access your AWS Inventory," on page 7 for detailed instructions.	1.1 From the NSX Cloud Dashboard, copy the URL of the JSON template file.	
		1.2. Create a new Stack in CloudFormation and use the JSON file copied in step 1.1.
		1.3. From the Outputs tab, copy IAMRoleARN, ExternalID, GatewayRoleName.
	1.4. From the CSM dashboard, click Add Account. Provide a distinct name for the account, and the values from step 1.3.	

Table 7-1. (Continued)

Task	NSX Cloud Workflow	AWS Workflow
2. Deploy PCG on a compute VPC in your AWS account. See Chapter 2, "Enable CSM to access your AWS Inventory," on page 7 for detailed instructions.		2.1 .For the compute VPC you want to manage with NSX, create three (six, if enabling HA) subnets and ensure this VPC has an Internet gateway with routing tables. Also ensure the VPC has DNS routing and DNS names enabled. Make a note of the PEM file for your AWS account. Alternatively, use the CloudFormation template, from the Resources tile on the NSX Cloud Dashboard, to create a compute VPC.
	2.2. From the CSM dashboard, go to VPCs. Select the compute VPC and click **Deploy Gateway**. Select the PEM file for your AWS account, and select whether you want to turn Quarantine Policy on or off.	
	2.3. Select whether you want to set up High Availability. Select the Availability Zone and the management, uplink, and downlink subnets. Select an additional Availability Zone and the three additional subnets in this zone if you picked HA. Click **Deploy**.	
		2.4. Automatic: As part of PCG deployment, a set of Security Groups are created in your AWS account. A new Type A Record Set is added with the name: "nsx-gw.vmware.com" in AWS Route 53.
	2.5. Automatic: As part of PCG deployment, a set of components -- including two default Logical Switches are created in NSX Manager.	
	2.6. From NSX Manager: Attach DHCP servers to the default overlay logical switch created in step 2.5. Also attach the auto-created tier-0 logical router to the overlay logical switch.	
3. Enable NSX to manage your VM. See Chapter 4, "Prepare your VMs for NSX," on page 17 for detailed instructions.		3.1. Download and Install the NSX-agent on your Windows and Linux VMs.

Table 7-1. (Continued)

Task	NSX Cloud Workflow	AWS Workflow
		3.2. Tag VMs with the key `nsx:network` with the value of either the logical switch UUID (overlay VMs) or `default` (non-overlay VMs)
	3.3. Automatic: After you install the NSX-agent on your VM and tag it in AWS, the VM is marked as NSX-managed and other essential NSX entities are created.	

Verify NSX Cloud Components

It is a best practice to verify that all components are up and running, before deploying in a production environment.

Verify whether NSX Agent is connected to CGW

To verify that the NSX Agent on your workload VM is connected to CGW, do the following:

1 Type the `nsxcli` command to open NSX-T CLI.

2 Type the following command to get the gateway connection status:

```
get gateway connection status
Public Cloud Gateway  : nsx-gw.vmware.com:5555
Connection Status     : ESTABLISHED
```

Verify the VM's Interface/Network Mode

The VM on which the NSX agent is installed, can have one of two switch modes -- overlay or non-overlay. Verify as follows:

1 Type the nsxcli command to open NSX-T CLI.

2 Type the command to view the switch mode.

```
get vm-network-mode
VM-Network-Mode : overlay
Interface : eth0
```

The `nsx:network` key must have the value `default` (non-overlay) or `<logical_switch_ID_from_NSX-T>` for the overlay Logical Switch ID.

Verify VM Interface Tag in AWS

The Windows and Ubuntu VMs must have the correct tags to connect to CGW.

1 Log in to the AWS console.

2 Verify the VM eth0 or interface tag.

AWS Tags for NSX Cloud

NSX Cloud uses AWS Tags extensively to allow NSX to manage your VMs and enable other services.

Important You can assign tags either to the VM or to an interface. Once you assign the mandatory `nsx:network` tag to either the VM or an interface, you must assign the other tags to the same.

