Setting Up VMware NSX-T for Photon Platform

Contents

1 Introduction

Here's how to set up VMware NSX-T 1.1 to work with Photon Controller 1.2. NSX-T must be in place before you install Photon Controller. After NSX-T is installed and configured to work with Photon Controller, you add the information about the NSX network to Photon Controller's YAML deployment file.

In this document, *NSX* refers to NSX-T version 1.1. Only minimal instructions are provided for installing and setting up NSX; if you need help, see the VMware documentation for NSX.

This document assumes that you have obtained valid licenses for NSX and have a VMware account with permission to access and download the NSX installers.

2 Requirements

- NSX-T 1.1.
- At least one ESXi host dedicated to NSX. The required version, update level, and patch number of ESXi appears in the NSX Installation Guide. The ESXi hosts that you use for NSX cannot be used for Photon Controller or Lightwave.
- An ESXi host dedicated to Photon Controller.
- An ESXi host dedicated to Lightwave.
- Each ESXi host must have at least 2 NIC cards.

Therefore, you need at least 3 ESXi hosts: one for NSX, one for Photon Controller, and one for the Lightwave security system—and all of them must have at least 2 NIC cards. NSX itself might require more than 1 ESXi host; see the NSX documentation for memory and other requirements.

ESXi Patch Requirement

This guide assumes that the ESXi hosts are in place with the following attributes. The ESXi host can be either the licensed or the free version.

- It is running VMware ESXi 6.5 Patch 201701001 (ESXi650-201701001), which you can find by searching for patches for ESXi 6.5.0 on the My VMware Product Patches web site at https://my.vmware.com/group/vmware/patch. The patch's build number is 4887370.

This guide also assumes that you have root access to all the ESXi hosts, know how to manage them with the vSphere Web Client, and understand basic networking in a virtualized environment. Only minimal instructions are provided for working with ESXi and its web client, which is also known as the VMware ESXi Host Client; if you need help, see the VMware documentation for vSphere and ESXi.

3 NSX Overview

NSX is a software-defined network that runs on a hypervisor to reproduce such networking services as switches, routers, and firewalls. NSX has three planes: management, control, and data. As a system administrator, you manage all the nodes in the NSX system by connecting to the management plane through the API or the user interface. The control plane computes state and disseminates information about the system's configuration and topology. The data plane processes packets according to tables populated by the control plane.

The planes run as software on three kinds of nodes or clusters of nodes: manager, controller, and Edge transport nodes. The manager hosts the API and other services. The controller deploys virtual networks across the NSX architecture. And the *NSX Edge transport node* connects virtual machines to logical switches by routing IP addresses and performing other IP services. On a transport node, NSX creates a hostswitch that binds logical router uplinks and downlinks to physical NICs.

A collection of transport nodes forms a *transport zone*—a fabric of logical switches that connects VMs to hypervisors. In NSX, a transport zone determines the extent of a Layer 2 network. An NSX Edge transport node can belong to one overlay transport zone and one or more VLAN transport zones. The overlay transport zone is for internal NSX tunneling between transport nodes. The VLAN transport zones are for the VLAN uplinks to the external physical network.

4 Understanding Fabric Topology

For Photon Controller, a single overlay transport zone is shared by all Photon Controller cloud hosts as well as the Edge node. The overlay transport zone provides L2 connectivity between VMs through a logical switch.

A single VLAN transport zone is also created. The purpose of this VLAN transport zone is to provide connectivity between the logical network and the external, physical network. The Edge node joins both the overlay transport zone and VLAN transport zone.

5 Virtual Network Topology

You create a single top-tier Tier-0 logical router to provide northbound connectivity with the external network and sounthbound connectivity to Tier-1 routers. The Tier-0 router also provides interconnectivity among Tier-1 routers.

In a Photon Controller project, you can create multiple Tier-1 logical routers to provide L3 connectivity; each Tier-1 router can contain multiple subnets. In NSX, a Tier-1 router is the second-tier router that, if the network type is ROUTED, connects to the Tier-0 router for northbound connectivity. A logical switch is created for each subnet to provide L2 connectivity. All VMs belonging to the same subnet are attached to the corresponding logical switch.

With an NSX network, a single Tier-0 router is created. It sits between the physical network and the virtual networks.

6 IP Addressing and Routing Requirements for Photon Controller

The virtual network topology for Photon Controller carries the following requirements for the NSX virtual network:

Physical router: You must be able to add a static route to a physical router outside the NSX virtual network so that if you choose to set up your Tier-0 router on a different subnet, you and others can access the virtual network. The physical router uses the static route to communicate with the virtual networks created by Photon Controller.

