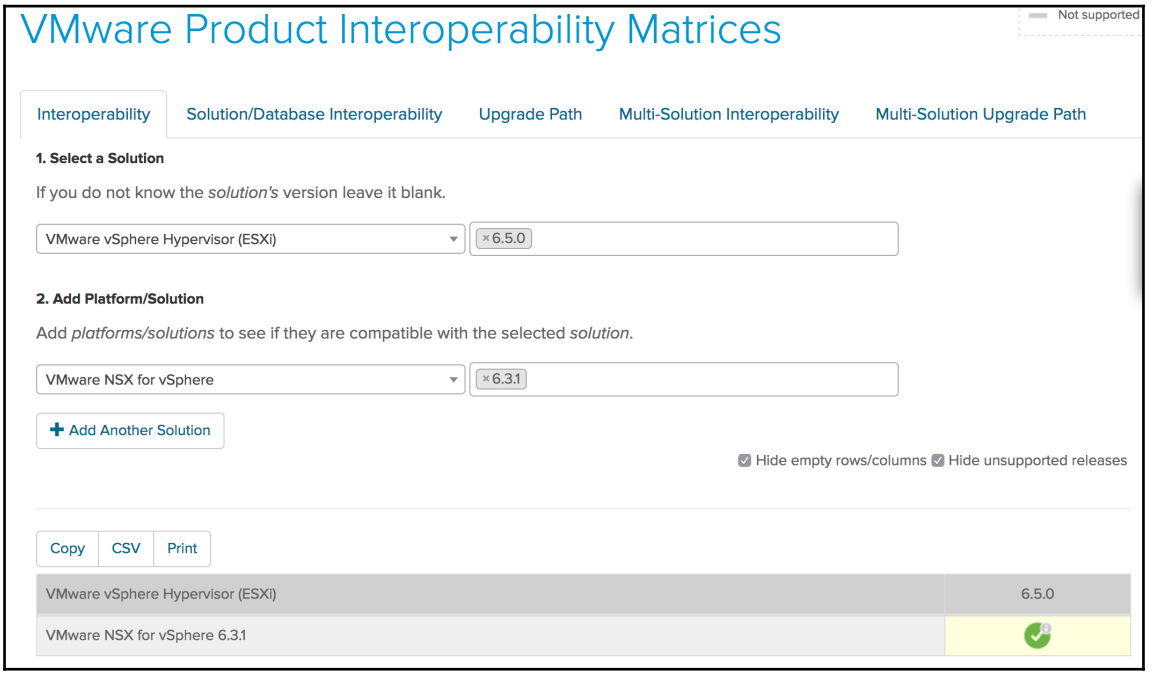
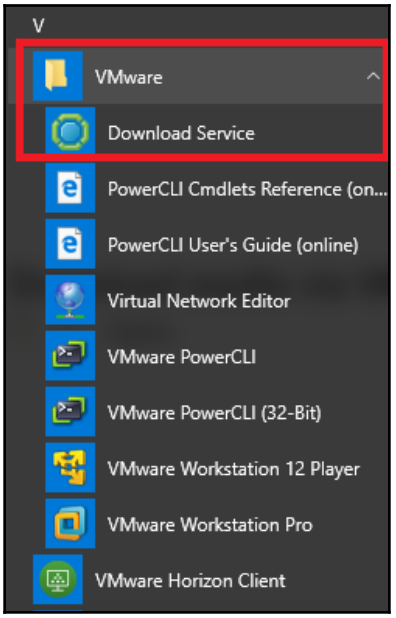
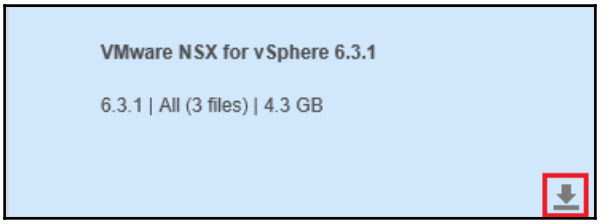
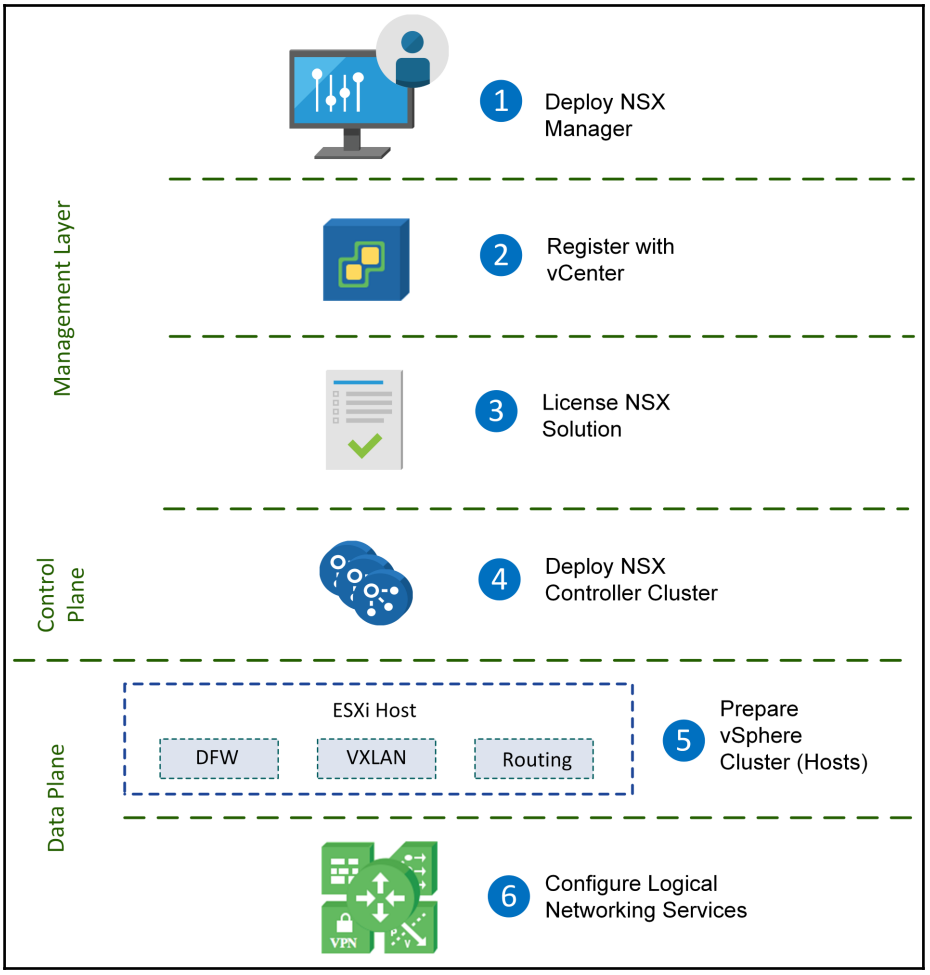
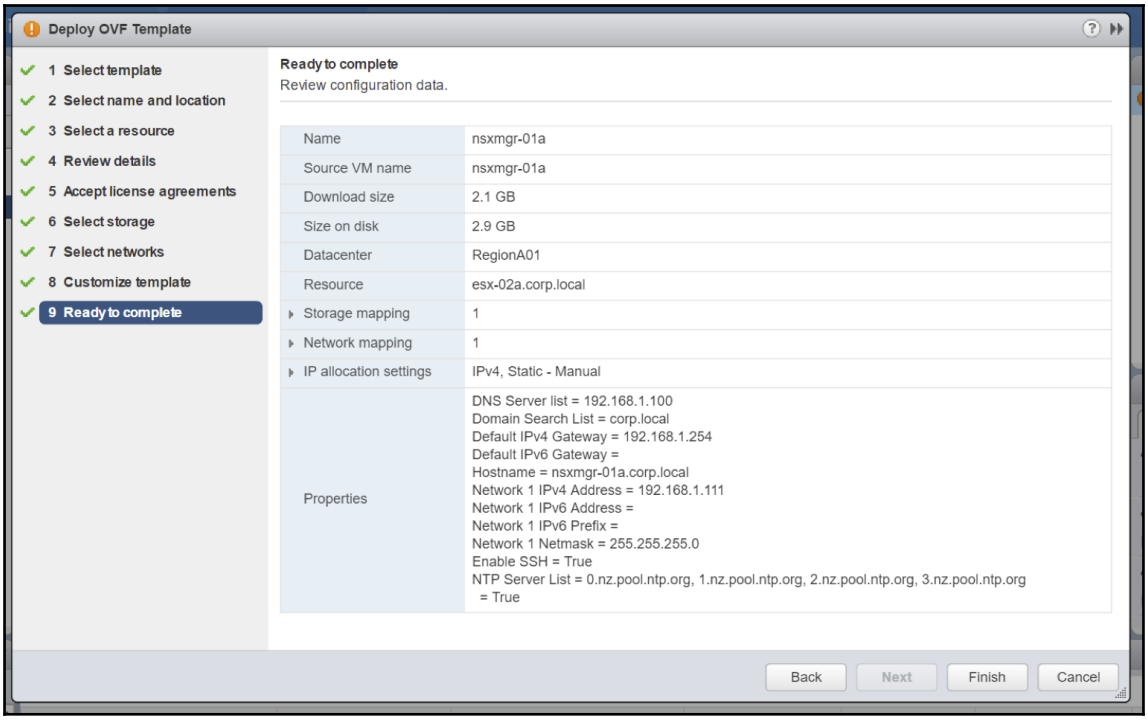
Chapter 01: Getting Started with VMware NSX for vSphere

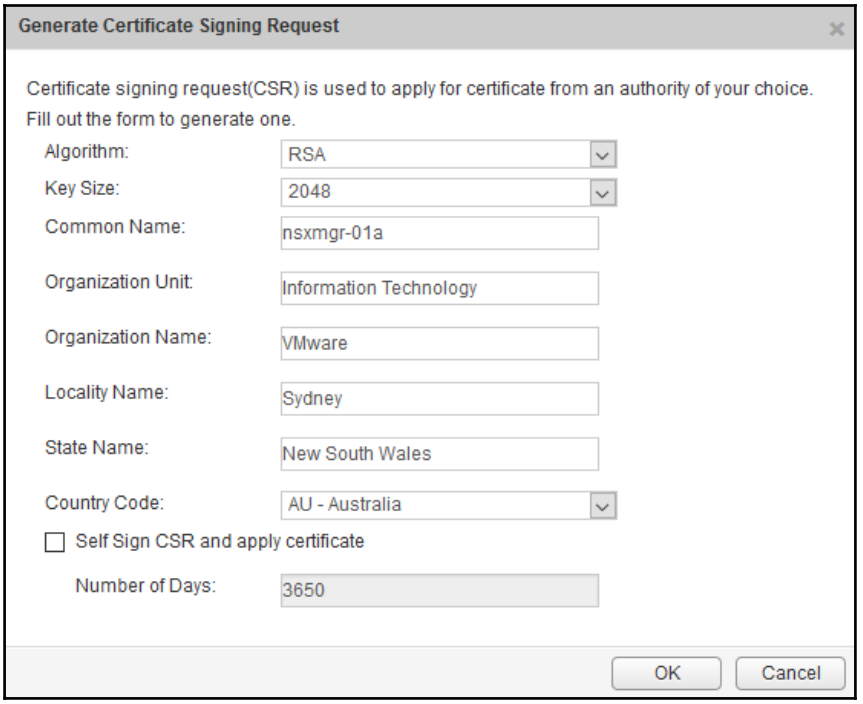


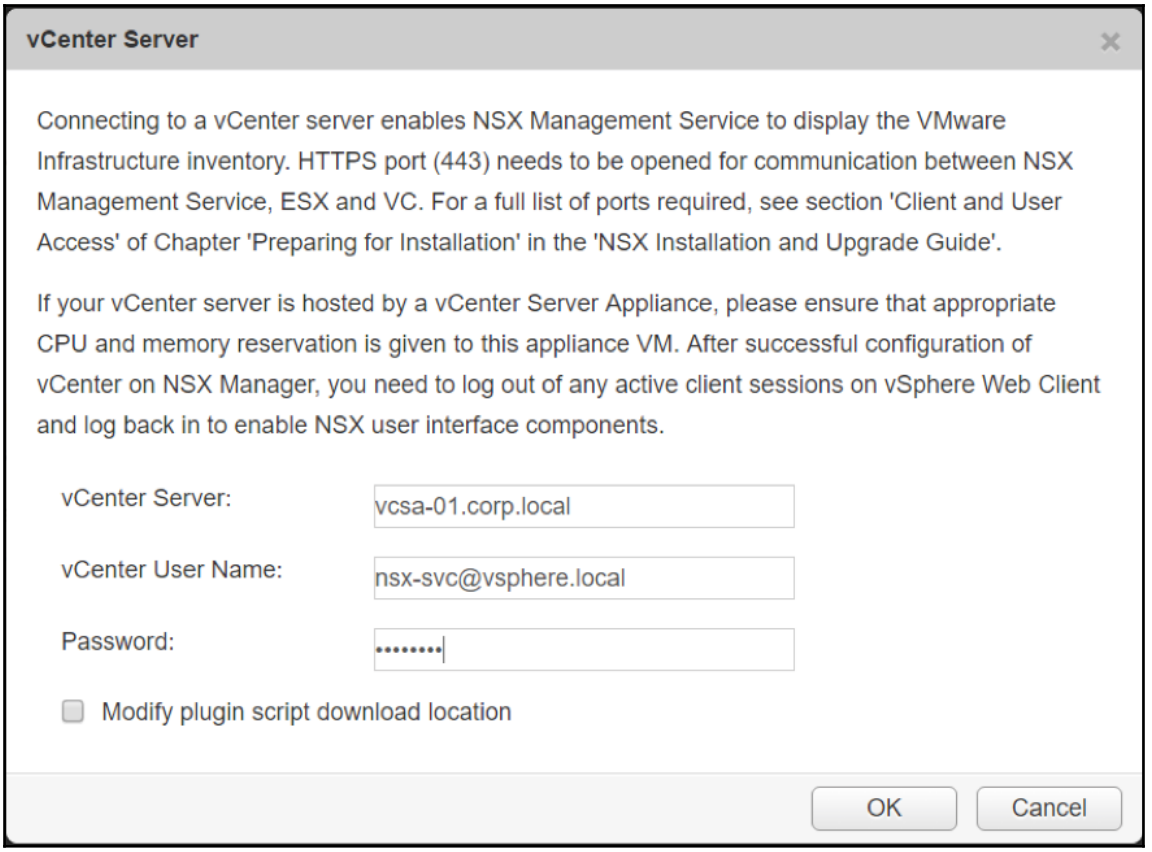

V
VMware
Download Service
PowerCLI Cmdlets Reference (on...
PowerCLI User's Guide (online)
Virtual Network Editor
VMware PowerCLI
VMware PowerCLI (32-Bit)
VMware Workstation 12 Player
VMware Workstation Pro
VMware Horizon Client

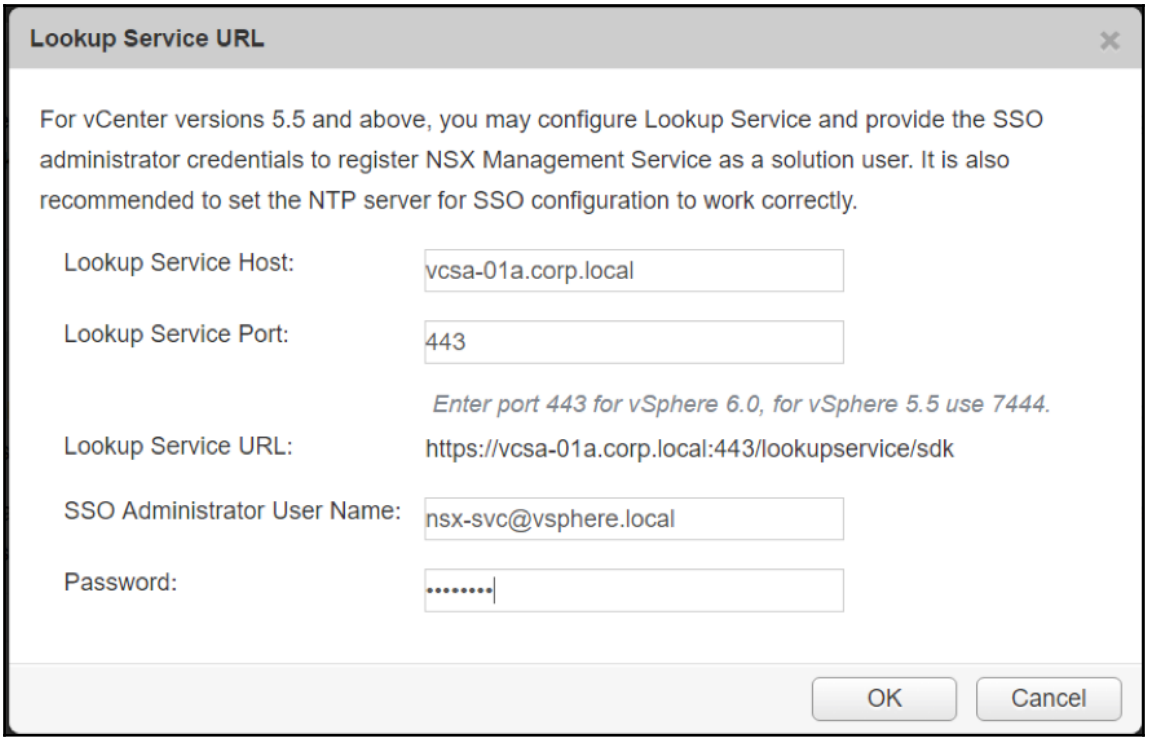

VMware NSX for vSphere 6.3.1
6.3.1 | All (3 files) | 4.3 GB

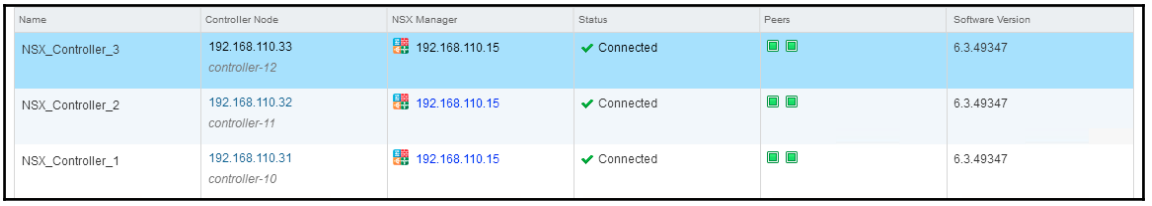

Management Layer
1
Deploy NSX Manager
2
Register with vCenter
3
License NSX Solution
Control Plane
4
Deploy NSX Controller Cluster
Data Plane
ESXi Host
DFW
VXLAN
Routing
5
Prepare vSphere Cluster (Hosts)
VPN
6
Configure Logical Networking Services

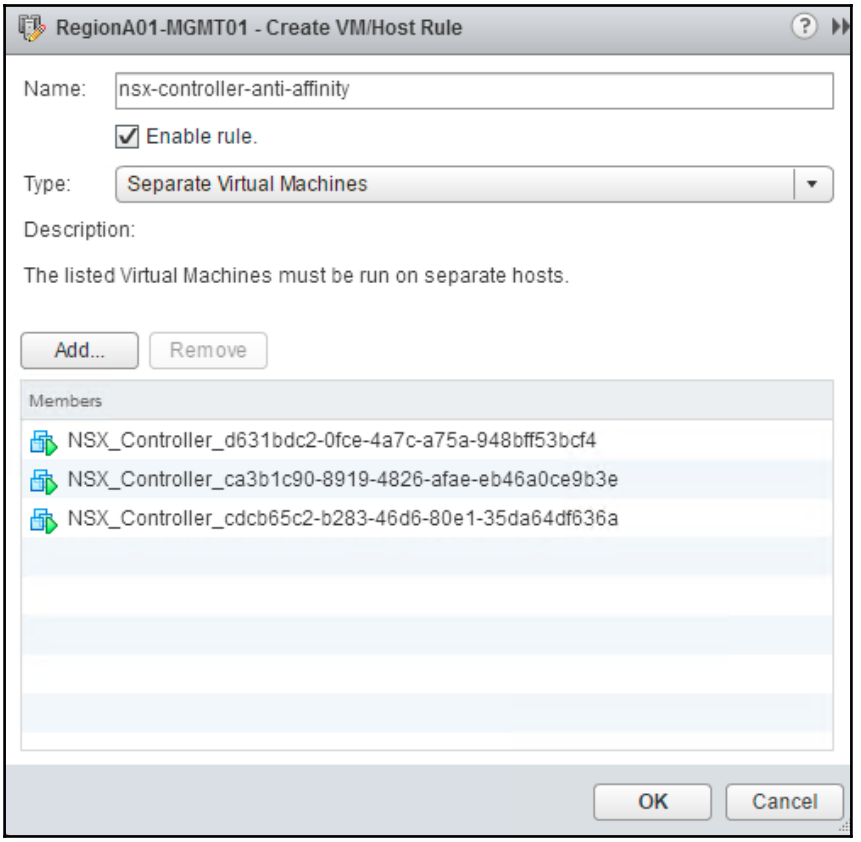

Deploy OVF Template
1 Select template
2 Select name and location
3 Select a resource
4 Review details
5 Accept license agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete
Ready to complete
Review configuration data.
Name
nsxmgr-01a
Source VM name
nsxmgr-01a
Download size
2.1 GB
Size on disk
2.9 GB
Datacenter
RegionA01
Resource
esx-02a.corp.local
Storage mapping
1
Network mapping
1
IP allocation settings
IPv4, Static - Manual
Properties
DNS Server list = 192.168.1.100
Domain Search List = corp.local
Default IPv4 Gateway = 192.168.1.254
Default IPv6 Gateway =
Hostname = nsxmgr-01a.corp.local
Network 1 IPv4 Address = 192.168.1.111
Network 1 IPv6 Address =
Network 1 IPv6 Prefix =
Network 1 Netmask = 255.255.255.0
Enable SSH = True
NTP Server List = 0.nz.pool.ntp.org, 1.nz.pool.ntp.org, 2.nz.pool.ntp.org, 3.nz.pool.ntp.org
= True
Back
Next
Finish
Cancel

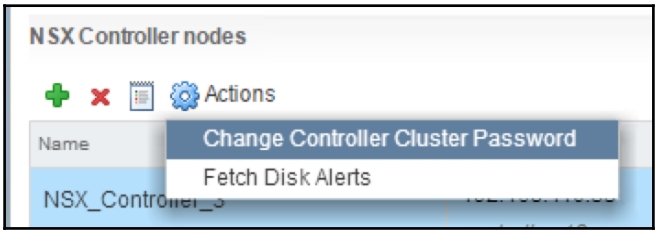

Generate Certificate Signing Request
Certificate signing request(CSR) is used to apply for certificate from an authority of your choice.
Fill out the form to generate one.
Algorithm:
RSA
Key Size:
2048
Common Name:
nsxmgr-01a
Organization Unit:
Information Technology
Organization Name:
VMware
Locality Name:
Sydney
State Name:
New South Wales
Country Code:
AU - Australia
Self Sign CSR and apply certificate
Number of Days:
3650
OK
Cancel

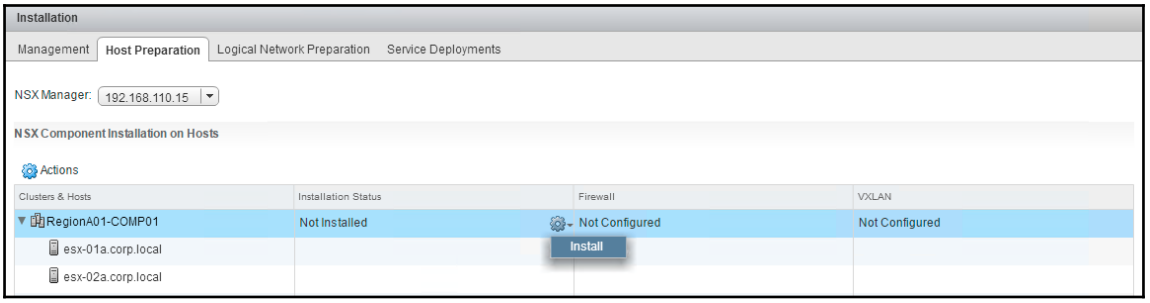

vCenter Server
Connecting to a vCenter server enables NSX Management Service to display the VMware Infrastructure inventory. HTTPS port (443) needs to be opened for communication between NSX Management Service, ESX and VC. For a full list of ports required, see section 'Client and User Access' of Chapter 'Preparing for Installation' in the 'NSX Installation and Upgrade Guide'.
If your vCenter server is hosted by a vCenter Server Appliance, please ensure that appropriate CPU and memory reservation is given to this appliance VM. After successful configuration of vCenter on NSX Manager, you need to log out of any active client sessions on vSphere Web Client and log back in to enable NSX user interface components.
vCenter Server:
vcsa-01.corp.local
vCenter User Name:
nsx-svc@vsphere.local
Password:
Modify plugin script download location
OK
Cancel

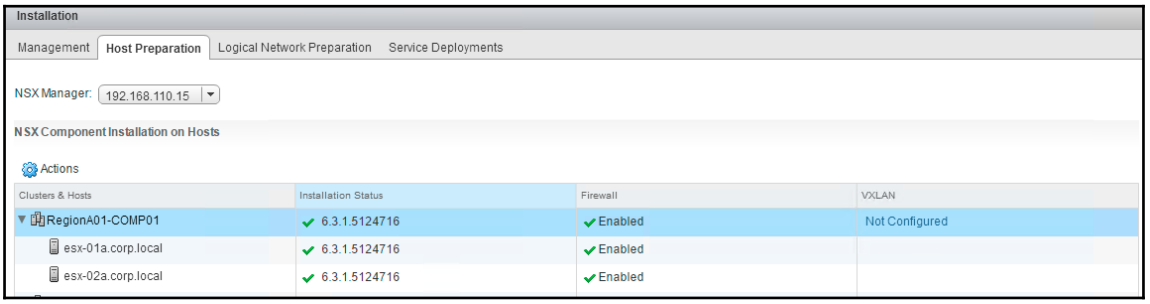

Lookup Service URL
For vCenter versions 5.5 and above, you may configure Lookup Service and provide the SSO administrator credentials to register NSX Management Service as a solution user. It is also recommended to set the NTP server for SSO configuration to work correctly.
Lookup Service Host:
vcsa-01a.corp.local
Lookup Service Port:
443
Enter port 443 for vSphere 6.0, for vSphere 5.5 use 7444.
Lookup Service URL:
https://vcsa-01a.corp.local:443/lookupservice/sdk
SSO Administrator User Name:
nsx-svc@vsphere.local
Password:
OK
Cancel

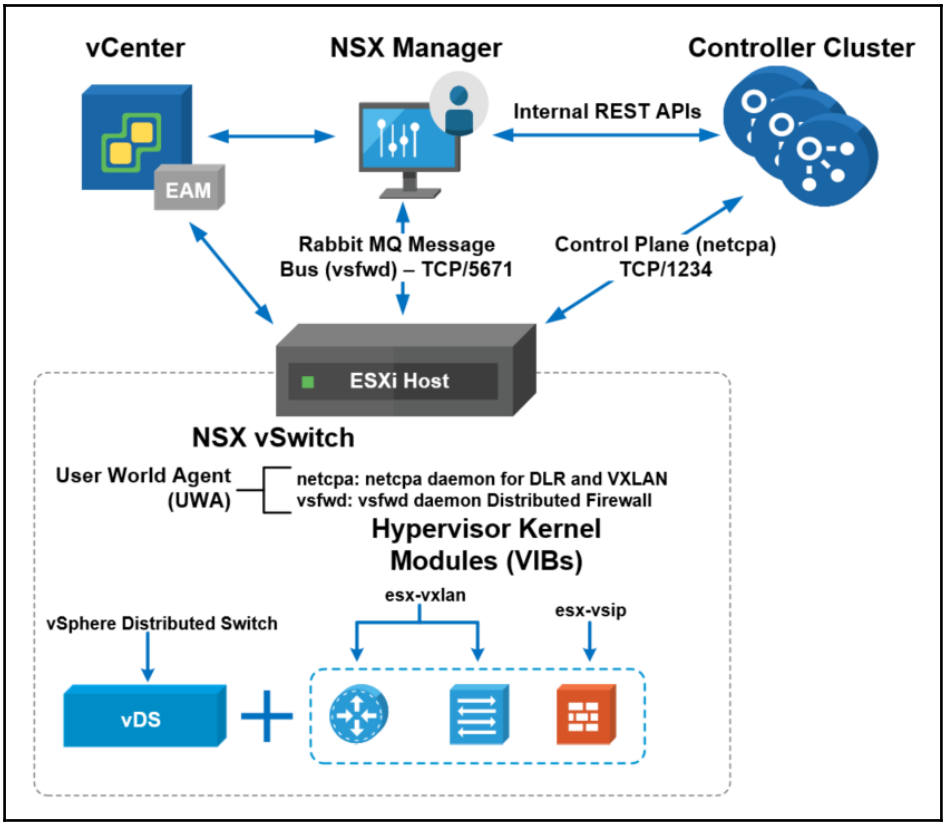

Name
Controller Node
NSX Manager
Status
Peers
Software Version
NSX_Controller_3
192.168.110.33
controller-12
192.168.110.15
Connected
6.3.49347
NSX_Controller_2
192.168.110.32
controller-11
192.168.110.15
Connected
6.3.49347
NSX_Controller_1
192.168.110.31
controller-10
192.168.110.15
Connected
6.3.49347


RegionA01-MGMT01 - Create VM/Host Rule
Name:
nsx-controller-anti-affinity
Enable rule.
Type:
Separate Virtual Machines
Description:
The listed Virtual Machines must be run on separate hosts.
Add...
Remove
Members
NSX_Controller_d631bdc2-0fce-4a7c-a75a-948bff53bcf4
NSX_Controller_ca3b1c90-8919-4826-afae-eb46a0ce9b3e
NSX_Controller_cdcb65c2-b283-46d6-80e1-35da64df636a
OK
Cancel


NSX Controller nodes
Actions
Name
Change Controller Cluster Password
Fetch Disk Alerts


Installation
Management
Host Preparation
Logical Network Preparation
Service Deployments
NSX Manager:
192.168.110.15
NSX Component Installation on Hosts
Actions
Clusters & Hosts
Installation Status
Firewall
VXLAN
RegionA01-COMP01
Not Installed
Not Configured
Not Configured
esx-01a.corp.local
esx-02a.corp.local
Install


Installation
Management
Host Preparation
Logical Network Preparation
Service Deployments
NSX Manager:
192.168.110.15
NSX Component Installation on Hosts
Actions
Clusters & Hosts
Installation Status
Firewall
VXLAN
RegionA01-COMP01
6.3.1.5124716
Enabled
Not Configured
esx-01a.corp.local
6.3.1.5124716
Enabled
esx-02a.corp.local
6.3.1.5124716
Enabled

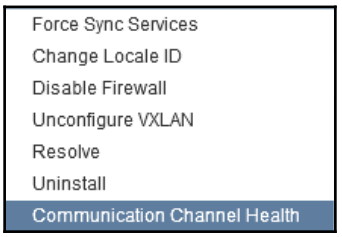


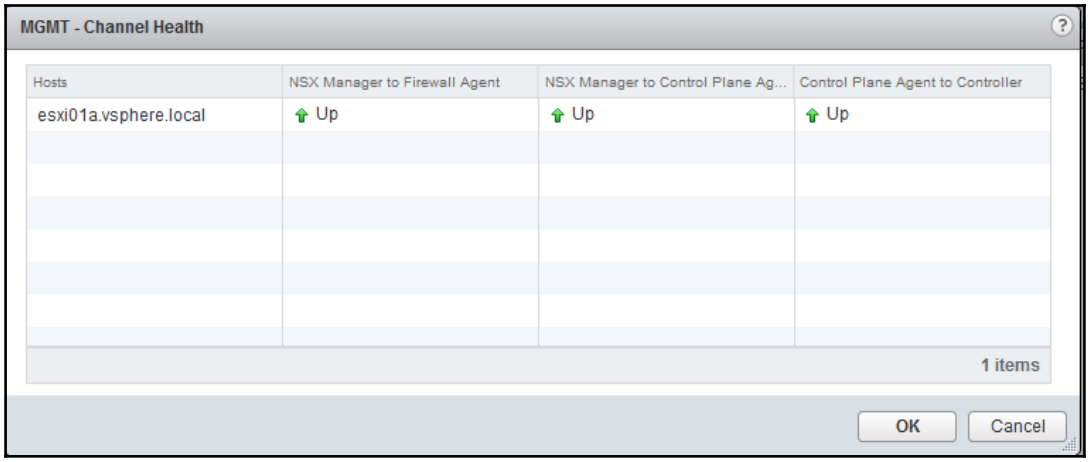

```
[root@esx-01a:~] esxcli network ip connection list | grep 1234
tcp         0       0  192.168.110.51:22642          192.168.110.31:1234   ESTABLISHED     67733  newreno  netcpa-worker
tcp         0       0  192.168.110.51:53116          192.168.110.32:1234   ESTABLISHED     67733  newreno  netcpa-worker
tcp         0       0  192.168.110.51:58976          192.168.110.33:1234   ESTABLISHED     68058  newreno  netcpa-worker
[root@esx-01a:~]
```

```
[root@esx-01a:~] cat /etc/vmware/netcpa/config-by-vsm.xml
<config>
  <connectionList>
    <connection id="0000">
      <port>1234</port>
      <server>192.168.110.31</server>
      <sslEnabled>true</sslEnabled>
      <thumbprint>C8:93:3C:24:FC:41:94:DE:7B:40:DE:53:3F:E9:34:72:47:73:02:1F</thumbprint>
    </connection>
    <connection id="0001">
      <port>1234</port>
      <server>192.168.110.32</server>
      <sslEnabled>true</sslEnabled>
      <thumbprint>12:3E:09:2E:BE:7A:56:64:8D:59:C4:21:6F:60:EE:93:6F:BF:80:6D</thumbprint>
    </connection>
    <connection id="0002">
      <port>1234</port>
      <server>192.168.110.33</server>
      <sslEnabled>true</sslEnabled>
      <thumbprint>6C:2D:11:24:45:46:F8:FA:EA:9F:C3:EE:C7:9F:C7:D9:06:1B:C3:63</thumbprint>
    </connection>
  </connectionList>
```

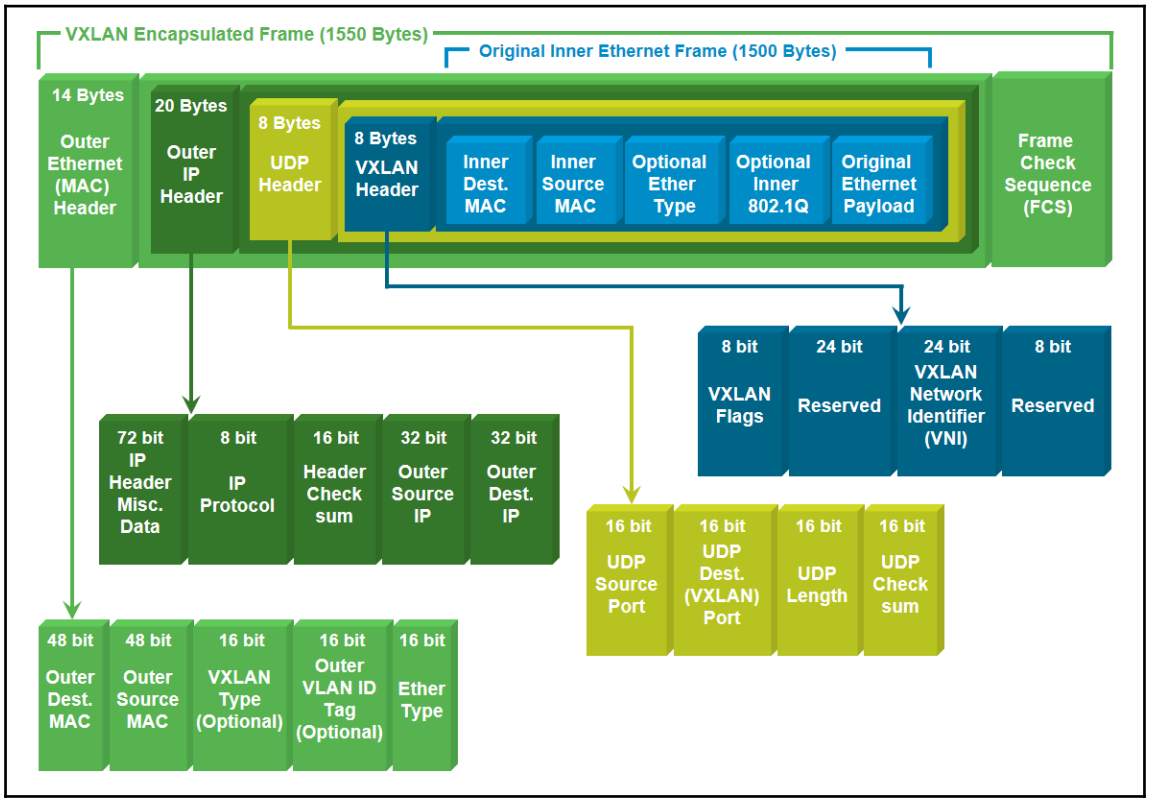
```
[root@esx-01a:~] esxcli network ip connection list | grep 5671
tcp         0       0  192.168.110.51:13893           192.168.110.42:5671   ESTABLISHED     68282  newreno  vsfwd
tcp         0       0  192.168.110.51:34904           192.168.110.42:5671   ESTABLISHED     68282  newreno  vsfwd
tcp         0       0  192.168.110.51:16196           192.168.110.42:5671   ESTABLISHED     68272  newreno  vsfwd
tcp         0       0  192.168.110.51:22734           192.168.110.42:5671   ESTABLISHED     68272  newreno  vsfwd
tcp         0       0  192.168.110.51:54175           192.168.110.42:5671   ESTABLISHED     68272  newreno  vsfwd
```

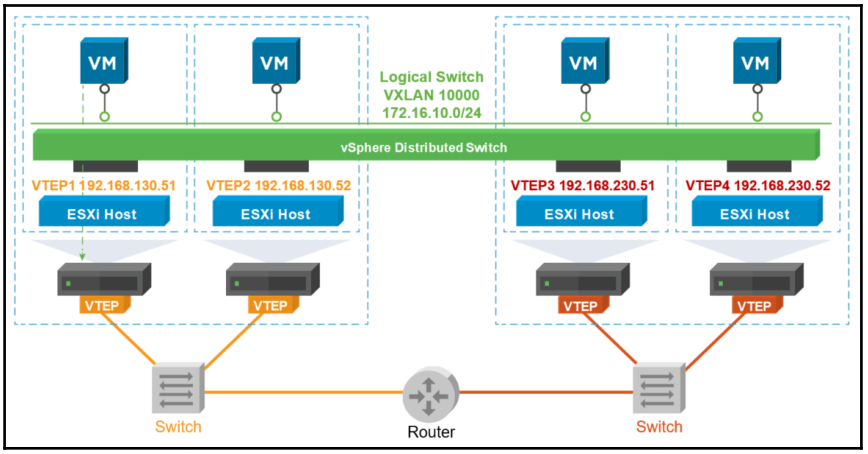
```
[root@esx-01a:~] esxcfg-advcfg -g /UserVars/RmqIpAddress
Value of RmqIpAddress is 192.168.110.42
[root@esx-01a:~]
```

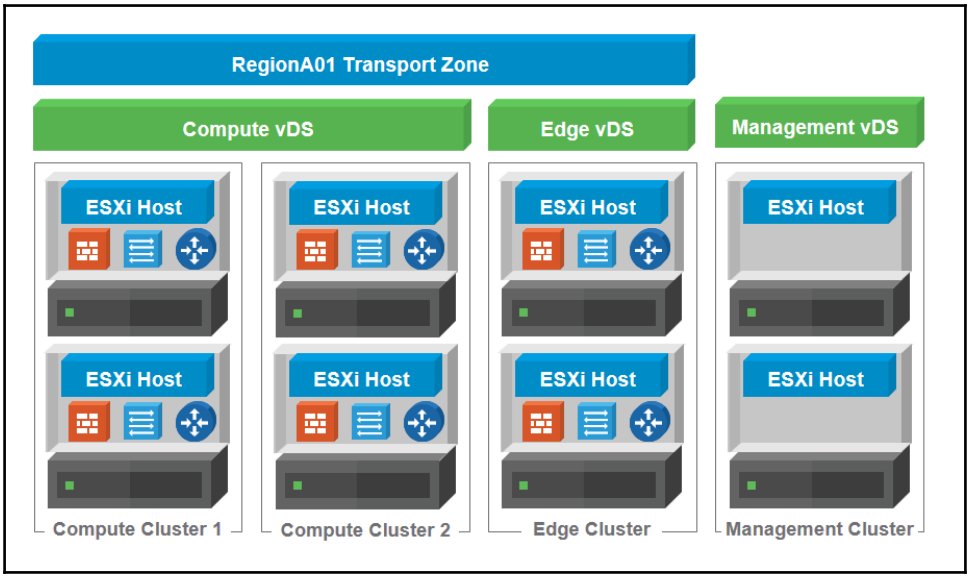


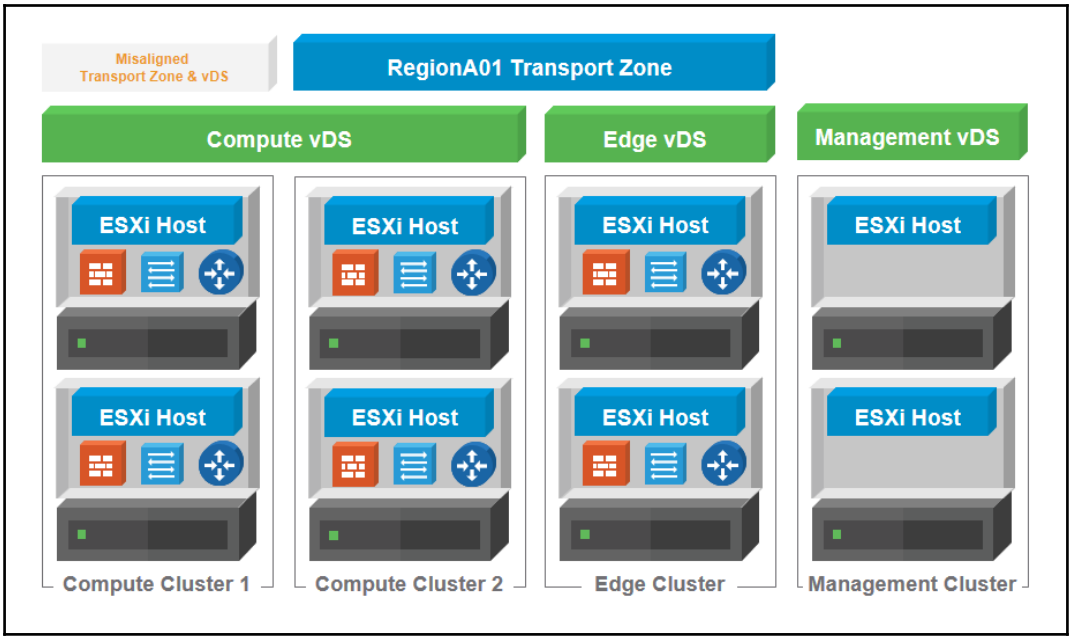

MGMT - Channel Health
Hosts
NSX Manager to Firewall Agent
NSX Manager to Control Plane Ag...
Control Plane Agent to Controller
esxi01a.vsphere.local
Up
Up
Up
1 items
OK
Cancel

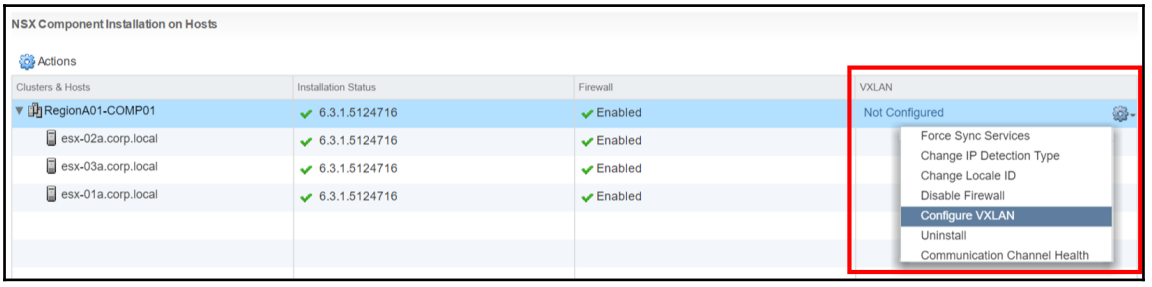
Chapter 02: Configuring VMware NSX Logical Switch Networks

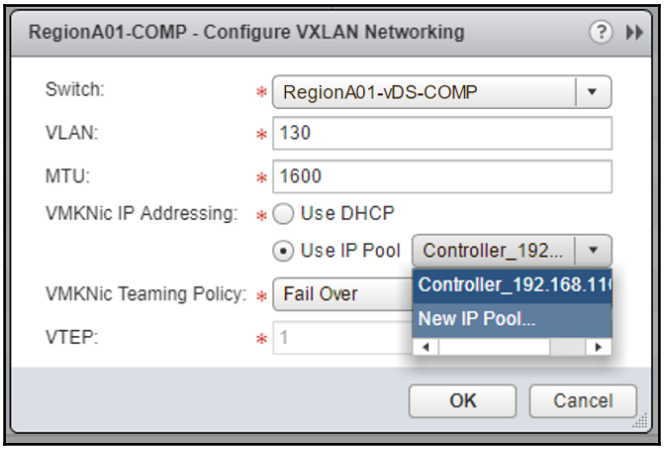


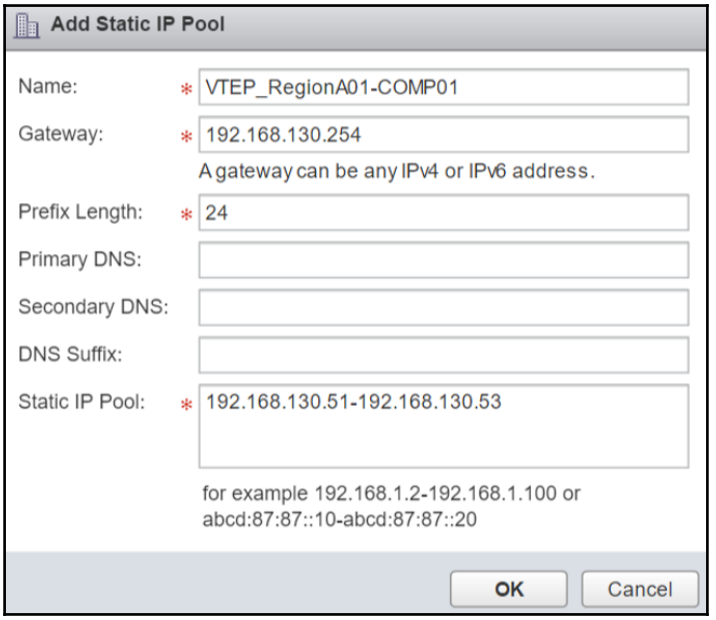

VM
VM
VM
VM
Logical Switch
VXLAN 10000
172.16.10.0/24
vSphere Distributed Switch
VTEP1 192.168.130.51
VTEP2 192.168.130.52
VTEP3 192.168.230.51
VTEP4 192.168.230.52
ESXi Host
ESXi Host
ESXi Host
ESXi Host
VTEP
VTEP
VTEP
VTEP
Switch
Router
Switch

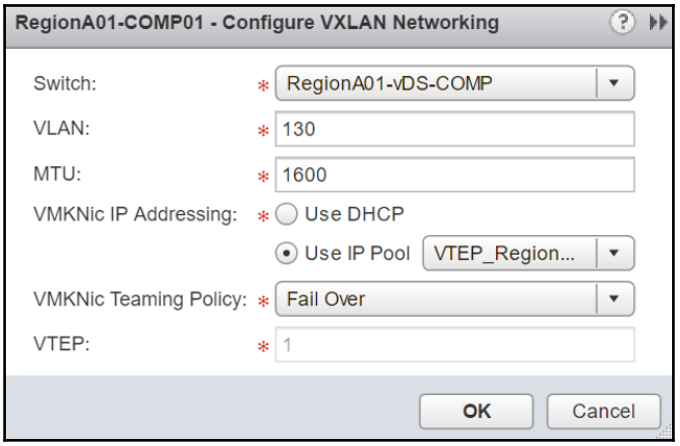

RegionA01 Transport Zone
Compute vDS
Edge vDS
Management vDS
ESXi Host
ESXi Host
ESXi Host
ESXi Host
ESXi Host
ESXi Host
ESXi Host
ESXi Host
Compute Cluster 1
Compute Cluster 2
Edge Cluster
Management Cluster

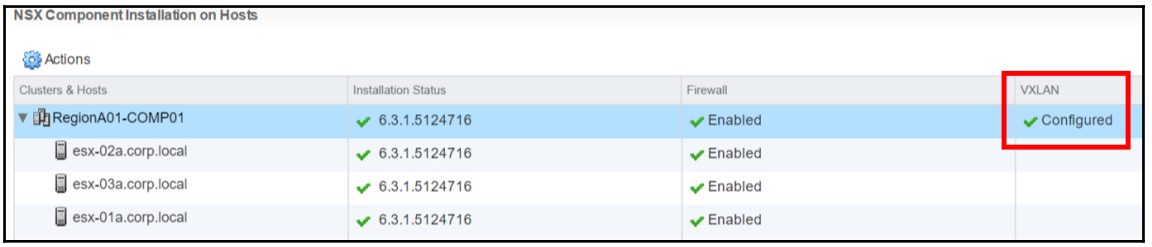

Misaligned
Transport Zone & vDS
RegionA01 Transport Zone
Compute vDS
Edge vDS
Management vDS
ESXi Host
Compute Cluster 1
Compute Cluster 2
Edge Cluster
Management Cluster

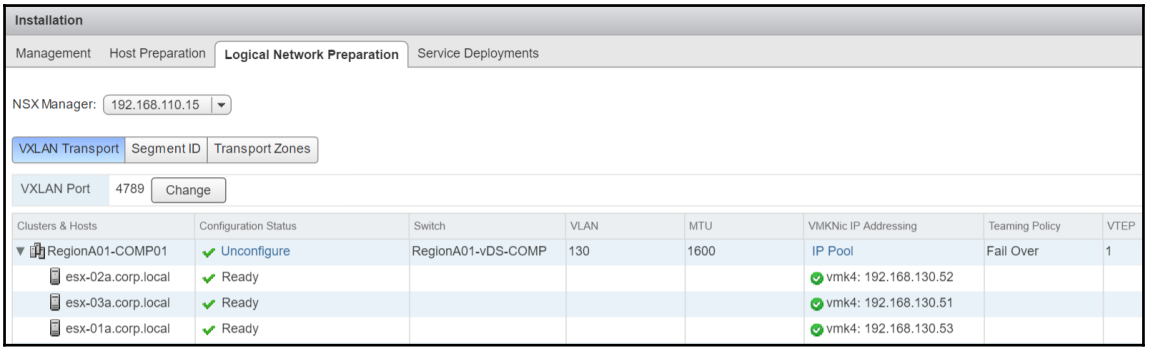

NSX Component Installation on Hosts
Actions
Clusters & Hosts
Installation Status
Firewall
VXLAN
RegionA01-COMP01
6.3.1.5124716
Enabled
Not Configured
esx-02a.corp.local
esx-03a.corp.local
esx-01a.corp.local
Force Sync Services
Change IP Detection Type
Change Locale ID
Disable Firewall
Configure VXLAN
Uninstall
Communication Channel Health

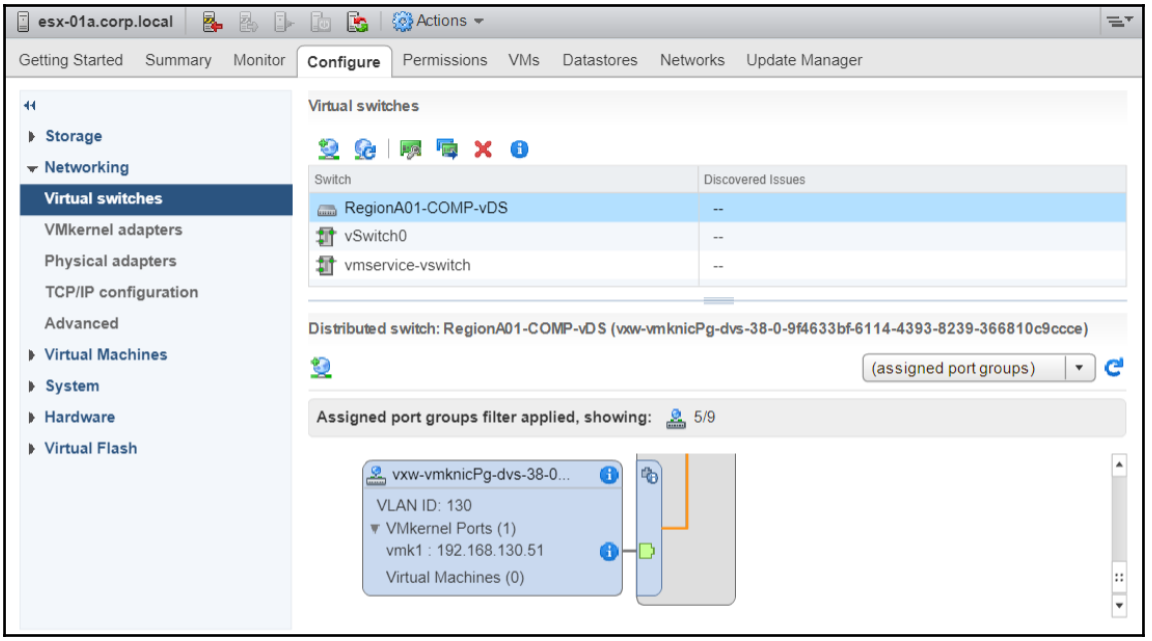

RegionA01-COMP - Configure VXLAN Networking
Switch:
RegionA01-vDS-COMP
VLAN:
130
MTU:
1600
VMKNic IP Addressing:
Use DHCP
Use IP Pool
Controller_192...
VMKNic Teaming Policy:
Fail Over
VTEP:
1
Controller_192.168.11
New IP Pool...
OK
Cancel

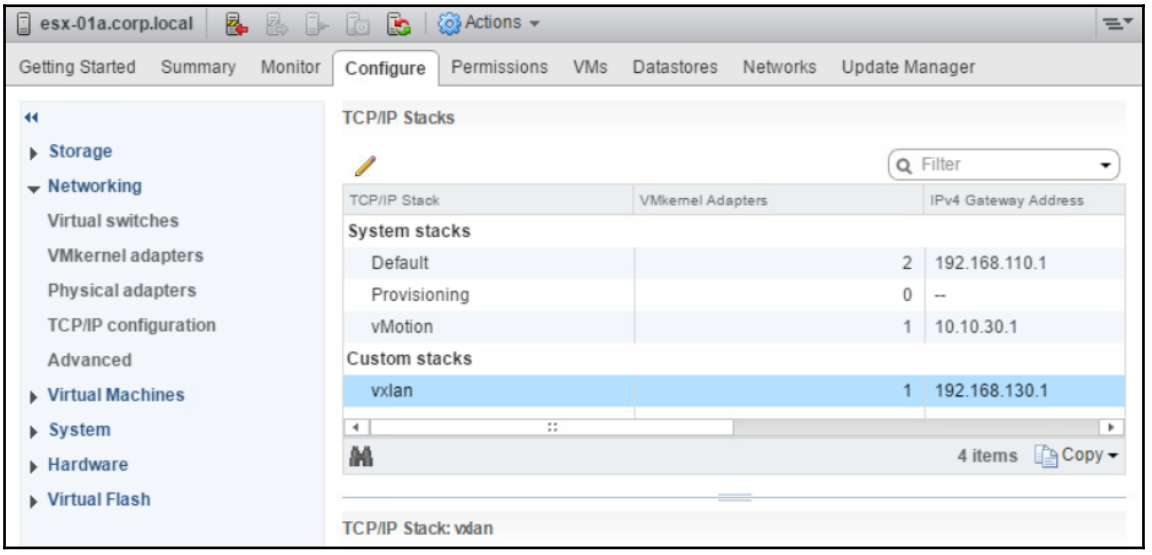

Add Static IP Pool
Name:
VTEP_RegionA01-COMP01
Gateway:
192.168.130.254
A gateway can be any IPv4 or IPv6 address.
Prefix Length:
24
Primary DNS:
Secondary DNS:
DNS Suffix:
Static IP Pool:
192.168.130.51-192.168.130.53
for example 192.168.1.2-192.168.1.100 or
abcd:87:87::10-abcd:87:87::20
OK
Cancel


RegionA01-COMP01 - Configure VXLAN Networking
Switch:
RegionA01-vDS-COMP
VLAN:
130
MTU:
1600
VMKNic IP Addressing:
Use DHCP
Use IP Pool
VTEP_Region...
VMKNic Teaming Policy:
Fail Over
VTEP:
1
OK
Cancel

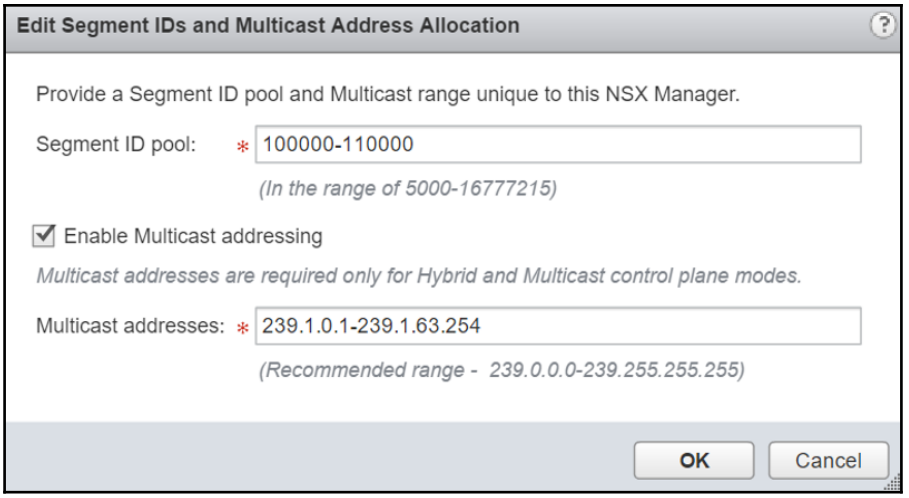

NSX Component Installation on Hosts
Actions
Clusters & Hosts
Installation Status
Firewall
VXLAN
RegionA01-COMP01
6.3.1.5124716
Enabled
Configured
esx-02a.corp.local
6.3.1.5124716
Enabled
esx-03a.corp.local
6.3.1.5124716
Enabled
esx-01a.corp.local
6.3.1.5124716
Enabled

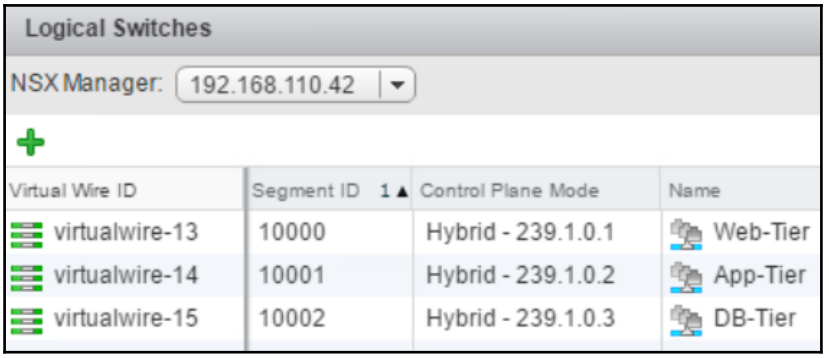

Installation
Management
Host Preparation
Logical Network Preparation
Service Deployments
NSX Manager:
192.168.110.15
VXLAN Transport
Segment ID
Transport Zones
VXLAN Port
4789
Change
Clusters & Hosts
Configuration Status
Switch
VLAN
MTU
VMKNic IP Addressing
Teaming Policy
VTEP
RegionA01-COMP01
Unconfigure
RegionA01-vDS-COMP
130
1600
IP Pool
Fail Over
1
esx-02a.corp.local
Ready
vmk4: 192.168.130.52
esx-03a.corp.local
Ready
vmk4: 192.168.130.51
esx-01a.corp.local
Ready
vmk4: 192.168.130.53


esx-01a.corp.local
Actions
Getting Started
Summary
Monitor
Configure
Permissions
VMs
Datastores
Networks
Update Manager
Storage
Networking
Virtual switches
VMkernel adapters
Physical adapters
TCP/IP configuration
Advanced
Virtual Machines
System
Hardware
Virtual Flash
Virtual switches
Switch
Discovered Issues
RegionA01-COMP-vDS
vSwitch0
vmservice-vswitch
Distributed switch: RegionA01-COMP-vDS (vxw-vmknicPg-dvs-38-0-9f4633bf-6114-4393-8239-366810c9ccce)
(assigned port groups)
Assigned port groups filter applied, showing: 5/9
vxw-vmknicPg-dvs-38-0...
VLAN ID: 130
VMkernel Ports (1)
vmk1 : 192.168.130.51
Virtual Machines (0)


esx-01a.corp.local
Actions
Getting Started
Summary
Monitor
Configure
Permissions
VMs
Datastores
Networks
Update Manager
Storage
Networking
Virtual switches
VMkernel adapters
Physical adapters
TCP/IP configuration
Advanced
Virtual Machines
System
Hardware
Virtual Flash
TCP/IP Stacks
Filter
TCP/IP Stack
VMkernel Adapters
IPv4 Gateway Address
System stacks
Default 2 192.168.110.1
Provisioning 0 --
vMotion 1 10.10.30.1
Custom stacks
vxlan 1 192.168.130.1
4 items
Copy
TCP/IP Stack: vxlan


Installation
Management
Host Preparation
Logical Network Preparation
Service Deployments
NSX Manager:
192.168.110.15
VXLAN Transport
Segment ID
Transport Zones
Segment IDs & Multicast Addresses allocation (system wide settings)
Edit
Reset
Segment ID pool:
Multicast addresses:


Edit Segment IDs and Multicast Address Allocation
Provide a Segment ID pool and Multicast range unique to this NSX Manager.
Segment ID pool:
100000-110000
(In the range of 5000-16777215)
Enable Multicast addressing
Multicast addresses are required only for Hybrid and Multicast control plane modes.
Multicast addresses:
239.1.0.1-239.1.63.254
(Recommended range - 239.0.0.0-239.255.255.255)
OK
Cancel


Logical Switches
NSX Manager:
192.168.110.42
Virtual Wire ID
Segment ID
Control Plane Mode
Name
virtualwire-13
10000
Hybrid - 239.1.0.1
Web-Tier
virtualwire-14
10001
Hybrid - 239.1.0.2
App-Tier
virtualwire-15
10002
Hybrid - 239.1.0.3
DB-Tier

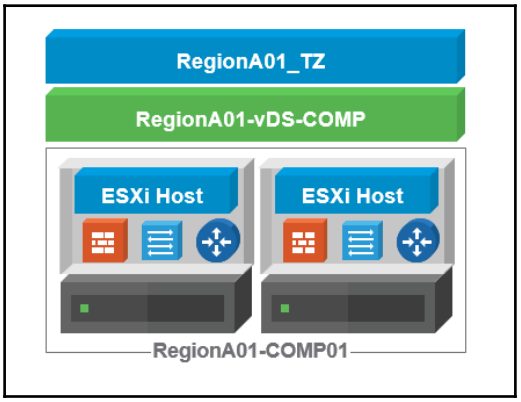
Dashboard

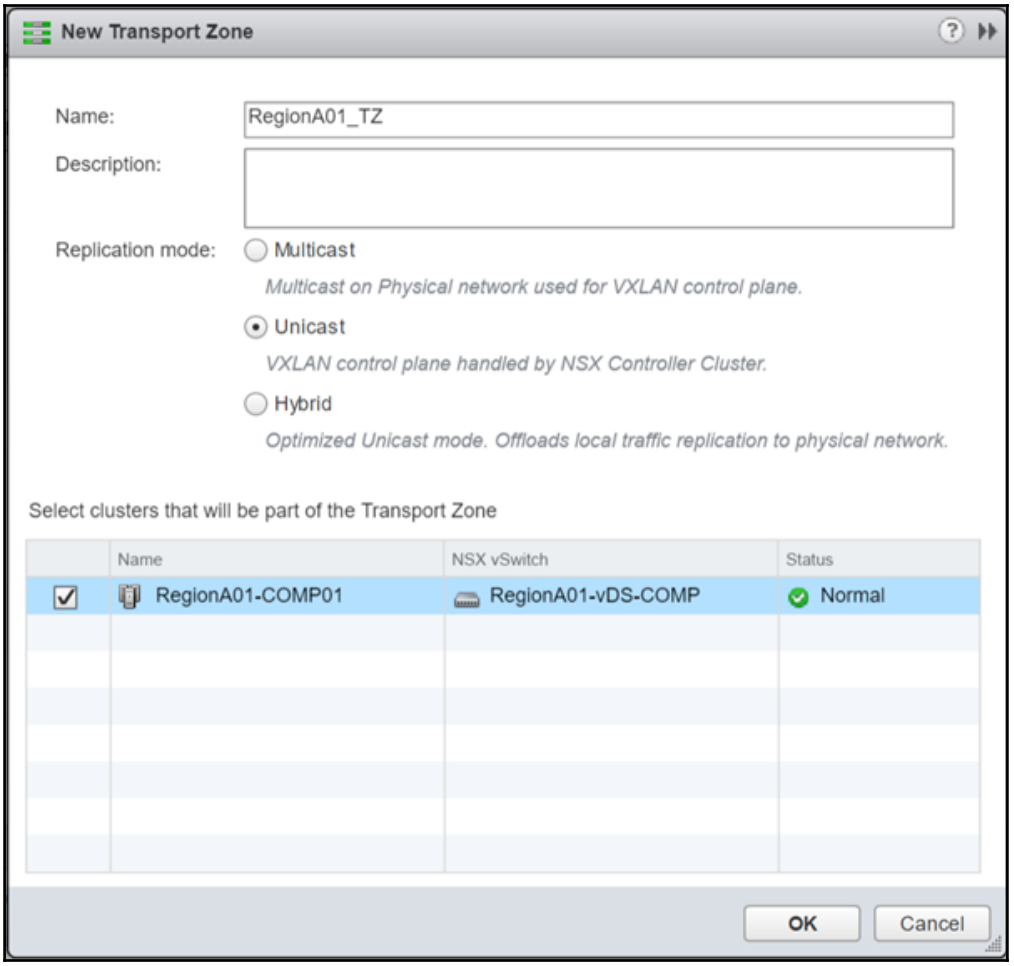
Overview | System Scale

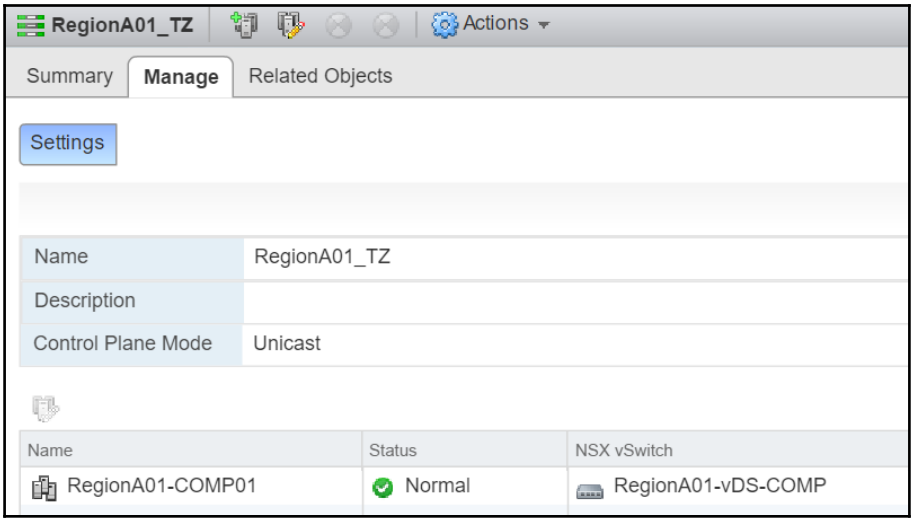
NSX Manager: 192.168.110.15 | Standalone

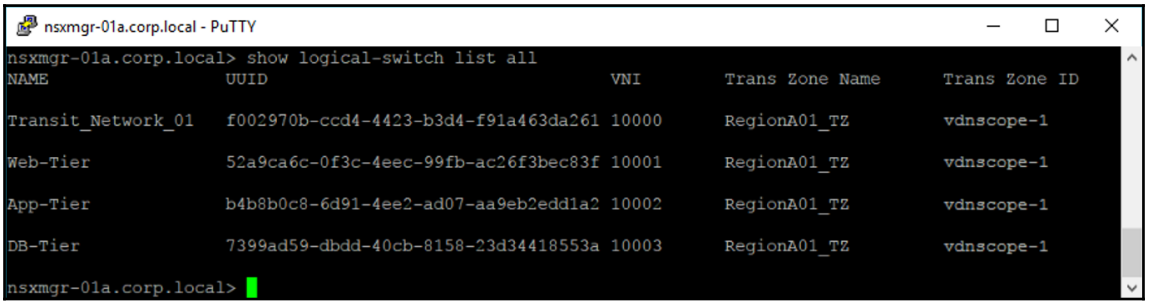
Usage Warning Threshold: 80%

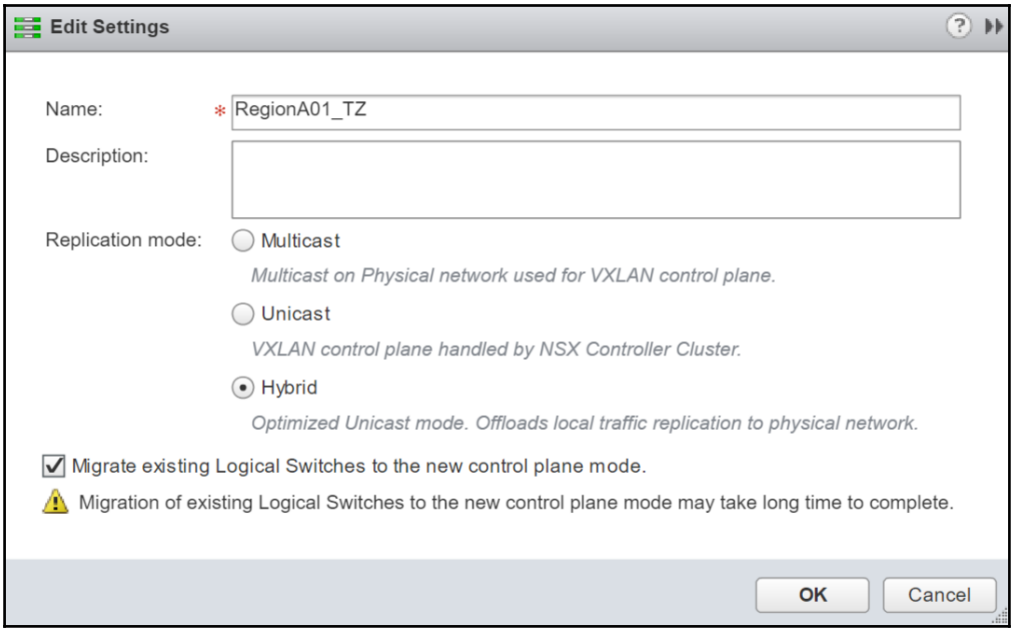
Object Type	Current Object Count	Max Object Count	Percentage Usage
Security Tags	11	9000	0.12
Firewall Sections	3	10000	0.03
Security Groups	1	10000	0.01
Logical Switches	0	10000	0
Controllers	0	3	0
IP Sets	0	10000	0
Hosts Prepared	0	512	0
Distributed Logical Routers	0	1000	0
Edge Service Gateways	0	2000	0
AD Domains	0	15	0
Firewall Rules	4	100000	0

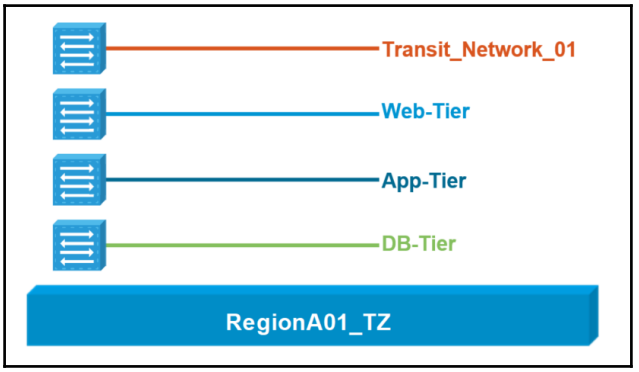


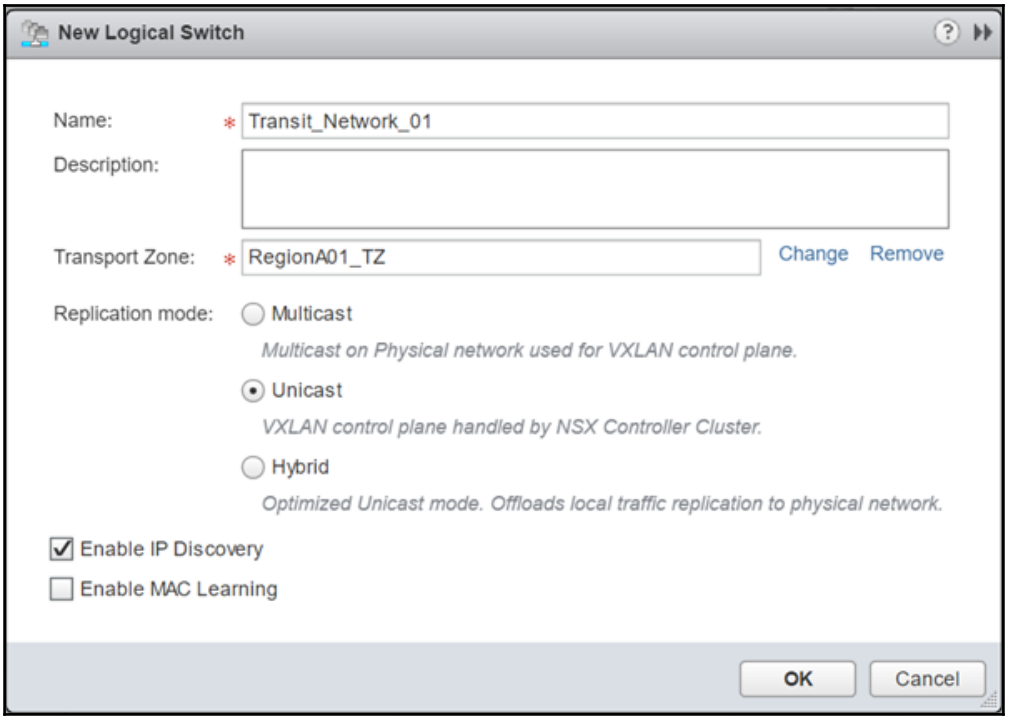

New Transport Zone
Name:
RegionA01_TZ
Description:
Replication mode:
Multicast
Multicast on Physical network used for VXLAN control plane.
Unicast
VXLAN control plane handled by NSX Controller Cluster.
Hybrid
Optimized Unicast mode. Offloads local traffic replication to physical network.
Select clusters that will be part of the Transport Zone
Name
NSX vSwitch
Status
RegionA01-COMP01
RegionA01-vDS-COMP
Normal
OK
Cancel

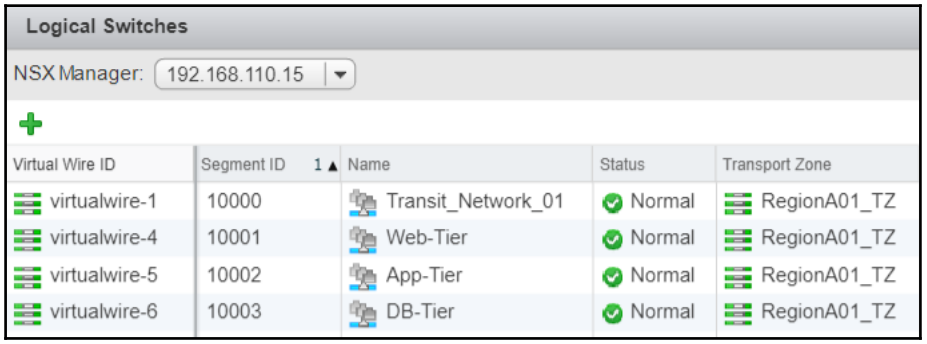

RegionA01_TZ
Actions
Summary
Manage
Related Objects
Settings
Name
RegionA01_TZ
Description
Control Plane Mode
Unicast
Name
Status
NSX vSwitch
RegionA01-COMP01
Normal
RegionA01-vDS-COMP

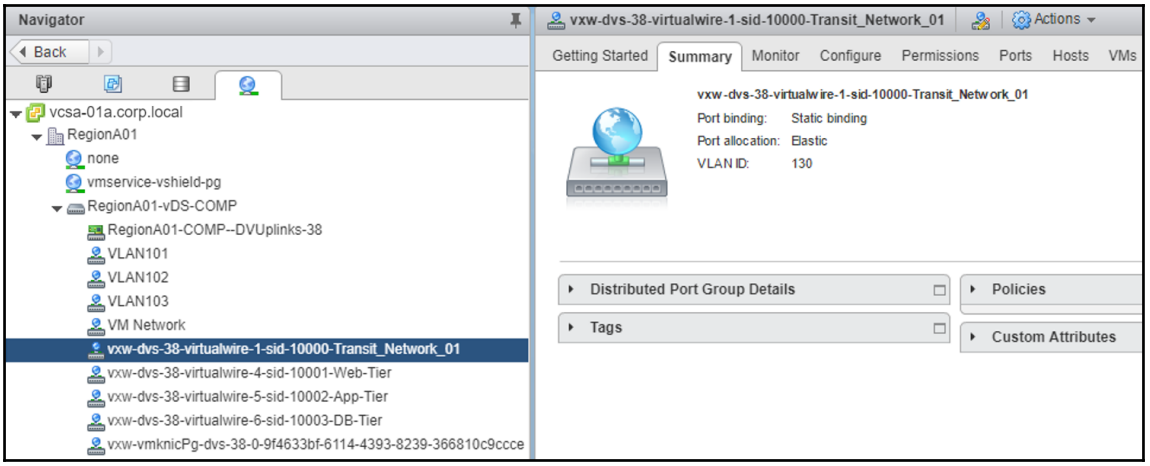

nsxmgr-01a.corp.local - PuTTY
nsxmgr-01a.corp.local> show logical-switch list all
NAME UUID VNI Trans Zone Name Trans Zone ID
Transit_Network_01 f002970b-ccd4-4423-b3d4-f91a463da261 10000 RegionA01_TZ vdnscope-1
Web-Tier 52a9ca6c-0f3c-4eec-99fb-ac26f3bec83f 10001 RegionA01_TZ vdnscope-1
App-Tier b4b8b0c8-6d91-4ee2-ad07-aa9eb2edd1a2 10002 RegionA01_TZ vdnscope-1
DB-Tier 7399ad59-dbdd-40cb-8158-23d34418553a 10003 RegionA01_TZ vdnscope-1
nsxmgr-01a.corp.local>

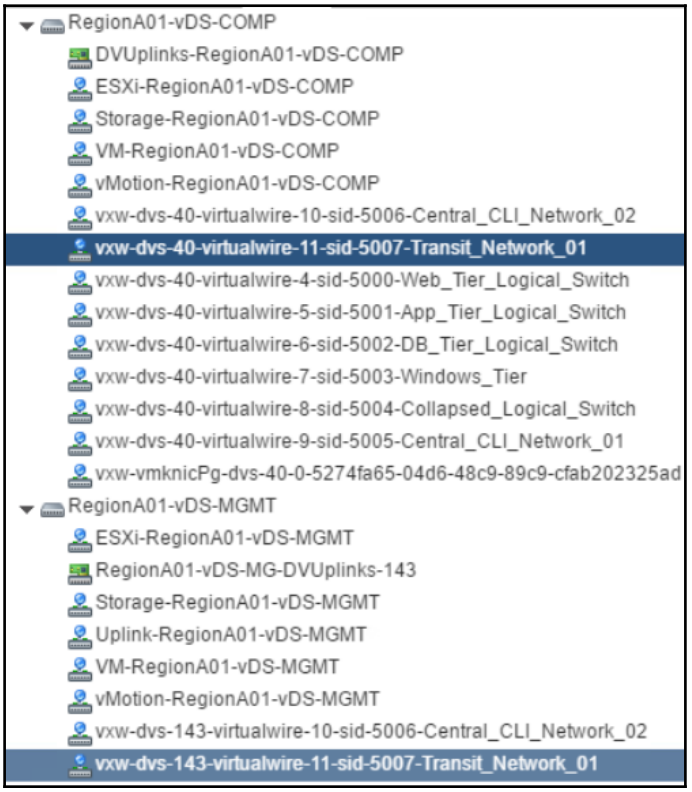

Edit Settings
Name:
RegionA01_TZ
Description:
Replication mode:
Multicast
Multicast on Physical network used for VXLAN control plane.
Unicast
VXLAN control plane handled by NSX Controller Cluster.
Hybrid
Optimized Unicast mode. Offloads local traffic replication to physical network.
Migrate existing Logical Switches to the new control plane mode.
Migration of existing Logical Switches to the new control plane mode may take long time to complete.
OK
Cancel

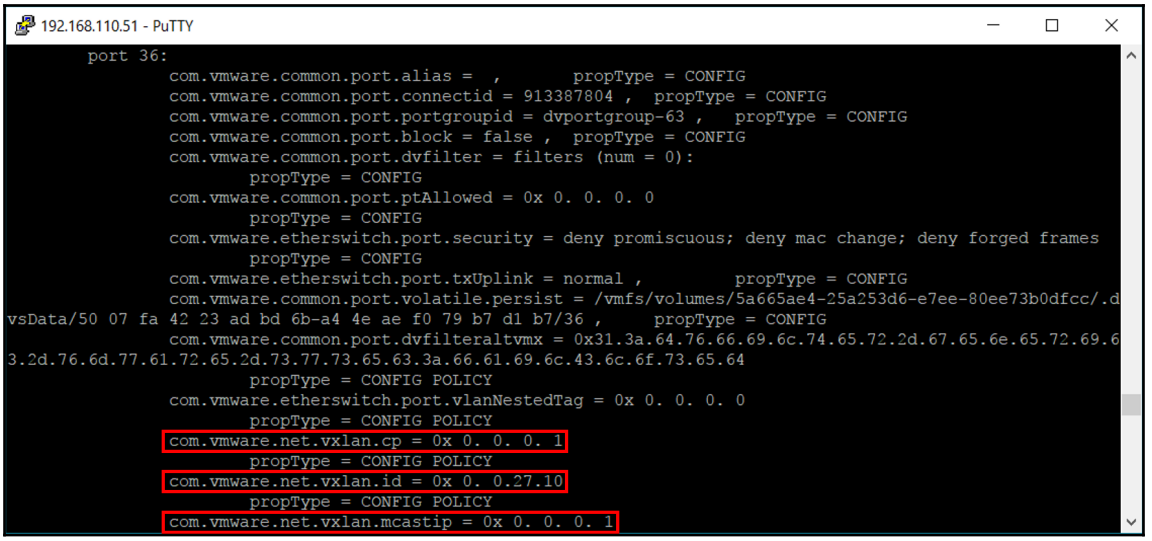

Transit_Network_01
Web-Tier
App-Tier
DB-Tier
RegionA01_TZ

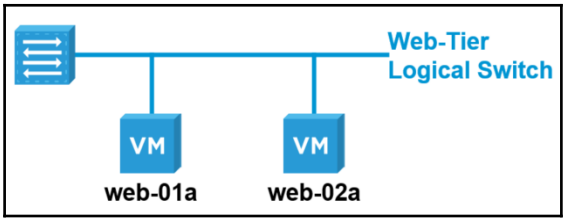

New Logical Switch
Name:
Transit_Network_01
Description:
Transport Zone:
RegionA01_TZ
Change
Remove
Replication mode:
Multicast
Multicast on Physical network used for VXLAN control plane.
Unicast
VXLAN control plane handled by NSX Controller Cluster.
Hybrid
Optimized Unicast mode. Offloads local traffic replication to physical network.
Enable IP Discovery
Enable MAC Learning
OK
Cancel

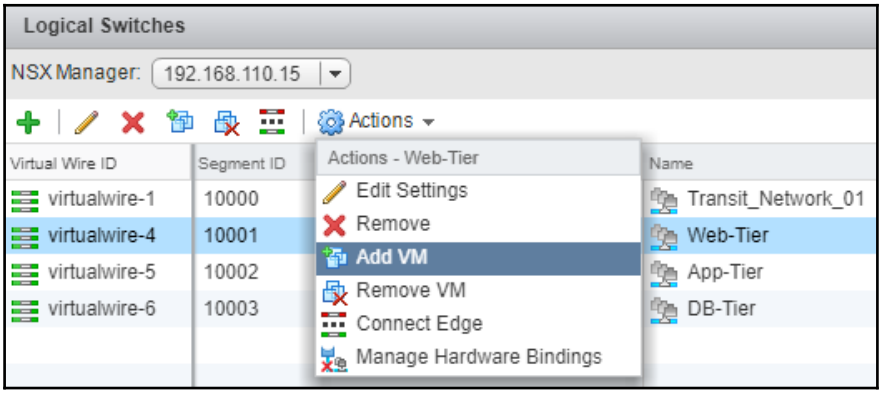

Logical Switches
NSX Manager:
192.168.110.15
Virtual Wire ID
Segment ID
Name
Status
Transport Zone
virtualwire-1
10000
Transit_Network_01
Normal
RegionA01_TZ
virtualwire-4
10001
Web-Tier
Normal
RegionA01_TZ
virtualwire-5
10002
App-Tier
Normal
RegionA01_TZ
virtualwire-6
10003
DB-Tier
Normal
RegionA01_TZ

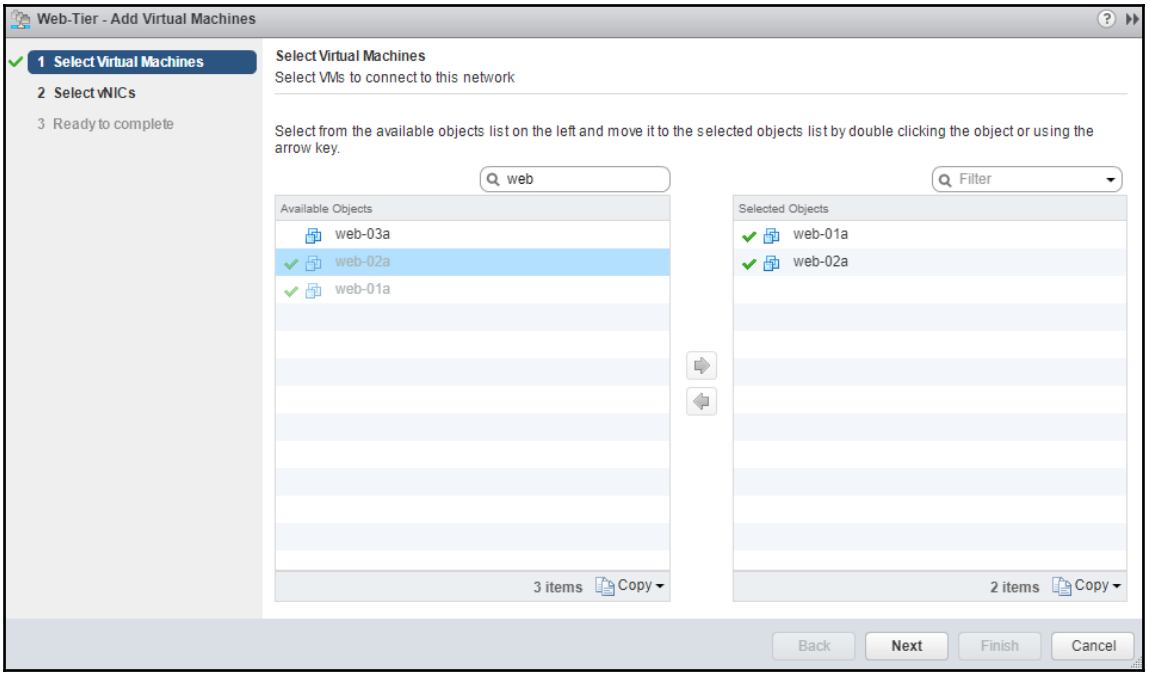

Navigator
Back
vcsa-01a.corp.local
RegionA01
none
vmservice-vshield-pg
RegionA01-vDS-COMP
RegionA01-COMP--DVUplinks-38
VLAN101
VLAN102
VLAN103
VM Network
vxw-dvs-38-virtualwire-1-sid-10000-Transit_Network_01
vxw-dvs-38-virtualwire-4-sid-10001-Web-Tier
vxw-dvs-38-virtualwire-5-sid-10002-App-Tier
vxw-dvs-38-virtualwire-6-sid-10003-DB-Tier
vxw-vmknicPg-dvs-38-0-9f4633bf-6114-4393-8239-366810c9ccce
vxw-dvs-38-virtualwire-1-sid-10000-Transit_Network_01
Actions
Getting Started
Summary
Monitor
Configure
Permissions
Ports
Hosts
VMs
vxw-dvs-38-virtualwire-1-sid-10000-Transit_Network_01
Port binding: Static binding
Port allocation: Elastic
VLAN ID: 130
Distributed Port Group Details
Policies
Tags
Custom Attributes

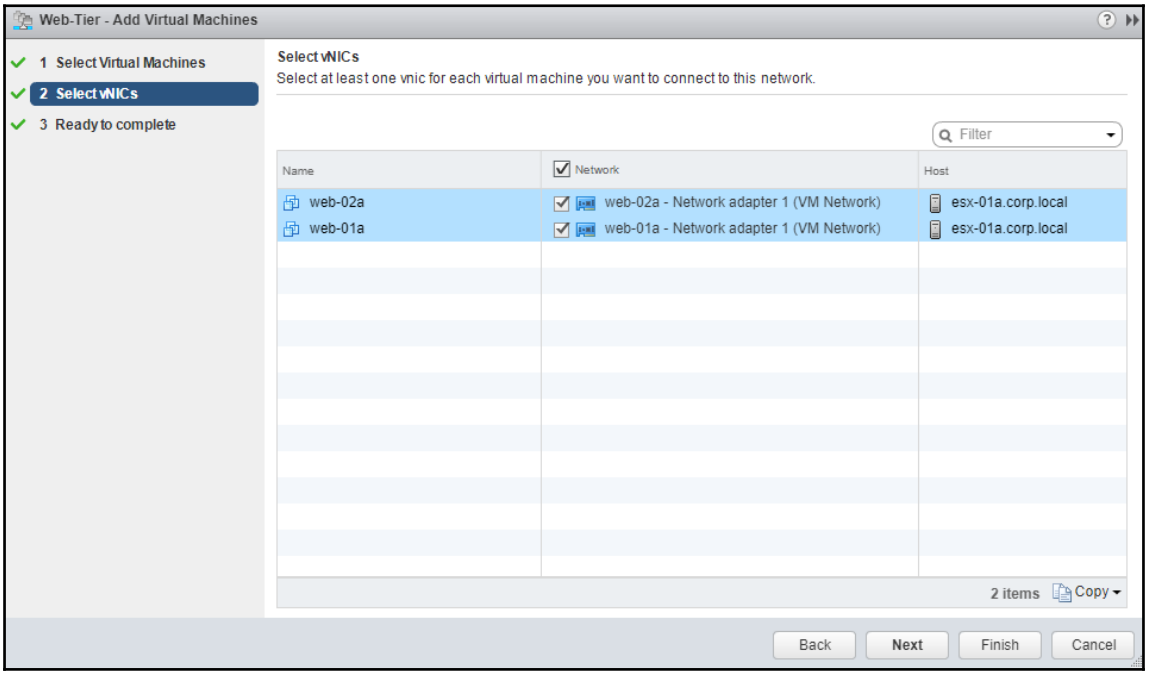

RegionA01-vDS-COMP
DVUplinks-RegionA01-vDS-COMP
ESXi-RegionA01-vDS-COMP
Storage-RegionA01-vDS-COMP
VM-RegionA01-vDS-COMP
vMotion-RegionA01-vDS-COMP
vxw-dvs-40-virtualwire-10-sid-5006-Central_CLI_Network_02
vxw-dvs-40-virtualwire-11-sid-5007-Transit_Network_01
vxw-dvs-40-virtualwire-4-sid-5000-Web_Tier_Logical_Switch
vxw-dvs-40-virtualwire-5-sid-5001-App_Tier_Logical_Switch
vxw-dvs-40-virtualwire-6-sid-5002-DB_Tier_Logical_Switch
vxw-dvs-40-virtualwire-7-sid-5003-Windows_Tier
vxw-dvs-40-virtualwire-8-sid-5004-Collapsed_Logical_Switch
vxw-dvs-40-virtualwire-9-sid-5005-Central_CLI_Network_01
vxw-vmknicPg-dvs-40-0-5274fa65-04d6-48c9-89c9-cfab202325ad
RegionA01-vDS-MGMT
ESXi-RegionA01-vDS-MGMT
RegionA01-vDS-MG-DVUplinks-143
Storage-RegionA01-vDS-MGMT
Uplink-RegionA01-vDS-MGMT
VM-RegionA01-vDS-MGMT
vMotion-RegionA01-vDS-MGMT
vxw-dvs-143-virtualwire-10-sid-5006-Central_CLI_Network_02
vxw-dvs-143-virtualwire-11-sid-5007-Transit_Network_01

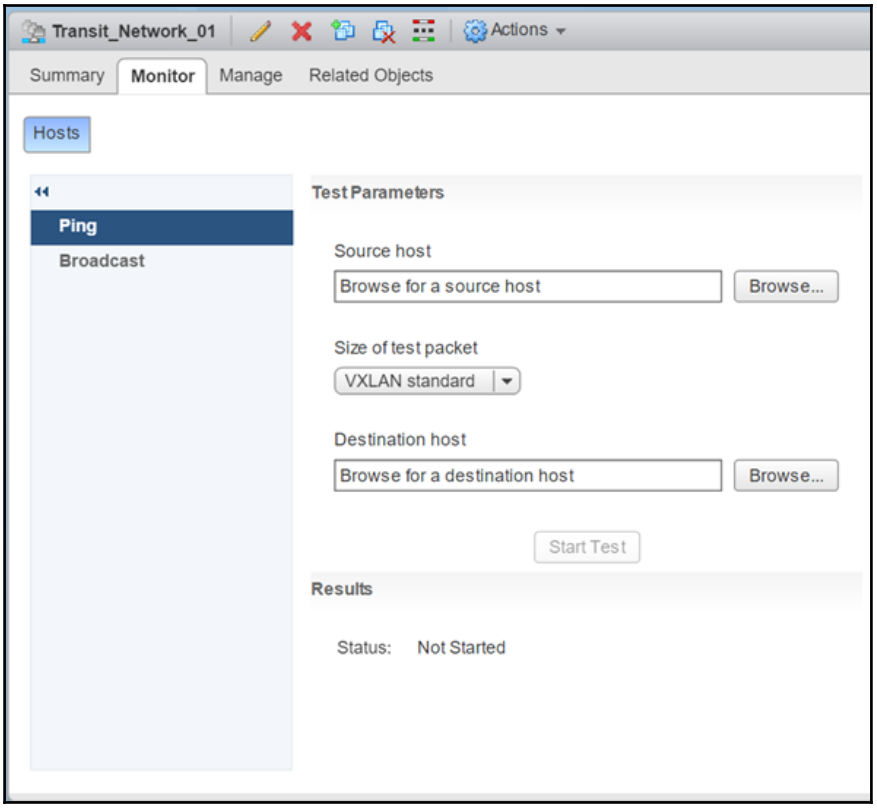

192.168.110.51 - PuTTY
port 36:
com.vmware.common.port.alias = , propType = CONFIG
com.vmware.common.port.connectid = 913387804 , propType = CONFIG
com.vmware.common.port.portgroupid = dvportgroup-63 , propType = CONFIG
com.vmware.common.port.block = false , propType = CONFIG
com.vmware.common.port.dvfilter = filters (num = 0):
propType = CONFIG
com.vmware.common.port.ptAllowed = 0x 0. 0. 0. 0
propType = CONFIG
com.vmware.etherswitch.port.security = deny promiscuous; deny mac change; deny forged frames
propType = CONFIG
com.vmware.etherswitch.port.txUplink = normal , propType = CONFIG
com.vmware.common.port.volatile.persist = /vmfs/volumes/5a665ae4-25a253d6-e7ee-80ee73b0dfcc/.dvsData/50 07 fa 42 23 ad bd 6b-a4 4e ae f0 79 b7 d1 b7/36 , propType = CONFIG
com.vmware.common.port.dvfilteraltvmx = 0x31.3a.64.76.66.69.6c.74.65.72.2d.67.65.6e.65.72.69.63.2d.76.6d.77.61.72.65.2d.73.77.73.65.63.3a.66.61.69.6c.43.6c.6f.73.65.64
propType = CONFIG POLICY
com.vmware.etherswitch.port.vlanNestedTag = 0x 0. 0. 0. 0
propType = CONFIG POLICY
com.vmware.net.vxlan.cp = 0x 0. 0. 0. 1
propType = CONFIG POLICY
com.vmware.net.vxlan.id = 0x 0. 0.27.10
propType = CONFIG POLICY
com.vmware.net.vxlan.mcastip = 0x 0. 0. 0. 1

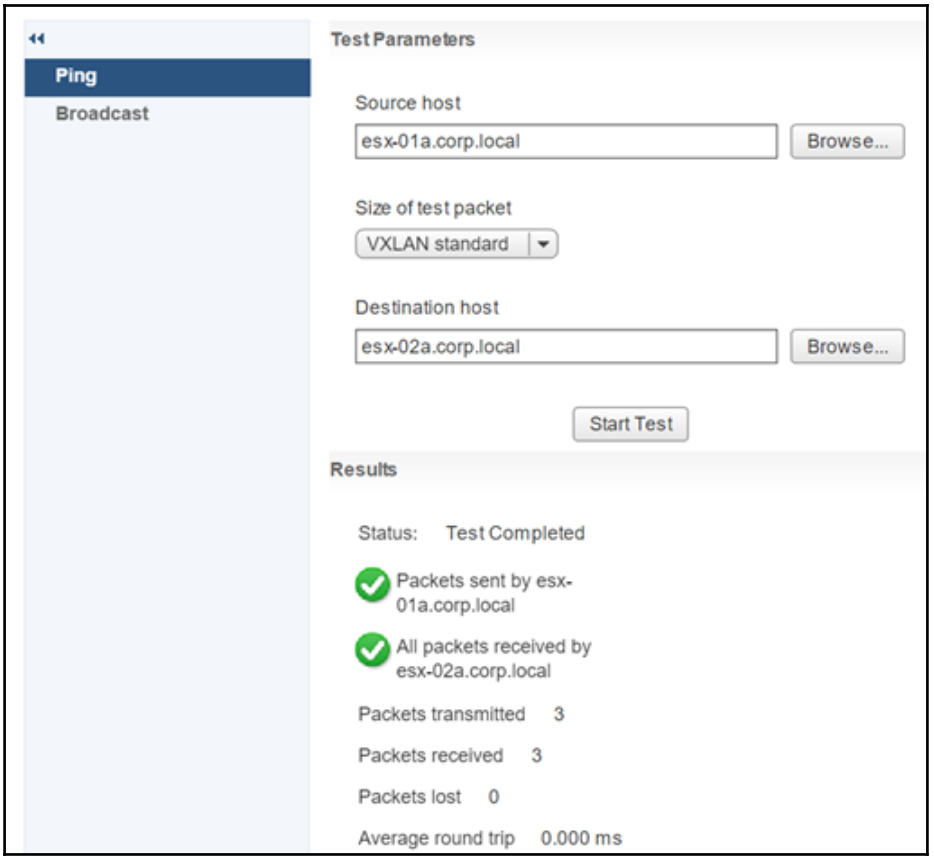

Web-Tier
Logical Switch
VM
VM
web-01a
web-02a

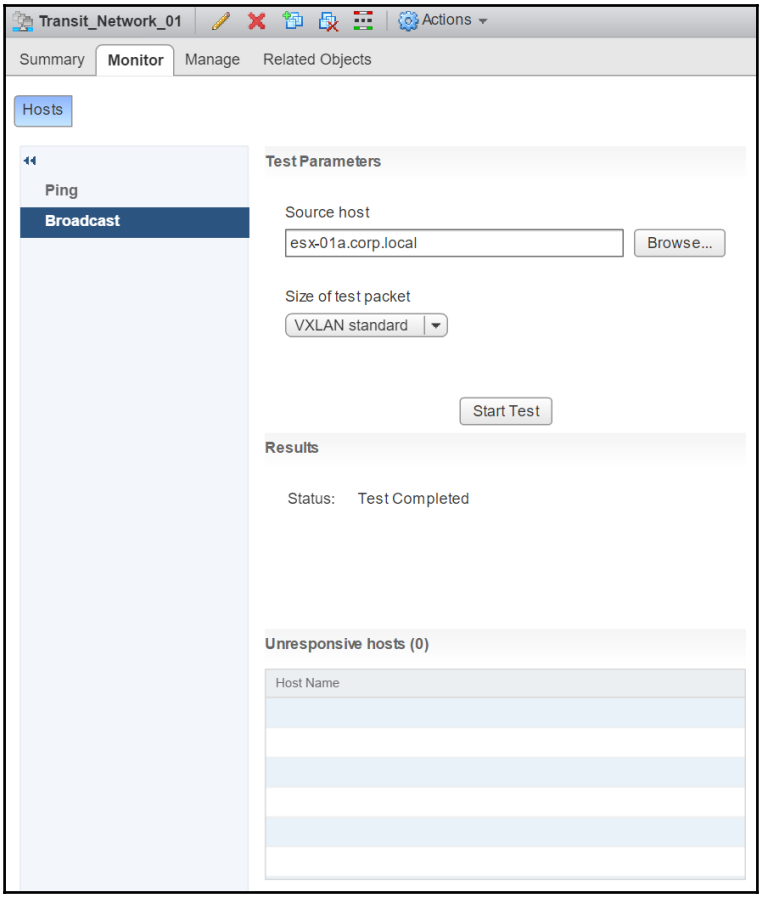

Logical Switches
NSX Manager: 192.168.110.15
Actions
Virtual Wire ID
Segment ID
Name
virtualwire-1
10000
Transit_Network_01
virtualwire-4
10001
Web-Tier
virtualwire-5
10002
App-Tier
virtualwire-6
10003
DB-Tier
Actions - Web-Tier
Edit Settings
Remove
Add VM
Remove VM
Connect Edge
Manage Hardware Bindings

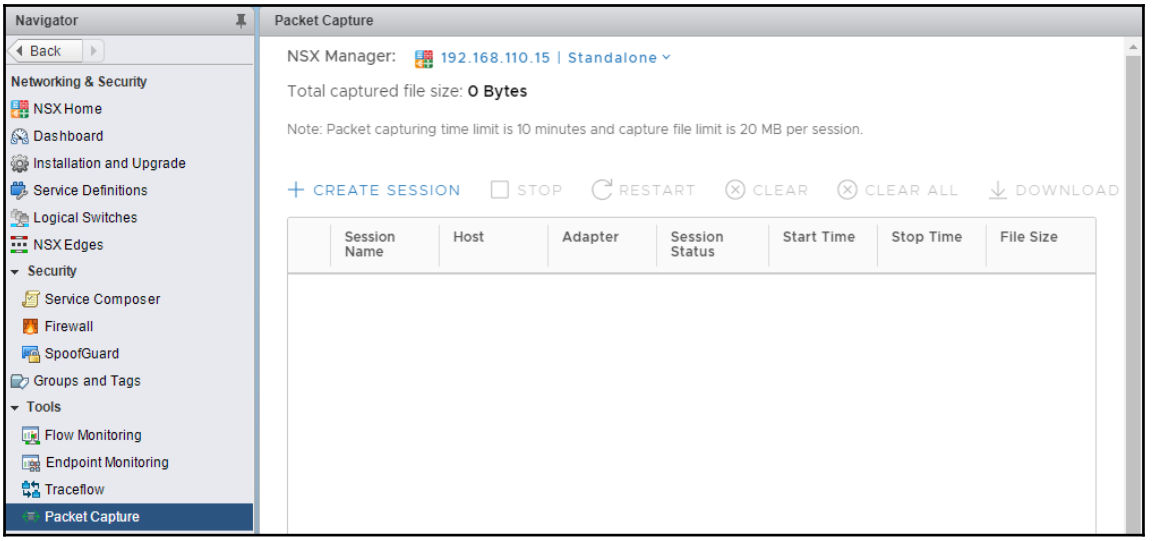

Web-Tier - Add Virtual Machines
1 Select Virtual Machines
2 Select vNICs
3 Ready to complete
Select Virtual Machines
Select VMs to connect to this network
Select from the available objects list on the left and move it to the selected objects list by double clicking the object or using the arrow key.
web
Filter
Available Objects
web-03a
web-02a
web-01a
Selected Objects
web-01a
web-02a
3 items
Copy
2 items
Copy
Back
Next
Finish
Cancel

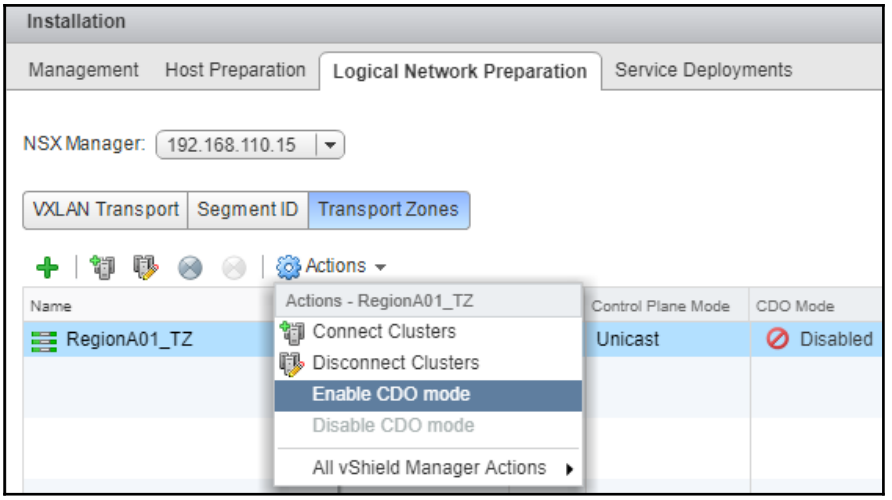

Web-Tier - Add Virtual Machines
1 Select Virtual Machines
2 Select vNICs
3 Ready to complete
Select vNICs
Select at least one vnic for each virtual machine you want to connect to this network.
Filter
Name
Network
Host
web-02a
web-02a - Network adapter 1 (VM Network)
esx-01a.corp.local
web-01a
web-01a - Network adapter 1 (VM Network)
esx-01a.corp.local
2 items
Copy
Back
Next
Finish
Cancel


Transit_Network_01
Actions
Summary
Monitor
Manage
Related Objects
Hosts
Ping
Broadcast
Test Parameters
Source host
Browse for a source host
Browse...
Size of test packet
VXLAN standard
Destination host
Browse for a destination host
Browse...
Start Test
Results
Status:
Not Started


Ping
Broadcast
Test Parameters
Source host
esx-01a.corp.local
Browse...
Size of test packet
VXLAN standard
Destination host
esx-02a.corp.local
Browse...
Start Test
Results
Status: Test Completed
Packets sent by esx-01a.corp.local
All packets received by esx-02a.corp.local
Packets transmitted 3
Packets received 3
Packets lost 0
Average round trip 0.000 ms


Transit_Network_01
Actions
Summary
Monitor
Manage
Related Objects
Hosts
Ping
Broadcast
Test Parameters
Source host
esx-01a.corp.local
Browse...
Size of test packet
VXLAN standard
Start Test
Results
Status: Test Completed
Unresponsive hosts (0)
Host Name


Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation and Upgrade
Service Definitions
Logical Switches
NSX Edges
Security
Service Composer
Firewall
SpoofGuard
Groups and Tags
Tools
Flow Monitoring
Endpoint Monitoring
Traceflow
Packet Capture
Packet Capture
NSX Manager: 192.168.110.15 | Standalone
Total captured file size: 0 Bytes
Note: Packet capturing time limit is 10 minutes and capture file limit is 20 MB per session.
CREATE SESSION
STOP
RESTART
CLEAR
CLEAR ALL
DOWNLOAD
Session Name
Host
Adapter
Session Status
Start Time
Stop Time
File Size


Installation
Management
Host Preparation
Logical Network Preparation
Service Deployments
NSX Manager: 192.168.110.15
VXLAN Transport
Segment ID
Transport Zones
Actions
Name
RegionA01_TZ
Actions - RegionA01_TZ
Connect Clusters
Disconnect Clusters
Enable CDO mode
Disable CDO mode
All vShield Manager Actions
Control Plane Mode
Unicast
CDO Mode
Disabled

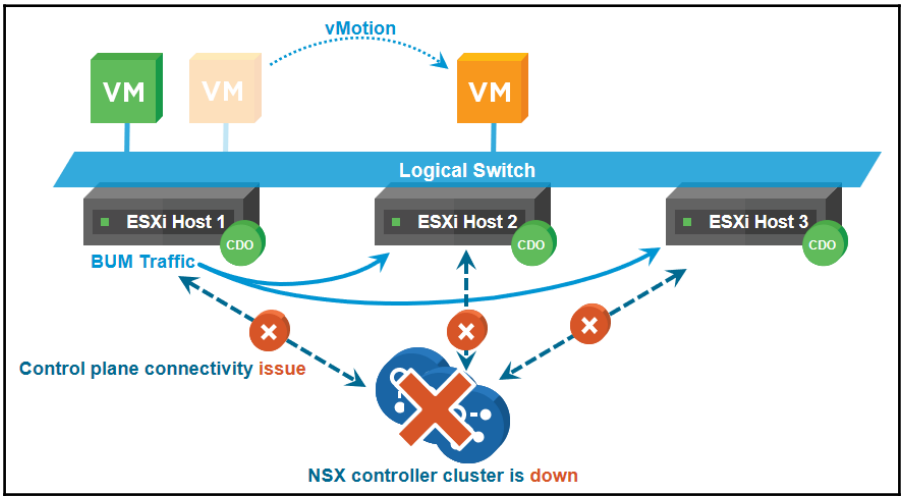
Installation

Management | Host Preparation | Logical Network Preparation | Service Deployments

NSX Manager: 192.168.110.15

VXLAN Transport | Segment ID | Transport Zones

Name	Description	Scope	Control Plane Mode	CDO Mode	Logical Switches
RegionA01_TZ	RegionA01 Transport Zone	Global	Unicast	Enabled (Segment ID: 10004)	4

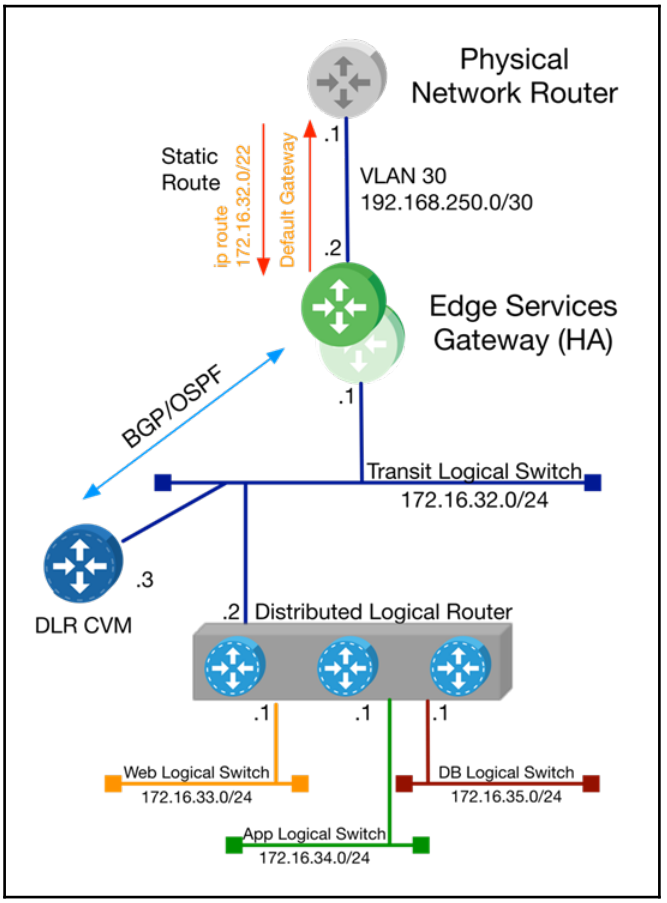


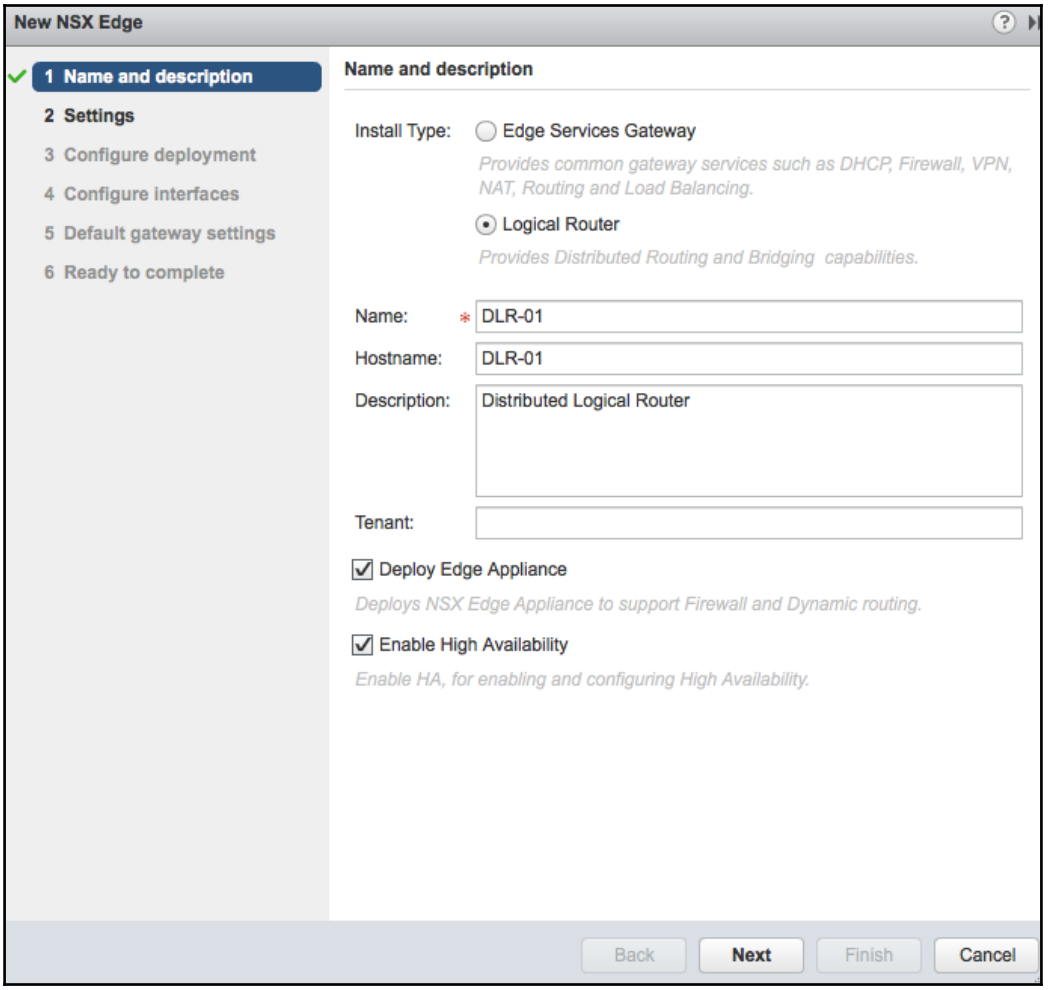
Logical Switches

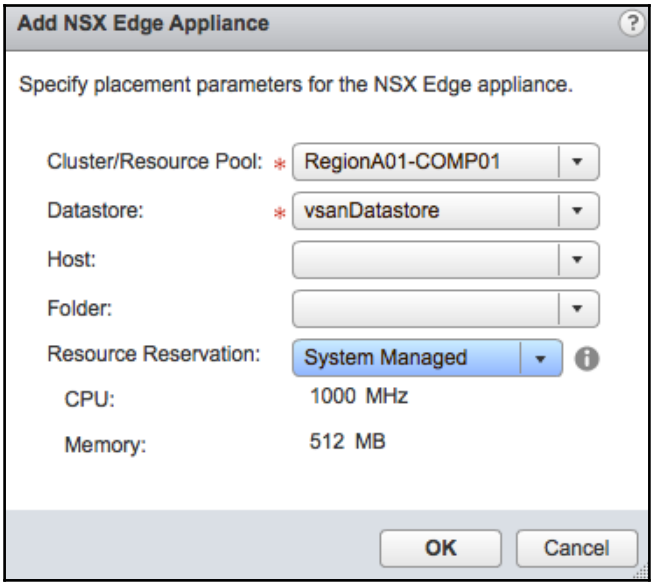
NSX Manager: 192.168.110.15

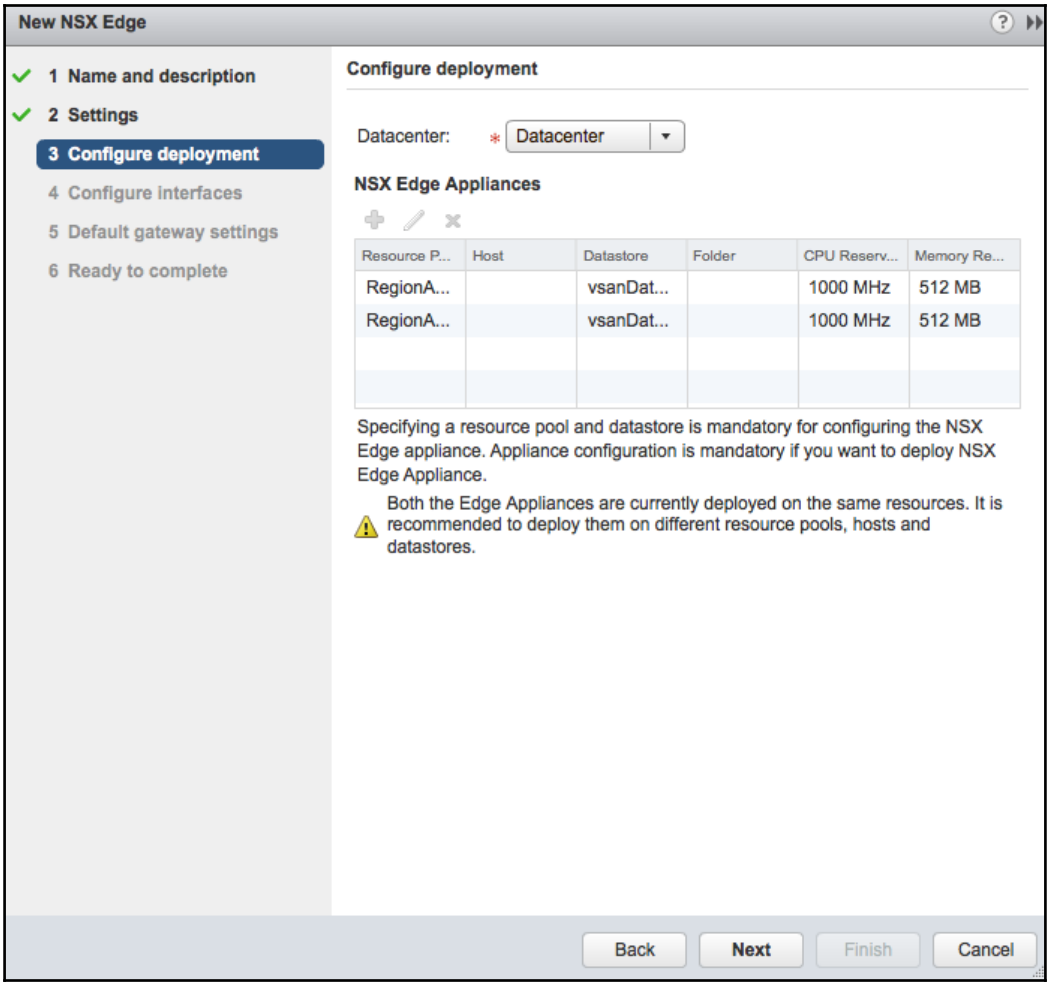
Virtual Wire ID	Segment ID	Name
virtualwire-1	10000	Transit_Network_01
virtualwire-4	10001	Web-Tier
virtualwire-5	10002	App-Tier
virtualwire-6	10003	DB-Tier
virtualwire-7	10005	New-Logical-Switch-After-CDO

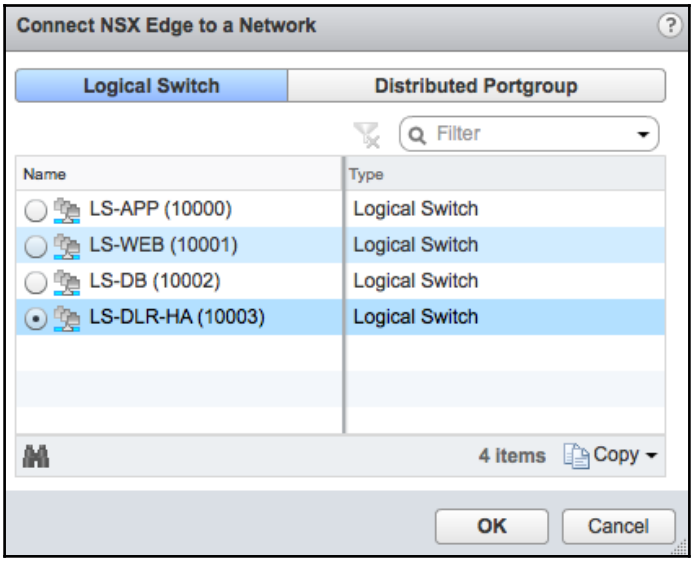
Chapter 03: Configuring VMware NSX Logical Routing

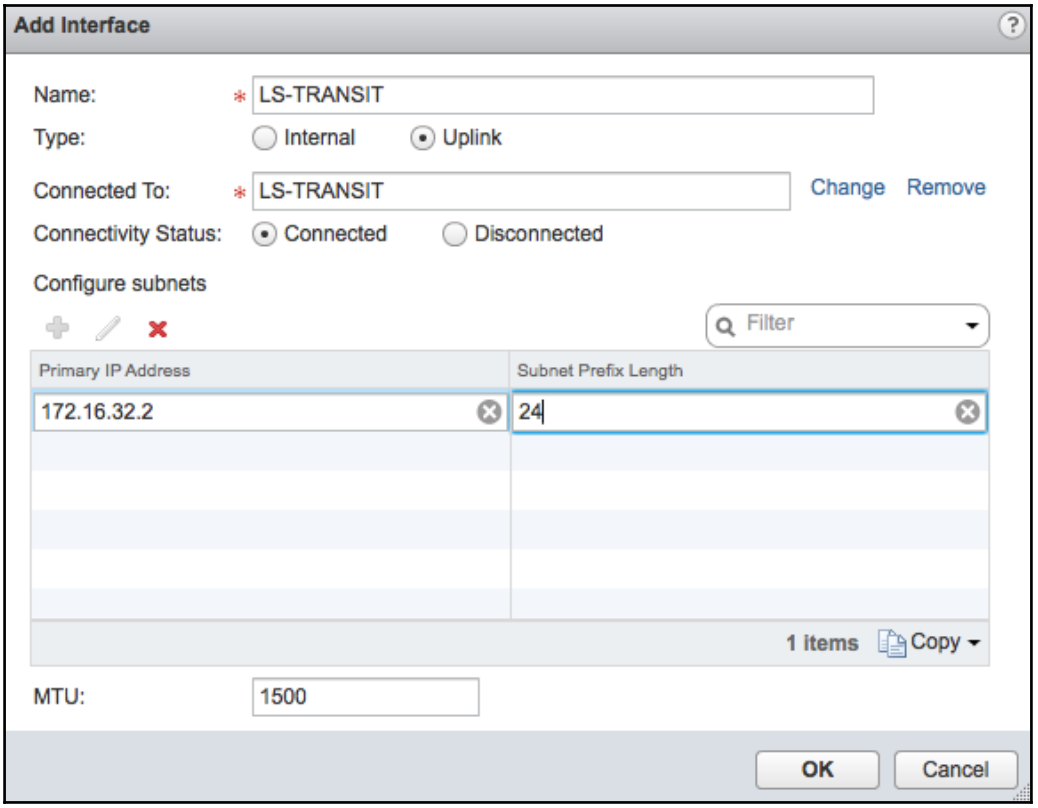


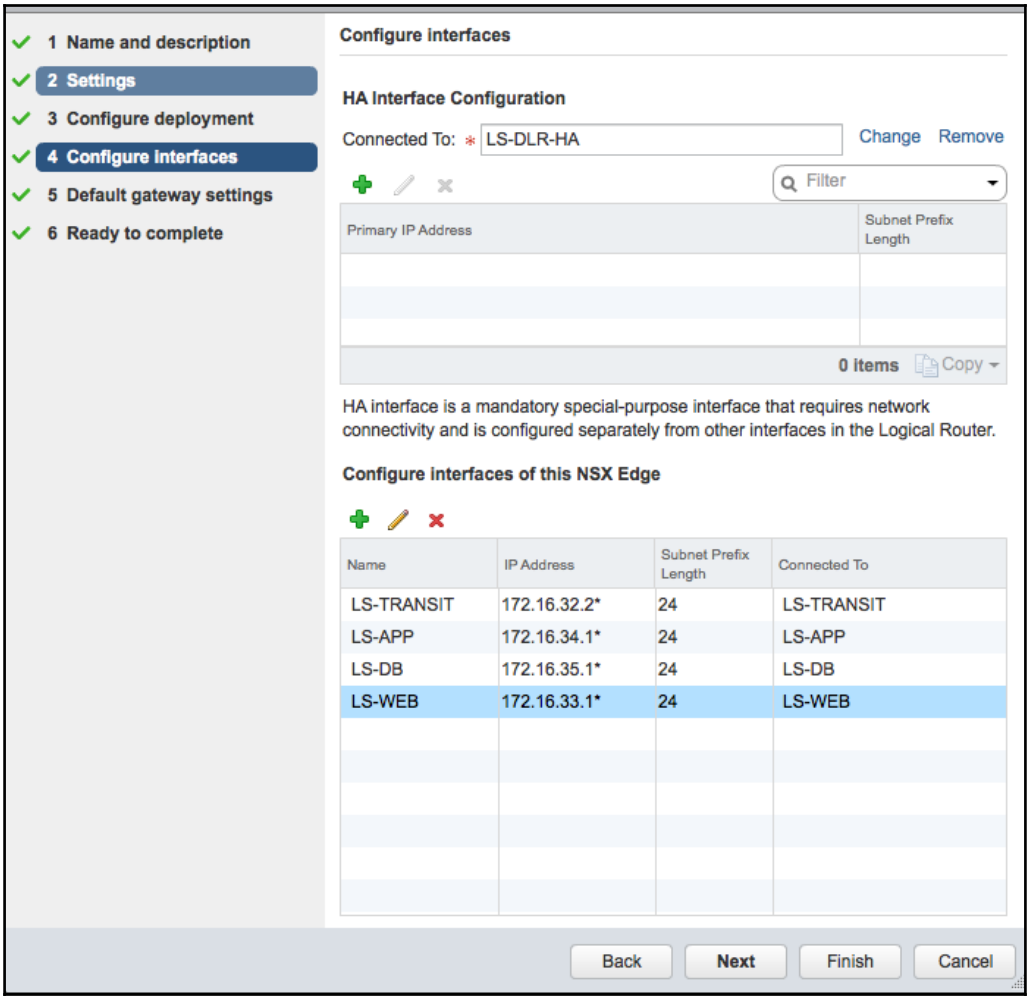

New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Ready to complete
Name and description
Install Type:
Edge Services Gateway
Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.
Logical Router
Provides Distributed Routing and Bridging capabilities.
Name:
DLR-01
Hostname:
DLR-01
Description:
Distributed Logical Router
Tenant:
Deploy Edge Appliance
Deploys NSX Edge Appliance to support Firewall and Dynamic routing.
Enable High Availability
Enable HA, for enabling and configuring High Availability.
Back
Next
Finish
Cancel

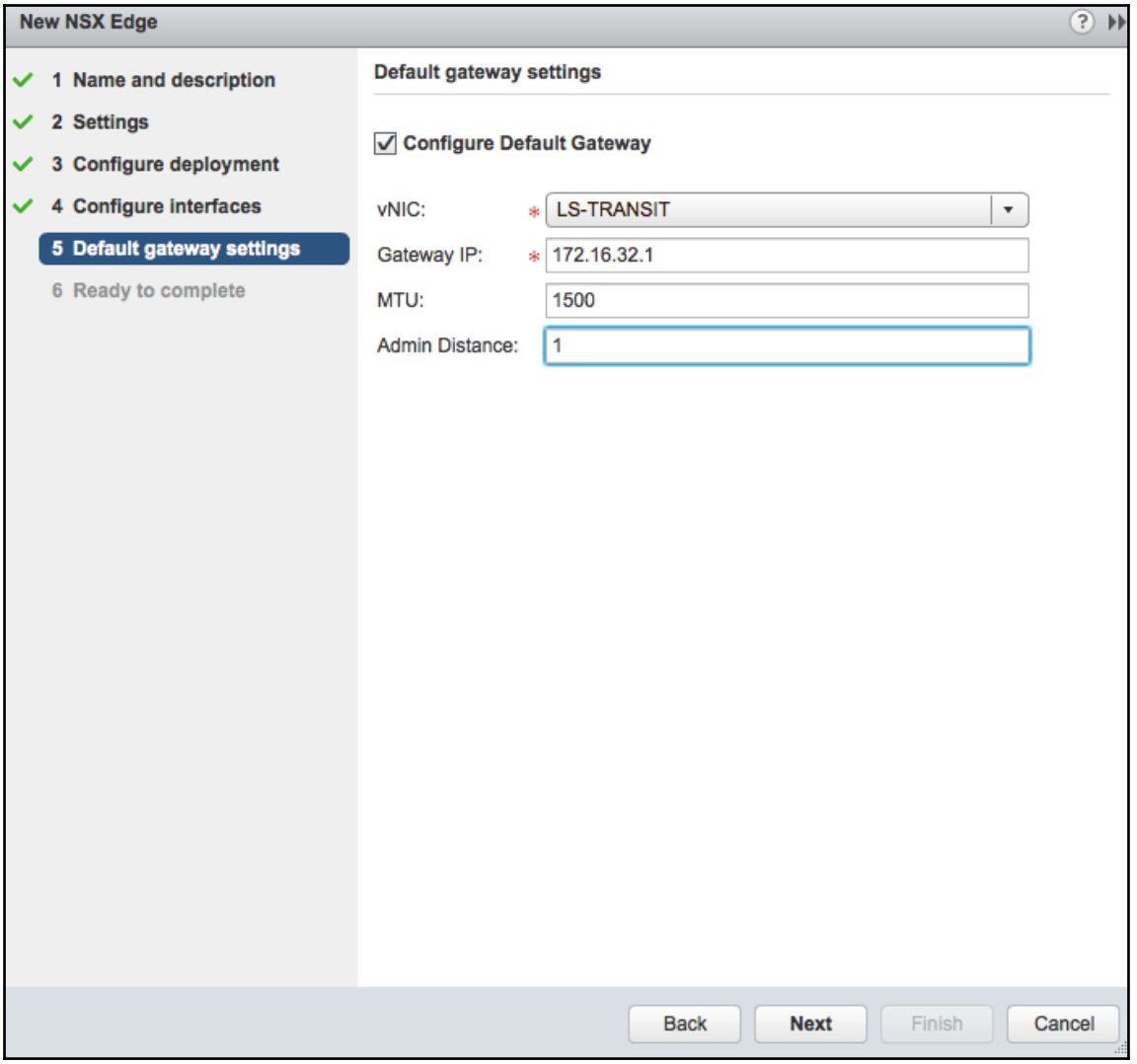

Add NSX Edge Appliance
Specify placement parameters for the NSX Edge appliance.
Cluster/Resource Pool:
RegionA01-COMP01
Datastore:
vsanDatastore
Host:
Folder:
Resource Reservation:
System Managed
CPU:
1000 MHz
Memory:
512 MB
OK
Cancel

