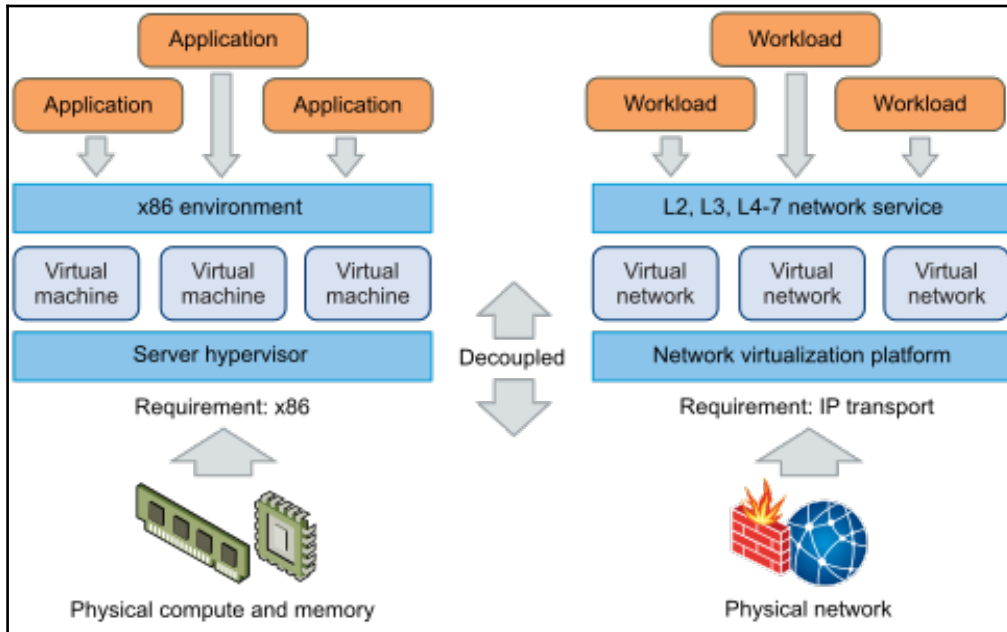
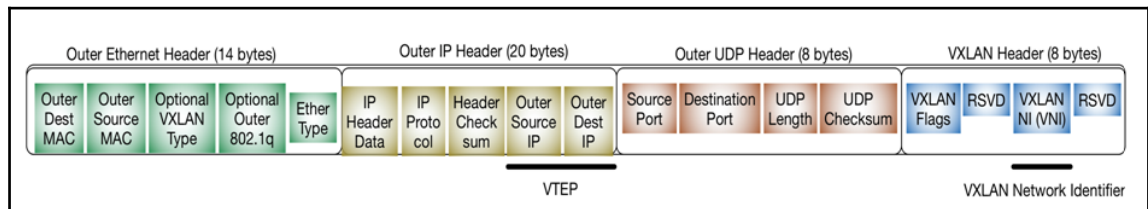
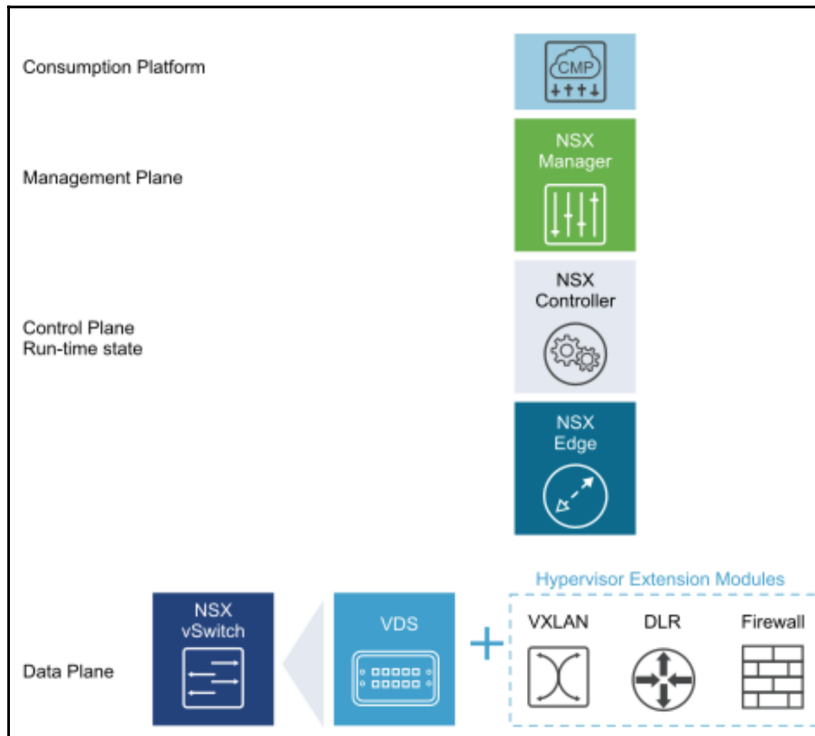
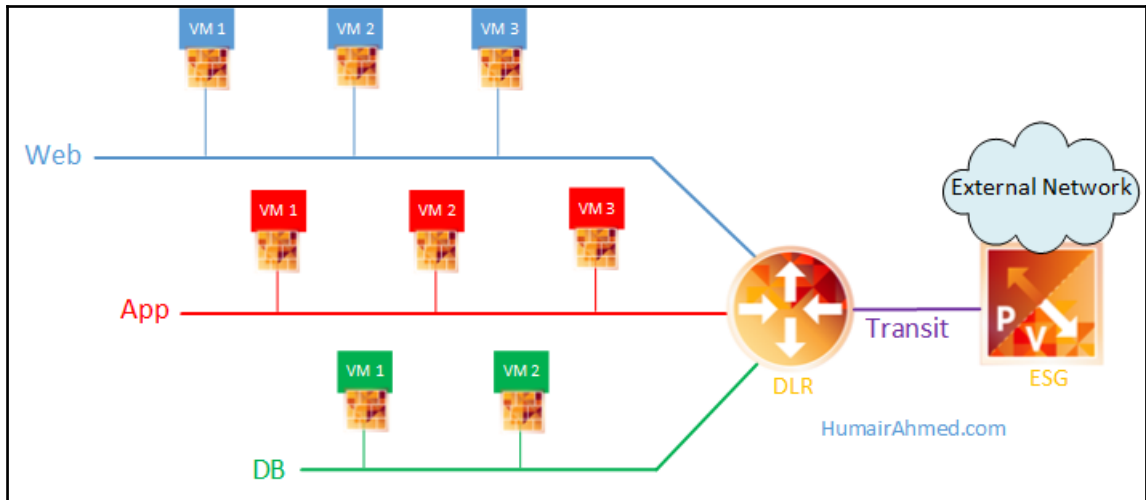
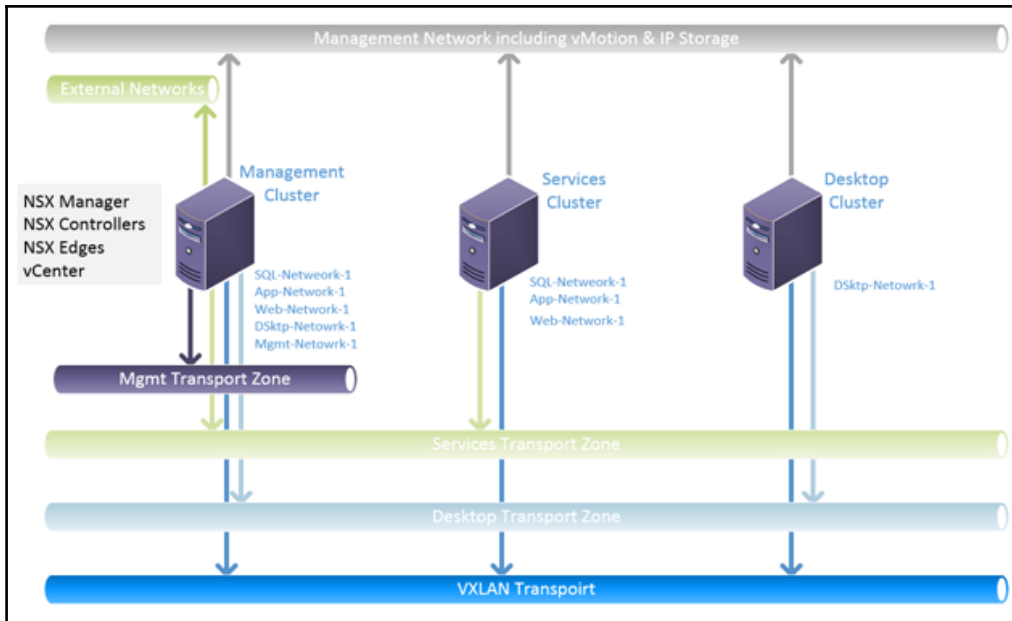


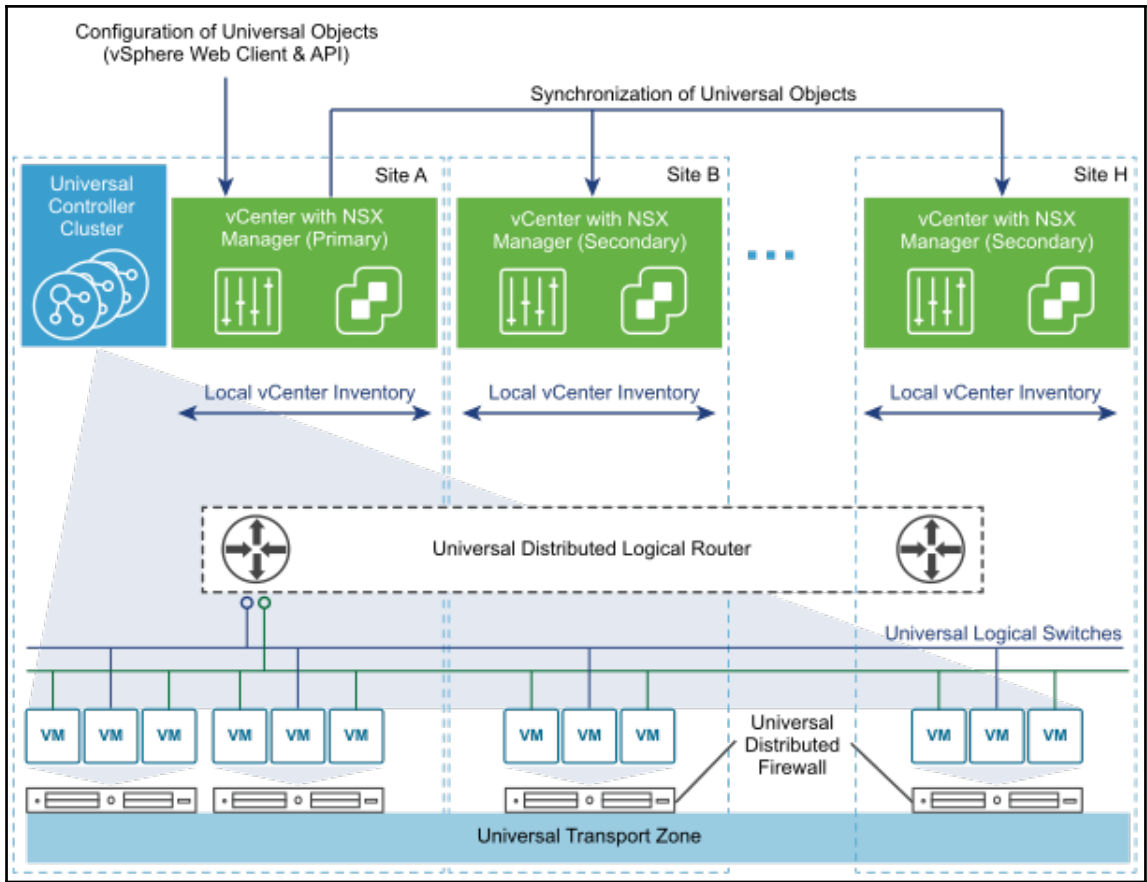
# Chapter 01: Introduction to Network Virtualization



# Chapter 02: NSX Core Components

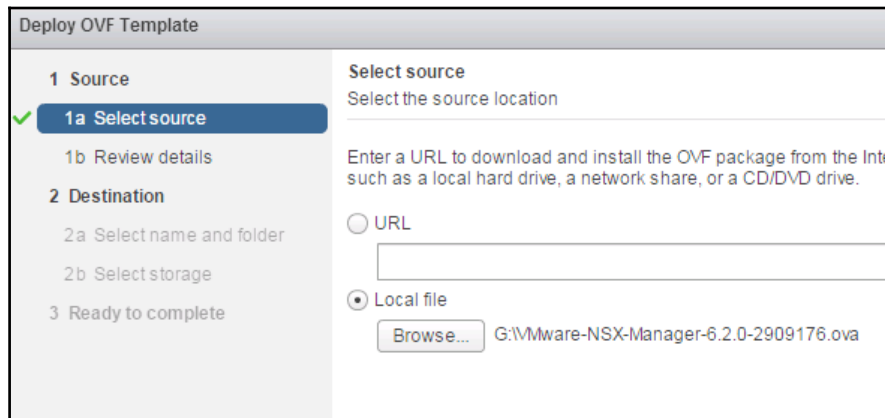
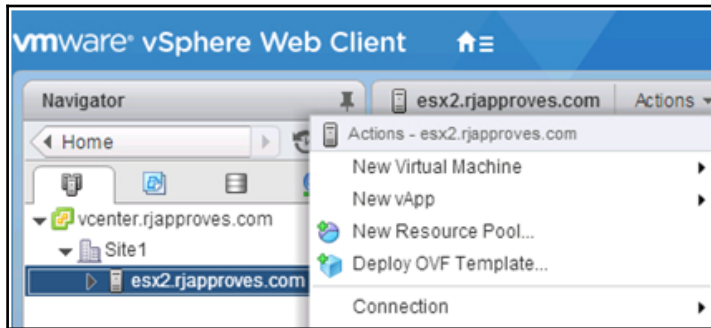








# Chapter 03: NSX Installation and Configuration



**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

**Review details**  
Verify the template details.

**⚠ The OVF package contains advanced configuration options, which might pose a security risk. Review the advanced configuration options below. Click next to accept the advanced configuration options.**

Product	<a href="#">NSX Manager</a>
Version	6.2.7-5343628
Vendor	<a href="#">VMware, Inc.</a>
Publisher	✓ VMware, Inc. (Trusted certificate)
Download size	2.5 GB
Size on disk	3.3 GB (thin provisioned) 60.0 GB (thick provisioned)
Description	NSX Manager is the centralized network management component of VMware NSX for vSphere. VMware NSX is the network virtualization platform that delivers the operational model of a VM for the network to transform data center operations and economics. NSX Manager is installed as a virtual appliance on any ESX™ host in your vCenter Server environment. You should install the NSX Manager virtual appliance on an ESX host separate from your NSX components. You may use the NSX Manager Appliance Management User Interface, Command Line Interface and vSphere Web Client User Interface to install, configure and maintain NSX components.
Extra configuration	keyboard.typematicMinDelay = 2000000 vshield.vminversion = 6.2.7 vshield.vminvtype = Manager vshield.vminvbuild = 5343628

Back Next Finish Cancel

**Deploy OVF Template**

- 1 Source
  - ✓ 1a Select source
  - ✓ 1b Review details
  - 1c Accept License Agreements**
- 2 Destination
  - 2a Select name and folder
  - 2b Select storage
  - 2c Setup networks
  - 2d Customize template
- 3 Ready to complete

**Accept License Agreements**  
You must read and accept the license agreements associated with this template before continuing.

VMWARE, INC. BETA LICENSE AGREEMENT

Note: BY CLICKING "I AGREE," ACCESSING, DOWNLOADING, INSTALLING, UPLOADING, COPYING OR USING THE BETA SOFTWARE, YOU CONCLUDE AND AGREE TO THIS BETA LICENSE AGREEMENT ("AGREEMENT") IN A LEGALLY BINDING MANNER WITH VMWARE, INC., 3401 HILLVIEW AVENUE, PALO ALTO, CA 94304, USA ("VMware"). IF YOU HAVE SPECIFIED IN CONNECTION WITH THE REGISTRATION PROCESS FOR THIS SOFTWARE BETA TEST PROGRAM THAT YOU ARE ACTING ON BEHALF OF A COMPANY OR OTHER ORGANIZATION, YOU REPRESENT THAT YOU ARE AUTHORIZED TO LEGALLY BIND SUCH ORGANIZATION AND THAT YOU CONCLUDE THE AGREEMENT ON BEHALF OF SUCH ORGANIZATION. IN THE FOLLOWING, THE TERMS "YOU" AND "LICENSEE" SHALL REFER, JOINTLY AND SEVERALLY, TO YOU INDIVIDUALLY AND ANY ORGANIZATION ON WHOSE BEHALF YOU ACT.

IF YOU DO NOT AGREE TO THE TERMS OF THIS BETA LICENSE AGREEMENT, THEN DO "NOT" CLICK "I AGREE," ACCESS, DOWNLOAD, INSTALL, UPLOAD, COPY OR USE THE BETA SOFTWARE.

1. DEFINITIONS.

(a) "Beta Software" shall mean the beta version of VMware's software and the media and Documentation provided by VMware to Licensee and for which Licensee is granted a use license pursuant to this Agreement. The Beta Software will be provided in object form only.

(b) "Documentation" shall mean the printed or online written reference material furnished to Licensee in conjunction with the

Accept

Back Next Finish Cancel



**Deploy OVF Template**

**1 Source**

- ✓ 1a Select source
- ✓ 1b Review details
- ✓ 1c Accept License Agreements

**2 Destination**

- ✓ 2a Select name and folder
- ✓ 2b Select storage
- ✓ 2c Setup networks**
- 2d Customize template

3 Ready to complete

**Setup networks**  
Configure the networks the deployed template should use

Source	Destination	Configuration
VSMgmt	VM Network	✓

IP protocol: IPv4      IP allocation: Static - Manual ⓘ

**Source: VSMgmt - Description**  
This network provides connectivity to this virtual machine.

**Destination: VM Network - Protocol settings**  
No configuration needed for this network

Back   Next   Finish   Cancel

**Deploy OVF Template**

**1 Source**

- ✓ 1a Select source
- ✓ 1b Review details
- ✓ 1c Accept License Agreements

**2 Destination**

- ✓ 2a Select name and folder
- ✓ 2b Select storage
- ✓ 2c Setup networks
- ✓ 2d Customize template**

3 Ready to complete

**Customize template**  
Customize the deployment properties of this software solution

ⓘ All properties have valid values      [Show next...](#)   [Collapse all...](#)

<ul style="list-style-type: none"> <li>▶ CLI of NSX Manager to confirm the configuration.</li> </ul>	2 settings
<ul style="list-style-type: none"> <li>▶ CLI "admin" User Password</li> </ul>	The password for default CLI user for this VM. Enter password: <input type="password"/> Confirm password: <input type="password"/>
<ul style="list-style-type: none"> <li>▶ CLI Privilege Mode Password</li> </ul>	The password for CLI privilege mode for this VM. Enter password: <input type="password"/> Confirm password: <input type="password"/>
<ul style="list-style-type: none"> <li>▶ Network properties (When DNS, IP address, etc are left blank, these properties will be supplied by DHCP server (LESS SECURE))</li> </ul>	7 settings
<ul style="list-style-type: none"> <li>▶ DNS</li> </ul>	2 settings
<ul style="list-style-type: none"> <li>▶ Services Configuration</li> </ul>	2 settings

Back   Next   Finish   Cancel

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	VMware-NSX-Manager-6.2.7-5343628
Source VM name	VMware-NSX-Manager-6.2.7-5343628
Download size	2.5 GB
Size on disk	60.0 GB
Datacenter	New Datacenter
Resource	csalab
Storage mapping	1
Network mapping	1
IP allocation settings	IPv4, Static - Manual
Properties	DNS Server list = 192.168.1.2 Domain Search List = lab.local Default IPv4 Gateway = Default IPv6 Gateway = Hostname = nsx.lab.local Network 1 IPv4 Address = Network 1 IPv6 Address = Network 1 IPv6 Prefix = Network 1 Netmask = Enable SSH = Sele

Back Next Finish Cancel

vmware vSphere Web Client Updated at 11:09 AM Administrator@RJAPPROVES.COM Help

Navigator

- History
- Home
- vCenter Inventory Lists

Task Console

Task Name	Target	Status	Initiator	Queued For
Deploy OVF template	Nsx-mgr.rjapprove...	24%	RJAPPROVES.COM...	


nsx.lab.local


Getting Started **Summary** Monitor Configure Permissions Snapshots Datastores Networks Update Manager


**nsx.lab.local**


Guest OS: Other Linux (64-bit)  
 Compatibility: ESXi 5.0 and later (VM version 8)  
 VMware Tools: Running, version:2147483647 (Guest Managed)  
[More info...](#)


DNS Name: nsx.lab.local  
 IP Addresses:  
 Host: esx3.csalab.local








 CPU USAGE  
130.00 MHz

 MEMORY USAGE  
163.00 MB

 STORAGE USAGE  
47.07 GB


**Powered On** 


**VM Hardware**

- ▶ CPU 4 CPU(s), 130 MHz used
- ▶ Memory  8192 MB, 163 MB memory active
- ▶ Hard disk 1 60.00 GB
- ▶ Network adapter 1 vlxw-dvs-84-virtualwire-1-sid-5000-Lab-vxlan (connected)
- ▶ CD/DVD drive 1 Disconnected  
- ▶ Floppy drive 1 Disconnected  
- ▶ Video card 4.00 MB
- ▶ Other Additional Hardware
- Compatibility ESXi 5.0 and later (VM version 8)

[Edit settings...](#)

**NSX Activity Monitoring**

Virtual Machine Data Collection  Disabled

Global Data Collection  Enabled

[Edit...](#)

**Security Tags**

Security tags can not be applied to a service virtual machine.

