VMware vCenter Server™ 6.0 Deployment Guide

TECHNICAL WHITE PAPER

V 1.0/FEBRUARY 2015/MIKE BROWN

Table of Contents

Introduction

The VMware vCenter Server™ 6.0 release introduces new, simplified deployment models. The components that make up a vCenter Server installation have been grouped into two types: *embedded* and *external*. Embedded refers to a deployment in which all components—this can but does not necessarily include the database—are installed on the same virtual machine. External refers to a deployment in which vCenter Server is installed on one virtual machine and the Platform Services Controller (PSC) is installed on another. The Platform Services Controller is new to vCenter Server 6.0 and comprises VMware vCenter™ Single Sign-On™, licensing, and the VMware Certificate Authority (VMCA).

Embedded installations are recommended for standalone environments in which there is only one vCenter Server system and replication to another Platform Services Controller is not required. If there is a need to replicate with other Platform Services Controllers or there is more than one vCenter Single Sign-On enabled solution, deploying the Platform Services Controller(s) on separate virtual machine(s)—via external deployment—from vCenter Server is required.

This paper defines the services installed as part of each deployment model, recommended deployment models (reference architectures), installation and upgrade instructions for each reference architecture, postdeployment steps, and certificate management in VMware vSphere 6.0.

VMware vCenter Server 6.0 Services

SERVICE	INSTALLED WITH
VMware AFD Service	vCenter Server and PSC
VMware Certificate Service	PSC
VMware Component Manager	vCenter Server and PSC
VMware Content Library Service	vCenter Server
VMware Directory Service	PSC
VMware ESX Agent Manager	vCenter Server
VMware HTTP Reverse Proxy	vCenter Server and PSC
VMware Identity Management Service	PSC
VMware vCenter Inventory Service	vCenter Server
VMware License Service	PSC
VMware Message Bus Configuration Service	vCenter Server
VMware Performance Charts	vCenter Server
VMware Postgres	vCenter Server (vCenter Server Appliance, Microsoft Windows if embedded database is chosen)
VMware Security Token Service	PSC
VMware Service Control Agent	vCenter Server and PSC
VMware Syslog Collector	vCenter Server
VMware System and Hardware Health Manager	vCenter Server
VMware vAPI Endpoint	vCenter Server

SERVICE	INSTALLED WITH
VMware vCenter Configuration Service	vCenter Server and PSC
VMware vCenter Workflow Manager	vCenter Server
VMware VirtualCenter Server	vCenter Server
VMware vService Manager	vCenter Server
VMware vSphere Auto Deploy Waiter	vCenter Server
VMware vSphere ESXi™ Dump Collector	vCenter Server
VMware vSphere ESXi Dump Collector Web Service	vCenter Server
VMware vSphere Profile-Driven Storage	vCenter Server
VMware vSphere Web Client	vCenter Server

Table 1. vCenter Server and Platform Services Controller Services

Requirements

General

A few requirements are common to both installing vCenter Server on Microsoft Windows and deploying VMware vCenter Server Appliance™. Ensure that all of these prerequisites are in place before proceeding with a new installation or an upgrade.

- DNS – Ensure that resolution is working for all system names via fully qualified domain name (FQDN), short name (host name), and IP address (reverse lookup).
- Time – Ensure that time is synchronized across the environment.
- Passwords – vCenter Single Sign-On passwords must contain only ASCII characters; non-ASCII and extended (or high) ASCII characters are not supported.

Windows Installation

Installing vCenter Server 6.0 on a Windows Server requires a Windows 2008 SP2 or higher 64-bit operating system (OS). Two options are presented: Use the local system account or use a Windows domain account. With a Windows domain account, ensure that it is a member of the local computer's administrator group and that it has been delegated the "Log on as a service" right and the "Act as part of the operating system" right. This option is not available when installing an external Platform Services Controller.

Windows installations can use either a supported external database or a local PostgreSQL database that is installed with vCenter Server and is limited to 20 hosts and 200 virtual machines. Supported external databases include Microsoft SQL Server 2008 R2, SQL Server 2012, SQL Server 2014, Oracle Database 11*g*, and Oracle Database 12*c*. When upgrading to vCenter Server 6.0, if SQL Server Express was used in the previous installation, it will be replaced with PostgreSQL. External databases require a 64-bit DSN. DSN aliases are not supported.

When upgrading vCenter Server to vCenter Server 6.0, only versions 5.0 and later are supported. If the vCenter Server system being upgraded is not version 5.0 or later, such an upgrade is required first.

Table 2 outlines minimum hardware requirements per deployment environment type and size when using an external database. If VMware vSphere Update Manager™ is installed on the same server, add 125GB of disk space and 4GB of RAM.

RESOURCES	TINY: UP TO 10 HOSTS/ 100 VIRTUAL MACHINES OR EXTERNAL PSC	SMALL: UP TO 100 HOSTS/ 1,000 VIRTUAL MACHINES	MEDIUM: UP TO 400 HOSTS/ 4,000 VIRTUAL MACHINES	LARGE: UP TO 1,000 HOSTS/ 10,000 VIRTUAL MACHINES
CPU	2	4	8	16
Memory	8GB	16GB	24GB	32GB
Disk Space	50GB 10GB (PSC)	100GB	100GB	100GB

Table 2. Minimum Hardware Requirements – Windows Installation

Appliance Deployment

vCenter Server Appliance can use either a local PostgreSQL database that is built in to the appliance, which is recommended, or an external database. Unlike Windows support for PostgreSQL, vCenter Server Appliance supports up to 1,000 hosts or 10,000 virtual machines at full vCenter Server scale. Supported external databases include Oracle Database 11*g* and Oracle Database 12*c*. External database support is being deprecated in this release; this is the last release that supports the use of an external database with vCenter Server Appliance.

When deploying vCenter Server Appliance, the target host must be ESXi 5.0 or later. In addition, prechecks such as connectivity to an external database, NTP server, DNS server, and so on, are performed on the client deploying the appliance rather than against the target host and destination port group. This does not ensure that all required connectivity is available from the ESXi host and the destination port group of vCenter Server Appliance. Users must ensure that the ESXi host and port group have the required connectivity.

Upgrading is possible only from versions 5.1 update 3 and later.

Table 3 outlines minimum hardware requirements per deployment environment type and size.

RESOURCES	TINY: UP TO 10 HOSTS/ 100 VIRTUAL MACHINES OR EXTERNAL PSC	SMALL: UP TO 100 HOSTS/ 1,000 VIRTUAL MACHINES	MEDIUM: UP TO 400 HOSTS/ 4,000 VIRTUAL MACHINES	LARGE: UP TO 1,000 HOSTS/ 10,000 VIRTUAL MACHINES
CPU	2	4	8	16
Memory	8GB	16GB	24GB	32GB
Disk Space (External PSC)	86GB (vCenter) 30GB (PSC)	106GB	245GB	295GB
Disk Space (Embedded PSC)	116GB	136GB	275GB	325GB

Table 3. Minimum Hardware Requirements – vCenter Server Appliance Deployment

Reference Architectures

We examine the following architectures in this deployment guide:

- Fresh embedded deployment
- Upgrade in which all vCenter Server components are installed on a single machine
- Fresh external deployments
- Upgrade with external vCenter Single Sign-On
- Fresh vCenter Single Sign-On high availability deployment
- Upgrade of vCenter Single Sign-On high availability

Fresh Embedded Deployment

A fresh, or new, embedded installation is the simplest of all the deployments. In this scenario, vCenter Server and the Platform Services Controller are deployed together onto a single virtual machine.

The vCenter Server database can be either local or remote. On the Windows platform, the local PostgreSQL database is limited to 20 hosts and 200 virtual machines.

Embedded installations are recommended for standalone environments in which there is only one vCenter Server and replication to another Platform Services Controller is not required. If there is a need to replicate with other Platform Services Controllers or there is more than one vCenter Single Sign-On enabled solution, deploying the Platform Services Controller(s) on separate virtual machine(s)—via external deployment—from vCenter Server is required.

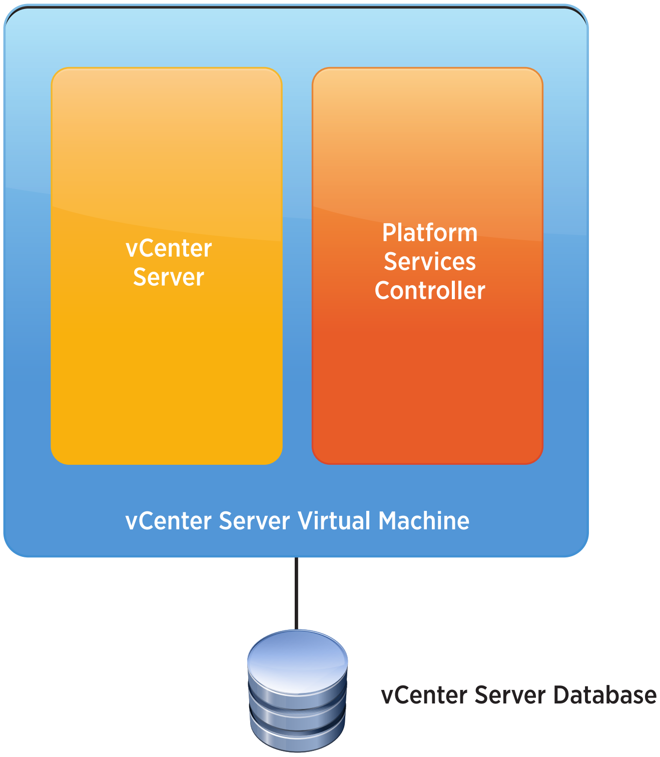


Figure 1. Embedded Architecture

Upgrade in Which All vCenter Server Components Are Installed on a Single Machine

Upgrading vCenter Server 5.0 or vCenter Server with vCenter Single Sign-On—that is, vCenter Server 5.1 or 5.5—installed on the same virtual machine can be accomplished using the embedded deployment method.

All vCenter Server components are upgraded. If upgrading from vCenter Server 5.0, an external Platform Services Controller can be installed or an embedded one can be used. vCenter Single Sign-On in vCenter Server 5.1 and 5.5 is upgraded to a Platform Services Controller. In all upgrade scenarios, all services listed in Table 1 are installed or upgraded.

The vCenter Server database is upgraded during vCenter Server upgrade. On Windows installations using the embedded SQL Server Express database, SQL Server Express is migrated to the PostgreSQL database during the upgrade.

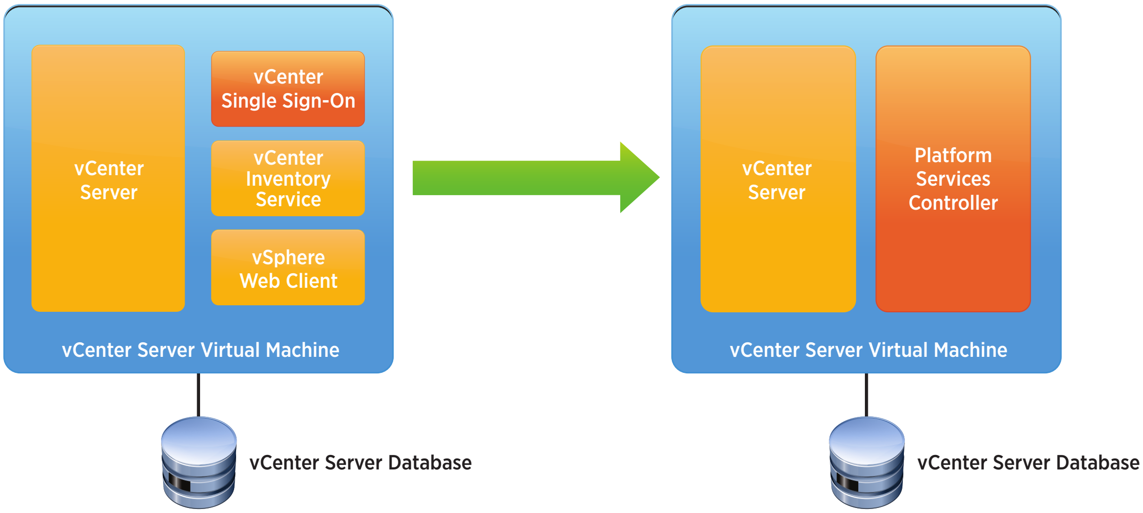


Figure 2. Upgraded Embedded Architecture

Fresh External Deployment

A fresh, or new, external deployment involves running the deployment wizard twice. The first time is to deploy the Platform Services Controller. After this successful deployment, vCenter Server is deployed.

The vCenter Server database can be either local or remote. On the Windows platform, the local PostgreSQL database is limited to 20 hosts and 200 virtual machines.

Deploying the Platform Services Controller externally is recommended for all but standalone vCenter Server systems.

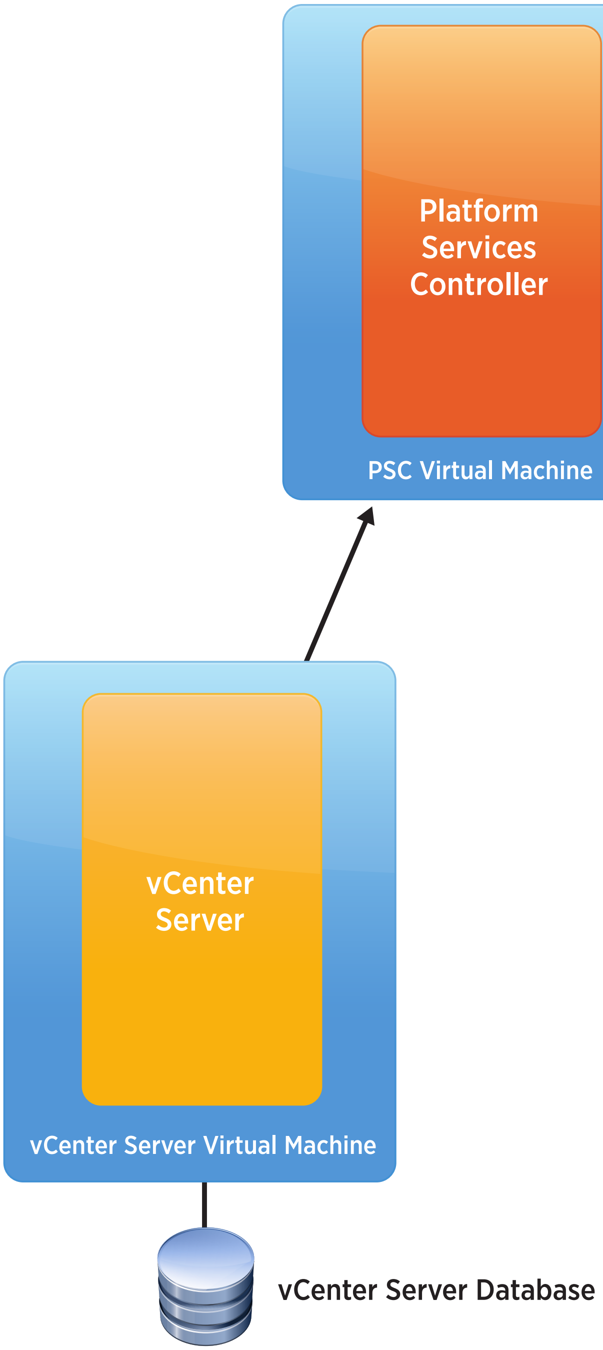


Figure 3. External Platform Services Controller Architecture

Upgrade External vCenter Single Sign-On

When upgrading from vCenter Server 5.1 or 5.5 and vCenter Single Sign-On is deployed externally from vCenter Server, vCenter Single Sign-On is first upgraded to a Platform Services Controller. After the Platform Services Controller has been deployed, the vCenter Server system can be upgraded.

The vCenter Server database is upgraded during the vCenter Server upgrade. In Windows installations using the embedded SQL Server Express database, SQL Server Express is migrated to the PostgreSQL database during the upgrade.

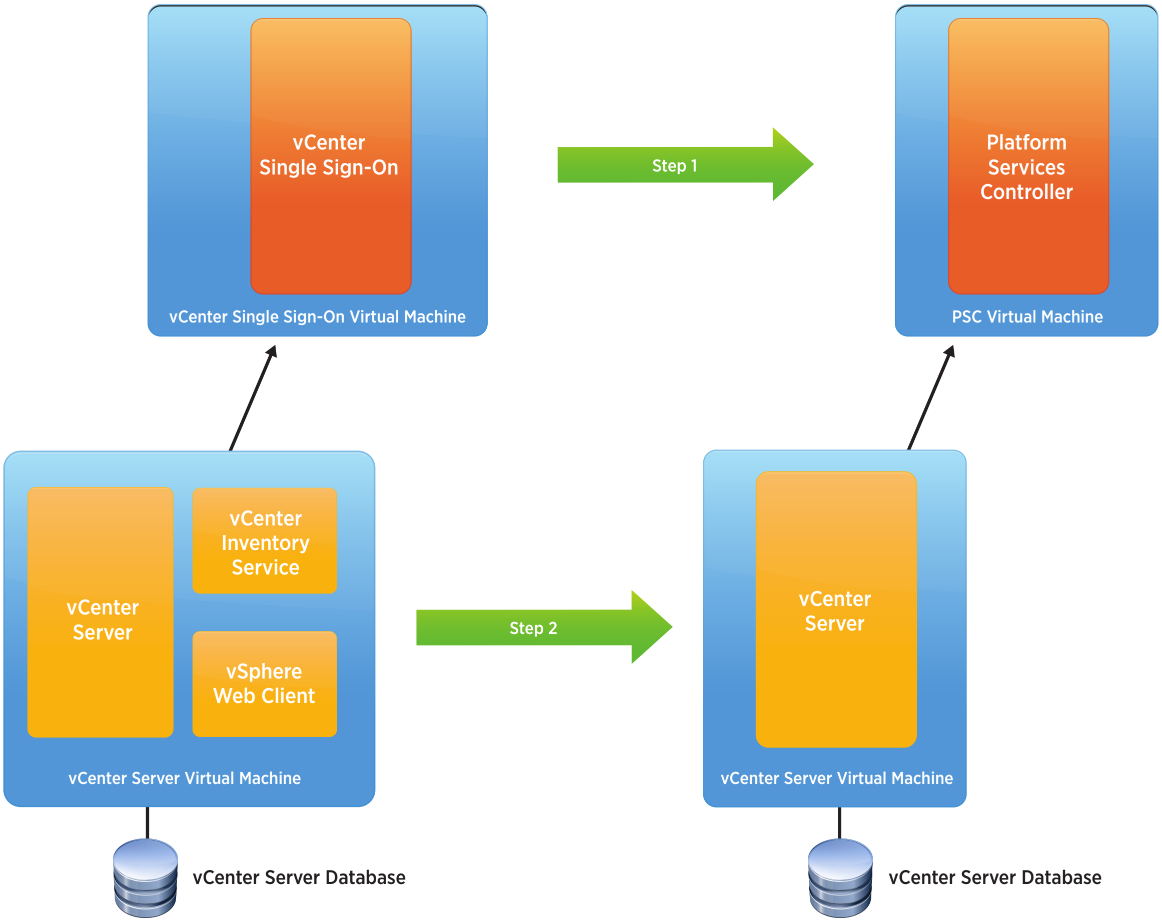

vCenter Single Sign-On
vCenter Single Sign-On Virtual Machine
Step 1
Platform Services Controller
PSC Virtual Machine
vCenter Server
vCenter Inventory Service
vSphere Web Client
vCenter Server Virtual Machine
Step 2
vCenter Server
vCenter Server Virtual Machine
vCenter Server Database
vCenter Server Database

Figure 4. Upgraded External Platform Services Controller Architecture

Fresh vCenter Single Sign-On High Availability Deployment

A fresh, or new, vCenter Single Sign-On high availability deployment is recommended when there are multiple vCenter Server systems or vCenter Single Sign-On enabled solutions that require a high level of uptime.

When deploying the Platform Services Controller externally for multiple services, availability of the Platform Services Controller must be considered. In some cases, simply having the Platform Services Controller located in a vSphere cluster with VMware vSphere High Availability enabled is sufficient. In other cases, having more than one Platform Services Controller deployed in a highly available architecture is recommended. This requires a network load balancer. In Figure 5, we examine redundant Platform Services Controllers behind a network load balancer.