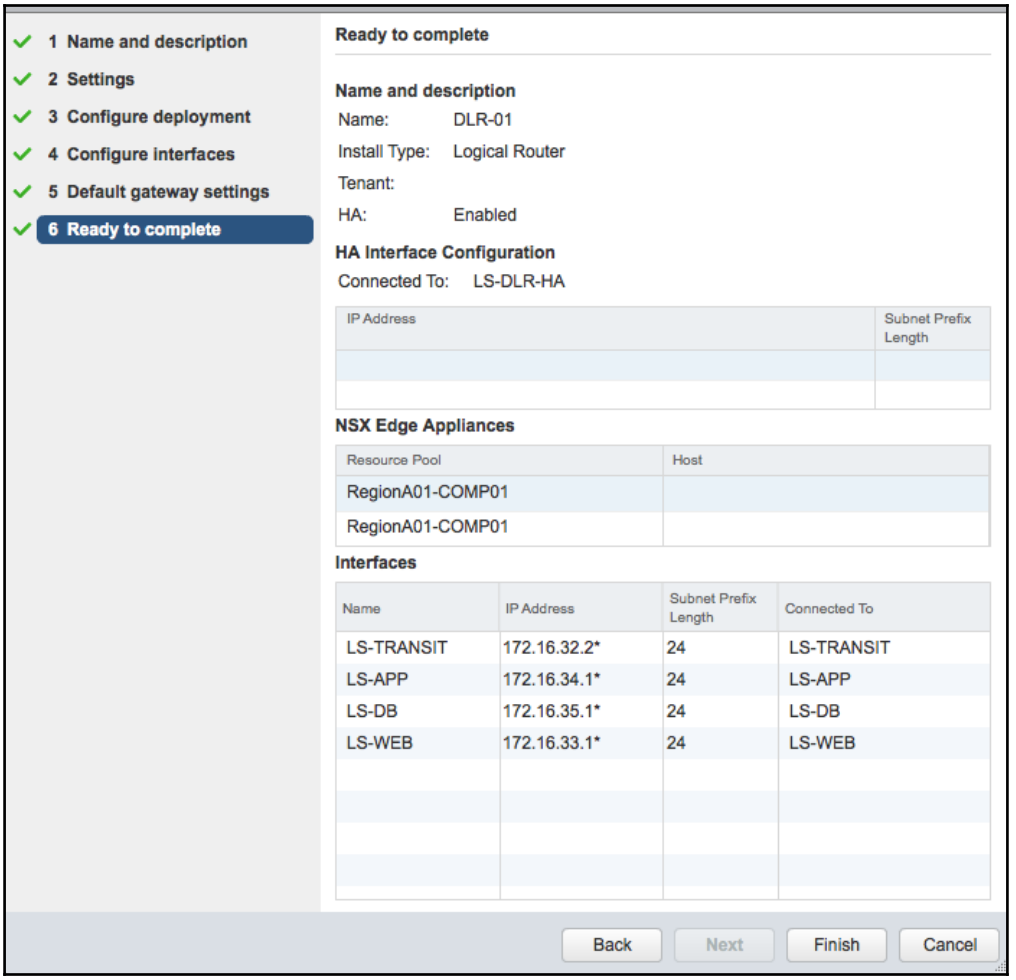

New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Ready to complete
Configure deployment
Datacenter:
Datacenter
NSX Edge Appliances
Resource P...
Host
Datastore
Folder
CPU Reserv...
Memory Re...
RegionA...
vsanDat...
1000 MHz
512 MB
RegionA...
vsanDat...
1000 MHz
512 MB
Specifying a resource pool and datastore is mandatory for configuring the NSX Edge appliance. Appliance configuration is mandatory if you want to deploy NSX Edge Appliance.
Both the Edge Appliances are currently deployed on the same resources. It is recommended to deploy them on different resource pools, hosts and datastores.
Back
Next
Finish
Cancel


Connect NSX Edge to a Network
Logical Switch
Distributed Portgroup
Filter
Name
Type
LS-APP (10000)
Logical Switch
LS-WEB (10001)
Logical Switch
LS-DB (10002)
Logical Switch
LS-DLR-HA (10003)
Logical Switch
4 items
Copy
OK
Cancel


Add Interface
Name:
LS-TRANSIT
Type:
Internal
Uplink
Connected To:
LS-TRANSIT
Change
Remove
Connectivity Status:
Connected
Disconnected
Configure subnets
Filter
Primary IP Address
Subnet Prefix Length
172.16.32.2
24
1 items
Copy
MTU:
1500
OK
Cancel


1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Ready to complete
Configure interfaces
HA Interface Configuration
Connected To: * LS-DLR-HA
Change
Remove
Filter
Primary IP Address
Subnet Prefix Length
0 items
Copy
HA interface is a mandatory special-purpose interface that requires network connectivity and is configured separately from other interfaces in the Logical Router.
Configure interfaces of this NSX Edge
Name
IP Address
Subnet Prefix Length
Connected To
LS-TRANSIT
172.16.32.2*
24
LS-TRANSIT
LS-APP
172.16.34.1*
24
LS-APP
LS-DB
172.16.35.1*
24
LS-DB
LS-WEB
172.16.33.1*
24
LS-WEB
Back
Next
Finish
Cancel

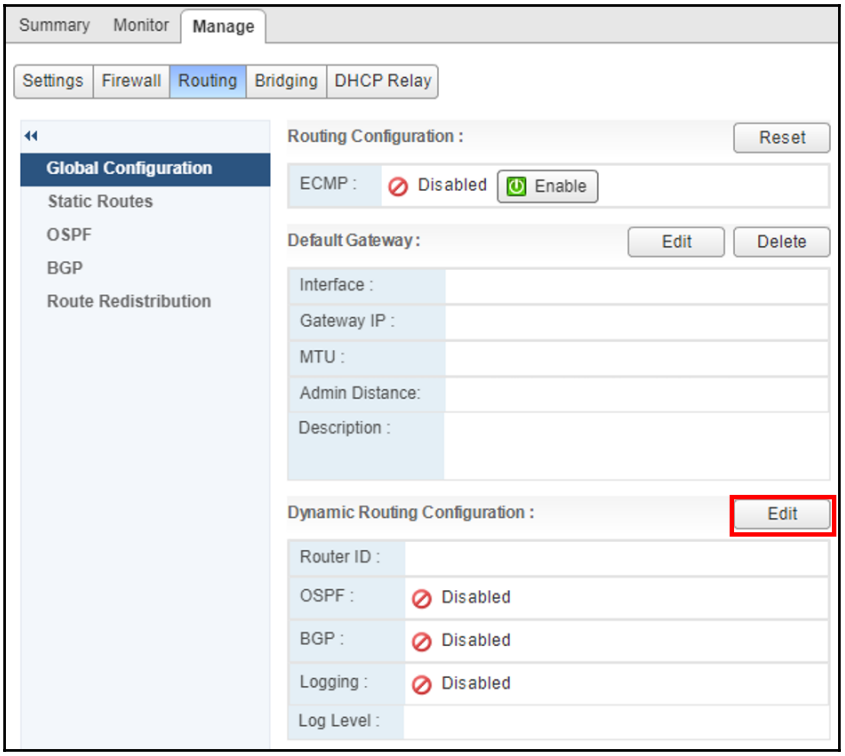

New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Ready to complete
Default gateway settings
Configure Default Gateway
vNIC:
LS-TRANSIT
Gateway IP:
172.16.32.1
MTU:
1500
Admin Distance:
1
Back
Next
Finish
Cancel

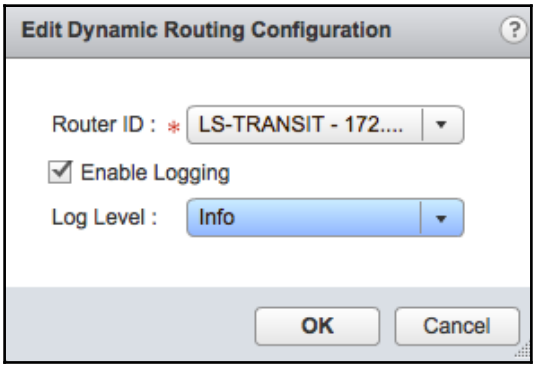


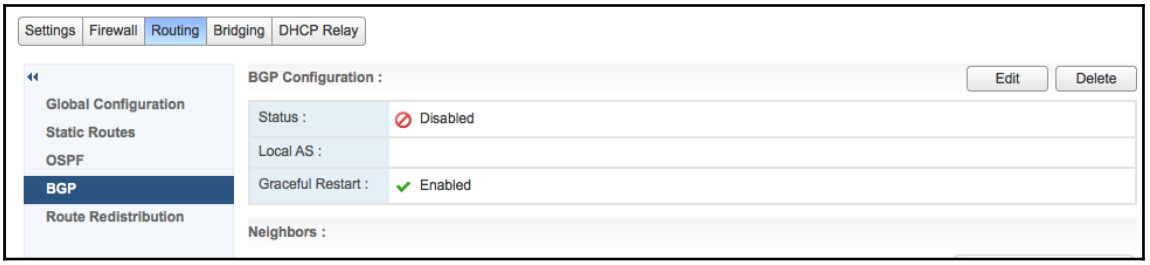
Id	Name	Type	Version	Status
edge-2	DLR-01	Logical Router	6.3.3	Deployed

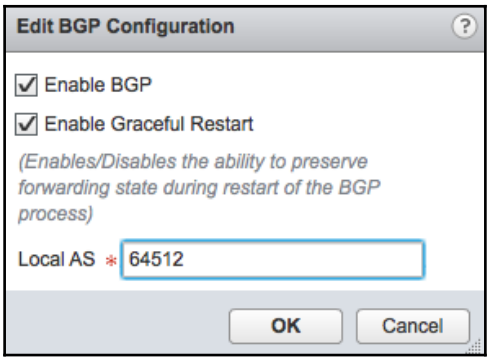
Id	Name	Type	Version	Status
edge-2	DLR-01	Logical Router	6.3.3	Deployed
edge-3	DLR-02	Logical Router	6.3.3	Undeployed

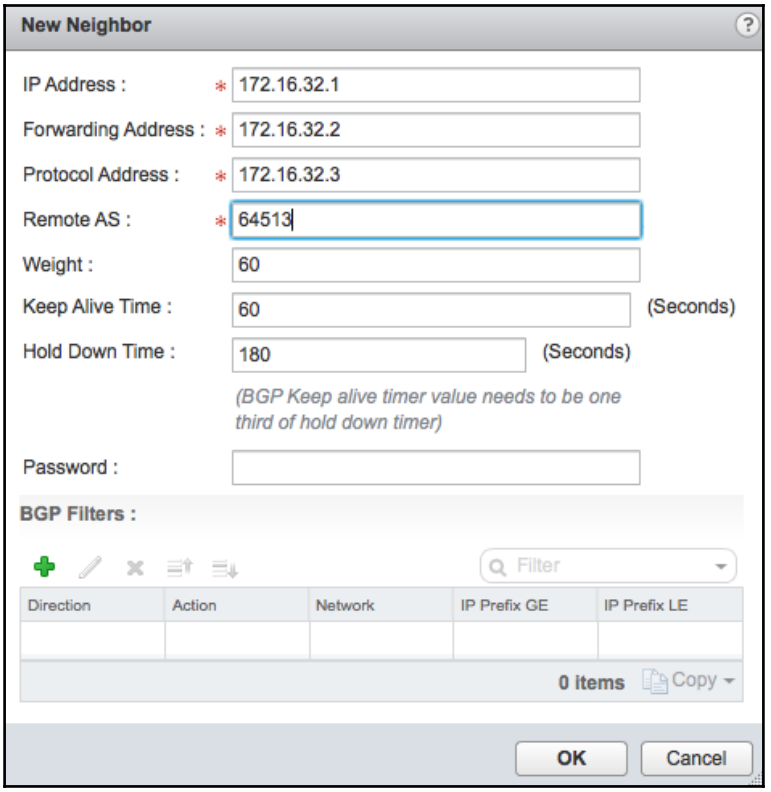
edge-2	DLR-01	Logical Router

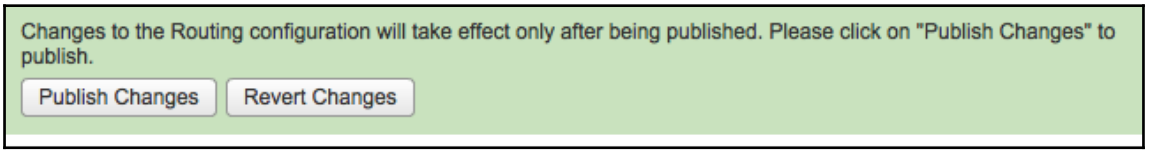

Summary
Monitor
Manage
Settings
Firewall
Routing
Bridging
DHCP Relay
Global Configuration
Static Routes
OSPF
BGP
Route Redistribution
Routing Configuration :
Reset
ECMP :
Disabled
Enable
Default Gateway :
Edit
Delete
Interface :
Gateway IP :
MTU :
Admin Distance:
Description :
Dynamic Routing Configuration :
Edit
Router ID :
OSPF :
Disabled
BGP :
Disabled
Logging :
Disabled
Log Level :

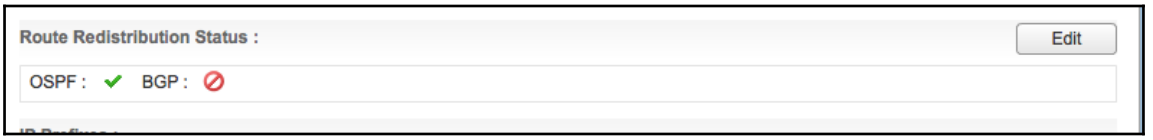

Edit Dynamic Routing Configuration
Router ID :
LS-TRANSIT - 172....
Enable Logging
Log Level :
Info
OK
Cancel

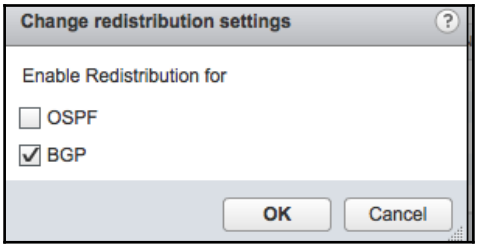

Settings
Firewall
Routing
Bridging
DHCP Relay
Global Configuration
Static Routes
OSPF
BGP
Route Redistribution
BGP Configuration :
Edit
Delete
Status :
Disabled
Local AS :
Graceful Restart :
Enabled
Neighbors :

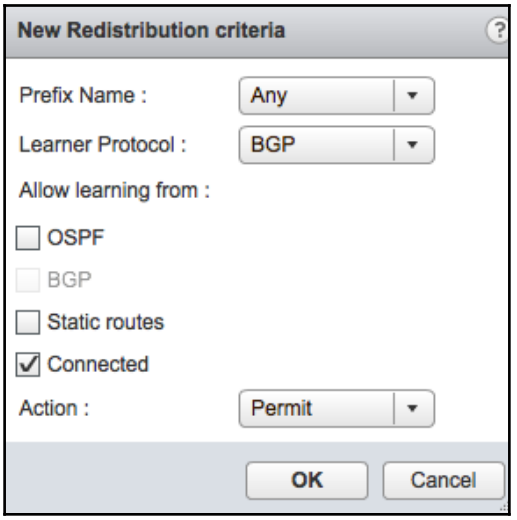

Edit BGP Configuration
Enable BGP
Enable Graceful Restart
(Enables/Disables the ability to preserve forwarding state during restart of the BGP process)
Local AS *
64512
OK
Cancel

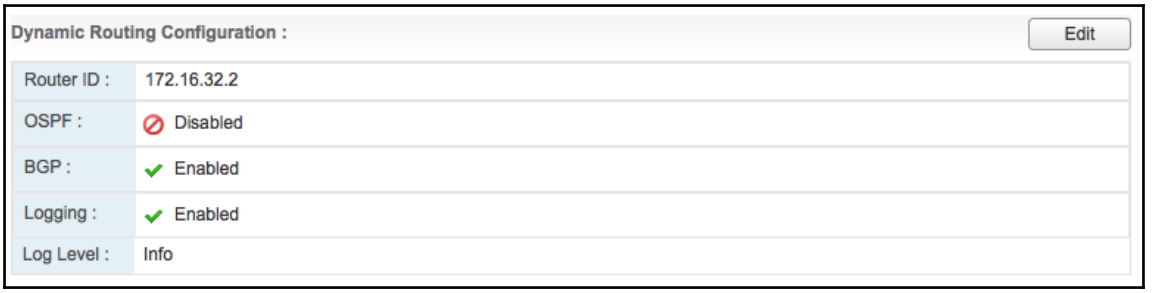

New Neighbor
IP Address : * 172.16.32.1
Forwarding Address : * 172.16.32.2
Protocol Address : * 172.16.32.3
Remote AS : * 64513
Weight : 60
Keep Alive Time : 60 (Seconds)
Hold Down Time : 180 (Seconds)
(BGP Keep alive timer value needs to be one third of hold down timer)
Password :
BGP Filters :
Filter
Direction
Action
Network
IP Prefix GE
IP Prefix LE
0 items
Copy
OK
Cancel

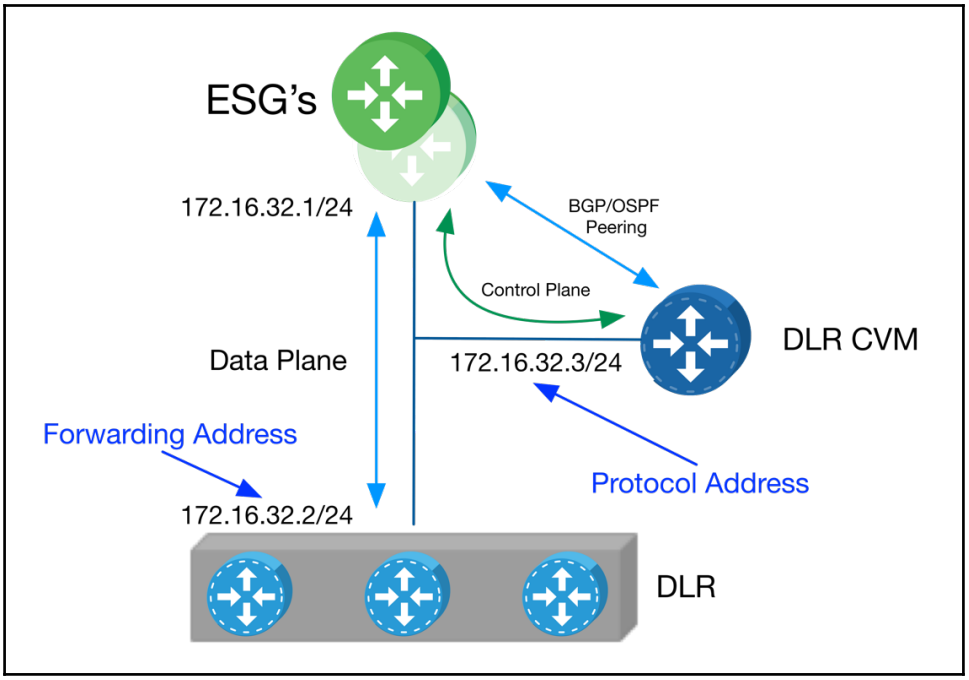

Changes to the Routing configuration will take effect only after being published. Please click on "Publish Changes" to publish.
Publish Changes
Revert Changes

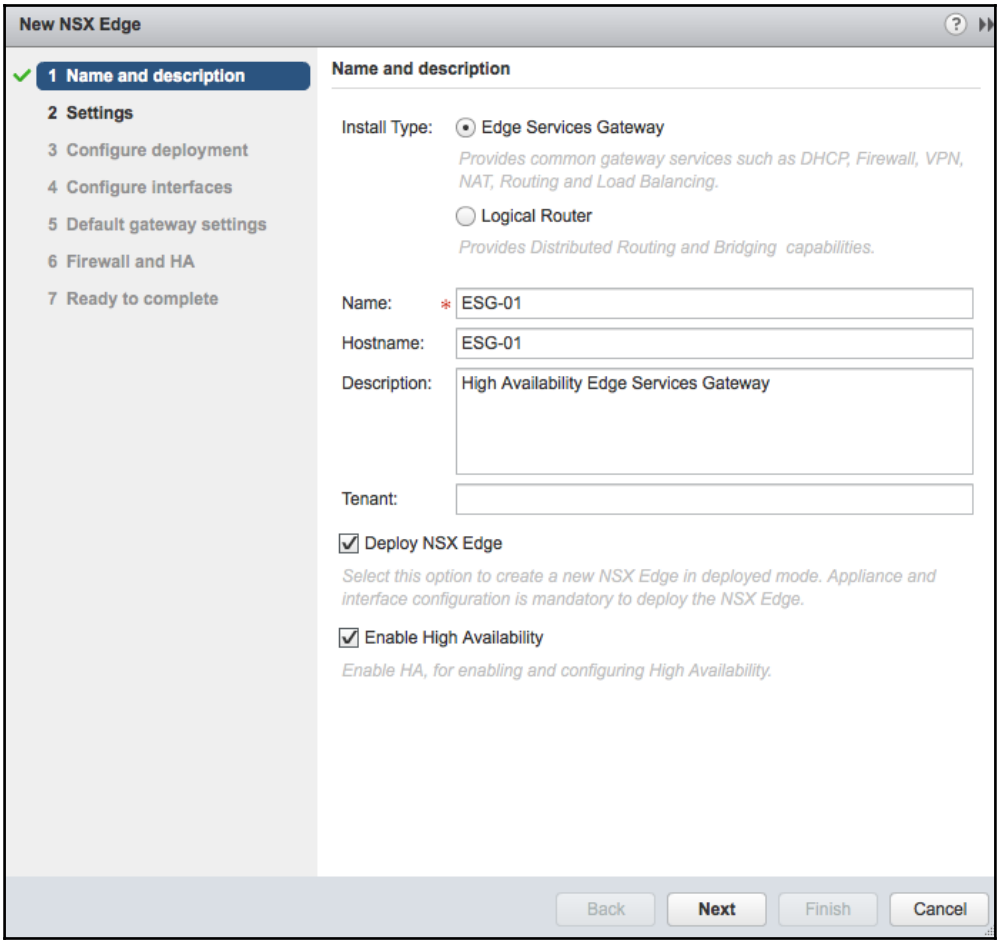

Route Redistribution Status :
Edit
OSPF :
BGP :

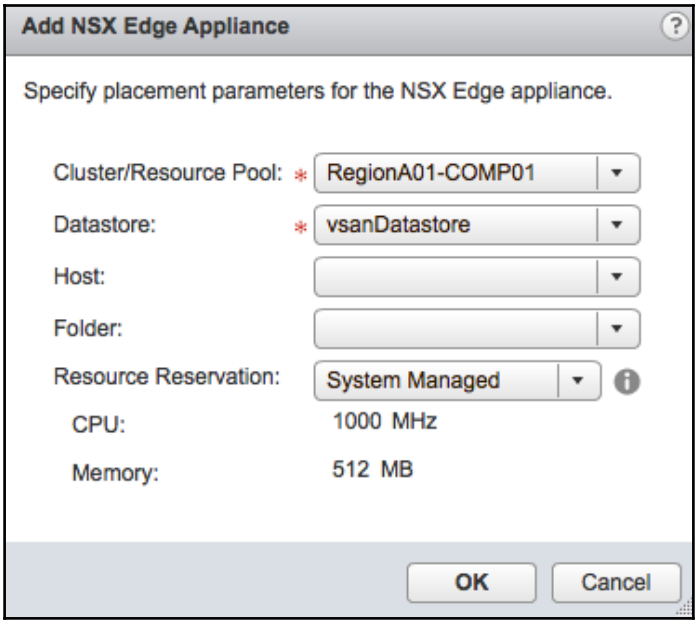

Change redistribution settings
Enable Redistribution for
OSPF
BGP
OK
Cancel

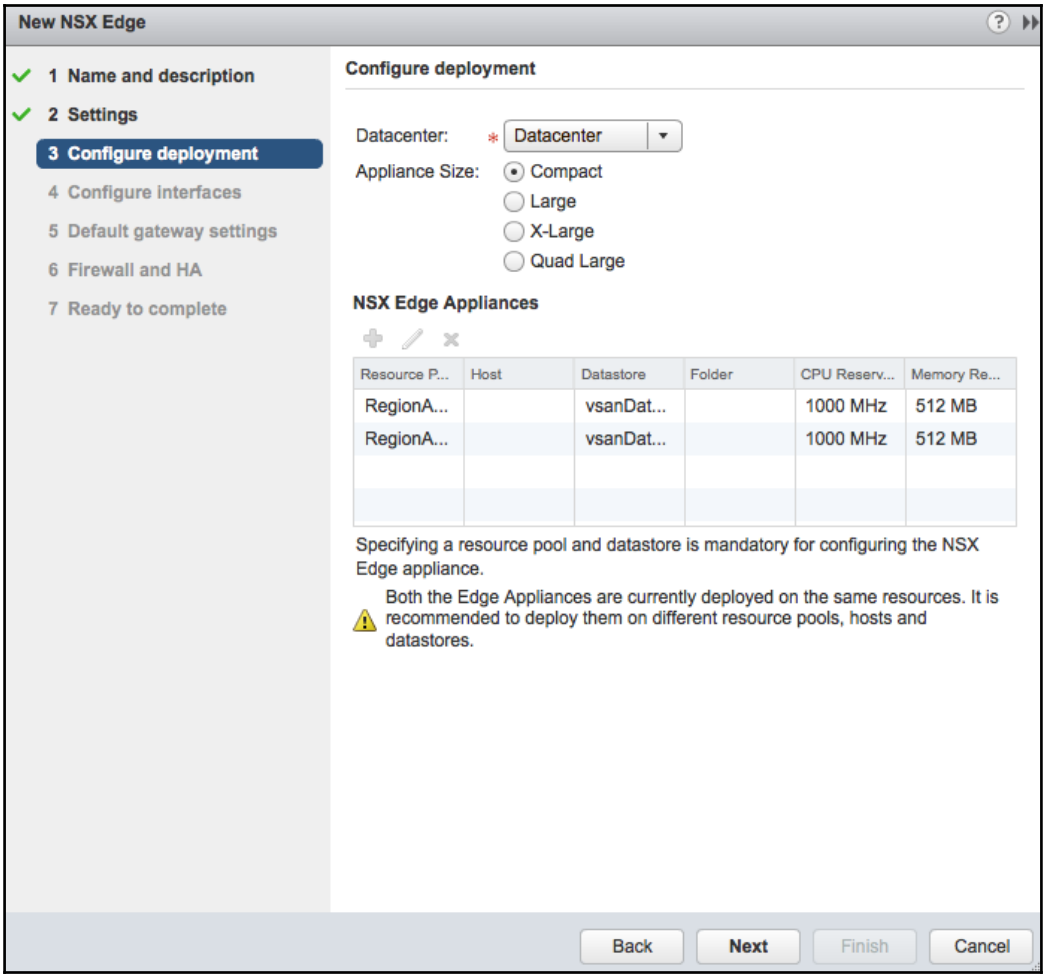

New Redistribution criteria
Prefix Name :
Any
Learner Protocol :
BGP
Allow learning from :
OSPF
BGP
Static routes
Connected
Action :
Permit
OK
Cancel

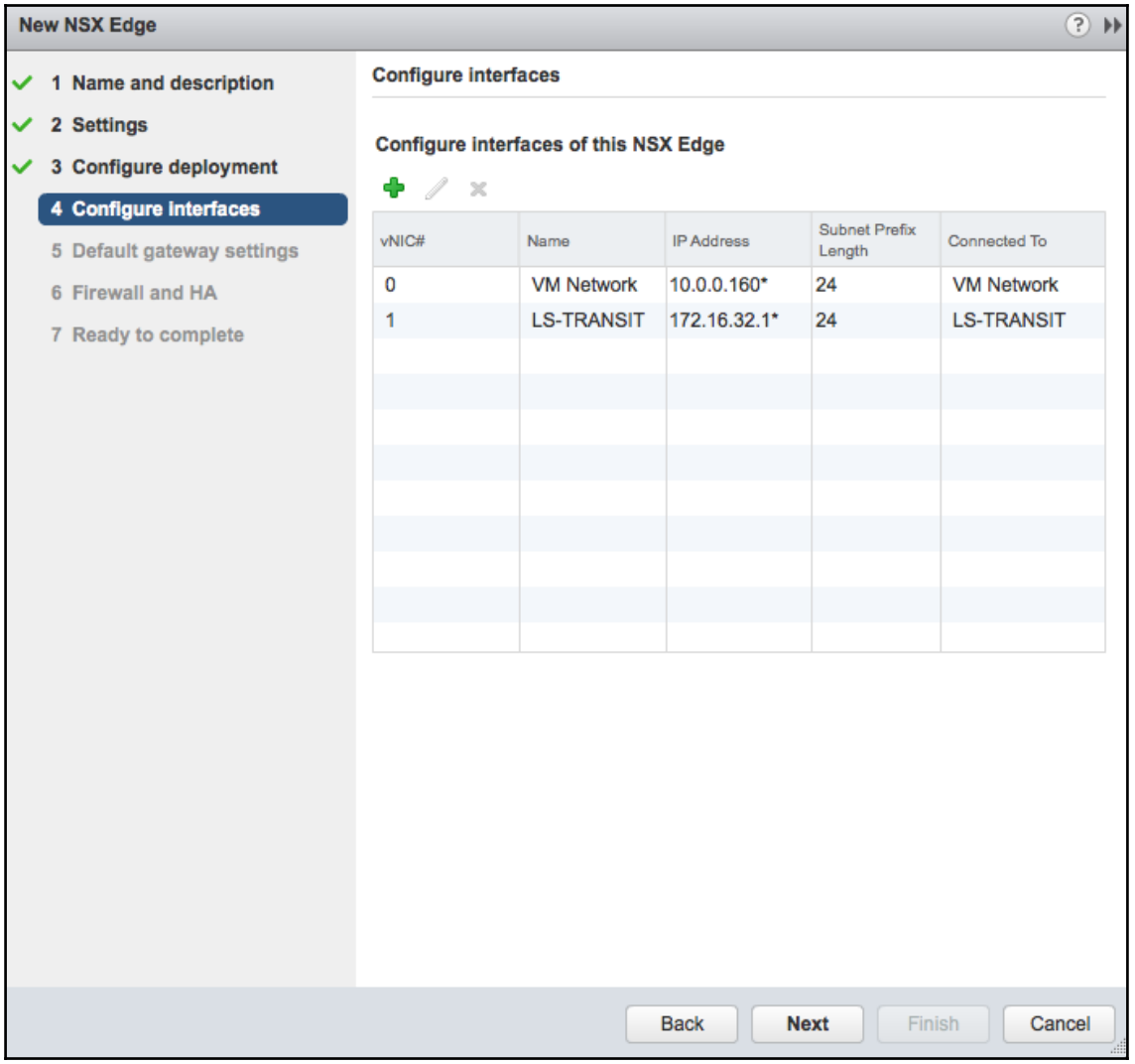

Dynamic Routing Configuration :
Edit
Router ID :
172.16.32.2
OSPF :
Disabled
BGP :
Enabled
Logging :
Enabled
Log Level :
Info

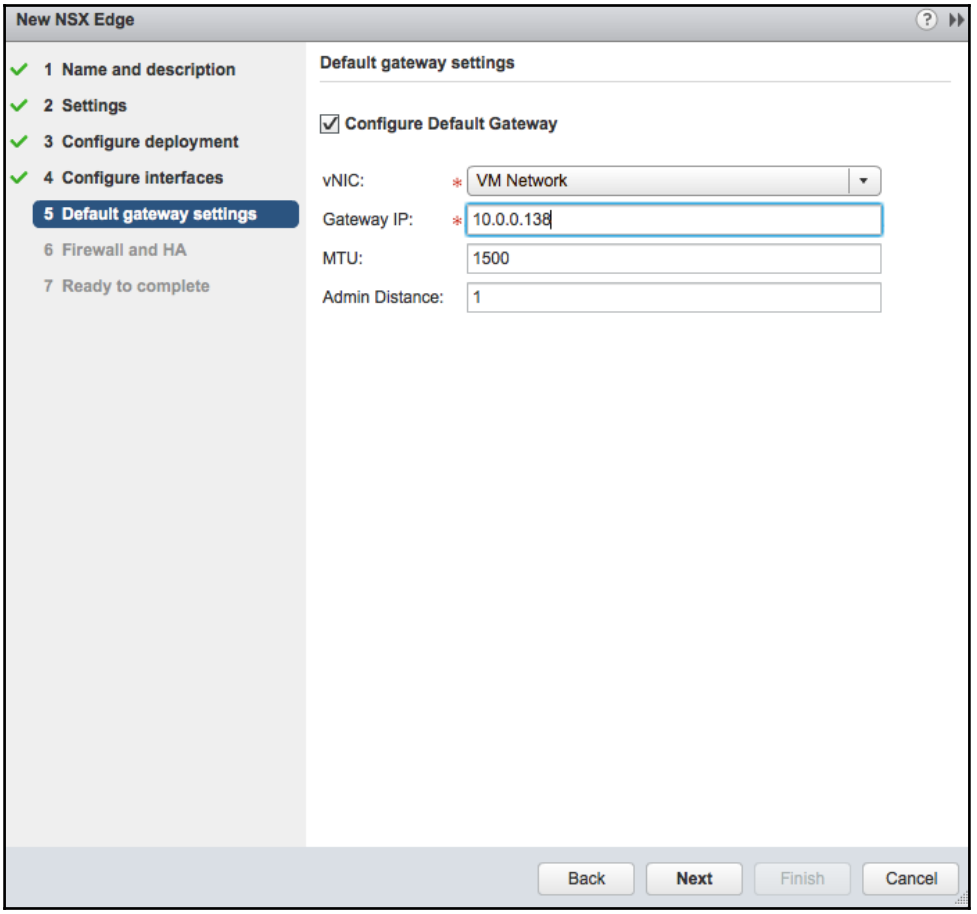

ESG's
172.16.32.1/24
BGP/OSPF
Peering
Control Plane
DLR CVM
Data Plane
172.16.32.3/24
Forwarding Address
Protocol Address
172.16.32.2/24
DLR

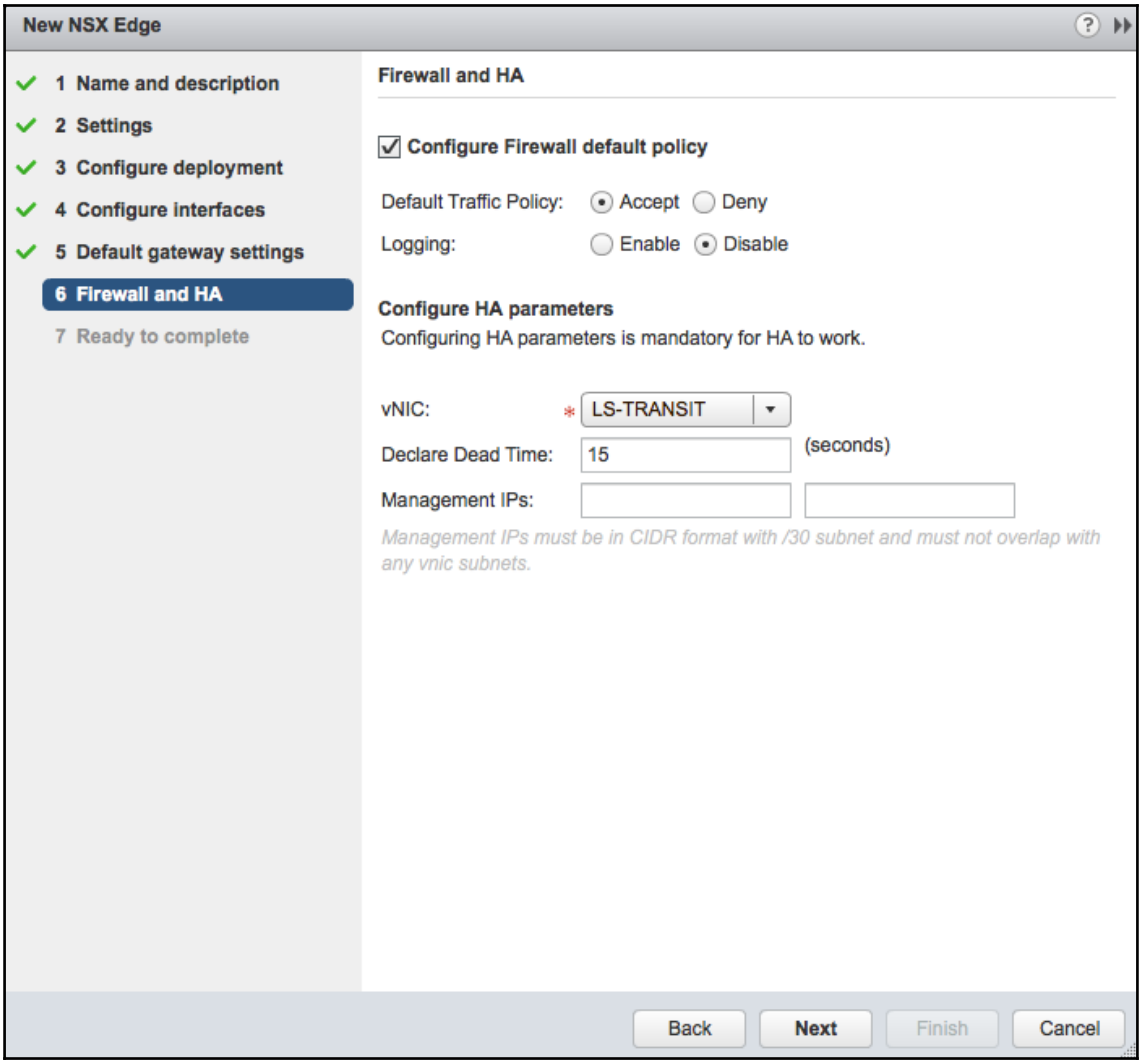

New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete
Name and description
Install Type:
Edge Services Gateway
Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.
Logical Router
Provides Distributed Routing and Bridging capabilities.
Name:
ESG-01
Hostname:
ESG-01
Description:
High Availability Edge Services Gateway
Tenant:
Deploy NSX Edge
Select this option to create a new NSX Edge in deployed mode. Appliance and interface configuration is mandatory to deploy the NSX Edge.
Enable High Availability
Enable HA, for enabling and configuring High Availability.
Back
Next
Finish
Cancel

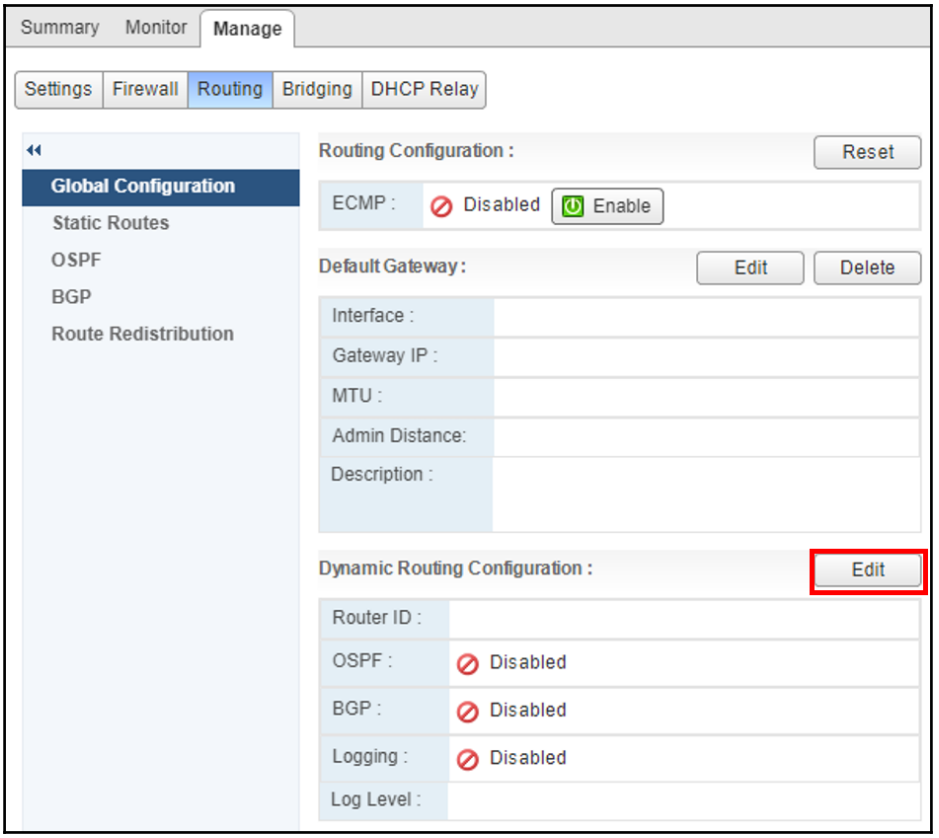

Add NSX Edge Appliance
Specify placement parameters for the NSX Edge appliance.
Cluster/Resource Pool:
RegionA01-COMP01
Datastore:
vsanDatastore
Host:
Folder:
Resource Reservation:
System Managed
CPU:
1000 MHz
Memory:
512 MB
OK
Cancel

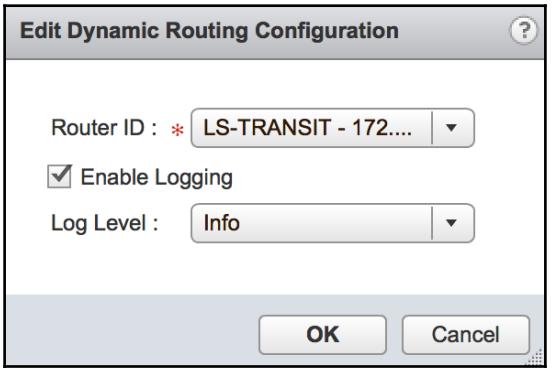

New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete
Configure deployment
Datacenter:
Datacenter
Appliance Size:
Compact
Large
X-Large
Quad Large
NSX Edge Appliances
Resource P...
Host
Datastore
Folder
CPU Reserv...
Memory Re...
RegionA...
vsanDat...
1000 MHz
512 MB
RegionA...
vsanDat...
1000 MHz
512 MB
Specifying a resource pool and datastore is mandatory for configuring the NSX Edge appliance.
Both the Edge Appliances are currently deployed on the same resources. It is recommended to deploy them on different resource pools, hosts and datastores.
Back
Next
Finish
Cancel

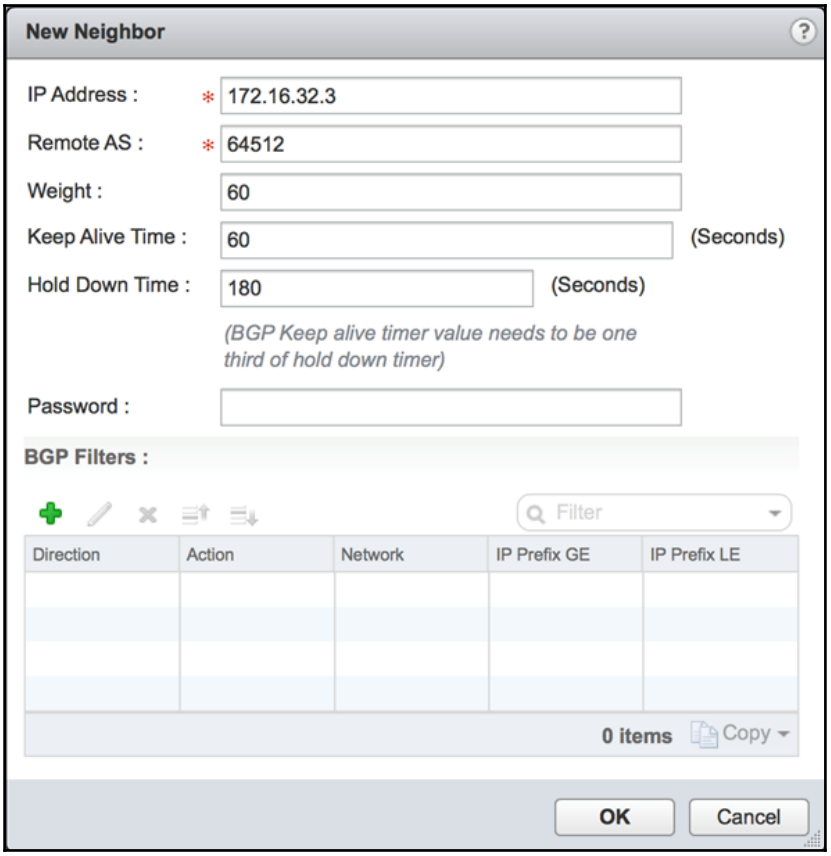

New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete
Configure interfaces
Configure interfaces of this NSX Edge
vNIC#
Name
IP Address
Subnet Prefix Length
Connected To
0
VM Network
10.0.0.160*
24
VM Network
1
LS-TRANSIT
172.16.32.1*
24
LS-TRANSIT
Back
Next
Finish
Cancel


New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete
Default gateway settings
Configure Default Gateway
vNIC:
VM Network
Gateway IP:
10.0.0.138
MTU:
1500
Admin Distance:
1
Back
Next
Finish
Cancel

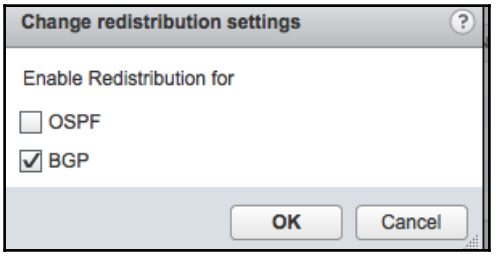

New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete
Firewall and HA
Configure Firewall default policy
Default Traffic Policy: Accept Deny
Logging: Enable Disable
Configure HA parameters
Configuring HA parameters is mandatory for HA to work.
vNIC: * LS-TRANSIT
Declare Dead Time: 15 (seconds)
Management IPs:
Management IPs must be in CIDR format with /30 subnet and must not overlap with any vnic subnets.
Back
Next
Finish
Cancel

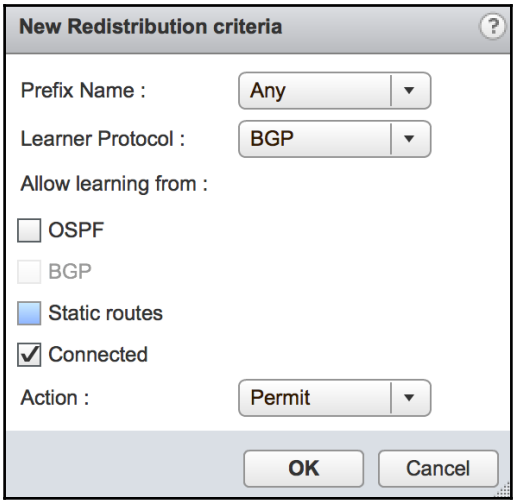

Summary
Monitor
Manage
Settings
Firewall
Routing
Bridging
DHCP Relay
Global Configuration
Static Routes
OSPF
BGP
Route Redistribution
Routing Configuration :
Reset
ECMP :
Disabled
Enable
Default Gateway :
Edit
Delete
Interface :
Gateway IP :
MTU :
Admin Distance:
Description :
Dynamic Routing Configuration :
Edit
Router ID :
OSPF :
Disabled
BGP :
Disabled
Logging :
Disabled
Log Level :

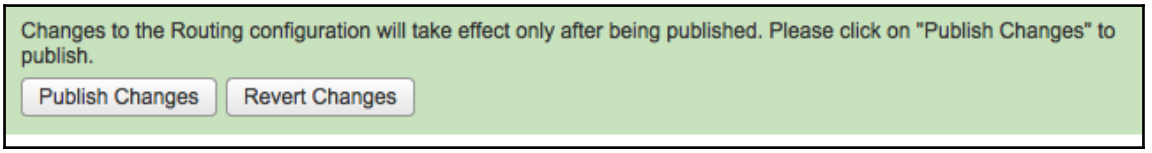

Edit Dynamic Routing Configuration
Router ID :
LS-TRANSIT - 172....
Enable Logging
Log Level :
Info
OK
Cancel

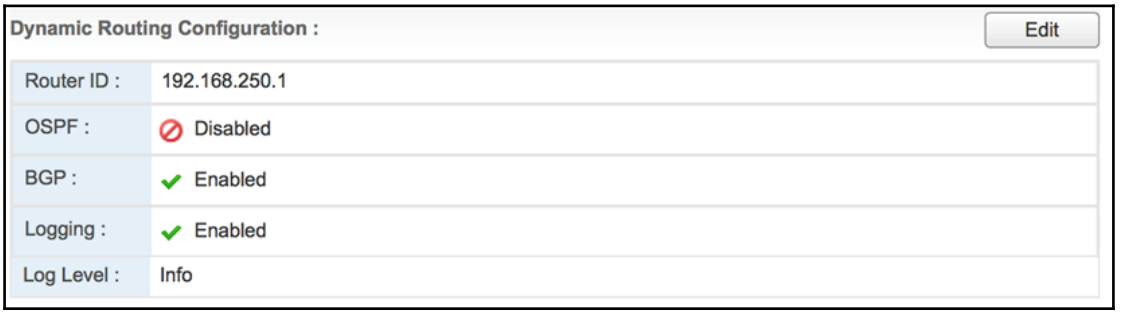

New Neighbor
IP Address :
172.16.32.3
Remote AS :
64512
Weight :
60
Keep Alive Time :
60
(Seconds)
Hold Down Time :
180
(Seconds)
(BGP Keep alive timer value needs to be one third of hold down timer)
Password :
BGP Filters :
Filter
Direction
Action
Network
IP Prefix GE
IP Prefix LE
0 items
Copy
OK
Cancel


Route Redistribution Status :
Edit
OSPF :
BGP :
IP Prefixes :

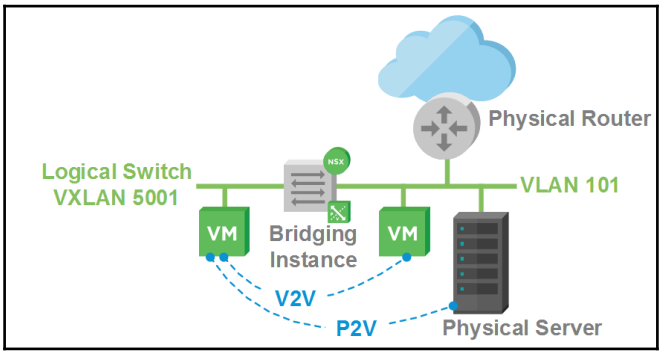

Change redistribution settings
Enable Redistribution for
OSPF
BGP
OK
Cancel

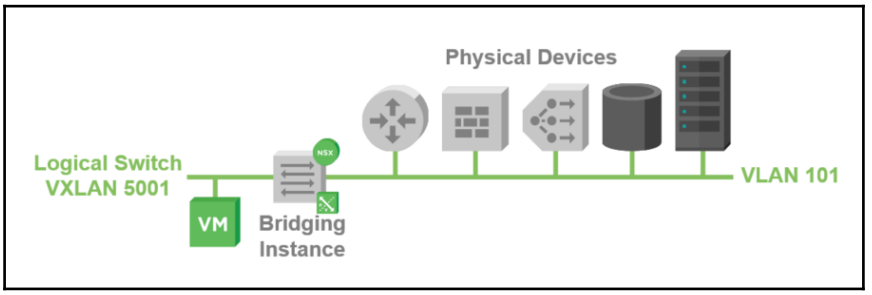

New Redistribution criteria
Prefix Name :
Any
Learner Protocol :
BGP
Allow learning from :
OSPF
BGP
Static routes
Connected
Action :
Permit
OK
Cancel

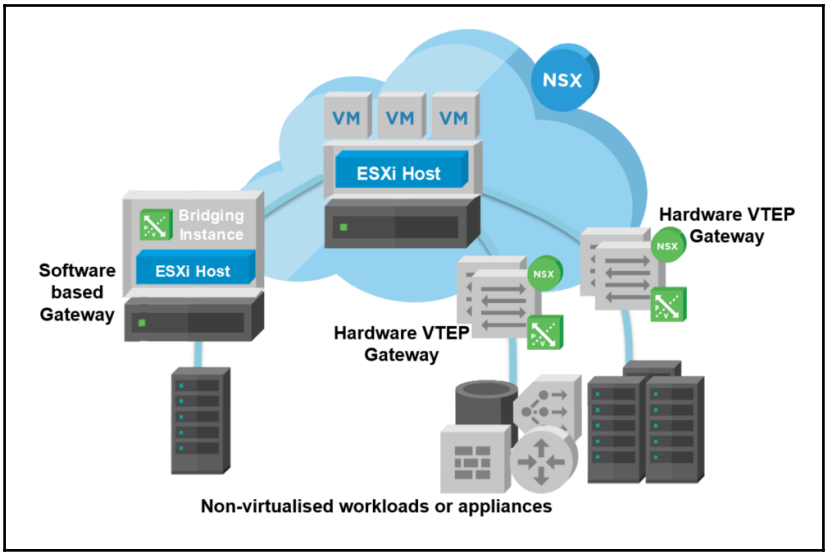

Changes to the Routing configuration will take effect only after being published. Please click on "Publish Changes" to publish.
Publish Changes
Revert Changes

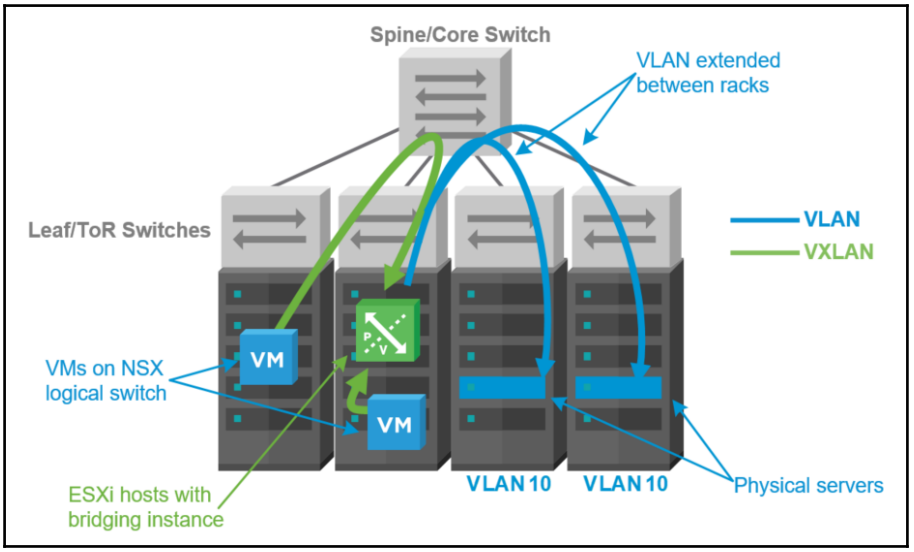

Dynamic Routing Configuration :
Edit
Router ID :
192.168.250.1
OSPF :
Disabled
BGP :
Enabled
Logging :
Enabled
Log Level :
Info

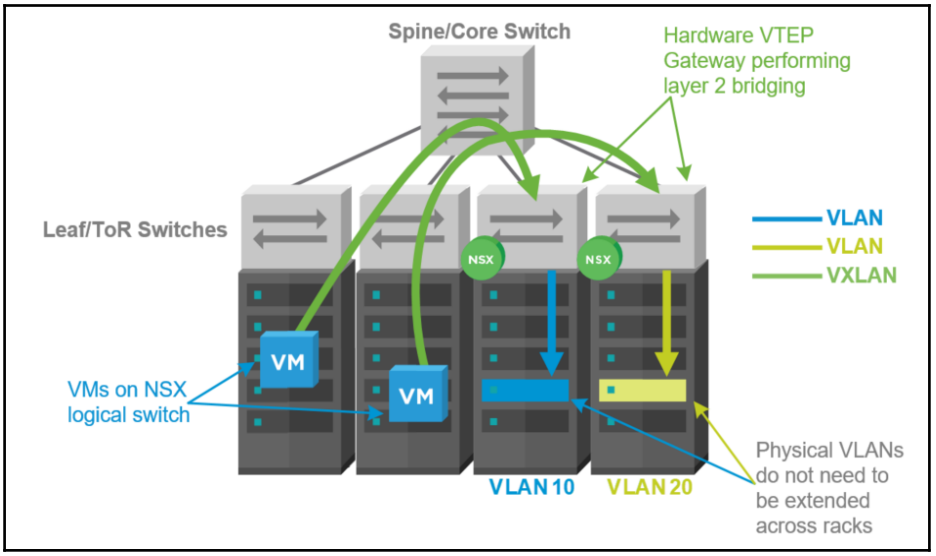
Chapter 04: Configuring VMware NSX Layer 2 Bridging

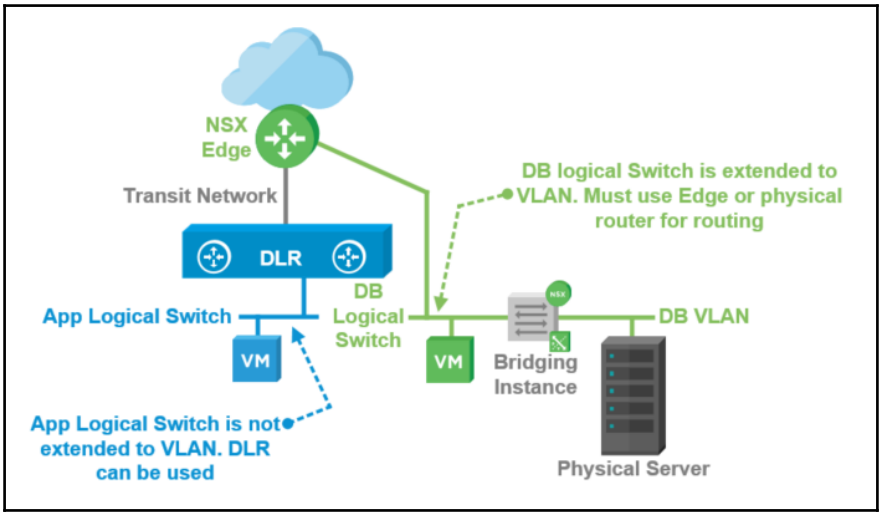


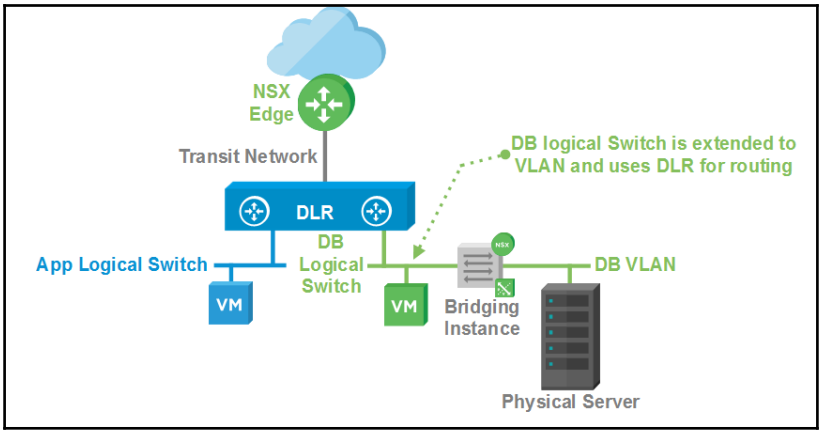


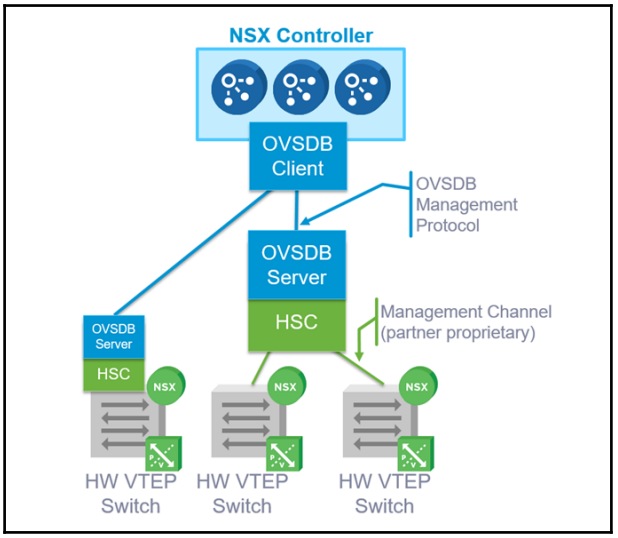

NSX
VM
VM
VM
ESXi Host
Bridging Instance
ESXi Host
Software based Gateway
Hardware VTEP Gateway
NSX
Hardware VTEP Gateway
NSX
Non-virtualised workloads or appliances

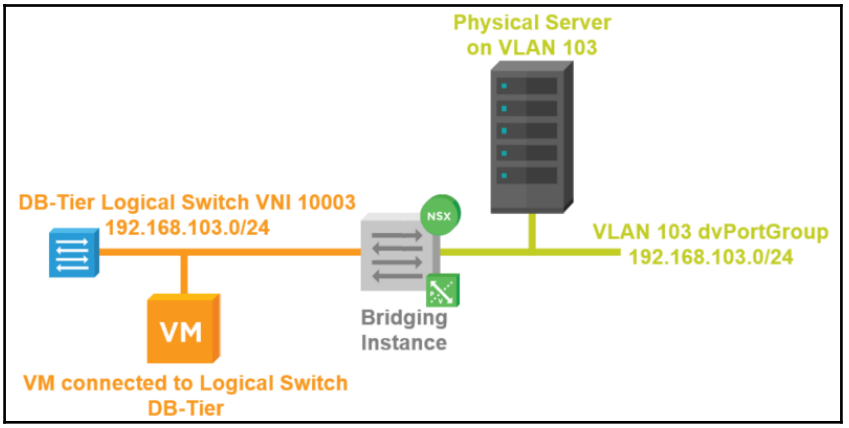

Spine/Core Switch
VLAN extended between racks
Leaf/ToR Switches
VLAN
VXLAN
VM
VMs on NSX logical switch
VM
ESXi hosts with bridging instance
VLAN 10
VLAN 10
Physical servers

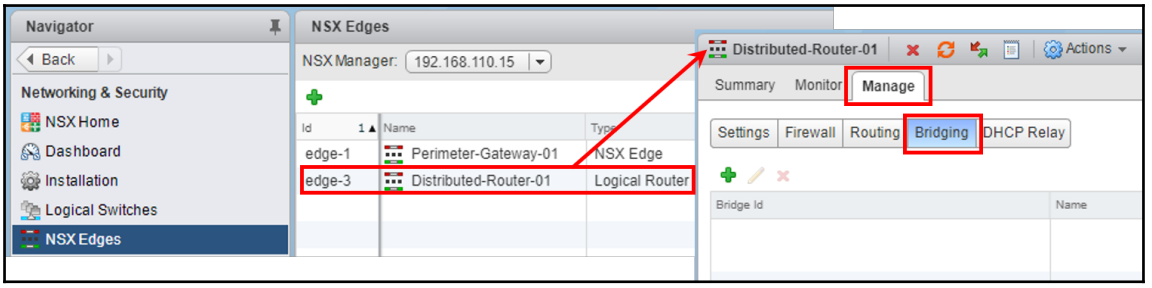

Spine/Core Switch
Hardware VTEP
Gateway performing
layer 2 bridging
Leaf/ToR Switches
VLAN
VLAN
VXLAN
NSX
NSX
VM
VM
VMs on NSX
logical switch
Physical VLANs
do not need to
be extended
across racks
VLAN 10
VLAN 20

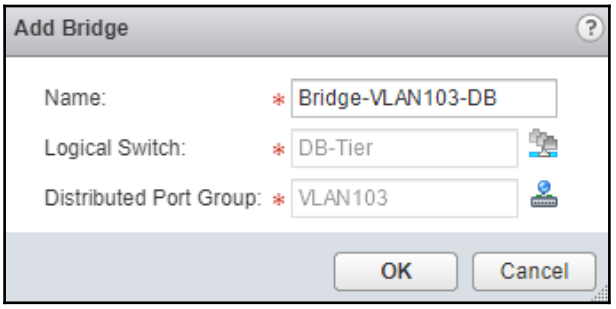

NSX
Edge
Transit Network
DLR
DB logical Switch is extended to
VLAN. Must use Edge or physical
router for routing
DB
Logical
Switch
App Logical Switch
DB VLAN
VM
VM
Bridging
Instance
App Logical Switch is not
extended to VLAN. DLR
can be used
Physical Server

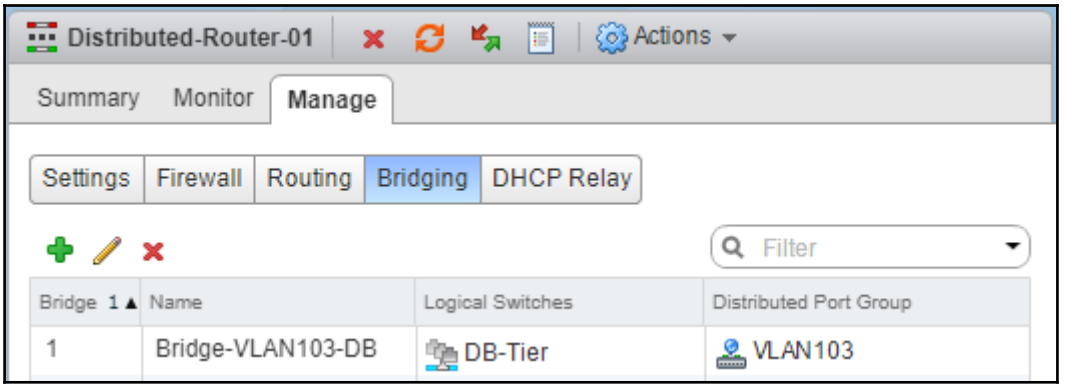

NSX
Edge
Transit Network
DB logical Switch is extended to
VLAN and uses DLR for routing
DLR
DB
Logical
Switch
App Logical Switch
DB VLAN
VM
VM
Bridging
Instance
Physical Server

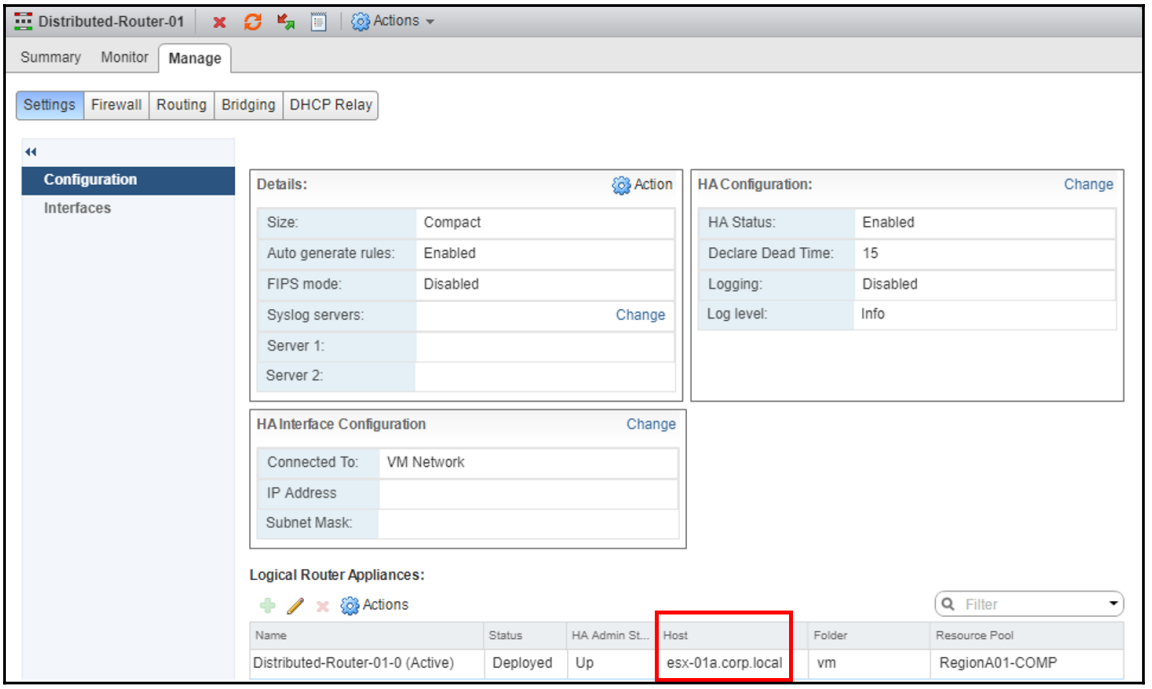

NSX Controller
OVSDB
Client
OVSDB
Management
Protocol
OVSDB
Server
HSC
Management Channel
(partner proprietary)
OVSDB
Server
HSC
NSX
NSX
NSX
HW VTEP
Switch
HW VTEP
Switch
HW VTEP
Switch

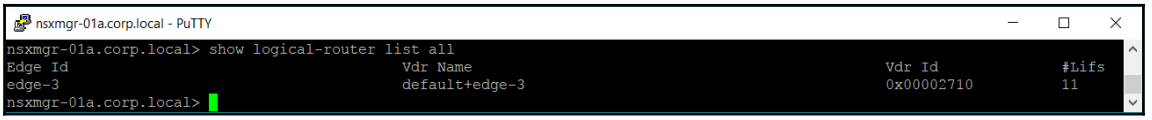

Physical Server
on VLAN 103
DB-Tier Logical Switch VNI 10003
192.168.103.0/24
NSX
VLAN 103 dvPortGroup
192.168.103.0/24
VM
Bridging
Instance
VM connected to Logical Switch
DB-Tier

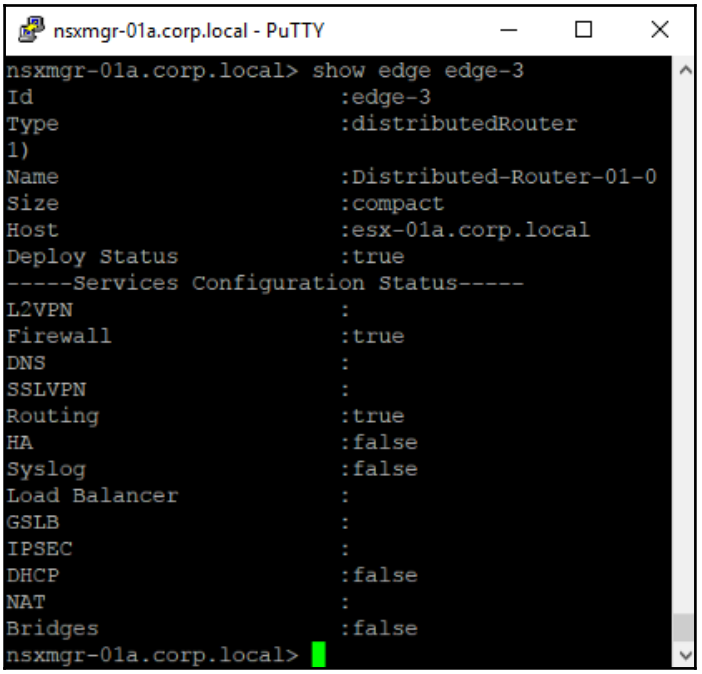

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
NSX Edges
NSX Manager:
192.168.110.15
Id
Name
Type
edge-1
Perimeter-Gateway-01
NSX Edge
edge-3
Distributed-Router-01
Logical Router
Distributed-Router-01
Actions
Summary
Monitor
Manage
Settings
Firewall
Routing
Bridging
DHCP Relay
Bridge Id
Name

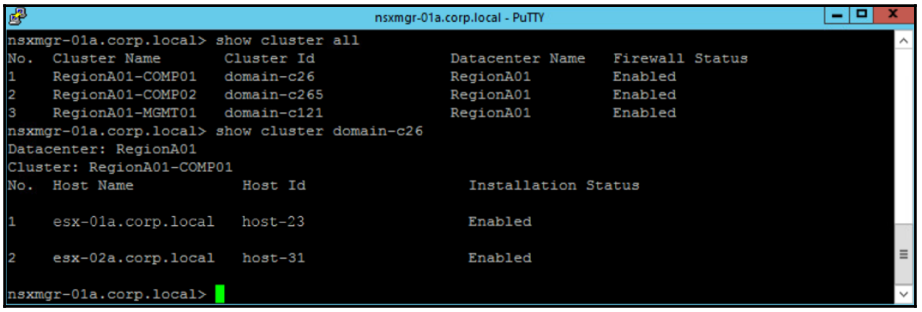

Add Bridge
Name:
Bridge-VLAN103-DB
Logical Switch:
DB-Tier
Distributed Port Group:
VLAN103
OK
Cancel

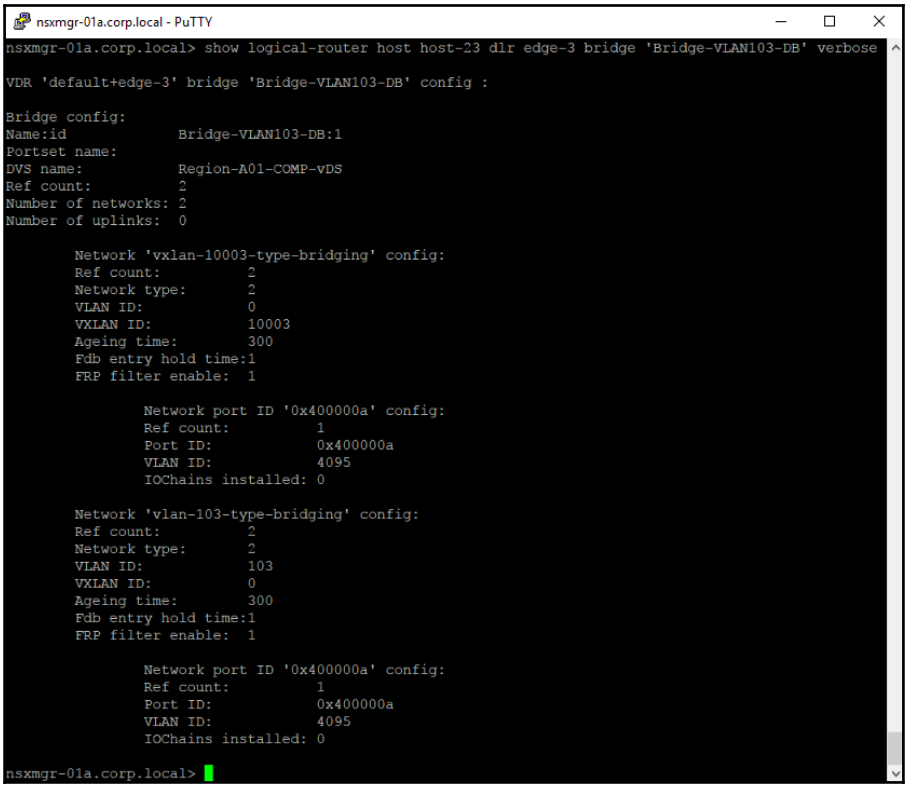

Distributed-Router-01
Actions
Summary
Monitor
Manage
Settings
Firewall
Routing
Bridging
DHCP Relay
Filter
Bridge 1
Name
Logical Switches
Distributed Port Group
1
Bridge-VLAN103-DB
DB-Tier
VLAN103

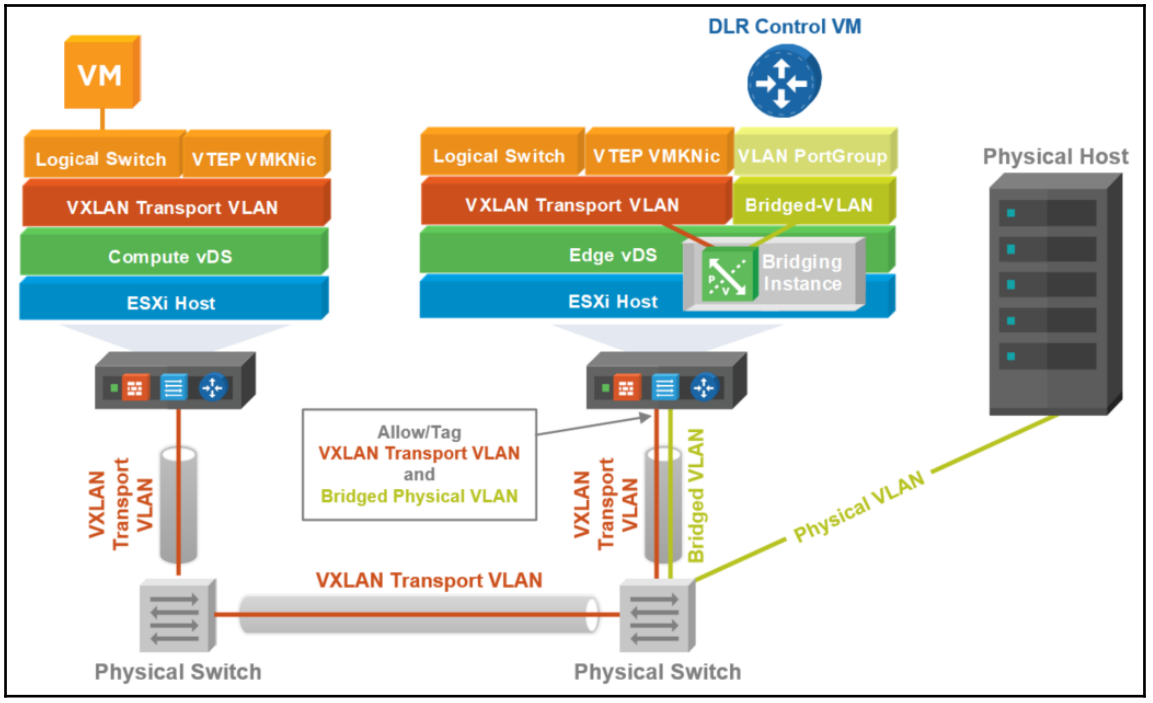

Distributed-Router-01
Actions
Summary
Monitor
Manage
Settings
Firewall
Routing
Bridging
DHCP Relay
Configuration
Interfaces
Details:
Action
Size:
Compact
Auto generate rules:
Enabled
FIPS mode:
Disabled
Syslog servers:
Change
Server 1:
Server 2:
HA Configuration:
Change
HA Status:
Enabled
Declare Dead Time:
15
Logging:
Disabled
Log level:
Info
HA Interface Configuration
Change
Connected To:
VM Network
IP Address
Subnet Mask:
Logical Router Appliances:
Actions
Filter
Name
Status
HA Admin St...
Host
Folder
Resource Pool
Distributed-Router-01-0 (Active)
Deployed
Up
esx-01a.corp.local
vm
RegionA01-COMP

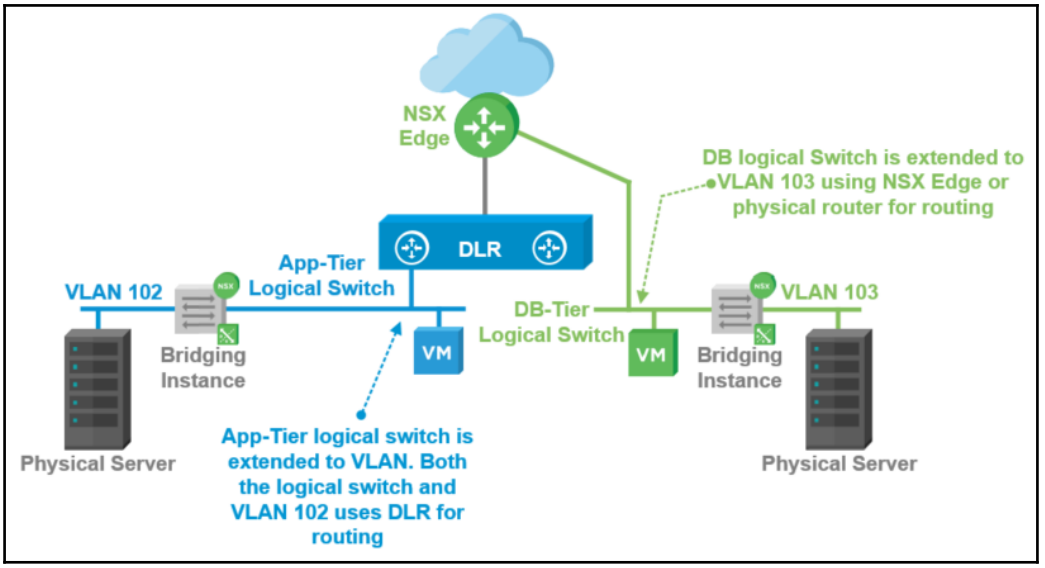

nsxmgr-01a.corp.local - PuTTY
nsxmgr-01a.corp.local> show logical-router list all
Edge Id
Vdr Name
Vdr Id
#Lifs
edge-3
default+edge-3
0x00002710
11
nsxmgr-01a.corp.local>

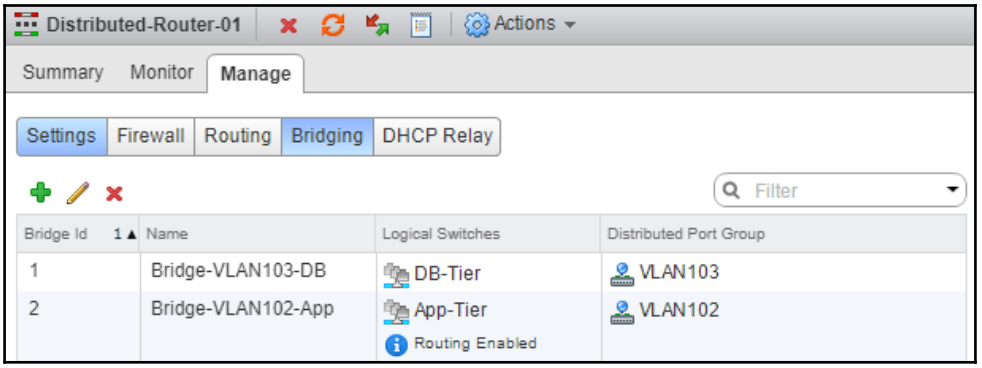

nsxmgr-01a.corp.local - PuTTY
nsxmgr-01a.corp.local> show edge edge-3
Id :edge-3
Type :distributedRouter
1)
Name :Distributed-Router-01-0
Size :compact
Host :esx-01a.corp.local
Deploy Status :true
-----Services Configuration Status-----
L2VPN :
Firewall :true
DNS :
SSLVPN :
Routing :true
HA :false
Syslog :false
Load Balancer :
GSLB :
IPSEC :
DHCP :false
NAT :
Bridges :false
nsxmgr-01a.corp.local>

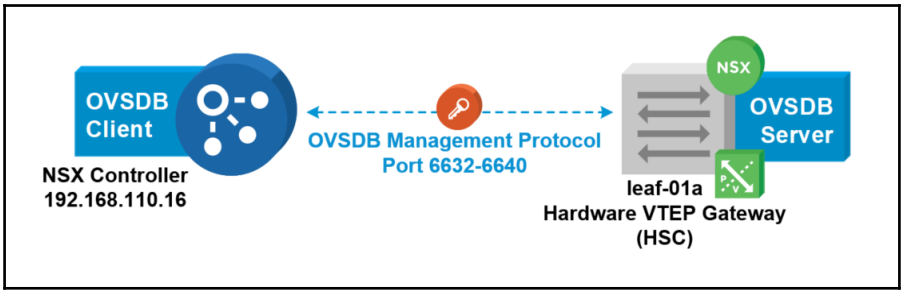

nsxmgr-01a.corp.local - PuTTY
nsxmgr-01a.corp.local> show cluster all
No. Cluster Name Cluster Id Datacenter Name Firewall Status
1 RegionA01-COMP01 domain-c26 RegionA01 Enabled
2 RegionA01-COMP02 domain-c265 RegionA01 Enabled
3 RegionA01-MGMT01 domain-c121 RegionA01 Enabled
nsxmgr-01a.corp.local> show cluster domain-c26
Datacenter: RegionA01
Cluster: RegionA01-COMP01
No. Host Name Host Id Installation Status
1 esx-01a.corp.local host-23 Enabled
2 esx-02a.corp.local host-31 Enabled
nsxmgr-01a.corp.local>

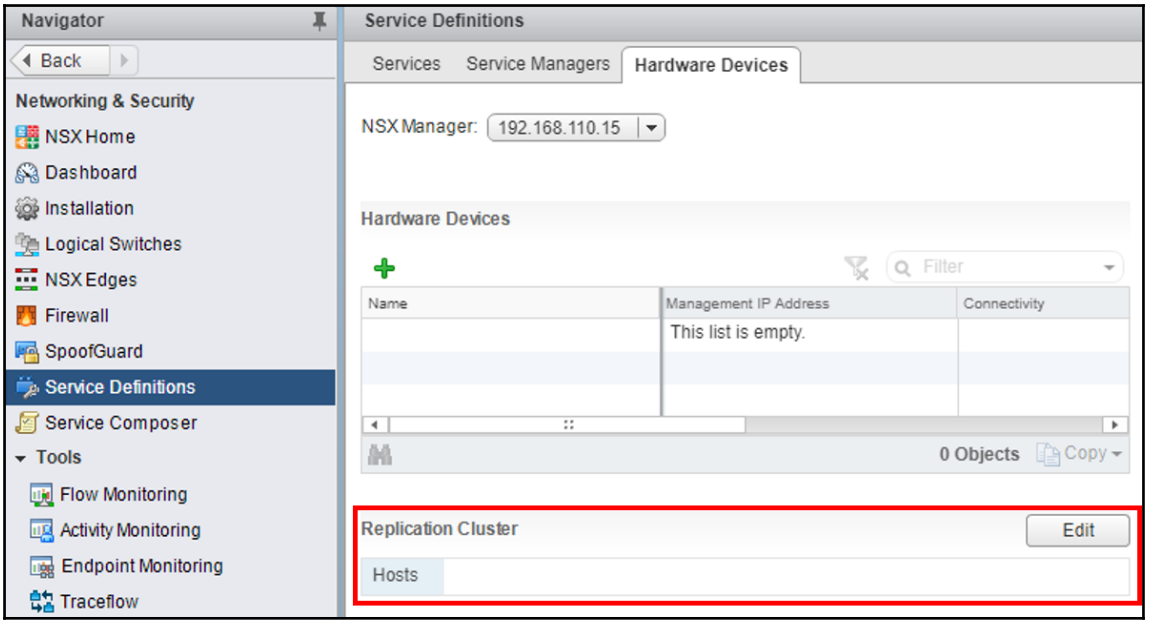

nsxmgr-01a.corp.local - PuTTY
nsxmgr-01a.corp.local> show logical-router host host-23 dlr edge-3 bridge 'Bridge-VLAN103-DB' verbose
VDR 'default+edge-3' bridge 'Bridge-VLAN103-DB' config :
Bridge config:
Name:id Bridge-VLAN103-DB:1
Portset name:
DVS name: Region-A01-COMP-vDS
Ref count: 2
Number of networks: 2
Number of uplinks: 0
Network 'vxlan-10003-type-bridging' config:
Ref count: 2
Network type: 2
VLAN ID: 0
VXLAN ID: 10003
Ageing time: 300
Fdb entry hold time:1
FRP filter enable: 1
Network port ID '0x400000a' config:
Ref count: 1
Port ID: 0x400000a
VLAN ID: 4095
IOChains installed: 0
Network 'vlan-103-type-bridging' config:
Ref count: 2
Network type: 2
VLAN ID: 103
VXLAN ID: 0
Ageing time: 300
Fdb entry hold time:1
FRP filter enable: 1
Network port ID '0x400000a' config:
Ref count: 1
Port ID: 0x400000a
VLAN ID: 4095
IOChains installed: 0
nsxmgr-01a.corp.local>

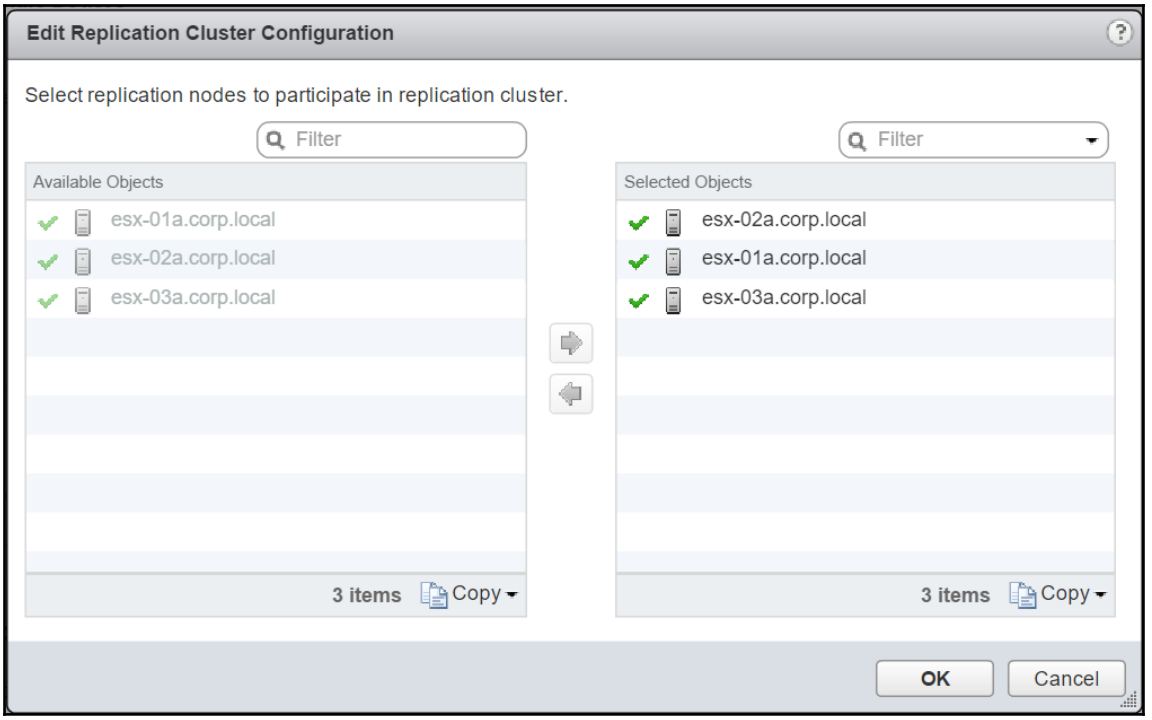

DLR Control VM
VM
Logical Switch
VTEP VMKNic
VXLAN Transport VLAN
Compute vDS
ESXi Host
Logical Switch
VTEP VMKNic
VLAN PortGroup
VXLAN Transport VLAN
Bridged-VLAN
Edge vDS
Bridging Instance
ESXi Host
Physical Host
Allow/Tag
VXLAN Transport VLAN
and
Bridged Physical VLAN
VXLAN Transport VLAN
VXLAN Transport VLAN
Bridged VLAN
Physical VLAN
VXLAN Transport VLAN
Physical Switch
Physical Switch


NSX Edge
DB logical Switch is extended to VLAN 103 using NSX Edge or physical router for routing
DLR
App-Tier Logical Switch
VLAN 102
Bridging Instance
VM
DB-Tier Logical Switch
VM
Bridging Instance
VLAN 103
Physical Server
App-Tier logical switch is extended to VLAN. Both the logical switch and VLAN 102 uses DLR for routing
Physical Server


Distributed-Router-01
Actions
Summary
Monitor
Manage
Settings
Firewall
Routing
Bridging
DHCP Relay
Filter
Bridge Id
Name
Logical Switches
Distributed Port Group
1
Bridge-VLAN103-DB
DB-Tier
VLAN103
2
Bridge-VLAN102-App
App-Tier
Routing Enabled
VLAN102

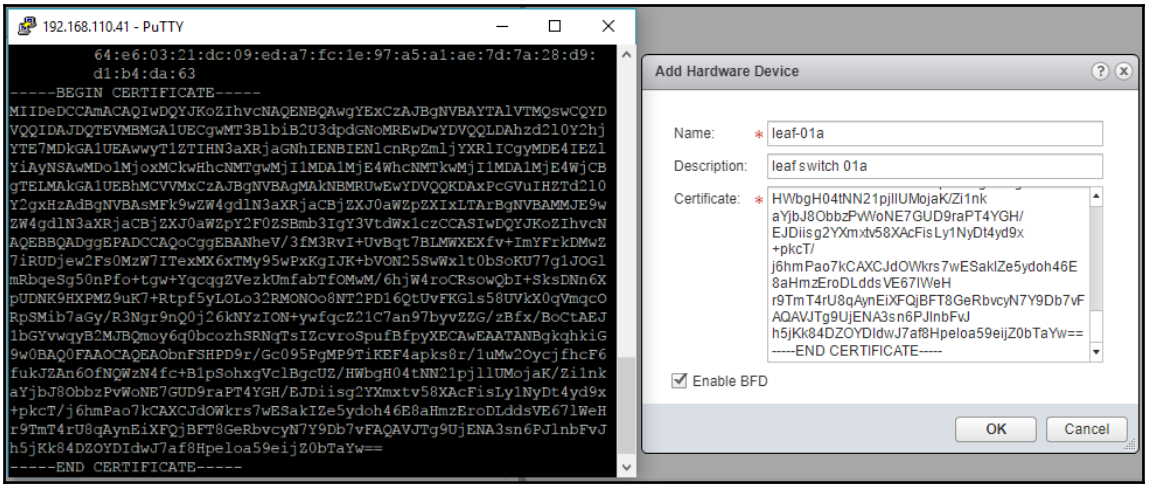

OVSDB Client
NSX Controller
192.168.110.16
OVSDB Management Protocol
Port 6632-6640
NSX
OVSDB Server
leaf-01a
Hardware VTEP Gateway
(HSC)

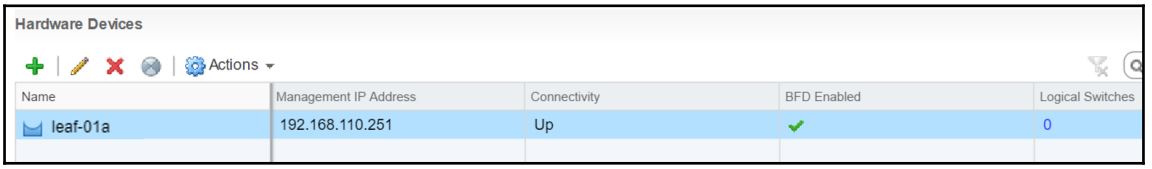

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Tools
Flow Monitoring
Activity Monitoring
Endpoint Monitoring
Traceflow
Service Definitions
Services
Service Managers
Hardware Devices
NSX Manager:
192.168.110.15
Hardware Devices
Filter
Name
Management IP Address
Connectivity
This list is empty.
0 Objects
Copy
Replication Cluster
Edit
Hosts

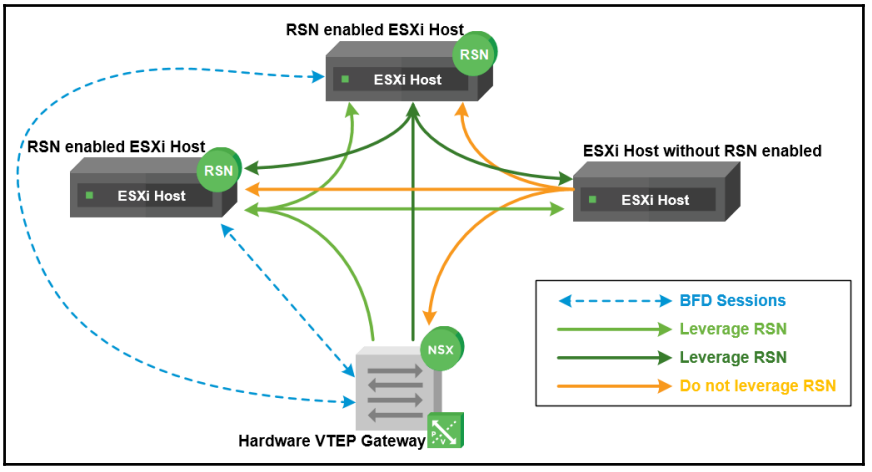

Edit Replication Cluster Configuration
Select replication nodes to participate in replication cluster.
Filter
Available Objects
esx-01a.corp.local
esx-02a.corp.local
esx-03a.corp.local
3 items
Copy
Filter
Selected Objects
esx-02a.corp.local
esx-01a.corp.local
esx-03a.corp.local
3 items
Copy
OK
Cancel

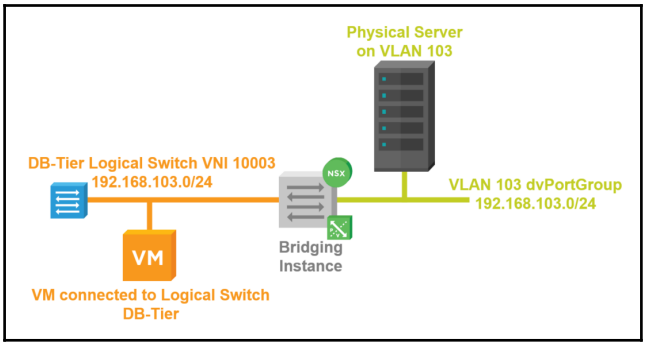

Replication Cluster
Edit
Hosts
esx-02a.corp.local
esx-01a.corp.local
esx-03a.corp.local
BFD Configuration
Edit
Status
Enabled
Probe interval
300 ms

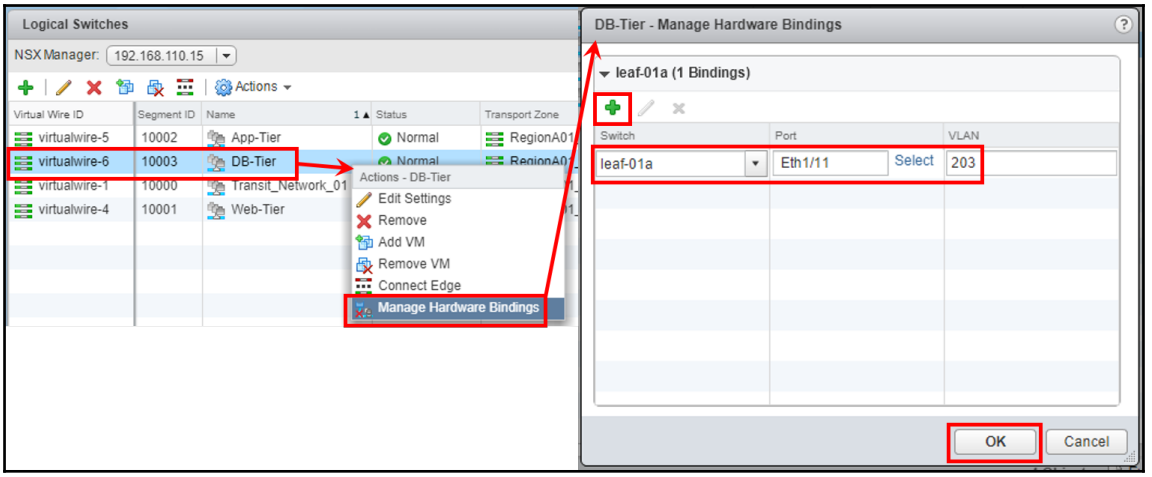

Replication Cluster
Edit
Hosts
esx-02a.corp.local
esx-01a.corp.local
esx-03a.corp.local
BFD Configuration
Edit
Status
Enabled
Probe interval
300 ms


192.168.110.41 - PuTTY
64:e6:03:21:dc:09:ed:a7:fc:1e:97:a5:a1:ae:7d:7a:28:d9:
d1:b4:da:63
-----BEGIN CERTIFICATE-----
MIIDeDCCAmACAQIwDQYJKoZIhvcNAQENBQAwgYExCzAJBgNVBAYTAlVTMQswCQYD
VQQIDAJDQTEVMBMGA1UECgwMT3BlbiB2U3dpdGNoMREwDwYDVQQLDAhzd2l0Y2hj
YTE7MDkGA1UEAwwyT1ZTIHN3aXRjaGNhIENBIENlcnRpZmljYXRlICgyMDE4IEZl
YiAyNSAwMDo1MjoxMCkwHhcNMTgwMjI1MDA1MjE4WhcNMTkwMjI1MDA1MjE4WjCB
gTELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAkNBMRUwEwYDVQQKDAxPcGVuIHZTd2l0
Y2gxHzAdBgNVBAsMFk9wZW4gdlN3aXRjaCBjZXJ0aWZpZXIxLTArBgNVBAMMJE9w
ZW4gdlN3aXRjaCBjZXJ0aWZpY2F0ZSBmb3IgY3VtdWx1czCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBANheV/3fM3RvI+UvBqt7BLMWXEXfv+ImYFrkDMwZ
7iRUDjew2Fs0MzW7ITexMX6xTMy95wPxKgIJK+bVON25SwWxlt0bSoKU77g1JOGl
mRbqeSg50nPfo+tgw+YqcqgZVezkUmfabTfOMwM/6hjW4roCRsowQbI+SksDNn6X
pUDNK9HXPMZ9uK7+Rtpf5yLOLo32RMONOo8NT2PD16QtUvFKGls58UVkX0qVmqcO
RpSMib7aGy/R3Ngr9nQ0j26kNYzION+ywfqcZ21C7an97byvZZG/zBfx/BoCtAEJ
lbGYvwqyB2MJBQmoy6q0bcozhSRNqTsIZcvroSpufBfpyXECAwEAATANBgkqhkiG
9w0BAQ0FAAOCAQEAObnFSHPD9r/Gc095PgMP9TiKEF4apks8r/1uMw2OycjfhcF6
fukJZAn6OfNQWzN4fc+B1pSohxgVclBgcUZ/HWbgH04tNN21pjllUMojaK/Zi1nk
aYjbJ8ObbzPvWoNE7GUD9raPT4YGH/EJDiisg2YXmxtv58XAcFisLylNyDt4yd9x
+pkcT/j6hmPao7kCAXCJdOWkrs7wESakIZe5ydoh46E8aHmzEroDLddsVE67lWeH
r9TmT4rU8qAynEiXFQjBFT8GeRbvcyN7Y9Db7vFAQAVJTg9UjENA3sn6PJlnbFvJ
h5jKk84DZOYDIdwJ7af8Hpeloa59eijZ0bTaYw==
-----END CERTIFICATE-----
Add Hardware Device
Name:
leaf-01a
Description:
leaf switch 01a
Certificate:
HWbgH04tNN21pjllUMojaK/Zi1nk
aYjbJ8ObbzPvWoNE7GUD9raPT4YGH/
EJDiisg2YXmxtv58XAcFisLy1NyDt4yd9x
+pkcT/
j6hmPao7kCAXCJdOWkrs7wESakIZe5ydoh46E
8aHmzEroDLddsVE67lWeH
r9TmT4rU8qAynEiXFQjBFT8GeRbvcyN7Y9Db7vF
AQAVJTg9UjENA3sn6PJlnbFvJ
h5jKk84DZOYDIdwJ7af8Hpeloa59eijZ0bTaYw==
-----END CERTIFICATE-----
Enable BFD
OK
Cancel

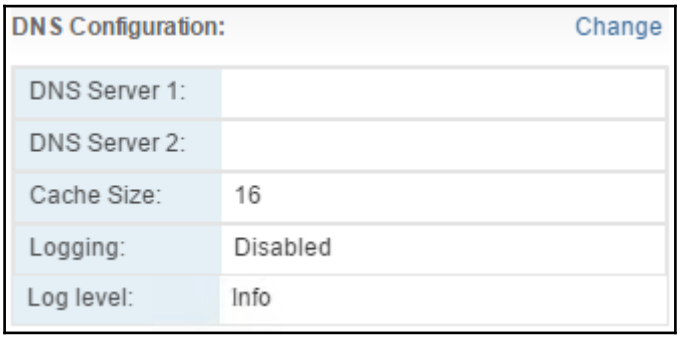

Hardware Devices
Actions
Name
Management IP Address
Connectivity
BFD Enabled
Logical Switches
leaf-01a
192.168.110.251
Up
0

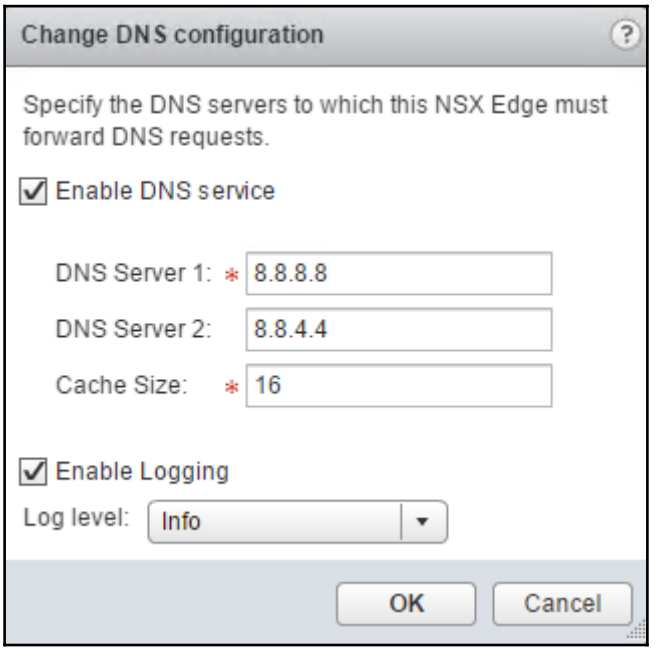

RSN enabled ESXi Host
RSN
ESXi Host
RSN enabled ESXi Host
RSN
ESXi Host
ESXi Host without RSN enabled
ESXi Host
NSX
Hardware VTEP Gateway
BFD Sessions
Leverage RSN
Leverage RSN
Do not leverage RSN


Physical Server
on VLAN 103
DB-Tier Logical Switch VNI 10003
192.168.103.0/24
VLAN 103 dvPortGroup
192.168.103.0/24
NSX
VM
Bridging
Instance
VM connected to Logical Switch
DB-Tier

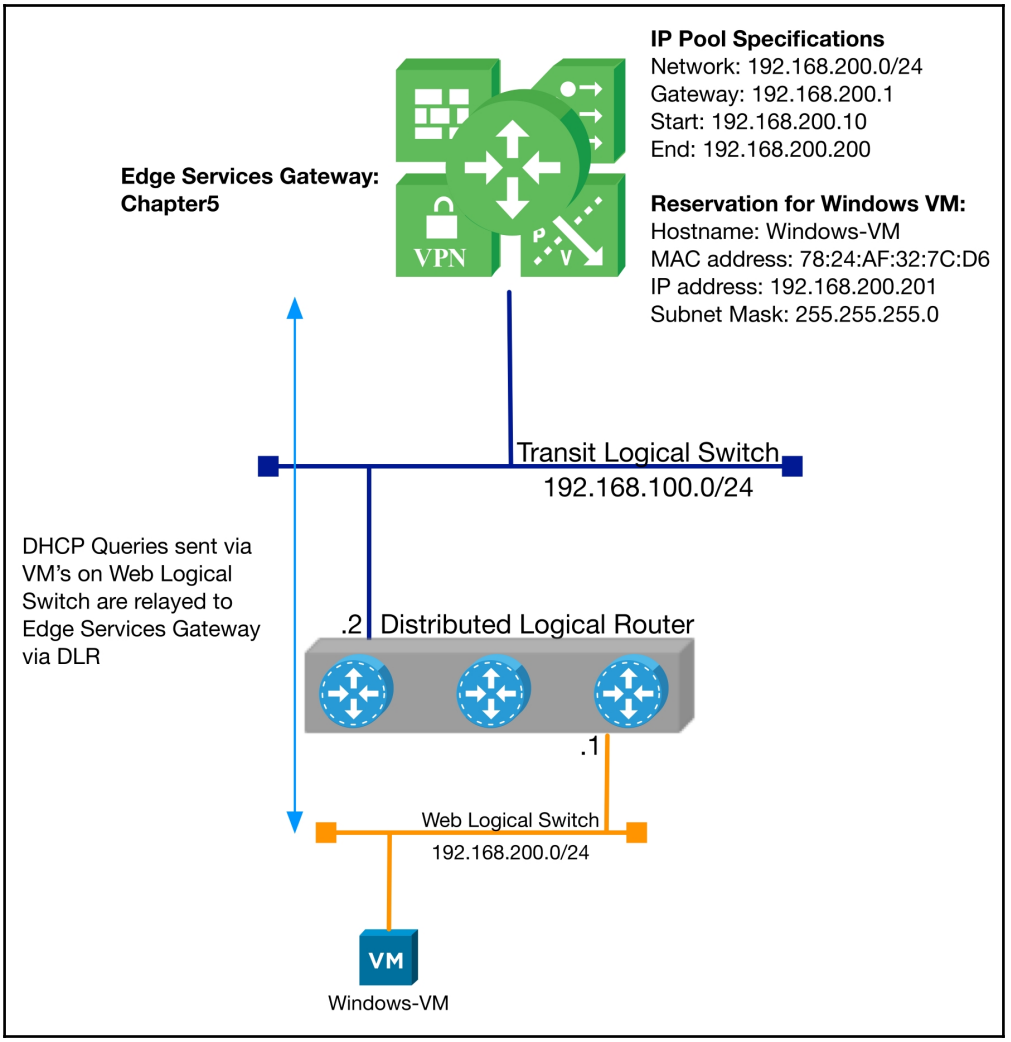

Logical Switches
NSX Manager: 192.168.110.15
Actions
Virtual Wire ID
Segment ID
Name
Status
Transport Zone
virtualwire-5
10002
App-Tier
Normal
RegionA01
virtualwire-6
10003
DB-Tier
virtualwire-1
10000
Transit_Network_01
virtualwire-4
10001
Web-Tier
Actions - DB-Tier
Edit Settings
Remove
Add VM
Remove VM
Connect Edge
Manage Hardware Bindings
DB-Tier - Manage Hardware Bindings
leaf-01a (1 Bindings)
Switch
Port
VLAN
leaf-01a
Eth1/11
Select
203
OK
Cancel

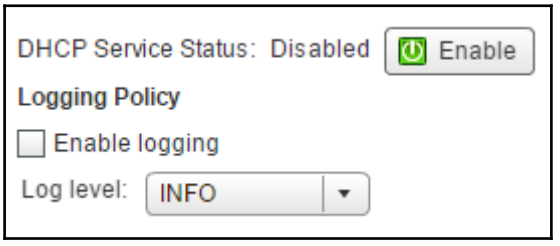
Chapter 05: Configuring VMware NSX Edge Services Gateway

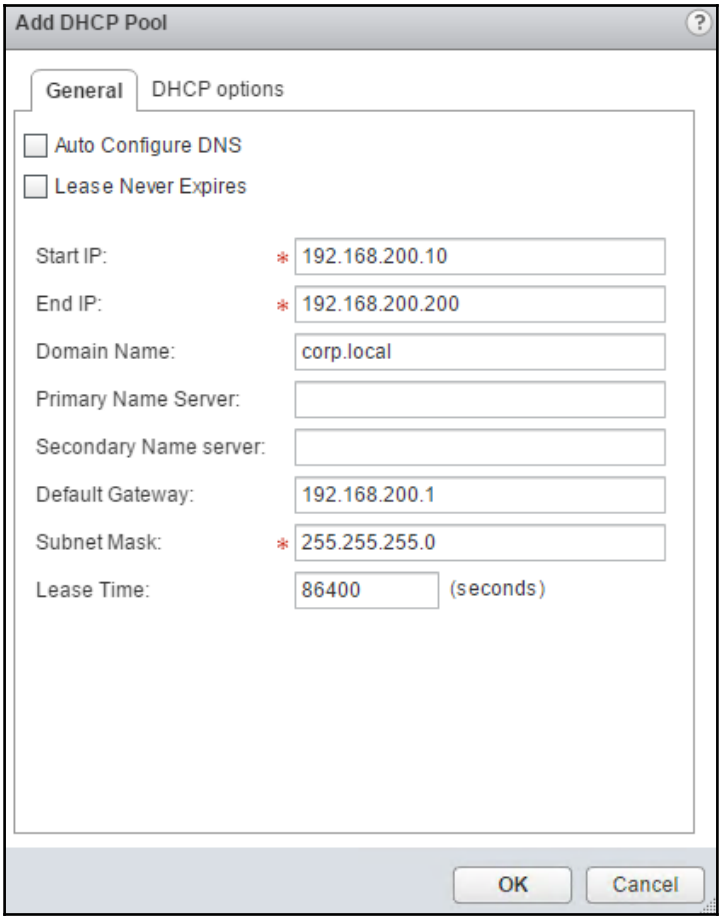


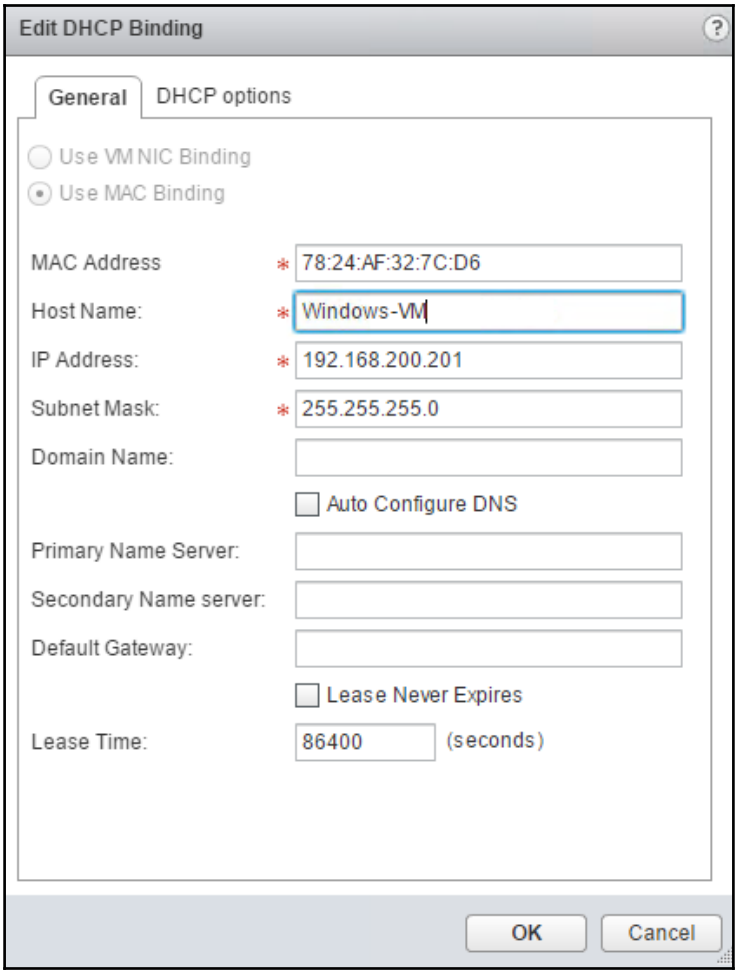


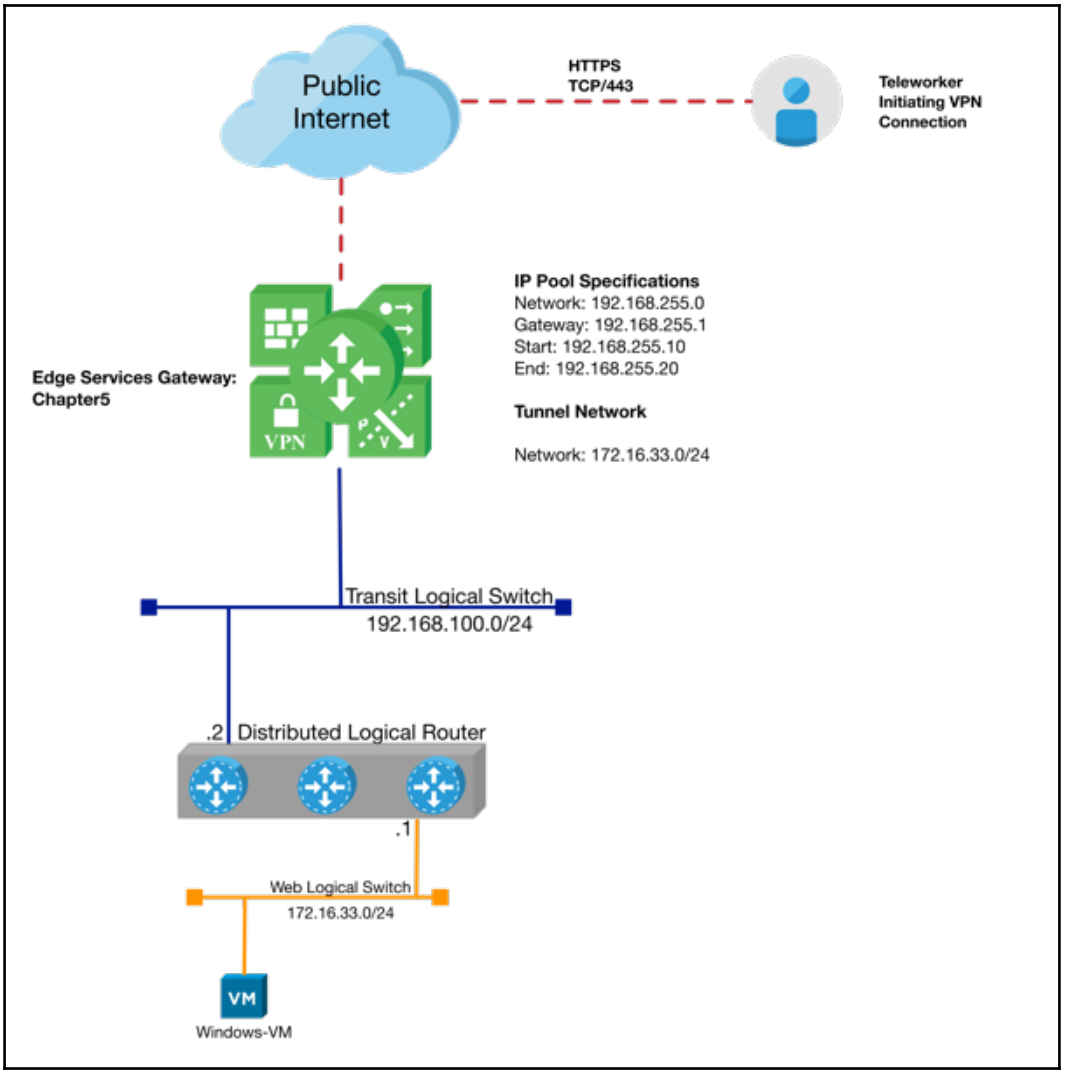
```
Chapter5-0> show service-monitor summary
The Monit daemon 5.13 uptime: 10m

Process 'rsync'                         Not monitored
Process 'openswan'                      Not monitored
Process 'haproxy'                       Not monitored
Process 'nrpe'                          Not monitored
Process 'nginx'                         Not monitored
Process 'rsyncInotify'                  Not monitored
Process 'conntrackd'                    Not monitored
Process 'l2vpn'                         Not monitored
Process 'msngr'                         Not monitored
Process 'sslvpn'                        Not monitored
Process 'ssh'                           Running
Process 'bind9'                         Running
Process 'syslog-ng'                     Running
Process 'dhcpd'                         Not monitored
Process 'nagios'                        Not monitored
Process 'dhcprelay'                     Not monitored
Process 'pound'                         Not monitored
```

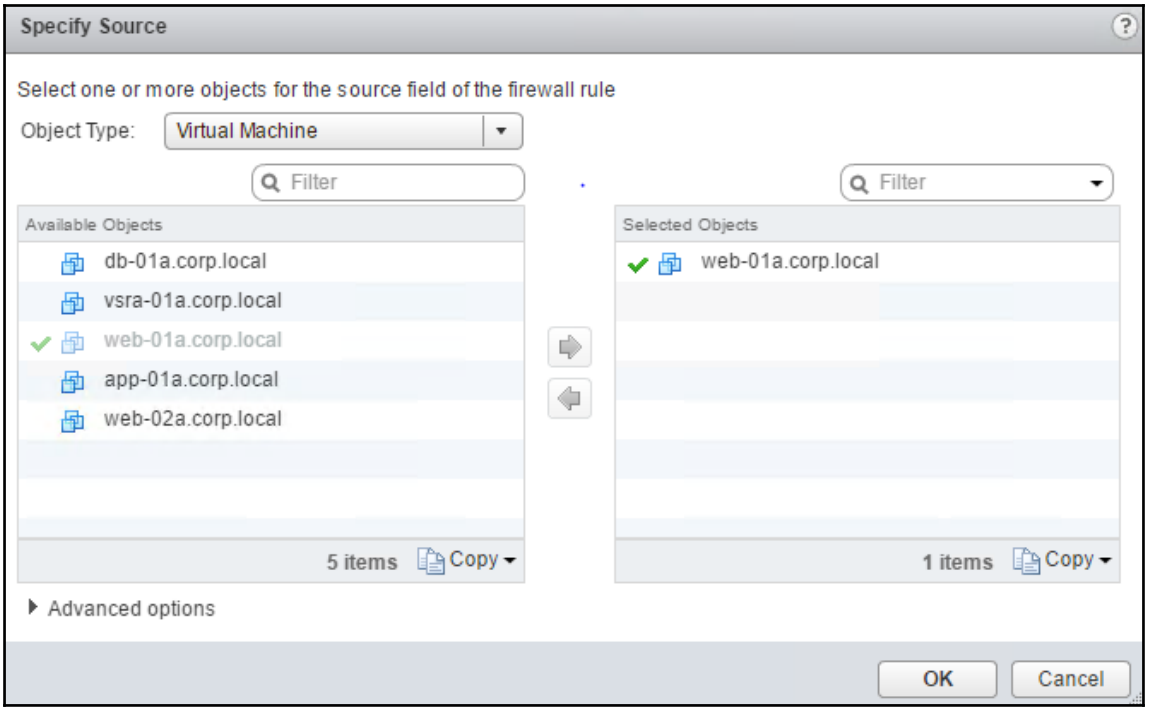

IP Pool Specifications
Network: 192.168.200.0/24
Gateway: 192.168.200.1
Start: 192.168.200.10
End: 192.168.200.200
Reservation for Windows VM:
Hostname: Windows-VM
MAC address: 78:24:AF:32:7C:D6
IP address: 192.168.200.201
Subnet Mask: 255.255.255.0
Edge Services Gateway:
Chapter5
VPN
Transit Logical Switch
192.168.100.0/24
DHCP Queries sent via VM's on Web Logical Switch are relayed to Edge Services Gateway via DLR
.2
Distributed Logical Router
.1
Web Logical Switch
192.168.200.0/24
VM
Windows-VM

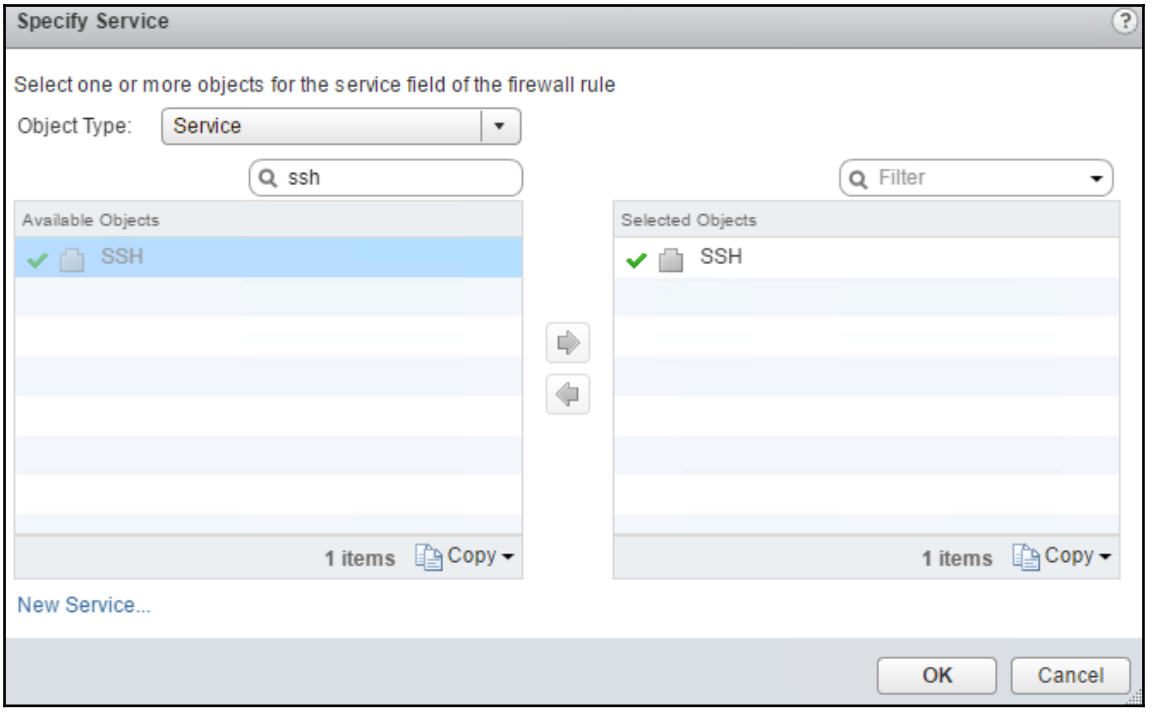

DHCP Service Status: Disabled
Enable
Logging Policy
Enable logging
Log level:
INFO

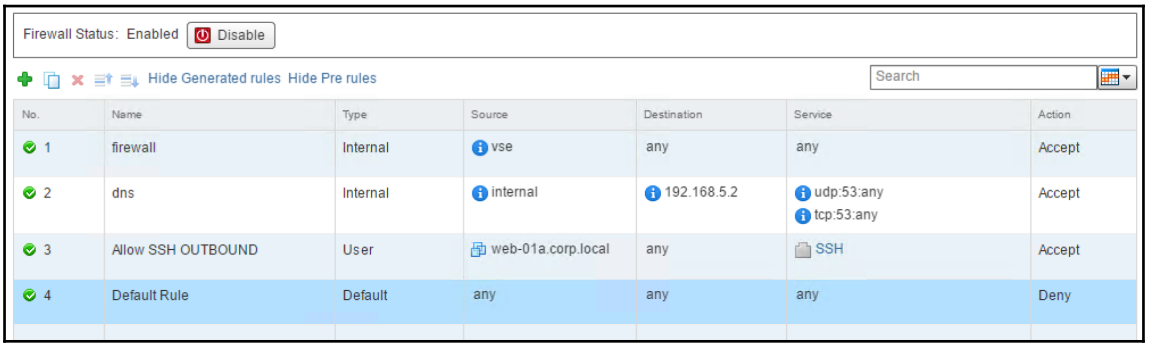

Add DHCP Pool
General
DHCP options
Auto Configure DNS
Lease Never Expires
Start IP:
192.168.200.10
End IP:
192.168.200.200
Domain Name:
corp.local
Primary Name Server:
Secondary Name server:
Default Gateway:
192.168.200.1
Subnet Mask:
255.255.255.0
Lease Time:
86400
(seconds)
OK
Cancel

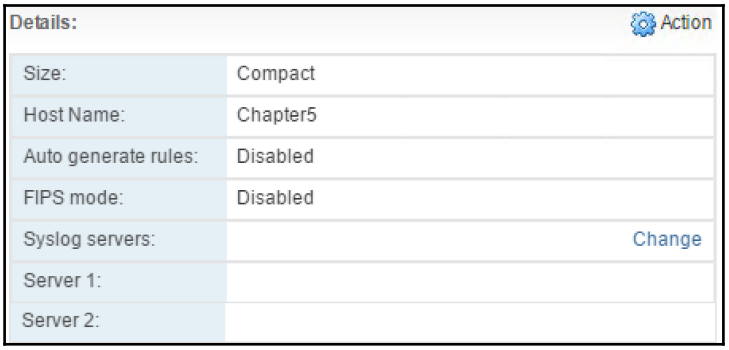

Edit DHCP Binding
General
DHCP options
Use VM NIC Binding
Use MAC Binding
MAC Address
78:24:AF:32:7C:D6
Host Name:
Windows-VM
IP Address:
192.168.200.201
Subnet Mask:
255.255.255.0
Domain Name:
Auto Configure DNS
Primary Name Server:
Secondary Name server:
Default Gateway:
Lease Never Expires
Lease Time:
86400
(seconds)
OK
Cancel

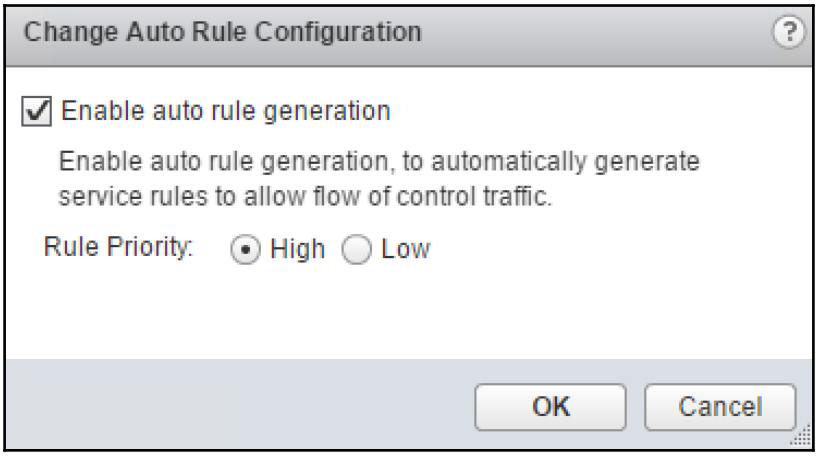

Public Internet
HTTPS
TCP/443
Teleworker Initiating VPN Connection
IP Pool Specifications
Network: 192.168.255.0
Gateway: 192.168.255.1
Start: 192.168.255.10
End: 192.168.255.20
Tunnel Network
Network: 172.16.33.0/24
Edge Services Gateway:
Chapter5
VPN
Transit Logical Switch
192.168.100.0/24
.2 Distributed Logical Router
.1
Web Logical Switch
172.16.33.0/24
VM
Windows-VM

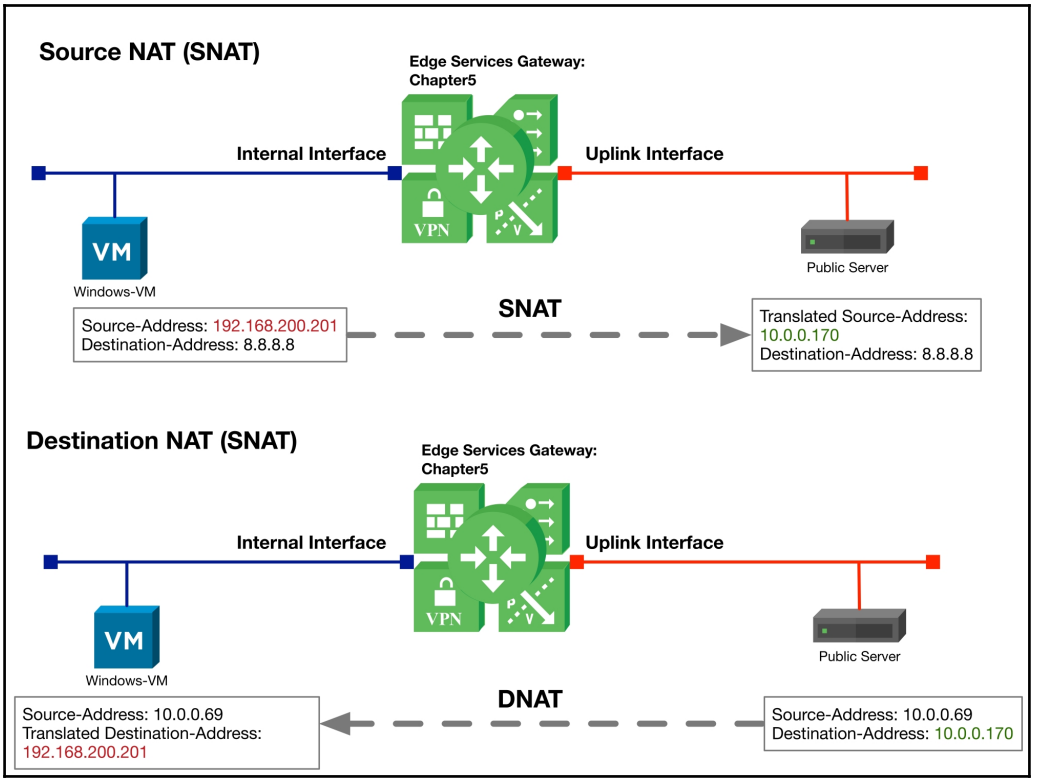

Specify Source
Select one or more objects for the source field of the firewall rule
Object Type:
Virtual Machine
Filter
Filter
Available Objects
db-01a.corp.local
vsra-01a.corp.local
web-01a.corp.local
app-01a.corp.local
web-02a.corp.local
5 items
Copy
Selected Objects
web-01a.corp.local
1 items
Copy
Advanced options
OK
Cancel

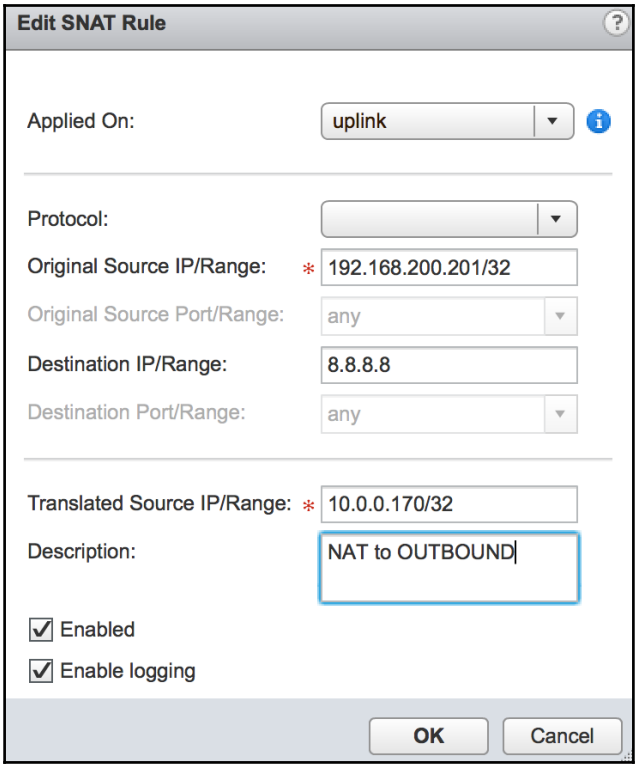

Specify Service
Select one or more objects for the service field of the firewall rule
Object Type:
Service
ssh
Filter
Available Objects
SSH
Selected Objects
SSH
1 items
Copy
1 items
Copy
New Service...
OK
Cancel