▶ **Advanced Configuration**

**Security Group Membership**

Name	Description
This list is empty.	

**Tags**

Assigned Tag	Category	Description
This list is empty.		

nsx.lab.local Actions

Getting Started Summary Monitor **Configure** Permissions Snapshots Datastores Networks Update Manager

Settings

- VM Hardware**
- VM Options
- VM SDRS Rules
- vApp Options
- NSX Activity Monitoring
- Guest User Mappings


More

- Policies

**VM Hardware**

CPU	4 CPU(s), 130 MHz used
Memory	8192 MB, 409 MB memory active
Hard disk 1	60.00 GB
Network adapter 1	vwx-dvs-84-virtualwire-1-sid-5000-Lab-vlan (connected)
CD/DVD drive 1	Disconnected
Floppy drive 1	Disconnected
Video card	4.00 MB
Other	Additional Hardware
Compatibility	ESXi 5.0 and later (VM version 8)

https://nsx-site1.rjapproves.com/login.jsp



User name:

Password:

Login

VMware NSX Manager Virtual Appliance

vmware NSX

P: 192.168.1.8 Version: 6.2.7 Build 5343628  
Name: nsx User: admin

### NSX Manager Virtual Appliance Management

View Summary

Download Tech Support Log

Manage Appliance Settings

Backup & Restore

Manage vCenter Registration

Upgrade

vmware NSX

P: 192.168.1.8 Version: 6.2.7 Build 5343628  
Name: nsx User: admin

Summary Manage

Upgrade the system virtual hardware to at least 16 GB RAM.

#### NSX Manager Virtual Appliance

DNS Name: nsx.lab.local  
IP Address: 192.168.1.8  
Version: 6.2.7 Build 5343628  
Uptime: 3 days, 6 hours, 55 minutes  
Current Time: Wednesday, 07 June 2017 10:39:46 PM CDT

**CPU**

Free: 1721 MHz

Used: 140 MHz Capacity: 1861 MHz

**MEMORY**

Free: 4496 MB

Used: 3477 MB Capacity: 7973 MB

**STORAGE**

Free: 57G

Used: 21G Capacity: 78G

**Common components**

Name	Version	Status	
vPostgres		Running	Stop
RabbitMQ		Running	Stop

**System-level components**

Name	Version	Status	
SSH Service		Stopped	Start

**NSX Management Components**

Name	Version	Status	
NSX Universal Synchronization Service		Stopped	Start
NSX Management Service	6.2.7 Build 5343628	Running	Stop



vmware NSX IP: 192.168.1.8 Version: 6.2.7 Build 5343628 Name: nsx User: admin

Summary Manage

SETTINGS

- General
- Network
- SSL Certificates
- Backups & Restore
- Upgrade

COMPONENTS

- NSX Management Service

Time Settings Unconfigure NTP Servers Edit

Specify NTP server below. For SSO configuration to work correctly it is required that the time on this virtual appliance and NTP server should be in sync. It is recommended to use the same NTP server used by the SSO server.

NTP Server	0 north-america.pool.ntp.org
Timezone	US/Central
Date/Time	06/07/2017 22:40:01

Syslog Server Edit

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	
Port	
Protocol	

Locale Edit

Below is the current locale information.

Locale	en-US
--------	-------

vmware NSX IP: 192.168.1.8 Version: 6.2.7 Build 5343628 Name: nsx User: admin

Summary Manage

SETTINGS

- General
- Network
- SSL Certificates
- Backups & Restore
- Upgrade
- 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://vcenter/lab.local:443/lookupservice/sdk
SSO Administrator User Name:	administrator@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:	vcenter.lab.local
vCenter User Name:	administrator@vsphere.local
Status:	● Connected - Last successful inventory update was on Thu, 08 Jun 2017 02:48:12 GMT ↻

IP: 192.168.1.8 Version: 6.2.7 Build 5343628

Name: nsx User: admin

- Reboot Appliance
- Download Tech Support Log
- About
- Logout

solution user. It is al

The screenshot shows the VMware NSX Management Service configuration interface. At the top, the VMware NSX logo is on the left, and system information (IP: 192.168.1.201, Version: 6.2.0 Build 2909176, Name: nsx-ssh1, User: admin) is on the right. A navigation menu on the left includes 'Summary' and 'Manage'. The main content area is titled 'NSX Management Service' and contains two sections: 'Lookup Service' and 'vCenter Server'. Each section has an 'Edit' button and a text input field. The 'vCenter Server' section includes detailed instructions about connecting to a vCenter server and ensuring proper CPU and memory reservation for a vCenter Server Appliance.

This dialog box, titled 'vCenter Server', provides instructions for connecting to a vCenter server. It contains the following text: '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.'

The dialog includes three input fields: 'vCenter Server:' with the value 'vcenter.lab.local', 'vCenter User Name:' with the value 'administrator@vsphere.local', and 'Password:' with masked characters. There is also a checkbox labeled 'Modify plugin script download location' which is currently unchecked. At the bottom right, there are 'OK' and 'Cancel' buttons.

This dialog box, titled 'Trust Certificate?', asks for confirmation to trust an SSL certificate. The text inside reads: 'vCenter Server vcenter.rjapproves.com presented an SSL certificate with the following thumbprint: 4C:2E:A7:68:F2:21:CA:AD:F4:B2:4C:10:89:35:56:03:D6:71:EE:9A. Proceed with this certificate?'. At the bottom right, there are 'Yes' and 'No' buttons.

**vCenter Server**

Connecting to a vCenter server enables NSX Management Service to display the VMware Infrastructure inventory. HTTPS port (443) needs to be open on the vCenter server 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 VM. You also 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:	vcenter.lab.local
vCenter User Name:	administrator@vsphere.local
Status:	● Connected - Last successful inventory update was on Thu, 08 Jun 2017 02:48:12 GMT ↻

**Lookup Service URL** [X]

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:

Lookup Service Port:

*Enter port 443 for vSphere 6.0, for vSphere 5.5 use 7444.*

Lookup Service URL:

SSO Administrator User Name:

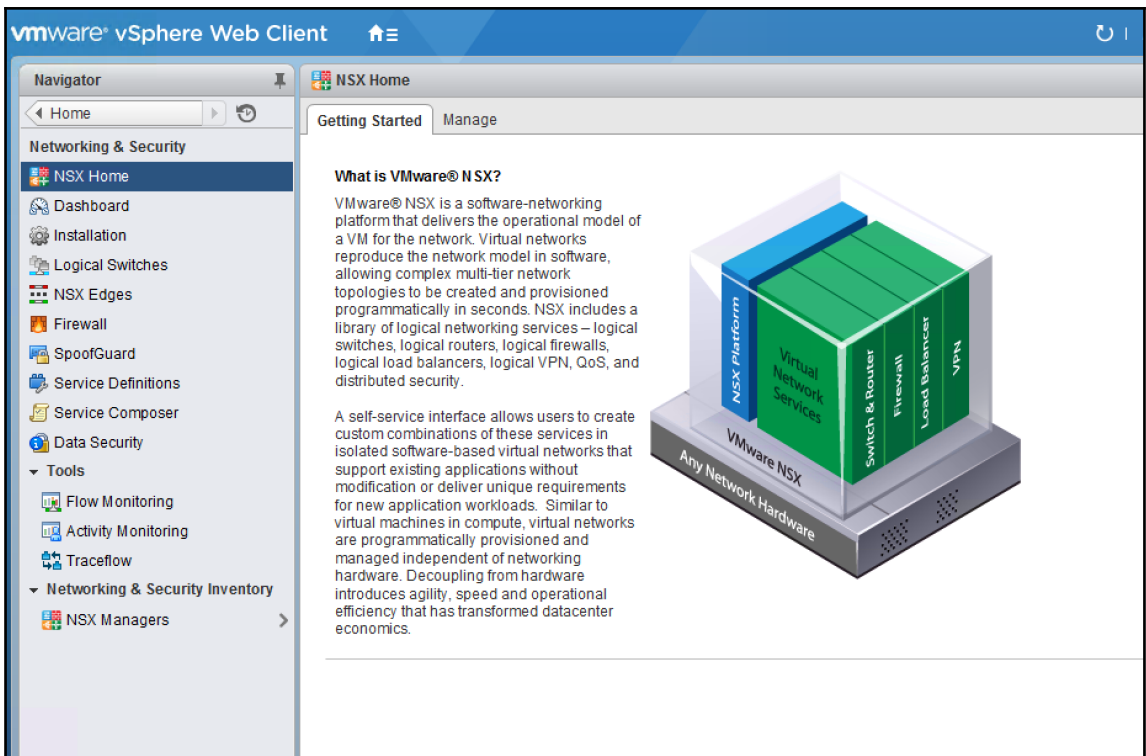
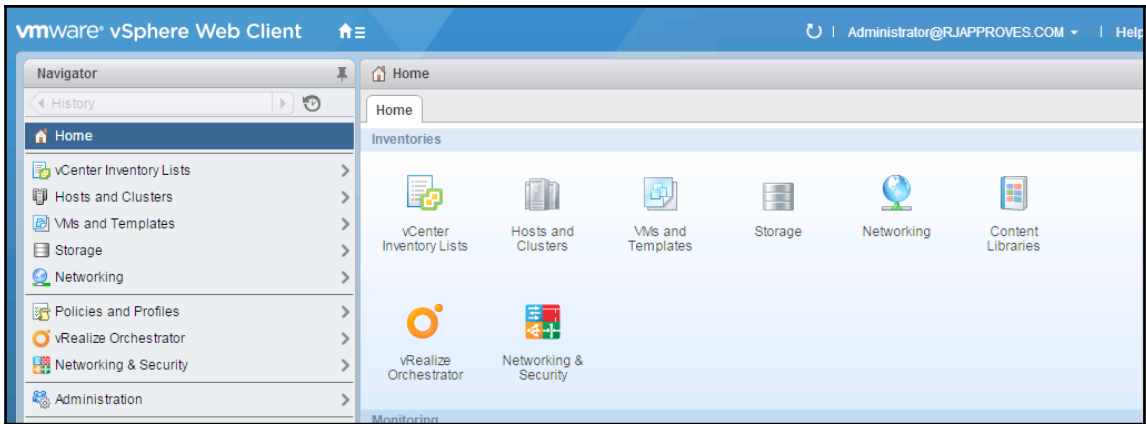
Password:

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 URL:	https://vcenter.lab.local:443/lookupservice/sdk
SSO Administrator User Name:	administrator@vsphere.local
Status:	● Connected ↻



vmware vSphere Web Client

Administrator@VSPHERE.LOCAL

Dashboard

NSX Manager: 192.168.1.8

**System Overview**

NSX Manager 1 ■

Controller Nodes 1 ■

**Host Preparation Status** 1 Cluster

There are no errors or warnings.

**Firewall Publish Status** 3 Hosts

There are no errors or warnings.

**Logical Switch Status** 2 Logical Switches

There are no errors or warnings.

vmware vSphere Web Client

NSX Managers

Objects

Actions

Name	IP Address	Version
192.168.1.8	192.168.1.8	6.2.7.5343628

192.168.1.8

Getting Started **Summary** Monitor Manage

**192.168.1.8**

ID: 421E9C9C-BB38-09E5-21F9-224BA7EE3302

IP Address: 192.168.1.8

Version: 6.2.7.5343628

**Navigator**

Home

**Administration**

- Access Control
  - Roles
  - Global Permissions
- Single Sign-On
  - Users and Groups
  - Configuration
- Licensing**
  - Licenses**
  - Reports

**Licenses**

License provider: All 6.0 vCenter Server instances

Getting Started Licenses Products **Assets**

vCenter Server systems Hosts Clusters **Solutions**

All Actions

Asset	Usage	Product
NSX for vSphere	0 Concurrent u...	NSX for vSphere

vmware vSphere Web Client Administrator@RJAPPROVES.COM Help

**Navigator**

Administration

NSX for vSphere

**Manage**

Licensing Assign License...

Usage: 0 VMs

Product: Evaluation Mode

License: Evaluation License

License expiration: ⚠ 10/15/2015

Evaluation capacity: Unlimited VMs

Available features

Feature	In Use
appfw	No
sdd	No
routing	No
edgefw	No
nat	No
dhcp	No
vpn	No
vxlan	No
si	No
lb	No
hafw	No
ident	No

New Licenses

1 Enter license keys  
2 Edit license names  
3 Ready to complete

Enter license keys  
Enter license keys from which to create new licenses.

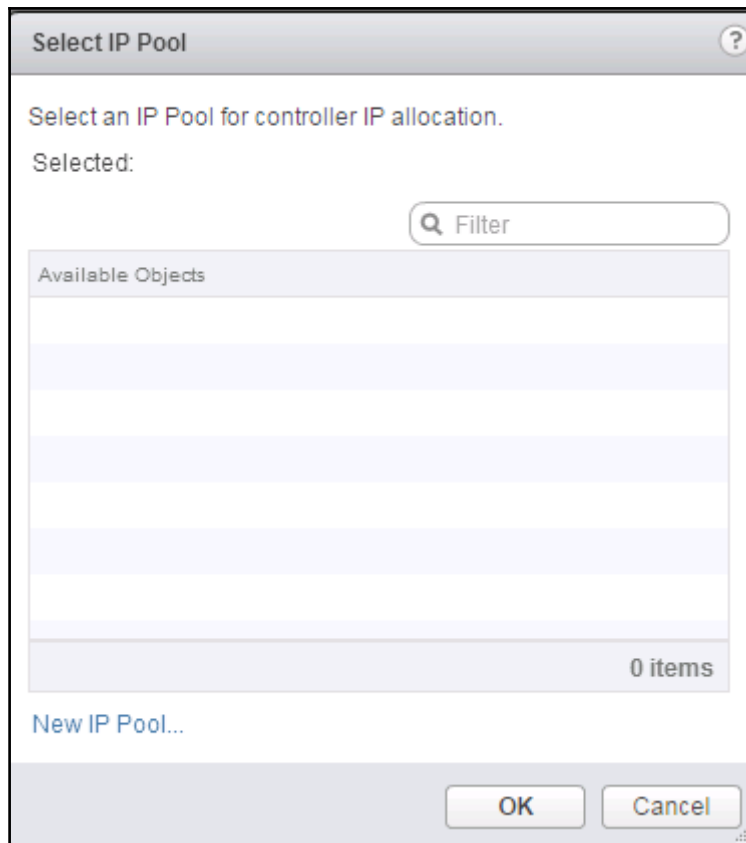
License keys (one per line):

Back Next Finish Cancel


Add Controller

NSX Manager: \* 192.168.1.201  
Datacenter: \* Site 1  
Cluster/Resource Pool: \* Site 1  
Datastore: \* Local-hlu001  
Host: esx2.rjapproves.com  
Folder: Discovered virtual machi...  
Connected To: \* VM Network Change Remove  
IP Pool: \* This field is required  
Password: \*  
Confirm password: \*

OK Cancel





 **Add Static IP Pool**

Name: \*

Gateway: \*   
A gateway can be any IPv4 or IPv6 address.

Prefix Length: \*

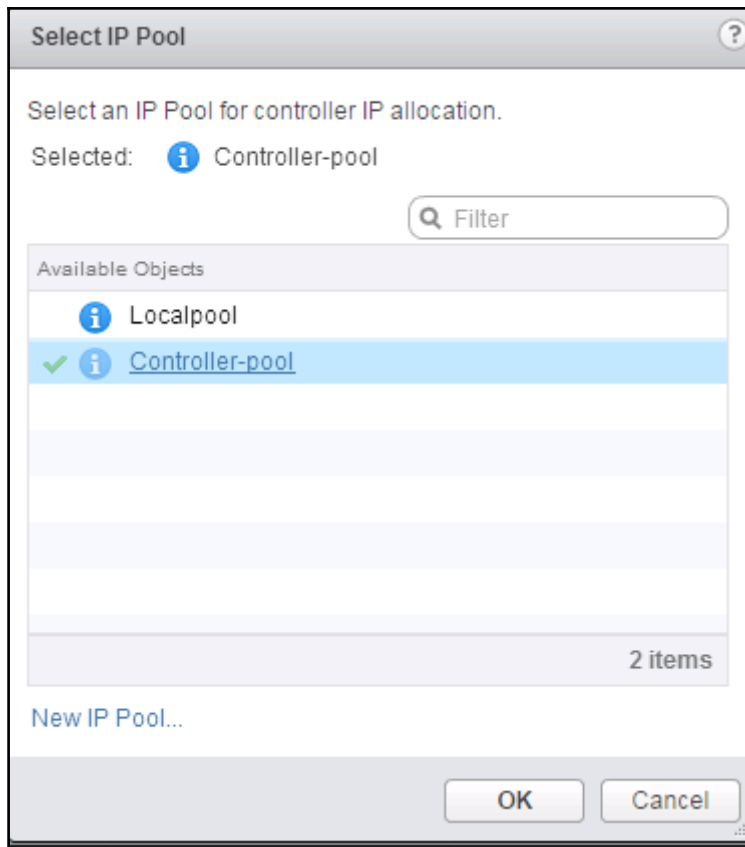
Primary DNS:

Secondary DNS:

DNS Suffix:

Static IP Pool: \*

for example 192.168.1.2-192.168.1.100 or  
abcd:87:87::10-abcd:87:87::20



NSX Controller nodes

Controller IP Address	ID	Status	Software Version	NSX Manager
192.168.1.210	controller-2	Deploying	6.2.44354	192.168.1.201

Recent Tasks		
Task Name	Target	Status
Deploy OVF template	NSX_Controller_37...	<div style="width: 64%;"><div style="width: 64%;"></div></div> 64 %

- ▼ New Cluster-1
  - esx1.lab.local
  - esx2.lab.local
  - esx3.lab.local
  - New Virtual Machine
  - NSX\_Controller\_7b76b7e2-263d-4eeb-93dc-b02438a01193**
  - pshell-host

NSX Controller nodes					
Name	Controller Node	NSX Manager	Status	Peers	Software Version
Controller-1	192.168.1.250 <i>controller-2</i>	192.168.1.8	✓ Connected		6.2.49576

**vmware vSphere Web Client** Updated at 11:22 PM | Administrator@RJAPPROVES.COM | Help | Search

**Navigator**

Home

**Networking & Security**

- NSX Home
- Installation**
- Logical Switches
- NSX Edges
- Firewall
- SpoofGuard
- Service Definitions
- Service Composer
- Data Security
- Tools
  - Flow Monitoring
  - Activity Monitoring
  - Traceflow

**Installation**

Management | **Host Preparation** | Logical Network Preparation | Service Deployments

NSX Manager: 192.168.1.201

NSX Component Installation on Hosts

**Actions**

Clusters & Hosts	Installation Status	Firewall	VXLAN
Site1	Not Installed	Not Configured	Not Configured
Compute Cluster	Not Installed	Not Configured	Not Configured

**NSX Component Installation on Hosts**

⚙️ Actions

Clusters & Hosts	Installation Status	Firewall
▶️ Site 1	Not Installed	Not Configured
▼️ Compute Cluster	Not Installed	Not Configured
esx1.rjapproves.com		Install

