

Higher Quality
Better Service!

EXAM SELL

Certified IT practice exam authority

Accurate study guides, High passing rate!

Exam Sell provides update free of charge in
one year!



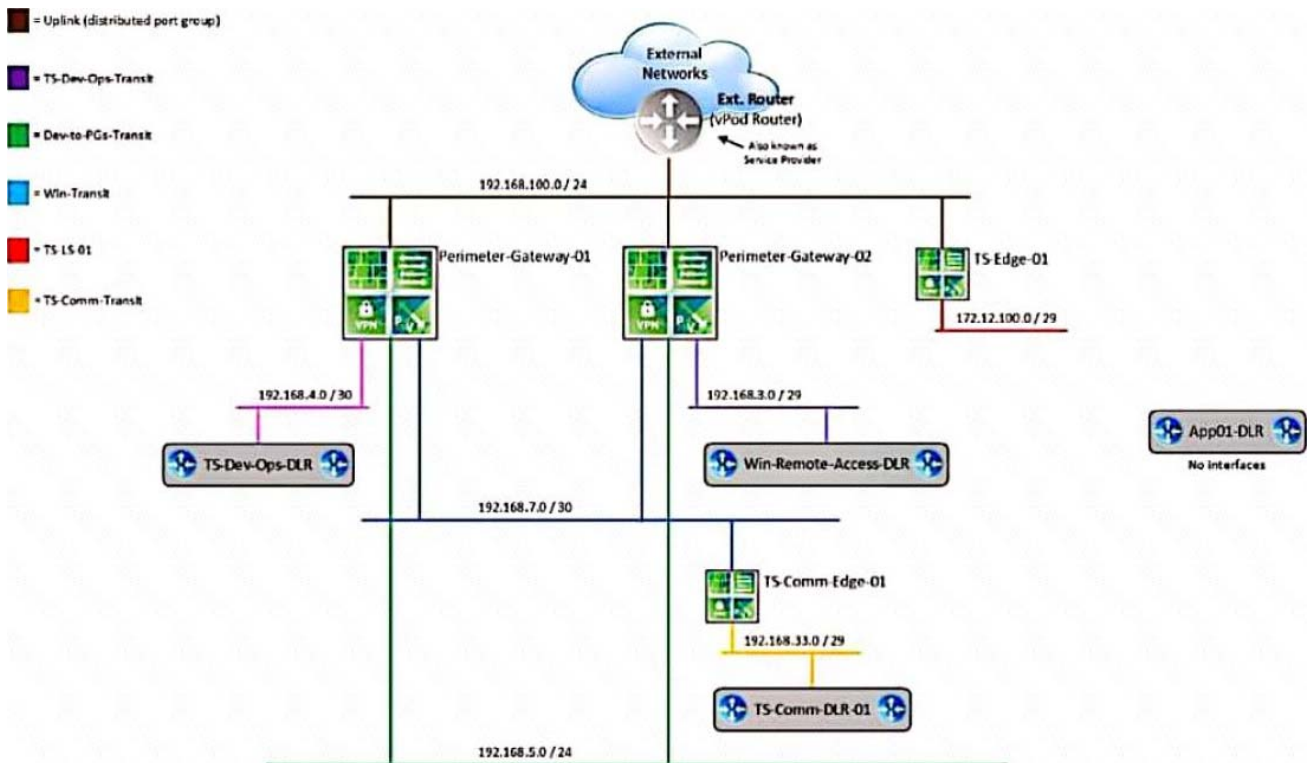
<http://www.examsell.com>

Exam : 3V0-643

Title : VMware Certified Advanced
Professional 6 - Network
Virtualization Deployment
Exam

Version : DEMO

1. Topic 1, Main Questions



Questions HOL LAB Modules and Pages for practice

1

<http://docs.hol.vmware.com/hol-isim/HOL-2019/hol-1903-01-nsxinstall-p1.htm>

HOL-1903-01 Page 16 or you can directly Open a NSX manager in the lab and edit the existing settings

bOpen PSC and NSX manager in HOL-1903-01 and look for NTP Server

load nation

cExport existing vDS config and Import back the config for practice in

HOL-1903-01

dNo Lab Module available

2

<http://docs.hol.vmware.com/hol-isim/HOL-2019/hol-1903-01-nsxinstall-p2.htm>

and LAB - HOL 1903-01 Page 26-36

3LAB - HOL 1903-01 Module 2 - Page 37-38

4LAB - HOL 1903-01 Module 4 – Practice and understand whole module Bridging and other questions 7, 8, 9 and LAB - HOL-1925-02 Module 1

5LAB - HOL 1903-01 Module 4 - shows how to deploy NSX Edge, you can also deploy Distributed logical router DLR in the same way the lab.

6LAB - HOL 1903-01 Module 3 – Practice and understand the whole module, it will be use full for other question like 20 and 22

7LAB - HOL 1903-01 Module 4 – Practice and understand whole module Bridging and other questions 7, 8, 9

8LAB - HOL 1903-01 Module 4 – Practice and understand whole module Bridging and other questions 7, 8, 9

9LAB - HOL 1903-01 Module 4 – Practice and understand whole module Bridging and other questions 7,

8, 9

10LAB - HOL-1903-02 Module 1 and 2

11LAB - HOL-1903-02 Module 1 and 2

12LAB - HOL-1903-02 directly follow the steps in this document for practice

13LAB - HOL 1903-01 - open an NSX manager in LAB and directly follow the steps in this document.

14LAB - HOL 1903-01 - open postman in the lab and directly follow the steps in this document.

15LAB - HOL 1903-01 - directly follow the steps in this document for practice.

16LAB - HOL 1903-01 - directly follow the steps in this document for practice.

17LAB - HOL-1925-02 Module 1

18LAB - HOL-1925-02 Module 1

19 LAB - HOL-1925-02 - directly follow the steps in this document for practice.

20LAB - HOL 1903-01 Module 3 – Practice and understand the whole module.

21No Lab Module available

22LAB - HOL 1903-01 Module 3 – Practice and understand the whole module.

23LAB - HOL 1903-01 - open postman in the lab and directly follow the steps in this document.

(Exam Topic 1)

Two administrators (John and Chris) share admin responsibilities for an NSX deployment that is leveraging Centralized CLI as part of their management. Security requirements prohibit use of shared admin accounts in Site A.

Requirements:

NSX Manager: nsxmgr-01a.crop.local

New administrator accounts: "John" and "Chris"

Default password: VMware1!

Create accounts for John and Chris.

Use one of the newly created accounts to display all clusters enabled for the distributed firewall.

Use Putty's "Copy All to Clipboard" feature to paste the command and output to a text file dfw-NEW.txt on the ControlCenter desktop.

NOTE:

Screenshot is shown on how to use Putty's Copy all to Clipboard feature.

HOL LAB for Practice:

See the explanation part for complete solution.

Answer:

SOLUTION:

13:(1) select vccenter - a. select datacenter A and click right mouse button select administrator. select user and groups click on + sign. select user tab enter user name john password VMware1!. click ok . do same for chris.

(2) select datacenter A. select manage tab. select permission. click + Sign. select Read Only from Assign Role. select All Privileges click on Add. select John and chris.checked Propagate to children and click on OK.

(3) go NsX Manager. select Nsx Manage-a. select manage select user from tab. click + sign. select identity user. check specify vcenter user. enter user name john@vsphere.local click next. select role Nsx Administrator. click finish. do same for chris. but use chris@vsphere.local and assign role of Nsx administrator click finish.

6 of 336

Enable

VMware1!

Conf t

User john password plaintext VMware1!

User chris password plaintext VMWare1!

Exit

Write memory

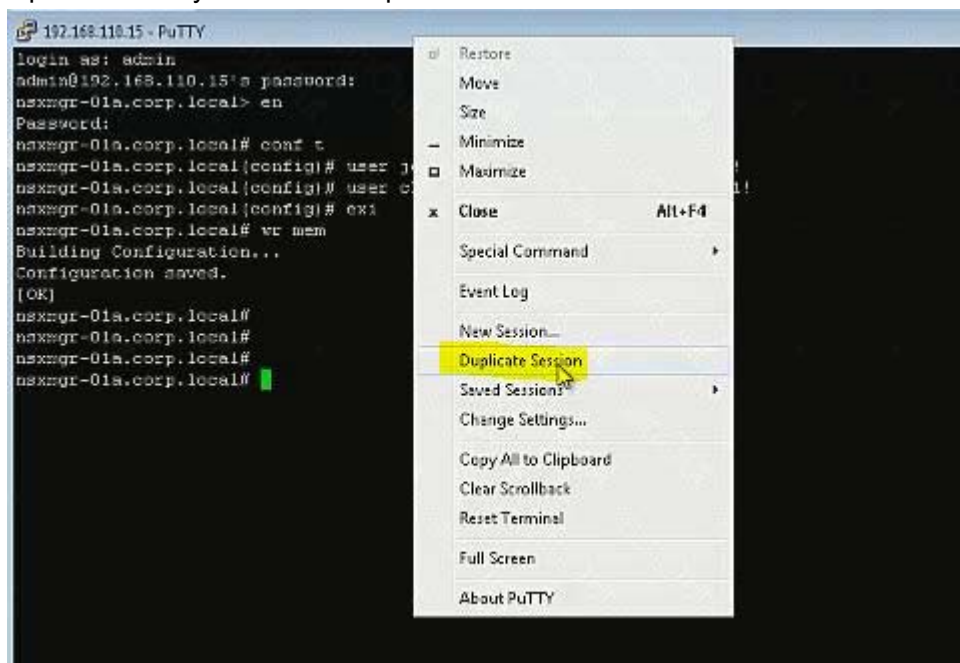


```

192.168.110.15 - PuTTY
login as: admin
admin@192.168.110.15's password:
nsxmgr-01a.corp.local> en
Password:
nsxmgr-01a.corp.local# conf t
nsxmgr-01a.corp.local(config)# user john password plaintext VMware1!
nsxmgr-01a.corp.local(config)# user chris password plaintext VMWare1!
nsxmgr-01a.corp.local(config)# exi
nsxmgr-01a.corp.local# wr mem
Building Configuration...
Configuration saved.
[OK]
nsxmgr-01a.corp.local#
nsxmgr-01a.corp.local#
nsxmgr-01a.corp.local#
nsxmgr-01a.corp.local#

```

Open new Putty session or Duplicate Session:

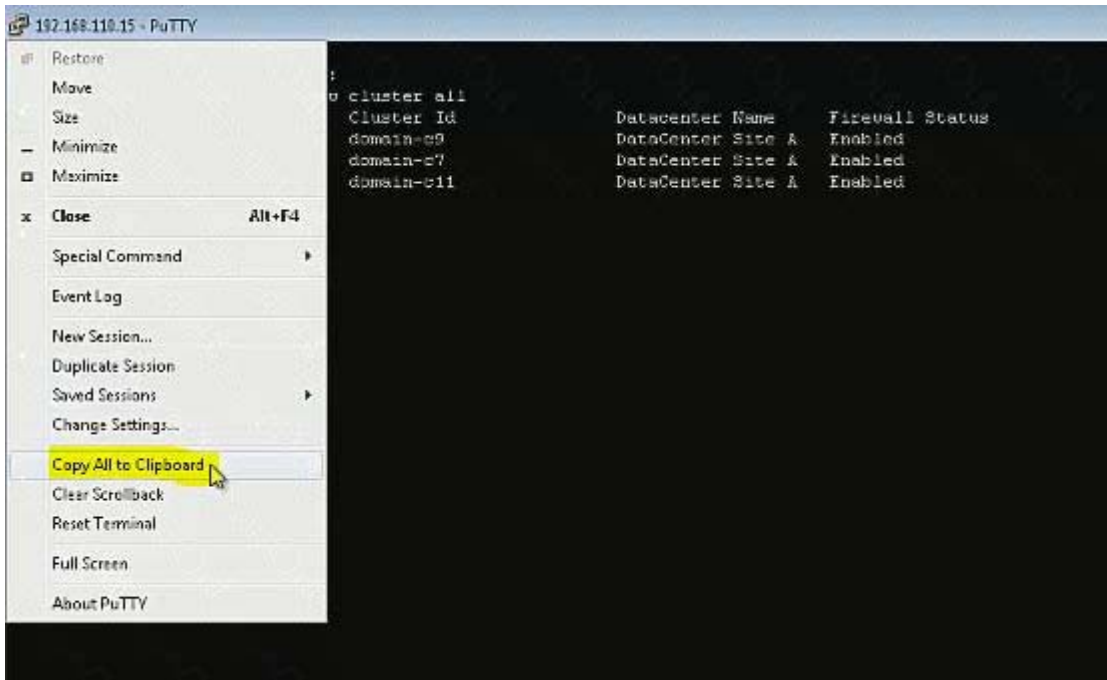


john

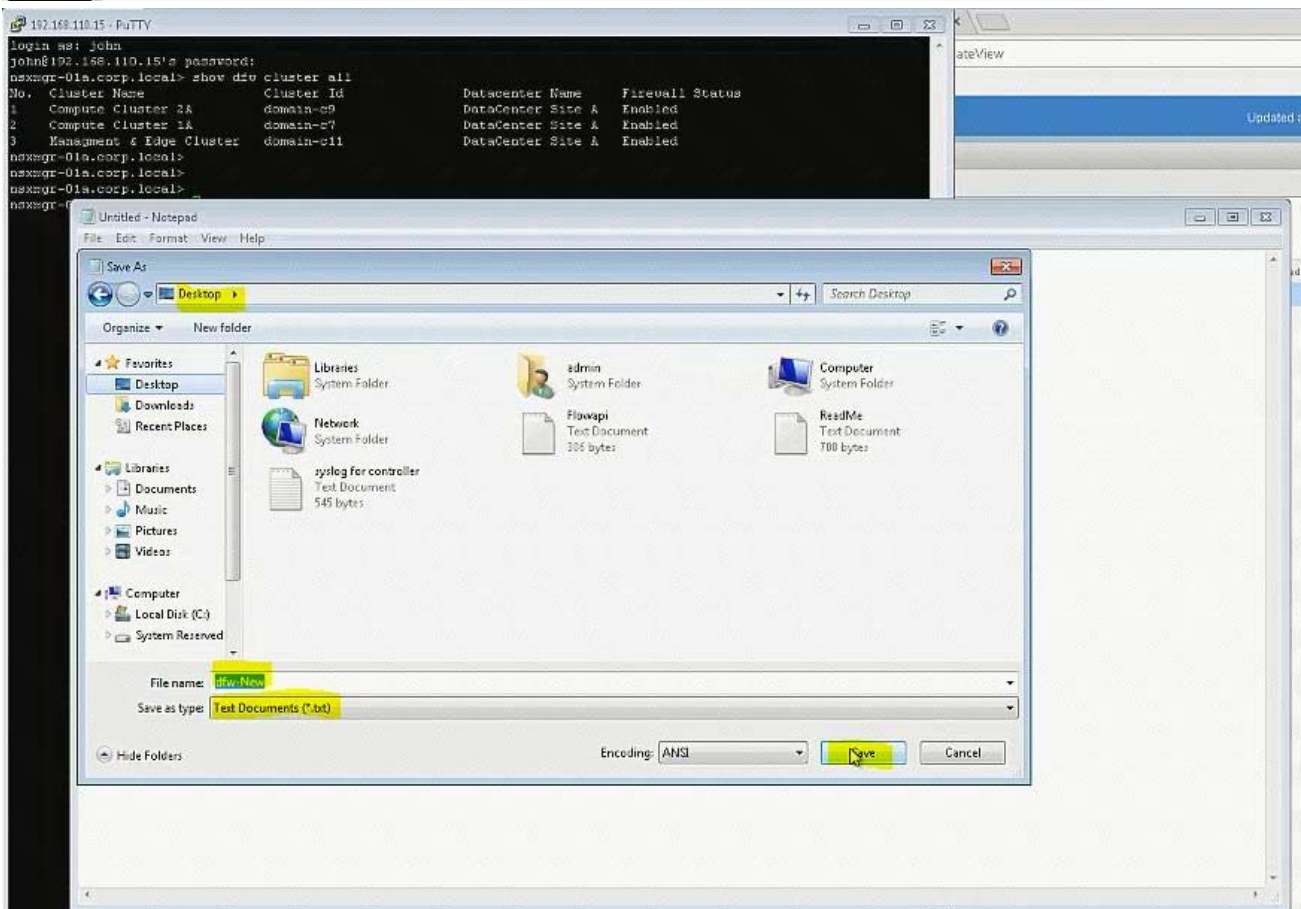
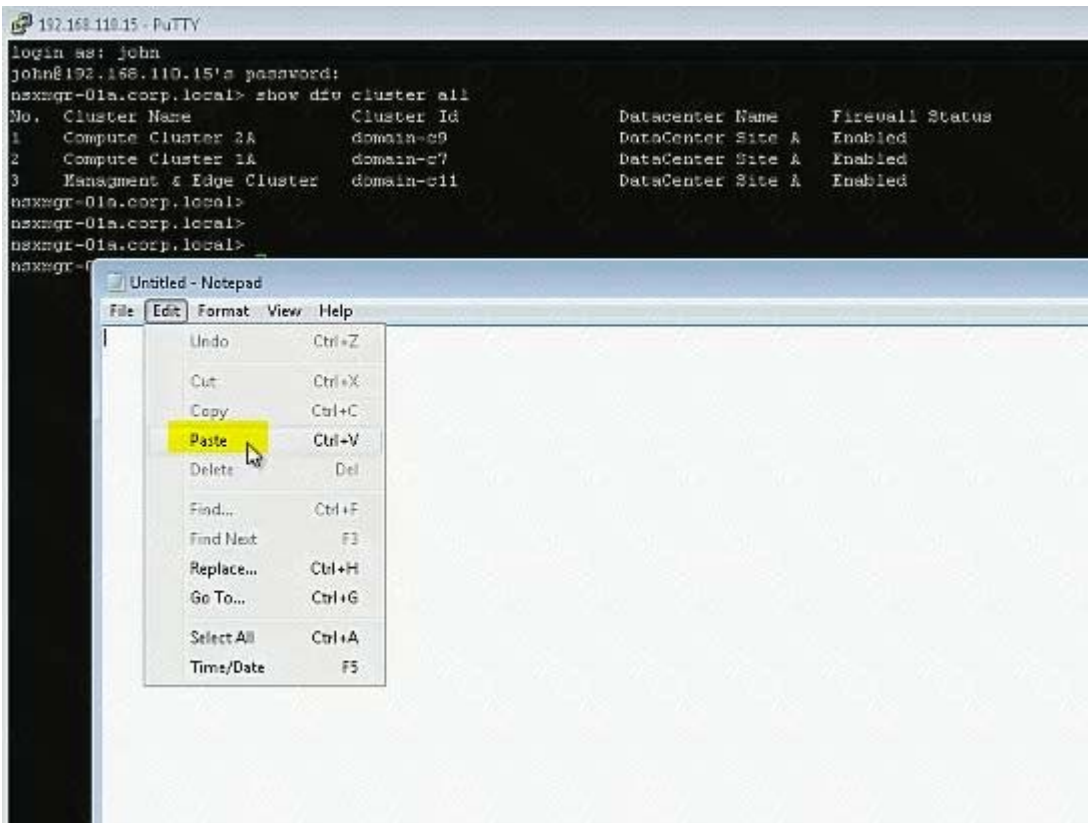
VMware1!

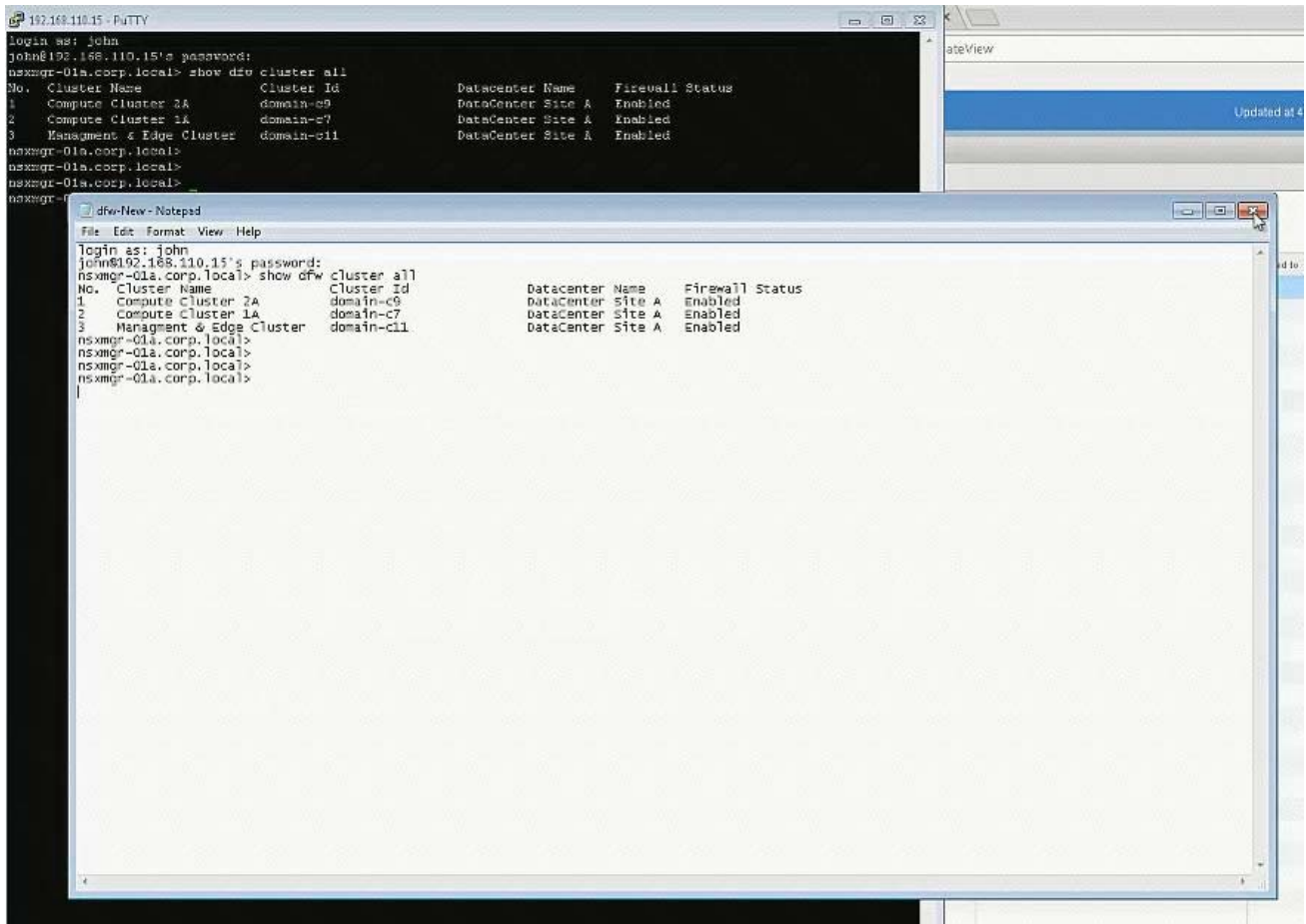
Show dfw cluster all

```
192.168.110.15 - PuTTY
login as: john
john@192.168.110.15's password:
nsxmgr-01a.corp.local> show dfc cluster all
No. Cluster Name Cluster Id Datacenter Name Firewall Status
1 Compute Cluster 2A domain-c9 DataCenter Site A Enabled
2 Compute Cluster 1A domain-c7 DataCenter Site A Enabled
3 Management & Edge Cluster domain-c11 DataCenter Site A Enabled
nsxmgr-01a.corp.local>
nsxmgr-01a.corp.local>
nsxmgr-01a.corp.local>
nsxmgr-01a.corp.local>
```



Ctrl+V don't work in exam.





2. (Exam Topic 1)

Management has approved an expansion of the virtual infrastructure. You have been tasked to prepare Cross vCenter configuration with the second vCenter Server. Another administrator has provided a pre-configured vDS configuration file located on the Control Center Server. All identifiers must be maintained.

Requirements:

vCenterB server: vcsa-01b.corp.local

Credentials: administrator@vsphere.local / VMware1!

vCenterB VAMI Credentials: root / VMware1!

Cluster: Computer Cluster 1B

ESXI Hosts: esx-01b.corp.local, esx-02.corp.local

Platform service controller: psc-01a.corp.local(192.168.110.9)

NSX Manager: nsmgr-01b.corp.local (192.168.210.15)

Credentials: admin / VMware1!

Time Zone: US/Pacific

*Configure nsmgr-01b.corp.local for vCenterB and psc-01a.corp.local

*Ensure nsxmgr-01b.corp.local uses the same NTP server as psc-01a.corp.local with a US/Pacific TimeZone.