Firewall Status: Enabled
Disable
Hide Generated rules
Hide Pre rules
Search
No.
Name
Type
Source
Destination
Service
Action
1
firewall
Internal
vse
any
any
Accept
2
dns
Internal
internal
192.168.5.2
udp:53:any
tcp:53:any
Accept
3
Allow SSH OUTBOUND
User
web-01a.corp.local
any
SSH
Accept
4
Default Rule
Default
any
any
any
Deny

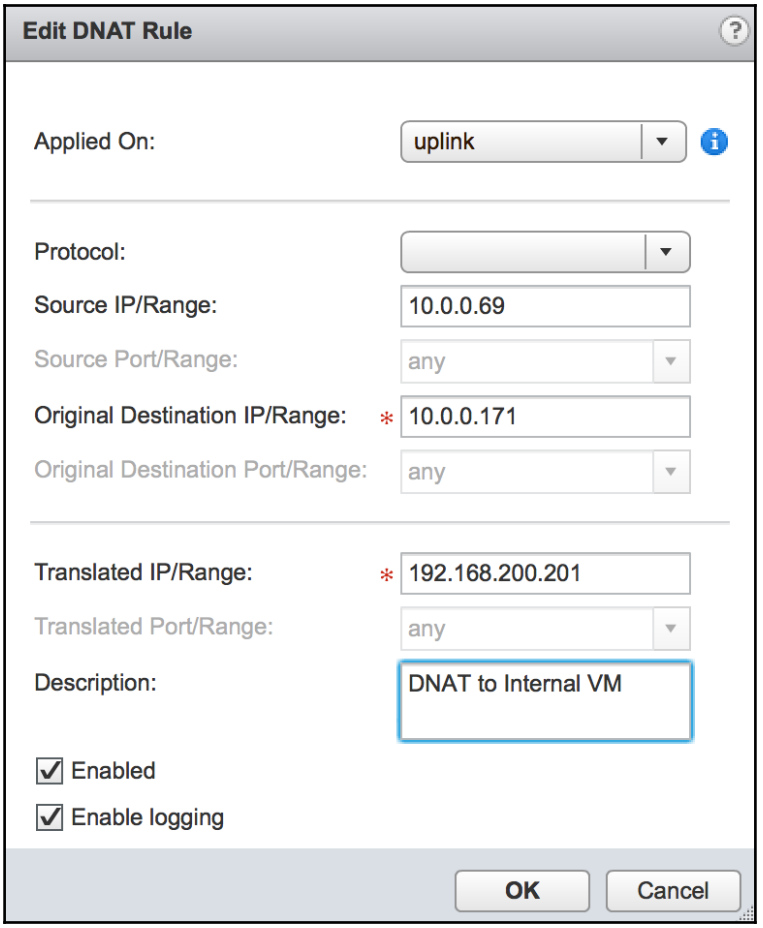

Details:
Action
Size:
Compact
Host Name:
Chapter5
Auto generate rules:
Disabled
FIPS mode:
Disabled
Syslog servers:
Change
Server 1:
Server 2:


Change Auto Rule Configuration
Enable auto rule generation
Enable auto rule generation, to automatically generate service rules to allow flow of control traffic.
Rule Priority:
High
Low
OK
Cancel

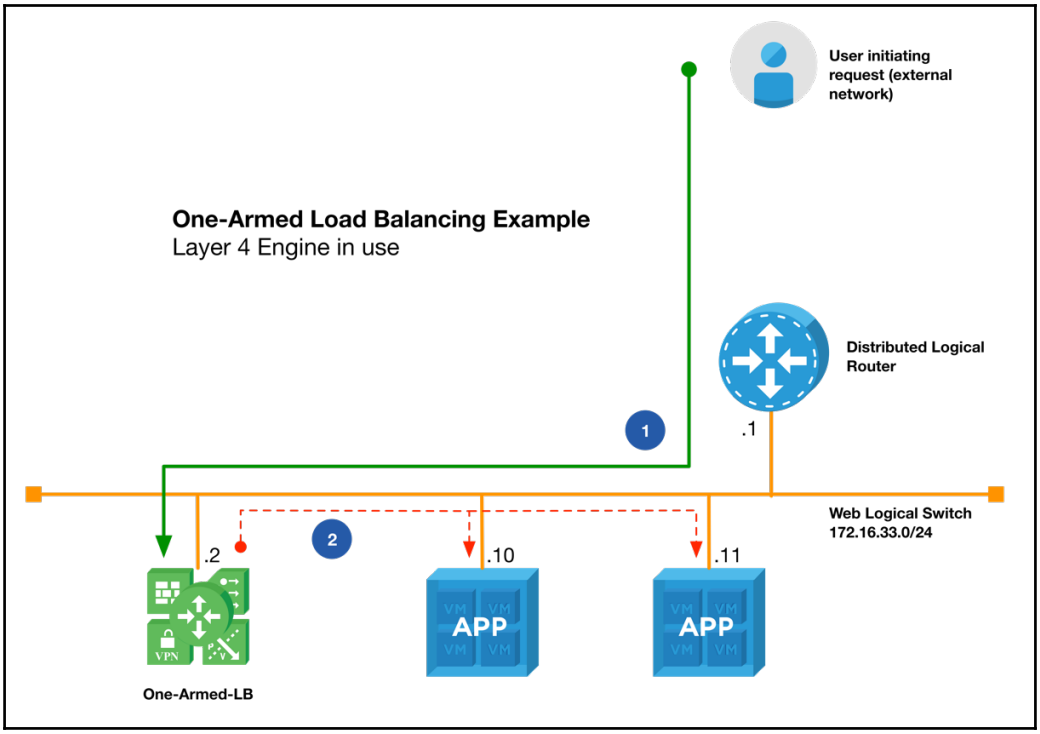

Source NAT (SNAT)
Edge Services Gateway:
Chapter5
Internal Interface
Uplink Interface
VPN
VM
Windows-VM
Public Server
SNAT
Source-Address: 192.168.200.201
Destination-Address: 8.8.8.8
Translated Source-Address:
10.0.0.170
Destination-Address: 8.8.8.8
Destination NAT (SNAT)
Edge Services Gateway:
Chapter5
Internal Interface
Uplink Interface
VPN
VM
Windows-VM
Public Server
DNAT
Source-Address: 10.0.0.69
Translated Destination-Address:
192.168.200.201
Source-Address: 10.0.0.69
Destination-Address: 10.0.0.170

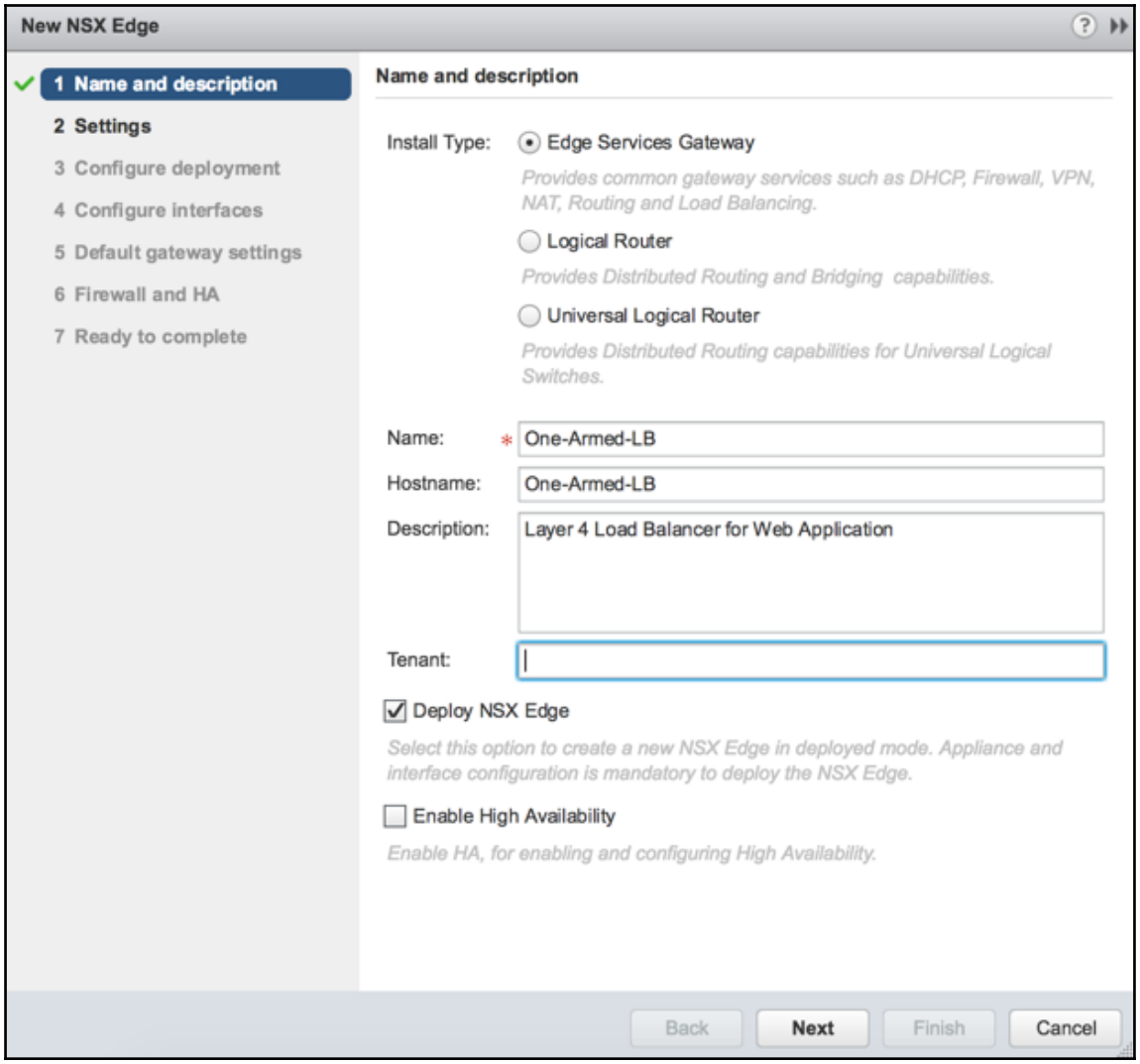


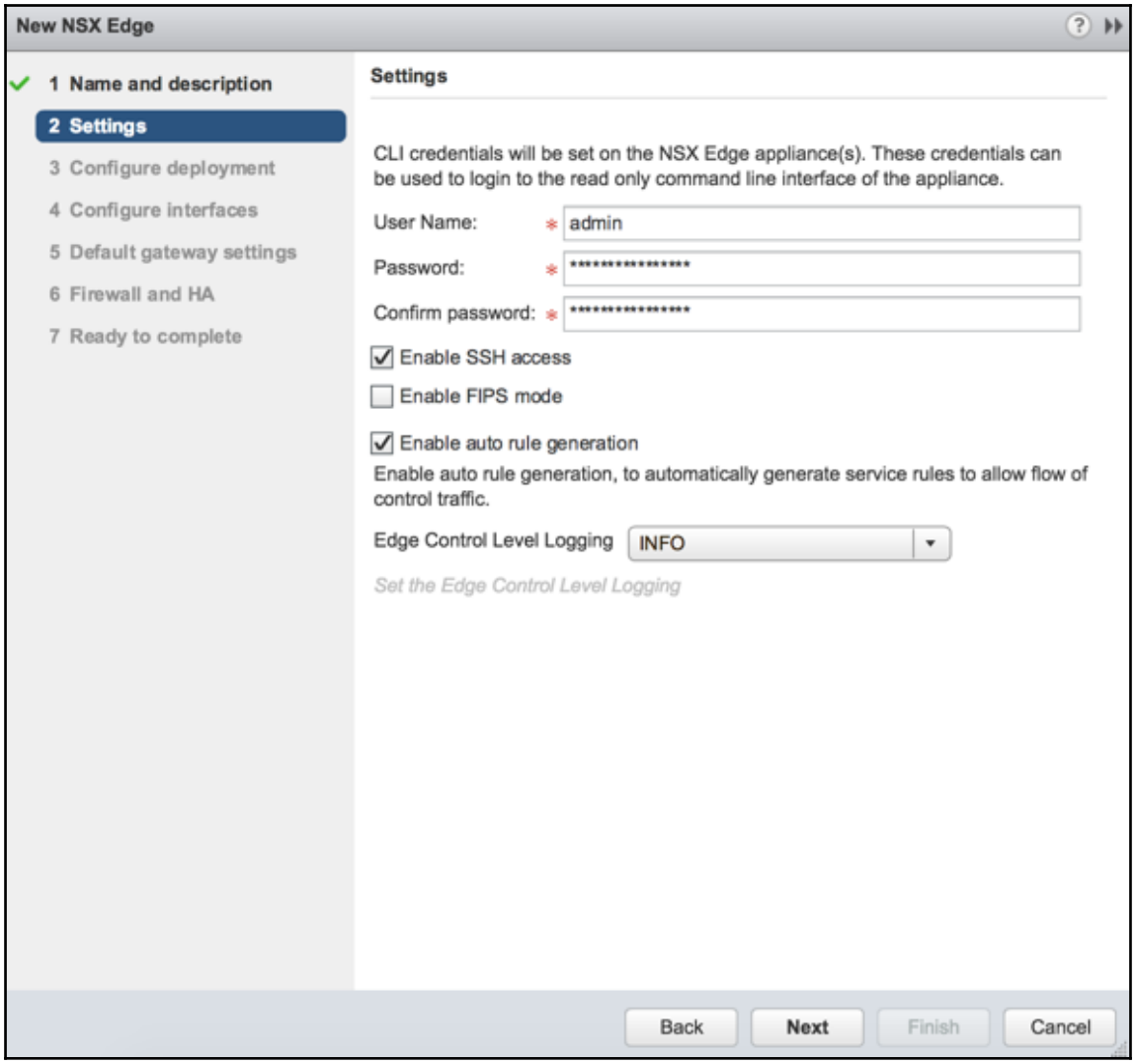

```
Chain usr_snat (1 references)
rid    pkts bytes target     prot opt in     out     source               destination
0         2   120 LOG        all  --  *      vNic_0  192.168.200.201      8.8.8.8             LOG flags 0 level 4 prefix "SNAT_"
0         2   120 SNAT       all  --  *      vNic_0  192.168.200.201      8.8.8.8             to:10.0.0.170
```

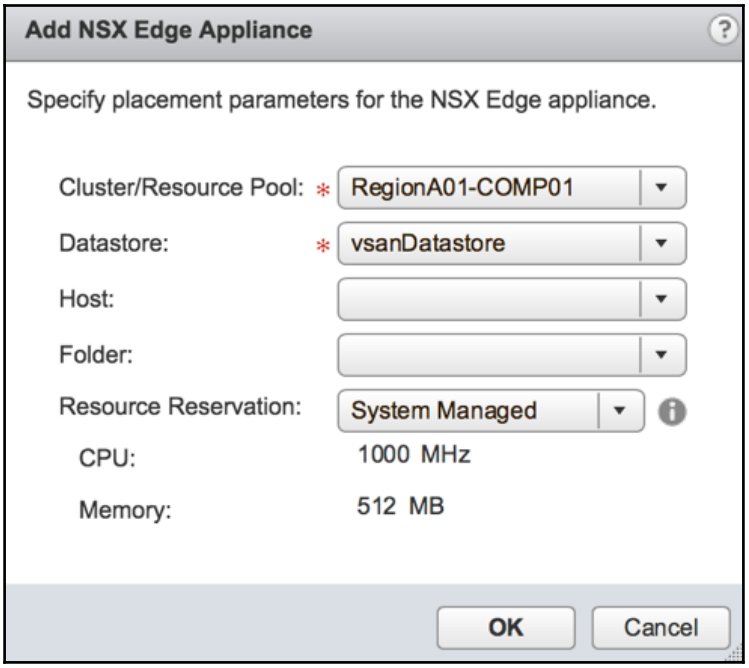


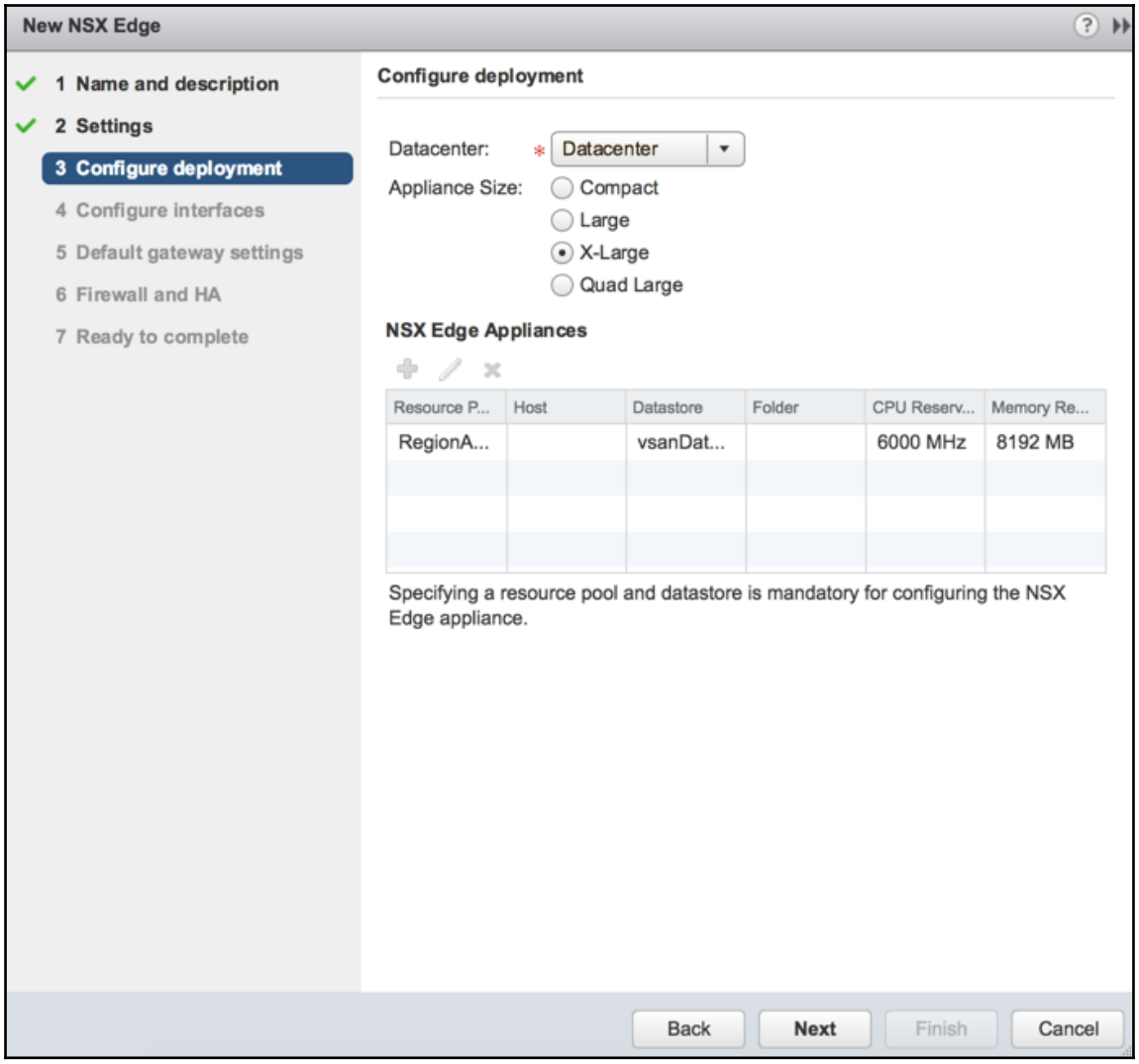

```
Chain usr_dnat (2 references)
rid    pkts bytes target     prot opt in     out     source               destination
0         2   148 LOG        all  --  vNic_0 *       10.0.0.69            10.0.0.171          LOG flags 0 level 4 prefix "DNAT_"
0         2   148 DNAT       all  --  vNic_0 *       10.0.0.69            10.0.0.171          to:192.168.200.201
```

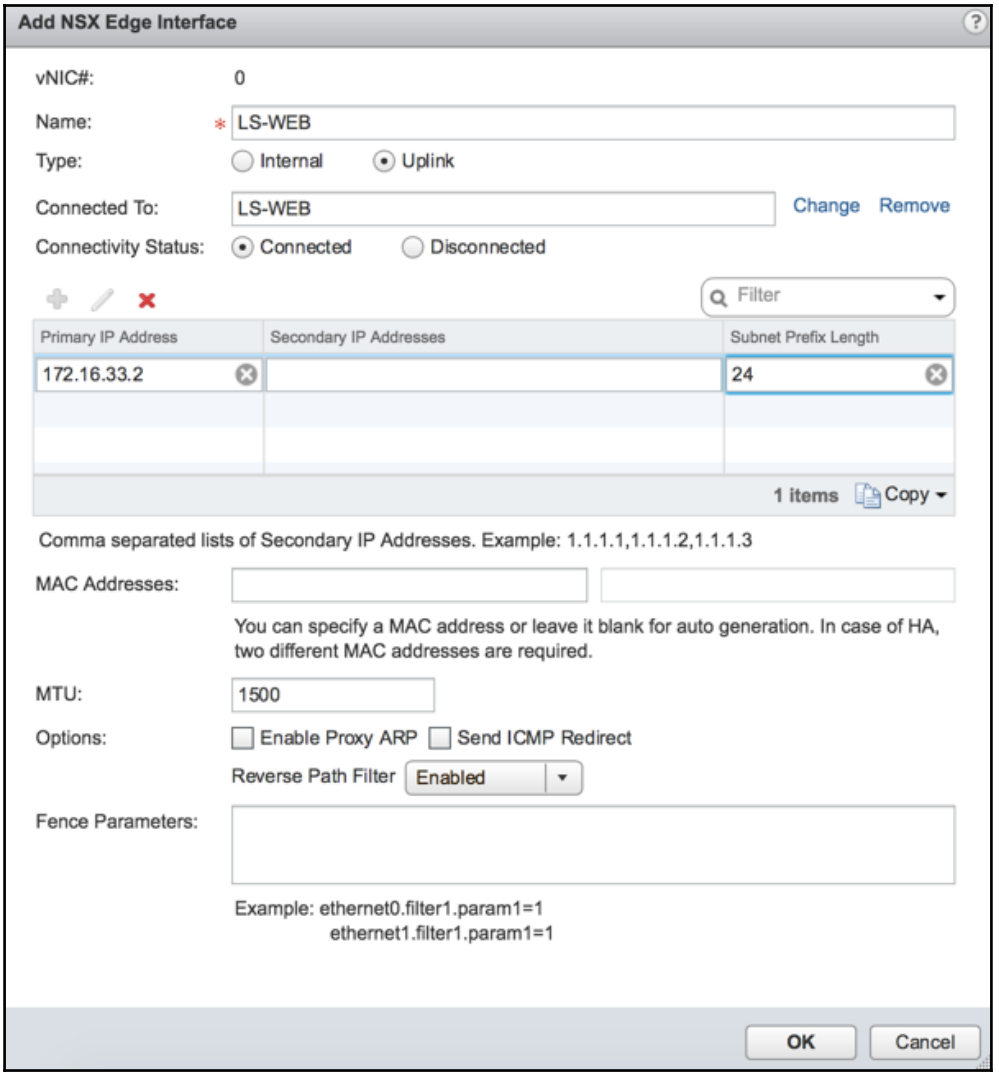

User initiating request (external network)
One-Armed Load Balancing Example
Layer 4 Engine in use
Distributed Logical Router
.1
1
2
.2
.10
.11
Web Logical Switch
172.16.33.0/24
APP
APP
VPN
One-Armed-LB

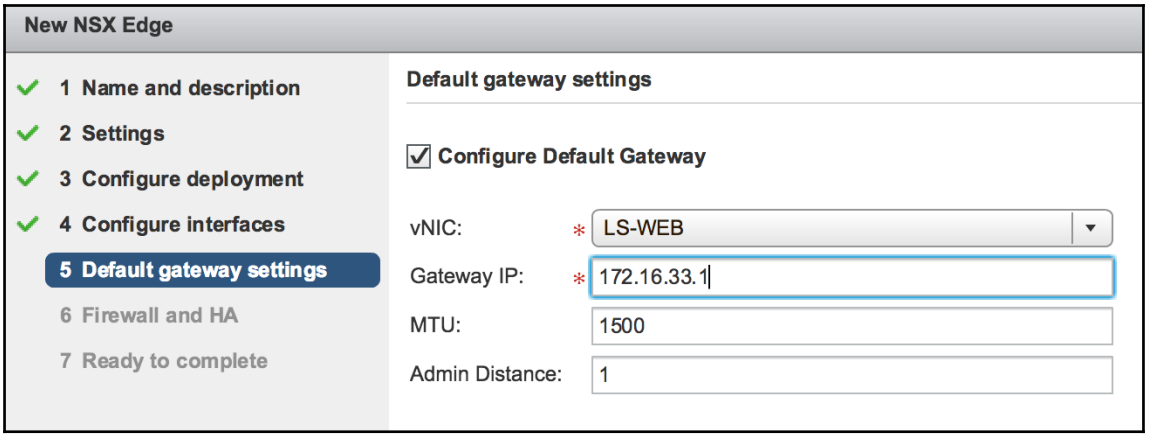

New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete
Name and description
Install Type:
Edge Services Gateway
Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.
Logical Router
Provides Distributed Routing and Bridging capabilities.
Universal Logical Router
Provides Distributed Routing capabilities for Universal Logical Switches.
Name:
One-Armed-LB
Hostname:
One-Armed-LB
Description:
Layer 4 Load Balancer for Web Application
Tenant:
Deploy NSX Edge
Select this option to create a new NSX Edge in deployed mode. Appliance and interface configuration is mandatory to deploy the NSX Edge.
Enable High Availability
Enable HA, for enabling and configuring High Availability.
Back
Next
Finish
Cancel

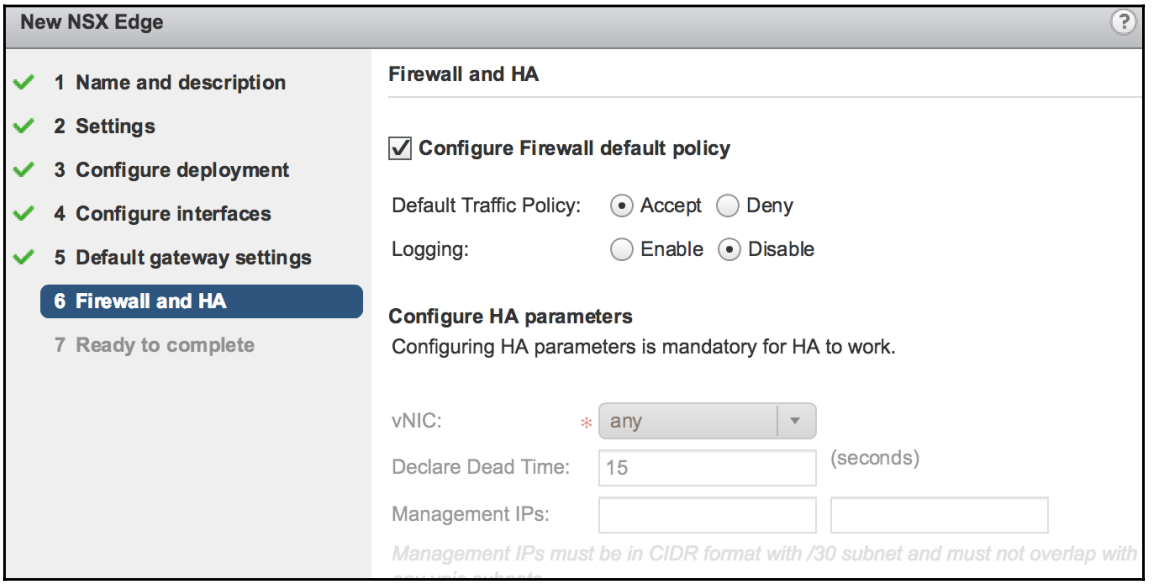

New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete
Settings
CLI credentials will be set on the NSX Edge appliance(s). These credentials can be used to login to the read only command line interface of the appliance.
User Name:
admin
Password:
Confirm password:
Enable SSH access
Enable FIPS mode
Enable auto rule generation
Enable auto rule generation, to automatically generate service rules to allow flow of control traffic.
Edge Control Level Logging
INFO
Set the Edge Control Level Logging
Back
Next
Finish
Cancel

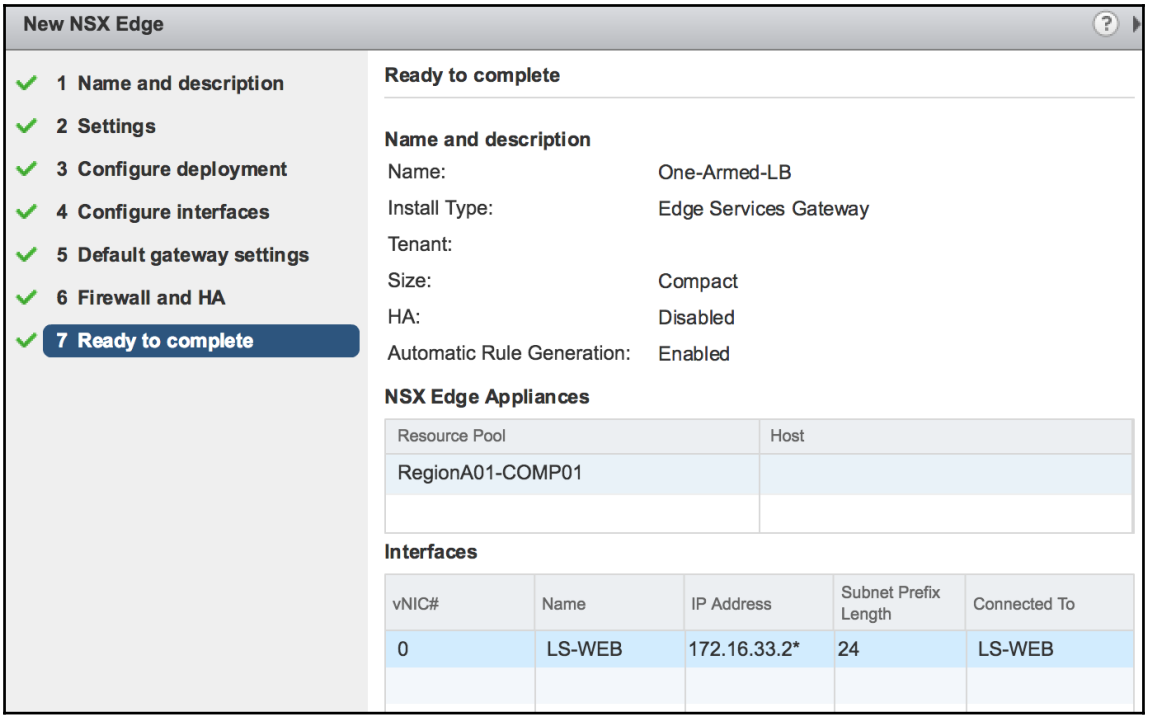

Add NSX Edge Appliance
Specify placement parameters for the NSX Edge appliance.
Cluster/Resource Pool: * RegionA01-COMP01
Datastore: * vsanDatastore
Host:
Folder:
Resource Reservation: System Managed
CPU: 1000 MHz
Memory: 512 MB
OK
Cancel

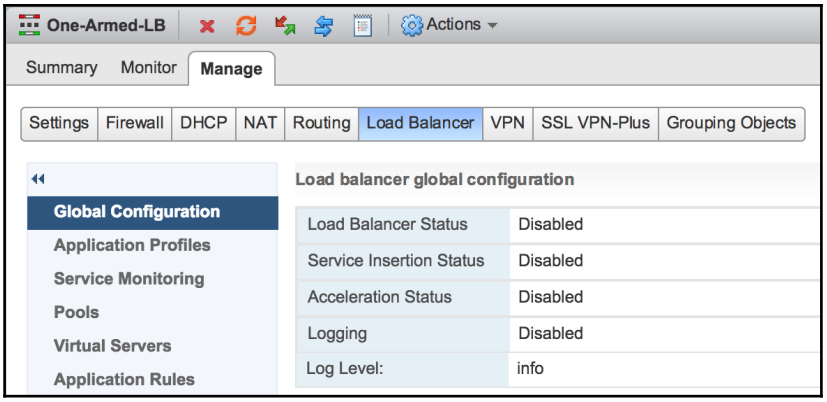

New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete
Configure deployment
Datacenter:
Datacenter
Appliance Size:
Compact
Large
X-Large
Quad Large
NSX Edge Appliances
Resource P...
Host
Datastore
Folder
CPU Reserv...
Memory Re...
RegionA...
vsanDat...
6000 MHz
8192 MB
Specifying a resource pool and datastore is mandatory for configuring the NSX Edge appliance.
Back
Next
Finish
Cancel

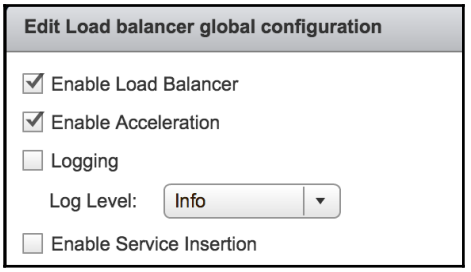

Add NSX Edge Interface
vNIC#:
0
Name:
LS-WEB
Type:
Internal
Uplink
Connected To:
LS-WEB
Change
Remove
Connectivity Status:
Connected
Disconnected
Filter
Primary IP Address
Secondary IP Addresses
Subnet Prefix Length
172.16.33.2
24
1 items
Copy
Comma separated lists of Secondary IP Addresses. Example: 1.1.1.1,1.1.1.2,1.1.1.3
MAC Addresses:
You can specify a MAC address or leave it blank for auto generation. In case of HA, two different MAC addresses are required.
MTU:
1500
Options:
Enable Proxy ARP
Send ICMP Redirect
Reverse Path Filter
Enabled
Fence Parameters:
Example: ethernet0.filter1.param1=1
ethernet1.filter1.param1=1
OK
Cancel

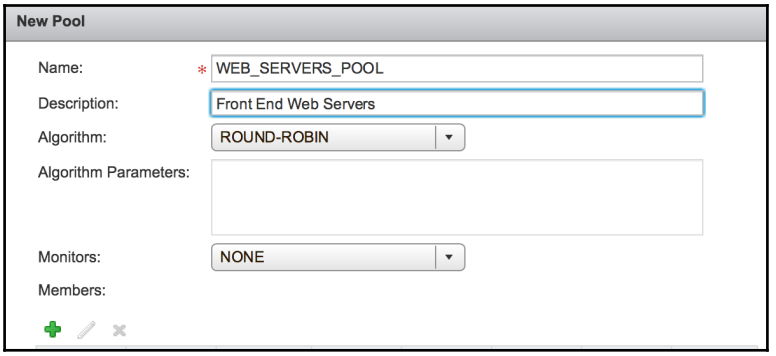

New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete
Default gateway settings
Configure Default Gateway
vNIC:
LS-WEB
Gateway IP:
172.16.33.1
MTU:
1500
Admin Distance:
1

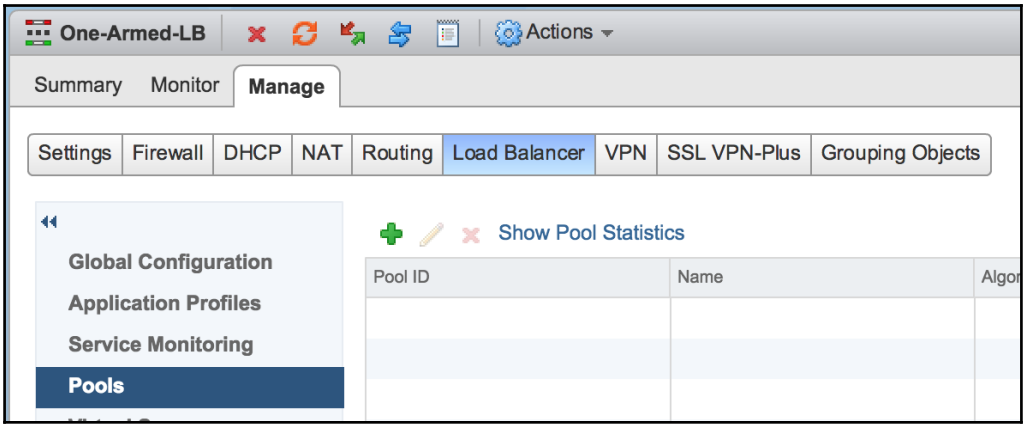

New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete
Firewall and HA
Configure Firewall default policy
Default Traffic Policy:
Accept
Deny
Logging:
Enable
Disable
Configure HA parameters
Configuring HA parameters is mandatory for HA to work.
vNIC:
any
Declare Dead Time:
15
(seconds)
Management IPs:
Management IPs must be in CIDR format with /30 subnet and must not overlap with

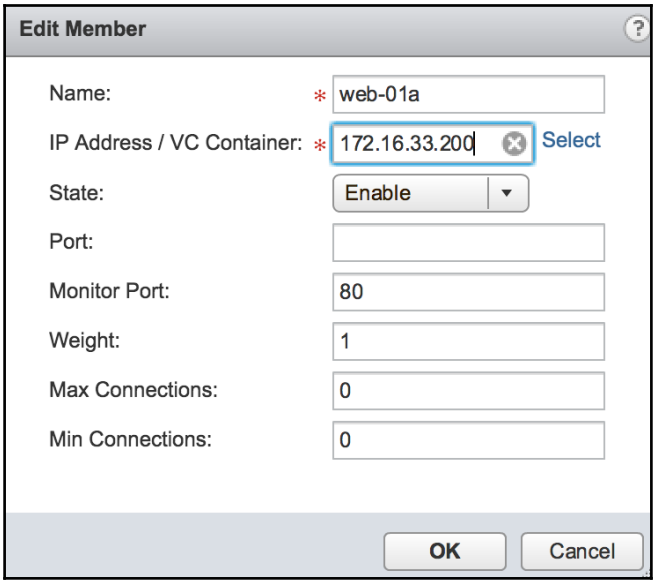

New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete
Ready to complete
Name and description
Name: One-Armed-LB
Install Type: Edge Services Gateway
Tenant:
Size: Compact
HA: Disabled
Automatic Rule Generation: Enabled
NSX Edge Appliances
Resource Pool
Host
RegionA01-COMP01
Interfaces
vNIC#
Name
IP Address
Subnet Prefix Length
Connected To
0
LS-WEB
172.16.33.2*
24
LS-WEB

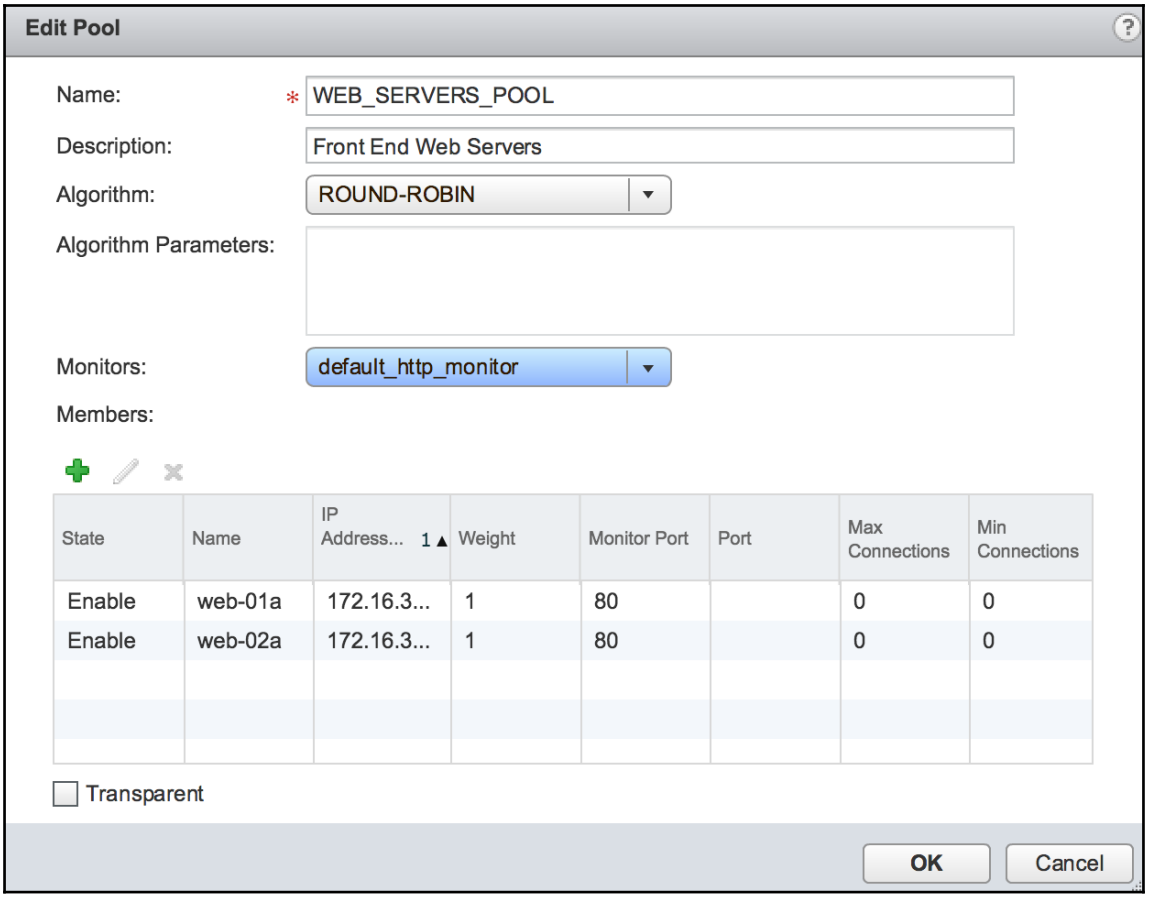

One-Armed-LB
Actions
Summary
Monitor
Manage
Settings
Firewall
DHCP
NAT
Routing
Load Balancer
VPN
SSL VPN-Plus
Grouping Objects
Global Configuration
Application Profiles
Service Monitoring
Pools
Virtual Servers
Application Rules
Load balancer global configuration
Load Balancer Status Disabled
Service Insertion Status Disabled
Acceleration Status Disabled
Logging Disabled
Log Level: info

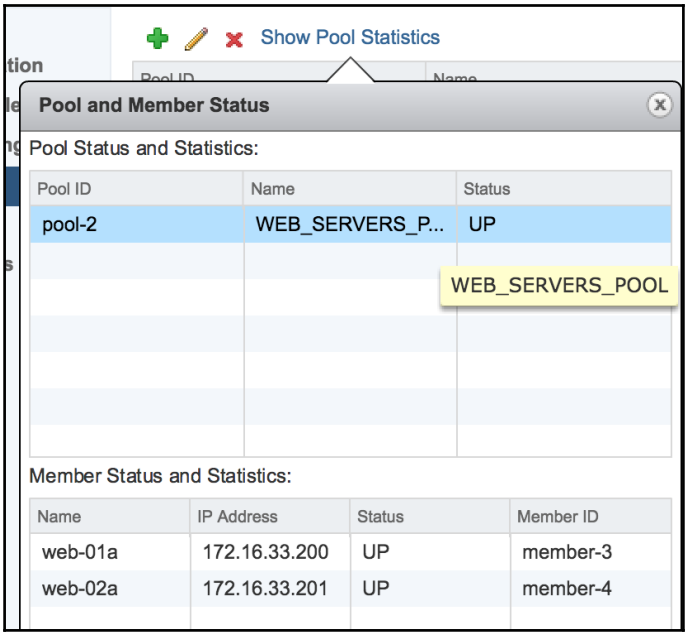

Edit Load balancer global configuration
Enable Load Balancer
Enable Acceleration
Logging
Log Level:
Info
Enable Service Insertion

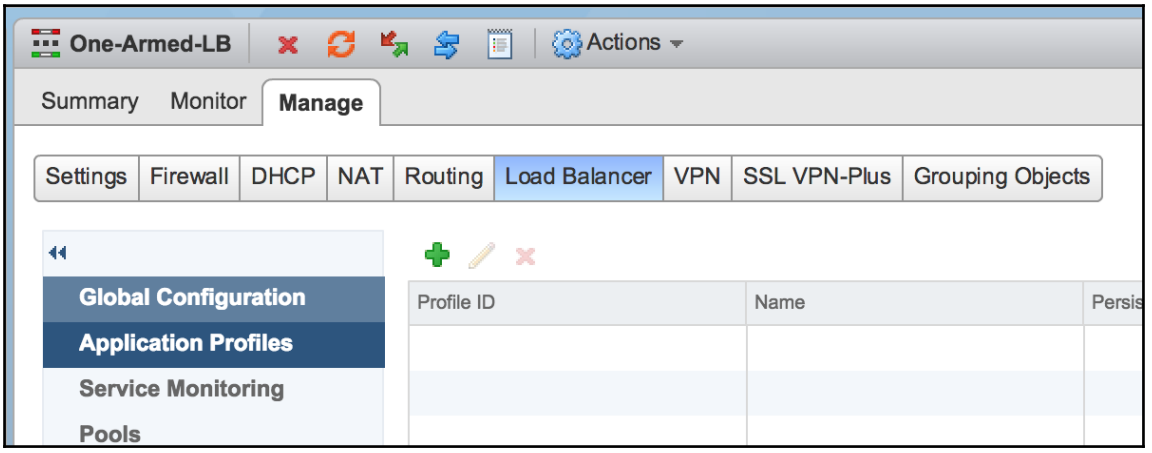

New Pool
Name:
WEB_SERVERS_POOL
Description:
Front End Web Servers
Algorithm:
ROUND-ROBIN
Algorithm Parameters:
Monitors:
NONE
Members:

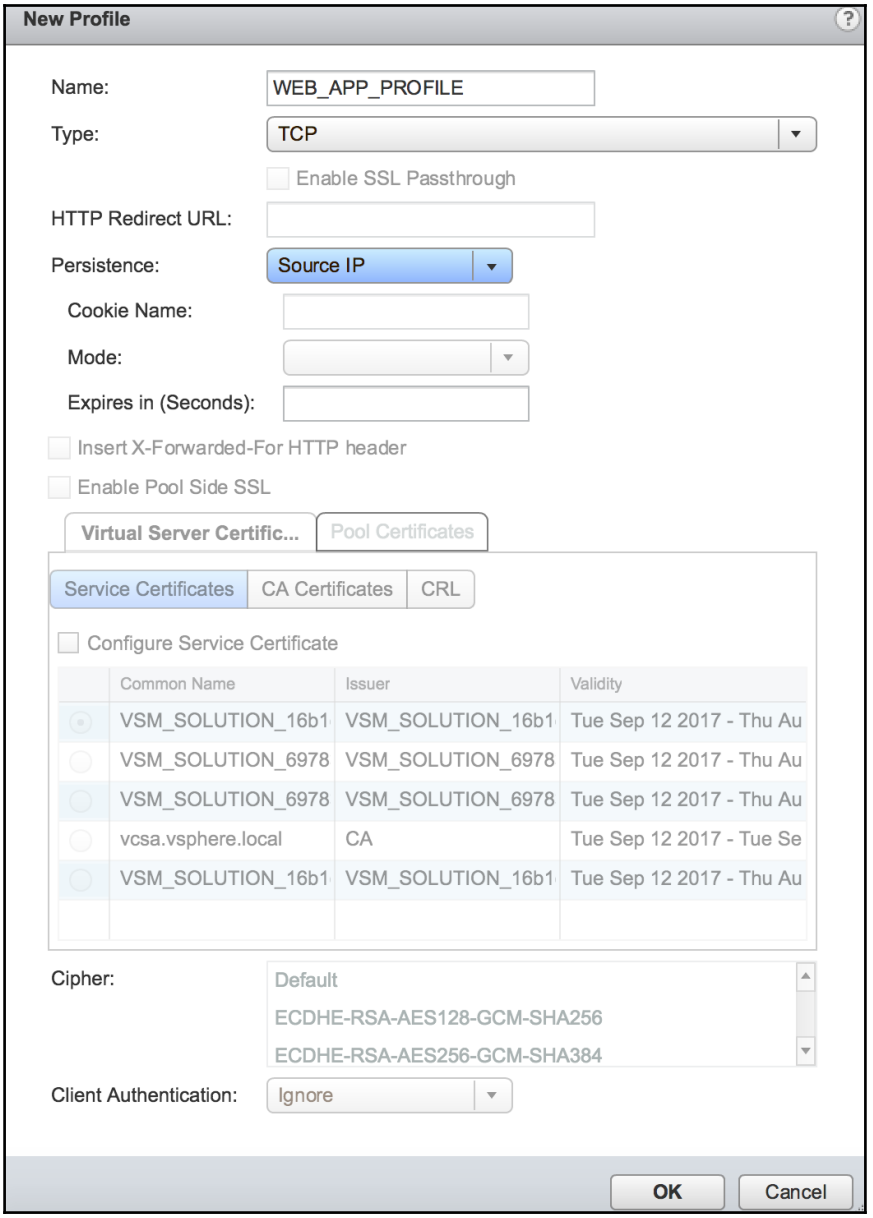

One-Armed-LB
Actions
Summary
Monitor
Manage
Settings
Firewall
DHCP
NAT
Routing
Load Balancer
VPN
SSL VPN-Plus
Grouping Objects
Global Configuration
Application Profiles
Service Monitoring
Pools
Show Pool Statistics
Pool ID
Name

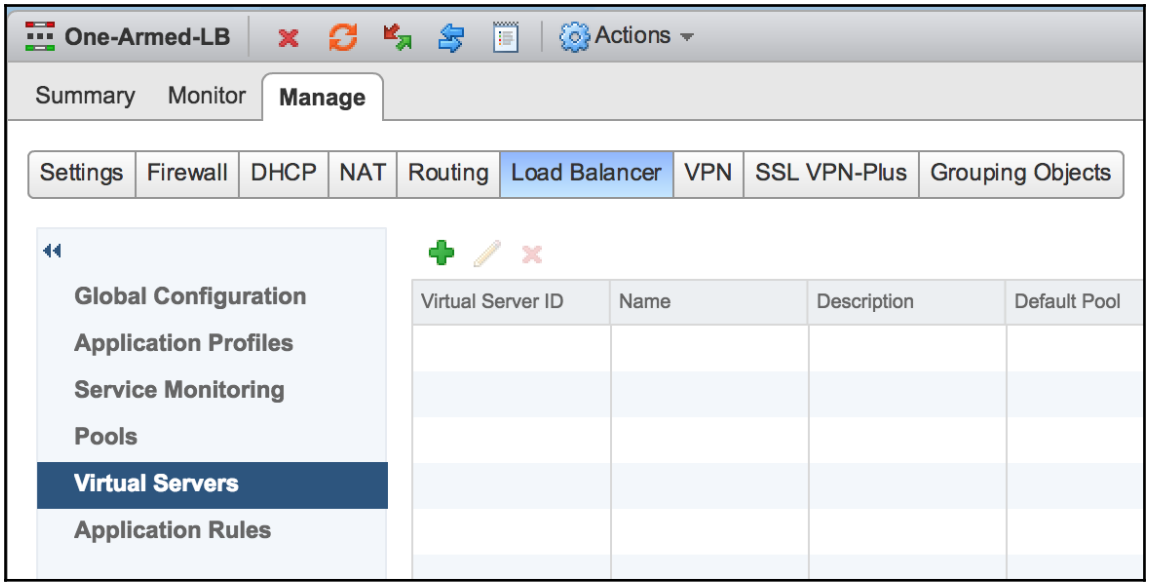

Edit Member
Name:
web-01a
IP Address / VC Container:
172.16.33.200
Select
State:
Enable
Port:
Monitor Port:
80
Weight:
1
Max Connections:
0
Min Connections:
0
OK
Cancel

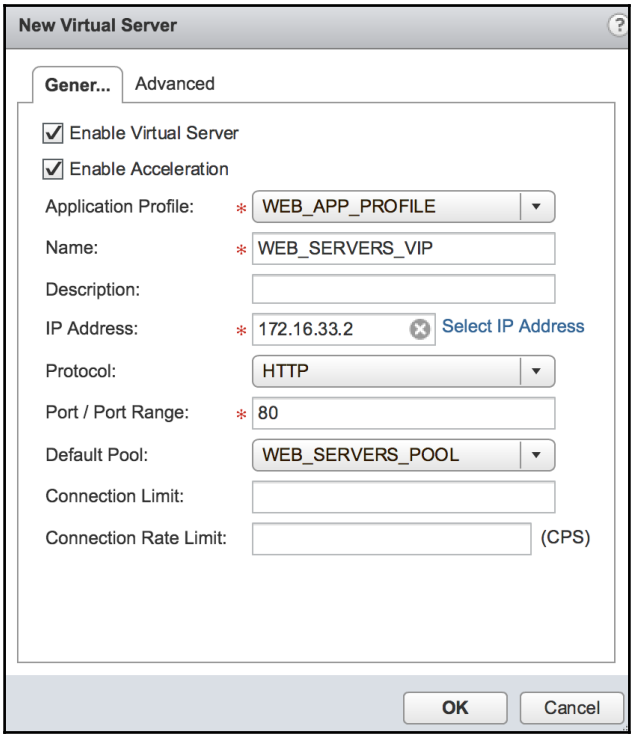

Edit Pool
Name:
WEB_SERVERS_POOL
Description:
Front End Web Servers
Algorithm:
ROUND-ROBIN
Algorithm Parameters:
Monitors:
default_http_monitor
Members:
State
Name
IP Address...
1
Weight
Monitor Port
Port
Max Connections
Min Connections
Enable
web-01a
172.16.3...
1
80
0
0
Enable
web-02a
172.16.3...
1
80
0
0
Transparent
OK
Cancel


Show Pool Statistics
Pool and Member Status
Pool Status and Statistics:
Pool ID
Name
Status
pool-2
WEB_SERVERS_P...
UP
WEB_SERVERS_POOL
Member Status and Statistics:
Name
IP Address
Status
Member ID
web-01a
172.16.33.200
UP
member-3
web-02a
172.16.33.201
UP
member-4

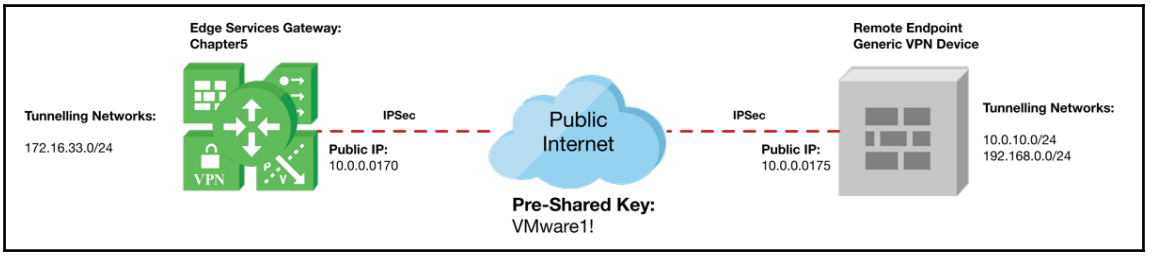

One-Armed-LB
Actions
Summary
Monitor
Manage
Settings
Firewall
DHCP
NAT
Routing
Load Balancer
VPN
SSL VPN-Plus
Grouping Objects
Global Configuration
Application Profiles
Service Monitoring
Pools
Profile ID
Name
Persis


New Profile
Name:
WEB_APP_PROFILE
Type:
TCP
Enable SSL Passthrough
HTTP Redirect URL:
Persistence:
Source IP
Cookie Name:
Mode:
Expires in (Seconds):
Insert X-Forwarded-For HTTP header
Enable Pool Side SSL
Virtual Server Certific...
Pool Certificates
Service Certificates
CA Certificates
CRL
Configure Service Certificate
Common Name
Issuer
Validity
VSM_SOLUTION_16b1
VSM_SOLUTION_16b1
Tue Sep 12 2017 - Thu Au
VSM_SOLUTION_6978
VSM_SOLUTION_6978
Tue Sep 12 2017 - Thu Au
VSM_SOLUTION_6978
VSM_SOLUTION_6978
Tue Sep 12 2017 - Thu Au
vcsa.vsphere.local
CA
Tue Sep 12 2017 - Tue Se
VSM_SOLUTION_16b1
VSM_SOLUTION_16b1
Tue Sep 12 2017 - Thu Au
Cipher:
Default
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES256-GCM-SHA384
Client Authentication:
Ignore
OK
Cancel


One-Armed-LB
Actions
Summary
Monitor
Manage
Settings
Firewall
DHCP
NAT
Routing
Load Balancer
VPN
SSL VPN-Plus
Grouping Objects
Global Configuration
Application Profiles
Service Monitoring
Pools
Virtual Servers
Application Rules
Virtual Server ID
Name
Description
Default Pool


New Virtual Server
Gener...
Advanced
Enable Virtual Server
Enable Acceleration
Application Profile:
WEB_APP_PROFILE
Name:
WEB_SERVERS_VIP
Description:
IP Address:
172.16.33.2
Select IP Address
Protocol:
HTTP
Port / Port Range:
80
Default Pool:
WEB_SERVERS_POOL
Connection Limit:
Connection Rate Limit:
(CPS)
OK
Cancel

```
Loadbalancer VirtualServer Statistics:

VIRTUAL WEB_SERVERS_VIP
|  ADDRESS [172.16.33.2]:80
|  SESSION (total) = (0)
|  RATE (cur) = (0)
|  BYTES in = (0), out = (0)
   +->POOL WEB_SERVERS_POOL
   |  LB METHOD round-robin
   |  LB PROTOCOL L4
   |  Transparent disabled
   |  SESSION (cur, cps, total) = (0, 0, 0)
   |  BYTES in = (0), out = (0)
      +->POOL MEMBER: WEB_SERVERS_POOL/web-01a, STATUS: UP
      |  |  HEALTH MONITOR = MONITOR SERVICE, default_http_monitor:OK
c     |  |  |  LAST STATE CHANGE: 2018-01-18 11:06:30
      |  |  |  LAST CHECK: 2018-01-18 11:06:30
d     |  |  SESSION (cur, cps, total) = (0, 0, 0)
0     |  |  BYTES in = (0), out = (0)
0     +->POOL MEMBER: WEB_SERVERS_POOL/web-02a, STATUS: UP
s     |  |  HEALTH MONITOR = MONITOR SERVICE, default_http_monitor:OK
```

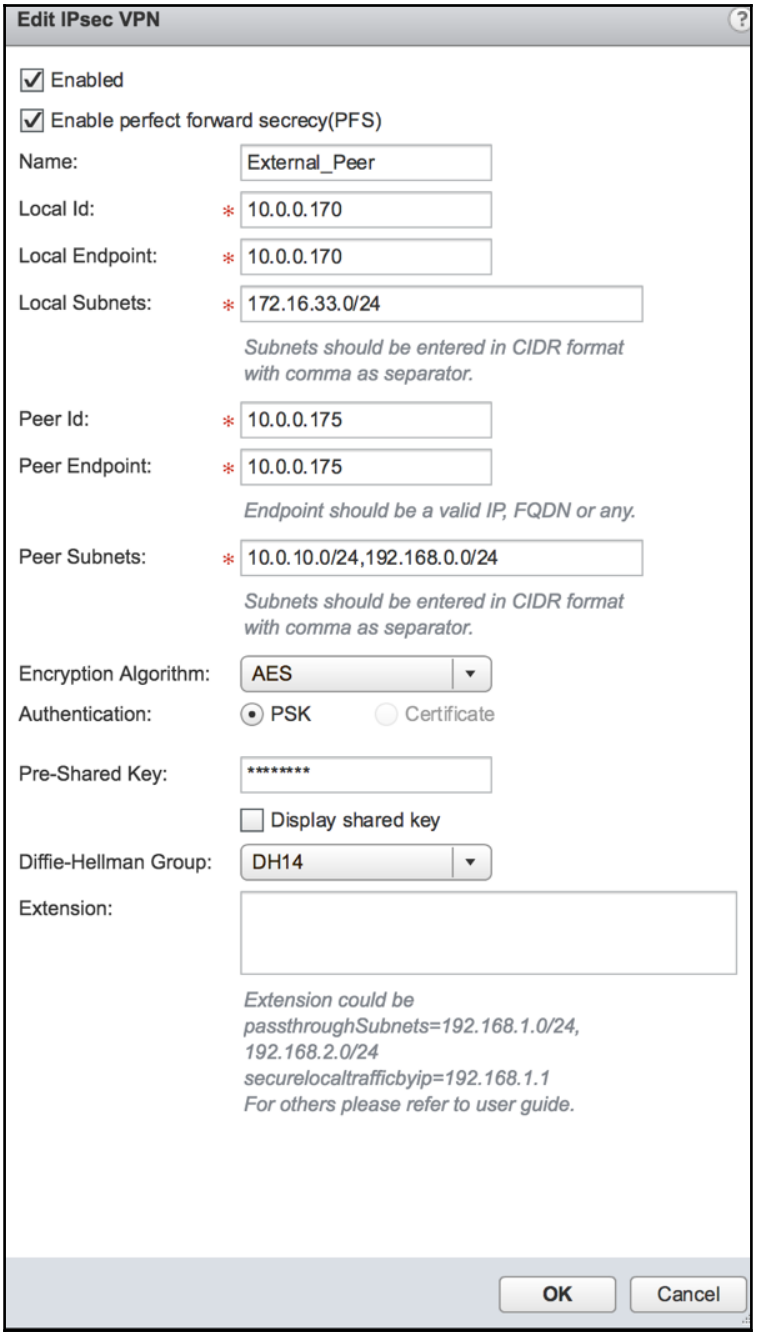


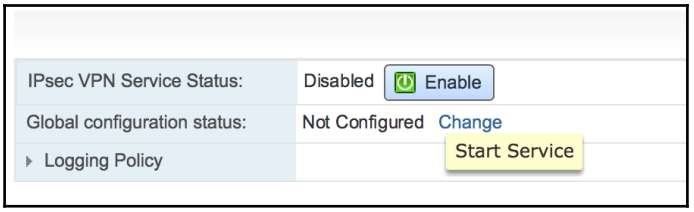
Configure interfaces of this NSX Edge.

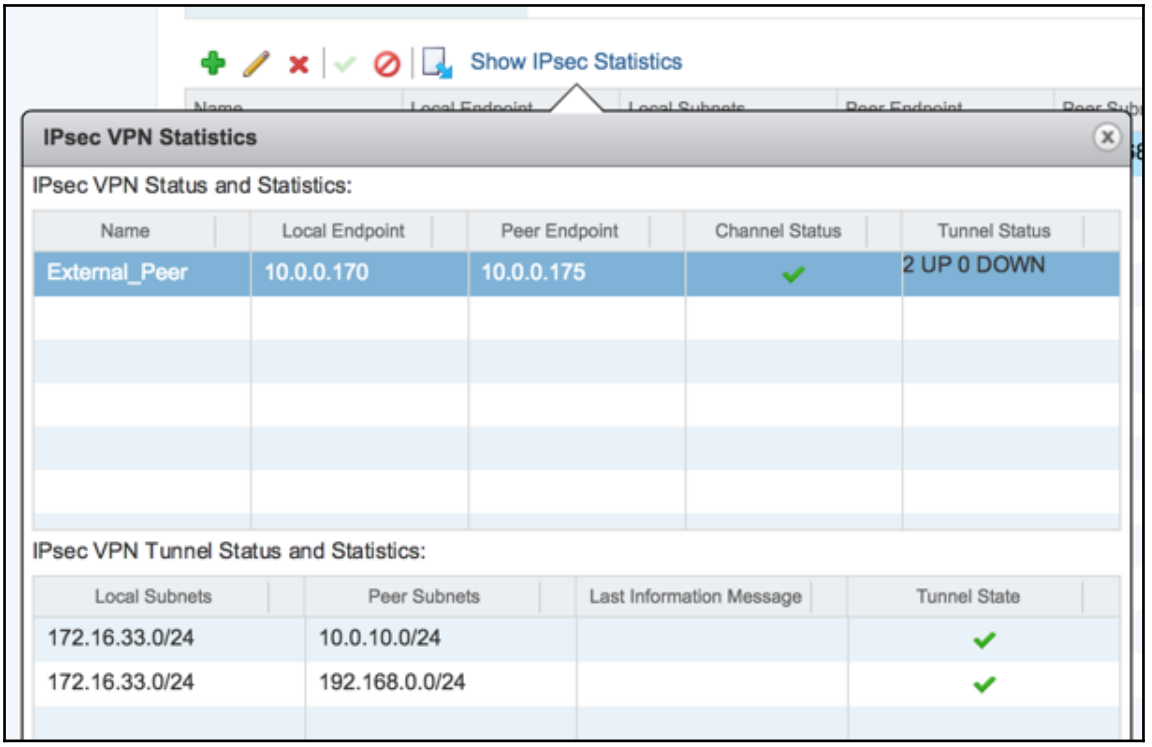
Actions

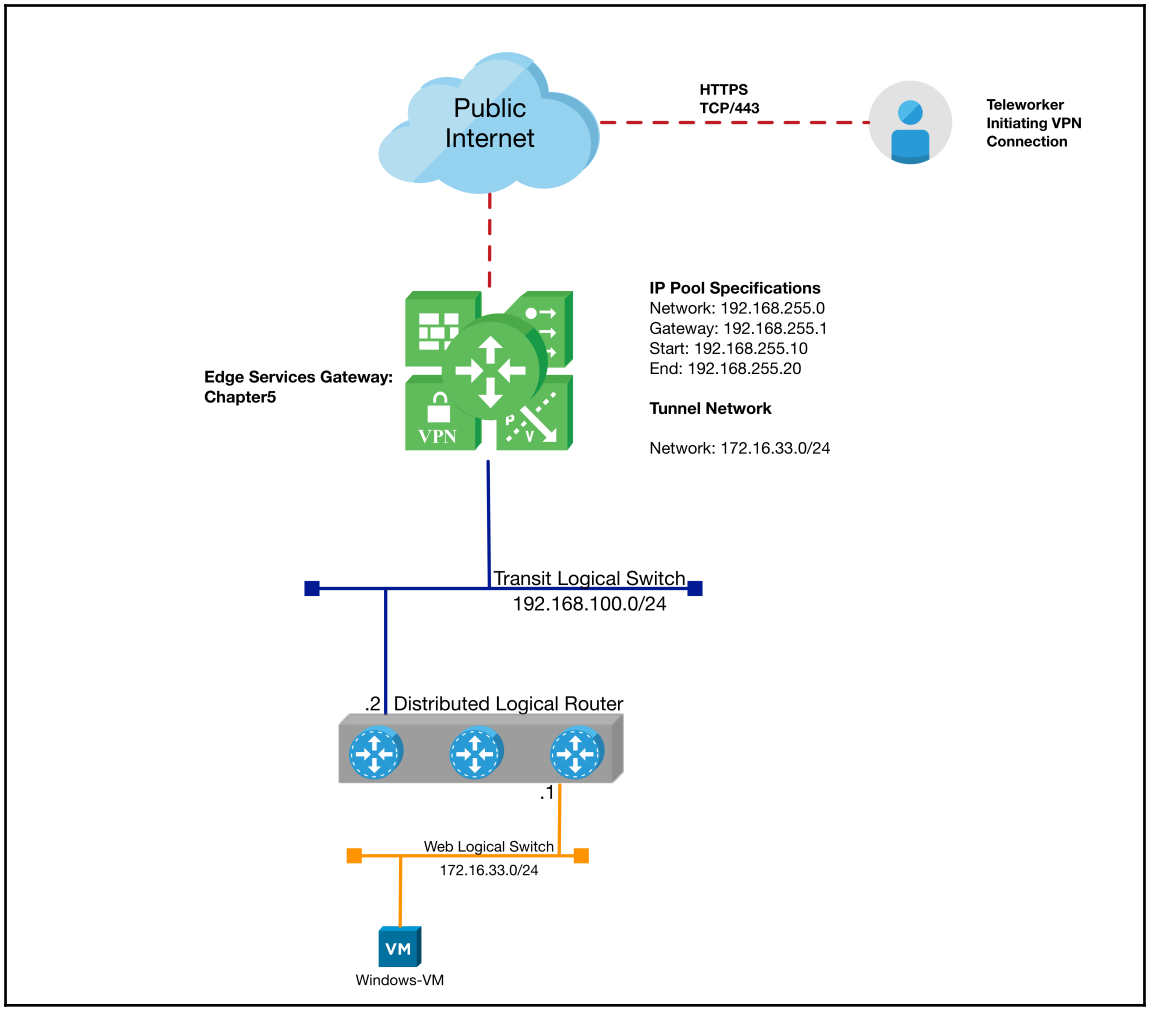
Filter

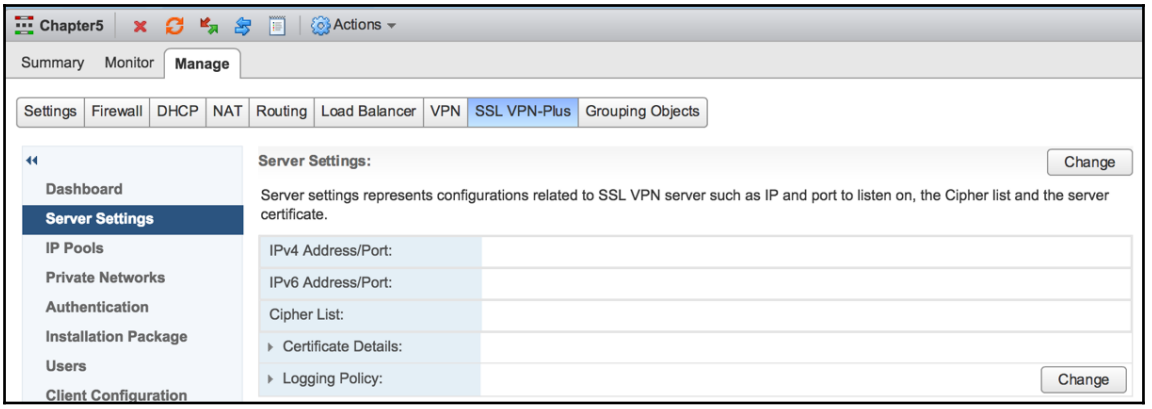
vNIC#	Name	IP Address	Subnet Prefix Length	Connected To	Type	Status
0	uplink	10.0.0.170*	24	VM Network	Uplink	✔

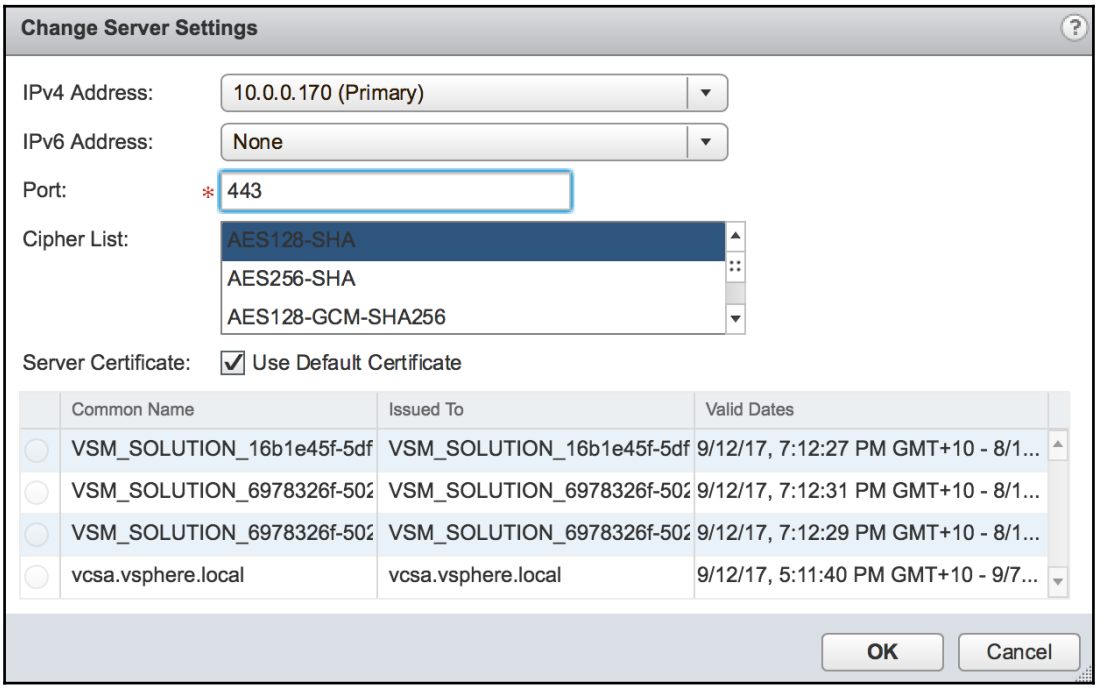

Edit IPsec VPN
Enabled
Enable perfect forward secrecy(PFS)
Name:
External_Peer
Local Id:
10.0.0.170
Local Endpoint:
10.0.0.170
Local Subnets:
172.16.33.0/24
Subnets should be entered in CIDR format with comma as separator.
Peer Id:
10.0.0.175
Peer Endpoint:
10.0.0.175
Endpoint should be a valid IP, FQDN or any.
Peer Subnets:
10.0.10.0/24,192.168.0.0/24
Subnets should be entered in CIDR format with comma as separator.
Encryption Algorithm:
AES
Authentication:
PSK
Certificate
Pre-Shared Key:
****
Display shared key
Diffie-Hellman Group:
DH14
Extension:
Extension could be passthroughSubnets=192.168.1.0/24, 192.168.2.0/24 securelocaltrafficbyip=192.168.1.1
For others please refer to user guide.
OK
Cancel

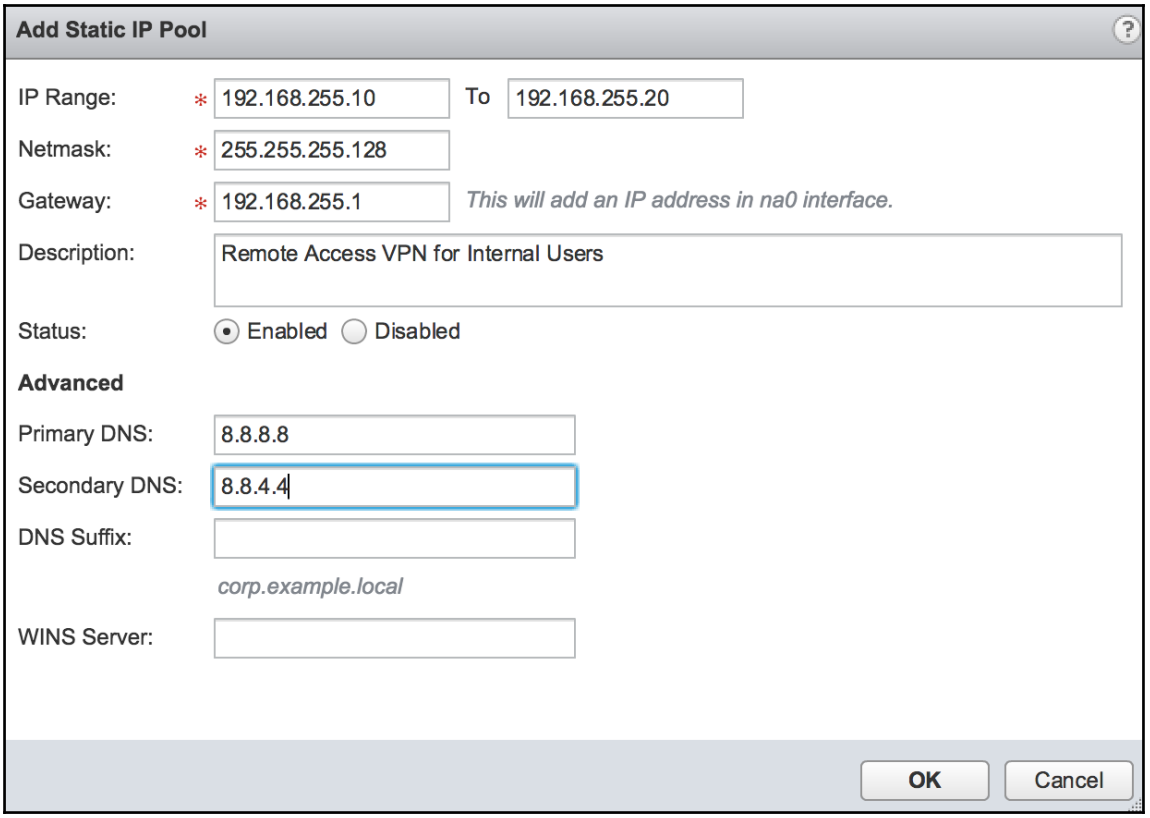

IPsec VPN Service Status:
Disabled
Enable
Global configuration status:
Not Configured
Change
Start Service
Logging Policy

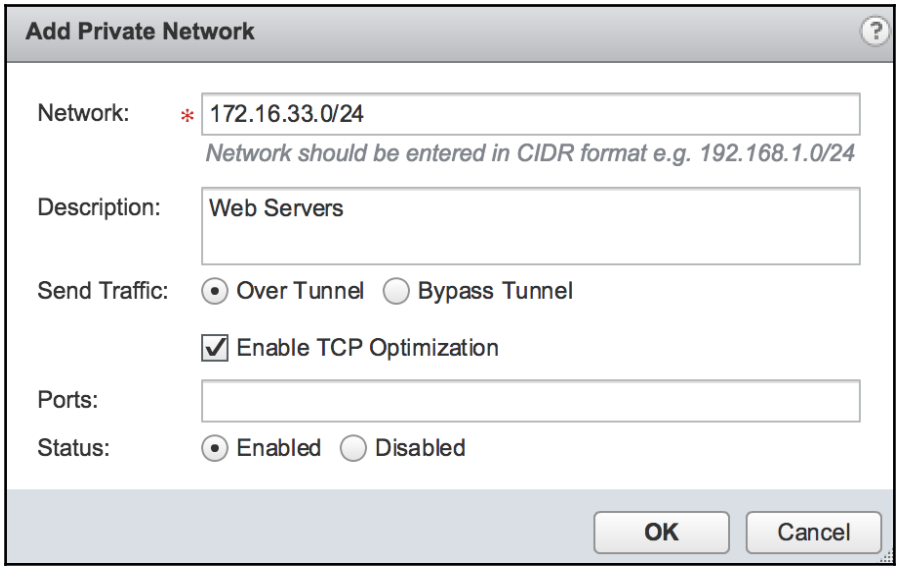

Show IPsec Statistics
IPsec VPN Statistics
IPsec VPN Status and Statistics:
Name
Local Endpoint
Peer Endpoint
Channel Status
Tunnel Status
External_Peer
10.0.0.170
10.0.0.175
2 UP 0 DOWN
IPsec VPN Tunnel Status and Statistics:
Local Subnets
Peer Subnets
Last Information Message
Tunnel State
172.16.33.0/24
10.0.10.0/24
172.16.33.0/24
192.168.0.0/24

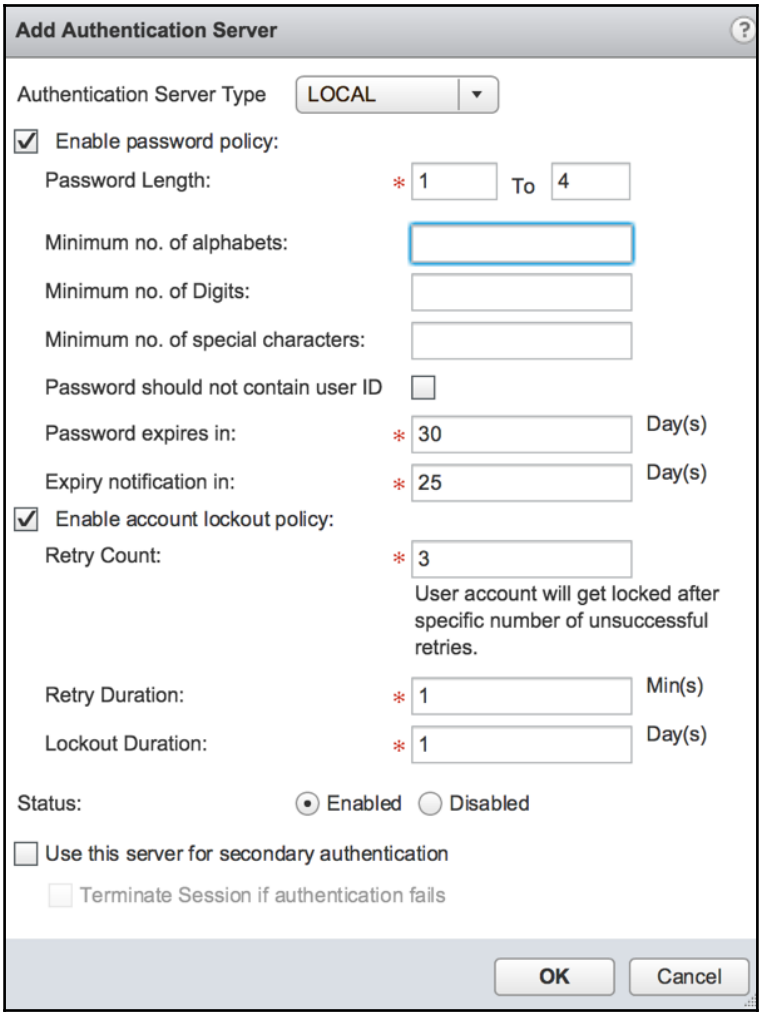

Public Internet
HTTPS
TCP/443
Teleworker Initiating VPN Connection
Edge Services Gateway: Chapter5
VPN
IP Pool Specifications
Network: 192.168.255.0
Gateway: 192.168.255.1
Start: 192.168.255.10
End: 192.168.255.20
Tunnel Network
Network: 172.16.33.0/24
Transit Logical Switch
192.168.100.0/24
.2
Distributed Logical Router
.1
Web Logical Switch
172.16.33.0/24
VM
Windows-VM

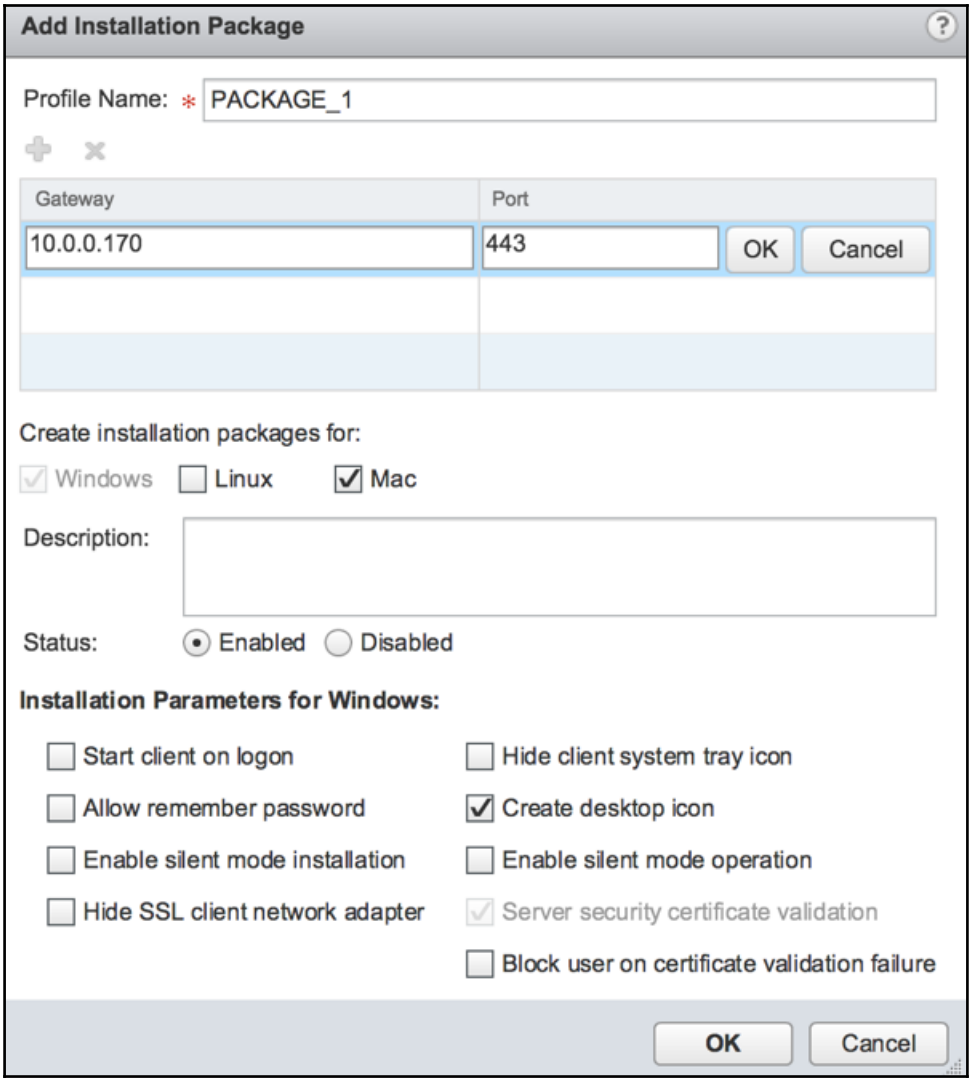

Chapter5
Actions
Summary
Monitor
Manage
Settings
Firewall
DHCP
NAT
Routing
Load Balancer
VPN
SSL VPN-Plus
Grouping Objects
Dashboard
Server Settings
IP Pools
Private Networks
Authentication
Installation Package
Users
Client Configuration
Server Settings:
Change
Server settings represents configurations related to SSL VPN server such as IP and port to listen on, the Cipher list and the server certificate.
IPv4 Address/Port:
IPv6 Address/Port:
Cipher List:
Certificate Details:
Logging Policy:
Change

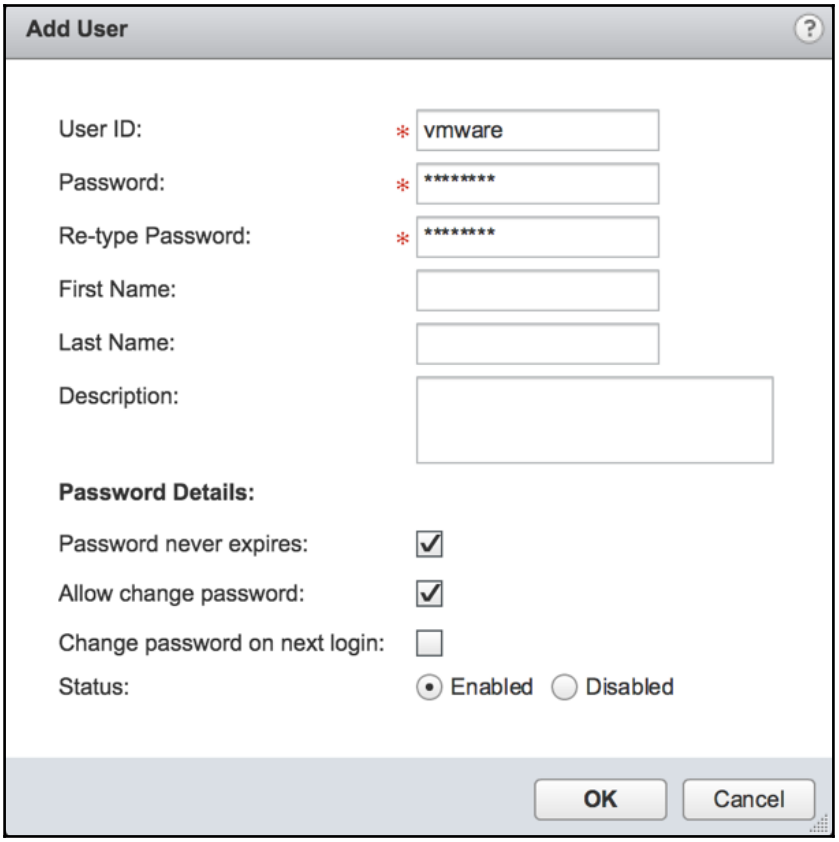

Change Server Settings
IPv4 Address:
10.0.0.170 (Primary)
IPv6 Address:
None
Port:
443
Cipher List:
AES128-SHA
AES256-SHA
AES128-GCM-SHA256
Server Certificate:
Use Default Certificate
Common Name
Issued To
Valid Dates
VSM_SOLUTION_16b1e45f-5df
VSM_SOLUTION_16b1e45f-5df
9/12/17, 7:12:27 PM GMT+10 - 8/1...
VSM_SOLUTION_6978326f-502
VSM_SOLUTION_6978326f-502
9/12/17, 7:12:31 PM GMT+10 - 8/1...
VSM_SOLUTION_6978326f-502
VSM_SOLUTION_6978326f-502
9/12/17, 7:12:29 PM GMT+10 - 8/1...
vcsa.vsphere.local
vcsa.vsphere.local
9/12/17, 5:11:40 PM GMT+10 - 9/7...
OK
Cancel

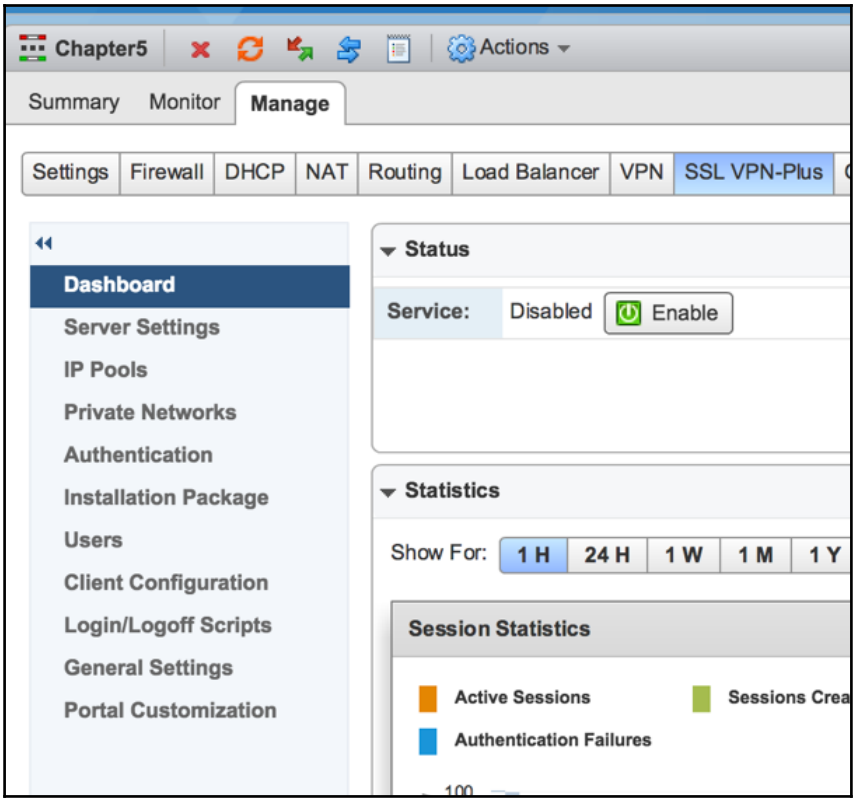

Add Static IP Pool
IP Range:
192.168.255.10
To
192.168.255.20
Netmask:
255.255.255.128
Gateway:
192.168.255.1
This will add an IP address in na0 interface.
Description:
Remote Access VPN for Internal Users
Status:
Enabled
Disabled
Advanced
Primary DNS:
8.8.8.8
Secondary DNS:
8.8.4.4
DNS Suffix:
corp.example.local
WINS Server:
OK
Cancel

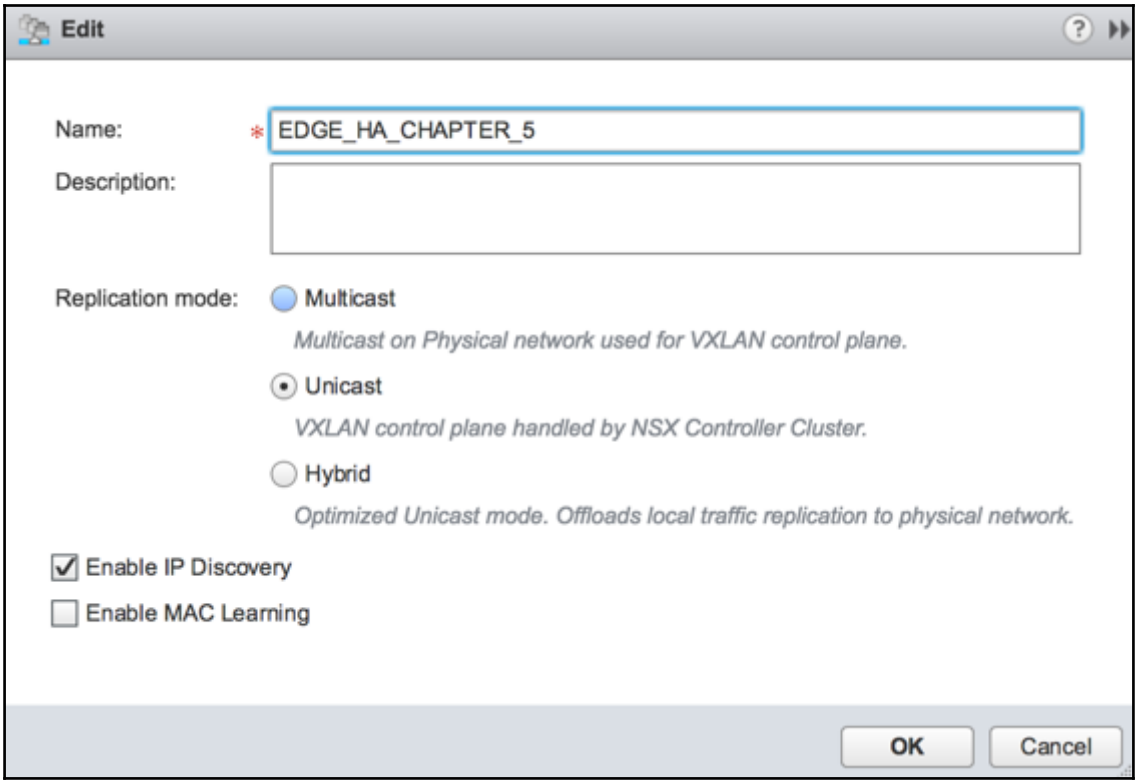

Add Private Network
Network:
172.16.33.0/24
Network should be entered in CIDR format e.g. 192.168.1.0/24
Description:
Web Servers
Send Traffic:
Over Tunnel
Bypass Tunnel
Enable TCP Optimization
Ports:
Status:
Enabled
Disabled
OK
Cancel

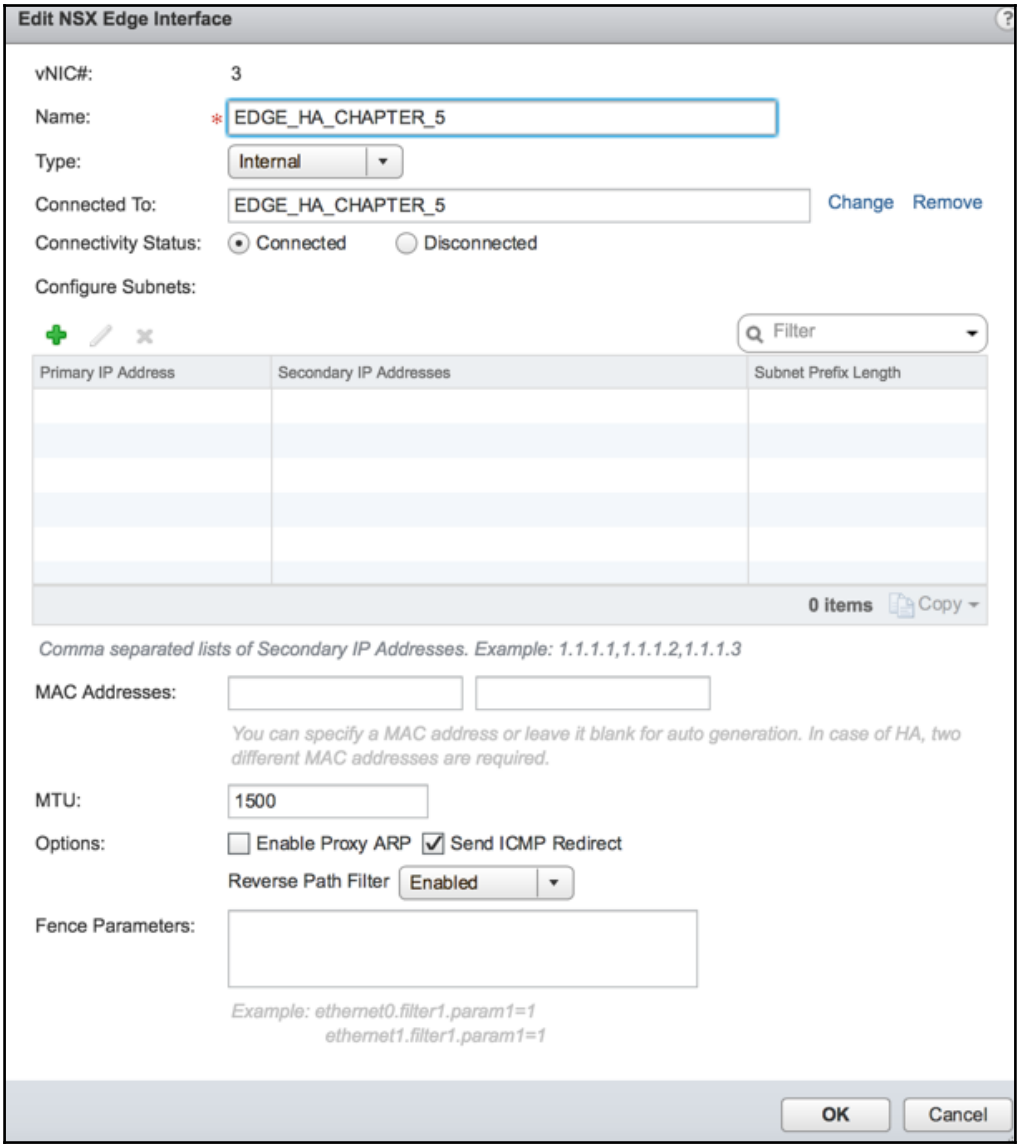

Add Authentication Server
Authentication Server Type
LOCAL
Enable password policy:
Password Length:
1
To
4
Minimum no. of alphabets:
Minimum no. of Digits:
Minimum no. of special characters:
Password should not contain user ID
Password expires in:
30
Day(s)
Expiry notification in:
25
Day(s)
Enable account lockout policy:
Retry Count:
3
User account will get locked after specific number of unsuccessful retries.
Retry Duration:
1
Min(s)
Lockout Duration:
1
Day(s)
Status:
Enabled
Disabled
Use this server for secondary authentication
Terminate Session if authentication fails
OK
Cancel

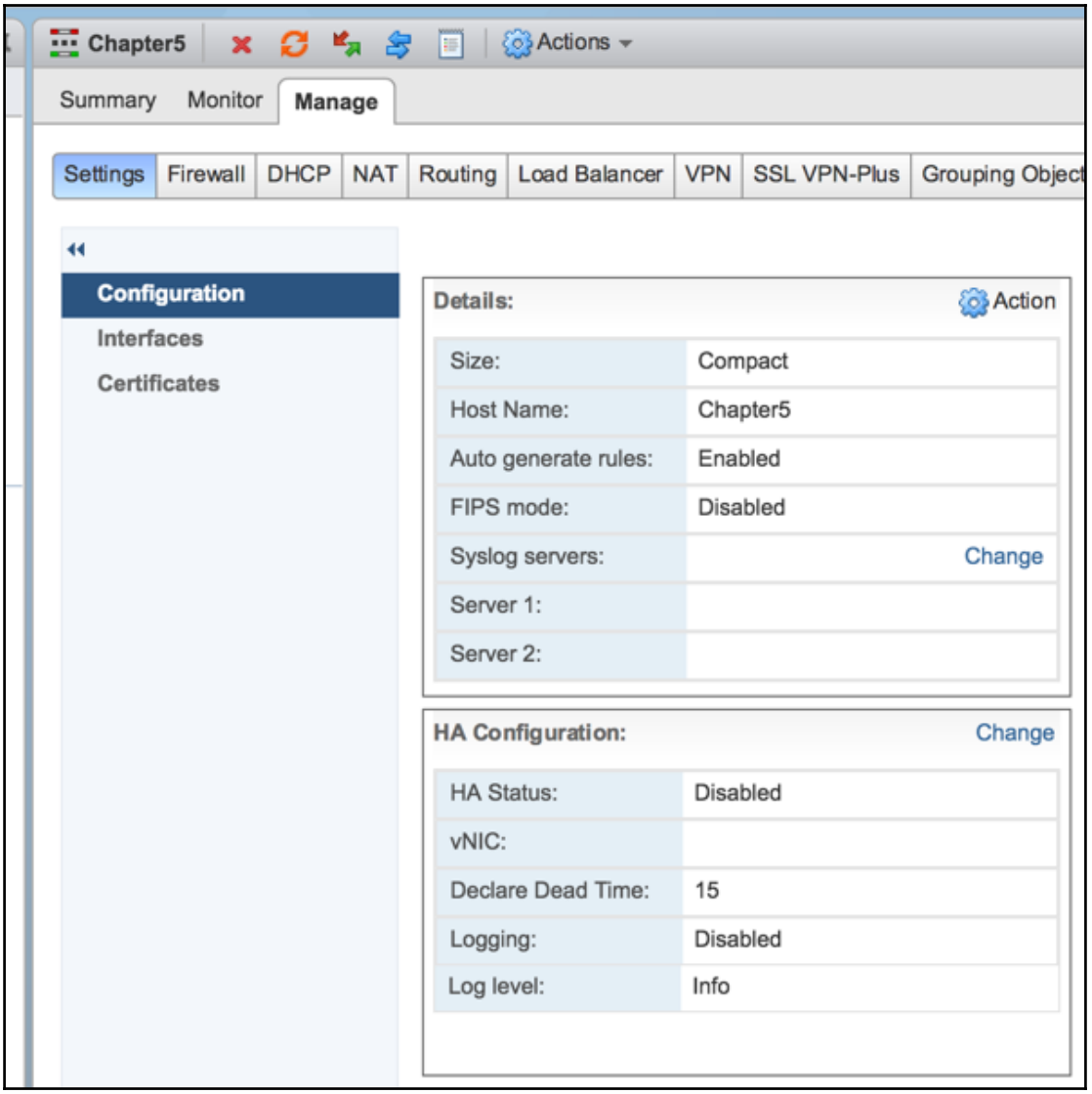

Add Installation Package
Profile Name: * PACKAGE_1
Gateway
Port
10.0.0.170
443
OK
Cancel
Create installation packages for:
Windows
Linux
Mac
Description:
Status:
Enabled
Disabled
Installation Parameters for Windows:
Start client on logon
Hide client system tray icon
Allow remember password
Create desktop icon
Enable silent mode installation
Enable silent mode operation
Hide SSL client network adapter
Server security certificate validation
Block user on certificate validation failure
OK
Cancel

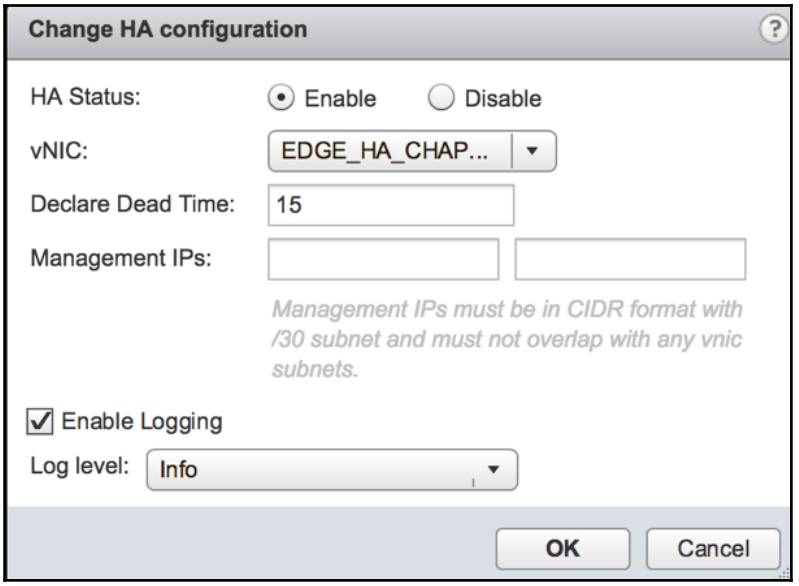

Add User
User ID:
vmware
Password:
****
Re-type Password:
****
First Name:
Last Name:
Description:
Password Details:
Password never expires:
Allow change password:
Change password on next login:
Status:
Enabled
Disabled
OK
Cancel

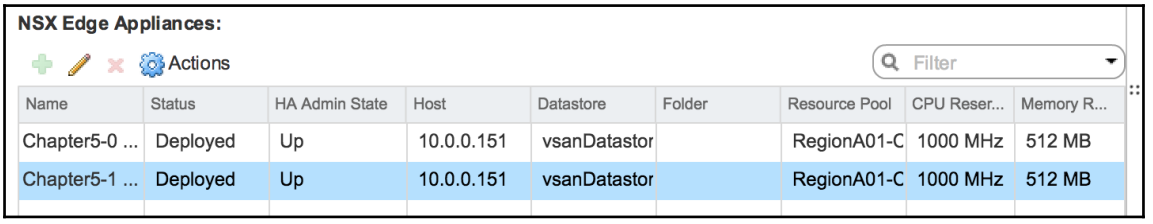

Chapter5
Actions
Summary
Monitor
Manage
Settings
Firewall
DHCP
NAT
Routing
Load Balancer
VPN
SSL VPN-Plus
Dashboard
Server Settings
IP Pools
Private Networks
Authentication
Installation Package
Users
Client Configuration
Login/Logoff Scripts
General Settings
Portal Customization
Status
Service:
Disabled
Enable
Statistics
Show For:
1 H
24 H
1 W
1 M
1 Y
Session Statistics
Active Sessions
Authentication Failures
100


Edit
Name:
EDGE_HA_CHAPTER_5
Description:
Replication mode:
Multicast
Multicast on Physical network used for VXLAN control plane.
Unicast
VXLAN control plane handled by NSX Controller Cluster.
Hybrid
Optimized Unicast mode. Offloads local traffic replication to physical network.
Enable IP Discovery
Enable MAC Learning
OK
Cancel


Edit NSX Edge Interface
vNIC#:
3
Name:
EDGE_HA_CHAPTER_5
Type:
Internal
Connected To:
EDGE_HA_CHAPTER_5
Change
Remove
Connectivity Status:
Connected
Disconnected
Configure Subnets:
Filter
Primary IP Address
Secondary IP Addresses
Subnet Prefix Length
0 items
Copy
Comma separated lists of Secondary IP Addresses. Example: 1.1.1.1,1.1.1.2,1.1.1.3
MAC Addresses:
You can specify a MAC address or leave it blank for auto generation. In case of HA, two different MAC addresses are required.
MTU:
1500
Options:
Enable Proxy ARP
Send ICMP Redirect
Reverse Path Filter
Enabled
Fence Parameters:
Example: ethernet0.filter1.param1=1
ethernet1.filter1.param1=1
OK
Cancel

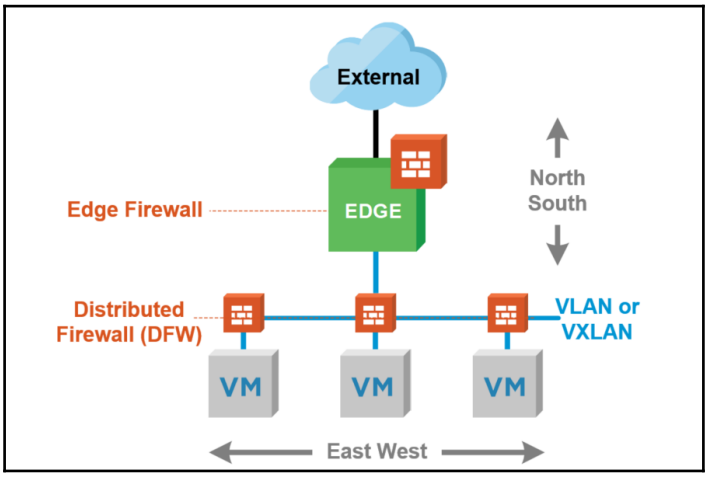

Chapter5
Actions
Summary
Monitor
Manage
Settings
Firewall
DHCP
NAT
Routing
Load Balancer
VPN
SSL VPN-Plus
Grouping Object
Configuration
Interfaces
Certificates
Details:
Action
Size:
Compact
Host Name:
Chapter5
Auto generate rules:
Enabled
FIPS mode:
Disabled
Syslog servers:
Change
Server 1:
Server 2:
HA Configuration:
Change
HA Status:
Disabled
vNIC:
Declare Dead Time:
15
Logging:
Disabled
Log level:
Info

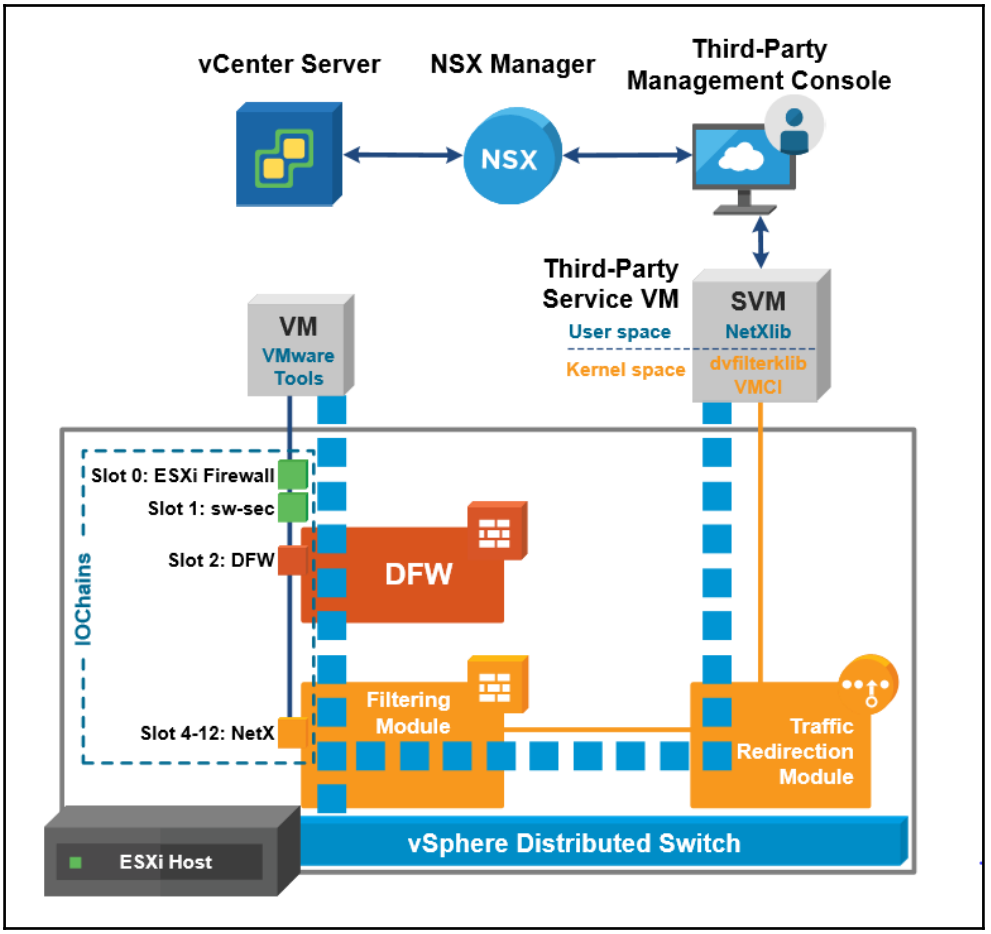

Change HA configuration
HA Status:
Enable
Disable
vNIC:
EDGE_HA_CHAP...
Declare Dead Time:
15
Management IPs:
Management IPs must be in CIDR format with /30 subnet and must not overlap with any vnic subnets.
Enable Logging
Log level:
Info
OK
Cancel

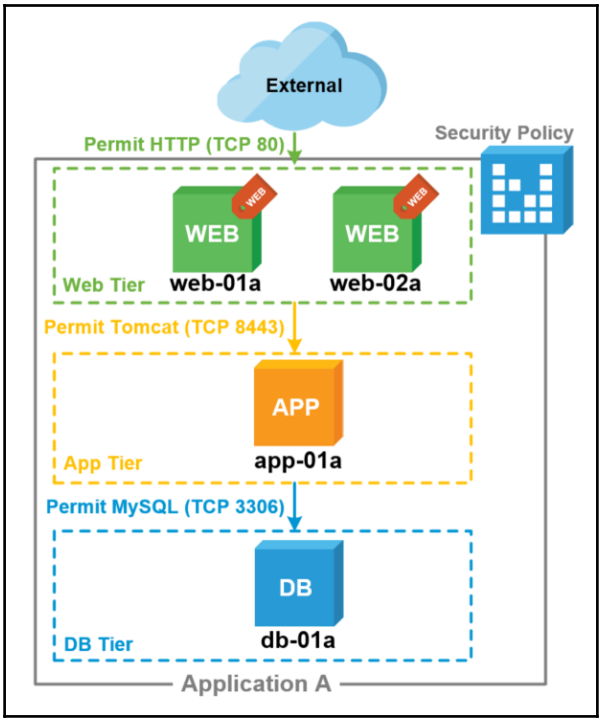

NSX Edge Appliances:
Actions
Filter
Name
Status
HA Admin State
Host
Datastore
Folder
Resource Pool
CPU Reser...
Memory R...
Chapter5-0 ...
Deployed
Up
10.0.0.151
vsanDatastor
RegionA01-C
1000 MHz
512 MB
Chapter5-1 ...
Deployed
Up
10.0.0.151
vsanDatastor
RegionA01-C
1000 MHz
512 MB

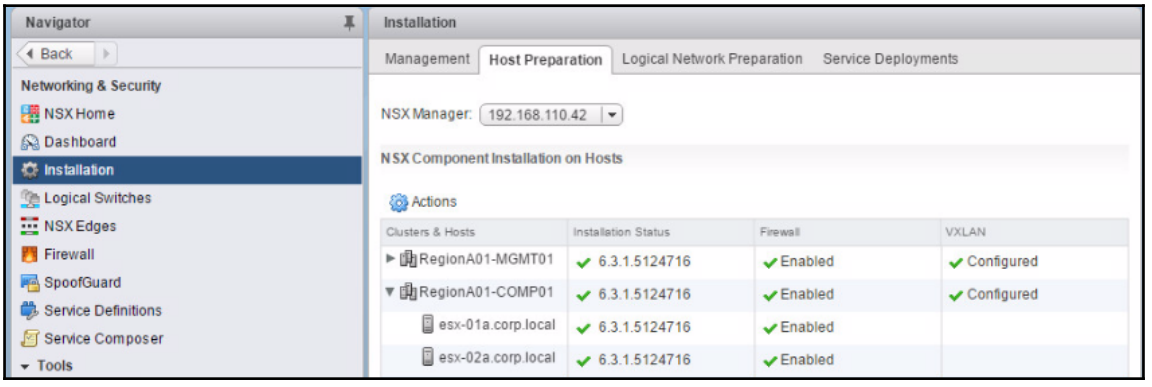
```
Chapter5-0> show service highavailability
Highavailability Service:
Highavailability Status:            Active
Highavailability State since:       2018-01-21 12:10:26.867
Highavailability Unit Id:           0
Highavailability Unit State:        Up
Highavailability Admin State:       Up
Highavailability Running Nodes:     0, 1
Unit Poll Policy:
    Frequency:                      3.75  seconds
    Deadtime:                       15    seconds
Highavailability Services Status:
    Healthcheck Config Channel:     Up
    Healthcheck Status Channel:     Up
Highavailability Healthcheck Status:
    This unit [0]: Up   Active: 1
    Peer unit [1]: Up   Active: 0
        Session via vNic_3: 169.254.1.9:169.254.1.10 Up
Config Engine:
    HA Configuration:               Enabled
    HA Admin State:                 Up
    Config Engine Status:           Active
Highavailability Stateful Logical Status:
    File-Sync                       running
    Connection-Sync                 running
      xmit       xerr       rcv        rerr
      3476       0          3096       0
```

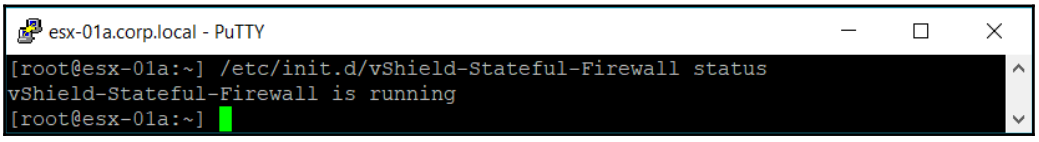
Chapter 06: Configuring VMware NSX Distributed Firewall (DFW) and SpoofGuard

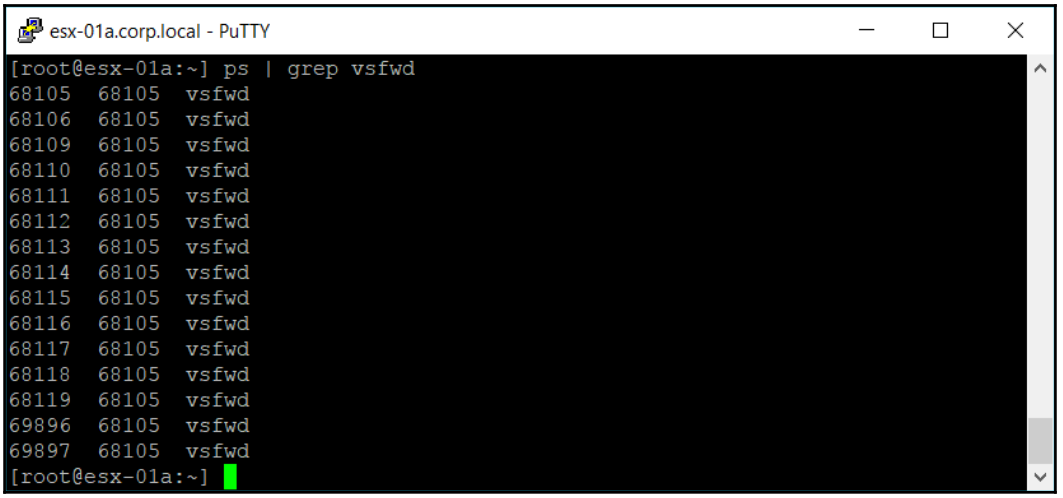


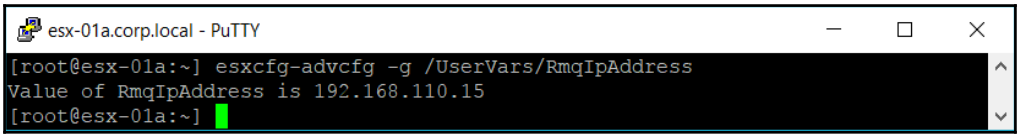

vCenter Server
NSX Manager
Third-Party Management Console
NSX
Third-Party Service VM
SVM
NetXlib
User space
Kernel space
dvfilterklib
VMCI
VM
VMware Tools
Slot 0: ESXi Firewall
Slot 1: sw-sec
Slot 2: DFW
DFW
IOChains
Filtering Module
Slot 4-12: NetX
Traffic Redirection Module
ESXi Host
vSphere Distributed Switch

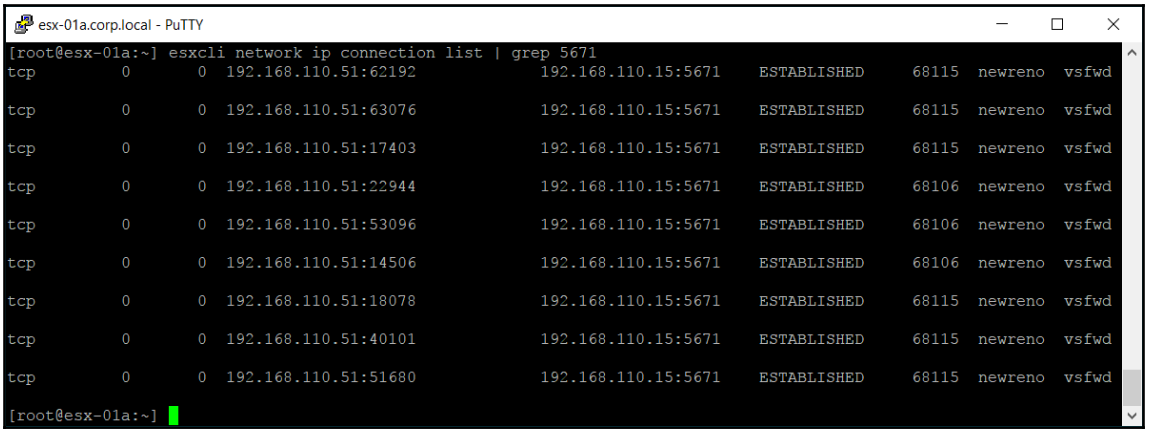

External
Permit HTTP (TCP 80)
Security Policy
WEB
WEB
Web Tier
web-01a
web-02a
Permit Tomcat (TCP 8443)
APP
App Tier
app-01a
Permit MySQL (TCP 3306)
DB
DB Tier
db-01a
Application A

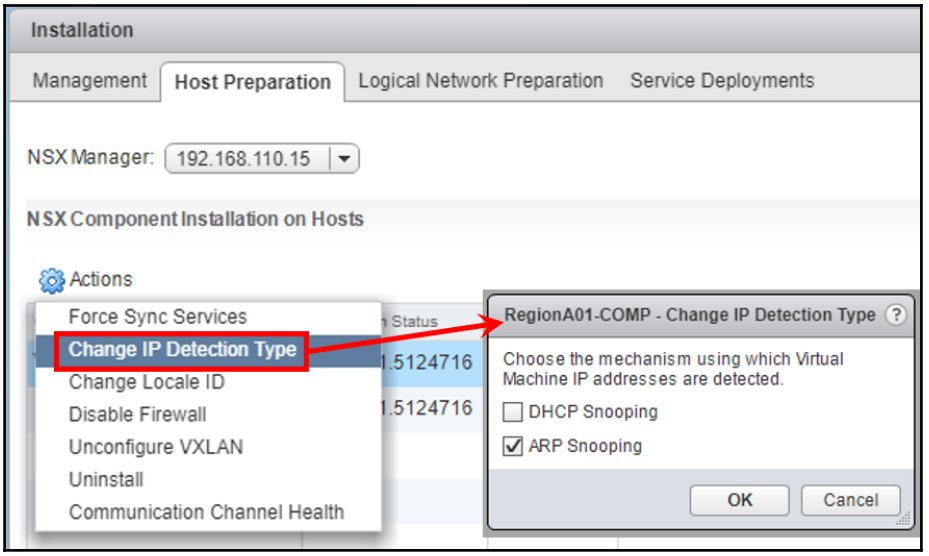

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Tools
Installation
Management
Host Preparation
Logical Network Preparation
Service Deployments
NSX Manager: 192.168.110.42
NSX Component Installation on Hosts
Actions
Clusters & Hosts
Installation Status
Firewall
VXLAN
RegionA01-MGMT01
6.3.1.5124716
Enabled
Configured
RegionA01-COMP01
6.3.1.5124716
Enabled
Configured
esx-01a.corp.local
6.3.1.5124716
Enabled
esx-02a.corp.local
6.3.1.5124716
Enabled

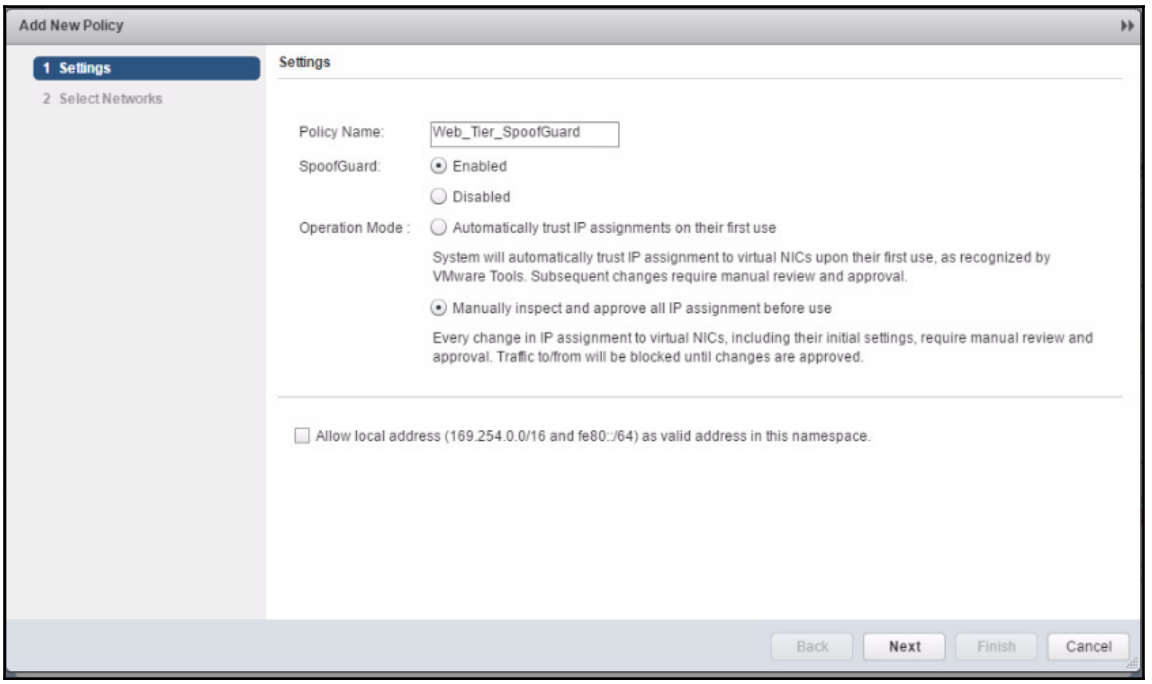

esx-01a.corp.local - PuTTY
[root@esx-01a:~] /etc/init.d/vShield-Stateful-Firewall status
vShield-Stateful-Firewall is running
[root@esx-01a:~]

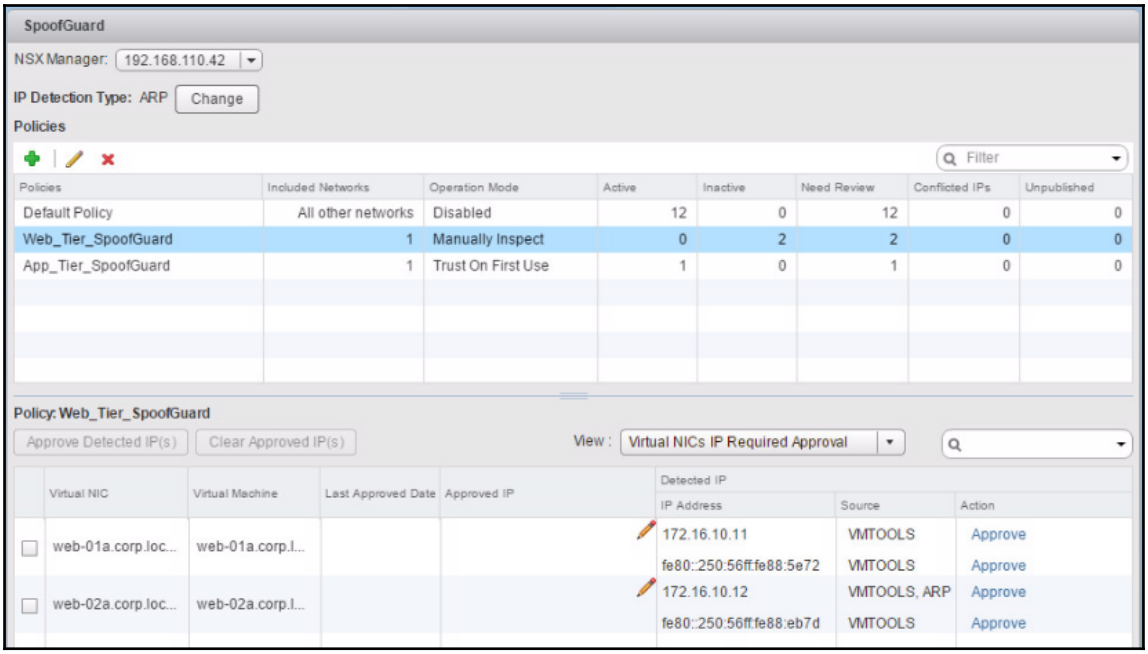

esx-01a.corp.local - PuTTY
[root@esx-01a:~] ps | grep vsfwd
68105 68105 vsfwd
68106 68105 vsfwd
68109 68105 vsfwd
68110 68105 vsfwd
68111 68105 vsfwd
68112 68105 vsfwd
68113 68105 vsfwd
68114 68105 vsfwd
68115 68105 vsfwd
68116 68105 vsfwd
68117 68105 vsfwd
68118 68105 vsfwd
68119 68105 vsfwd
69896 68105 vsfwd
69897 68105 vsfwd
[root@esx-01a:~]

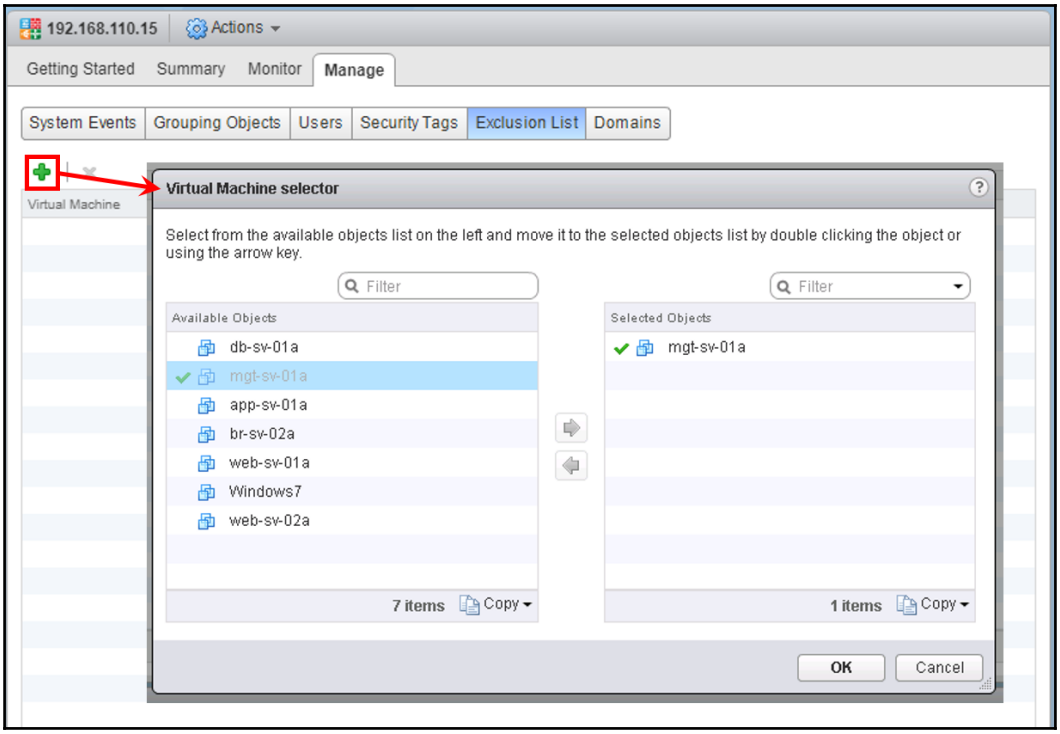

esx-01a.corp.local - PuTTY
[root@esx-01a:~] esxcfg-advcfg -g /UserVars/RmqIpAddress
Value of RmqIpAddress is 192.168.110.15
[root@esx-01a:~]