**NSX Component Installation on Hosts**

⚙️ Actions

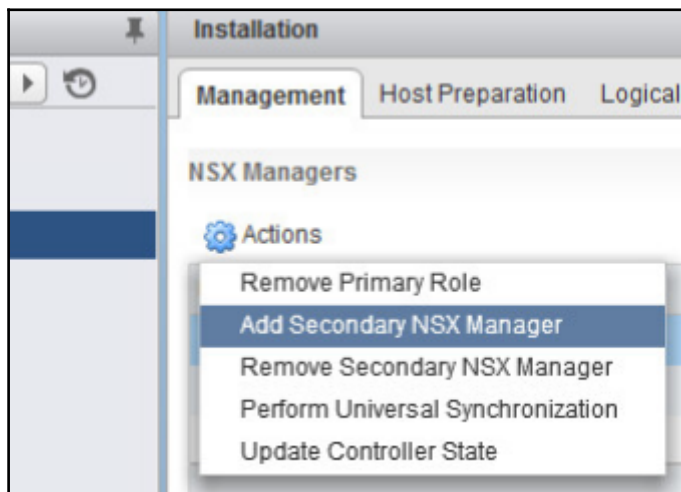
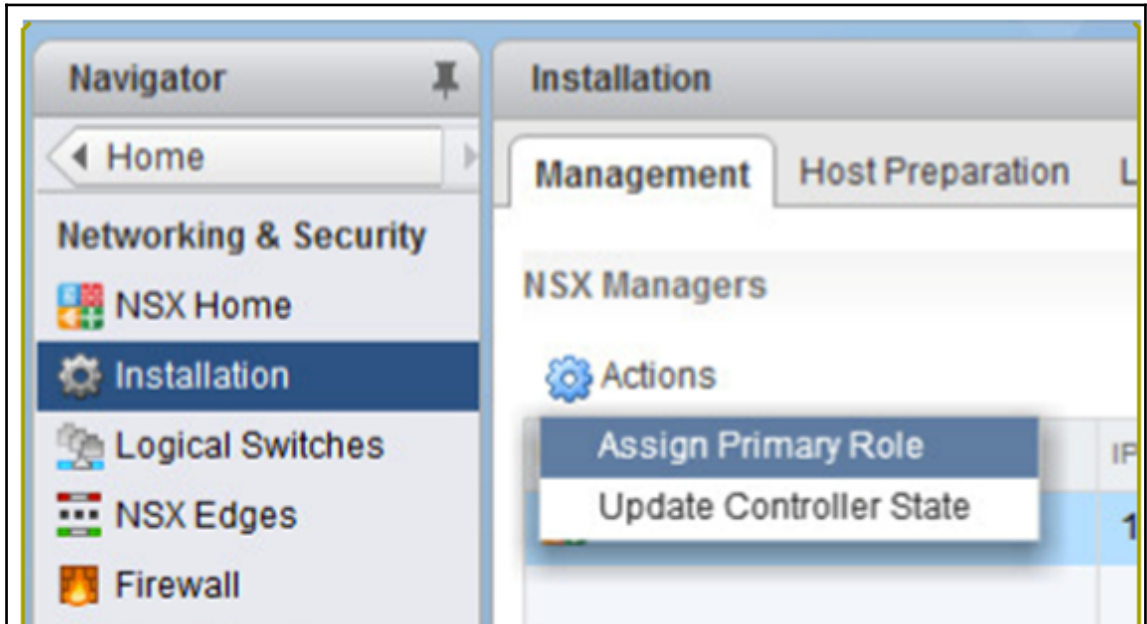
Clusters & Hosts	Installation Status	Firewall	VXLAN
▼️ New Cluster-1	✔️ 6.2.7.5343628	✔️ Enabled	✔️ Configured
esx3.lab.local	✔️ 6.2.7.5343628	✔️ Enabled	
esx1.lab.local	✔️ 6.2.7.5343628	✔️ Enabled	
esx2.lab.local	✔️ 6.2.7.5343628	✔️ Enabled	

```

esx-vsip                6.0.0-0.0.5325006
areCertified    2017-05-03
esx-vxlan                6.0.0-0.0.5325006
areCertified    2017-05-03

```

# Chapter 04: NSX Functional Services



**192.168.110.15 - Add Secondary NSX Manager** ?


NSX Manager: \* 192.168.210.15 ▼





User Name: \* ADMIN

Password: \* \*\*\*\*\*

Confirm password: \* \*\*\*\*\*

**NSX Component Installation on Hosts**

 Actions

Clusters & Hosts	Installation Status	Firewall	VXLAN
▼  New Cluster-1	✓ 6.3.2.5672532	✓ Enabled	Not Configured
 esx3.lab.local	✓ 6.3.2.5672532	✓ Enabled	
 esx1.lab.local	✓ 6.3.2.5672532	✓ Enabled	
 esx2.lab.local	✓ 6.3.2.5672532	✓ Enabled	

**New Cluster-1 - Configure VXLAN Networking** ? ▶▶

Switch: \* dvSwitch ▼

VLAN: \* 0

MTU: \* 1600

VMKNic IP Addressing: \*  Use DHCP  
\*  Use IP Pool New IP Pool... ▼

VMKNic Teaming Policy: \* Fail Over ▼

VTEP: \* 1

OK Cancel

### Add Static IP Pool

Name: \*

Gateway: \*   
 A gateway can be any IPv4 or IPv6 address.

Prefix Length: \*

Primary DNS:

Secondary DNS:

DNS Suffix:

Static IP Pool: \*

for example 192.168.1.2-192.168.1.100 or  
 abcd:87:87::10-abcd:87:87::20

OK Cancel

Actions

Clusters & Hosts	Installation Status	Firewall	VXLAN
<ul style="list-style-type: none"> <li>New Cluster-1               <ul style="list-style-type: none"> <li>esx3.lab.local</li> <li>esx1.lab.local</li> <li>esx2.lab.local</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>✓ 6.3.2.5672532</li> <li>✓ 6.3.2.5672532</li> <li>✓ 6.3.2.5672532</li> <li>✓ 6.3.2.5672532</li> </ul>	<ul style="list-style-type: none"> <li>✓ Enabled</li> <li>✓ Enabled</li> <li>✓ Enabled</li> <li>✓ Enabled</li> </ul>	<ul style="list-style-type: none"> <li>✓ Configured</li> <li></li> <li></li> <li></li> </ul>



**dvSwitch**  
**dvSwitch-DVUplinks-33**  
**OutboundPG**  
**vxw-vmknicPg-dvs-33-0-76b97d0e-d587-4ca9-833a-ae3866fac1a**

**Installation**

Management   Host Preparation   **Logical Network Preparation**   Service Deployments

NSX Manager:

VXLAN Port:

Clusters & Hosts	Configuration Status	Switch	VLAN	MTU	VMKNic IP Addressing	Teaming Policy	VTEP
<b>New Cluster-1</b> esx1.lab.local esx2.lab.local esx3.lab.local	✓ <b>Unconfigure</b> ✓ Ready ✓ Ready ✓ Ready	dvSwitch	0	1600	IP Pool ✓ vmk1: 192.168.1.18 ✓ vmk1: 192.168.1.19 ✓ vmk1: 192.168.1.17	Fail Over	1

Clusters & Hosts	Configuration Status	Switch	VLAN	MTU	VMKNic IP Addressing
<b>New Cluster-1</b> esx1.lab.local esx2.lab.local esx3.lab.local	✓ <b>Unconfigure</b> ✓ Ready ✓ Ready ✓ Ready	dvSwitch	0	1600	IP Pool ✓ vmk1: 192.168.1.18 ✓ vmk1: 192.168.1.19 ✓ vmk1: 192.168.1.17

**New Cluster-1 - Unconfigure cluster**

Do you want unconfigure VXLAN on the selected Cluster 'New Cluster-1'?

NSX Manager: 192.168.1.8

VXLAN Transport Segment ID Transport Zones

Segment IDs & Multicast Addresses allocation (system wide settings) Edit Reset

Segment ID pool: 5000-5100

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: \* 5000-5100  
*(In the range of 5000-16777215)*

Enable Multicast addressing  
*Multicast addresses are required only for Hybrid and Multicast control plane modes.*

OK Cancel

**Edit Segment IDs and Multicast Address Allocation** ?

Provide a Segment ID pool and Multicast range unique to this NSX Manager.

Segment ID pool: \* 5000-5100  
*(In the range of 5000-16777215)*

Enable Multicast addressing  
*Multicast addresses are required only for Hybrid and Multicast control plane modes.*

Multicast addresses: \*  
*(Recommended range - 239.0.0.0-239.255.255.255)*

OK Cancel

New Transport Zone
? >>

Mark this object for Universal Synchronization

Name:

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

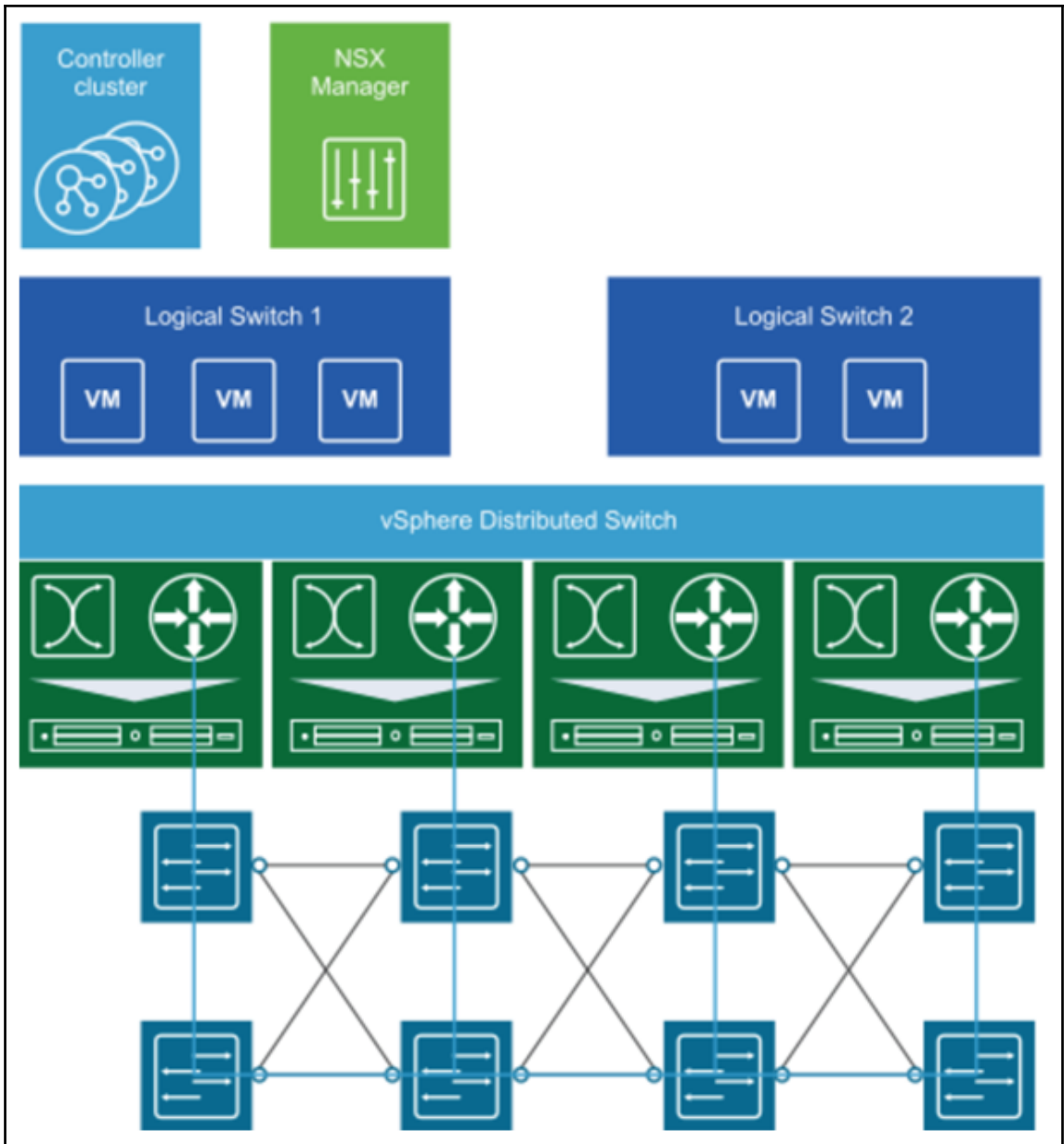
	Name	NSX vSwitch	Status
<input checked="" type="checkbox"/>	Compute Cluster	Site1-DvSwitch	<span style="color: green; font-weight: bold;">✔</span> Normal

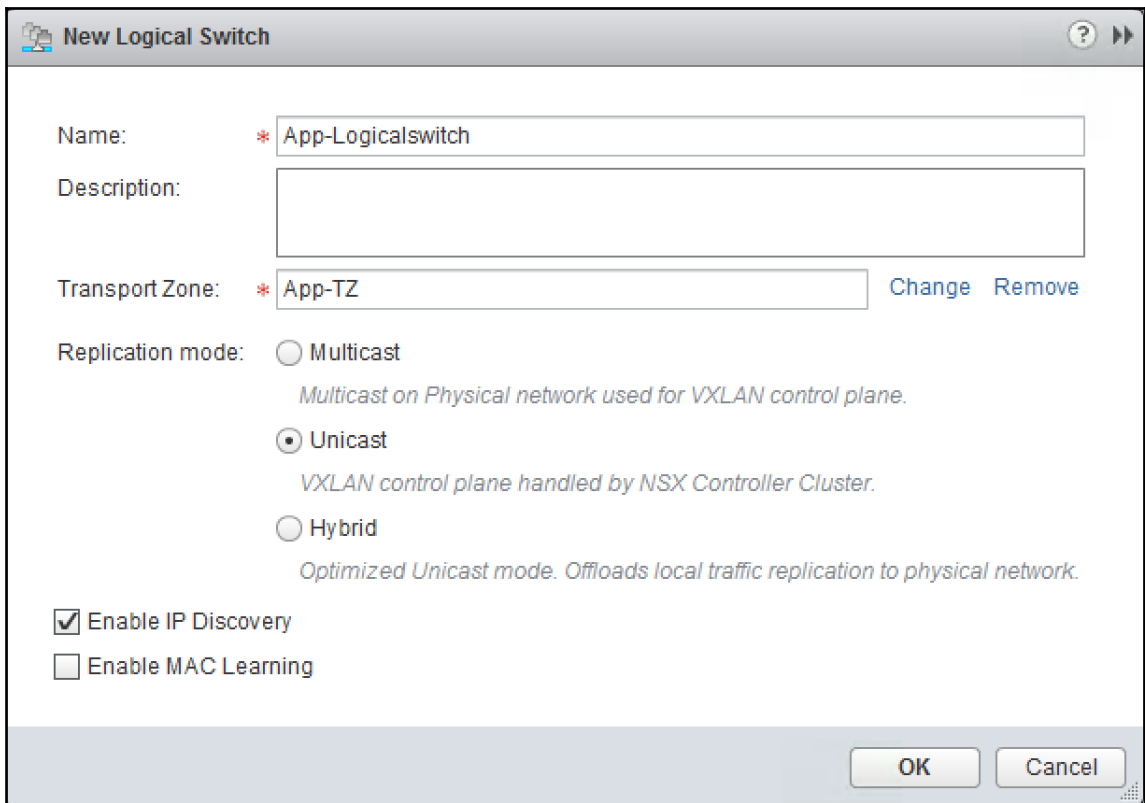
NSX Manager: 192.168.1.201 (Role: Primary) ▾

VXLAN Transport Segment ID Transport Zones

    Actions ▾

Name	1 ▲	Description	Scope	Control Plane Mode
 App-TZ			Global	Unicast
 Universal-TZ-App			Universal	Unicast





**Logical Switches**

NSX Manager: 192.168.1.8

+ | ✎ | ✖ | 📄 | 🗑️ | 📊 | ⚙️ Actions

Segment ID	Name	Status	Transport Zone
5000	App-Logicals witch	Normal	App-TZ

**Logical Switches**

NSX Manager: 192.168.1.8

+ | ✎ | ✖ | 📄 | 🗑️ | 📊 | ⚙️ Actions

Segment ID	Name	Status	Transport Zone
5000	App-Logicals witch	Normal	App-TZ

**App-Logicals witch - 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.

Available Objects

- testvm
- New Virtual Machine
- pshell-host
- Win2012-Linkedclone
- Win2012-base
- CentOS

6 items

➡

⬅

Selected Objects

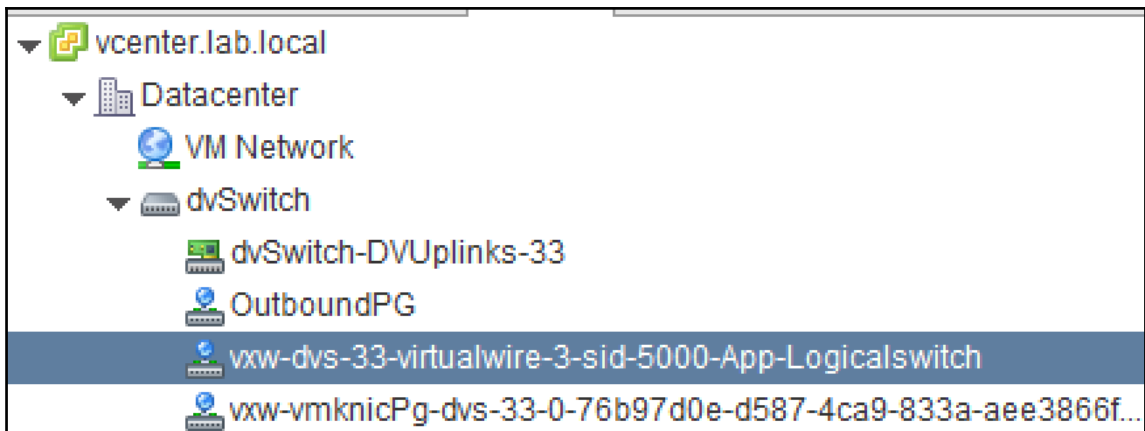
- testvm

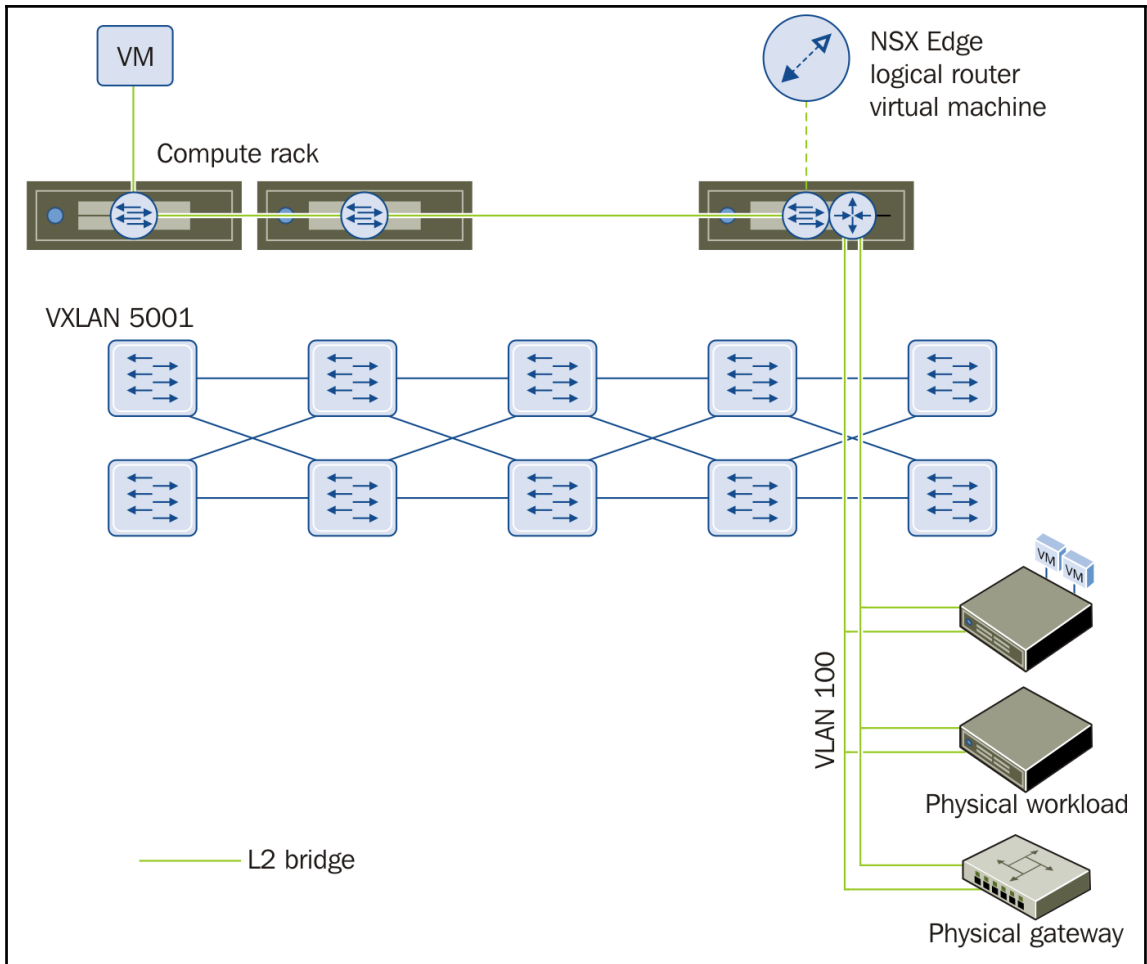
1 items

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

### 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.*

Name: \*

Hostname:

Description:

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

New NSX Edge ? >>

✓ **1 Name and description**

**2 Settings**

3 Configure deployment

4 Configure interfaces

5 Default gateway settings

6 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: \*

Password: \*

Confirm password: \*

Enable SSH access

edge.listing.addEdge.edgeAppliance.EnableFIPSMode

Edge Control Level Logging  ▼

*Set the Edge Control Level Logging*

Back Next Finish Cancel

**Configure deployment**

Datcenter: \* Site1 ▼

**NSX Edge Appliances**

+ ✎ ✕

Resource Pool	Host	Datastore	Folder

Specify  
Edge a  
Edge A

**Add NSX Edge Appliance** ?

Specify placement parameters for the NSX Edge appliance.