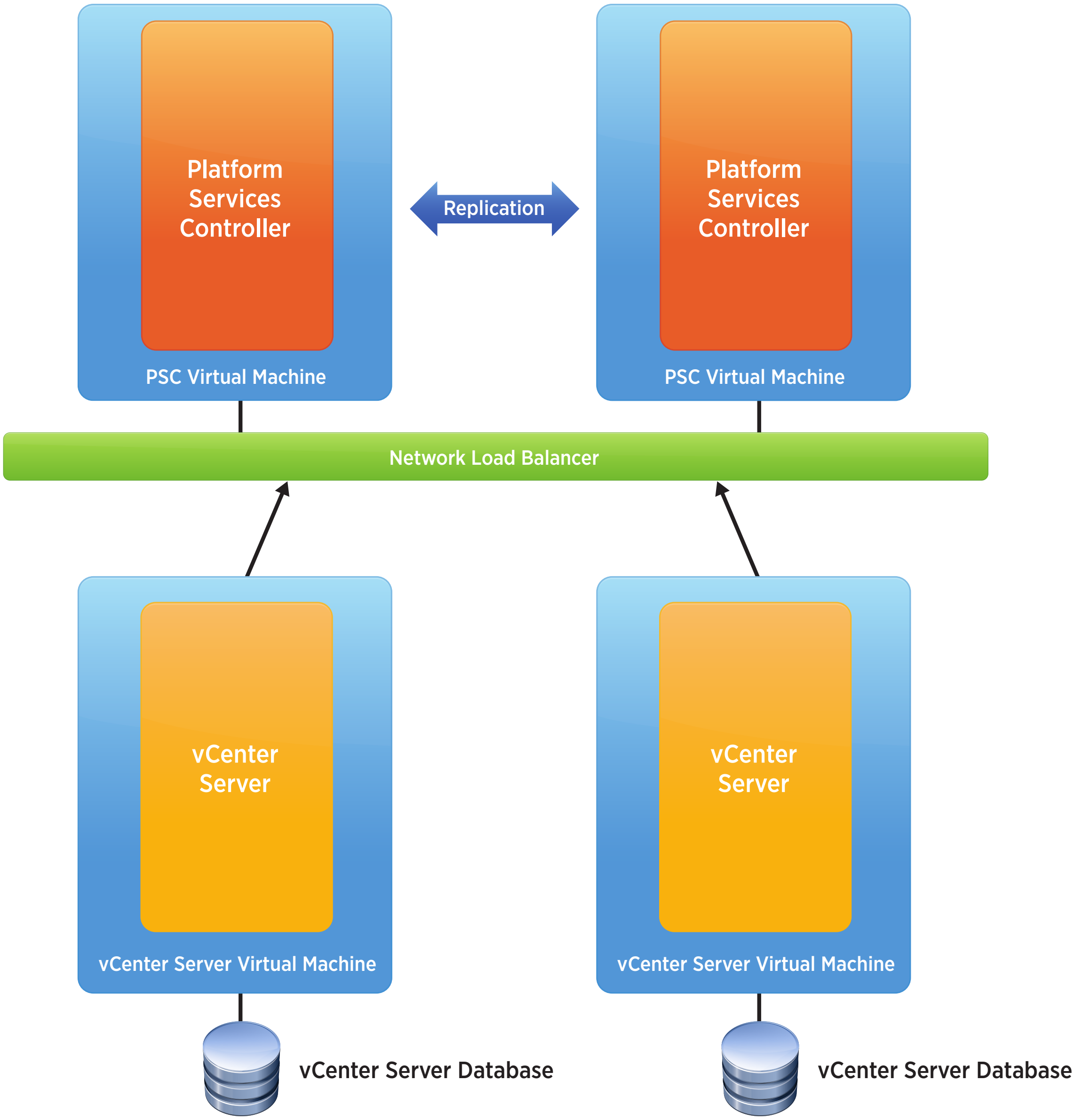


Figure 5. Highly Available Platform Services Controllers

Upgrade of vCenter Single Sign-On High Availability

Upgrading an existing vCenter Single Sign-On high availability deployment converts vCenter Single Sign-On servers to Platform Services Controllers. vCenter Single Sign-On 5.5 and previous versions do not work with vCenter Server 6.0, so upgrading vCenter Single Sign-On to Platform Services Controller is a prerequisite.

After the Platform Services Controllers are up and running, the load balancer rules must be adjusted to load-balance the Platform Services Controller ports before attempting to upgrade vCenter Server. Session affinity is required based on source address and must-span ports. If vCenter Server initiates communication to the Platform Services Controller on port 443 and is placed on the first Platform Services Controller, all subsequent requests must also go to the first Platform Services Controller.

Upgrading from vCenter Single Sign-On high availability has been tested and validated only when upgrading from vCenter Server 5.5 and when the vCenter Single Sign-On with network load balancer guide is followed to set up the vCenter Single Sign-On high availability environment.

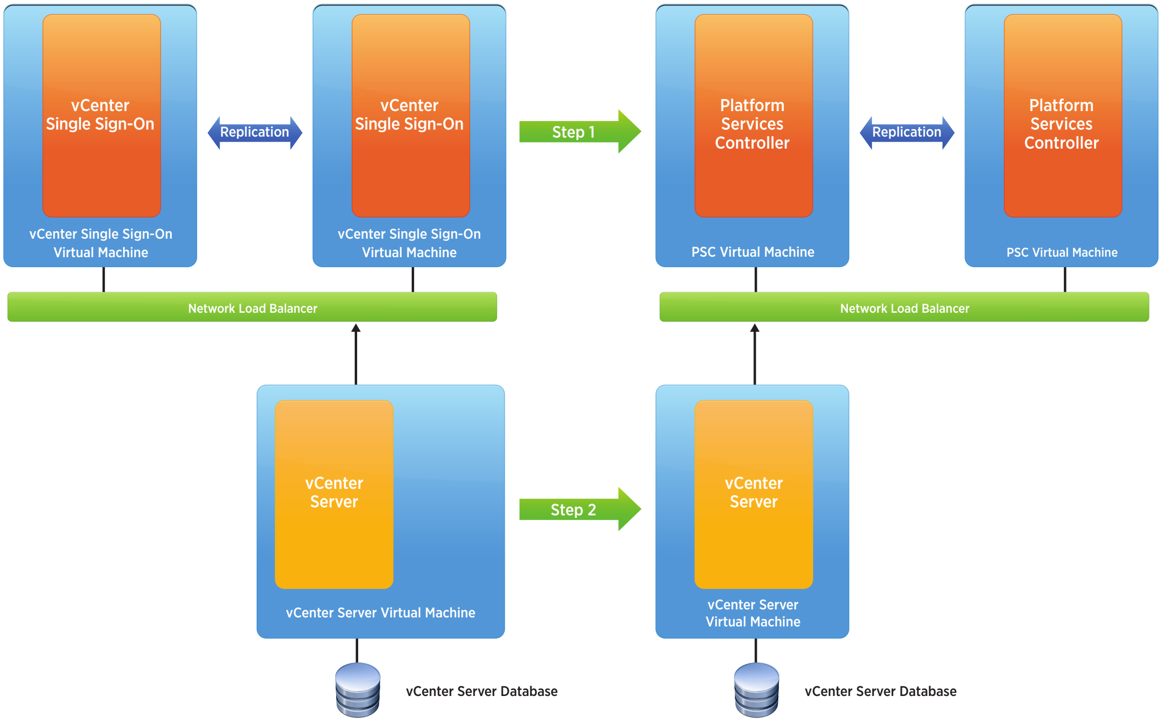


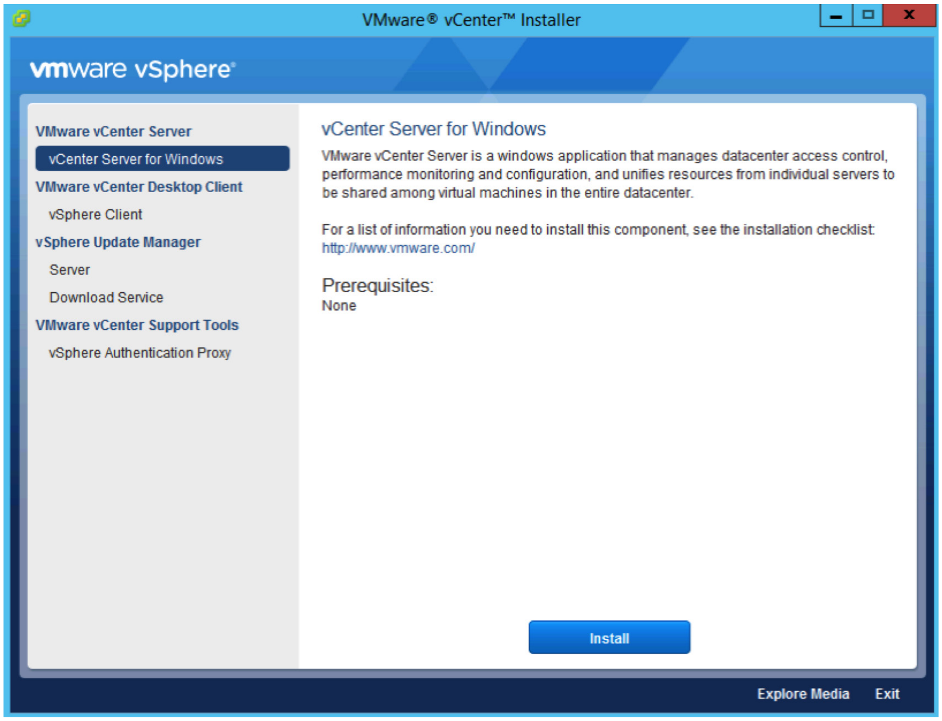
Figure 6. Upgrade of Highly Available Single Sign-On to Highly Available Platform Services Controller

Deploying vCenter Server 6.0

Fresh Embedded Deployment

Windows Deployment

1. Verify all prerequisites.
2. If using a remote database, ensure that a 64-bit DSN has been created. DSN aliases are not supported. This step is not necessary if using the local PostgreSQL database.
3. Mount the vCenter Server 6.0 ISO image.
4. If autorun does not start, execute autorun.exe.
5. Select **vCenter Server for Windows** and click **Install**.


VMware® vCenter™ Installer
vmware vSphere
VMware vCenter Server
vCenter Server for Windows
VMware vCenter Desktop Client
vSphere Client
vSphere Update Manager
Server
Download Service
VMware vCenter Support Tools
vSphere Authentication Proxy
Install
Explore Media
Exit

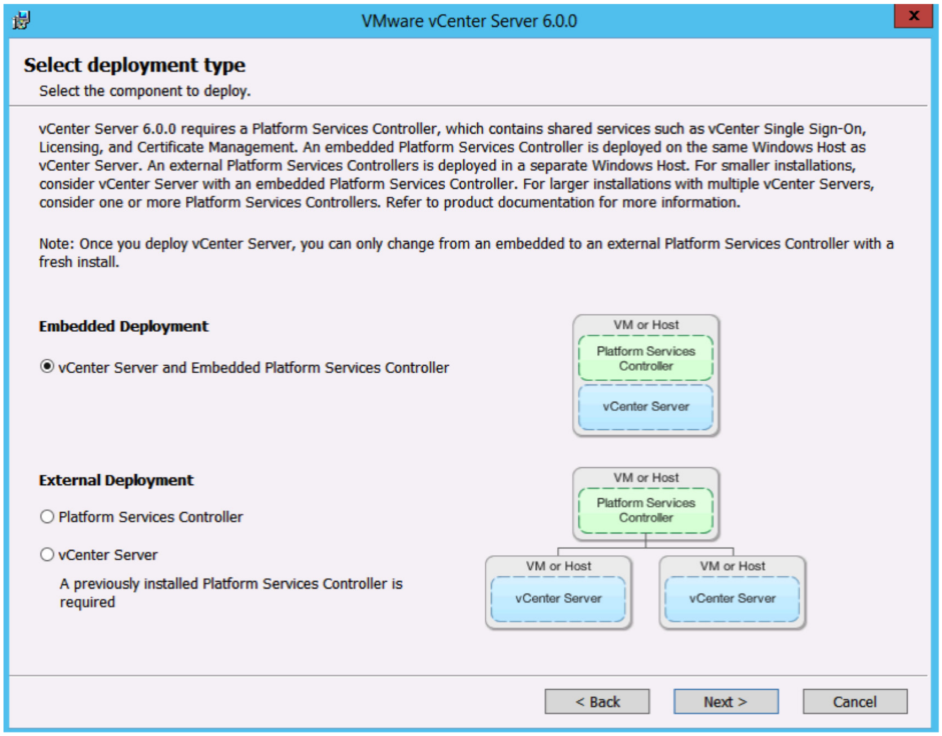
vCenter Server for Windows

VMware vCenter Server is a windows application that manages datacenter access control, performance monitoring and configuration, and unifies resources from individual servers to be shared among virtual machines in the entire datacenter.

For a list of information you need to install this component, see the installation checklist: http://www.vmware.com/

Prerequisites:
None

6. Click **Next**.
7. Accept the license agreements.
8. Select **Embedded Deployment** and click **Next**.



Select deployment type

Select the component to deploy.

vCenter Server 6.0.0 requires a Platform Services Controller, which contains shared services such as vCenter Single Sign-On, Licensing, and Certificate Management. An embedded Platform Services Controller is deployed on the same Windows Host as vCenter Server. An external Platform Services Controllers is deployed in a separate Windows Host. For smaller installations, consider vCenter Server with an embedded Platform Services Controller. For larger installations with multiple vCenter Servers, consider one or more Platform Services Controllers. Refer to product documentation for more information.

Note: Once you deploy vCenter Server, you can only change from an embedded to an external Platform Services Controller with a fresh install.

Embedded Deployment

● vCenter Server and Embedded Platform Services Controller

External Deployment

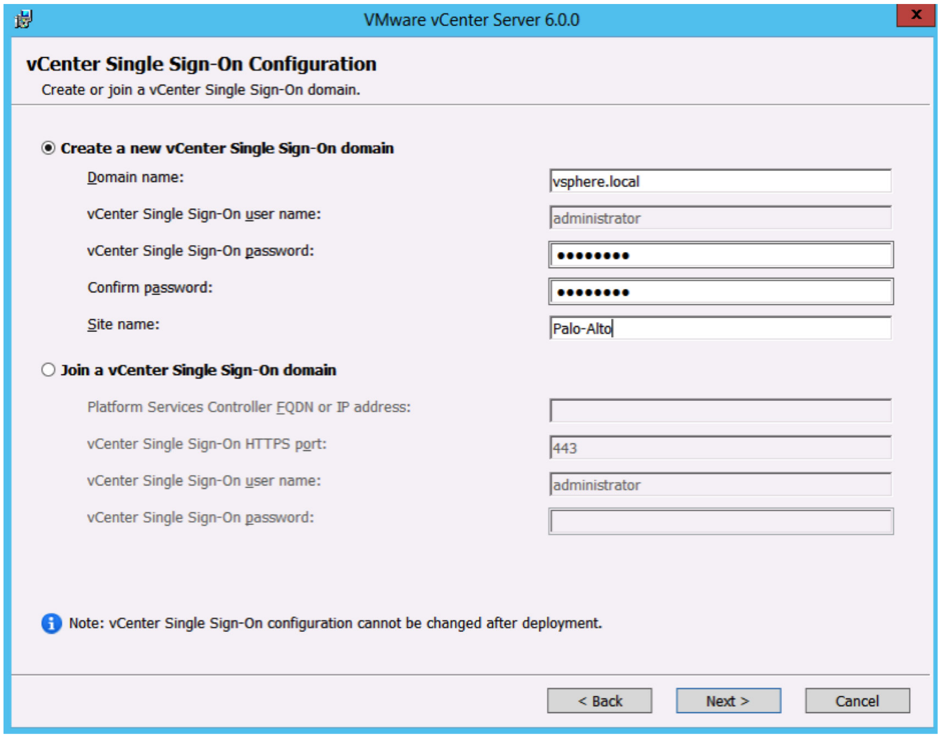
○ Platform Services Controller

○ vCenter Server

A previously installed Platform Services Controller is required

9. Verify that the FQDN is correct and click **Next**.

10. Enter a **password** and **Site name** for vCenter Single Sign-On and click **Next**.



vCenter Single Sign-On Configuration

Create or join a vCenter Single Sign-On domain.

● **Create a new vCenter Single Sign-On domain**

Domain name: vsphere.local

vCenter Single Sign-On user name: administrator

vCenter Single Sign-On password: ••••••••

Confirm password: ••••••••

Site name: Palo-Alto

○ **Join a vCenter Single Sign-On domain**

Platform Services Controller FQDN or IP address:

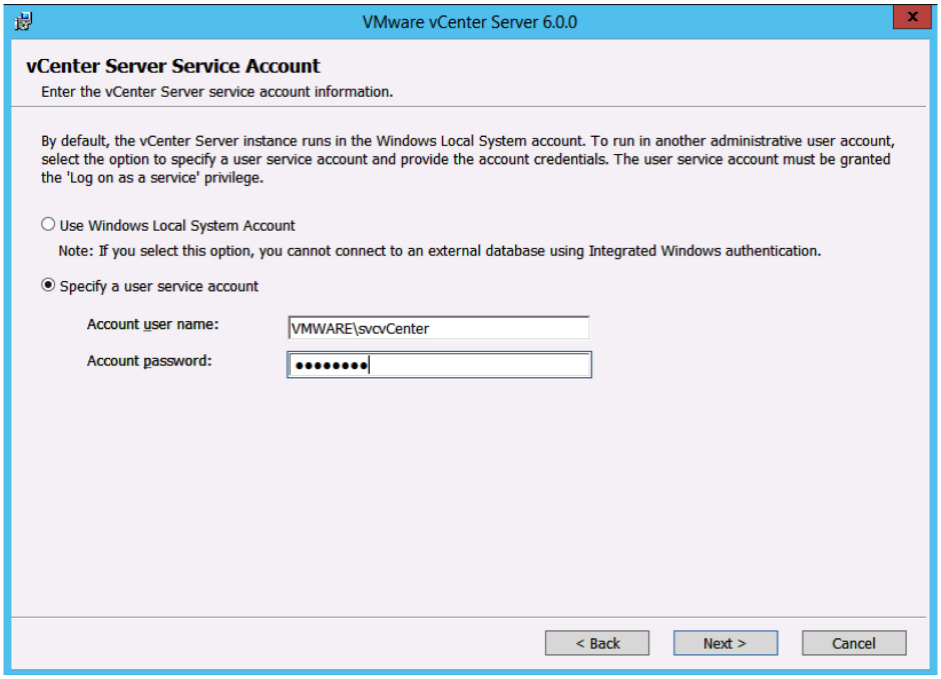
vCenter Single Sign-On HTTPS port: 443

vCenter Single Sign-On user name: administrator

vCenter Single Sign-On password:

Note: vCenter Single Sign-On configuration cannot be changed after deployment.

11. Select the local system account or enter the service account **user name** and **password**.



VMware vCenter Server 6.0.0

vCenter Server Service Account

Enter the vCenter Server service account information.

By default, the vCenter Server instance runs in the Windows Local System account. To run in another administrative user account, select the option to specify a user service account and provide the account credentials. The user service account must be granted the 'Log on as a service' privilege.

○ Use Windows Local System Account

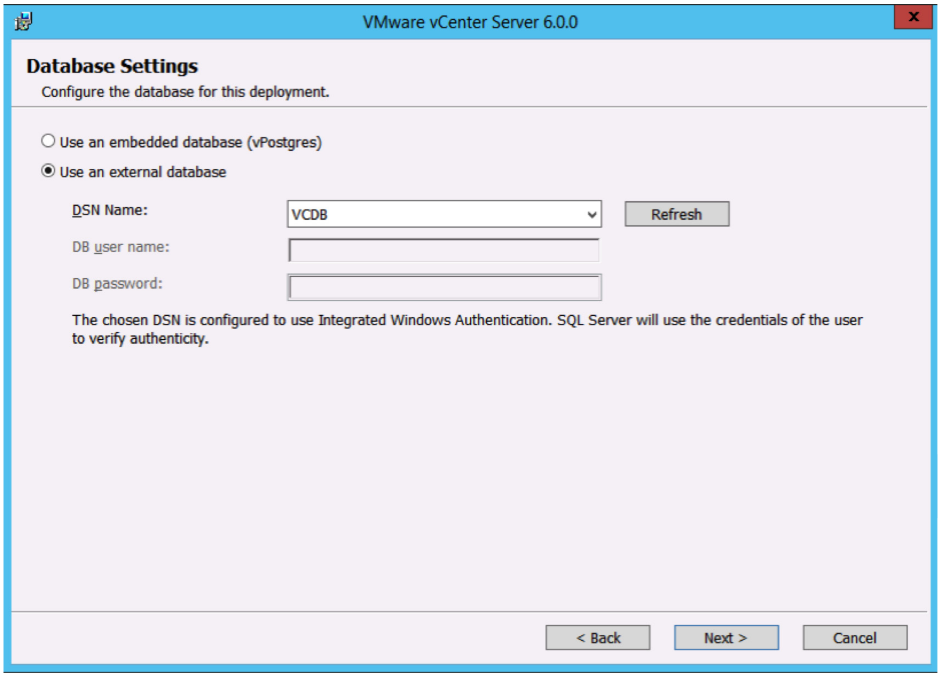
Note: If you select this option, you cannot connect to an external database using Integrated Windows authentication.

