VMware vCloud® Architecture Toolkit™
for Service Providers

VMware vCloud Networking and Security™ Upgrade to VMware NSX® in VMware vCloud Director® Environments

Version 2.9

January 2018

Tomas Fojta

VMware, Inc.
3401 Hillview Ave
Palo Alto, CA 94304
www.vmware.com

Contents

List of Tables

List of Figures

Introduction

VMware vCloud Director® relies on VMware vCloud® Networking and Security™ or VMware NSX® for vSphere® to provide abstraction of the networking services. Until now, both platforms could be used interchangeably because they both provide the same APIs that vCloud Director uses to provide networks and networking services.

The vCloud Networking and Security platform end-of-support (EOS) date is 19 September 2016. Only NSX for vSphere will be supported with vCloud Director after the vCloud Networking and Security end-of-support date.

To secure the highest level of support and compatibility going forward, migrate from vCloud Networking and Security to NSX for vSphere. This document provides guidance and considerations to simplify the process and to understand the impact of changes to the environment.

NSX for vSphere provides a smooth, in-place upgrade from vCloud Networking and Security. The upgrade process is documented in the corresponding VMware NSX Upgrade Guides (versions 6.0[1], v6.1[2], 6.2[3]). This document is not meant to replace these guides. Instead, it augments them with specific information that applies to the usage of vCloud Director in service provider environments.

[1] http://pubs.vmware.com/NSX-6/topic/com.vmware.ICbase/PDF/nsx_6_install.pdf

[2] http://pubs.vmware.com/NSX-61/topic/com.vmware.ICbase/PDF/nsx_61_install.pdf

[3] http://pubs.vmware.com/NSX-62/topic/com.vmware.nsx.upgrade.doc/GUID-4613AC10-BC73-4404-AF80-26E924EF5FE0.html

Interoperability and Upgrade Path

VMware provides solution interoperability and upgrade path matrixes[4] that list verified and supported product combinations. These matrixes are updated frequently as new product versions are released. Therefore, refer to the matrixes before the actual migration planning.

2.1 Solution Interoperability

The following figure highlights key constraints and considerations that are valid at the time of this writing. The key consideration focuses on vCloud Director support of the underlying networking platform releases.

Figure 1. vCloud Director to vCloud Networking and Security and VMware NSX Interoperability

VMware vCloud Director	8.10	8.0.1	8.0	5.6.5	5.6.4	5.6.3	5.5.6	5.5.5	5.5.4	5.5.3	5.5.2	5.5.1	5.5	5.1.3	5.1.2	5.1.1	5.1
VMware NSX 6.2.3	✓	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
VMware NSX 6.2.2	✓	✓	✓	—	—	—	✓	—	—	—	—	—	—	—	—	—	—
VMware NSX 6.2.1	—	✓	✓	—	—	—	—	—	—	—	—	—	—	—	—	—	—
VMware NSX 6.2	—	—	✓	—	—	—	—	—	—	—	—	—	—	—	—	—	—
VMware NSX 6.1.7	✓	✓	—	—	—	—	✓	✓	✓	—	—	—	—	—	—	—	—
VMware NSX 6.1.6	✓	✓	—	—	—	—	✓	✓	✓	—	—	—	—	—	—	—	—
VMware NSX 6.1.5	✓	✓	✓	✓	—	—	✓	✓	—	—	—	—	—	—	—	—	—
VMware NSX 6.1.4	—	✓	✓	✓	✓	—	✓	✓	✓	✓	—	—	—	—	—	—	—
VMware NSX 6.1.3	—	—	—	—	—	—	✓	✓	✓	✓	—	—	—	—	—	—	—
VMware NSX 6.1.2	—	✓	✓	✓	✓	—	✓	✓	✓	✓	✓	—	—	—	—	—	—
VMware NSX 6.1.1	—	—	✓	—	—	—	—	—	—	—	—	—	—	—	—	—	—
VMware NSX 6.0.7	—	—	✓	✓	✓	✓	—	—	—	—	—	—	—	—	—	—	—
VMware NSX 6.0.5	—	—	—	—	—	—	—	—	—	✓	✓	✓	✓	—	—	—	—
VMware NSX 6.0.4	—	—	—	—	—	—	—	—	—	✓	✓	✓	✓	—	—	—	—
VMware NSX 6.0.3	—	—	—	—	—	—	—	—	—	✓	✓	✓	✓	—	—	—	—
VMware NSX 6.0.2	—	—	—	—	—	—	—	—	—	✓	✓	✓	✓	—	—	—	—
VMware NSX 6.0.1	—	—	—	—	—	—	—	—	—	✓	✓	✓	✓	—	—	—	—
VMware NSX 6.0	—	—	—	—	—	—	—	—	—	✓	✓	✓	✓	—	—	—	—
vCloud Networking and Security 5.5.4	—	✓	✓	✓	—	—	✓	✓	✓	✓	—	—	—	—	—	—	—
vCloud Networking and Security 5.5.3	—	—	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	—	—	—	—	—
vCloud Networking and Security 5.5.2	—	—	—	—	—	—	✓	✓	—	✓	✓	✓	✓	—	—	—	—
vCloud Networking and Security 5.5.1	—	—	—	—	—	—	✓	✓	—	✓	✓	✓	✓	—	—	—	—
vCloud Networking and Security 5.5	—	—	—	—	—	—	✓	✓	—	✓	✓	✓	✓	—	—	—	—
vCloud Networking and Security 5.1.4	—	—	—	—	—	—	—	—	—	—	—	—	—	✓	✓	—	—
vCloud Networking and Security 5.1.3	—	—	—	—	—	—	—	—	—	—	—	—	—	✓	✓	✓	✓
vCloud Networking and Security 5.1.2	—	—	—	—	—	—	—	—	—	—	—	—	—	✓	✓	✓	✓
vCloud Networking and Security 5.1.1	—	—	—	—	—	—	—	—	—	—	—	—	—	✓	✓	✓	✓
vCloud Networking and Security 5.1	—	—	—	—	—	—	—	—	—	—	—	—	—	✓	✓	✓	✓

[4] http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php

Note vCloud Director 8.10 supports only VMware NSX and is not compatible with vCloud Networking and Security. This means migration from vCloud Networking and Security to VMware NSX must be done while running a vCloud Director version earlier than 8.10. The network platform version is stored in vCloud database and checked during a vCloud Director 8.10 upgrade.