Table 7-2. AWS Tags for NSX Cloud

Mandatory or Optional	AWS Tag: Key	AWS Tag: Value	Purpose
Mandatory	nsx:network	■ Overlay VM: UUID of the Logical Switch attached to this VM ■ Non-overlay VM: `default`	When this tag is applied to a VM with the NSX agent installed on it, the VM becomes NSX-managed. See Chapter 4, "Prepare your VMs for NSX," on page 17 for detailed instructions.
Optional	nsx:publicip	Elastic IP address from AWS	This tag enables NAT on the VM. See "Enable NAT on NSX-managed VMs," on page 26 for detailed instructions.
Optional	nsx:directroute.[n]	IPv4 CIDR or `vpc-cidr-block`	This tag enables outbound Distributed Services Routing. See "Access AWS Services in the Underlay Network," on page 25 for detailed instructions.
Optional	nsx:directinbound	`true` (case-sensitive)	This tag, along with the `nsx:directroute.[n]` tag, enables inbound Distributed Services Routing. See "Access AWS Services in the Underlay Network," on page 25 for detailed instructions.

NSX Agent Install Script Options and Uninstallation

The NSX Agent installation script provides configurable options. This table lists these options.

NSX Agent Install Script Options for Windows VMs

Table 7-3.

Option	Description
`-gateway <ip|dns>`	NSX public cloud gateway IP or DNS name. Specify this option if you want to use an IP address for the PCG. The default DNS name of the PCG is `nsx-gw.vmware.local` which is used if this parameter is not specified.
`-noStart true`	You can create an AMI of the VM after the NSX agent is installed on it. Run the install script with this option. Then from the AWS console, create an AMI of this VM.

Table 7-3. (Continued)

Option	Description
`–downloadPath <path>`	This is the path to the directory in which the files should be downloaded. If the path includes escape characters, enclose them in single quotation marks. Default = %temp%
`–silentInstall <true/false>`	If this is set to `true`, the script runs a silent installation. Default is `false`
`–noSigCheck <true/false>`	This allows you to specify whether to check the signatures on the binaries or not. Default = `false`
`–logLevel <value>`	This allows you to specify the log level for NSX components Default = 1 Verbose = 3
`–operation <install/uninstall>`	This allows you to specify the operation to perform: `install` or `uninstall` Default = `install`
`–bundlePath <path>`	This allows you to specify the local path to the NSX VM agent bundle Default option is to download the bundle from PCG.

Uninstalling NSX agent from a Windows VM

1 Remote log in to the VM using RDP.

2 Run the installation script with the uninstall option:

```
\nsx_install.ps1  –operation uninstall
```

NSX Agent Install Script Options for Linux VMs

Table 7-4.

Option	Description
`––gateway <ip|dns>`	NSX public cloud gateway IP or DNS name. Specify this option if you want to use an IP address for the PCG. The default DNS name of the PCG is `nsx–gw.vmware.local` which is used if this parameter is not specified.
`––no–start`	You can create an AMI of the VM after the NSX agent is installed on it. Run the install script with this option. Then from the AWS console, create an AMI of this VM.

Uninstalling NSX agent from a Linux VM

Remote log in as `root` and run the following commands on the VM:

Note To log in to a VM in overlay mode using SSH, use port 8888.

1 Stop NSX services:

```
service nsx-agent stop
service nsx-agent clear-everything
```

Note In overlay mode, SSH connection will be lost. Log in to the VM again to complete the uninstallation.