● Specify a user service account

Account user name: VMWARE\svcvCenter

Account password: ••••••••

12. Select **Use an embedded database (vPostgres)** or **Use an external database** server's **DSN Name** and click **Next**.



VMware vCenter Server 6.0.0

Database Settings

Configure the database for this deployment.

○ Use an embedded database (vPostgres)

● Use an external database

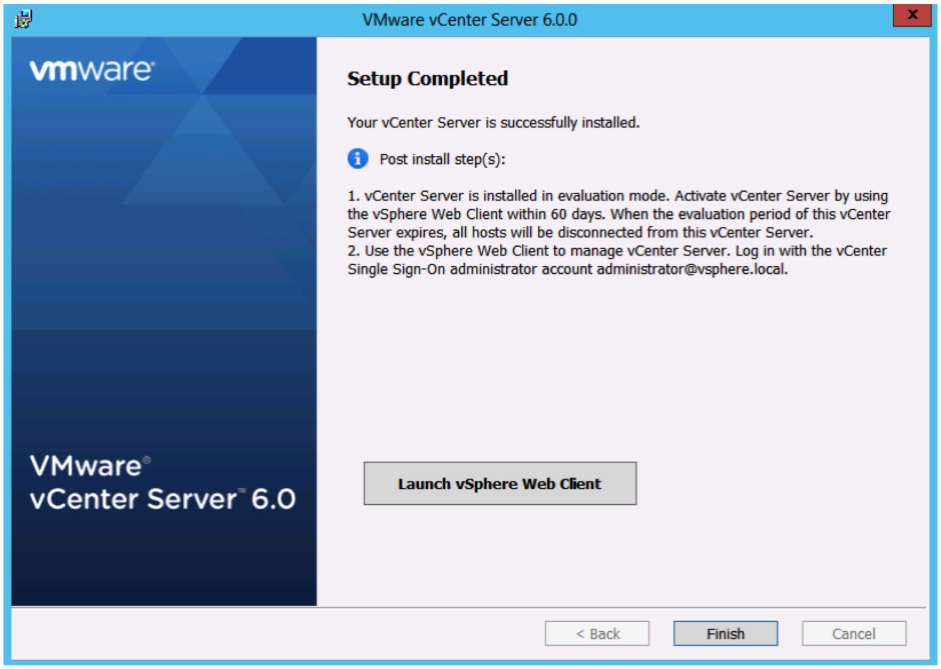
DSN Name: VCDB

DB user name:

DB password:

The chosen DSN is configured to use Integrated Windows Authentication. SQL Server will use the credentials of the user to verify authenticity.

13. Unless required, leave all ports at their defaults and click **Next**.
14. Unless required, leave the default paths for installation and click **Next**.
15. Review and then click **Install**.



Setup Completed

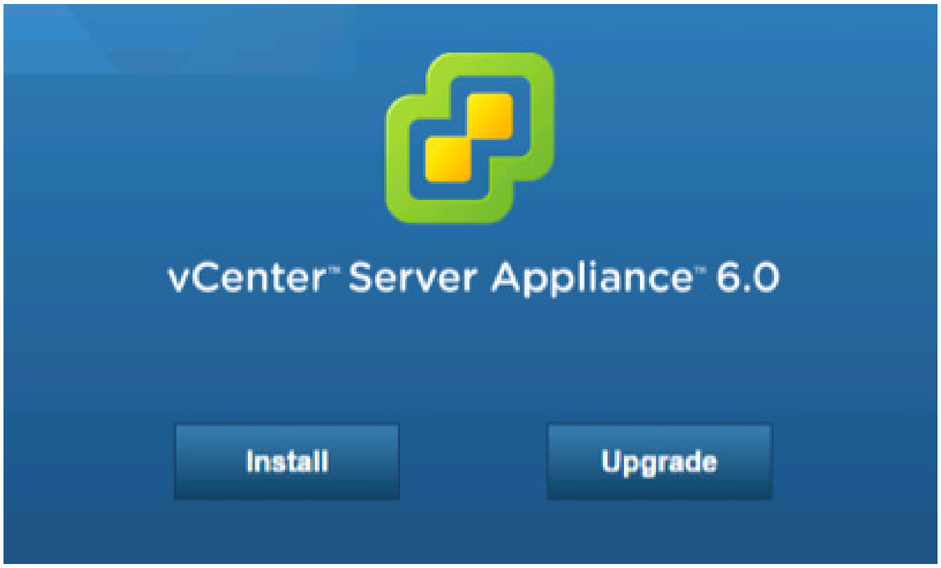
Your vCenter Server is successfully installed.

Post install step(s):

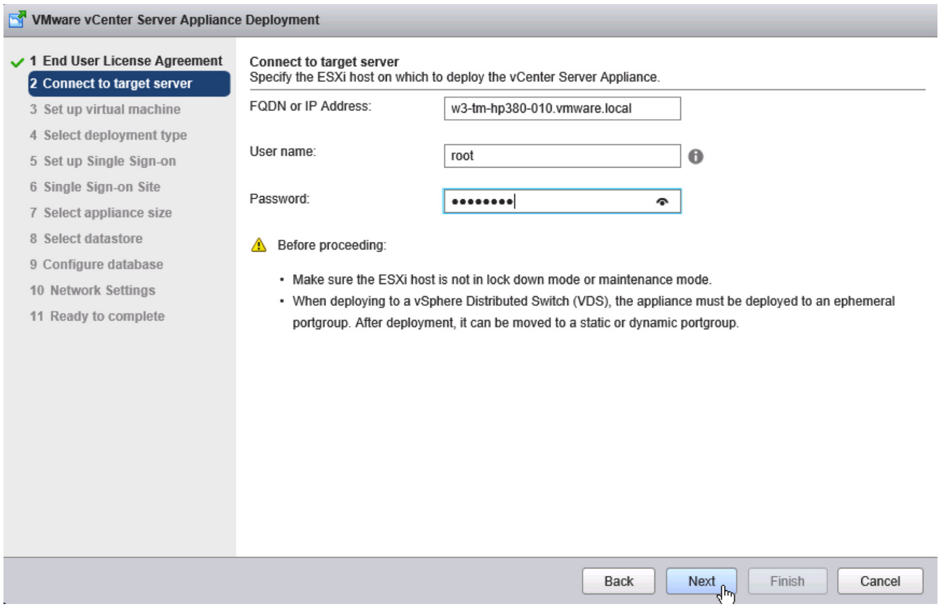
1. vCenter Server is installed in evaluation mode. Activate vCenter Server by using the vSphere Web Client within 60 days. When the evaluation period of this vCenter Server expires, all hosts will be disconnected from this vCenter Server.
2. Use the vSphere Web Client to manage vCenter Server. Log in with the vCenter Single Sign-On administrator account administrator@vsphere.local.

vCenter Server Appliance Deployment

1. Mount the ISO image on PC.
2. Open the vcsa folder and install the plug-in.
3. In the root of the ISO image, double-click the vcsa-setup.html file.
4. Wait until you are prompted to enable the client integration plug-in to run. Click **Install**.



5. Accept the **License Agreement** and click **Next**.
6. Enter a target host and a **User name** and **Password** on the host with root access.



VMware vCenter Server Appliance Deployment

- ✓ 1 End User License Agreement
- 2 Connect to target server
- 3 Set up virtual machine
- 4 Select deployment type
- 5 Set up Single Sign-on
- 6 Single Sign-on Site
- 7 Select appliance size
- 8 Select datastore
- 9 Configure database
- 10 Network Settings
- 11 Ready to complete

Connect to target server
Specify the ESXi host on which to deploy the vCenter Server Appliance.

FQDN or IP Address: w3-tm-hp380-010.vmware.local

User name: root

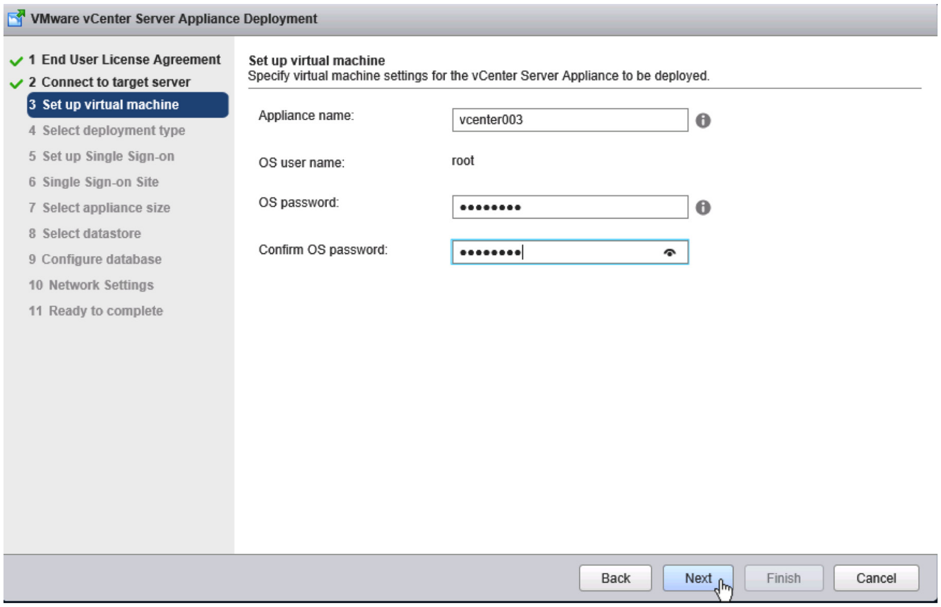
Password: ••••••••

⚠ Before proceeding:

- Make sure the ESXi host is not in lock down mode or maintenance mode.
- When deploying to a vSphere Distributed Switch (VDS), the appliance must be deployed to an ephemeral portgroup. After deployment, it can be moved to a static or dynamic portgroup.

7. Click **Yes** to accept the host’s certificate.

8. Enter an **Appliance name** and the root **OS password** you want to assign. Click **Next**.



VMware vCenter Server Appliance Deployment

- ✓ 1 End User License Agreement
- ✓ 2 Connect to target server
- 3 Set up virtual machine
- 4 Select deployment type
- 5 Set up Single Sign-on
- 6 Single Sign-on Site
- 7 Select appliance size
- 8 Select datastore
- 9 Configure database
- 10 Network Settings
- 11 Ready to complete

Set up virtual machine
Specify virtual machine settings for the vCenter Server Appliance to be deployed.

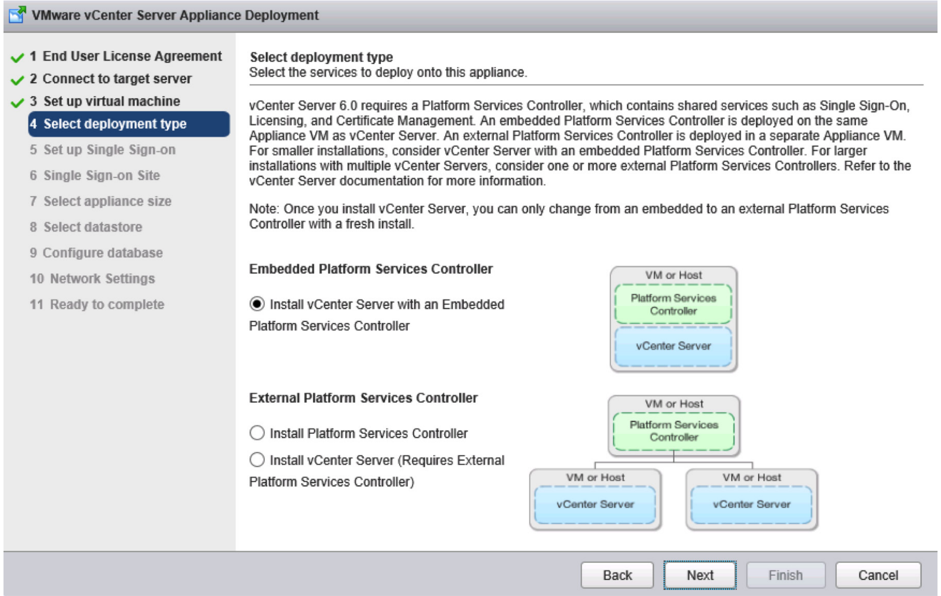
Appliance name: vcenter003

OS user name: root

OS password: ••••••••

Confirm OS password: ••••••••

9. Select **Install vCenter Server with an Embedded Platform Services Controller** and click **Next**.



Select deployment type
Select the services to deploy onto this appliance.

vCenter Server 6.0 requires a Platform Services Controller, which contains shared services such as Single Sign-On, Licensing, and Certificate Management. An embedded Platform Services Controller is deployed on the same Appliance VM as vCenter Server. An external Platform Services Controller is deployed in a separate Appliance VM. For smaller installations, consider vCenter Server with an embedded Platform Services Controller. For larger installations with multiple vCenter Servers, consider one or more external Platform Services Controllers. Refer to the vCenter Server documentation for more information.

Note: Once you install vCenter Server, you can only change from an embedded to an external Platform Services Controller with a fresh install.

Embedded Platform Services Controller

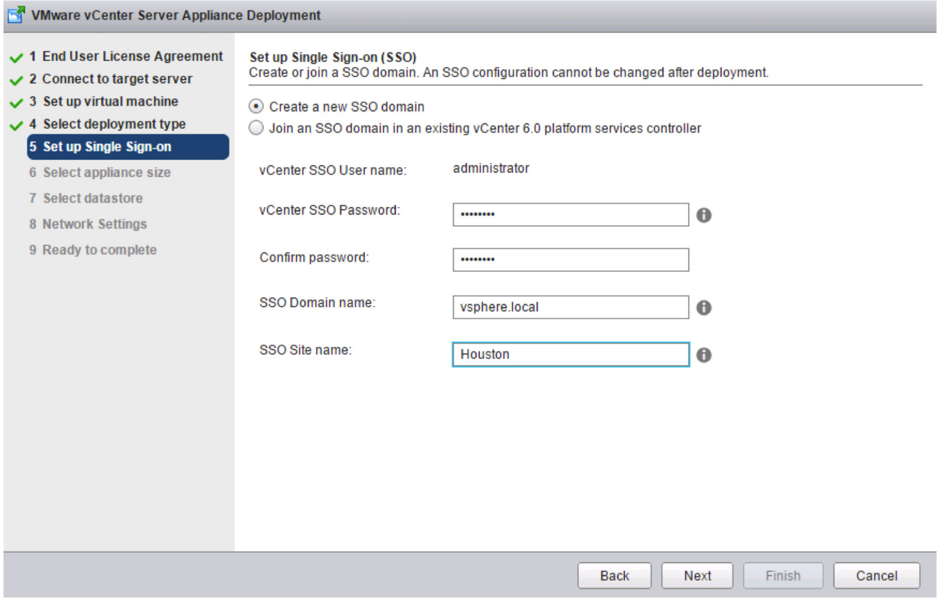
● Install vCenter Server with an Embedded Platform Services Controller

External Platform Services Controller

○ Install Platform Services Controller

○ Install vCenter Server (Requires External Platform Services Controller)

10. Select **Create a new SSO Domain** and enter an administrator **vCenter SSO Password**; enter an **SSO Domain name** such as vsphere.local and an **SSO Site name** such as a city or physical location name.


VMware vCenter Server Appliance Deployment
✓ 1 End User License Agreement
✓ 2 Connect to target server
✓ 3 Set up virtual machine
✓ 4 Select deployment type
5 Set up Single Sign-on
6 Select appliance size
7 Select datastore
8 Network Settings
9 Ready to complete
Back
Next
Finish
Cancel

Set up Single Sign-on (SSO)
Create or join a SSO domain. An SSO configuration cannot be changed after deployment.

● Create a new SSO domain
○ Join an SSO domain in an existing vCenter 6.0 platform services controller

vCenter SSO User name: administrator

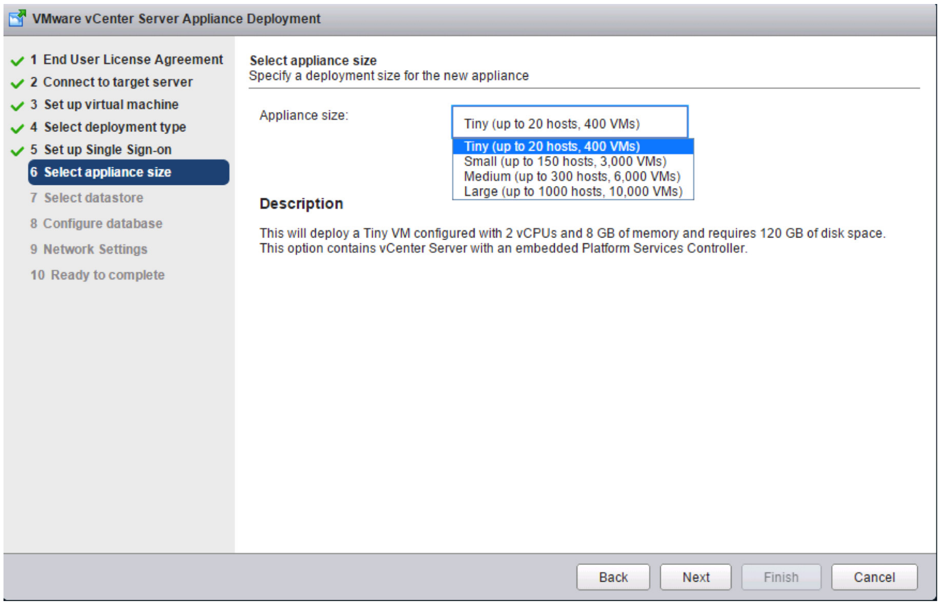
vCenter SSO Password: ••••••••

Confirm password: ••••••••

SSO Domain name: vsphere.local

SSO Site name: Houston

11. **Select appliance size** from the drop-down list and click **Next**.



VMware vCenter Server Appliance Deployment

- ✓ 1 End User License Agreement
- ✓ 2 Connect to target server
- ✓ 3 Set up virtual machine
- ✓ 4 Select deployment type
- ✓ 5 Set up Single Sign-on
- 6 Select appliance size
- 7 Select datastore
- 8 Configure database
- 9 Network Settings
- 10 Ready to complete

Select appliance size
Specify a deployment size for the new appliance

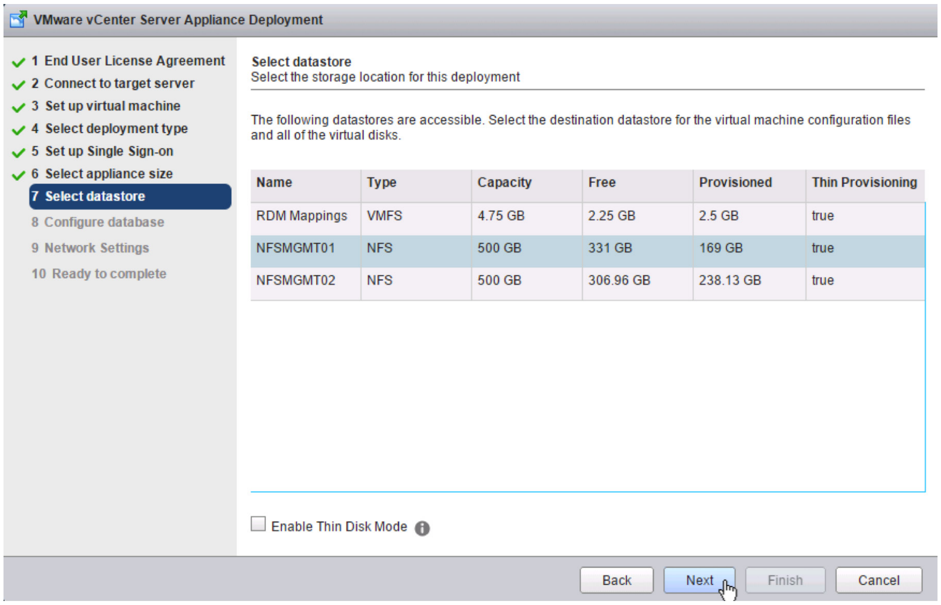
Appliance size: Tiny (up to 20 hosts, 400 VMs)

- Tiny (up to 20 hosts, 400 VMs)
- Small (up to 150 hosts, 3,000 VMs)
- Medium (up to 300 hosts, 6,000 VMs)
- Large (up to 1000 hosts, 10,000 VMs)

Description

This will deploy a Tiny VM configured with 2 vCPUs and 8 GB of memory and requires 120 GB of disk space. This option contains vCenter Server with an embedded Platform Services Controller.