*Import the new vDS configuration vds-site-b-Compute-New.zip

All identifiers must be maintained.

*Assign the remaining two used vmnics for the ESXi hosts to the newly imported vDS.

NOTE:

Do not migrate VMkernels from the standard switches on the hosts.

HOL LAB for Practice:

a <http://docs.hol.vmware.com/hol-isim/HOL-2019/hol-1903-01-nsxinstall-p1.htm>

HOL-1903-01 Page 16 or you can directly Open a NSX manager in the lab and edit the existing settings

bOpen PSC and NSX manager in HOL-1903-01 and look for NTP Server load cation

cExport existing vDS config and Import back the config for practice in HOL-1903-01

dNo Lab Module available

See the explanation part for complete solution.

Answer:

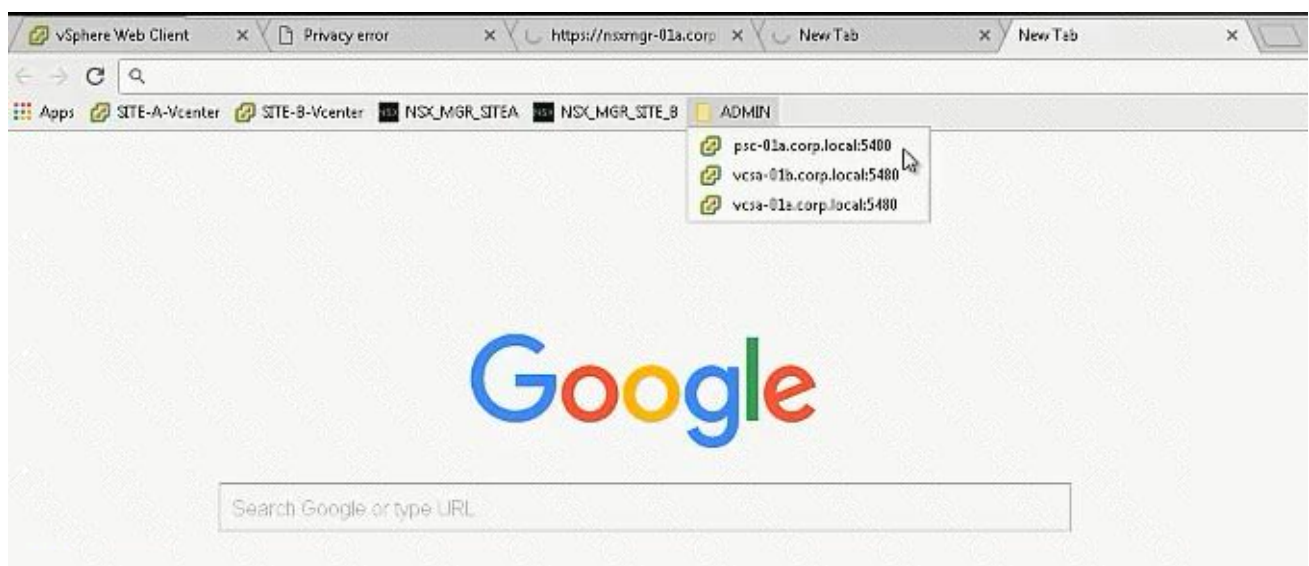
SOLUTION:

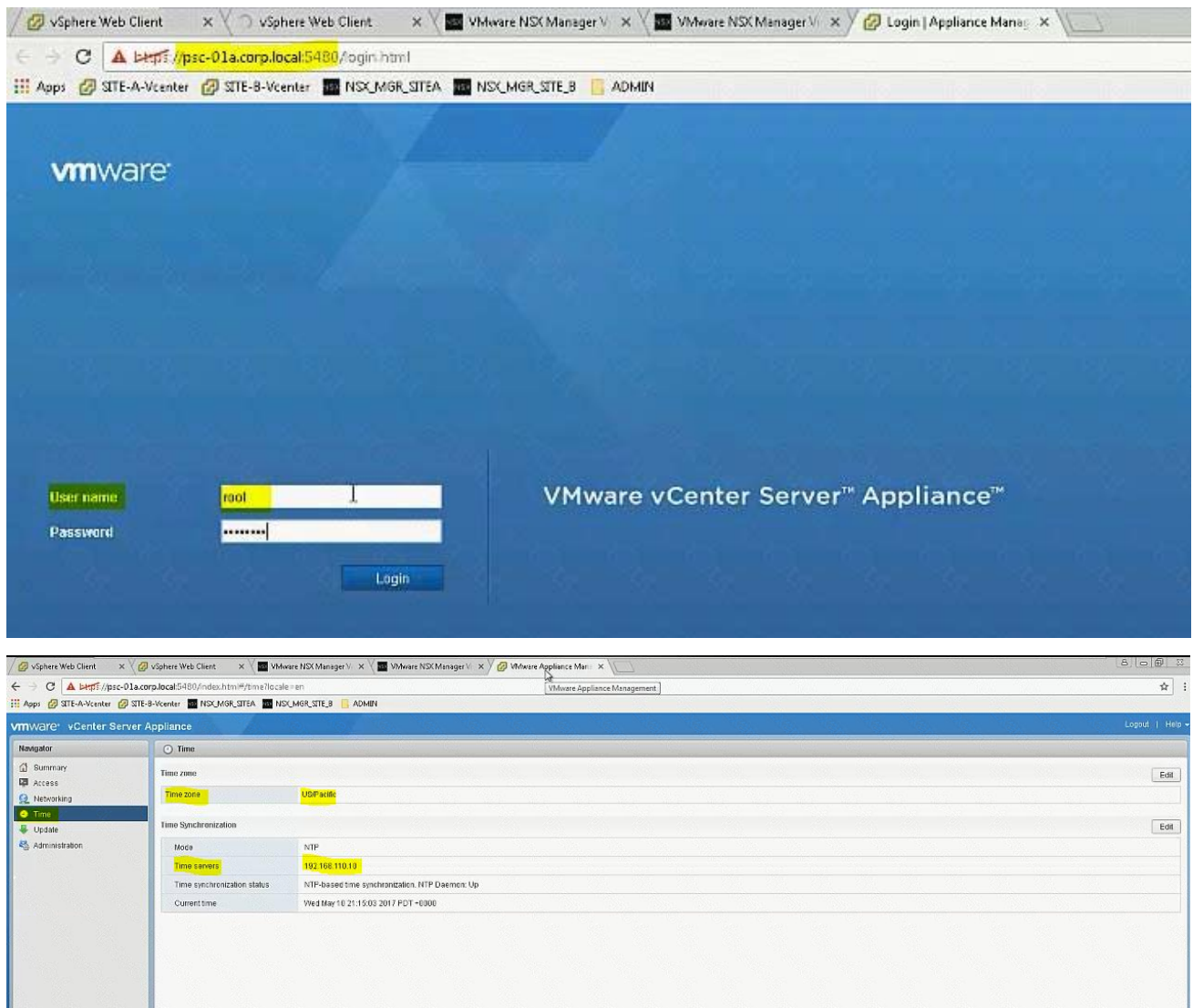
Step 1: Login to PSC using VAMI credentials and note down the time zone and server details and use the same in SiteB NSX Manager time settings.

Step 2: Update the time settings, complete lookup service configuration, associate SiteB NSX manager to SiteB vCenter. Check the status from SiteA vCenter Webclient -> Networking & Security -> Installation -> Management.

Step 3: Import the Distributed switch to Cluster B, add the hosts & assign the interfaces.

Login to <https://psc-01a.corp.local:5480/> to check the NTP server details and note it down. Use the VAMI credentials given to login. Need to click on Edit to see the server details in here as it is not showing up in the main page (In exam, it is showing in the main page itself).

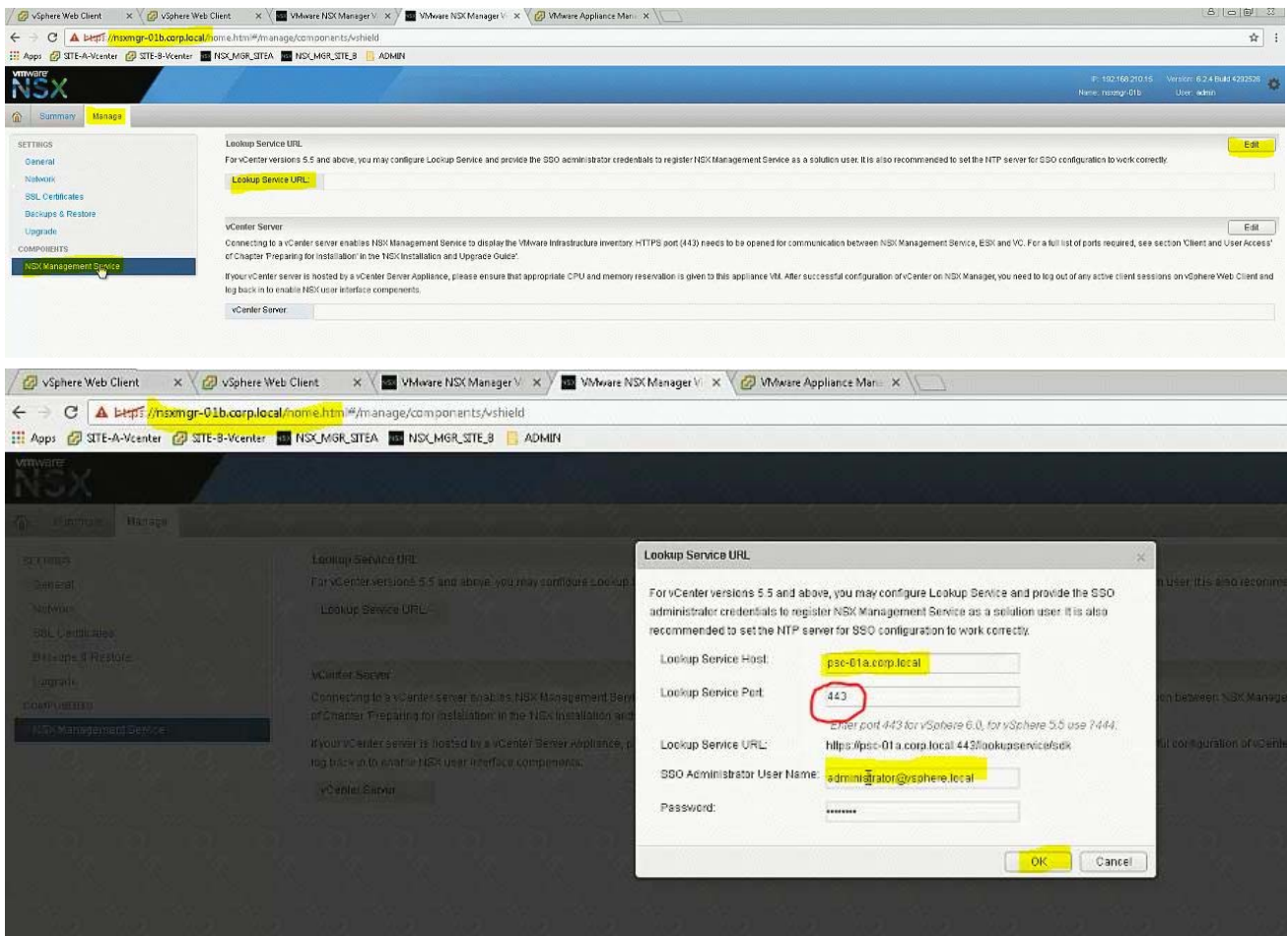




The first screenshot shows the VMware NSX Manager Virtual Appliance login screen. The browser address bar displays `https://nsxmgr-01b.corp.local/login.jsp?sessionId=F4FBF0172A022A3051F91F874D6D4915`. The login form has 'User name: admin' and 'Password: *****'. The 'Login' button is visible.

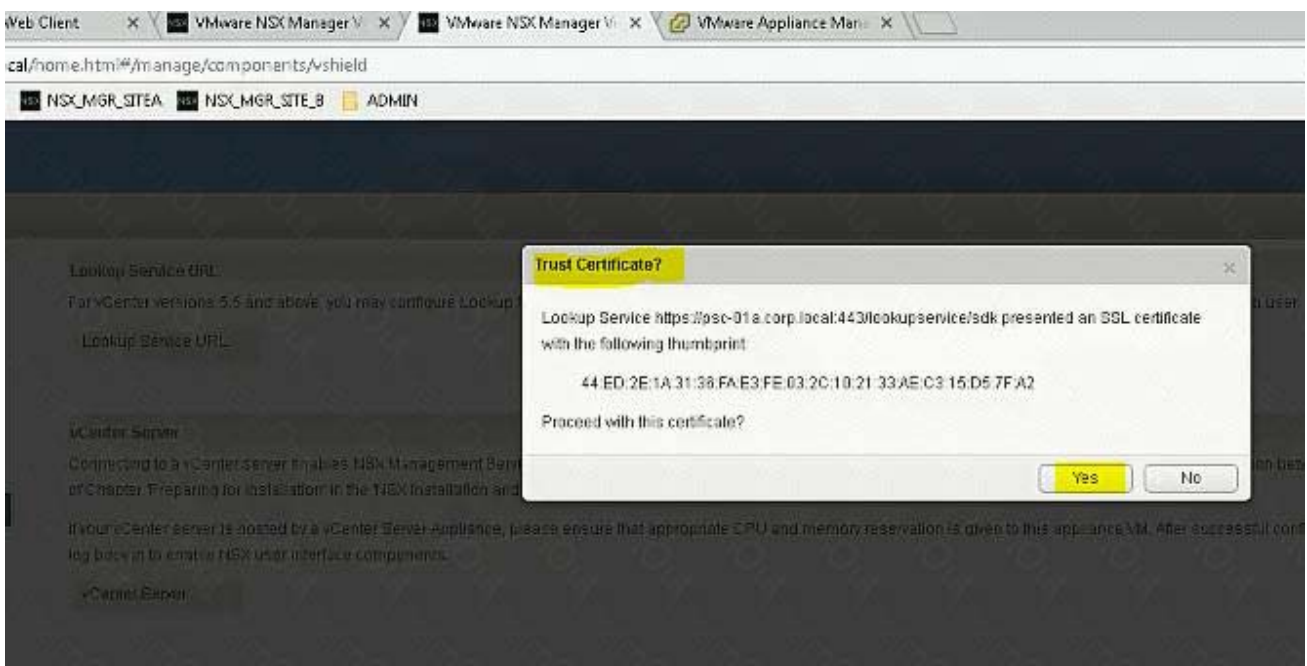
The second screenshot shows the 'Time Settings' dialog box. It prompts the user to 'Specify NTP server below. For SSO configuration to work correctly it is required that the time on this virtual appliance and NTP server should be in sync. It is recommended to use the same NTP server used by the SSO server.' The 'NTP Server' is set to '192.168.110.10', 'Timezone' is 'US Pacific', and 'Date/Time' is 'MM/DD/YYYY HH:MM:SS'.

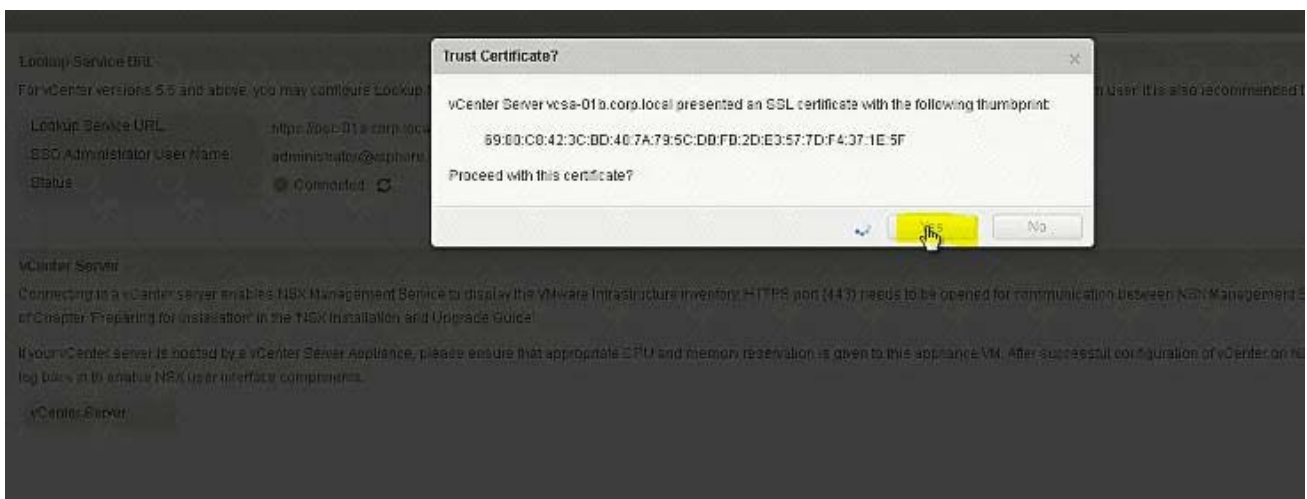
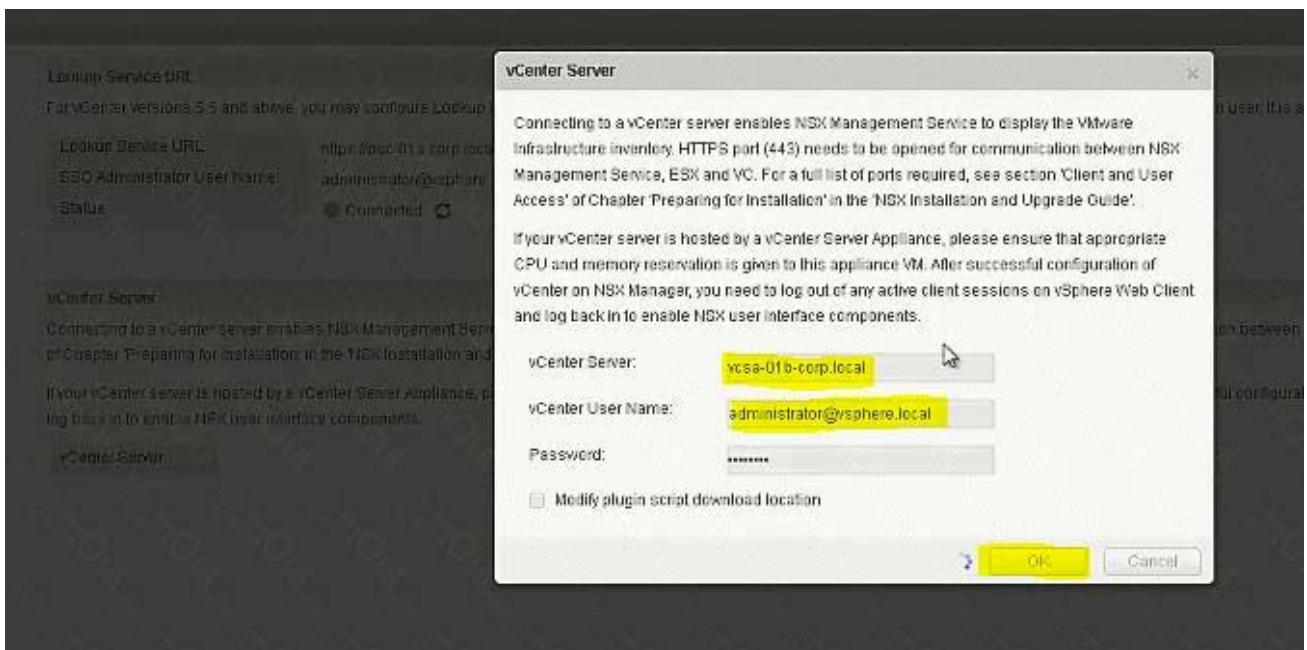
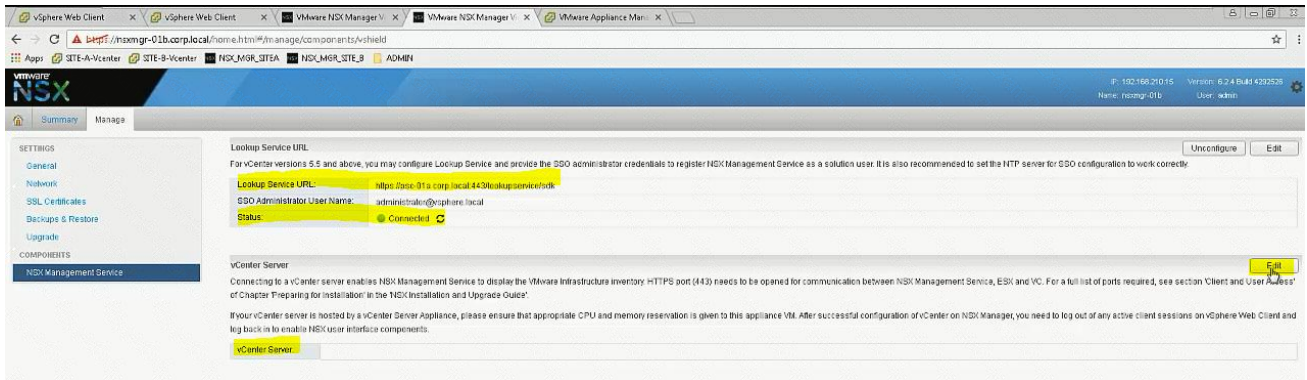
The third screenshot shows the 'Settings' page in the VMware NSX Manager. A message at the top states: 'NTP server settings has been changed. NSX Management Service needs to be restarted for NTP server settings to take effect.' The 'Time Settings' section shows 'NTP Server' as '192.168.110.10', 'Timezone' as 'US Pacific', and 'Date/Time' as '05/10/2017 21:19:57'. The 'Syslog Server' section is also visible.



Important NOTE:

In exam change Lookup Service Port according to NSX Manager of Site A which is working one. It's 7444 in exam.