Cluster/Resource Pool: \* ▼

Datastore: \* ▼

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 interfaces

---

#### HA Interface Configuration

Connected To: \*  Change Remove

+ ✎ ✖

Primary IP Address	Subnet Prefix Length
192.168.1.66 <span style="float: right;">✖</span>	24 <span style="float: right;">✖</span>
1 items	

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
app	172.16.0.1*	24	App-Logicals switch
to-ESG	192.168.1.67*	27	OutboundPG

Back
Next
Finish
Cancel

**Edit Interface** ?

Name: \*

Type:  Internal  Uplink

Connected To: \*  Change Remove

Connectivity Status:  Connected  Disconnected

Configure subnets

+ ✎ ✖ 🔍 Filter ▾

Primary IP Address	Subnet Prefix Length
172.16.0.1	24
1 items	

MTU:

**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: \*  ▼

Gateway IP: \*

MTU:

Admin Distance:

Back **Next** Finish Cancel

**NSX Edges**

NSX Manager:  ▼

+ | ⚙️ Actions ▼ 
🔄 1 Installing
🚫 4 Failed

Id	Name	Type	Tenant
edge-5	App-DLR	Logical Router	Default



vmware vSphere Web Client

App-DLR

Summary Monitor **Manage**


Settings Firewall Routing **Bridging** DHCP Relay


+ ✎ ✖

Bridge Id	Name

### Add Bridge

Name: \*

Logical Switch: \*  




Distributed Port Group: \*  

App-DLR

Summary Monitor **Manage**

Settings Firewall Routing **Bridging** DHCP Relay

+ ✎ ✖

Bridge Id	Name	Logical Switches	Distributed Port Group
1	app-to-physical	 App-Logicals witch  Routing Enabled	 APP-Physical-PG

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 (Distributed) Router  
*Provides Distributed Routing and Bridging capabilities.*

Universal Logical (Distributed) Router  
*Provides Distributed Routing capabilities for Universal Logical Switches.*

Name: \*

Hostname:

Description:

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

### Configure deployment

Datcenter: \*  ▾

Appliance Size:  Compact  
 Large  
 X-Large  
 Quad Large

#### NSX Edge Appliances

+ ✎ ✕

Resource Pool	Host	Datastore	Folder
New Cluster-1		nfs-datastore	

Specifying a resource pool and datastore is mandatory for configuring the NSX Edge appliance.

**Add NSX Edge Interface** ?

vNIC#: 0

Name: \*

Type:  Internal  Uplink

Connected To:  Change Remove

Connectivity Status:  Connected  Disconnected

+
✎
✖

Q Filter ▼

Primary IP Address	Secondary IP Addresses	Subnet Prefix Length
192.168.0.1 <span style="float: right;">✖</span>		24 <span style="float: right;">✖</span>
<b>1 items</b>		

*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:

Options:  Enable Proxy ARP  Send ICMP Redirect

Reverse Path Filter  ▼

Fence Parameters:

Example: ethernet0.filter1.param1=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

### Configure interfaces

Configure interfaces of this NSX Edge

+ ✎ ✕

vNIC#	Name	IP Address	Subnet Prefix Length	Connected To
0	app-internal	192.168.0.1*	24	App-Logicals...
1	uplink-exte...	192.168.1.99*	24	OutboundPG

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: \*  ▼

Gateway IP: \*

MTU:

Admin Distance:

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: \*  ▼

Declare Dead Time:  (seconds)

Management IPs:

*Management IPs must be in CIDR format with /30 subnet and must not overlap with any vnic subnets.*

NSX Edges			
NSX Manager: 192.168.1.8 (Role: Primary)			
		Actions	
		1 Installing	4 Failed
Id	Name	Type	Tenant
edge-5	App-DLR	Logical Router	Default
edge-6	ESG1	NSX Edge	Default

### Navigator

History

**Networking & Security**

- NSX Home
- Dashboard
- Installation
- Logical Switches
- NSX Edges
- Firewall**
- SpoofGuard
- Service Definitions
- Service Composer
- Tools

### Firewall

Configuration | Saved Configurations | Settings

NSX Manager: 192.168.1.8 (Role: Primary)

Last publish operation succeeded 6/13/2017 12:55:07 PM

General | Ethernet | Partner security services

No.	Name	Rule ID	Source
▶  Default Section Layer3 (Rule 1 - 3)			

No.	Name	Source
▶  Default Section Layer3 (Rule 1 - 3)		

- Add rule
- Add section
- Edit section
- Merge section
- Delete section

**New Section** ?

Name: \*

Position:

Add above

Add below

Mark this section for Universal Synchronization

General | Ethernet | Partner security services

📅

No.	Name	Rule ID	Source	Destination	Service	Action	Applied To
<input type="button" value="📄"/> App-rules <span style="float: right;"> <input type="button" value="📄"/> <input type="button" value="🔄"/> <input type="button" value="+"/> <input type="button" value="📄"/> <input type="button" value="✖"/> <input type="button" value="⇄"/> <input type="button" value="🔍"/> </span>							

General | Ethernet | Partner security services

No.	Name	Source	Destination	Service
<input type="button" value="📄"/> App-FWL3-Section (Rule 1)				
✓ 1		• any	• any	• any



No.	Name
App-FWL3-Section (Rule 1 - 2)	
✓ 1	
✓ 2	

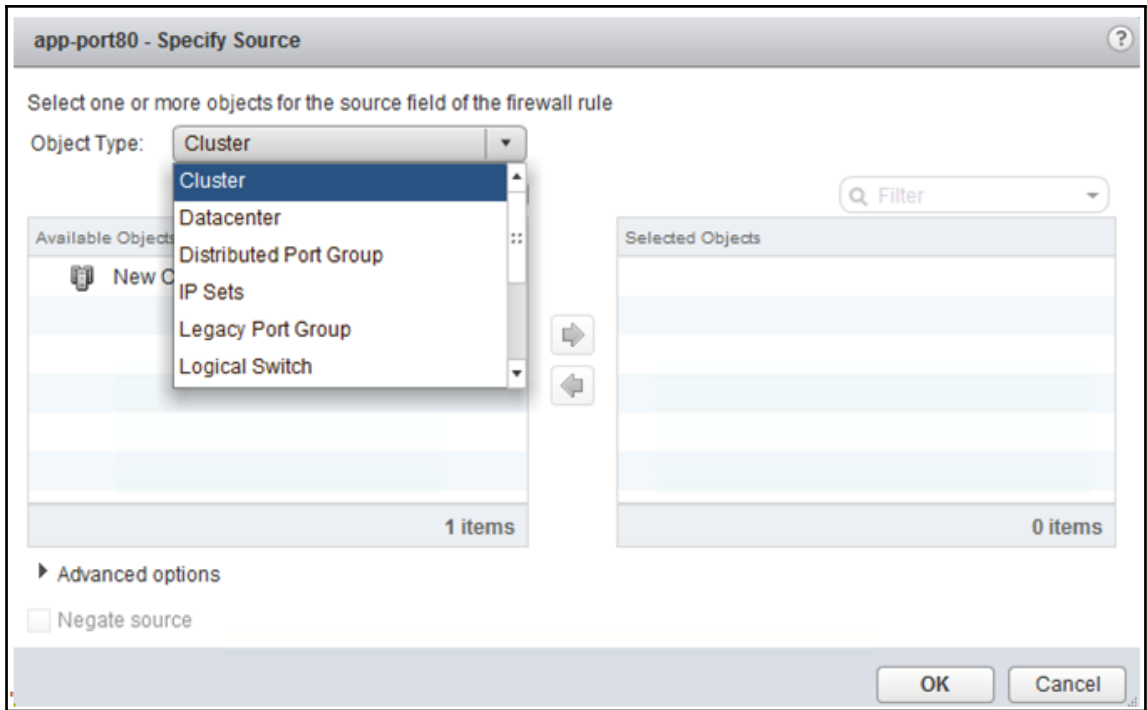
No.	Name	Rule ID
App-rules (Rule 1)		
✓ 1	app-port80	* a

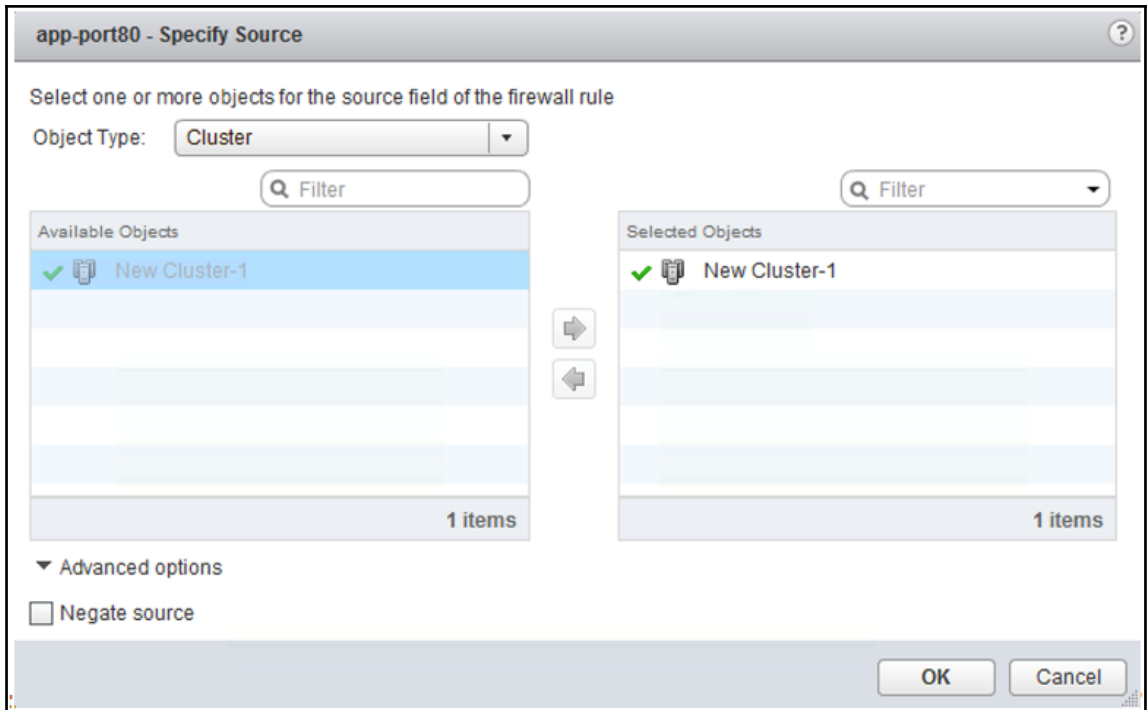
**app-port80 - Source Raw IP** ?

IP Address:  IPV4  IPV6

Value: \*

*eg: 192.168.200.1, 192.168.200.1/24, 192.168.200.1-192.168.200.24*





app-port80 - Service Raw IP



Protocol:

TCP



Ports:

any

*e.g.: 7001-7020,7100,8000-9000*

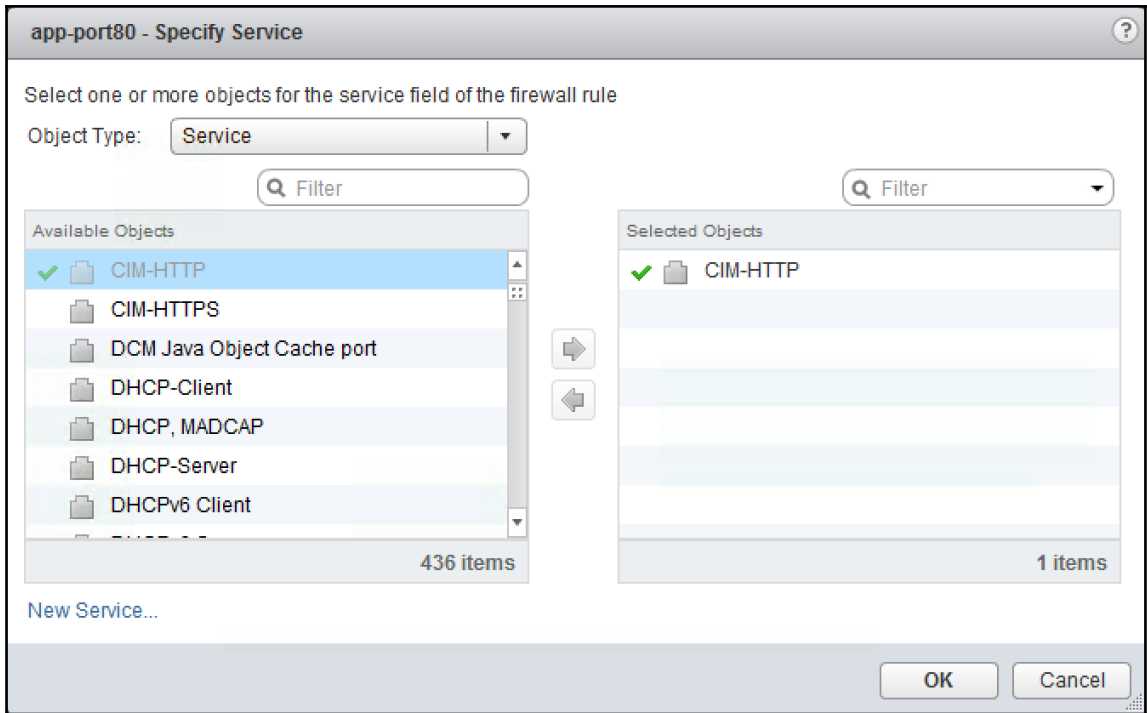
Source ports:

any

*e.g.: 7001-7020,7100,8000-9000*

Save

Cancel



**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: \*

Description:

Protocol:  ▼

Scope: Global

Enable inheritance to allow visibility at underlying scopes

**app-port80 - Edit Action** ?

Action:  ▼

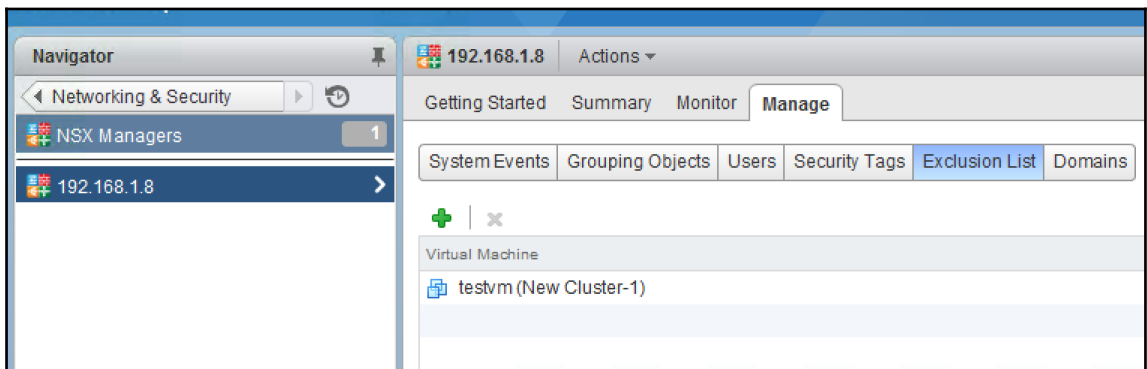
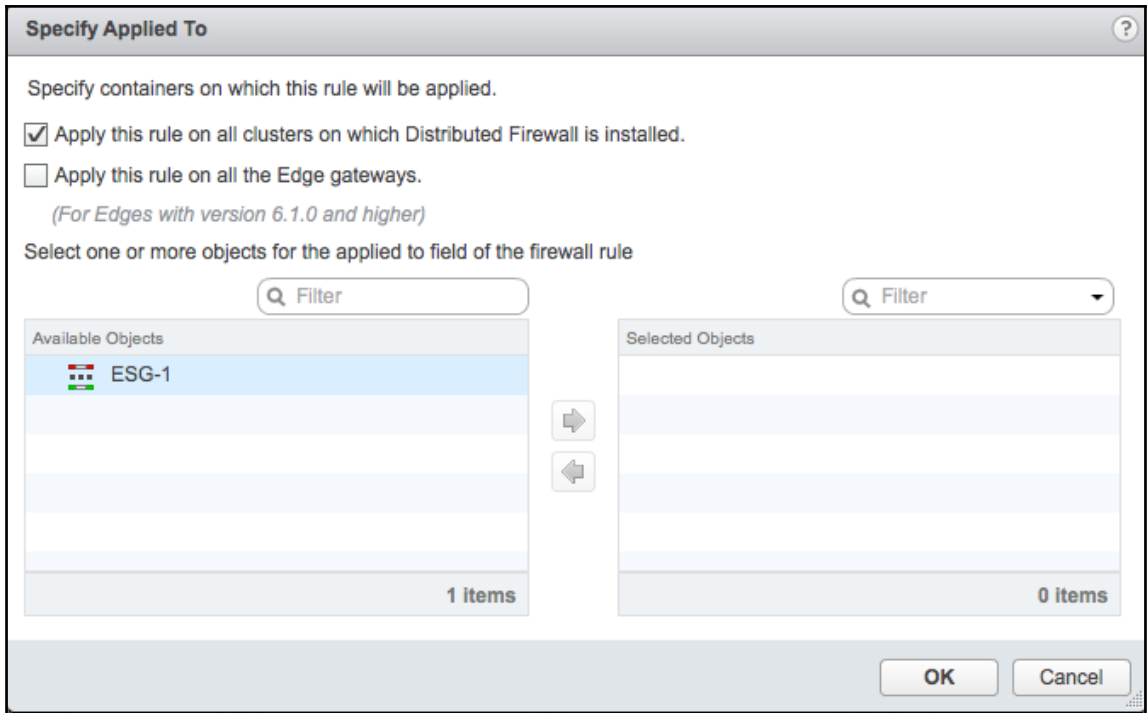
Direction:  ▼

Packet Type:  ▼

Tag:

Log:  Log  Do not log

Comments:

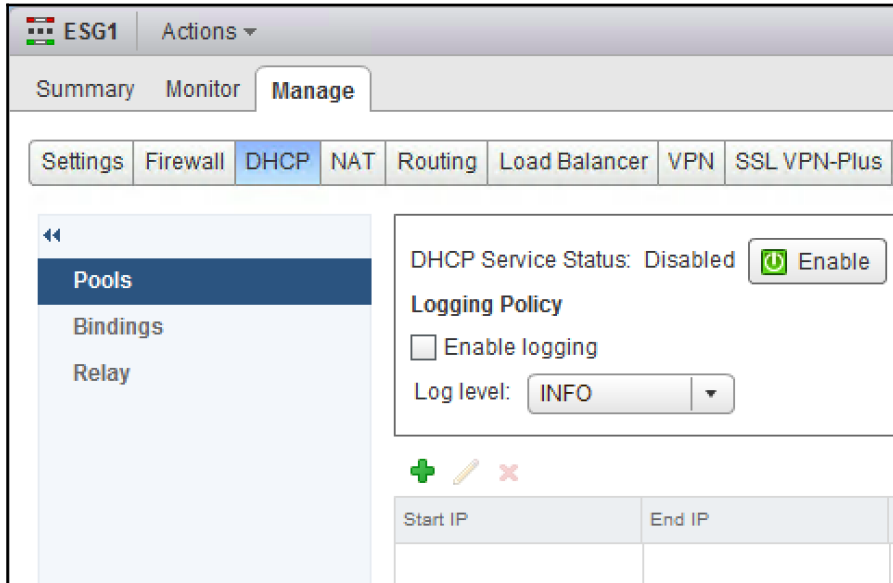




The screenshot shows the Mikrotik WinBox interface for configuring the Firewall on device ESG1. The Firewall is currently enabled, and the configuration page displays a table of firewall rules.

