Getting Started Guide

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

Getting Started with NSX Cloud

The NSX Cloud *Getting Started Guide* provides information on how to configure theVMware NSX Cloud™ components for your public cloud, such as the Amazon Web Services (AWS) environment to provide network and security across public clouds.

Intended Audience

This information is intended for anyone who wants to use NSX for the public cloud. The information is written for experienced system administrators who are familiar with virtual machine technology and virtual networking concepts and operations.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

Understanding VMware NSX Cloud 1

NSX Cloud uses NSX-T components and integrates them with your public cloud.

NSX Cloud workloads for public cloud provide a multi-tenant dashboard, which is integrated with VMware Cloud services. The service deployment, upgrade, backup, and restore are managed by the VMware Service Reliability Engineering (SRE) team.

NSX Cloud lets you develop and test applications using the same network and security profiles used in the production environment. Developers can manage their applications until they are ready for deployment. With disaster recovery, you can recover from an unplanned outage or a security threat to your public cloud. You can also migrate your workloads between your public clouds.

This chapter includes the following topics:

NSX Cloud Architecture

NSX Cloud uses the NSX-T core components -- NSX Manager and Controllers -- and integrates them with your public cloud to provide network and security across your implementations.

NSX Cloud is agnostic of provider-specific networking that does not require Hypervisor access in a public cloud. Integration with CSP provides AWS Identity and Access Management (IAM), billing, logging, and security support for a public cloud environment.

The VMware SRE team deploys, monitors, and troubleshoots any errors that might occur in the public cloud.

The core NSX Cloud components are:

- NSX Manager for the management plane with role-based access control (RBAC) defined.
- NSX Controller for the control plane and run-time state.
- Cloud Service Manager (CSM) for integration with NSX Manager to provide public cloud-specific information to the management plane.
- NSX Public Cloud Gateway (CGW or PCG) for connectivity to the NSX management and control planes, NSX Edge gateway services, and for API-based communications with the public cloud entities in the compute VPC (such as VPCs, EC2 Instances, and Security Groups). The CGW is deployed in a compute VPC via CSM.

- NSX Agent functionality that provides NSX-managed datapath for workload VMs.

Management VPC and Compute VPC

NSX Cloud components, namely, NSX Manager, Controller Cluster, and Cloud Service Manager, are hosted inside VMware's AWS account in, what we call, a management VPC.

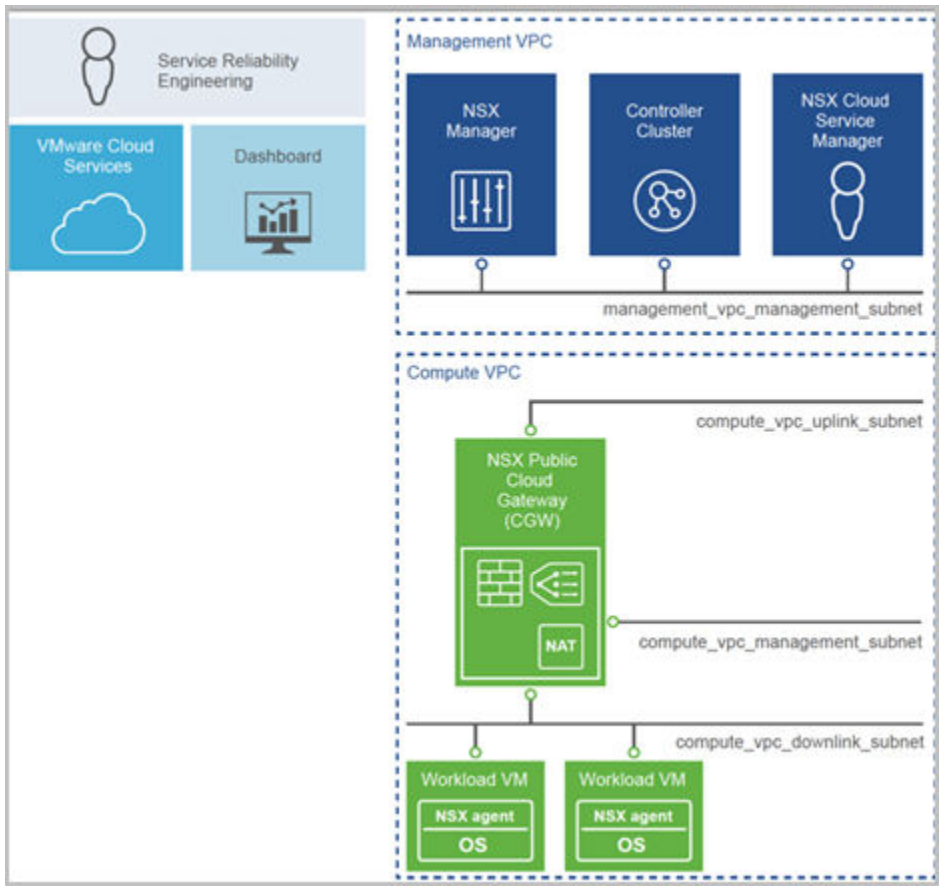
The VPC that you want to manage with NSX via NSX Cloud is, what we call, a compute VPC.