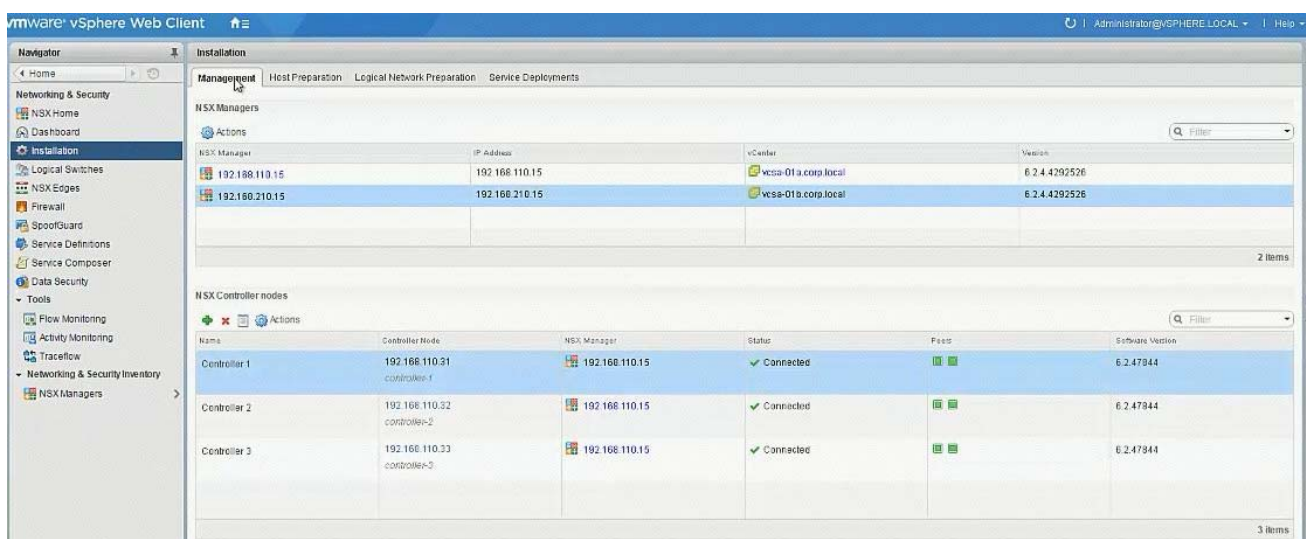
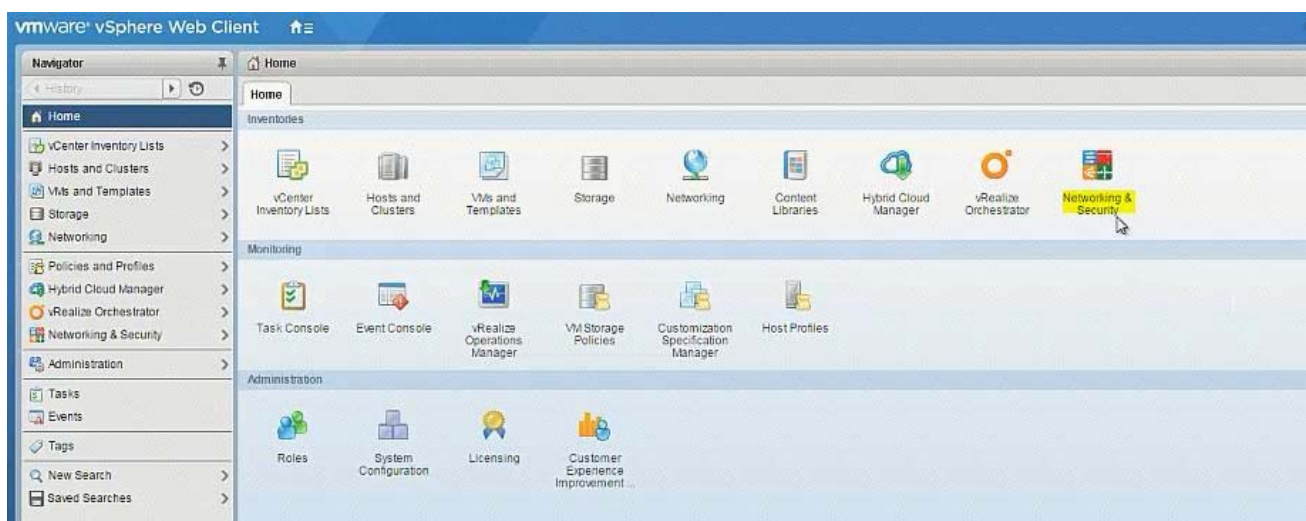


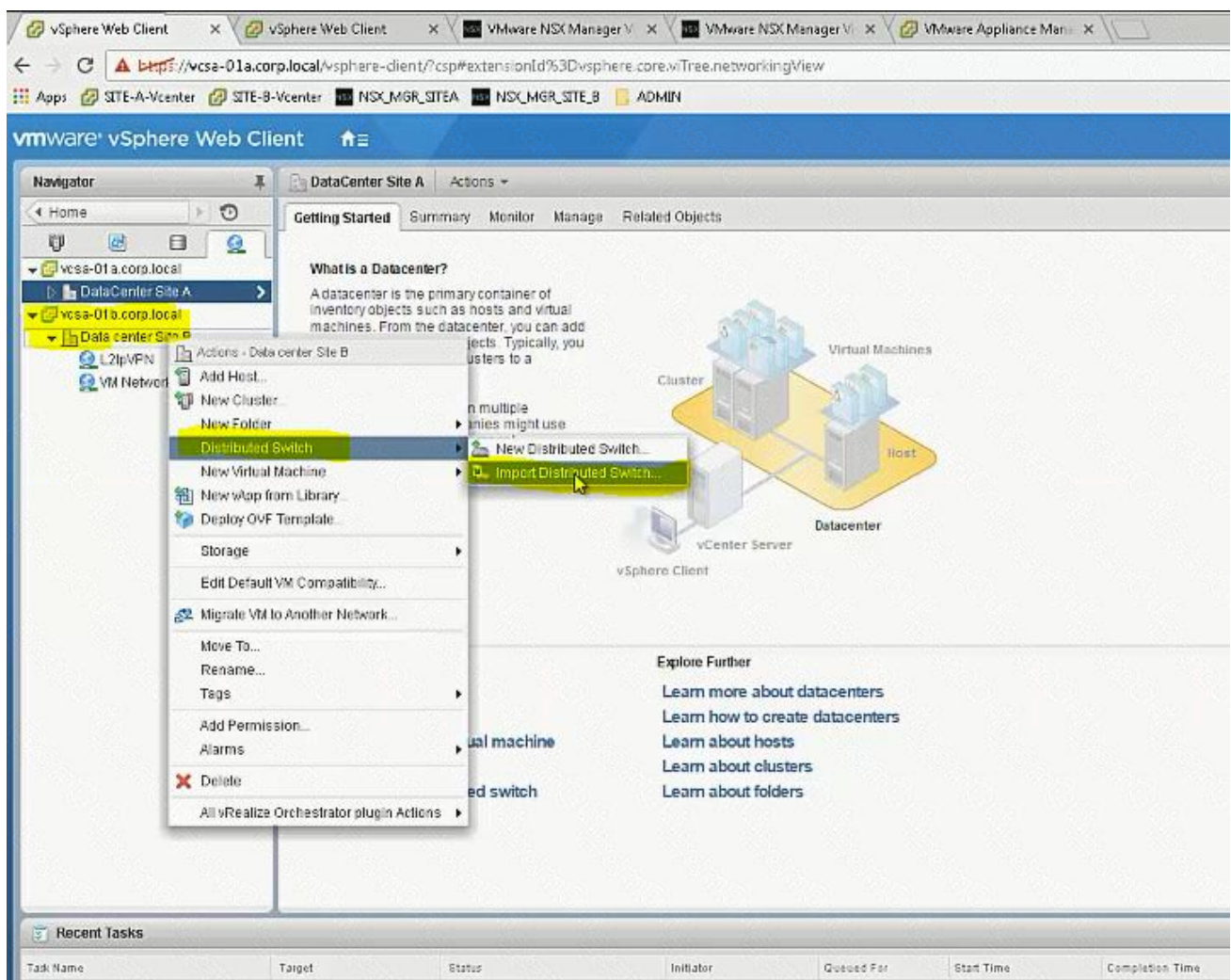
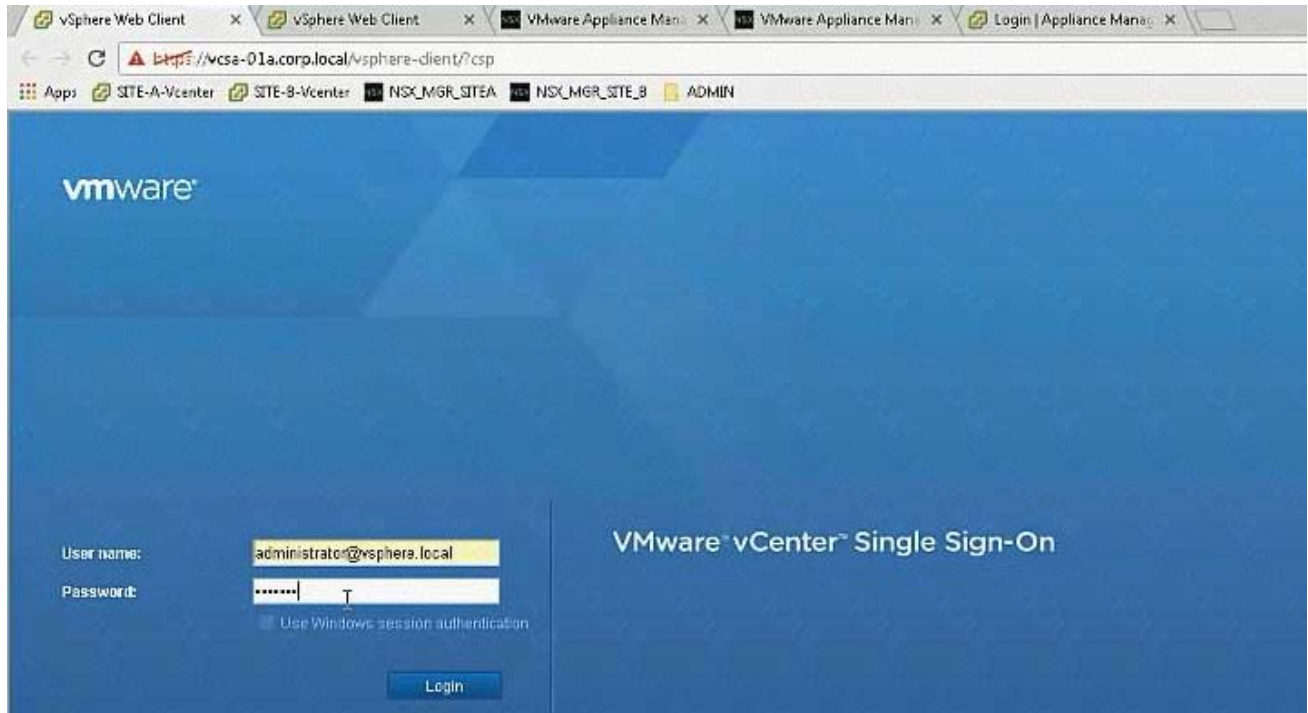


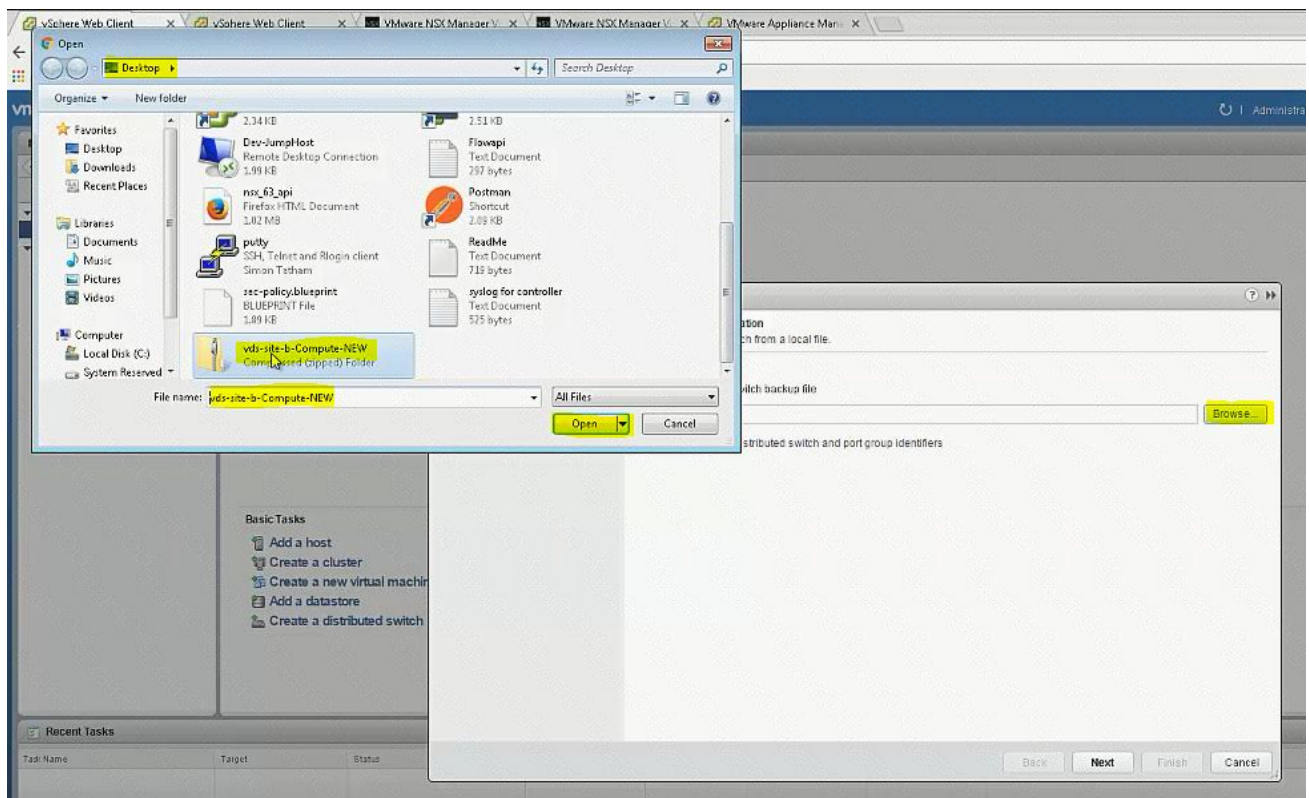
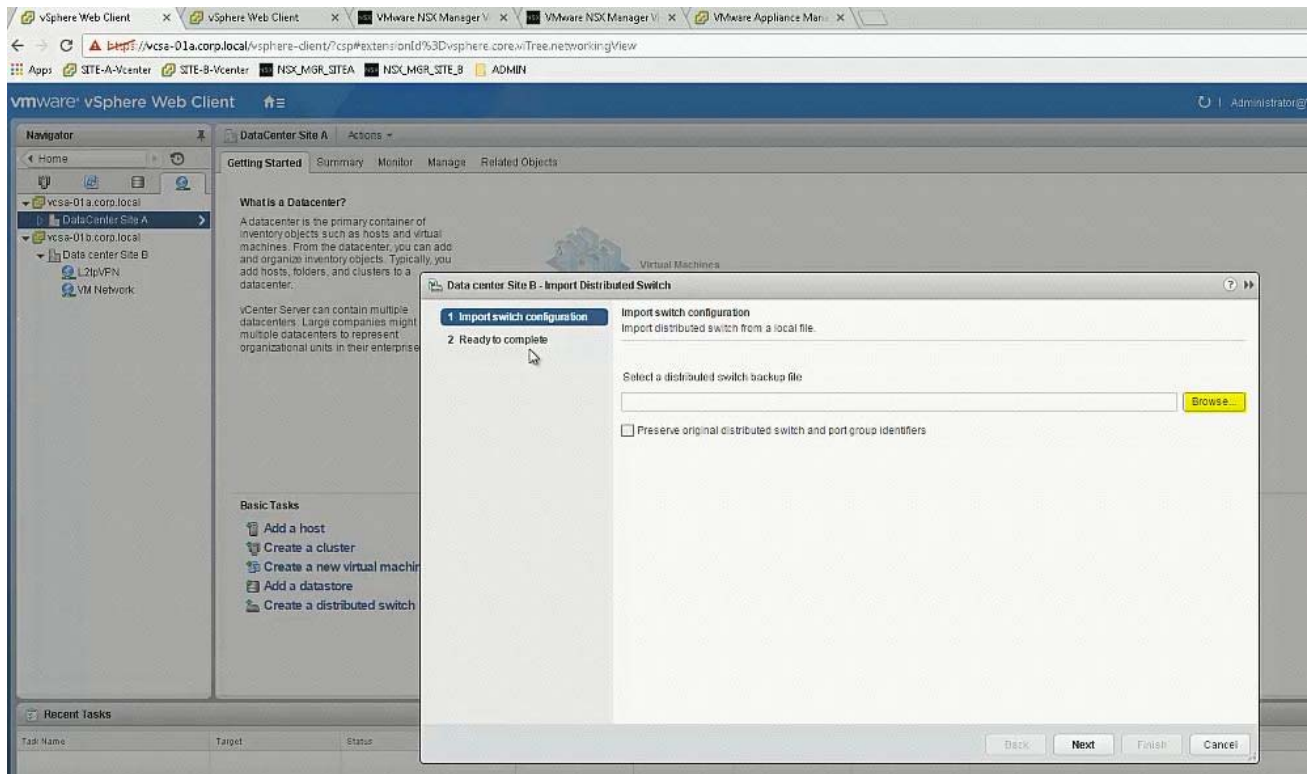


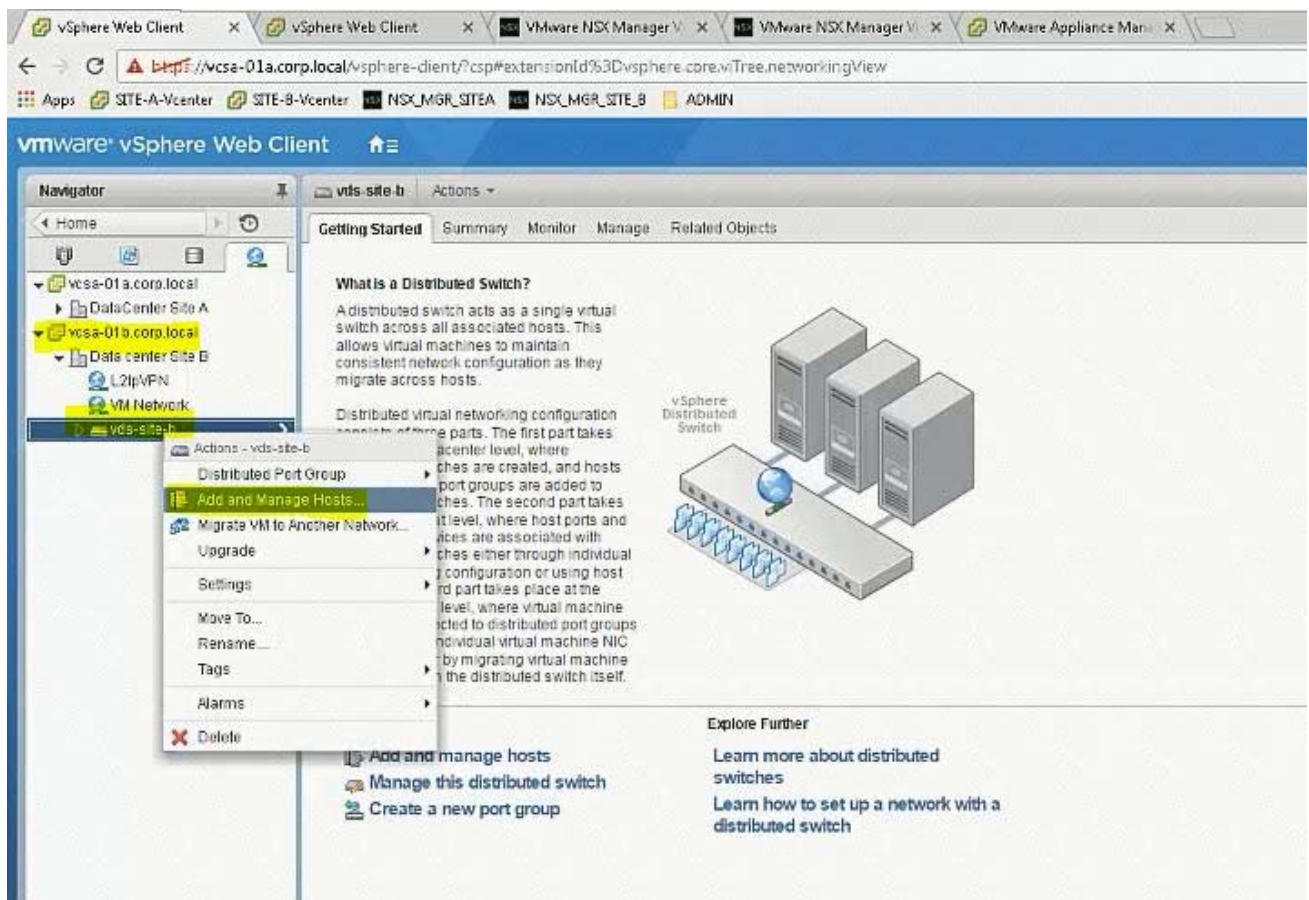
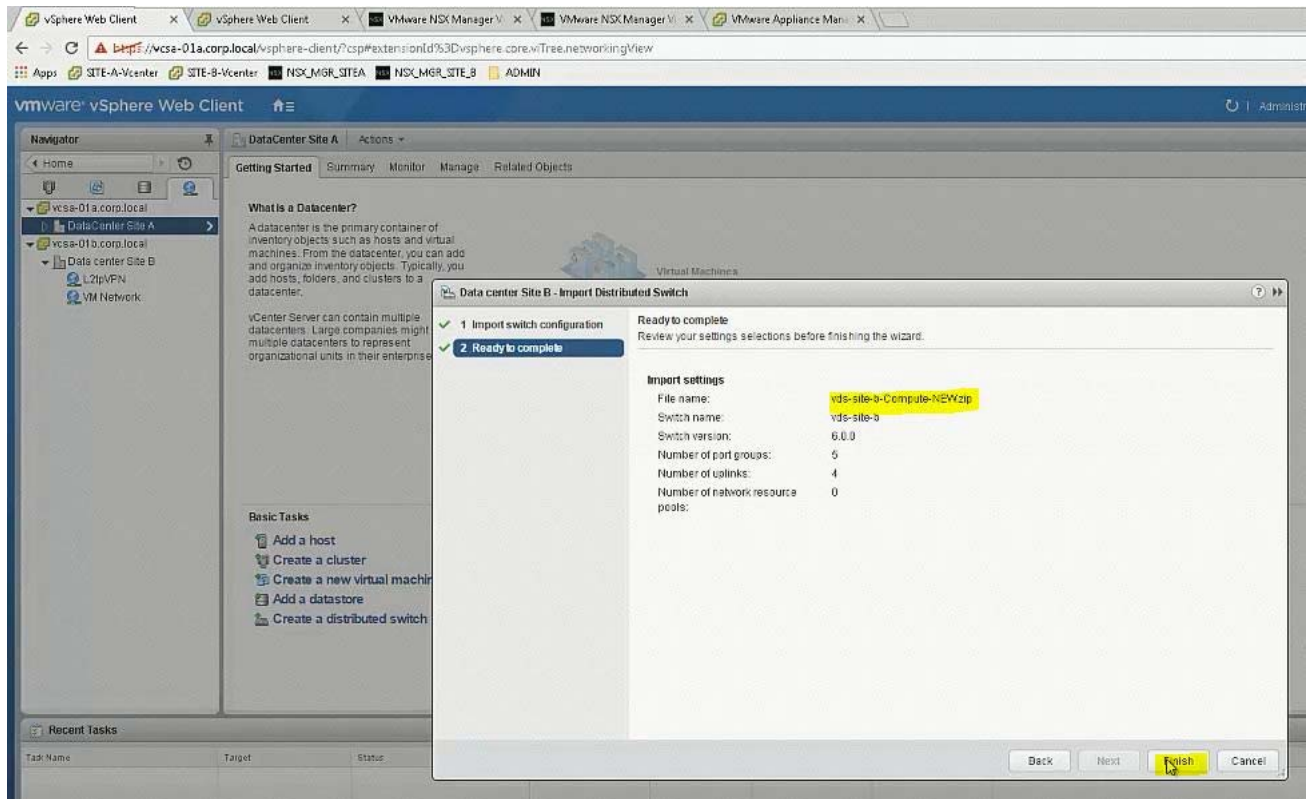
Click refresh if in case it shows as disconnected.