There are also other solution interoperability constraints based on service provider environments. For example, while VMware NSX provides backward compatibility for VMware vShield™ APIs (so that most of the tools using these APIs still function), service providers are encouraged to verify support prior to their actual production upgrade.

These tools might include custom network monitoring or metering solutions. For example, VMware vCenter® Chargeback Manager™ collects network transfer data through the VMware vShield Manager™ Data Collector that uses a vShield API.

Note At the time of writing this document, the most recent version of vCenter Chargeback Manager, version 2.7.1, is not supported with vSphere 6 and vCloud Director 8.10.

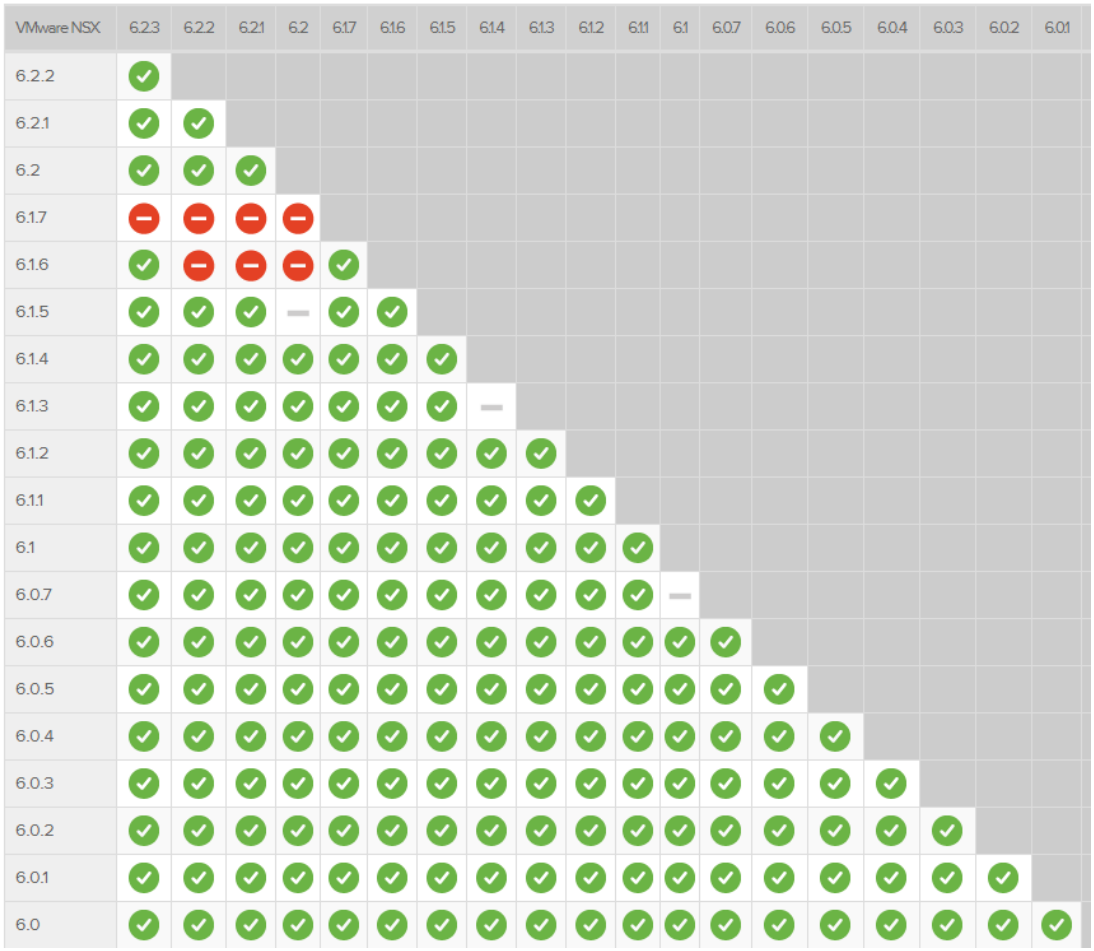
Figure 2. vCloud Director to vCenter Chargeback Interoperability

VMware vCloud Director	8.10	8.0.1	8.0	5.6.5	5.6.4	5.6.3	5.5.6	5.5.5	5.5.4	5.5.3	5.5.2	5.5.1	5.5
VMware vCenter Chargeback 2.7.1	⊖	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
VMware vCenter Chargeback 2.7	–	–	–	✓	✓	✓	✓	✓	✓	–	–	–	–
VMware vCenter Chargeback 2.6	–	–	–	–	–	–	–	–	–	✓	✓	✓	✓
VMware vCenter Chargeback 2.5.1	–	–	–	–	–	–	–	–	–	–	–	✓	✓

2.2 Upgrade Paths

In general, the upgrade from vCloud Networking and Security to NSX for vSphere is achieved by upgrading vShield Manager with a special *VMware-vShield-Manager-Upgrade-bundle-to-NSX* upgrade bundle. Currently this upgrade bundle is available for all NSX for vSphere releases, except 6.2.1. VMware recommends upgrading to the highest supported VMware NSX version based on the various solutions and tools incorporated in the service provider environment (vCloud Director, vSphere, and so on).