You need to set up three subnets in this compute VPC that separate out the management, uplink, and downlink traffic. The management traffic is for NSX Manager and this subnet needs one IP address per PCG. The uplink subnet is for Internet traffic, and the downlink subnet is for data traffic in and out of your compute VPC.

As part of configuring your compute VPC, you deploy a single (or HA pair) of CGW and select these subnets to configure the gateway. This forms the basis of allowing NSX to manage your workload VMs.

Your application instances will be launched in this compute VPC.

Figure 1-1. NSX Cloud Architecture



Micro-segmentation Security Support

With Micro-segmentation, you can control East-West traffic between application instances running in the AWS cloud.

With NSX Cloud micro-segmentation security, you can control East-West traffic between application instances running in the AWS cloud. NSX Cloud applies policy based on VM attributes, and the policy stays applied even when the instance moves. You can define a policy for example, to isolate a VM to avoid the spread of advanced persistent threat. Once this policy configuration is applied, it is used across multiple VPCs and availability zones without having to recreate them for each VPC.

IT can enforce security controls on North-South traffic flowing to and from individual instances and the Internet. Micro-segmentation security can also be enforced at the instance-level. You can define security rules based on, for example, VM name, OS type, AMI ID, and user-defined tags.

NSX Cloud also enables real-time logging and monitoring of security events by integrating with common security information and event management (SIEM) tools.

Overlay Networking Support

NSX Cloud provides an abstraction layer independent of the underlying cloud constructs.

NSX Cloud provides an abstraction layer independent of the underlying cloud networking constructs. It provides a model for provisioning and managing networking and security for applications and workloads running in the public cloud.

IT can use overlay networking to control networking topologies, traffic flows, IP addressing, and protocols within and across cloud VPCs. For example, IT can stretch NSX Cloud subnets for application workloads running in multiple availability zones. IT can also deploy multicast-aware applications in VPCs.

Extensive Troubleshooting Support

NSX Cloud offers extensive troubleshooting capabilities that can be used with existing tools and processes.

NSX Cloud offers extensive troubleshooting capabilities that can be used with existing tools and processes. These tools can track application traffic flows within and between VPCs to provide real-time diagnostics and troubleshooting capabilities.

NSX Cloud uses standard protocols such as, IPFIX, Traceflow, and Port-Connect to enable diagnostics and troubleshooting. IT can analyze traffic flows from the NSX Cloud management console or use the common on-premises network management tools. These tools reduce the time it takes to identify and resolve network connectivity and performance issues in the public cloud.

Adding Users and Assigning Roles 2

Follow this process to add users and assign roles.

This chapter includes the following topics:

Add Users

NSX Cloud uses VMware Cloud Services for authentication and access control.

As an early access participant, you receive an email invitation containing a link that you can use to sign up for VMware Cloud. You can use this link only once.

You sign up for a VMware Cloud account with your VMware ID. If you do not have a My VMware account, you create one as you sign up.