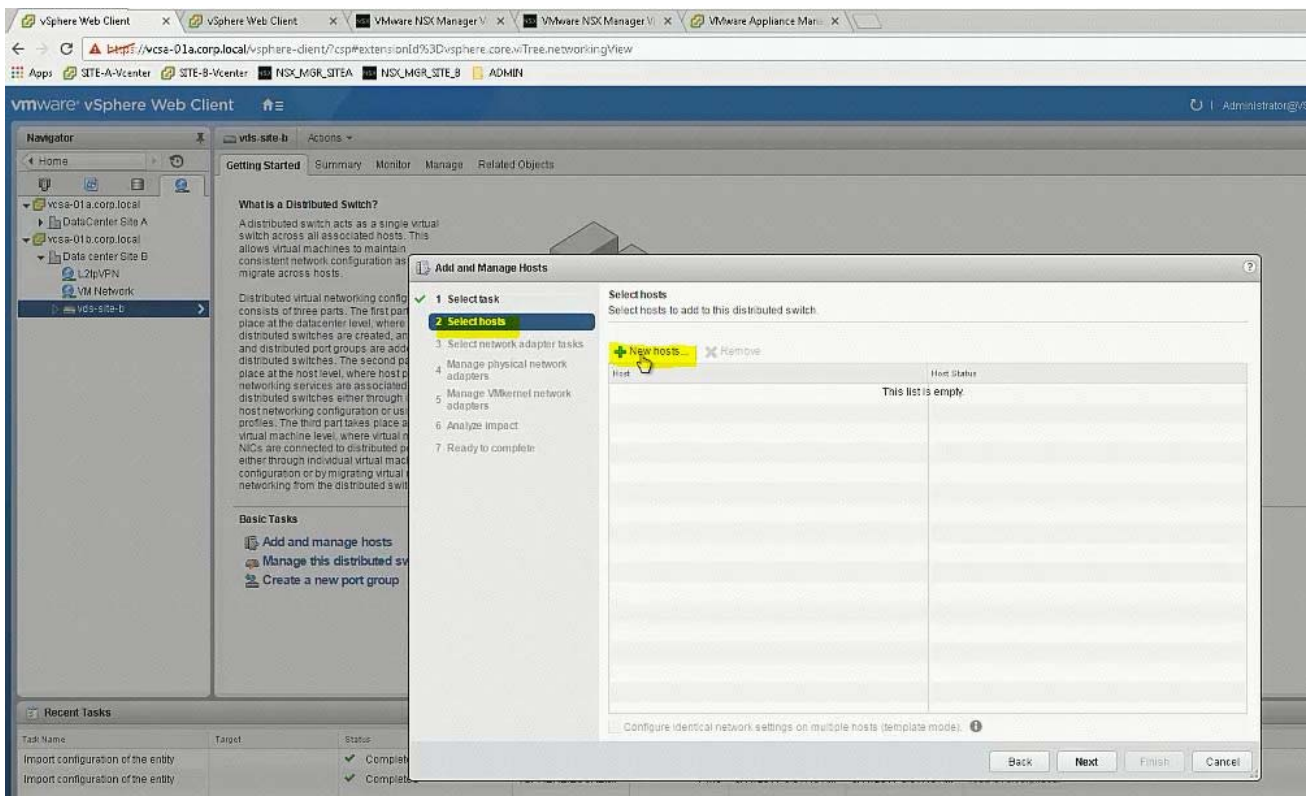
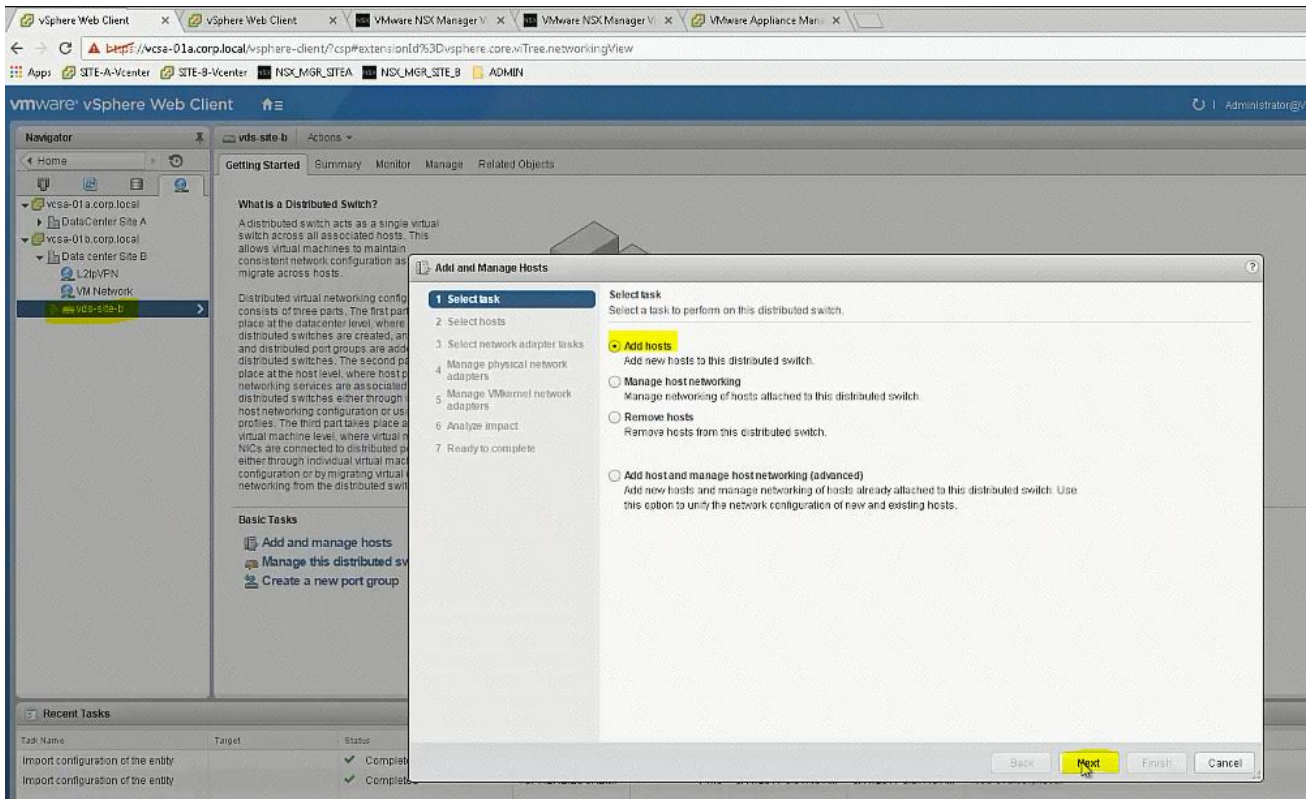
Login to SiteA vCenter using Web Client and confirm the status of both the NSX Managers: Installation -> Management.

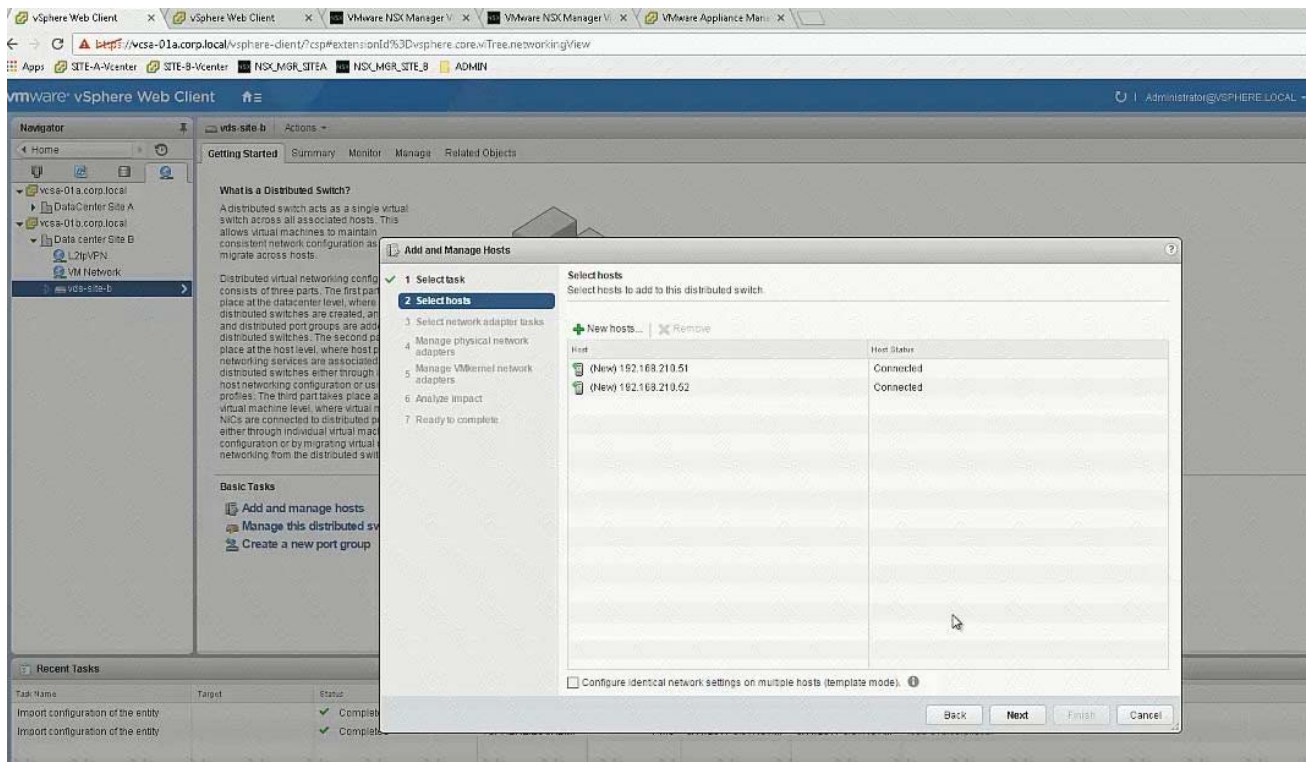
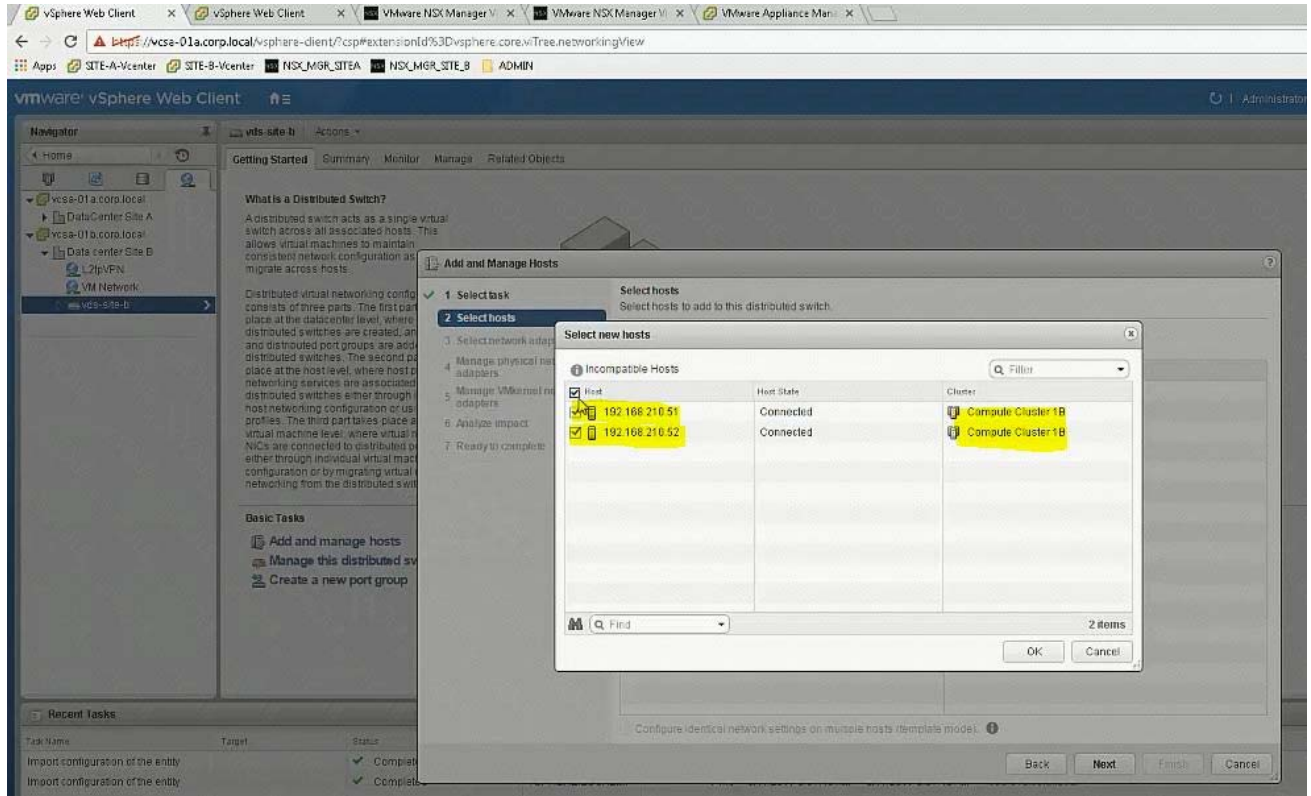


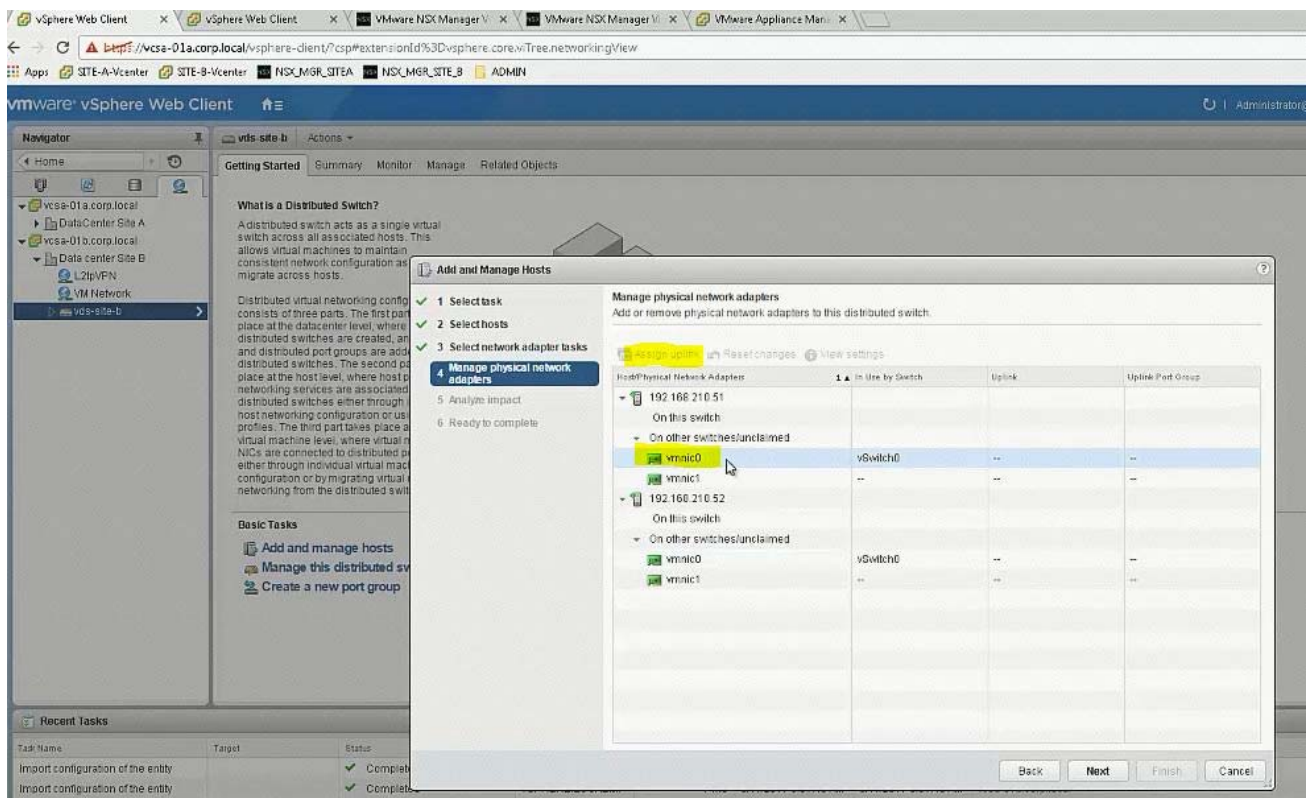
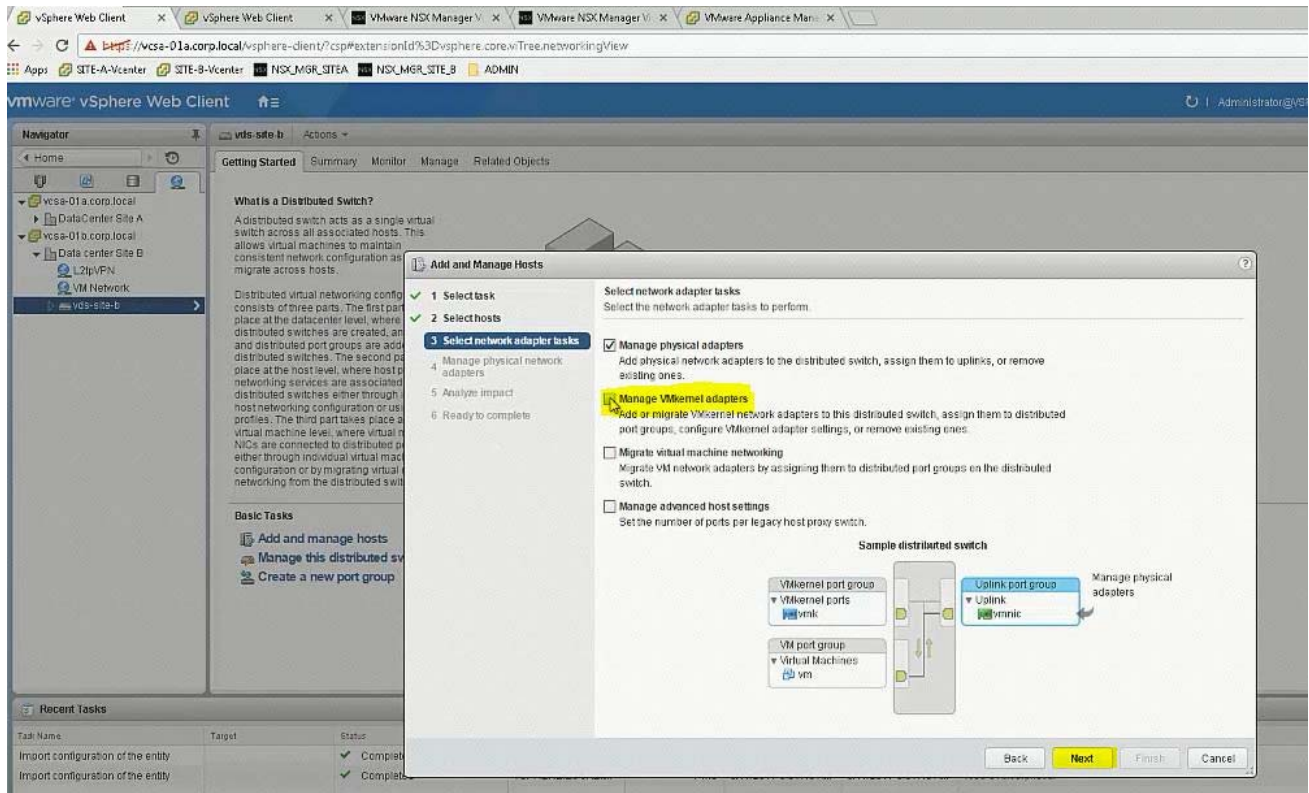


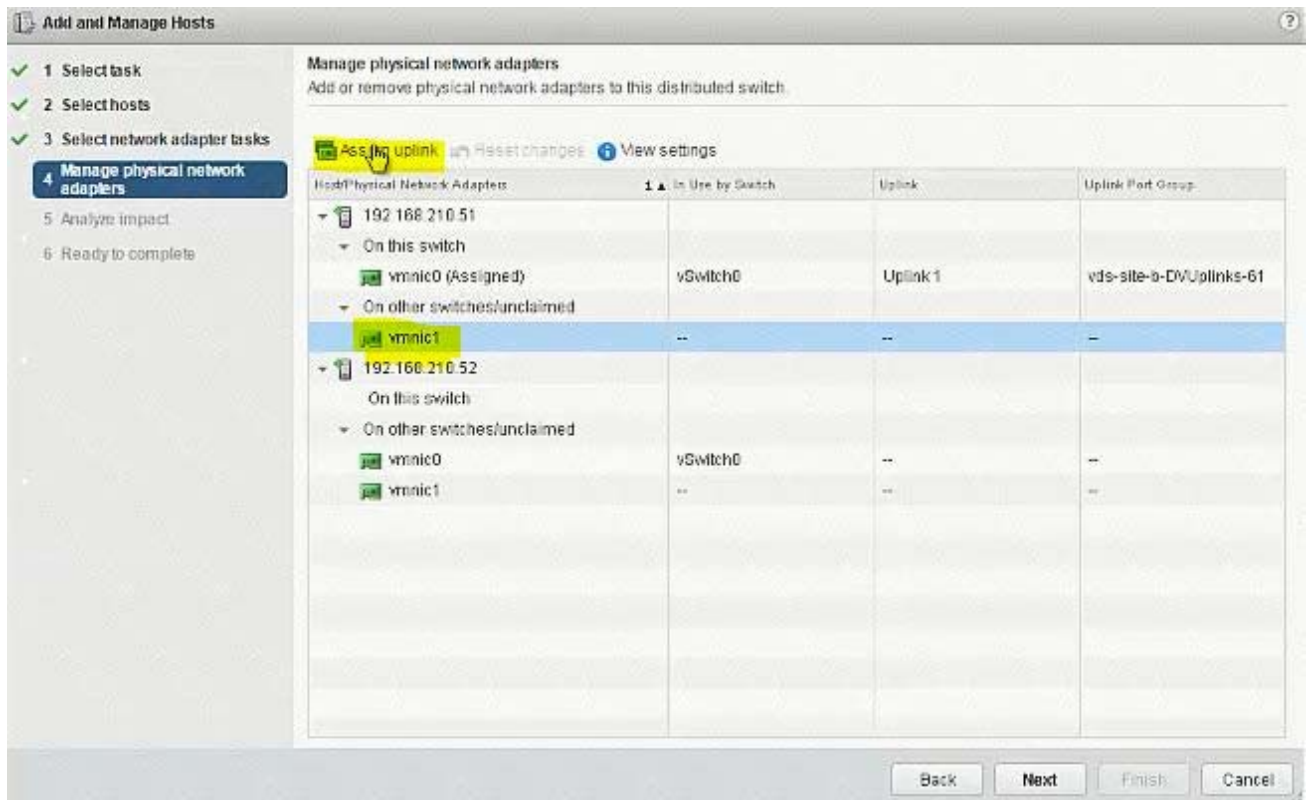
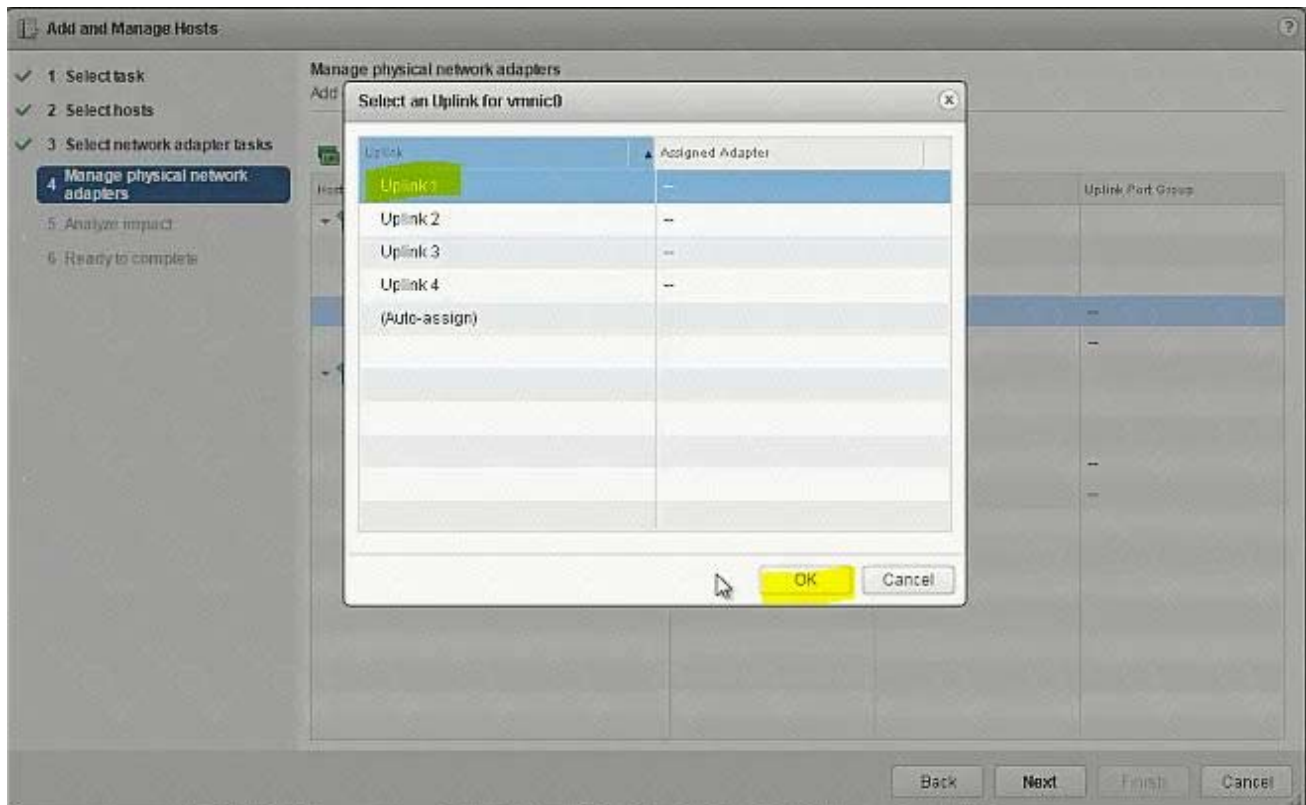