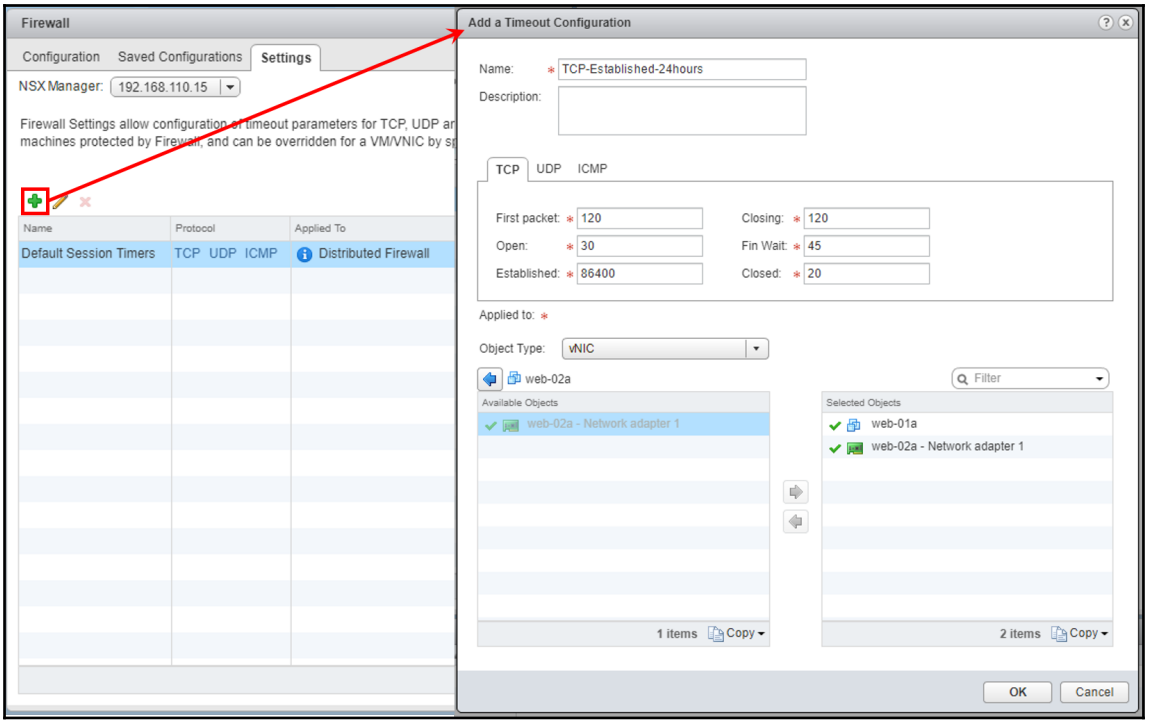

esx-01a.corp.local - PuTTY
[root@esx-01a:~] esxcli network ip connection list | grep 5671
tcp 0 0 192.168.110.51:62192 192.168.110.15:5671 ESTABLISHED 68115 newreno vsfwd
tcp 0 0 192.168.110.51:63076 192.168.110.15:5671 ESTABLISHED 68115 newreno vsfwd
tcp 0 0 192.168.110.51:17403 192.168.110.15:5671 ESTABLISHED 68115 newreno vsfwd
tcp 0 0 192.168.110.51:22944 192.168.110.15:5671 ESTABLISHED 68106 newreno vsfwd
tcp 0 0 192.168.110.51:53096 192.168.110.15:5671 ESTABLISHED 68106 newreno vsfwd
tcp 0 0 192.168.110.51:14506 192.168.110.15:5671 ESTABLISHED 68106 newreno vsfwd
tcp 0 0 192.168.110.51:18078 192.168.110.15:5671 ESTABLISHED 68115 newreno vsfwd
tcp 0 0 192.168.110.51:40101 192.168.110.15:5671 ESTABLISHED 68115 newreno vsfwd
tcp 0 0 192.168.110.51:51680 192.168.110.15:5671 ESTABLISHED 68115 newreno vsfwd
[root@esx-01a:~]

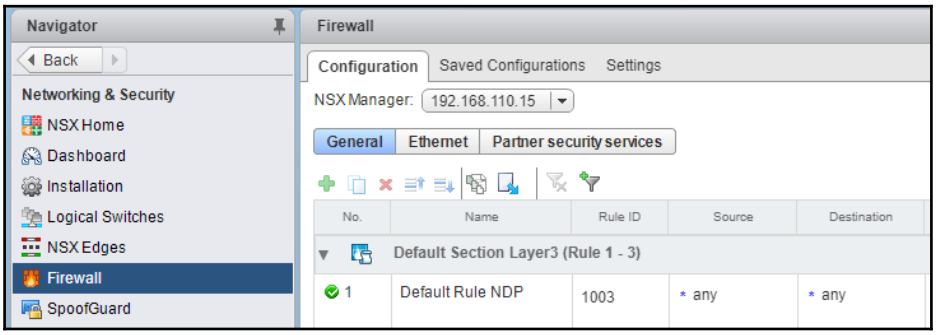

Installation
Management
Host Preparation
Logical Network Preparation
Service Deployments
NSX Manager:
192.168.110.15
NSX Component Installation on Hosts
Actions
Force Sync Services
Change IP Detection Type
Change Locale ID
Disable Firewall
Unconfigure VXLAN
Uninstall
Communication Channel Health
Status
RegionA01-COMP - Change IP Detection Type
Choose the mechanism using which Virtual Machine IP addresses are detected.
DHCP Snooping
ARP Snooping
OK
Cancel

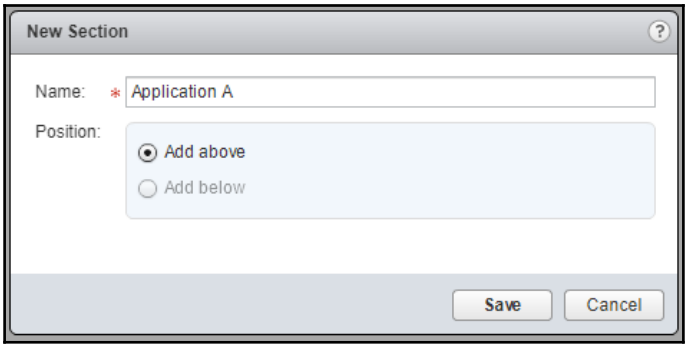

Add New Policy
1 Settings
2 Select Networks
Settings
Policy Name:
Web_Tier_SpoofGuard
SpoofGuard:
Enabled
Disabled
Operation Mode :
Automatically trust IP assignments on their first use
System will automatically trust IP assignment to virtual NICs upon their first use, as recognized by VMware Tools. Subsequent changes require manual review and approval.
Manually inspect and approve all IP assignment before use
Every change in IP assignment to virtual NICs, including their initial settings, require manual review and approval. Traffic to/from will be blocked until changes are approved.
Allow local address (169.254.0.0/16 and fe80::/64) as valid address in this namespace.
Back
Next
Finish
Cancel

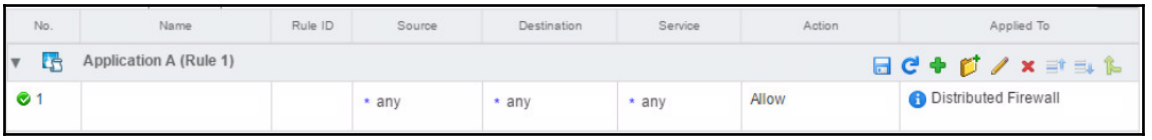

SpoofGuard
NSX Manager: 192.168.110.42
IP Detection Type: ARP
Change
Policies
Filter
Policies
Included Networks
Operation Mode
Active
Inactive
Need Review
Conflicted IPs
Unpublished
Default Policy
All other networks
Disabled
12
0
12
0
0
Web_Tier_SpoofGuard
1
Manually Inspect
0
2
2
0
0
App_Tier_SpoofGuard
1
Trust On First Use
1
0
1
0
0
Policy: Web_Tier_SpoofGuard
Approve Detected IP(s)
Clear Approved IP(s)
View :
Virtual NICs IP Required Approval
Virtual NIC
Virtual Machine
Last Approved Date
Approved IP
Detected IP
IP Address
Source
Action
web-01a.corp.loc...
web-01a.corp.l...
172.16.10.11
VMTOOLS
Approve
fe80::250:56ff:fe88:5e72
VMTOOLS
Approve
web-02a.corp.loc...
web-02a.corp.l...
172.16.10.12
VMTOOLS, ARP
Approve
fe80::250:56ff:fe88:eb7d
VMTOOLS
Approve

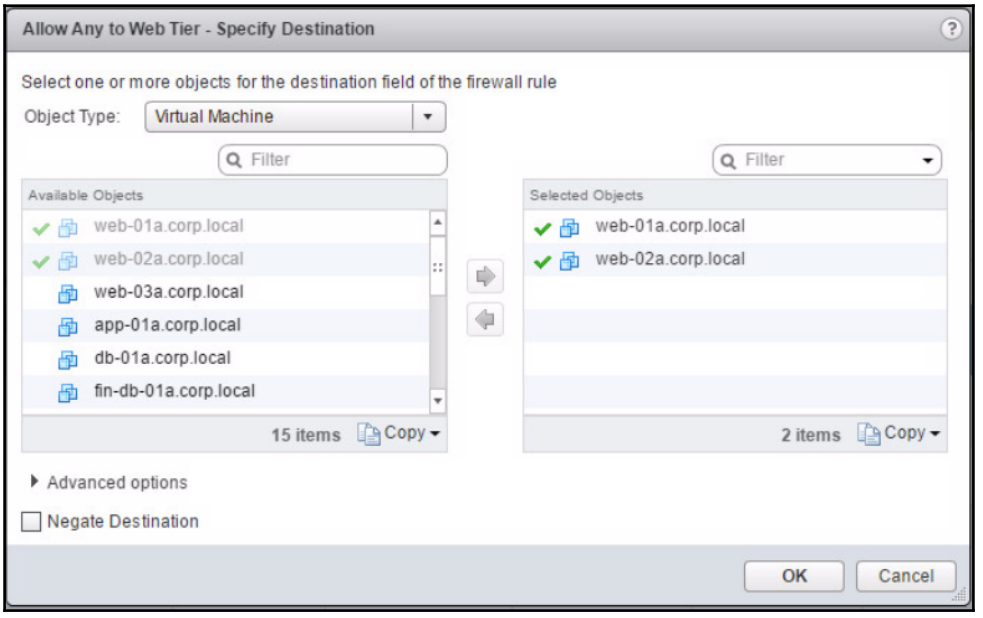

192.168.110.15
Actions
Getting Started
Summary
Monitor
Manage
System Events
Grouping Objects
Users
Security Tags
Exclusion List
Domains
Virtual Machine
Virtual Machine selector
Select from the available objects list on the left and move it to the selected objects list by double clicking the object or using the arrow key.
Filter
Available Objects
db-sv-01a
mgt-sv-01a
app-sv-01a
br-sv-02a
web-sv-01a
Windows7
web-sv-02a
7 items
Copy
Filter
Selected Objects
mgt-sv-01a
1 items
Copy
OK
Cancel

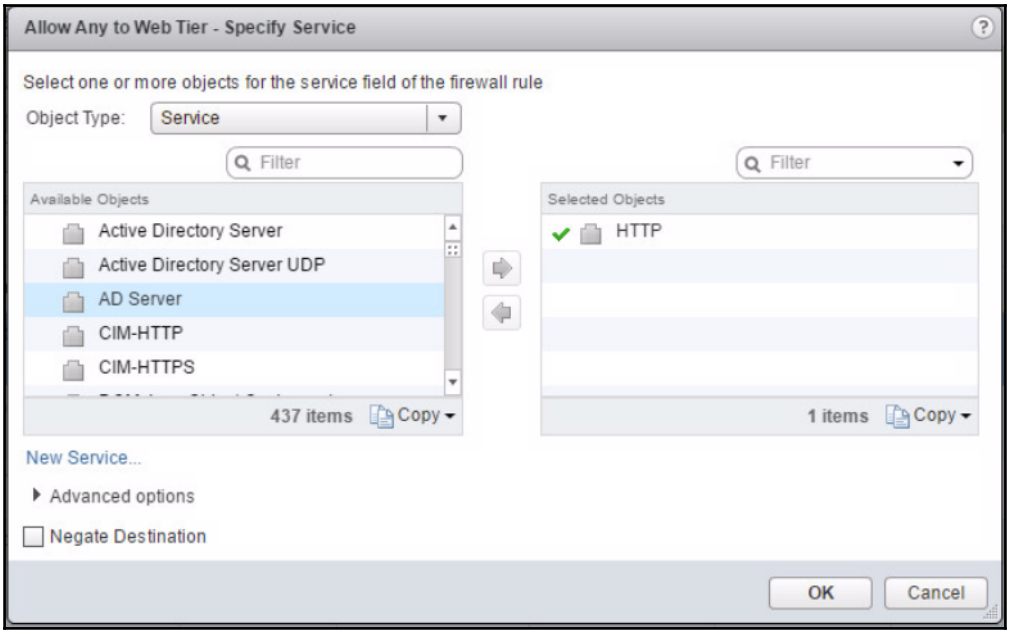

Firewall
Configuration
Saved Configurations
Settings
NSX Manager:
192.168.110.15
Firewall Settings allow configuration of timeout parameters for TCP, UDP ar
machines protected by Firewall, and can be overridden for a VM/VNIC by sp
Name
Protocol
Applied To
Default Session Timers
TCP UDP ICMP
Distributed Firewall
Add a Timeout Configuration
Name:
TCP-Established-24hours
Description:
TCP
UDP
ICMP
First packet:
120
Closing:
120
Open:
30
Fin Wait:
45
Established:
86400
Closed:
20
Applied to:
Object Type:
vNIC
web-02a
Filter
Available Objects
web-02a - Network adapter 1
Selected Objects
web-01a
web-02a - Network adapter 1
1 items
Copy
2 items
Copy
OK
Cancel

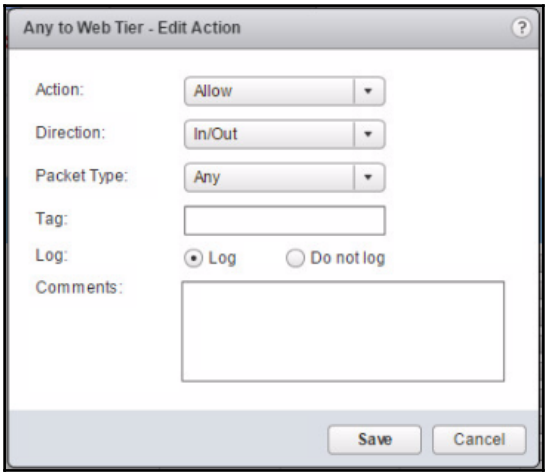

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Firewall
Configuration
Saved Configurations
Settings
NSX Manager:
192.168.110.15
General
Ethernet
Partner security services
No.
Name
Rule ID
Source
Destination
Default Section Layer3 (Rule 1 - 3)
1
Default Rule NDP
1003
any
any


New Section
Name:
Application A
Position:
Add above
Add below
Save
Cancel

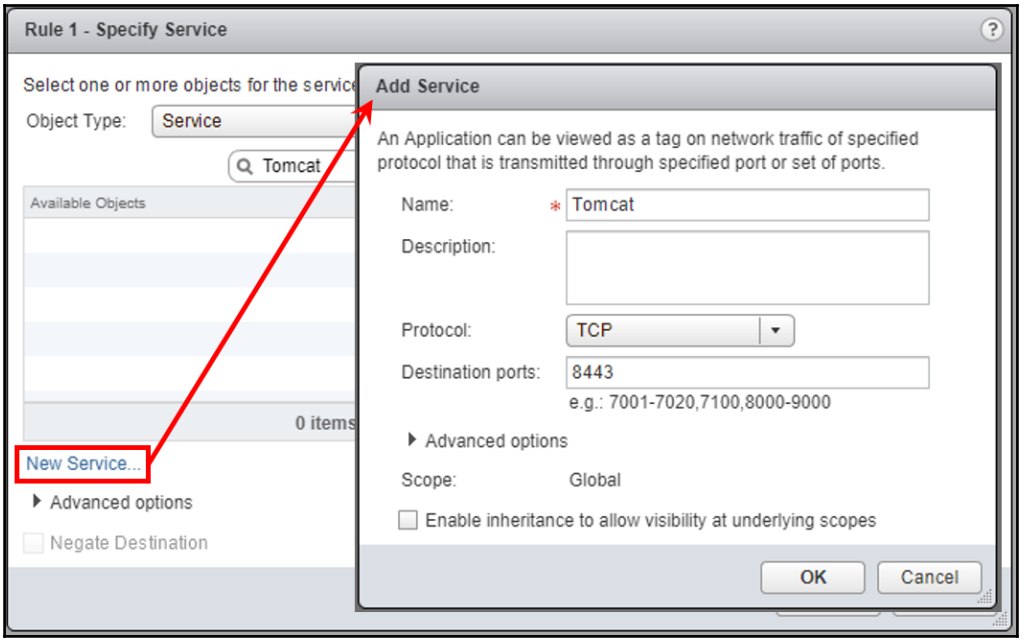

No.
Name
Rule ID
Source
Destination
Service
Action
Applied To
Application A (Rule 1)
1
any
any
any
Allow
Distributed Firewall

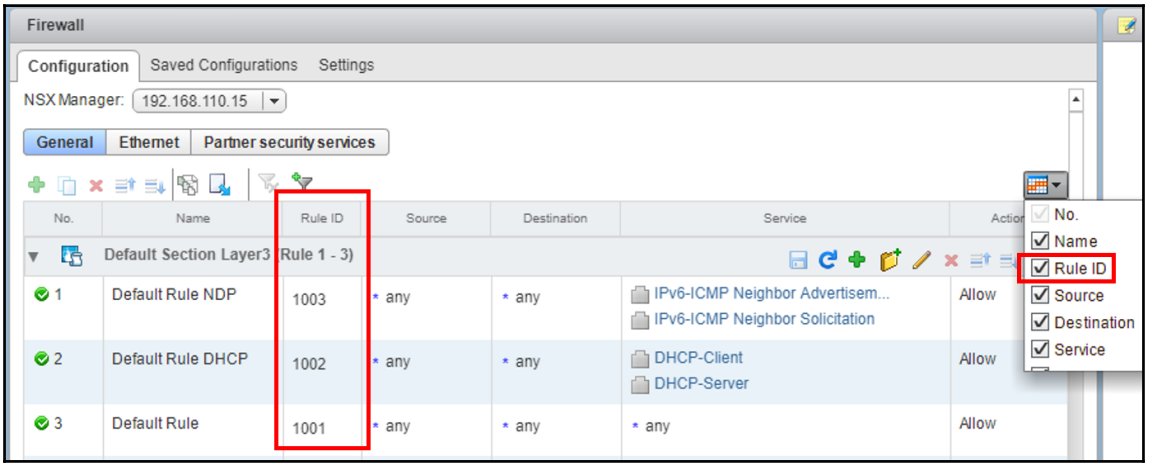

Allow Any to Web Tier - Specify Destination
Select one or more objects for the destination field of the firewall rule
Object Type:
Virtual Machine
Filter
Available Objects
web-01a.corp.local
web-02a.corp.local
web-03a.corp.local
app-01a.corp.local
db-01a.corp.local
fin-db-01a.corp.local
15 items
Copy
Filter
Selected Objects
web-01a.corp.local
web-02a.corp.local
2 items
Copy
Advanced options
Negate Destination
OK
Cancel

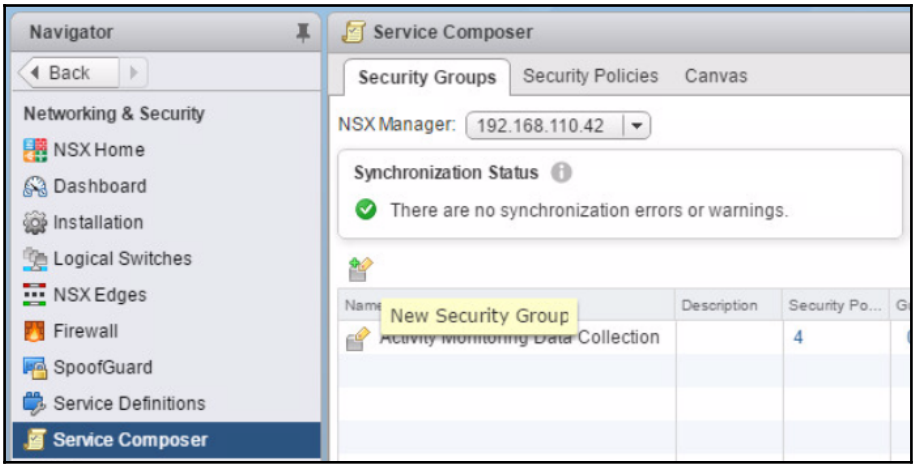

Allow Any to Web Tier - Specify Service
Select one or more objects for the service field of the firewall rule
Object Type:
Service
Filter
Filter
Available Objects
Active Directory Server
Active Directory Server UDP
AD Server
CIM-HTTP
CIM-HTTPS
437 items
Copy
Selected Objects
HTTP
1 items
Copy
New Service...
Advanced options
Negate Destination
OK
Cancel

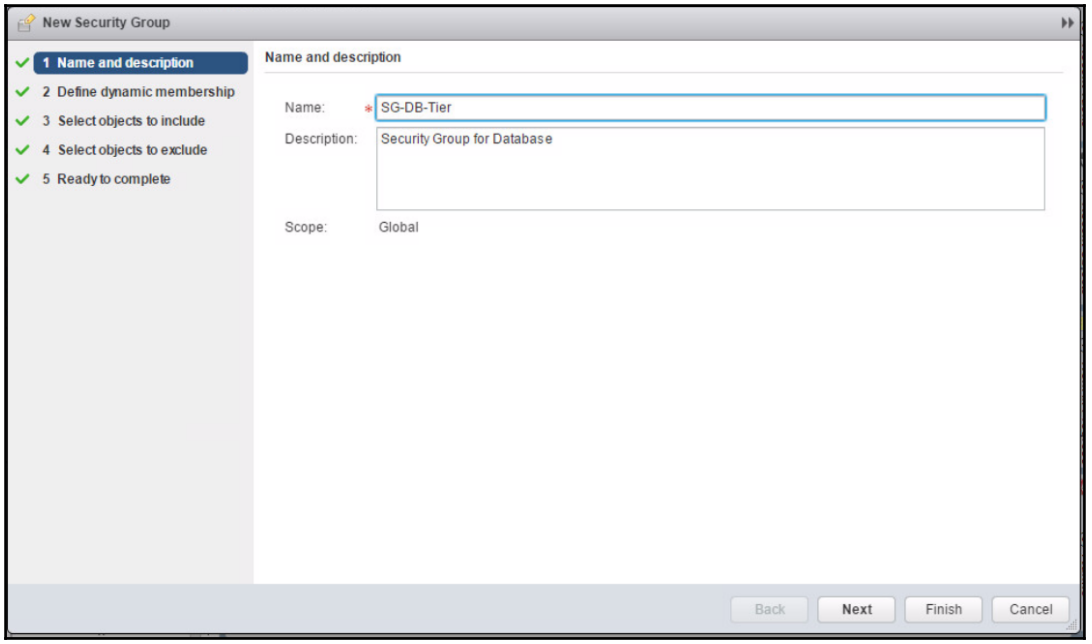

Any to Web Tier - Edit Action
Action:
Allow
Direction:
In/Out
Packet Type:
Any
Tag:
Log:
Log
Do not log
Comments:
Save
Cancel

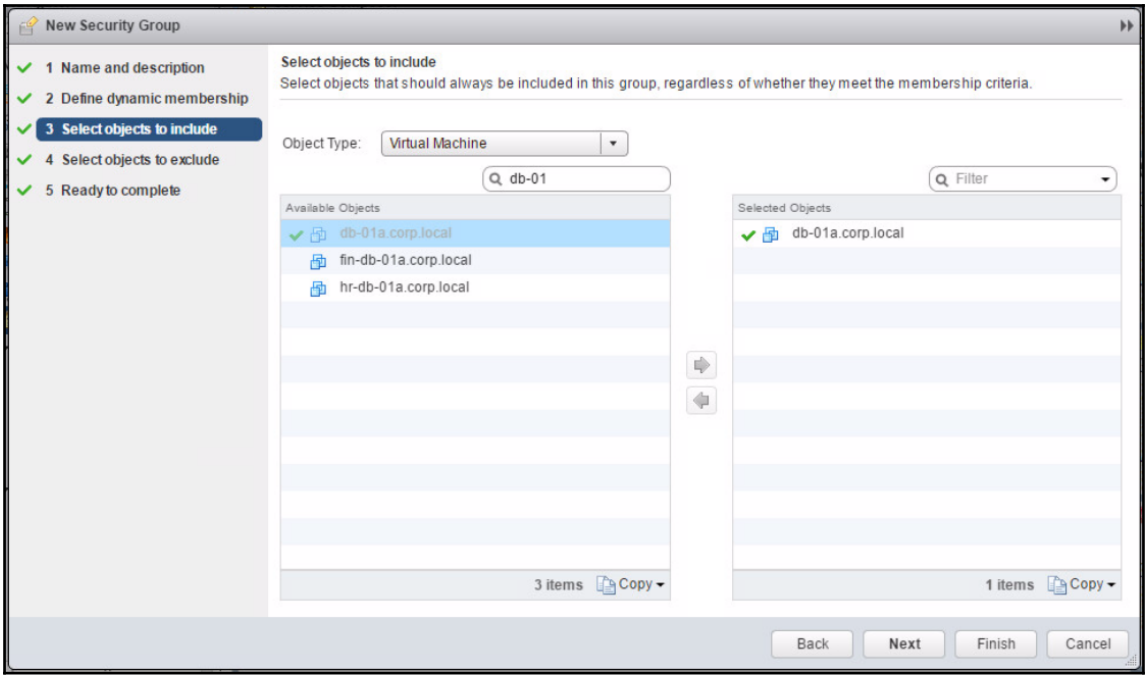

Application A (Rule 1 - 3)
1
Allow HTTP to Web Tier
1009
any
web-01...
web-02...
HTTP
Allow
Distributed Fir...
2
Allow Web Tier to App Tier
1008
web-01a....
web-02a....
app-01...
Tomcat
Allow
Distributed Fir...
3
Allow App Tier to DB Tier
1007
app-01a....
db-01a....
MySQL
Allow
Distributed Fir...

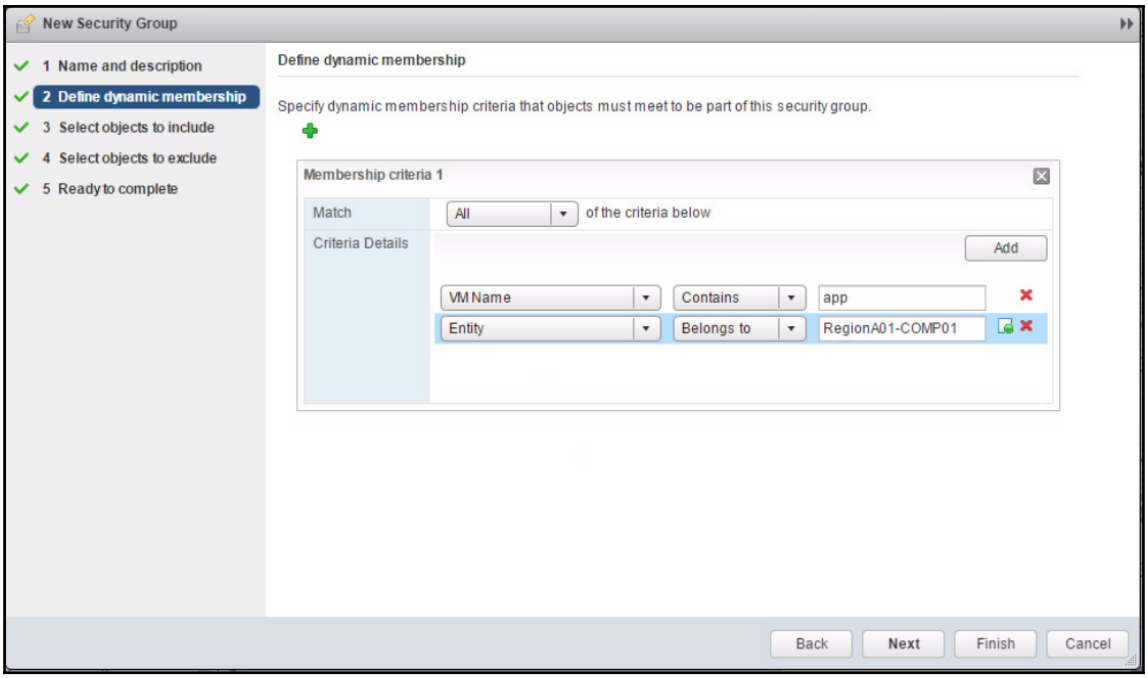

Rule 1 - Specify Service
Select one or more objects for the service
Object Type:
Service
Tomcat
Available Objects
0 items
New Service...
Advanced options
Negate Destination
Add Service
An Application can be viewed as a tag on network traffic of specified protocol that is transmitted through specified port or set of ports.
Name:
Tomcat
Description:
Protocol:
TCP
Destination ports:
8443
e.g.: 7001-7020,7100,8000-9000
Advanced options
Scope:
Global
Enable inheritance to allow visibility at underlying scopes
OK
Cancel

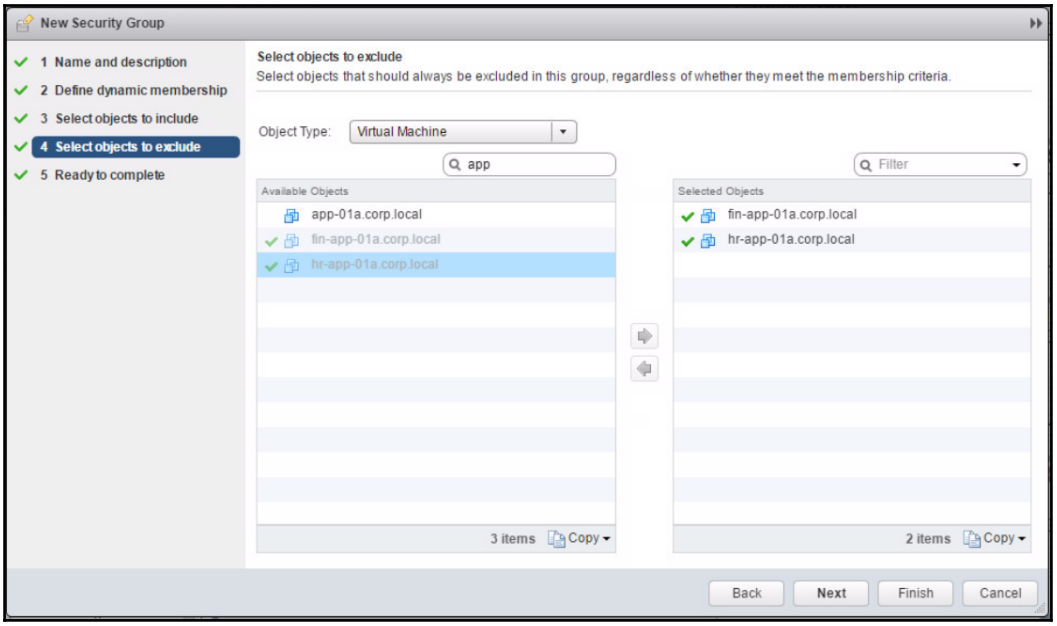

Firewall
Configuration
Saved Configurations
Settings
NSX Manager:
192.168.110.15
General
Ethernet
Partner security services
No.
Name
Rule ID
Source
Destination
Service
Action
Default Section Layer3 (Rule 1 - 3)
1
Default Rule NDP
1003
any
any
IPv6-ICMP Neighbor Advertisem...
IPv6-ICMP Neighbor Solicitation
Allow
2
Default Rule DHCP
1002
any
any
DHCP-Client
DHCP-Server
Allow
3
Default Rule
1001
any
any
any
Allow
No.
Name
Rule ID
Source
Destination
Service

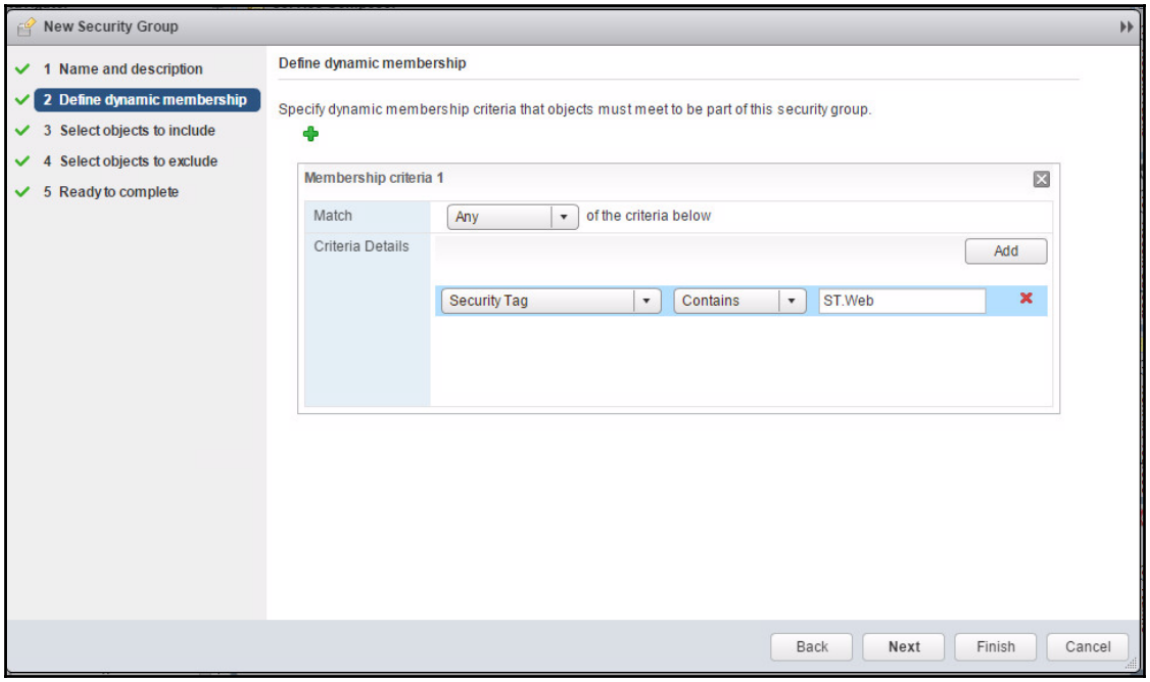

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Service Composer
Security Groups
Security Policies
Canvas
NSX Manager:
192.168.110.42
Synchronization Status
There are no synchronization errors or warnings.
New Security Group
Description
Security Po...
4

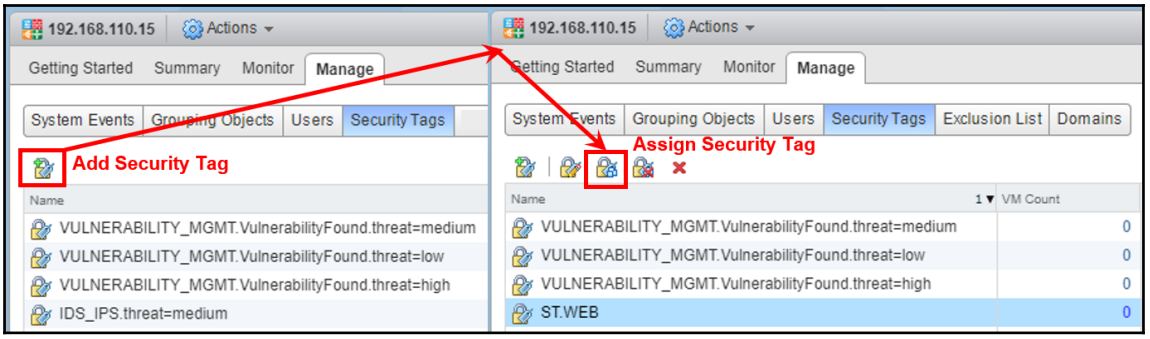

New Security Group
1 Name and description
2 Define dynamic membership
3 Select objects to include
4 Select objects to exclude
5 Ready to complete
Name and description
Name:
SG-DB-Tier
Description:
Security Group for Database
Scope:
Global
Back
Next
Finish
Cancel

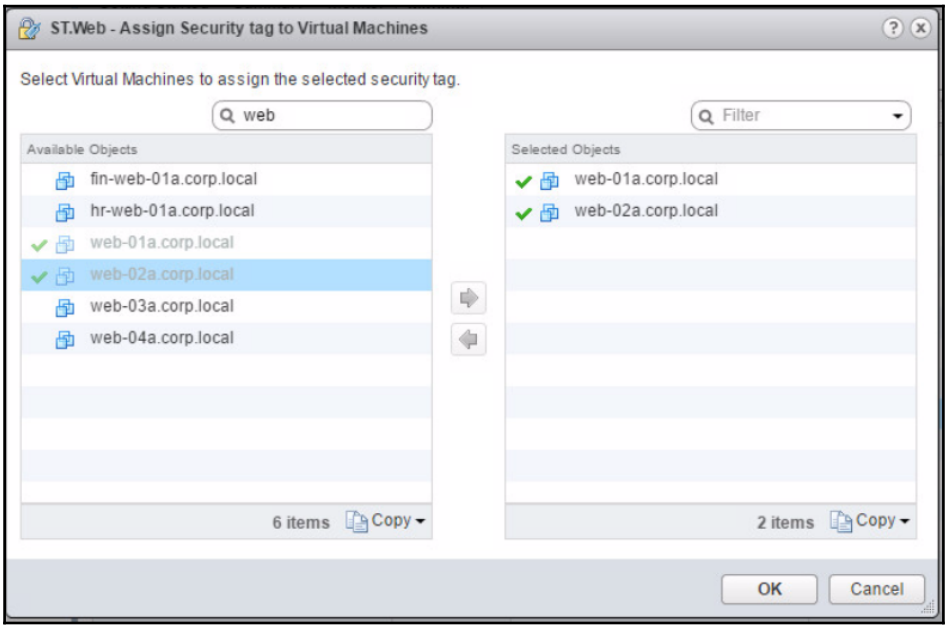

New Security Group
1 Name and description
2 Define dynamic membership
3 Select objects to include
4 Select objects to exclude
5 Ready to complete
Select objects to include
Select objects that should always be included in this group, regardless of whether they meet the membership criteria.
Object Type:
Virtual Machine
db-01
Filter
Available Objects
db-01a.corp.local
fin-db-01a.corp.local
hr-db-01a.corp.local
Selected Objects
db-01a.corp.local
3 items
Copy
1 items
Copy
Back
Next
Finish
Cancel

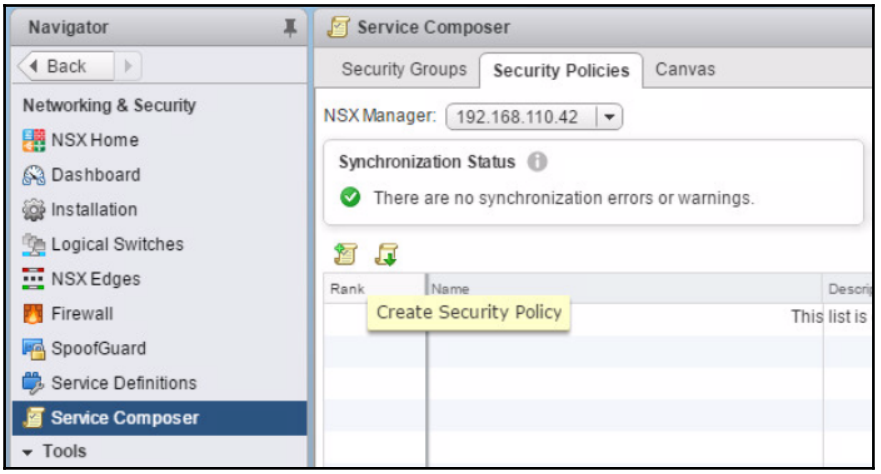

New Security Group
1 Name and description
2 Define dynamic membership
3 Select objects to include
4 Select objects to exclude
5 Ready to complete
Define dynamic membership
Specify dynamic membership criteria that objects must meet to be part of this security group.
Membership criteria 1
Match
All
of the criteria below
Criteria Details
Add
VM Name
Contains
app
Entity
Belongs to
RegionA01-COMP01
Back
Next
Finish
Cancel

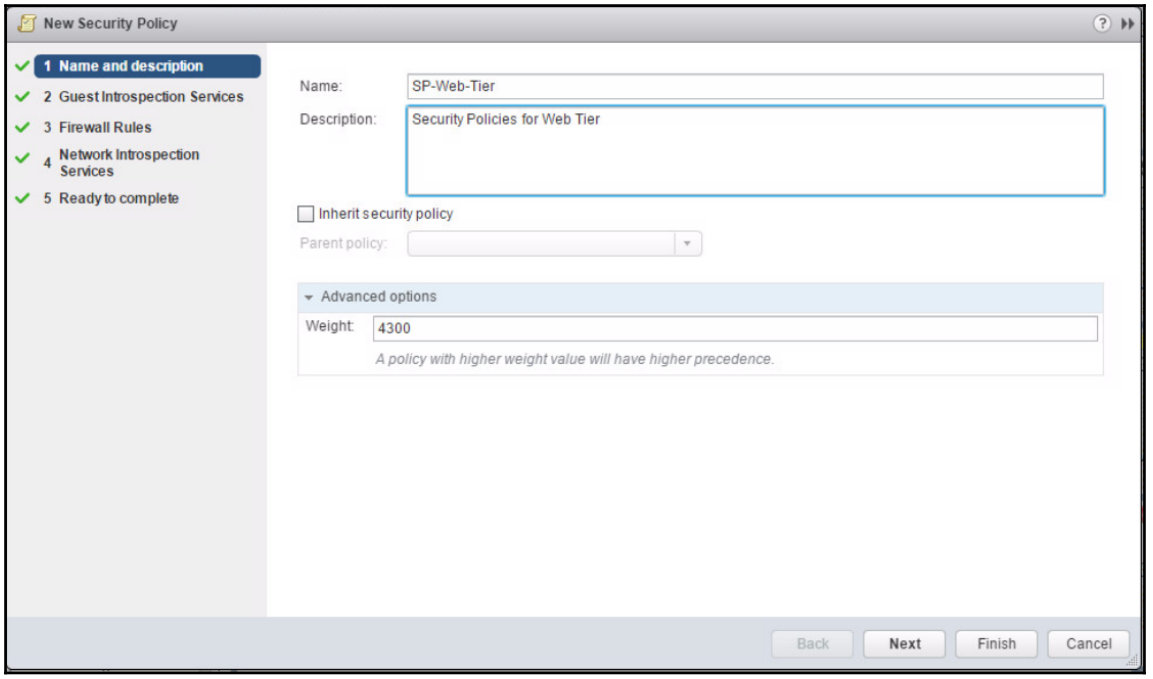

New Security Group
1 Name and description
2 Define dynamic membership
3 Select objects to include
4 Select objects to exclude
5 Ready to complete
Select objects to exclude
Select objects that should always be excluded in this group, regardless of whether they meet the membership criteria.
Object Type: Virtual Machine
app
Filter
Available Objects
app-01a.corp.local
fin-app-01a.corp.local
hr-app-01a.corp.local
Selected Objects
fin-app-01a.corp.local
hr-app-01a.corp.local
3 items
Copy
2 items
Copy
Back
Next
Finish
Cancel

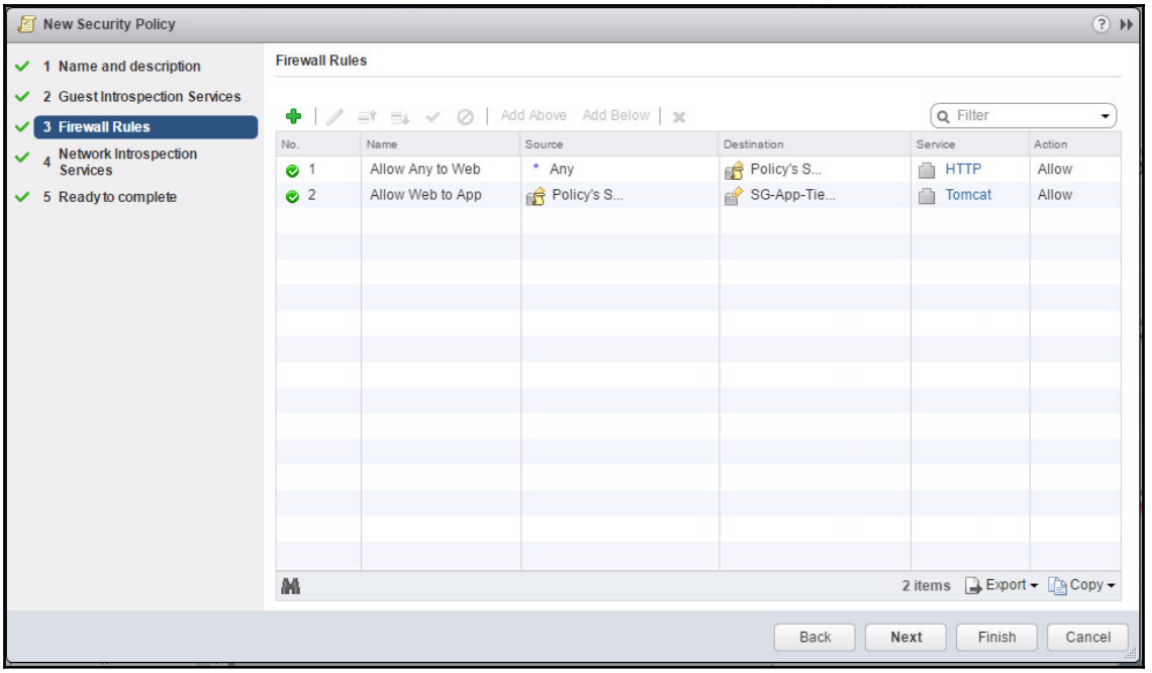

New Security Group
1 Name and description
2 Define dynamic membership
3 Select objects to include
4 Select objects to exclude
5 Ready to complete
Define dynamic membership
Specify dynamic membership criteria that objects must meet to be part of this security group.
Membership criteria 1
Match
Any
of the criteria below
Criteria Details
Add
Security Tag
Contains
ST.Web
Back
Next
Finish
Cancel

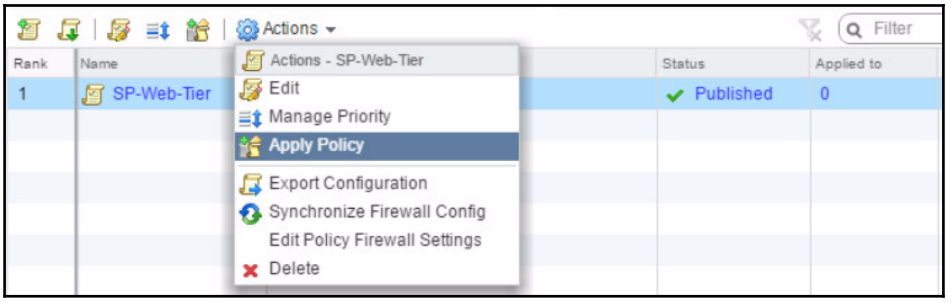

192.168.110.15
Actions
Getting Started
Summary
Monitor
Manage
System Events
Grouping Objects
Users
Security Tags
Add Security Tag
Name
VULNERABILITY_MGMT.VulnerabilityFound.threat=medium
VULNERABILITY_MGMT.VulnerabilityFound.threat=low
VULNERABILITY_MGMT.VulnerabilityFound.threat=high
IDS_IPS.threat=medium
192.168.110.15
Actions
Getting Started
Summary
Monitor
Manage
System Events
Grouping Objects
Users
Security Tags
Exclusion List
Domains
Assign Security Tag
Name
VM Count
VULNERABILITY_MGMT.VulnerabilityFound.threat=medium 0
VULNERABILITY_MGMT.VulnerabilityFound.threat=low 0
VULNERABILITY_MGMT.VulnerabilityFound.threat=high 0
ST.WEB 0

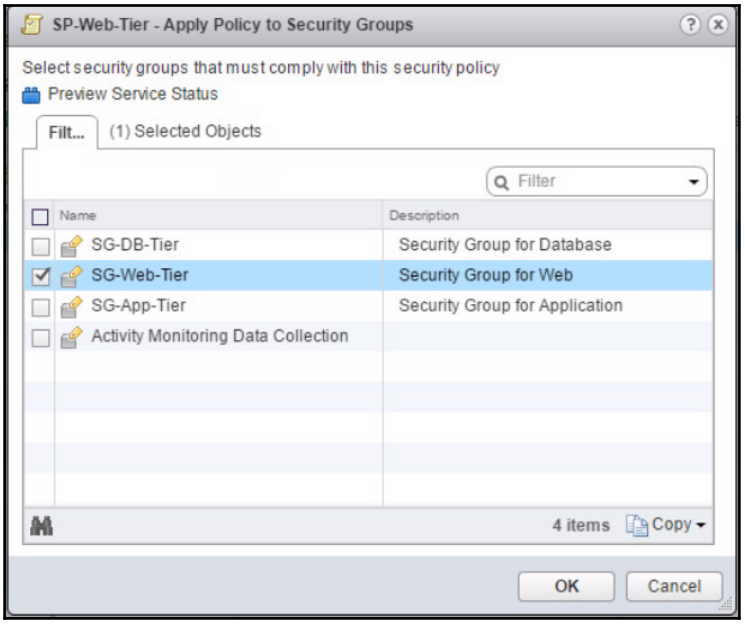

ST.Web - Assign Security tag to Virtual Machines
Select Virtual Machines to assign the selected security tag.
web
Filter
Available Objects
fin-web-01a.corp.local
hr-web-01a.corp.local
web-01a.corp.local
web-02a.corp.local
web-03a.corp.local
web-04a.corp.local
Selected Objects
web-01a.corp.local
web-02a.corp.local
6 items
Copy
2 items
Copy
OK
Cancel

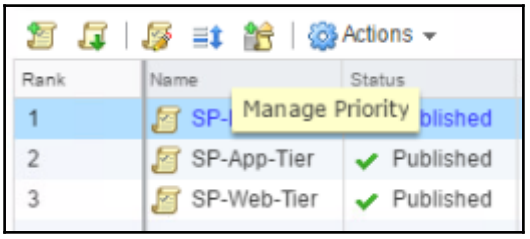

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Tools
Service Composer
Security Groups
Security Policies
Canvas
NSX Manager:
192.168.110.42
Synchronization Status
There are no synchronization errors or warnings.
Rank
Name
Create Security Policy
This list is

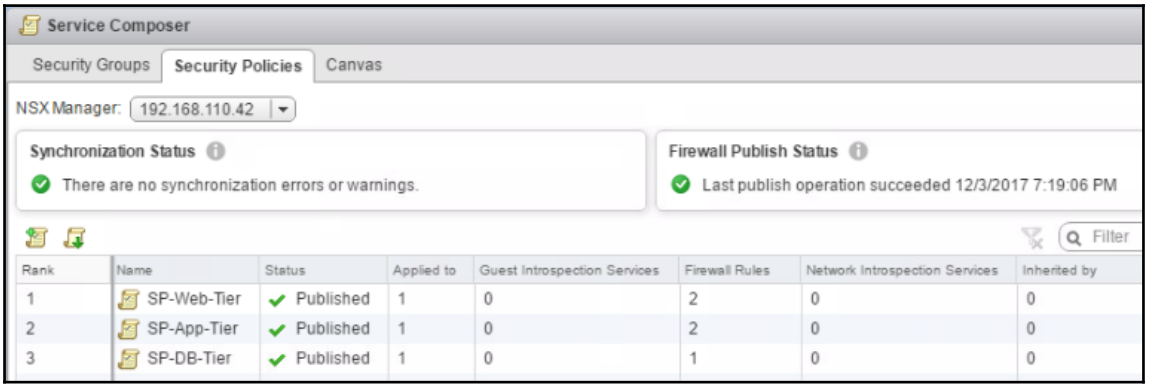

New Security Policy
1 Name and description
2 Guest Introspection Services
3 Firewall Rules
4 Network Introspection Services
5 Ready to complete
Name:
SP-Web-Tier
Description:
Security Policies for Web Tier
Inherit security policy
Parent policy:
Advanced options
Weight:
4300
A policy with higher weight value will have higher precedence.
Back
Next
Finish
Cancel

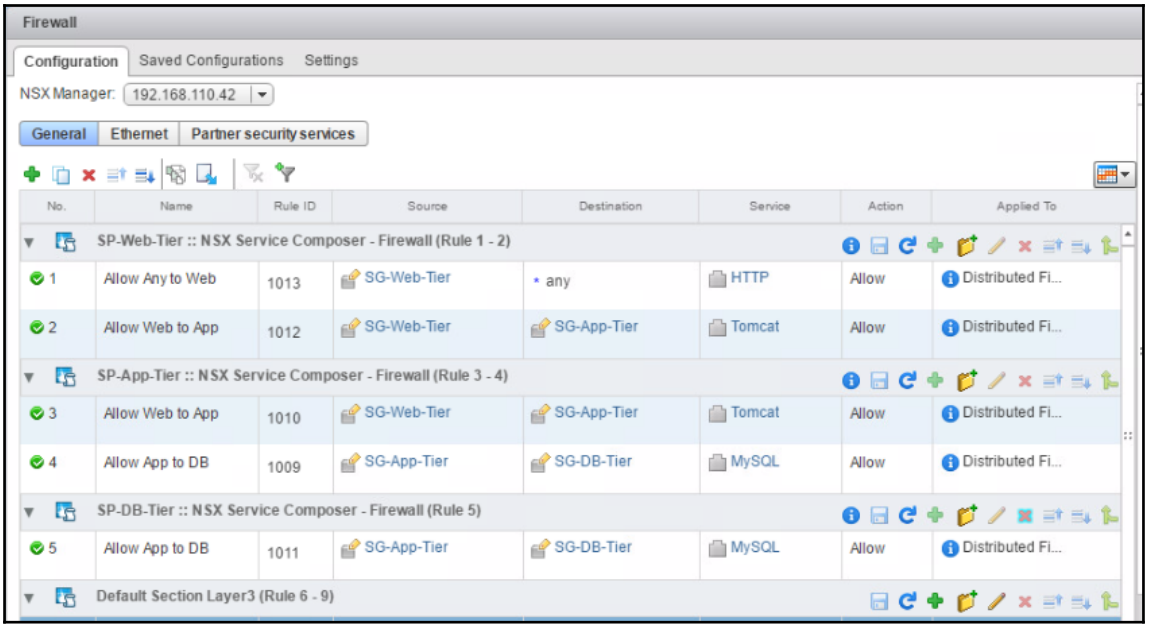

New Security Policy
1 Name and description
2 Guest Introspection Services
3 Firewall Rules
4 Network Introspection Services
5 Ready to complete
Firewall Rules
Add Above
Add Below
Filter
No.
Name
Source
Destination
Service
Action
1
Allow Any to Web
Any
Policy's S...
HTTP
Allow
2
Allow Web to App
Policy's S...
SG-App-Tie...
Tomcat
Allow
2 items
Export
Copy
Back
Next
Finish
Cancel


Actions
Filter
Rank
Name
Status
Applied to
1
SP-Web-Tier
Published
0
Actions - SP-Web-Tier
Edit
Manage Priority
Apply Policy
Export Configuration
Synchronize Firewall Config
Edit Policy Firewall Settings
Delete

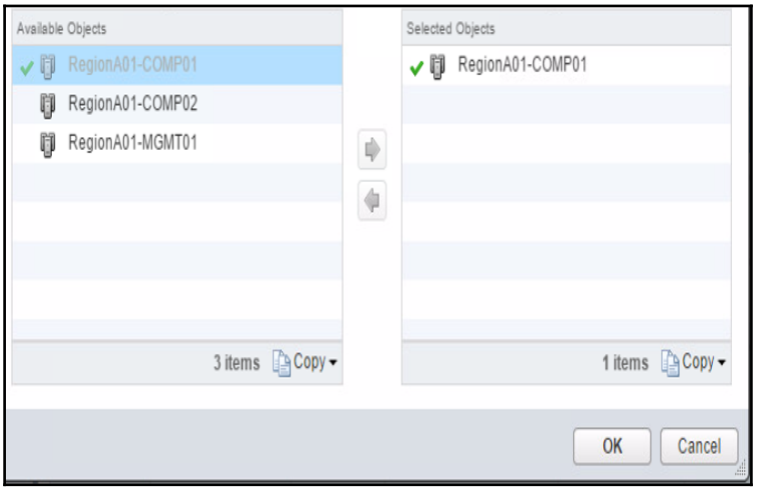

SP-Web-Tier - Apply Policy to Security Groups
Select security groups that must comply with this security policy
Preview Service Status
Filt...
(1) Selected Objects
Filter
Name
Description
SG-DB-Tier
Security Group for Database
SG-Web-Tier
Security Group for Web
SG-App-Tier
Security Group for Application
Activity Monitoring Data Collection
4 items
Copy
OK
Cancel

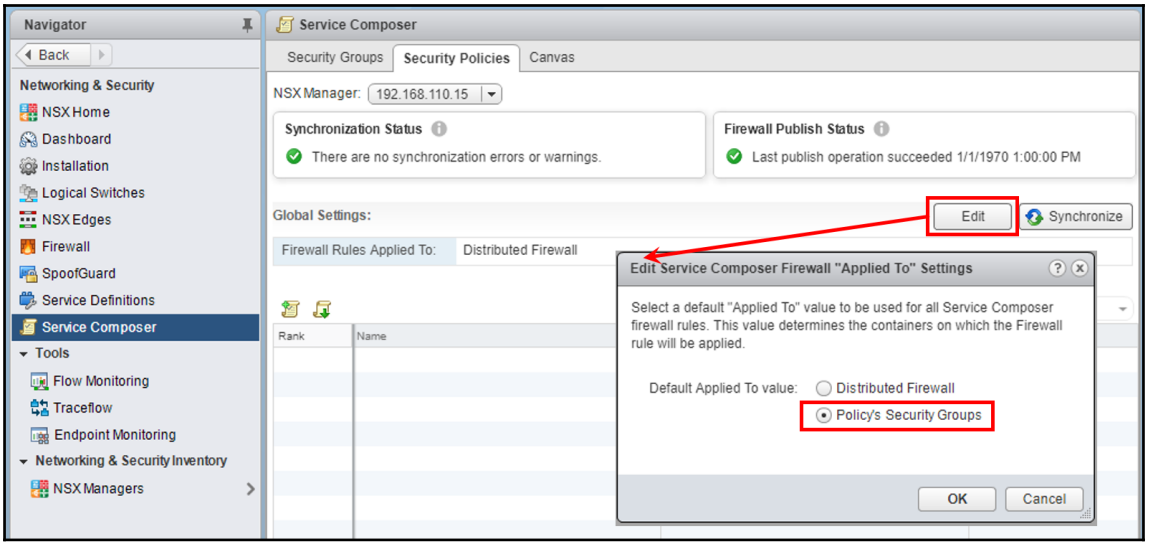

Actions
Rank
Name
Status
1
Manage Priority
2
SP-App-Tier
Published
3
SP-Web-Tier
Published

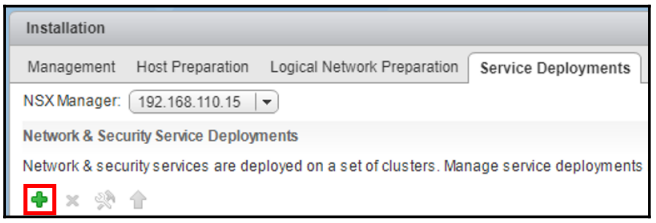

Service Composer
Security Groups
Security Policies
Canvas
NSX Manager:
192.168.110.42
Synchronization Status
There are no synchronization errors or warnings.
Firewall Publish Status
Last publish operation succeeded 12/3/2017 7:19:06 PM
Filter
Rank
Name
Status
Applied to
Guest Introspection Services
Firewall Rules
Network Introspection Services
Inherited by
1
SP-Web-Tier
Published
1
0
2
0
0
2
SP-App-Tier
Published
1
0
2
0
0
3
SP-DB-Tier
Published
1
0
1
0
0

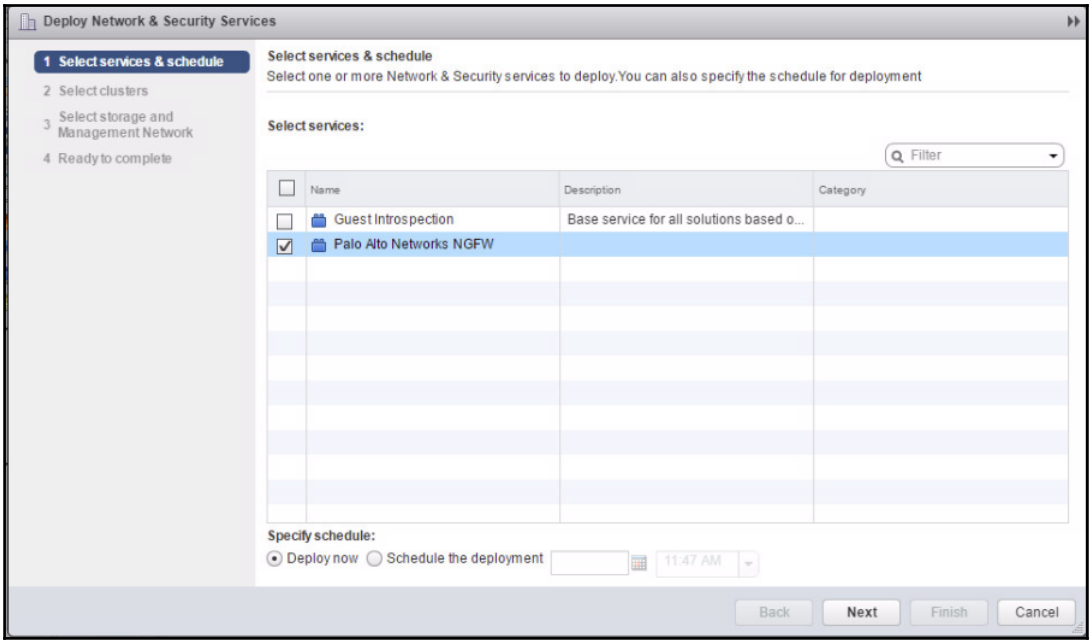

Firewall
Configuration
Saved Configurations
Settings
NSX Manager: 192.168.110.42
General
Ethernet
Partner security services
No.
Name
Rule ID
Source
Destination
Service
Action
Applied To
SP-Web-Tier :: NSX Service Composer - Firewall (Rule 1 - 2)
1 Allow Any to Web 1013 SG-Web-Tier any HTTP Allow Distributed Fi...
2 Allow Web to App 1012 SG-Web-Tier SG-App-Tier Tomcat Allow Distributed Fi...
SP-App-Tier :: NSX Service Composer - Firewall (Rule 3 - 4)
3 Allow Web to App 1010 SG-Web-Tier SG-App-Tier Tomcat Allow Distributed Fi...
4 Allow App to DB 1009 SG-App-Tier SG-DB-Tier MySQL Allow Distributed Fi...
SP-DB-Tier :: NSX Service Composer - Firewall (Rule 5)
5 Allow App to DB 1011 SG-App-Tier SG-DB-Tier MySQL Allow Distributed Fi...
Default Section Layer3 (Rule 6 - 9)

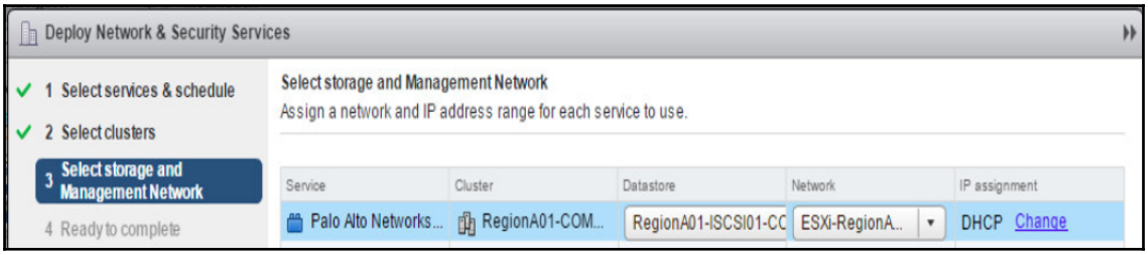

1 Rule 1 any any any Allow Distributed Firewall

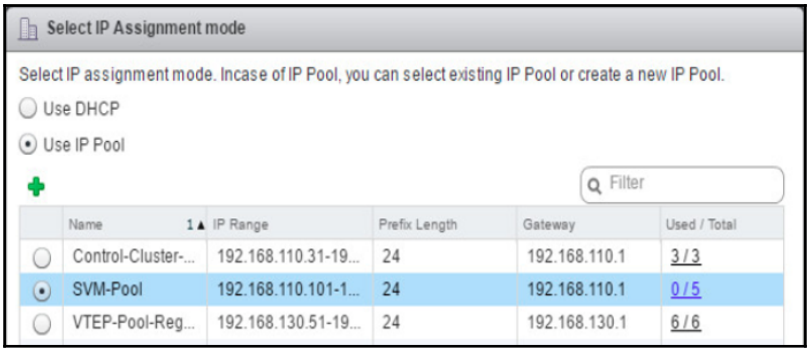

Available Objects
RegionA01-COMP01
RegionA01-COMP02
RegionA01-MGMT01
3 items Copy
Selected Objects
RegionA01-COMP01
1 items Copy
OK
Cancel

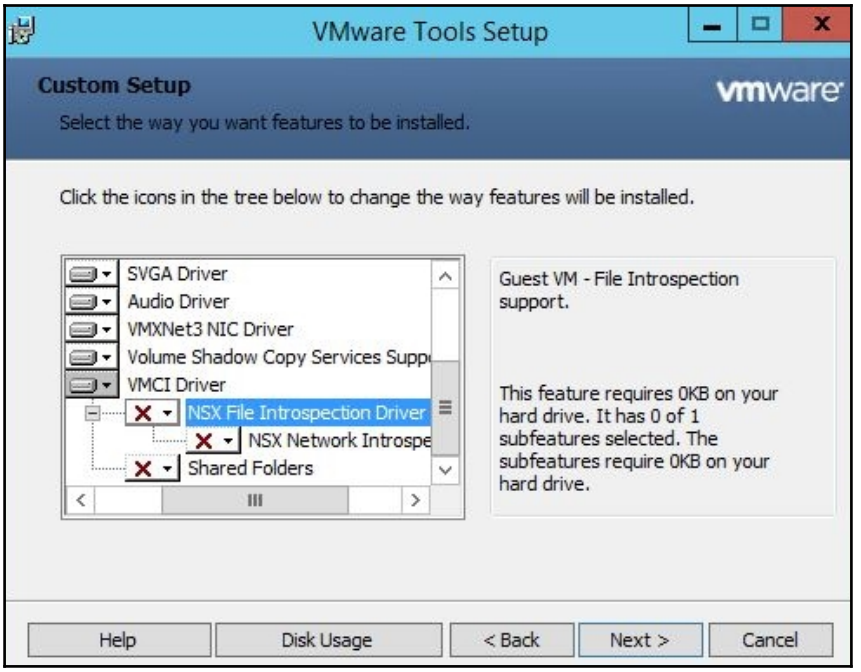

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Tools
Flow Monitoring
Traceflow
Endpoint Monitoring
Networking & Security Inventory
NSX Managers
Service Composer
Security Groups
Security Policies
Canvas
NSX Manager: 192.168.110.15
Synchronization Status
There are no synchronization errors or warnings.
Firewall Publish Status
Last publish operation succeeded 1/1/1970 1:00:00 PM
Global Settings:
Edit
Synchronize
Firewall Rules Applied To:
Distributed Firewall
Rank
Name
Edit Service Composer Firewall "Applied To" Settings
Select a default "Applied To" value to be used for all Service Composer firewall rules. This value determines the containers on which the Firewall rule will be applied.
Default Applied To value:
Distributed Firewall
Policy's Security Groups
OK
Cancel

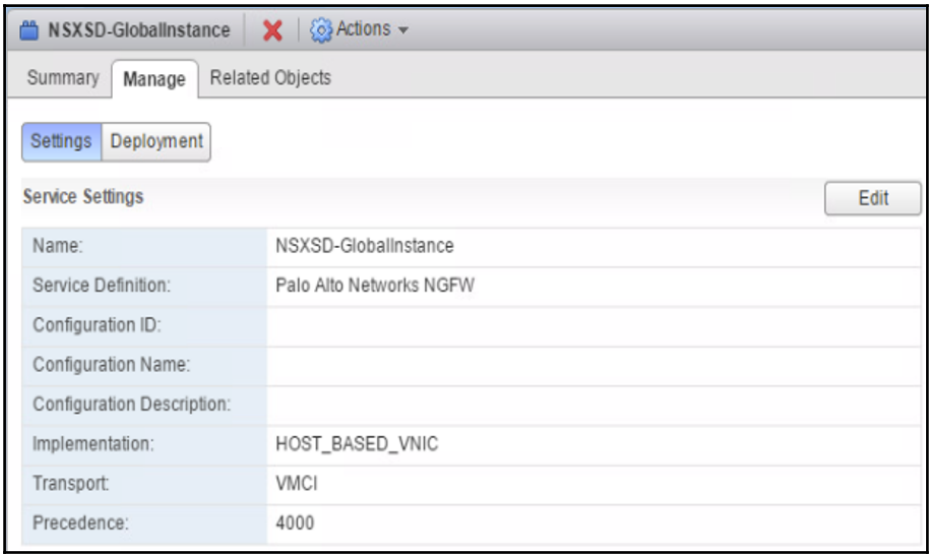

Installation
Management
Host Preparation
Logical Network Preparation
Service Deployments
NSX Manager: 192.168.110.15
Network & Security Service Deployments
Network & security services are deployed on a set of clusters. Manage service deployments


Deploy Network & Security Services
1 Select services & schedule
2 Select clusters
3 Select storage and Management Network
4 Ready to complete
Select services & schedule
Select one or more Network & Security services to deploy.You can also specify the schedule for deployment
Select services:
Filter
Name
Description
Category
Guest Introspection
Base service for all solutions based o...
Palo Alto Networks NGFW
Specify schedule:
Deploy now
Schedule the deployment
11:47 AM
Back
Next
Finish
Cancel

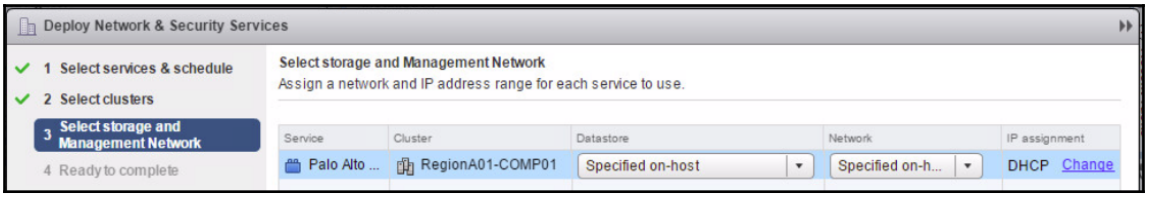

Deploy Network & Security Services
1 Select services & schedule
2 Select clusters
3 Select storage and Management Network
4 Ready to complete
Select storage and Management Network
Assign a network and IP address range for each service to use.
Service
Cluster
Datastore
Network
IP assignment
Palo Alto Networks...
RegionA01-COM...
RegionA01-ISCSI01-CC
ESXi-RegionA...
DHCP
Change

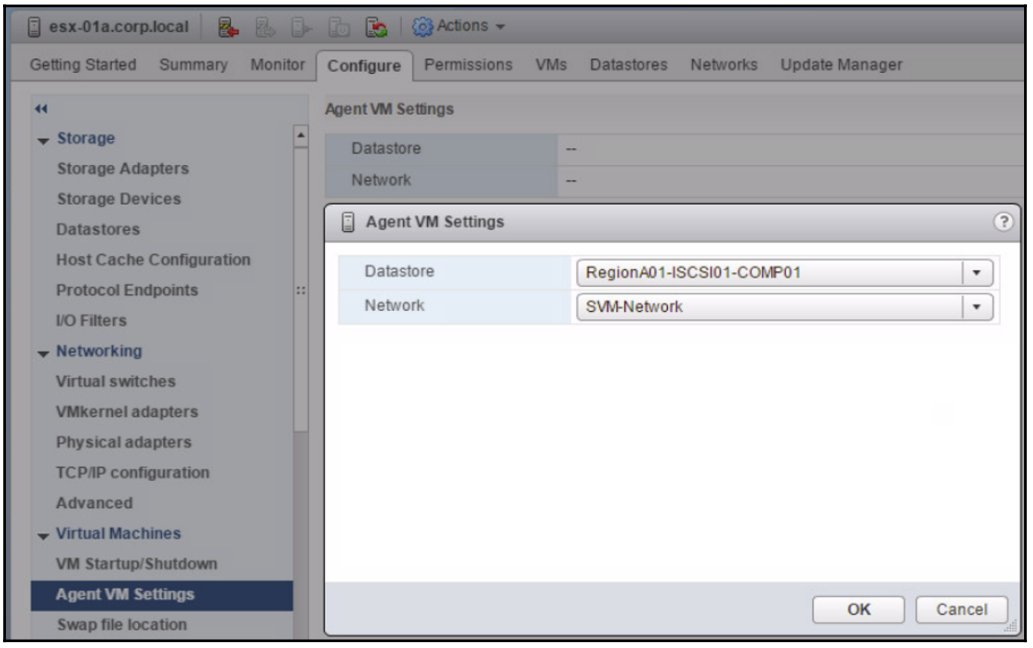

Select IP Assignment mode
Select IP assignment mode. Incase of IP Pool, you can select existing IP Pool or create a new IP Pool.
Use DHCP
Use IP Pool
Filter
Name
IP Range
Prefix Length
Gateway
Used / Total
Control-Cluster-...
192.168.110.31-19...
24
192.168.110.1
3 / 3
SVM-Pool
192.168.110.101-1...
24
192.168.110.1
0 / 5
VTEP-Pool-Reg...
192.168.130.51-19...
24
192.168.130.1
6 / 6

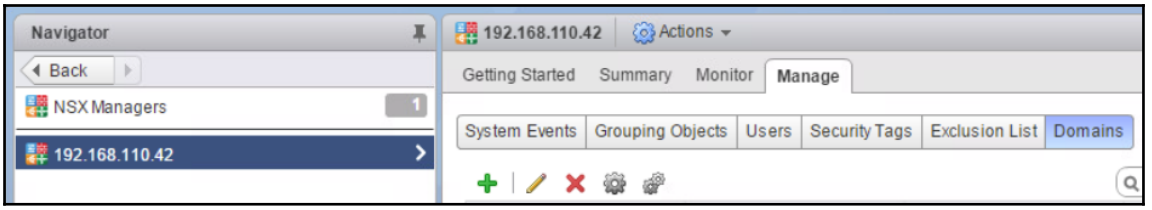

VMware Tools Setup
Custom Setup
Select the way you want features to be installed.
vmware
Click the icons in the tree below to change the way features will be installed.
SVGA Driver
Audio Driver
VMXNet3 NIC Driver
Volume Shadow Copy Services Supp
VMCI Driver
NSX File Introspection Driver
NSX Network Introspe
Shared Folders
Guest VM - File Introspection support.
This feature requires 0KB on your hard drive. It has 0 of 1 subfeatures selected. The subfeatures require 0KB on your hard drive.
Help
Disk Usage
< Back
Next >
Cancel

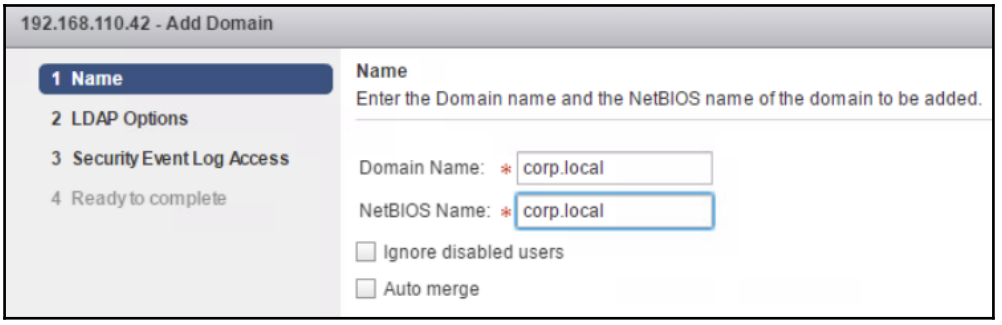

NSXSD-GlobalInstance
Actions
Summary
Manage
Related Objects
Settings
Deployment
Service Settings
Edit
Name: NSXSD-GlobalInstance
Service Definition: Palo Alto Networks NGFW
Configuration ID:
Configuration Name:
Configuration Description:
Implementation: HOST_BASED_VNIC
Transport: VMCI
Precedence: 4000

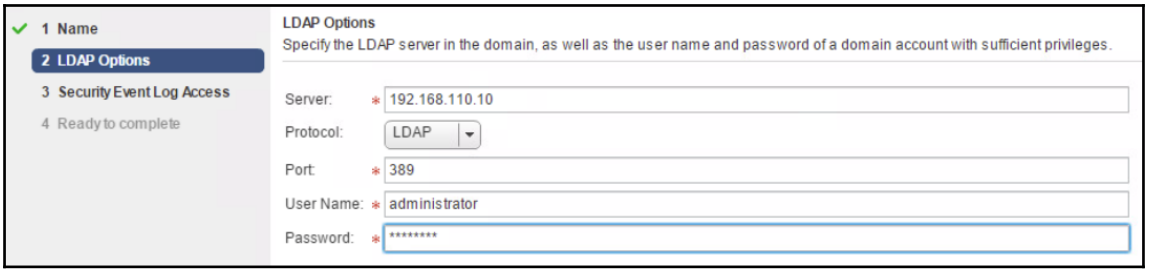

General
Ethernet
Partner security services
No.
Name
Rule ID
Source
Destination
Default Section Layer2 (Rule 1 - 2)
1
Allow IP Protocols
1008
any
any
2
Default Rule
1004
any
any

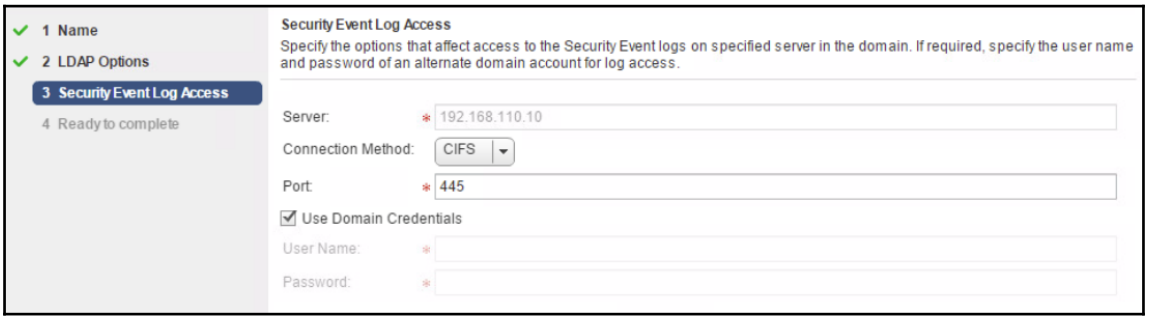

Deploy Network & Security Services
1 Select services & schedule
2 Select clusters
3 Select storage and Management Network
4 Ready to complete
Select storage and Management Network
Assign a network and IP address range for each service to use.
Service
Cluster
Datastore
Network
IP assignment
Palo Alto ...
RegionA01-COMP01
Specified on-host
Specified on-h...
DHCP
Change

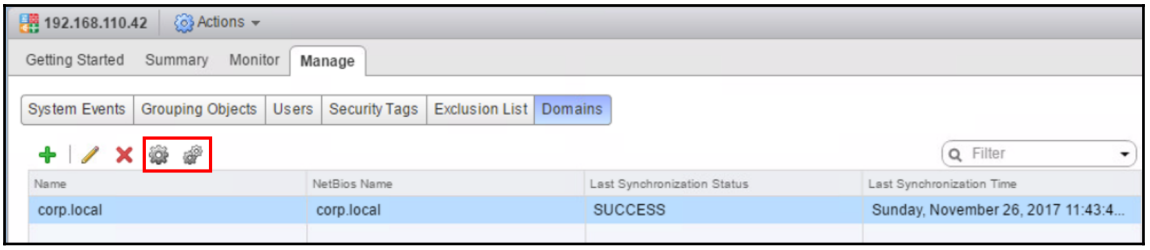

esx-01a.corp.local
Actions
Getting Started
Summary
Monitor
Configure
Permissions
VMs
Datastores
Networks
Update Manager
Storage
Storage Adapters
Storage Devices
Datastores
Host Cache Configuration
Protocol Endpoints
I/O Filters
Networking
Virtual switches
VMkernel adapters
Physical adapters
TCP/IP configuration
Advanced
Virtual Machines
VM Startup/Shutdown
Agent VM Settings
Swap file location
Agent VM Settings
Datastore
--
Network
--
Agent VM Settings
Datastore
RegionA01-ISCSI01-COMP01
Network
SVM-Network
OK
Cancel

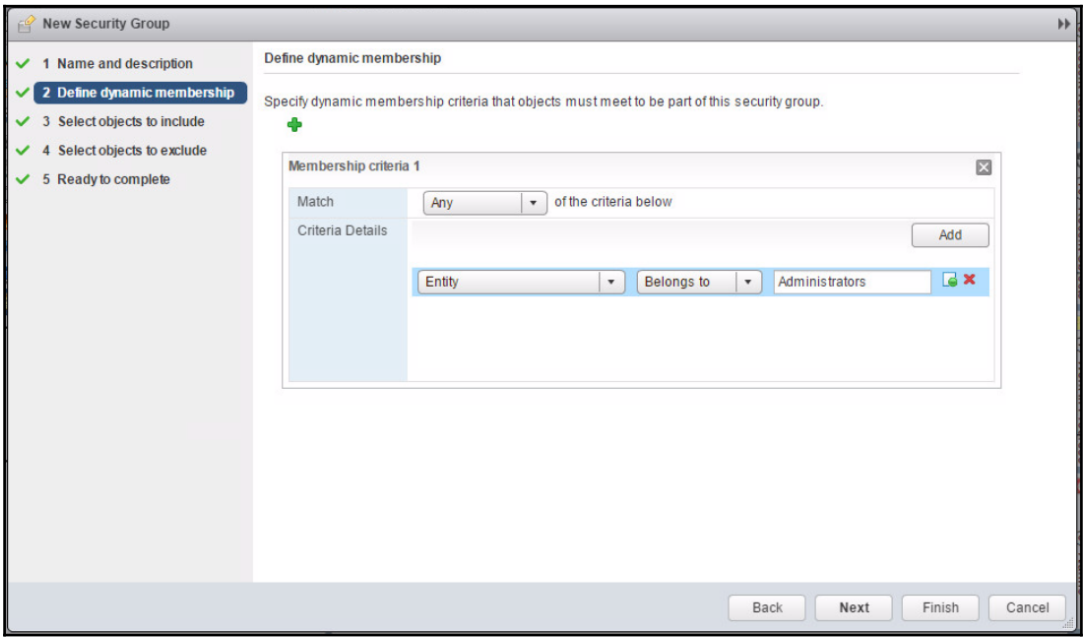

Navigator
Back
NSX Managers
1
192.168.110.42
192.168.110.42
Actions
Getting Started
Summary
Monitor
Manage
System Events
Grouping Objects
Users
Security Tags
Exclusion List
Domains

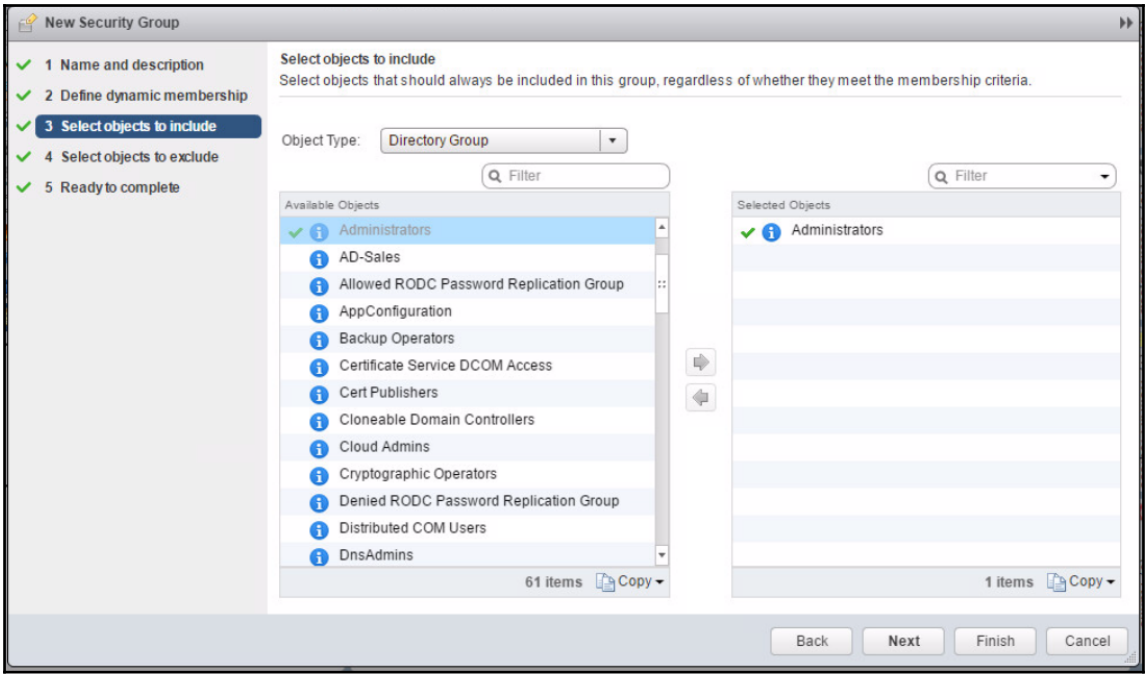

192.168.110.42 - Add Domain
1 Name
2 LDAP Options
3 Security Event Log Access
4 Ready to complete
Name
Enter the Domain name and the NetBIOS name of the domain to be added.
Domain Name: * corp.local
NetBIOS Name: * corp.local
Ignore disabled users
Auto merge


1 Name
2 LDAP Options
3 Security Event Log Access
4 Ready to complete
LDAP Options
Specify the LDAP server in the domain, as well as the user name and password of a domain account with sufficient privileges.
Server: * 192.168.110.10
Protocol: LDAP
Port: * 389
User Name: * administrator
Password: * ********


1 Name
2 LDAP Options
3 Security Event Log Access
4 Ready to complete
Security Event Log Access
Specify the options that affect access to the Security Event logs on specified server in the domain. If required, specify the user name and password of an alternate domain account for log access.
Server: * 192.168.110.10
Connection Method: CIFS
Port: * 445
Use Domain Credentials
User Name: *
Password: *

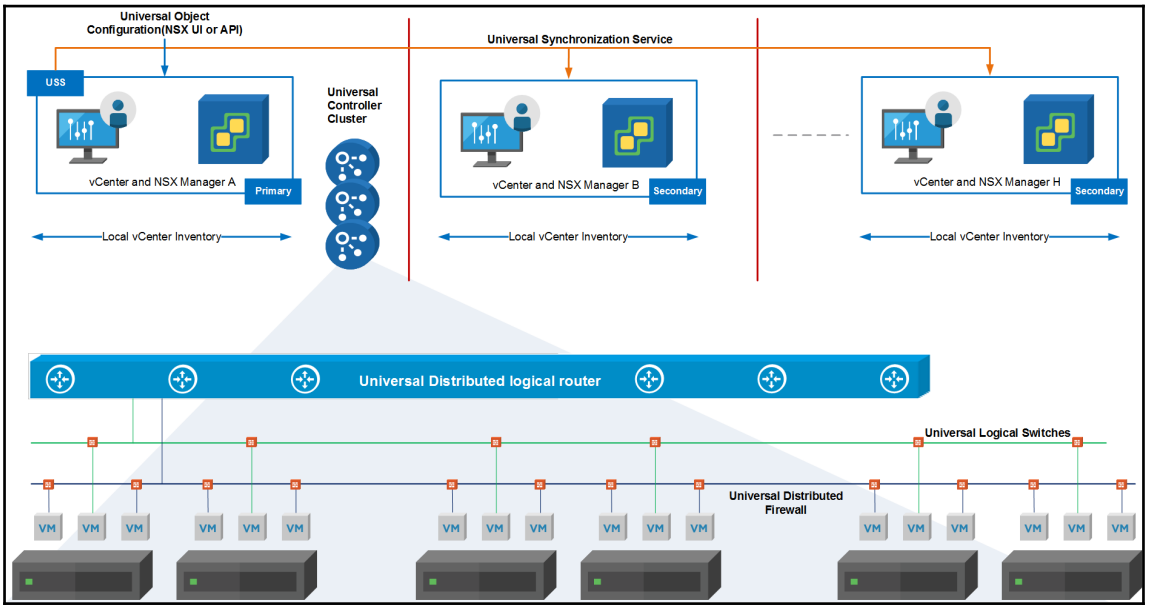

192.168.110.42
Actions
Getting Started
Summary
Monitor
Manage
System Events
Grouping Objects
Users
Security Tags
Exclusion List
Domains
Filter
Name
NetBios Name
Last Synchronization Status
Last Synchronization Time
corp.local
corp.local
SUCCESS
Sunday, November 26, 2017 11:43:4...

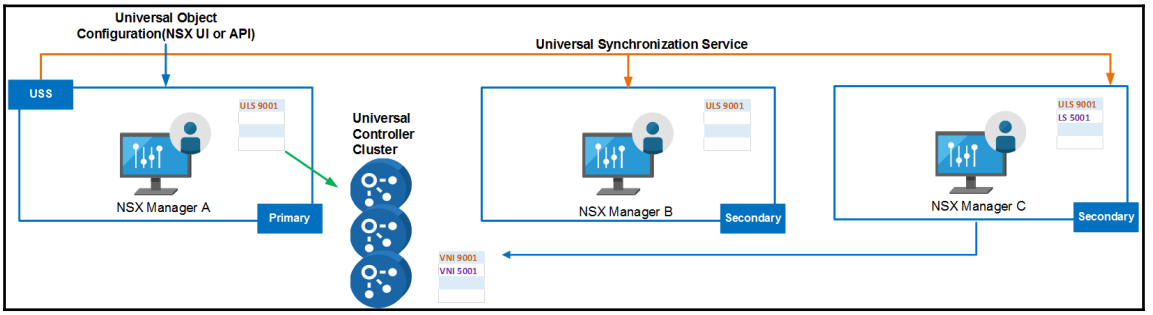

New Security Group
1 Name and description
2 Define dynamic membership
3 Select objects to include
4 Select objects to exclude
5 Ready to complete
Define dynamic membership
Specify dynamic membership criteria that objects must meet to be part of this security group.
Membership criteria 1
Match
Any
of the criteria below
Criteria Details
Add
Entity
Belongs to
Administrators
Back
Next
Finish
Cancel

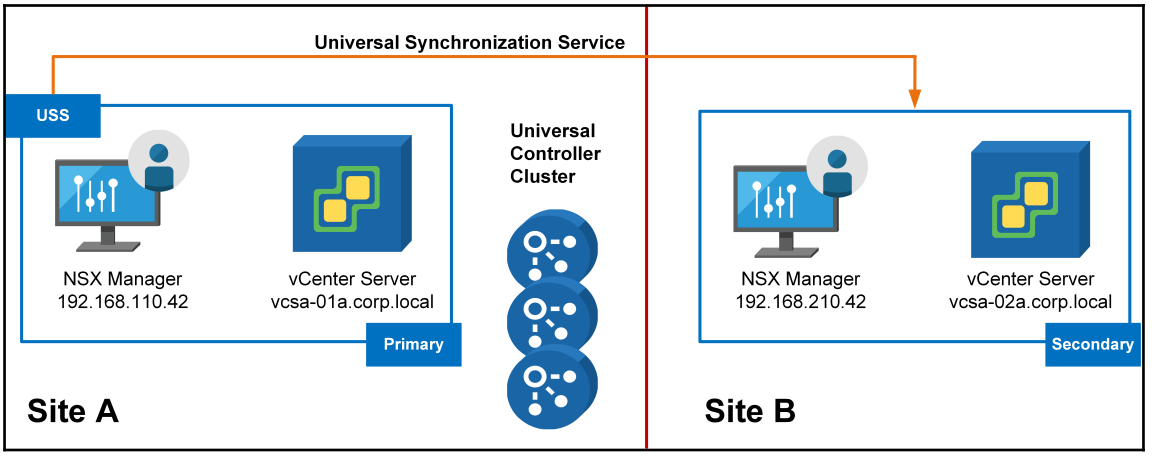

New Security Group
1 Name and description
2 Define dynamic membership
3 Select objects to include
4 Select objects to exclude
5 Ready to complete
Select objects to include
Select objects that should always be included in this group, regardless of whether they meet the membership criteria.
Object Type:
Directory Group
Filter
Available Objects
Administrators
AD-Sales
Allowed RODC Password Replication Group
AppConfiguration
Backup Operators
Certificate Service DCOM Access
Cert Publishers
Cloneable Domain Controllers
Cloud Admins
Cryptographic Operators
Denied RODC Password Replication Group
Distributed COM Users
DnsAdmins
61 items
Copy
Filter
Selected Objects
Administrators
1 items
Copy
Back
Next
Finish
Cancel

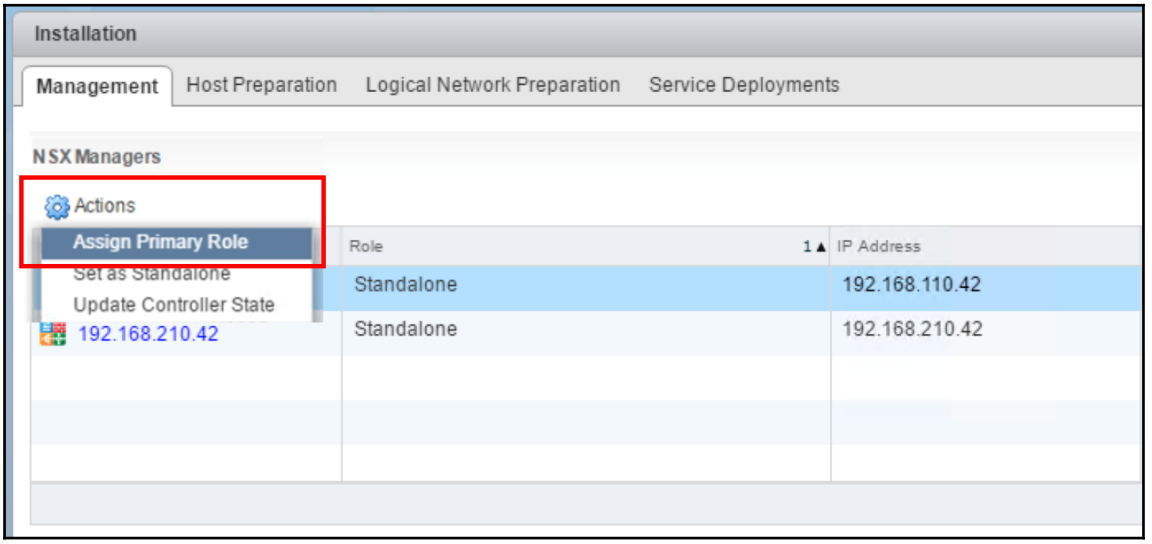

No.
Name
Rule ID
Source
Destination
Service
Action
Identity Firewall (Rule 1)
1
Allow Admin SSH to Internal
1007
Administrators
RegionA01-COMP01
SSH
Allow

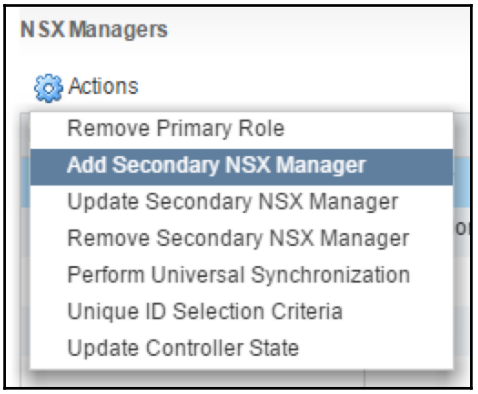
Chapter 07: Configuring Cross-vCenter NSX

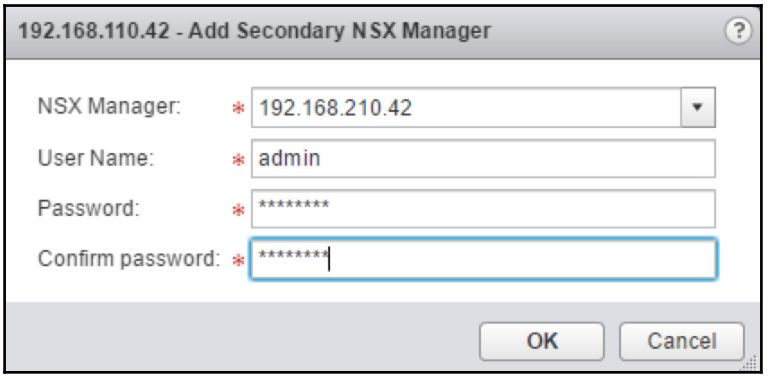


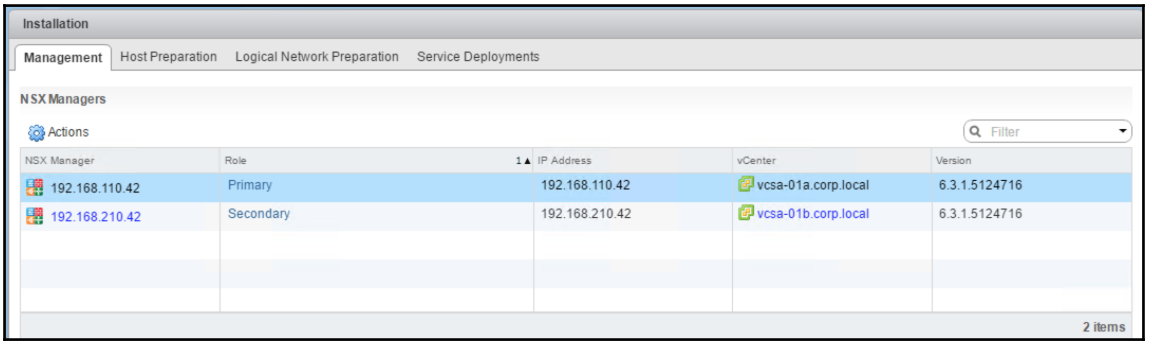


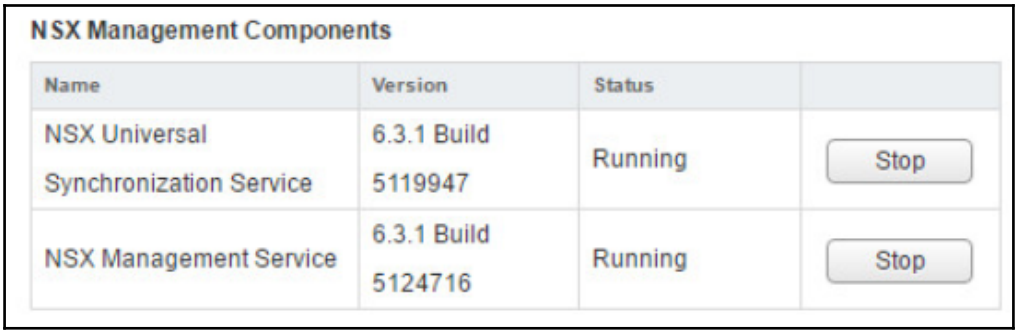

Universal Synchronization Service
USS
NSX Manager
192.168.110.42
vCenter Server
vcsa-01a.corp.local
Primary
Universal
Controller
Cluster
NSX Manager
192.168.210.42
vCenter Server
vcsa-02a.corp.local
Secondary
Site A
Site B

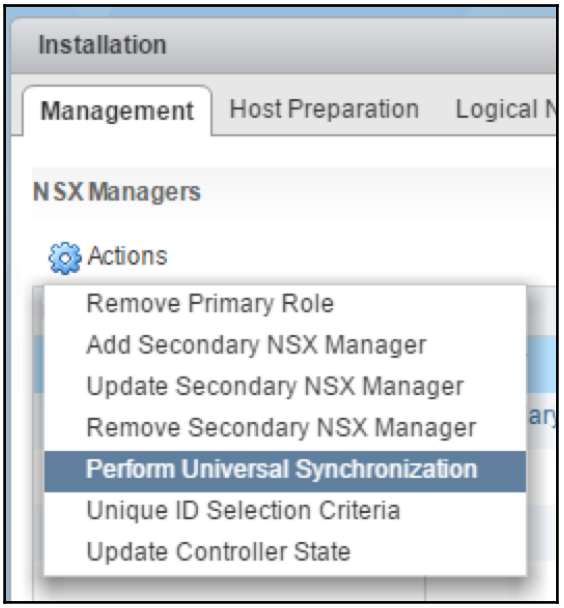

Installation
Management
Host Preparation
Logical Network Preparation
Service Deployments
NSX Managers
Actions
Assign Primary Role
Set as Standalone
Update Controller State
192.168.210.42
Role
IP Address
Standalone
192.168.110.42
Standalone
192.168.210.42

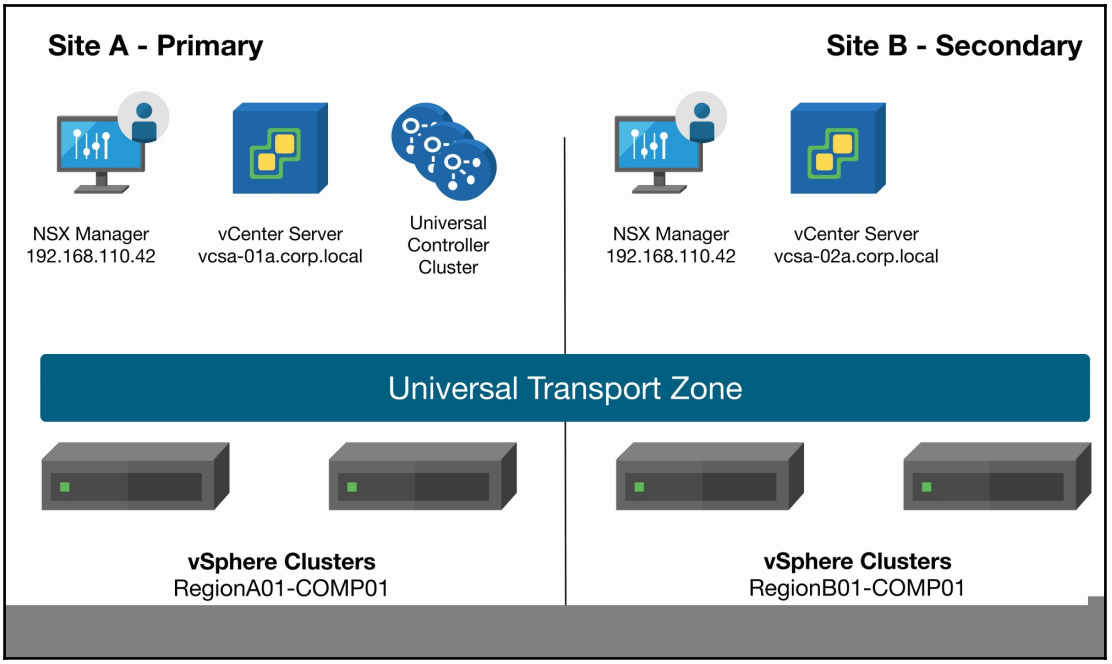

NSX Managers
Actions
Remove Primary Role
Add Secondary NSX Manager
Update Secondary NSX Manager
Remove Secondary NSX Manager
Perform Universal Synchronization
Unique ID Selection Criteria
Update Controller State

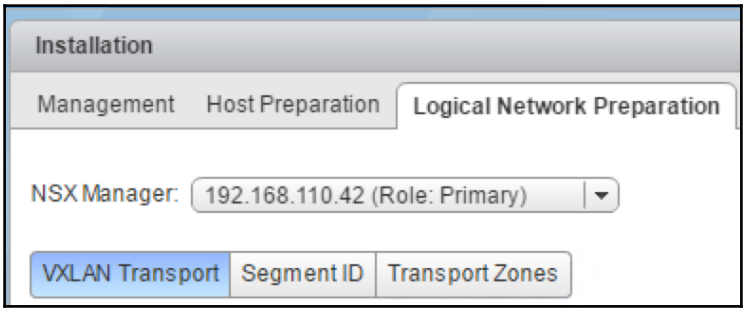

192.168.110.42 - Add Secondary NSX Manager
NSX Manager:
192.168.210.42
User Name:
admin
Password:
Confirm password:
OK
Cancel

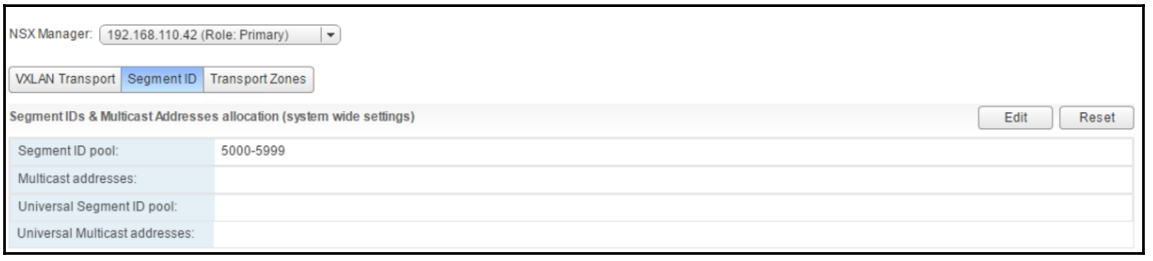

Installation
Management
Host Preparation
Logical Network Preparation
Service Deployments
NSX Managers
Actions
Filter
NSX Manager
Role
IP Address
vCenter
Version
192.168.110.42
Primary
192.168.110.42
vcsa-01a.corp.local
6.3.1.5124716
192.168.210.42
Secondary
192.168.210.42
vcsa-01b.corp.local
6.3.1.5124716
2 items

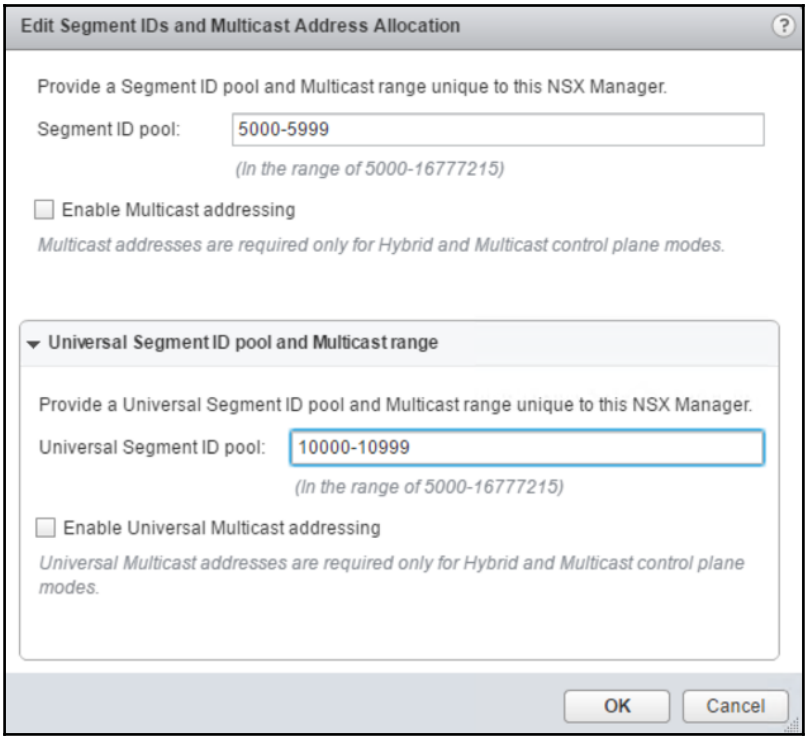

NSX Management Components
Name
Version
Status
NSX Universal Synchronization Service
6.3.1 Build 5119947
Running
Stop
NSX Management Service
6.3.1 Build 5124716
Running
Stop

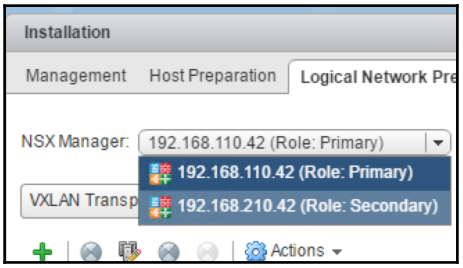

Installation
Management
Host Preparation
NSX Managers
Actions
Remove Primary Role
Add Secondary NSX Manager
Update Secondary NSX Manager
Remove Secondary NSX Manager
Perform Universal Synchronization
Unique ID Selection Criteria
Update Controller State

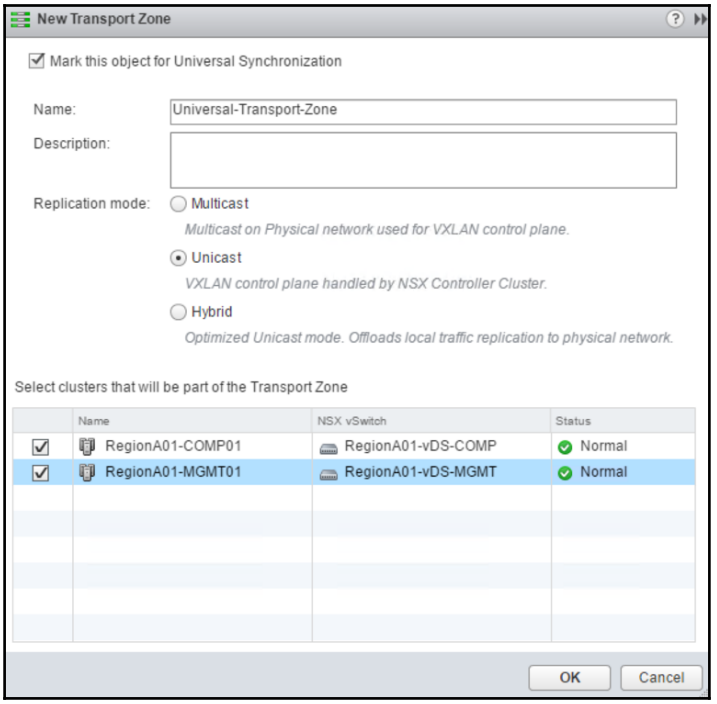

Site A - Primary
Site B - Secondary
NSX Manager
192.168.110.42
vCenter Server
vcsa-01a.corp.local
Universal
Controller
Cluster
NSX Manager
192.168.110.42
vCenter Server
vcsa-02a.corp.local
Universal Transport Zone
vSphere Clusters
RegionA01-COMP01
vSphere Clusters
RegionB01-COMP01

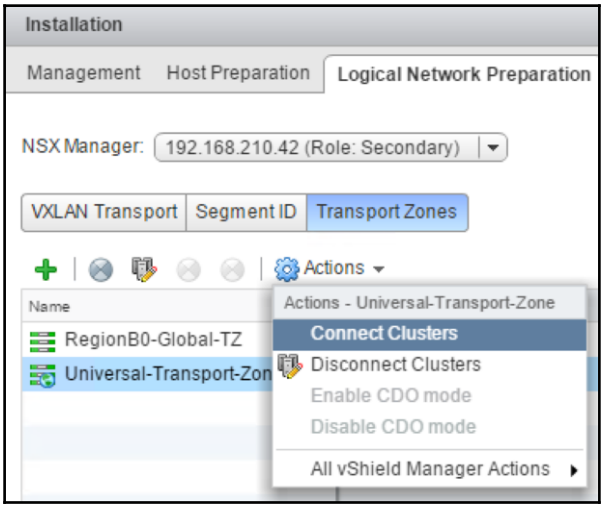

Installation
Management
Host Preparation
Logical Network Preparation
NSX Manager:
192.168.110.42 (Role: Primary)
VXLAN Transport
Segment ID
Transport Zones

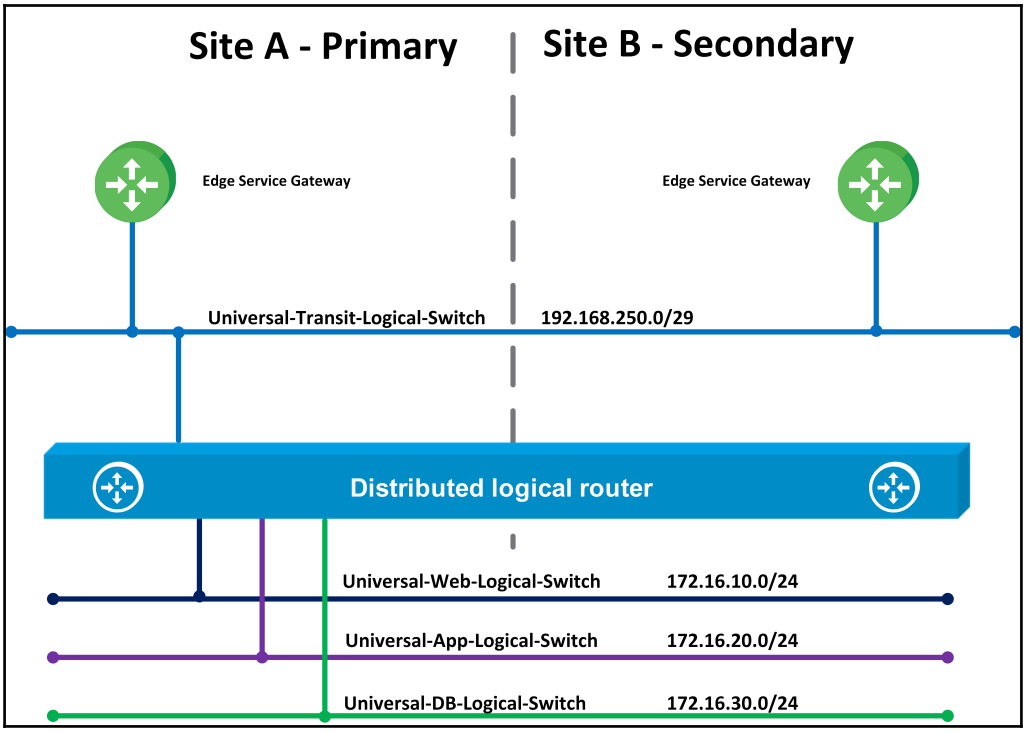

NSX Manager:
192.168.110.42 (Role: Primary)
VXLAN Transport
Segment ID
Transport Zones
Segment IDs & Multicast Addresses allocation (system wide settings)
Edit
Reset
Segment ID pool:
5000-5999
Multicast addresses:
Universal Segment ID pool:
Universal Multicast addresses:

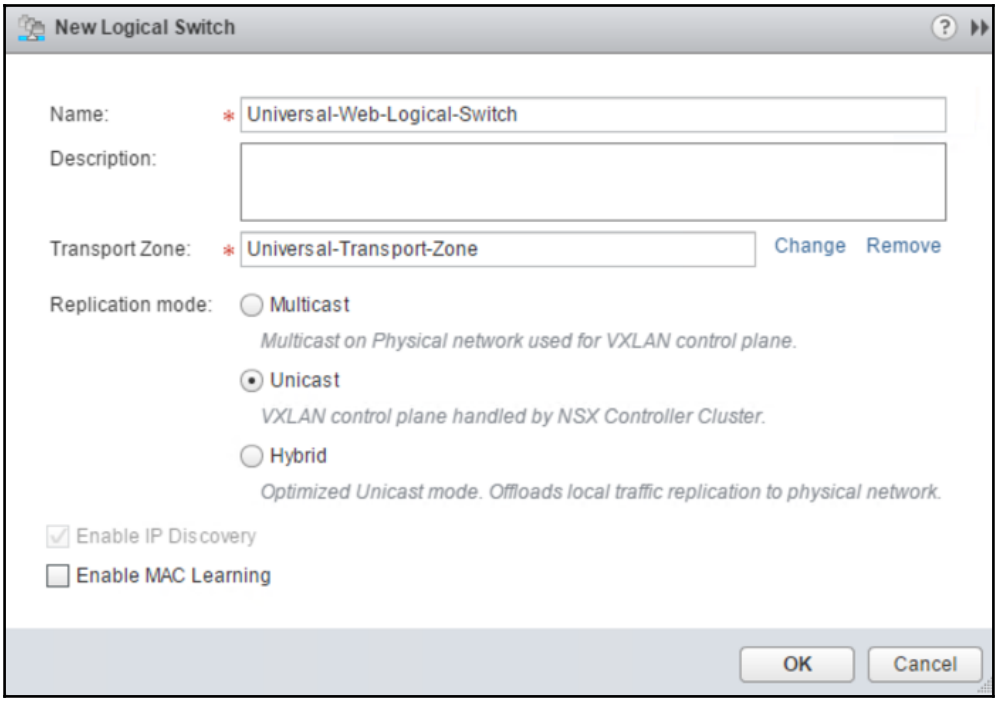

Edit Segment IDs and Multicast Address Allocation
Provide a Segment ID pool and Multicast range unique to this NSX Manager.
Segment ID pool:
5000-5999
(In the range of 5000-16777215)
Enable Multicast addressing
Multicast addresses are required only for Hybrid and Multicast control plane modes.
Universal Segment ID pool and Multicast range
Provide a Universal Segment ID pool and Multicast range unique to this NSX Manager.
Universal Segment ID pool:
10000-10999
(In the range of 5000-16777215)
Enable Universal Multicast addressing
Universal Multicast addresses are required only for Hybrid and Multicast control plane modes.
OK
Cancel

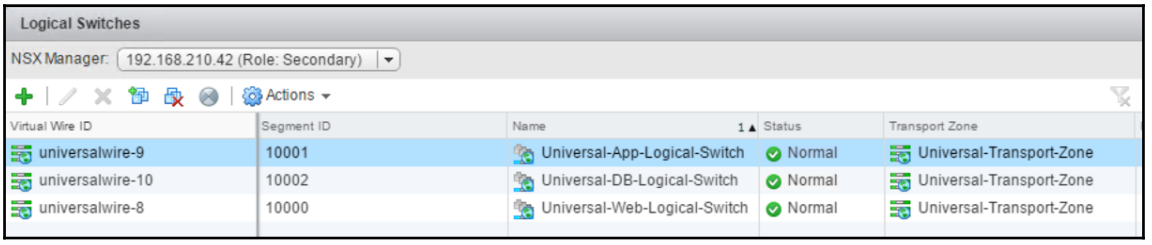

Installation
Management
Host Preparation
Logical Network Pre
NSX Manager:
192.168.110.42 (Role: Primary)
192.168.110.42 (Role: Primary)
192.168.210.42 (Role: Secondary)
VXLAN Transp
Actions

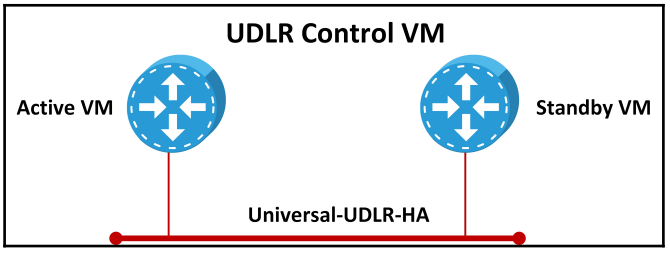

New Transport Zone
Mark this object for Universal Synchronization
Name:
Universal-Transport-Zone
Description:
Replication mode:
Multicast
Multicast on Physical network used for VXLAN control plane.
Unicast
VXLAN control plane handled by NSX Controller Cluster.
Hybrid
Optimized Unicast mode. Offloads local traffic replication to physical network.
Select clusters that will be part of the Transport Zone
Name
NSX vSwitch
Status
RegionA01-COMP01
RegionA01-vDS-COMP
Normal
RegionA01-MGMT01
RegionA01-vDS-MGMT
Normal
OK
Cancel

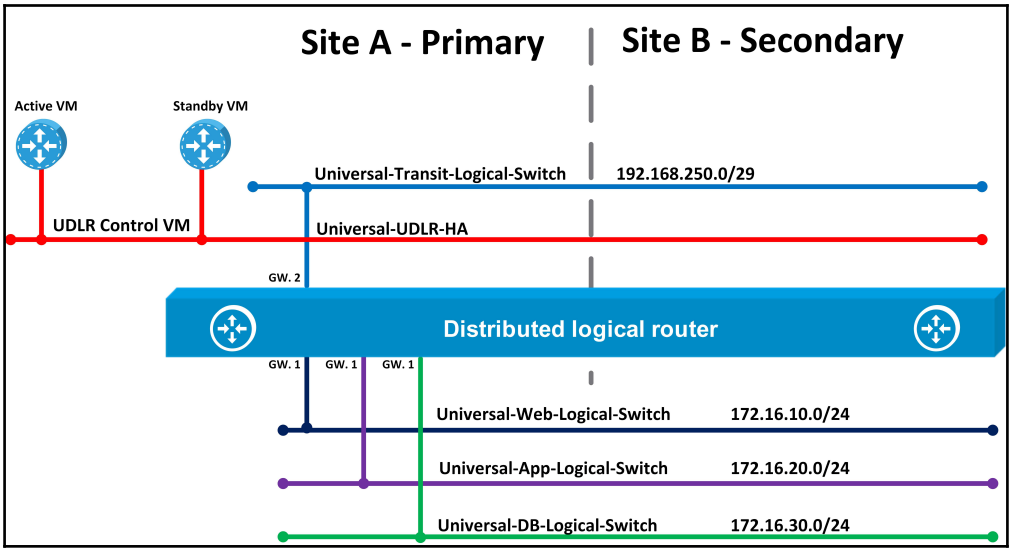

Installation
Management
Host Preparation
Logical Network Preparation
NSX Manager:
192.168.210.42 (Role: Secondary)
VXLAN Transport
Segment ID
Transport Zones
Actions
Name
RegionB0-Global-TZ
Universal-Transport-Zon
Actions - Universal-Transport-Zone
Connect Clusters
Disconnect Clusters
Enable CDO mode
Disable CDO mode
All vShield Manager Actions

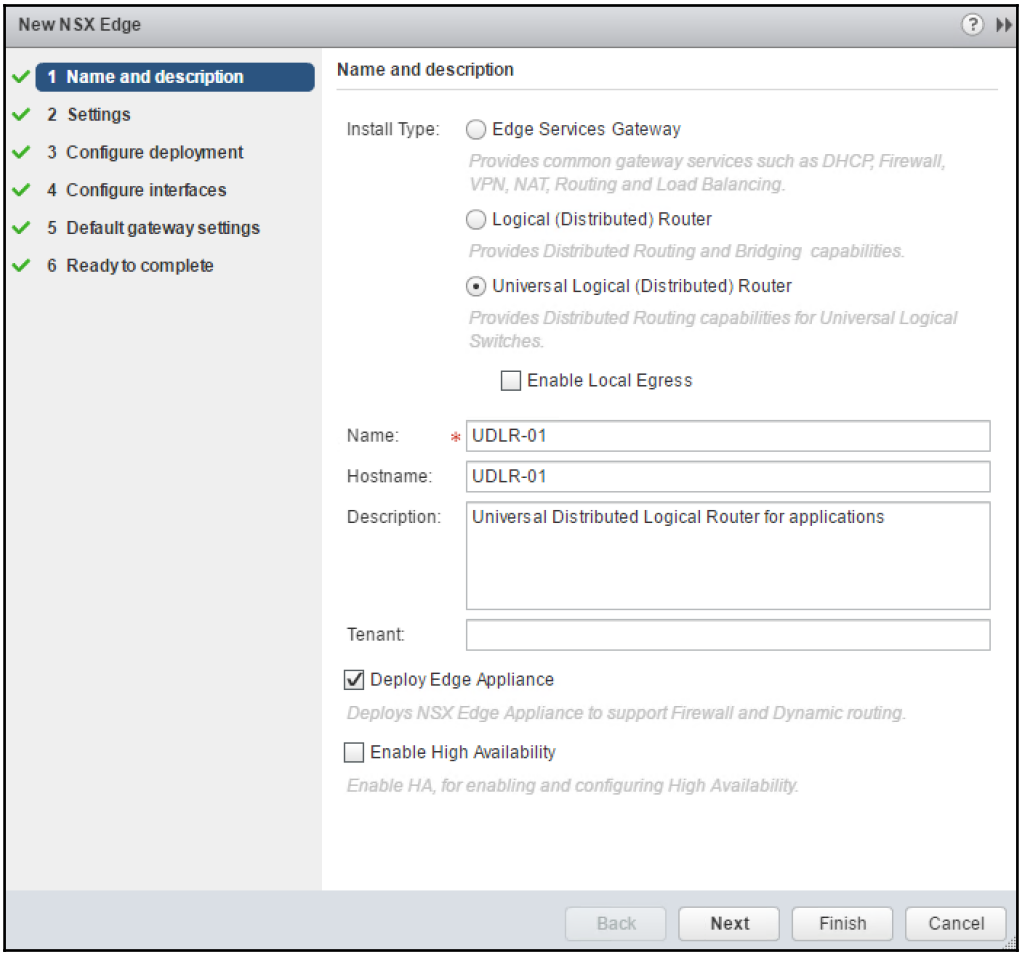

Site A - Primary
Site B - Secondary
Edge Service Gateway
Edge Service Gateway
Universal-Transit-Logical-Switch
192.168.250.0/29
Distributed logical router
Universal-Web-Logical-Switch
172.16.10.0/24
Universal-App-Logical-Switch
172.16.20.0/24
Universal-DB-Logical-Switch
172.16.30.0/24

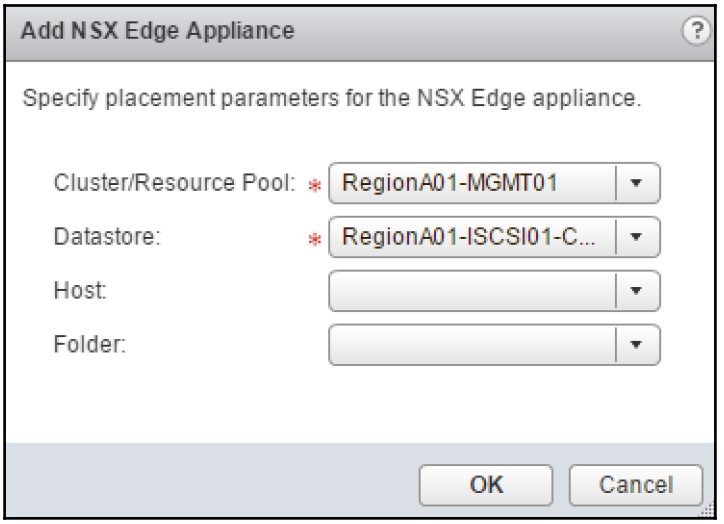

New Logical Switch
Name:
Universal-Web-Logical-Switch
Description:
Transport Zone:
Universal-Transport-Zone
Change
Remove
Replication mode:
Multicast
Multicast on Physical network used for VXLAN control plane.
Unicast
VXLAN control plane handled by NSX Controller Cluster.
Hybrid
Optimized Unicast mode. Offloads local traffic replication to physical network.
Enable IP Discovery
Enable MAC Learning
OK
Cancel

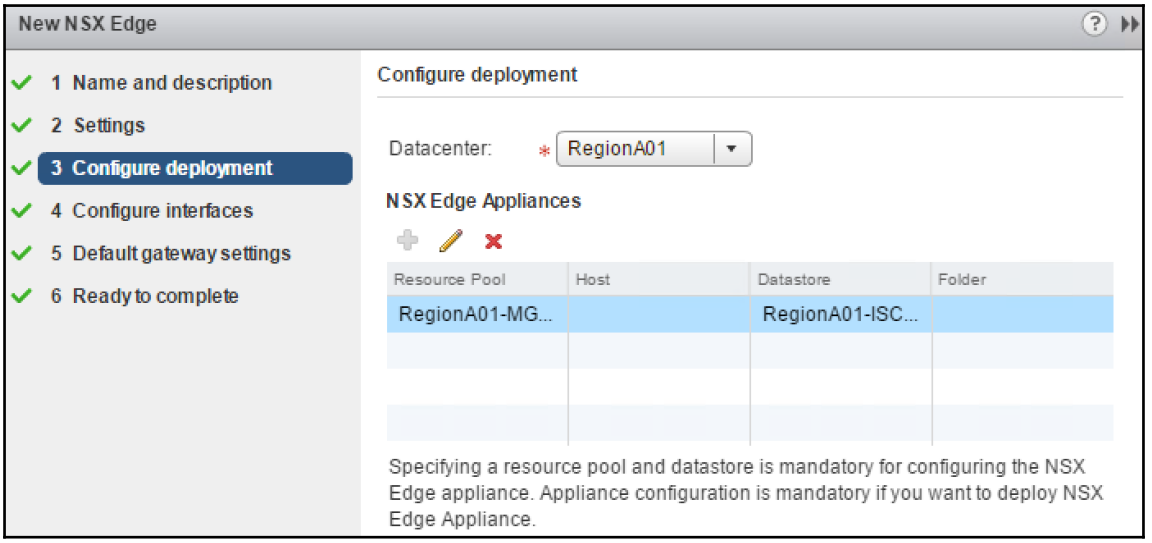

Logical Switches
NSX Manager:
192.168.210.42 (Role: Secondary)
Actions
Virtual Wire ID
Segment ID
Name
Status
Transport Zone
universalwire-9
10001
Universal-App-Logical-Switch
Normal
Universal-Transport-Zone
universalwire-10
10002
Universal-DB-Logical-Switch
Normal
Universal-Transport-Zone
universalwire-8
10000
Universal-Web-Logical-Switch
Normal
Universal-Transport-Zone

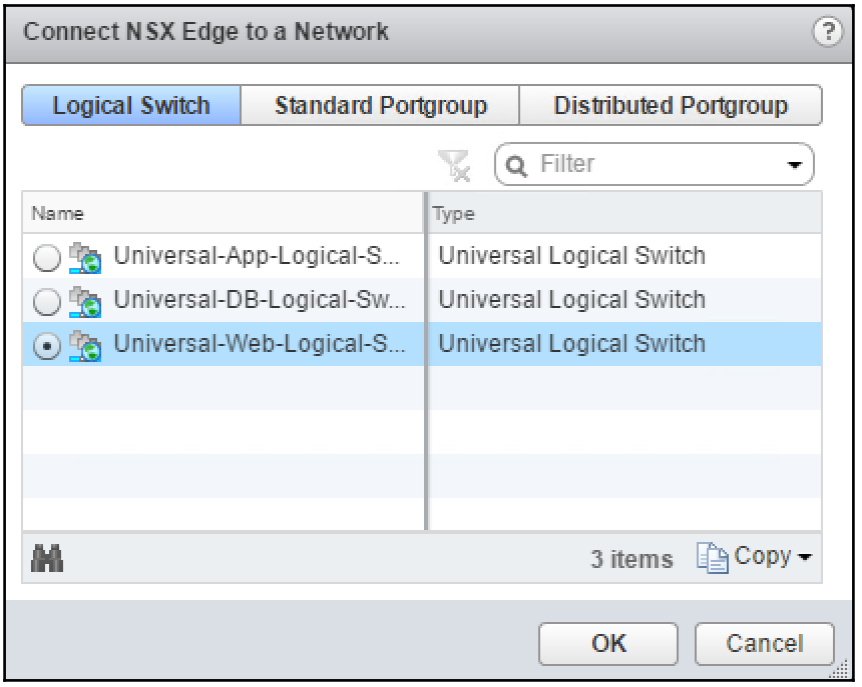

UDLR Control VM
Active VM
Standby VM
Universal-UDLR-HA

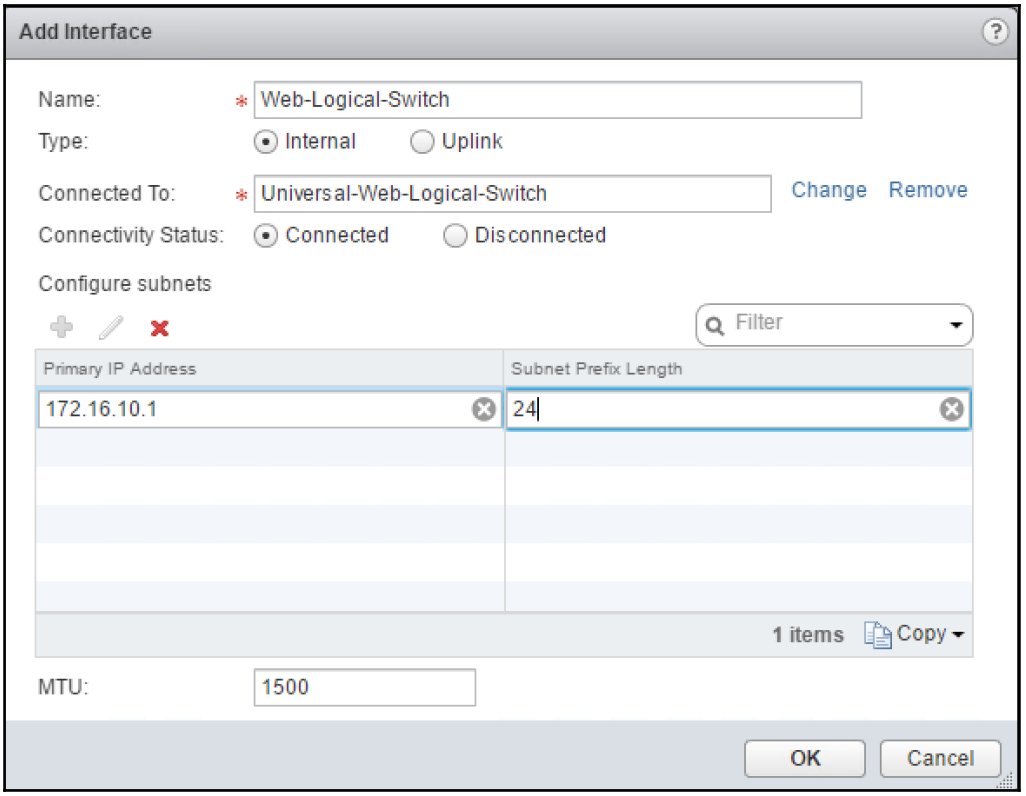

Site A - Primary
Site B - Secondary
Active VM
Standby VM
Universal-Transit-Logical-Switch
192.168.250.0/29
UDLR Control VM
Universal-UDLR-HA
GW. 2
Distributed logical router
GW. 1
GW. 1
GW. 1
Universal-Web-Logical-Switch
172.16.10.0/24
Universal-App-Logical-Switch
172.16.20.0/24
Universal-DB-Logical-Switch
172.16.30.0/24

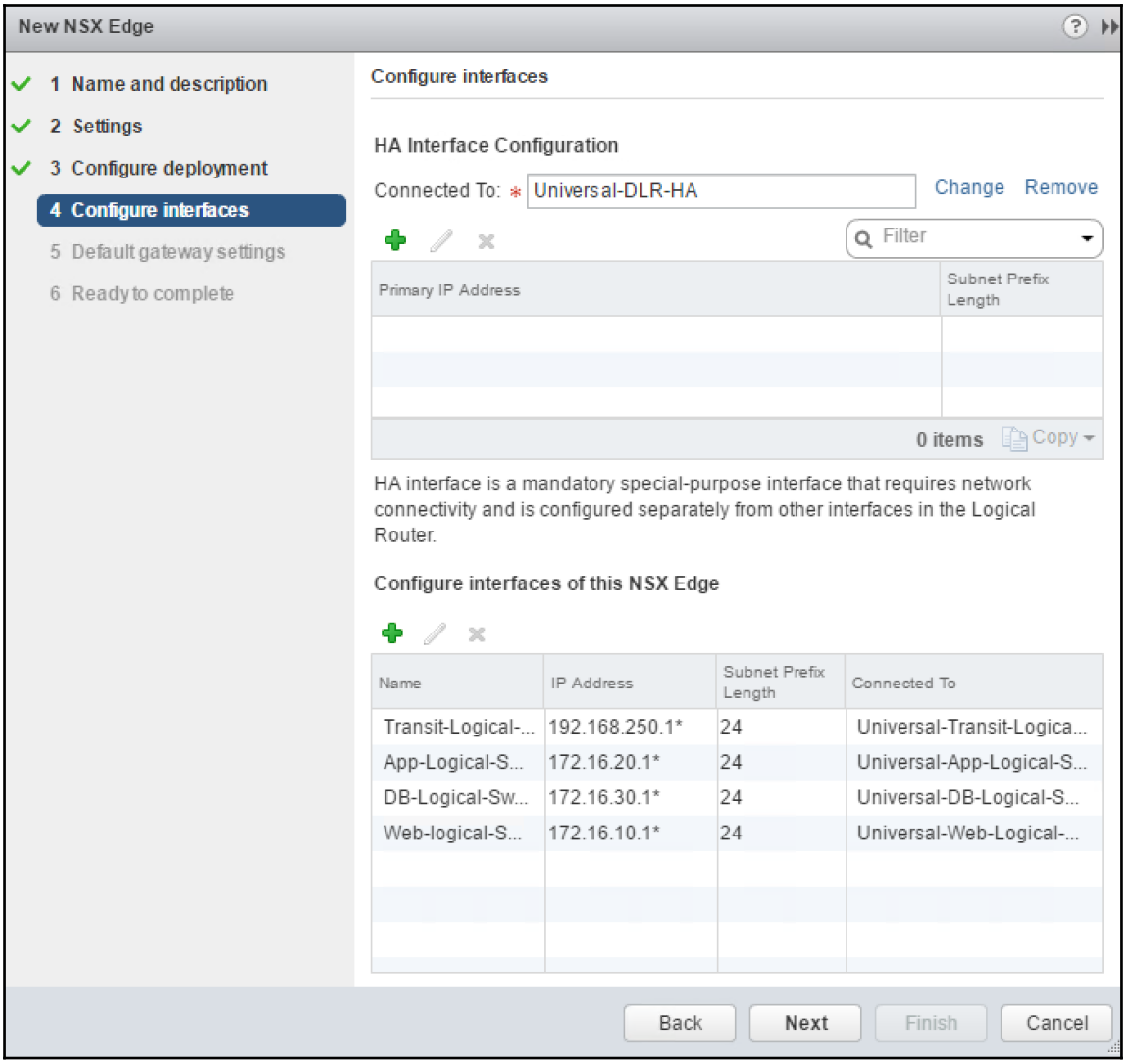

New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Ready to complete
Name and description
Install Type:
Edge Services Gateway
Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.
Logical (Distributed) Router
Provides Distributed Routing and Bridging capabilities.
Universal Logical (Distributed) Router
Provides Distributed Routing capabilities for Universal Logical Switches.
Enable Local Egress
Name: * UDLR-01
Hostname: UDLR-01
Description: Universal Distributed Logical Router for applications
Tenant:
Deploy Edge Appliance
Deploys NSX Edge Appliance to support Firewall and Dynamic routing.
Enable High Availability
Enable HA, for enabling and configuring High Availability.
Back
Next
Finish
Cancel

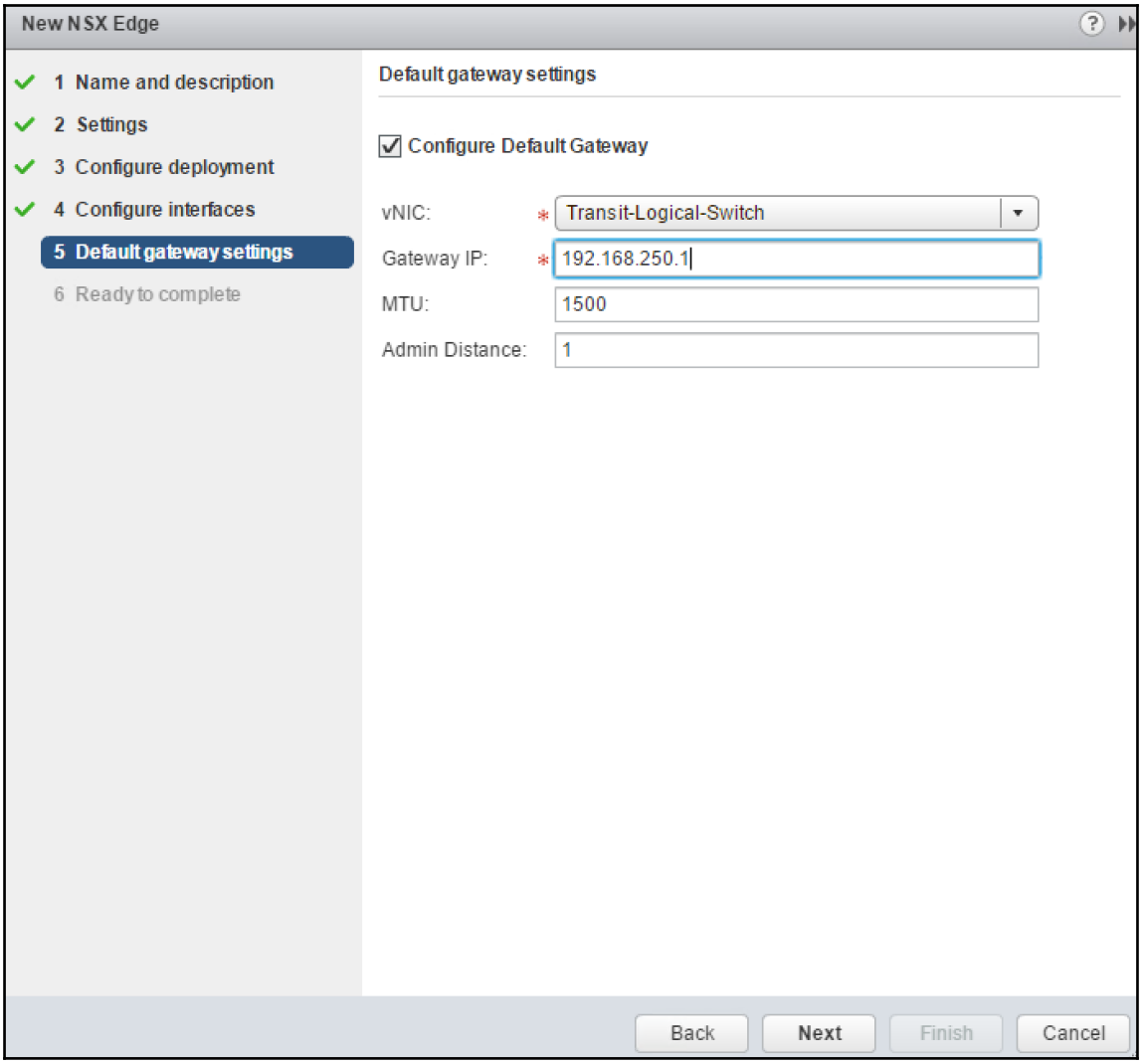

Add NSX Edge Appliance
Specify placement parameters for the NSX Edge appliance.
Cluster/Resource Pool:
RegionA01-MGMT01
Datastore:
RegionA01-ISCSI01-C...
Host:
Folder:
OK
Cancel

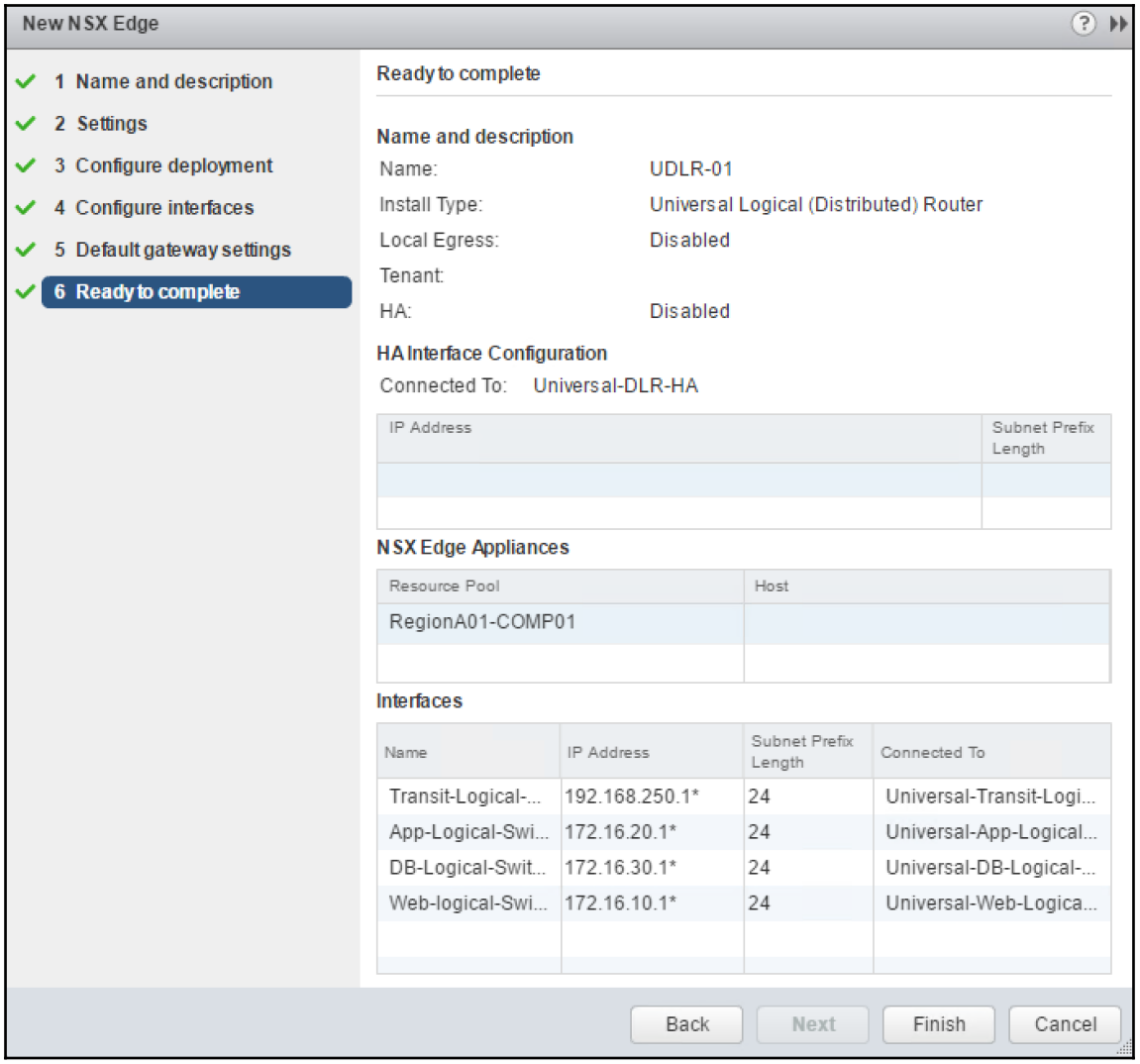

New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Ready to complete
Configure deployment
Datacenter:
RegionA01
NSX Edge Appliances
Resource Pool
Host
Datastore
Folder
RegionA01-MG...
RegionA01-ISC...
Specifying a resource pool and datastore is mandatory for configuring the NSX Edge appliance. Appliance configuration is mandatory if you want to deploy NSX Edge Appliance.