No.	Name
✓ 1	firewall
✓ 2	Default Rule

# Chapter 05: Edge Services Gateway



**Add DHCP Pool** ?

Auto Configure DNS

Lease Never Expires

Start IP: \*

End IP: \*

Domain Name:

Primary Name Server:

Secondary Name server:

Default Gateway:

Subnet Mask:

Lease Time:  (seconds)

ESG1 Actions

Summary Monitor **Manage**

Settings Firewall DHCP NAT Routing Load Balancer VPN SSL VPN-Plus Grouping Objects

Configuration  
Interfaces  
Certificates

Details: Action

Size:	Compact
Host Name:	esg1.lab.local
Auto generate rules:	Enabled
FIPS mode:	Disabled
Syslog servers:	<span>Change</span>
Server 1:	
Server 2:	

Services: **Status last updated on: Monday, June 19, 2017 4:34:39 PM** Refresh

Firewall	Applied
Load Balancer	Down
IPsec VPN	Not Configured
DHCP	Not Configured
NAT	Not Configured
High Availability	Not Configured
Syslog	Not Configured
SSL VPN Plus	Not Configured

HA Configuration: Change

HA Status:	Disabled
vNIC:	
Declare Dead Time:	15
Logging:	Disabled
Log level:	Info

DNS Configuration: Change

DNS Status:	Disabled
DNS Server 1:	
DNS Server 2:	
Cache Size:	16
Logging:	Disabled
Log level:	Info

NSX Edge Appliances

### Change DNS configuration ?

Specify the DNS servers to which this NSX Edge must forward DNS requests.

Enable DNS service

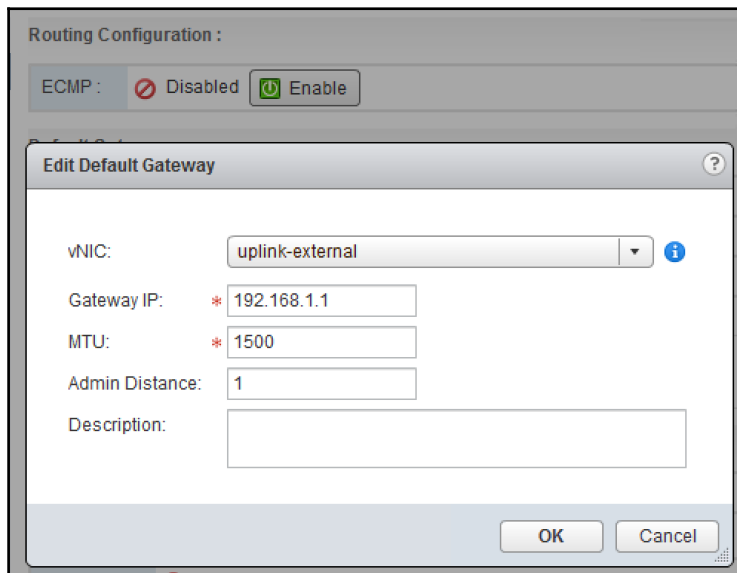
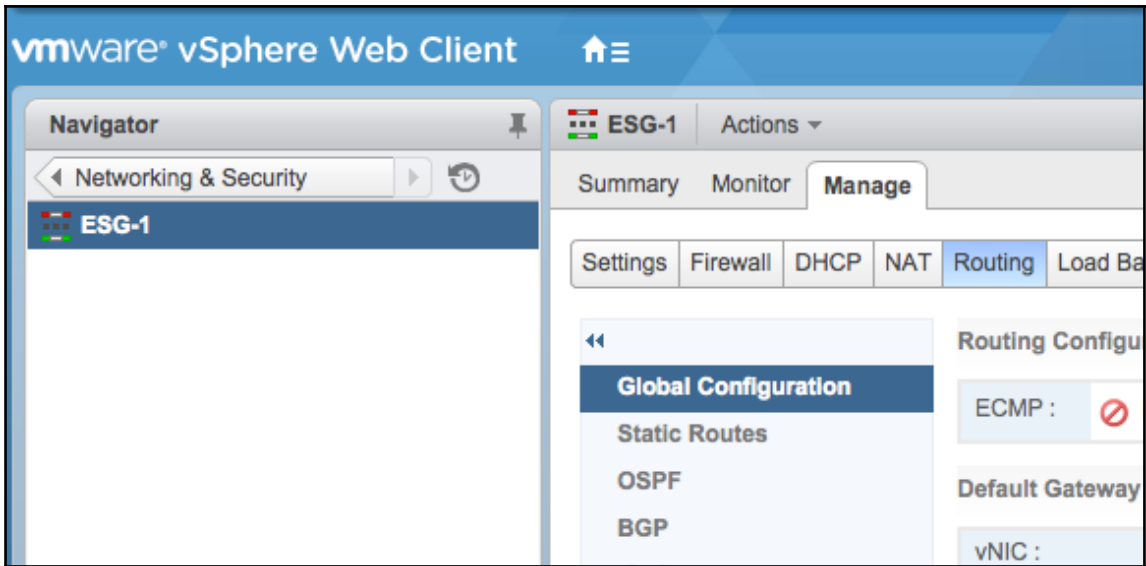
DNS Server 1: \*

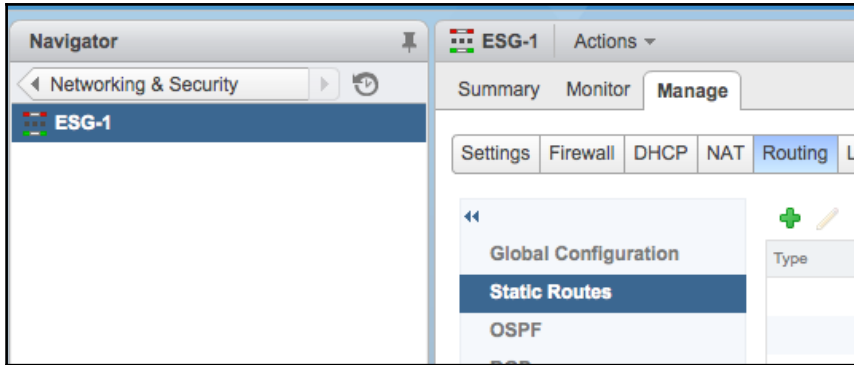
DNS Server 2:

Cache Size: \*

Enable Logging

Log level:





**Add Static Route** ?

Network: \*   
*Network should be entered in CIDR format  
e.g. 192.169.1.0/24*

Next Hop: \*

Interface:  i

MTU:

Admin Distance:

Description:

ESG1 Actions

Summary Monitor **Manage**

Settings Firewall DHCP NAT **Routing** Load Balancer VPN SSL VPN-Plus Grouping Objects

Global Configuration  
 Static Routes  
**OSPF**  
 BGP  
 Route Redistribution

OSPF Configuration :

Status :  Disabled  
 Graceful Restart :  Enabled  
 Default Originate :  Disabled

Area Definitions :

+ ✎ ✕

Area ID	Type
51	NSSA
0	Normal

OSPF Configuration

Enable OSPF  
 Enable Graceful Restart  
*(Enables/Disables the capability to perform Non-Stop Forwarding of packets during restart of OSPF process)*  
 Enable Default Originate  
*(Enables/Disables the capability to advertise a default route to its neighbors.)*

OK Cancel

New Area Definition

Area ID : \*   
 Type : Normal  
 Authentication : None  
 Value :

OK Cancel

**New Area to Interface Mapping** ?

NIC : Uplink i

Area : \* 51 v

Ignore Interface MTU setting

Advanced	
Hello Interval *	10 (seconds)
Dead Interval *	40 (seconds)
Priority *	128
Cost *	1

OK Cancel

**Distributed-Router** Actions v

Summary **Manage**

Settings Firewall **Routing** Bridging DHCP Relay

Global Configuration  
Static Routes  
**OSPF**  
BGP

OSPF Configuration :

Status :	<span style="color: red;">⊘</span> Disabled
Protocol Address :	
Forwarding Address :	



### OSPF Configuration ?

Enable OSPF

Protocol Address : \*

Forwarding Address : \*

Enable Graceful Restart  
*(Enables/Disables the capability to perform Non-Stop Forwarding of packets during restart of OSPF process)*

Enable Default Originate  
*(Enables/Disables the capability to advertise a default route to its neighbors.)*

ESG1
Actions ▾

Summary
Monitor
Manage

Settings
Firewall
DHCP
NAT
Routing
Load Balancer
VPN
SSL VPN-Plus
Grouping

←

- Global Configuration
- Static Routes
- OSPF
- BGP
- Route Redistribution

**BGP Configuration :**

Status :	⊘ Disabled
Local AS :	
Graceful Restart :	✔ Enabled
Default Originate :	⊘ Disabled

**Neighbors :**

+
✎
✕

**Edit BGP Configuration** ?

Enable BGP

Enable Graceful Restart  
*(Enables/Disables the ability to preserve forwarding state during restart of the BGP process)*

Enable Default Originate  
*(Enables/Disables the capability to advertise a default route to its neighbors.)*

Local AS \*

OK Cancel

**New Neighbour** ?

IP Address : \*

Remote AS : \*

Weight :

Keep Alive Time :  (Seconds)

Hold Down Time :  (Seconds)  
*(BGP Keep alive timer value needs to be one third of hold down timer)*

Password :

BGP Filters :

+ ✎ ✕

Direction	Action	Network	IP Prefix GE	IP Prefix LE

0 items

OK Cancel

**New BGP Filter** ?

Direction \*  ▼

Action \*  ▼

Network \*

*Network should be specified as 'ANY' or in CIDR format e.g. 192.169.1.0/24.*

IP Prefix GE

*Expected IP Prefix GE (0-32)*

IP Prefix LE

*Expected IP Prefix LE (0-32)*

ESG1 Actions ▼

Summary Monitor **Manage**

Settings Firewall DHCP NAT **Routing** Load Balancer VPN SSL VPN

Global Configuration  
Static Routes  
OSPF  
BGP  
**Route Redistribution**

Route Redistribution Status :

OSPF :  BGP :

IP Prefixes :

Name

**Change redistribution settings** ?

Enable Redistribution for

OSPF

BGP

ISIS

**New IP Prefix** ?

Name \*

IP/Network \*

*IP/Network should be entered in CIDR format e.g. 192.169.1.0/24*

**New Redistribution criteria** ?

Prefix Name :

Learner Protocol :

Allow learning from :

OSPF

BGP

Static routes

Connected

Action :

ESG1 Actions ▾

Summary Monitor **Manage**

Settings Firewall DHCP NAT Routing **Load Balancer** VPN SSL VPN

⏪

**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  
 Service Definition:   
 Service Configuration:   
 Deployment Specification:

Runtime NICs | Attributes | Typed Attributes

Name	Connected To	ConnectivityType	IP Address	Subnet Mask	Gateway Address
app-internal	App-Logicals witch	Data	192.168.0.1	255.255.255.0	192.168.0.1
uplink-external	OutboundPG	Data	192.168.1.99	255.255.255.0	192.168.1.99
vnic2					
vnic3					
vnic4					
vnic5					
vnic6					
vnic7					
vnic8					
vnic9					

OK Cancel

**ESG1** Actions

Summary Monitor **Manage**

Settings | Firewall | DHCP | NAT | Routing | **Load Balancer** | VPN | SSL VPN

Global Configuration  
 Application Profiles  
 Service Monitoring  
 Pools  
 Virtual Servers  
 Application Rules

**Load balancer global configuration**

Load Balancer Status	Enabled
Service Insertion Status	Disabled
Acceleration Status	Enabled
Logging	Disabled
Log Level:	info

ESG1 Actions ▾

Summary Monitor **Manage**

Settings Firewall DHCP NAT Routing **Load Balancer** VPN SSL VPN-Plus Gr

Global Configuration  
Application Profiles  
**Service Monitoring**  
Pools  
Virtual Servers  
Application Rules

+ ✎ ✕

Monitor ID	Name
monitor-1	default_tcp_monitor
monitor-2	default_http_monitor
monitor-3	default_https_monitor

**New Service Monitor** ?

Name: \*

Interval:  (seconds)

Timeout:  (seconds)

Max Retries:

Type:  ▾

Expected:

Method:  ▾

URL:

Send:

Receive:

Extension:

OK Cancel

ESG1 Actions ▾

Summary Monitor **Manage**

Settings Firewall DHCP NAT Routing **Load Balancer** VPN SSL VPN-Plus Gro

◀◀  
 Global Configuration  
 Application Profiles  
 Service Monitoring  
**Pools**  
 Virtual Servers  
 Application Rules

+ ✎ ✕ Show Pool Statistics  
 Pool ID Name  


New Pool ?

Name: \*

Description:

Algorithm: ROUND-ROBIN ▾

Algorithm Parameters:

Monitors: NONE ▾

Members:

+ ✎ ✕

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connection.

Transparent

OK Cancel

**New Member** ?

Name: \*

IP Address / VC Container: \*  [Select](#)

State:  ▾

Port:

Monitor Port:

Weight:

Max Connections:

Min Connections:

**ESG1** Actions ▾

Summary Monitor **Manage**

Settings Firewall DHCP NAT Routing **Load Balancer** VPN

◀

- Global Configuration
- Application Profiles**
- Service Monitoring
- Pools
- Virtual Servers
- Application Rules

+ ✎ ✕

Profile ID




New Profile
?

Name:

Type: TCP ▼

Enable SSL Passthrough

HTTP Redirect URL:

Persistence: None ▼

Cookie Name:

Mode:  ▼

Expires in (Seconds):

Insert X-Forwarded-For HTTP header

Enable Pool Side SSL

Virtual Server Certifica...
Pool Certificates

Service Certificates
CA Certificates
CRL

Configure Service Certificate

	Common Name	Issuer	Validity
<input checked="" type="radio"/>	vcenter.lab.local	CA	Mon Jul 11 2016 - Mon Jul
<input type="radio"/>	VSM_SOLUTION_1100	VSM_SOLUTION_1100	Tue May 2 2017 - Thu Apr
<input type="radio"/>	VSM_SOLUTION_1100	VSM_SOLUTION_1100	Tue May 2 2017 - Thu Apr
<input type="radio"/>	VSM_SOLUTION_7d3b	VSM_SOLUTION_7d3b	Tue May 2 2017 - Thu Apr
<input type="radio"/>	VSM_SOLUTION_7d3b	VSM_SOLUTION_7d3b	Tue May 2 2017 - Thu Apr

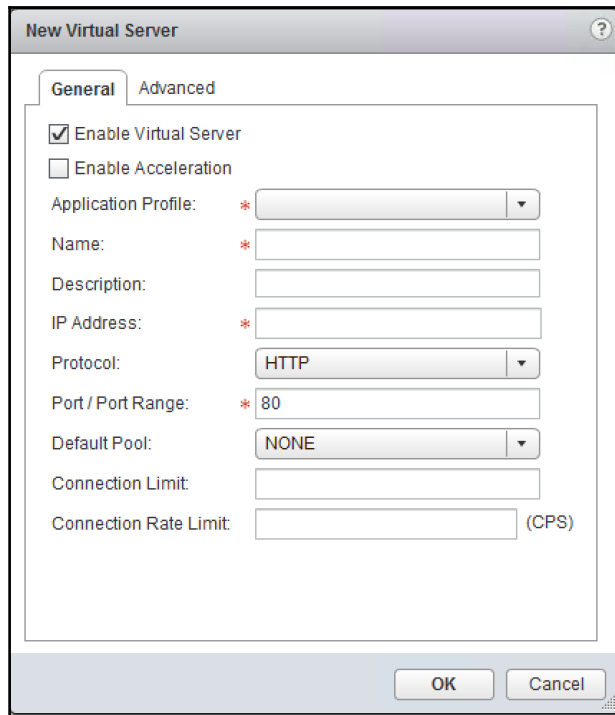
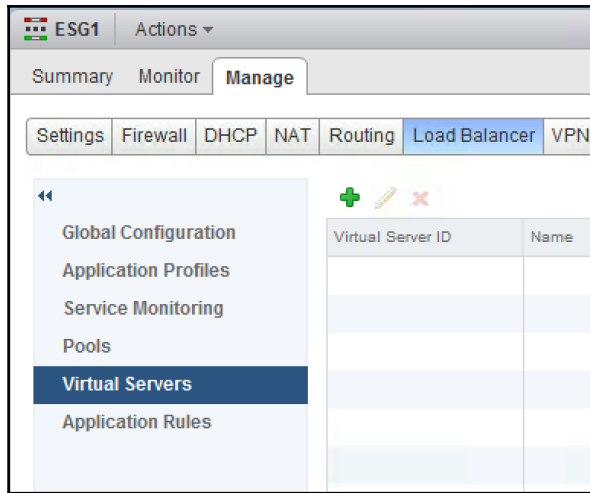
Cipher: Default ▲

ECDHE-RSA-AES128-GCM-SHA256

ECDHE-RSA-AES256-GCM-SHA384

Client Authentication: Ignore ▼

OK
Cancel



ESG1 Actions ▾

Summary Monitor **Manage**

Settings Firewall DHCP NAT Routing **Load Balancer** VF

◀

- Global Configuration
- Application Profiles
- Service Monitoring
- Pools
- Virtual Servers
- Application Rules**

+ ✎ ✕

Rule Id


**Add Application Rule** ?

Name: Redirect rule script

Script:

```
acl is_foo hdr_dom(host) -i foo
acl is_bar hdr_dom(host) -i bar
use_backend pool_1 if is_foo
use_backend pool_2 if is_bar
```

OK Cancel

ESG1 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**

Rule Id	Name	Script
applicationRule-5	applicationRule-1	acl is_foo hdr_dom(host) -i foo acl is_bar hdr_dom(host) -i bar use_backend pool_1 if is_foo use_backend pool_2 if is_bar

ESG1 Actions

Summary Monitor **Manage**

Settings Firewall DHCP NAT Routing Load Balancer VPN **SSL VPN-Plus** Grouping Objects

Dashboard  
Server Settings  
IP Pool  
Private Networks  
Authentication  
Installation Package  
Users  
Client Configuration  
Login/Logout Scripts  
General Settings  
Portal Customization

**Status**

Service: Disabled  Enable

Concurrent Sessions:  
Number of Active Sessions: 0 [Details](#)  
Maximum Active Sessions allowed: 50

**Statistics**

Show For: 1 H 24 H 1 W 1 M 1 Y

**Session Statistics**

Active Sessions Sessions Created Authentication Failures

Active Sessions & Authentication Failures (Left Y-axis, 0-100)  
Sessions Created (Right Y-axis, 0-100)

Time: 5:53 PM, 6:06 PM, 6:20 PM, 6:33 PM, 6:46 PM

**Data Flow**

Sent Bytes Received Bytes

kbps

Time: 5:53 PM, 6:03 PM, 6:13 PM, 6:23 PM, 6:33 PM, 6:43 PM, 6:53 PM

### Change Server Settings

IPv4 Address: 192.168.1.99 (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
<input type="radio"/>			7/11/2016 2:59:57 PM - 7/6/2026 3... ▲
<input type="radio"/>			7/11/2016 2:59:57 PM - 7/6/2026 3...
<input type="radio"/>	vcenter.lab.local	vcenter.lab.local	7/11/2016 3:09:43 PM - 7/6/2026 3...
<input type="radio"/>	VSM SOLUTION 11005fad-bd:	VSM SOLUTION 11005fad-bd:	5/2/2017 7:08:28 PM - 4/8/2117 7:... ▼

OK Cancel

### Add Static IP Pool

IP Range: \* [ ] To [ ]

Netmask: \* [ ]

Gateway: \* [ ] *This will add an IP address in na0 interface.*

Description: [ ]

Status:  Enabled  Disabled

**Advanced**

Primary DNS: [ ]

Secondary DNS: [ ]

DNS Suffix: [ ]  
*Example.eng.vmware.com*

WINS Server: [ ]

OK Cancel

**Add Private Network** ?

Network: \*   
*Network should be entered in CIDR format e.g. 192.169.1.0/24*

Description:

Send Traffic:  Over Tunnel  Bypass Tunnel

Enable TCP Optimization

Ports:

Status:  Enabled  Disabled

OK Cancel

**Add Authentication Server** ?

Authentication Server Type: AD

Enable SSL:

IP Address: \*

Port: \* 389

Timeout: 10 Sec(s)

Status:  Enabled  Disabled

**Advanced:**

Search base: \*

Bind DN: \*

Bind Password:

Retype Bind Password:

Login Attribute Name: \* sAMAccountName

Search Filter: \* objectClass=\*

Use this server for secondary authentication

Terminate Session if authentication fails

OK Cancel

**Add Installation Package** ?

Profile Name: \*

Gateway	Port		
<input type="text"/>	443	<input type="button" value="OK"/>	<input type="button" value="Cancel"/>

Create installation packages for:

Windows  Linux  Mac

Description:

Status:  Enabled  Disabled

**Installation Parameters for Windows:**

<input type="checkbox"/> Start client on logon	<input type="checkbox"/> Hide client system tray icon
<input type="checkbox"/> Allow remember password	<input checked="" type="checkbox"/> Create desktop icon
<input type="checkbox"/> Enable silent mode installation	<input type="checkbox"/> Enable silent mode operation
<input type="checkbox"/> Hide SSL client network adapter	<input type="checkbox"/> Server security certificate validation

**Add User** ?

User ID: \*

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

Summary Monitor **Manage**

Settings Firewall DHCP NAT Routing Load Balancer VPN **SSL V**

←

**Dashboard**

Server Settings

IP Pool

Private Networks

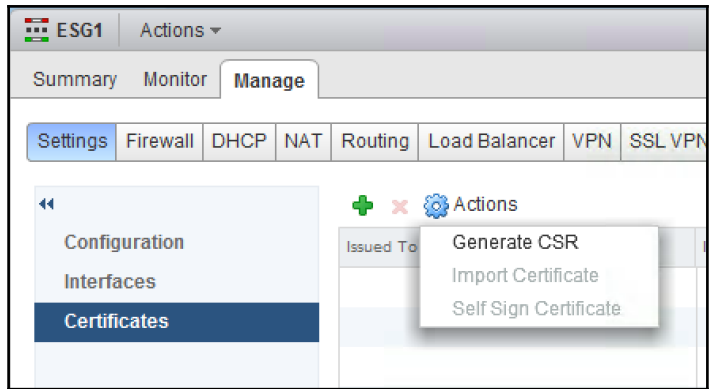
Authentication

**Service enabled successfully!**

▼ Status

Service: Enabled





The screenshot shows the 'Generate CSR' dialog box. It has a title bar with 'Generate CSR' and a help icon. The dialog contains the following fields and options:

- Common Name: \*
- Organization Name: \*
- Organization Unit: \*
- Locality: \*
- State: \*
- Country: \*
- Message Algorithm:
- Key Size:
- Description:

At the bottom right, there are 'OK' and 'Cancel' buttons.