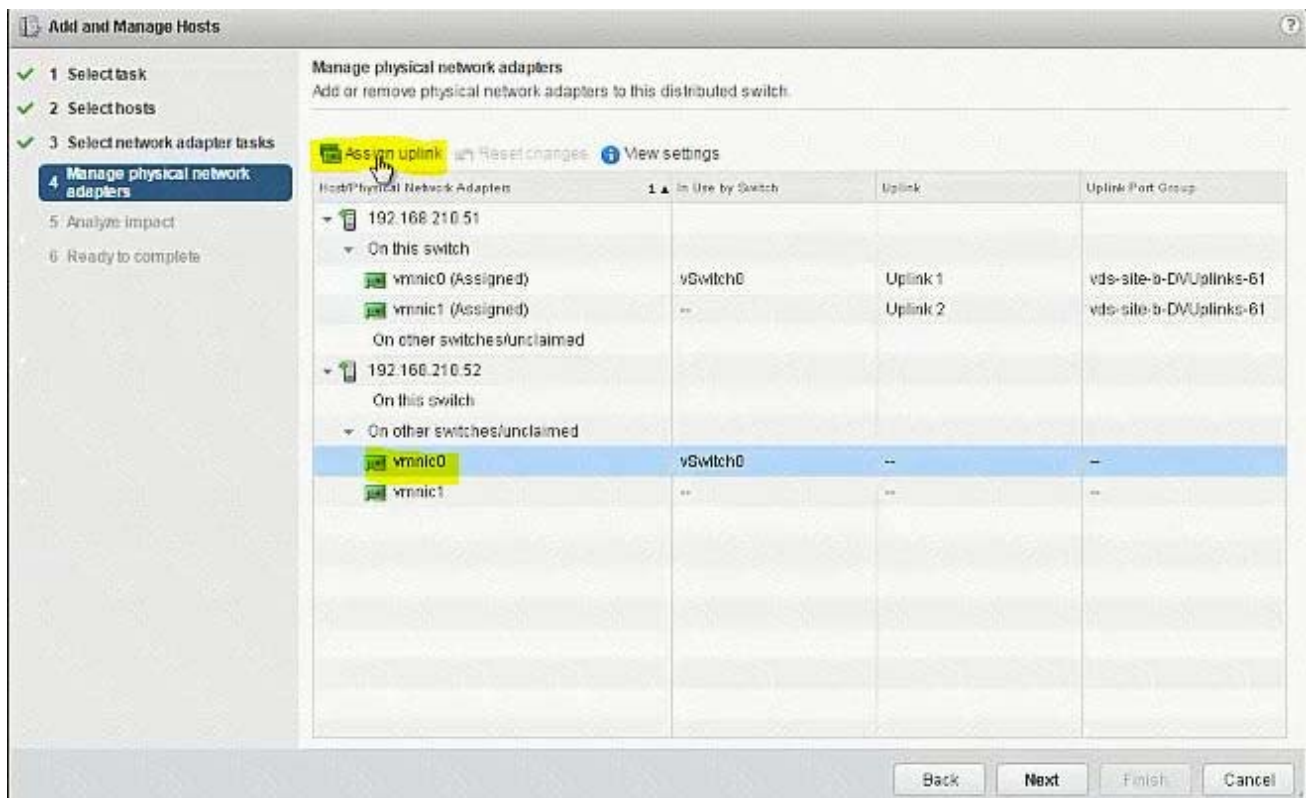
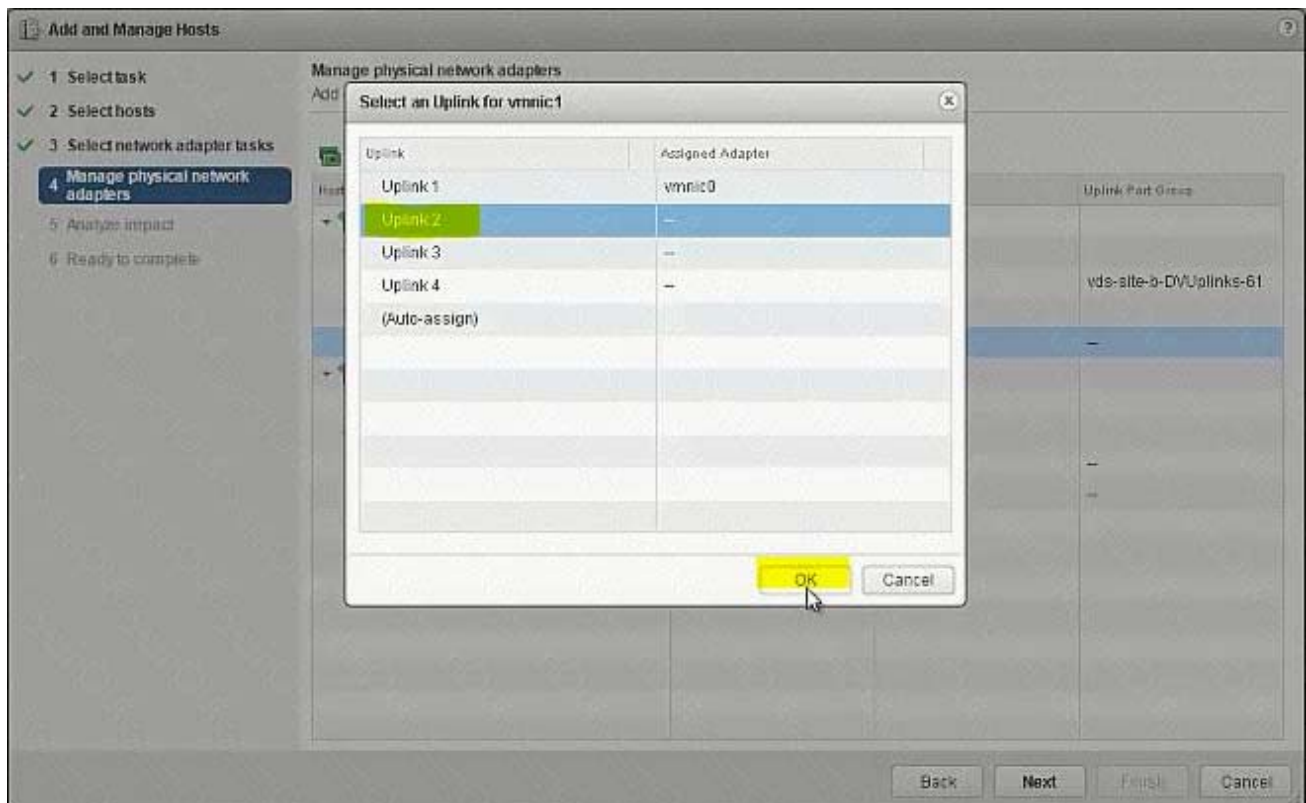


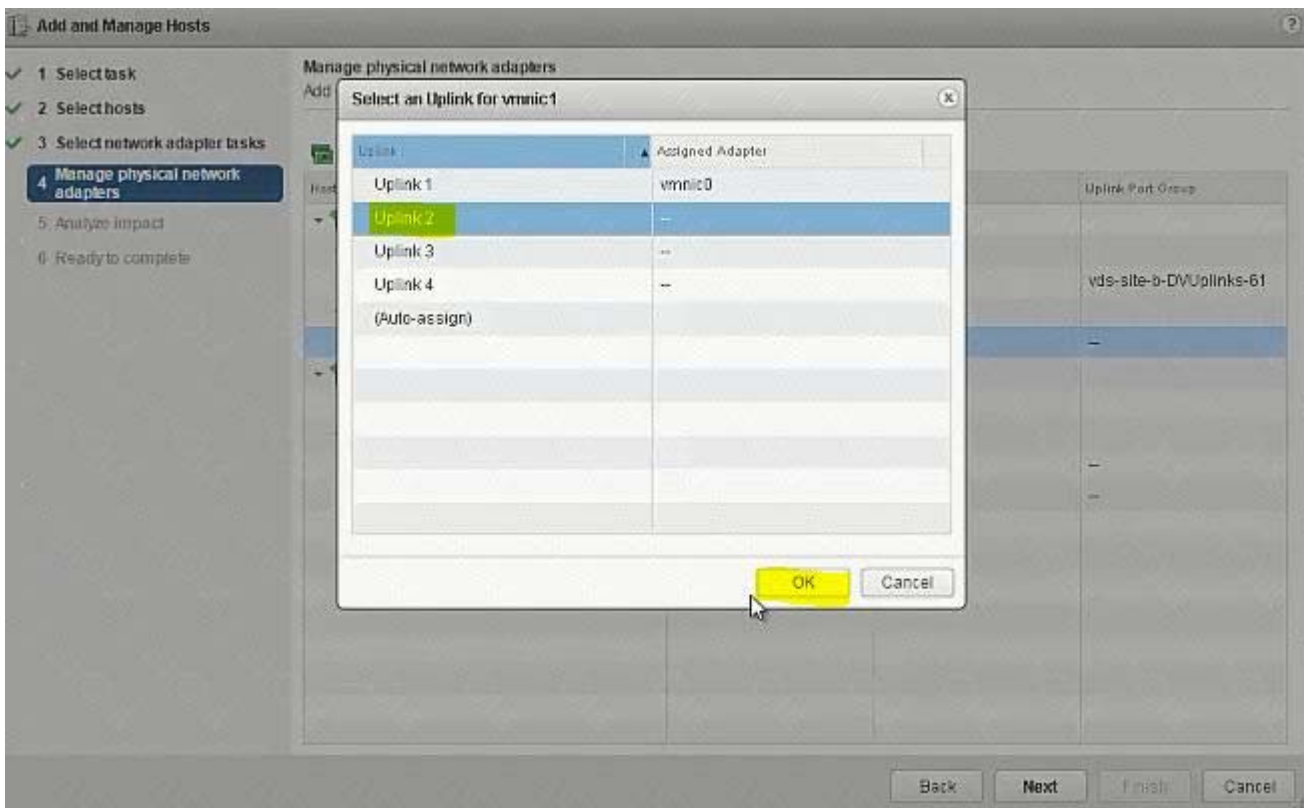
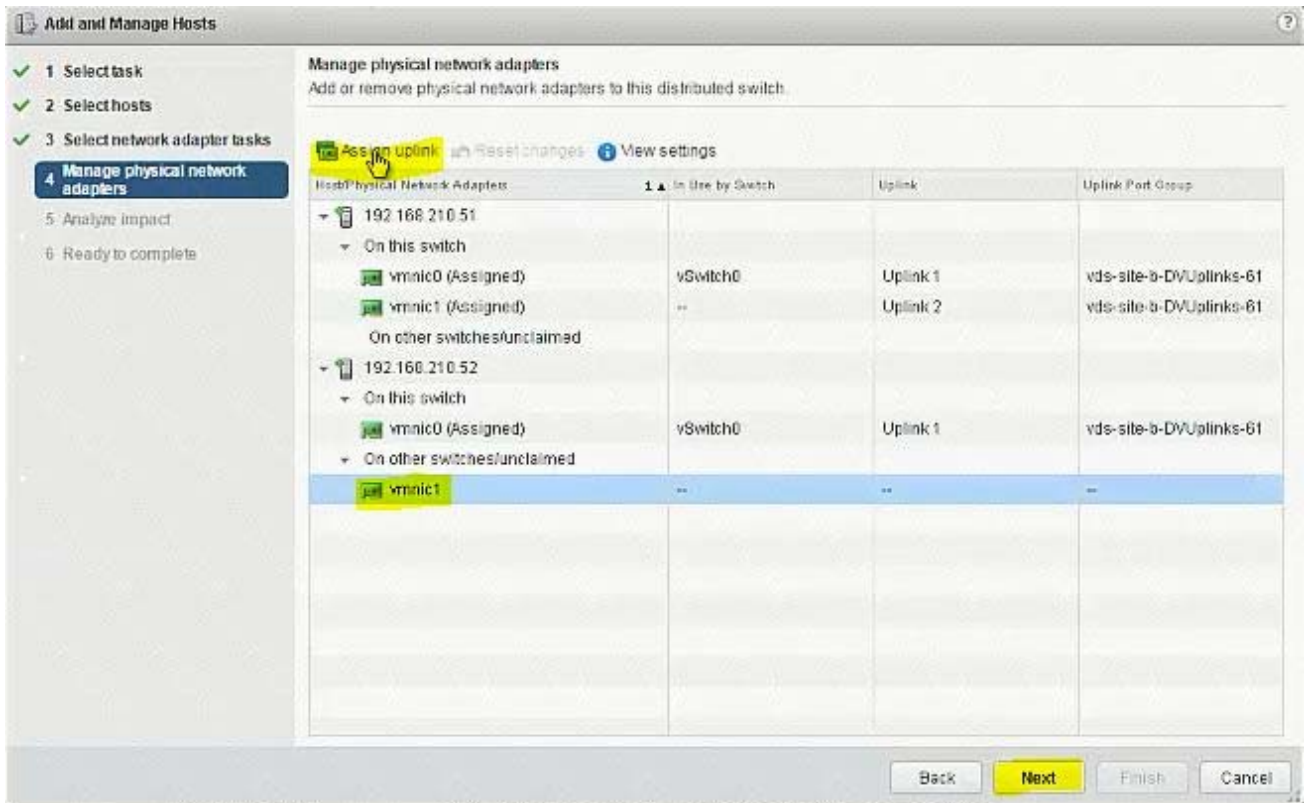


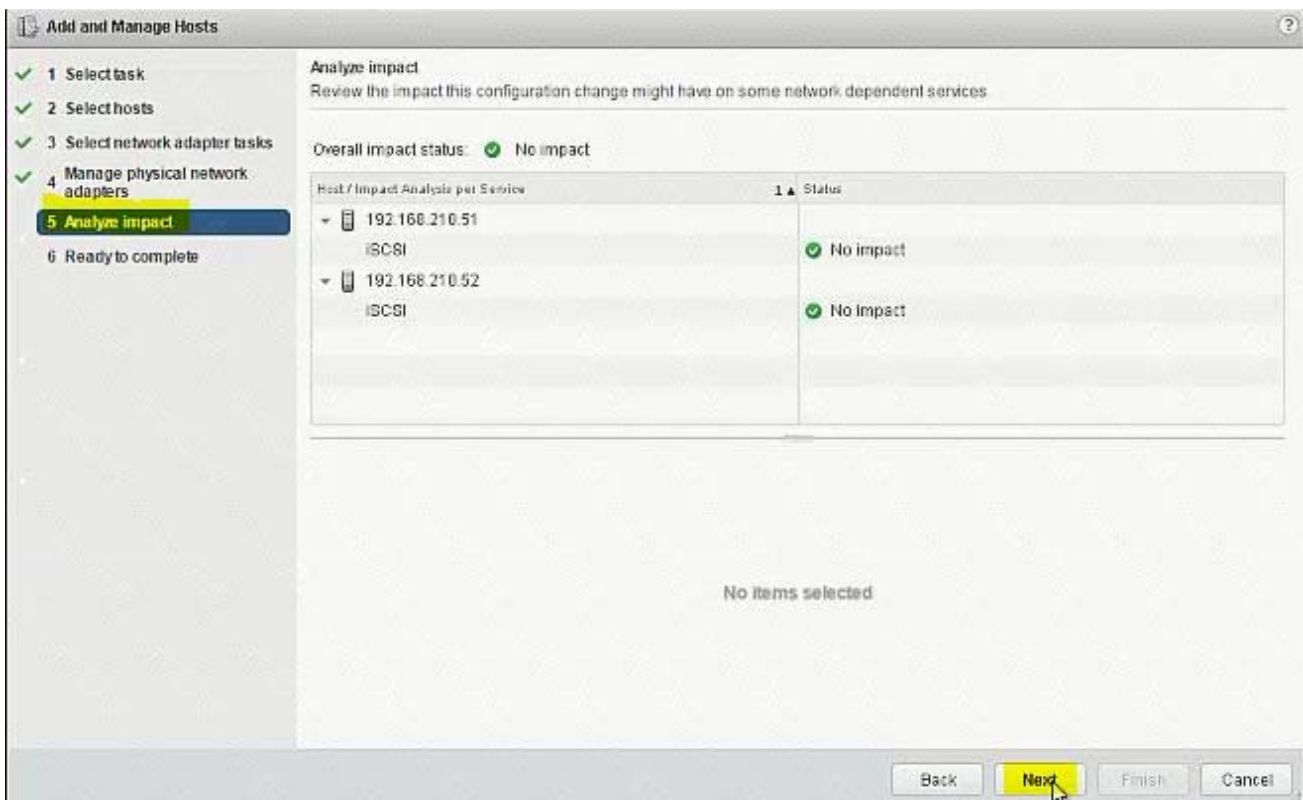
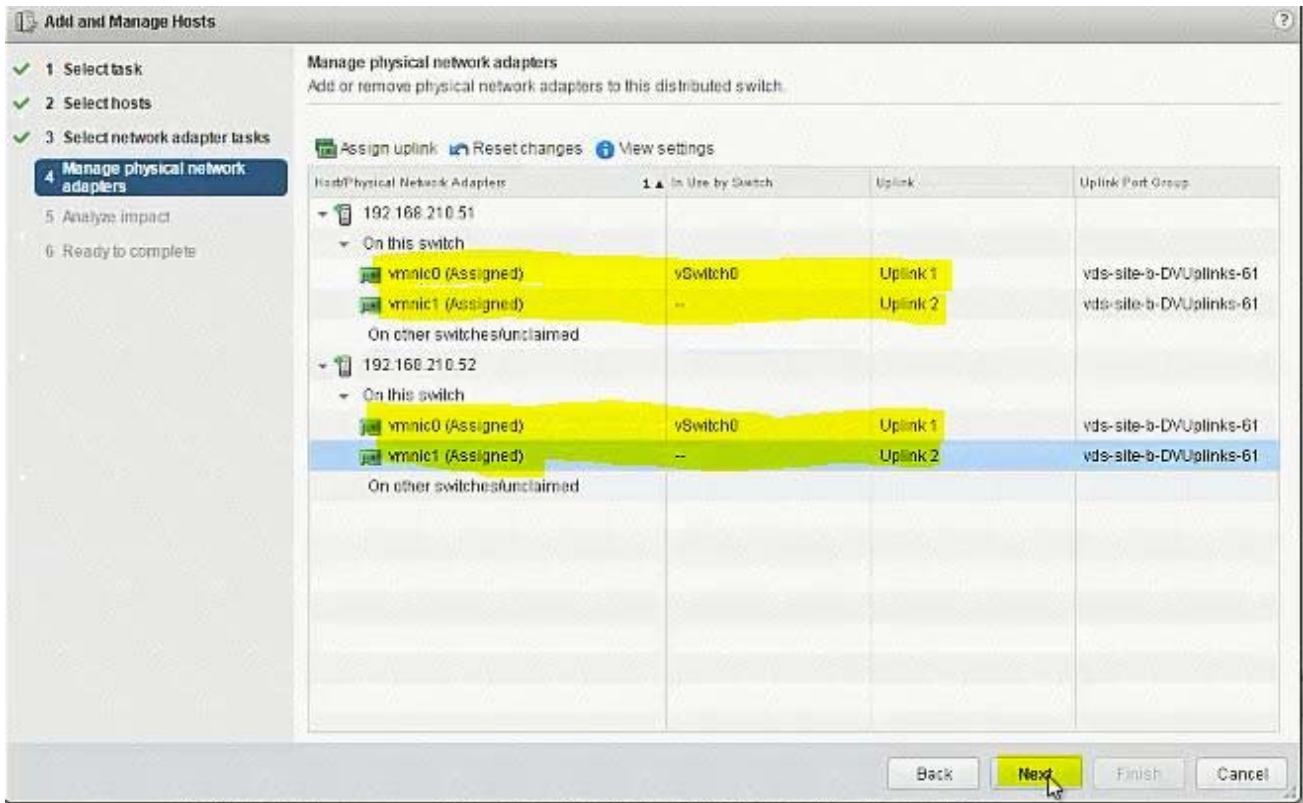


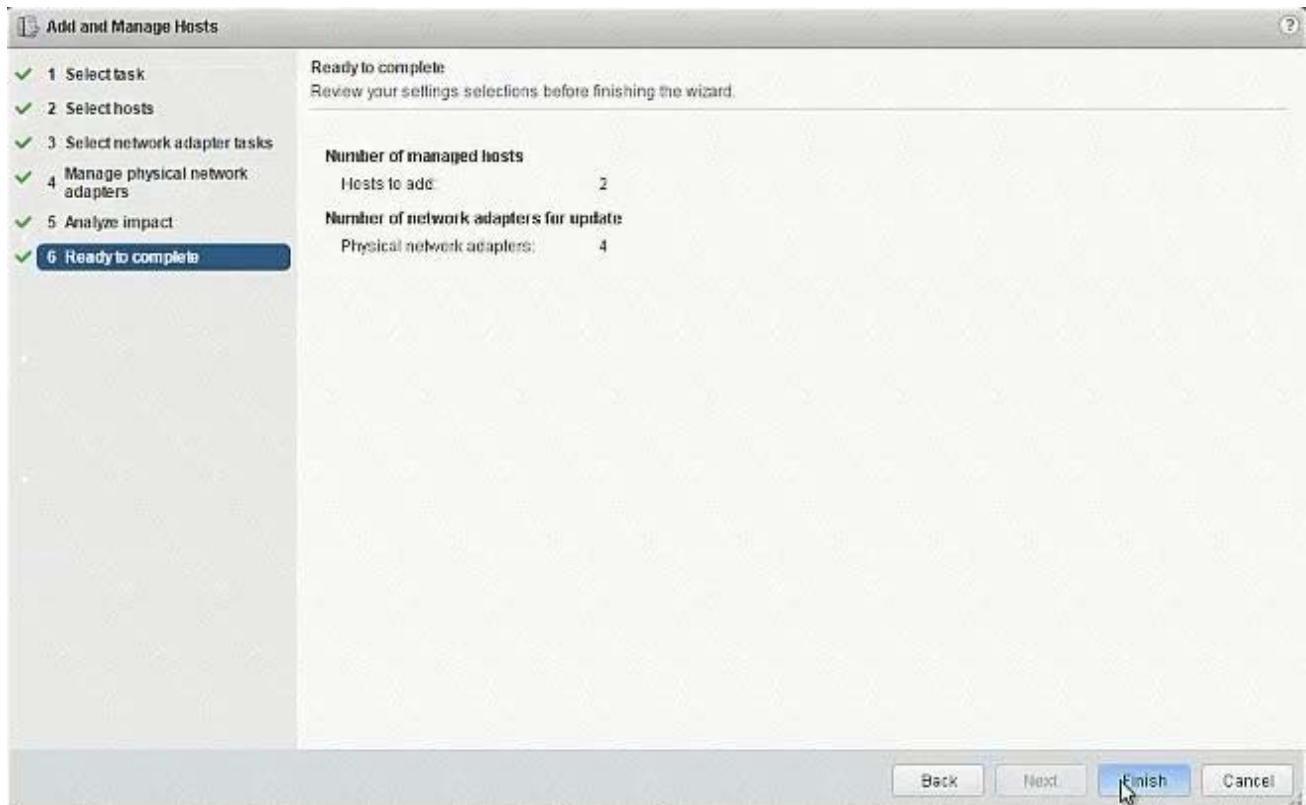












3. (Exam Topic 1)

The security team has requested that administrator@corp.local have the ability to fully manage NSX Manager (192.168.210.15) for Site B.

Requirements:

vCenter: vcsa-01b.corp.local

Credentials: administrator@vsphere.local / VMware1!

Ensure administrator@corp.local has the ability to fully manage NSX Manager in SiteB.

NOTE:

You may have to log out of the web client and back in for 192.168.210.15 to show in web client.

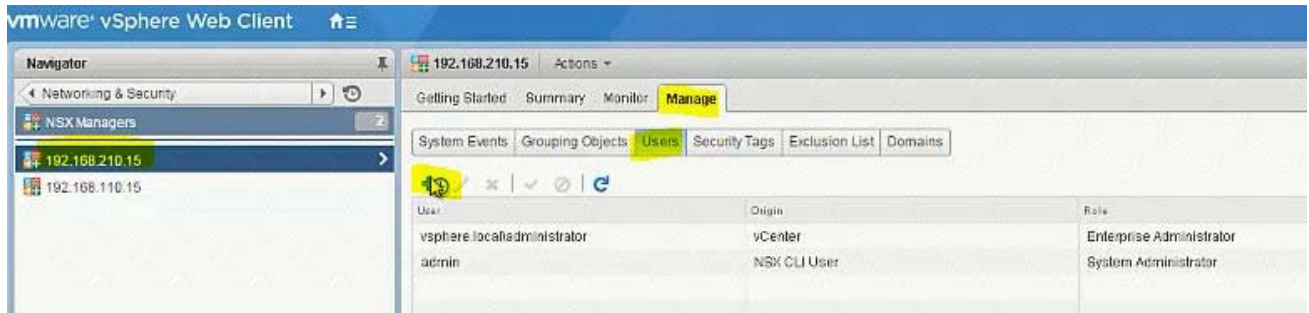
HOL LAB for Practice:

See the explanation part for complete solution.