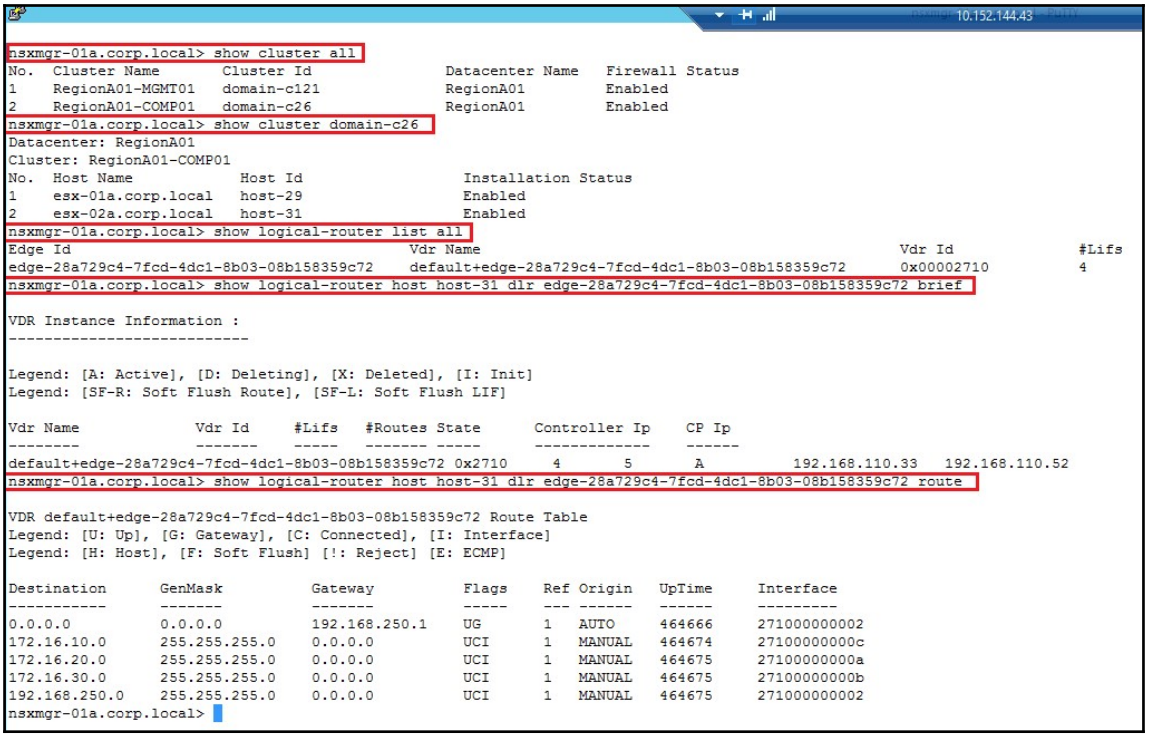

Connect NSX Edge to a Network
Logical Switch
Standard Portgroup
Distributed Portgroup
Filter
Name
Type
Universal-App-Logical-S...
Universal Logical Switch
Universal-DB-Logical-Sw...
Universal Logical Switch
Universal-Web-Logical-S...
Universal Logical Switch
3 items
Copy
OK
Cancel

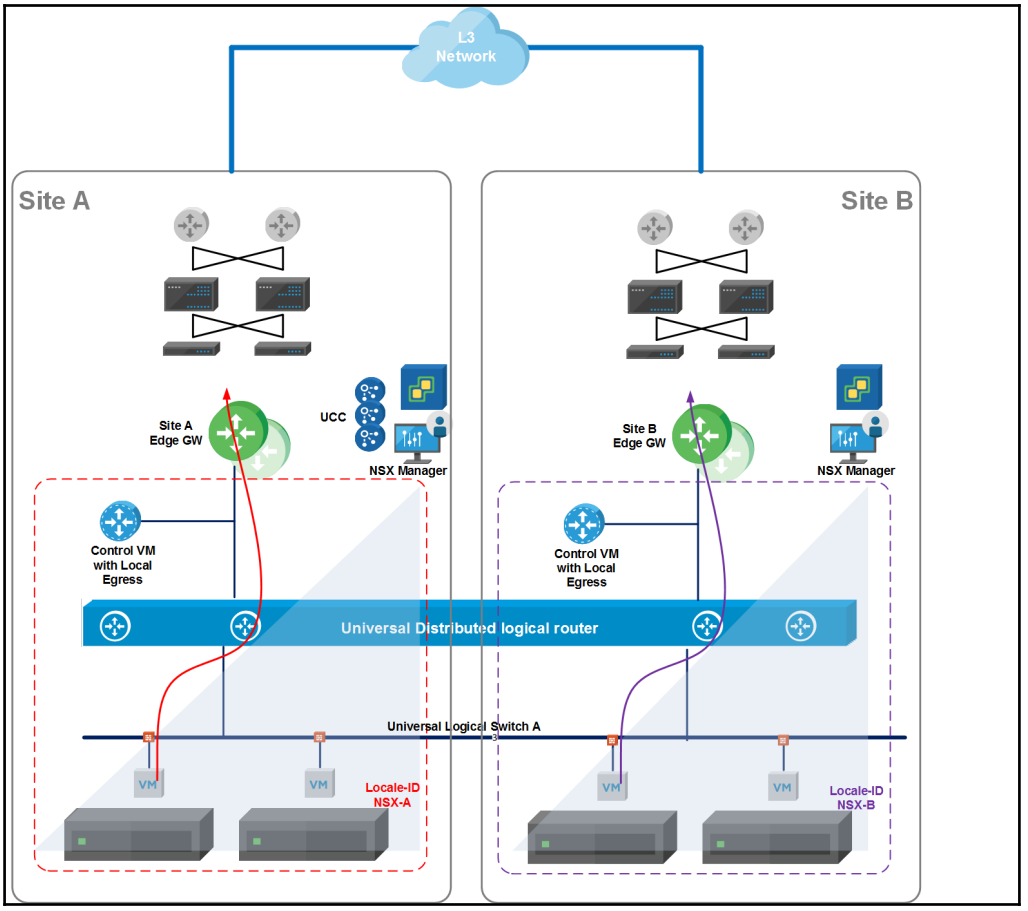

Add Interface
Name:
Web-Logical-Switch
Type:
Internal
Uplink
Connected To:
Universal-Web-Logical-Switch
Change
Remove
Connectivity Status:
Connected
Disconnected
Configure subnets
Filter
Primary IP Address
Subnet Prefix Length
172.16.10.1
24
1 items
Copy
MTU:
1500
OK
Cancel

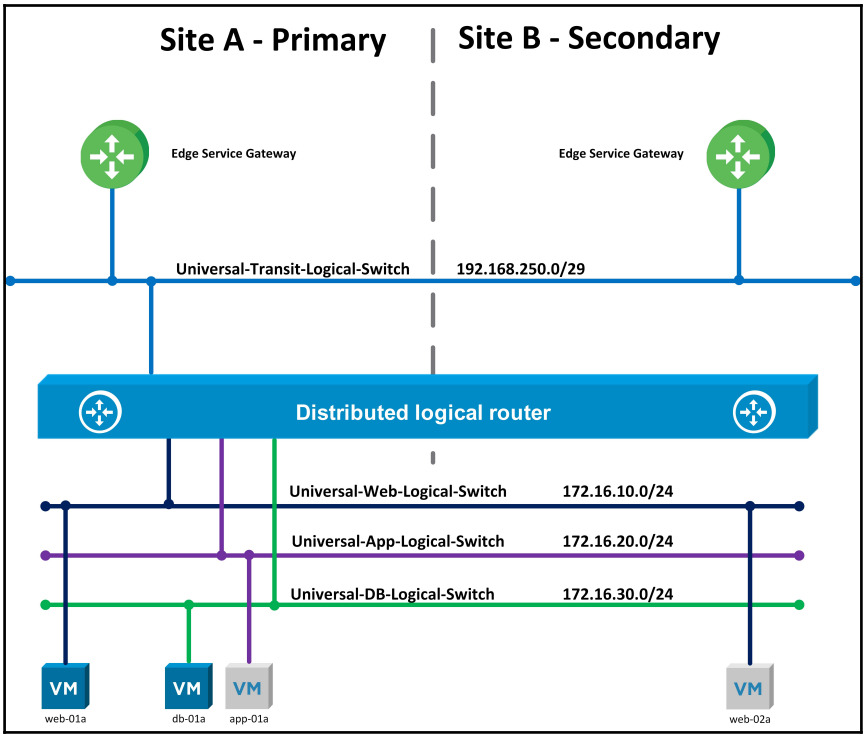

New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Ready to complete
Configure interfaces
HA Interface Configuration
Connected To: * Universal-DLR-HA
Change
Remove
Filter
Primary IP Address
Subnet Prefix Length
0 items
Copy
HA interface is a mandatory special-purpose interface that requires network connectivity and is configured separately from other interfaces in the Logical Router.
Configure interfaces of this NSX Edge
Name
IP Address
Subnet Prefix Length
Connected To
Transit-Logical-... 192.168.250.1* 24 Universal-Transit-Logica...
App-Logical-S... 172.16.20.1* 24 Universal-App-Logical-S...
DB-Logical-Sw... 172.16.30.1* 24 Universal-DB-Logical-S...
Web-logical-S... 172.16.10.1* 24 Universal-Web-Logical-...
Back
Next
Finish
Cancel

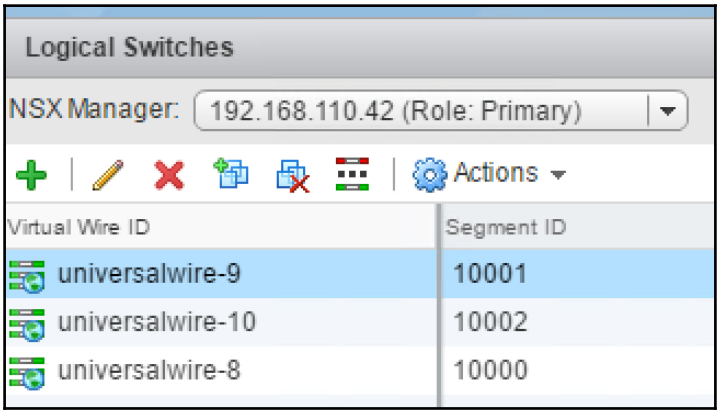

New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Ready to complete
Default gateway settings
Configure Default Gateway
vNIC:
Transit-Logical-Switch
Gateway IP:
192.168.250.1
MTU:
1500
Admin Distance:
1
Back
Next
Finish
Cancel

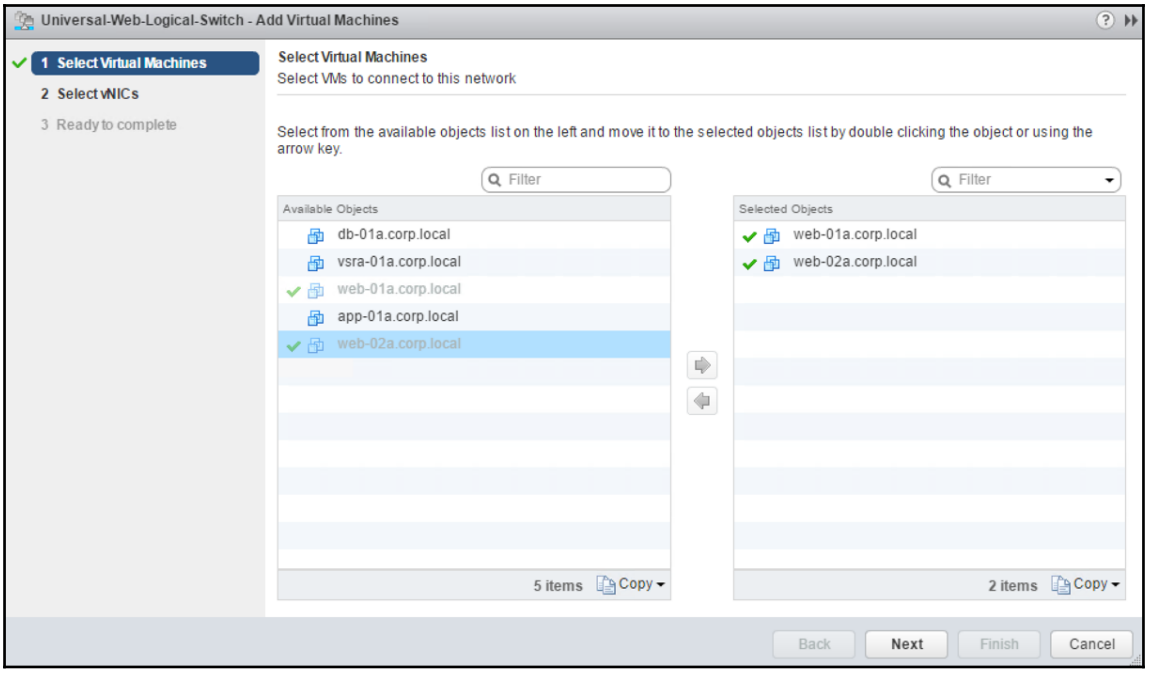

New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Ready to complete
Ready to complete
Name and description
Name: UDLR-01
Install Type: Universal Logical (Distributed) Router
Local Egress: Disabled
Tenant:
HA: Disabled
HA Interface Configuration
Connected To: Universal-DLR-HA
IP Address
Subnet Prefix Length
NSX Edge Appliances
Resource Pool
Host
RegionA01-COMP01
Interfaces
Name
IP Address
Subnet Prefix Length
Connected To
Transit-Logical-... 192.168.250.1* 24 Universal-Transit-Logi...
App-Logical-Swi... 172.16.20.1* 24 Universal-App-Logical...
DB-Logical-Swit... 172.16.30.1* 24 Universal-DB-Logical-...
Web-logical-Swi... 172.16.10.1* 24 Universal-Web-Logica...
Back
Next
Finish
Cancel

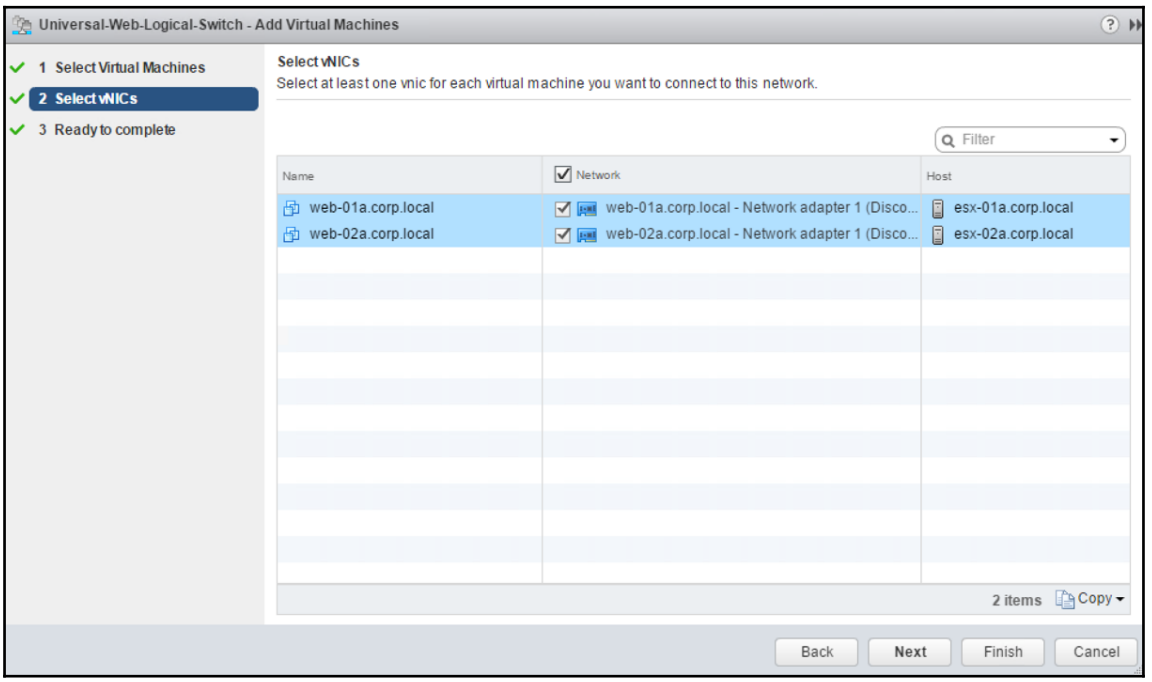

10.152.144.43
nsxmgr-01a.corp.local> show cluster all
No. Cluster Name Cluster Id Datacenter Name Firewall Status
1 RegionA01-MGMT01 domain-c121 RegionA01 Enabled
2 RegionA01-COMP01 domain-c26 RegionA01 Enabled
nsxmgr-01a.corp.local> show cluster domain-c26
Datacenter: RegionA01
Cluster: RegionA01-COMP01
No. Host Name Host Id Installation Status
1 esx-01a.corp.local host-29 Enabled
2 esx-02a.corp.local host-31 Enabled
nsxmgr-01a.corp.local> show logical-router list all
Edge Id Vdr Name Vdr Id #Lifs
edge-28a729c4-7fcd-4dc1-8b03-08b158359c72 default+edge-28a729c4-7fcd-4dc1-8b03-08b158359c72 0x00002710 4
nsxmgr-01a.corp.local> show logical-router host host-31 dlr edge-28a729c4-7fcd-4dc1-8b03-08b158359c72 brief
VDR Instance Information :
Legend: [A: Active], [D: Deleting], [X: Deleted], [I: Init]
Legend: [SF-R: Soft Flush Route], [SF-L: Soft Flush LIF]
Vdr Name Vdr Id #Lifs #Routes State Controller Ip CP Ip
default+edge-28a729c4-7fcd-4dc1-8b03-08b158359c72 0x2710 4 5 A 192.168.110.33 192.168.110.52
nsxmgr-01a.corp.local> show logical-router host host-31 dlr edge-28a729c4-7fcd-4dc1-8b03-08b158359c72 route
VDR default+edge-28a729c4-7fcd-4dc1-8b03-08b158359c72 Route Table
Legend: [U: Up], [G: Gateway], [C: Connected], [I: Interface]
Legend: [H: Host], [F: Soft Flush] [!: Reject] [E: ECMP]
Destination GenMask Gateway Flags Ref Origin UpTime Interface
0.0.0.0 0.0.0.0 192.168.250.1 UG 1 AUTO 464666 271000000002
172.16.10.0 255.255.255.0 0.0.0.0 UCI 1 MANUAL 464674 27100000000c
172.16.20.0 255.255.255.0 0.0.0.0 UCI 1 MANUAL 464675 27100000000a
172.16.30.0 255.255.255.0 0.0.0.0 UCI 1 MANUAL 464675 27100000000b
192.168.250.0 255.255.255.0 0.0.0.0 UCI 1 MANUAL 464675 271000000002
nsxmgr-01a.corp.local>

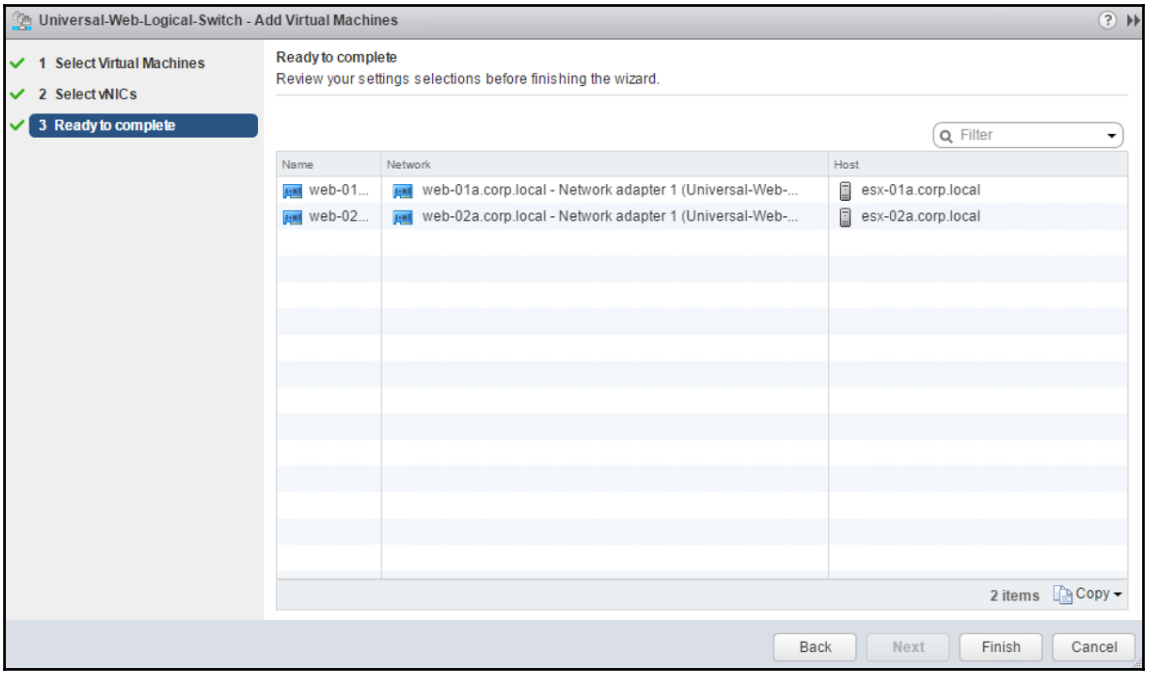

L3
Network
Site A
Site B
Site A
Edge GW
UCC
NSX Manager
Site B
Edge GW
NSX Manager
Control VM
with Local
Egress
Control VM
with Local
Egress
Universal Distributed logical router
Universal Logical Switch A
VM
VM
Locale-ID
NSX-A
VM
VM
Locale-ID
NSX-B


Site A - Primary
Site B - Secondary
Edge Service Gateway
Edge Service Gateway
Universal-Transit-Logical-Switch
192.168.250.0/29
Distributed logical router
Universal-Web-Logical-Switch
172.16.10.0/24
Universal-App-Logical-Switch
172.16.20.0/24
Universal-DB-Logical-Switch
172.16.30.0/24
VM
web-01a
VM
db-01a
VM
app-01a
VM
web-02a

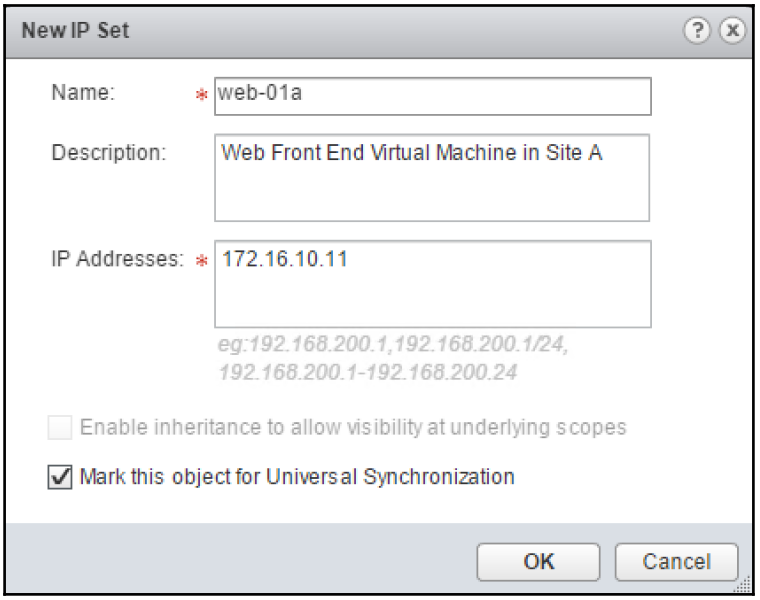

Logical Switches
NSX Manager:
192.168.110.42 (Role: Primary)
Actions
Virtual Wire ID
Segment ID
universalwire-9
10001
universalwire-10
10002
universalwire-8
10000

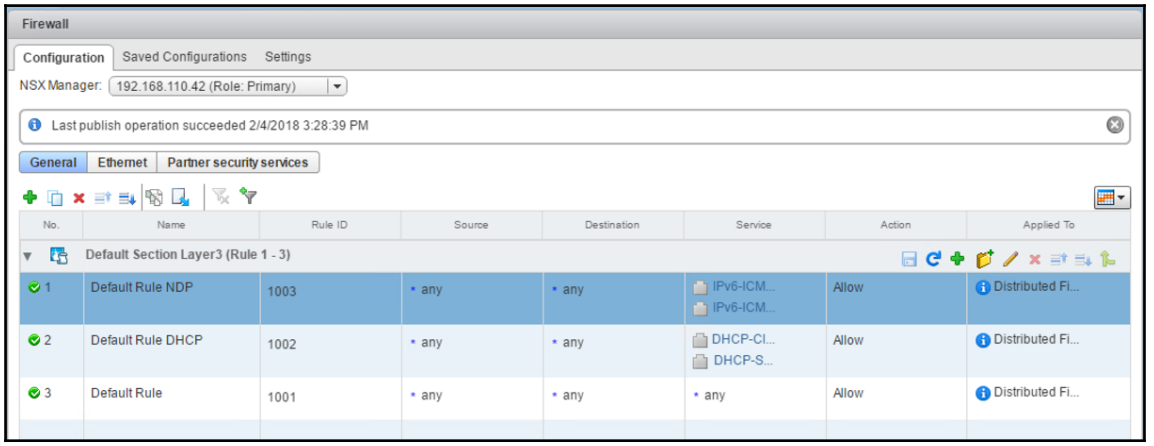

Universal-Web-Logical-Switch - Add Virtual Machines
1 Select Virtual Machines
2 Select vNICs
3 Ready to complete
Select Virtual Machines
Select VMs to connect to this network
Select from the available objects list on the left and move it to the selected objects list by double clicking the object or using the arrow key.
Filter
Available Objects
db-01a.corp.local
vsra-01a.corp.local
web-01a.corp.local
app-01a.corp.local
web-02a.corp.local
5 items
Copy
Filter
Selected Objects
web-01a.corp.local
web-02a.corp.local
2 items
Copy
Back
Next
Finish
Cancel

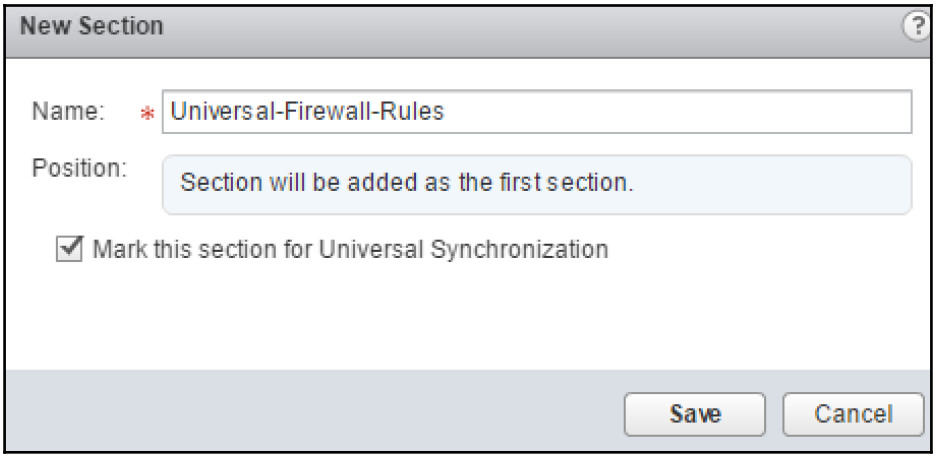

Universal-Web-Logical-Switch - Add Virtual Machines
1 Select Virtual Machines
2 Select vNICs
3 Ready to complete
Select vNICs
Select at least one vnic for each virtual machine you want to connect to this network.
Filter
Name
Network
Host
web-01a.corp.local
web-01a.corp.local - Network adapter 1 (Disco...
esx-01a.corp.local
web-02a.corp.local
web-02a.corp.local - Network adapter 1 (Disco...
esx-02a.corp.local
2 items
Copy
Back
Next
Finish
Cancel



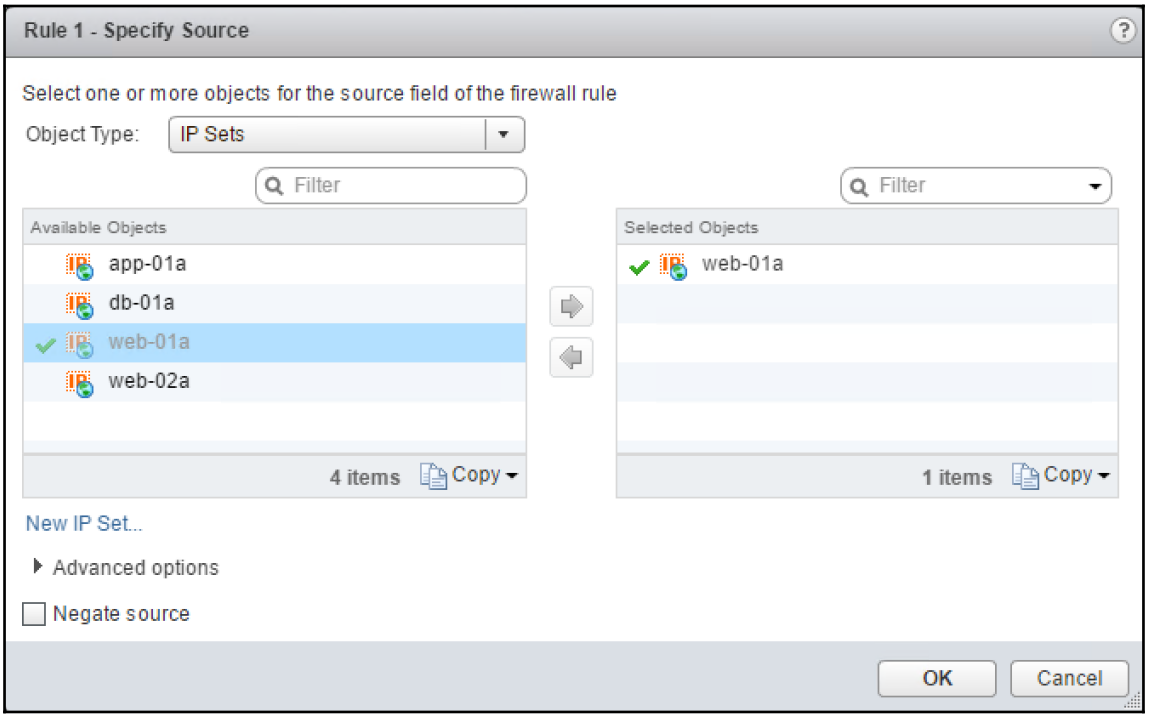

```
root@web-01a [ ~ ]# ping -c 4 172.16.10.12
PING 172.16.10.12 (172.16.10.12) 56(84) bytes of data.
64 bytes from 172.16.10.12: icmp_seq=1 ttl=64 time=1.09 ms
64 bytes from 172.16.10.12: icmp_seq=2 ttl=64 time=1.05 ms
64 bytes from 172.16.10.12: icmp_seq=3 ttl=64 time=0.923 ms
64 bytes from 172.16.10.12: icmp_seq=4 ttl=64 time=1.09 ms

--- 172.16.10.12 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 4506ms
rtt min/avg/max/mdev = 0.923/1.042/1.098/0.074 ms
root@web-01a [ ~ ]# _
```

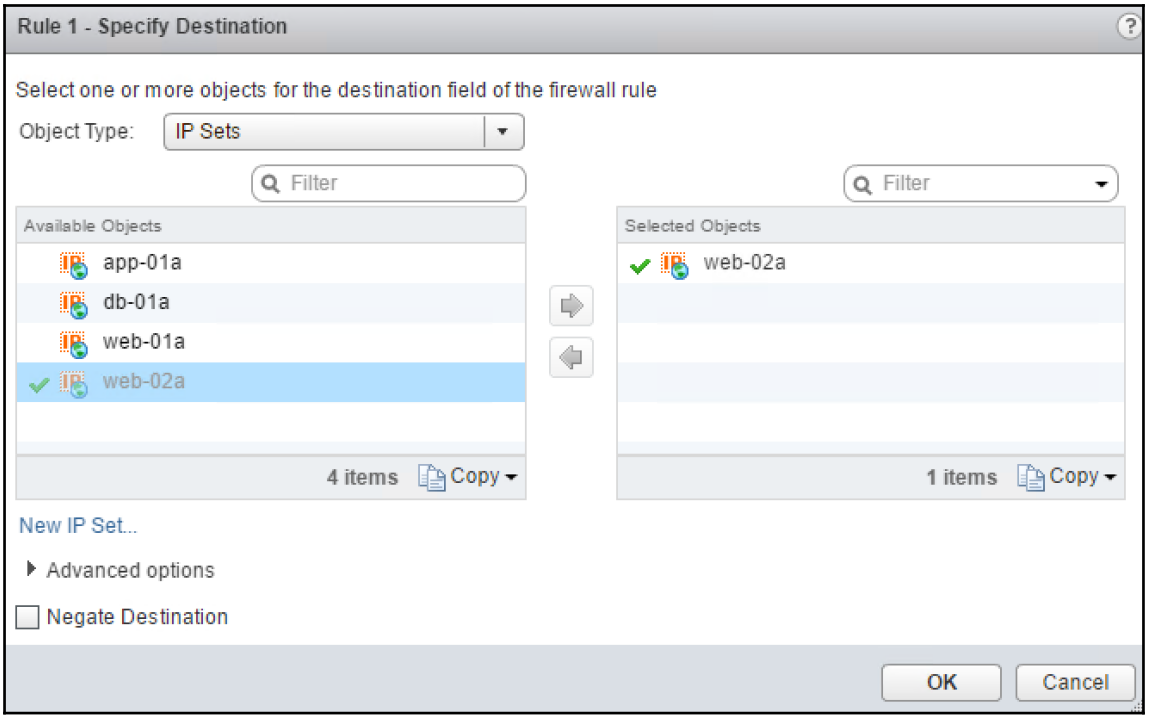

New IP Set
Name:
web-01a
Description:
Web Front End Virtual Machine in Site A
IP Addresses:
172.16.10.11
eg:192.168.200.1,192.168.200.1/24,
192.168.200.1-192.168.200.24
Enable inheritance to allow visibility at underlying scopes
Mark this object for Universal Synchronization
OK
Cancel

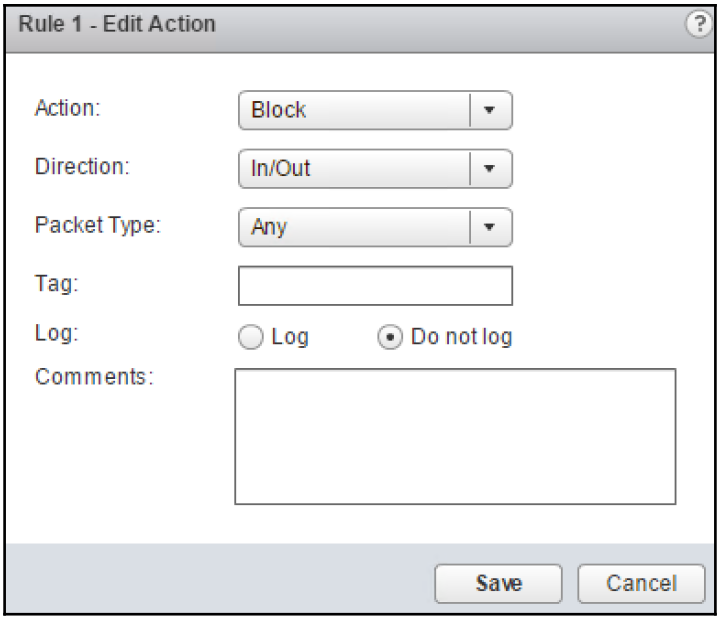

Firewall
Configuration
Saved Configurations
Settings
NSX Manager:
192.168.110.42 (Role: Primary)
Last publish operation succeeded 2/4/2018 3:28:39 PM
General
Ethernet
Partner security services
No.
Name
Rule ID
Source
Destination
Service
Action
Applied To
Default Section Layer3 (Rule 1 - 3)
1
Default Rule NDP
1003
any
any
IPv6-ICM...
IPv6-ICM...
Allow
Distributed Fi...
2
Default Rule DHCP
1002
any
any
DHCP-Cl...
DHCP-S...
Allow
Distributed Fi...
3
Default Rule
1001
any
any
any
Allow
Distributed Fi...

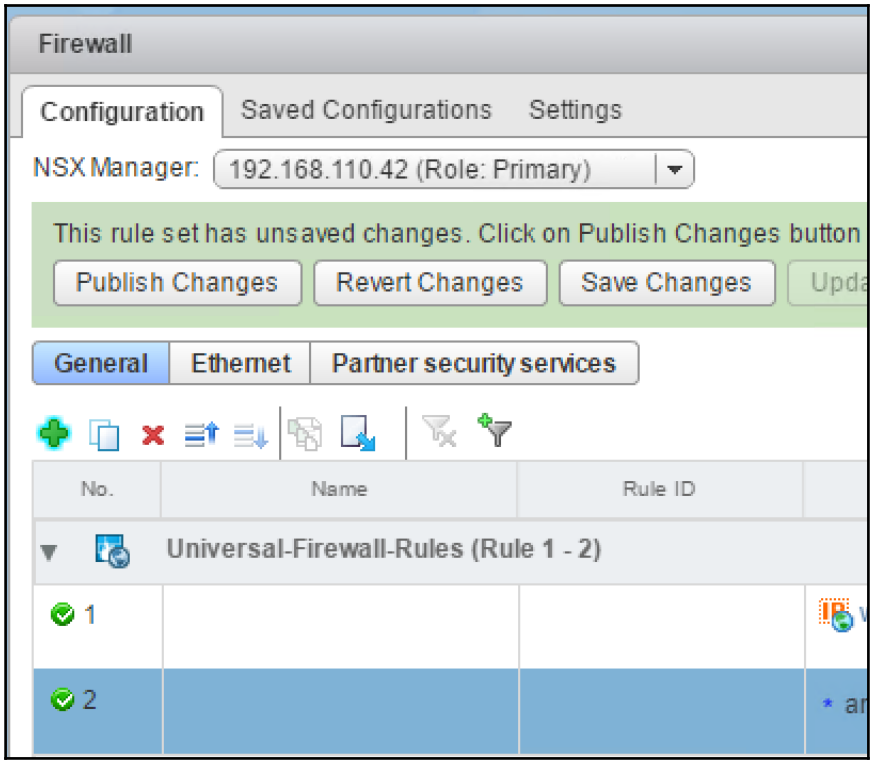

New Section
Name:
Universal-Firewall-Rules
Position:
Section will be added as the first section.
Mark this section for Universal Synchronization
Save
Cancel

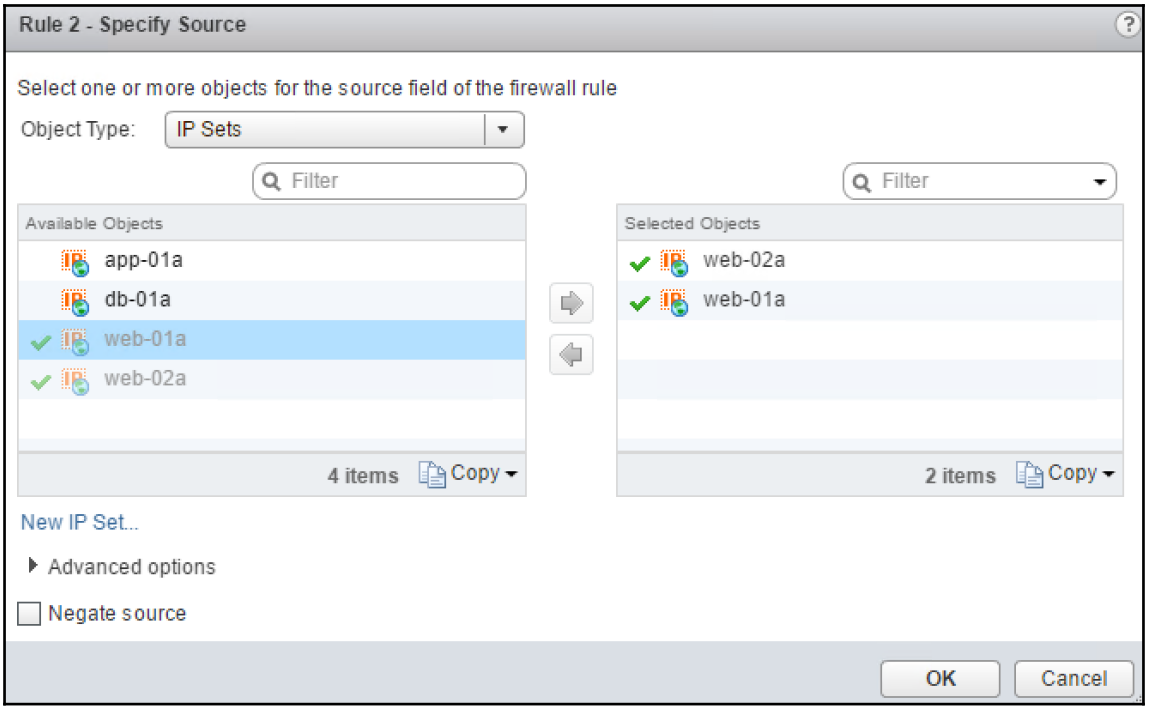

Universal-Firewall-Rules

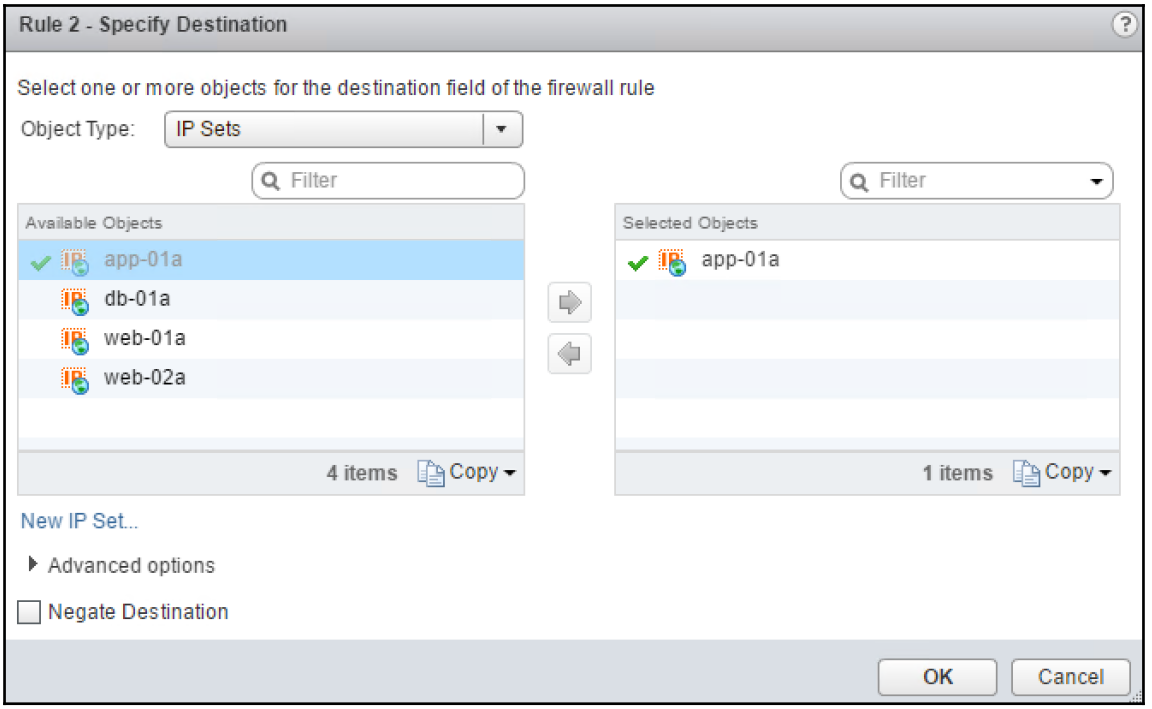

Rule 1 - Specify Source
Select one or more objects for the source field of the firewall rule
Object Type:
IP Sets
Filter
Filter
Available Objects
app-01a
db-01a
web-01a
web-02a
4 items
Copy
Selected Objects
web-01a
1 items
Copy
New IP Set...
Advanced options
Negate source
OK
Cancel

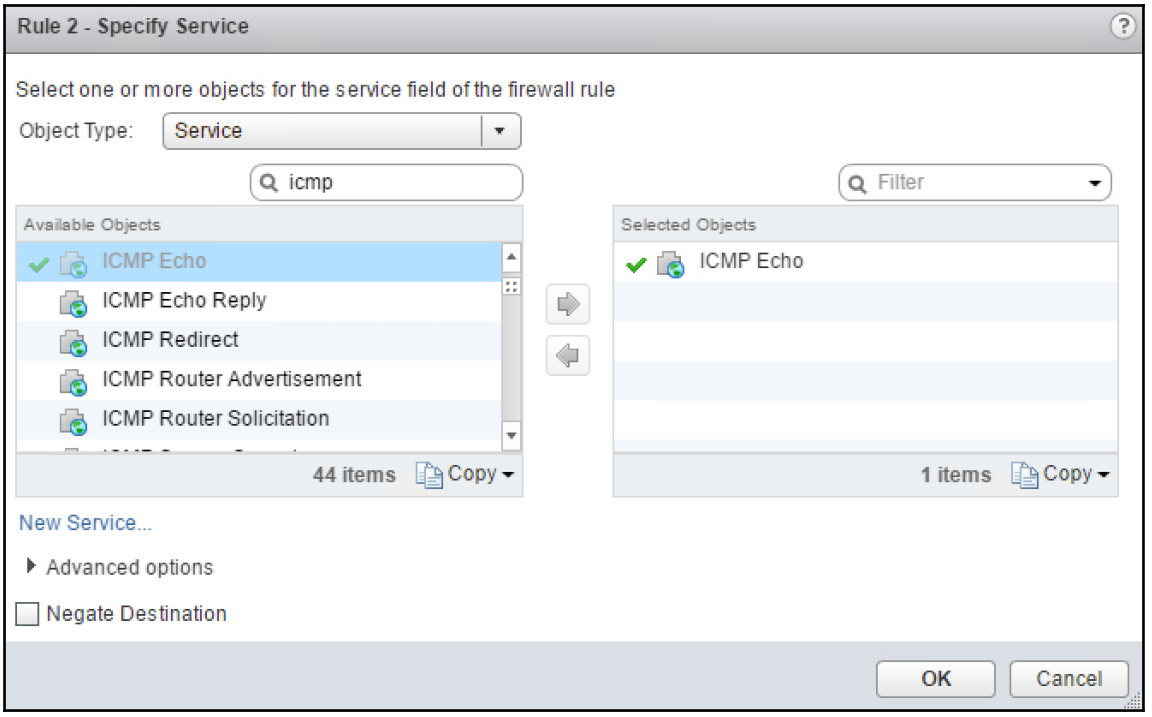

Rule 1 - Specify Destination
Select one or more objects for the destination field of the firewall rule
Object Type:
IP Sets
Filter
Filter
Available Objects
app-01a
db-01a
web-01a
web-02a
4 items
Copy
Selected Objects
web-02a
1 items
Copy
New IP Set...
Advanced options
Negate Destination
OK
Cancel

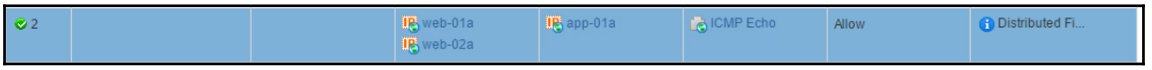

Rule 1 - Edit Action
Action:
Block
Direction:
In/Out
Packet Type:
Any
Tag:
Log:
Log
Do not log
Comments:
Save
Cancel

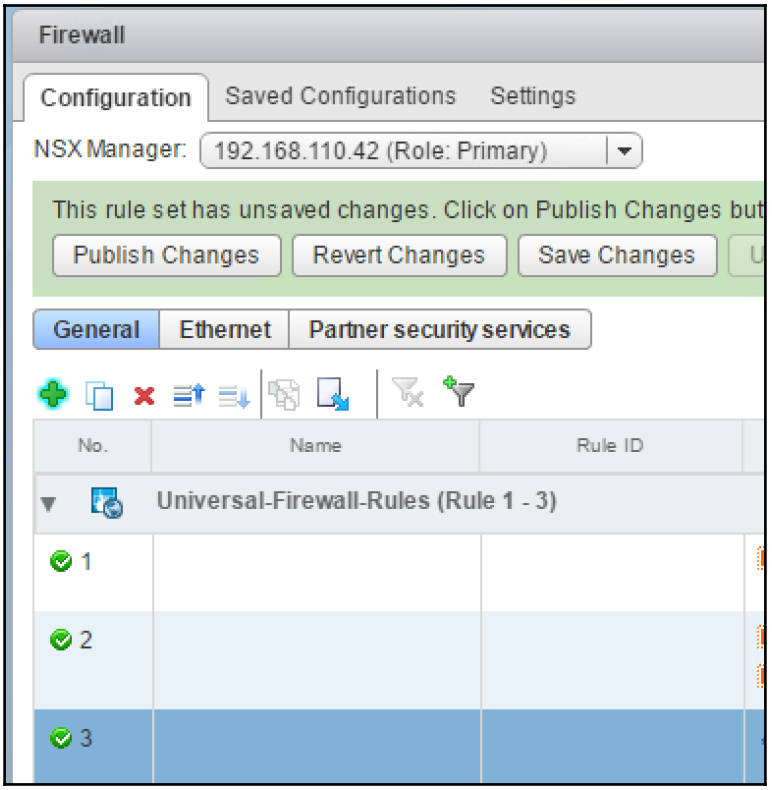

Firewall
Configuration
Saved Configurations
Settings
NSX Manager:
192.168.110.42 (Role: Primary)
This rule set has unsaved changes. Click on Publish Changes button
Publish Changes
Revert Changes
Save Changes
General
Ethernet
Partner security services
No.
Name
Rule ID
Universal-Firewall-Rules (Rule 1 - 2)
1
2

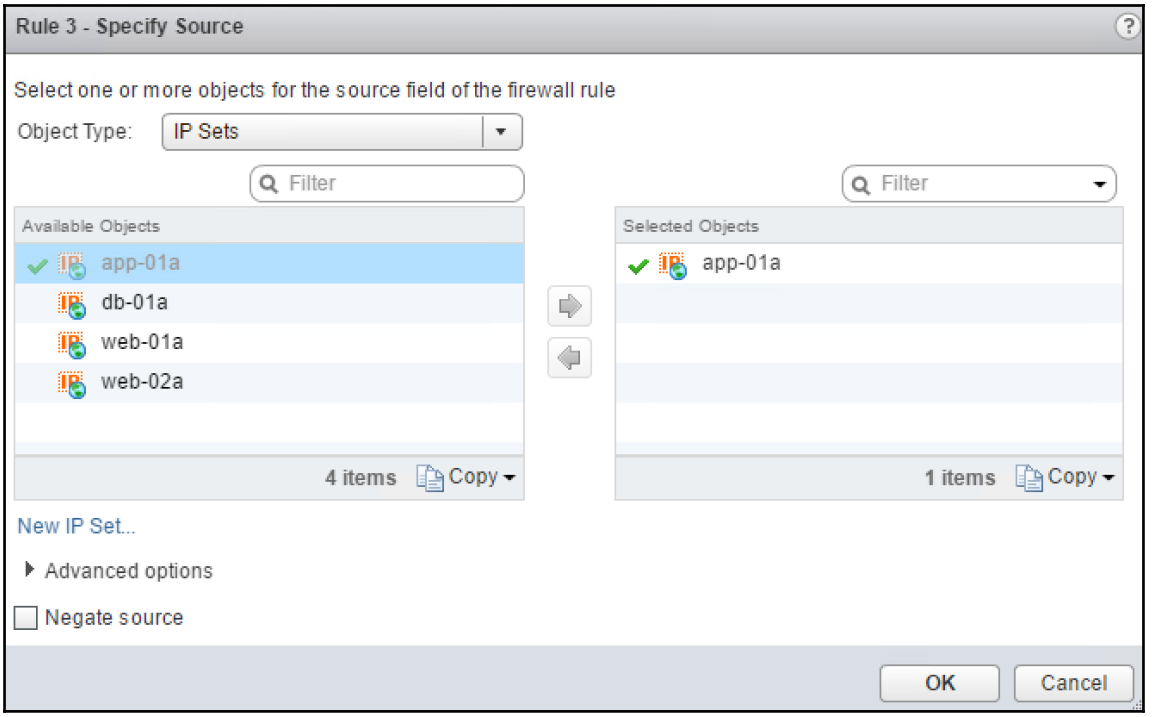

Rule 2 - Specify Source
Select one or more objects for the source field of the firewall rule
Object Type:
IP Sets
Filter
Filter
Available Objects
app-01a
db-01a
web-01a
web-02a
4 items
Copy
Selected Objects
web-02a
web-01a
2 items
Copy
New IP Set...
Advanced options
Negate source
OK
Cancel

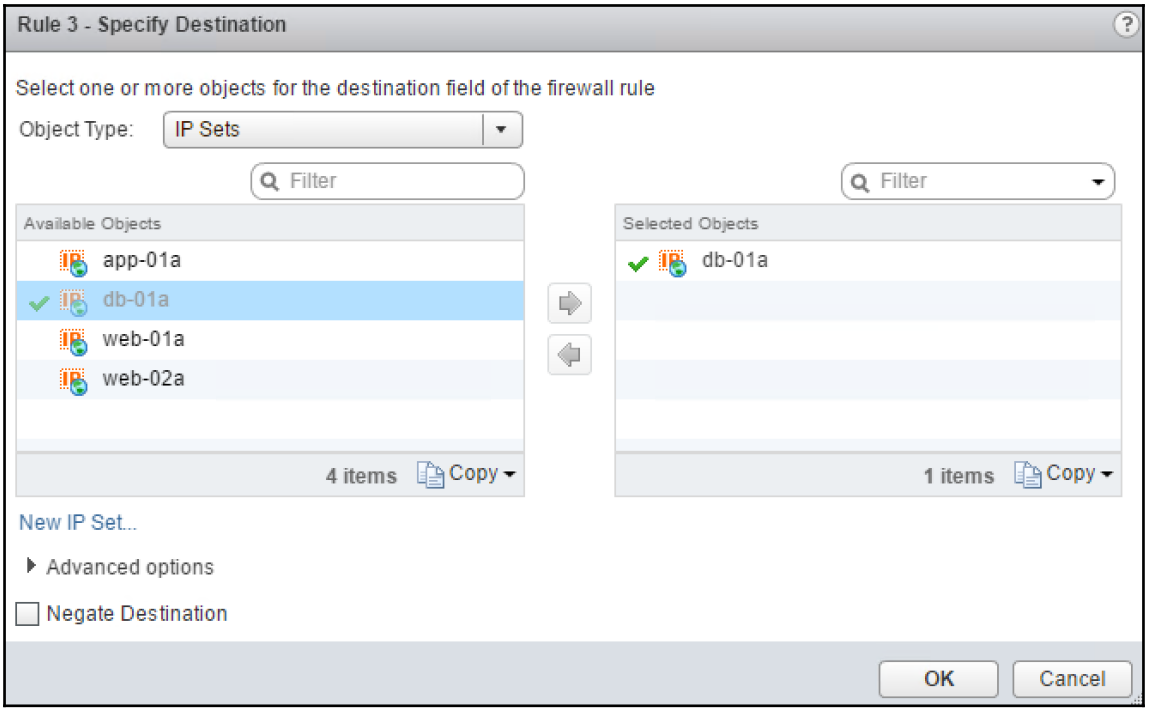

Rule 2 - Specify Destination
Select one or more objects for the destination field of the firewall rule
Object Type:
IP Sets
Filter
Filter
Available Objects
app-01a
db-01a
web-01a
web-02a
4 items
Copy
Selected Objects
app-01a
1 items
Copy
New IP Set...
Advanced options
Negate Destination
OK
Cancel

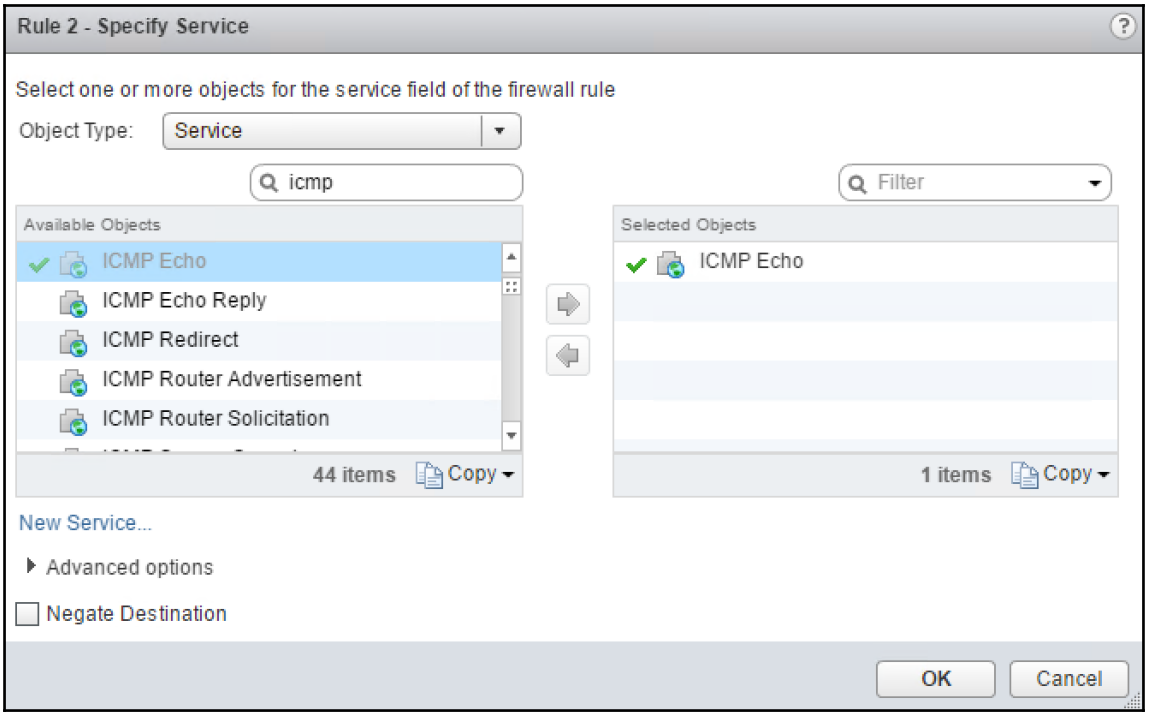

Rule 2 - Specify Service
Select one or more objects for the service field of the firewall rule
Object Type:
Service
icmp
Filter
Available Objects
ICMP Echo
ICMP Echo Reply
ICMP Redirect
ICMP Router Advertisement
ICMP Router Solicitation
44 items
Copy
Selected Objects
ICMP Echo
1 items
Copy
New Service...
Advanced options
Negate Destination
OK
Cancel


2
web-01a
web-02a
app-01a
ICMP Echo
Allow
Distributed Fi...

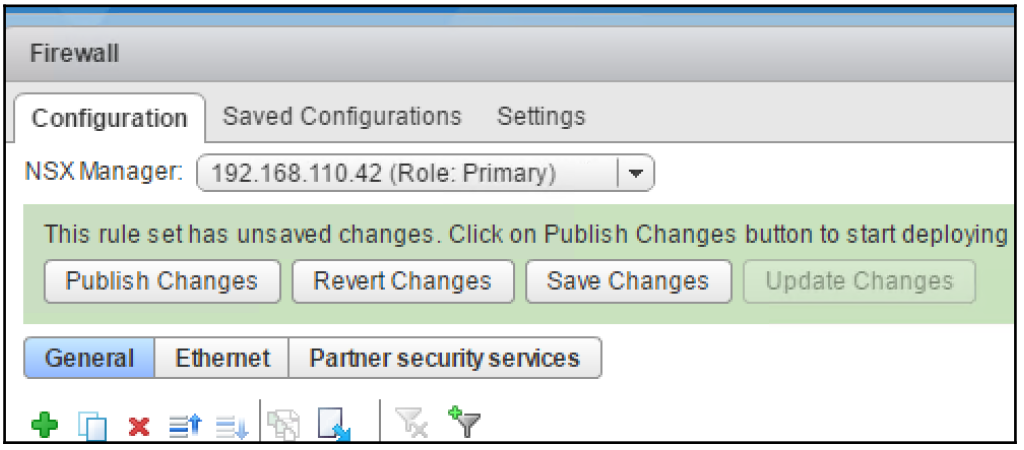

Firewall
Configuration
Saved Configurations
Settings
NSX Manager:
192.168.110.42 (Role: Primary)
This rule set has unsaved changes. Click on Publish Changes but
Publish Changes
Revert Changes
Save Changes
General
Ethernet
Partner security services
No.
Name
Rule ID
Universal-Firewall-Rules (Rule 1 - 3)
1
2
3

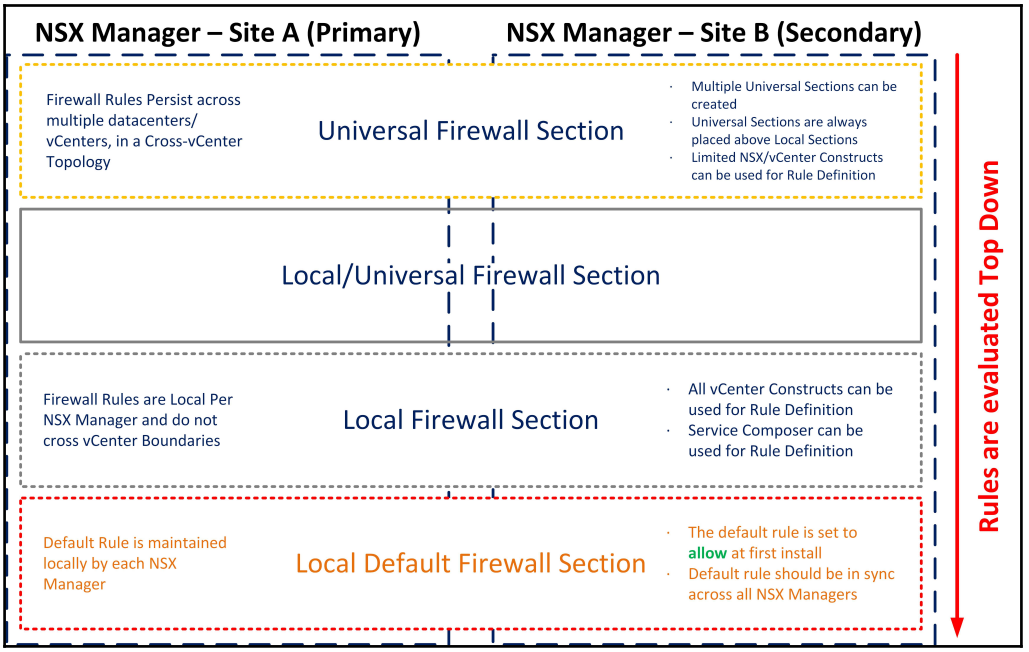

Rule 3 - Specify Source
Select one or more objects for the source field of the firewall rule
Object Type:
IP Sets
Filter
Filter
Available Objects
app-01a
db-01a
web-01a
web-02a
4 items
Copy
Selected Objects
app-01a
1 items
Copy
New IP Set...
Advanced options
Negate source
OK
Cancel


Rule 3 - Specify Destination
Select one or more objects for the destination field of the firewall rule
Object Type:
IP Sets
Filter
Filter
Available Objects
app-01a
db-01a
web-01a
web-02a
4 items
Copy
Selected Objects
db-01a
1 items
Copy
New IP Set...
Advanced options
Negate Destination
OK
Cancel

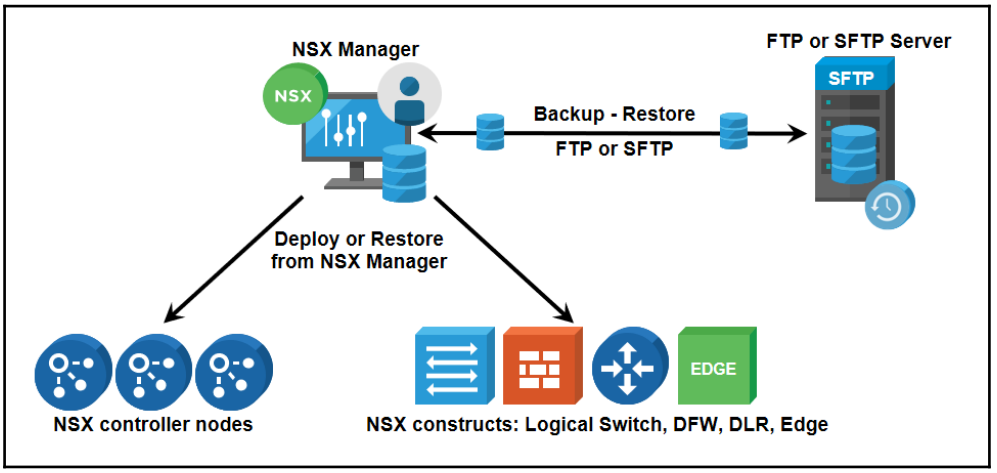

Rule 2 - Specify Service
Select one or more objects for the service field of the firewall rule
Object Type:
Service
icmp
Filter
Available Objects
ICMP Echo
ICMP Echo Reply
ICMP Redirect
ICMP Router Advertisement
ICMP Router Solicitation
44 items
Copy
Selected Objects
ICMP Echo
1 items
Copy
New Service...
Advanced options
Negate Destination
OK
Cancel

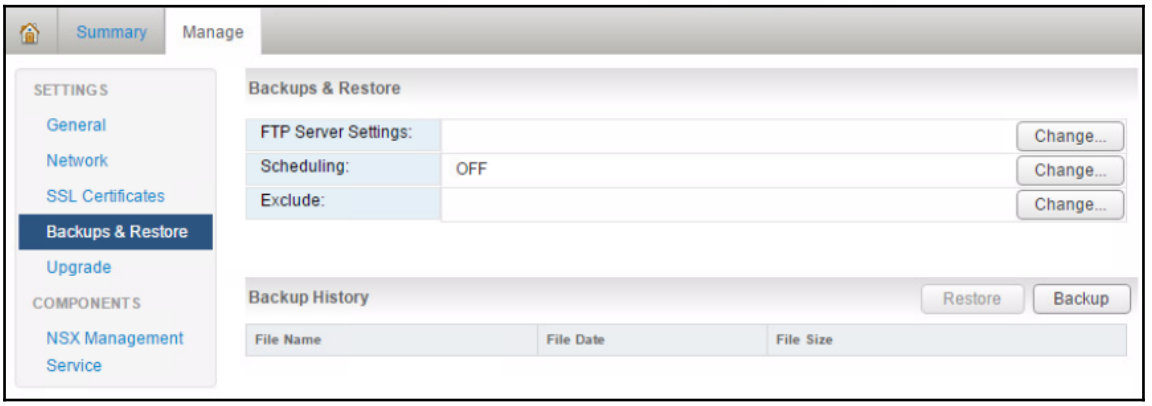

3
app-01a
db-01a
any
Allow
Distributed Fi...

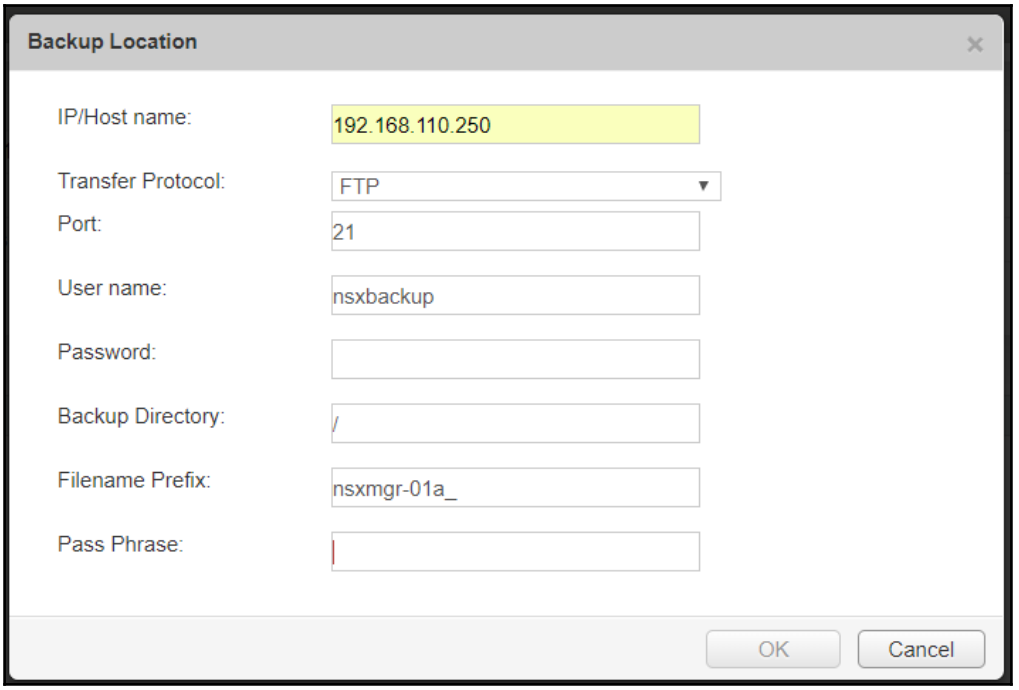

Firewall
Configuration
Saved Configurations
Settings
NSX Manager:
192.168.110.42 (Role: Primary)
This rule set has unsaved changes. Click on Publish Changes button to start deploying
Publish Changes
Revert Changes
Save Changes
Update Changes
General
Ethernet
Partner security services

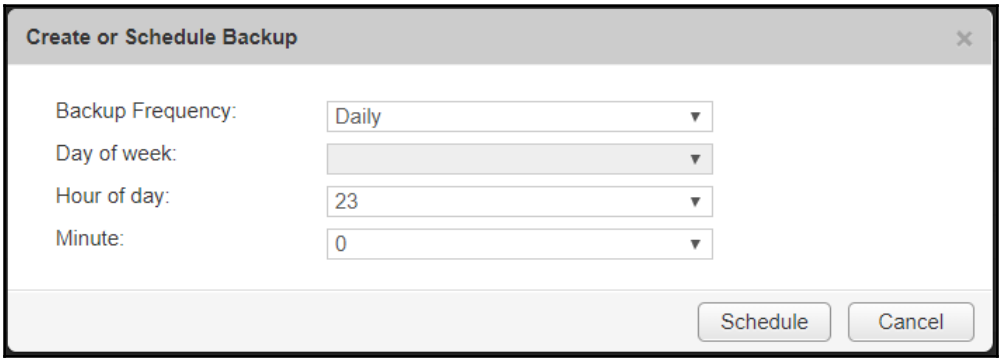

NSX Manager – Site A (Primary)
NSX Manager – Site B (Secondary)
Firewall Rules Persist across multiple datacenters/ vCenters, in a Cross-vCenter Topology
Universal Firewall Section
Multiple Universal Sections can be created
Universal Sections are always placed above Local Sections
Limited NSX/vCenter Constructs can be used for Rule Definition
Local/Universal Firewall Section
Firewall Rules are Local Per NSX Manager and do not cross vCenter Boundaries
Local Firewall Section
All vCenter Constructs can be used for Rule Definition
Service Composer can be used for Rule Definition
Default Rule is maintained locally by each NSX Manager
Local Default Firewall Section
The default rule is set to allow at first install
Default rule should be in sync across all NSX Managers
Rules are evaluated Top Down

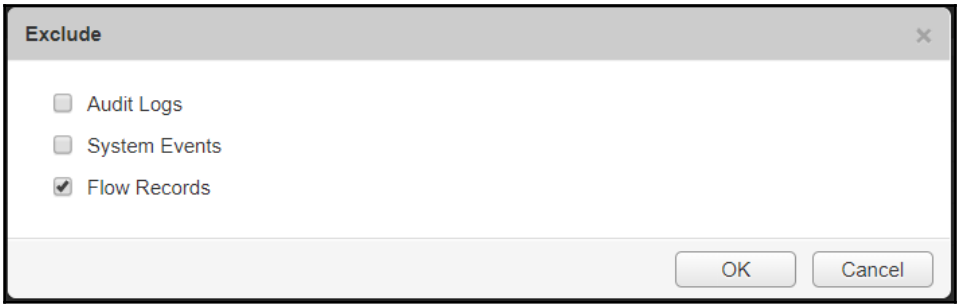
Chapter 08: Backing up and Restoring VMware NSX Components

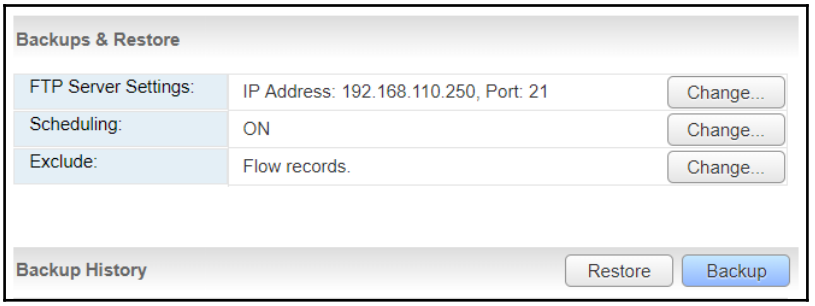


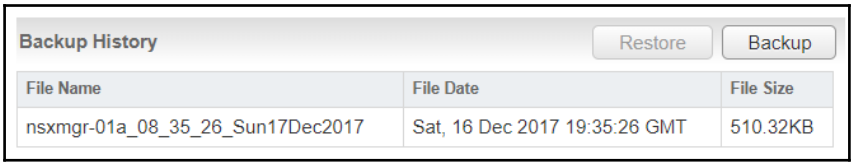


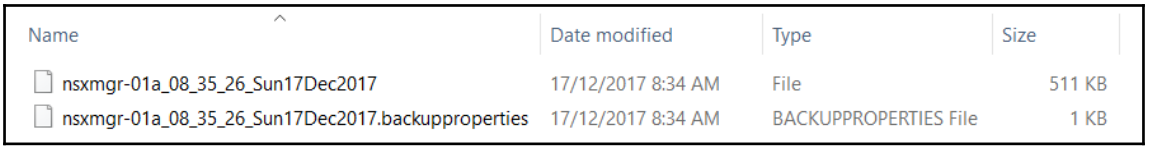

Backup Location
IP/Host name:
192.168.110.250
Transfer Protocol:
FTP
Port:
21
User name:
nsxbackup
Password:
Backup Directory:
/
Filename Prefix:
nsxmgr-01a_
Pass Phrase:
OK
Cancel


Create or Schedule Backup
Backup Frequency:
Daily
Day of week:
Hour of day:
23
Minute:
0
Schedule
Cancel


Exclude
Audit Logs
System Events
Flow Records
OK
Cancel

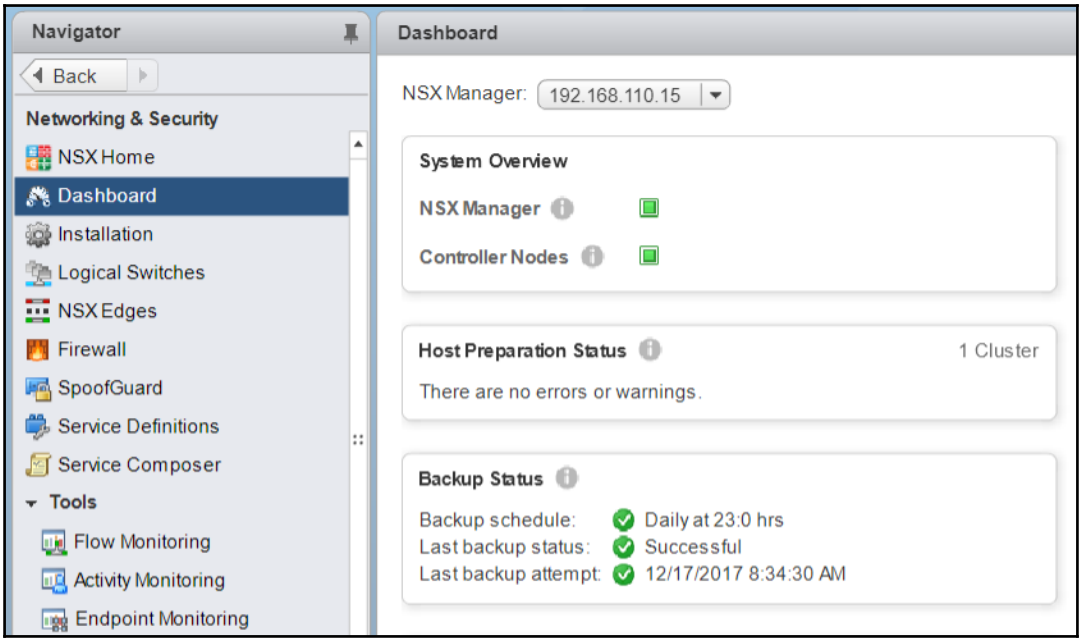

Backups & Restore
FTP Server Settings:
IP Address: 192.168.110.250, Port: 21
Change...
Scheduling:
ON
Change...
Exclude:
Flow records.
Change...
Backup History
Restore
Backup

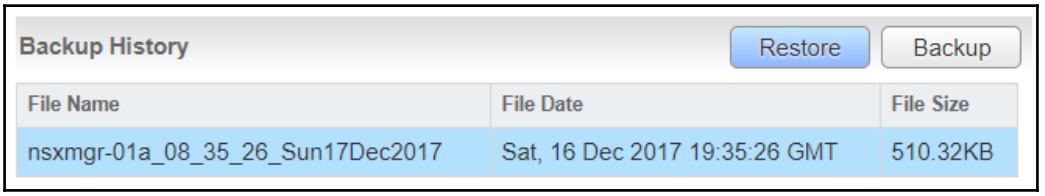

Backup History
Restore
Backup
File Name
File Date
File Size
nsxmgr-01a_08_35_26_Sun17Dec2017
Sat, 16 Dec 2017 19:35:26 GMT
510.32KB

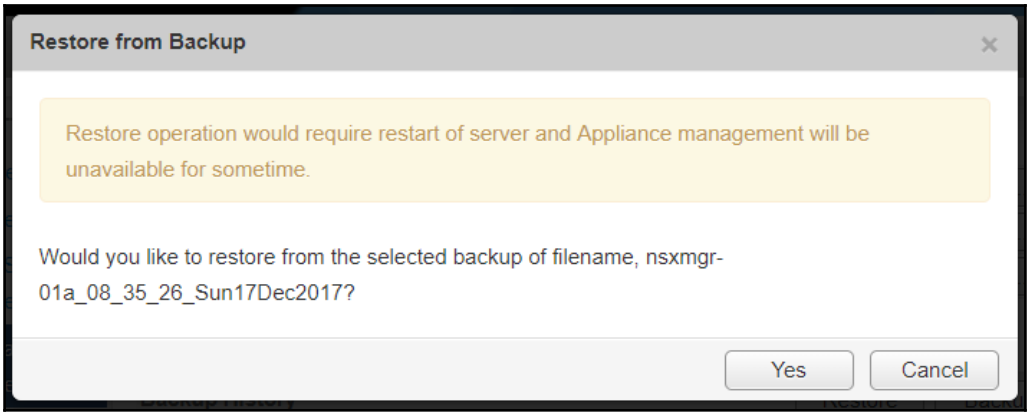

Name
Date modified
Type
Size
nsxmgr-01a_08_35_26_Sun17Dec2017
17/12/2017 8:34 AM
File
511 KB
nsxmgr-01a_08_35_26_Sun17Dec2017.backupproperties
17/12/2017 8:34 AM
BACKUPPROPERTIES File
1 KB

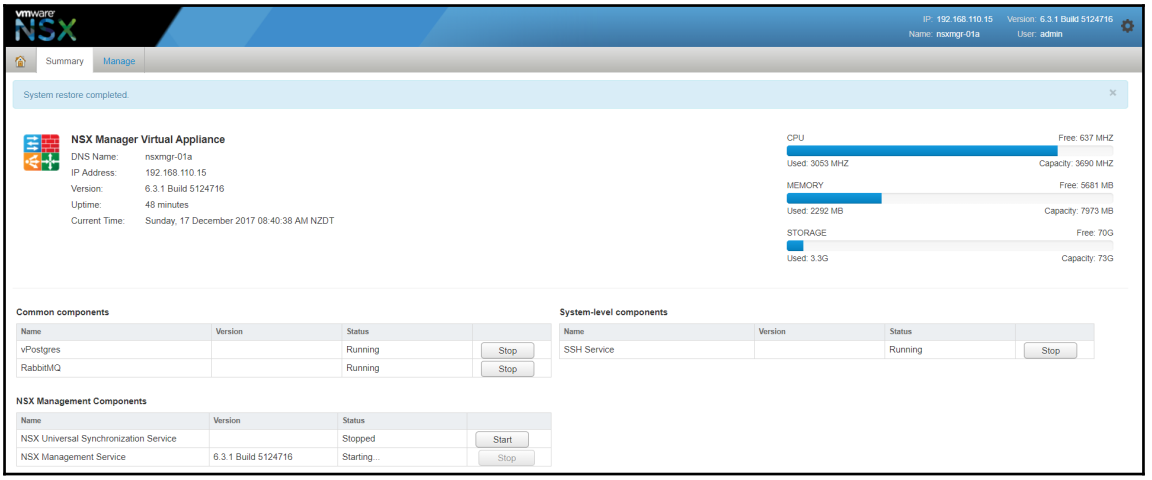
nsxmgr-01a_08_35_26_Sun17Dec2017.backupproperties

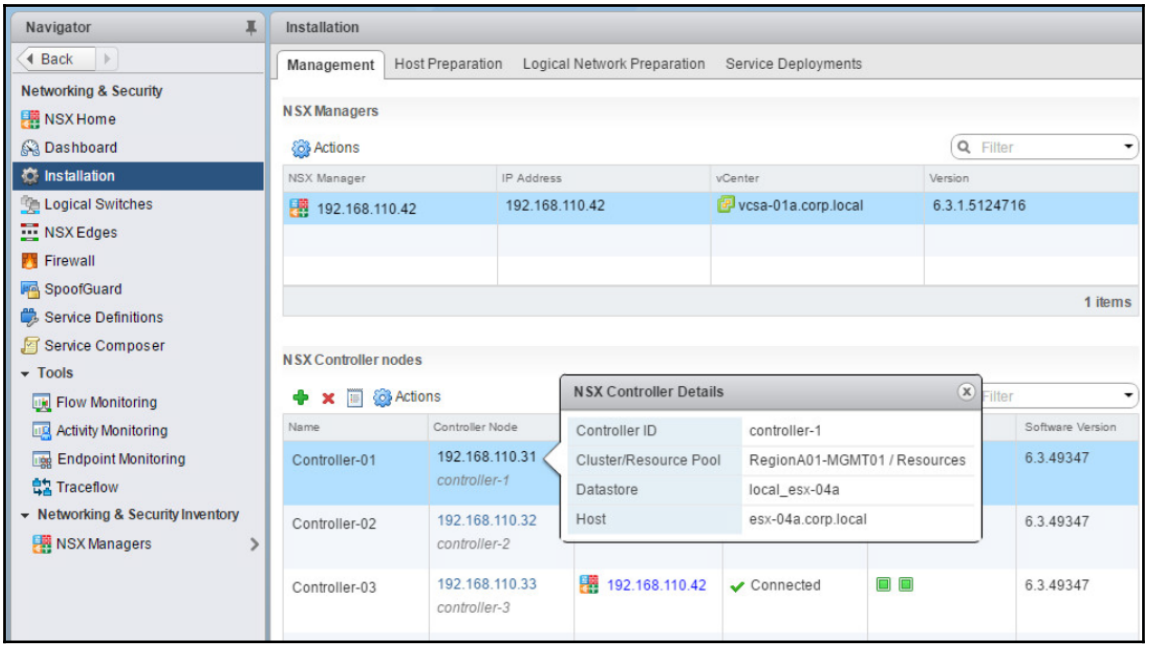
```
#vShield version information
#Fri, 24 Feb 2017 21:00:25 -0800

em.majorVersion=16
em.minorVersion=3
em.buildNumber=5124716
em.preReleaseType=release
em.marketingMajorVersion=6
em.marketingMinorVersion=3
em.marketingPatchVersion=1
```

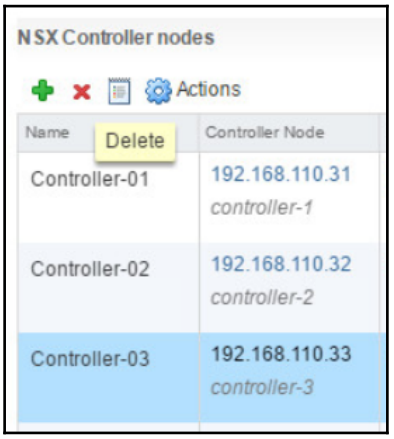


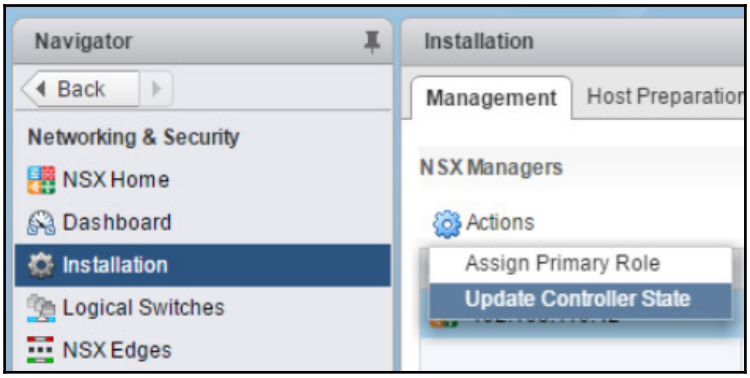


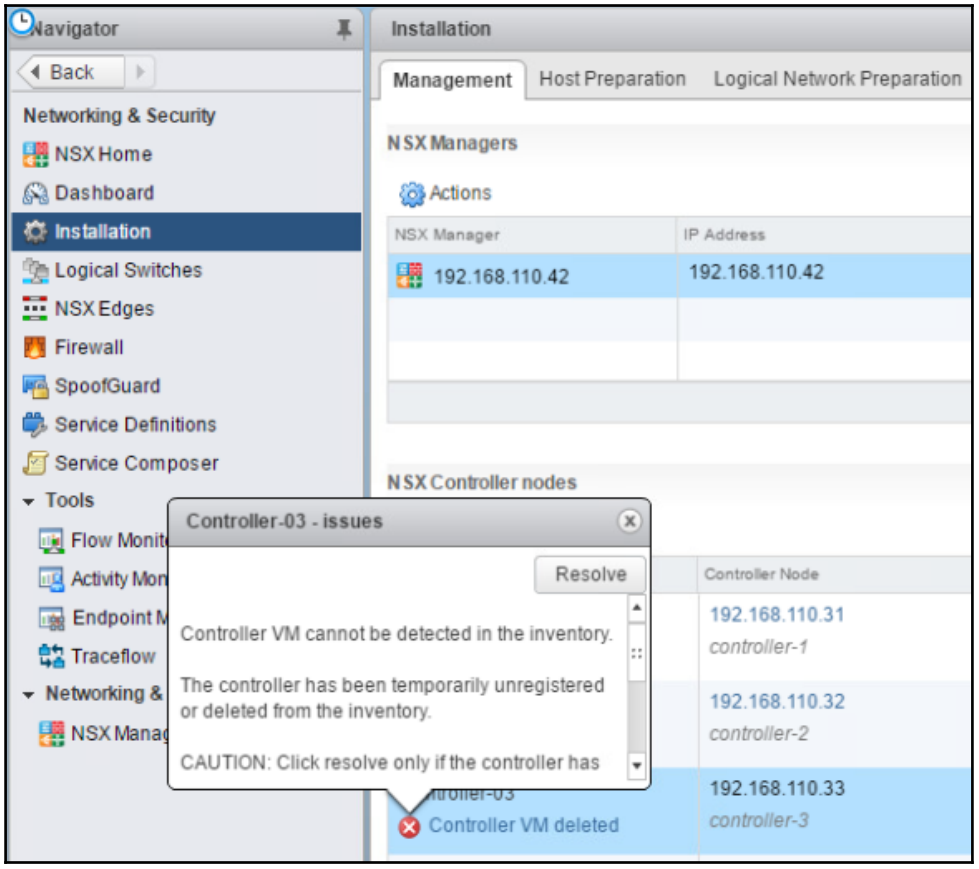

Restore from Backup
Restore operation would require restart of server and Appliance management will be unavailable for sometime.
Would you like to restore from the selected backup of filename, nsxmgr-01a_08_35_26_Sun17Dec2017?
Yes
Cancel

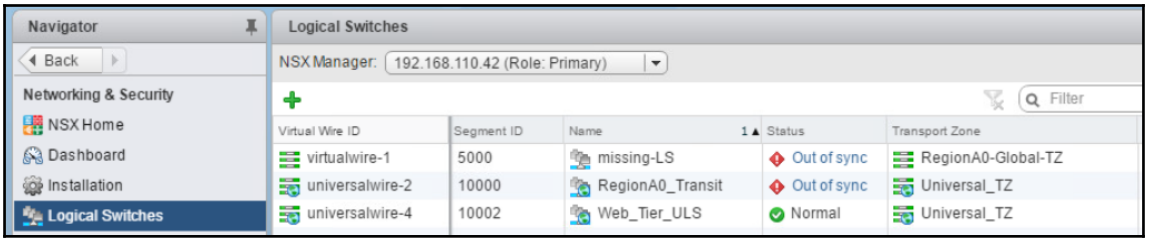

vmware NSX
IP: 192.168.110.15
Name: nsxmgr-01a
Version: 6.3.1 Build 5124716
User: admin
Summary
Manage
System restore completed.
NSX Manager Virtual Appliance
DNS Name: nsxmgr-01a
IP Address: 192.168.110.15
Version: 6.3.1 Build 5124716
Uptime: 48 minutes
Current Time: Sunday, 17 December 2017 08:40:38 AM NZDT
CPU
Free: 637 MHZ
Used: 3053 MHZ
Capacity: 3690 MHZ
MEMORY
Free: 5681 MB
Used: 2292 MB
Capacity: 7973 MB
STORAGE
Free: 70G
Used: 3.3G
Capacity: 73G
Common components
Name
Version
Status
vPostgres
Running
Stop
RabbitMQ
Running
Stop
System-level components
Name
Version
Status
SSH Service
Running
Stop
NSX Management Components
Name
Version
Status
NSX Universal Synchronization Service
Stopped
Start
NSX Management Service
6.3.1 Build 5124716
Starting...
Stop

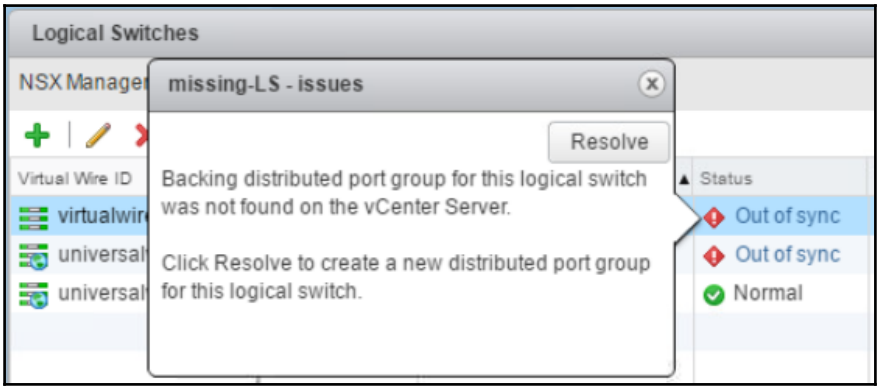

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Tools
Flow Monitoring
Activity Monitoring
Endpoint Monitoring
Traceflow
Networking & Security Inventory
NSX Managers
Installation
Management
Host Preparation
Logical Network Preparation
Service Deployments
NSX Managers
Actions
Filter
NSX Manager
IP Address
vCenter
Version
192.168.110.42
192.168.110.42
vcsa-01a.corp.local
6.3.1.5124716
1 items
NSX Controller nodes
Actions
Filter
Name
Controller Node
Software Version
Controller-01
192.168.110.31
controller-1
6.3.49347
Controller-02
192.168.110.32
controller-2
6.3.49347
Controller-03
192.168.110.33
controller-3
192.168.110.42
Connected
6.3.49347
NSX Controller Details
Controller ID
controller-1
Cluster/Resource Pool
RegionA01-MGMT01 / Resources
Datastore
local_esx-04a
Host
esx-04a.corp.local

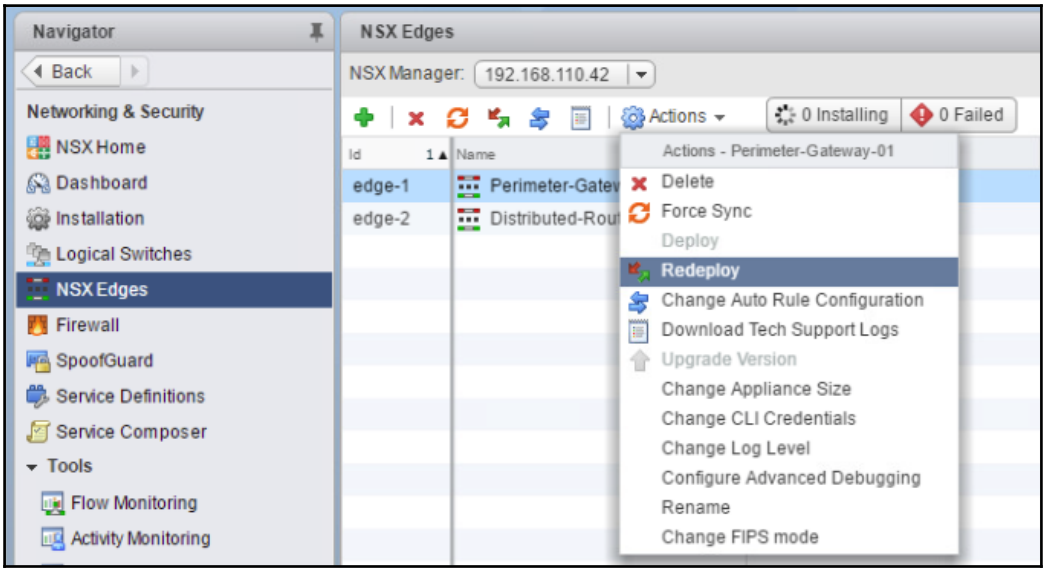

NSX Controller nodes
Actions
Name
Delete
Controller Node
Controller-01
192.168.110.31
controller-1
Controller-02
192.168.110.32
controller-2
Controller-03
192.168.110.33
controller-3

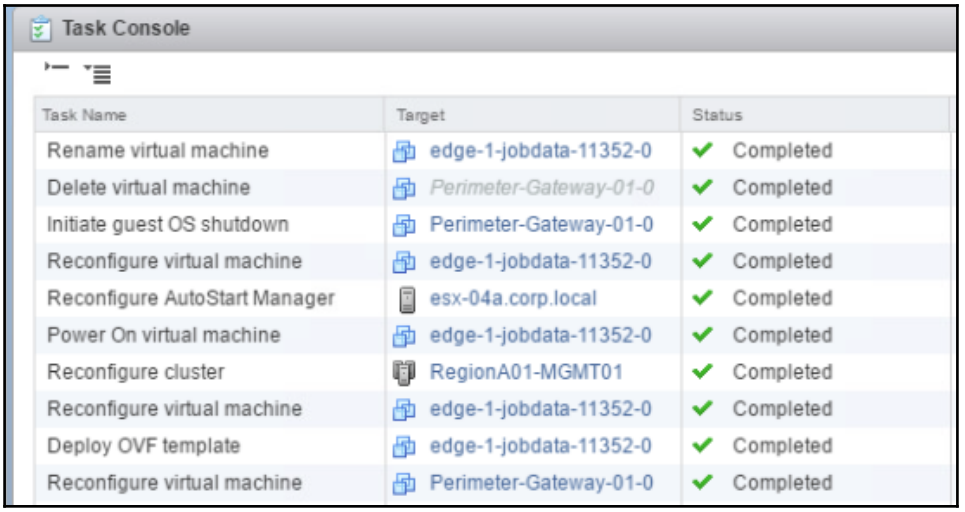

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Installation
Management
Host Preparation
NSX Managers
Actions
Assign Primary Role
Update Controller State

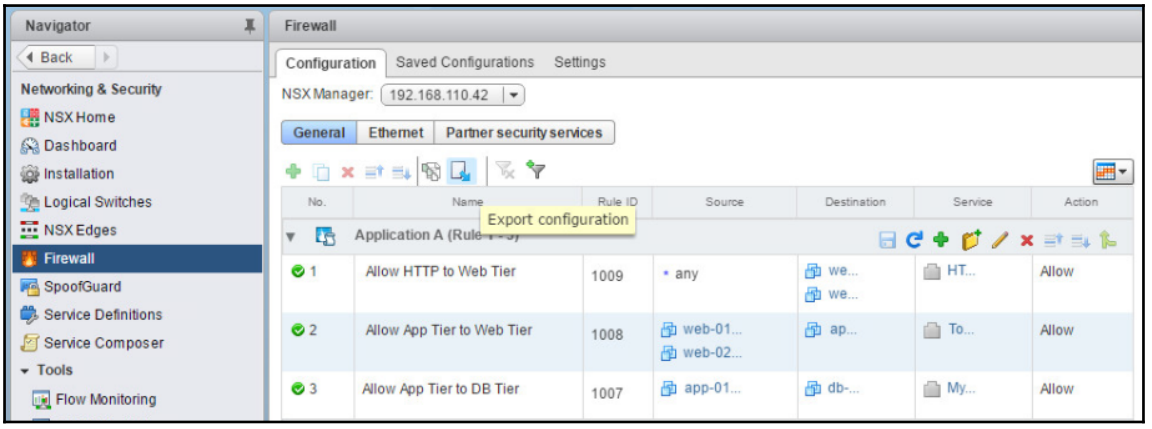

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Tools
Flow Monit
Activity Mon
Endpoint M
Traceflow
Networking &
NSX Manag
Installation
Management
Host Preparation
Logical Network Preparation
NSX Managers
Actions
NSX Manager
IP Address
192.168.110.42
192.168.110.42
NSX Controller nodes
Controller-03 - issues
Resolve
Controller VM cannot be detected in the inventory.
The controller has been temporarily unregistered or deleted from the inventory.
CAUTION: Click resolve only if the controller has
Controller Node
192.168.110.31
controller-1
192.168.110.32
controller-2
192.168.110.33
controller-3
Controller VM deleted

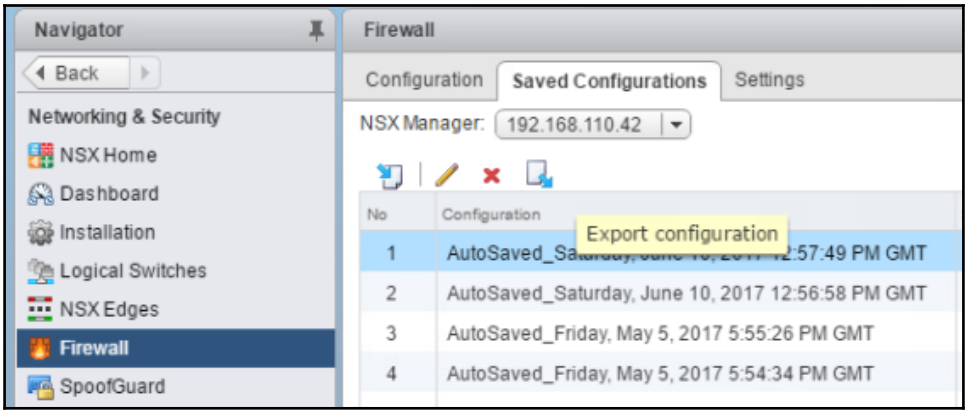

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
Logical Switches
NSX Manager: 192.168.110.42 (Role: Primary)
Filter
Virtual Wire ID
Segment ID
Name
Status
Transport Zone
virtualwire-1
5000
missing-LS
Out of sync
RegionA0-Global-TZ
universalwire-2
10000
RegionA0_Transit
Out of sync
Universal_TZ
universalwire-4
10002
Web_Tier_ULS
Normal
Universal_TZ

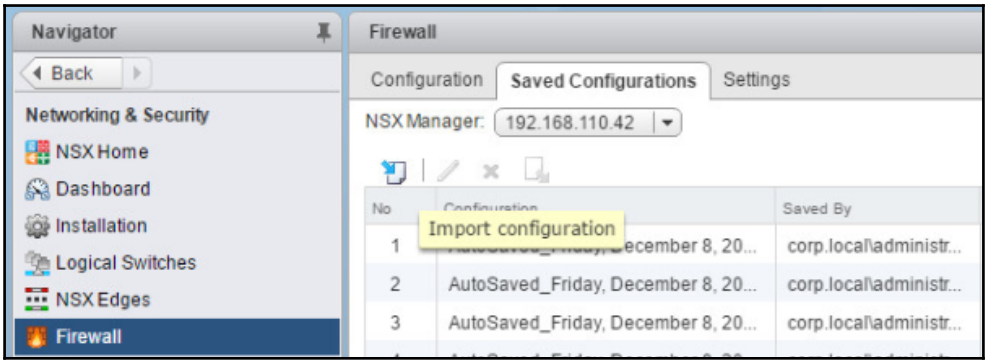

Logical Switches
NSX Manager
missing-LS - issues
Resolve
Backing distributed port group for this logical switch was not found on the vCenter Server.
Click Resolve to create a new distributed port group for this logical switch.
Virtual Wire ID
Status
Out of sync
Out of sync
Normal

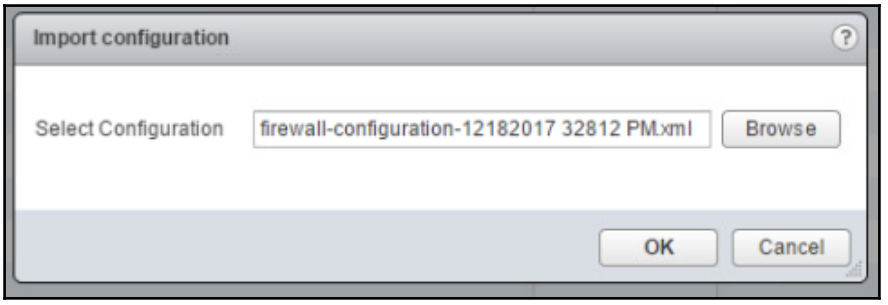

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Tools
Flow Monitoring
Activity Monitoring
NSX Edges
NSX Manager: 192.168.110.42
Actions
0 Installing
0 Failed
Id
Name
edge-1
Perimeter-Gatew
edge-2
Distributed-Rout
Actions - Perimeter-Gateway-01
Delete
Force Sync
Deploy
Redeploy
Change Auto Rule Configuration
Download Tech Support Logs
Upgrade Version
Change Appliance Size
Change CLI Credentials
Change Log Level
Configure Advanced Debugging
Rename
Change FIPS mode

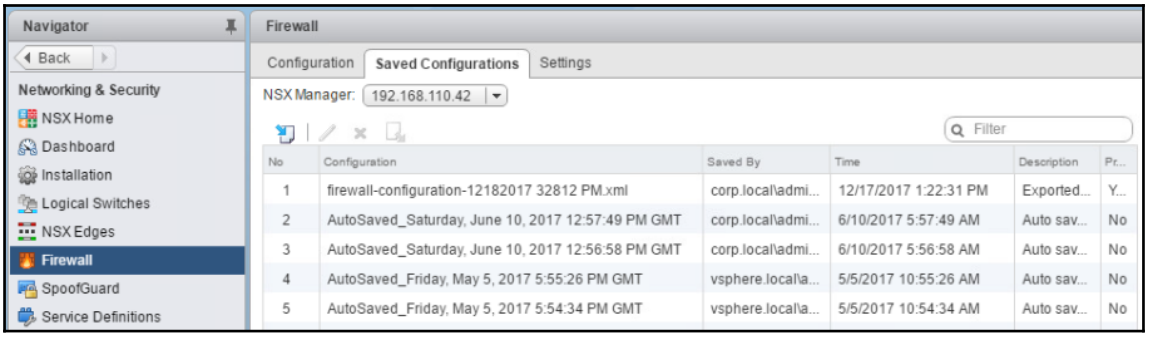

Task Console
Task Name
Target
Status
Rename virtual machine
edge-1-jobdata-11352-0
Completed
Delete virtual machine
Perimeter-Gateway-01-0
Completed
Initiate guest OS shutdown
Perimeter-Gateway-01-0
Completed
Reconfigure virtual machine
edge-1-jobdata-11352-0
Completed
Reconfigure AutoStart Manager
esx-04a.corp.local
Completed
Power On virtual machine
edge-1-jobdata-11352-0
Completed
Reconfigure cluster
RegionA01-MGMT01
Completed
Reconfigure virtual machine
edge-1-jobdata-11352-0
Completed
Deploy OVF template
edge-1-jobdata-11352-0
Completed
Reconfigure virtual machine
Perimeter-Gateway-01-0
Completed

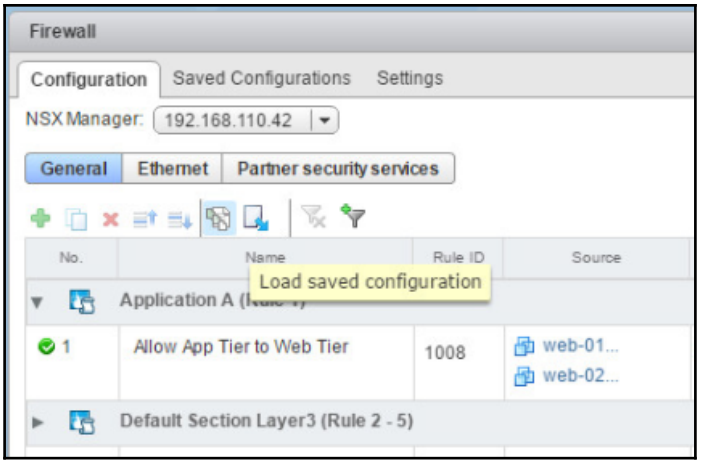

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Tools
Flow Monitoring
Firewall
Configuration
Saved Configurations
Settings
NSX Manager:
192.168.110.42
General
Ethernet
Partner security services
Export configuration
No.
Name
Rule ID
Source
Destination
Service
Action
Application A (Rule
1
Allow HTTP to Web Tier
1009
any
we...
we...
HT...
Allow
2
Allow App Tier to Web Tier
1008
web-01...
web-02...
ap...
To...
Allow
3
Allow App Tier to DB Tier
1007
app-01...
db-...
My...
Allow

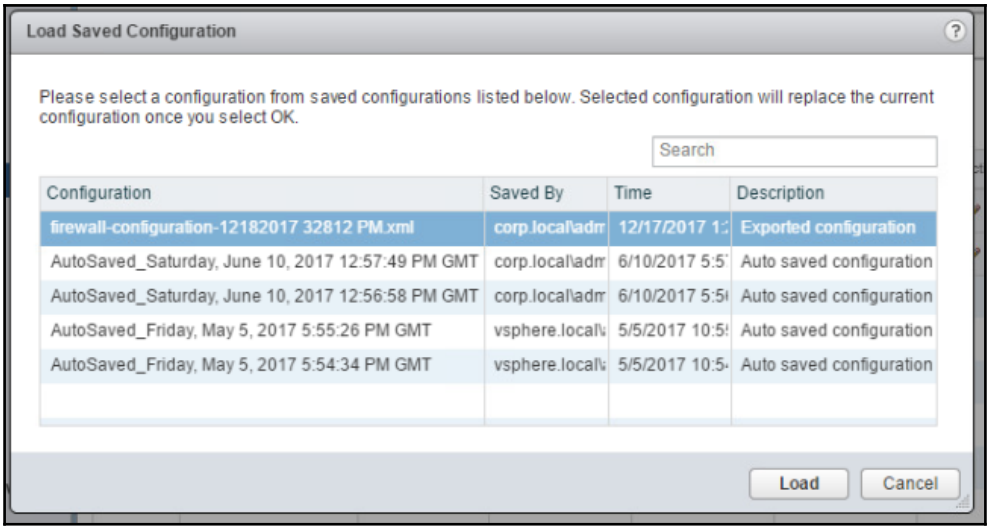

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Firewall
Configuration
Saved Configurations
Settings
NSX Manager:
192.168.110.42
No
Configuration
Export configuration
1
2
AutoSaved_Saturday, June 10, 2017 12:56:58 PM GMT
3
AutoSaved_Friday, May 5, 2017 5:55:26 PM GMT
4
AutoSaved_Friday, May 5, 2017 5:54:34 PM GMT

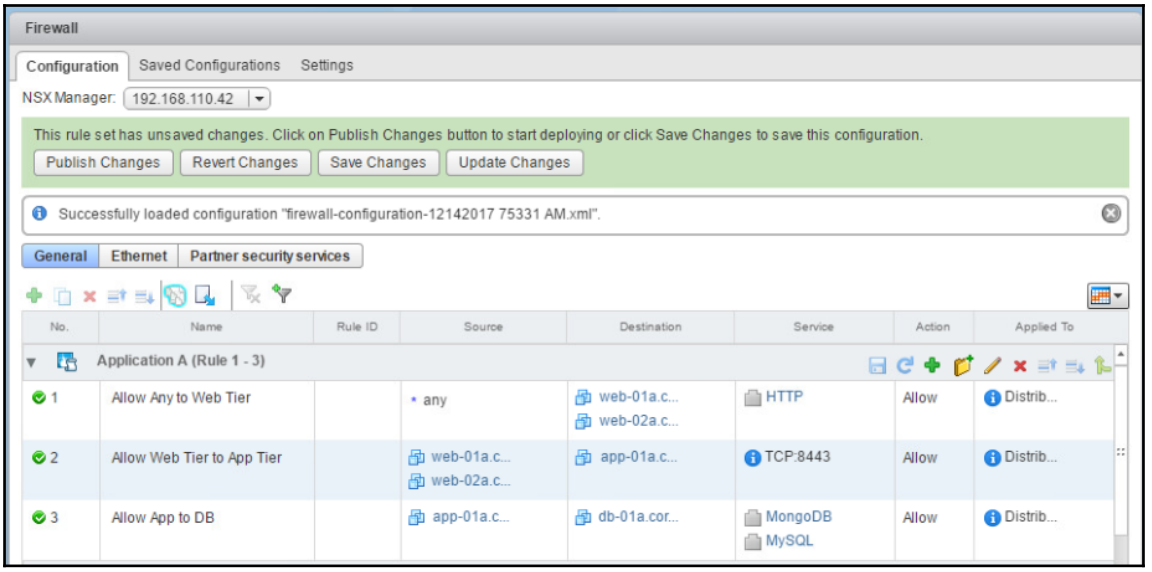

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
Firewall
Configuration
Saved Configurations
Settings
NSX Manager:
192.168.110.42
No
Import configuration
Saved By
2
AutoSaved_Friday, December 8, 20...
corp.local\administr...
3
AutoSaved_Friday, December 8, 20...
corp.local\administr...

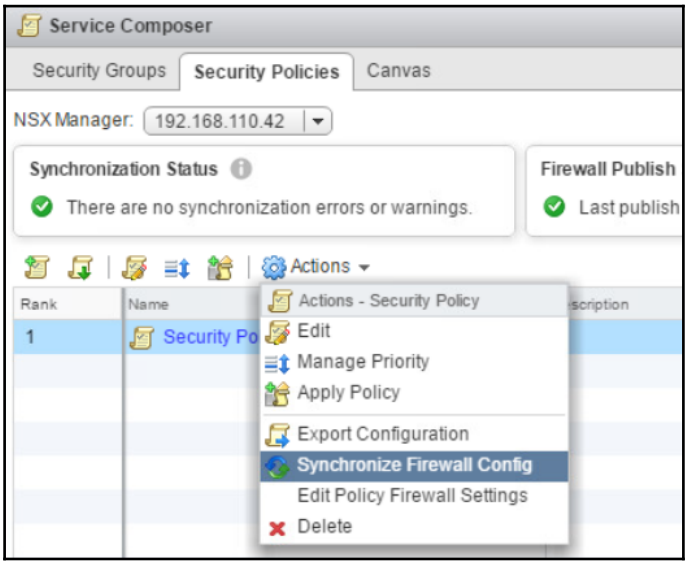

Import configuration
Select Configuration
firewall-configuration-12182017 32812 PM.xml
Browse
OK
Cancel

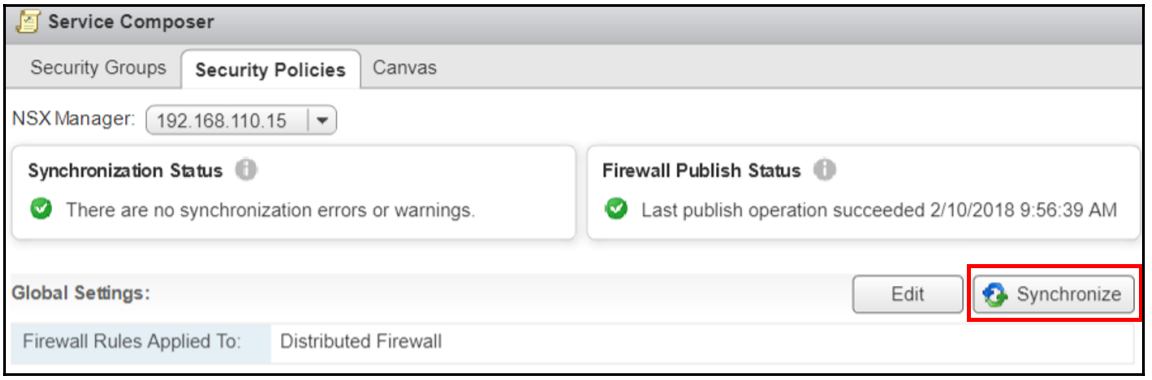

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Firewall
Configuration
Saved Configurations
Settings
NSX Manager: 192.168.110.42
Filter
No
Configuration
Saved By
Time
Description
1 firewall-configuration-12182017 32812 PM.xml corp.local\admi... 12/17/2017 1:22:31 PM Exported...
2 AutoSaved_Saturday, June 10, 2017 12:57:49 PM GMT corp.local\admi... 6/10/2017 5:57:49 AM Auto sav... No
3 AutoSaved_Saturday, June 10, 2017 12:56:58 PM GMT corp.local\admi... 6/10/2017 5:56:58 AM Auto sav... No
4 AutoSaved_Friday, May 5, 2017 5:55:26 PM GMT vsphere.local\a... 5/5/2017 10:55:26 AM Auto sav... No
5 AutoSaved_Friday, May 5, 2017 5:54:34 PM GMT vsphere.local\a... 5/5/2017 10:54:34 AM Auto sav... No

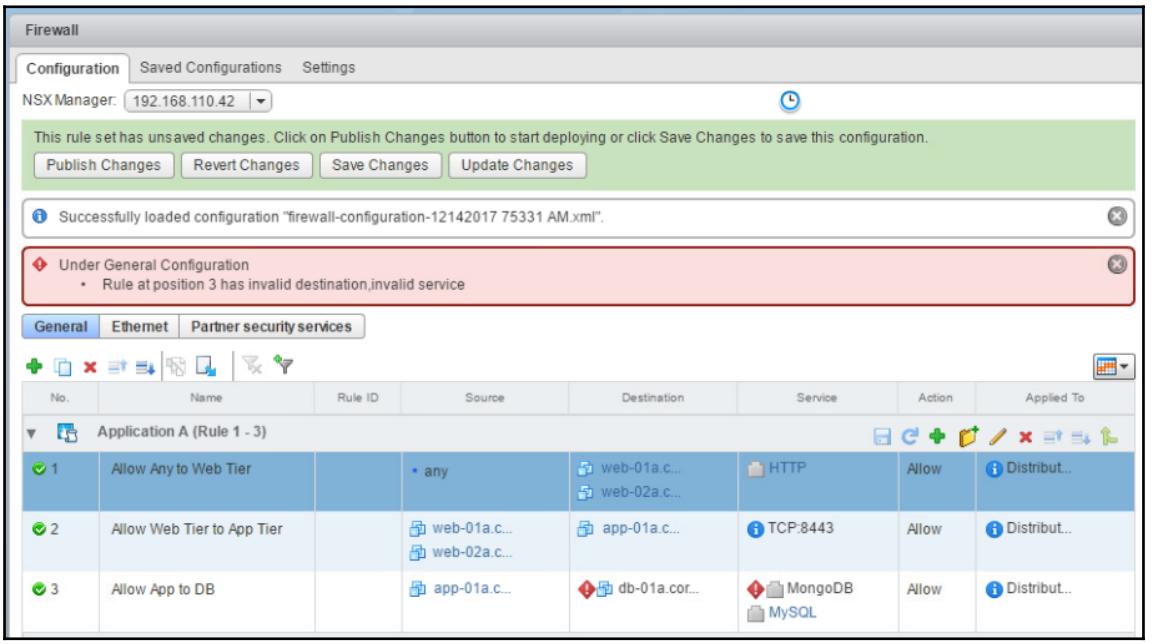

Firewall
Configuration
Saved Configurations
Settings
NSX Manager: 192.168.110.42
General
Ethernet
Partner security services
No.
Name
Rule ID
Source
Load saved configuration
Application A
1
Allow App Tier to Web Tier
1008
web-01...
web-02...
Default Section Layer3 (Rule 2 - 5)

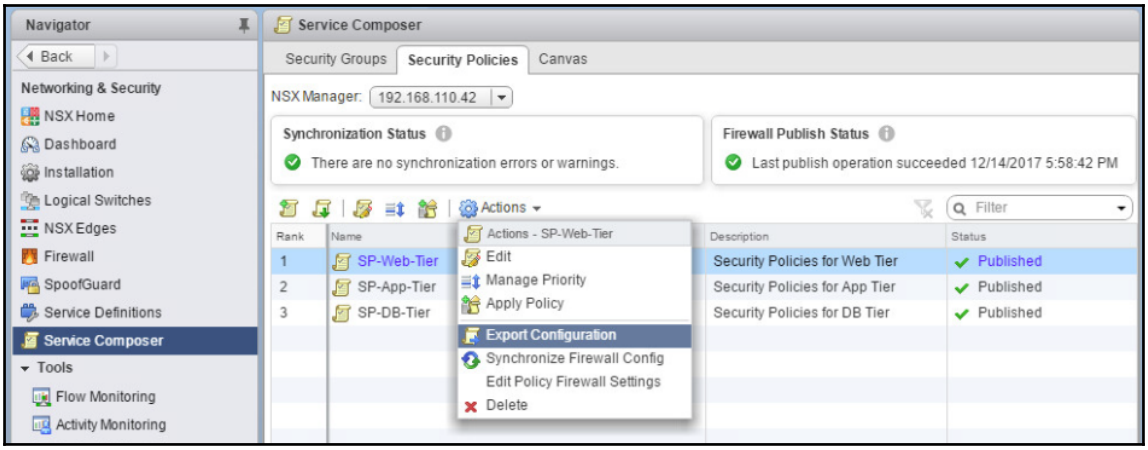

Load Saved Configuration
Please select a configuration from saved configurations listed below. Selected configuration will replace the current configuration once you select OK.
Search
Configuration
Saved By
Time
Description
firewall-configuration-12182017 32812 PM.xml corp.local\adm 12/17/2017 1: Exported configuration
AutoSaved_Saturday, June 10, 2017 12:57:49 PM GMT corp.local\adm 6/10/2017 5:5 Auto saved configuration
AutoSaved_Saturday, June 10, 2017 12:56:58 PM GMT corp.local\adm 6/10/2017 5:5 Auto saved configuration
AutoSaved_Friday, May 5, 2017 5:55:26 PM GMT vsphere.local\ 5/5/2017 10:5 Auto saved configuration
AutoSaved_Friday, May 5, 2017 5:54:34 PM GMT vsphere.local\ 5/5/2017 10:5 Auto saved configuration
Load
Cancel

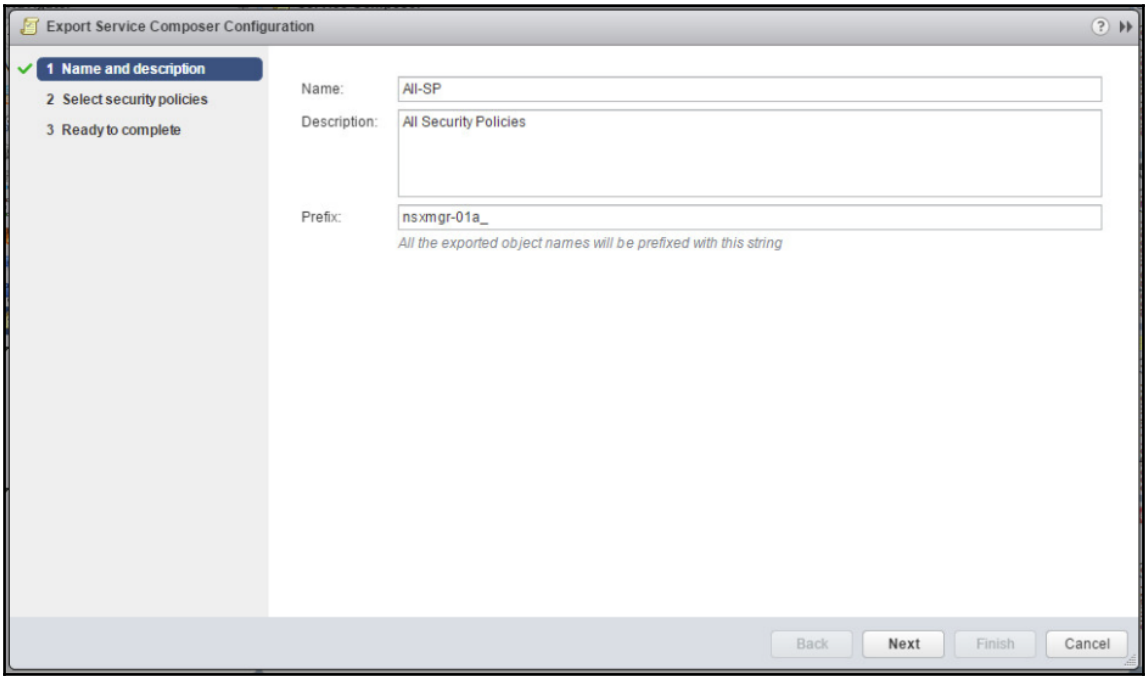

Firewall
Configuration
Saved Configurations
Settings
NSX Manager: 192.168.110.42
This rule set has unsaved changes. Click on Publish Changes button to start deploying or click Save Changes to save this configuration.
Publish Changes
Revert Changes
Save Changes
Update Changes
Successfully loaded configuration "firewall-configuration-12142017 75331 AM.xml".
General
Ethernet
Partner security services
No.
Name
Rule ID
Source
Destination
Service
Action
Applied To
Application A (Rule 1 - 3)
1
Allow Any to Web Tier
any
web-01a.c...
web-02a.c...
HTTP
Allow
Distrib...
2
Allow Web Tier to App Tier
web-01a.c...
web-02a.c...
app-01a.c...
TCP:8443
Allow
Distrib...
3
Allow App to DB
app-01a.c...
db-01a.cor...
MongoDB
MySQL
Allow
Distrib...