ESG1 Actions

Summary Monitor **Manage**

Settings Firewall DHCP NAT Routing Load Balancer **VPN** SSL VPN-Plus Grouping Objects

IPsec VPN

L2 VPN

IPsec VPN Service Status: Disabled

Global configuration status: Not Configured [Change](#)

Logging Policy

[+](#) [✎](#) [✕](#) [✓](#) [⊘](#) [📄](#) Show IPsec Statistics

Name	Local Endpoint	Local Subnets

Global Configuration ?

Pre-Shared Key:


Display shared key  
*The global pre-shared key is shared by all the sites whose peer endpoint is set to 'any'.*

Extension:

Server Certificate:  Enable Certificate Authentication

Service Certificates CA Certificates CRL

	Common Name	Issuer	Validity
<input type="radio"/>	vcenter.lab.local	CA	Monday, July 11, 2016 - Monday, J...
<input type="radio"/>	VSM_SOLUTION_11005fad-bd	VSM_SOLUTION_11005fad-bd	Tuesday, May 2, 2017 - Thursday, ...
<input type="radio"/>	VSM_SOLUTION_11005fad-bd	VSM_SOLUTION_11005fad-bd	Tuesday, May 2, 2017 - Thursday, ...
<input type="radio"/>	VSM_SOLUTION_7d3b2bef-46	VSM_SOLUTION_7d3b2bef-46	Tuesday, May 2, 2017 - Thursday, ...
<input type="radio"/>	VSM_SOLUTION_7d3b2bef-46	VSM_SOLUTION_7d3b2bef-46	Tuesday, May 2, 2017 - Thursday, ...

IPsec VPN Service Status:	Disabled	 Enable
Global configuration status:	Configured	<a href="#">Change</a>
▼ Logging Policy		
Enable logging	<input type="checkbox"/>	
Log level:	INFO ▼	

**Add IPsec VPN** ?

Enabled

Enable perfect forward secrecy(PFS)

Name:

Local Id: \*

Local Endpoint: \*

Local Subnets: \*

*Subnets should be entered in CIDR format with comma as separator.*

Peer Id: \*

Peer Endpoint: \*

*Endpoint should be a valid IP, FQDN or any.*

Peer Subnets: \*

*Subnets should be entered in CIDR format with comma as separator.*

Encryption Algorithm:  ▼

Authentication:  PSK  Certificate

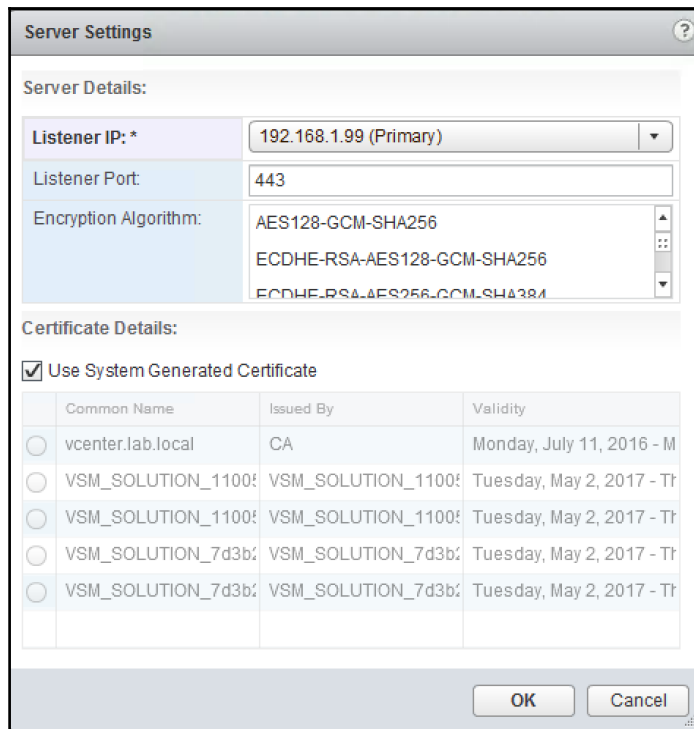
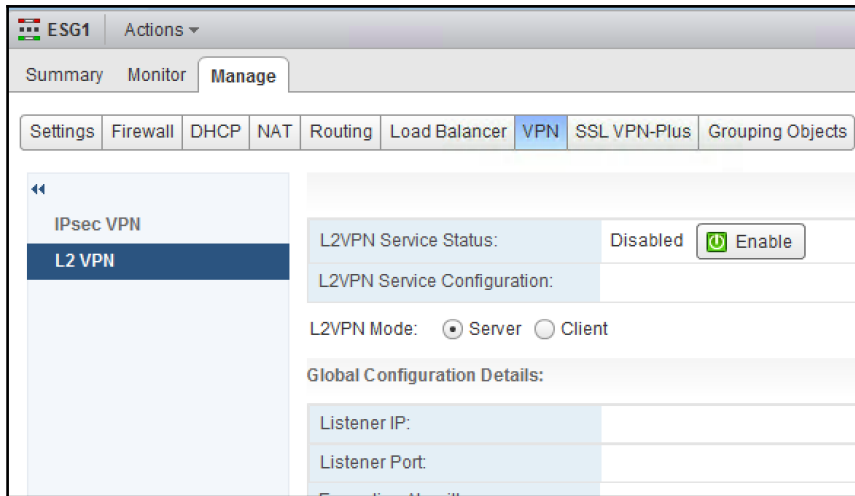
Pre-Shared Key:

Display shared key

Diffie-Hellman Group:  ▼

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.*



**Add Peer Site** ?

Enable Peer Site

Name: \*

Description:

User Id: \*

Password: \*

Confirm Password: \*

Stretched Interfaces: \*  [Select Sub Interfaces](#)

Egress Optimization Gateway Address:

*Example: Comma separated list of IP address  
Ex: 191.1.1.1,192.1.1.1*

Enable Unstretched Networks

Unstretched Networks:

*Example: Comma separated list of networks  
Ex: 192.168.10.0/24,192.168.20.0/24*

ESG1 Actions ▾

Summary Monitor **Manage**

Settings Firewall DHCP NAT Routing Load Balancer **VPN** SSL VPN-Plus Grouping Objects

IPsec VPN  
**L2 VPN**

L2VPN Service Status: Disabled

L2VPN Service Configuration:

L2VPN Mode:  Server  Client

Global Configuration Details:

Server Address:

Server Port:

Encryption Algorithm:

Stretched Interface:

Egress Optimization Gateway Address:

Unstretched Networks:

User Id:

▸ CA Certificate:

▸ Proxy Settings:

**Client Settings** [?]

**Client Details** | Advanced

**Client Details:**

<b>Server Address: *</b>	<input type="text"/>
Server Port:	<input type="text" value="443"/>
Encryption Algorithm:	<input type="text" value="AES128-GCM-SHA256"/> <input type="text" value="ECDHE-RSA-AES128-GCM-SHA256"/>
Stretched Interfaces:	<input type="text"/> <a href="#">Select Sub Interfaces</a>
Egress Optimization Gateway Address:	<input type="text"/> <i>Example: Comma separated list of IP address Ex: 191.1.1.1, 192.1.1.1</i>
Unstretched Networks:	<input type="checkbox"/> <b>Enable Unstretched Networks</b> <input type="text"/> <i>Example: Comma separated list of networks Ex: 192.168.10.0/24, 192.168.20.0/24</i>

**User Details:**

<b>User Id: *</b>	<input type="text"/>
<b>Password: *</b>	<input type="password"/>
<b>Confirm Password: *</b>	<input type="password"/>

OK Cancel



ESG1 Actions






Summary Monitor **Manage**

Settings Firewall DHCP NAT Routing Load Balancer VPN SSL VPN-Plus Grouping Objects

Configuration  
**Interfaces**  
 Certificates

0 Job(s) In Progress

Configure interfaces of this NSX Edge.

     Actions

vNIC#	1 ▲	Name	IP Address	Subnet Prefix Length
0		app-internal	192.168.0.1*	24
1		uplink-external	192.168.1.99*	24
2		vnic2		
3		vnic3		
4		vnic4		
5		vnic5		

**Edit NSX Edge Interface**
?

vNIC#: 2

Name: \*

Type: Trunk ▼

Connected To:  [Change](#) [Remove](#)

Connectivity Status:  Connected  Disconnected

Sub Interfaces:

+
✎
✖

Q Filter

vNIC#	Name	Network	VLAN / VNI	Tunnel ID	Status

\* indicates new SubInterface

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:

OK
Cancel

Add Sub Interface
?

Enable Sub-Interface

Name: \*

Tunnel Id: \*   
Values from 1-4093

Backing Type: Network ▾

Network:  Select Remove

Configure Subnets:

+
✎
✕
Filter

Primary IP Address	Secondary IP Address	Subnet Prefix Length

MTU:   
Values from 68-9000

Options:  Enable Send Redirect

Reverse Path Filter: Enabled ▾

OK
Cancel

**NSX Edges**

NSX Manager: 192.168.1.8 (Role: Primary)

Actions

Id	Actions - App-DLR	Type
edge-5	<ul style="list-style-type: none"> <li>Delete</li> <li>Force Sync</li> <li>Deploy</li> <li>Redeploy</li> <li>Change Auto Rule Configuration</li> <li>Download Tech Support Logs</li> <li>Upgrade Version</li> <li>Change Appliance Size</li> </ul>	Logical Router
edge-6		NSX Edge

**ESG1** Actions

Summary Monitor **Manage**

Settings Firewall DHCP NAT Routing Load Balancer VPN SSL VPN-Plus Grouping Objects

Configuration

- Interfaces
- Certificates

Details:

Size:	Compact
Host Name:	esg1.lab.local
Auto generate rules:	Enabled
FIPS mode:	Disabled
Syslog servers:	<a href="#">Change</a>
Server 1:	
Server 2:	

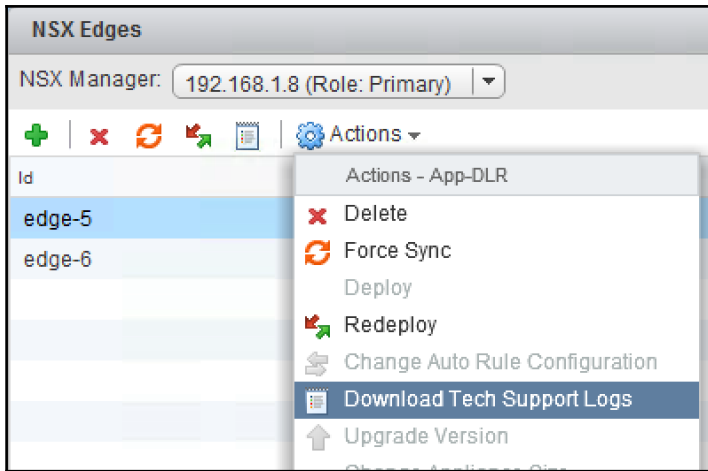
**Edit Syslog Servers Configuration**

Syslog Server 1: \*

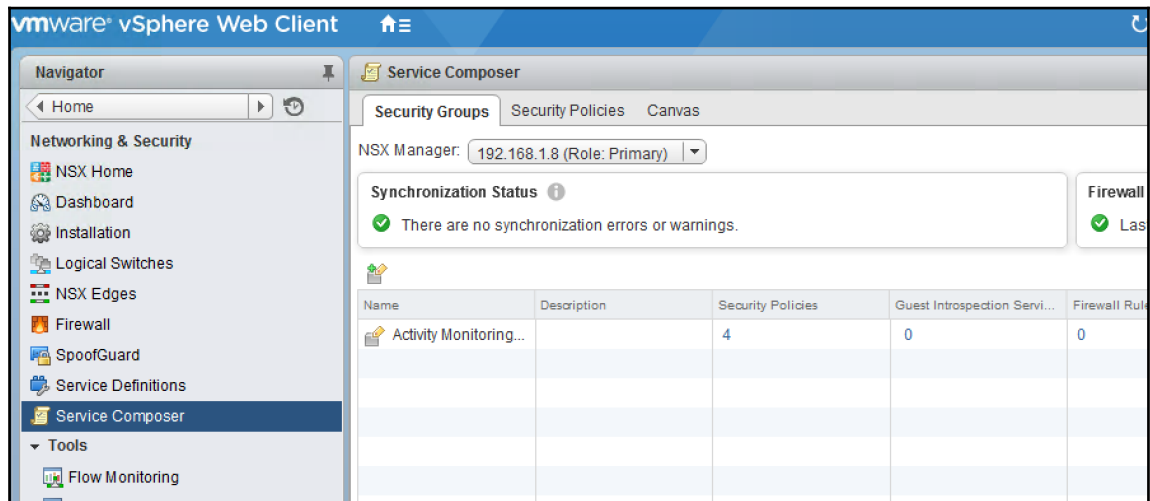
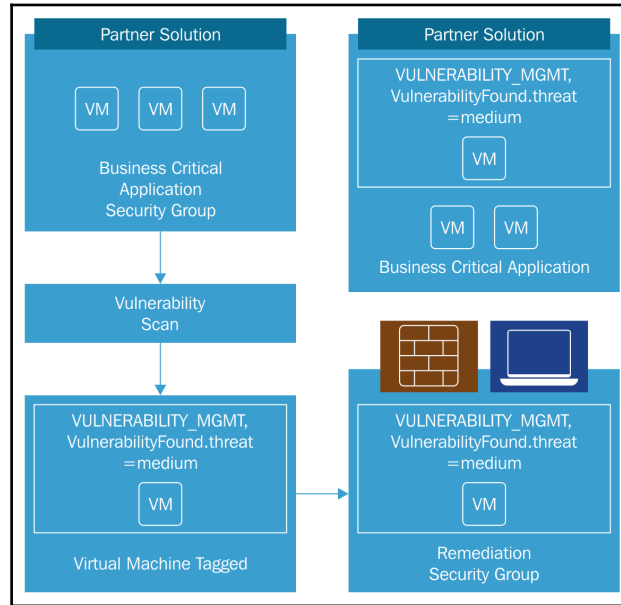
Syslog Server 2:

Protocol: tcp

OK Cancel



# Chapter 06: Service Composer



**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: \*

Description:

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

**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

Computer OS Name Contains Web

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**

Available Objects (9 items):

app-02a
db-02a
✓ web-04a
✓ web-02a
db-01a
✓ web-03a
✓ win8-01a
✓ web-01a
app-01a

Selected Objects (5 items):

✓ web-02a
✓ web-04a
✓ web-01a
✓ win8-01a
✓ web-03a

Buttons: 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: **Security Group**

Available Objects (4 items):

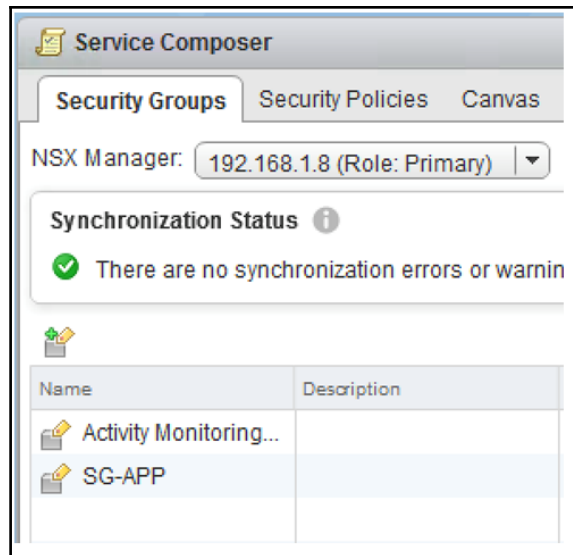
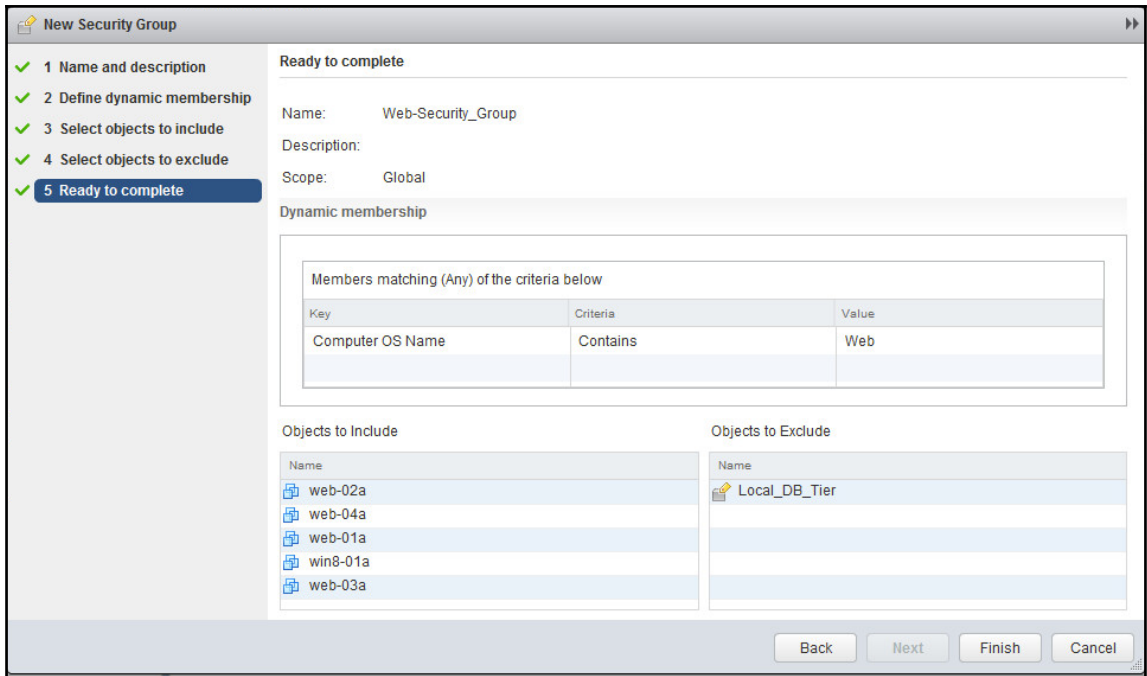
Activity Monitoring Data Collection
Local_App_Tier
✓ Local_DB_Tier
Local_Web_Tier

Selected Objects (1 item):

✓ Local_DB_Tier
-----------------

Buttons: Back, Next, Finish, Cancel





**Navigator**

Home

**Networking & Security**

- NSX Home
- Dashboard
- Installation
- Logical Switches
- NSX Edges
- Firewall
- SpoofGuard
- Service Definitions
- Service Composer**
- Tools
- Flow Monitoring

**Service Composer**

Security Groups | **Security Policies** | Canvas

NSX Manager: 192.168.1.8 (Role: Primary)

**Synchronization Status** ⓘ

✓ There are no synchronization errors or warnings.