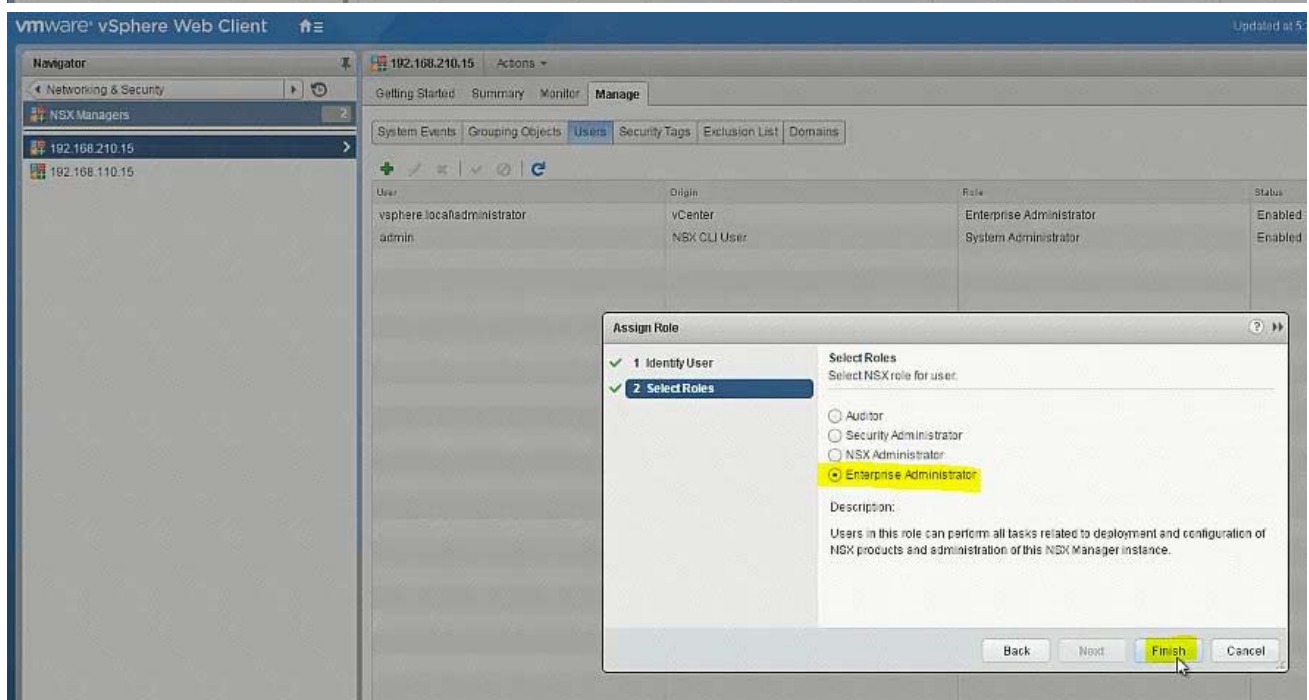
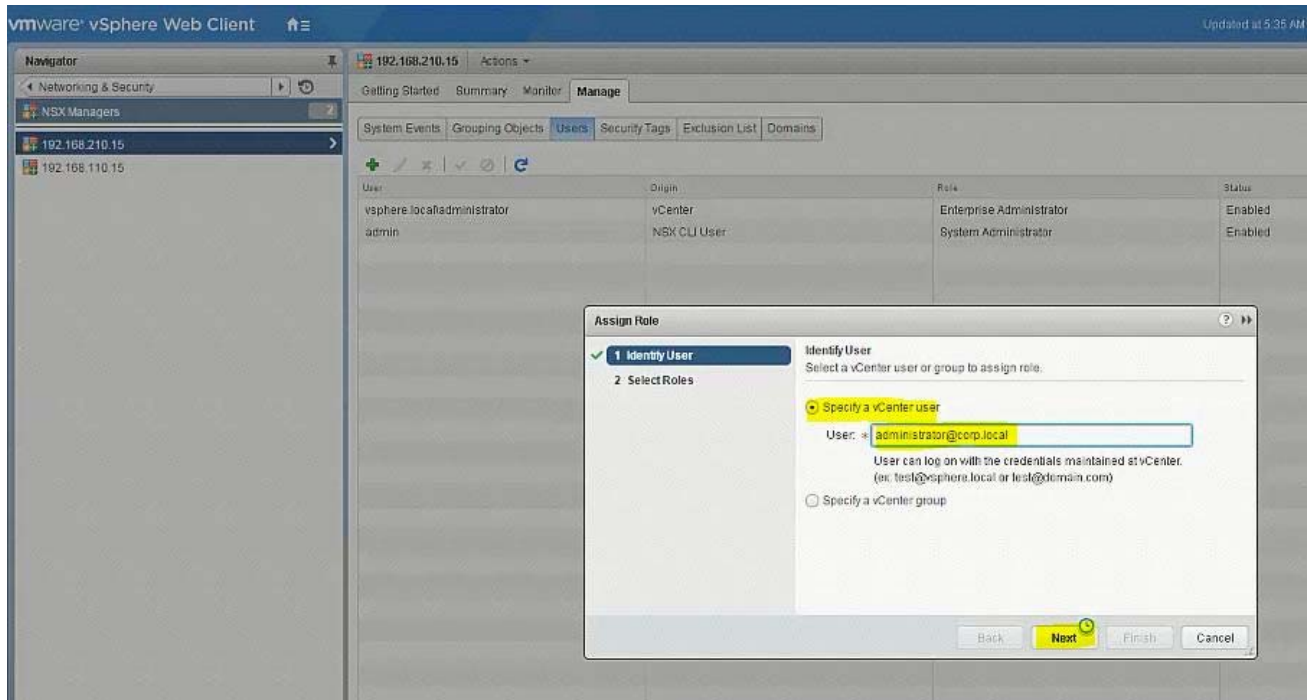
Answer:

SOLUTION:

NSX Manager in SiteB



administrator@corp.local



go to Nsx manager - b. select Manage Vcenter registration. check if lookup service

is configured if not configured it will the details.

lookup service ip = Nsx Manager - a IP Address

Lookup service port = 7444

Lookup service= https://192.168.110.15:7444/lookupservice/sdk

SSO administrator = administrator@vsphere.local

password = VMware1!

click on ok. click on yes.

NOTE: it will show u connected. if not connected. logout and login again

4. (Exam Topic 1)

Create a backup of only the vDS portgroup the NSX controllers utilize along with the NSX Firewall configuration. Also, the security team had identified a missing security policy that needs to be added.

Requirements:

vCenter: vcsa-01a.corp.local

Credentials: administrator@vsphere.local / VMware1!

Components to backup:

- vDS Portgroup that the controllers utilize.

- NSX Firewall configuration.

- Backup file name: vdsPortGroup-backup-NEW.zip, nsxfw-backup-NEW.xml

- Backup file location: Desktop of the ControlCenter.

Security Policy:

File to import: sec-policy-blueprint located on the desktop of the ControlCenter.

- Backup only the vDS portgroup that the NSX Controllers utilize.

- Backup the NSX Firewall configuration.

- Import the sec-policy.blueprint file

Ensure requirements are met.

HOL LAB for Practice:

See the explanation part for complete solution.

Answer:

SOLUTION:

select Network & Security. select service composer. select 192.168.110.15.

select security policy tab. click on + sign enter name sec-policy-blueprint.

click next 3 times. click finish. select sec-policy-blueprint. click right mouse

button select export configuration. enter name sec-policy-blueprint. click next

select sec-policy-blueprint. click next. click finish. select desktop location.

enter name sec-policy-blueprint. click save. select sec-policy-web and delete it.

Verify NSX Controllers' vDS Portgroup

Vds-mgmt-a_Management network (under site A vcenter networking)

vmware vSphere Web Client

Navigator

- Home
- vcasa-01a.corp.local
 - DataCenter Site A
 - none
 - VM Network
 - vds-mgmt-edge-a
 - yds-HSA-NEW
 - yds-mgmt-a_Management network**
 - yds-mgmt-a_storage network
 - yds-mgmt-a_transit network
 - yds-mgmt-a_trunk network
 - yds-mgmt-a_UPLINK network
 - yds-mgmt-a_VM network
 - yds-mgmt-a_vmotion network
 - yds-mgmt-edge-a DVUplinks-36
 - www-dvs-36-virtualwire-10-sid-5008-T8-Dev...
 - www-dvs-36-virtualwire-11-sid-5009-T3-DevD...
 - www-dvs-36-virtualwire-12-sid-5010-T6-Ls-01
 - www-dvs-36-virtualwire-13-sid-5011-Dav-Web...
 - www-dvs-36-virtualwire-14-sid-5012-Dev-App...
 - www-dvs-36-virtualwire-15-sid-5013-Dev-DB...
 - www-dvs-36-virtualwire-16-sid-5014-App01...
 - www-dvs-36-virtualwire-17-sid-5015-App01...

yds-mgmt-a_Management network

Getting Started Summary Monitor **Manage** Related Objects

Settings Alarm Definitions Tags Permissions Network Protocol Profile **Ports**

| Port ID | Name | Connectee | Runtime MAC Address | Port Group | DirectPath I/O | State |
|---------|--------------------|-------------------|---------------------|-------------------|----------------|---------|
| 0 | | 192.168.110.56 - | 00:50:56:a3:1f:62 | vds-mgmt-a_Man... | -- | Link Up |
| 1 | | 192.168.110.58 - | 00:50:56:a3:9e:e8 | vds-mgmt-a_Man... | -- | Link Up |
| 2 | | 192.168.110.57 - | 00:50:56:a3:97:a6 | vds-mgmt-a_Man... | -- | Link Up |
| 3 | | -- | -- | vds-mgmt-a_Man... | -- | Link Up |
| 4 | NSX_Controller_... | 00:50:56:91:78:55 | vds-mgmt-a_Man... | Inactive | Link Up | |
| 5 | NSX_Controller_... | 00:50:56:91:ea:7c | vds-mgmt-a_Man... | Inactive | Link Up | |
| 6 | NSX_Controller_... | 00:50:56:91:bb:95 | vds-mgmt-a_Man... | Inactive | Link Up | |
| 7 | | -- | -- | vds-mgmt-a_Man... | -- | Link Up |
| 108 | | -- | -- | vds-mgmt-a_Man... | -- | Link Up |
| 109 | | -- | -- | vds-mgmt-a_Man... | -- | Link Up |
| 110 | | -- | -- | vds-mgmt-a_Man... | -- | Link Up |
| 111 | | -- | -- | vds-mgmt-a_Man... | -- | Link Up |

Port ID: 4

vmware vSphere Web Client

Navigator

- Home
- vcasa-01a.corp.local
 - DataCenter Site A
 - none
 - VM Network
 - vds-mgmt-edge-a
 - yds-HSA-NEW
 - yds-mgmt-a_Management network**
 - yds-mgmt-a_storage network
 - yds-mgmt-a_transit network
 - yds-mgmt-a_trunk network
 - yds-mgmt-a_UPLINK network
 - yds-mgmt-a_VM network
 - yds-mgmt-a_vmotion network
 - yds-mgmt-edge-a DVUplinks-36
 - www-dvs-36-virtualwire-10-sid-5008-T8-Dev...
 - www-dvs-36-virtualwire-11-sid-5009-T3-DevD...
 - www-dvs-36-virtualwire-12-sid-5010-T6-Ls-01
 - www-dvs-36-virtualwire-13-sid-5011-Dav-Web...
 - www-dvs-36-virtualwire-14-sid-5012-Dev-App...
 - www-dvs-36-virtualwire-15-sid-5013-Dev-DB...
 - www-dvs-36-virtualwire-16-sid-5014-App01...
 - www-dvs-36-virtualwire-17-sid-5015-App01...

yds-mgmt-a_Management network

Getting Started Summary Monitor **Manage** Related Objects

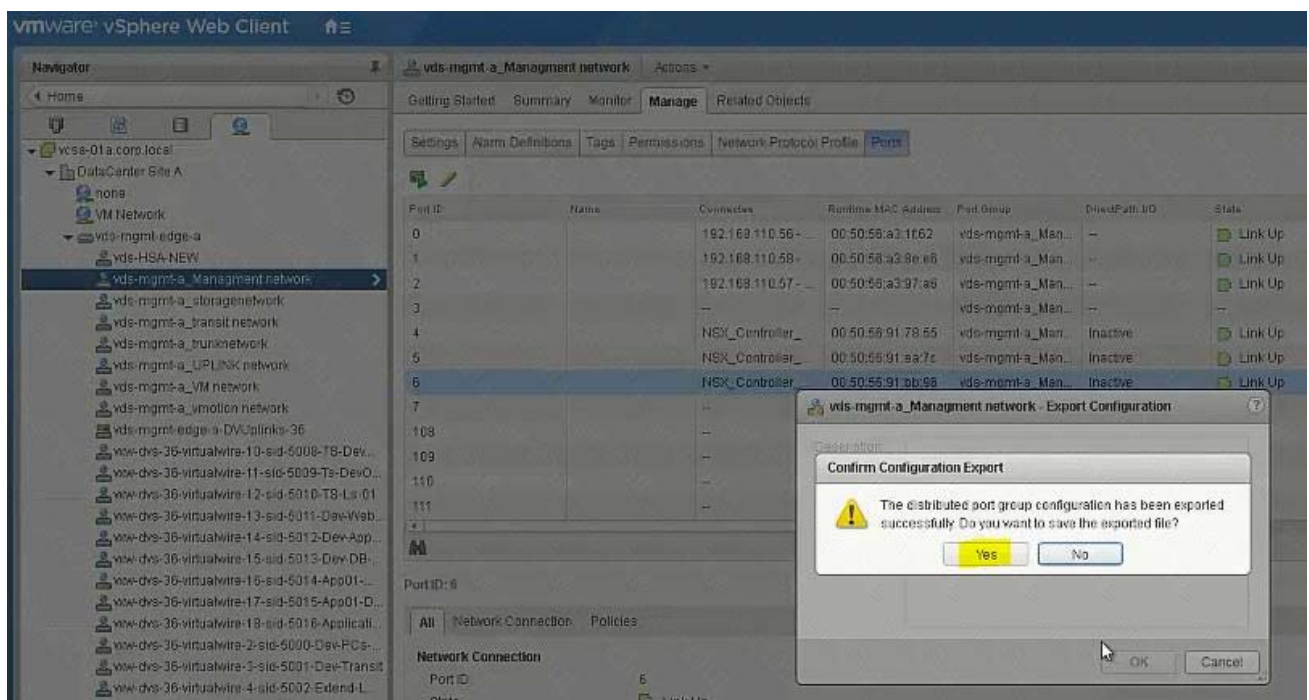
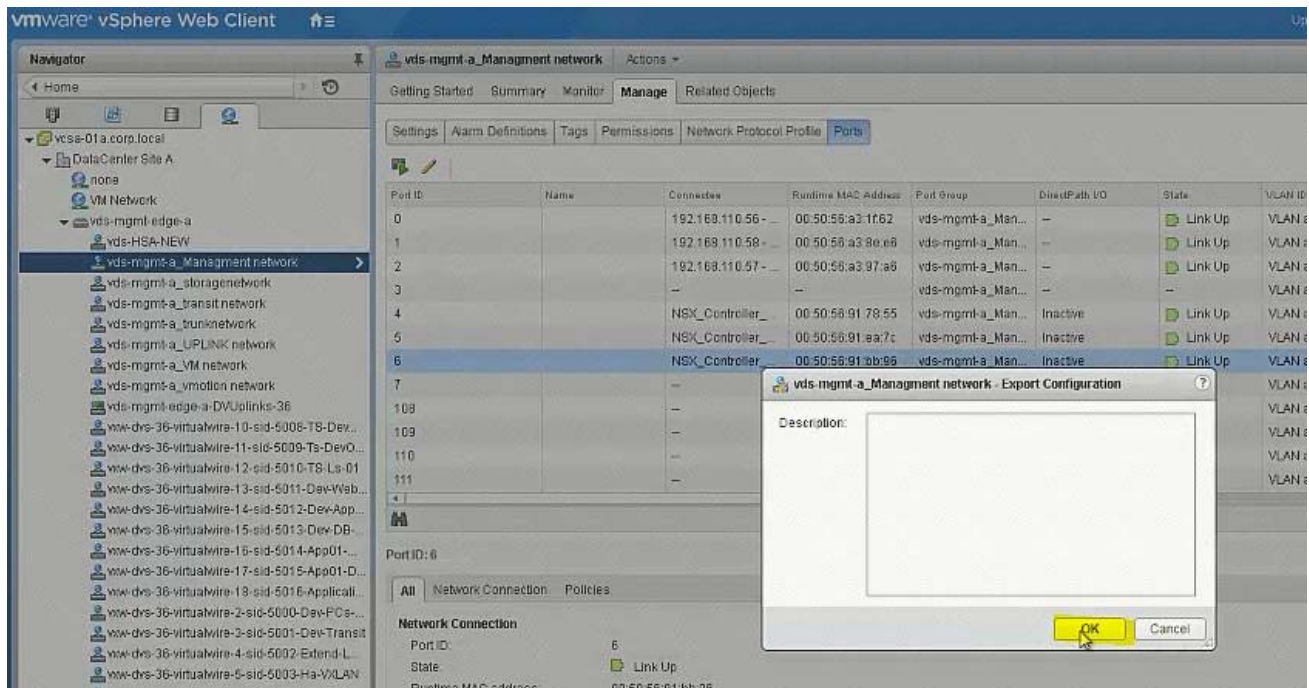
Settings Alarm Definitions Tags Permissions Network Protocol Profile **Ports**

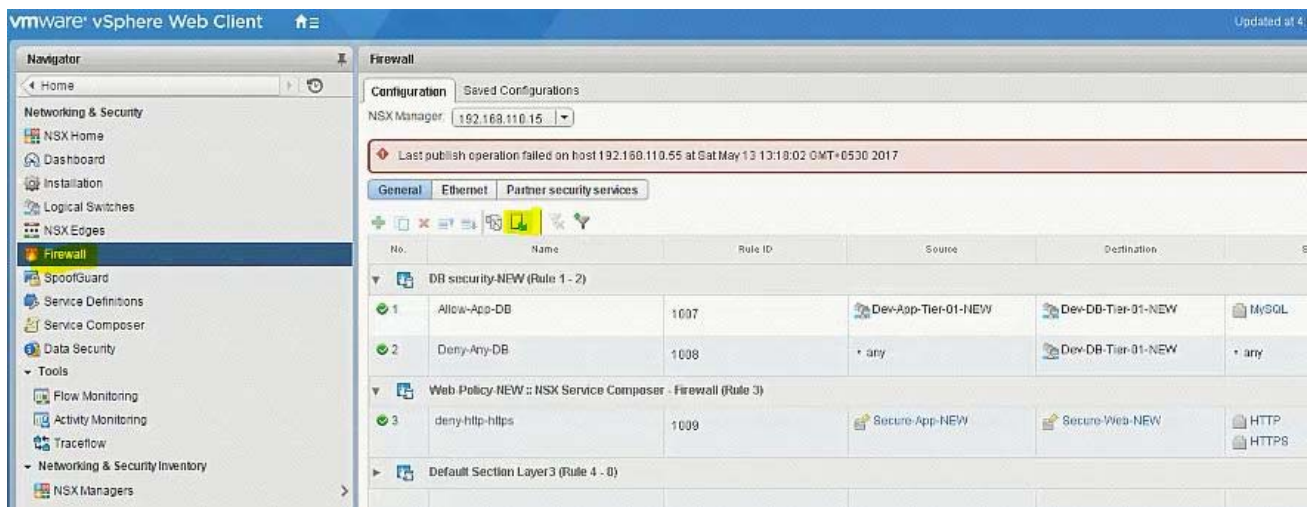
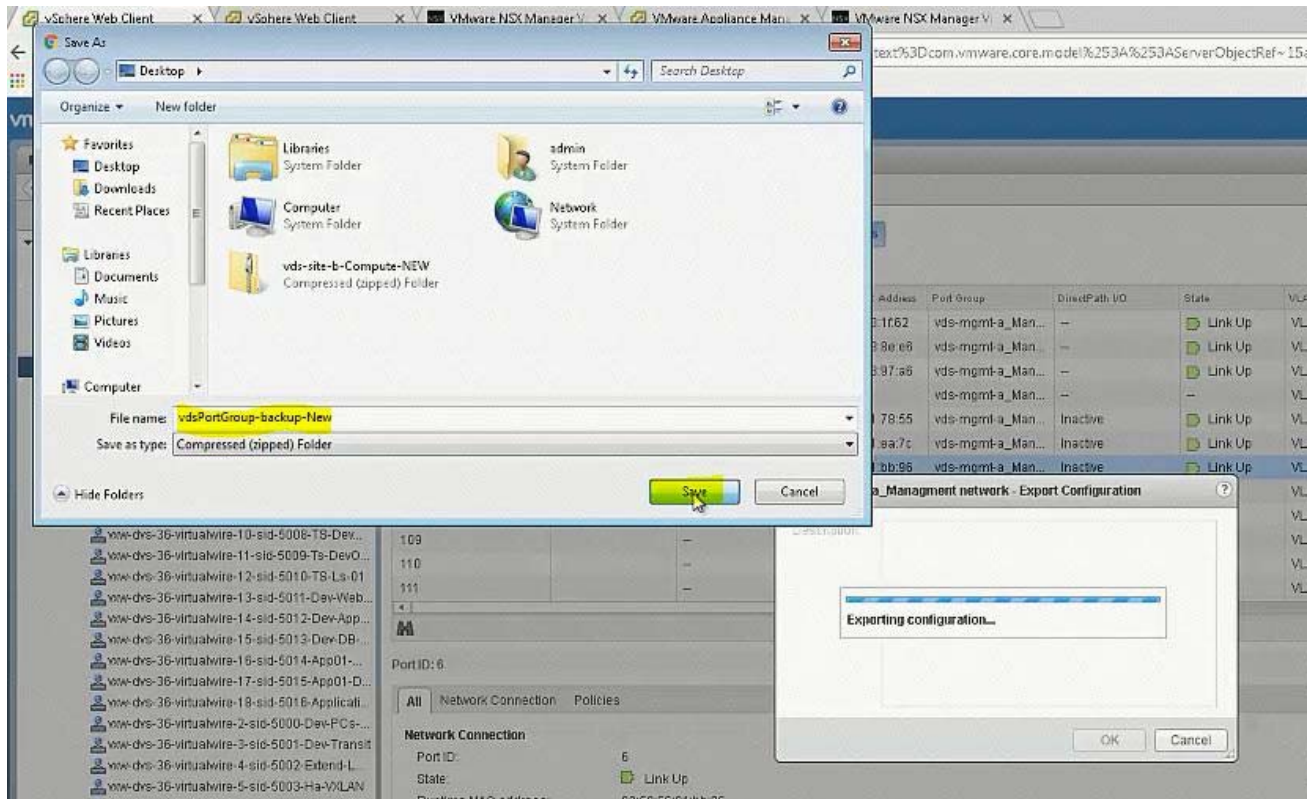
| Port ID | Name | Connectee | Runtime MAC Address | Port Group | DirectPath I/O | State | VLAN |
|---------|--------------------|-------------------|---------------------|-------------------|----------------|---------|------|
| 0 | | 192.168.110.56 - | 00:50:56:a3:1f:62 | vds-mgmt-a_Man... | -- | Link Up | V/L |
| 1 | | 192.168.110.58 - | 00:50:56:a3:9e:e8 | vds-mgmt-a_Man... | -- | Link Up | V/L |
| 2 | | 192.168.110.57 - | 00:50:56:a3:97:a6 | vds-mgmt-a_Man... | -- | Link Up | V/L |
| 3 | | -- | -- | vds-mgmt-a_Man... | -- | Link Up | V/L |
| 4 | NSX_Controller_... | 00:50:56:91:78:55 | vds-mgmt-a_Man... | Inactive | Link Up | V/L | |
| 5 | NSX_Controller_... | 00:50:56:91:ea:7c | vds-mgmt-a_Man... | Inactive | Link Up | V/L | |
| 6 | NSX_Controller_... | 00:50:56:91:bb:95 | vds-mgmt-a_Man... | Inactive | Link Up | V/L | |
| 7 | | -- | -- | vds-mgmt-a_Man... | -- | Link Up | V/L |
| 108 | | -- | -- | vds-mgmt-a_Man... | -- | Link Up | V/L |
| 109 | | -- | -- | vds-mgmt-a_Man... | -- | Link Up | V/L |
| 110 | | -- | -- | vds-mgmt-a_Man... | -- | Link Up | V/L |
| 111 | | -- | -- | vds-mgmt-a_Man... | -- | Link Up | V/L |