Figure 3. VMware NSX Upgrade Paths



VMware NSX	6.2.3	6.2.2	6.2.1	6.2	6.1.7	6.1.6	6.1.5	6.1.4	6.1.3	6.1.2	6.1.1	6.1	6.0.7	6.0.6	6.0.5	6.0.4	6.0.3	6.0.2	6.0.1
6.2.2	✓																		
6.2.1	✓	✓																	
6.2	✓	✓	✓																
6.1.7	⊖	⊖	⊖	⊖															
6.1.6	✓	⊖	⊖	⊖	✓														
6.1.5	✓	✓	✓	—	✓	✓													
6.1.4	✓	✓	✓	✓	✓	✓	✓												
6.1.3	✓	✓	✓	✓	✓	✓	✓	—											
6.1.2	✓	✓	✓	✓	✓	✓	✓	✓	✓										
6.1.1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓									
6.1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓								
6.0.7	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	—							
6.0.6	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓						
6.0.5	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓					
6.0.4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				
6.0.3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			
6.0.2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
6.0.1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
6.0	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Figure 4. vCloud Director Upgrade Paths

VMware vCloud Director	8.10	8.0.1	8.0	5.6.5	5.6.4	5.6.3	5.5.6	5.5.5	5.5.4	5.5.3	5.5.2	5.5.1
8.0.1	✓											
8.0	—	✓										
5.6.5	✓	✓	—									
5.6.4	—	✓	✓	✓								
5.6.3	—	—	—	✓	✓							
5.5.5	—	✓	—	—	—	—	✓					
5.5.4	—	✓	✓	—	—	—	✓	✓				
5.5.3	—	—	—	—	—	—	✓	✓	✓			
5.5.2	—	—	—	✓	✓	—	✓	✓	✓	✓		
5.5.1	—	—	—	—	—	✓	✓	✓	✓	✓	✓	
5.5	—	—	—	—	—	—	✓	✓	✓	✓	✓	✓

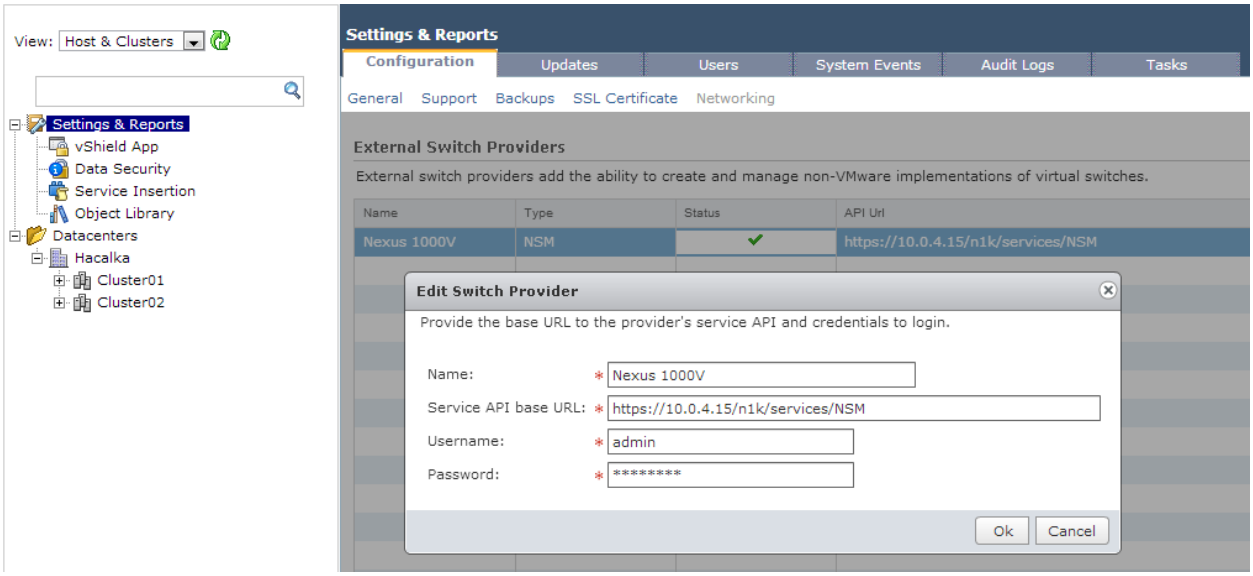
Impact of Network Virtualization Technology

vCloud Director currently supports various network virtualization technologies, some of which are legacy technologies that are no longer recommended going forward. The most scalable recommended virtualization technology is Virtual Extensible LAN (VXLAN).

3.1 Cisco Nexus 1000V

vCloud Director supports the Cisco Nexus 1000V virtual distributed switch through the External Switch Provider feature of vShield Manager. The vShield API calls to deploy, manage, or delete virtual networks are then translated to Network Segmentation Manager APIs, which run on the Cisco Virtual Supervisor Module—the management component of Nexus 1000V switch. The logical networks can be VLAN-based or VXLAN-based.

Figure 5. vCloud Networking and Security Integration with External Switch Providers



This functionality is no longer supported with VMware NSX. In such cases, you must first migrate from Cisco Nexus 1000V to VMware vSphere Distributed Switch™ and then subsequently migrate to VMware NSX.

The actual migration steps are out of scope for this document.

3.2 vCloud Director Network Isolation (VCDNI)

Before VXLAN gained mass adoption, vCloud Director relied on vCloud network isolation technology to provide a logical network overlay. This MAC-in-MAC proprietary encapsulation technology is still supported, however, support for this technology is now deprecated. Unlike VXLAN logical networks, VCDNI logical networks are created directly by vCloud Director, which communicates with VMware ESXi™ hosts through the vCloud Agent running in the VMkernel. Therefore, a vCloud Networking and Security upgrade has no impact on VCDNI networks and there is no limitation of using them together with VMware NSX.

Service providers are, however, encouraged to use VXLAN technology because VCDNI is a deprecated technology and is supported only for legacy deployments. The migration steps from VCDNI to VXLAN are out of scope for this document.

Migration Considerations

4.1 Port Requirements

NSX for vSphere requires additional ports to be opened between various components of the service provider's solution. This is due to the new control plane mechanism as well as the management plane message bus.