12. **Select datastore** to deploy the appliance on and click **Next**.



VMware vCenter Server Appliance Deployment

- ✓ 1 End User License Agreement
- ✓ 2 Connect to target server
- ✓ 3 Set up virtual machine
- ✓ 4 Select deployment type
- ✓ 5 Set up Single Sign-on
- ✓ 6 Select appliance size
- 7 Select datastore
- 8 Configure database
- 9 Network Settings
- 10 Ready to complete

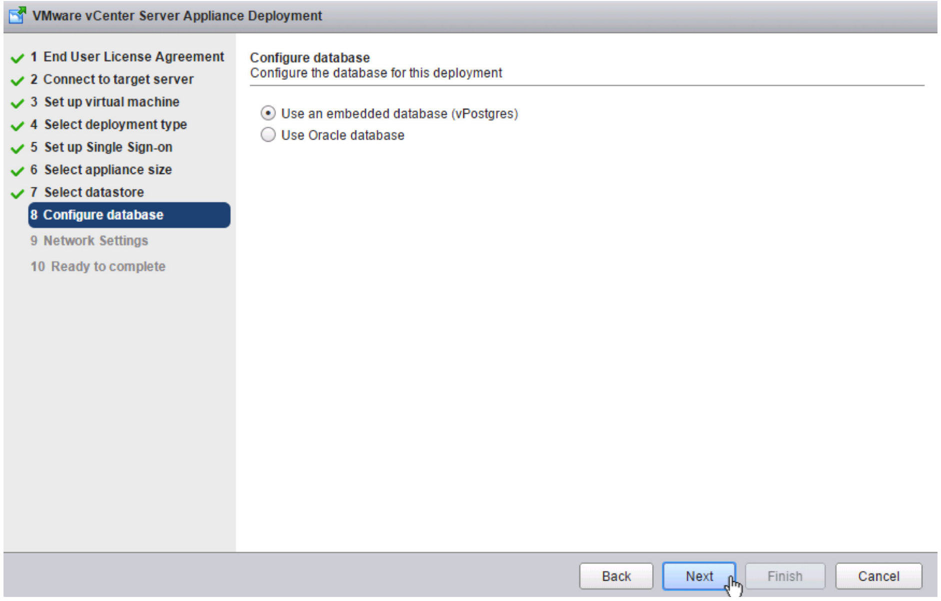
Select datastore
Select the storage location for this deployment

The following datastores are accessible. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Type	Capacity	Free	Provisioned	Thin Provisioning
RDM Mappings	VMFS	4.75 GB	2.25 GB	2.5 GB	true
NFSMGMT01	NFS	500 GB	331 GB	169 GB	true
NFSMGMT02	NFS	500 GB	306.96 GB	238.13 GB	true

□ Enable Thin Disk Mode

13. Select **Use an embedded database (vPostgres)**, which is recommended, or **Use Oracle database** and click **Next**.



VMware vCenter Server Appliance Deployment

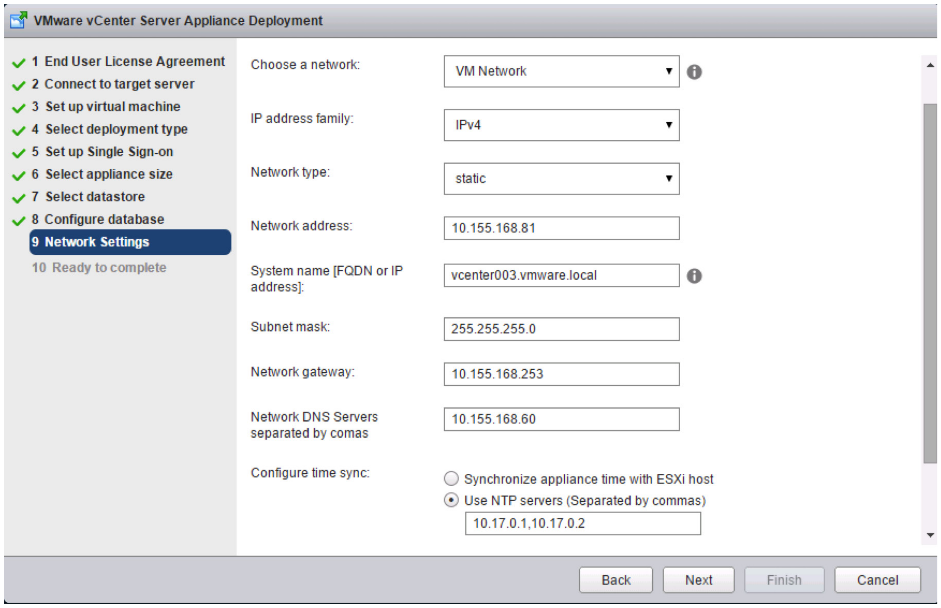
- ✓ 1 End User License Agreement
- ✓ 2 Connect to target server
- ✓ 3 Set up virtual machine
- ✓ 4 Select deployment type
- ✓ 5 Set up Single Sign-on
- ✓ 6 Select appliance size
- ✓ 7 Select datastore
- 8 Configure database
- 9 Network Settings
- 10 Ready to complete

Configure database
Configure the database for this deployment

● Use an embedded database (vPostgres)
○ Use Oracle database

14. Enter **Network Settings** and click **Next**.

NOTE: The FQDN and IP addresses entered here must be resolvable by the DNS server specified or the deployment will fail.

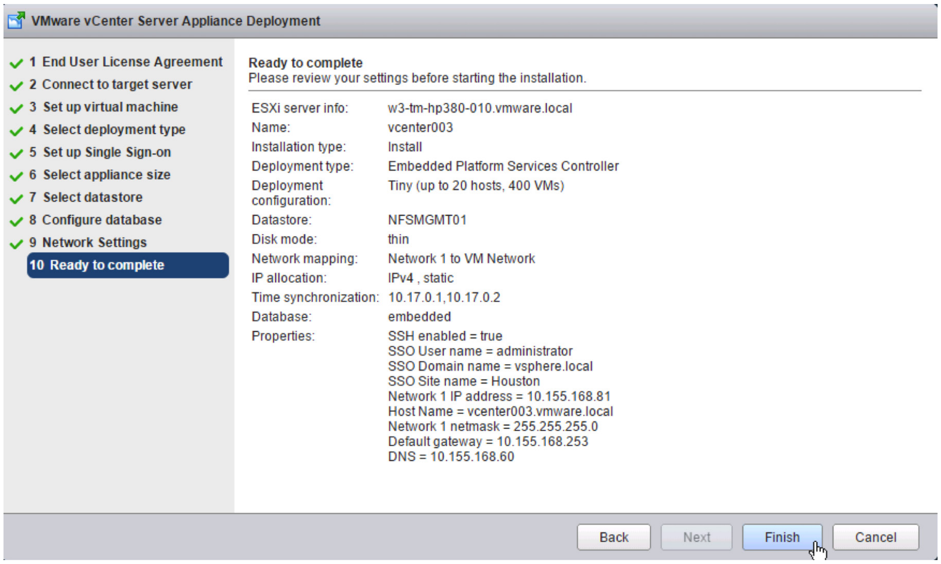


VMware vCenter Server Appliance Deployment

- ✓ 1 End User License Agreement
- ✓ 2 Connect to target server
- ✓ 3 Set up virtual machine
- ✓ 4 Select deployment type
- ✓ 5 Set up Single Sign-on
- ✓ 6 Select appliance size
- ✓ 7 Select datastore
- ✓ 8 Configure database
- 9 Network Settings
- 10 Ready to complete

Choose a network:	VM Network
IP address family:	IPv4
Network type:	static
Network address:	10.155.168.81
System name [FQDN or IP address]:	vcenter003.vmware.local
Subnet mask:	255.255.255.0
Network gateway:	10.155.168.253
Network DNS Servers separated by comas	10.155.168.60
Configure time sync:	○ Synchronize appliance time with ESXi host ● Use NTP servers (Separated by commas) 10.17.0.1,10.17.0.2

15. Review and click **Finish**.



VMware vCenter Server Appliance Deployment

1. End User License Agreement ✓
2. Connect to target server ✓
3. Set up virtual machine ✓
4. Select deployment type ✓
5. Set up Single Sign-on ✓
6. Select appliance size ✓
7. Select datastore ✓
8. Configure database ✓
9. Network Settings ✓
10. Ready to complete

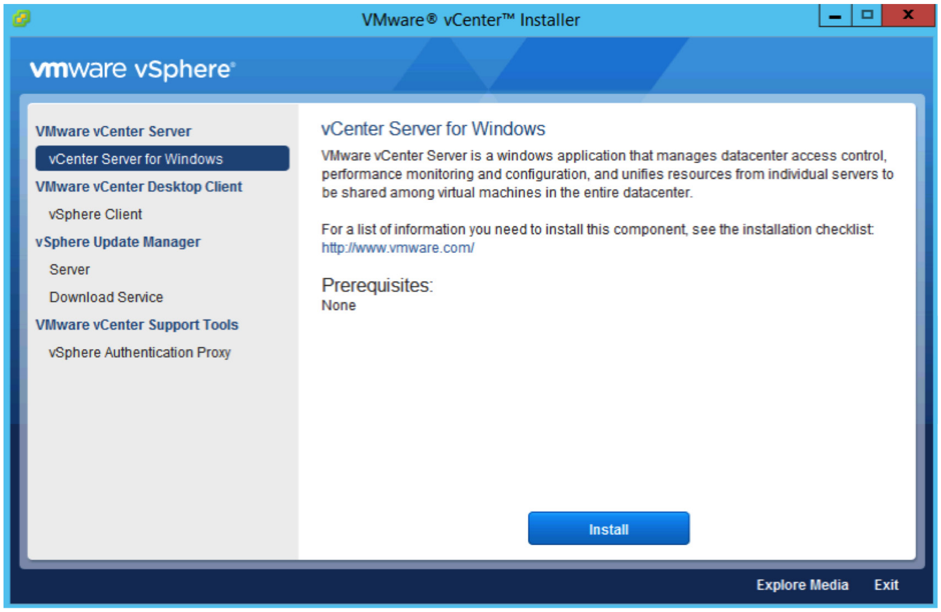
Ready to complete
Please review your settings before starting the installation.

ESXi server info:	w3-tm-hp380-010.vmware.local
Name:	vcenter003
Installation type:	Install
Deployment type:	Embedded Platform Services Controller
Deployment configuration:	Tiny (up to 20 hosts, 400 VMs)
Datastore:	NFSMGMT01
Disk mode:	thin
Network mapping:	Network 1 to VM Network
IP allocation:	IPv4 , static
Time synchronization:	10.17.0.1,10.17.0.2
Database:	embedded
Properties:	SSH enabled = true SSO User name = administrator SSO Domain name = vsphere.local SSO Site name = Houston Network 1 IP address = 10.155.168.81 Host Name = vcenter003.vmware.local Network 1 netmask = 255.255.255.0 Default gateway = 10.155.168.253 DNS = 10.155.168.60

Upgrade in Which All vCenter Server Components Are Installed on a Single Machine

Windows Upgrade

1. Verify all prerequisites.
2. Mount the vCenter Server 6.0 ISO image.
3. If autorun does not start, execute autorun.exe.
4. Select **vCenter Server for Windows** and click **Install**.



VMware® vCenter™ Installer
vmware vSphere
VMware vCenter Server
vCenter Server for Windows
VMware vCenter Desktop Client
vSphere Client
vSphere Update Manager
Server
Download Service
VMware vCenter Support Tools
vSphere Authentication Proxy

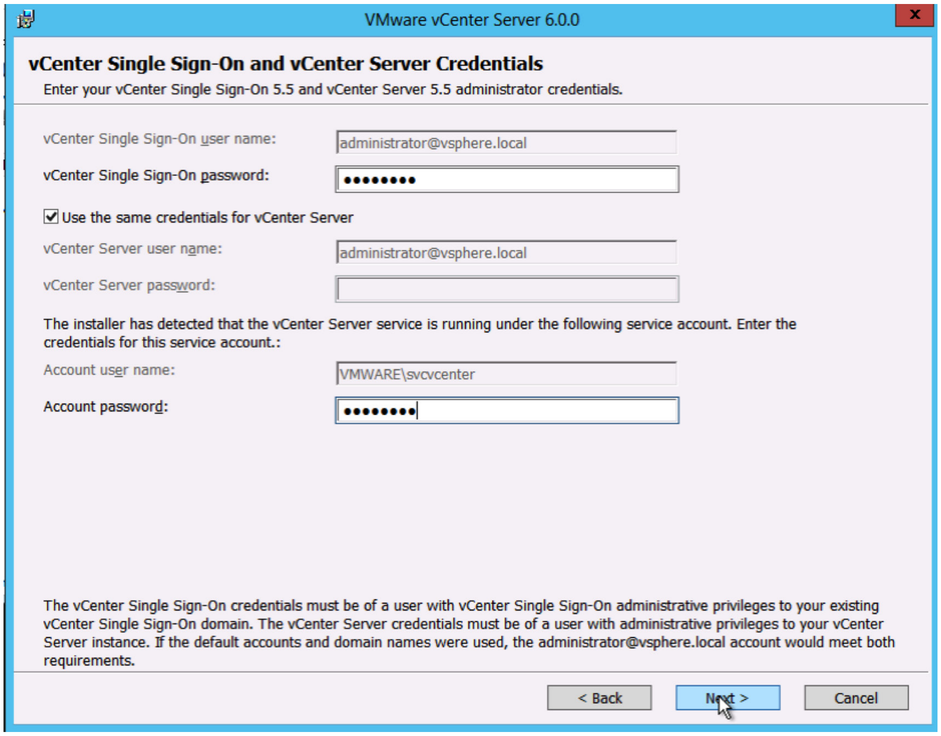
vCenter Server for Windows

VMware vCenter Server is a windows application that manages datacenter access control, performance monitoring and configuration, and unifies resources from individual servers to be shared among virtual machines in the entire datacenter.

For a list of information you need to install this component, see the installation checklist: http://www.vmware.com/

Prerequisites:
None

5. Click **Next**.
6. Accept the license agreements.
7. Enter the **vCenter Single Sign-On password** and the service account **password** if applicable. Click **Next**.



vCenter Single Sign-On and vCenter Server Credentials

Enter your vCenter Single Sign-On 5.5 and vCenter Server 5.5 administrator credentials.

vCenter Single Sign-On user name: administrator@vsphere.local

vCenter Single Sign-On password: ••••••••

☑ Use the same credentials for vCenter Server

vCenter Server user name: administrator@vsphere.local

vCenter Server password:

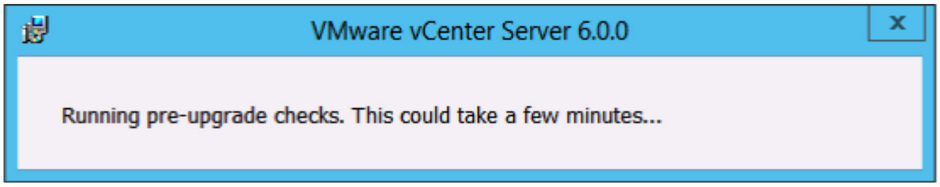
The installer has detected that the vCenter Server service is running under the following service account. Enter the credentials for this service account.:

Account user name: VMWARE\svcvcenter

Account password: ••••••••

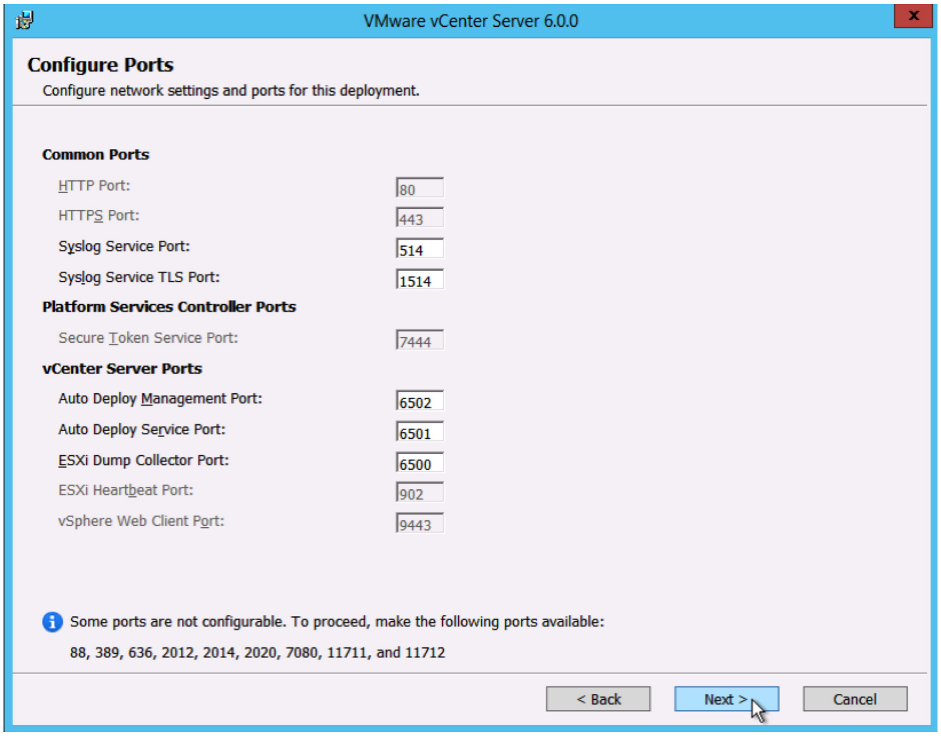
The vCenter Single Sign-On credentials must be of a user with vCenter Single Sign-On administrative privileges to your existing vCenter Single Sign-On domain. The vCenter Server credentials must be of a user with administrative privileges to your vCenter Server instance. If the default accounts and domain names were used, the administrator@vsphere.local account would meet both requirements.

8. Wait for the **pre-upgrade checks** to complete.



Running pre-upgrade checks. This could take a few minutes...

9. Accept the default ports and click **Next**.



VMware vCenter Server 6.0.0

Configure Ports

Configure network settings and ports for this deployment.

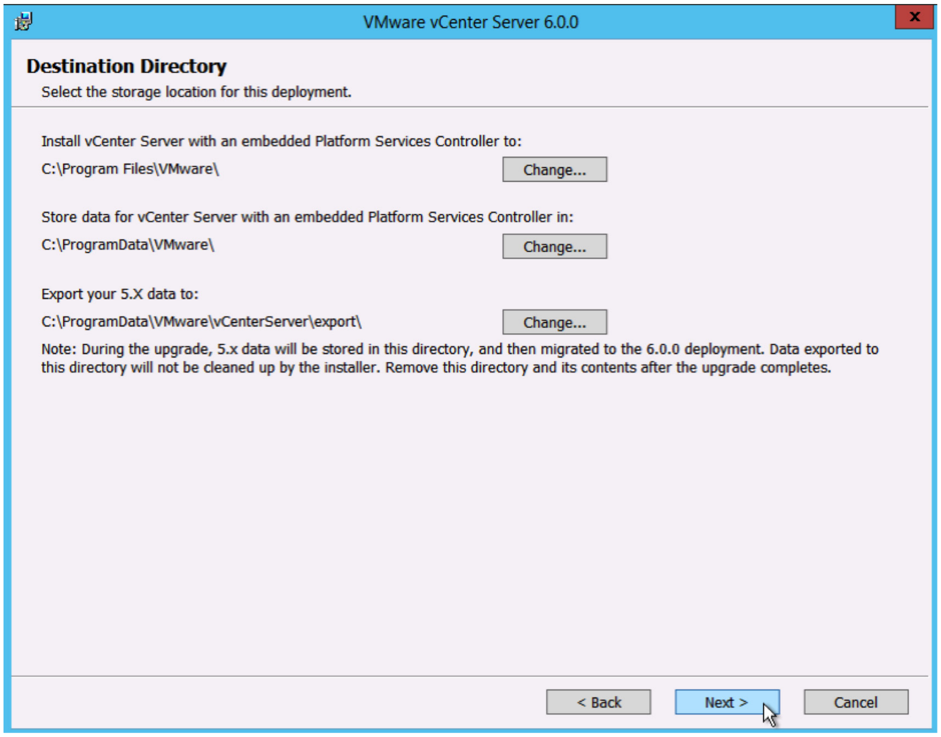
Common Ports

HTTP Port:	80
HTTPS Port:	443
Syslog Service Port:	514
Syslog Service TLS Port:	1514
Platform Services Controller Ports	
Secure Token Service Port:	7444
vCenter Server Ports	
Auto Deploy Management Port:	6502
Auto Deploy Service Port:	6501
ESXi Dump Collector Port:	6500
ESXi Heartbeat Port:	902
vSphere Web Client Port:	9443

Some ports are not configurable. To proceed, make the following ports available:

88, 389, 636, 2012, 2014, 2020, 7080, 11711, and 11712

10. Accept or change the installation paths as necessary. Click **Next**.



VMware vCenter Server 6.0.0

Destination Directory

Select the storage location for this deployment.