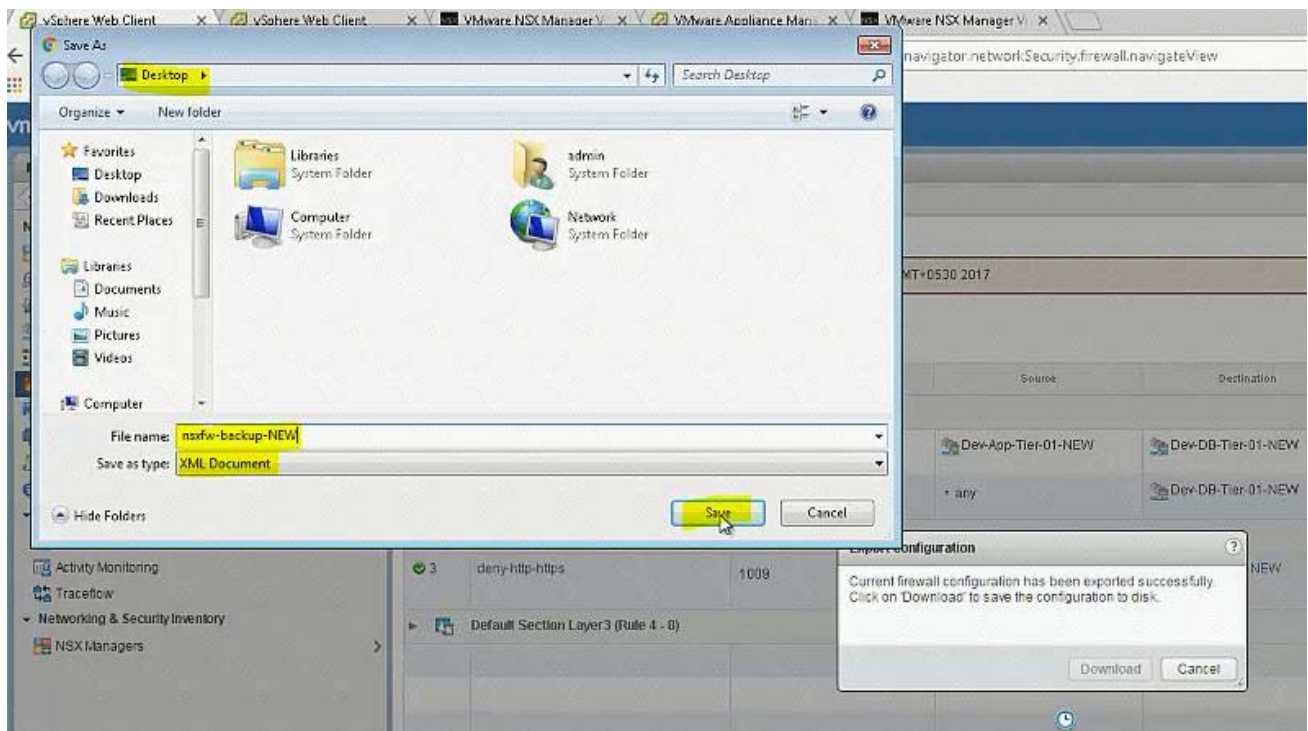
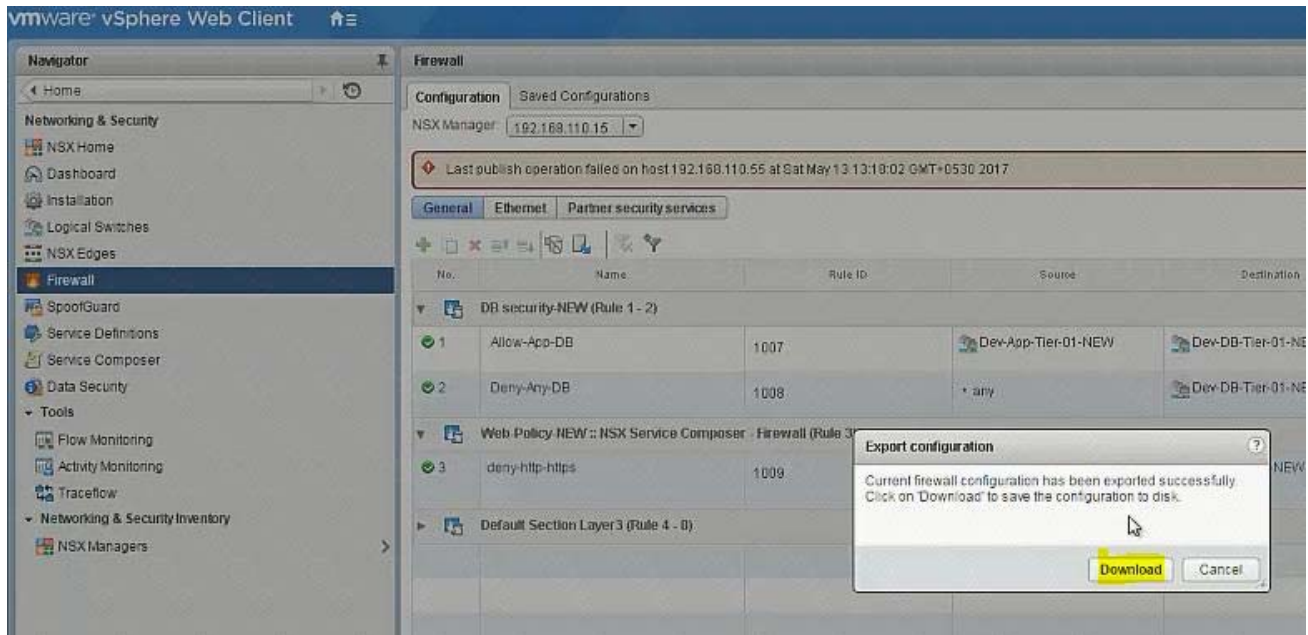
Port ID: 6

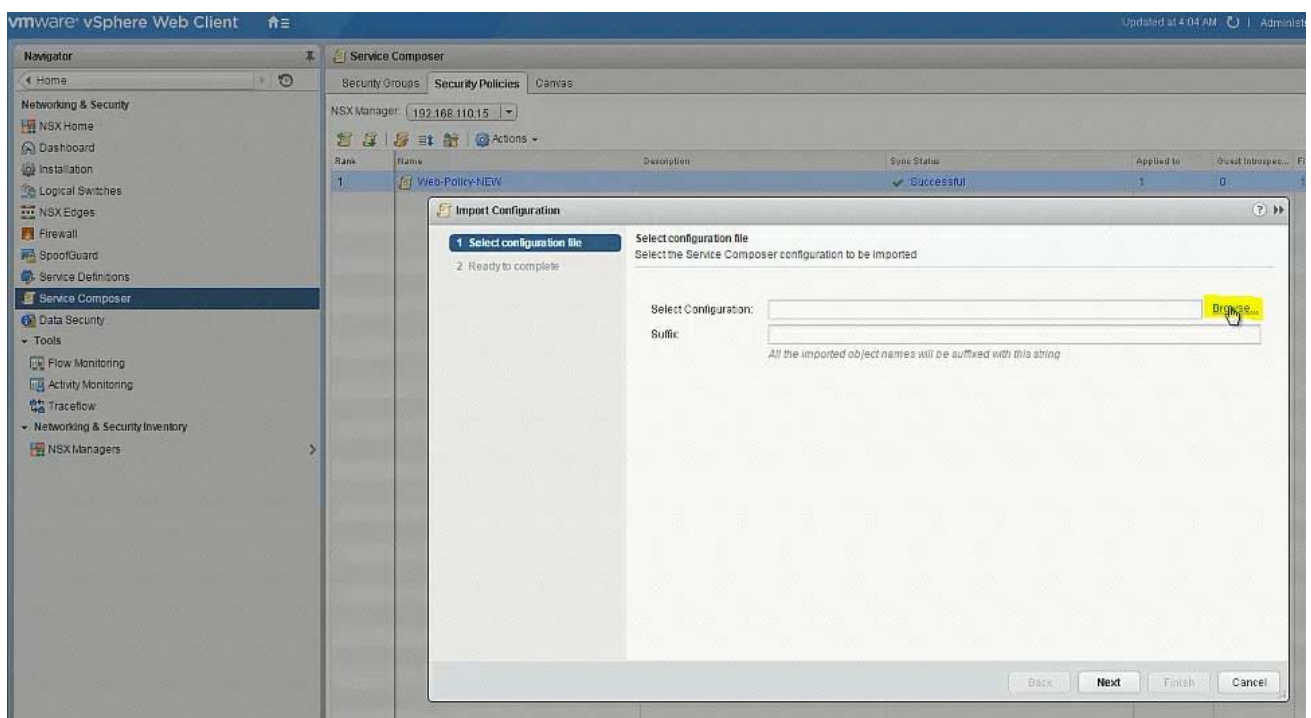
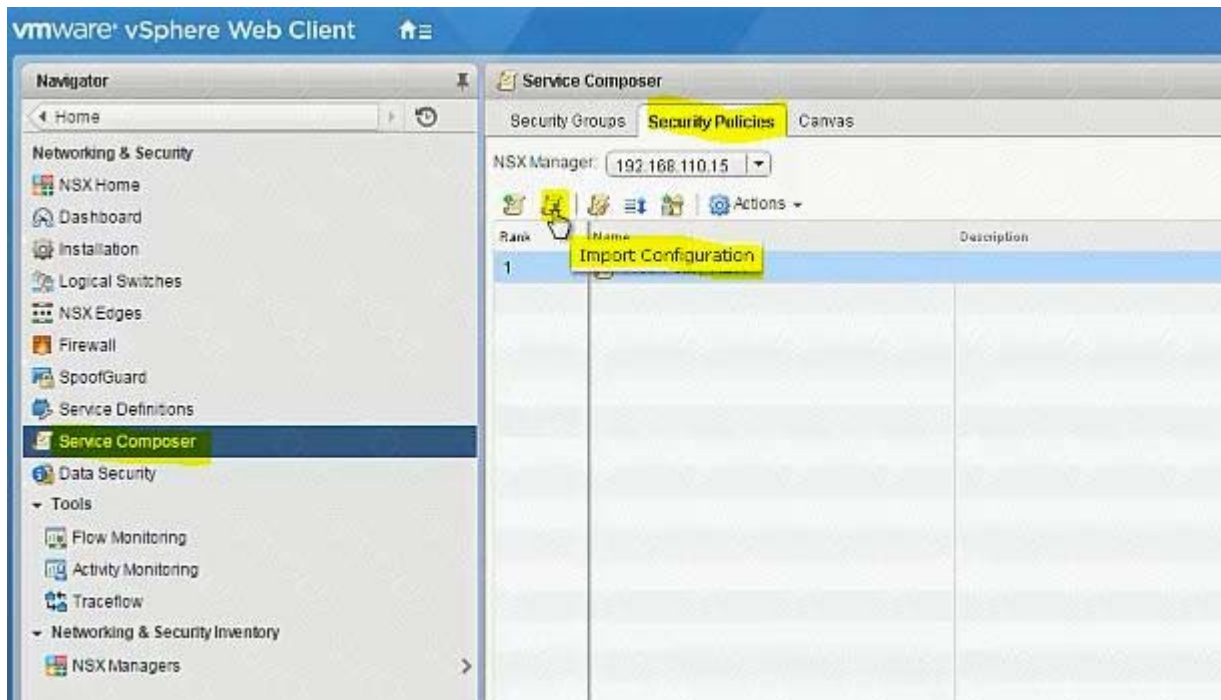
Actions - yds-mgmt-a_Management network

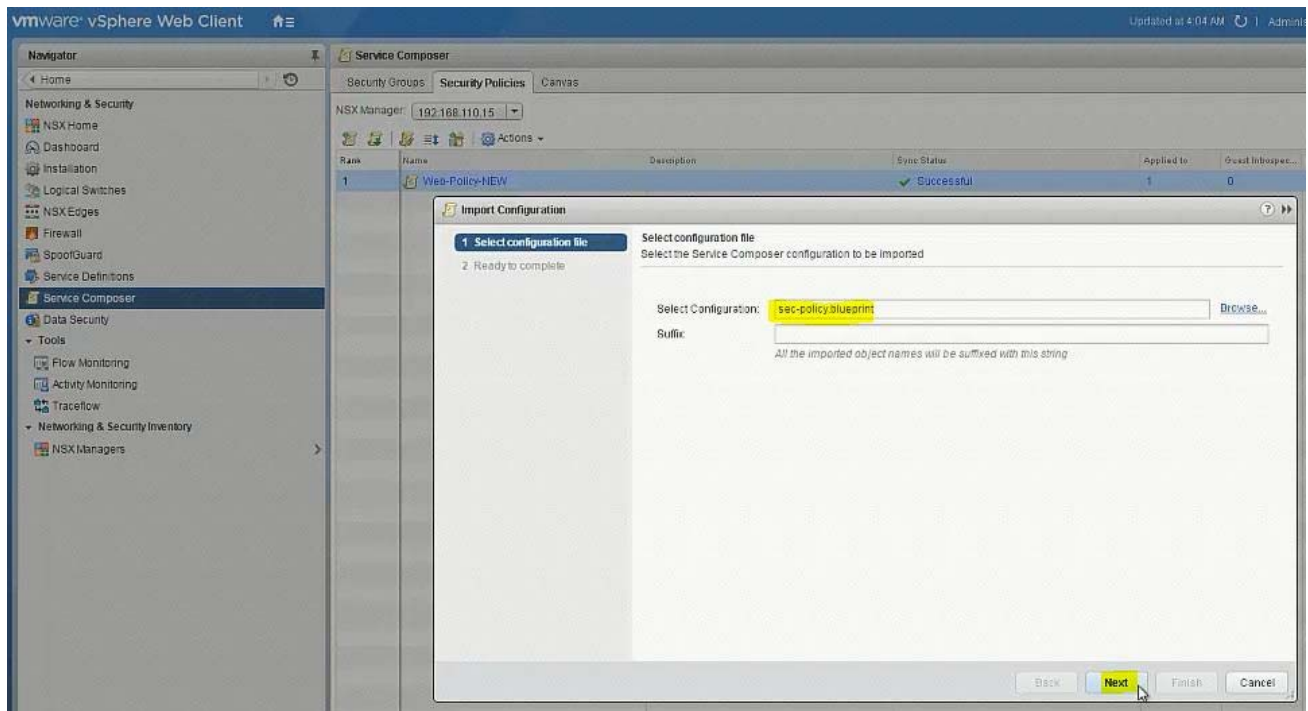
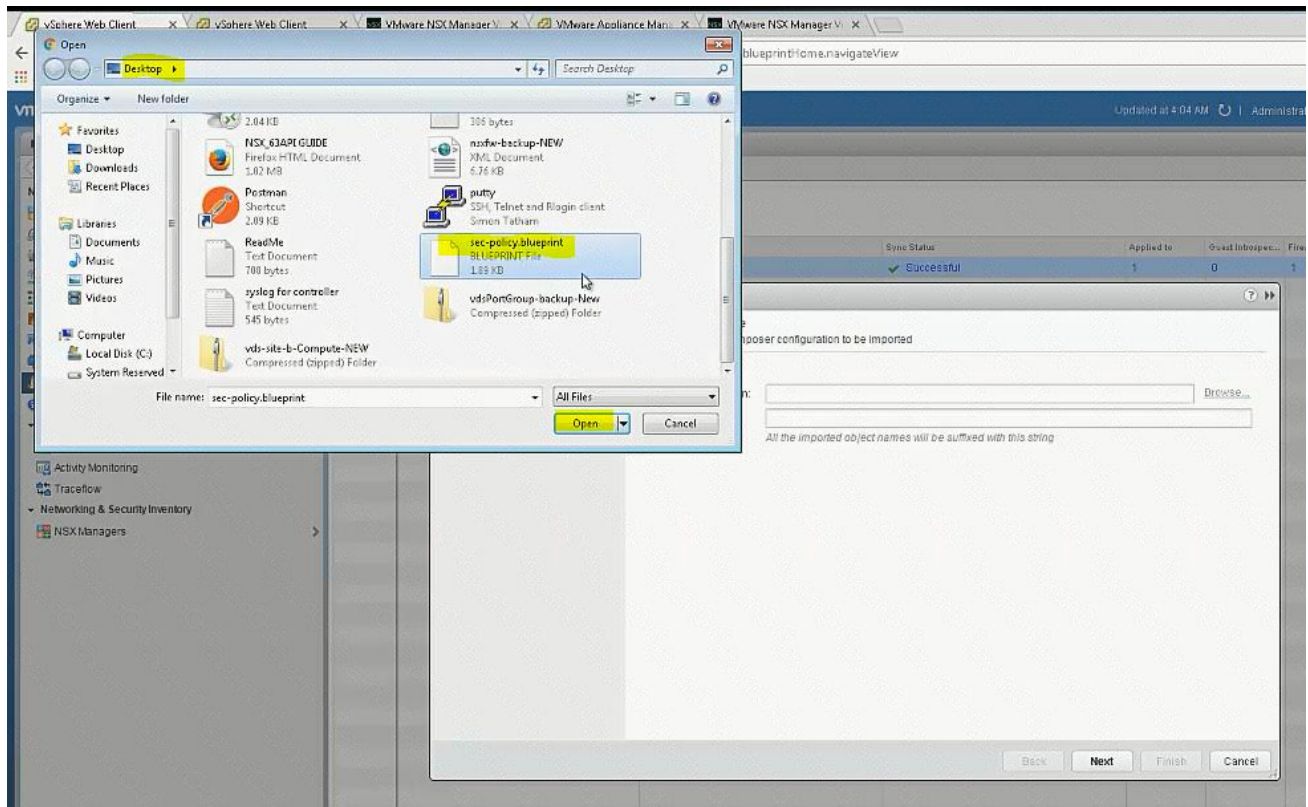
- Edit Settings
- Export Configuration**
- Restore Configuration...
- Rename...
- Tags
- Add Permission...
- Alarms
- Delete

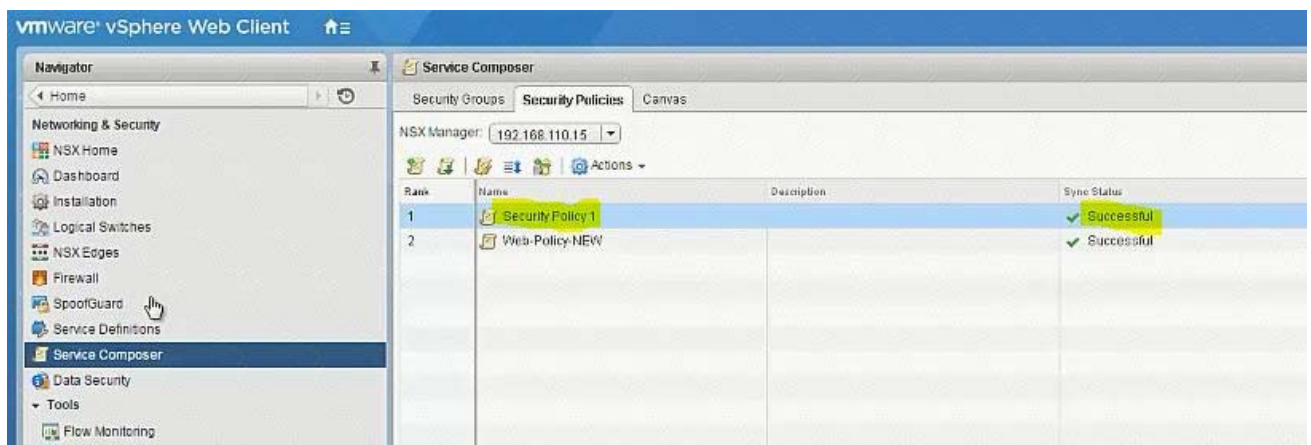
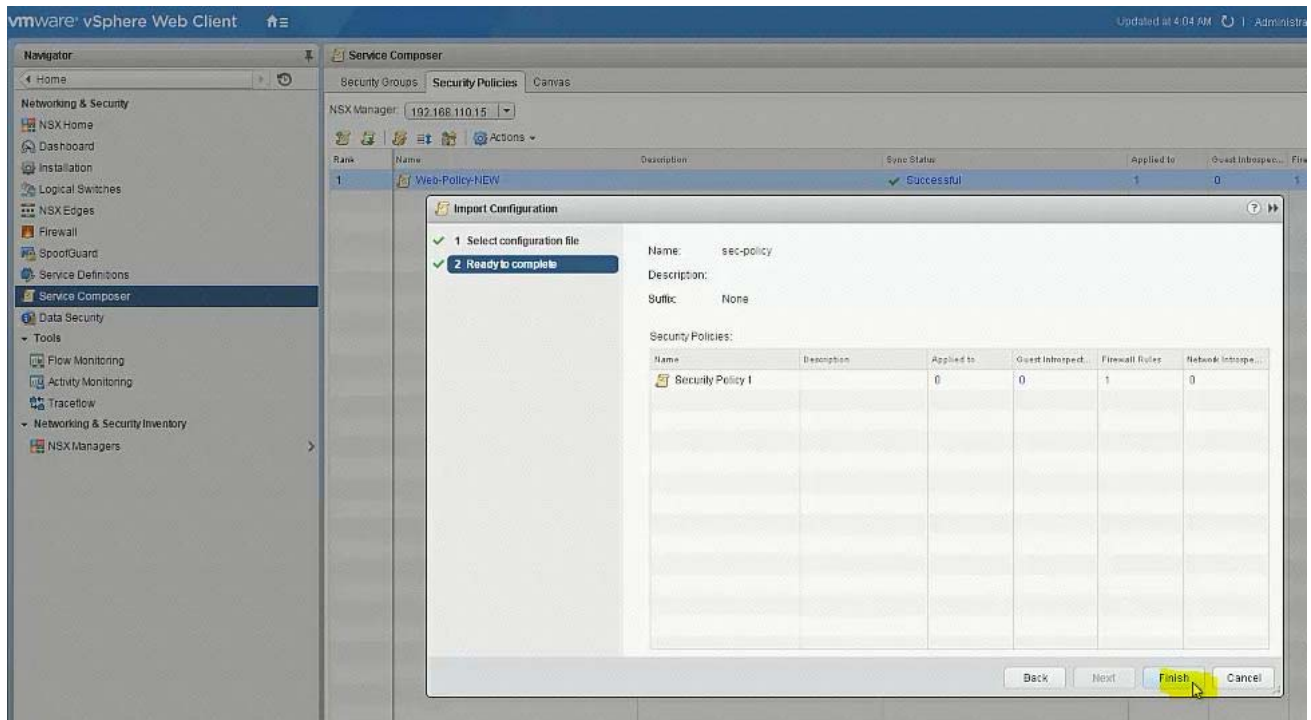












5. (Exam Topic 1)

Routing through TS-Edge-01 is not working. The service provider (SP) has confirmed their configuration is correct.

Requirements:

vCenter: vcsa01a.corp.local

Credential: administrator@vsphere.local / VMware1!

Edge: TS-Edge-01

Credential: admin / VMware1!VMware1!

Problem Edge: TS-Edge01

Local IP Address: 192.168.100.202

SP provided configuration:

Area ID: 10

Type: Normal

Authentication: None

Ensure the OSPF session is established.

Ensure all learned OSPF routes appear.

Copy OSPF routing table information and output to file on ControlCenter Desktop named TS-Edge-01_OSPF.txt

NOTE:

Do not use static route or configure Default Gateway on any Edge.

HOL LAB for Practice:

See the explanation part for complete solution.