Rank	Name

**New Security Policy**

- ✓ 1 **Name and description**
- ✓ 2 Guest Introspection Services
- ✓ 3 Firewall Rules
- ✓ 4 Network Introspection Services
- ✓ 5 Ready to complete

Name: App Security Policy

Description:

Inherit security policy

Parent policy:

Advanced options

Back Next Finish Cancel

**Add Guest Introspection Service**

Name:

Description:

Action:  Apply  
 Block

Service Type:

Service Name:

Service Profile:

State:  Enabled  
 Disabled

Enforce:  Yes  
 No

**Add Guest Introspection Service**

Name:

Description:

Action:  Apply  
 Block

Service Type:  ▼

Service Name:

Service Profile:

State:  Enabled  
 Disabled

Enforce:  Yes  
 No

**New Firewall Rule** [X]

Name:

Description/Comments:

Action:  Allow  
 Block  
 Reject

Source: Policy's Security Groups [Change...](#)  
 Negate source

Destination: Any [Change...](#)  
 Negate destination

**i** *Either source or destination selection (or both) must be "Policy's Security Groups".  
Current selection will apply to "Outgoing" traffic from the security groups where this policy gets applied to specified Destination.*

Service: Any [Change...](#)

State:  Enabled  
 Disabled

Log:  Log  
 Do not log

OK Cancel

Name:

Description:

Action:  Redirect to service  
 Do not redirect

Service Name:

Profile:

Source: Policy's Security Groups [Change...](#)  
 Negate source

Destination: Any [Change...](#)  
 Negate destination

**i** *Either source or destination selection (or both) must be "Policy's Security Groups".  
Current selection will apply to "Outgoing" traffic from the security groups where this policy gets applied to specified Destination.*

Service: Any [Change...](#)

State:  Enabled  
 Disabled

Log:  Log  
 Do not log

**Service Composer**

Security Groups | **Security Policies** | Canvas

NSX Manager: 192.168.1.8 (Role: Primary) ▼

**Synchronization Status** ⓘ

✔ There are no synchronization errors or warnings.

Actions ▼

Rank	Name
1	App Security Policy

**App Security Policy** Actions ▼

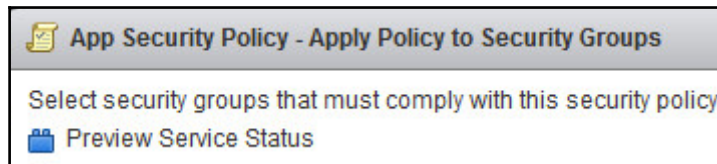
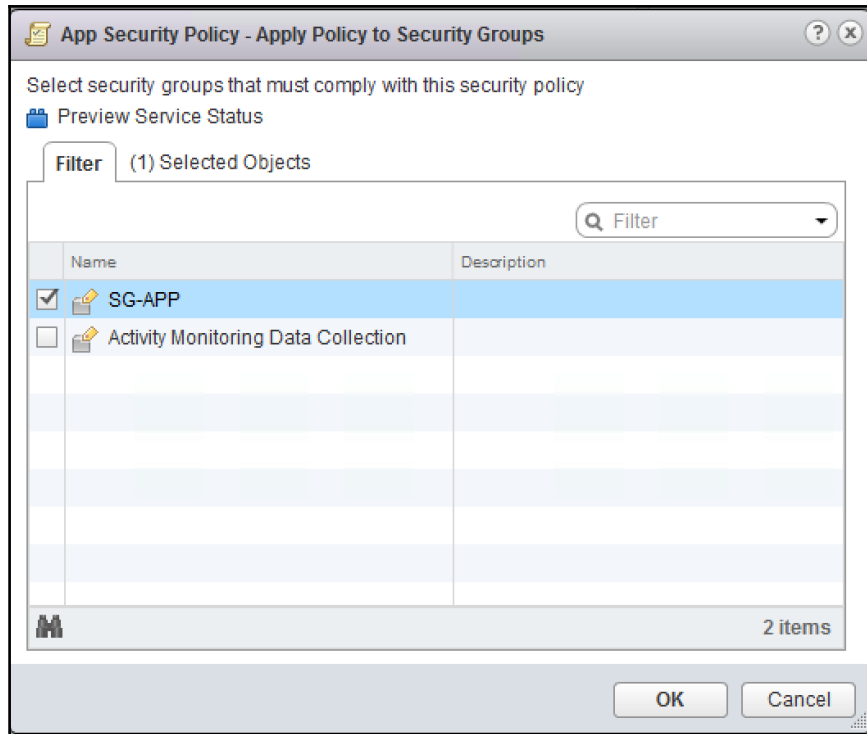
Summary | Monitor | Manage | Related Objects

**App Security Policy**

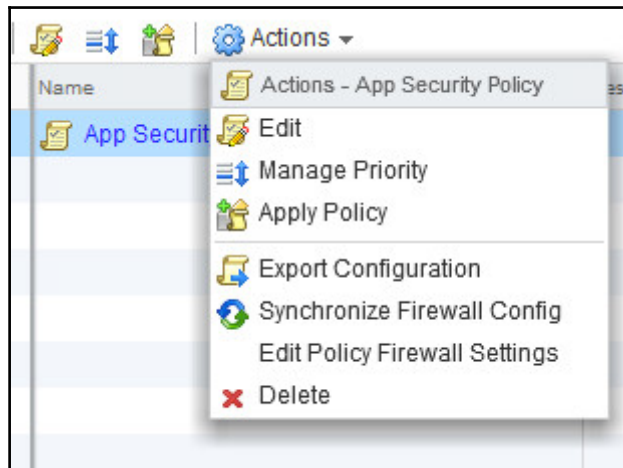
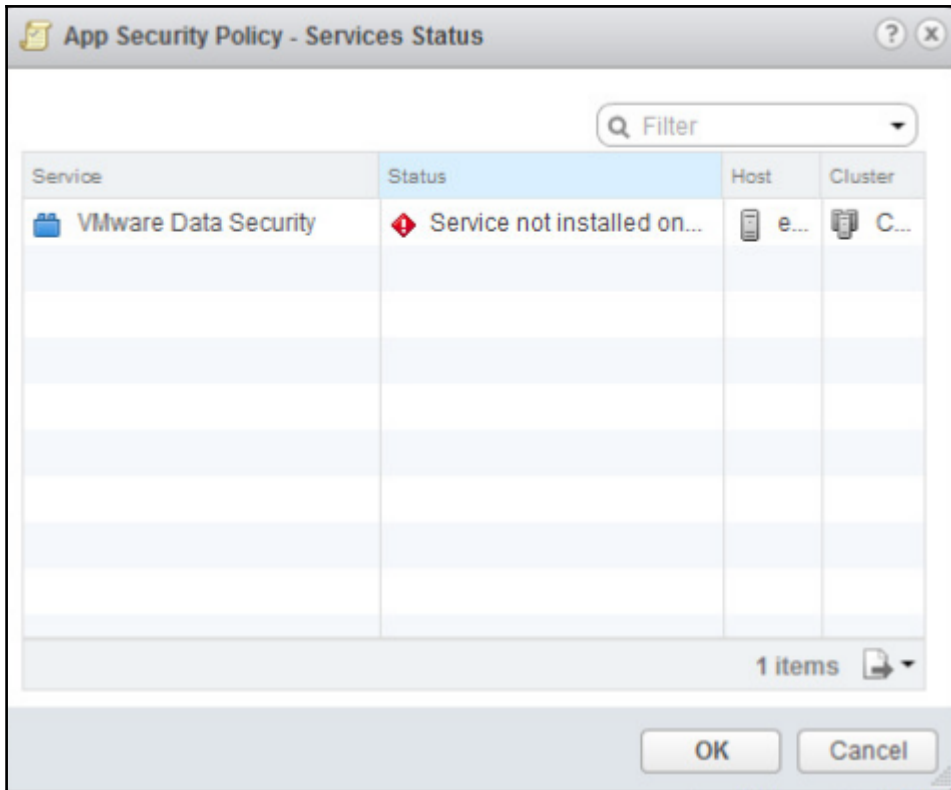
Description:  
Weight: 4300  
Inherits from:  
Sync Status: Successful

Guest Introspection Services			
No.	Name	Action	Enforce
✔ 1	App-vms	Block Anti Virus	No

Firewall Rules			
No.	Name	Source	Destination
✔ 1	Port 80 rule	Policy's S...	Any







Navigator

- Home
- 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

Firewall

Configuration | Saved Configurations | Settings

NSX Manager: 192.168.1.8 (Role: Primary)

Last publish operation succeeded 6/13/2017 1:56:28 PM

General | Ethernet | Partner security services

No.	Name	Rule ID	Source	Destination	Service	Action	Applied To
App-rules (Rule 1)							
1	app-port80	1006	New Clust...	any	CIM-HTTP	Allow	
Default Section Layer3 (Rule 2 - 4)							
2	Default Rule NDP	1003	any	any	IPv6-ICMP ... IPv6-ICMP ...	Allow	Distributed Fire...
3	Default Rule DHCP	1002	any	any	DHCP-Clie... DHCP-Ser...	Allow	Distributed Fire...
4	Default Rule	1001	any	any	any	Allow	Distributed Fire...

Navigator

- History
- 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: 192.168.1.8 (Role: Primary)

Network & Security Service Deployments

Network & security services are deployed on a set of clusters. Manage service deployments here by ad

Service	Version	Installation Status	Service Status
Guest Introspecti...	6.3.2.5672679	✓ Succeeded	⚠ Warning

**Navigator**

History

**Networking & Security**

- NSX Home
- Dashboard
- Installation
- Logical Switches
- NSX Edges
- Firewall**
- SpoofGuard
- Service Definitions
- Service Composer

**Firewall**

Configuration | Saved Configurations | Settings

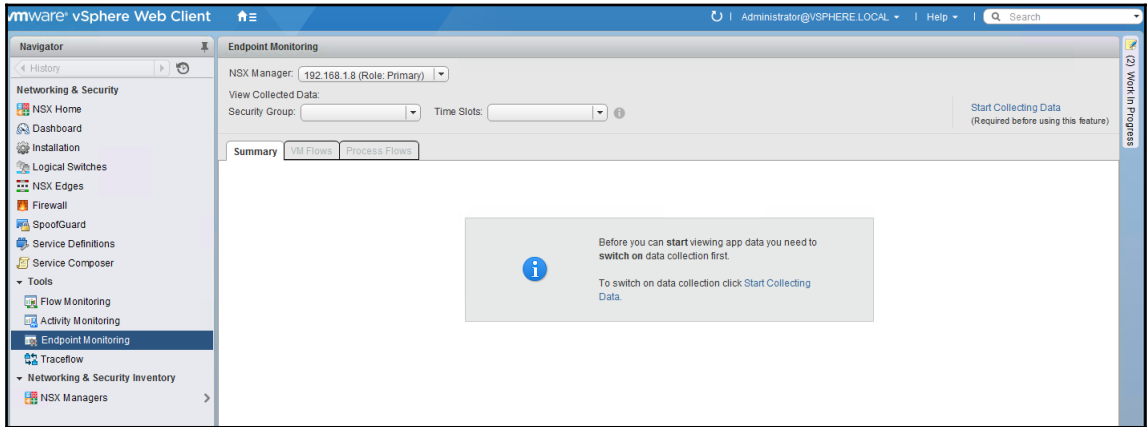
NSX Manager: 192.168.1.8 (Role: Primary)

General | Ethernet | **Partner security services**


+ [Icons]

No.	Name	Rule ID
Default Section		

# Chapter 07: Monitoring




**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-APP** [Change](#)

VM list for SG-APP

 CentOS	▲
 New Virtual Machine	⋮
 pshell-host	
 testvm	▼


6 items

---

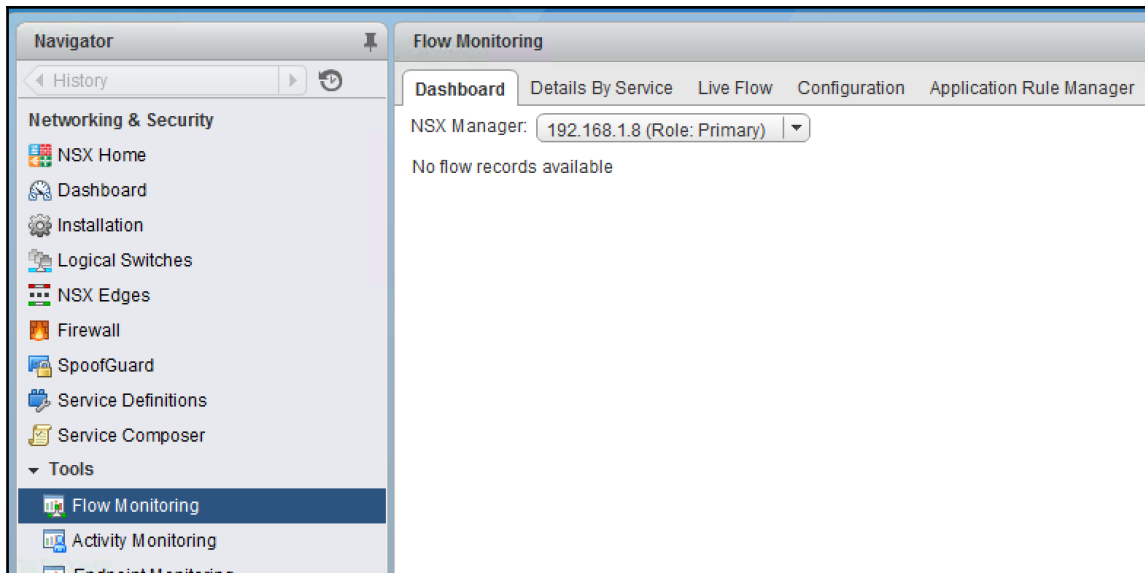
2. Switch data collection ON or OFF:

Data collection:  ON  OFF

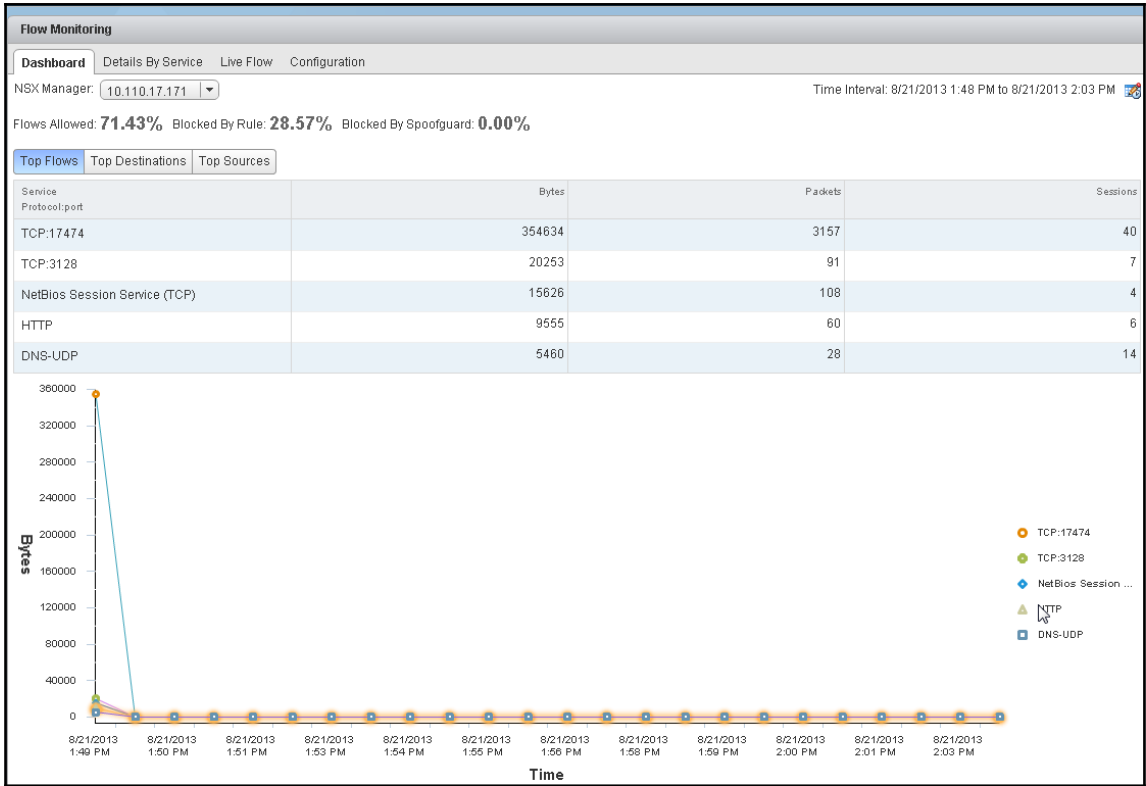
**IMPORTANT:** Your completed sessions will be automatically deleted...

 Data collection is enabled but there is no data available yet. Come back later to check again.

Collecting Data: SG-APP  
[Stop Collecting Data](#)



The screenshot shows the NSX Flow Monitoring interface. On the left is a 'Navigator' pane with a 'History' dropdown and a list of items under 'Networking & Security' and 'Tools'. 'Flow Monitoring' is selected in the 'Tools' section. The main area is titled 'Flow Monitoring' and has tabs for 'Dashboard', 'Details By Service', 'Live Flow', 'Configuration', and 'Application Rule Manager'. The 'Dashboard' tab is active, showing 'NSX Manager: 192.168.1.8 (Role: Primary)' and the message 'No flow records available'.



#### Change Time Interval

Last 15 minutes  
 Last 1 hour  
 Last 12 hours  
 Last 24 hours  
 Last 1 week  
 Last 2 weeks  
 From: 10/28/2015 11:53 : To: 10/28/2015 12:08

NSX Manager: 192.168.110.15  
 Flows Allowed: **100.00%** Blocked By Rule: **0.00%** Blocked By Spoofguard: **0.00%**

Top Flows		Top Destinations	Top Sources
Service Protocol:port	Bytes	Packets	
DNS-UDP	12.76 KB	131	
DNS-UDP	9.35 KB	123	
NetBios Session Service (TCP)	6.16 KB	48	
ICMP:echo-reply	5.97 KB	102	
IPv6-ICMP	2.20 KB	28	

Top Flows		Top Destinations	Top Sources
Destination	Incoming Traffic (Bytes)	Packets	
192.168.110.10	15.51 KB	171	
fd53::11	12.97 KB	134	
8.8.8.8	5.74 KB	98	
win8-01a (fe80::d1fc:198e:f37e:aa37)	904	11	
00:50:56:01:20:a5	598	13	

Top Flows		Top Destinations	Top Sources
Source	Outgoing Traffic (Bytes)	Packets	
win8-01a (192.168.100.222)	21.64 KB	275	
win8-01a (fe80::d1fc:198e:f37e:aa37)	13.74 KB	145	
fe80::1	744	7	
00:50:56:01:20:a5	598	13	
00:50:56:ae:09:87	598	13	

Dashboard	Details By Service	Live Flow	Configuration
NSX Manager: 192.168.110.15		Time Interval: 10/28/2015 11	
Allowed Flows		Blocked Flows	
Type	Service	Bytes	Session
UDP	DNS-UDP	12.76 KB	17
UDP	DNS-UDP	9.35 KB	16
TCP	NetBios Session Service (TCP)	6.16 KB	2
OTHER	ICMP:echo-reply	5.97 KB	2
OTHER	IPv6-ICMP:0	2.20 KB	28



**Flow Monitoring**

Dashboard Details By Service **Live Flow**

NSX Manager: 192.168.110.15

Live Flow will be shown for the selected vNIC. Please

vNIC: [Browse](#)

**Select Virtual Machine & vNIC**

Select a Virtual Machine

Filter

VM Name
Linux-01a
web-04a
web-01a
web-00a

8 Objects

Select the vNIC for Live Flow collection

vNIC Name
Linux-01a - Network adapter 1

1 items

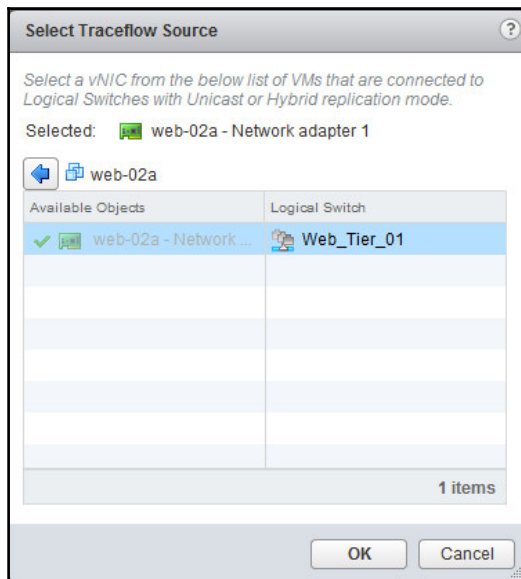
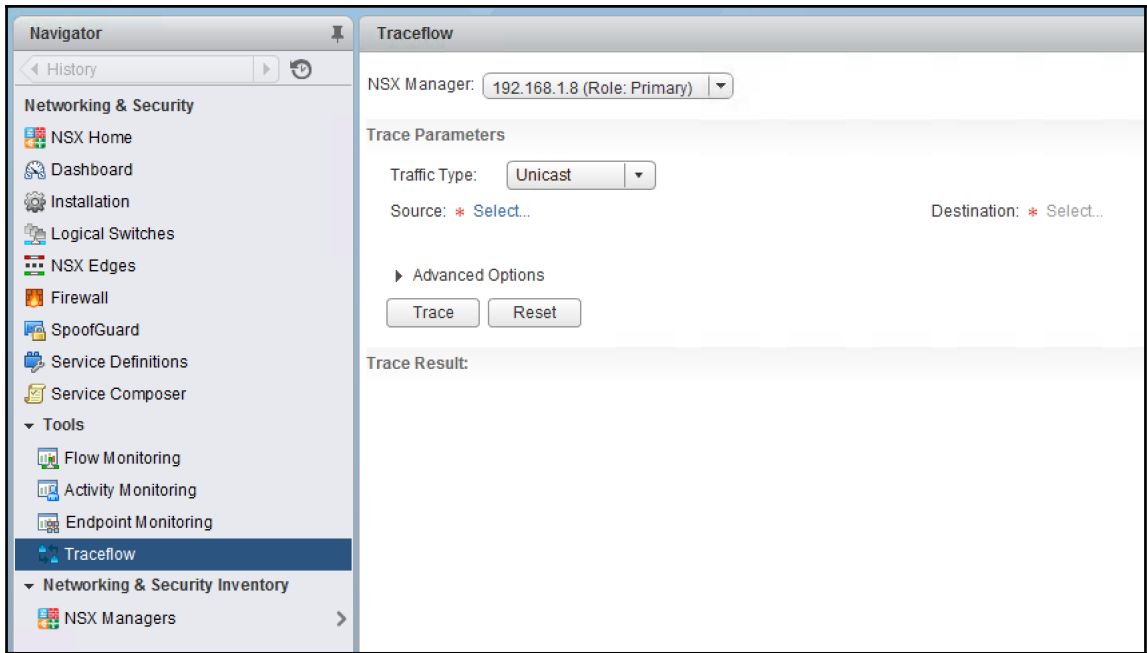
NSX Manager: 192.168.110.15

Live Flow will be shown for the selected vNIC. Please select a vNIC and press start to s

vNIC: win8-01a - Network adapter 1 [Browse](#)

Refresh Rate: 5 Seconds

RuleId	Direction	Flow Type	Protocol	Source IP	Source Port	Des
1001	OUT	Active	UDP	fe80::d1fc:198e:f3	49440	fd53::
1001	OUT	Active	UDP	192.168.100.222	58835	192.1
1001	OUT	Active	UDP	fe80::d1fc:198e:f3	58933	fd53::
1001	OUT	Inactive	UDP	fe80::d1fc:198e:f3	61723	fd53::
1001	OUT	Active	UDP	fe80::d1fc:198e:f3	52444	fd53::
1001	OUT	Active	UDP	192.168.100.222	58933	192.1
1001	OUT	Active	UDP	fe80::d1fc:198e:f3	61870	fd53::
1001	OUT	Inactive	UDP	192.168.100.222	61723	192.1
1001	OUT	Active	UDP	192.168.100.222	52444	192.1



**Select Traceflow Source** ?

Select a vNIC from the below list of VMs that are connected to Logical Switches with Unicast or Hybrid replication mode.