Figure 6. VMware NSX Communication Requirements

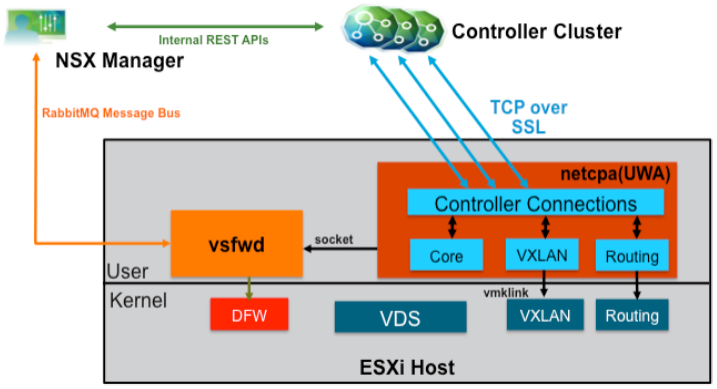


Table 1. Required Network Ports

Source	Target	Port	Protocol	Notes
ESXi Host	VMware NSX Manager™	5671	TCP	New requirement (RabbitMQ)
ESXi Host	VMware NSX Controller™	1234	TCP	New requirement (User World Agent)
NSX Manager	NSX Controller	443	TCP	New requirement
NSX Controller	NSX Controller	2878, 2888, 3888,7777, 30865	TCP	New requirement
NSX Manager	VMware vCenter Server®	443, 902	TCP	Same as vShield Manager
vCenter Server	NSX Manager	80	TCP	Same as vShield Manager
NSX Manager	ESXi Host	443, 902	TCP	Same as vShield Manager
NSX Manager	ESXi Host	8301, 8302	UDP	New requirement (DVS Sync)

Source	Target	Port	Protocol	Notes
ESXi Host	NSX Manager	8301, 8302	UDP	New requirement (DVS Sync)
ESXi Host	vCenter Server	80	TCP	Same as vShield Manager
vCenter Server	ESXi Host	80	TCP	Same as vShield Manager

Note Additional ports are needed for NTP (TCP 123), DNS (TCP 53), and Syslog (TCP 514).

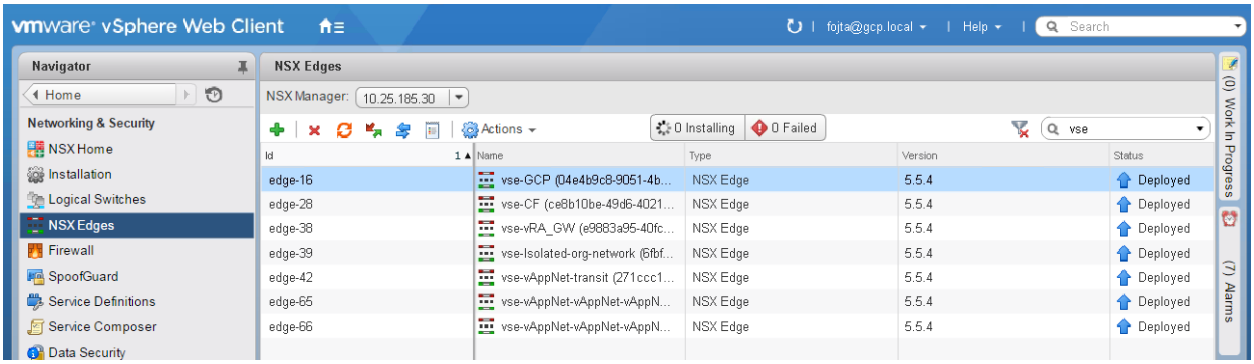
4.2 vCloud Director Legacy Edge Compatibility

There are changes in behavior between vCloud Director 8.10 and previous versions.

4.2.1 vCloud Director 8.0 and Earlier

In vCloud Director 8.0 and earlier versions, Organization VDC and vApp edge gateways are deployed in vShield (legacy) compatibility mode (NSX Edge version 5.5.4).

Figure 7. NSX Edge Nodes in Legacy Compatibility Mode



It is important in vCloud Director 8.0 and earlier not to upgrade legacy edge services gateways to VMware NSX version 6 because this will break vCloud Director compatibility. Older versions of vCloud Director 5.5.x and 5.6.x have a bug that results in an edge upgrade on vCloud Director redeploy action. To prevent this behavior, the following vCloud Director database change is necessary prior to vCloud Network and Security migration.

When upgrading to VMware NSX 6.2, add the following line to the *config* table in the vCloud Director SQL Server database:

```
INSERT INTO config (cat, name, value, sortorder) VALUES ('vcloud',
'networking.edge_version_for_vsm6.2', '5.5', 0);
```

Note Use `networking.edge_version_for_vsm6.1` if NSX 6.1 is used or `networking.edge_version_for_vsm6.0` if NSX 6.0 is used.

For more information, see the following VMware Knowledge Base articles: http://kb.vmware.com/kb/2096351 and http://kb.vmware.com/kb/2108913.

4.2.2 vCloud Director 8.10

In vCloud Director 8.10, edge gateways and vApp edges are deployed as full NSX Edge nodes (version 6.x) with the same feature set, accessible through the user interface or API, as legacy NSX Edge nodes.

vCloud Director 8.10 also supports legacy edges deployed before upgrade to vCloud Director 8.10. VMware recommends redeploying the old edges in vCloud Director or upgrading them in VMware NSX to leverage the more efficient message bus communication mode with NSX Manager as opposed to the legacy VIX API mode. If the NSX Edge nodes are upgraded directly in VMware NSX, verify that vCloud Director is still running because it needs to be notified about the NSX Edge version change.