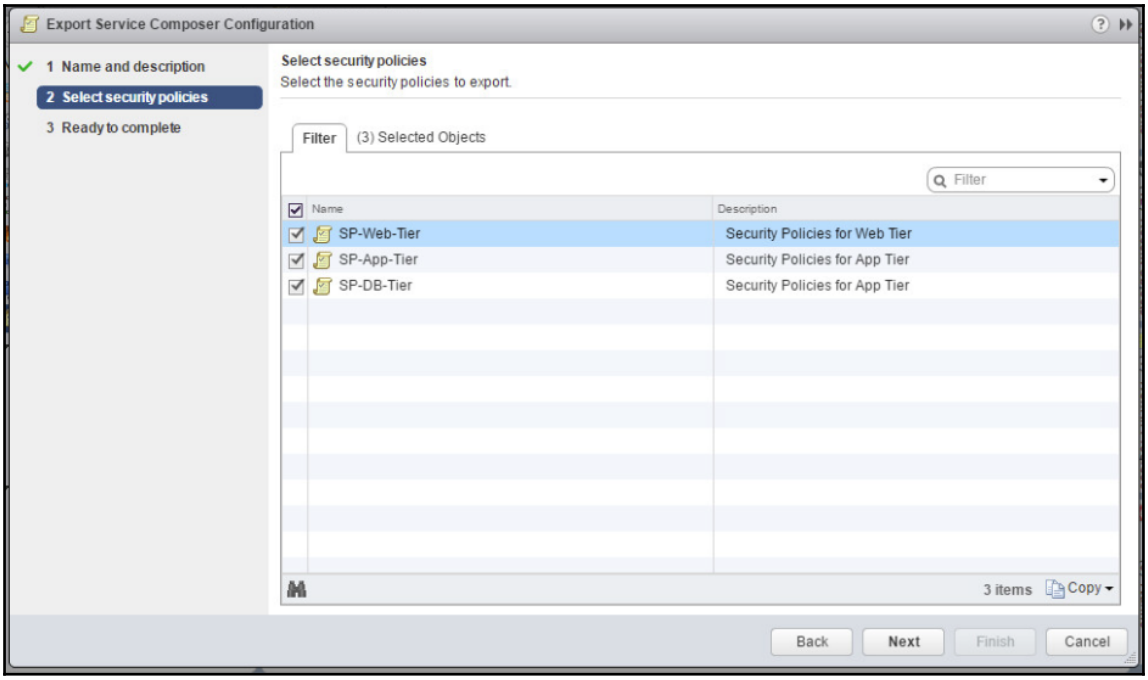

Service Composer
Security Groups
Security Policies
Canvas
NSX Manager: 192.168.110.42
Synchronization Status
There are no synchronization errors or warnings.
Firewall Publish
Last publish
Actions
Rank
Name
1
Security Po
Actions - Security Policy
Edit
Manage Priority
Apply Policy
Export Configuration
Synchronize Firewall Config
Edit Policy Firewall Settings
Delete

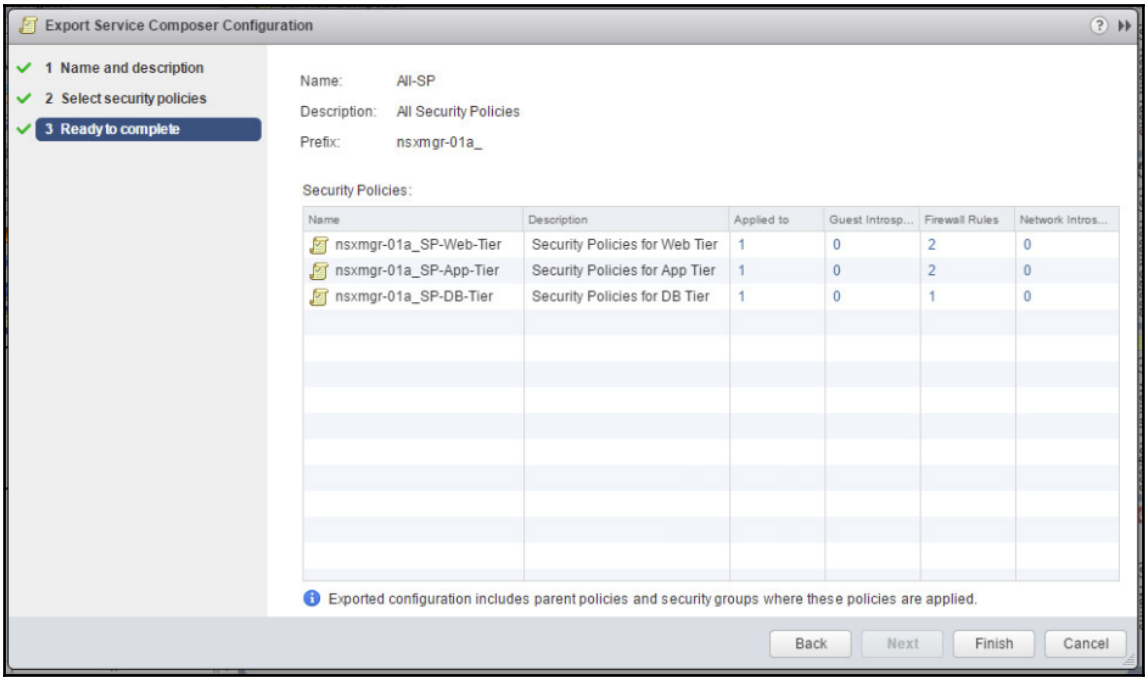

Service Composer
Security Groups
Security Policies
Canvas
NSX Manager: 192.168.110.15
Synchronization Status
There are no synchronization errors or warnings.
Firewall Publish Status
Last publish operation succeeded 2/10/2018 9:56:39 AM
Global Settings:
Edit
Synchronize
Firewall Rules Applied To:
Distributed Firewall

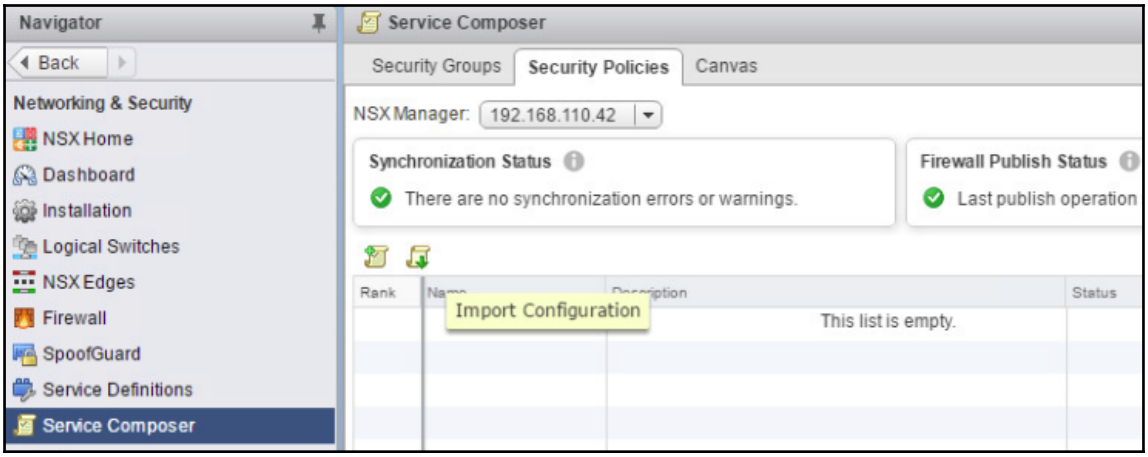

Firewall
Configuration
Saved Configurations
Settings
NSX Manager: 192.168.110.42
This rule set has unsaved changes. Click on Publish Changes button to start deploying or click Save Changes to save this configuration.
Publish Changes
Revert Changes
Save Changes
Update Changes
Successfully loaded configuration "firewall-configuration-12142017 75331 AM.xml".
Under General Configuration
Rule at position 3 has invalid destination,invalid service
General
Ethernet
Partner security services
No.
Name
Rule ID
Source
Destination
Service
Action
Applied To
Application A (Rule 1 - 3)
1
Allow Any to Web Tier
any
web-01a.c...
web-02a.c...
HTTP
Allow
Distribut...
2
Allow Web Tier to App Tier
web-01a.c...
web-02a.c...
app-01a.c...
TCP:8443
Allow
Distribut...
3
Allow App to DB
app-01a.c...
db-01a.cor...
MongoDB
MySQL
Allow
Distribut...

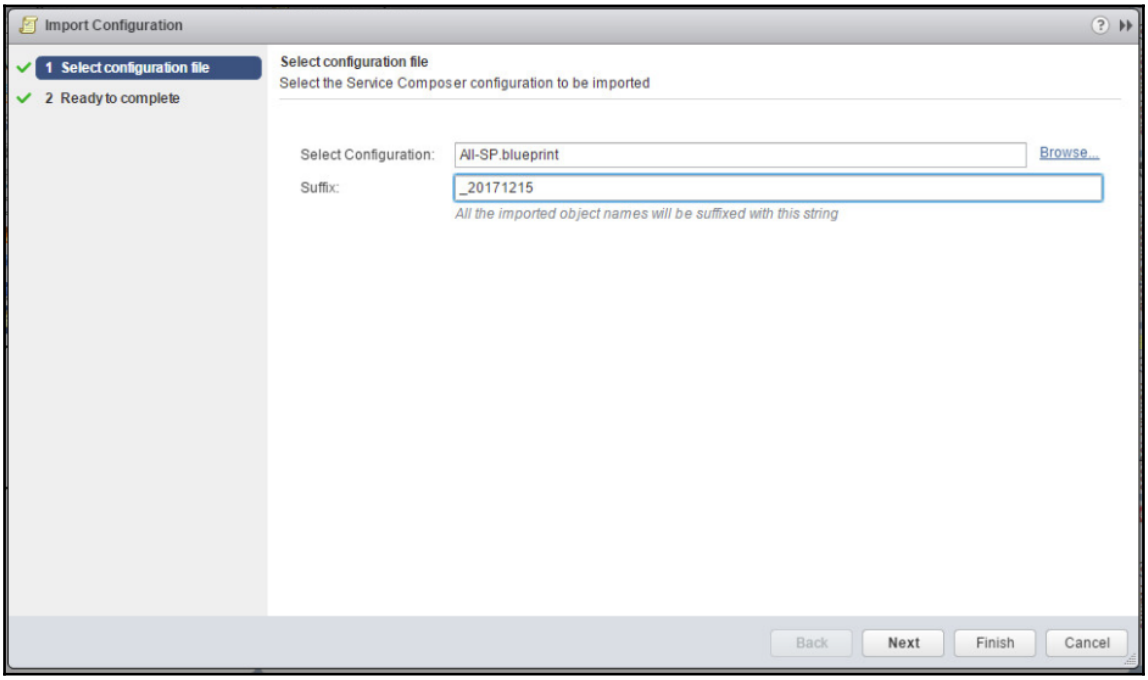

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Tools
Flow Monitoring
Activity Monitoring
Service Composer
Security Groups
Security Policies
Canvas
NSX Manager: 192.168.110.42
Synchronization Status
There are no synchronization errors or warnings.
Firewall Publish Status
Last publish operation succeeded 12/14/2017 5:58:42 PM
Actions
Filter
Rank
Name
Description
Status
1
SP-Web-Tier
Security Policies for Web Tier
Published
2
SP-App-Tier
Security Policies for App Tier
Published
3
SP-DB-Tier
Security Policies for DB Tier
Published
Actions - SP-Web-Tier
Edit
Manage Priority
Apply Policy
Export Configuration
Synchronize Firewall Config
Edit Policy Firewall Settings
Delete

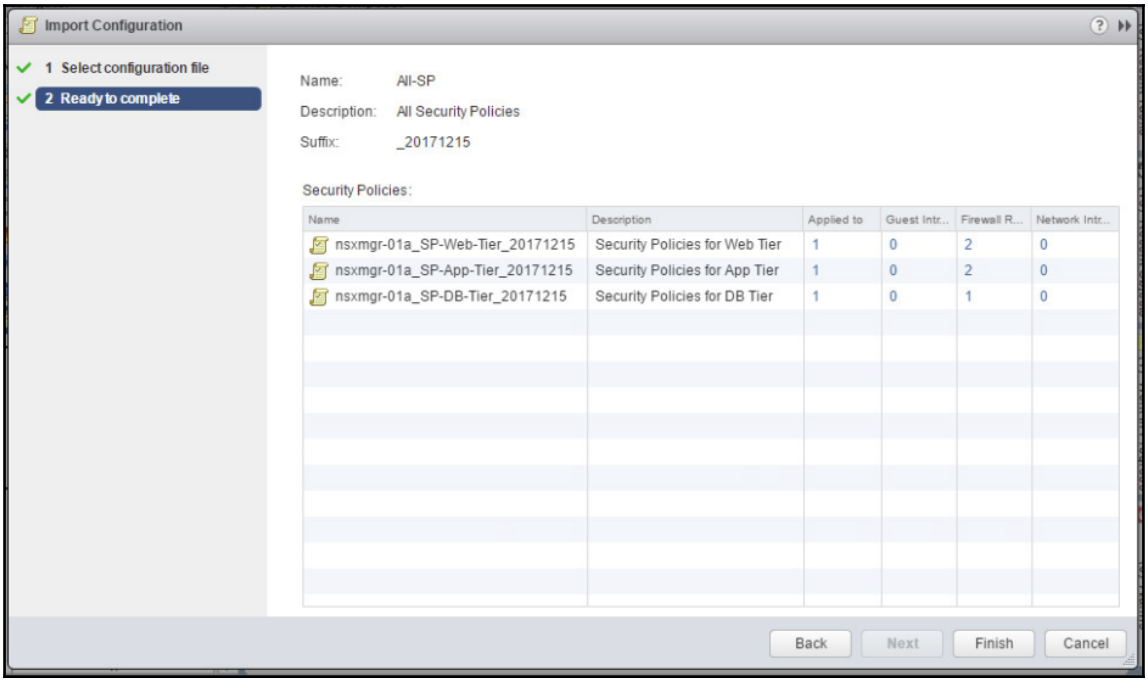

Export Service Composer Configuration
1 Name and description
2 Select security policies
3 Ready to complete
Name:
All-SP
Description:
All Security Policies
Prefix:
nsxmgr-01a_
All the exported object names will be prefixed with this string
Back
Next
Finish
Cancel

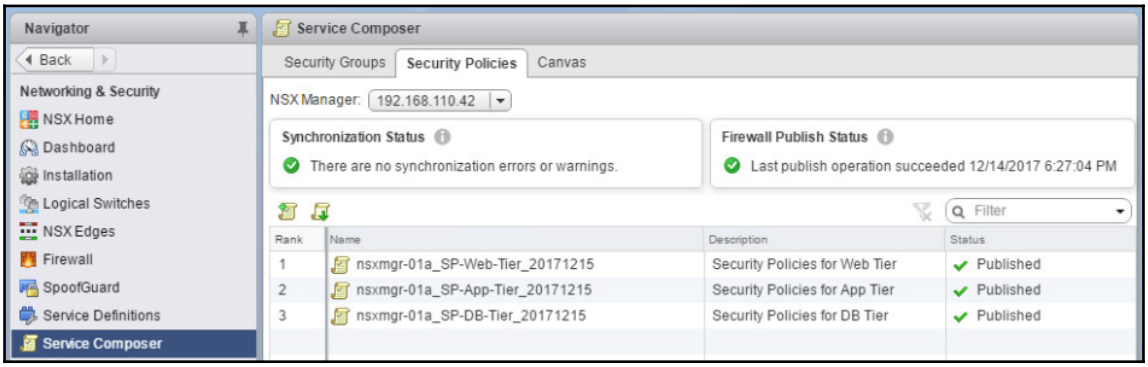

Export Service Composer Configuration
1 Name and description
2 Select security policies
3 Ready to complete
Select security policies
Select the security policies to export.
Filter
(3) Selected Objects
Filter
Name
Description
SP-Web-Tier
Security Policies for Web Tier
SP-App-Tier
Security Policies for App Tier
SP-DB-Tier
Security Policies for App Tier
3 items
Copy
Back
Next
Finish
Cancel

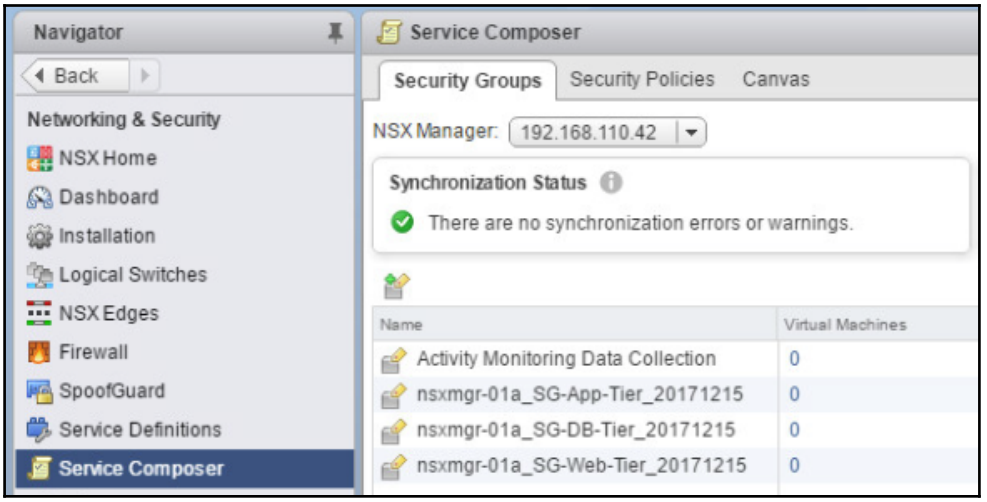

Export Service Composer Configuration
1 Name and description
2 Select security policies
3 Ready to complete
Name: All-SP
Description: All Security Policies
Prefix: nsxmgr-01a_
Security Policies:
Name
Description
Applied to
Guest Introsp...
Firewall Rules
Network Intros...
nsxmgr-01a_SP-Web-Tier
Security Policies for Web Tier
1
0
2
0
nsxmgr-01a_SP-App-Tier
Security Policies for App Tier
1
0
2
0
nsxmgr-01a_SP-DB-Tier
Security Policies for DB Tier
1
0
1
0
Exported configuration includes parent policies and security groups where these policies are applied.
Back
Next
Finish
Cancel


Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Service Composer
Security Groups
Security Policies
Canvas
NSX Manager:
192.168.110.42
Synchronization Status
There are no synchronization errors or warnings.
Firewall Publish Status
Last publish operation
Rank
Name
Description
Status
Import Configuration
This list is empty.

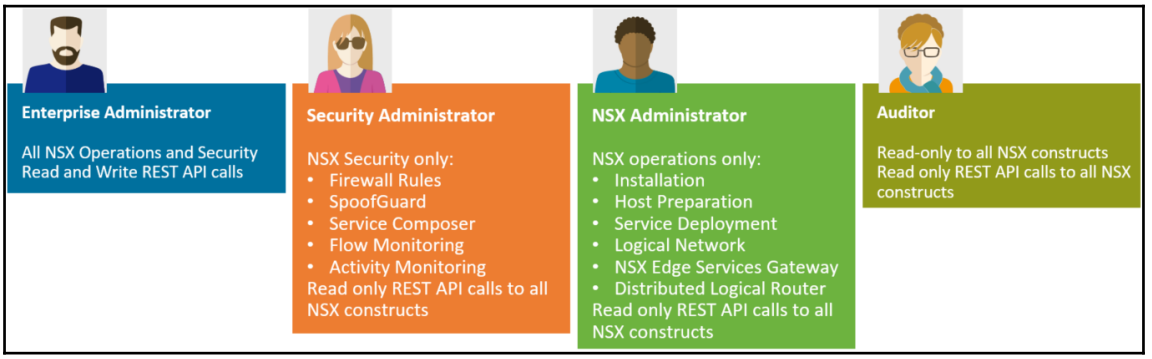

Import Configuration
1 Select configuration file
2 Ready to complete
Select configuration file
Select the Service Composer configuration to be imported
Select Configuration:
All-SP.blueprint
Browse...
Suffix:
_20171215
All the imported object names will be suffixed with this string
Back
Next
Finish
Cancel

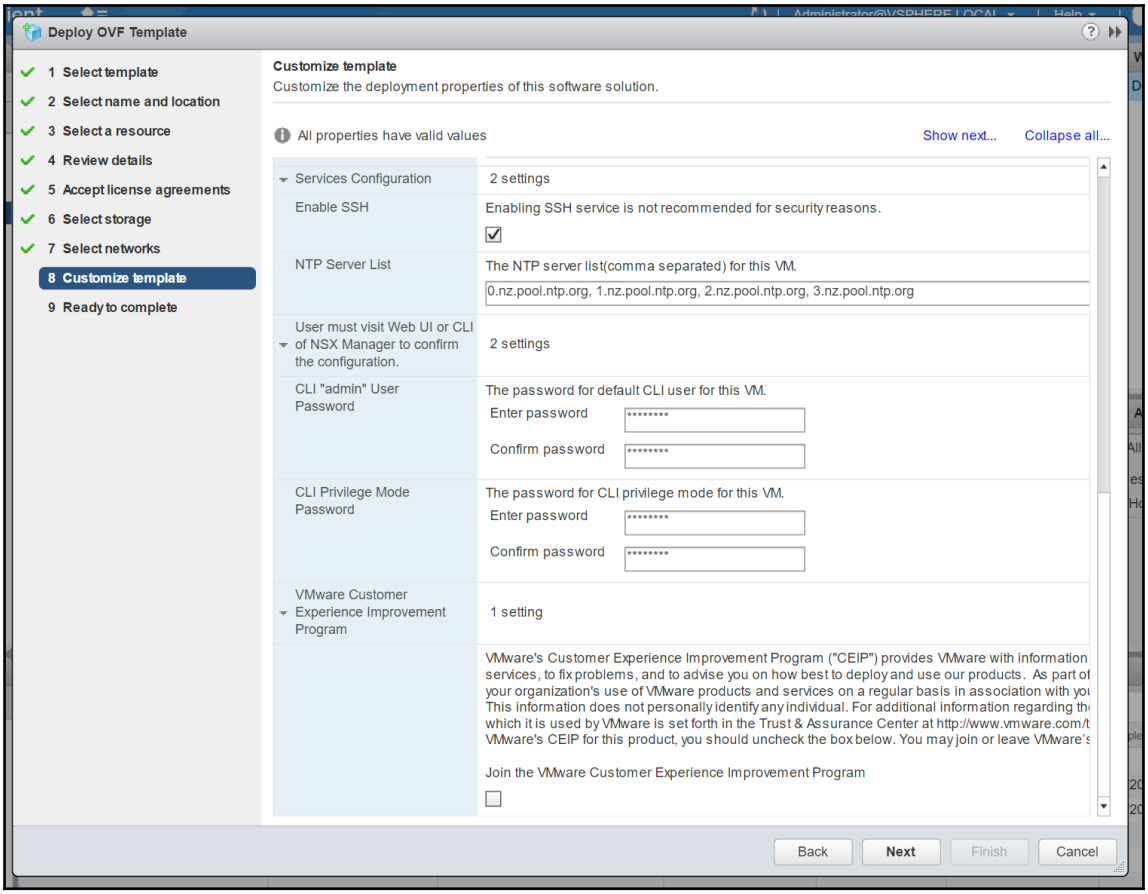

Import Configuration
1 Select configuration file
2 Ready to complete
Name: All-SP
Description: All Security Policies
Suffix: _20171215
Security Policies:
Name
Description
Applied to
Guest Intr...
Firewall R...
Network Intr...
nsxmgr-01a_SP-Web-Tier_20171215
Security Policies for Web Tier
1
0
2
0
nsxmgr-01a_SP-App-Tier_20171215
Security Policies for App Tier
1
0
2
0
nsxmgr-01a_SP-DB-Tier_20171215
Security Policies for DB Tier
1
0
1
0
Back
Next
Finish
Cancel

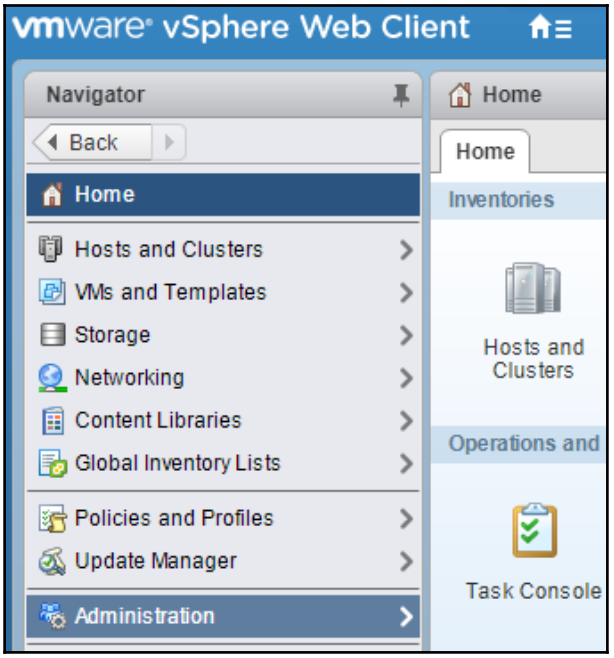

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Service Composer
Security Groups
Security Policies
Canvas
NSX Manager: 192.168.110.42
Synchronization Status
There are no synchronization errors or warnings.
Firewall Publish Status
Last publish operation succeeded 12/14/2017 6:27:04 PM
Filter
Rank
Name
Description
Status
1
nsxmgr-01a_SP-Web-Tier_20171215
Security Policies for Web Tier
Published
2
nsxmgr-01a_SP-App-Tier_20171215
Security Policies for App Tier
Published
3
nsxmgr-01a_SP-DB-Tier_20171215
Security Policies for DB Tier
Published

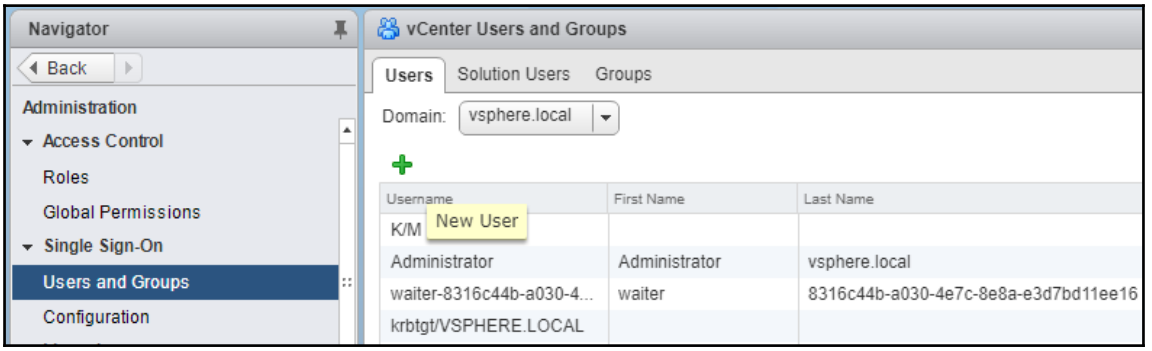

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Service Composer
Security Groups
Security Policies
Canvas
NSX Manager:
192.168.110.42
Synchronization Status
There are no synchronization errors or warnings.
Name
Virtual Machines
Activity Monitoring Data Collection
0
nsxmgr-01a_SG-App-Tier_20171215
0
nsxmgr-01a_SG-DB-Tier_20171215
0
nsxmgr-01a_SG-Web-Tier_20171215
0

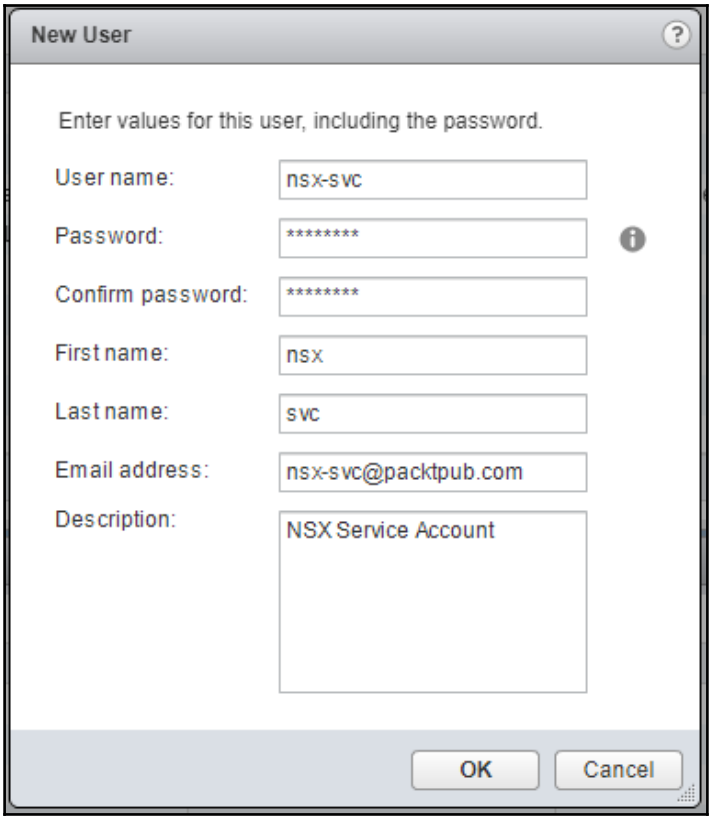
Chapter 09: Managing User Accounts in VMware NSX

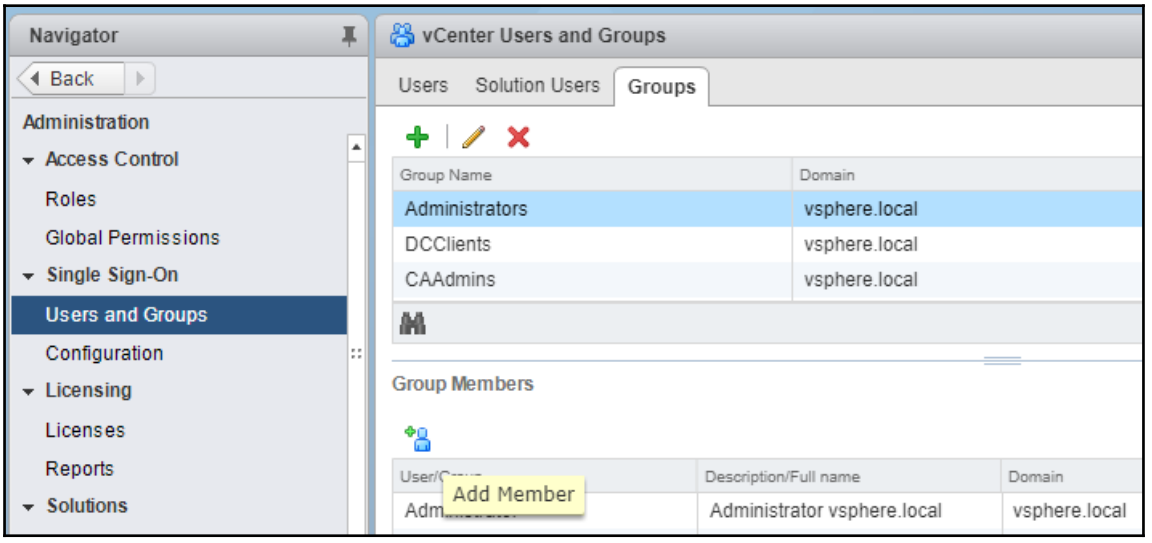


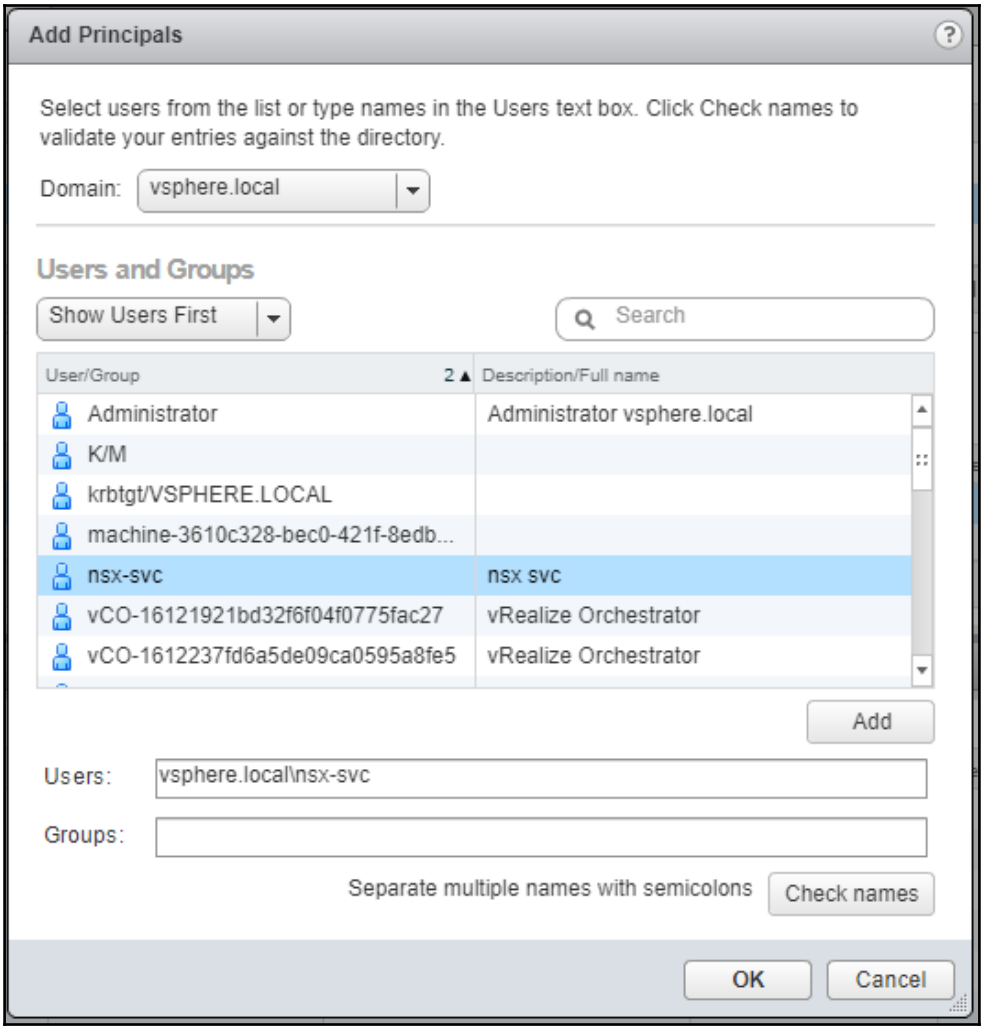

Deploy OVF Template
1 Select template
2 Select name and location
3 Select a resource
4 Review details
5 Accept license agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete
Customize template
Customize the deployment properties of this software solution.
All properties have valid values
Show next...
Collapse all...
Services Configuration
2 settings
Enable SSH
Enabling SSH service is not recommended for security reasons.
NTP Server List
The NTP server list(comma separated) for this VM.
0.nz.pool.ntp.org, 1.nz.pool.ntp.org, 2.nz.pool.ntp.org, 3.nz.pool.ntp.org
User must visit Web UI or CLI of NSX Manager to confirm the configuration.
2 settings
CLI "admin" User Password
The password for default CLI user for this VM.
Enter password
Confirm password
CLI Privilege Mode Password
The password for CLI privilege mode for this VM.
Enter password
Confirm password
VMware Customer Experience Improvement Program
1 setting
VMware's Customer Experience Improvement Program ("CEIP") provides VMware with information
services, to fix problems, and to advise you on how best to deploy and use our products. As part of
your organization's use of VMware products and services on a regular basis in association with you
This information does not personally identify any individual. For additional information regarding th
which it is used by VMware is set forth in the Trust & Assurance Center at http://www.vmware.com/t
VMware's CEIP for this product, you should uncheck the box below. You may join or leave VMware's
Join the VMware Customer Experience Improvement Program
Back
Next
Finish
Cancel

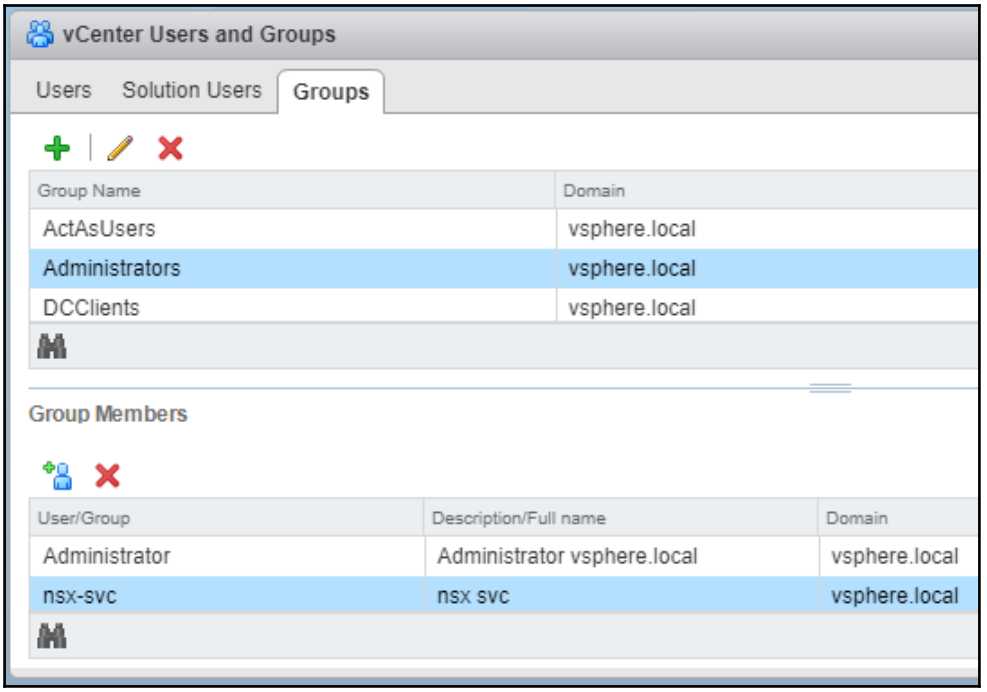

vmware vSphere Web Client
Navigator
Back
Home
Hosts and Clusters
VMs and Templates
Storage
Networking
Content Libraries
Global Inventory Lists
Policies and Profiles
Update Manager
Administration
Home
Home
Inventories
Hosts and Clusters
Operations and
Task Console

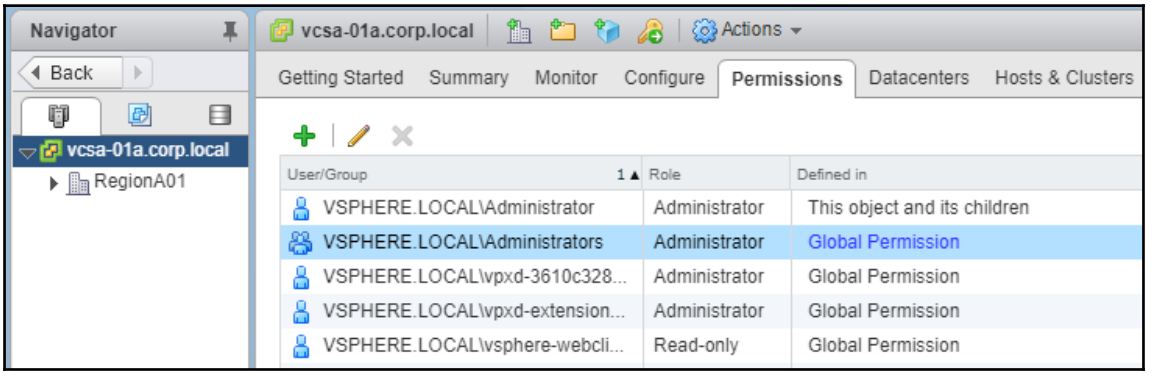

Navigator
Back
Administration
Access Control
Roles
Global Permissions
Single Sign-On
Users and Groups
Configuration
vCenter Users and Groups
Users
Solution Users
Groups
Domain:
vsphere.local
Username
First Name
Last Name
K/M
New User
Administrator
Administrator
vsphere.local
waiter-8316c44b-a030-4...
waiter
8316c44b-a030-4e7c-8e8a-e3d7bd11ee16
krbtgt/VSPHERE.LOCAL

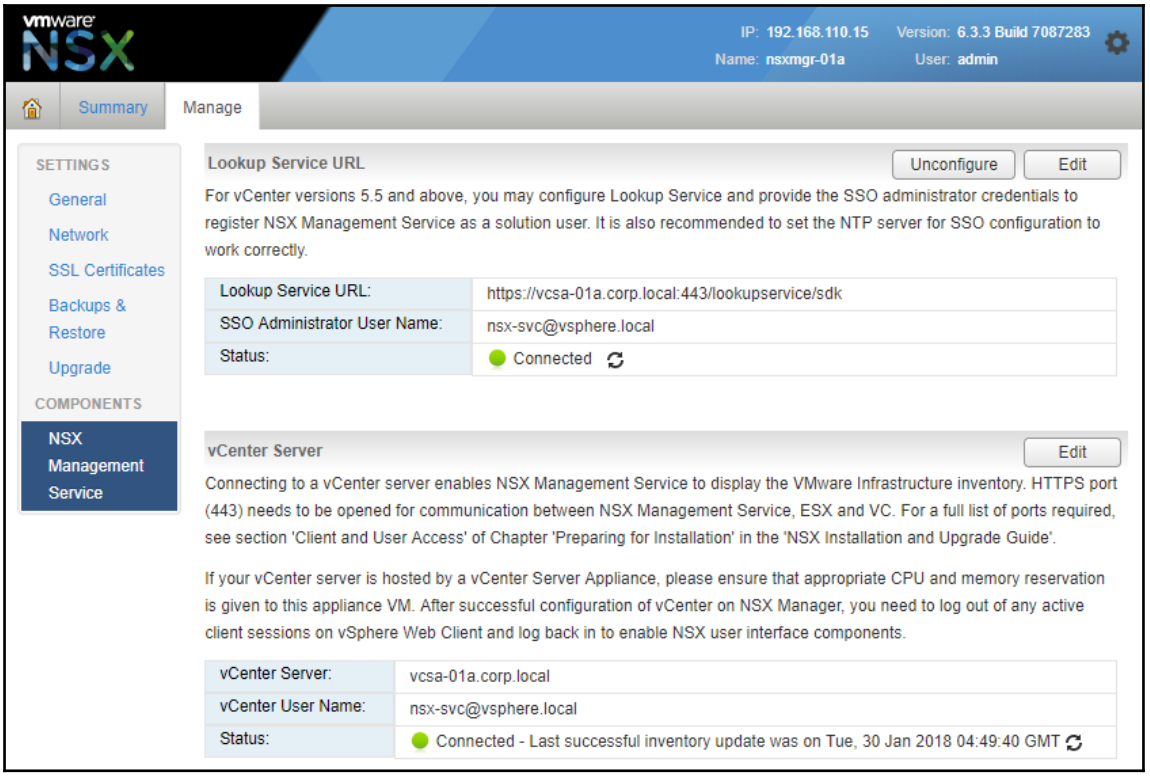

New User
Enter values for this user, including the password.
User name:
nsx-svc
Password:
****
Confirm password:
****
First name:
nsx
Last name:
svc
Email address:
nsx-svc@packtpub.com
Description:
NSX Service Account
OK
Cancel

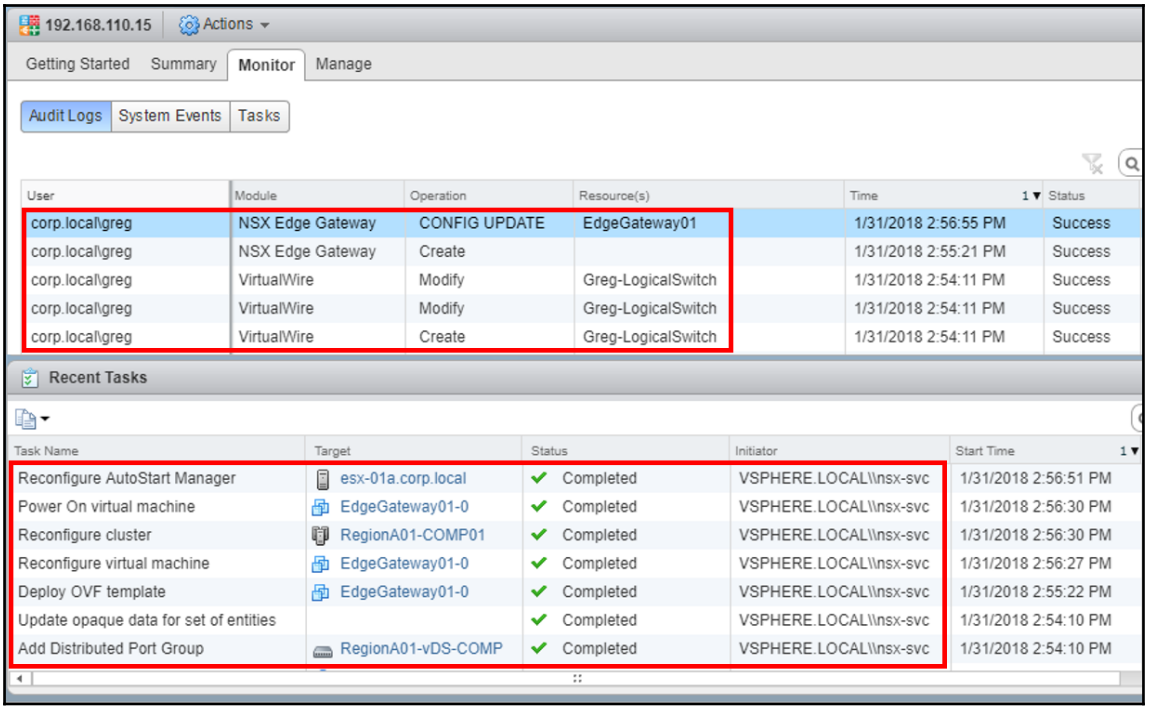

Navigator
Back
Administration
Access Control
Roles
Global Permissions
Single Sign-On
Users and Groups
Configuration
Licensing
Licenses
Reports
Solutions
vCenter Users and Groups
Users
Solution Users
Groups
Group Name
Domain
Administrators
vsphere.local
DCClients
vsphere.local
CAAdmins
vsphere.local
Group Members
Add Member
Description/Full name
Domain
Administrator vsphere.local
vsphere.local

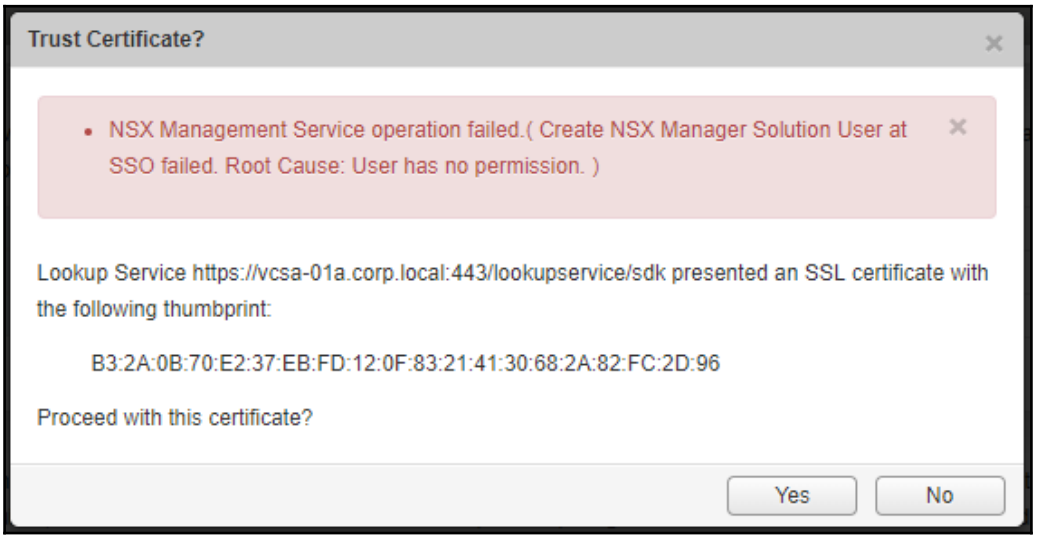

Add Principals
Select users from the list or type names in the Users text box. Click Check names to validate your entries against the directory.
Domain: vsphere.local
Users and Groups
Show Users First
Search
User/Group
2
Description/Full name
Administrator
Administrator vsphere.local
K/M
krbtgt/VSPHERE.LOCAL
machine-3610c328-bec0-421f-8edb...
nsx-svc
nsx svc
vCO-16121921bd32f6f04f0775fac27
vRealize Orchestrator
vCO-1612237fd6a5de09ca0595a8fe5
vRealize Orchestrator
Add
Users:
vsphere.local\nsx-svc
Groups:
Separate multiple names with semicolons
Check names
OK
Cancel

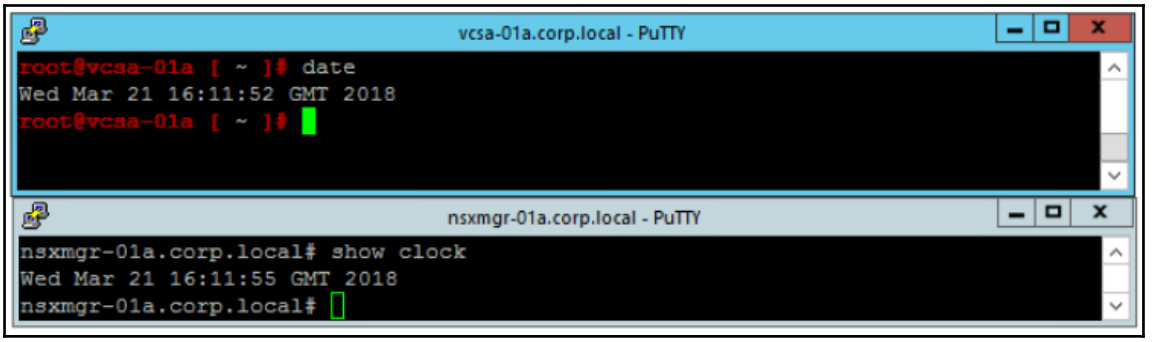

vCenter Users and Groups
Users
Solution Users
Groups
Group Name
Domain
ActAsUsers
vsphere.local
Administrators
vsphere.local
DCClients
vsphere.local
Group Members
User/Group
Description/Full name
Domain
Administrator
Administrator vsphere.local
vsphere.local
nsx-svc
nsx svc
vsphere.local

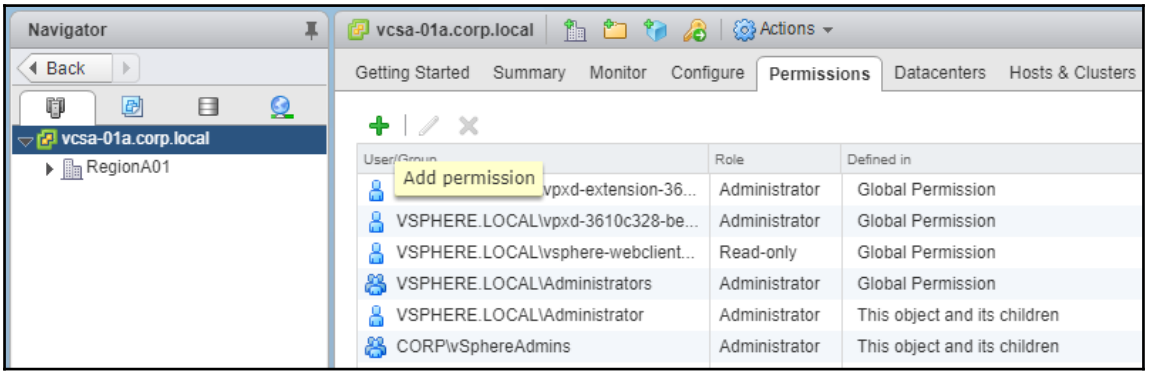

Navigator
Back
vcsa-01a.corp.local
RegionA01
vcsa-01a.corp.local
Actions
Getting Started
Summary
Monitor
Configure
Permissions
Datacenters
Hosts & Clusters
User/Group
Role
Defined in
VSPHERE.LOCAL\Administrator
Administrator
This object and its children
VSPHERE.LOCAL\Administrators
Administrator
Global Permission
VSPHERE.LOCAL\vpxd-3610c328...
Administrator
Global Permission
VSPHERE.LOCAL\vpxd-extension...
Administrator
Global Permission
VSPHERE.LOCAL\vsphere-webcli...
Read-only
Global Permission

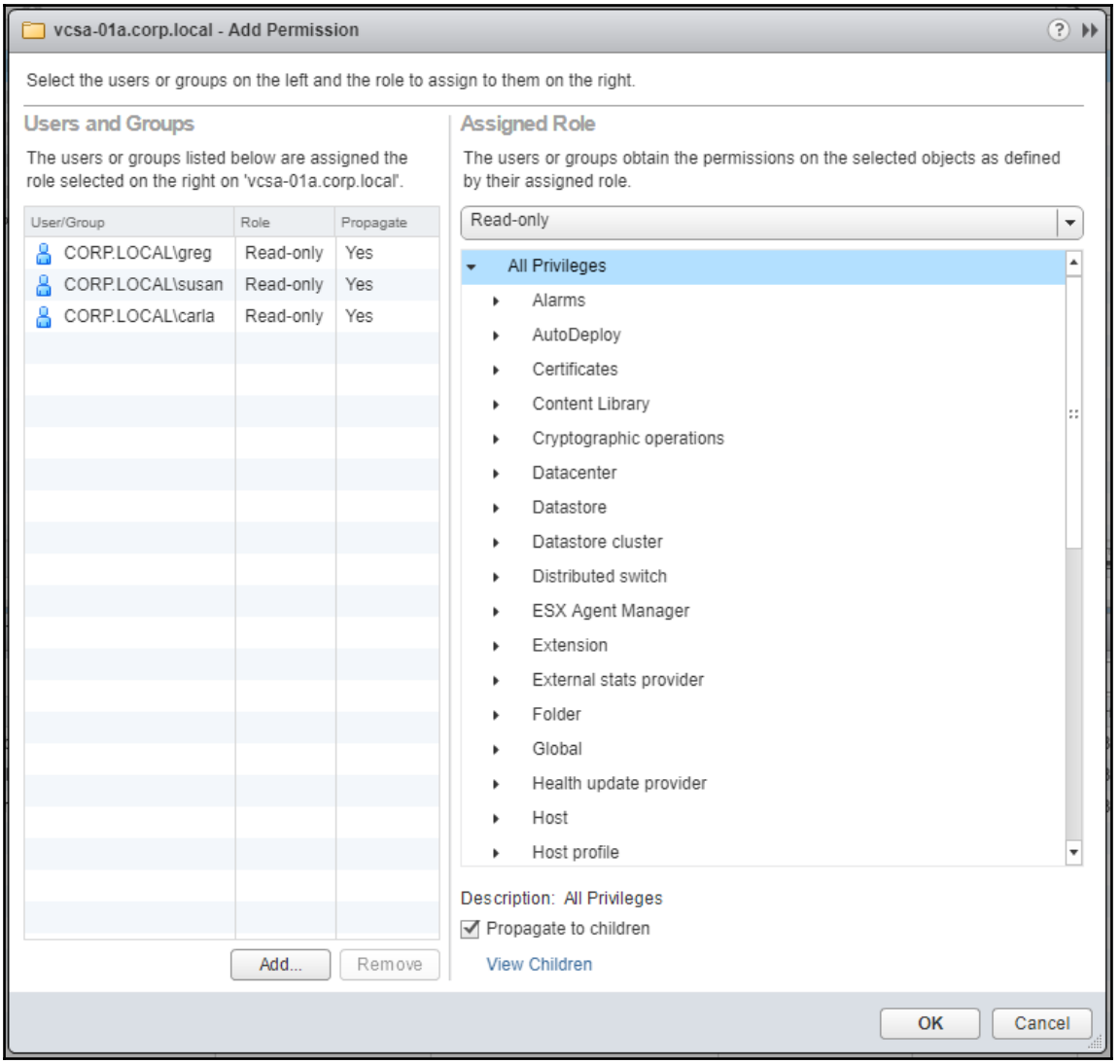

vmware NSX
IP: 192.168.110.15
Version: 6.3.3 Build 7087283
Name: nsxmgr-01a
User: admin
Summary
Manage
SETTINGS
General
Network
SSL Certificates
Backups & Restore
Upgrade
COMPONENTS
NSX Management Service
Lookup Service URL
Unconfigure
Edit
For vCenter versions 5.5 and above, you may configure Lookup Service and provide the SSO administrator credentials to register NSX Management Service as a solution user. It is also recommended to set the NTP server for SSO configuration to work correctly.
Lookup Service URL: https://vcsa-01a.corp.local:443/lookupservice/sdk
SSO Administrator User Name: nsx-svc@vsphere.local
Status: Connected
vCenter Server
Edit
Connecting to a vCenter server enables NSX Management Service to display the VMware Infrastructure inventory. HTTPS port (443) needs to be opened for communication between NSX Management Service, ESX and VC. For a full list of ports required, see section 'Client and User Access' of Chapter 'Preparing for Installation' in the 'NSX Installation and Upgrade Guide'.
If your vCenter server is hosted by a vCenter Server Appliance, please ensure that appropriate CPU and memory reservation is given to this appliance VM. After successful configuration of vCenter on NSX Manager, you need to log out of any active client sessions on vSphere Web Client and log back in to enable NSX user interface components.
vCenter Server: vcsa-01a.corp.local
vCenter User Name: nsx-svc@vsphere.local
Status: Connected - Last successful inventory update was on Tue, 30 Jan 2018 04:49:40 GMT

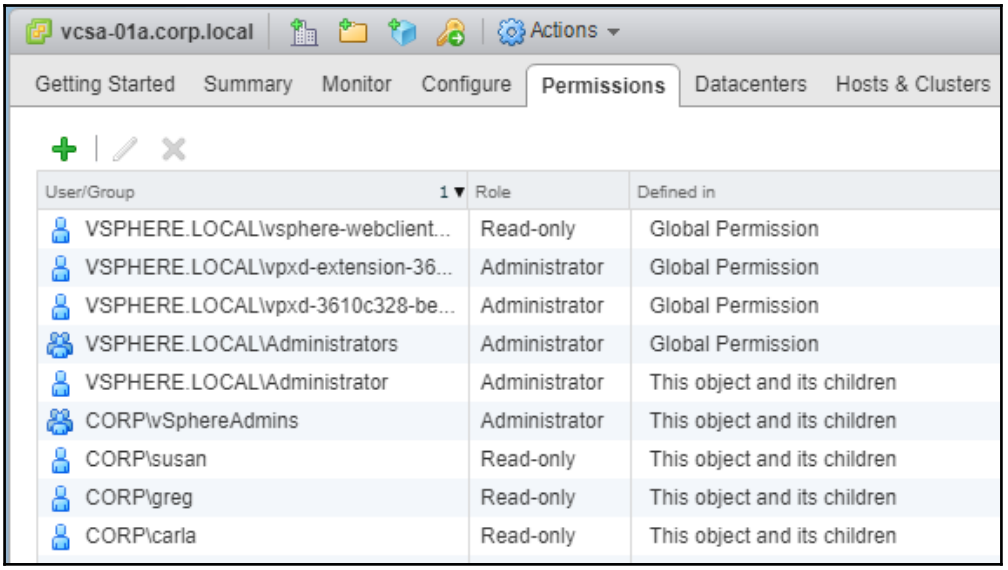

192.168.110.15
Actions
Getting Started
Summary
Monitor
Manage
Audit Logs
System Events
Tasks
User
Module
Operation
Resource(s)
Time
Status
corp.local\greg
NSX Edge Gateway
CONFIG UPDATE
EdgeGateway01
1/31/2018 2:56:55 PM
Success
corp.local\greg
NSX Edge Gateway
Create
1/31/2018 2:55:21 PM
Success
corp.local\greg
VirtualWire
Modify
Greg-LogicalSwitch
1/31/2018 2:54:11 PM
Success
corp.local\greg
VirtualWire
Modify
Greg-LogicalSwitch
1/31/2018 2:54:11 PM
Success
corp.local\greg
VirtualWire
Create
Greg-LogicalSwitch
1/31/2018 2:54:11 PM
Success
Recent Tasks
Task Name
Target
Status
Initiator
Start Time
Reconfigure AutoStart Manager
esx-01a.corp.local
Completed
VSPHERE.LOCAL\\nsx-svc
1/31/2018 2:56:51 PM
Power On virtual machine
EdgeGateway01-0
Completed
VSPHERE.LOCAL\\nsx-svc
1/31/2018 2:56:30 PM
Reconfigure cluster
RegionA01-COMP01
Completed
VSPHERE.LOCAL\\nsx-svc
1/31/2018 2:56:30 PM
Reconfigure virtual machine
EdgeGateway01-0
Completed
VSPHERE.LOCAL\\nsx-svc
1/31/2018 2:56:27 PM
Deploy OVF template
EdgeGateway01-0
Completed
VSPHERE.LOCAL\\nsx-svc
1/31/2018 2:55:22 PM
Update opaque data for set of entities
Completed
VSPHERE.LOCAL\\nsx-svc
1/31/2018 2:54:10 PM
Add Distributed Port Group
RegionA01-vDS-COMP
Completed
VSPHERE.LOCAL\\nsx-svc
1/31/2018 2:54:10 PM

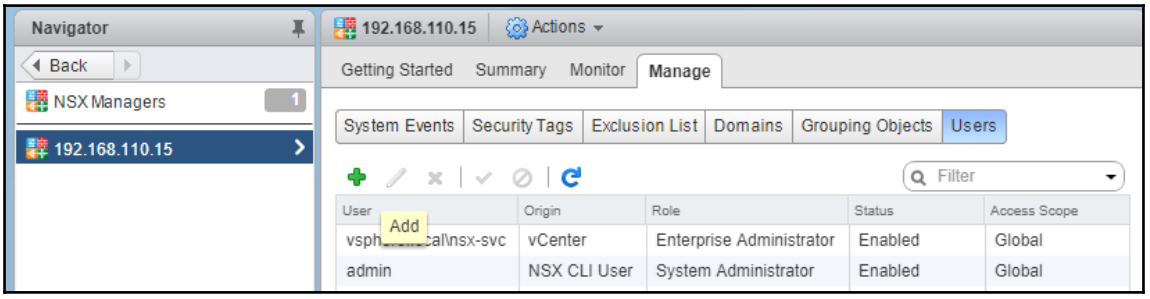

Trust Certificate?
NSX Management Service operation failed.(Create NSX Manager Solution User at SSO failed. Root Cause: User has no permission.)
Lookup Service https://vcsa-01a.corp.local:443/lookupservice/sdk presented an SSL certificate with the following thumbprint:
B3:2A:0B:70:E2:37:EB:FD:12:0F:83:21:41:30:68:2A:82:FC:2D:96
Proceed with this certificate?
Yes
No

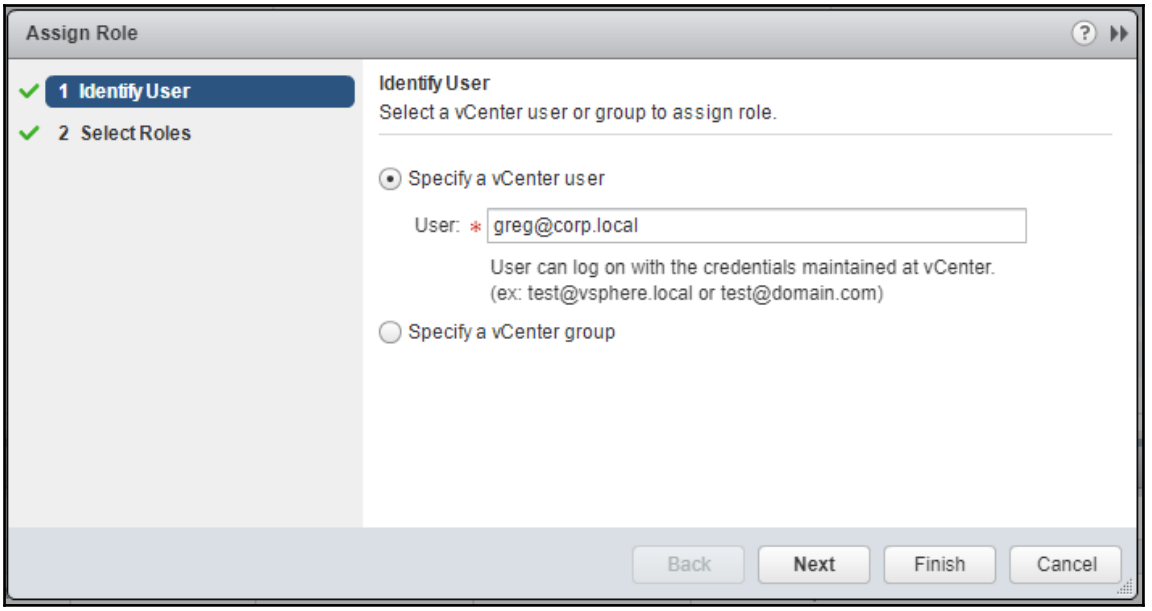

vcsa-01a.corp.local - PuTTY
root@vcsa-01a [~]# date
Wed Mar 21 16:11:52 GMT 2018
root@vcsa-01a [~]#
nsxmgr-01a.corp.local - PuTTY
nsxmgr-01a.corp.local# show clock
Wed Mar 21 16:11:55 GMT 2018
nsxmgr-01a.corp.local#

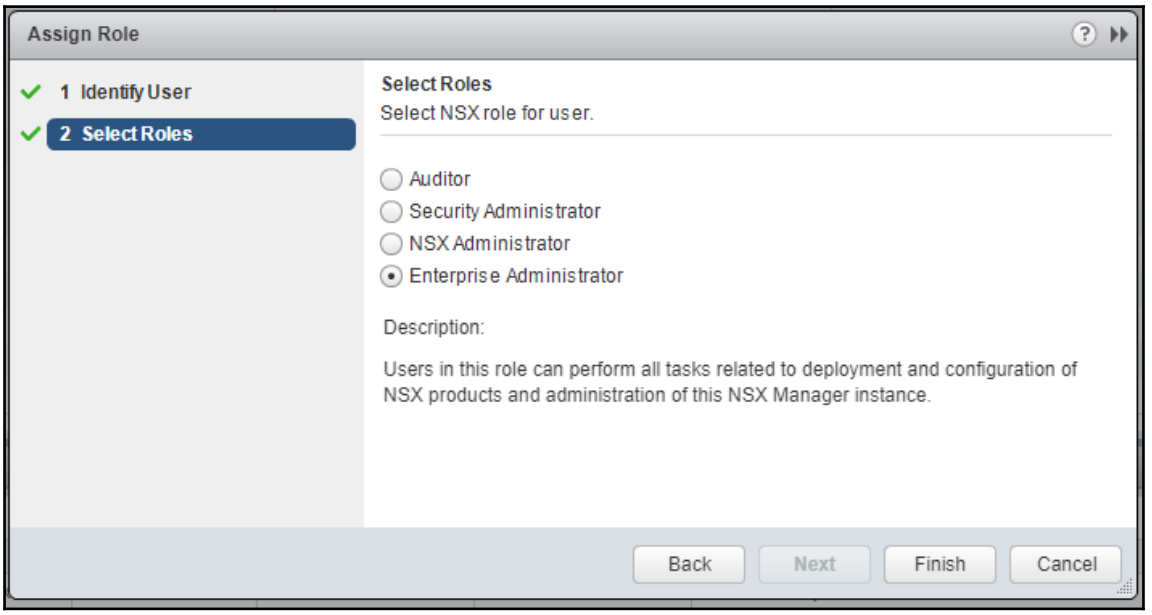

Navigator
Back
vcsa-01a.corp.local
RegionA01
vcsa-01a.corp.local
Actions
Getting Started
Summary
Monitor
Configure
Permissions
Datacenters
Hosts & Clusters
Add permission
User/Group
Role
Defined in
vpxd-extension-36...
Administrator
Global Permission
VSPHERE.LOCAL\vpxd-3610c328-be...
Administrator
Global Permission
VSPHERE.LOCAL\vsphere-webclient...
Read-only
Global Permission
VSPHERE.LOCAL\Administrators
Administrator
Global Permission
VSPHERE.LOCAL\Administrator
Administrator
This object and its children
CORP\vSphereAdmins
Administrator
This object and its children

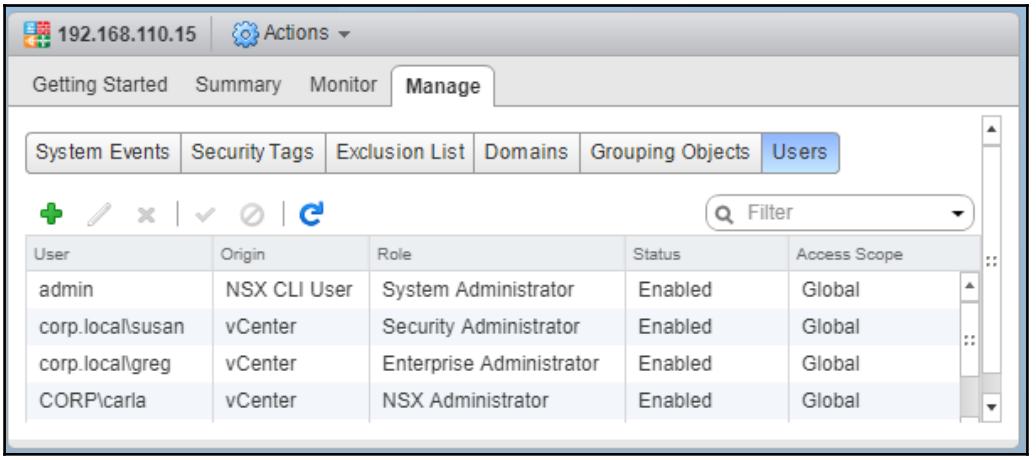

vcsa-01a.corp.local - Add Permission
Select the users or groups on the left and the role to assign to them on the right.
Users and Groups
The users or groups listed below are assigned the role selected on the right on 'vcsa-01a.corp.local'.
User/Group
Role
Propagate
CORP.LOCAL\greg
Read-only
Yes
CORP.LOCAL\susan
Read-only
Yes
CORP.LOCAL\carla
Read-only
Yes
Add...
Remove
Assigned Role
The users or groups obtain the permissions on the selected objects as defined by their assigned role.
Read-only
All Privileges
Alarms
AutoDeploy
Certificates
Content Library
Cryptographic operations
Datacenter
Datastore
Datastore cluster
Distributed switch
ESX Agent Manager
Extension
External stats provider
Folder
Global
Health update provider
Host
Host profile
Description: All Privileges
Propagate to children
View Children
OK
Cancel

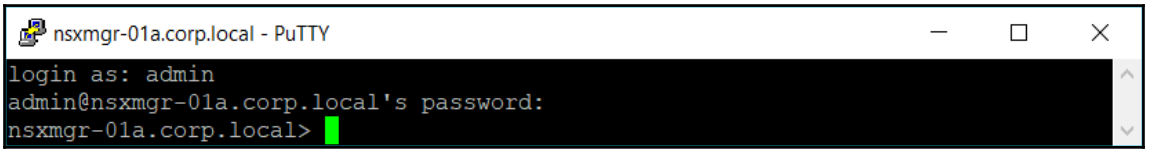

vcsa-01a.corp.local
Actions
Getting Started
Summary
Monitor
Configure
Permissions
Datacenters
Hosts & Clusters
User/Group
Role
Defined in
VSPHERE.LOCAL\vsphere-webclient...
Read-only
Global Permission
VSPHERE.LOCAL\vpxd-extension-36...
Administrator
Global Permission
VSPHERE.LOCAL\vpxd-3610c328-be...
Administrator
Global Permission
VSPHERE.LOCAL\Administrators
Administrator
Global Permission
VSPHERE.LOCAL\Administrator
Administrator
This object and its children
CORP\vSphereAdmins
Administrator
This object and its children
CORP\susan
Read-only
This object and its children
CORP\greg
Read-only
This object and its children
CORP\carla
Read-only
This object and its children

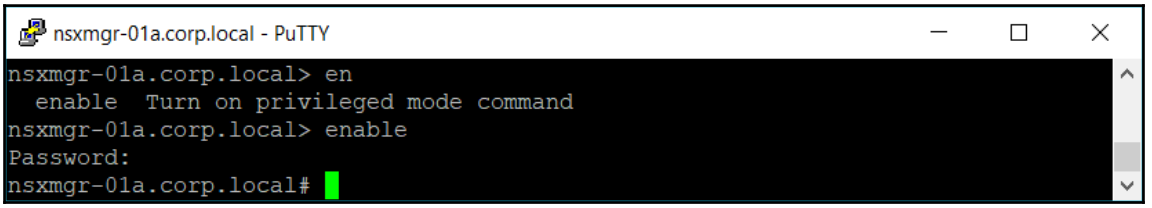

Navigator
Back
NSX Managers
1
192.168.110.15
192.168.110.15
Actions
Getting Started
Summary
Monitor
Manage
System Events
Security Tags
Exclusion List
Domains
Grouping Objects
Users
Filter
User
Origin
Role
Status
Access Scope
Add
vsph...cal\nsx-svc
vCenter
Enterprise Administrator
Enabled
Global
admin
NSX CLI User
System Administrator
Enabled
Global

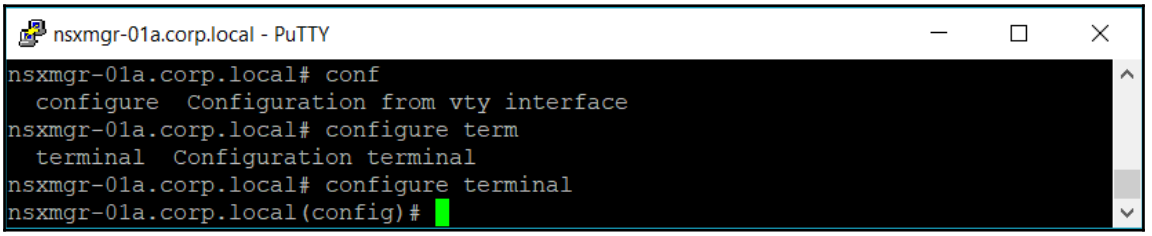

Assign Role
1 Identify User
2 Select Roles
Identify User
Select a vCenter user or group to assign role.
Specify a vCenter user
User: * greg@corp.local
User can log on with the credentials maintained at vCenter.
(ex: test@vsphere.local or test@domain.com)
Specify a vCenter group
Back
Next
Finish
Cancel

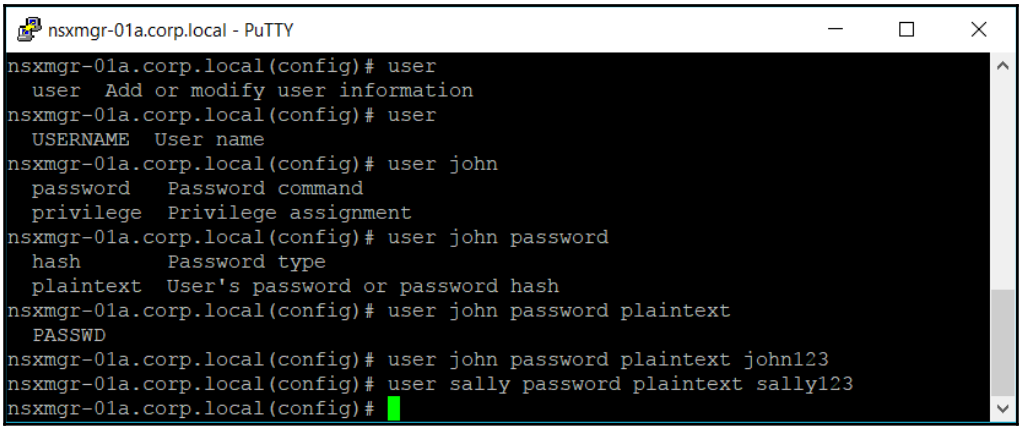

Assign Role
1 Identify User
2 Select Roles
Select Roles
Select NSX role for user.
Auditor
Security Administrator
NSX Administrator
Enterprise Administrator
Description:
Users in this role can perform all tasks related to deployment and configuration of NSX products and administration of this NSX Manager instance.
Back
Next
Finish
Cancel

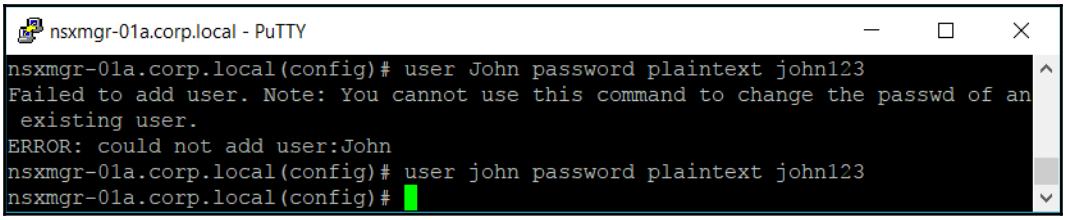

192.168.110.15
Actions
Getting Started
Summary
Monitor
Manage
System Events
Security Tags
Exclusion List
Domains
Grouping Objects
Users
Filter
User
Origin
Role
Status
Access Scope
admin
NSX CLI User
System Administrator
Enabled
Global
corp.local\susan
vCenter
Security Administrator
Enabled
Global
corp.local\greg
vCenter
Enterprise Administrator
Enabled
Global
CORP\carla
vCenter
NSX Administrator
Enabled
Global

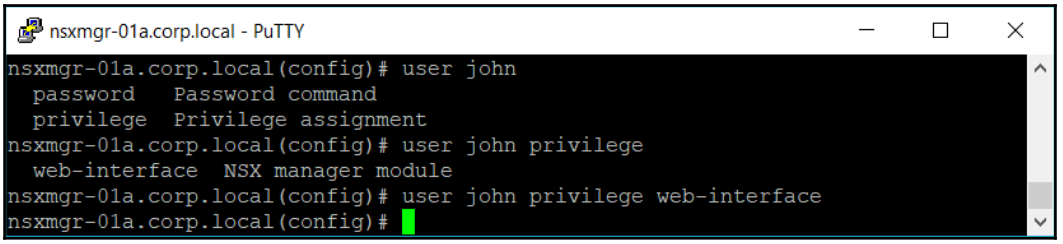

nsxmgr-01a.corp.local - PuTTY
login as: admin
admin@nsxmgr-01a.corp.local's password:
nsxmgr-01a.corp.local>

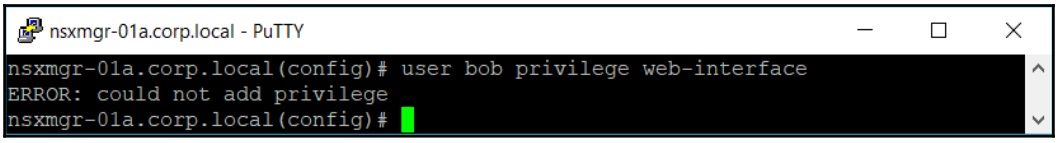

nsxmgr-01a.corp.local - PuTTY
nsxmgr-01a.corp.local> en
enable Turn on privileged mode command
nsxmgr-01a.corp.local> enable
Password:
nsxmgr-01a.corp.local#

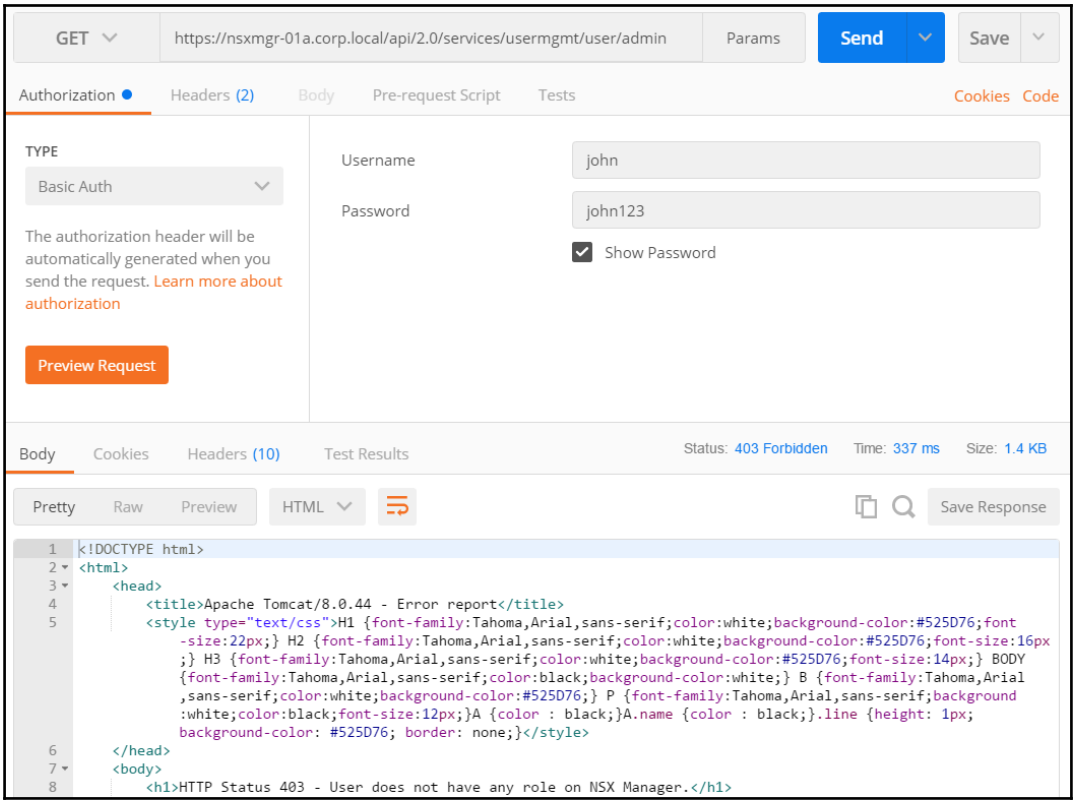

nsxmgr-01a.corp.local - PuTTY
nsxmgr-01a.corp.local# conf
configure Configuration from vty interface
nsxmgr-01a.corp.local# configure term
terminal Configuration terminal
nsxmgr-01a.corp.local# configure terminal
nsxmgr-01a.corp.local(config)#

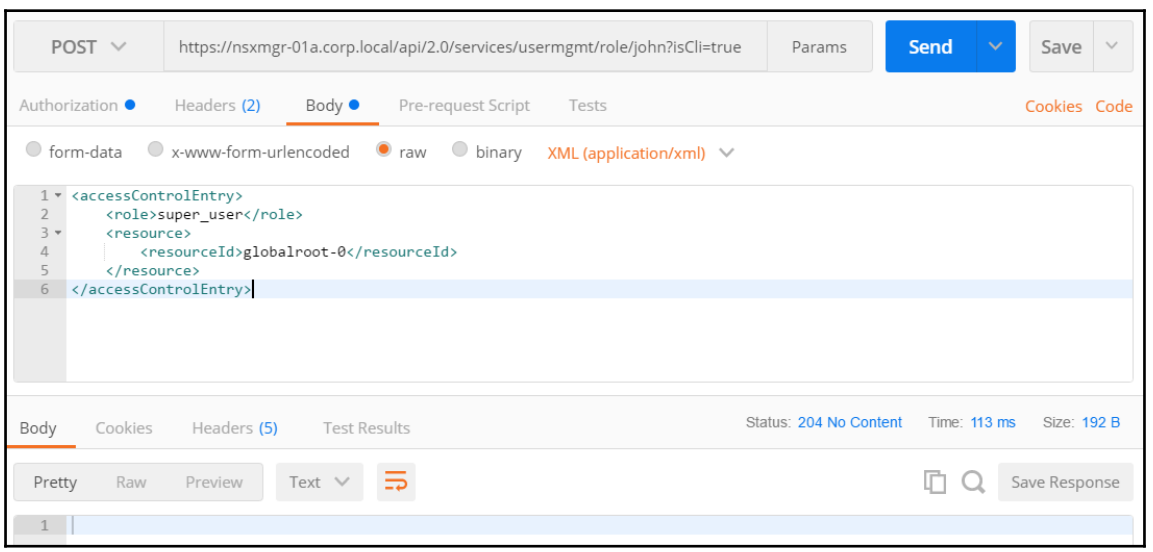

nsxmgr-01a.corp.local - PuTTY
nsxmgr-01a.corp.local(config)# user
user Add or modify user information
nsxmgr-01a.corp.local(config)# user
USERNAME User name
nsxmgr-01a.corp.local(config)# user john
password Password command
privilege Privilege assignment
nsxmgr-01a.corp.local(config)# user john password
hash Password type
plaintext User's password or password hash
nsxmgr-01a.corp.local(config)# user john password plaintext
PASSWD
nsxmgr-01a.corp.local(config)# user john password plaintext john123
nsxmgr-01a.corp.local(config)# user sally password plaintext sally123
nsxmgr-01a.corp.local(config)#


nsxmgr-01a.corp.local - PuTTY
nsxmgr-01a.corp.local(config)# user John password plaintext john123
Failed to add user. Note: You cannot use this command to change the passwd of an
existing user.
ERROR: could not add user:John
nsxmgr-01a.corp.local(config)# user john password plaintext john123
nsxmgr-01a.corp.local(config)#


nsxmgr-01a.corp.local - PuTTY
nsxmgr-01a.corp.local(config)# user john
password Password command
privilege Privilege assignment
nsxmgr-01a.corp.local(config)# user john privilege
web-interface NSX manager module
nsxmgr-01a.corp.local(config)# user john privilege web-interface
nsxmgr-01a.corp.local(config)#


nsxmgr-01a.corp.local - PuTTY
nsxmgr-01a.corp.local(config)# user bob privilege web-interface
ERROR: could not add privilege
nsxmgr-01a.corp.local(config)#

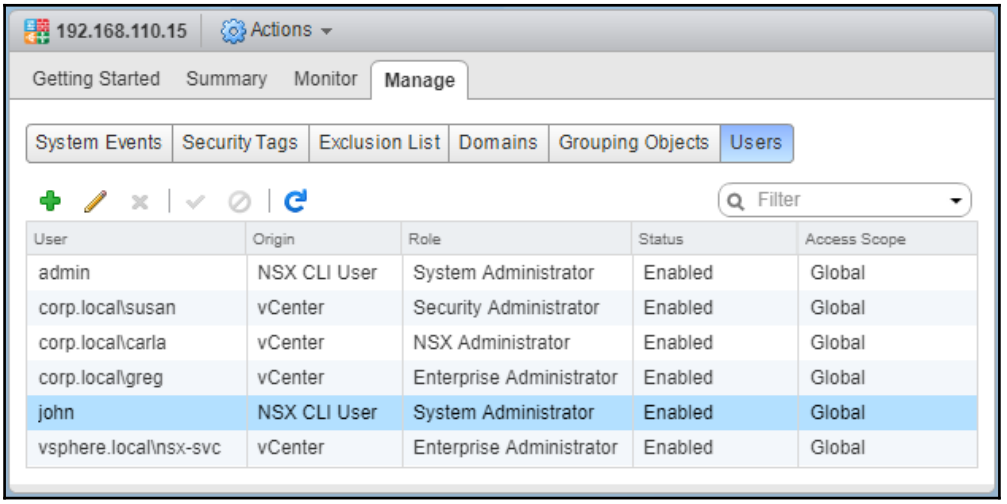

GET
https://nsxmgr-01a.corp.local/api/2.0/services/usermgmt/user/admin
Params
Send
Save
Authorization
Headers (2)
Body
Pre-request Script
Tests
Cookies
Code
TYPE
Basic Auth
The authorization header will be automatically generated when you send the request. Learn more about authorization
Preview Request
Username
john
Password
john123
Show Password
Body
Cookies
Headers (10)
Test Results
Status: 403 Forbidden
Time: 337 ms
Size: 1.4 KB
Pretty
Raw
Preview
HTML
Save Response
<!DOCTYPE html>
<html>
<head>
<title>Apache Tomcat/8.0.44 - Error report</title>
<style type="text/css">H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P {font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}.line {height: 1px;background-color: #525D76; border: none;}</style>
</head>
<body>
<h1>HTTP Status 403 - User does not have any role on NSX Manager.</h1>

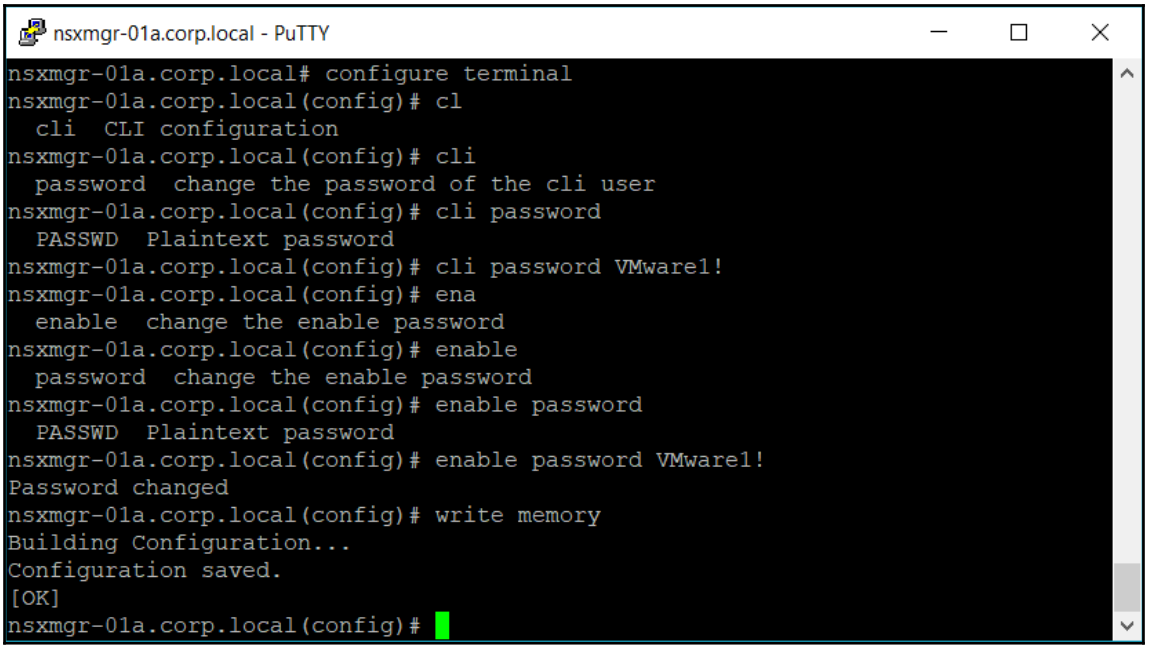

POST
https://nsxmgr-01a.corp.local/api/2.0/services/usermgmt/role/john?isCli=true
Params
Send
Save
Authorization
Headers (2)
Body
Pre-request Script
Tests
Cookies
Code
form-data
x-www-form-urlencoded
raw
binary
XML (application/xml)
<accessControlEntry>
<role>super_user</role>
<resource>
<resourceId>globalroot-0</resourceId>
</resource>
</accessControlEntry>
Body
Cookies
Headers (5)
Test Results
Status: 204 No Content
Time: 113 ms
Size: 192 B
Pretty
Raw
Preview
Text
Save Response

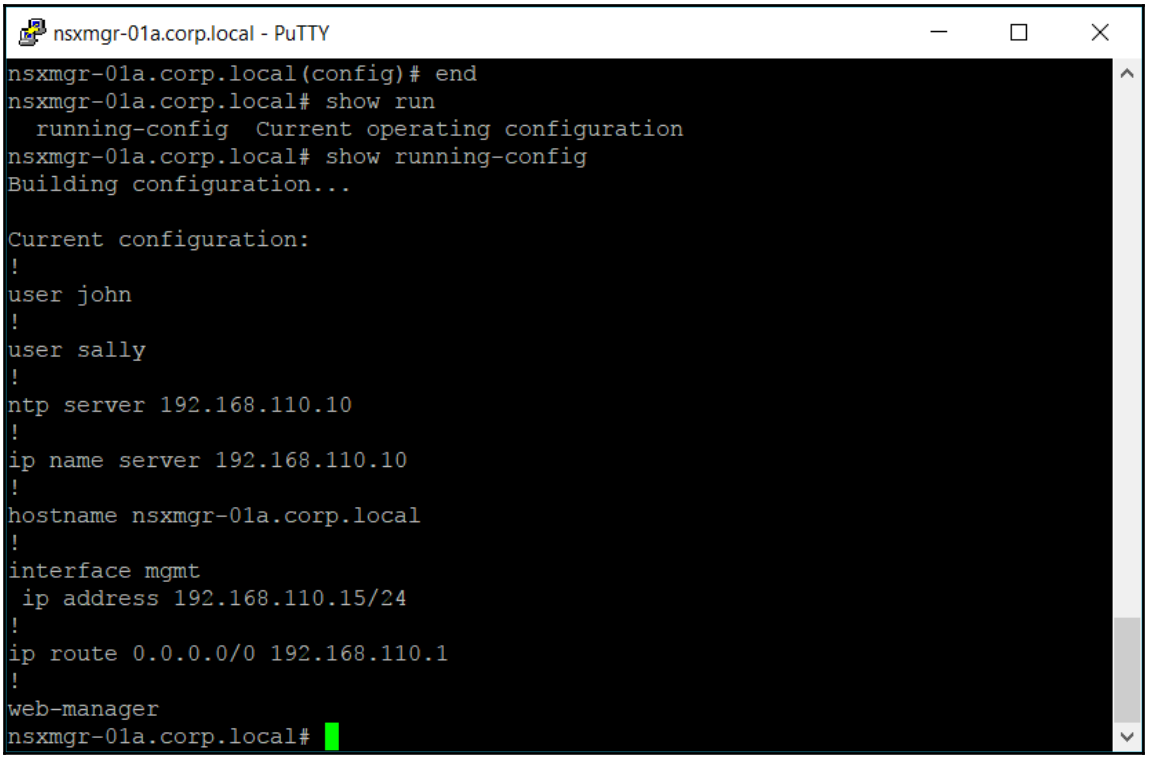
Body Cookies Headers (7) Test Results Status: 400 Bad Request Time: 118 ms Size: 494 B

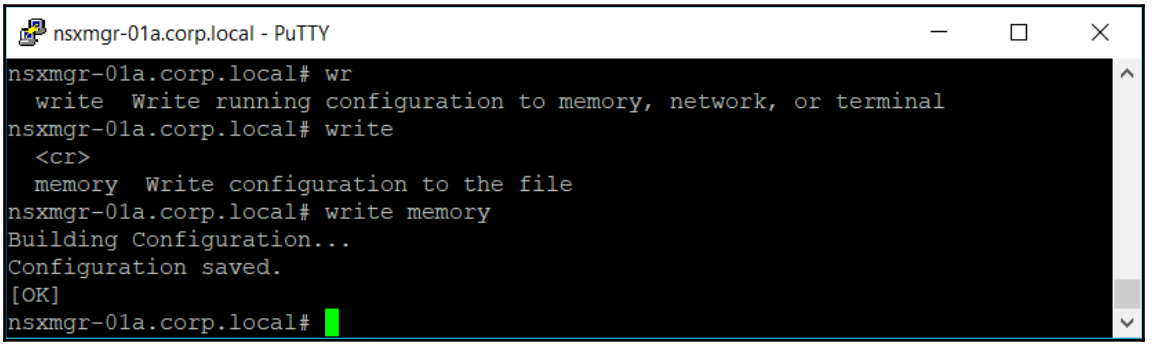
Pretty Raw Preview XML Save Response

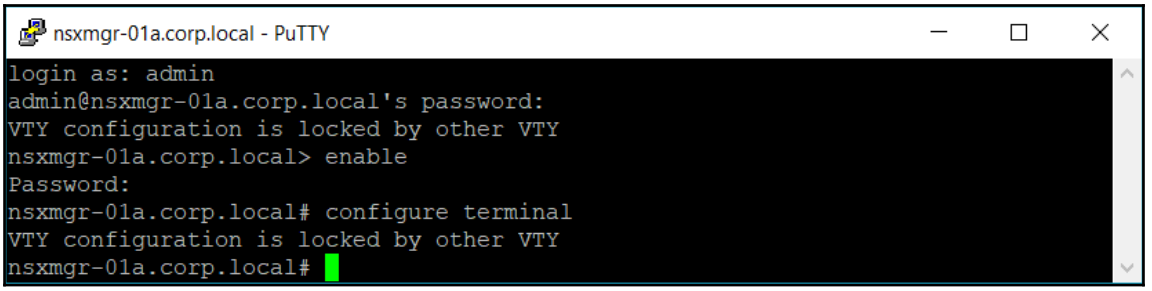
```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <error>
3      <details>Invalid user role specified enterprise_admin. Valid roles are [super_user, security_admin, auditor].</details
       >
4      <errorCode>421</errorCode>
5      <moduleName>core-services</moduleName>
6  </error>
```

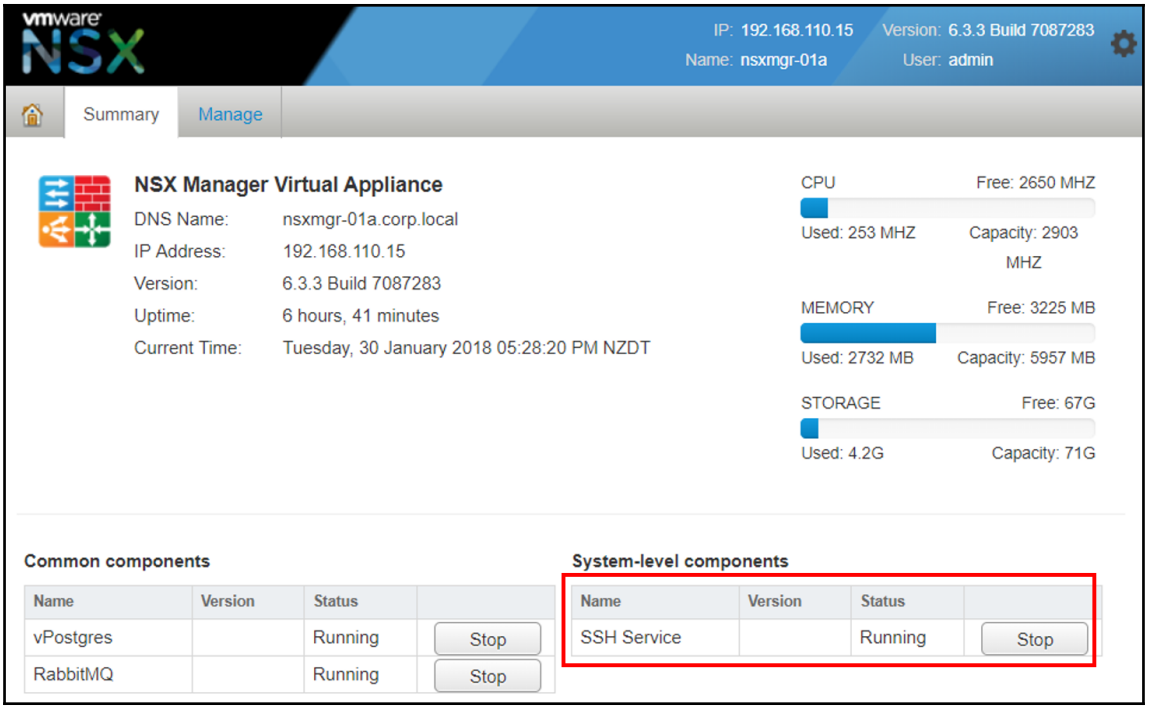



nsxmgr-01a.corp.local - PuTTY
nsxmgr-01a.corp.local# configure terminal
nsxmgr-01a.corp.local(config)# cl
cli CLI configuration
nsxmgr-01a.corp.local(config)# cli
password change the password of the cli user
nsxmgr-01a.corp.local(config)# cli password
PASSWD Plaintext password
nsxmgr-01a.corp.local(config)# cli password VMware1!
nsxmgr-01a.corp.local(config)# ena
enable change the enable password
nsxmgr-01a.corp.local(config)# enable
password change the enable password
nsxmgr-01a.corp.local(config)# enable password
PASSWD Plaintext password
nsxmgr-01a.corp.local(config)# enable password VMware1!
Password changed
nsxmgr-01a.corp.local(config)# write memory
Building Configuration...
Configuration saved.
[OK]
nsxmgr-01a.corp.local(config)#

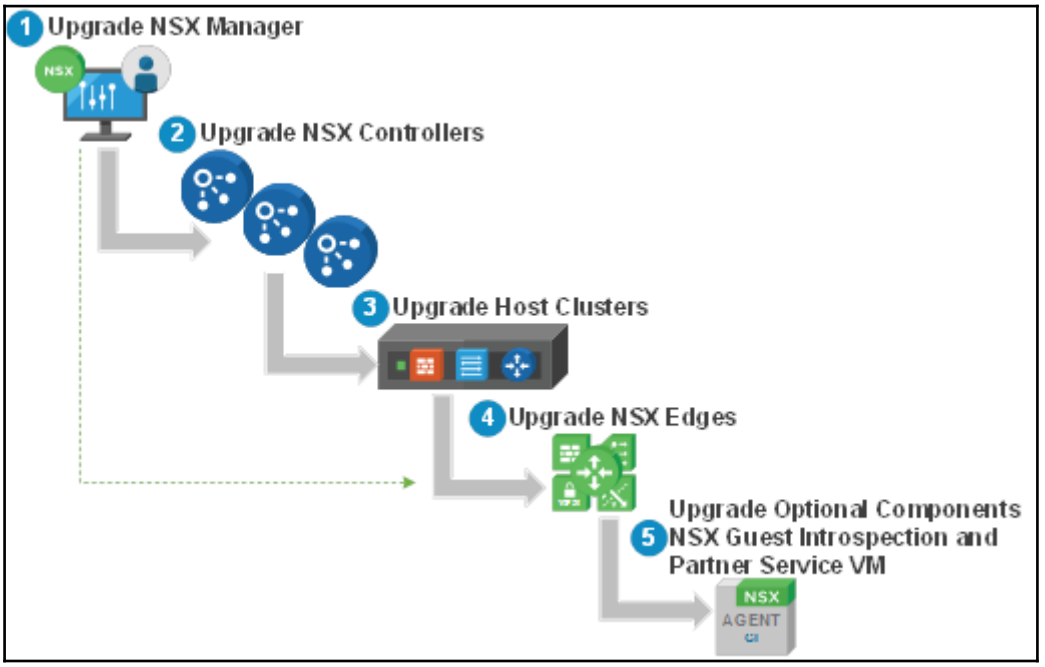

nsxmgr-01a.corp.local - PuTTY
nsxmgr-01a.corp.local(config)# end
nsxmgr-01a.corp.local# show run
  running-config Current operating configuration
nsxmgr-01a.corp.local# show running-config
Building configuration...
Current configuration:
!
user john
!
user sally
!
ntp server 192.168.110.10
!
ip name server 192.168.110.10
!
hostname nsxmgr-01a.corp.local
!
interface mgmt
 ip address 192.168.110.15/24
!
ip route 0.0.0.0/0 192.168.110.1
!
web-manager
nsxmgr-01a.corp.local#

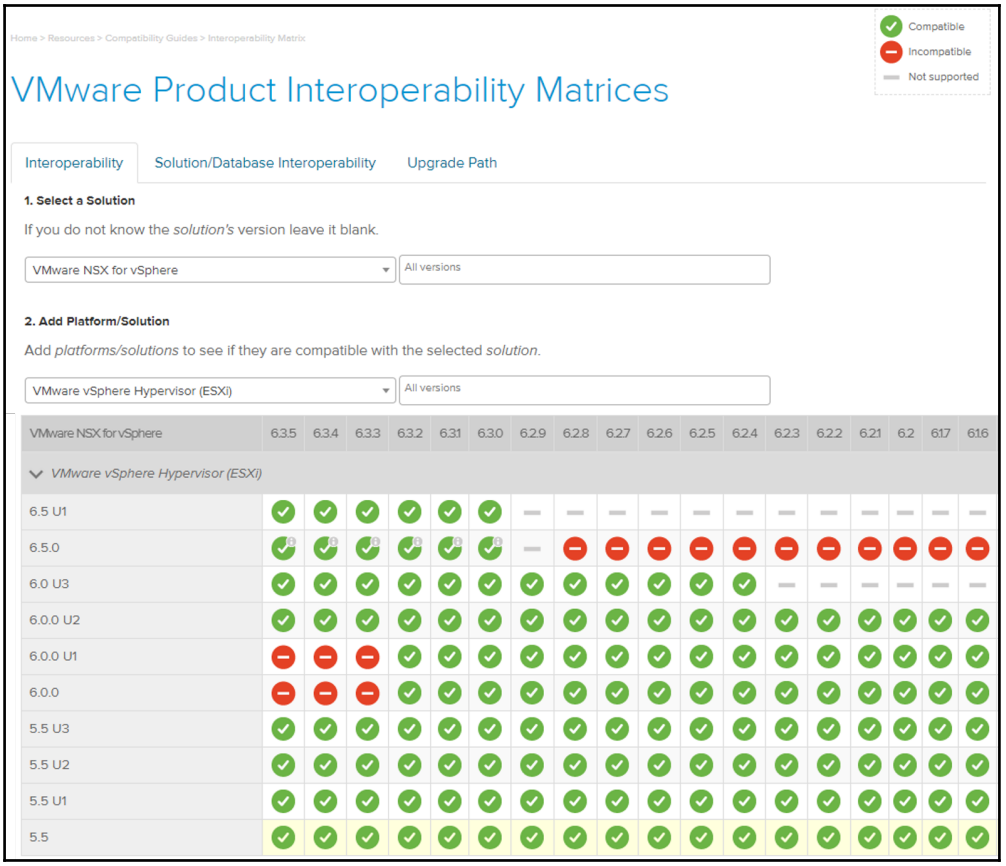

nsxmgr-01a.corp.local - PuTTY
nsxmgr-01a.corp.local# wr
  write Write running configuration to memory, network, or terminal
nsxmgr-01a.corp.local# write
  <cr>
  memory Write configuration to the file
nsxmgr-01a.corp.local# write memory
Building Configuration...
Configuration saved.
[OK]
nsxmgr-01a.corp.local#


nsxmgr-01a.corp.local - PuTTY
login as: admin
admin@nsxmgr-01a.corp.local's password:
VTY configuration is locked by other VTY
nsxmgr-01a.corp.local> enable
Password:
nsxmgr-01a.corp.local# configure terminal
VTY configuration is locked by other VTY
nsxmgr-01a.corp.local#


vmware NSX
IP: 192.168.110.15
Version: 6.3.3 Build 7087283
Name: nsxmgr-01a
User: admin
Summary
Manage
NSX Manager Virtual Appliance
DNS Name: nsxmgr-01a.corp.local
IP Address: 192.168.110.15
Version: 6.3.3 Build 7087283
Uptime: 6 hours, 41 minutes
Current Time: Tuesday, 30 January 2018 05:28:20 PM NZDT
CPU
Free: 2650 MHZ
Used: 253 MHZ
Capacity: 2903 MHZ
MEMORY
Free: 3225 MB
Used: 2732 MB
Capacity: 5957 MB
STORAGE
Free: 67G
Used: 4.2G
Capacity: 71G
Common components
Name
Version
Status
vPostgres
Running
Stop
RabbitMQ
Running
Stop
System-level components
Name
Version
Status
SSH Service
Running
Stop

Chapter 10: Upgrading VMware NSX





Home > Resources > Compatibility Guides > Interoperability Matrix

Compatible
Incompatible
Not supported

VMware Product Interoperability Matrices

Interoperability | Solution/Database Interoperability | Upgrade Path

1. Select a Solution

If you do not know the *solution's* version leave it blank.

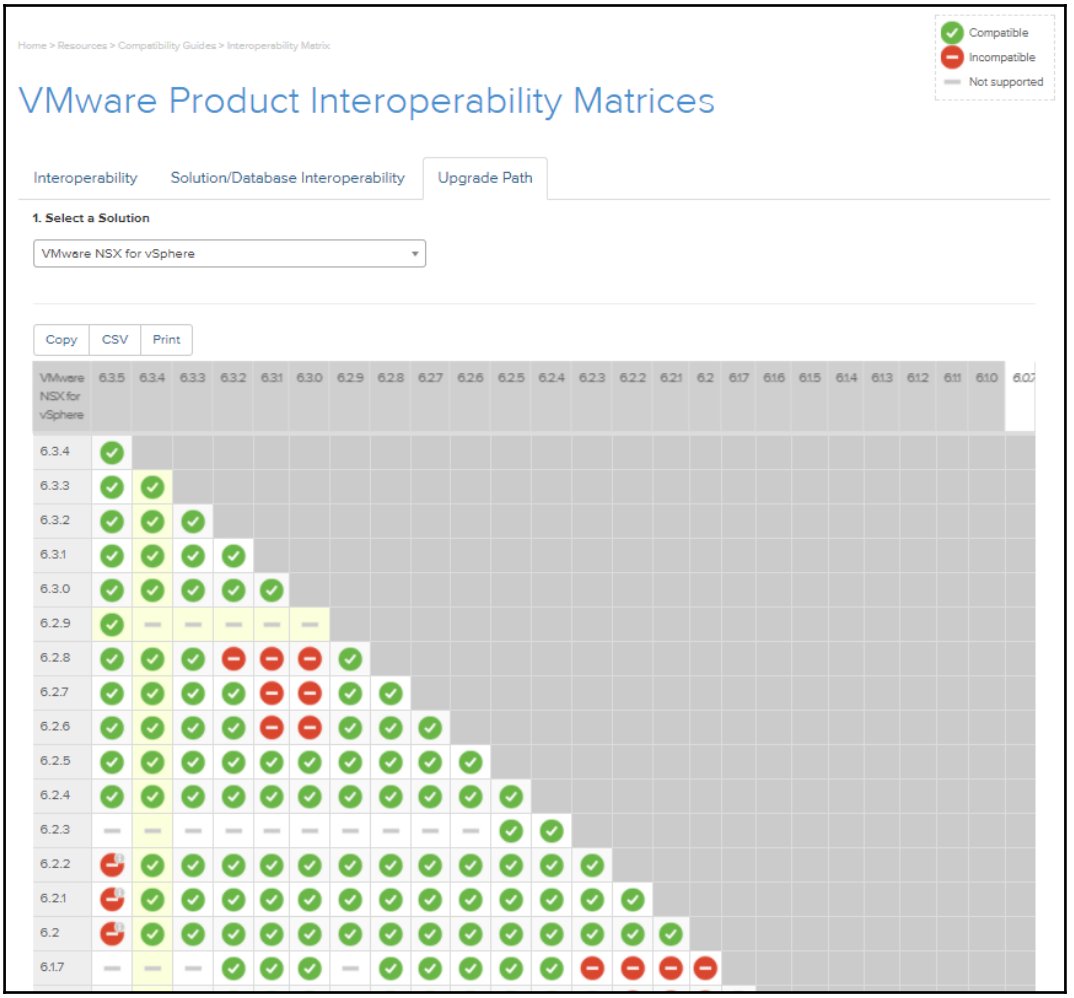
VMware NSX for vSphere | All versions

2. Add Platform/Solution

Add *platforms/solutions* to see if they are compatible with the selected *solution*.

VMware vSphere Hypervisor (ESXi) | All versions

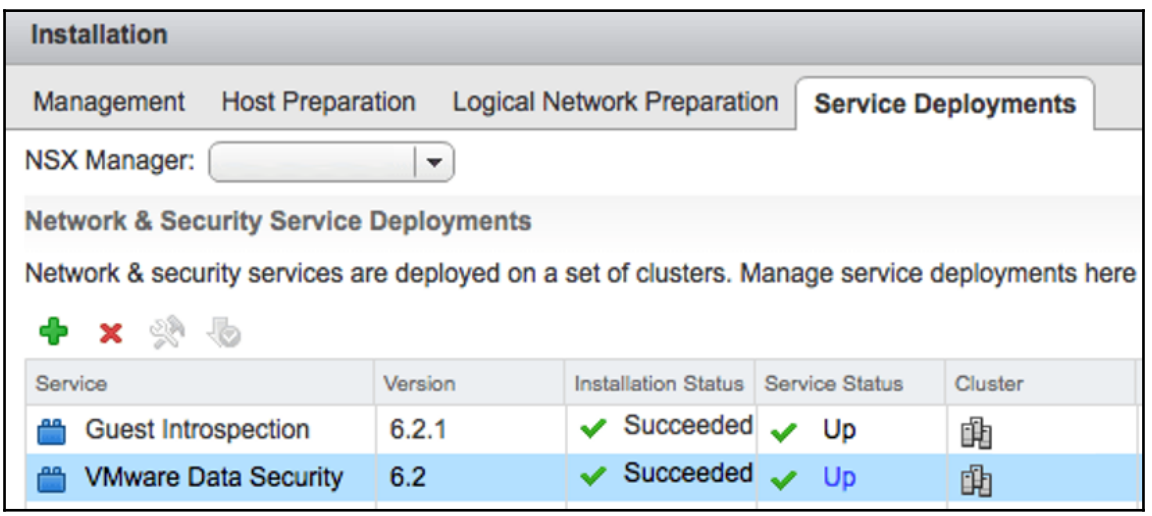
VMware NSX for vSphere	6.3.5	6.3.4	6.3.3	6.3.2	6.3.1	6.3.0	6.2.9	6.2.8	6.2.7	6.2.6	6.2.5	6.2.4	6.2.3	6.2.2	6.2.1	6.2	6.1.7	6.1.6
VMware vSphere Hypervisor (ESXi)																		
6.5 U1	✓	✓	✓	✓	✓	✓	—	—	—	—	—	—	—	—	—	—	—	—
6.5.0	✓	✓	✓	✓	✓	✓	—	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖
6.0 U3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	—	—	—	—	—	—
6.0.0 U2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
6.0.0 U1	⊖	⊖	⊖	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
6.0.0	⊖	⊖	⊖	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.5 U3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.5 U2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.5 U1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.5	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

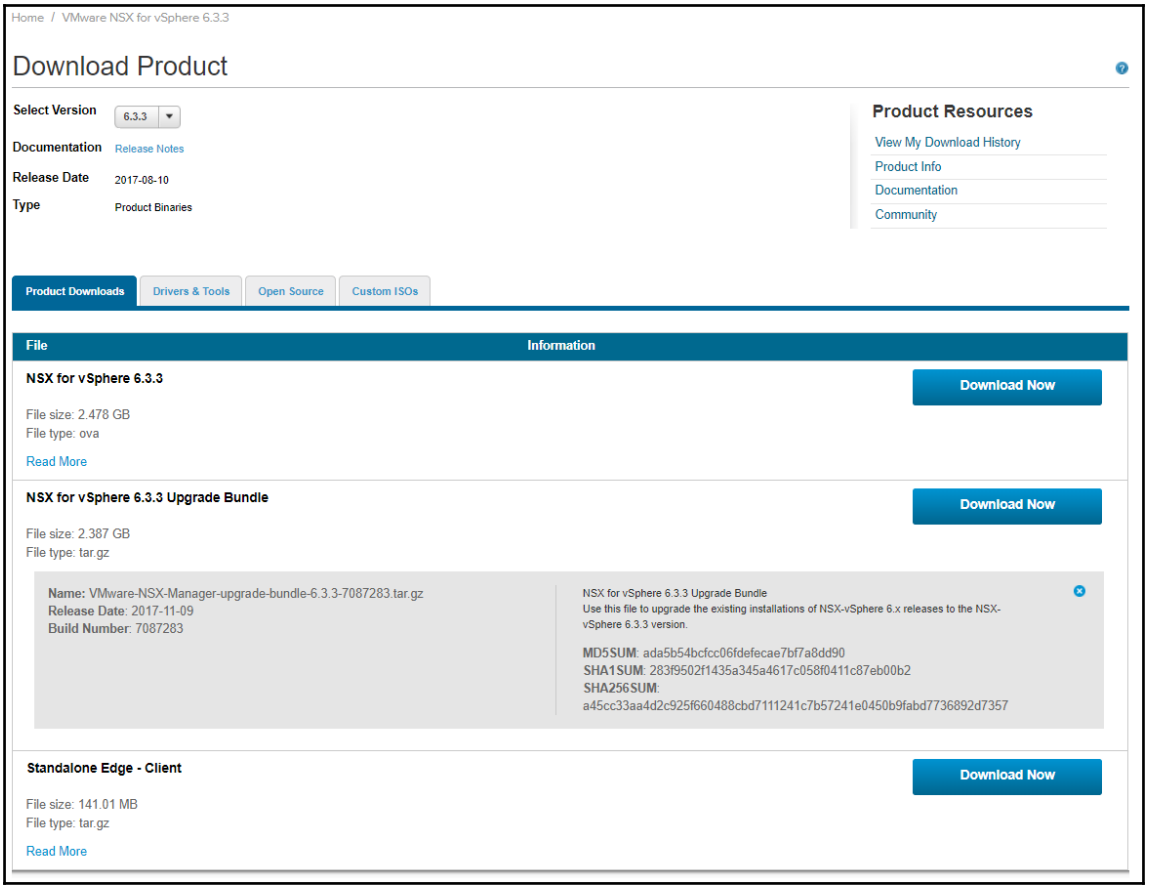

Home > Resources > Compatibility Guides > Interoperability Matrix
Compatible
Incompatible
Not supported
VMware Product Interoperability Matrices
Interoperability
Solution/Database Interoperability
Upgrade Path
1. Select a Solution
VMware NSX for vSphere
Copy
CSV
Print
VMware NSX for vSphere
6.3.5 6.3.4 6.3.3 6.3.2 6.3.1 6.3.0 6.2.9 6.2.8 6.2.7 6.2.6 6.2.5 6.2.4 6.2.3 6.2.2 6.2.1 6.2 6.1.7 6.1.6 6.1.5 6.1.4 6.1.3 6.1.2 6.1.1 6.1.0 6.0.7
6.3.4
6.3.3
6.3.2
6.3.1
6.3.0
6.2.9
6.2.8
6.2.7
6.2.6
6.2.5
6.2.4
6.2.3
6.2.2
6.2.1
6.2
6.1.7

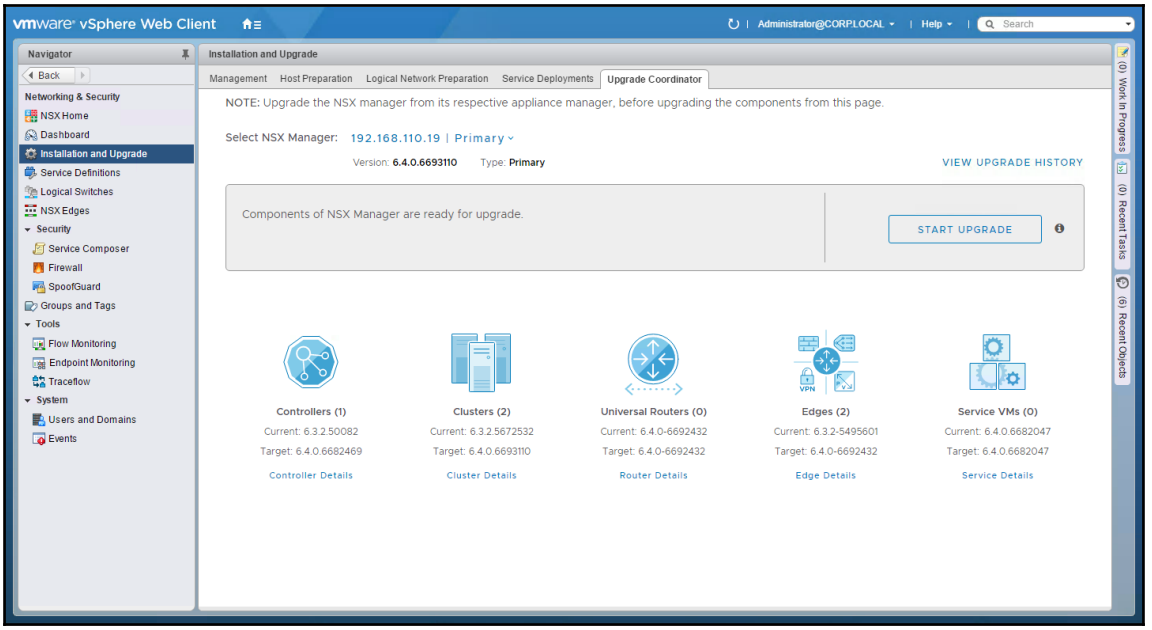
Supported Update Sequence:

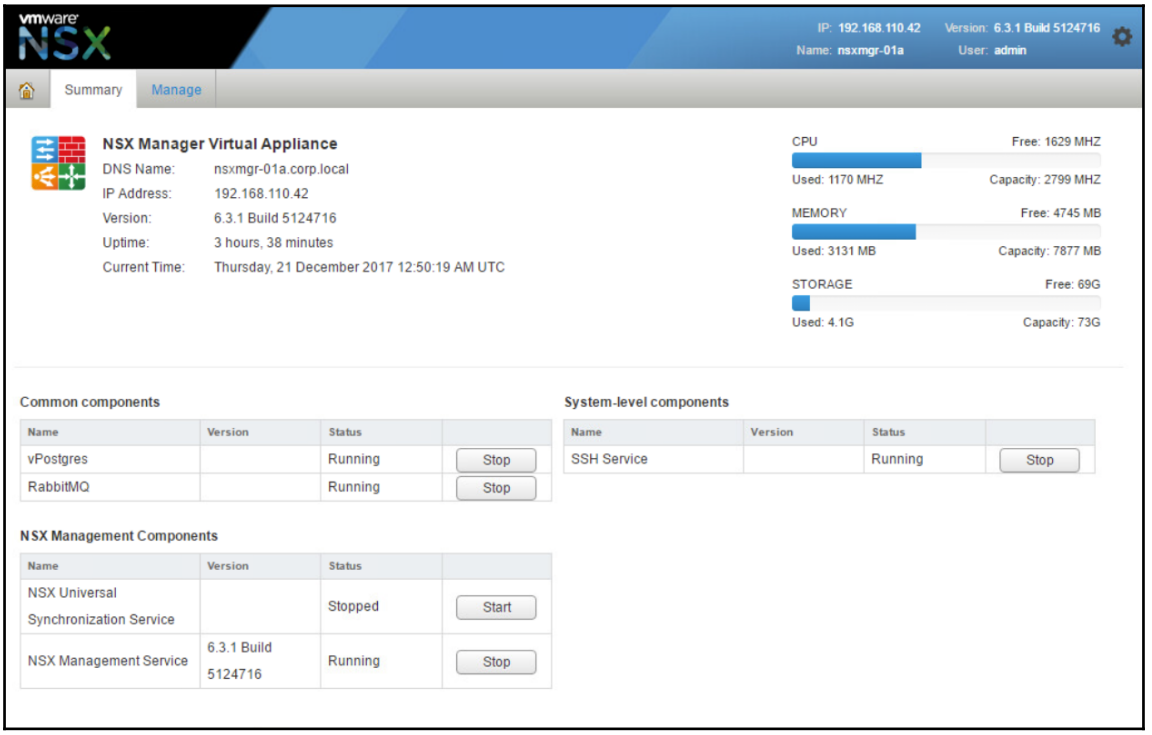
Use the scroll bar in the table to view the complete list.