The gateway IP address of the physical network will be used to route all traffic to and from the NSX virtual networks.

The NSX Tier-0 router: You must use a static IP address accessible by the physical network written in CIDR format–for example, 198.51.100.9/24.

The IP address pool for Photon Controller must contain only private IP addresses specified in CIDR format.

The host uplink vLAN ID that is in the YAML deployment template for Photon Controller must be specified so that it can be used in the NSX host uplink profile to register the ESXi host with NSX. To complete this field, look up the port group vLAN ID on the switch that your ESXi hosts are connected to.

The DNS server IP address is the IP addresses of the DNS server that you are using for NSX. You add this value to the `dnsServerAddresses` key in the NSX section of the Photon Controller YAML deployment file. You can specify a maximum of two DNS server IP addresses for NSX.

The floating IP address pool for Photon Controller contains public IP addresses. The floating IP addresses will be assigned to VMs so that each VM is publicly accessible.

7 Installation Prerequisites

- Read the NSX Release Notes.
- Read the NSX Installation Guide to understand basic NSX concepts.
- Follow chapter 5 of the NSX Installation Guide to deploy NSX Manager on an ESXi host.
- Follow chapter 6 of the NSX Installation Guide to deploy NSX Controller on an ESXi host.
- Follow chapter 7 of the NSX Installation Guide to deploy NSX Edge on an ESXi host.

Do not proceed with the installation of NSX and its configuration for Photon Platform until you have read the NSX documentation.

8 Download and Install the NSX OVAs

Use your My VMware account to download version 1.1 of the following NSX-T OVAs from My VMware:

- The NSX Manager OVA.
- The NSX Controller OVA.
- The NSX Edge OVA.

For help, see the requirements and the instructions in the NSX Installation Guide. If you need additional instructions on how to deploy an OVA on ESXi, see the vSphere documentation.

9 NSX Configuration

After installing the NSX components, you must configure NSX for Photon Controller before deploying Photon Controller. The following steps are required:

- Create a VLAN transport zone.
- Create an overlay transport zone.
- Create an uplink profile.
- Create an IP address pool.
- Configure an Edge transport node.
- Create an Edge cluster.
- Create a Tier-0 router.
- Connect the Tier-0 router to the external network.

You can complete these steps by logging in to your NSX Manager at the following URL:

`https://<ip-address-of-nsx-manager>`

9.1 Create a VLAN Transport Zone

Select `Fabric` > `Transport Zones` and click `Add`.

The Name can be something like tz-vlan and the Host Switch Name can be something like vlan-host-switch. For Traffic Type, select VLAN.

See Chapter 9 of the NSX Installation Guide for more on information creating a VLAN transport zone.

9.2 Create an Overlay Transport Zone

Select Fabric > Transport Zones and click Add.

The Name can be something like tz-overlay and the Host Switch Name can be something like overlay-host-switch. For Traffic Type, select Overlay.

See chapter 9 of the NSX Installation Guide for more information creating an overlay transport zone.

9.3 Create an Uplink Profile

The default uplink profile created by NSX defines a stand-by uplink, which is not supported by transport zone uplinks.

To create a new uplink profile, click Fabric > Profiles > Uplink Profiles and click Add.

The name can be, for example, tz-uplink-profile. For Teaming Policy, select Failover Order. For Active Uplinks, enter uplink-1. For Transport VLAN, enter 0.

9.4 Create an IP Address Pool for Tunnel Endpoints

The IP address pool provides internal IP addresses for NSX tunnel endpoints, that is, the ESXi hosts and the Edge node. Choose an internal IP address range that does not conflict with the IP addresses on the physical network; for example, 192.168.150.100-192.168.150.200.

Select Inventory > Groups > IP Pools and click Add.

See Chapter 9 of the NSX Installation Guide for more information about creating an IP address pool.

9.5 Configure an Edge Transport Node

During NSX installation, an Edge entity automatically appears in the NSX Manager web interface after the Edge is joined to the management plain. You can find the Edge entity under Fabric > Nodes > Edges.

To configure the Edge entity as a transport node, select the Edge entity, and then click Actions > Configure as Transport Node.

For the overlay host switch only, you need to choose the IP address pool that you created for the tunnel endpoints.

You must choose the corresponding vNICs for each virtual NIC. See the NSX Installation Guide on how to choose and set up NSX Edge vNICs.