2 Uninstall packages:

```
apt-get -y purge libgoogle-glog0
apt-get -y purge libjson-spirit
apt-get -y purge nicira-ovs-hypervisor-node
apt-get -y purge nsx-agent-public-cloud
apt-get -y purge nsx-aggservice
apt-get -y purge nsx-host-public-cloud
apt-get -y purge nsx-logical-exporter public-cloud
apt-get -y purge nsx-public-cloud-vm-cli
apt-get -y purge openvswitch-common
apt-get -y purge openvswitch-datapath-dkms
apt-get -y purge openvswitch-pki
apt-get -y purge openvswitch-switch
apt-get -y purge python-openvswitchVerify
```

3 Clear configurations and dependencies:

```
apt-get -y autoremove
apt-get -y autoclean
apt-get -y clean
```

4 Clean up directories:

```
rm -rf /config/vmware
rm -rf /etc/vmware
rm -rf /opt/vmware
rm -rf /run/vmware
rm -rf /var/log/vmware
rm -rf /var/vmware
```

5 Go to the VM in the AWS console and remove the `nsx:network` tag from the VM or interface.

Undeploying PCG

You can undeploy PCG from a VPC, but remember to delete all logical entities associated with it first.

Undeploying PCG

To undeploy PCG, click **Undeploy Gateway** from the VPC. The default entities created by NSX Cloud are removed automatically when a PCG is undeployed.

Delete all the logical entities you created in NSX Manager before undeploying the gateway. Refer to the list below to find your entities to delete:

- AWS: DNS entry in route 53
- DDI: DHCP profile
- Routing: SNAT rule
- Routing: static Router
- Routing: Logical Router Port
- Routing: Logical Router
- Fabric-Nodes: Edge Cluster
- Fabric-Nodes: Transport Nodes
- Fabric-Nodes: Edges
- Fabric-Profiles: PCG-Uplink-HostSwitch-Profile
- Switching: Logical Switch ports
- Switching: Logical Switches
- Fabric-Transport Zones: Transport Zones
- Switching: PublicCloud-Global-SpoofGuardProfile

Remote log in to an Overlay VM

If Quarantine Policy is enabled, access to overlay VMs is restricted and if you need to log in to one remotely, you need to use the `vm-override-sg` security group.

To access an overlay VM using SSH or RDP, do the following:

1. Apply the `vm-override-sg` security group to this VM. This takes the VM out of the `vm-overlay-sg` security group and becomes open for remote login.
2. Use port 8888 to reach Ubuntu VMs using SSH.
3. You can reach Windows VMs using RDP using the standard port, but only via a jump host.
4. After completing your task in the VM using remote login, remove the `vm-override-sg` security group from the VM. NSX Cloud automatically attaches the appropriate security group to VMs within 60 seconds.

Using NSX Manager

8

NSX Manager provides an interface that allows you to configure and manage networking for VMware NSX-T.

NSX Cloud pre-configures the essential NSX components — logical switches, a tier-0 router, transport zones and transport nodes. See "Behind the Scenes: after adding AWS account and deploying PCG," on page 11.

Important Do not delete any of the NSX-created entities.

See the *NSX-T Administration Guide* for instructions on using NSX features that are supported in this NSX Cloud release.

Note The NSX-T Administration Guide provides the following instruction for accessing NSX Manager:

```
From your browser, log in to NSX Manager at https://nsx-manager-ip-address.
```

For NSX Cloud, follow this instruction:

```
From the NSX Cloud dashboard, click NSX Manager
to open the NSX Manager console in the current browser window.
```

Table 8-1. NSX-T Task Reference for NSX Cloud

NSX-T Task	Note for NSX Cloud	Reference
Creating Logical Switches	Layer 2 Bridging is not supported in the current release	Creating Logical Switches and Configuring VM Attachment
Configuring a Tier-0 Logical Router	A Tier-0 logical router is created automatically. Follow instructions in this guide to attach the logical router to the overlay logical switch	Configuring a Tier-0 Logical Router
Firewall Sections and Firewall Rules	All Firewall features are supported, except Edge Firewall.	Firewall Sections and Firewall Rules
Setting up DHCP Servers	All DHCP-related tasks are supported, except DHCP relay.	DHCP
Configuring IPFIX	Supported in NSX Cloud	Configure IPFIX
Traceflow Monitoring	Supported in NSX Cloud	Tracefolw Monitoring
Port Connection Tool	Supported in NSX Cloud	Port Connection Tool

Index