The following PowerShell script shows how the VMware NSX API can be used to automate the upgrade of all NSX Edge nodes (shown for informational purposes only).

```
$Username = "admin"
$Password = "default"
$NSXManager = "nsx01.gcp.local"
$TargetVersion = "6.2.3"

### Create authorization string and store in $head
$auth =
[System.Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes($Username +
":" + $Password))
$head = @{"Authorization"="Basic $auth"}

##Get total number of edges
$Request = "https://$NSXManager/api/4.0/edges"
$r = Invoke-WebRequest -Uri ($Request+"?startIndex=0&pageSize=1") -Headers $head -
ContentType "application/xml" -ErrorAction:Stop
if ($r.StatusCode -eq "200") {Write-Host -BackgroundColor:Black -
ForegroundColor:Green Status: Connected to $NSXManager successfully.}
$TotalNumberOfEdges = ([xml]$r.content).pagedEdgeList.edgePage.pagingInfo.totalCount

##Get all edges
$r = Invoke-WebRequest -Uri ($Request+"?startIndex=0&pageSize="+$TotalNumberOfEdges)
-Headers $head -ContentType "application/xml" -ErrorAction:Stop
[xml]$rxml = $r.Content
$Edges = @()
foreach ($EdgeSummary in $rxml.pagedEdgeList.edgePage.edgeSummary)
{
$n = @{} | select Name, Id, Version
$n.Name = $edgeSummary.Name
$n.Id = $edgeSummary.objectId
$n.Version = $edgeSummary.appliancesSummary.vmVersion
$Edges += $n
}

##Upgrade all edges
foreach ($Edge in $Edges) {
       if ($Edge.Version -ne $TargetVersion) {
       ## Upgrade edge
       Write-Host "Upgrading Edge" $Edge.Name
       $Uri = "https://$NSXManager/api/4.0/edges"+"/"+$Edge.Id+"?action=upgrade"
       $r = Invoke-WebRequest -URI $Uri -Method Post -Headers $head -ContentType
"application/xml" -Body $sxml.OuterXML -ErrorAction:Stop
       }
       }
```

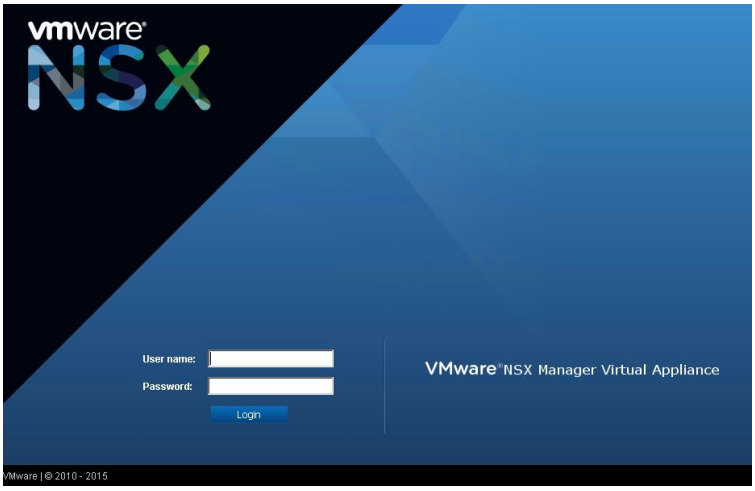
Note: The upgrade (or redeploy) of an NSX Edge gateway impacts network traffic for a short time.

4.3 Management

vCloud Networking and Security is managed from a user interface that is accessed through the vShield Manager appliance FQDN or through the VMware vSphere Client™ (the installable version). When vShield Manager is upgraded to NSX Manager, its user interface is used only for management of the appliance, while the VMware NSX management is performed from the VMware vSphere Web Client NSX plug-in.

The NSX Manager appliance user interface is accessed with a local account. This is the account used for accessing the vShield Manager CLI.

Figure 8. NSX Manager Appliance User Interface



The VMware NSX user interface in the vSphere Web Client (see Figure 10) is accessed with the VMware vCenter Single Sign-On™ user who has the necessary privileges in VMware NSX (see the following figure).

Figure 9. VMware vCenter Single Sign-On User Configured in VMware NSX

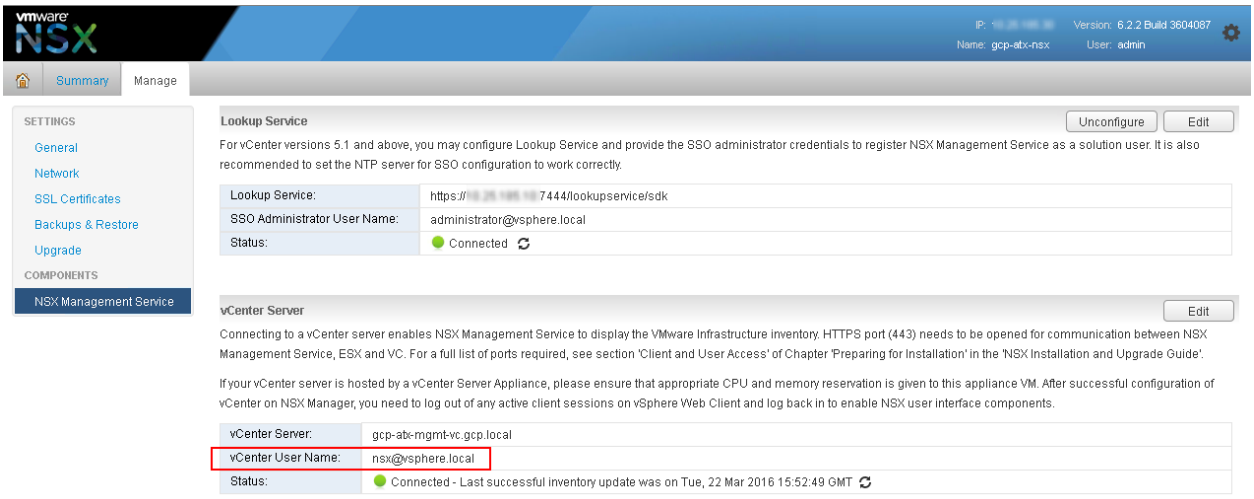
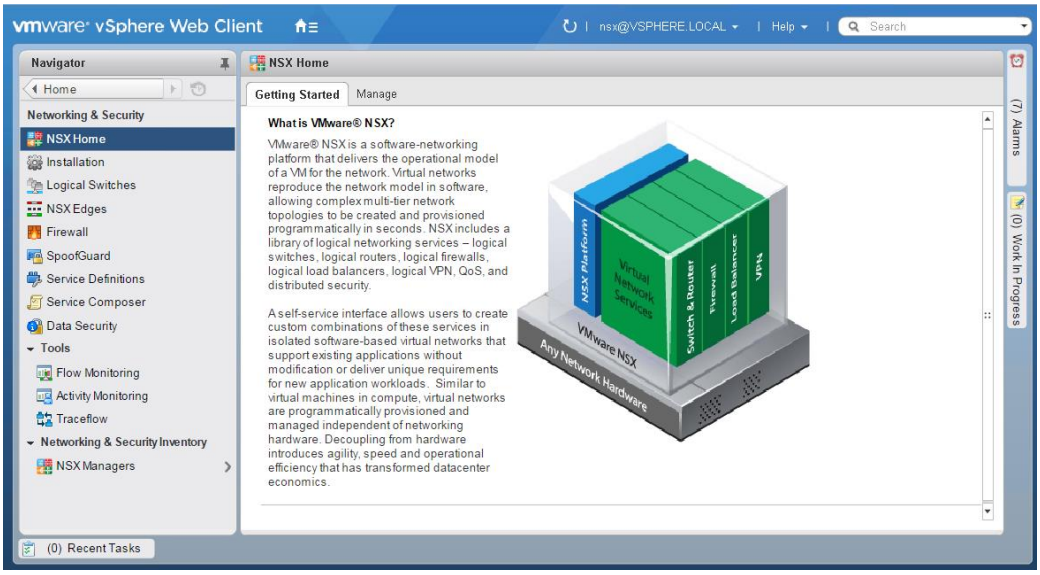