Selected:

Filter

Available Objects

app-01a	>
db-01a	>
web-01a	>
web-02a	>

4 items

OK Cancel

**Select Traceflow Destination** ?

Specify Destination MAC and IP Address

Select Destination vNIC

Select a vNIC from the below list of VMs that are connected to Logical Switches with Unicast or Hybrid replication mode.

Selected:

Filter

Available Objects

web-01a	>
web-02a	>

2 items

OK Cancel

**Trace Parameters**


Traffic Type:   High volume of traffic may get generated for this traffic type.


Source: \*  web-02a - Network adapter 1 [Change...](#) Subnet Prefix Length: \*

IP: 172.16.10.12, MAC: 00:50:56:ae:19:72

▶ Advanced Options

**Trace Parameters**

Traffic Type:   High volume of traffic may get generated for this traffic type.

Source: \*  web-02a - Network adapter 1 [Change...](#) Destination IP: \*  e.g. 239.0.0.1

IP: 172.16.10.12, MAC: 00:50:56:ae:19:72

▶ Advanced Options

▼ Advanced Options

Protocol:

Timeout (ms):

ICMP ID:

























Frame Size:
















Sequence:

TTL:

Trace Result: Traceflow delivered observation(s) reported

**1 Delivered**

Sequence	1 ▲	Observation Type	Host	Component Type	Component Name
0		 Injected	 esx-03a.corp.local	vNIC	 vNIC
1		 Received	 esx-03a.corp.local	Firewall	 Firewall
2		 Forwarded	 esx-03a.corp.local	Firewall	 Firewall
3		 Forwarded	 esx-03a.corp.local	Physical	 esx-03a.corp.local
3		 Forwarded	 esx-03a.corp.local	Physical	 esx-03a.corp.local
4		 Received	 esx-05a.corp.local	Physical	 esx-05a.corp.local
4		 Received	 esx-05a.corp.local	Physical	 esx-05a.corp.local
4		 Received	 esx-05a.corp.local	Physical	 esx-05a.corp.local

4		 Received	 esx-01a.corp.local	Physical	 esx-01a.corp.local
4		 Received	 esx-01a.corp.local	Physical	 <a href="#">esx-01a.corp.local</a>
5		 Received	 esx-01a.corp.local	Firewall	 Firewall
6		 Forwarded	 esx-01a.corp.local	Firewall	 Firewall
7		 Delivered	 esx-01a.corp.local	vNIC	 vNIC

# Chapter 08: Managing NSX

Time Settings	
Specify NTP server below. For SSO configuration to work correctly it is required that the time on this virtual appliance and NTP server should be in sync. It is recommended to use the same NTP server used by the SSO server.	
NTP Server	192.168.110.1
Timezone	UTC
Date/Time	11/12/2015 03:29:39

**Time Settings** [X]

Specify NTP server below. For SSO configuration to work correctly it is required that the time on this virtual appliance and NTP server should be in sync. It is recommended to use the same NTP server used by the SSO server.

NTP Server:

Timezone:

Date/Time:

Syslog Server	
You can specify the IP address or name of the s	
Syslog Server	
Port	
Protocol	

**Syslog Server** [X]

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:

Port:

Protocol:

OK Cancel

**DNS Servers**

To resolve all objects referenced using a hostname, you must provide one or more DNS servers common to vCenter, ESX hosts and other vSphere components (If primary or secondary server is removed, the next available dns server in the line would assume the responsibility).

IPv4 DNS Servers	
Primary Server	192.168.110.10
Secondary Server	
IPv6 DNS Servers	
Primary Server	
Secondary Server	
Search Domains	corp.local

**DNS Servers** [X]

To resolve all objects referenced using a hostname, you must provide one or more DNS servers common to vCenter, ESX hosts and other vSphere components (If primary or secondary server is removed, the next available dns server in the line would assume the responsibility).

**IPv4 DNS Servers**

Primary Server:

Secondary Server:

**IPv6 DNS Servers**

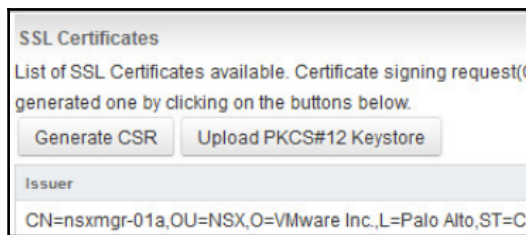
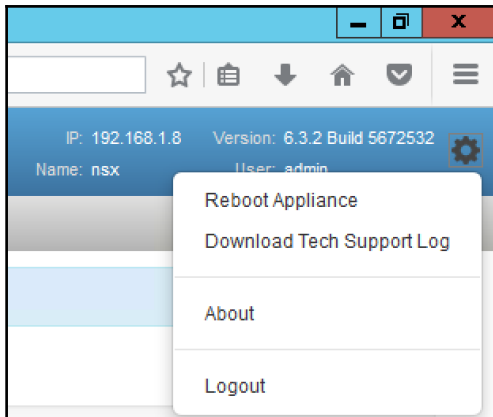
Primary Server:

Secondary Server:

**Domain Search List**

Search Domains:

OK 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:

Key Size:

Common Name:

Organization Unit:

Organization Name:

Locality Name:

State Name:

Country Code:

Self Sign CSR and apply certificate

Number of Days:

OK Cancel

Backups & Restore	
FTP Server Settings:	
Scheduling:	OFF
Exclude:	
Backup History	
File Name	

**Backup Location** x

IP/Host name:

Transfer Protocol:

Port:  Invalid Port number

User name:

Password:

Backup Directory:

Filename Prefix:

Pass Phrase:

**Create or Schedule Backup**

Backup Frequency:

Day of week:

Hour of day:

Minute:



**NSX Edges**

NSX Manager: 192.168.1.8 (Role: Primary)

+ | × | ↻ | ↶ | 📅 | ⚙️ Actions ▾

Id	Actions - App-DLR
edge-5	× Delete ↻ Force Sync Deploy ↶ ↷ Redeploy
edge-6	

**Firewall**

Configuration | Saved Configurations | Settings

NSX Manager: 192.168.1.8 (Role: Primary)

📘 Last publish operation succeeded 6/26/2017 3:07:53 PM

General | Ethernet | Partner security services

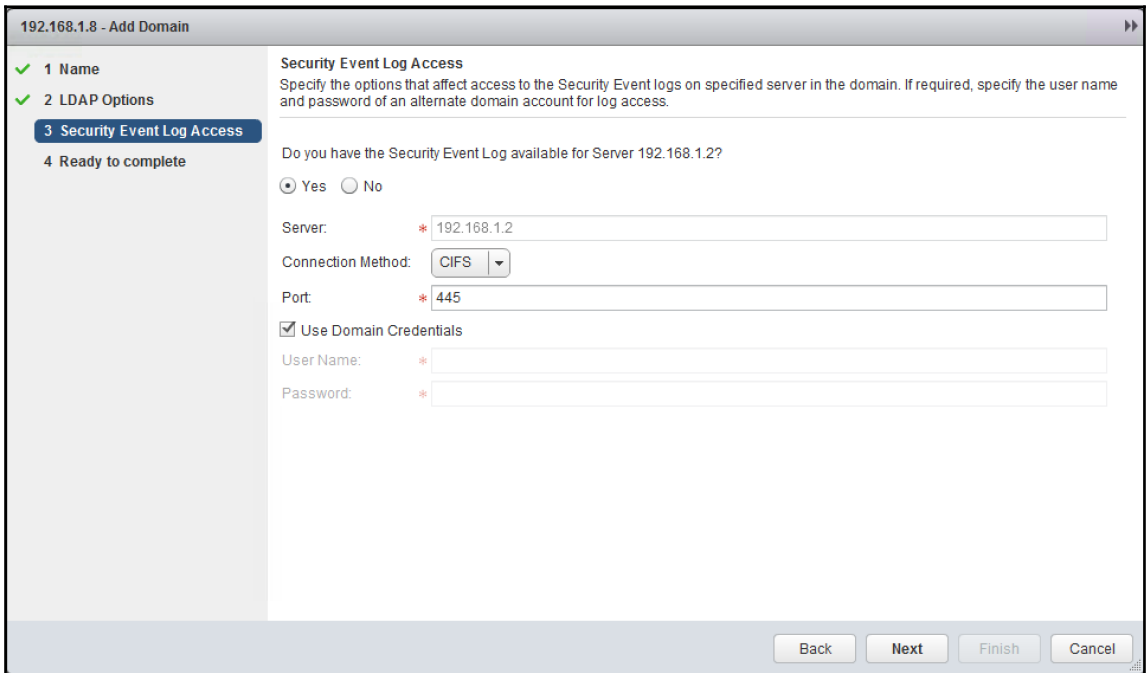
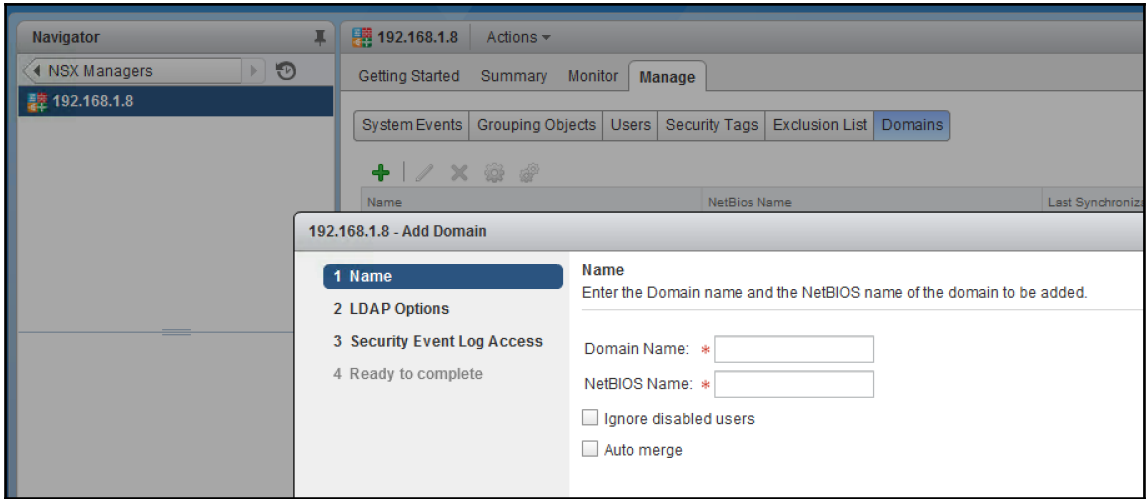
+ | 📄 | × | ⬆️ | ⬇️ | 📄 | 📄 | 🔍 | 🌱

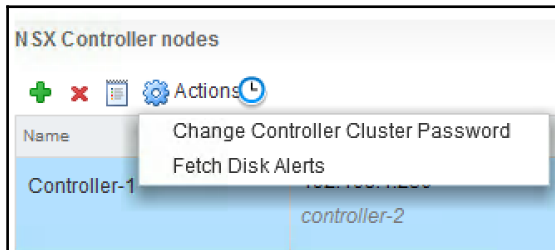
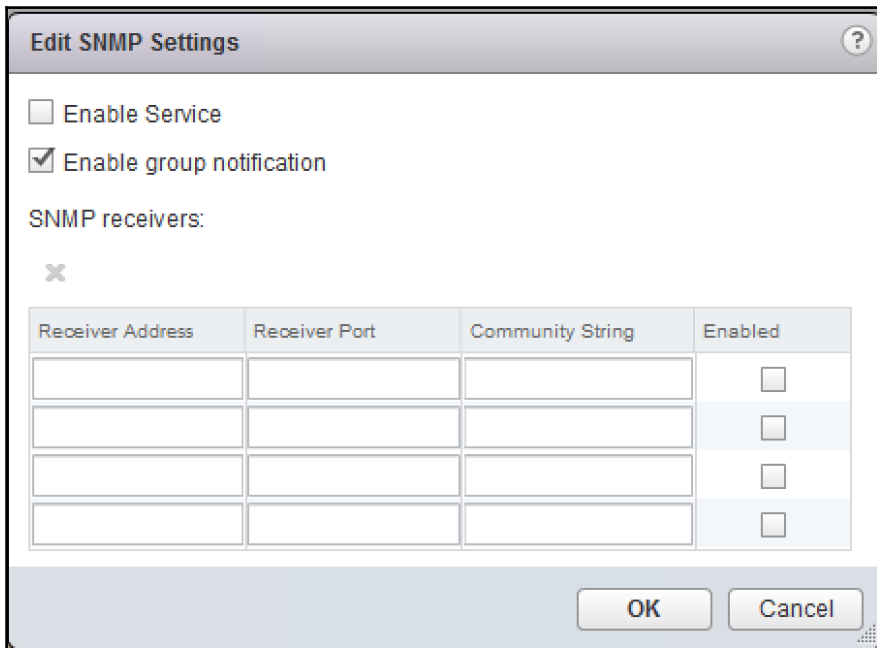
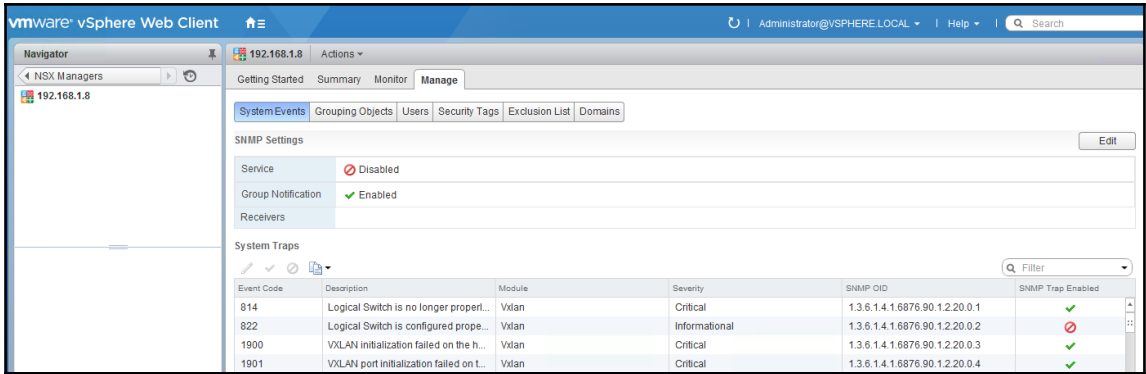
No.	Name	Rule ID	Source	Destination
▶	App-rules (Rule 1)			
▶	Default Section Layer3 (Rule 2 - 4)			

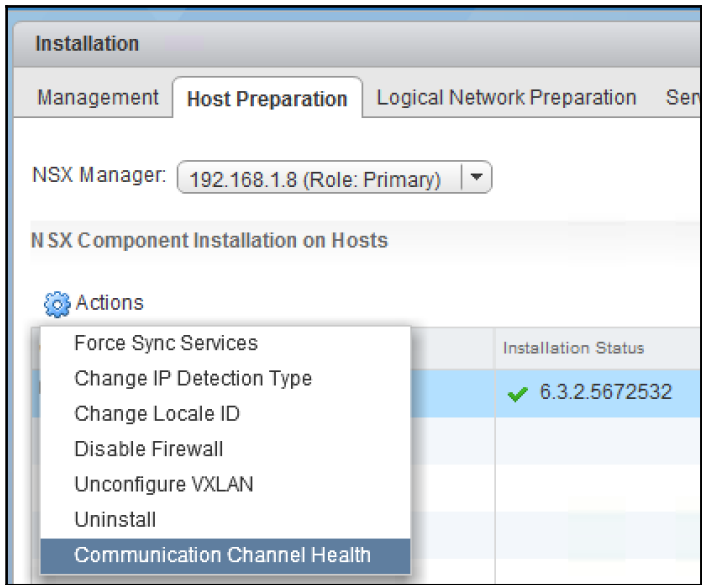
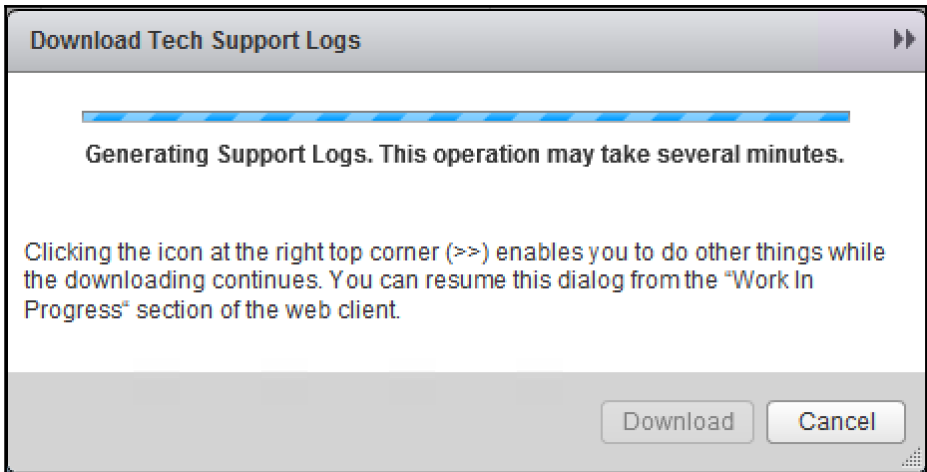
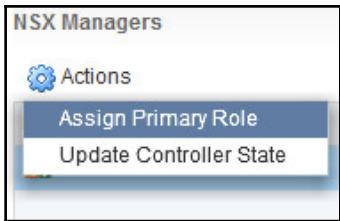
**Export configuration** ⓘ

Current firewall configuration has been exported successfully. Click on 'Download' to save the configuration to disk.









New Cluster-1 - Channel Health <span style="float: right;">?</span>			
Hosts	NSX Manager to Firewall Agent	NSX Manager to Control Plane Ag...	Control Plane Agent to Controller
esx3.lab.local	↑ Up	↑ Up	↑ Up
esx1.lab.local	↑ Up	↑ Up	↑ Up
esx2.lab.local	↑ Up	↑ Up	↑ Up
			3 items