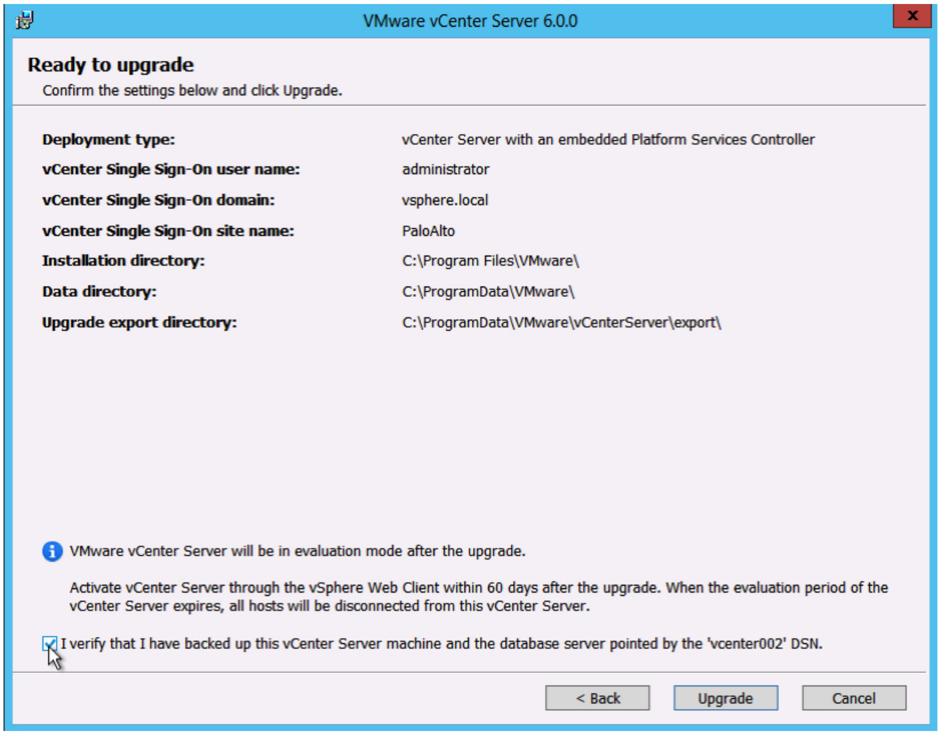
Install vCenter Server with an embedded Platform Services Controller to:
C:\Program Files\VMware\

Store data for vCenter Server with an embedded Platform Services Controller in:
C:\ProgramData\VMware\

Export your 5.X data to:
C:\ProgramData\VMware\vCenterServer\export\

Note: During the upgrade, 5.x data will be stored in this directory, and then migrated to the 6.0.0 deployment. Data exported to this directory will not be cleaned up by the installer. Remove this directory and its contents after the upgrade completes.

11. Check the box to verify that you have backed up this vCenter Server and its database. Click **Upgrade**.



Ready to upgrade

Confirm the settings below and click Upgrade.

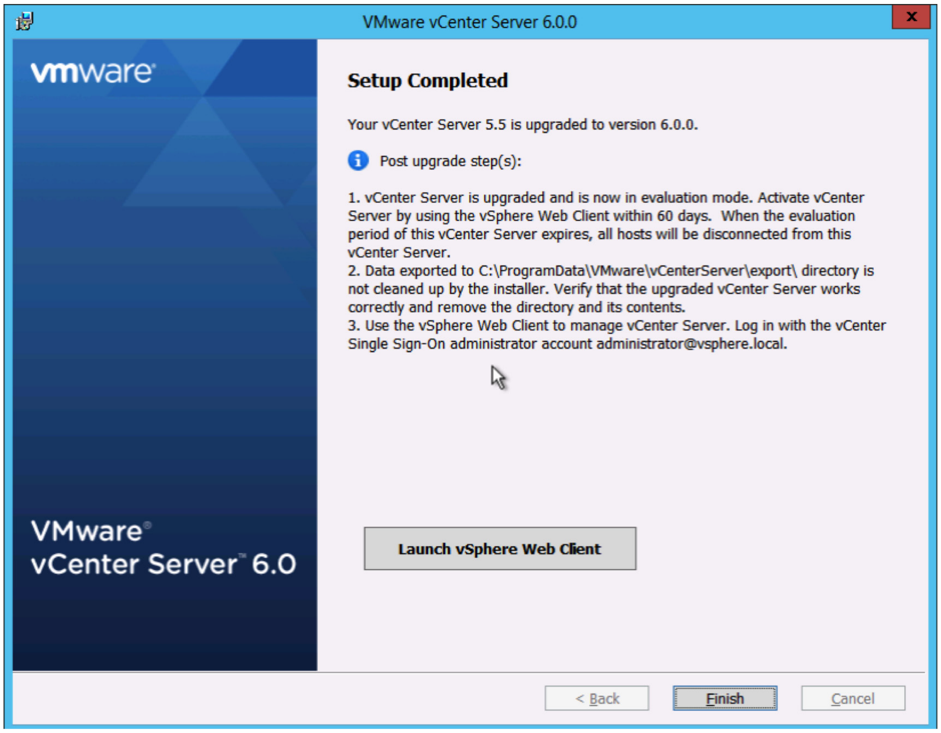
Deployment type:	vCenter Server with an embedded Platform Services Controller
vCenter Single Sign-On user name:	administrator
vCenter Single Sign-On domain:	vsphere.local
vCenter Single Sign-On site name:	PaloAlto
Installation directory:	C:\Program Files\VMware\
Data directory:	C:\ProgramData\VMware\
Upgrade export directory:	C:\ProgramData\VMware\vCenterServer\export\

VMware vCenter Server will be in evaluation mode after the upgrade.

Activate vCenter Server through the vSphere Web Client within 60 days after the upgrade. When the evaluation period of the vCenter Server expires, all hosts will be disconnected from this vCenter Server.

☑ I verify that I have backed up this vCenter Server machine and the database server pointed by the 'vcenter002' DSN.

12. When completed, click **Finish**.



Setup Completed

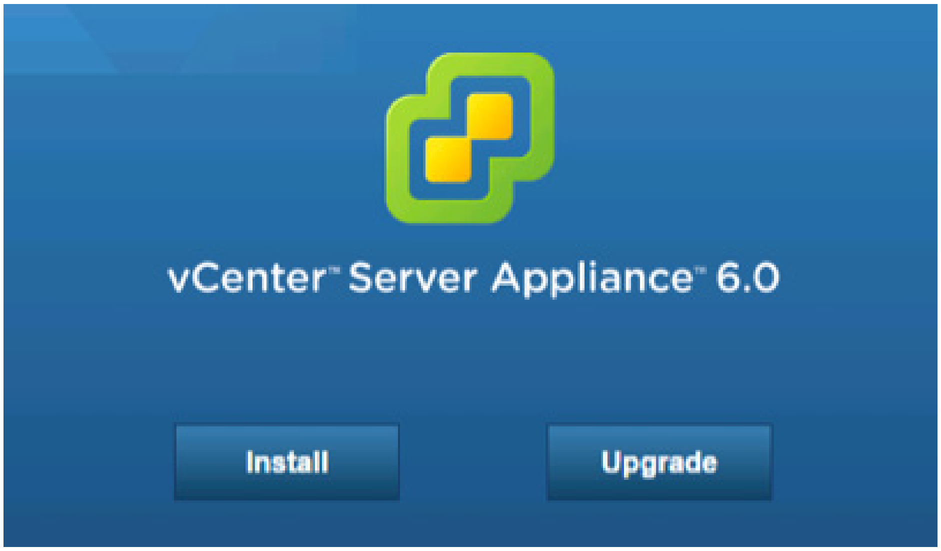
Your vCenter Server 5.5 is upgraded to version 6.0.0.

Post upgrade step(s):

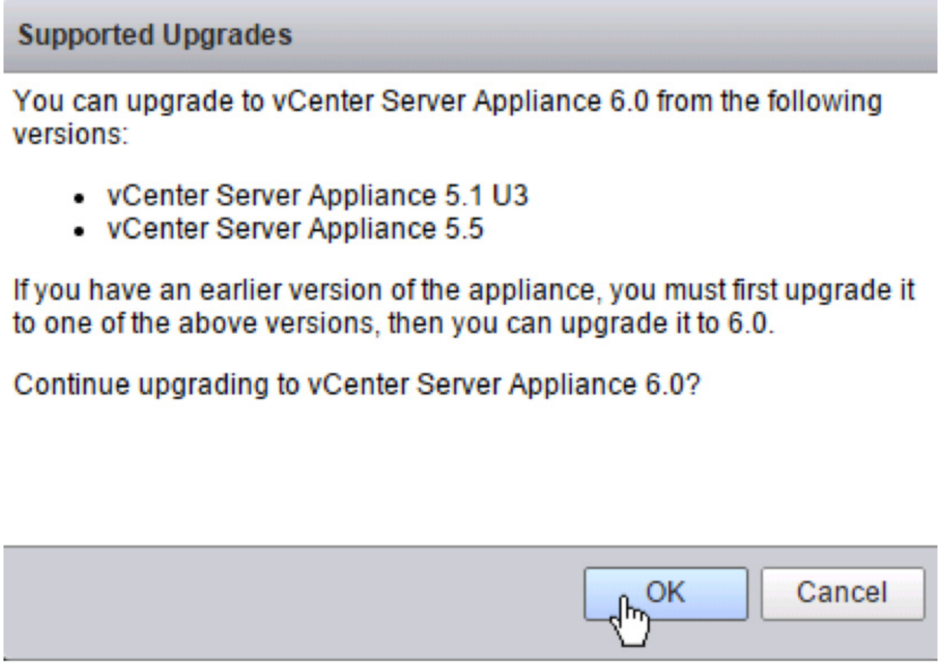
1. vCenter Server is upgraded and is now in evaluation mode. Activate vCenter Server by using the vSphere Web Client within 60 days. When the evaluation period of this vCenter Server expires, all hosts will be disconnected from this vCenter Server.
2. Data exported to C:\ProgramData\VMware\vCenterServer\export\ directory is not cleaned up by the installer. Verify that the upgraded vCenter Server works correctly and remove the directory and its contents.
3. Use the vSphere Web Client to manage vCenter Server. Log in with the vCenter Single Sign-On administrator account administrator@vsphere.local.

vCenter Server Appliance Upgrade

1. Mount the ISO image on PC.
2. Open the vcsa folder and install the plug-in.
3. In the root of the ISO image, double-click the vcsa-setup.html file.
4. Wait until you are prompted to enable the client integration plug-in to run. Click **Upgrade**.



5. Click **OK** to the supported upgrades pop-up.



Supported Upgrades

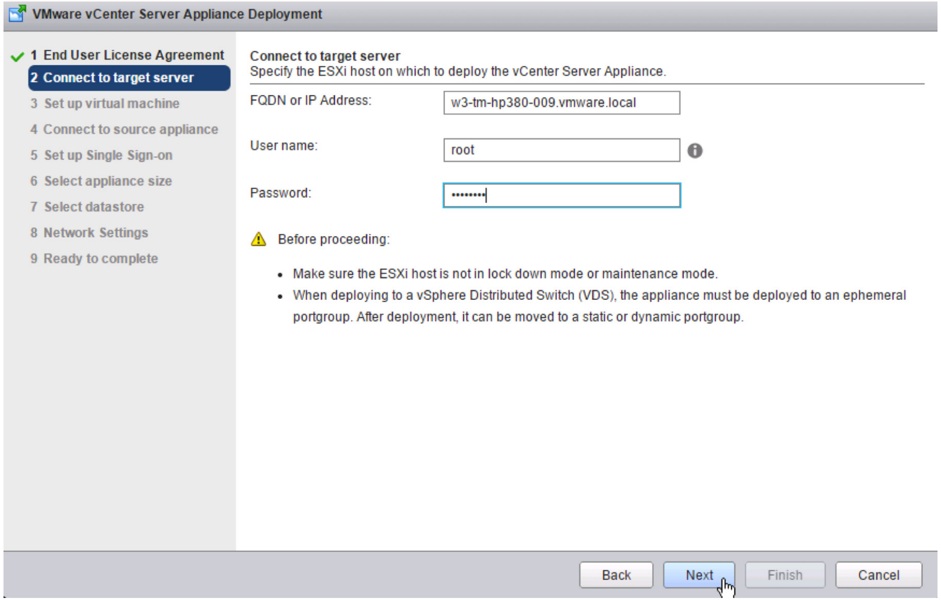
You can upgrade to vCenter Server Appliance 6.0 from the following versions:

- vCenter Server Appliance 5.1 U3
- vCenter Server Appliance 5.5

If you have an earlier version of the appliance, you must first upgrade it to one of the above versions, then you can upgrade it to 6.0.

Continue upgrading to vCenter Server Appliance 6.0?

6. Accept the license agreement and click **Next**.
7. Enter a target host and a **User name** and **Password** on the host with root access.



VMware vCenter Server Appliance Deployment

Connect to target server
Specify the ESXi host on which to deploy the vCenter Server Appliance.

FQDN or IP Address: w3-tm-hp380-009.vmware.local

User name: root

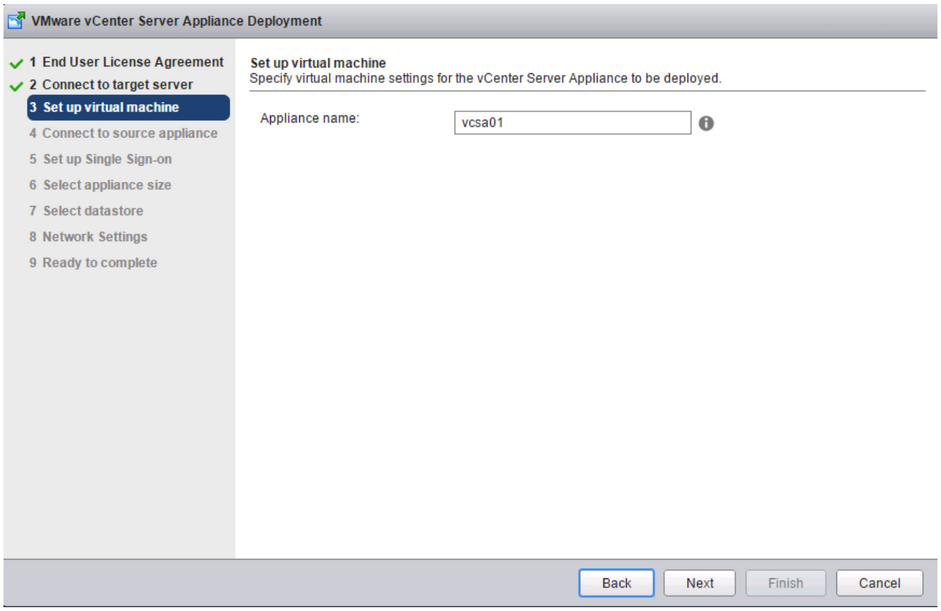
Password: ••••••••

Before proceeding:

- Make sure the ESXi host is not in lock down mode or maintenance mode.
- When deploying to a vSphere Distributed Switch (VDS), the appliance must be deployed to an ephemeral portgroup. After deployment, it can be moved to a static or dynamic portgroup.

8. Click **Yes** to accept the host's certificate.

9. Enter an **Appliance name** and **Enable SSH** if required. Click **Next**.

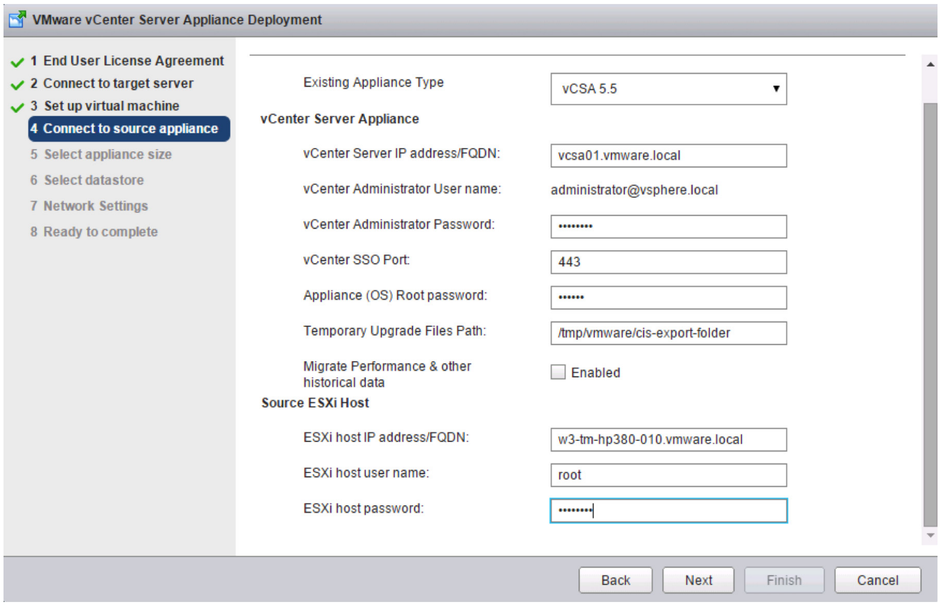


VMware vCenter Server Appliance Deployment

Set up virtual machine
Specify virtual machine settings for the vCenter Server Appliance to be deployed.

Appliance name: vcsa01

10. Enter the **vCenter Server** version, **FQDN**, **Password**, **vCenter SSO Port** (443), **ESXi host FQDN**, **user name**, and **password**. Click **Next**.



VMware vCenter Server Appliance Deployment

Existing Appliance Type: vCSA 5.5

vCenter Server Appliance

vCenter Server IP address/FQDN: vcsa01.vmware.local

vCenter Administrator User name: administrator@vsphere.local

vCenter Administrator Password: ••••••••

vCenter SSO Port: 443

Appliance (OS) Root password: ••••••

Temporary Upgrade Files Path: /tmp/vmware/cis-export-folder

Migrate Performance & other historical data: □ Enabled

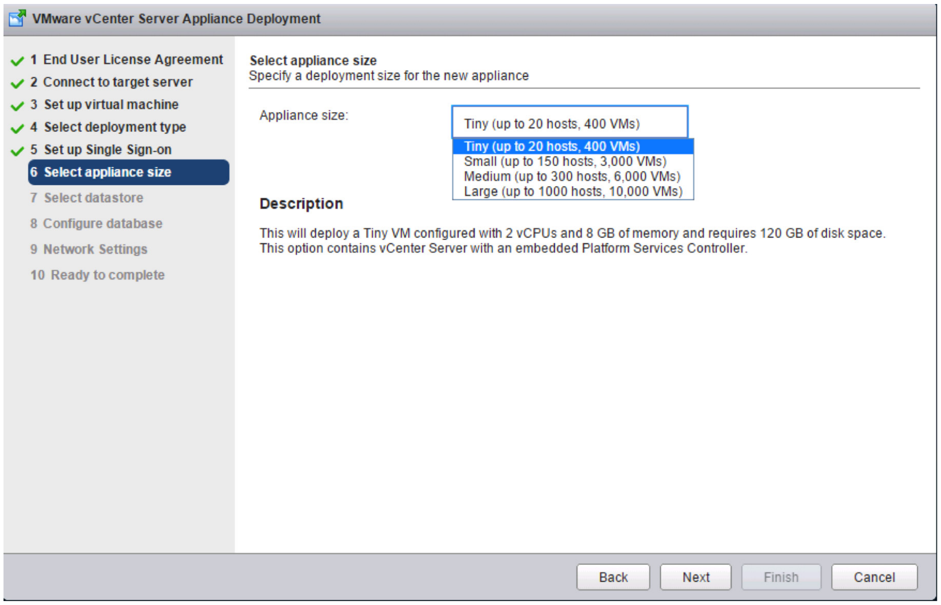
Source ESXi Host

ESXi host IP address/FQDN: w3-tm-hp380-010.vmware.local

ESXi host user name: root

ESXi host password: ••••••••

11. Select **Appliance size** from the drop-down list and click **Next**.



VMware vCenter Server Appliance Deployment

Select appliance size
Specify a deployment size for the new appliance

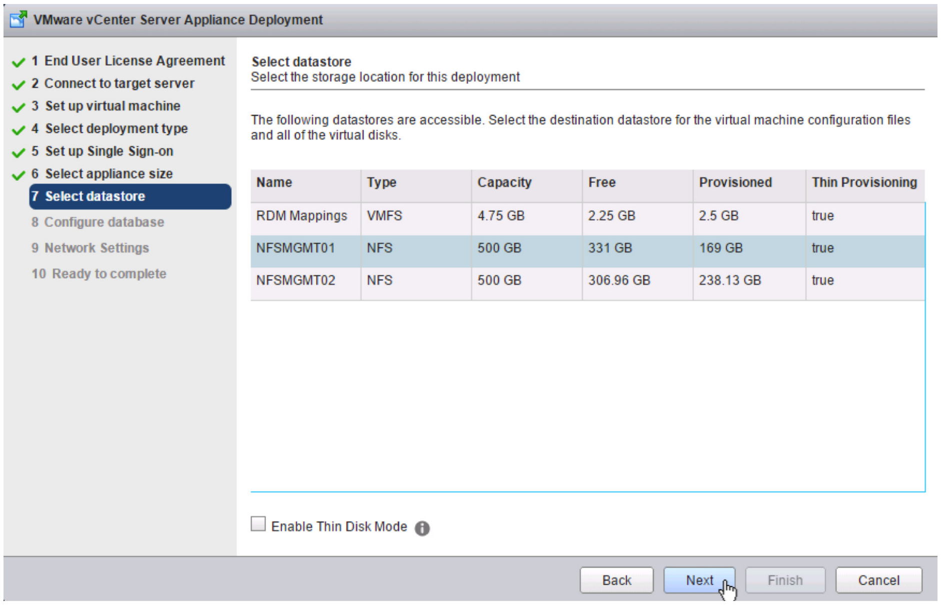
Appliance size: Tiny (up to 20 hosts, 400 VMs)

- Tiny (up to 20 hosts, 400 VMs)
- Small (up to 150 hosts, 3,000 VMs)
- Medium (up to 300 hosts, 6,000 VMs)
- Large (up to 1000 hosts, 10,000 VMs)

Description

This will deploy a Tiny VM configured with 2 vCPUs and 8 GB of memory and requires 120 GB of disk space. This option contains vCenter Server with an embedded Platform Services Controller.