Figure 10. VMware NSX User Interface in vSphere Web Client



4.4 Licensing

VMware NSX uses a different license key than vCloud Networking and Security. After an upgrade of vShield Manager to NSX Manager, VMware NSX will run under a 60-day trial license. You must assign a VMware NSX license key in the vSphere Web Client.

4.5 NSX Controller Cluster

The NSX Controller cluster is a completely new component, which is deployed after successful NSX Manager migration. The cluster must be deployed before any of the advanced VMware NSX features that require it can be used.

Table 2. NSX Controller Cluster Requirements

NSX Feature	NSX Controller Cluster Requirement
VXLAN transport control plane	
• Multicast	✗
• Hybrid	✓
• Unicast	✓
Distributed firewall*	✗
NSX Edge services gateways	✗
Distributed Logical Router*	✓
VXLAN – VLAN bridging*	✓
ARP suppression	✓

*These features are not natively exposed through the vCloud Director user interface or API.

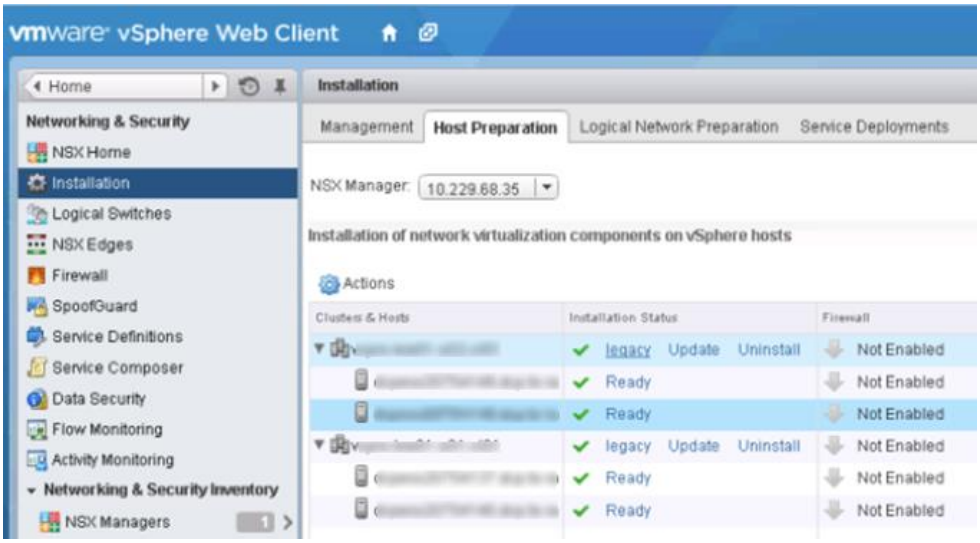
The following are NSX Controller cluster design considerations:

- The NSX Controller cluster consists of NSX Controller nodes, which are deployed by NSX Manager to the vSphere environment which the NSX Manager is paired with. Therefore, the NSX Controller is running in the resource group (customer workload) vSphere clusters.
- An NSX Controller cluster always consists of three nodes (virtual machines) deployed by NSX Manager.
- For high availability purposes, each NSX Controller node must be placed on a different host. This can be achieved with a manually-created, anti-affinity DRS rule within vSphere.
- The NSX Controller node VM must be connected to a standard or distributed port group. It cannot be connected to a VXLAN-based port group (logical switch).
- NSX Controller instances must have network connectivity to NSX Manager and ESXi management vmknics. They do not need to be deployed in the same L2 subnet or vSphere cluster.

4.6 VMware NSX VIB Upgrade

VMware NSX must replace the vShield VMkernel modules and install new VMware Installation Bundles (VIBs) on every vCloud Director managed ESXi host. This is done in the VMware NSX user interface by clicking **Update** next to each vSphere cluster.

Figure 11. VMware NSX VIB Upgrade



The upgrade of vShield or VMware NSX VIBs requires a reload of the new ESXi image and, therefore, a reboot of the ESXi host. VMware NSX automatically tries to put each host into maintenance mode and reboot it. This action, however, is not recommended in vCloud Director environments for two reasons:

- Before a host is put into a vSphere maintenance mode, disable it in vCloud Director so that vCloud Director does not try to schedule tasks on the host (for example, to perform image uploads).
- All workloads (not only running VMs) must be evacuated during the maintenance mode. A customer who decides to power on a VM or clone a VM that is registered to a rebooting (and temporarily unavailable) host would be otherwise impacted.