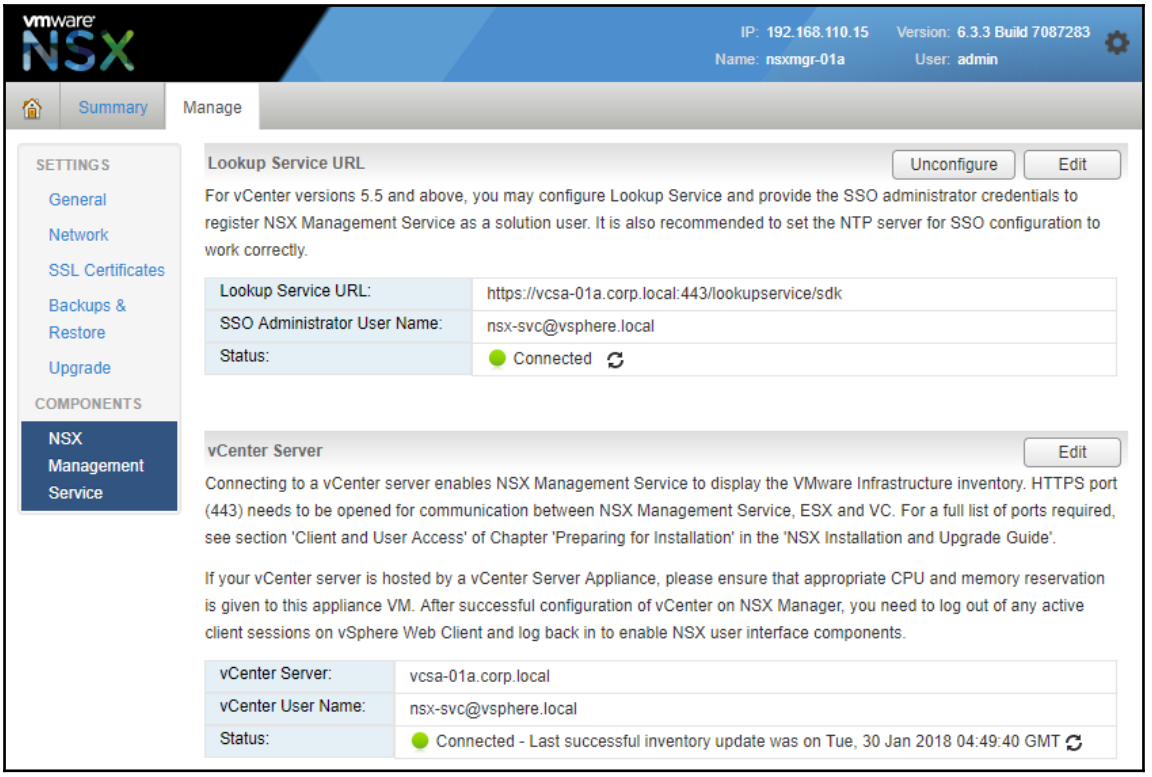
	View Composer	View Connection Server	PSC / SSO External	vRA*	VCM	vRB*	*vCD*	*NSX Manager*	*NSX Controllers*	VDP	vCenter Server	vRO*	VR	VUM	vROPs	*VIN*
Seq.	1															
		2														
			3													
				4	4	4										
							5									
								6								
									7							
										8						
											9					
												10	10	10	10	10

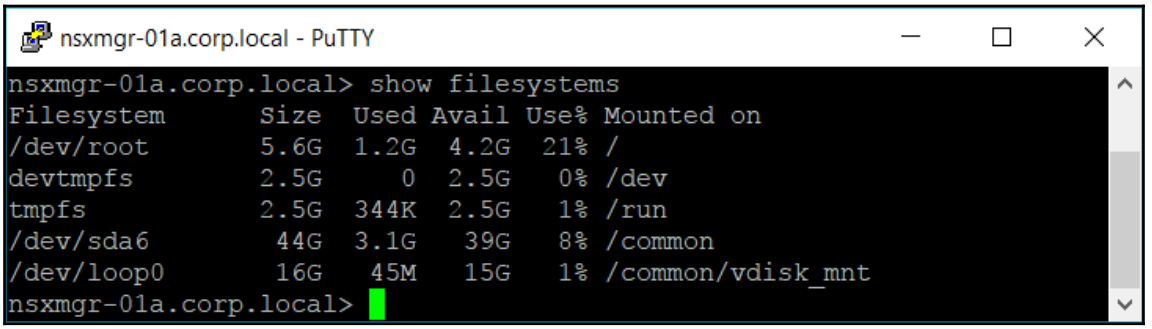


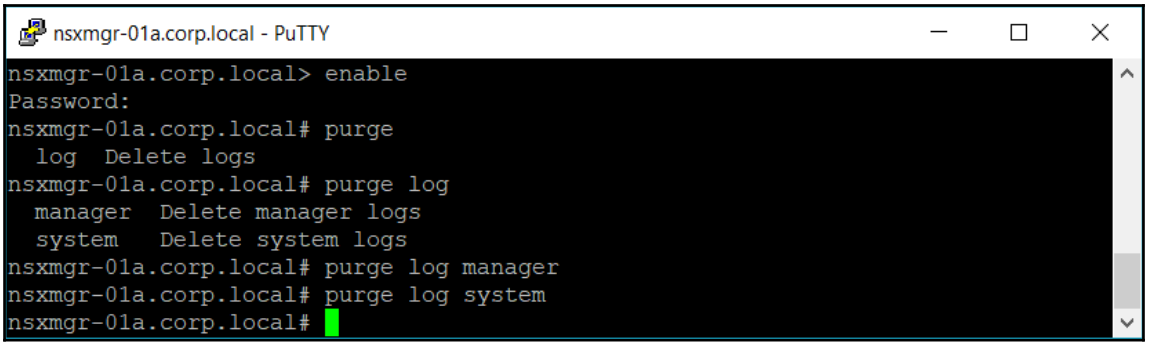

Home / VMware NSX for vSphere 6.3.3
Download Product
Select Version
6.3.3
Documentation
Release Notes
Release Date
2017-08-10
Type
Product Binaries
Product Resources
View My Download History
Product Info
Documentation
Community
Product Downloads
Drivers & Tools
Open Source
Custom ISOs
File
Information
NSX for vSphere 6.3.3
Download Now
File size: 2.478 GB
File type: ova
Read More
NSX for vSphere 6.3.3 Upgrade Bundle
Download Now
File size: 2.387 GB
File type: tar.gz
Name: VMware-NSX-Manager-upgrade-bundle-6.3.3-7087283.tar.gz
Release Date: 2017-11-09
Build Number: 7087283
NSX for vSphere 6.3.3 Upgrade Bundle
Use this file to upgrade the existing installations of NSX-vSphere 6.x releases to the NSX-vSphere 6.3.3 version.
MD5SUM: ada5b54bcfcc06fdefecae7bf7a8dd90
SHA1SUM: 283f9502f1435a345a4617c058f0411c87eb00b2
SHA256SUM:
a45cc33aa4d2c925f660488cbd7111241c7b57241e0450b9fabd7736892d7357
Standalone Edge - Client
Download Now
File size: 141.01 MB
File type: tar.gz
Read More


vmware vSphere Web Client
Administrator@CORP.LOCAL
Help
Search
Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation and Upgrade
Service Definitions
Logical Switches
NSX Edges
Security
Service Composer
Firewall
SpoofGuard
Groups and Tags
Tools
Flow Monitoring
Endpoint Monitoring
Traceflow
System
Users and Domains
Events
Installation and Upgrade
Management
Host Preparation
Logical Network Preparation
Service Deployments
Upgrade Coordinator
NOTE: Upgrade the NSX manager from its respective appliance manager, before upgrading the components from this page.
Select NSX Manager: 192.168.110.19 | Primary
Version: 6.4.0.6693110
Type: Primary
VIEW UPGRADE HISTORY
Components of NSX Manager are ready for upgrade.
START UPGRADE
Controllers (1)
Current: 6.3.2.50082
Target: 6.4.0.6682469
Controller Details
Clusters (2)
Current: 6.3.2.5672532
Target: 6.4.0.6693110
Cluster Details
Universal Routers (0)
Current: 6.4.0-6692432
Target: 6.4.0-6692432
Router Details
Edges (2)
Current: 6.3.2-5495601
Target: 6.4.0-6692432
Edge Details
Service VMs (0)
Current: 6.4.0.6682047
Target: 6.4.0.6682047
Service Details
(0) Work In Progress
(0) Recent Tasks
(6) Recent Objects

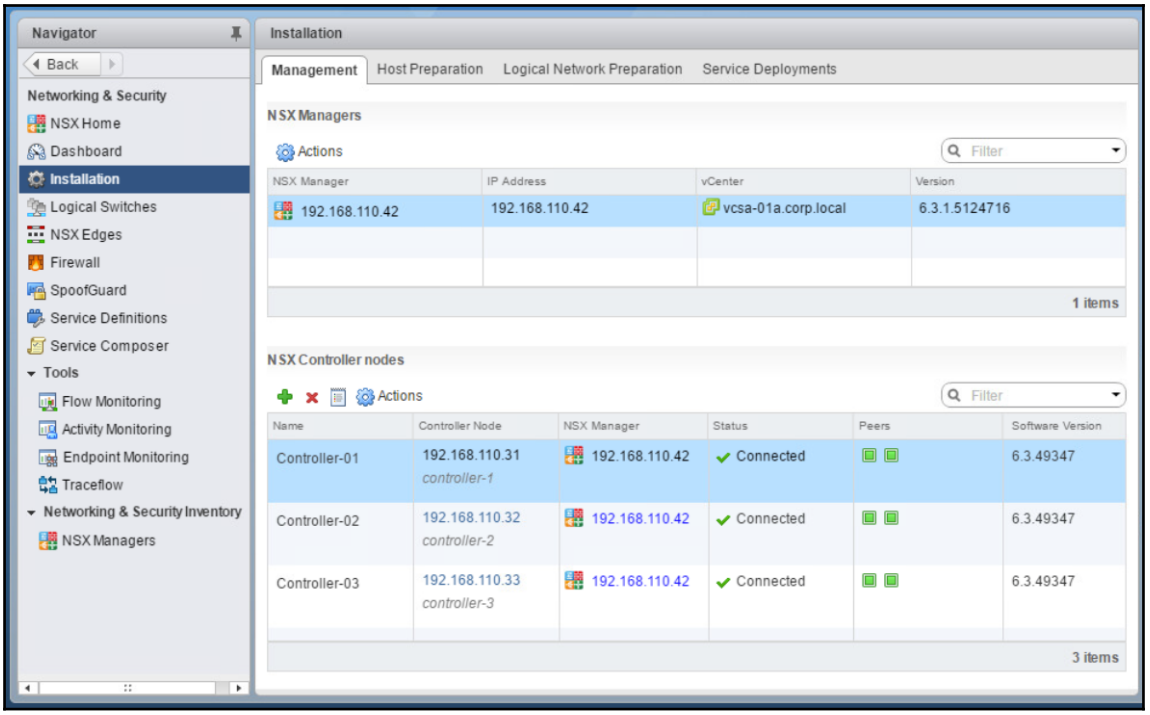

vmware NSX
IP: 192.168.110.42
Name: nsxmgr-01a
Version: 6.3.1 Build 5124716
User: admin
Summary
Manage
NSX Manager Virtual Appliance
DNS Name: nsxmgr-01a.corp.local
IP Address: 192.168.110.42
Version: 6.3.1 Build 5124716
Uptime: 3 hours, 38 minutes
Current Time: Thursday, 21 December 2017 12:50:19 AM UTC
CPU
Free: 1629 MHZ
Used: 1170 MHZ
Capacity: 2799 MHZ
MEMORY
Free: 4745 MB
Used: 3131 MB
Capacity: 7877 MB
STORAGE
Free: 69G
Used: 4.1G
Capacity: 73G
Common components
Name
Version
Status
vPostgres
Running
Stop
RabbitMQ
Running
Stop
System-level components
Name
Version
Status
SSH Service
Running
Stop
NSX Management Components
Name
Version
Status
NSX Universal Synchronization Service
Stopped
Start
NSX Management Service
6.3.1 Build 5124716
Running
Stop


vmware NSX
IP: 192.168.110.15
Version: 6.3.3 Build 7087283
Name: nsxmgr-01a
User: admin
Summary
Manage
SETTINGS
General
Network
SSL Certificates
Backups & Restore
Upgrade
COMPONENTS
NSX Management Service
Lookup Service URL
Unconfigure
Edit
For vCenter versions 5.5 and above, you may configure Lookup Service and provide the SSO administrator credentials to register NSX Management Service as a solution user. It is also recommended to set the NTP server for SSO configuration to work correctly.
Lookup Service URL: https://vcsa-01a.corp.local:443/lookupservice/sdk
SSO Administrator User Name: nsx-svc@vsphere.local
Status: Connected
vCenter Server
Edit
Connecting to a vCenter server enables NSX Management Service to display the VMware Infrastructure inventory. HTTPS port (443) needs to be opened for communication between NSX Management Service, ESX and VC. For a full list of ports required, see section 'Client and User Access' of Chapter 'Preparing for Installation' in the 'NSX Installation and Upgrade Guide'.
If your vCenter server is hosted by a vCenter Server Appliance, please ensure that appropriate CPU and memory reservation is given to this appliance VM. After successful configuration of vCenter on NSX Manager, you need to log out of any active client sessions on vSphere Web Client and log back in to enable NSX user interface components.
vCenter Server: vcsa-01a.corp.local
vCenter User Name: nsx-svc@vsphere.local
Status: Connected - Last successful inventory update was on Tue, 30 Jan 2018 04:49:40 GMT


nsxmgr-01a.corp.local - PuTTY
nsxmgr-01a.corp.local> show filesystems
Filesystem Size Used Avail Use% Mounted on
/dev/root 5.6G 1.2G 4.2G 21% /
devtmpfs 2.5G 0 2.5G 0% /dev
tmpfs 2.5G 344K 2.5G 1% /run
/dev/sda6 44G 3.1G 39G 8% /common
/dev/loop0 16G 45M 15G 1% /common/vdisk_mnt
nsxmgr-01a.corp.local>

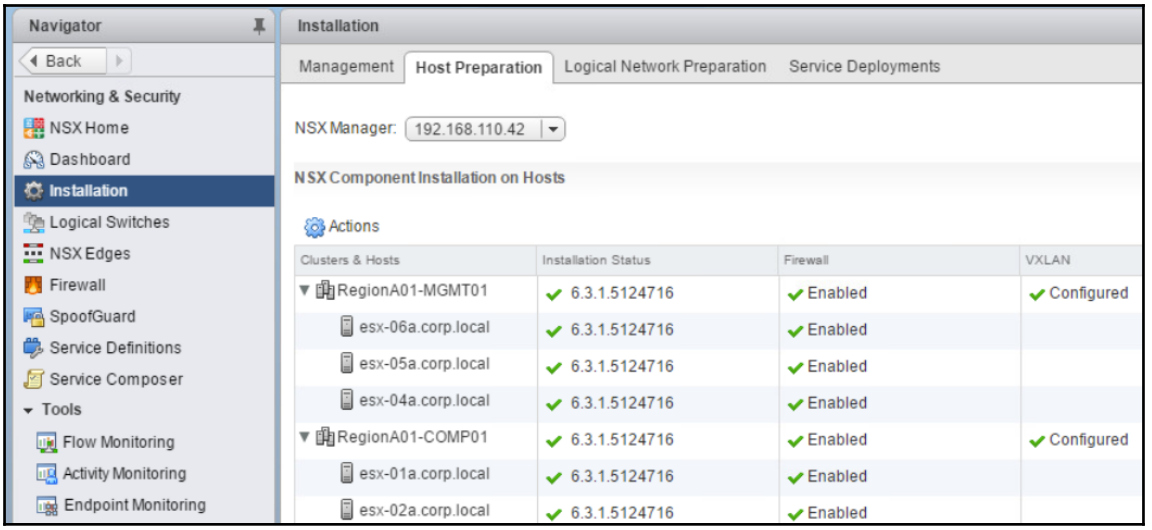

nsxmgr-01a.corp.local - PuTTY
nsxmgr-01a.corp.local> enable
Password:
nsxmgr-01a.corp.local# purge
log Delete logs
nsxmgr-01a.corp.local# purge log
manager Delete manager logs
system Delete system logs
nsxmgr-01a.corp.local# purge log manager
nsxmgr-01a.corp.local# purge log system
nsxmgr-01a.corp.local#

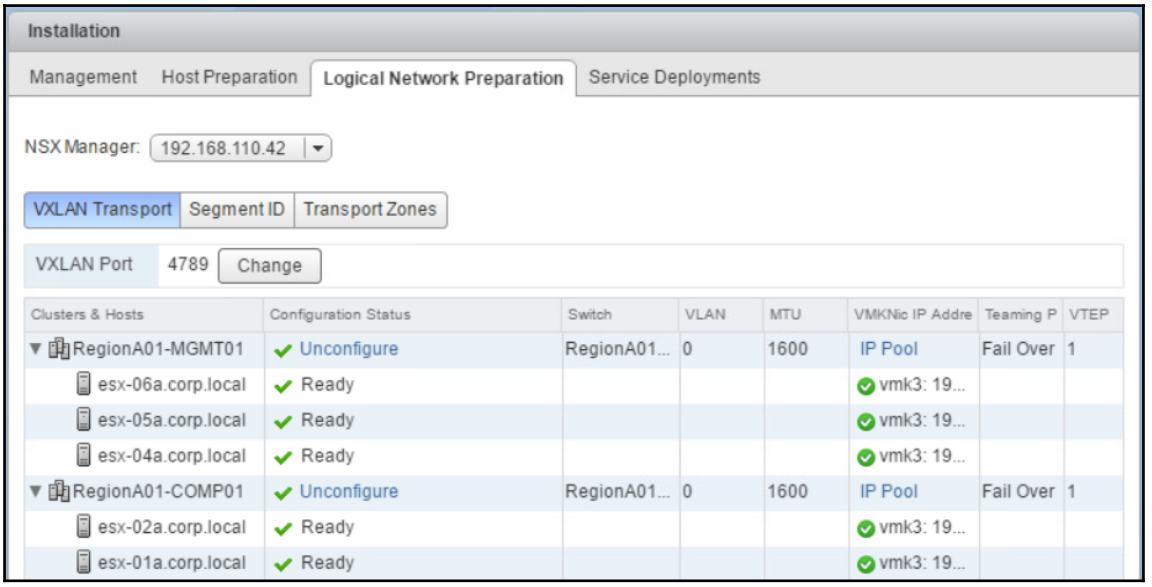

vmware vSphere Web Client
Navigator
Back
Home
Hosts and Clusters
VMs and Templates
Storage
Networking
Content Libraries
Global Inventory Lists
Policies and Profiles
Update Manager
Networking & Security
Home
Home
Inventories
Hosts and Clusters
VMs and Templates
Networking & Security

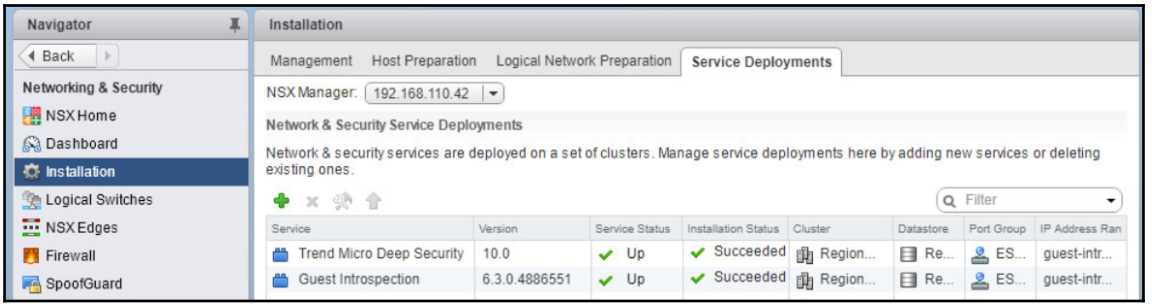


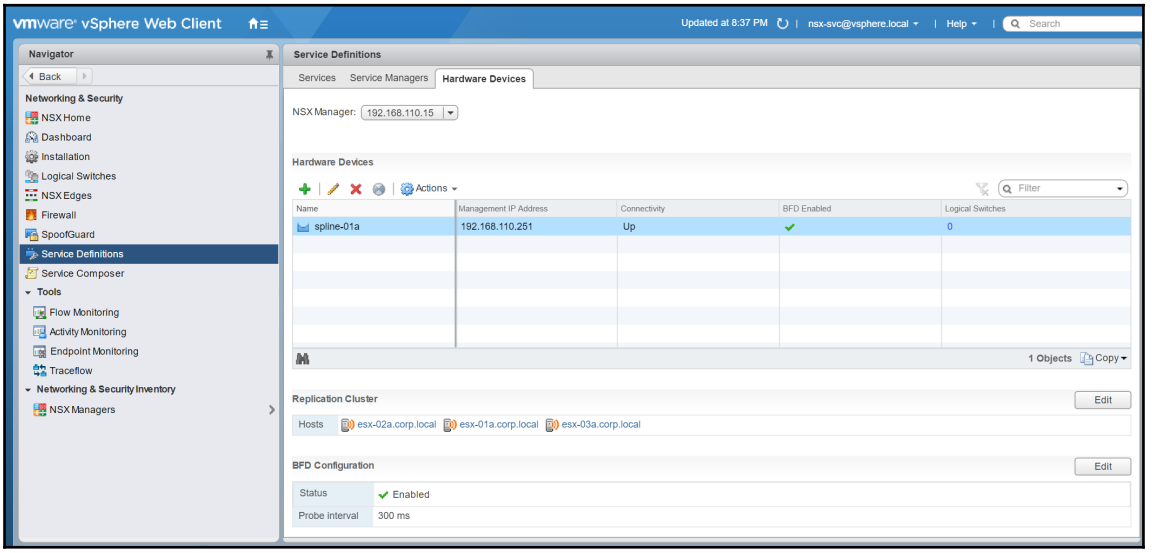
192.168.110.31 - PuTTY

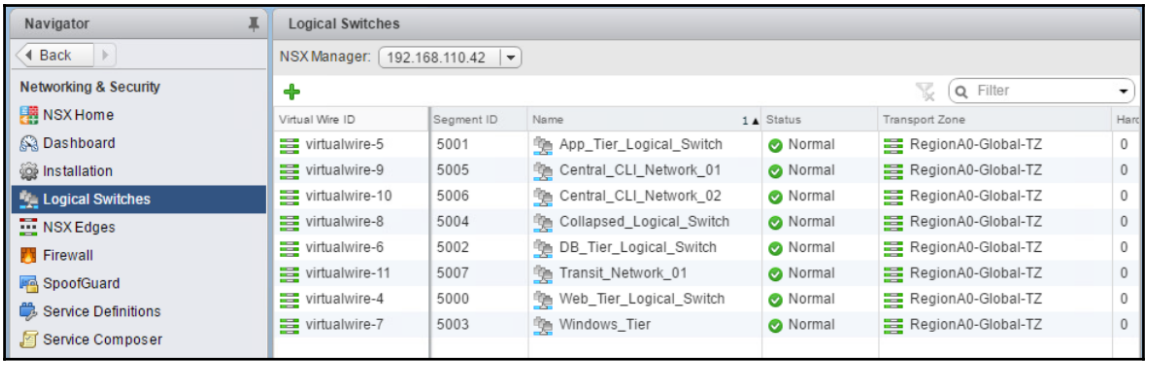
```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Thu Feb 15 17:50:06 2018 from 192.168.110.250
VMware NSX Controller 6.3.3 Build (7087285)
nsx-controller # show control-cluster status
Type                Status                                                  Since
--------------------------------------------------------------------------------
Join status:        Join complete                                           02/15 17:40:23
Majority status:    Connected to cluster majority                           02/15 17:40:06
Restart status:     This controller can be safely restarted                 02/15 17:40:31
Cluster ID:         968934f0-dfd8-40be-b67e-026948280c89
Node UUID:          d5a2a764-954b-4de9-aca7-810e04b9ed66

Role                Configured status   Active status
--------------------------------------------------------------------------------
api_provider        enabled             activated
persistence_server  enabled             activated
switch_manager      enabled             activated
logical_manager     enabled             activated
directory_server    enabled             activated
```

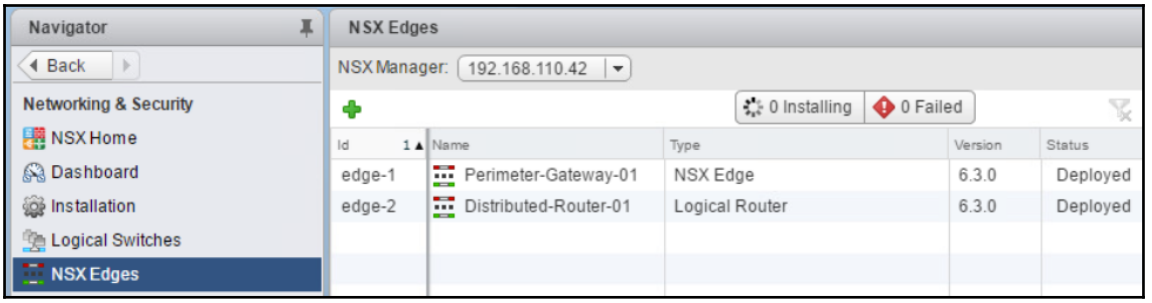

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Tools
Flow Monitoring
Activity Monitoring
Endpoint Monitoring
Installation
Management
Host Preparation
Logical Network Preparation
Service Deployments
NSX Manager: 192.168.110.42
NSX Component Installation on Hosts
Actions
Clusters & Hosts
Installation Status
Firewall
VXLAN
RegionA01-MGMT01
6.3.1.5124716
Enabled
Configured
esx-06a.corp.local
esx-05a.corp.local
esx-04a.corp.local
RegionA01-COMP01
esx-01a.corp.local
esx-02a.corp.local

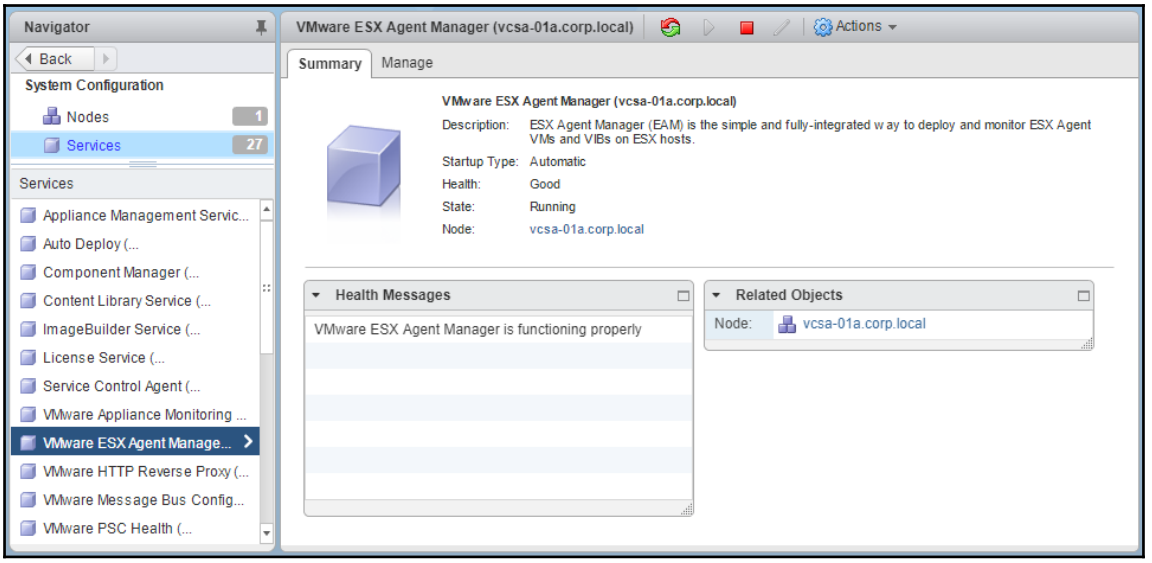

Installation
Management
Host Preparation
Logical Network Preparation
Service Deployments
NSX Manager: 192.168.110.42
VXLAN Transport
Segment ID
Transport Zones
VXLAN Port
4789
Change
Clusters & Hosts
Configuration Status
Switch
VLAN
MTU
VMKNic IP Addre
Teaming P
VTEP
RegionA01-MGMT01
Unconfigure
RegionA01...
0
1600
IP Pool
Fail Over
1
esx-06a.corp.local
Ready
vmk3: 19...
esx-05a.corp.local
esx-04a.corp.local
RegionA01-COMP01
esx-02a.corp.local
esx-01a.corp.local

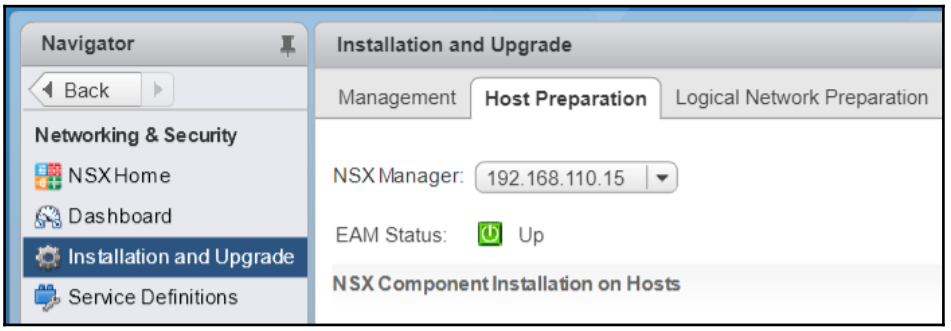

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Installation
Management
Host Preparation
Logical Network Preparation
Service Deployments
NSX Manager: 192.168.110.42
Network & Security Service Deployments
Network & security services are deployed on a set of clusters. Manage service deployments here by adding new services or deleting existing ones.
Filter
Service
Version
Service Status
Installation Status
Cluster
Datastore
Port Group
IP Address Ran
Trend Micro Deep Security
10.0
Up
Succeeded
Region...
Re...
ES...
guest-intr...
Guest Introspection
6.3.0.4886551
Up
Succeeded
Region...
Re...
ES...
guest-intr...

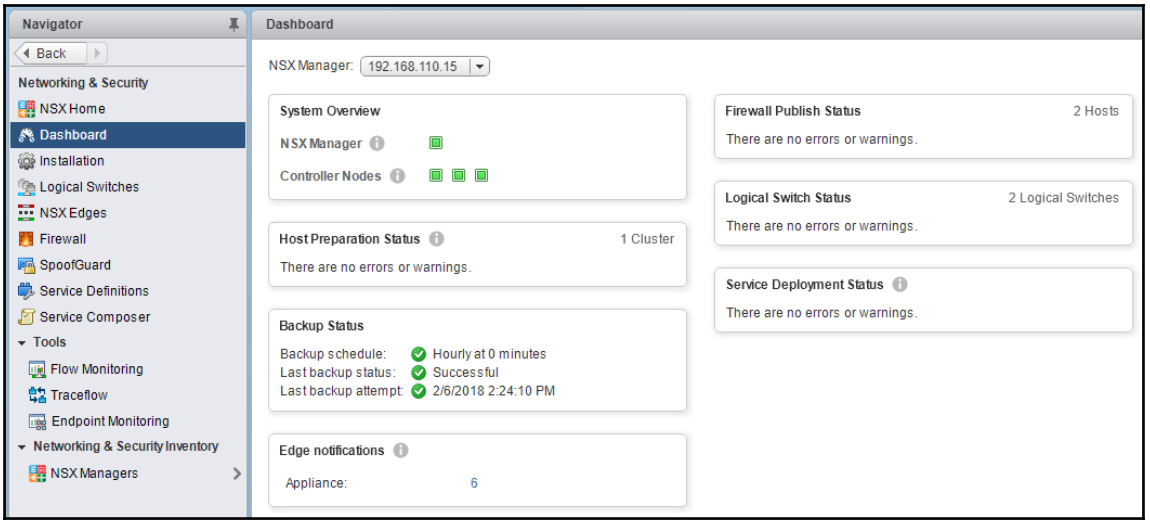

vmware vSphere Web Client
Updated at 8:37 PM
nsx-svc@vsphere.local
Help
Search
Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Tools
Flow Monitoring
Activity Monitoring
Endpoint Monitoring
Traceflow
Networking & Security Inventory
NSX Managers
Service Definitions
Services
Service Managers
Hardware Devices
NSX Manager: 192.168.110.15
Hardware Devices
Actions
Filter
Name
Management IP Address
Connectivity
BFD Enabled
Logical Switches
spline-01a
192.168.110.251
Up
0
1 Objects
Copy
Replication Cluster
Edit
Hosts
esx-02a.corp.local
esx-01a.corp.local
esx-03a.corp.local
BFD Configuration
Edit
Status
Enabled
Probe interval
300 ms

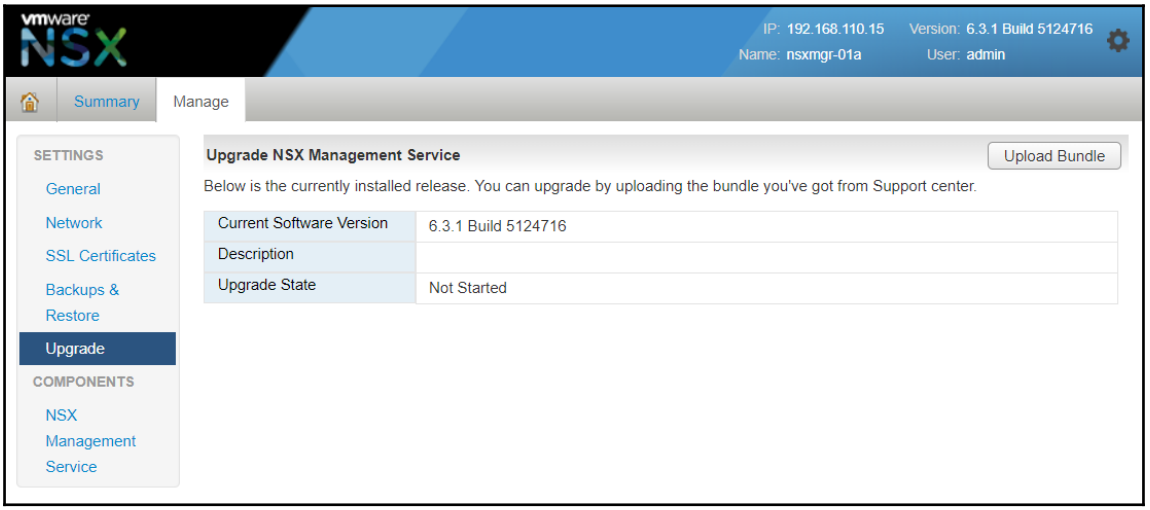

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Logical Switches
NSX Manager: 192.168.110.42
Filter
Virtual Wire ID
Segment ID
Name
Status
Transport Zone
virtualwire-5
5001
App_Tier_Logical_Switch
Normal
RegionA0-Global-TZ
virtualwire-9
5005
Central_CLI_Network_01
Normal
RegionA0-Global-TZ
virtualwire-10
5006
Central_CLI_Network_02
Normal
RegionA0-Global-TZ
virtualwire-8
5004
Collapsed_Logical_Switch
Normal
RegionA0-Global-TZ
virtualwire-6
5002
DB_Tier_Logical_Switch
Normal
RegionA0-Global-TZ
virtualwire-11
5007
Transit_Network_01
Normal
RegionA0-Global-TZ
virtualwire-4
5000
Web_Tier_Logical_Switch
Normal
RegionA0-Global-TZ
virtualwire-7
5003
Windows_Tier
Normal
RegionA0-Global-TZ

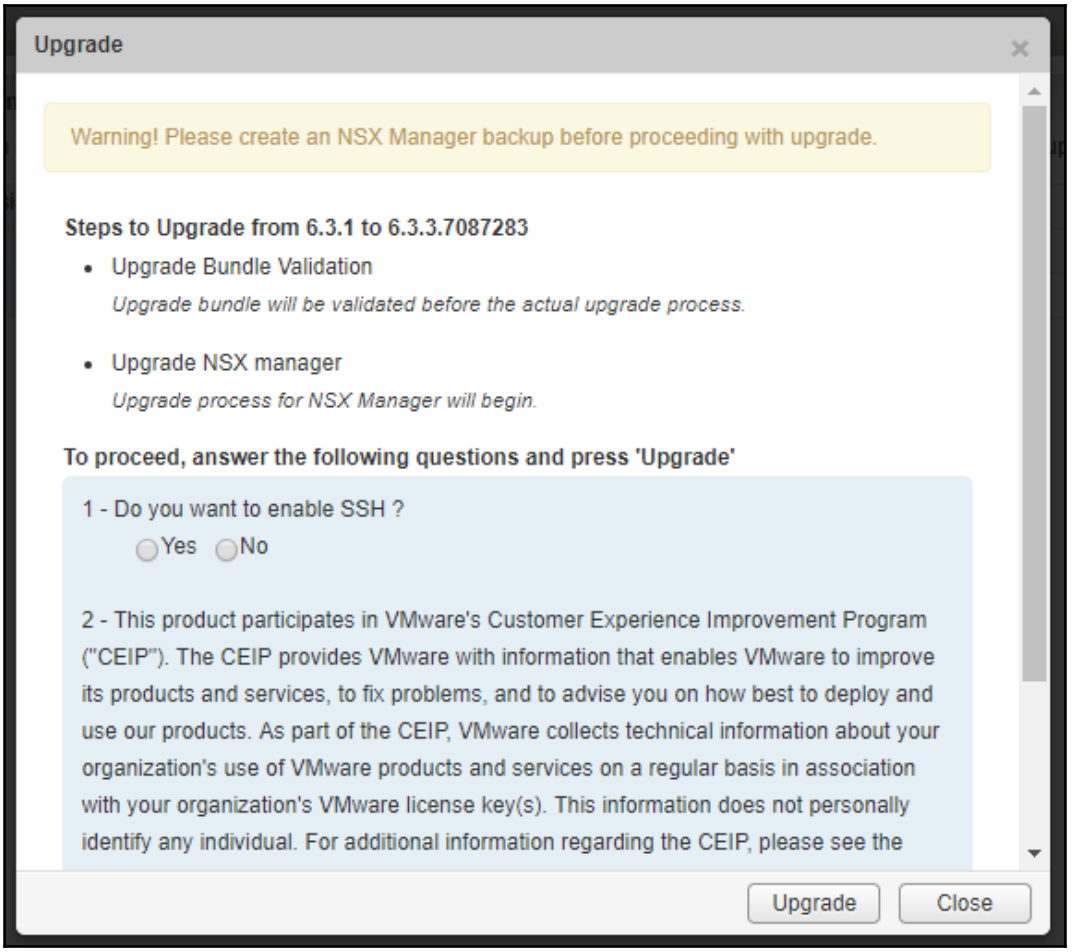

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
NSX Edges
NSX Manager: 192.168.110.42
0 Installing
0 Failed
Id
Name
Type
Version
Status
edge-1
Perimeter-Gateway-01
NSX Edge
6.3.0
Deployed
edge-2
Distributed-Router-01
Logical Router
6.3.0
Deployed

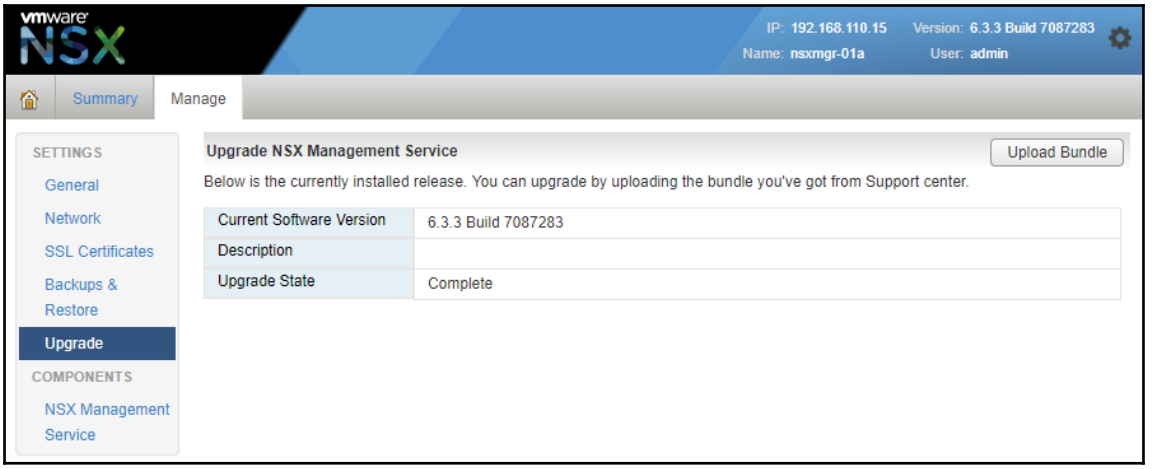

Navigator
Back
System Configuration
Nodes 1
Services 27
Services
Appliance Management Servic...
Auto Deploy (...
Component Manager (...
Content Library Service (...
ImageBuilder Service (...
License Service (...
Service Control Agent (...
VMware Appliance Monitoring ...
VMware ESX Agent Manage...
VMware HTTP Reverse Proxy (...
VMware Message Bus Config...
VMware PSC Health (...
VMware ESX Agent Manager (vcsa-01a.corp.local)
Actions
Summary
Manage
VMware ESX Agent Manager (vcsa-01a.corp.local)
Description: ESX Agent Manager (EAM) is the simple and fully-integrated w ay to deploy and monitor ESX Agent VMs and VIBs on ESX hosts.
Startup Type: Automatic
Health: Good
State: Running
Node: vcsa-01a.corp.local
Health Messages
VMware ESX Agent Manager is functioning properly
Related Objects
Node: vcsa-01a.corp.local

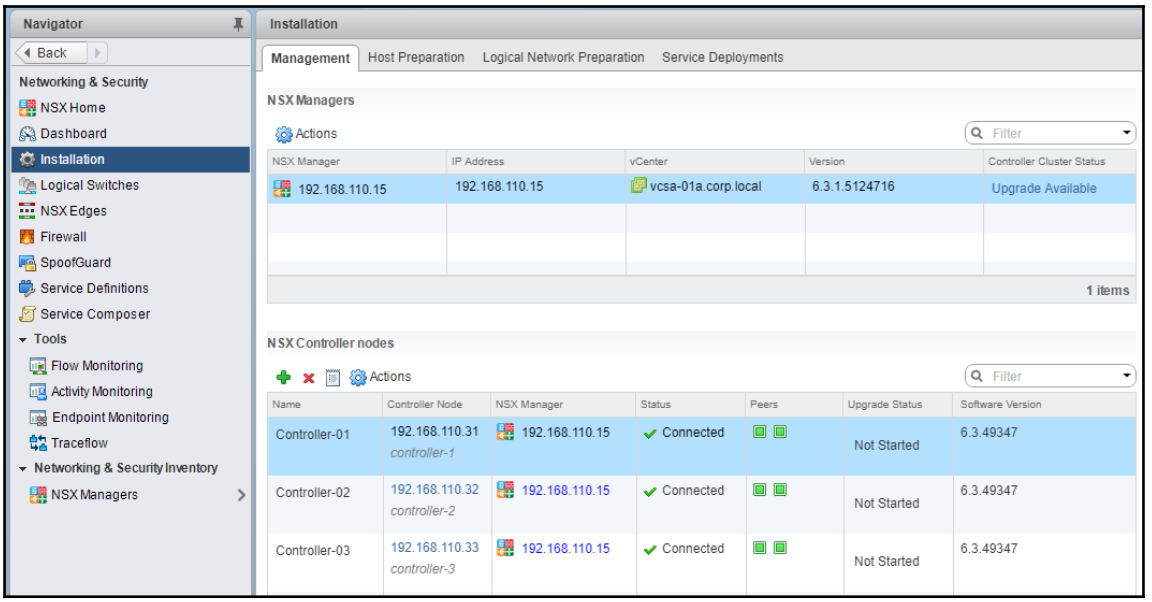

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation and Upgrade
Service Definitions
Installation and Upgrade
Management
Host Preparation
Logical Network Preparation
NSX Manager: 192.168.110.15
EAM Status: Up
NSX Component Installation on Hosts

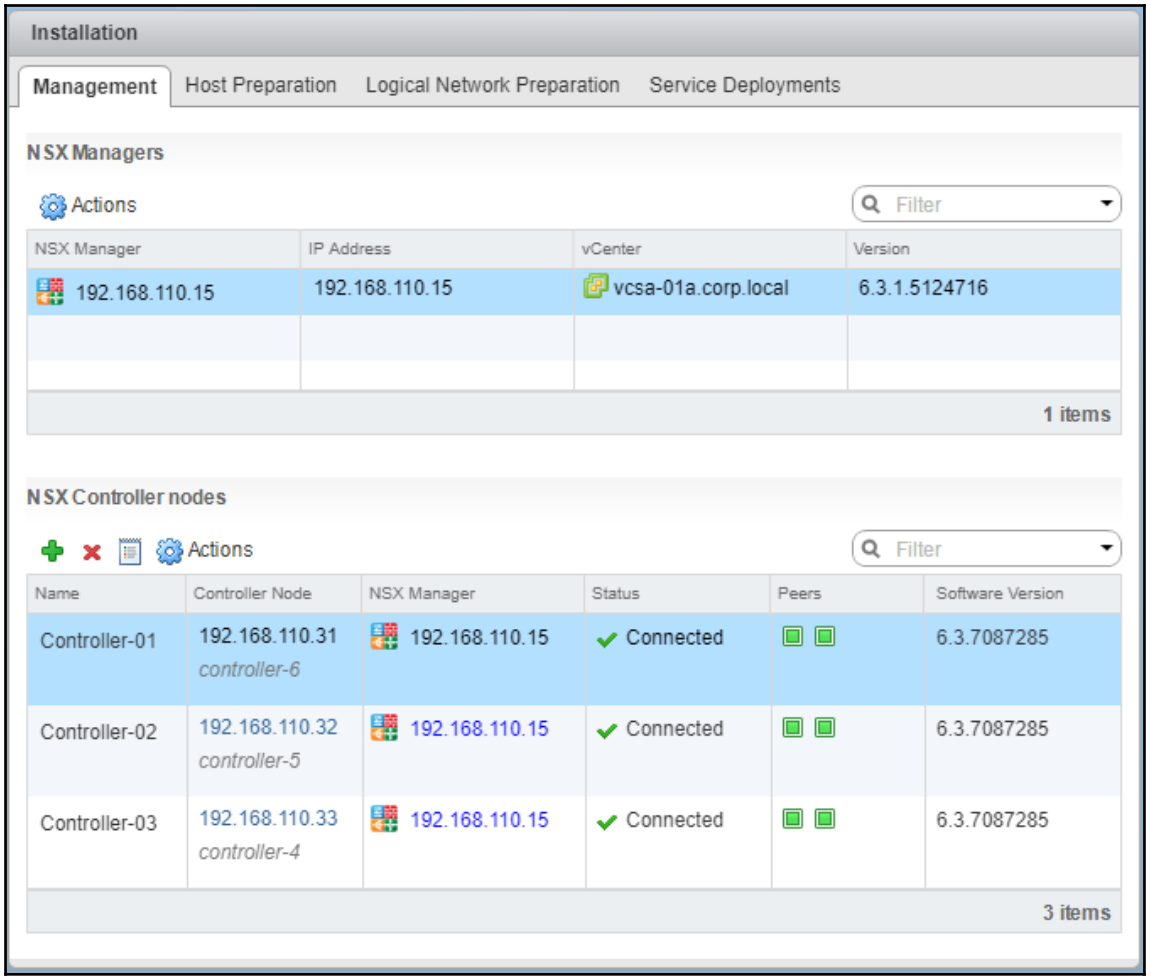

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Tools
Flow Monitoring
Traceflow
Endpoint Monitoring
Networking & Security Inventory
NSX Managers
Dashboard
NSX Manager: 192.168.110.15
System Overview
NSX Manager
Controller Nodes
Host Preparation Status
1 Cluster
There are no errors or warnings.
Backup Status
Backup schedule: Hourly at 0 minutes
Last backup status: Successful
Last backup attempt: 2/6/2018 2:24:10 PM
Edge notifications
Appliance: 6
Firewall Publish Status
2 Hosts
There are no errors or warnings.
Logical Switch Status
2 Logical Switches
There are no errors or warnings.
Service Deployment Status
There are no errors or warnings.

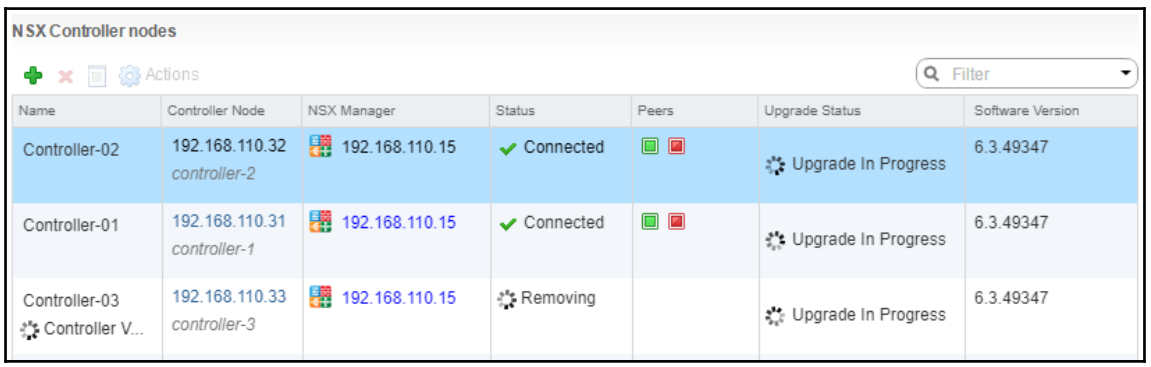

vmware NSX
IP: 192.168.110.15
Version: 6.3.1 Build 5124716
Name: nsxmgr-01a
User: admin
Summary
Manage
SETTINGS
General
Network
SSL Certificates
Backups & Restore
Upgrade
COMPONENTS
NSX Management Service
Upgrade NSX Management Service
Upload Bundle
Below is the currently installed release. You can upgrade by uploading the bundle you've got from Support center.
Current Software Version
6.3.1 Build 5124716
Description
Upgrade State
Not Started

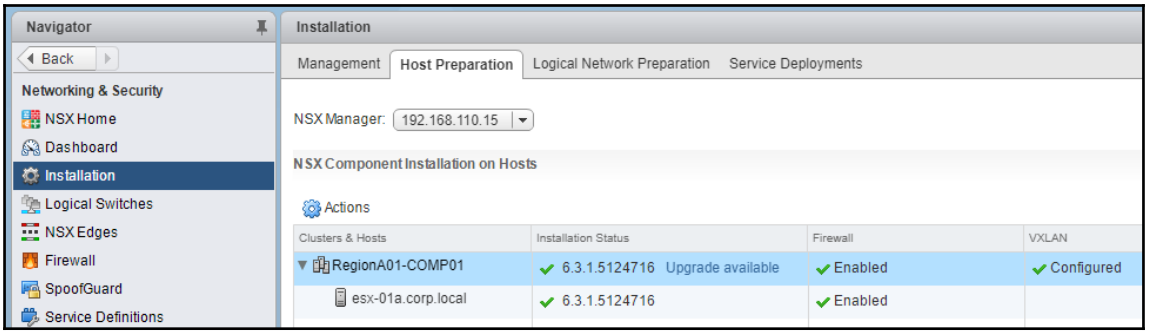

Upgrade
Warning! Please create an NSX Manager backup before proceeding with upgrade.
Steps to Upgrade from 6.3.1 to 6.3.3.7087283
Upgrade Bundle Validation
Upgrade bundle will be validated before the actual upgrade process.
Upgrade NSX manager
Upgrade process for NSX Manager will begin.
To proceed, answer the following questions and press 'Upgrade'
1 - Do you want to enable SSH ?
Yes
No
2 - This product participates in VMware's Customer Experience Improvement Program ("CEIP"). The CEIP provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products. As part of the CEIP, VMware collects technical information about your organization's use of VMware products and services on a regular basis in association with your organization's VMware license key(s). This information does not personally identify any individual. For additional information regarding the CEIP, please see the
Upgrade
Close

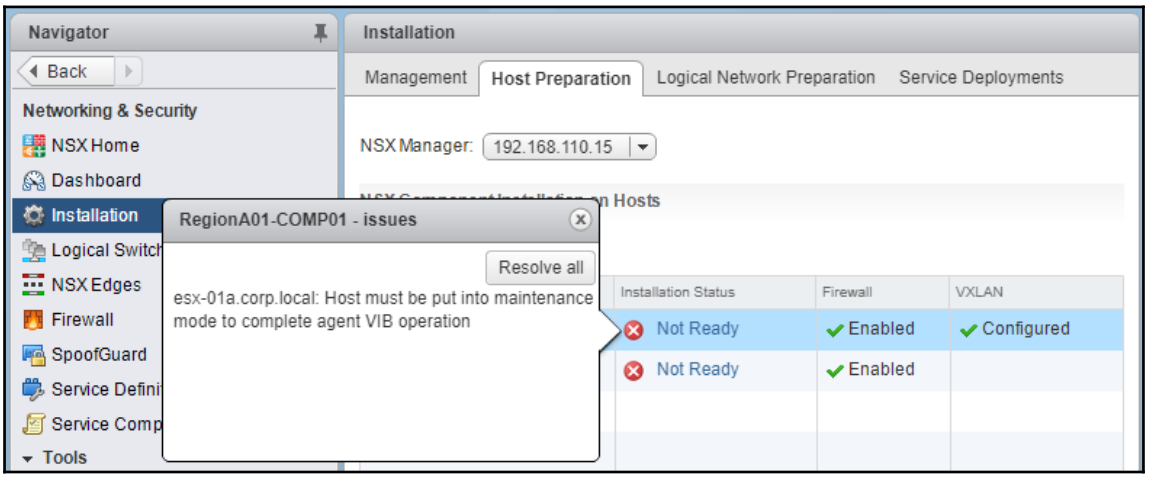

vmware NSX
IP: 192.168.110.15
Version: 6.3.3 Build 7087283
Name: nsxmgr-01a
User: admin
Summary
Manage
SETTINGS
General
Network
SSL Certificates
Backups & Restore
Upgrade
COMPONENTS
NSX Management Service
Upgrade NSX Management Service
Upload Bundle
Below is the currently installed release. You can upgrade by uploading the bundle you've got from Support center.
Current Software Version
6.3.3 Build 7087283
Description
Upgrade State
Complete

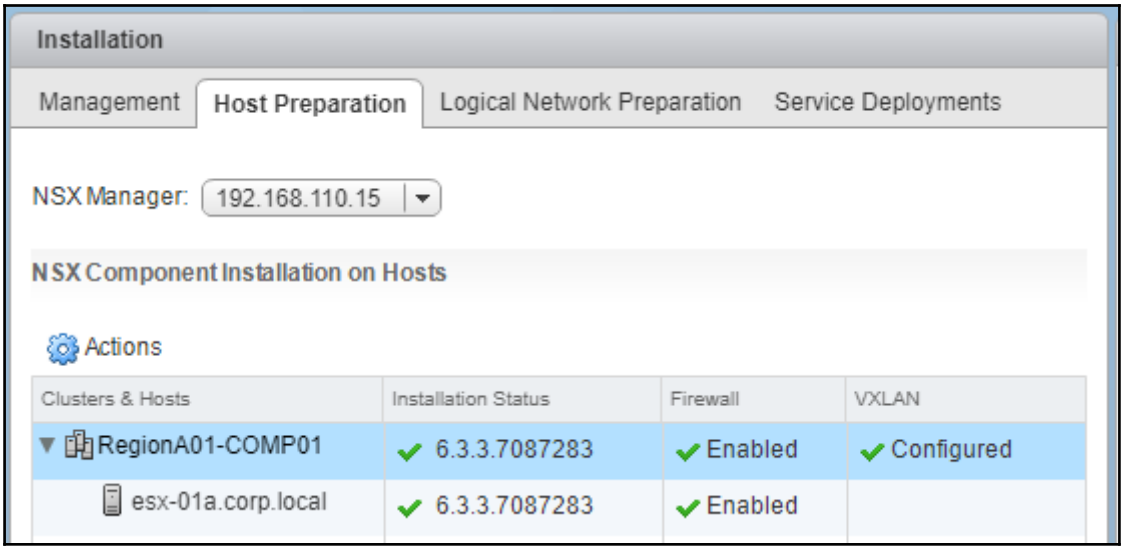

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Tools
Flow Monitoring
Activity Monitoring
Endpoint Monitoring
Traceflow
Networking & Security Inventory
NSX Managers
Installation
Management
Host Preparation
Logical Network Preparation
Service Deployments
NSX Managers
Actions
Filter
NSX Manager
IP Address
vCenter
Version
Controller Cluster Status
192.168.110.15
192.168.110.15
vcsa-01a.corp.local
6.3.1.5124716
Upgrade Available
1 items
NSX Controller nodes
Actions
Filter
Name
Controller Node
NSX Manager
Status
Peers
Upgrade Status
Software Version
Controller-01
192.168.110.31
controller-1
192.168.110.15
Connected
Not Started
6.3.49347
Controller-02
192.168.110.32
controller-2
192.168.110.15
Connected
Not Started
6.3.49347
Controller-03
192.168.110.33
controller-3
192.168.110.15
Connected
Not Started
6.3.49347

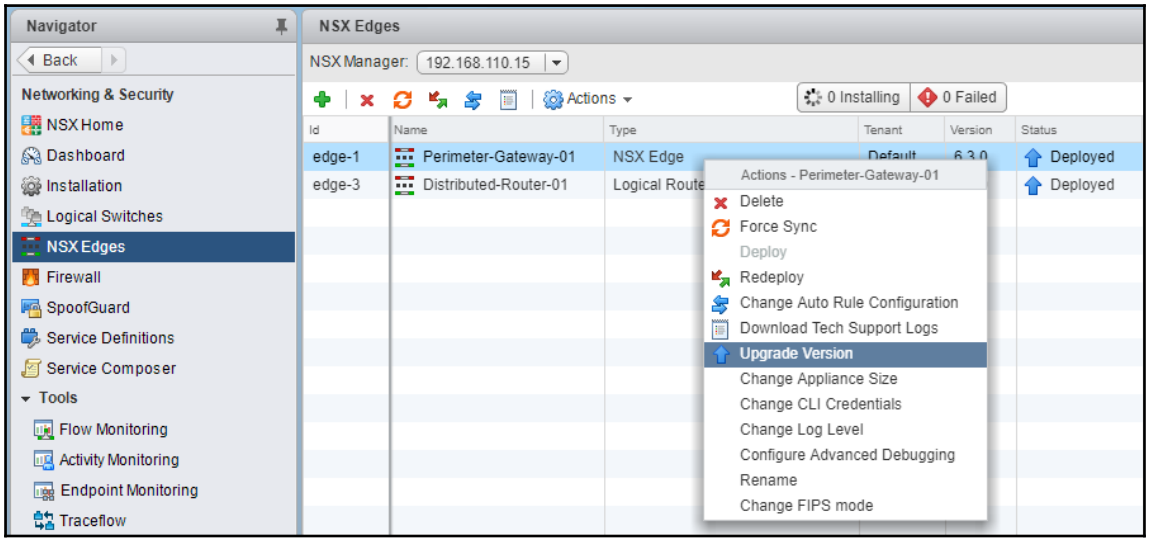

Installation
Management
Host Preparation
Logical Network Preparation
Service Deployments
NSX Managers
Actions
Filter
NSX Manager
IP Address
vCenter
Version
192.168.110.15
192.168.110.15
vcsa-01a.corp.local
6.3.1.5124716
1 items
NSX Controller nodes
Actions
Filter
Name
Controller Node
NSX Manager
Status
Peers
Software Version
Controller-01
192.168.110.31
controller-6
192.168.110.15
Connected
6.3.7087285
Controller-02
192.168.110.32
controller-5
192.168.110.15
Connected
6.3.7087285
Controller-03
192.168.110.33
controller-4
192.168.110.15
Connected
6.3.7087285
3 items

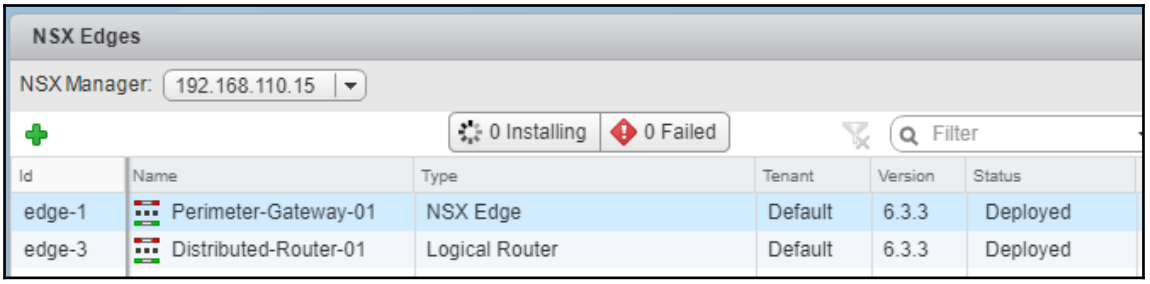

NSX Controller nodes
Actions
Filter
Name
Controller Node
NSX Manager
Status
Peers
Upgrade Status
Software Version
Controller-02
192.168.110.32
controller-2
192.168.110.15
Connected
Upgrade In Progress
6.3.49347
Controller-01
192.168.110.31
controller-1
192.168.110.15
Connected
Upgrade In Progress
6.3.49347
Controller-03
Controller V...
192.168.110.33
controller-3
192.168.110.15
Removing
Upgrade In Progress
6.3.49347

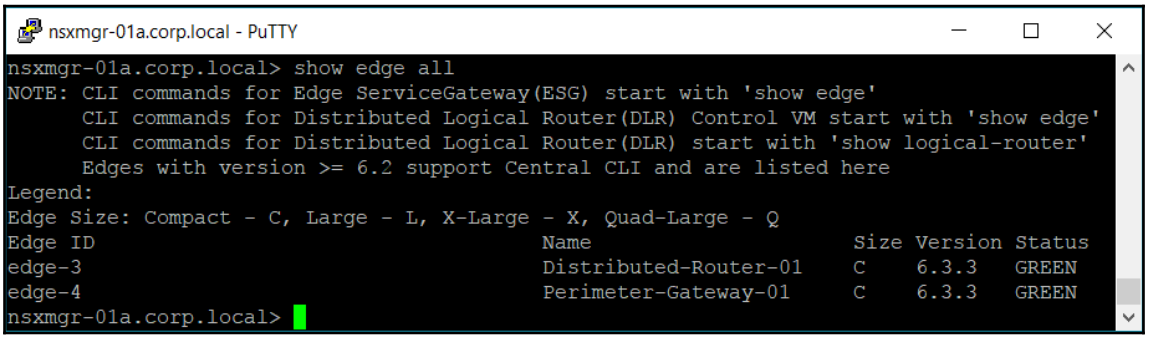

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Installation
Management
Host Preparation
Logical Network Preparation
Service Deployments
NSX Manager:
192.168.110.15
NSX Component Installation on Hosts
Actions
Clusters & Hosts
Installation Status
Firewall
VXLAN
RegionA01-COMP01
6.3.1.5124716
Upgrade available
Enabled
Configured
esx-01a.corp.local
6.3.1.5124716
Enabled

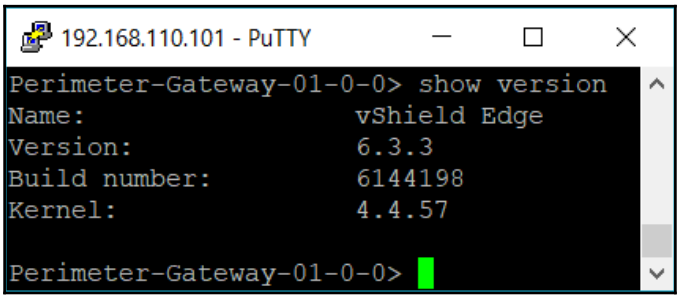

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switch
NSX Edges
Firewall
SpoofGuard
Service Defini
Service Comp
Tools
Installation
Management
Host Preparation
Logical Network Preparation
Service Deployments
NSX Manager:
192.168.110.15
RegionA01-COMP01 - issues
Resolve all
esx-01a.corp.local: Host must be put into maintenance mode to complete agent VIB operation
Installation Status
Firewall
VXLAN
Not Ready
Enabled
Configured
Not Ready
Enabled

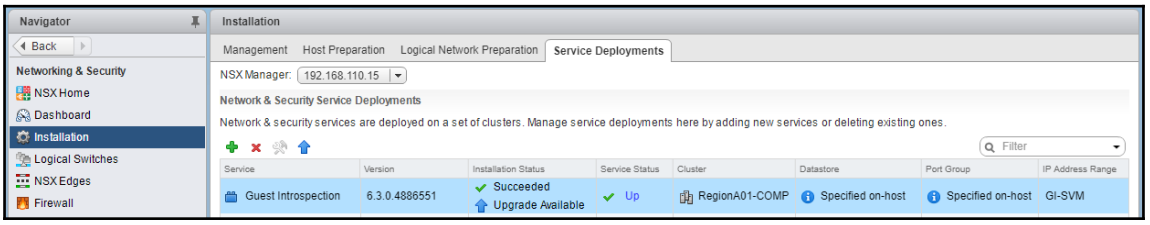

Installation
Management
Host Preparation
Logical Network Preparation
Service Deployments
NSX Manager: 192.168.110.15
NSX Component Installation on Hosts
Actions
Clusters & Hosts
Installation Status
Firewall
VXLAN
RegionA01-COMP01
6.3.3.7087283
Enabled
Configured
esx-01a.corp.local
6.3.3.7087283
Enabled

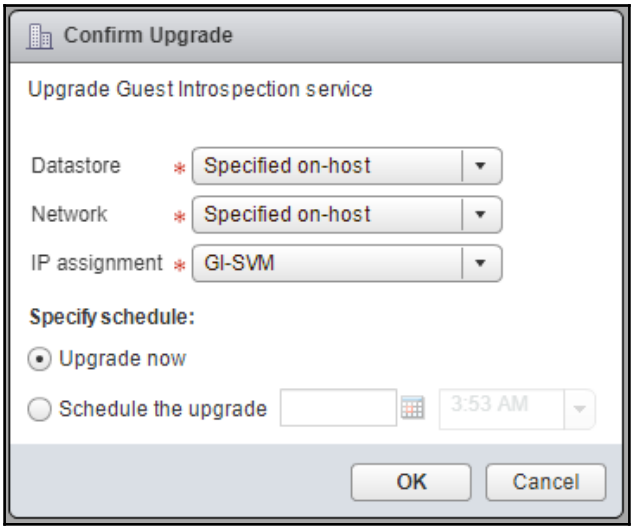

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Tools
Flow Monitoring
Activity Monitoring
Endpoint Monitoring
Traceflow
NSX Edges
NSX Manager: 192.168.110.15
Actions
0 Installing
0 Failed
Id
Name
Type
Tenant
Version
Status
edge-1
Perimeter-Gateway-01
NSX Edge
Deployed
edge-3
Distributed-Router-01
Logical Route
Deployed
Actions - Perimeter-Gateway-01
Delete
Force Sync
Deploy
Redeploy
Change Auto Rule Configuration
Download Tech Support Logs
Upgrade Version
Change Appliance Size
Change CLI Credentials
Change Log Level
Configure Advanced Debugging
Rename
Change FIPS mode

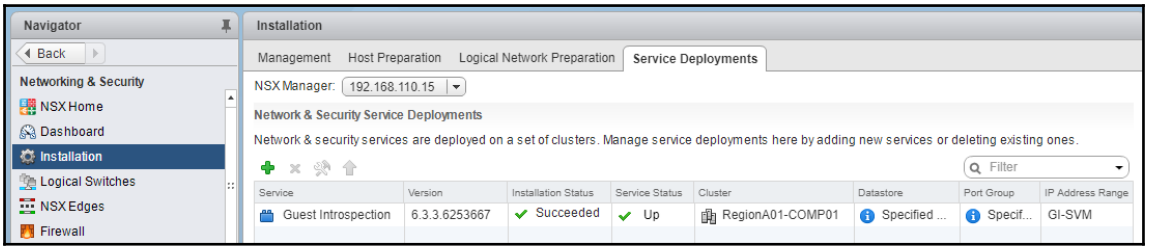

NSX Edges
NSX Manager: 192.168.110.15
0 Installing
0 Failed
Filter
Id
Name
Type
Tenant
Version
Status
edge-1
Perimeter-Gateway-01
NSX Edge
Default
6.3.3
Deployed
edge-3
Distributed-Router-01
Logical Router
Default
6.3.3
Deployed

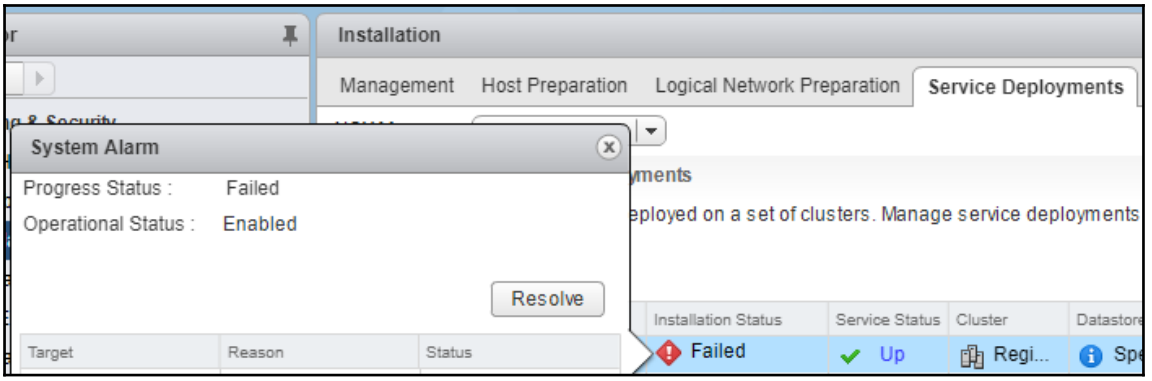

nsxmgr-01a.corp.local - PuTTY
nsxmgr-01a.corp.local> show edge all
NOTE: CLI commands for Edge ServiceGateway(ESG) start with 'show edge'
CLI commands for Distributed Logical Router(DLR) Control VM start with 'show edge'
CLI commands for Distributed Logical Router(DLR) start with 'show logical-router'
Edges with version >= 6.2 support Central CLI and are listed here
Legend:
Edge Size: Compact - C, Large - L, X-Large - X, Quad-Large - Q
Edge ID Name Size Version Status
edge-3 Distributed-Router-01 C 6.3.3 GREEN
edge-4 Perimeter-Gateway-01 C 6.3.3 GREEN
nsxmgr-01a.corp.local>


192.168.110.101 - PuTTY
Perimeter-Gateway-01-0-0> show version
Name: vShield Edge
Version: 6.3.3
Build number: 6144198
Kernel: 4.4.57
Perimeter-Gateway-01-0-0>

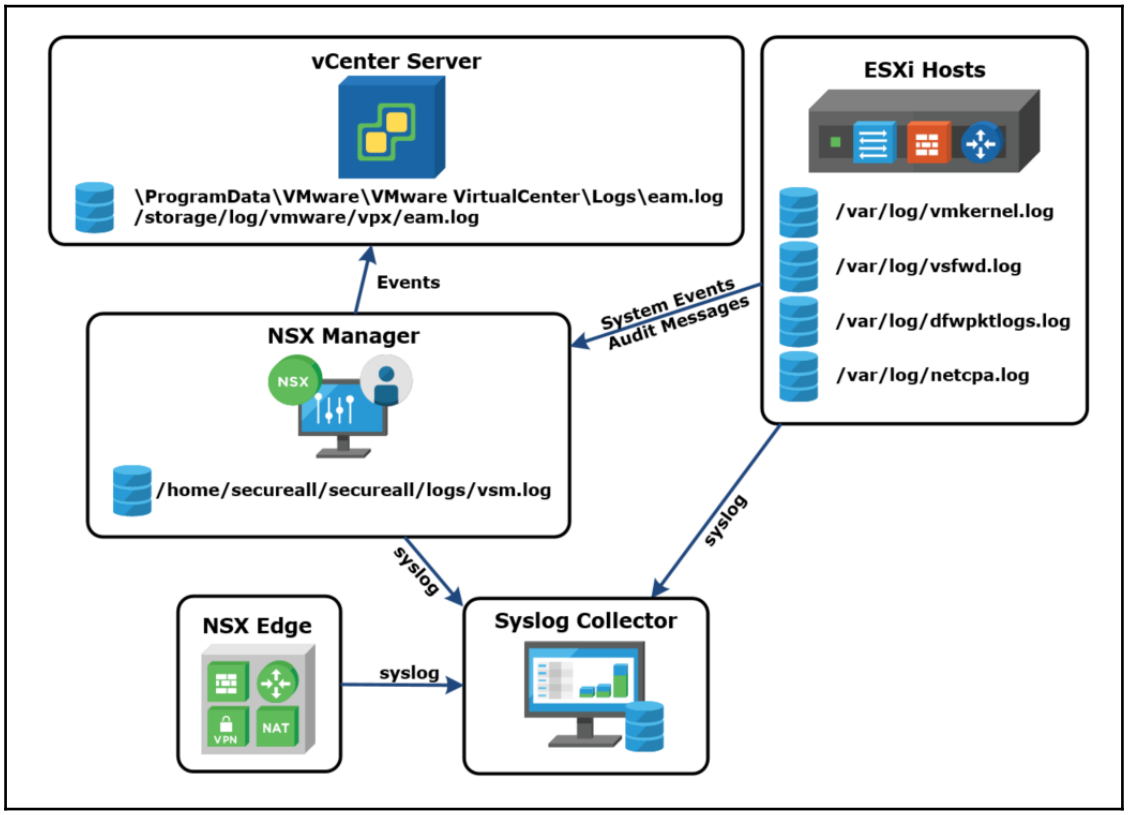

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
Installation
Management
Host Preparation
Logical Network Preparation
Service Deployments
NSX Manager: 192.168.110.15
Network & Security Service Deployments
Network & security services are deployed on a set of clusters. Manage service deployments here by adding new services or deleting existing ones.
Filter
Service
Version
Installation Status
Service Status
Cluster
Datastore
Port Group
IP Address Range
Guest Introspection
6.3.0.4886551
Succeeded
Upgrade Available
Up
RegionA01-COMP
Specified on-host
Specified on-host
GI-SVM

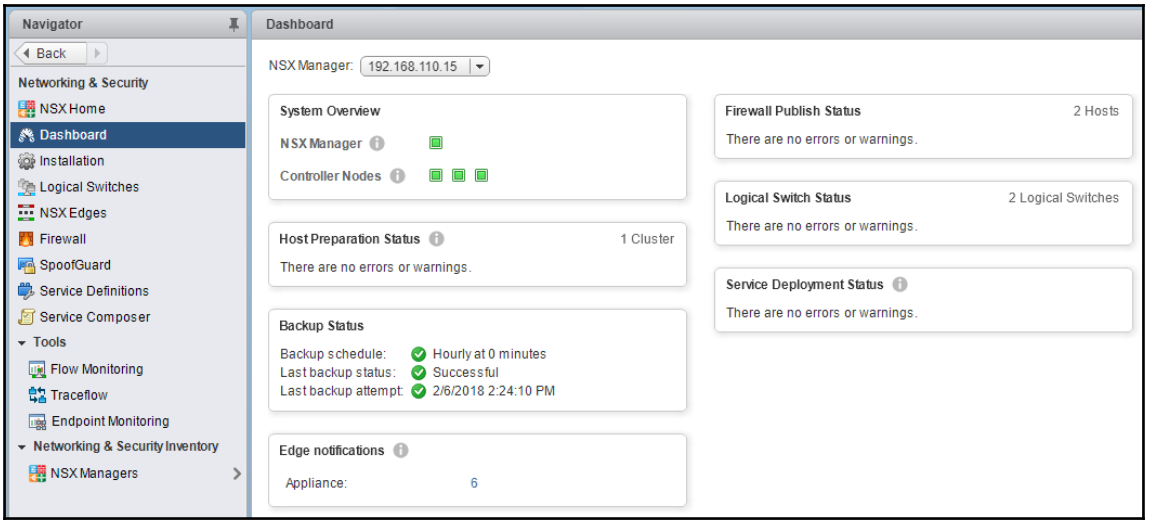

Confirm Upgrade
Upgrade Guest Introspection service
Datastore
Specified on-host
Network
Specified on-host
IP assignment
GI-SVM
Specify schedule:
Upgrade now
Schedule the upgrade
3:53 AM
OK
Cancel

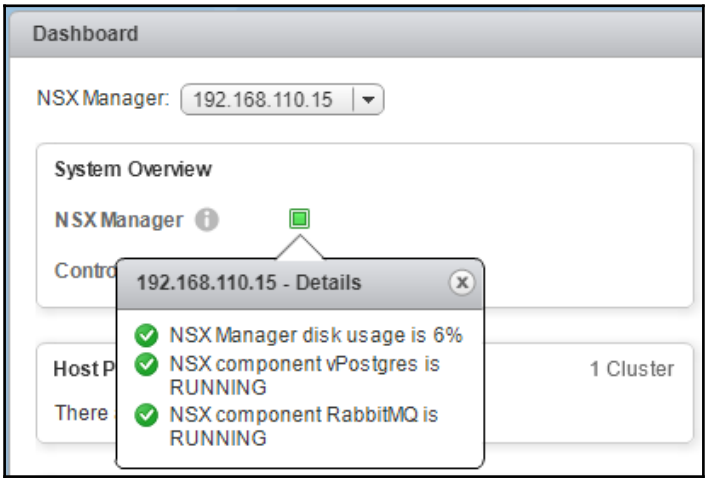

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
Installation
Management
Host Preparation
Logical Network Preparation
Service Deployments
NSX Manager:
192.168.110.15
Network & Security Service Deployments
Network & security services are deployed on a set of clusters. Manage service deployments here by adding new services or deleting existing ones.
Filter
Service
Version
Installation Status
Service Status
Cluster
Datastore
Port Group
IP Address Range
Guest Introspection
6.3.3.6253667
Succeeded
Up
RegionA01-COMP01
Specified ...
Specif...
GI-SVM

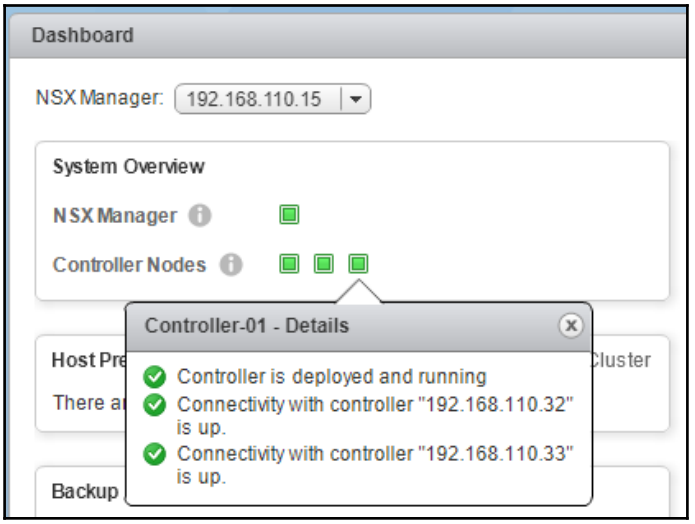

Installation
Management
Host Preparation
Logical Network Preparation
Service Deployments
System Alarm
Progress Status :
Failed
Operational Status :
Enabled
Resolve
Target
Reason
Status
Installation Status
Service Status
Cluster
Failed
Up
Regi...

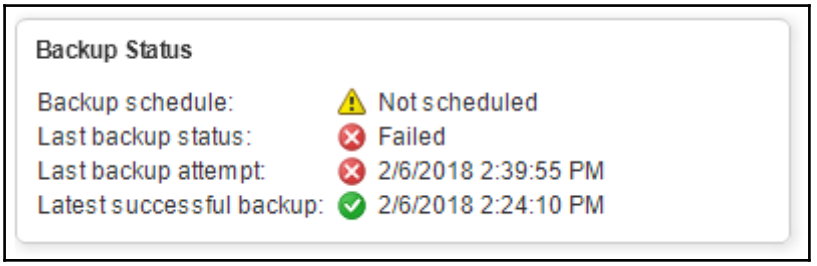
Chapter 11: Managing and Monitoring VMware NSX Platform

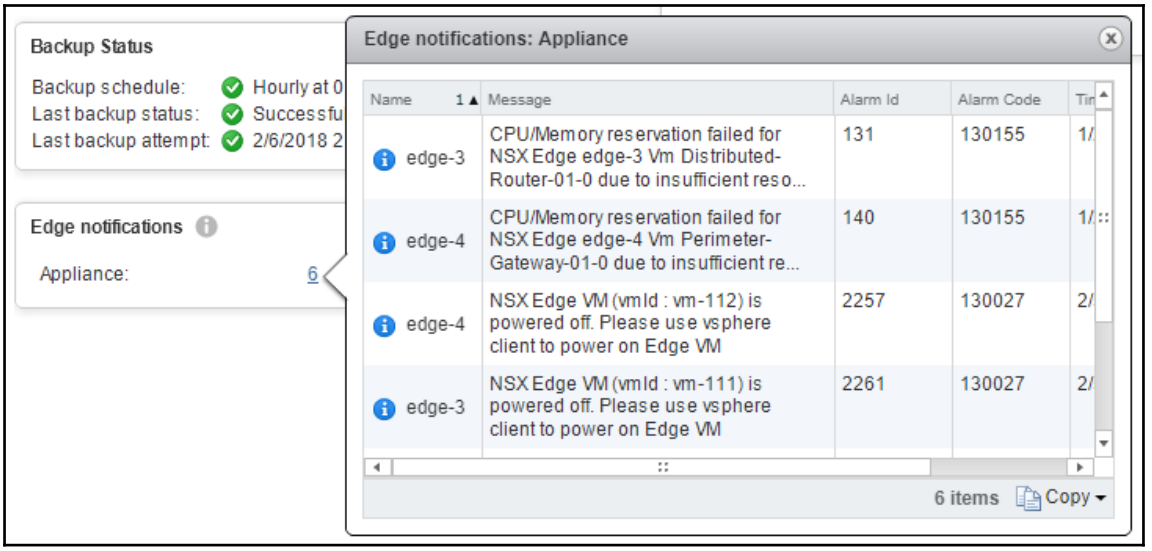


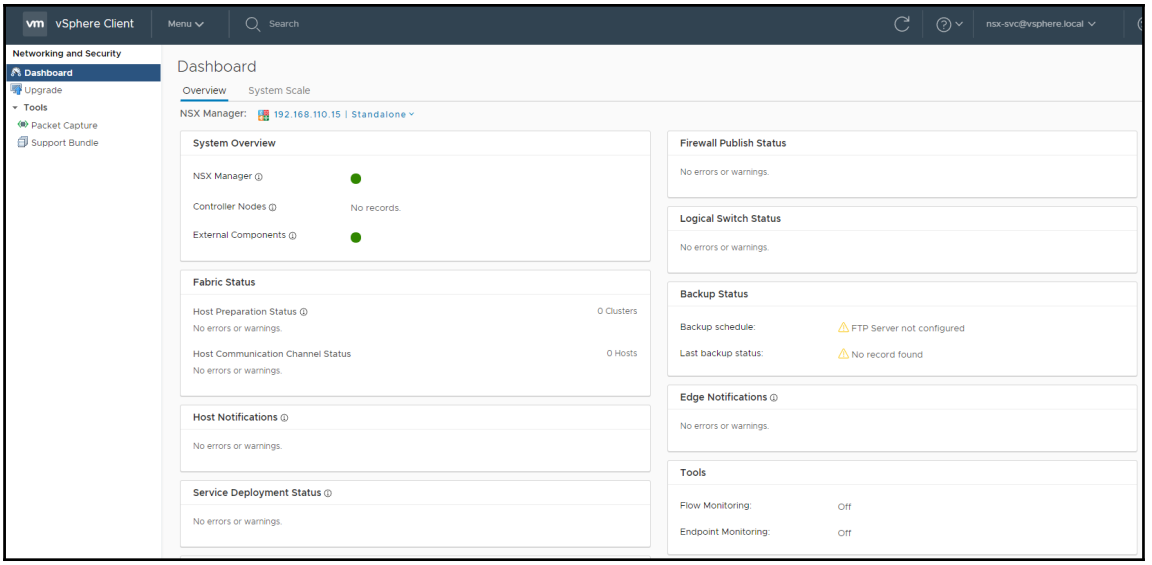

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Tools
Flow Monitoring
Traceflow
Endpoint Monitoring
Networking & Security Inventory
NSX Managers
Dashboard
NSX Manager: 192.168.110.15
System Overview
NSX Manager
Controller Nodes
Host Preparation Status
1 Cluster
There are no errors or warnings.
Backup Status
Backup schedule: Hourly at 0 minutes
Last backup status: Successful
Last backup attempt: 2/6/2018 2:24:10 PM
Edge notifications
Appliance: 6
Firewall Publish Status
2 Hosts
There are no errors or warnings.
Logical Switch Status
2 Logical Switches
There are no errors or warnings.
Service Deployment Status
There are no errors or warnings.

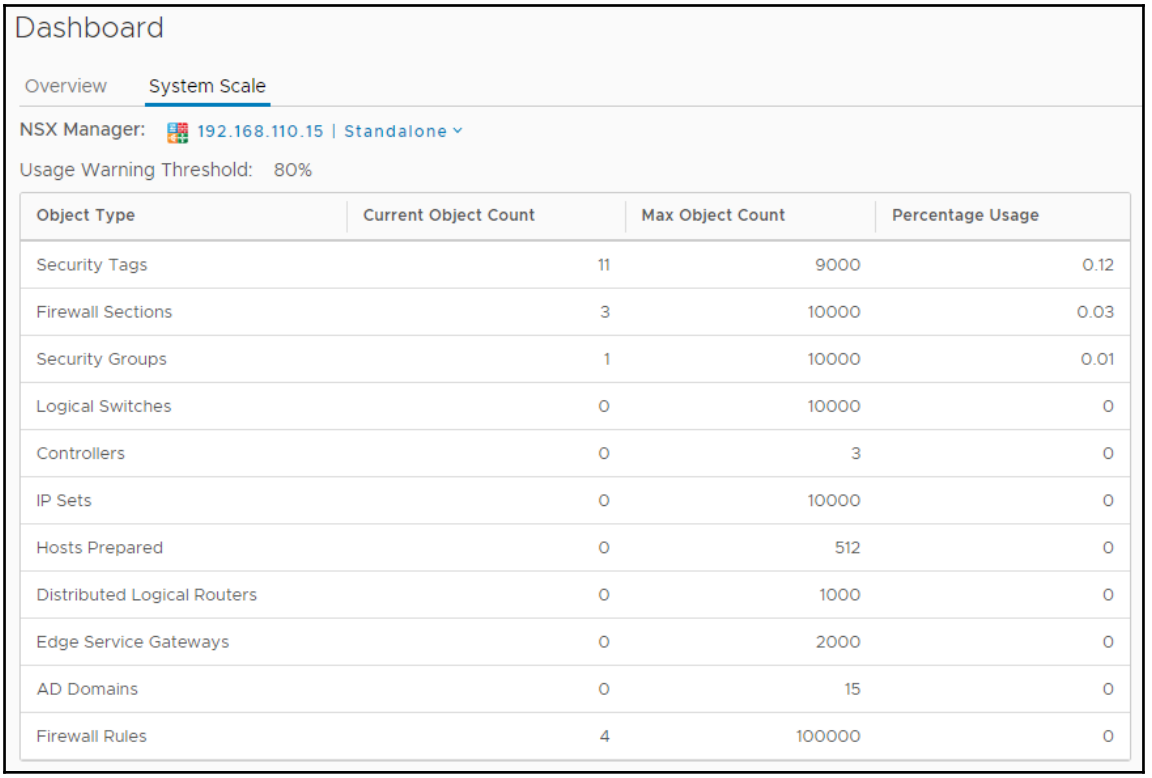

Dashboard
NSX Manager: 192.168.110.15
System Overview
NSX Manager
192.168.110.15 - Details
NSX Manager disk usage is 6%
NSX component vPostgres is RUNNING
NSX component RabbitMQ is RUNNING
1 Cluster


Dashboard
NSX Manager: 192.168.110.15
System Overview
NSX Manager
Controller Nodes
Controller-01 - Details
Controller is deployed and running
Connectivity with controller "192.168.110.32" is up.
Connectivity with controller "192.168.110.33" is up.
Backup

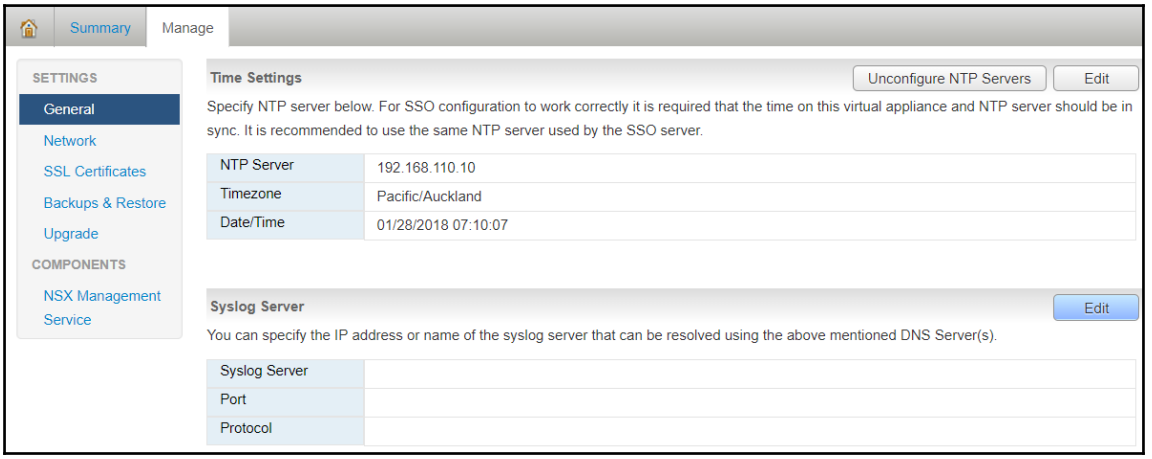

Backup Status
Backup schedule: Not scheduled
Last backup status: Failed
Last backup attempt: 2/6/2018 2:39:55 PM
Latest successful backup: 2/6/2018 2:24:10 PM

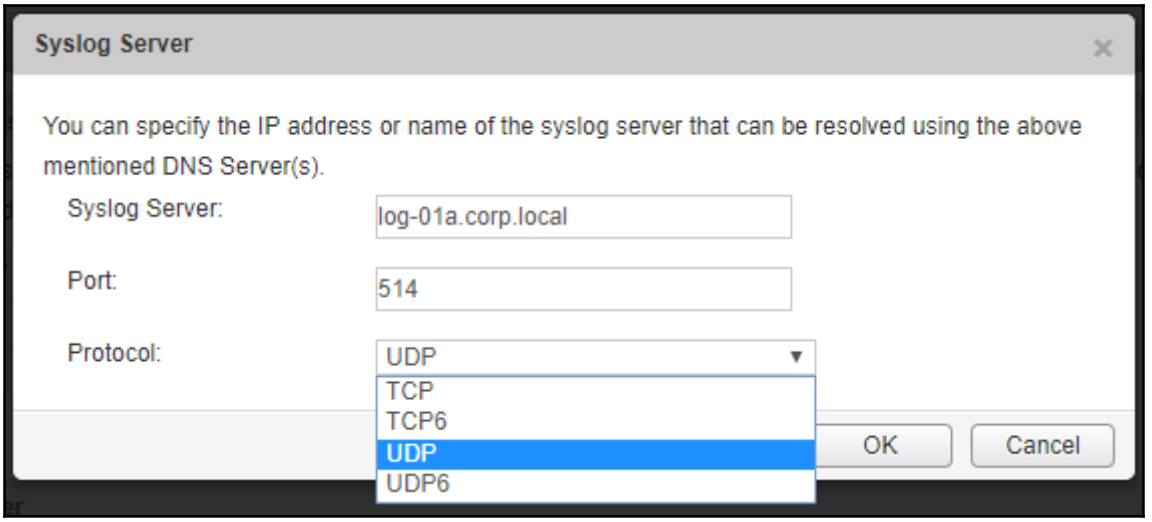

Backup Status
Backup schedule:
Hourly at 0
Last backup status:
Successfu
Last backup attempt:
2/6/2018 2
Edge notifications
Appliance:
6
Edge notifications: Appliance
Name
1
Message
Alarm Id
Alarm Code
edge-3
CPU/Memory reservation failed for NSX Edge edge-3 Vm Distributed-Router-01-0 due to insufficient reso...
131
130155
edge-4
CPU/Memory reservation failed for NSX Edge edge-4 Vm Perimeter-Gateway-01-0 due to insufficient re...
140
130155
edge-4
NSX Edge VM (vmId : vm-112) is powered off. Please use vsphere client to power on Edge VM
2257
130027
edge-3
NSX Edge VM (vmId : vm-111) is powered off. Please use vsphere client to power on Edge VM
2261
130027
6 items
Copy

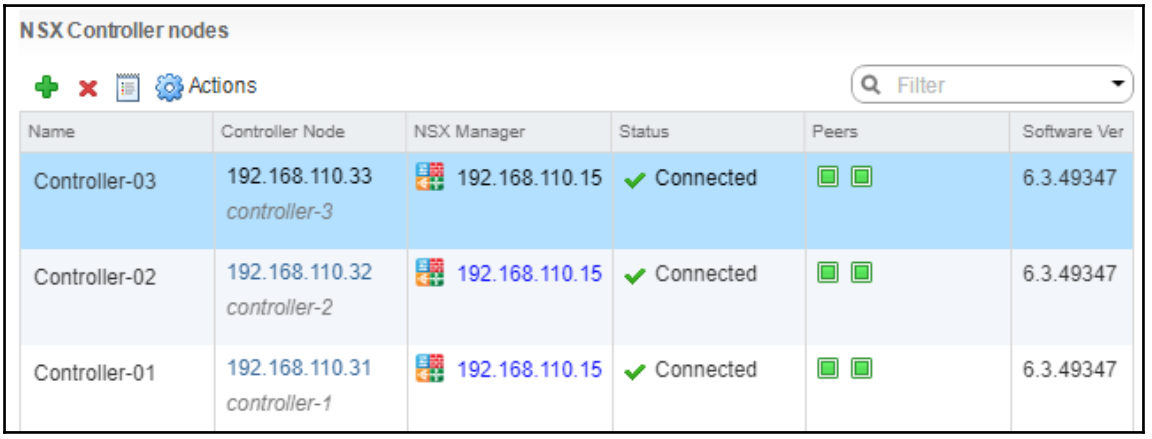

vSphere Client
Menu
Search
nsx-svc@vsphere.local
Networking and Security
Dashboard
Upgrade
Tools
Packet Capture
Support Bundle
Dashboard
Overview
System Scale
NSX Manager:
192.168.110.15 | Standalone
System Overview
NSX Manager
Controller Nodes
No records.
External Components
Fabric Status
Host Preparation Status
0 Clusters
No errors or warnings.
Host Communication Channel Status
0 Hosts
No errors or warnings.
Host Notifications
No errors or warnings.
Service Deployment Status
No errors or warnings.
Firewall Publish Status
No errors or warnings.
Logical Switch Status
No errors or warnings.
Backup Status
Backup schedule:
FTP Server not configured
Last backup status:
No record found
Edge Notifications
No errors or warnings.
Tools
Flow Monitoring:
Off
Endpoint Monitoring:
Off

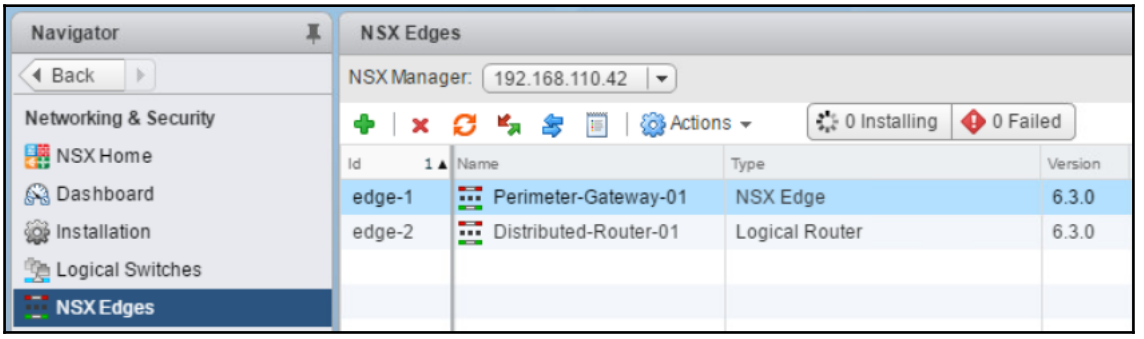


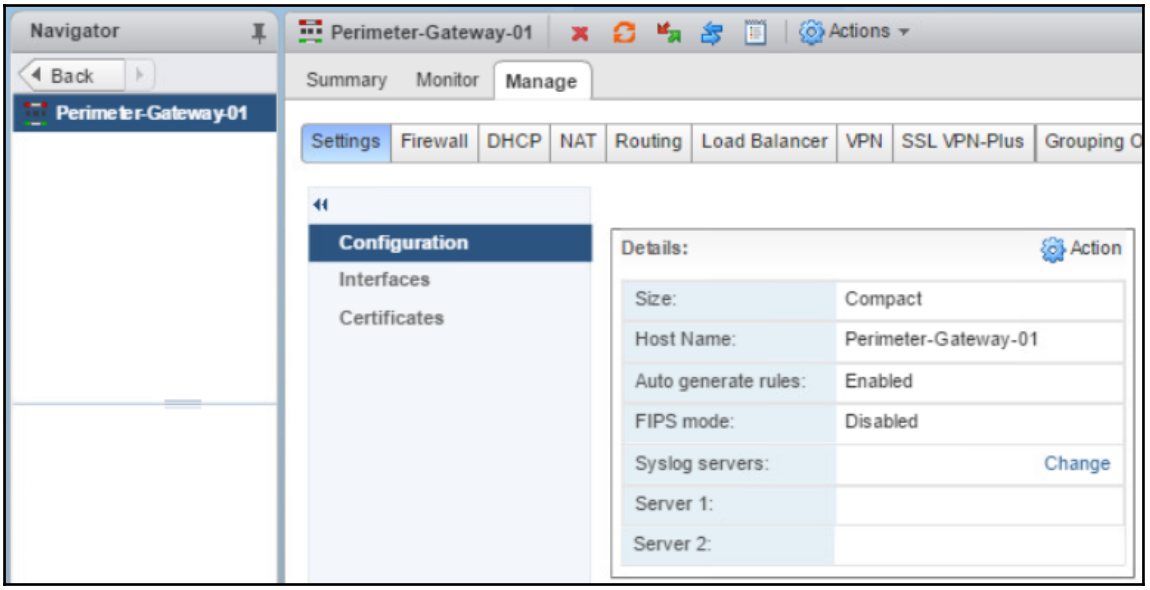
Object Type	Current Object Count	Max Object Count	Percentage Usage
Security Tags	11	9000	0.12
Firewall Sections	3	10000	0.03
Security Groups	1	10000	0.01
Logical Switches	0	10000	0
Controllers	0	3	0
IP Sets	0	10000	0
Hosts Prepared	0	512	0
Distributed Logical Routers	0	1000	0
Edge Service Gateways	0	2000	0
AD Domains	0	15	0
Firewall Rules	4	100000	0

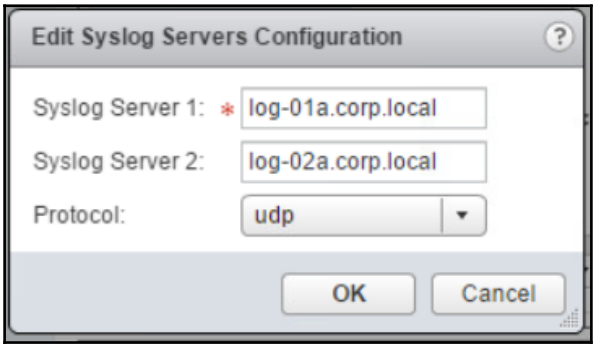


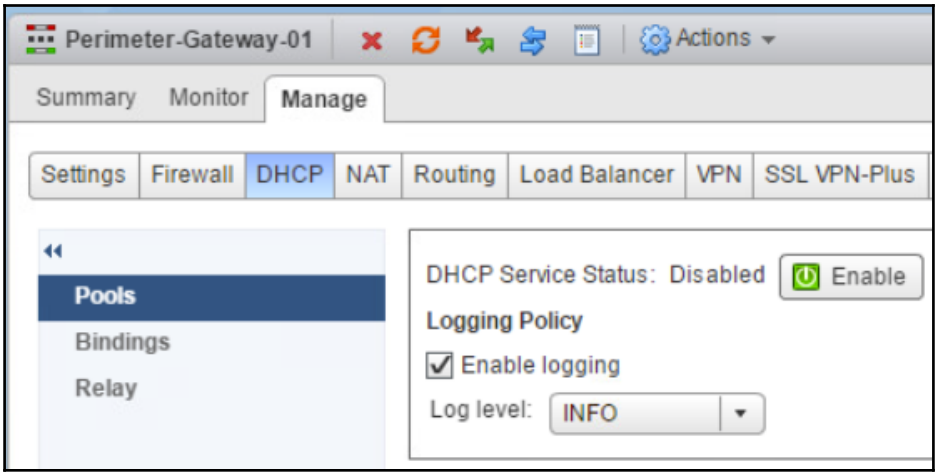

Syslog Server
You can specify the IP address or name of the syslog server that can be resolved using the above mentioned DNS Server(s).
Syslog Server:
log-01a.corp.local
Port:
514
Protocol:
UDP
TCP
TCP6
UDP
UDP6
OK
Cancel

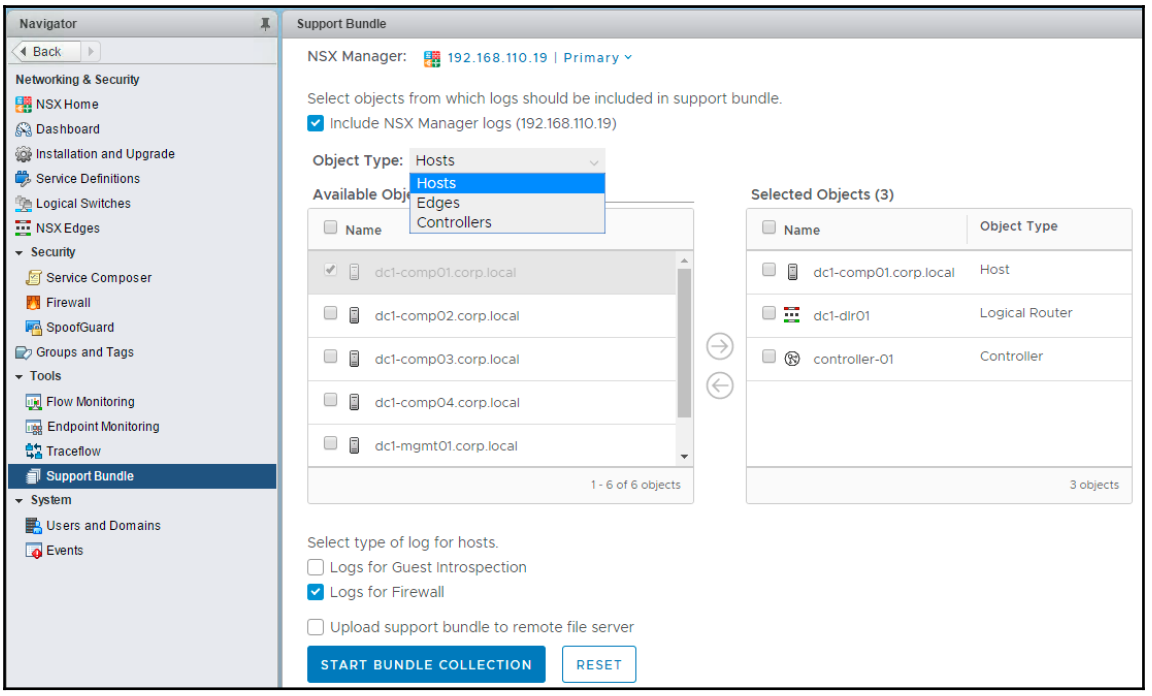

NSX Controller nodes
Actions
Filter
Name
Controller Node
NSX Manager
Status
Peers
Software Ver
Controller-03
192.168.110.33
controller-3
192.168.110.15
Connected
6.3.49347
Controller-02
192.168.110.32
controller-2
192.168.110.15
Connected
6.3.49347
Controller-01
192.168.110.31
controller-1
192.168.110.15
Connected
6.3.49347

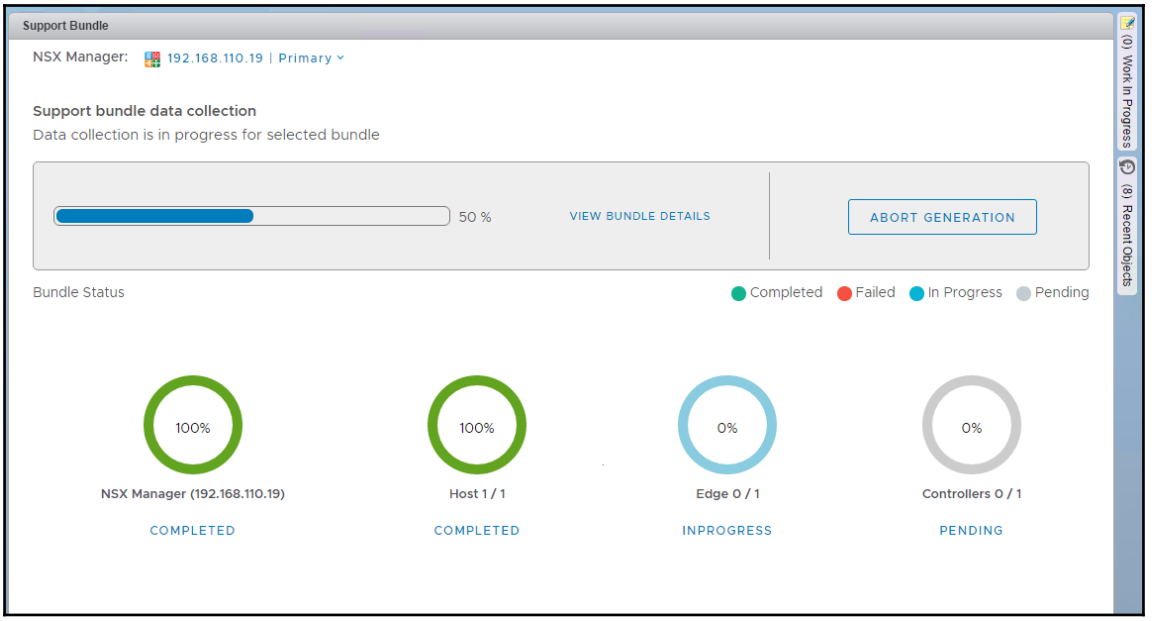

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
NSX Edges
NSX Manager:
192.168.110.42
Actions
0 Installing
0 Failed
Id
Name
Type
Version
edge-1
Perimeter-Gateway-01
NSX Edge
6.3.0
edge-2
Distributed-Router-01
Logical Router
6.3.0

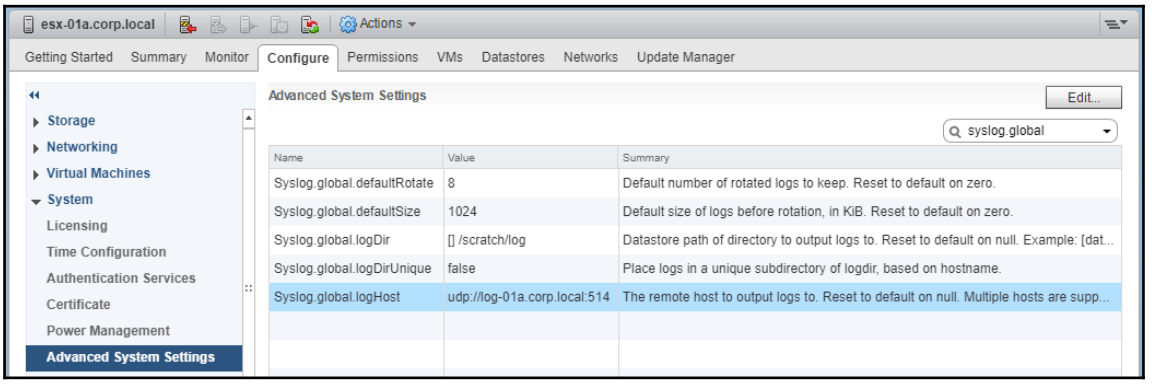

Navigator
Back
Perimeter-Gateway-01
Perimeter-Gateway-01
Actions
Summary
Monitor
Manage
Settings
Firewall
DHCP
NAT
Routing
Load Balancer
VPN
SSL VPN-Plus
Grouping O
Configuration
Interfaces
Certificates
Details:
Action
Size:
Compact
Host Name:
Perimeter-Gateway-01
Auto generate rules:
Enabled
FIPS mode:
Disabled
Syslog servers:
Change
Server 1:
Server 2:

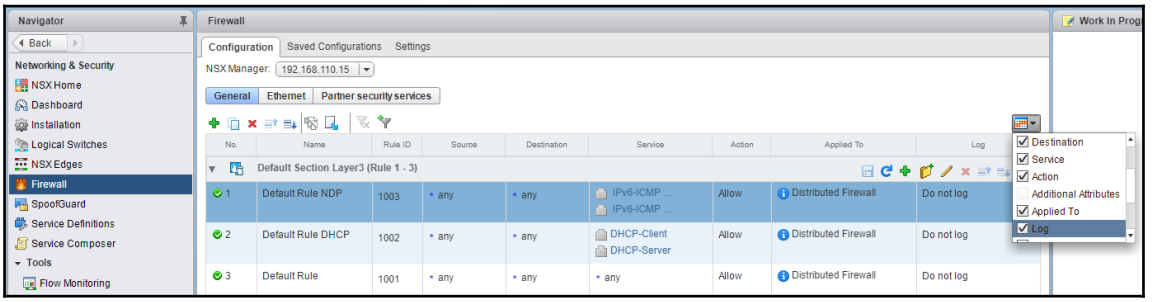

Edit Syslog Servers Configuration
Syslog Server 1:
log-01a.corp.local
Syslog Server 2:
log-02a.corp.local
Protocol:
udp
OK
Cancel

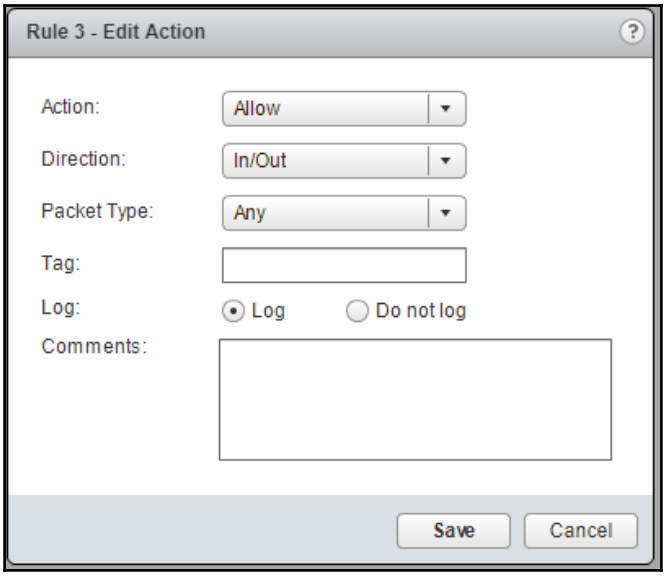

Perimeter-Gateway-01
Actions
Summary
Monitor
Manage
Settings
Firewall
DHCP
NAT
Routing
Load Balancer
VPN
SSL VPN-Plus
Pools
Bindings
Relay
DHCP Service Status: Disabled
Enable
Logging Policy
Enable logging
Log level:
INFO

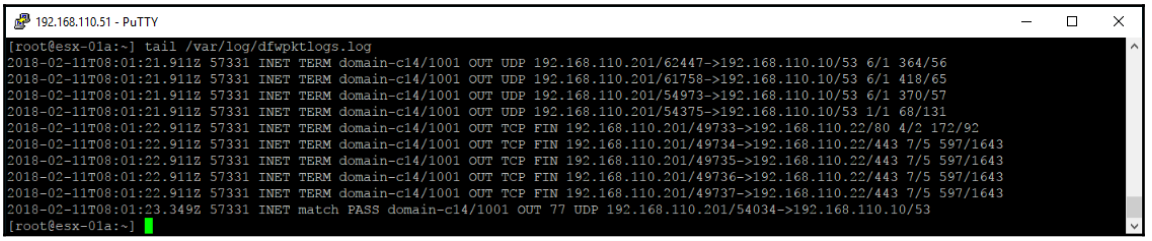

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation and Upgrade
Service Definitions
Logical Switches
NSX Edges
Security
Service Composer
Firewall
SpoofGuard
Groups and Tags
Tools
Flow Monitoring
Endpoint Monitoring
Traceflow
Support Bundle
System
Users and Domains
Events
Support Bundle
NSX Manager: 192.168.110.19 | Primary
Select objects from which logs should be included in support bundle.
Include NSX Manager logs (192.168.110.19)
Object Type: Hosts
Hosts
Edges
Controllers
Available Obj
Name
dc1-comp01.corp.local
dc1-comp02.corp.local
dc1-comp03.corp.local
dc1-comp04.corp.local
dc1-mgmt01.corp.local
1 - 6 of 6 objects
Selected Objects (3)
Name
Object Type
dc1-comp01.corp.local
Host
dc1-dlr01
Logical Router
controller-01
Controller
3 objects
Select type of log for hosts.
Logs for Guest Introspection
Logs for Firewall
Upload support bundle to remote file server
START BUNDLE COLLECTION
RESET

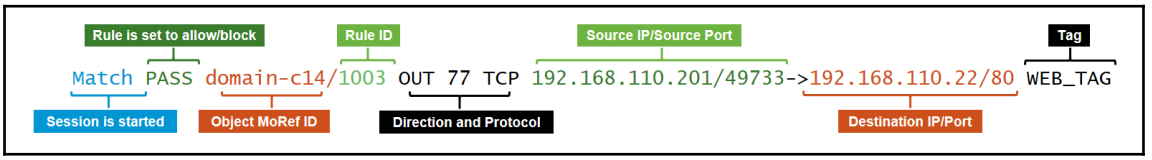

Support Bundle
NSX Manager: 192.168.110.19 | Primary
Support bundle data collection
Data collection is in progress for selected bundle
50 %
VIEW BUNDLE DETAILS
ABORT GENERATION
Bundle Status
Completed
Failed
In Progress
Pending
100%
NSX Manager (192.168.110.19)
COMPLETED
100%
Host 1 / 1
COMPLETED
0%
Edge 0 / 1
INPROGRESS
0%
Controllers 0 / 1
PENDING
(0) Work In Progress
(8) Recent Objects

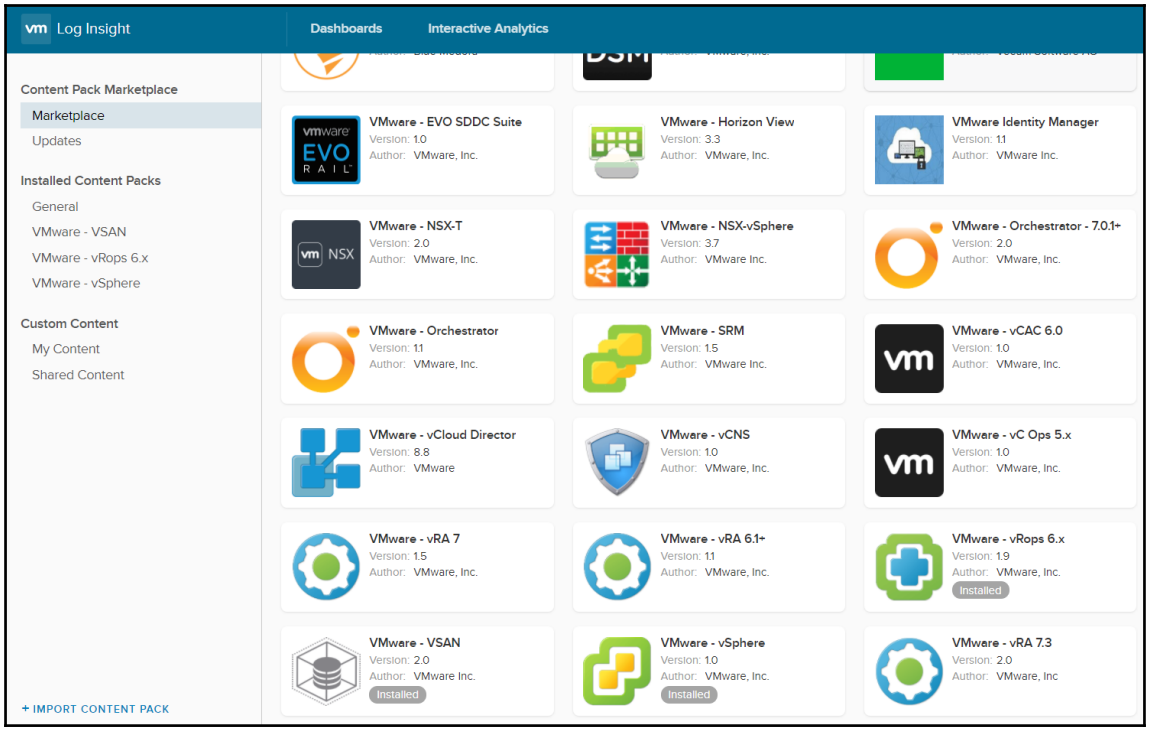

esx-01a.corp.local
Actions
Getting Started
Summary
Monitor
Configure
Permissions
VMs
Datastores
Networks
Update Manager
Storage
Networking
Virtual Machines
System
Licensing
Time Configuration
Authentication Services
Certificate
Power Management
Advanced System Settings
Advanced System Settings
Edit...
syslog.global
Name
Value
Summary
Syslog.global.defaultRotate
8
Default number of rotated logs to keep. Reset to default on zero.
Syslog.global.defaultSize
1024
Default size of logs before rotation, in KiB. Reset to default on zero.
Syslog.global.logDir
[] /scratch/log
Datastore path of directory to output logs to. Reset to default on null. Example: [dat...
Syslog.global.logDirUnique
false
Place logs in a unique subdirectory of logdir, based on hostname.
Syslog.global.logHost
udp://log-01a.corp.local:514
The remote host to output logs to. Reset to default on null. Multiple hosts are supp...

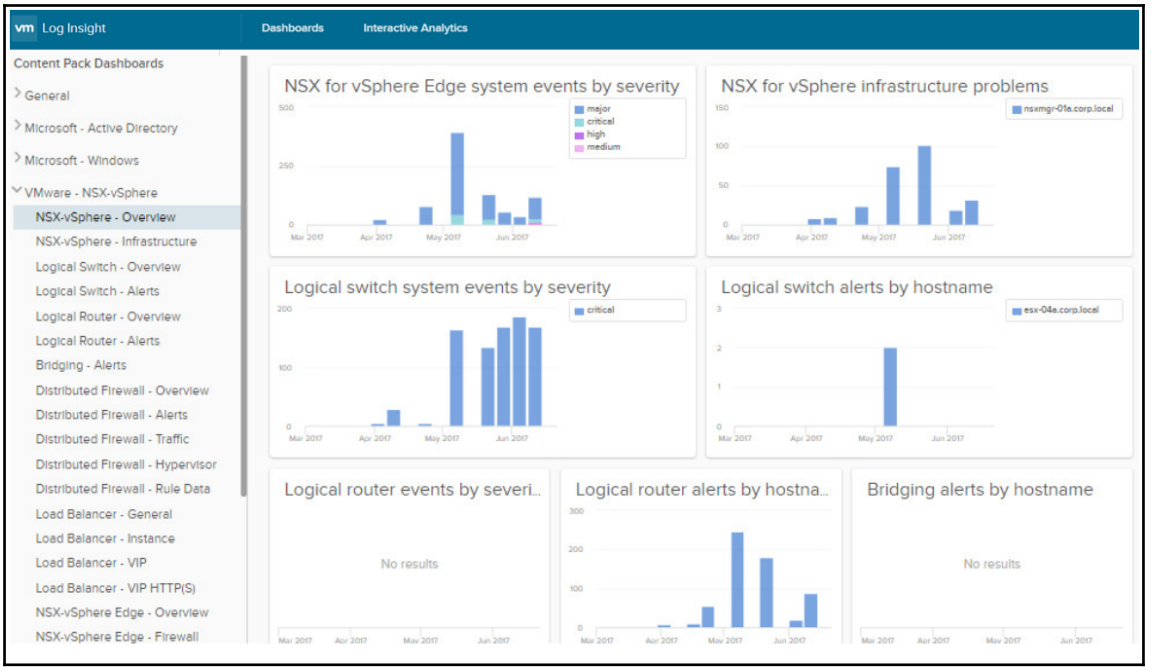

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Tools
Flow Monitoring
Firewall
Configuration
Saved Configurations
Settings
NSX Manager: 192.168.110.15
General
Ethernet
Partner security services
Default Section Layer3 (Rule 1 - 3)
Default Rule NDP
Default Rule DHCP
Default Rule
Allow
Distributed Firewall
Do not log
Destination
Service
Action
Additional Attributes
Applied To
Log
Work In Prog


Rule 3 - Edit Action
Action:
Allow
Direction:
In/Out
Packet Type:
Any
Tag:
Log:
Log
Do not log
Comments:
Save
Cancel

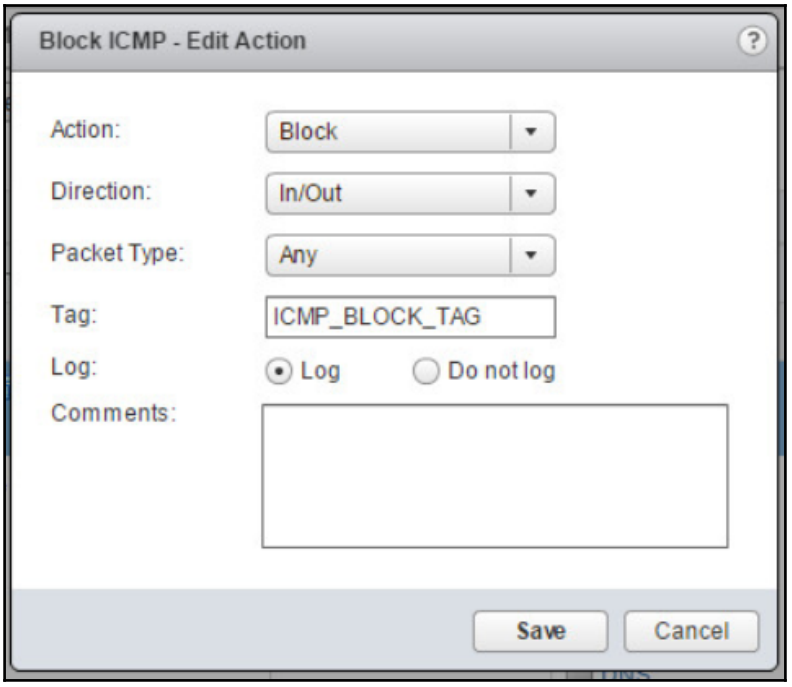

192.168.110.51 - PuTTY
[root@esx-01a:~] tail /var/log/dfwpktlogs.log
2018-02-11T08:01:21.911Z 57331 INET TERM domain-c14/1001 OUT UDP 192.168.110.201/62447->192.168.110.10/53 6/1 364/56
2018-02-11T08:01:21.911Z 57331 INET TERM domain-c14/1001 OUT UDP 192.168.110.201/61758->192.168.110.10/53 6/1 418/65
2018-02-11T08:01:21.911Z 57331 INET TERM domain-c14/1001 OUT UDP 192.168.110.201/54973->192.168.110.10/53 6/1 370/57
2018-02-11T08:01:21.911Z 57331 INET TERM domain-c14/1001 OUT UDP 192.168.110.201/54375->192.168.110.10/53 1/1 68/131
2018-02-11T08:01:22.911Z 57331 INET TERM domain-c14/1001 OUT TCP FIN 192.168.110.201/49733->192.168.110.22/80 4/2 172/92
2018-02-11T08:01:22.911Z 57331 INET TERM domain-c14/1001 OUT TCP FIN 192.168.110.201/49734->192.168.110.22/443 7/5 597/1643
2018-02-11T08:01:22.911Z 57331 INET TERM domain-c14/1001 OUT TCP FIN 192.168.110.201/49735->192.168.110.22/443 7/5 597/1643
2018-02-11T08:01:22.911Z 57331 INET TERM domain-c14/1001 OUT TCP FIN 192.168.110.201/49736->192.168.110.22/443 7/5 597/1643
2018-02-11T08:01:22.911Z 57331 INET TERM domain-c14/1001 OUT TCP FIN 192.168.110.201/49737->192.168.110.22/443 7/5 597/1643
2018-02-11T08:01:23.349Z 57331 INET match PASS domain-c14/1001 OUT 77 UDP 192.168.110.201/54034->192.168.110.10/53
[root@esx-01a:~]

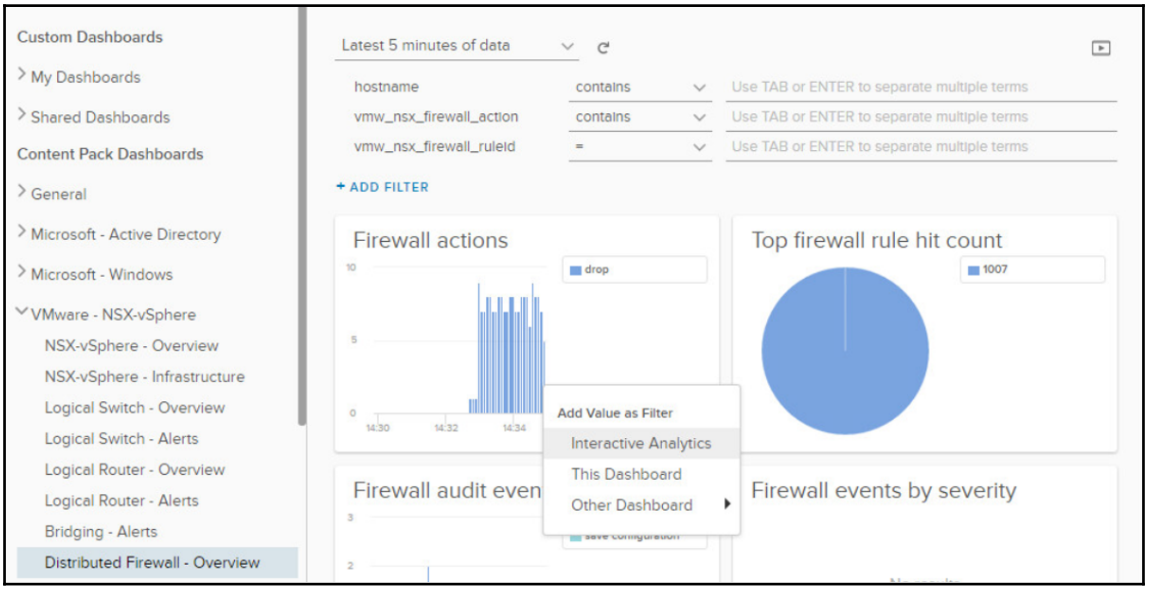

Rule is set to allow/block
Rule ID
Source IP/Source Port
Tag
Match PASS domain-c14/1003 OUT 77 TCP 192.168.110.201/49733->192.168.110.22/80 WEB_TAG
Session is started
Object MoRef ID
Direction and Protocol
Destination IP/Port

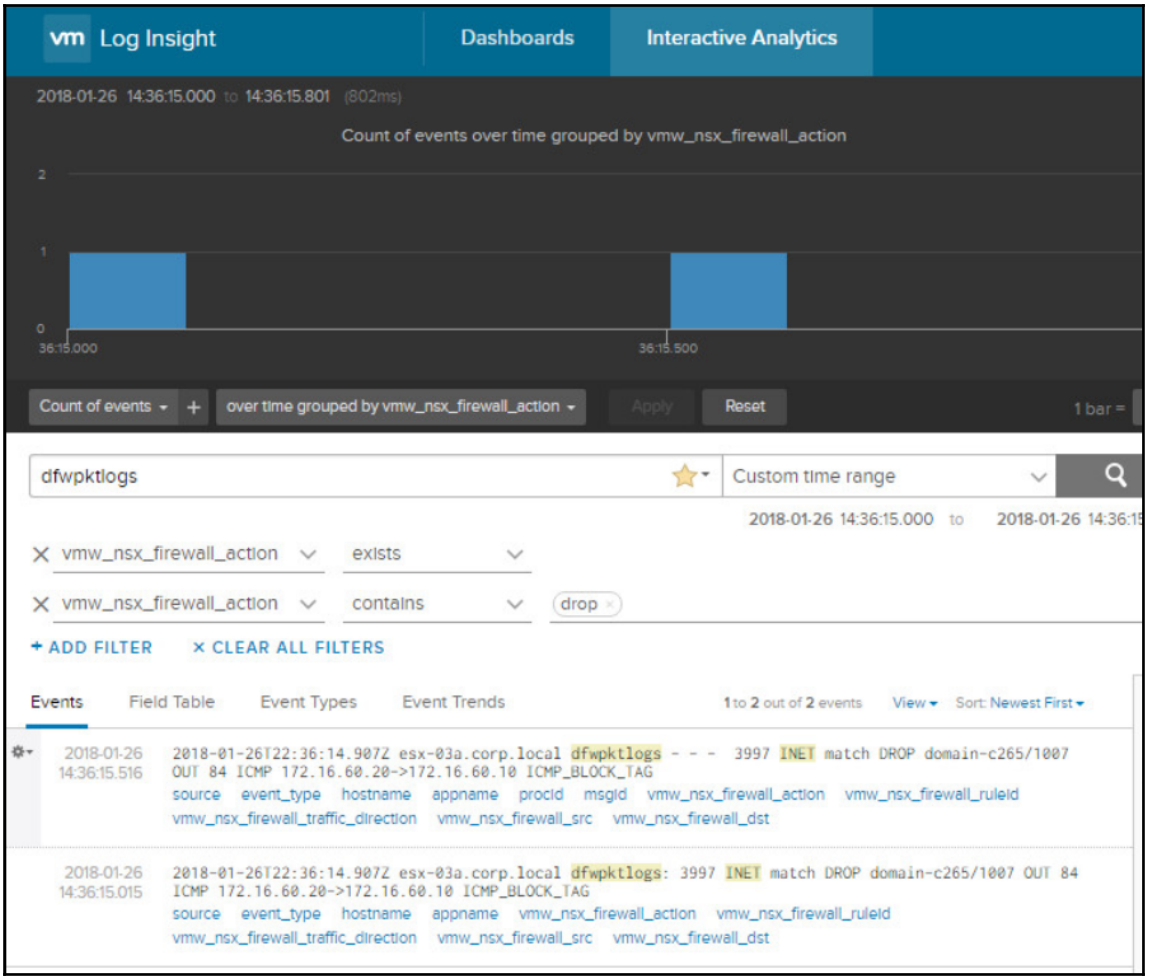

Log Insight
Dashboards
Interactive Analytics
Content Pack Marketplace
Marketplace
Updates
Installed Content Packs
General
VMware - VSAN
VMware - vRops 6.x
VMware - vSphere
Custom Content
My Content
Shared Content
+ IMPORT CONTENT PACK
VMware - EVO SDDC Suite
Version: 1.0
Author: VMware, Inc.
VMware - Horizon View
Version: 3.3
Author: VMware, Inc.
VMware Identity Manager
Version: 1.1
Author: VMware Inc.
VMware - NSX-T
Version: 2.0
Author: VMware, Inc.
VMware - NSX-vSphere
Version: 3.7
Author: VMware Inc.
VMware - Orchestrator - 7.0.1+
Version: 2.0
Author: VMware, Inc.
VMware - Orchestrator
Version: 1.1
Author: VMware, Inc.
VMware - SRM
Version: 1.5
Author: VMware Inc.
VMware - vCAC 6.0
Version: 1.0
Author: VMware, Inc.
VMware - vCloud Director
Version: 8.8
Author: VMware
VMware - vCNS
Version: 1.0
Author: VMware, Inc.
VMware - vC Ops 5.x
Version: 1.0
Author: VMware, Inc.
VMware - vRA 7
Version: 1.5
Author: VMware, Inc.
VMware - vRA 6.1+
Version: 1.1
Author: VMware, Inc.
VMware - vRops 6.x
Version: 1.9
Author: VMware, Inc.
Installed
VMware - VSAN
Version: 2.0
Author: VMware Inc.
Installed
VMware - vSphere
Version: 1.0
Author: VMware, Inc.
Installed
VMware - vRA 7.3
Version: 2.0
Author: VMware, Inc

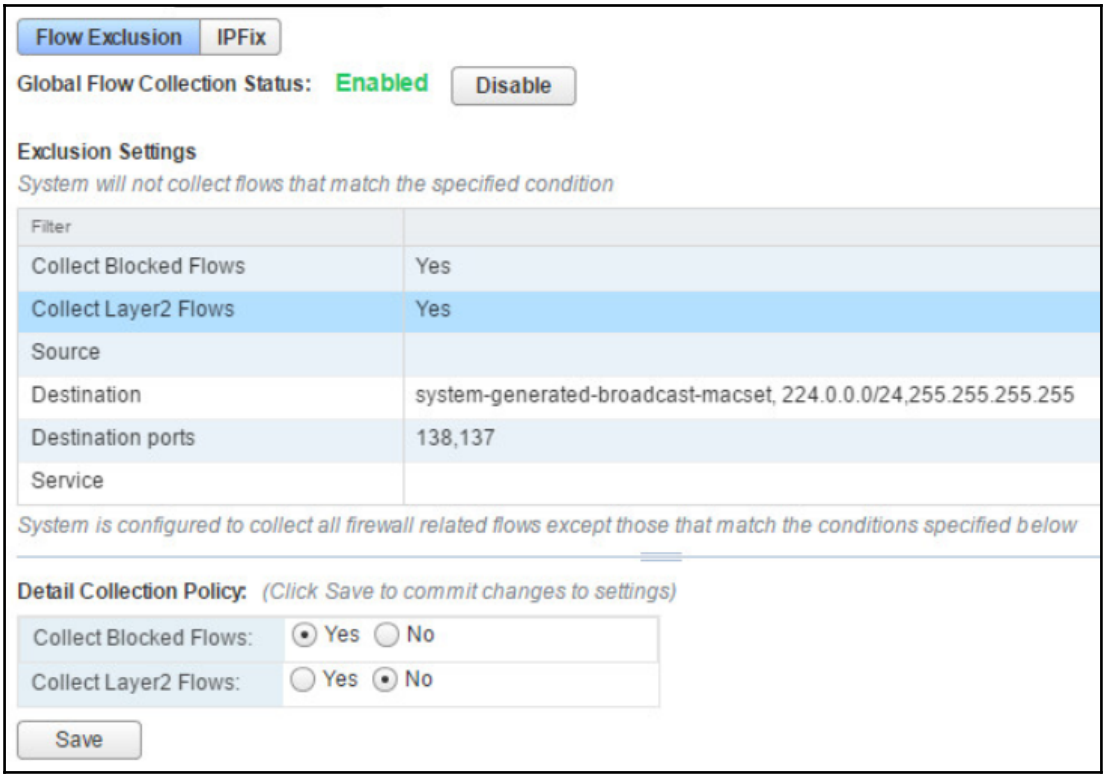


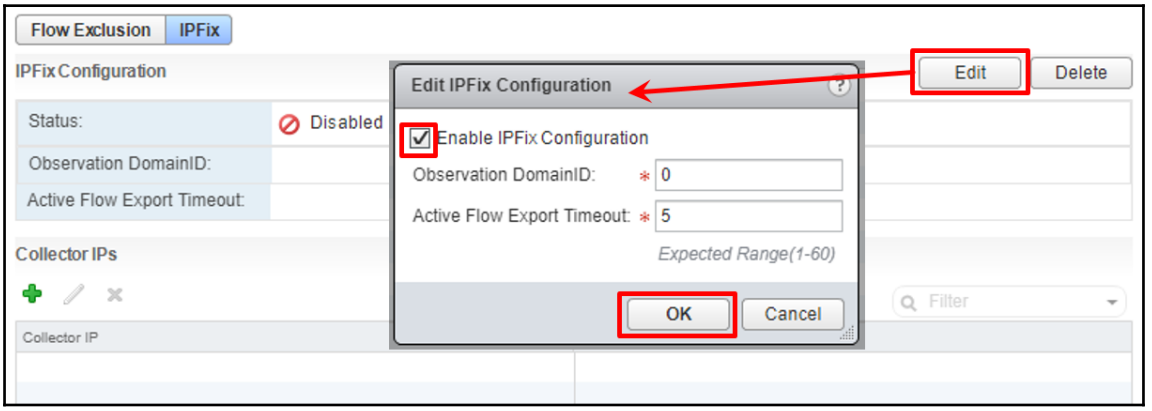
2	Block ICMP	1007	fin-web-01a....	hr-web-01a...	ICMP Echo ICMP Echo...	Block	Distrib...