12. **Select datastore** to deploy the appliance on and click **Next**.



VMware vCenter Server Appliance Deployment

- ✓ 1 End User License Agreement
- ✓ 2 Connect to target server
- ✓ 3 Set up virtual machine
- ✓ 4 Select deployment type
- ✓ 5 Set up Single Sign-on
- ✓ 6 Select appliance size
- 7 Select datastore
- 8 Configure database
- 9 Network Settings
- 10 Ready to complete

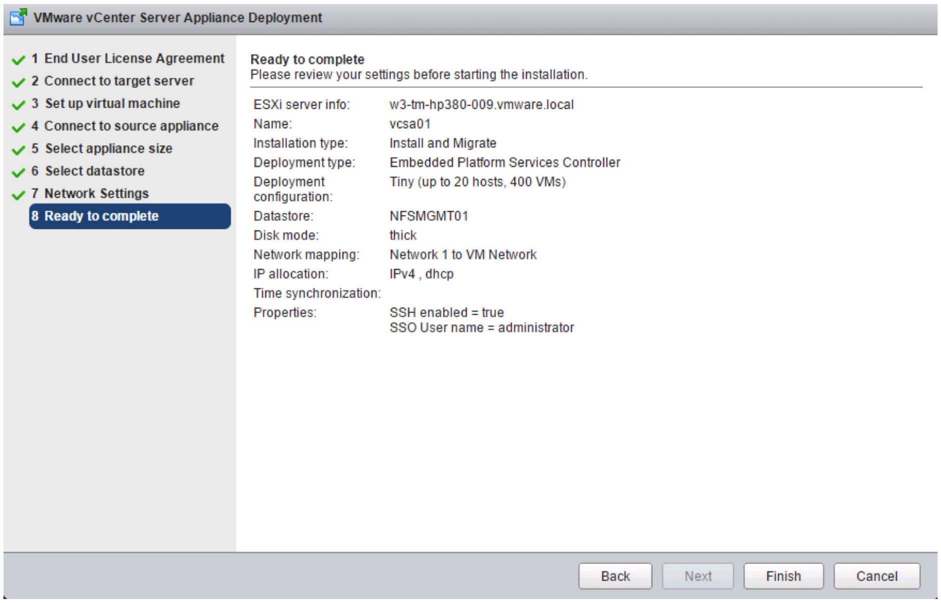
Select datastore
Select the storage location for this deployment

The following datastores are accessible. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Type	Capacity	Free	Provisioned	Thin Provisioning
RDM Mappings	VMFS	4.75 GB	2.25 GB	2.5 GB	true
NFSMGMT01	NFS	500 GB	331 GB	169 GB	true
NFSMGMT02	NFS	500 GB	306.96 GB	238.13 GB	true

□ Enable Thin Disk Mode

13. Review and click **Finish**.



VMware vCenter Server Appliance Deployment

- ✓ 1 End User License Agreement
- ✓ 2 Connect to target server
- ✓ 3 Set up virtual machine
- ✓ 4 Connect to source appliance
- ✓ 5 Select appliance size
- ✓ 6 Select datastore
- ✓ 7 Network Settings
- 8 Ready to complete

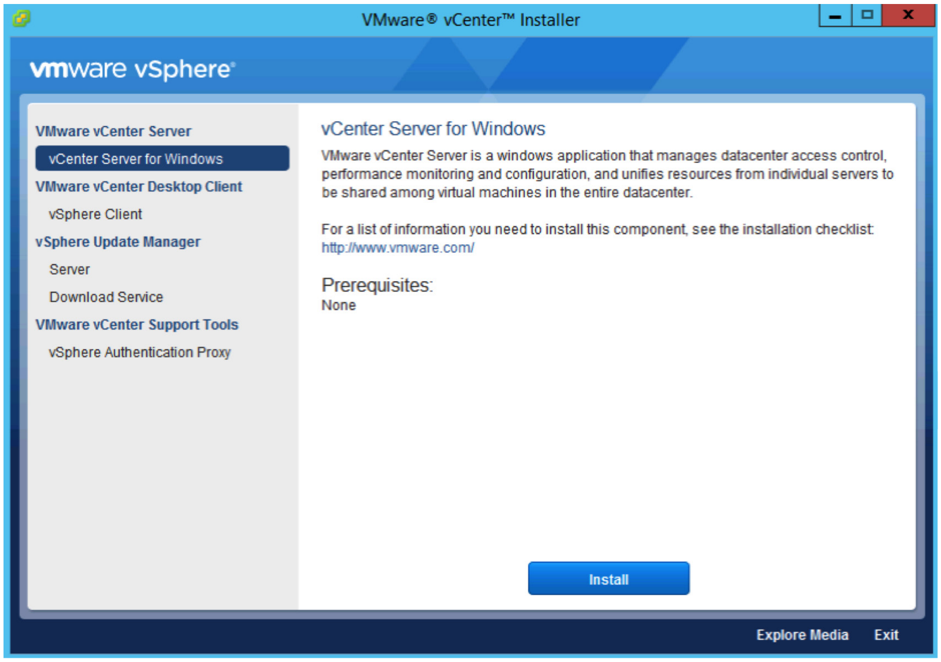
Ready to complete
Please review your settings before starting the installation.

ESXi server info:	w3-tm-hp380-009.vmware.local
Name:	vcsa01
Installation type:	Install and Migrate
Deployment type:	Embedded Platform Services Controller
Deployment configuration:	Tiny (up to 20 hosts, 400 VMs)
Datastore:	NFSMGMT01
Disk mode:	thick
Network mapping:	Network 1 to VM Network
IP allocation:	IPv4 , dhcp
Time synchronization:	
Properties:	SSH enabled = true SSO User name = administrator

Fresh External Platform Services Controller Deployment

Windows Deployment

1. Verify all prerequisites.
2. Mount the vCenter Server 6.0 ISO image.
3. If autorun does not start, execute autorun.exe.
4. Select **vCenter Server for Windows** and click **Install**.



VMware® vCenter™ Installer
vmware vSphere
VMware vCenter Server
vCenter Server for Windows
VMware vCenter Desktop Client
vSphere Client
vSphere Update Manager
Server
Download Service
VMware vCenter Support Tools
vSphere Authentication Proxy
Install
Explore Media
Exit

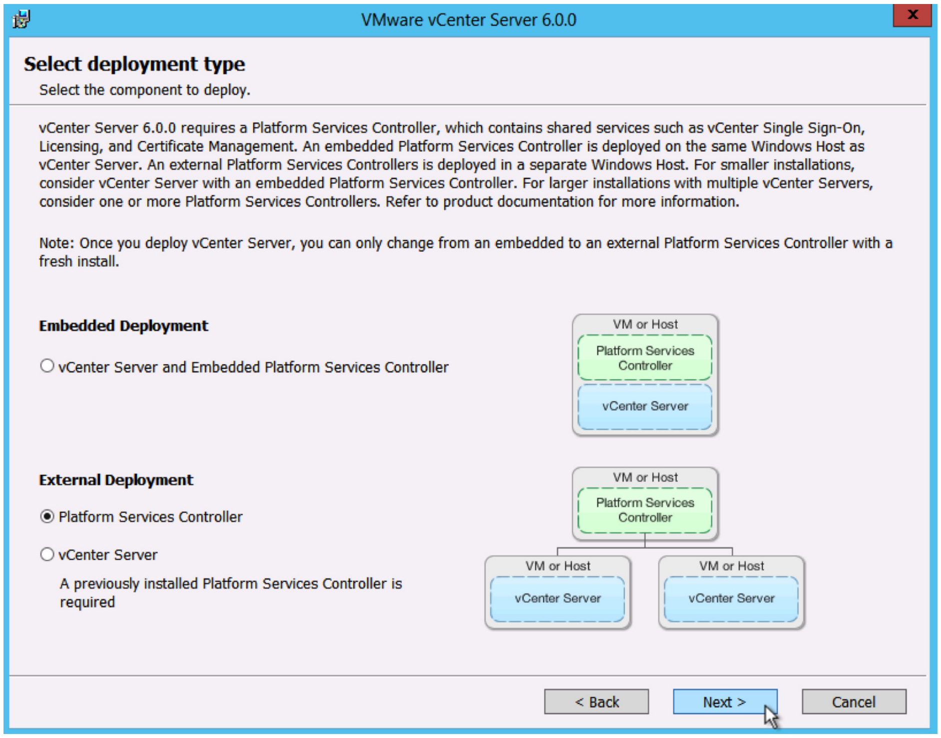
vCenter Server for Windows

VMware vCenter Server is a windows application that manages datacenter access control, performance monitoring and configuration, and unifies resources from individual servers to be shared among virtual machines in the entire datacenter.

For a list of information you need to install this component, see the installation checklist: http://www.vmware.com/

Prerequisites:
None

5. Click **Next**.
6. Accept the license agreements.
7. Select **External Deployment Platform Services Controller** and click **Next**.



Select deployment type

Select the component to deploy.

vCenter Server 6.0.0 requires a Platform Services Controller, which contains shared services such as vCenter Single Sign-On, Licensing, and Certificate Management. An embedded Platform Services Controller is deployed on the same Windows Host as vCenter Server. An external Platform Services Controllers is deployed in a separate Windows Host. For smaller installations, consider vCenter Server with an embedded Platform Services Controller. For larger installations with multiple vCenter Servers, consider one or more Platform Services Controllers. Refer to product documentation for more information.

Note: Once you deploy vCenter Server, you can only change from an embedded to an external Platform Services Controller with a fresh install.

Embedded Deployment

○ vCenter Server and Embedded Platform Services Controller

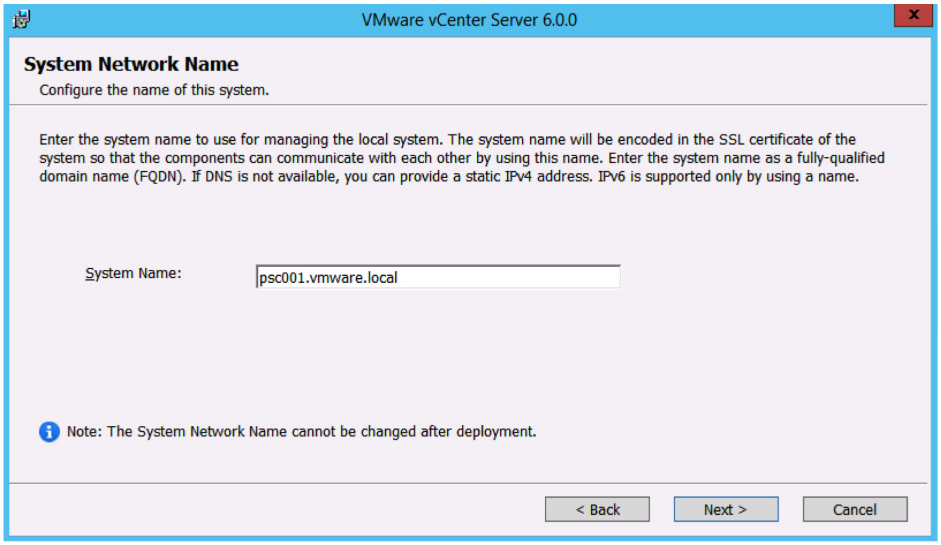
External Deployment

● Platform Services Controller

○ vCenter Server

A previously installed Platform Services Controller is required

8. Verify the system name and click **Next**.



VMware vCenter Server 6.0

System Network Name

Configure the name of this system.

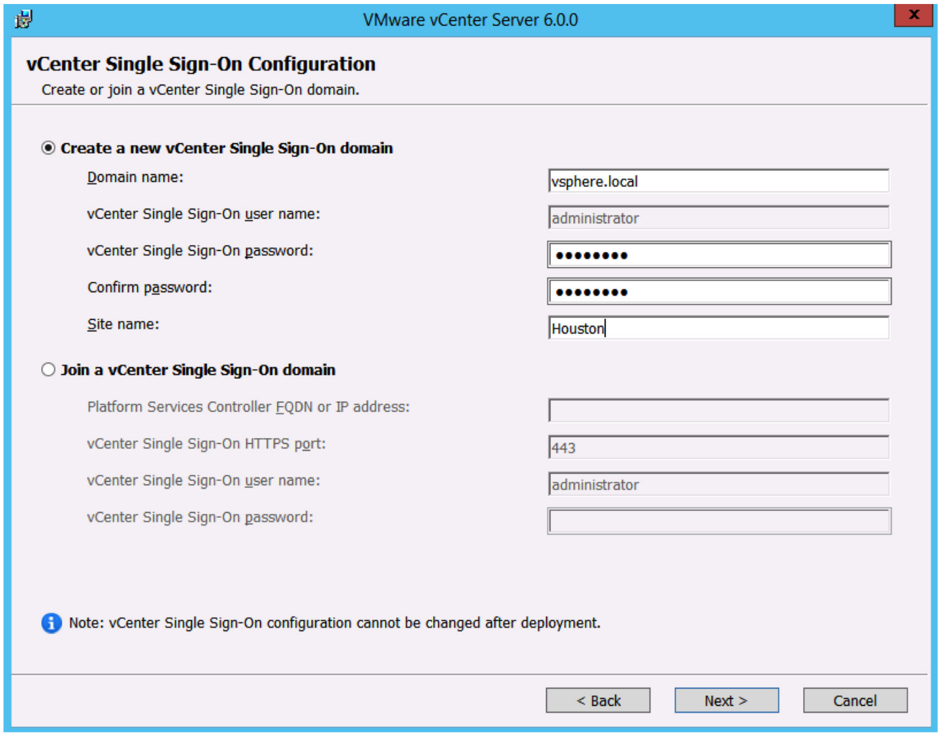
Enter the system name to use for managing the local system. The system name will be encoded in the SSL certificate of the system so that the components can communicate with each other by using this name. Enter the system name as a fully-qualified domain name (FQDN). If DNS is not available, you can provide a static IPv4 address. IPv6 is supported only by using a name.

System Name: psc001.vmware.local

Note: The System Network Name cannot be changed after deployment.

9. If this is the first Platform Services Controller, select **Create a new vCenter Single Sign-On domain**. If this is an additional Platform Services Controller, select **Join a vCenter Single Sign-On domain**.

    a. For a new vCenter Single Sign-On domain, enter a **password** for the vCenter Single Sign-On administrator, a **Domain name** such as vsphere.local, and a **Site name** such as a city or physical building name.



VMware vCenter Server 6.0

vCenter Single Sign-On Configuration

Create or join a vCenter Single Sign-On domain.

● **Create a new vCenter Single Sign-On domain**

Domain name: vsphere.local

vCenter Single Sign-On user name: administrator

vCenter Single Sign-On password: ••••••••

Confirm password: ••••••••

Site name: Houston

○ **Join a vCenter Single Sign-On domain**

Platform Services Controller FQDN or IP address:

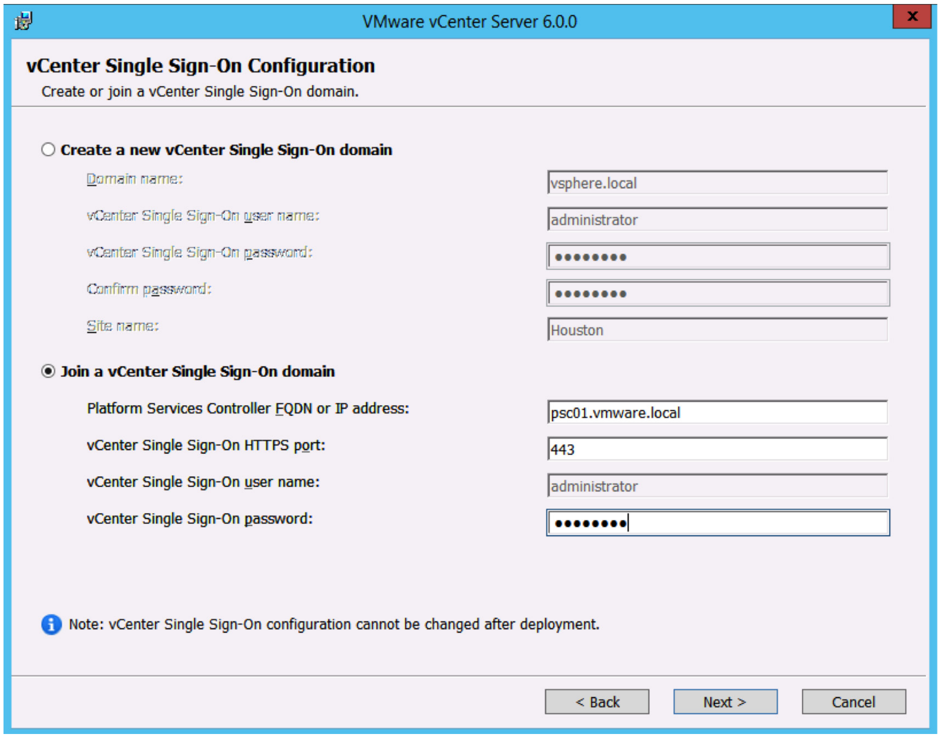
vCenter Single Sign-On HTTPS port: 443

vCenter Single Sign-On user name: administrator

vCenter Single Sign-On password:

Note: vCenter Single Sign-On configuration cannot be changed after deployment.

b. To join an existing vCenter Single Sign-On domain, enter the FQDN of an existing Platform Services Controller and the vCenter Single Sign-On administrator's password. Click **Next**. Choose a site to join from the drop-down list. Click **Next**.



vCenter Single Sign-On Configuration

Create or join a vCenter Single Sign-On domain.