Therefore, VMware recommends the following steps instead:

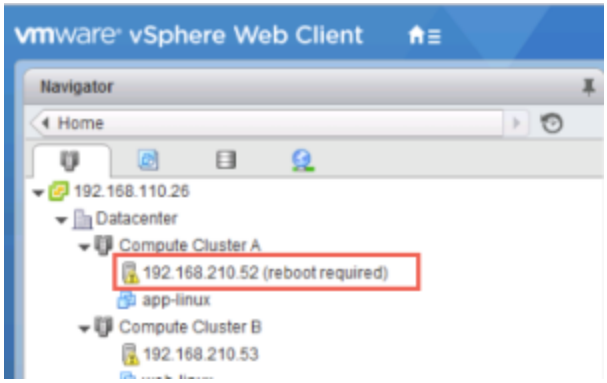
1. Before a VIB upgrade, change the VMware vSphere Distributed Resource Scheduler™ (DRS) automation mode to manual on each vSphere cluster to prevent VMware NSX from attempting to put hosts in maintenance mode.

Caution Do not disable DRS. Disabling DRS will delete your resource pools and corrupt your vCloud Director installation.

2. After the VIB installation finishes, change the DRS automation mode to the initial setting. In the VMware NSX user interface, hosts will be in the Not Ready state and will require a reboot in vSphere.

Figure 12. Not Ready State in VMware NSX User Interface

Figure 13. Reboot Required in vSphere



3. Make sure that each vSphere cluster has enough capacity to temporarily run without one host. (It is very common to have at least N+1 HA redundancy.)
4. Disable the host in vCloud Director.
5. Put the host into vSphere maintenance mode while evacuating all running, suspended, and powered-off VMs.
6. Reboot the host.
7. When the host comes up, exit the maintenance mode.
8. Enable the host in vCloud Director.
9. Repeat with other hosts.

Steps 4-9 can be easily automated and scripted, for example, with VMware vSphere PowerCLI™.

The following script is shown for informational purposes only.

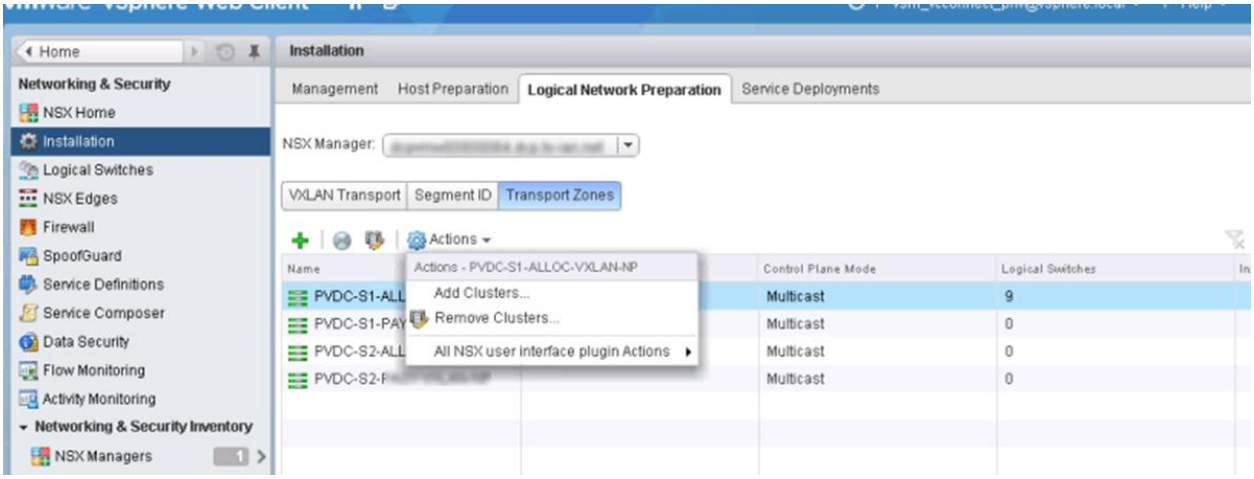
```
## Connect to vCloud Director and all vCenter Servers it manages
Connect-CIServer -Server vcloud.gcp.local -User Administrator -Password
VMware1!
Connect-VIServer -Server vcenter.gcp.local -User Administrator -Password
VMware1!

$ESXiHosts = Search-cloud -QueryType Host
foreach ($ESXiHost in $ESXiHosts) {
    $CloudHost = Get-CIView -SearchResult $ESXiHost
    Write-Host
    Write-Host "Working on host" $CloudHost.Name
    Write-Host "Disabling host in vCloud Director"
    $CloudHost.Disable()
    Write-Host "Evacuating host"
    Set-VMHost $CloudHost.Name -State Maintenance -Evacuate | Out-Null
    Write-Host "Rebooting host"
    Restart-VMHost $CloudHost.Name -Confirm:$false | Out-Null
    Write-Host -NoNewline "Waiting for host to come online "
    do {
        sleep 15
        $HostState = (get-vmhost $CloudHost.Name).ConnectionState
        Write-Host -NoNewline "."
    }
    while ($HostState -ne "NotResponding")
    do {
        sleep 15
        $HostState = (get-vmhost $CloudHost.Name).ConnectionState
        Write-Host -NoNewline "."
    }
    while ($HostState -ne "Maintenance")
    Write-Host
    Write-Host "Host rebooted"
    Set-VMHost $CloudHost.Name -State Connected | Out-Null
    Write-Host "Enabling Host in vCloud Director"
    $CloudHost.Enable()
}
```

4.7 Control Plane Mode

When the NSX Controller cluster is deployed, the multicast control plane mode can optionally be changed to unicast or hybrid modes to enable controller-based VXLAN overlays. The unicast control plane mode does not require multicast in the underlying network at all. Hybrid mode does not require multicast routing across L3 domains (PIM) but relies on multicast in each L2 switching domain.