When you sign up, you join an organization. Think of an organization as a container for users and the cloud services they have permission to access. If you are the first person to sign up in the organization, you are assigned the role of Organization Owner. As Organization Owner, you register your default VMware credit fund as your method of payment.

Procedure:

1 Click the link in your invitation email.

2 Sign up for NSX Cloud:

   a If you have a VMware ID, sign up for NSX Cloud with your VMware ID credentials.

      If you do not have a VMware ID, first create your My VMware account, and then sign up for VMware Cloud.

   b If you do not have a VMware ID, first create your My VMware account, and then sign up for VMware Cloud.

3 Log in to VMware Cloud with your VMware ID. If you are not redirected to the main VMware NSX Cloud page, go to https://console.nsx.cloud.vmware.com.

Access your Organization

When you access VMware Cloud services, you are logged in to the organization to which you were invited. You can see the name of the organization on the menu, under your user name. If you belong to more than one organization, you can switch between organizations.

Procedure

1 On the menu, click the arrow next to your user name. A drop-down menu appears showing the name of the organization.

2 Click the arrow next to the organization. A drop-down menu appears showing the organizations to which you belong.

3 Select the organization you want to access.

Manage Multiple Organizations

If you belong to multiple organizations, you have the option to set up a default organization. You can also switch between organizations.

- Specify a default organization: From the VMware Cloud Services dashboard, click on **your username > Set Default Organization**. Select the organization you want to set as the default. Once you set up a default organization, every time you log in to NSX Cloud, you will be signed in with this organiztion.
- Switch between organizations: From the VMware Cloud Services dashboard, click on your username. You see the list of organizations by clicking on the organization name that you are currently logged in with. Select any other organization from the list.

Note If the organization you select to switch to, does not have access to NSX Cloud, you are redirected to the VMware Cloud Services dashboard with a message indicating your lack of access to NSX Cloud.

Add Users to Your Organization

As a VMware Cloud services organization owner, you invite users to your organization and give them access to the services associated with it. The users you invite to VMware NSX Cloud will have predefined roles.

Procedure

1 Click the **VMware Cloud Services** icon at the top right corner, and click **Identity Access Management**.

2 Click **Add Users**.

3 Type in the email address of the user you want to add to your organization. To invite more than one user, you can add multiple email addresses separated by commas.

4 Select a role from the **Role** in organization drop-down menu. Pick the role that the user will use in the organization.

5 Select a role from the **Role in service** drop-down menu.

6 Click **Add service access**.

7 Select VMware NSX Cloud

8 Click **Add** to send an invitation to the user.

See Using VMware Cloud Services for more information on signing up, managing, and organizing users.

Assign NSX Cloud Roles

Assign roles to NSX Cloud users .

When adding users to the NSX Cloud organization from the VMware Cloud dashboard, you can select one or both of the following roles:

- Cloud Service Admin

- Cloud Service Auditor

Note If you select both the roles, the Cloud Service Admin role is applied to the user because that is the role with higher privileges.

Table 2-1. NSX Manager Privileges by Role

Role	Privileges
Cloud Service Admin	CRUD privileges for all NSX Manager tasks including managing Firewalls, setting up routing, setting up switching, etc. See "Role-Based Access Control for NSX Manager," on page 13 for a detailed list.
Cloud Service Auditor	Read-Only privileges for NSX Manager tasks

Table 2-2. Cloud Service Manager (CSM) Privileges by Role

Role	Privileges
Cloud Service Admin	CRUD privileges for all Cloud Service Manager tasks including: * Deploying/Undeploying Public Cloud Gateway (CGW) * Changing Quarantine Policy * Adding AWS Accounts
Cloud Service Auditor	Read-Only privileges for Cloud Service Manager Tasks

Role-Based Access Control for NSX Manager

With role-based access control (RBAC), you can restrict system access to authorized users. Users are assigned roles and each role has specific permissions.

There are four types of permissions:

- CRUD (Create, Retrieve, Update and Delete)
- Execute
- Read
- None

NSX Cloud has the following built-in roles. You cannot add any new roles.