9.6 Create an Edge Cluster

To create an Edge cluster, click Fabric > Nodes > Edge Clusters > Add.

To add the Edge transport node to the cluster, click Edit. For Type, select Virtual Machine, and then move the Edge Transport Node from Available to Selected.

9.7 Create a Tier-0 Router

To create a Tier-0 router, click `Routing` > `Add` > `Tier-0 Router`. For `High Availability Mode`, select `Active-Active`.

9.8 Connect the Tier-0 Router to the External Network

First, to connect the Tier-0 router to the external network, create a VLAN logical switch that connects to the Tier-0 router.

Click `Switching` > `Switches` > `Add`.

Set the `Admin State` to `Up`, select `None` for the `Switching Profiles Type`, and set the `VLAN` to `0`.

Second, create a new router port on the Tier-0 router that connects to the VLAN logical switch.

Click `Routing` > `Routers`, and then click the Tier-0 router. Click `Configuration` > `Router Ports` > `Add`.

For `Type`, select `Uplink`. For `Transport Node`, select the Edge transport node that you created earlier. For `Logical Switch Port`, select `Attach to new switch port`. For `Switch Port Name`, you can name it something like `vlan-switch-to-tier0-router`. For `IP Address/mask`, the IP address that you enter must be in CIDR notation and must be accessible on the physical network.

Third, create a static route for the IP assigned to the port. Click the Tier-0 router, and then click `Routing` > `Static Routes` > `Add`. Use `0.0.0.0/0` in the network field, and click Insert Row to add the gateway for the next hop.

For information about setting the public IP address and the gateway, see the section above on IP Addressing and Routing Requirements for Photon Controller.

10 Deploy Photon Controller

You need to supply the NSX metadata to the Photon Controller deployment YAML file when the virtual network is enabled. For instructions on how to deploy Photon Controller, see the Photon Controller Quick Start Guide.

Here's an example of the YAML code block for NSX. The value for the `ipaddress` key in the `nsxconfig` section is the IP address of your NSX Network Manager.

```
nsxconfig:
  ipaddress: "203.0.113.220"
  credential:
    username: "admin"
    password: "secret$1"
  privateIpRootCidr: "192.168.2.0/24"
  floatingIpRootRange: "203.0.113.160-203.0.113.170"
  t0RouterId: "d3b1a8gr-6c58-2062-2562-2drc8977e414"
  edgeClusterId: "55338b48-4r72-38b0-8d4r-65b29084c99a"
  overlayTransportZoneId: "dg821bea-c5r3-34b2-a32g-b02d44726d24"
  tunnelIpPoolId: "b4h8c34d-7714-507c-78g2-ef93b6b2db2a"
  hostUplinkPnic: "vmnic4"
  hostUplinkVlanId: "0"
  dnsServerAddresses: "198.51.100.12"
```

10.1 Additional Items to Check Before Installing Photon Platform with NSX

- If ESXi hosts don't use a shared datastore for Photon Controller's image repository, make sure their datastore names are unique.
- Make sure that the hostname of each ESXi host is set and is unique. Check `/etc/hosts` to verify this requirement. If you need to set a hostname, see the documentation for ESXi.
- Make sure each ESXi host has NTP enabled, configured correctly, and working properly. To check, connect to the ESXi host by using SSH and then run the following command: `ntpq -p`
- Make sure that no NSX VIBs on any of the ESXi hosts that you are using for Photon Platform.