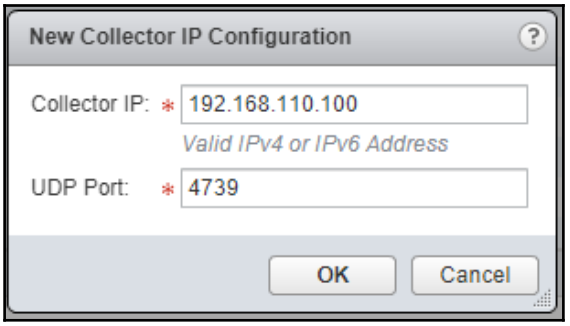

Block ICMP - Edit Action
Action:
Block
Direction:
In/Out
Packet Type:
Any
Tag:
ICMP_BLOCK_TAG
Log:
Log
Do not log
Comments:
Save
Cancel

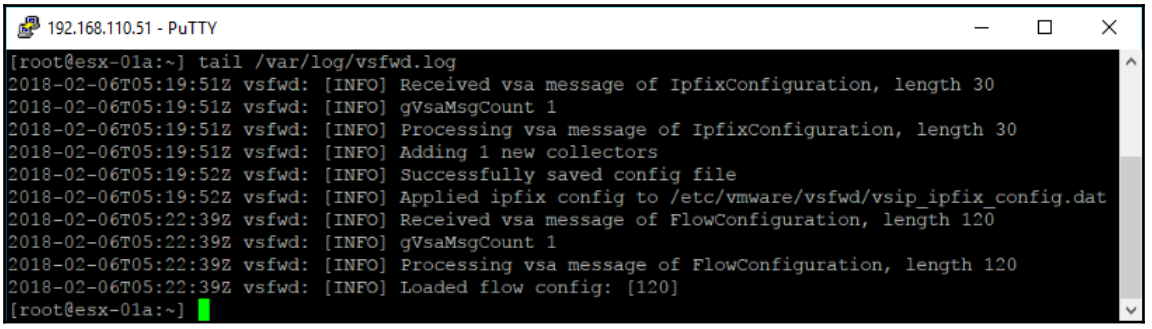

Custom Dashboards
My Dashboards
Shared Dashboards
Content Pack Dashboards
General
Microsoft - Active Directory
Microsoft - Windows
VMware - NSX-vSphere
NSX-vSphere - Overview
NSX-vSphere - Infrastructure
Logical Switch - Overview
Logical Switch - Alerts
Logical Router - Overview
Logical Router - Alerts
Bridging - Alerts
Distributed Firewall - Overview
Latest 5 minutes of data
hostname
contains
Use TAB or ENTER to separate multiple terms
vmw_nsx_firewall_action
contains
Use TAB or ENTER to separate multiple terms
vmw_nsx_firewall_ruleId
=
Use TAB or ENTER to separate multiple terms
+ ADD FILTER
Firewall actions
drop
Top firewall rule hit count
1007
Add Value as Filter
Interactive Analytics
This Dashboard
Other Dashboard
Firewall audit even
Firewall events by severity

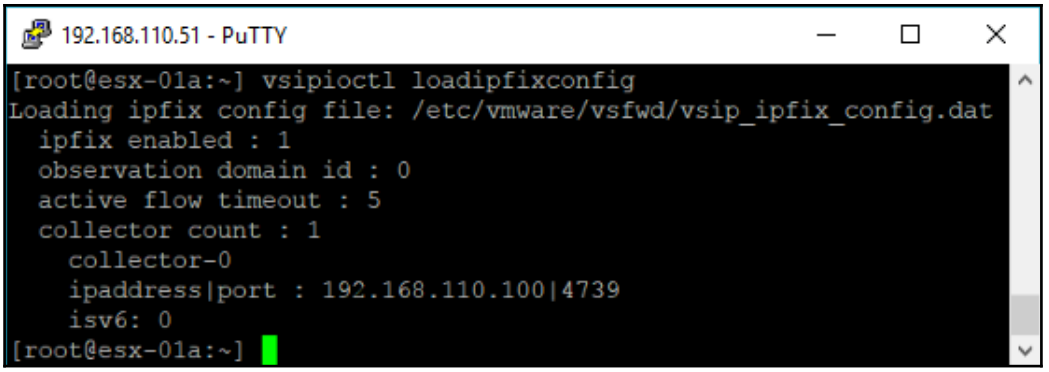

vm Log Insight
Dashboards
Interactive Analytics
2018-01-26 14:36:15.000 to 14:36:15.801 (802ms)
Count of events over time grouped by vmw_nsx_firewall_action
2
1
0
36:15.000
36:15.500
Count of events
over time grouped by vmw_nsx_firewall_action
Apply
Reset
1 bar =
dfwpktlogs
Custom time range
2018-01-26 14:36:15.000 to 2018-01-26 14:36:15
vmw_nsx_firewall_action
exists
vmw_nsx_firewall_action
contains
drop
+ ADD FILTER
× CLEAR ALL FILTERS
Events
Field Table
Event Types
Event Trends
1 to 2 out of 2 events
View
Sort: Newest First
2018-01-26 14:36:15.516
2018-01-26T22:36:14.907Z esx-03a.corp.local dfwpktlogs - - - 3997 INET match DROP domain-c265/1007 OUT 84 ICMP 172.16.60.20->172.16.60.10 ICMP_BLOCK_TAG
source event_type hostname appname procid msgid vmw_nsx_firewall_action vmw_nsx_firewall_ruleId
vmw_nsx_firewall_traffic_direction vmw_nsx_firewall_src vmw_nsx_firewall_dst
2018-01-26 14:36:15.015
2018-01-26T22:36:14.907Z esx-03a.corp.local dfwpktlogs: 3997 INET match DROP domain-c265/1007 OUT 84 ICMP 172.16.60.20->172.16.60.10 ICMP_BLOCK_TAG
source event_type hostname appname vmw_nsx_firewall_action vmw_nsx_firewall_ruleId
vmw_nsx_firewall_traffic_direction vmw_nsx_firewall_src vmw_nsx_firewall_dst

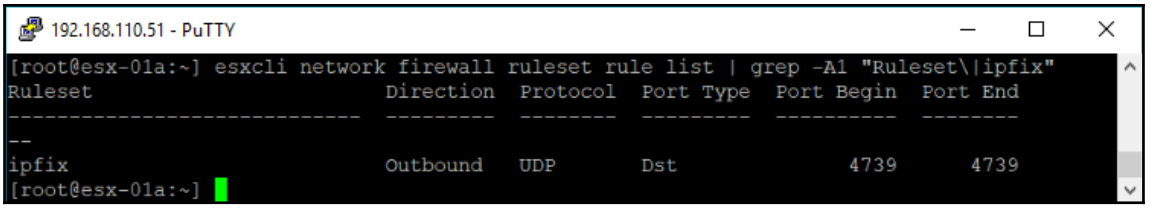

Flow Exclusion
IPFix
Global Flow Collection Status: Enabled
Disable
Exclusion Settings
System will not collect flows that match the specified condition
Filter
Collect Blocked Flows
Yes
Collect Layer2 Flows
Yes
Source
Destination
system-generated-broadcast-macset, 224.0.0.0/24,255.255.255.255
Destination ports
138,137
Service
System is configured to collect all firewall related flows except those that match the conditions specified below
Detail Collection Policy: (Click Save to commit changes to settings)
Collect Blocked Flows: Yes No
Collect Layer2 Flows: Yes No
Save

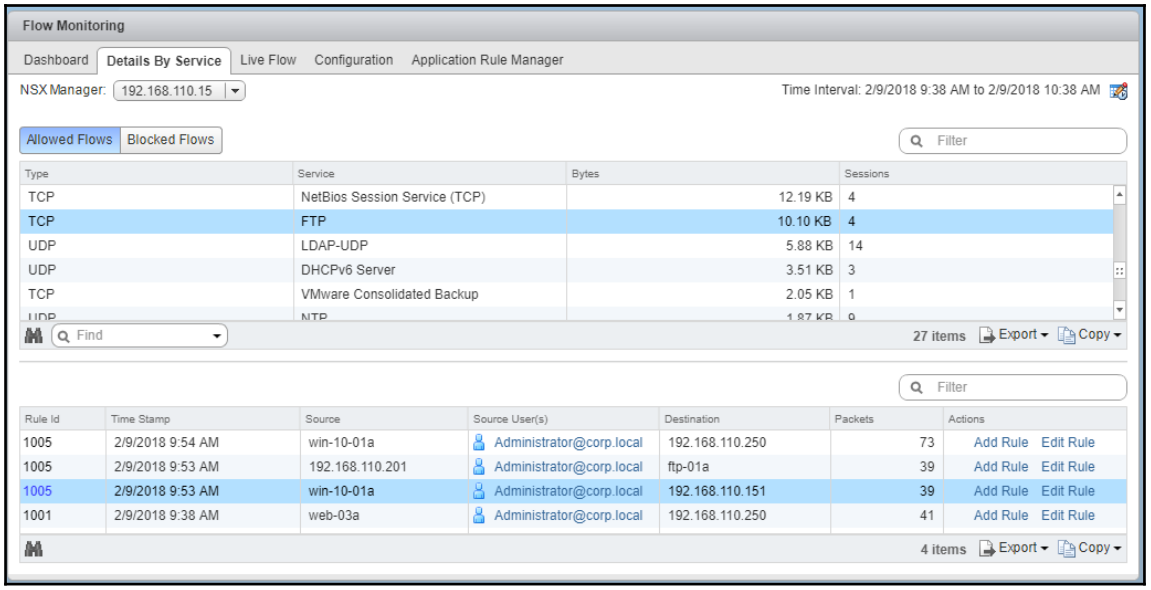

Flow Exclusion
IPFix
IPFix Configuration
Edit
Delete
Status:
Disabled
Observation DomainID:
Active Flow Export Timeout:
Collector IPs
Collector IP
Filter
Edit IPFix Configuration
Enable IPFix Configuration
Observation DomainID: * 0
Active Flow Export Timeout: * 5
Expected Range(1-60)
OK
Cancel

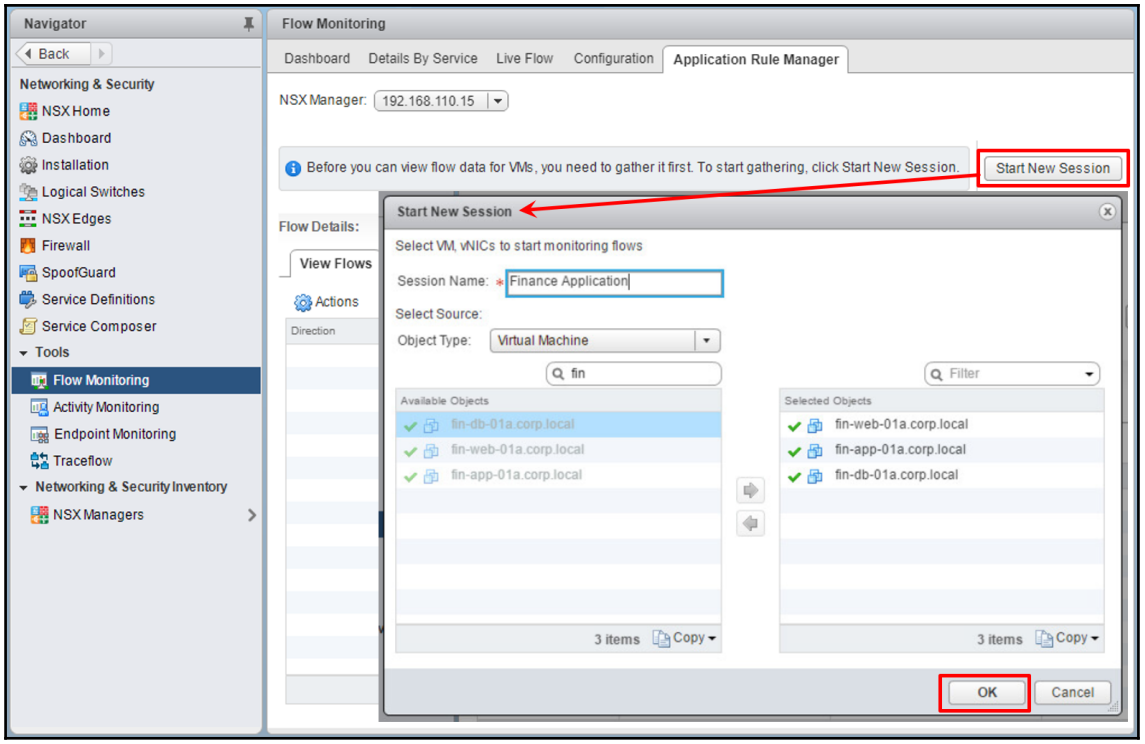

New Collector IP Configuration
Collector IP: * 192.168.110.100
Valid IPv4 or IPv6 Address
UDP Port: * 4739
OK
Cancel

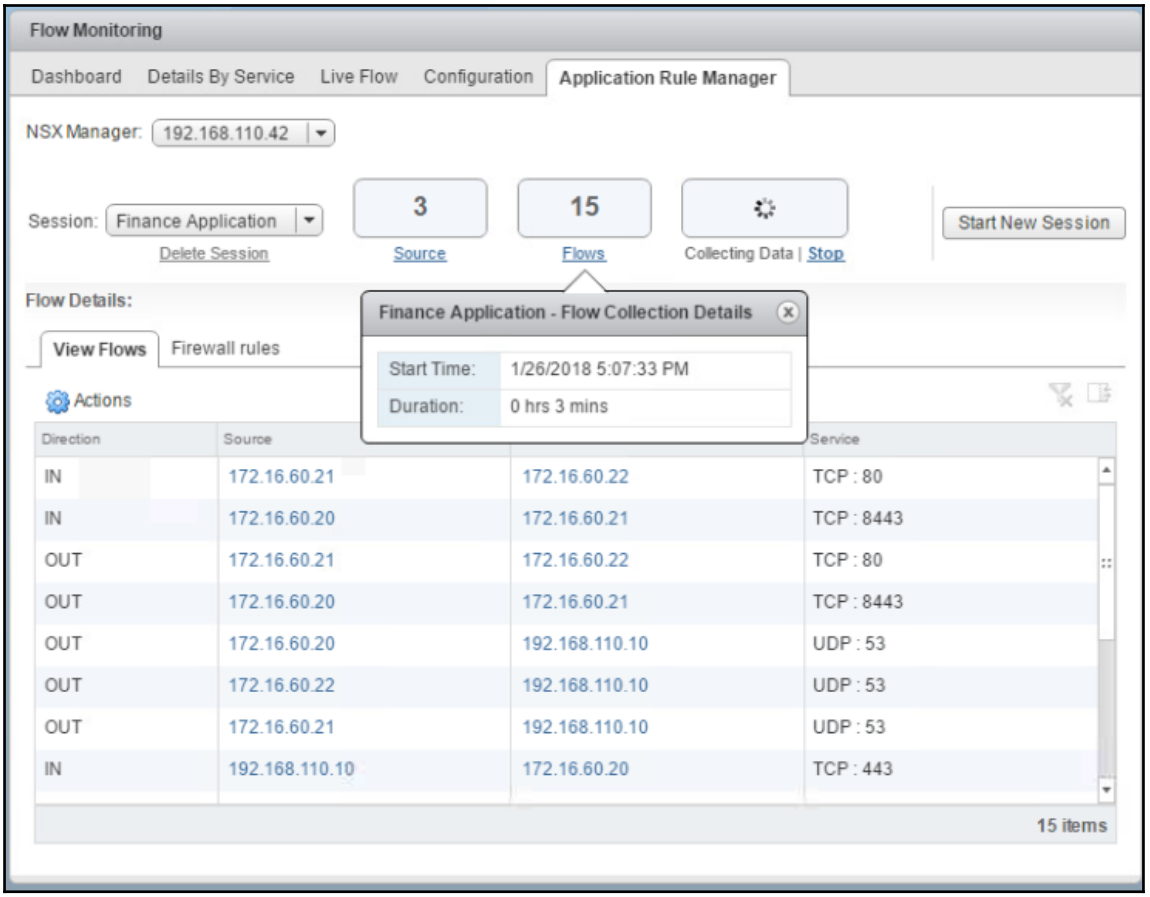

192.168.110.51 - PuTTY
[root@esx-01a:~] tail /var/log/vsfwd.log
2018-02-06T05:19:51Z vsfwd: [INFO] Received vsa message of IpfixConfiguration, length 30
2018-02-06T05:19:51Z vsfwd: [INFO] gVsaMsgCount 1
2018-02-06T05:19:51Z vsfwd: [INFO] Processing vsa message of IpfixConfiguration, length 30
2018-02-06T05:19:51Z vsfwd: [INFO] Adding 1 new collectors
2018-02-06T05:19:52Z vsfwd: [INFO] Successfully saved config file
2018-02-06T05:19:52Z vsfwd: [INFO] Applied ipfix config to /etc/vmware/vsfwd/vsip_ipfix_config.dat
2018-02-06T05:22:39Z vsfwd: [INFO] Received vsa message of FlowConfiguration, length 120
2018-02-06T05:22:39Z vsfwd: [INFO] gVsaMsgCount 1
2018-02-06T05:22:39Z vsfwd: [INFO] Processing vsa message of FlowConfiguration, length 120
2018-02-06T05:22:39Z vsfwd: [INFO] Loaded flow config: [120]
[root@esx-01a:~]

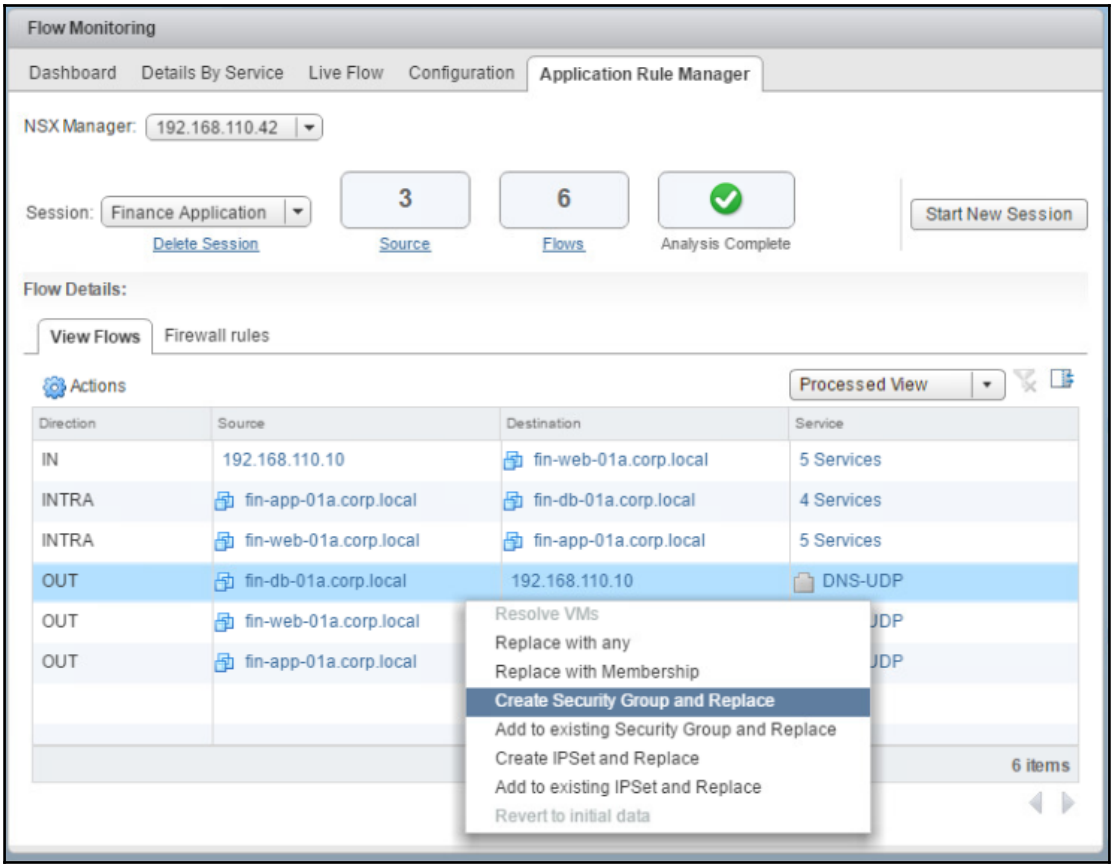

192.168.110.51 - PuTTY
[root@esx-01a:~] vsipioctl loadipfixconfig
Loading ipfix config file: /etc/vmware/vsfwd/vsip_ipfix_config.dat
ipfix enabled : 1
observation domain id : 0
active flow timeout : 5
collector count : 1
collector-0
ipaddress|port : 192.168.110.100|4739
isv6: 0
[root@esx-01a:~]

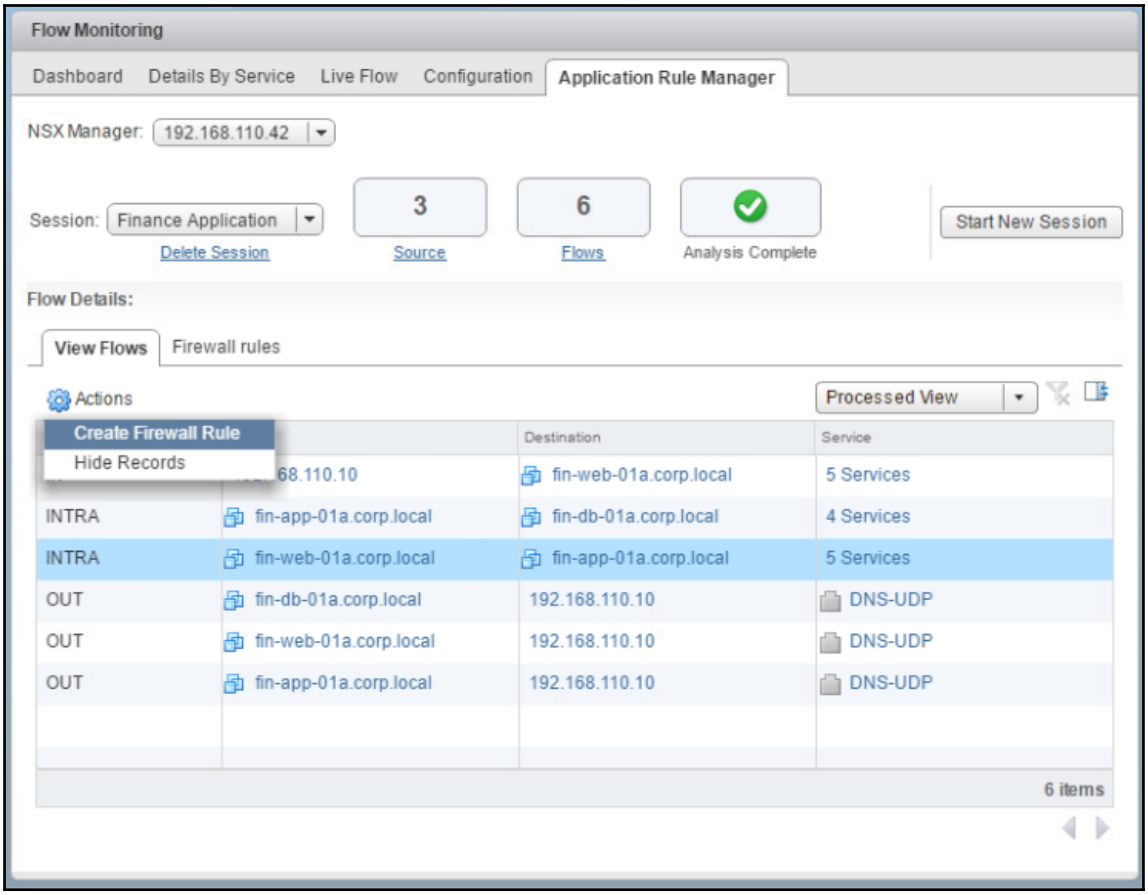

192.168.110.51 - PuTTY
[root@esx-01a:~] esxcli network firewall ruleset rule list | grep -A1 "Ruleset\|ipfix"
Ruleset Direction Protocol Port Type Port Begin Port End
--
ipfix Outbound UDP Dst 4739 4739
[root@esx-01a:~]

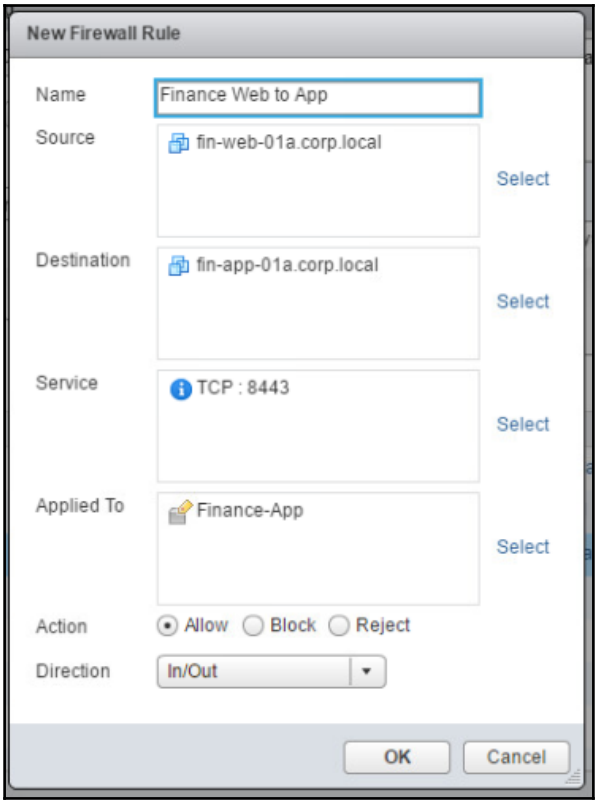

Flow Monitoring
Dashboard
Details By Service
Live Flow
Configuration
Application Rule Manager
NSX Manager: 192.168.110.15
Time Interval: 2/9/2018 9:38 AM to 2/9/2018 10:38 AM
Allowed Flows
Blocked Flows
Filter
Type
Service
Bytes
Sessions
TCP
NetBios Session Service (TCP)
12.19 KB
4
TCP
FTP
10.10 KB
4
UDP
LDAP-UDP
5.88 KB
14
UDP
DHCPv6 Server
3.51 KB
3
TCP
VMware Consolidated Backup
2.05 KB
1
Find
27 items
Export
Copy
Filter
Rule Id
Time Stamp
Source
Source User(s)
Destination
Packets
Actions
1005
2/9/2018 9:54 AM
win-10-01a
Administrator@corp.local
192.168.110.250
73
Add Rule
Edit Rule
1005
2/9/2018 9:53 AM
192.168.110.201
Administrator@corp.local
ftp-01a
39
Add Rule
Edit Rule
1005
2/9/2018 9:53 AM
win-10-01a
Administrator@corp.local
192.168.110.151
39
Add Rule
Edit Rule
1001
2/9/2018 9:38 AM
web-03a
Administrator@corp.local
192.168.110.250
41
Add Rule
Edit Rule
4 items
Export
Copy

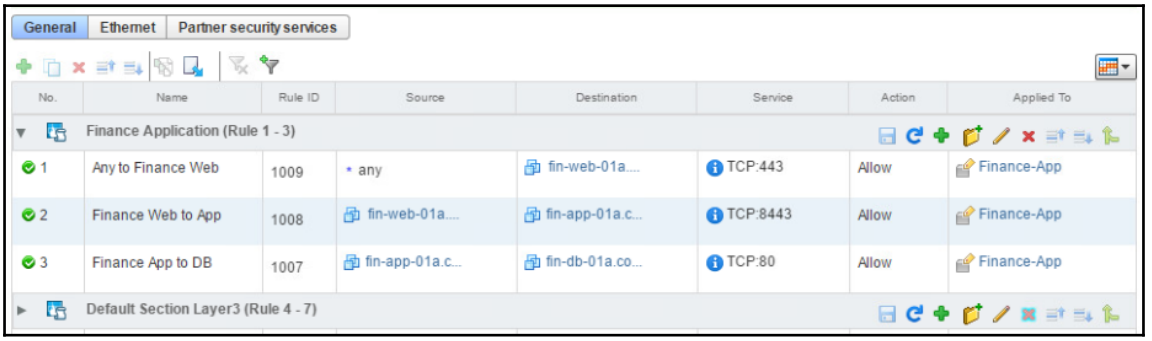

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Tools
Flow Monitoring
Activity Monitoring
Endpoint Monitoring
Traceflow
Networking & Security Inventory
NSX Managers
Flow Monitoring
Dashboard
Details By Service
Live Flow
Configuration
Application Rule Manager
NSX Manager: 192.168.110.15
Before you can view flow data for VMs, you need to gather it first. To start gathering, click Start New Session.
Start New Session
Flow Details:
View Flows
Actions
Direction
Start New Session
Select VM, vNICs to start monitoring flows
Session Name: * Finance Application
Select Source:
Object Type: Virtual Machine
fin
Filter
Available Objects
fin-db-01a.corp.local
fin-web-01a.corp.local
fin-app-01a.corp.local
3 items
Copy
Selected Objects
fin-web-01a.corp.local
fin-app-01a.corp.local
fin-db-01a.corp.local
3 items
Copy
OK
Cancel

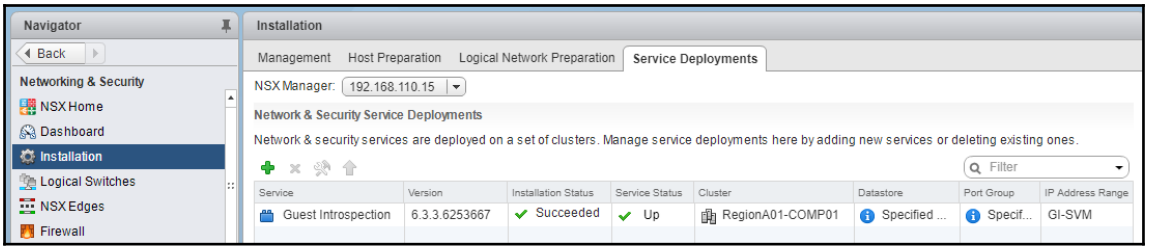

Flow Monitoring
Dashboard
Details By Service
Live Flow
Configuration
Application Rule Manager
NSX Manager: 192.168.110.42
Session: Finance Application
Delete Session
3
Source
15
Flows
Collecting Data | Stop
Start New Session
Flow Details:
Finance Application - Flow Collection Details
Start Time: 1/26/2018 5:07:33 PM
Duration: 0 hrs 3 mins
View Flows
Firewall rules
Actions
Direction
Source
Service
IN 172.16.60.21 172.16.60.22 TCP : 80
IN 172.16.60.20 172.16.60.21 TCP : 8443
OUT 172.16.60.21 172.16.60.22 TCP : 80
OUT 172.16.60.20 172.16.60.21 TCP : 8443
OUT 172.16.60.20 192.168.110.10 UDP : 53
OUT 172.16.60.22 192.168.110.10 UDP : 53
OUT 172.16.60.21 192.168.110.10 UDP : 53
IN 192.168.110.10 172.16.60.20 TCP : 443
15 items

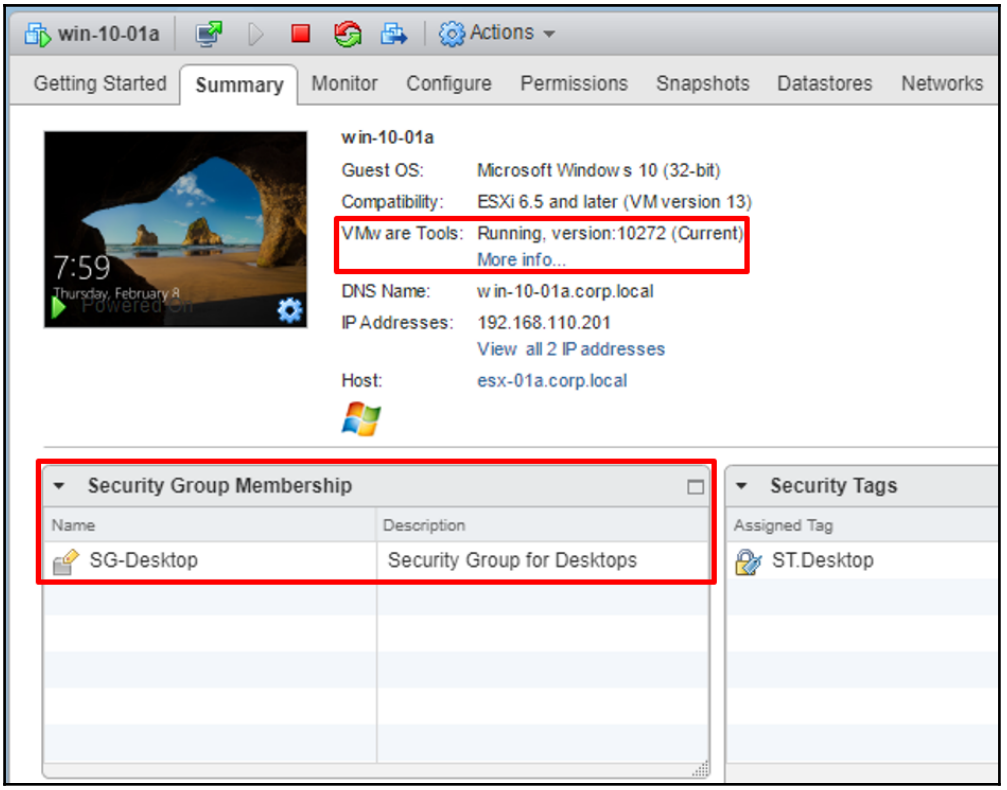

Flow Monitoring
Dashboard
Details By Service
Live Flow
Configuration
Application Rule Manager
NSX Manager: 192.168.110.42
Session: Finance Application
Delete Session
3
Source
6
Flows
Analysis Complete
Start New Session
Flow Details:
View Flows
Firewall rules
Actions
Processed View
Direction
Source
Destination
Service
IN
192.168.110.10
fin-web-01a.corp.local
5 Services
INTRA
fin-app-01a.corp.local
fin-db-01a.corp.local
4 Services
INTRA
fin-web-01a.corp.local
fin-app-01a.corp.local
5 Services
OUT
fin-db-01a.corp.local
192.168.110.10
DNS-UDP
OUT
fin-web-01a.corp.local
OUT
fin-app-01a.corp.local
Resolve VMs
Replace with any
Replace with Membership
Create Security Group and Replace
Add to existing Security Group and Replace
Create IPSet and Replace
Add to existing IPSet and Replace
Revert to initial data
6 items

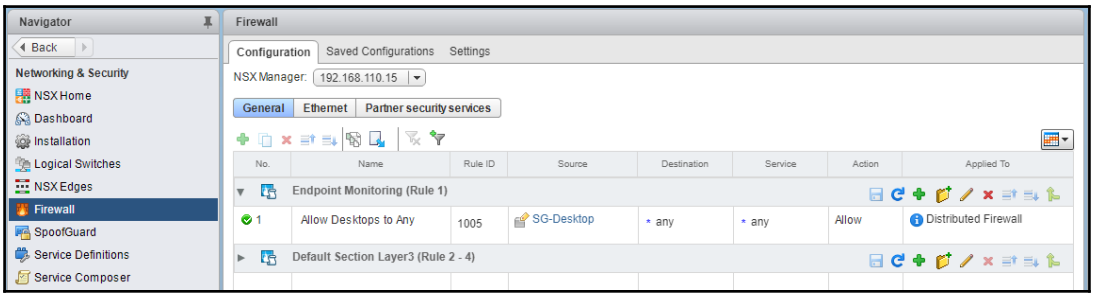

Flow Monitoring
Dashboard
Details By Service
Live Flow
Configuration
Application Rule Manager
NSX Manager: 192.168.110.42
Session: Finance Application
Delete Session
3
Source
6
Flows
Analysis Complete
Start New Session
Flow Details:
View Flows
Firewall rules
Actions
Processed View
Create Firewall Rule
Hide Records
Destination
Service
68.110.10
fin-web-01a.corp.local
5 Services
INTRA
fin-app-01a.corp.local
fin-db-01a.corp.local
4 Services
INTRA
fin-web-01a.corp.local
fin-app-01a.corp.local
5 Services
OUT
fin-db-01a.corp.local
192.168.110.10
DNS-UDP
OUT
fin-web-01a.corp.local
192.168.110.10
DNS-UDP
OUT
fin-app-01a.corp.local
192.168.110.10
DNS-UDP
6 items

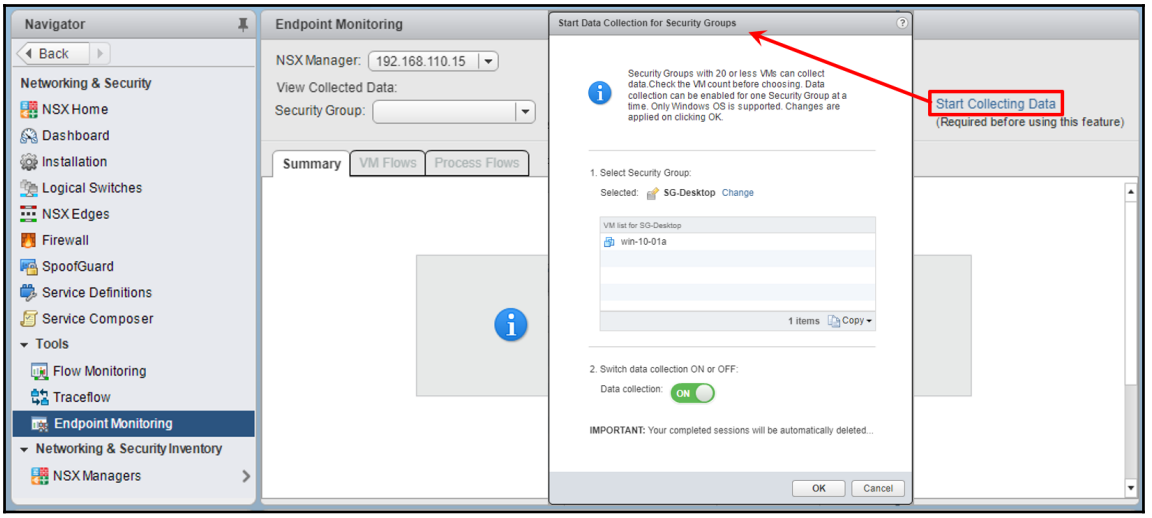

New Firewall Rule
Name
Finance Web to App
Source
fin-web-01a.corp.local
Select
Destination
fin-app-01a.corp.local
Select
Service
TCP : 8443
Select
Applied To
Finance-App
Select
Action
Allow
Block
Reject
Direction
In/Out
OK
Cancel

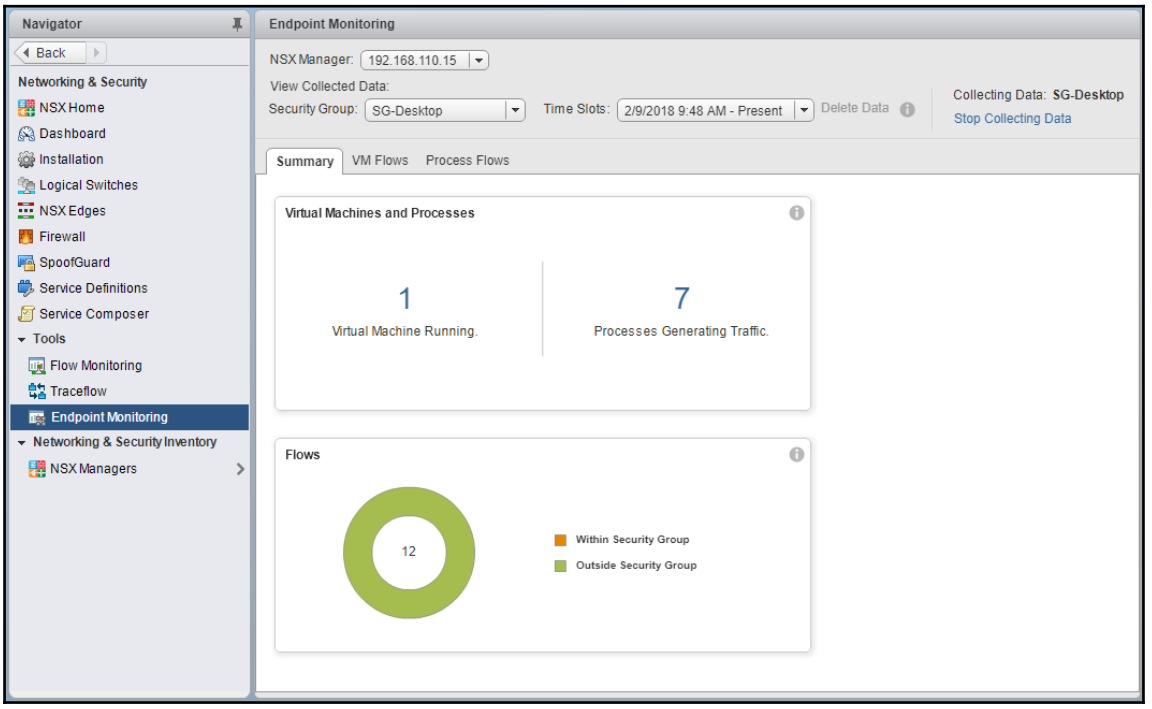

General
Ethernet
Partner security services
No.
Name
Rule ID
Source
Destination
Service
Action
Applied To
Finance Application (Rule 1 - 3)
1
Any to Finance Web
1009
any
fin-web-01a....
TCP:443
Allow
Finance-App
2
Finance Web to App
1008
fin-web-01a....
fin-app-01a.c...
TCP:8443
Allow
Finance-App
3
Finance App to DB
1007
fin-app-01a.c...
fin-db-01a.co...
TCP:80
Allow
Finance-App
Default Section Layer3 (Rule 4 - 7)

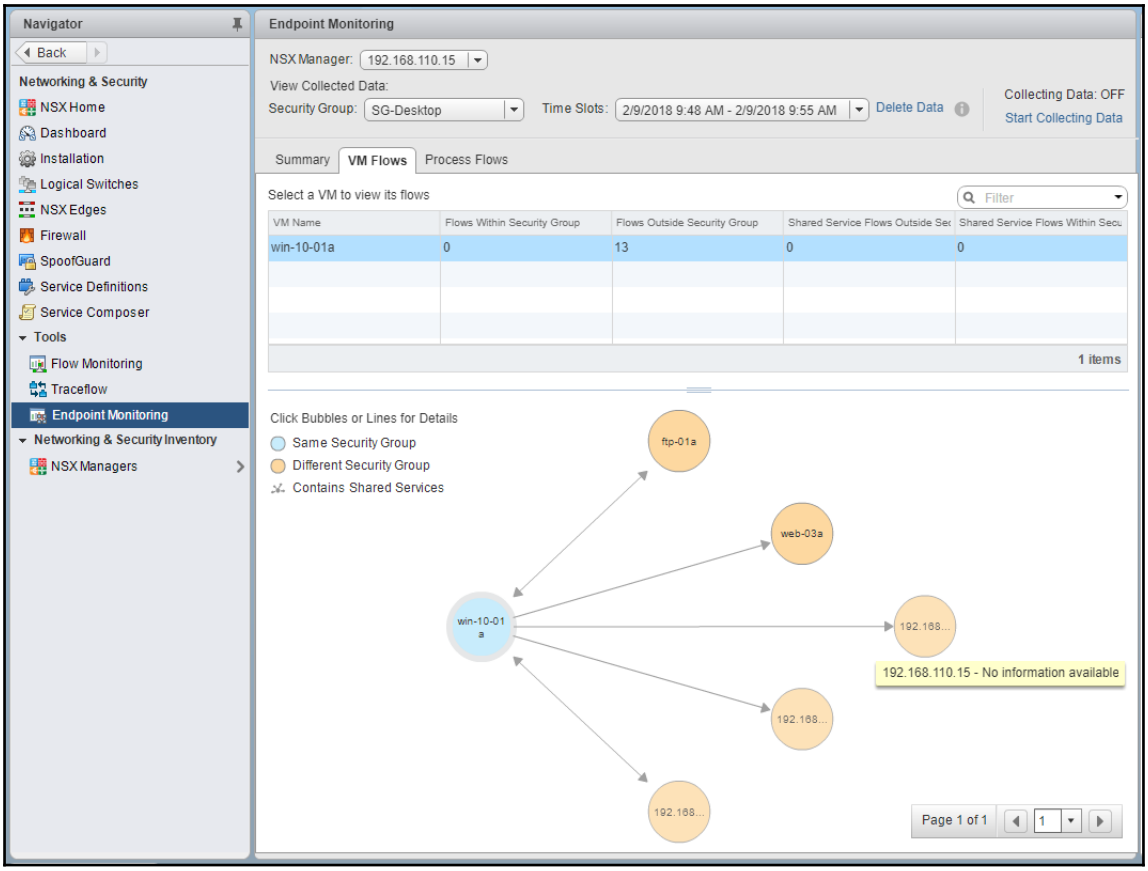

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
Installation
Management
Host Preparation
Logical Network Preparation
Service Deployments
NSX Manager: 192.168.110.15
Network & Security Service Deployments
Network & security services are deployed on a set of clusters. Manage service deployments here by adding new services or deleting existing ones.
Filter
Service
Version
Installation Status
Service Status
Cluster
Datastore
Port Group
IP Address Range
Guest Introspection
6.3.3.6253667
Succeeded
Up
RegionA01-COMP01
Specified ...
Specif...
GI-SVM


win-10-01a
Actions
Getting Started
Summary
Monitor
Configure
Permissions
Snapshots
Datastores
Networks
win-10-01a
Guest OS:
Microsoft Windows 10 (32-bit)
Compatibility:
ESXi 6.5 and later (VM version 13)
VMware Tools:
Running, version:10272 (Current)
More info...
DNS Name:
win-10-01a.corp.local
IP Addresses:
192.168.110.201
View all 2 IP addresses
Host:
esx-01a.corp.local
Security Group Membership
Name
Description
SG-Desktop
Security Group for Desktops
Security Tags
Assigned Tag
ST.Desktop

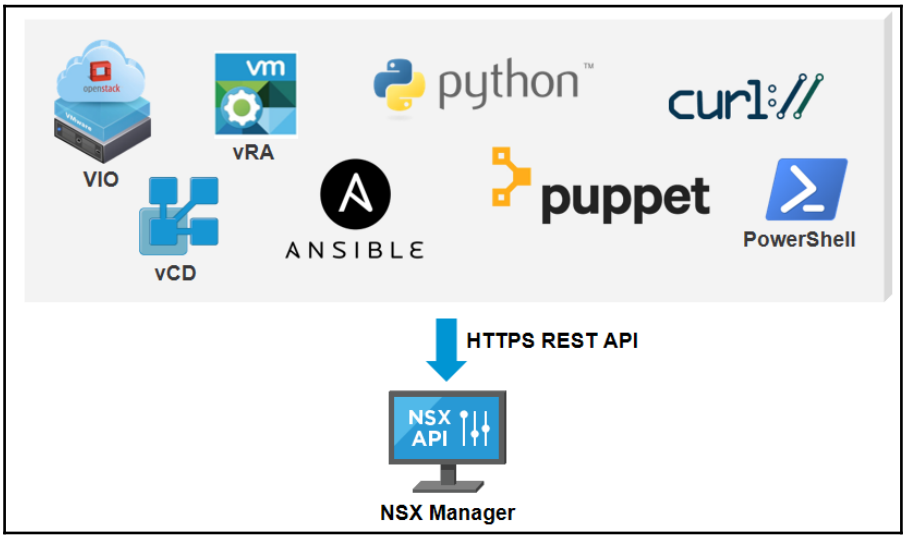

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Firewall
Configuration
Saved Configurations
Settings
NSX Manager: 192.168.110.15
General
Ethernet
Partner security services
No.
Name
Rule ID
Source
Destination
Service
Action
Applied To
Endpoint Monitoring (Rule 1)
1
Allow Desktops to Any
1005
SG-Desktop
any
any
Allow
Distributed Firewall
Default Section Layer3 (Rule 2 - 4)

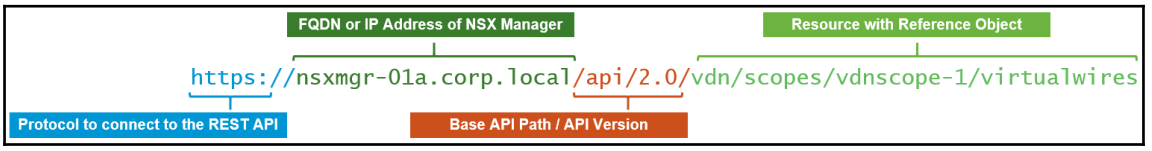

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Tools
Flow Monitoring
Traceflow
Endpoint Monitoring
Networking & Security Inventory
NSX Managers
Endpoint Monitoring
NSX Manager: 192.168.110.15
View Collected Data:
Security Group:
Summary
VM Flows
Process Flows
Start Data Collection for Security Groups
Security Groups with 20 or less VMs can collect data.Check the VM count before choosing. Data collection can be enabled for one Security Group at a time. Only Windows OS is supported. Changes are applied on clicking OK.
1. Select Security Group:
Selected: SG-Desktop Change
VM list for SG-Desktop
win-10-01a
1 items Copy
2. Switch data collection ON or OFF:
Data collection: ON
IMPORTANT: Your completed sessions will be automatically deleted...
OK
Cancel
Start Collecting Data
(Required before using this feature)

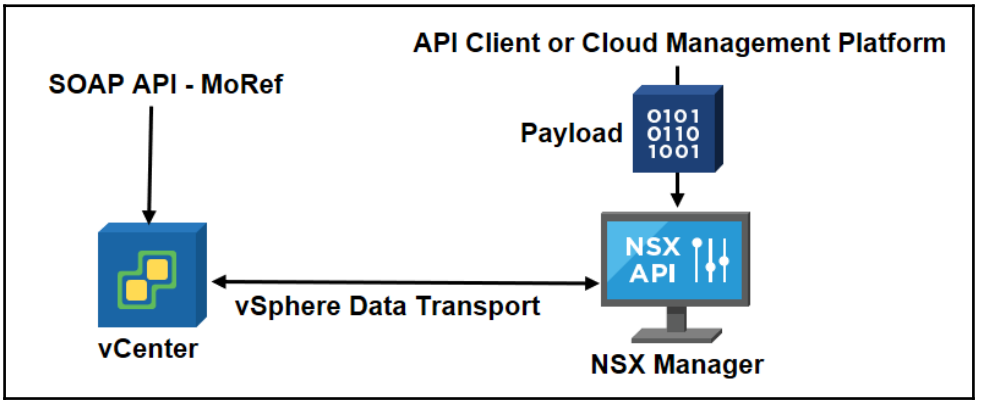

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Tools
Flow Monitoring
Traceflow
Endpoint Monitoring
Networking & Security Inventory
NSX Managers
Endpoint Monitoring
NSX Manager: 192.168.110.15
View Collected Data:
Security Group: SG-Desktop
Time Slots: 2/9/2018 9:48 AM - Present
Delete Data
Collecting Data: SG-Desktop
Stop Collecting Data
Summary
VM Flows
Process Flows
Virtual Machines and Processes
1
Virtual Machine Running.
7
Processes Generating Traffic.
Flows
12
Within Security Group
Outside Security Group


Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Tools
Flow Monitoring
Traceflow
Endpoint Monitoring
Networking & Security Inventory
NSX Managers
Endpoint Monitoring
NSX Manager: 192.168.110.15
View Collected Data:
Security Group: SG-Desktop
Time Slots: 2/9/2018 9:48 AM - 2/9/2018 9:55 AM
Delete Data
Collecting Data: OFF
Start Collecting Data
Summary
VM Flows
Process Flows
Select a VM to view its flows
Filter
VM Name
Flows Within Security Group
Flows Outside Security Group
Shared Service Flows Outside Sec
Shared Service Flows Within Secu
win-10-01a
0
13
0
0
1 items
Click Bubbles or Lines for Details
Same Security Group
Different Security Group
Contains Shared Services
ftp-01a
web-03a
win-10-01a
192.168...
192.168.110.15 - No information available
192.168...
192.168...
Page 1 of 1
1

Chapter 12: Leveraging the VMware NSX REST API for Management and Automation







Working With Logical Switches in a Specific Transport Zone

`GET /api/2.0/vdn/scopes/{scopeId}/virtualwires`

URI Parameters:

`scopeId` (required)	A valid transport zone ID (vdnScope objectId).

Query Parameters:

`startindex`	The starting point for returning results.
`pagesize`	The number of results to return. Range is 1-1024.

Description:
Retrieve information about all logical switches in the specified transport zone (network scope).

`POST /api/2.0/vdn/scopes/{scopeId}/virtualwires`

URI Parameters:

`scopeId` (required)	A valid transport zone ID (vdnScope objectId).

Description:
Create a logical switch.

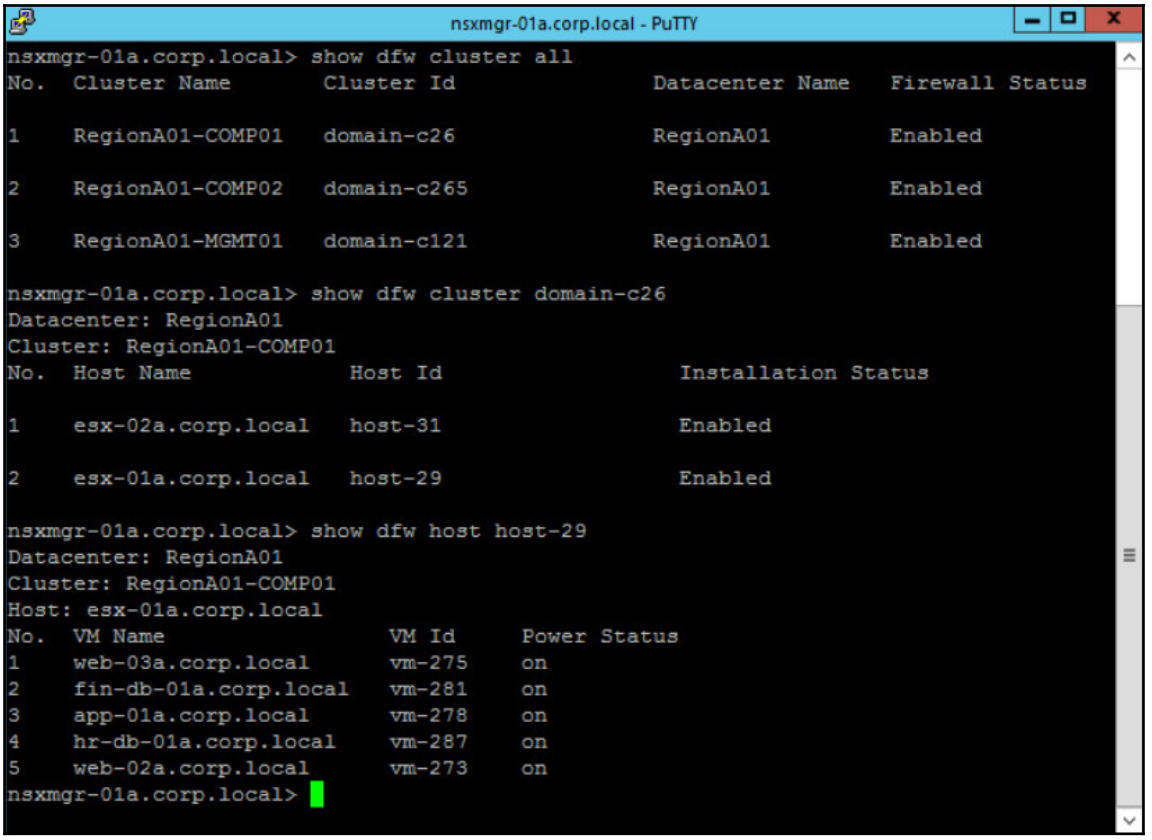
To create a universal logical switch use *universalvdnscope* as the scopeId in the URI and send the request to the primary NSX Manager. Request body parameters:

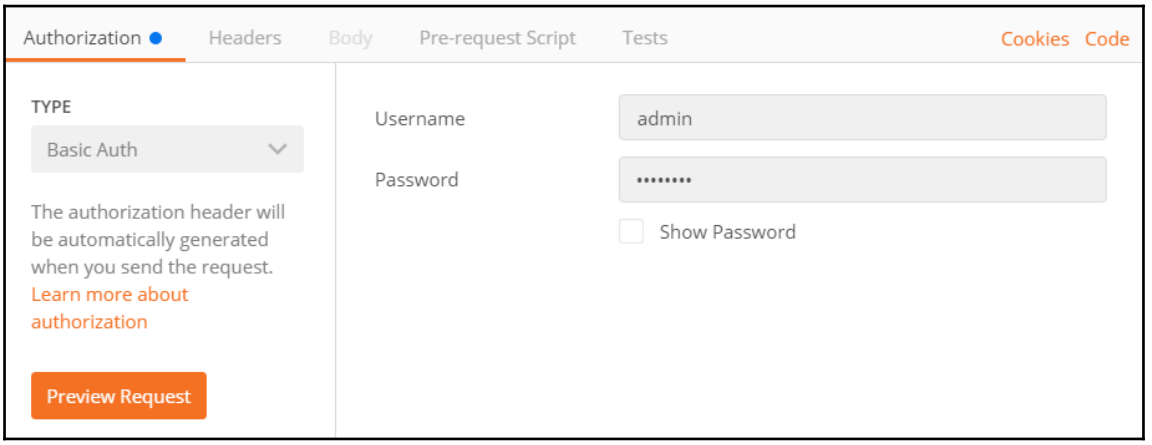
- **name** - Optional. The name of the logical switch.
- **description** - Optional. Description of the logical switch.
- **tenantId** - Required.
- **controlPlaneMode** - Optional. The control plane mode. If not specified, the **controlPlaneMode** of the transport zone is used. It can be one of the following:
  - *UNICAST_MODE*
  - *HYBRID_MODE*
  - *MULTICAST_MODE*
- **guestVlanAllowed** - Optional. Default is *false*.

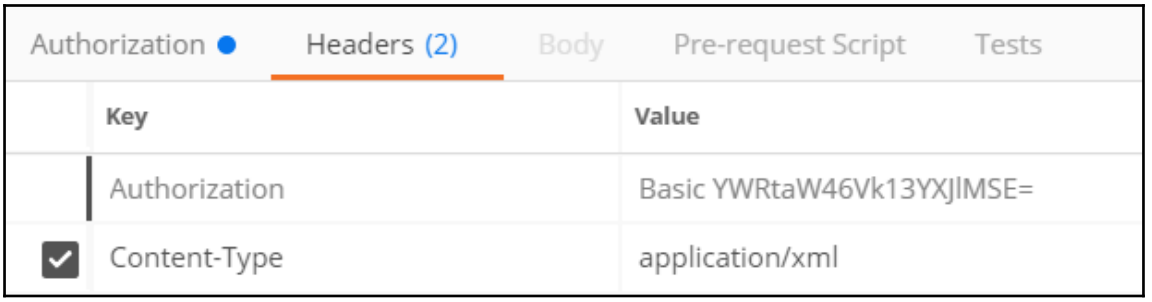
Request:

Body: application/xml

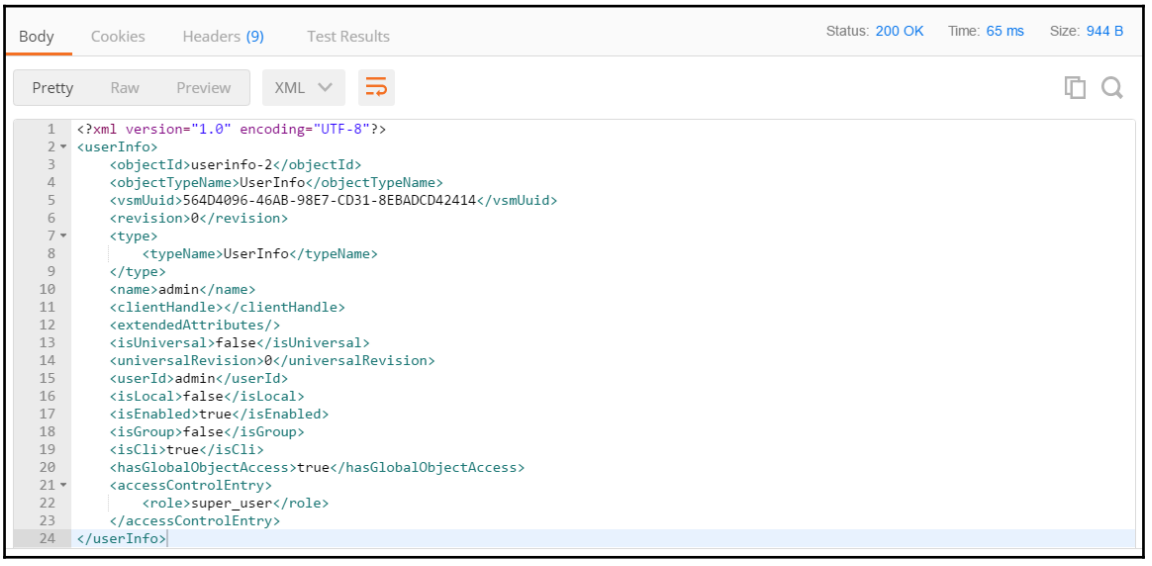
```
<virtualWireCreateSpec>
 <name>Web-Tier-01</name>
 <description>Web tier network</description>
 <tenantId>virtual wire tenant</tenantId>
 <controlPlaneMode>UNICAST_MODE</controlPlaneMode>
 <guestVlanAllowed>false</guestVlanAllowed>
</virtualWireCreateSpec>
```

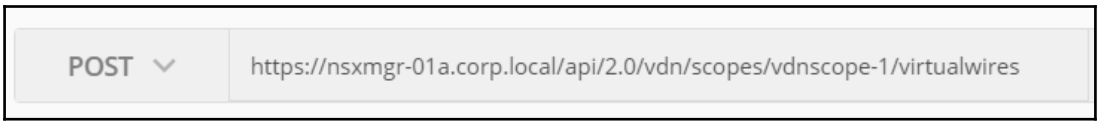

nsxmgr-01a.corp.local - PuTTY
nsxmgr-01a.corp.local> show dfw cluster all
No. Cluster Name Cluster Id Datacenter Name Firewall Status
1 RegionA01-COMP01 domain-c26 RegionA01 Enabled
2 RegionA01-COMP02 domain-c265 RegionA01 Enabled
3 RegionA01-MGMT01 domain-c121 RegionA01 Enabled
nsxmgr-01a.corp.local> show dfw cluster domain-c26
Datacenter: RegionA01
Cluster: RegionA01-COMP01
No. Host Name Host Id Installation Status
1 esx-02a.corp.local host-31 Enabled
2 esx-01a.corp.local host-29 Enabled
nsxmgr-01a.corp.local> show dfw host host-29
Datacenter: RegionA01
Cluster: RegionA01-COMP01
Host: esx-01a.corp.local
No. VM Name VM Id Power Status
1 web-03a.corp.local vm-275 on
2 fin-db-01a.corp.local vm-281 on
3 app-01a.corp.local vm-278 on
4 hr-db-01a.corp.local vm-287 on
5 web-02a.corp.local vm-273 on
nsxmgr-01a.corp.local>

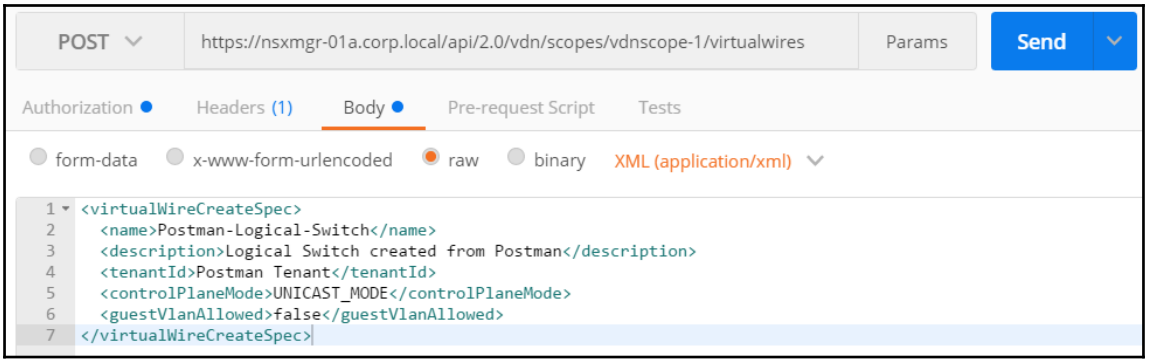

Authorization
Headers
Body
Pre-request Script
Tests
Cookies
Code
TYPE
Basic Auth
The authorization header will be automatically generated when you send the request.
Learn more about authorization
Preview Request
Username
admin
Password
Show Password

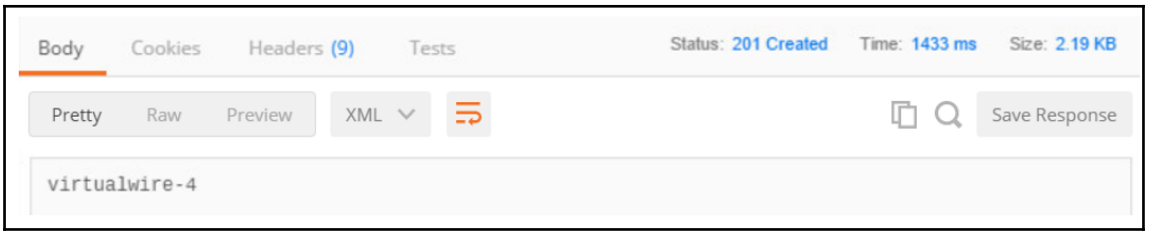

Authorization
Headers (2)
Body
Pre-request Script
Tests
Key
Value
Authorization
Basic YWRtaW46Vk13YXJlMSE=
Content-Type
application/xml

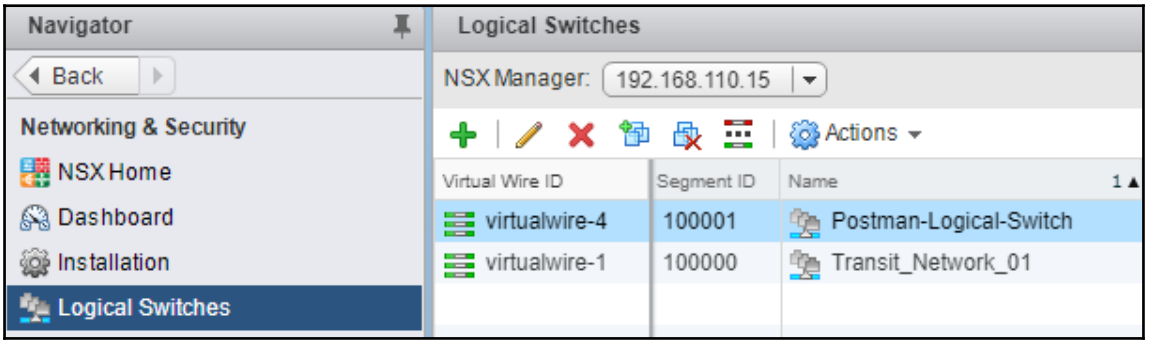

GET
https://nsxmgr-01a.corp.local/api/2.0/services/usermgmt/user/admin
Params
Send
Save

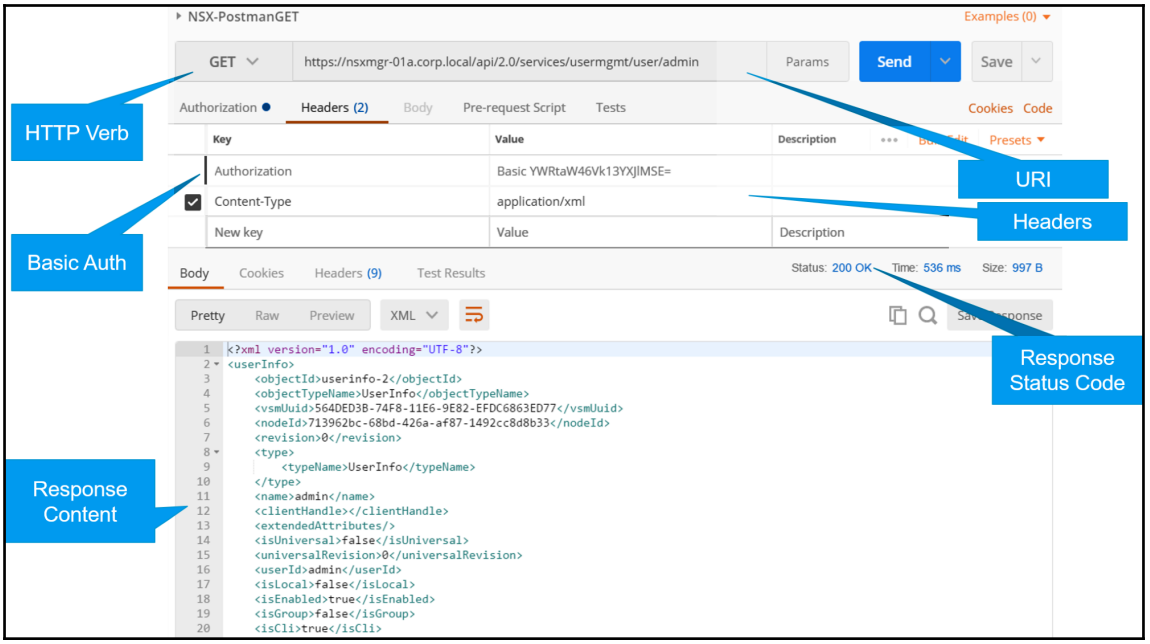

Body
Cookies
Headers (9)
Test Results
Status: 200 OK
Time: 65 ms
Size: 944 B
Pretty
Raw
Preview
XML
<?xml version="1.0" encoding="UTF-8"?>
<userInfo>
<objectId>userinfo-2</objectId>
<objectTypeName>UserInfo</objectTypeName>
<vsmUuid>564D4096-46AB-98E7-CD31-8EBADCD42414</vsmUuid>
<revision>0</revision>
<type>
<typeName>UserInfo</typeName>
</type>
<name>admin</name>
<clientHandle></clientHandle>
<extendedAttributes/>
<isUniversal>false</isUniversal>
<universalRevision>0</universalRevision>
<userId>admin</userId>
<isLocal>false</isLocal>
<isEnabled>true</isEnabled>
<isGroup>false</isGroup>
<isCli>true</isCli>
<hasGlobalObjectAccess>true</hasGlobalObjectAccess>
<accessControlEntry>
<role>super_user</role>
</accessControlEntry>
</userInfo>

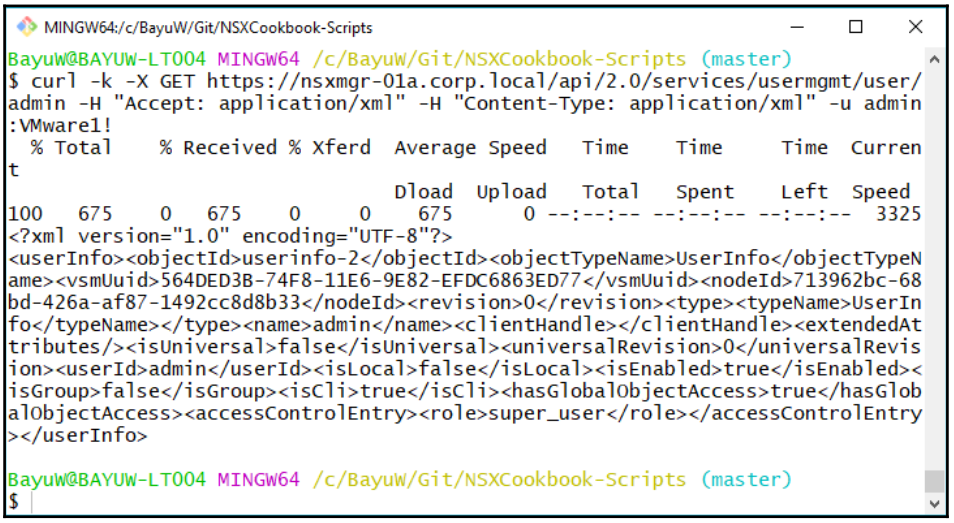

POST
https://nsxmgr-01a.corp.local/api/2.0/vdn/scopes/vdnscope-1/virtualwires


POST
https://nsxmgr-01a.corp.local/api/2.0/vdn/scopes/vdnscope-1/virtualwires
Params
Send
Authorization
Headers (1)
Body
Pre-request Script
Tests
form-data
x-www-form-urlencoded
raw
binary
XML (application/xml)
<virtualWireCreateSpec>
<name>Postman-Logical-Switch</name>
<description>Logical Switch created from Postman</description>
<tenantId>Postman Tenant</tenantId>
<controlPlaneMode>UNICAST_MODE</controlPlaneMode>
<guestVlanAllowed>false</guestVlanAllowed>
</virtualWireCreateSpec>

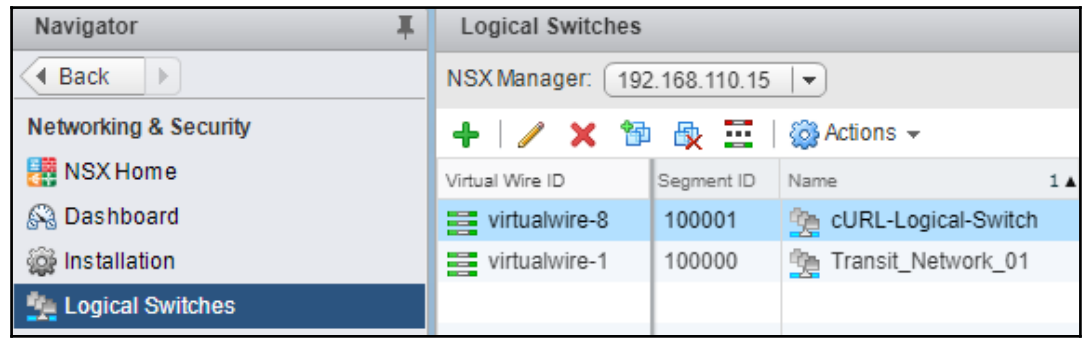

Body
Cookies
Headers (9)
Tests
Status: 201 Created
Time: 1433 ms
Size: 2.19 KB
Pretty
Raw
Preview
XML
Save Response
virtualwire-4

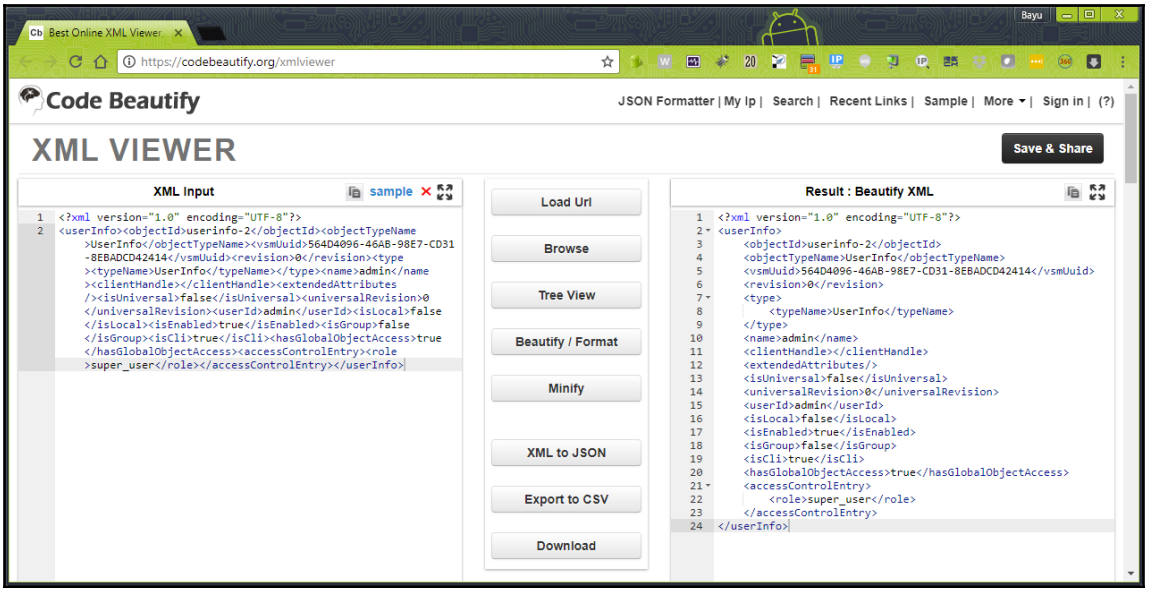

Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
Logical Switches
NSX Manager:
192.168.110.15
Actions
Virtual Wire ID
Segment ID
Name
virtualwire-4
100001
Postman-Logical-Switch
virtualwire-1
100000
Transit_Network_01

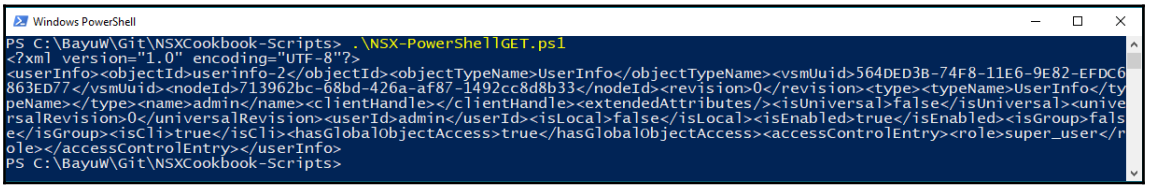

NSX-PostmanGET
Examples (0)
GET
https://nsxmgr-01a.corp.local/api/2.0/services/usermgmt/user/admin
Params
Send
Save
Authorization
Headers (2)
Body
Pre-request Script
Tests
Cookies
Code
Key
Value
Description
Presets
Authorization
Basic YWRtaW46Vk13YXJlMSE=
Content-Type
application/xml
New key
Value
Description
Body
Cookies
Headers (9)
Test Results
Status: 200 OK
Time: 536 ms
Size: 997 B
Pretty
Raw
Preview
XML
HTTP Verb
Basic Auth
URI
Headers
Response Status Code
Response Content
<?xml version="1.0" encoding="UTF-8"?>
<userInfo>
<objectId>userinfo-2</objectId>
<objectTypeName>UserInfo</objectTypeName>
<vsmUuid>564DED3B-74F8-11E6-9E82-EFDC6863ED77</vsmUuid>
<nodeId>713962bc-68bd-426a-af87-1492cc8d8b33</nodeId>
<revision>0</revision>
<type>
<typeName>UserInfo</typeName>
</type>
<name>admin</name>
<clientHandle></clientHandle>
<extendedAttributes/>
<isUniversal>false</isUniversal>
<universalRevision>0</universalRevision>
<userId>admin</userId>
<isLocal>false</isLocal>
<isEnabled>true</isEnabled>
<isGroup>false</isGroup>
<isCli>true</isCli>


MINGW64:/c/BayuW/Git/NSXCookbook-Scripts
BayuW@BAYUW-LT004 MINGW64 /c/BayuW/Git/NSXCookbook-Scripts (master)
$ curl -k -X GET https://nsxmgr-01a.corp.local/api/2.0/services/usermgmt/user/admin -H "Accept: application/xml" -H "Content-Type: application/xml" -u admin:VMware1!
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 675 0 675 0 0 675 0 --:--:-- --:--:-- --:--:-- 3325
<?xml version="1.0" encoding="UTF-8"?>
<userInfo><objectId>userinfo-2</objectId><objectTypeName>UserInfo</objectTypeName><vsmUuid>564DED3B-74F8-11E6-9E82-EFDC6863ED77</vsmUuid><nodeId>713962bc-68bd-426a-af87-1492cc8d8b33</nodeId><revision>0</revision><type><typeName>UserInfo</typeName></type><name>admin</name><clientHandle></clientHandle><extendedAttributes/><isUniversal>false</isUniversal><universalRevision>0</universalRevision><userId>admin</userId><isLocal>false</isLocal><isEnabled>true</isEnabled><isGroup>false</isGroup><isCli>true</isCli><hasGlobalObjectAccess>true</hasGlobalObjectAccess><accessControlEntry><role>super_user</role></accessControlEntry></userInfo>
BayuW@BAYUW-LT004 MINGW64 /c/BayuW/Git/NSXCookbook-Scripts (master)
$

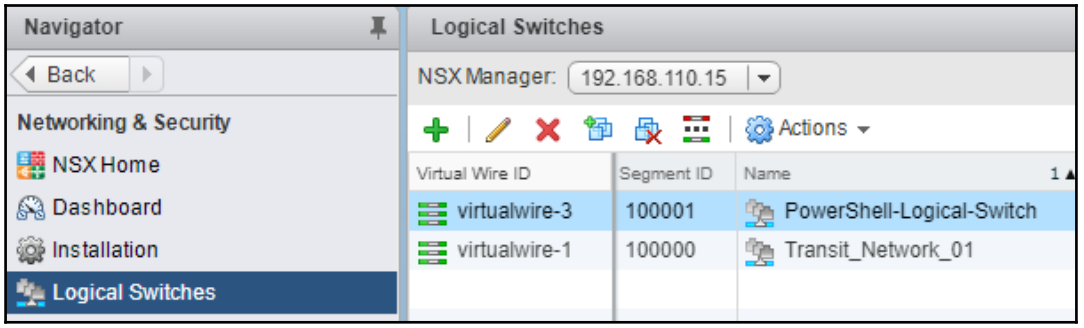
```
MINGW64:/c/BayuW/Git/NSXCookbook-Scripts

BayuW@BAYUW-LT004 MINGW64 /c/BayuW/Git/NSXCookbook-Scripts (master)
$ curl -k -X POST https://nsxmgr-01a.corp.local/api/2.0/vdn/scopes/vdnscope-1/
virtualwires -H "Accept: application/xml" -H "Content-Type: application/xml" -
u admin:VMware1! -d "<virtualWireCreateSpec><name>cURL-Logical-Switch</name><d
escription>Logical Switch created from cURL</description><tenantId>cURL Tenant
</tenantId><controlPlaneMode>UNICAST_MODE</controlPlaneMode><guestVlanAllowed>
false</guestVlanAllowed></virtualWireCreateSpec>"
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Curren
t
                                 Dload  Upload   Total   Spent    Left  Speed
100   274  100    13  100   261     13    261  0:00:01 --:--:--  0:00:01   350
virtualwire-8

BayuW@BAYUW-LT004 MINGW64 /c/BayuW/Git/NSXCookbook-Scripts (master)
$
```

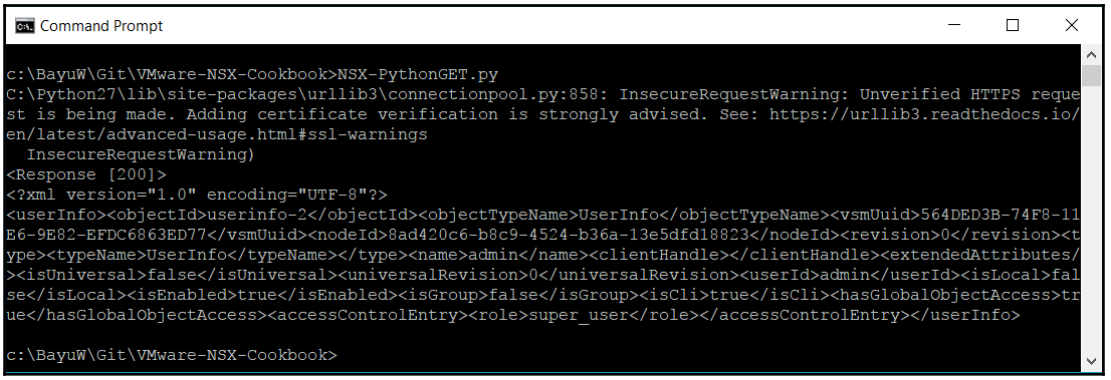


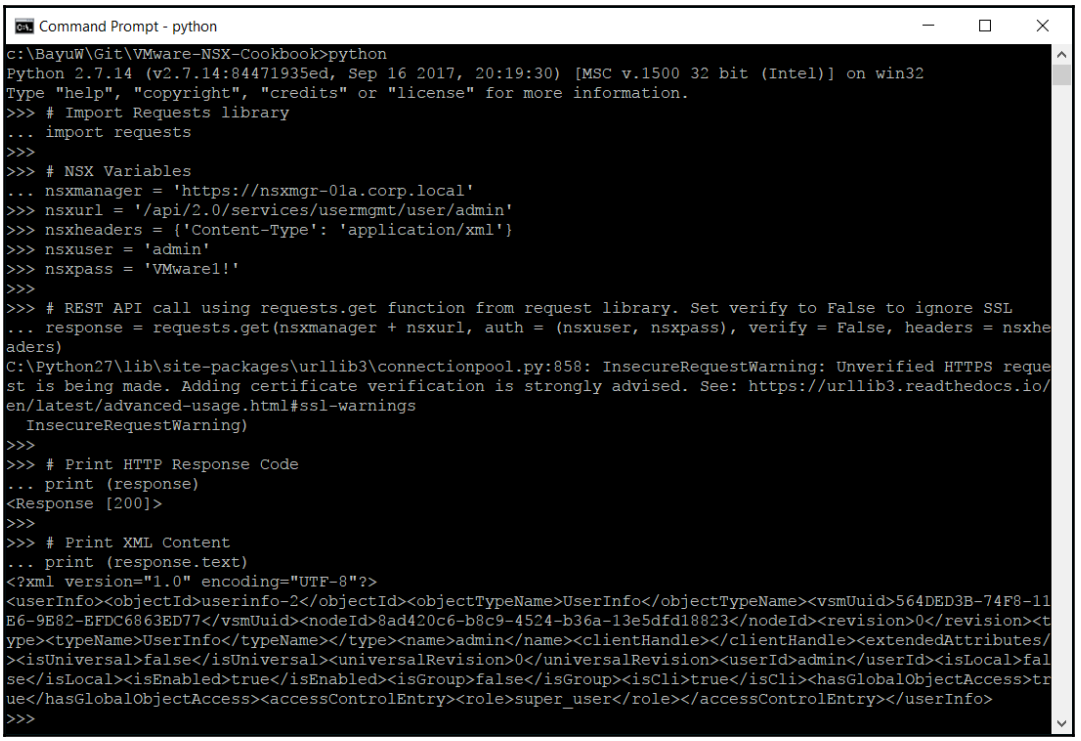

Best Online XML Viewer
https://codebeautify.org/xmlviewer
Code Beautify
JSON Formatter | My Ip | Search | Recent Links | Sample | More | Sign in | (?)
XML VIEWER
Save & Share
XML Input
sample
<?xml version="1.0" encoding="UTF-8"?>
<userInfo><objectId>userinfo-2</objectId><objectTypeName>UserInfo</objectTypeName><vsmUuid>564D4096-46AB-98E7-CD31-8EBADCD42414</vsmUuid><revision>0</revision><type><typeName>UserInfo</typeName></type><name>admin</name><clientHandle></clientHandle><extendedAttributes/><isUniversal>false</isUniversal><universalRevision>0</universalRevision><userId>admin</userId><isLocal>false</isLocal><isEnabled>true</isEnabled><isGroup>false</isGroup><isCli>true</isCli><hasGlobalObjectAccess>true</hasGlobalObjectAccess><accessControlEntry><role>super_user</role></accessControlEntry></userInfo>
Load Url
Browse
Tree View
Beautify / Format
Minify
XML to JSON
Export to CSV
Download
Result : Beautify XML
<?xml version="1.0" encoding="UTF-8"?>
<userInfo>
<objectId>userinfo-2</objectId>
<objectTypeName>UserInfo</objectTypeName>
<vsmUuid>564D4096-46AB-98E7-CD31-8EBADCD42414</vsmUuid>
<revision>0</revision>
<type>
<typeName>UserInfo</typeName>
</type>
<name>admin</name>
<clientHandle></clientHandle>
<extendedAttributes/>
<isUniversal>false</isUniversal>
<universalRevision>0</universalRevision>
<userId>admin</userId>
<isLocal>false</isLocal>
<isEnabled>true</isEnabled>
<isGroup>false</isGroup>
<isCli>true</isCli>
<hasGlobalObjectAccess>true</hasGlobalObjectAccess>
<accessControlEntry>
<role>super_user</role>
</accessControlEntry>
</userInfo>


Windows PowerShell
PS C:\BayuW\Git\NSXCookbook-Scripts> .\NSX-PowerShellGET.ps1
<?xml version="1.0" encoding="UTF-8"?>
<userInfo><objectId>userinfo-2</objectId><objectTypeName>UserInfo</objectTypeName><vsmUuid>564DED3B-74F8-11E6-9E82-EFDC6863ED77</vsmUuid><nodeId>713962bc-68bd-426a-af87-1492cc8d8b33</nodeId><revision>0</revision><type><typeName>UserInfo</typeName></type><name>admin</name><clientHandle></clientHandle><extendedAttributes/><isUniversal>false</isUniversal><universalRevision>0</universalRevision><userId>admin</userId><isLocal>false</isLocal><isEnabled>true</isEnabled><isGroup>false</isGroup><isCli>true</isCli><hasGlobalObjectAccess>true</hasGlobalObjectAccess><accessControlEntry><role>super_user</role></accessControlEntry></userInfo>
PS C:\BayuW\Git\NSXCookbook-Scripts>

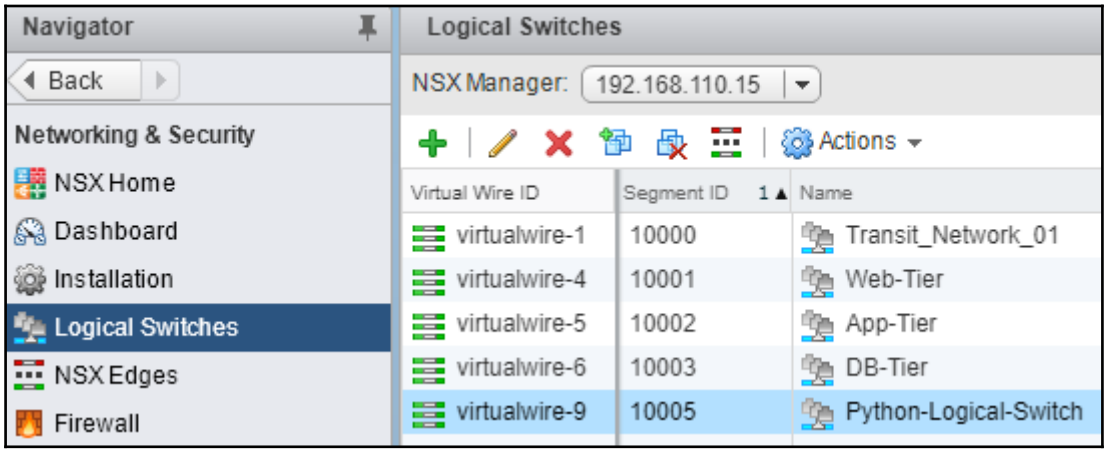
```
Windows PowerShell
PS C:\BayuW\Git\NSXCookbook-Scripts> # NSX Variables
PS C:\BayuW\Git\NSXCookbook-Scripts> $NSXUsername = "admin"
PS C:\BayuW\Git\NSXCookbook-Scripts> $NSXPassword = "VMware1!"
PS C:\BayuW\Git\NSXCookbook-Scripts> $NSXManager = "https://nsxmgr-01a.corp.local"
PS C:\BayuW\Git\NSXCookbook-Scripts> $NSXURI = "/api/2.0/vdn/scopes/vdnscope-1/virtualwires"
PS C:\BayuW\Git\NSXCookbook-Scripts>
PS C:\BayuW\Git\NSXCookbook-Scripts> # NSX Authorization Header
PS C:\BayuW\Git\NSXCookbook-Scripts> $NSXAuth = [System.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes($
NSXUsername + ":" + $NSXPassword))
PS C:\BayuW\Git\NSXCookbook-Scripts> $NSXAuthHeader = @{"Authorization"="Basic $NSXAuth"}
PS C:\BayuW\Git\NSXCookbook-Scripts>
PS C:\BayuW\Git\NSXCookbook-Scripts> # NSX XML Payload
PS C:\BayuW\Git\NSXCookbook-Scripts> [xml]$XMLBody = "<virtualWireCreateSpec>
>>   <name>PowerShell-Logical-Switch</name>
>>   <description>Logical Switch created from PowerShell</description>
>>   <tenantId>PowerShell Tenant</tenantId>
>>   <controlPlaneMode>UNICAST_MODE</controlPlaneMode>
>>   <guestVlanAllowed>false</guestVlanAllowed>
>> </virtualWireCreateSpec>"
PS C:\BayuW\Git\NSXCookbook-Scripts>
PS C:\BayuW\Git\NSXCookbook-Scripts> # Add code to allow untrusted SSL certs - taken from https://d-fens.ch/2013/12/20/n
obrainer-ssl-connection-error-when-using-powershell/
PS C:\BayuW\Git\NSXCookbook-Scripts> Add-Type @"
>>     using System;
>>     using System.Net;
>>     using System.Net.Security;
>>     using System.Security.Cryptography.X509Certificates;
>>     public class ServerCertificateValidationCallback
>>     {
>>         public static void Ignore()
>>         {
>>             ServicePointManager.ServerCertificateValidationCallback +=
>>                 delegate
>>                 (
>>                     Object obj,
>>                     X509Certificate certificate,
>>                     X509Chain chain,
>>                     SslPolicyErrors errors
>>                 )
>>                 {
>>                     return true;
>>                 };
>>         }
>>     }
>> "@
PS C:\BayuW\Git\NSXCookbook-Scripts> [ServerCertificateValidationCallback]::Ignore();
PS C:\BayuW\Git\NSXCookbook-Scripts>
PS C:\BayuW\Git\NSXCookbook-Scripts> # REST API Call via Invoke-WebRequest cmdlet
PS C:\BayuW\Git\NSXCookbook-Scripts> $response = Invoke-WebRequest -Uri "$NSXManager$NSXURI" -Method:Post -Body $XMLBody
 -Headers $NSXAuthHeader -ContentType "application/xml" -ErrorAction:Stop -TimeoutSec 180
PS C:\BayuW\Git\NSXCookbook-Scripts> Write-Host "$response"
virtualwire-3
PS C:\BayuW\Git\NSXCookbook-Scripts>
```




Command Prompt
c:\BayuW\Git\VMware-NSX-Cookbook>NSX-PythonGET.py
C:\Python27\lib\site-packages\urllib3\connectionpool.py:858: InsecureRequestWarning: Unverified HTTPS reque
st is being made. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/
en/latest/advanced-usage.html#ssl-warnings
InsecureRequestWarning)
<Response [200]>
<?xml version="1.0" encoding="UTF-8"?>
<userInfo><objectId>userinfo-2</objectId><objectTypeName>UserInfo</objectTypeName><vsmUuid>564DED3B-74F8-11
E6-9E82-EFDC6863ED77</vsmUuid><nodeId>8ad420c6-b8c9-4524-b36a-13e5dfd18823</nodeId><revision>0</revision><t
ype><typeName>UserInfo</typeName></type><name>admin</name><clientHandle></clientHandle><extendedAttributes/
><isUniversal>false</isUniversal><universalRevision>0</universalRevision><userId>admin</userId><isLocal>fal
se</isLocal><isEnabled>true</isEnabled><isGroup>false</isGroup><isCli>true</isCli><hasGlobalObjectAccess>tr
ue</hasGlobalObjectAccess><accessControlEntry><role>super_user</role></accessControlEntry></userInfo>
c:\BayuW\Git\VMware-NSX-Cookbook>


Command Prompt - python
c:\BayuW\Git\VMware-NSX-Cookbook>python
Python 2.7.14 (v2.7.14:84471935ed, Sep 16 2017, 20:19:30) [MSC v.1500 32 bit (Intel)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> # Import Requests library
... import requests
>>>
>>> # NSX Variables
... nsxmanager = 'https://nsxmgr-01a.corp.local'
>>> nsxurl = '/api/2.0/services/usermgmt/user/admin'
>>> nsxheaders = {'Content-Type': 'application/xml'}
>>> nsxuser = 'admin'
>>> nsxpass = 'VMware1!'
>>>
>>> # REST API call using requests.get function from request library. Set verify to False to ignore SSL
... response = requests.get(nsxmanager + nsxurl, auth = (nsxuser, nsxpass), verify = False, headers = nsxhe
aders)
C:\Python27\lib\site-packages\urllib3\connectionpool.py:858: InsecureRequestWarning: Unverified HTTPS reque
st is being made. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/
en/latest/advanced-usage.html#ssl-warnings
InsecureRequestWarning)
>>>
>>> # Print HTTP Response Code
... print (response)
<Response [200]>
>>>
>>> # Print XML Content
... print (response.text)
<?xml version="1.0" encoding="UTF-8"?>
<userInfo><objectId>userinfo-2</objectId><objectTypeName>UserInfo</objectTypeName><vsmUuid>564DED3B-74F8-11
E6-9E82-EFDC6863ED77</vsmUuid><nodeId>8ad420c6-b8c9-4524-b36a-13e5dfd18823</nodeId><revision>0</revision><t
ype><typeName>UserInfo</typeName></type><name>admin</name><clientHandle></clientHandle><extendedAttributes/
><isUniversal>false</isUniversal><universalRevision>0</universalRevision><userId>admin</userId><isLocal>fal
se</isLocal><isEnabled>true</isEnabled><isGroup>false</isGroup><isCli>true</isCli><hasGlobalObjectAccess>tr
ue</hasGlobalObjectAccess><accessControlEntry><role>super_user</role></accessControlEntry></userInfo>
>>>

```
Command Prompt

c:\BayuW\Git\VMware-NSX-Cookbook>NSX-PythonPOST.py
C:\Python27\lib\site-packages\urllib3\connectionpool.py:858: InsecureRequestWarning: Unverified HTTPS reque
st is being made. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/
en/latest/advanced-usage.html#ssl-warnings
  InsecureRequestWarning)
<Response [201]>
virtualwire-9

c:\BayuW\Git\VMware-NSX-Cookbook>
```



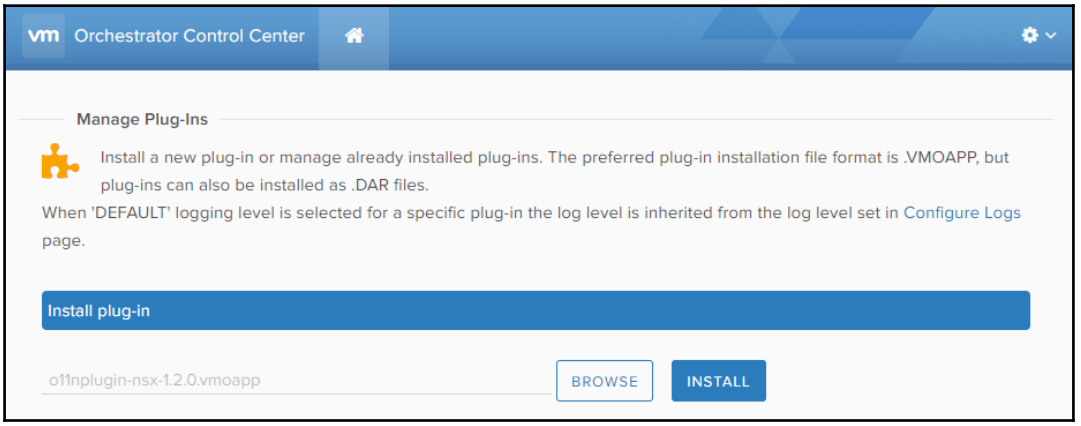
GENERATE CODE SNIPPETS

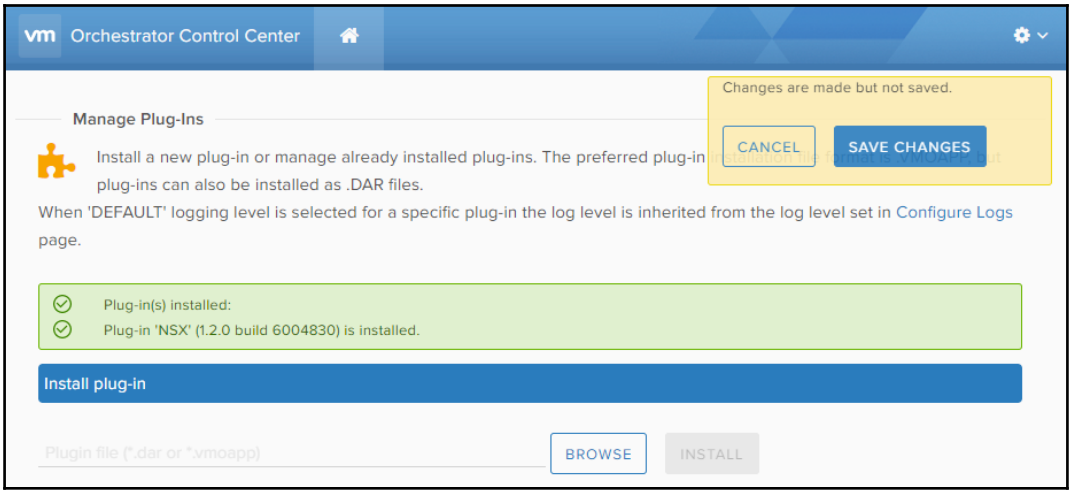
Python Requests

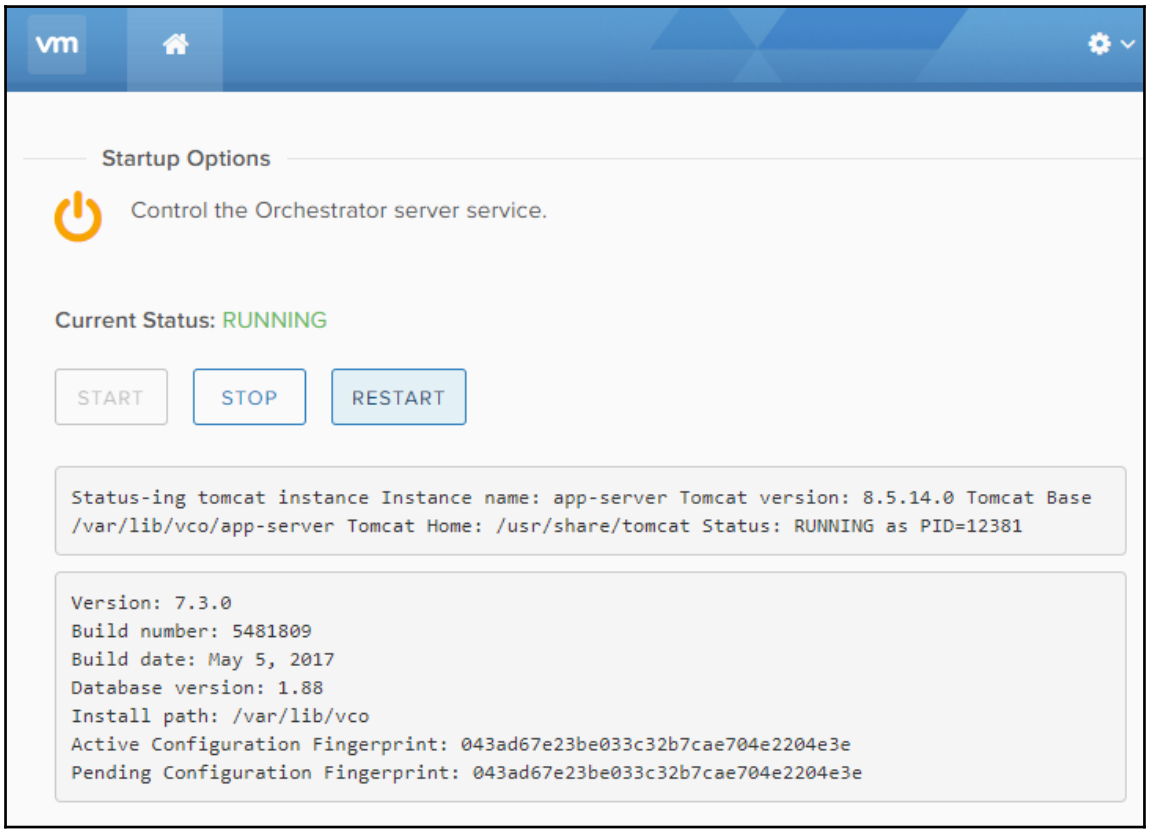
Copy to Clipboard

```python
import requests

url = "https://nsxmgr-01a.corp.local/api/2.0/services/usermgmt/user/admin"

headers = {
    'Content-Type': "application/xml",
    'Cache-Control': "no-cache",
    'Postman-Token': "0e3e668e-206e-e23d-c60e-723a6f56f9a8"
    }

response = requests.request("POST", url, headers=headers)

print(response.text)
```

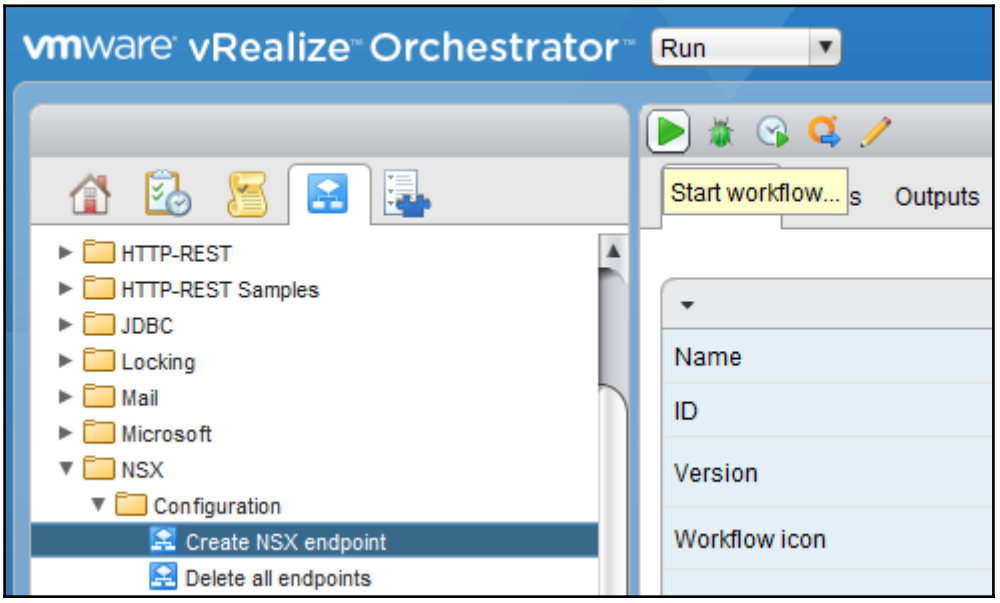

Home / VMware Realize Orchestrator Plugin for NSX 1.2.0
Download VMware Realize Orchestrator Plugin for NSX 1.2.0
Product Resources
View My Download History
Product Info
Documentation
Community
Version 1.2.0
Description VMware Realize Orchestrator Plugin for NSX 1.2.0
Documentation Release Notes
Release Date 2017-08-10
Type Drivers & Tools
Product Downloads
Version History
Product/Details
VMware vRealize Orchestrator Plugin 1.2.0 for NSX
File size: 6.68 MB
File type: vmoapp
Download
Download Manager
Name: o11nplugin-nsx-1.2.0.vmoapp
Release Date: 2017-08-03
Build Number: 6004830
VMware vRealize Orchestrator Plugin 1.2.0 for NSX
NSX - vRO Plugin 1.2.0. This Plug-in can be utilized by vRO 7.2.0, NSX-vSphere 6.3.3, NSX-vSphere 6.2.8
MD5SUM: 2fc8ab9d25ecdec7f77d9492b8eeceff
SHA1SUM: 34a38aeb427fc1aa56c77f461140a4b4ecfea75f
SHA256SUM:
c39ad6fbf245ad4d062fb38973d47f83f0bc2760cb7487de09c0e2eeb77fd1c5
Information about MD5 checksums and SHA1 checksums and SHA256 checksums .

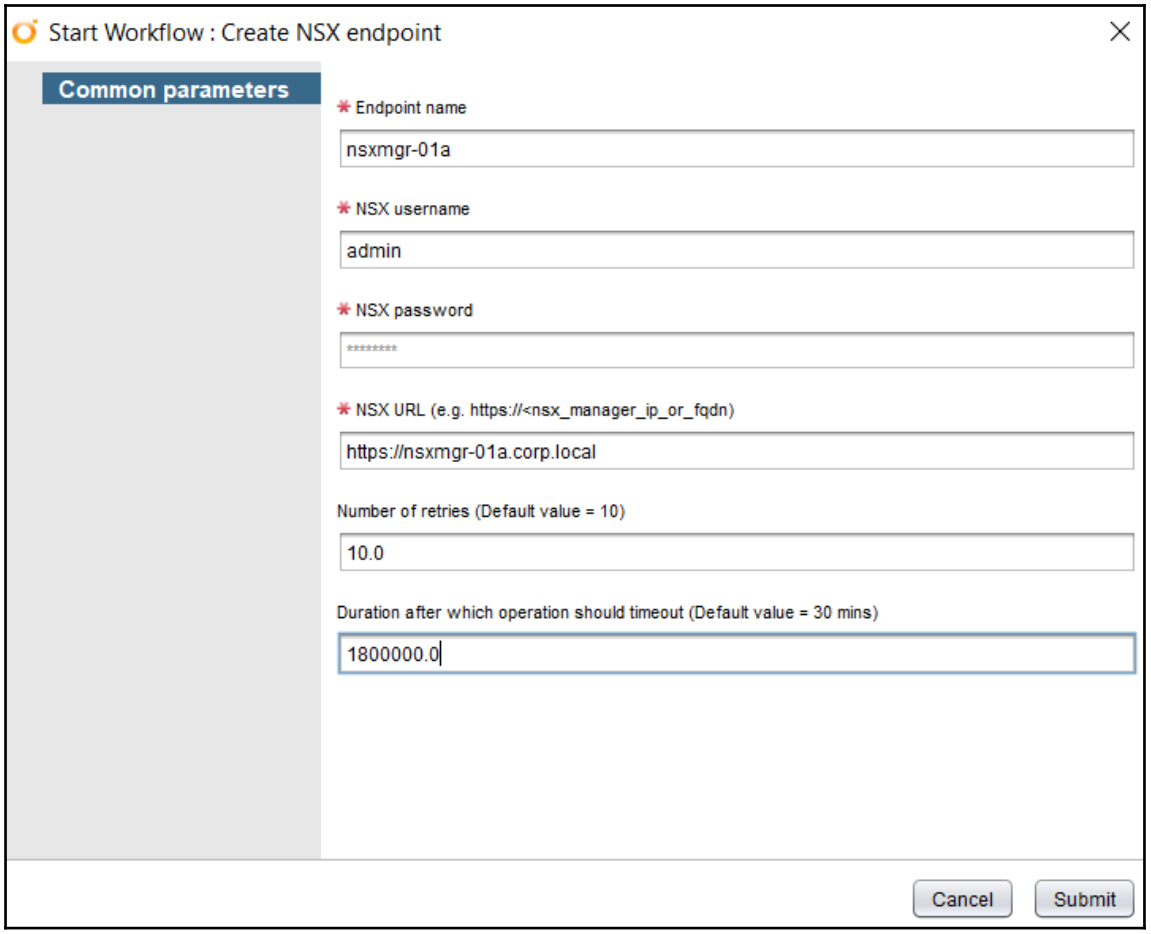

vm Orchestrator Control Center
Manage Plug-Ins
Install a new plug-in or manage already installed plug-ins. The preferred plug-in installation file format is .VMOAPP, but plug-ins can also be installed as .DAR files.
When 'DEFAULT' logging level is selected for a specific plug-in the log level is inherited from the log level set in Configure Logs page.
Install plug-in
o11nplugin-nsx-1.2.0.vmoapp
BROWSE
INSTALL

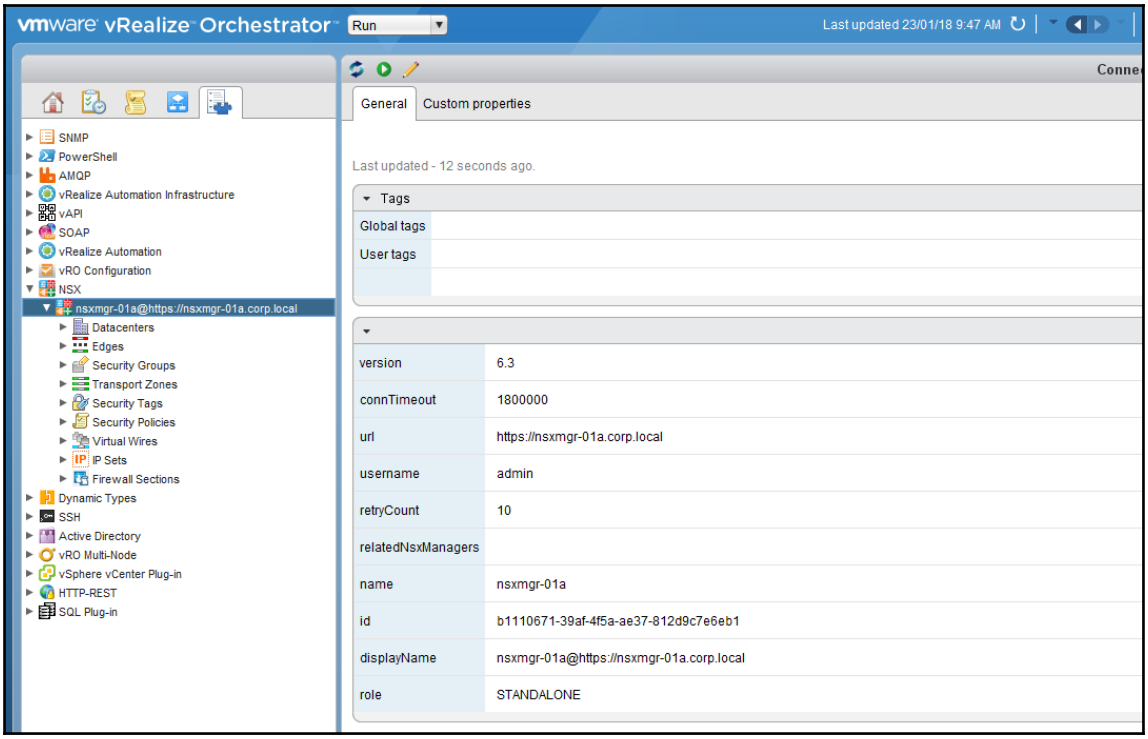

Orchestrator Control Center
Changes are made but not saved.
CANCEL
SAVE CHANGES
Manage Plug-Ins
Install a new plug-in or manage already installed plug-ins. The preferred plug-in
plug-ins can also be installed as .DAR files.
When 'DEFAULT' logging level is selected for a specific plug-in the log level is inherited from the log level set in Configure Logs
page.
Plug-in(s) installed:
Plug-in 'NSX' (1.2.0 build 6004830) is installed.
Install plug-in
Plugin file (*.dar or *.vmoapp)
BROWSE
INSTALL

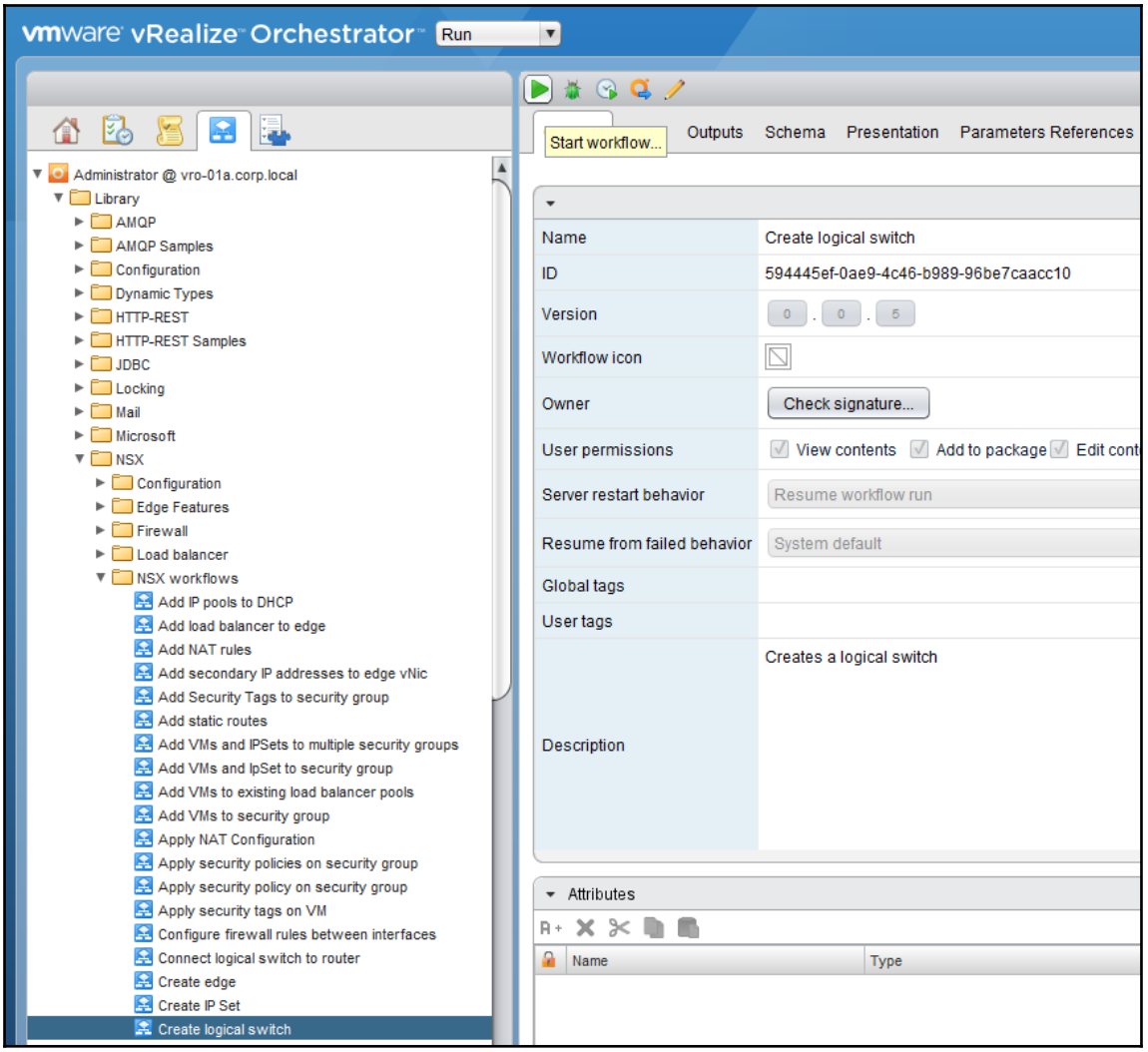

Startup Options
Control the Orchestrator server service.
Current Status: RUNNING
START
STOP
RESTART
Status-ing tomcat instance Instance name: app-server Tomcat version: 8.5.14.0 Tomcat Base
/var/lib/vco/app-server Tomcat Home: /usr/share/tomcat Status: RUNNING as PID=12381
Version: 7.3.0
Build number: 5481809
Build date: May 5, 2017
Database version: 1.88
Install path: /var/lib/vco
Active Configuration Fingerprint: 043ad67e23be033c32b7cae704e2204e3e
Pending Configuration Fingerprint: 043ad67e23be033c32b7cae704e2204e3e

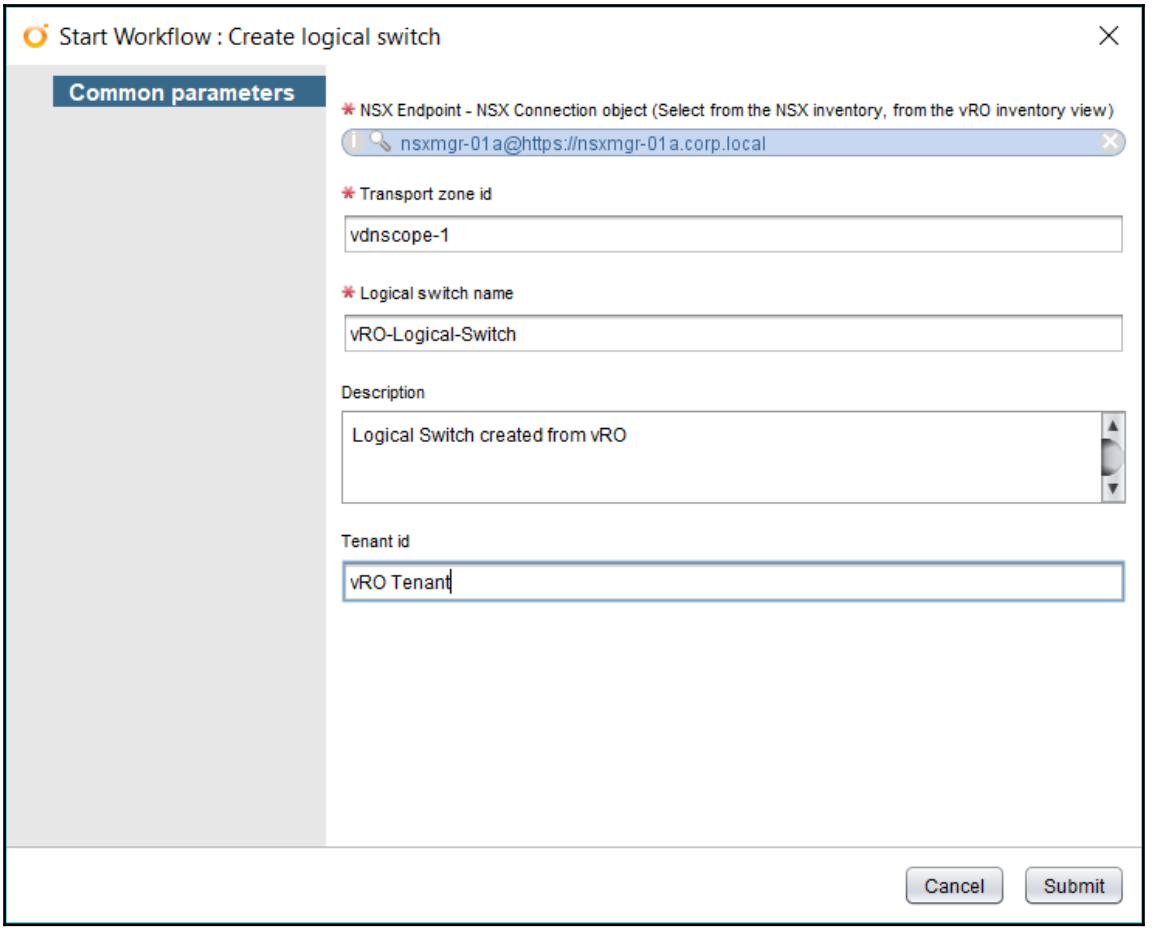
Plug-In	Logging level	Enable plug-in
AD 3.0.5.5377446 Active Directory	DEFAULT	
AMQP 1.0.4.5244874 AMQP Plug-in	DEFAULT	
Configurator 7.3.0.5481809 Configuration plug-in for vRealize Orchestrator	DEFAULT	
DynamicTypes 1.3.0.5416411 Dynamic Types plug-in for vRealize Orchestrator	DEFAULT	
Enums 7.0.1.4939616 Common enumerated types	Select...	
Library 7.0.1.4939616 Library plug-in for vRealize Orchestrator	Select...	
Mail 7.0.1.4939616 Mail Plug-in	DEFAULT	
NSX 1.2.0.6004830 NSX Plug-in for vCenter Orchestrator	DEFAULT	

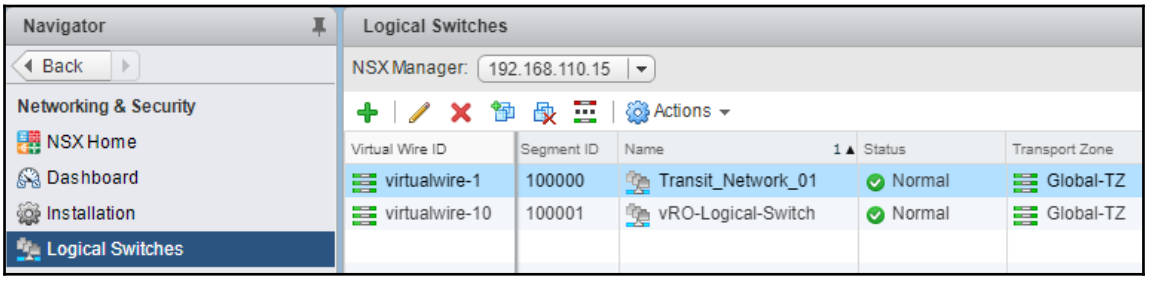


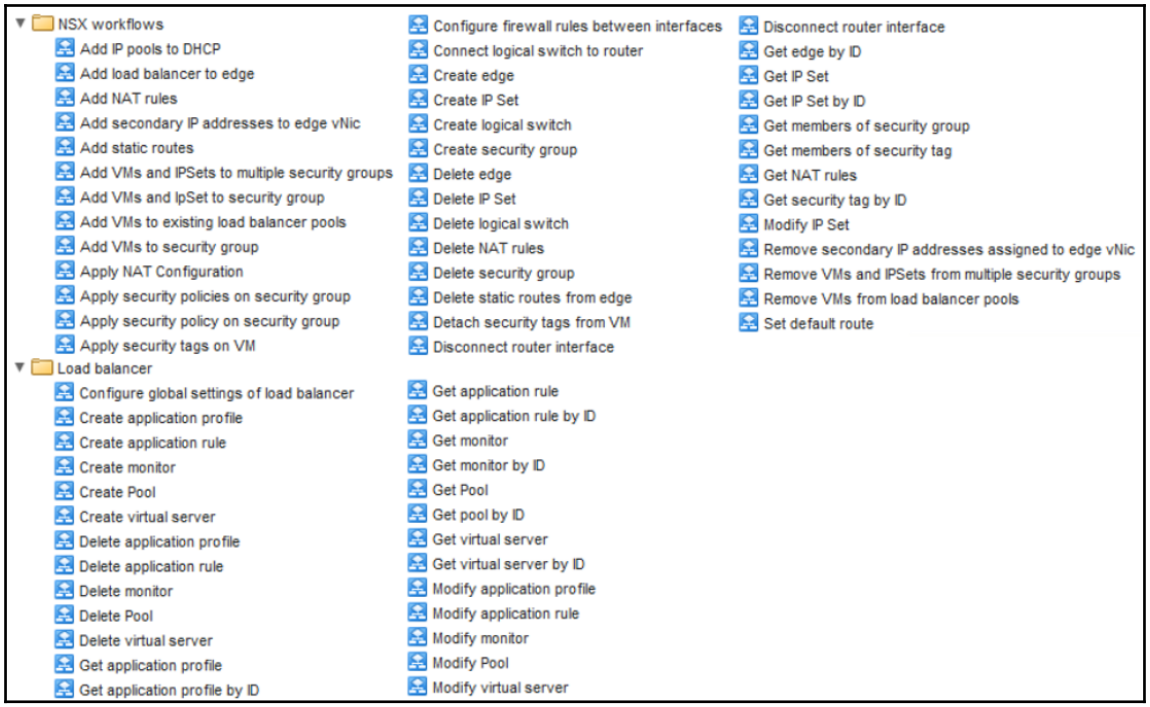

Start Workflow : Create NSX endpoint
Common parameters
* Endpoint name
nsxmgr-01a
* NSX username
admin
* NSX password
****
* NSX URL (e.g. https://<nsx_manager_ip_or_fqdn)
https://nsxmgr-01a.corp.local
Number of retries (Default value = 10)
10.0
Duration after which operation should timeout (Default value = 30 mins)
1800000.0
Cancel
Submit

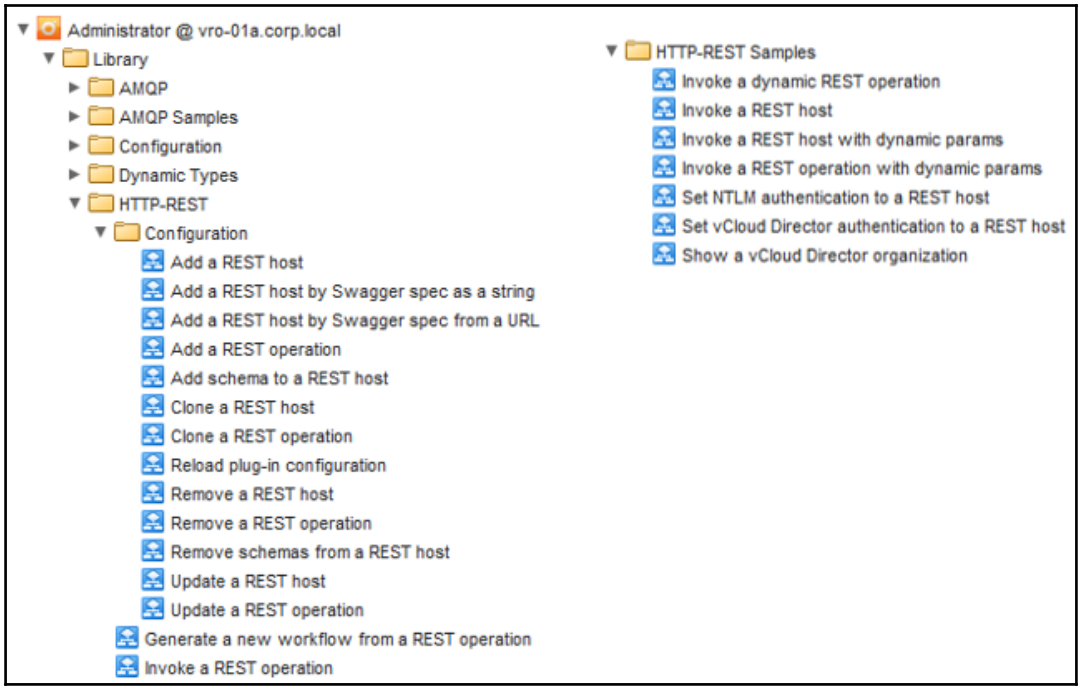

vmware vRealize Orchestrator
Run
Last updated 23/01/18 9:47 AM
SNMP
PowerShell
AMQP
vRealize Automation Infrastructure
vAPI
SOAP
vRealize Automation
vRO Configuration
NSX
nsxmgr-01a@https://nsxmgr-01a.corp.local
Datacenters
Edges
Security Groups
Transport Zones
Security Tags
Security Policies
Virtual Wires
IP Sets
Firewall Sections
Dynamic Types
SSH
Active Directory
vRO Multi-Node
vSphere vCenter Plug-in
HTTP-REST
SQL Plug-in
General
Custom properties
Last updated - 12 seconds ago.
Tags
Global tags
User tags
version 6.3
connTimeout 1800000
url https://nsxmgr-01a.corp.local
username admin
retryCount 10
relatedNsxManagers
name nsxmgr-01a
id b1110671-39af-4f5a-ae37-812d9c7e6eb1
displayName nsxmgr-01a@https://nsxmgr-01a.corp.local
role STANDALONE


vmware vRealize Orchestrator
Run
Administrator @ vro-01a.corp.local
Library
AMQP
AMQP Samples
Configuration
Dynamic Types
HTTP-REST
HTTP-REST Samples
JDBC
Locking
Mail
Microsoft
NSX
Configuration
Edge Features
Firewall
Load balancer
NSX workflows
Add IP pools to DHCP
Add load balancer to edge
Add NAT rules
Add secondary IP addresses to edge vNic
Add Security Tags to security group
Add static routes
Add VMs and IPSets to multiple security groups
Add VMs and IpSet to security group
Add VMs to existing load balancer pools
Add VMs to security group
Apply NAT Configuration
Apply security policies on security group
Apply security policy on security group
Apply security tags on VM
Configure firewall rules between interfaces
Connect logical switch to router
Create edge
Create IP Set
Create logical switch
Start workflow...
Outputs
Schema
Presentation
Parameters References
Name
Create logical switch
ID
594445ef-0ae9-4c46-b989-96be7caacc10
Version
0 . 0 . 5
Workflow icon
Owner
Check signature...
User permissions
View contents
Add to package
Edit cont
Server restart behavior
Resume workflow run
Resume from failed behavior
System default
Global tags
User tags
Description
Creates a logical switch
Attributes
Name
Type


Start Workflow : Create logical switch
Common parameters
* NSX Endpoint - NSX Connection object (Select from the NSX inventory, from the vRO inventory view)
nsxmgr-01a@https://nsxmgr-01a.corp.local
* Transport zone id
vdnscope-1
* Logical switch name
vRO-Logical-Switch
Description
Logical Switch created from vRO
Tenant id
vRO Tenant
Cancel
Submit


Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
Logical Switches
NSX Manager: 192.168.110.15
Actions
Virtual Wire ID
Segment ID
Name
Status
Transport Zone
virtualwire-1
100000
Transit_Network_01
Normal
Global-TZ
virtualwire-10
100001
vRO-Logical-Switch
Normal
Global-TZ


NSX workflows
Add IP pools to DHCP
Add load balancer to edge
Add NAT rules
Add secondary IP addresses to edge vNic
Add static routes
Add VMs and IPSets to multiple security groups
Add VMs and IpSet to security group
Add VMs to existing load balancer pools
Add VMs to security group
Apply NAT Configuration
Apply security policies on security group
Apply security policy on security group
Apply security tags on VM
Configure firewall rules between interfaces
Connect logical switch to router
Create edge
Create IP Set
Create logical switch
Create security group
Delete edge
Delete IP Set
Delete logical switch
Delete NAT rules
Delete security group
Delete static routes from edge
Detach security tags from VM
Disconnect router interface
Disconnect router interface
Get edge by ID
Get IP Set
Get IP Set by ID
Get members of security group
Get members of security tag
Get NAT rules
Get security tag by ID
Modify IP Set
Remove secondary IP addresses assigned to edge vNic
Remove VMs and IPSets from multiple security groups
Remove VMs from load balancer pools
Set default route
Load balancer
Configure global settings of load balancer
Create application profile
Create application rule
Create monitor
Create Pool
Create virtual server
Delete application profile
Delete application rule
Delete monitor
Delete Pool
Delete virtual server
Get application profile
Get application profile by ID
Get application rule
Get application rule by ID
Get monitor
Get monitor by ID
Get Pool
Get pool by ID
Get virtual server
Get virtual server by ID
Modify application profile
Modify application rule
Modify monitor
Modify Pool
Modify virtual server


Administrator @ vro-01a.corp.local
Library
AMQP
AMQP Samples
Configuration
Dynamic Types
HTTP-REST
Configuration
Add a REST host
Add a REST host by Swagger spec as a string
Add a REST host by Swagger spec from a URL
Add a REST operation
Add schema to a REST host
Clone a REST host
Clone a REST operation
Reload plug-in configuration
Remove a REST host
Remove a REST operation
Remove schemas from a REST host
Update a REST host
Update a REST operation
Generate a new workflow from a REST operation
Invoke a REST operation
HTTP-REST Samples
Invoke a dynamic REST operation
Invoke a REST host
Invoke a REST host with dynamic params
Invoke a REST operation with dynamic params
Set NTLM authentication to a REST host
Set vCloud Director authentication to a REST host
Show a vCloud Director organization