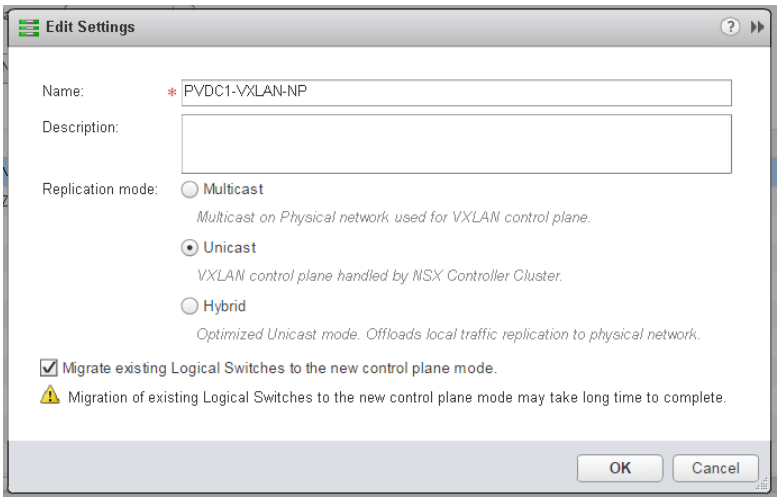
The change of the control plane mode is made in the VMware NSX user interface on the transport zones corresponding to each Provider Virtual Data Center (PVDC) VXLAN network pool. All existing logical switches (VXLAN logical networks) must be migrated to the new control plane mode as well.

Figure 14. Change of Transport Zone Control Plane Mode (1 of 2)



The change of control plane mode and migration of existing logical switches has no impact on the networking data plane traffic.

Figure 15. Change of Transport Zone Control Plane Mode (2 of 2)



4.8 VMware vShield App and VMware vShield Endpoint

vCloud Networking and Security offers a hypervisor-based firewall (VMware vShield App™) and antivirus and anti-malware platform (VMware vShield Endpoint™) for third-party virtual appliances. When upgrading to VMware NSX, these technologies are migrated to the VMware NSX Distributed Firewall and VMware NSX Guest Introspection.

Because neither of these two technologies is provided through vCloud Director, descriptions of the process for their migration are out of scope for this document. The VMware NSX Upgrade Guides provide a reference for the migration steps and describe the service impact.

Migration Scenario with Minimal Production Impact

The following scenario shows an example of a service provider migrating from vCloud Networking and Security, while at the same time upgrading to new versions of vCloud Director and vSphere. Impact on the duration of the maintenance window (and thus on end users) is also discussed.

Table 3. Solution Version Overview

Solution	Initial Version	Target Version
vCloud Director	5.6.4	8.10
vCloud Networking and Security / VMware NSX	vCloud Networking and Security 5.5.4	VMware NSX 6.2.2
vSphere (vCenter Server and ESXi)	5.5U2	6.0U2
vCenter Chargeback Manager	2.7	2.7.x[5]

The recommended path for the solution installation and upgrades is described in the following table together with the impact on the vCloud Director portal, the ability to manage vCloud Director objects through the vCloud UI/API, and the impact on customer's running workloads.

Table 4. Upgrade Scenario Steps

Step	Description	vCloud Director Portal Impact	Manageability Impact	Workload Impact
1.	Upgrade vCenter Chargeback Manager from 2.7 to 2.7.x.	None	None	None
2.	Upgrade vCloud Director from 5.6.4 to 8.0.1. This can be done as a rolling upgrade when only the last cell and database *configure* script actually requires vCloud Director downtime.	Yes (in minutes)	Yes (in minutes)	None
3.	Disable a specific vCenter Server instance in vCloud Director[6]. Then upgrade the related vShield Manager with the *VMware-vShield-Manager-Upgrade-bundle-to-NSX* upgrade bundle. After the upgrade is complete, enable the vCenter Server in vCloud Director.	None	Yes for the workloads managed by the specific vCenter Server (30-60 mins)	None

[5] At the time of this writing, vCenter Chargeback Manager is not compatible with vSphere 6.

[6] See *Disabled vCenter Server Continues to Accept vCloud Director Operations* (https://kb.vmware.com/kb/2145610) for important considerations.

Step	Description	vCloud Director Portal Impact	Manageability Impact	Workload Impact
4.	Repeat step 3 for all other vCenter Server instances managed by vCloud Director.			
5.	Deploy the NSX Controller cluster.	None	None	None
6.	Upgrade VMware NSX VIBs on all hosts (see Section 4.6).	None	None	None
7.	(Optional) Change the control plane mode and migrate all VXLAN networks.	None	None	None
8.	Disable a specific vCenter Server instance in vCloud Director[7]. Upgrade the vCenter Server from 5.5U2 to 6.0U2. When complete, enable the vCenter Server in vCloud Director.	None	Yes, for the workloads managed by the specific vCenter Server (30-60 mins)	None
9.	Repeat step 8 for all other vCenter Server instances managed by vCloud Director.			
10.	Upgrade each ESXi host. (Use a similar approach to that discussed in Section 4.6.)	None	None	None
11.	Upgrade vCloud Director from 8.0.1 to 8.10. This can be done as a rolling upgrade when only the last cell and database *configure* script actually requires vCloud Director downtime.	Yes (in minutes)	Yes (in minutes)	None
12.	(Optional) Upgrade all NSX Edge gateways to version 6.2.	None	None	A few seconds of network impact on each NSX Edge gateway

[7] See *Disabled vCenter Server Continues to Accept vCloud Director Operations* (https://kb.vmware.com/kb/2145610) for important considerations.

Reference Documents

Item	URL
VMware NSX 6.2 Upgrade Guide	http://pubs.vmware.com/NSX-62/index.jsp?topic=%2Fcom.vmware.nsx.upgrade.doc%2FGUID-C4A1FE0E-7319-494A-A776-BAD3D9208FDA.html
VMware NSX 6.1 Installation and Upgrade Guide	http://pubs.vmware.com/NSX-61/topic/com.vmware.ICbase/PDF/nsx_61_install.pdf
VMware NSX 6.0 Installation and Upgrade Guide	http://pubs.vmware.com/NSX-6/topic/com.vmware.ICbase/PDF/nsx_6_install.pdf
VMware Product Interoperability Matrixes	http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php
Architecting a VMware vCloud Director Solution for the VMware Cloud Provider™ Program	http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/vcat/vmware-architecting-a-vcloud-director-solution.pdf
VMware vCloud Architecture Toolkit for Service Providers (vCAT-SP)	http://www.vmware.com/solutions/cloud-computing/vcat-sp.html
vCloud Architecture Toolkit Blog	http://blogs.vmware.com/vcat/