○ Create a new vCenter Single Sign-On domain

Domain name: vsphere.local

vCenter Single Sign-On user name: administrator

vCenter Single Sign-On password: ••••••••

Confirm password: ••••••••

Site name: Houston

● Join a vCenter Single Sign-On domain

Platform Services Controller FQDN or IP address: psc01.vmware.local

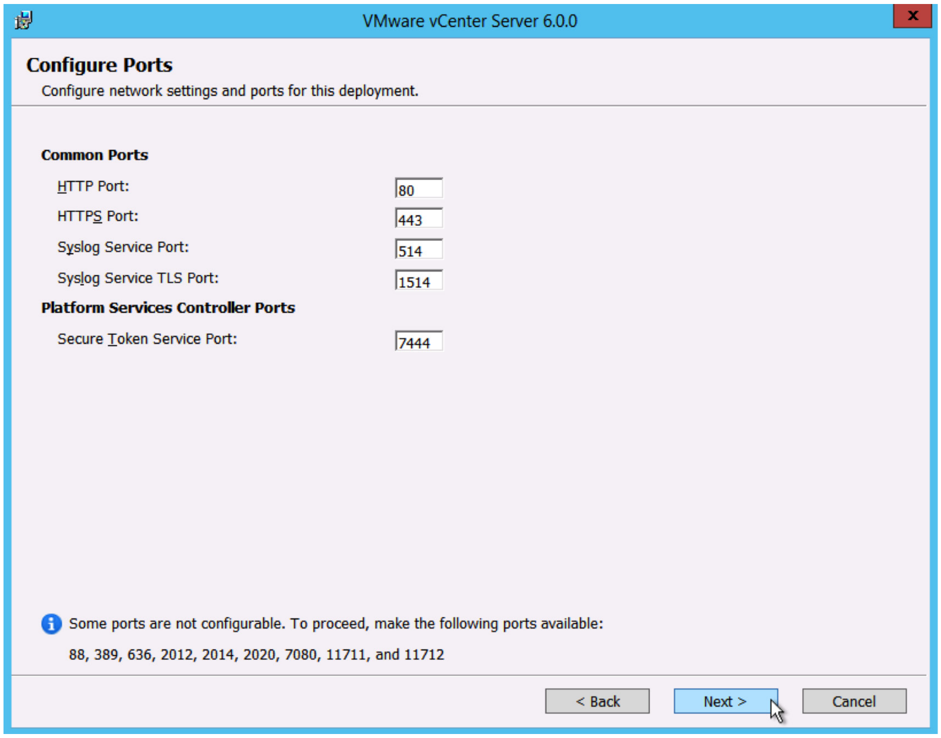
vCenter Single Sign-On HTTPS port: 443

vCenter Single Sign-On user name: administrator

vCenter Single Sign-On password: ••••••••

Note: vCenter Single Sign-On configuration cannot be changed after deployment.

10. Accept the default ports and click **Next**.



Configure Ports

Configure network settings and ports for this deployment.

Common Ports

HTTP Port: 80

HTTPS Port: 443

Syslog Service Port: 514

Syslog Service TLS Port: 1514

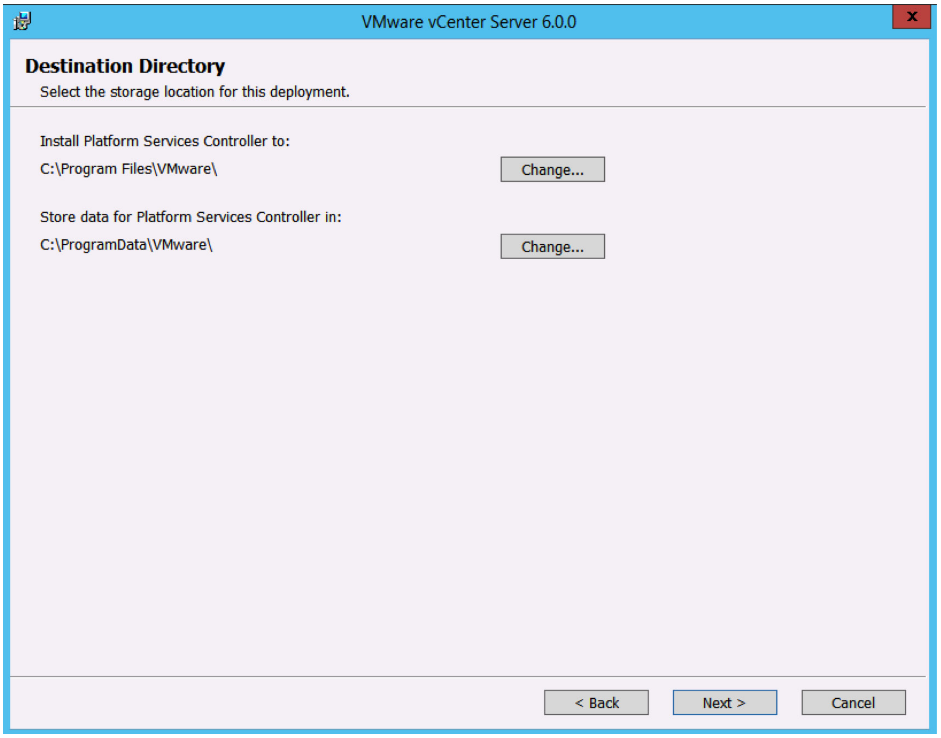
Platform Services Controller Ports

Secure Token Service Port: 7444

Some ports are not configurable. To proceed, make the following ports available:

88, 389, 636, 2012, 2014, 2020, 7080, 11711, and 11712

11. Accept or change the installation paths as necessary. Click **Next**.



Destination Directory

Select the storage location for this deployment.

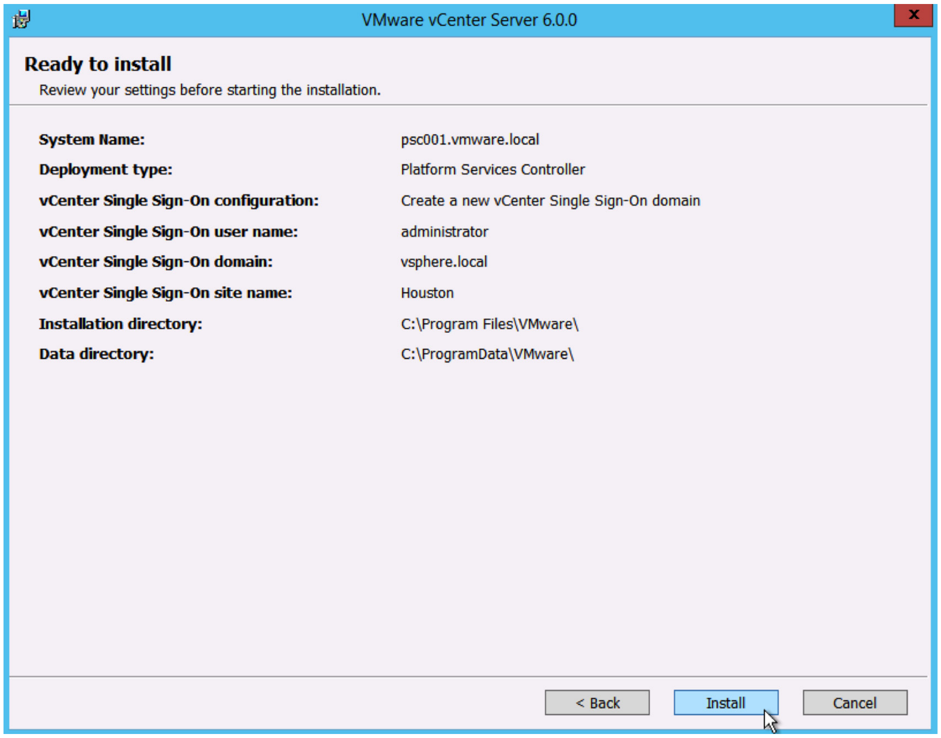
Install Platform Services Controller to:

C:\Program Files\VMware\

Store data for Platform Services Controller in:

C:\ProgramData\VMware\

12. Review and click **Install**.



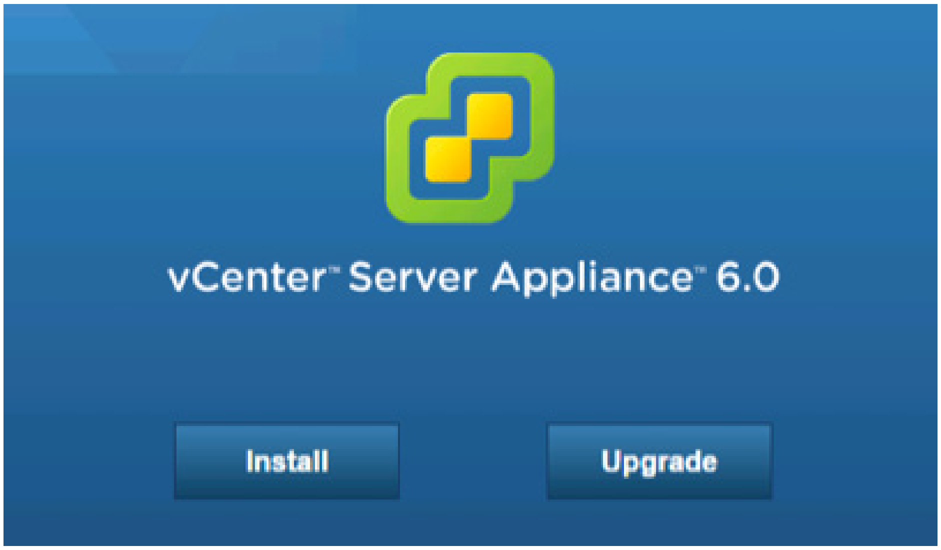
Ready to install

Review your settings before starting the installation.

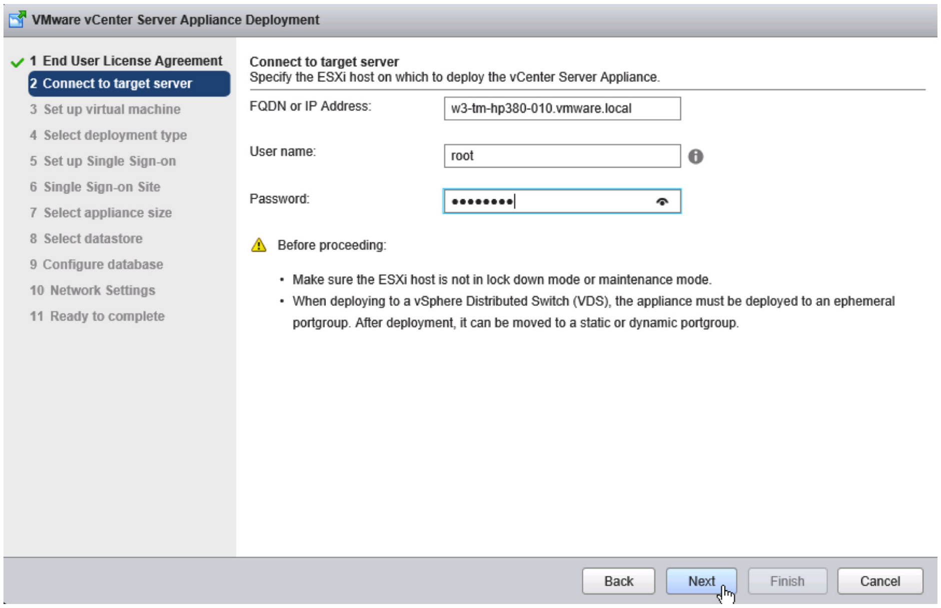
System Name:	psc001.vmware.local
Deployment type:	Platform Services Controller
vCenter Single Sign-On configuration:	Create a new vCenter Single Sign-On domain
vCenter Single Sign-On user name:	administrator
vCenter Single Sign-On domain:	vsphere.local
vCenter Single Sign-On site name:	Houston
Installation directory:	C:\Program Files\VMware\
Data directory:	C:\ProgramData\VMware\

vCenter Server Appliance Deployment

1. Mount the ISO image on a PC.
2. Open the vcsa folder and install the plug-in.
3. In the root of the ISO image, double-click the vcsa-setup.html file.
4. Wait until you are prompted to enable the client integration plug-in to run. Click **Install**.



5. Accept the license agreement and click **Next.**
6. Enter a target host and a **User name** and **Password** on the host with root access.



Connect to target server
Specify the ESXi host on which to deploy the vCenter Server Appliance.

FQDN or IP Address: w3-tm-hp380-010.vmware.local

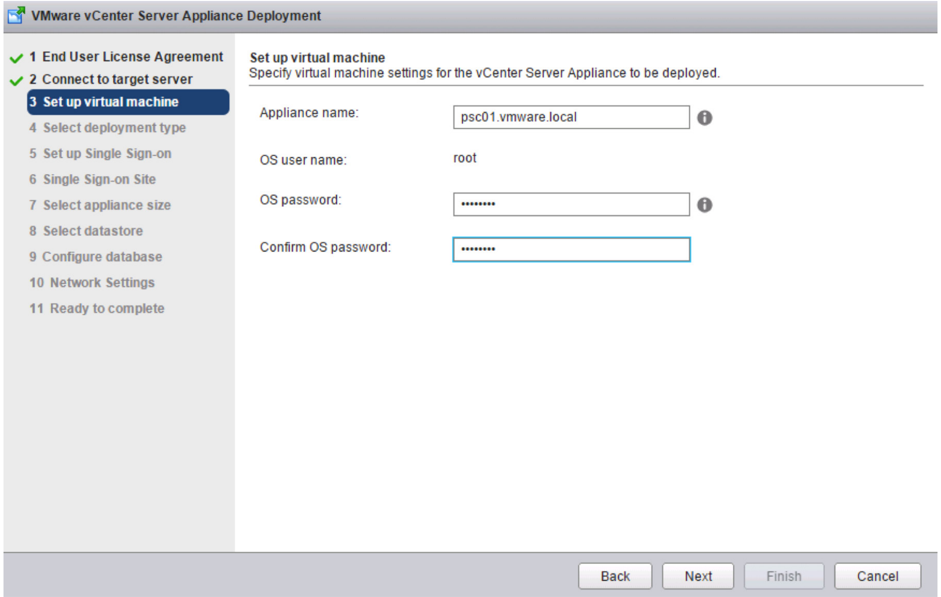
User name: root

Password: ••••••••

Before proceeding:

- Make sure the ESXi host is not in lock down mode or maintenance mode.
- When deploying to a vSphere Distributed Switch (VDS), the appliance must be deployed to an ephemeral portgroup. After deployment, it can be moved to a static or dynamic portgroup.

7. Click **Yes** to accept the host's certificate.
8. Enter an **Appliance name** and the root **password** you want to assign. Click **Next**.



Set up virtual machine
Specify virtual machine settings for the vCenter Server Appliance to be deployed.

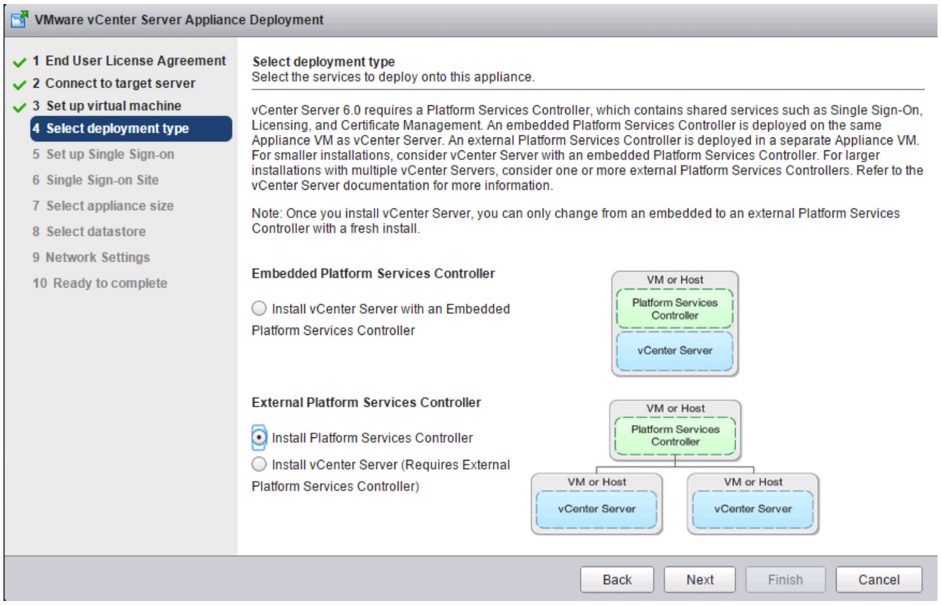
Appliance name: psc01.vmware.local

OS user name: root

OS password: ••••••••

Confirm OS password: ••••••••

9. Under **External Platform Services Controller**, select **Install Platform Services Controller**. Click **Next**.



Select deployment type
Select the services to deploy onto this appliance.

vCenter Server 6.0 requires a Platform Services Controller, which contains shared services such as Single Sign-On, Licensing, and Certificate Management. An embedded Platform Services Controller is deployed on the same Appliance VM as vCenter Server. An external Platform Services Controller is deployed in a separate Appliance VM. For smaller installations, consider vCenter Server with an embedded Platform Services Controller. For larger installations with multiple vCenter Servers, consider one or more external Platform Services Controllers. Refer to the vCenter Server documentation for more information.

Note: Once you install vCenter Server, you can only change from an embedded to an external Platform Services Controller with a fresh install.

Embedded Platform Services Controller

○ Install vCenter Server with an Embedded Platform Services Controller

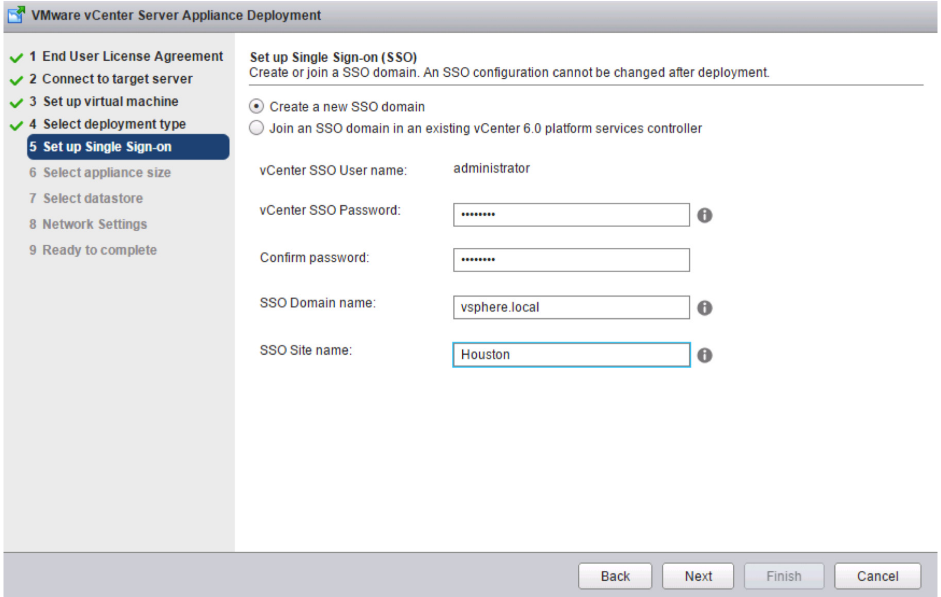
External Platform Services Controller

● Install Platform Services Controller

○ Install vCenter Server (Requires External Platform Services Controller)

10. If this is the first Platform Services Controller, select **Create a new SSO domain**. If this is an additional Platform Services Controller, select **Join an SSO Domain**.

    a. For a new vCenter Single Sign-On domain, enter an administrator **vCenter SSO Password**, an **SSO Domain name** such as vsphere.local, and an **SSO Site name**.



VMware vCenter Server Appliance Deployment

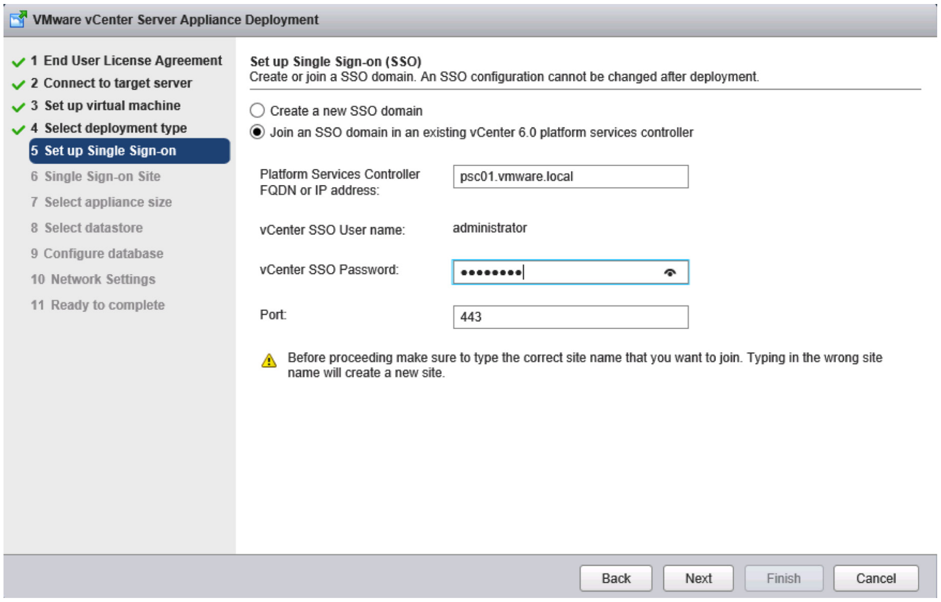
- ✓ 1 End User License Agreement
- ✓ 2 Connect to target server
- ✓ 3 Set up virtual machine
- ✓ 4 Select deployment type
- 5 Set up Single Sign-on
- 6 Select appliance size
- 7 Select datastore
- 8 Network Settings
- 9 Ready to complete

Set up Single Sign-on (SSO)
Create or join a SSO domain. An SSO configuration cannot be changed after deployment.