10.2 Example YAML File

Here's a complete example YAML file that installs Photon Platform on an NSX network:

```
compute:
  hypervisors:
    esxi-1:
      hostname: "pc-1"
      ipaddress: "198.51.100.1"
      dns: "198.51.100.12"
      credential:
        username: "root"
        password: "Secret1!"
    esxi-2:
      hostname: "pc-2"
      ipaddress: "198.51.100.12"
      dns: "198.51.100.12"
      credential:
        username: "root"
        password: "Secret1!"
    esxi-3:
      hostname: "pc-3"
      ipaddress: "198.51.100.3"
      dns: "198.51.100.12"
      credential:
        username: "root"
        password: "Secret1!"
    esxi-4:
      hostname: "pc-4"
      ipaddress: "198.51.100.4"
      dns: "198.51.100.12"
      credential:
        username: "root"
        password: "Secret1!"
    esxi-5:
      hostname: "pc-5"
      ipaddress: "198.51.100.8"
      dns: "198.51.100.12"
      credential:
        username: "root"
        password: "Secret1!"
lightwave:
  domain: "example.com"
  credential:
```

```
    username: "administrator"
    password: "Secret123$"
  controllers:
    lightwave-1:
      site: "new york"
      appliance:
        hostref: "esxi-1"
        datastore: "datastore1"
        memoryMb: 2048
        cpus: 2
        credential:
          username: "root"
          password: "Secret1!"
        network-config:
          type: "static"
          hostname: "lightwave-1.example.com"
          ipaddress: "198.51.100.12"
          network: "NAT=VM Network"
          dns: "198.51.100.12,198.51.100.13"
          ntp: "203.0.113.1"
          netmask: "255.255.252.0"
          gateway: "198.51.100.253"
    lightwave-2:
      site: "cambridge"
      partner: "198.51.100.13"
      appliance:
        hostref: "esxi-1"
        datastore: "datastore1"
        memoryMb: 2048
        cpus: 2
        credential:
          username: "root"
          password: "Secret1!"
        network-config:
          type: "static"
          hostname: "lightwave-2.example.com"
          ipaddress: "198.51.100.13"
          network: "NAT=VM Network"
          dns: "198.51.100.12,198.51.100.13"
          ntp: "203.0.113.1"
          netmask: "255.255.252.0"
          gateway: "198.51.100.253"
photon:
  imagestore:
    img-store-1:
      datastore: "datastore1, datastore2"
      enableimagestoreforvms: "true"
  cloud:
    hostref-1: "esxi-5"
    hostref-2: "esxi-3"
  administrator-group: "example.com\\Administrators"
  syslog:
    ipaddress: "198.51.100.23"
  controllers:
```

```
    pc-1:
      appliance:
        hostref: "esxi-1"
        datastore: "datastore1"
        memoryMb: 2048
        cpus: 2
        credential:
          username: "root"
          password: "Secret1!"
        network-config:
          type: "static"
          hostname: "pc-1.example.com"
          ipaddress: "198.51.100.14"
          network: "NAT=VM Network"
          netmask: "255.255.252.0"
          dns: "198.51.100.12,198.51.100.13"
          ntp: "203.0.113.1"
          gateway: "198.51.100.253"
    pc-2:
      appliance:
        hostref: "esxi-1"
        datastore: "datastore1"
        memoryMb: 2048
        cpus: 2
        credential:
          username: "root"
          password: "Secret1!"
        network-config:
          type: "static"
          hostname: "pc-2.example.com"
          ipaddress: "198.51.100.15"
          network: "NAT=VM Network"
          netmask: "255.255.252.0"
          dns: "198.51.100.12,198.51.100.13"
          ntp: "203.0.113.1"
          gateway: "198.51.100.253"
vsan:
  vsan-1:
    appliance:
      hostref: "esxi-1"
      datastore: "datastore1"
      memoryMb: 2048
      cpus: 2
      credential:
        username: "root"
        password: "Secret1!"
      network-config:
        type: "static"
        hostname: "vsan-1.example.com"
        ipaddress: "198.51.100.20"
        network: "NAT=VM Network"
        netmask: "255.255.252.0"
        dns: "198.51.100.12,198.51.100.13"
        ntp: "203.0.113.1"
```

```
        gateway: "198.51.100.253"
loadBalancer:
  load-balancer-1:
    appliance:
      hostref: "esxi-1"
      datastore: "datastore1"
      memoryMb: 2048
      cpus: 2
      credential:
        username: "root"
        password: "Secret1!"
      network-config:
        type: "static"
        hostname: "lb-1.example.com"
        ipaddress: "198.51.100.21"
        network: "NAT=VM Network"
        netmask: "255.255.252.0"
        dns: "198.51.100.12,198.51.100.13"
        ntp: "203.0.113.1"
        gateway: "198.51.100.253"
nsxconfig:
  ipaddress: "203.0.0.1"
  credential:
    username: "root"
    password: "Secret1!"
  privateIpRootCidr: "192.168.2.0/24"
  floatingIpRootRange: "203.0.113.160-203.0.113.170"
  t0RouterId: "123"
  edgeCLusterId: "456"
  overlayTransportZoneId: "123"
  tunnelIpPoolId: "123"
  hostUplinkPnic: "vmnic4"
  hostUplinkVlanId: "0"
  dnsServerAddresses: "198.51.100.12"
```

After NSX is installed, see the NSX Admin Guide for instructions on how to manage the virtual network.