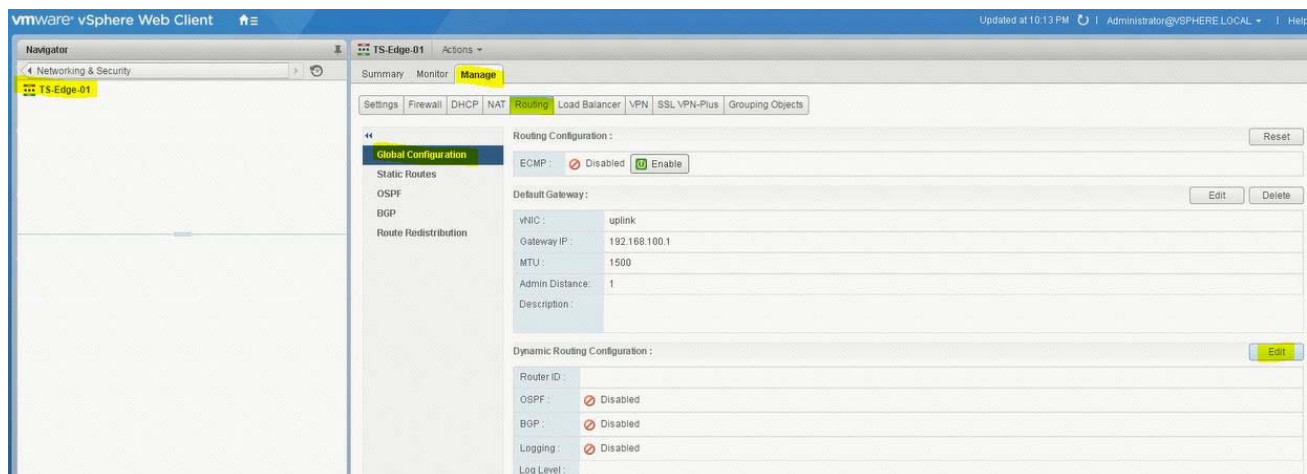
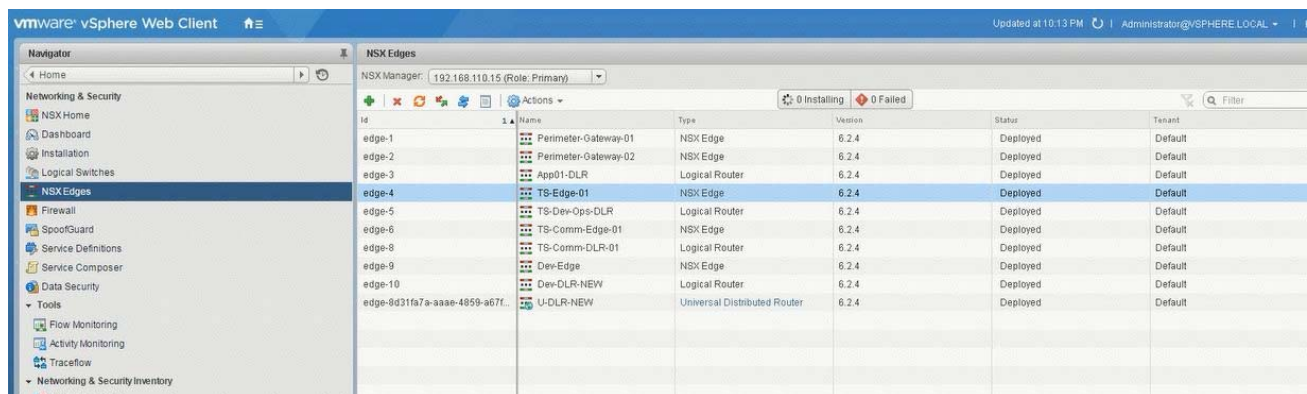
Answer:

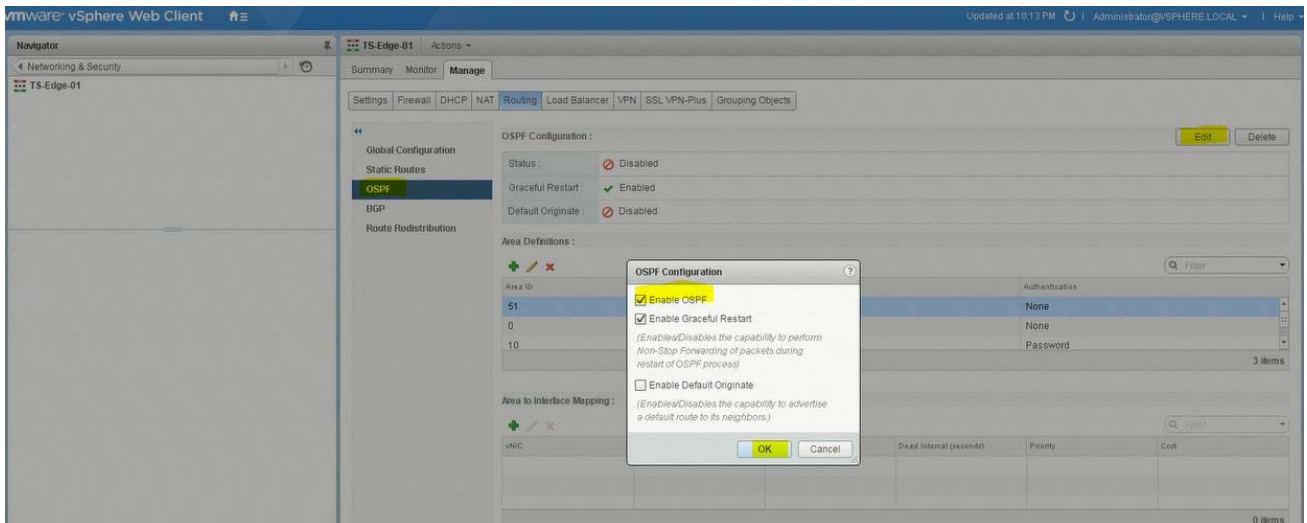
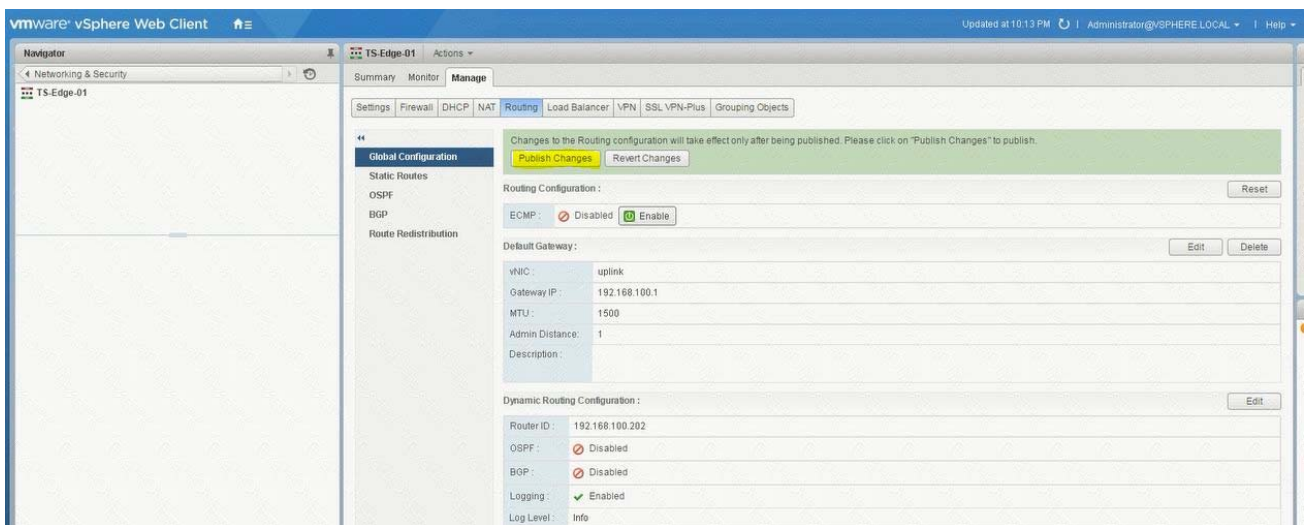
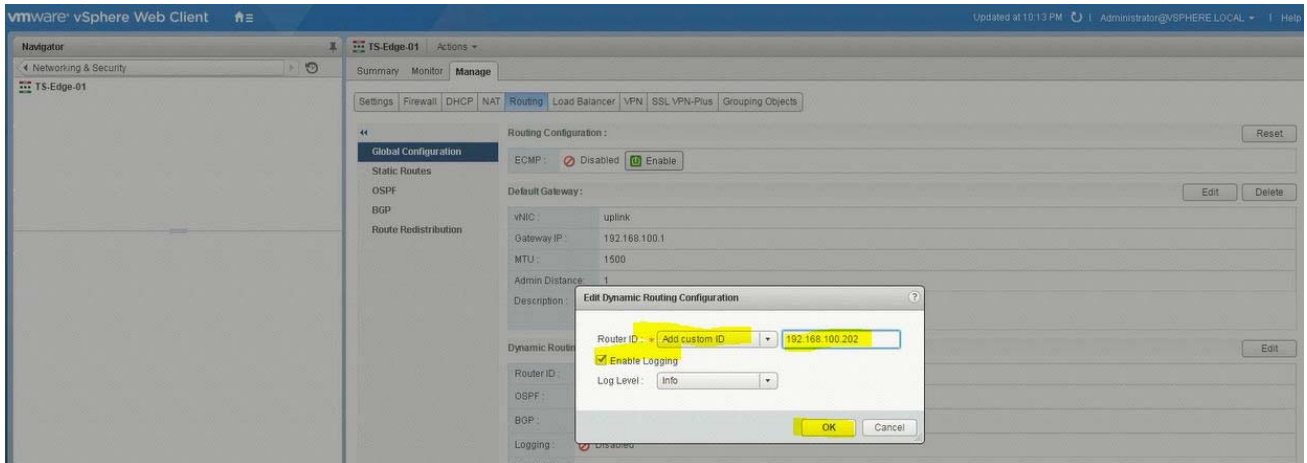
SOLUTION:

(1) select Home. select Network & Security. select NsX Edge. select Nsx Manager-a.

select TS-EDGE-01. select manage tab and select settings.

select interface. check ip address and mask of the vnic.





TS-Edge-01 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

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

OSPF Configuration : [Edit](#) [Delete](#)

Status : ☒ Enabled
Graceful Restart : ☒ Enabled
Default Originate : ☐ Disabled

Area Definitions :

| Area ID | Type | Authentication |
|---------|------|----------------|
| 10 | NSSA | Password |

3 Items

Area to Interface Mapping :

| vNIC | Area ID | Hello Interval (seconds) | Dead Interval (seconds) | Priority | Cost |
|------|---------|--------------------------|-------------------------|----------|------|
|------|---------|--------------------------|-------------------------|----------|------|

0 Items

TS-Edge-01 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 : [Edit](#) [Delete](#)

Status : ☒ Enabled
Graceful Restart : ☒ Enabled
Default Originate : ☐ Disabled

Area Definitions :

| Area ID | Type | Authentication |
|---------|--------|----------------|
| 51 | | None |
| 0 | | None |
| 10 | Normal | None |

3 Items

Area to Interface Mapping :

| vNIC | Area ID | Hello Interval (seconds) | Dead Interval (seconds) | Priority | Cost |
|------|---------|--------------------------|-------------------------|----------|------|
|------|---------|--------------------------|-------------------------|----------|------|

0 Items

Edit Area Definition

Area ID : 10
Type : Normal
Authentication : None
Value :
[OK](#) [Cancel](#)

The image displays two screenshots of the Mikrotik WinBox interface, specifically the OSPF configuration page for TS-Edge-01. The interface is divided into a left sidebar with navigation options (Global Configuration, Static Routes, OSPF, BGP, Route Redistribution) and a main content area. The top navigation bar includes tabs for Settings, Firewall, DHCP, NAT, Routing, Load Balancer, VPN, SSL VPN-Plus, and Grouping Objects. The bottom navigation bar includes tabs for Summary, Monitor, and Manage. The main content area shows the OSPF Configuration section with a status bar indicating that changes will take effect after publishing. The OSPF Configuration section includes fields for Status (Enabled), Graceful Restart (Enabled), and Default Originate (Disabled). Below this is the Area Definitions section, which contains a table with columns for Area ID, Type, and Authentication. The table shows one entry: Area ID 51, Type NSSA, Authentication None. Below the Area Definitions section is the Area to Interface Mapping section, which contains a table with columns for vNIC, Area ID, Hello Interval (seconds), Dead Interval (seconds), Priority, and Cost. The table is currently empty. The bottom screenshot shows the same configuration page, but with an additional entry in the Area Definitions table: Area ID 10, Type Normal, Authentication None. The status bar at the top of the bottom screenshot indicates that changes will take effect after publishing.

TS-Edge-01 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

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

Publish Changes Revert Changes

OSPF Configuration:

Status: ☒ Enabled
Graceful Restart: ☒ Enabled
Default Originate: ☐ Disabled

Area Definitions:

| Area ID | Type | Authentication |
|---------|------|----------------|
| 51 | NSSA | None |

Area to Interface Mapping:

| vNIC | Area ID | Hello Interval (seconds) | Dead Interval (seconds) | Priority | Cost |
|------|---------|--------------------------|-------------------------|----------|------|
|------|---------|--------------------------|-------------------------|----------|------|

TS-Edge-01 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: ☒ Enabled
Graceful Restart: ☒ Enabled
Default Originate: ☐ Disabled

Area Definitions:

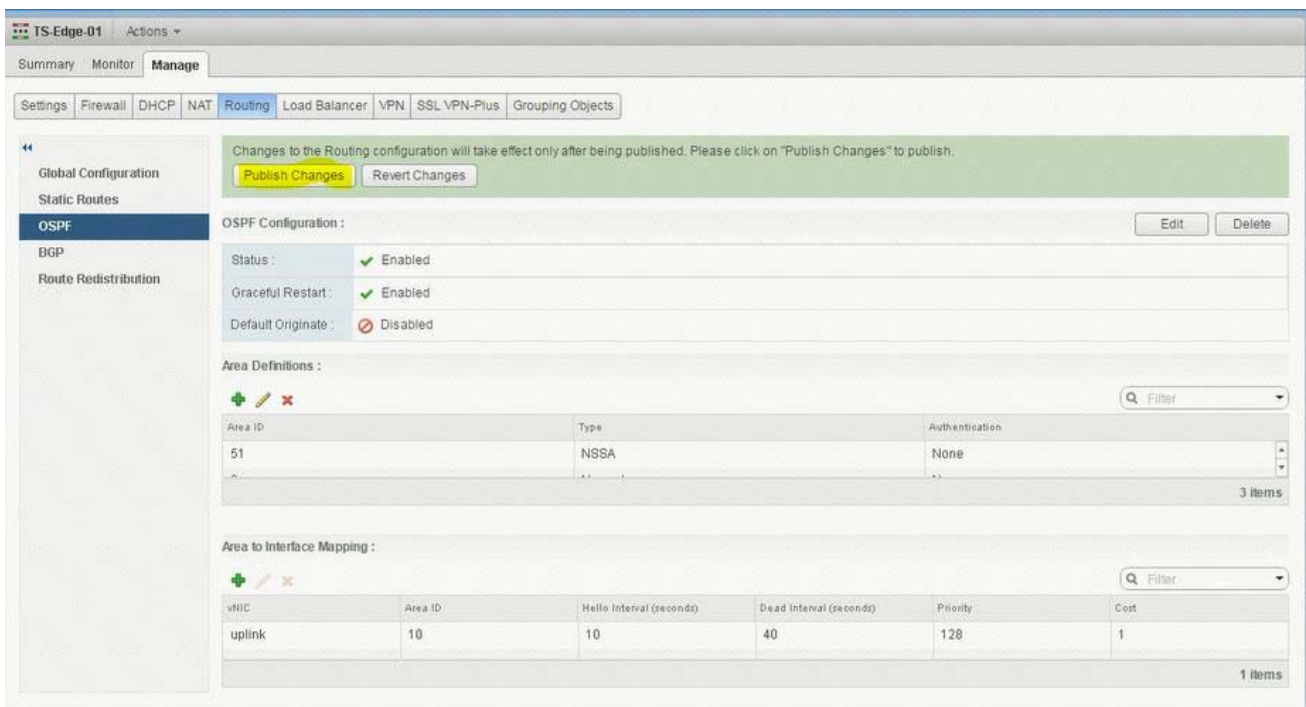
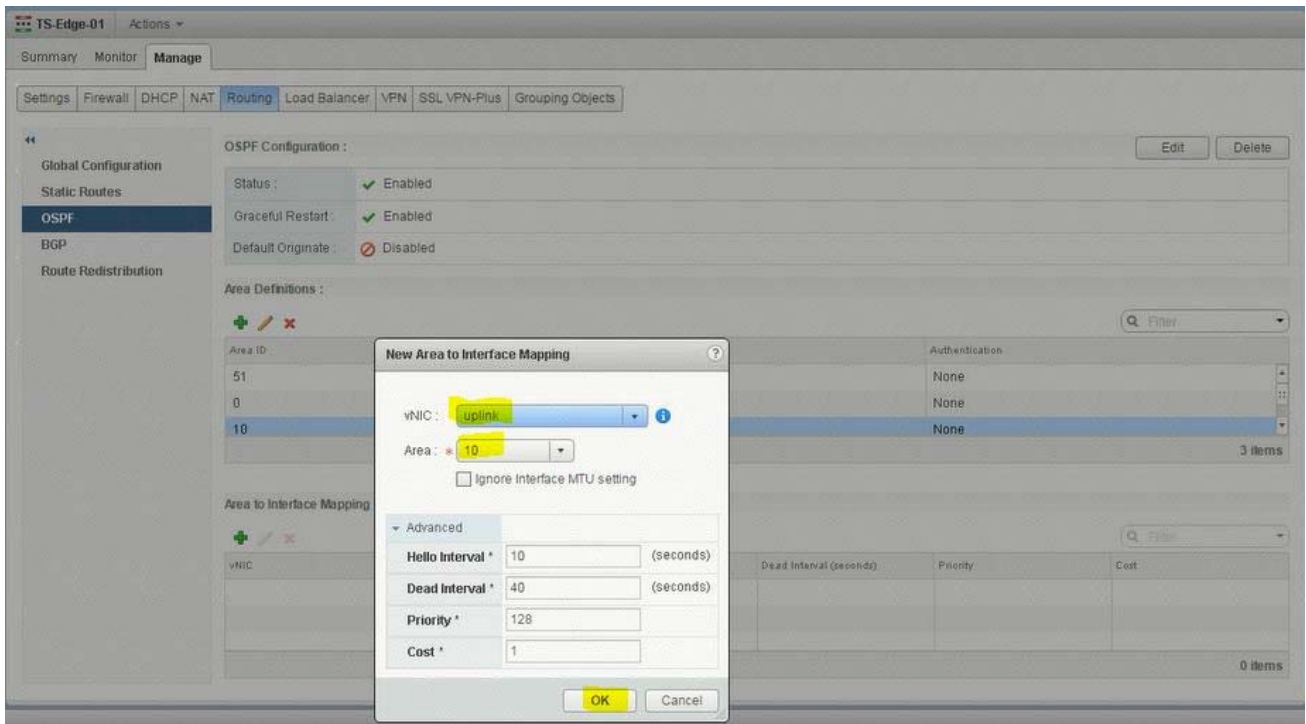
| Area ID | Type | Authentication |
|---------|--------|----------------|
| 51 | NSSA | None |
| 0 | Normal | None |
| 10 | Normal | None |

3 items

Area to Interface Mapping:

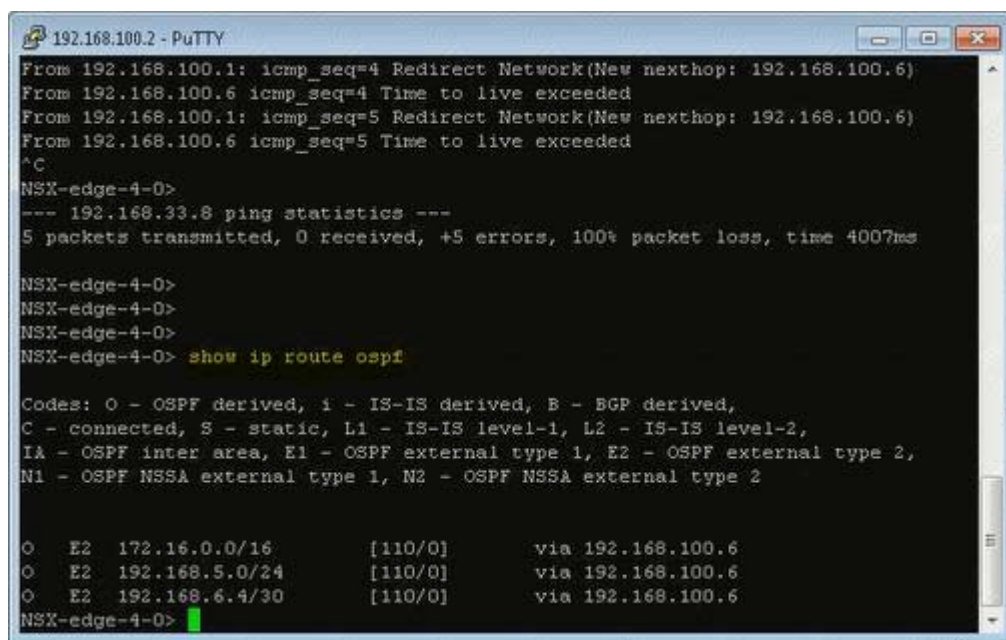
| vNIC | Area ID | Hello Interval (seconds) | Dead Interval (seconds) | Priority | Cost |
|------|---------|--------------------------|-------------------------|----------|------|
|------|---------|--------------------------|-------------------------|----------|------|

0 items



open putty. enter ip address 192.168.100.202.

enter command show ip route ospf. copy the ouput and save in a text file name TS-Edge-01.txt.



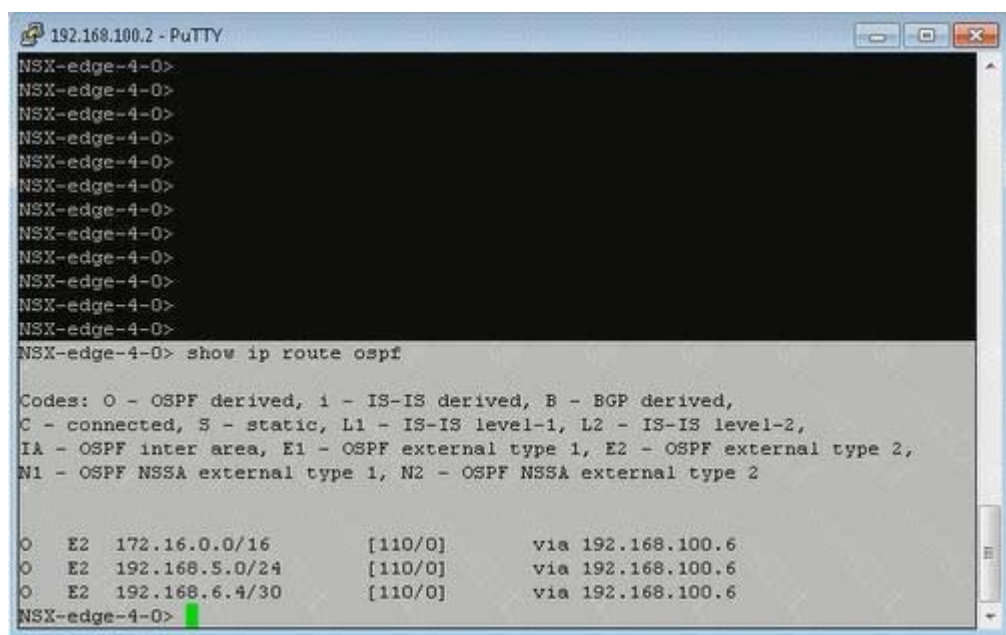
```
192.168.100.2 - PuTTY
From 192.168.100.1: icmp_seq=4 Redirect Network(New nexthop: 192.168.100.6)
From 192.168.100.6 icmp_seq=4 Time to live exceeded
From 192.168.100.1: icmp_seq=5 Redirect Network(New nexthop: 192.168.100.6)
From 192.168.100.6 icmp_seq=5 Time to live exceeded
^C
NSX-edge-4-0>
--- 192.168.33.8 ping statistics ---
5 packets transmitted, 0 received, +5 errors, 100% packet loss, time 4007ms

NSX-edge-4-0>
NSX-edge-4-0>
NSX-edge-4-0>
NSX-edge-4-0> show ip route ospf

Codes: O - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

O E2 172.16.0.0/16 [110/0] via 192.168.100.6
O E2 192.168.5.0/24 [110/0] via 192.168.100.6
O E2 192.168.6.4/30 [110/0] via 192.168.100.6
NSX-edge-4-0>
```

Copy and save OSPF route table in notepad.



```
192.168.100.2 - PuTTY
NSX-edge-4-0>
NSX-edge-4-0>
NSX-edge-4-0>
NSX-edge-4-0>
NSX-edge-4-0>
NSX-edge-4-0>
NSX-edge-4-0>
NSX-edge-4-0>
NSX-edge-4-0>
NSX-edge-4-0>
NSX-edge-4-0>
NSX-edge-4-0>
NSX-edge-4-0>
NSX-edge-4-0> show ip route ospf

Codes: O - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

O E2 172.16.0.0/16 [110/0] via 192.168.100.6
O E2 192.168.5.0/24 [110/0] via 192.168.100.6
O E2 192.168.6.4/30 [110/0] via 192.168.100.6
NSX-edge-4-0>
```