- Cloud Service Administrator
- Cloud Service Auditor

Roles and Permissions

Table 2-3. Roles and Permissions

NSX-T Operation	Cloud Service Admin	Cloud Service Auditor
Tools > Port Connection	E	R
Tools > Traceflow	E	R
Tools > Port Mirroring	CRUD	R
Tools > IPFIX	CRUD	R
Firewall	CRUD	R

Table 2-3. Roles and Permissions (Continued)

NSX-T Operation	Cloud Service Admin	Cloud Service Auditor
Routing > Routers	CRUD	R
Routing > NAT	CRUD	R
DDI > DHCP > Server Profiles	CRUD	R
DDI > DHCP > Servers	CRUD	R
DDI > DHCP > Relay Profiles	CRUD	R
DDI > DHCP > Relay Services	CRUD	R
Switching > Switches	CRUD	R
Switching > Ports	CRUD	R
Switching > Switching Profiles	CRUD	R
Fabric > Nodes > Hosts	R	R
Fabric > Nodes > Edges	R	R
Fabric > Nodes > Edge Clusters	R	R
Fabric > Nodes > Transport Nodes	R	R
Fabric > Profiles > Uplink Profiles	R	R
Fabric > Profiles > Edge Cluster Profiles	R	R
Fabric > Profiles > Configuration	R	R
Fabric > Transport Zones	R	R
Fabric > Compute Managers	R	R
System > Utilities > Support Bundle	R	R

Using the NSX Cloud Dashboard 3

The NSX Cloud Dashboard is the entry point for CSM and NSX Manager. This is where you select the maintenance window for automatic upgrades.

When you log in from the VMware Cloud Services dashboard and request deployment of NSX Cloud for your chosen region, the NSX Cloud Dashboard is the first user interface that opens up.

For every subsequent login, the NSX Cloud Dashboard is the entry point for CSM and NSX Manager.

From the Dashboard you can do the following:

1 Go to Cloud Service Manager: Click the **Cloud Service Manager** button. An instance of CSM opens in the current browser window.

2 Go to NSX Manager: Click the **NSX Manager** button. An NSX Manager instance opens in the current browser window.

Note Currently you cannot right-click to open CSM or NSX Manager in a new tab or window. If you want to open both the appliances, log in to the NSX Cloud console from two separate browser tabs or windows to open instances of the NSX Cloud Dashboard from where you can open CSM in one tab and NSX Manager in the other.

---

3 Get an overview of your AWS VPCs: In the Inventory tile you can see the number of VPCs and EC2 Instances your AWS account hosts. Hover the mouse pointer over the donut charts for a quick glance at:
   a The number of VPCs or EC2 Instances (VMs) managed by NSX Cloud.

   b The state of the managed VPCs, denoted by colors. Green indicates the managed VMs are up and running. Red indicates errors in the managed VMs. Grey indicates unmanaged VMs.

4 Choose an Upgrade and Maintenance window: NSX Cloud upgrades are pushed automatically to ensure the latest features and bug-fixes are available for your environment. You have the option to pick a day and time from the maintenance window to schedule the upgrade. If you do not make a choice, upgrades are pushed to your deployment on the last available day in the maintenance window.

Getting Started Checklist

4

Use this checklist to track your tasks as you configure AWS and NSX Cloud.

Table 4-1. Getting Started Checklist

Task	Detail
❑ Read the Release Notes	See VMware NSX Cloud Release Notes
❑ Add Users and Assign Roles	See Chapter 2, "Adding Users and Assigning Roles," on page 11
❑ Enable CSM to access your AWS inventory	See Enable CSM to access your AWS inventory
❑ Prep VMs for NSX	See Prepare your VMs for NSX
❑ Select a Maintenance Window for Upgrades	See Chapter 3, "Using the NSX Cloud Dashboard," on page 15
❑ Find support	Pick a support option: ■ Call: +1-877-486-9273 ■ Email: support@vmware.com ■ Chat: Click on the Chat icon from any of the NSX Cloud screens. A support person can help you with your questions in real-time.

Index