● Create a new SSO domain
○ Join an SSO domain in an existing vCenter 6.0 platform services controller

vCenter SSO User name: administrator
vCenter SSO Password: ••••••••
Confirm password: ••••••••
SSO Domain name: vsphere.local
SSO Site name: Houston

b. To join an existing vCenter Single Sign-On domain, enter the FQDN of an existing Platform Services Controller and the vCenter Single Sign-On administrator's password. Then click **Next**. Choose a site to join from the drop-down list. Click **Next**.



VMware vCenter Server Appliance Deployment

- ✓ 1 End User License Agreement
- ✓ 2 Connect to target server
- ✓ 3 Set up virtual machine
- ✓ 4 Select deployment type
- 5 Set up Single Sign-on
- 6 Single Sign-on Site
- 7 Select appliance size
- 8 Select datastore
- 9 Configure database
- 10 Network Settings
- 11 Ready to complete

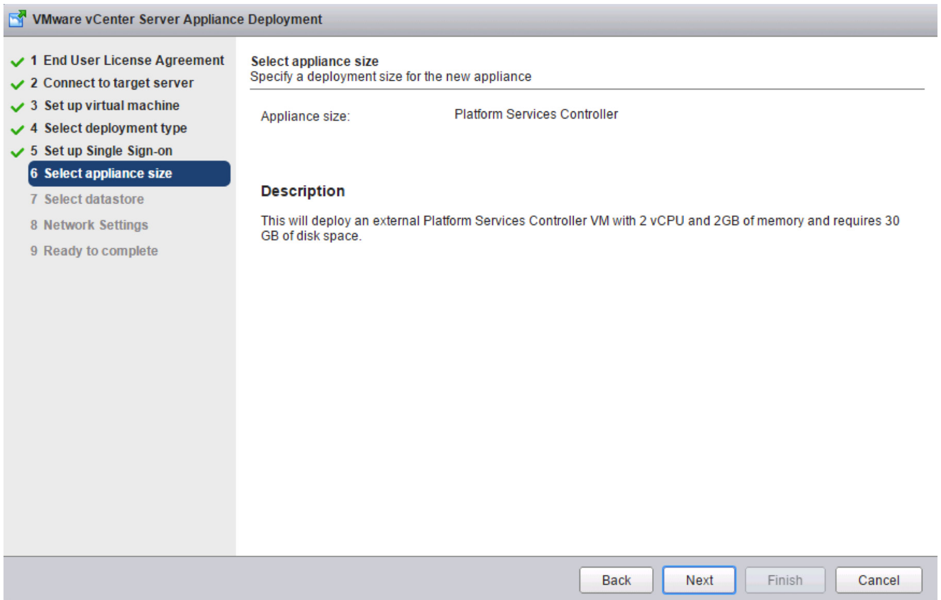
Set up Single Sign-on (SSO)
Create or join a SSO domain. An SSO configuration cannot be changed after deployment.

○ Create a new SSO domain
● Join an SSO domain in an existing vCenter 6.0 platform services controller

Platform Services Controller FQDN or IP address: psc01.vmware.local
vCenter SSO User name: administrator
vCenter SSO Password: ••••••••
Port: 443

⚠ Before proceeding make sure to type the correct site name that you want to join. Typing in the wrong site name will create a new site.

11. Click **Next**. There is only one appliance size for the Platform Services Controller.


VMware vCenter Server Appliance Deployment
✓ 1 End User License Agreement
✓ 2 Connect to target server
✓ 3 Set up virtual machine
✓ 4 Select deployment type
✓ 5 Set up Single Sign-on
6 Select appliance size
7 Select datastore
8 Network Settings
9 Ready to complete
Back
Next
Finish
Cancel

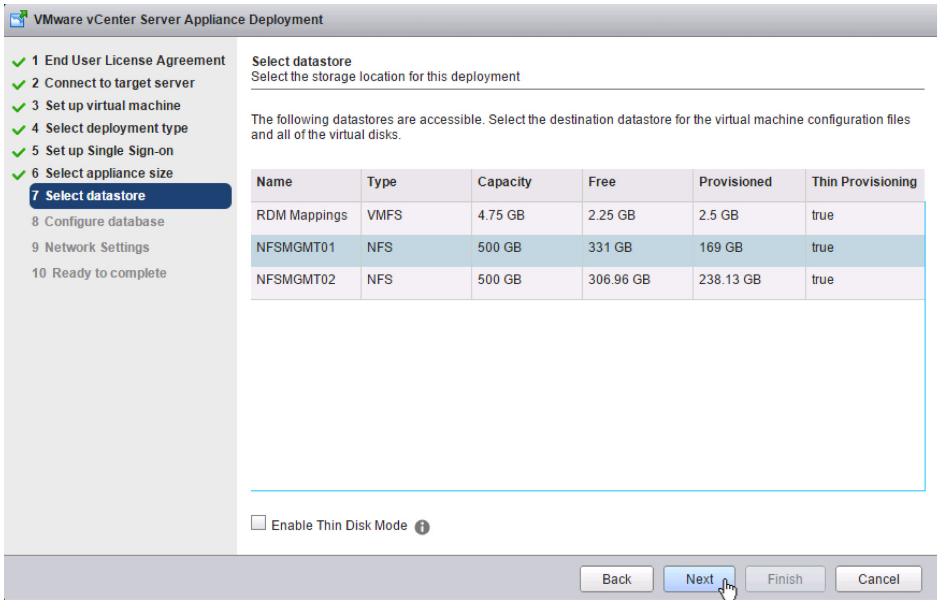
Select appliance size
Specify a deployment size for the new appliance

Appliance size: Platform Services Controller

Description

This will deploy an external Platform Services Controller VM with 2 vCPU and 2GB of memory and requires 30 GB of disk space.

12. Select a datastore to deploy the appliance on and click **Next**.


VMware vCenter Server Appliance Deployment
✓ 1 End User License Agreement
✓ 2 Connect to target server
✓ 3 Set up virtual machine
✓ 4 Select deployment type
✓ 5 Set up Single Sign-on
✓ 6 Select appliance size
7 Select datastore
8 Configure database
9 Network Settings
10 Ready to complete
Back
Next
Finish
Cancel

Select datastore
Select the storage location for this deployment

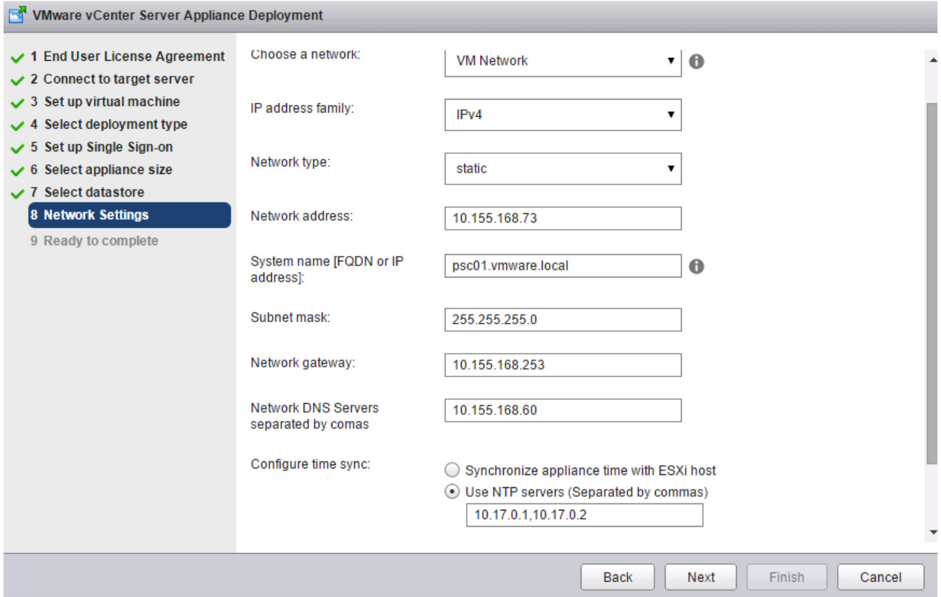
The following datastores are accessible. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Type	Capacity	Free	Provisioned	Thin Provisioning
RDM Mappings	VMFS	4.75 GB	2.25 GB	2.5 GB	true
NFSMGMT01	NFS	500 GB	331 GB	169 GB	true
NFSMGMT02	NFS	500 GB	306.96 GB	238.13 GB	true

☐ Enable Thin Disk Mode

13. Enter **Network Settings** and click **Next**.

NOTE: The FQDN and IP addresses entered here must be resolvable by the DNS server specified or the deployment will fail.


VMware vCenter Server Appliance Deployment
✓ 1 End User License Agreement
✓ 2 Connect to target server
✓ 3 Set up virtual machine
✓ 4 Select deployment type
✓ 5 Set up Single Sign-on
✓ 6 Select appliance size
✓ 7 Select datastore
8 Network Settings
9 Ready to complete
Back
Next
Finish
Cancel

Choose a network: VM Network

IP address family: IPv4

Network type: static

Network address: 10.155.168.73

System name [FQDN or IP address]: psc01.vmware.local

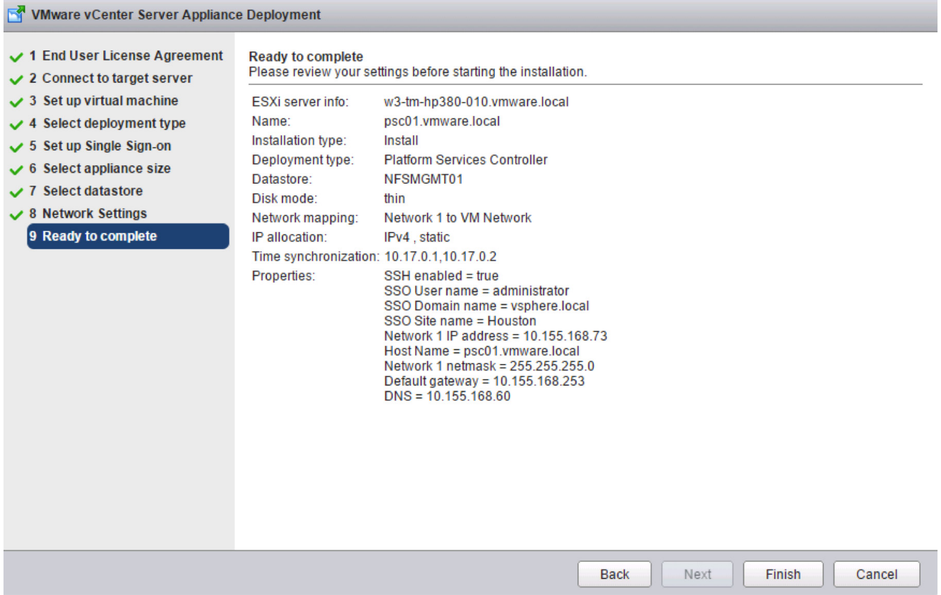
Subnet mask: 255.255.255.0

Network gateway: 10.155.168.253

Network DNS Servers separated by comas: 10.155.168.60

Configure time sync:
○ Synchronize appliance time with ESXi host
● Use NTP servers (Separated by commas)
10.17.0.1,10.17.0.2

14. Review and click **Finish**.


VMware vCenter Server Appliance Deployment
✓ 1 End User License Agreement
✓ 2 Connect to target server
✓ 3 Set up virtual machine
✓ 4 Select deployment type
✓ 5 Set up Single Sign-on
✓ 6 Select appliance size
✓ 7 Select datastore
✓ 8 Network Settings
9 Ready to complete
Back
Next
Finish
Cancel

Ready to complete
Please review your settings before starting the installation.

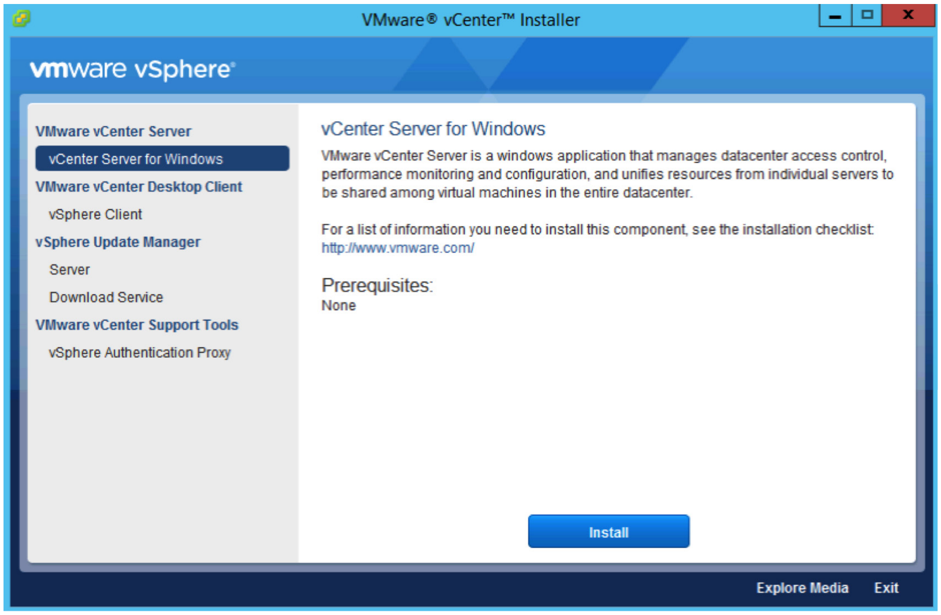
ESXi server info:	w3-tm-hp380-010.vmware.local
Name:	psc01.vmware.local
Installation type:	Install
Deployment type:	Platform Services Controller
Datastore:	NFSMGMT01
Disk mode:	thin
Network mapping:	Network 1 to VM Network
IP allocation:	IPv4 , static
Time synchronization:	10.17.0.1,10.17.0.2
Properties:	SSH enabled = true SSO User name = administrator SSO Domain name = vsphere.local SSO Site name = Houston Network 1 IP address = 10.155.168.73 Host Name = psc01.vmware.local Network 1 netmask = 255.255.255.0 Default gateway = 10.155.168.253 DNS = 10.155.168.60

Fresh External vCenter Server Deployment

Windows Deployment

1. Verify all prerequisites.
2. If using a remote database, ensure that a 64-bit DSN has been created. This step is not necessary if using the local PostgreSQL database.
3. Mount the vCenter Server 6.0 ISO image.
4. If autorun does not start, execute autorun.exe.

5. Select **vCenter Server for Windows** and click **Install**.


VMware® vCenter™ Installer
vmware vSphere
VMware vCenter Server
vCenter Server for Windows
VMware vCenter Desktop Client
vSphere Client
vSphere Update Manager
Server
Download Service
VMware vCenter Support Tools
vSphere Authentication Proxy
Install
Explore Media
Exit

vCenter Server for Windows

VMware vCenter Server is a windows application that manages datacenter access control, performance monitoring and configuration, and unifies resources from individual servers to be shared among virtual machines in the entire datacenter.

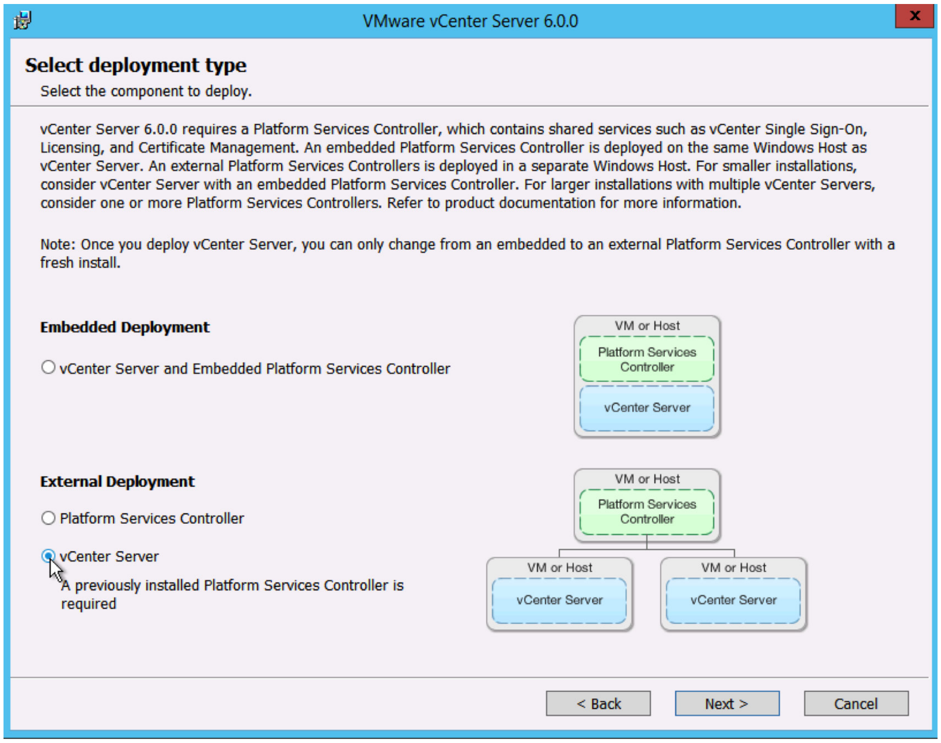
For a list of information you need to install this component, see the installation checklist: http://www.vmware.com/

Prerequisites:
None

6. Click **Next**.

7. Accept the license agreements.

8. Under **External Deployment**, select **vCenter Server**. Click **Next**.



Select deployment type
Select the component to deploy.

vCenter Server 6.0.0 requires a Platform Services Controller, which contains shared services such as vCenter Single Sign-On, Licensing, and Certificate Management. An embedded Platform Services Controller is deployed on the same Windows Host as vCenter Server. An external Platform Services Controllers is deployed in a separate Windows Host. For smaller installations, consider vCenter Server with an embedded Platform Services Controller. For larger installations with multiple vCenter Servers, consider one or more Platform Services Controllers. Refer to product documentation for more information.

Note: Once you deploy vCenter Server, you can only change from an embedded to an external Platform Services Controller with a fresh install.

Embedded Deployment

○ vCenter Server and Embedded Platform Services Controller

External Deployment

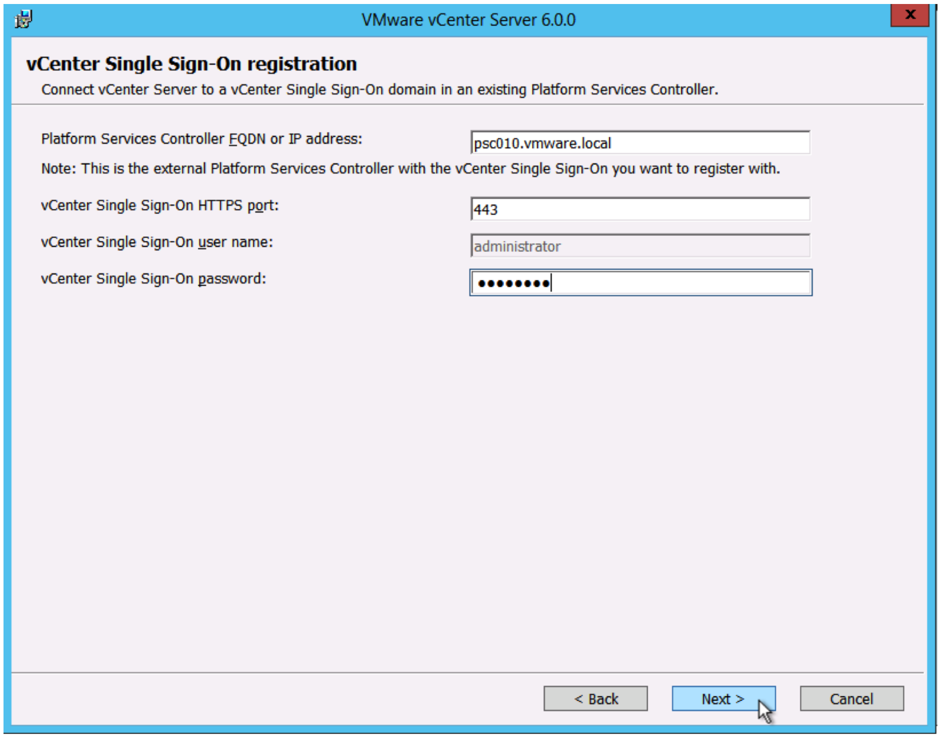
○ Platform Services Controller

● vCenter Server

A previously installed Platform Services Controller is required

9. Verify that the FQDN is correct and click **Next**.

10. Enter the external **Platform Services Controller FQDN** and **vCenter Single Sign-On password**. Click **Enter**.



VMware vCenter Server 6.0.0

vCenter Single Sign-On registration

Connect vCenter Server to a vCenter Single Sign-On domain in an existing Platform Services Controller.

Platform Services Controller FQDN or IP address: psc010.vmware.local

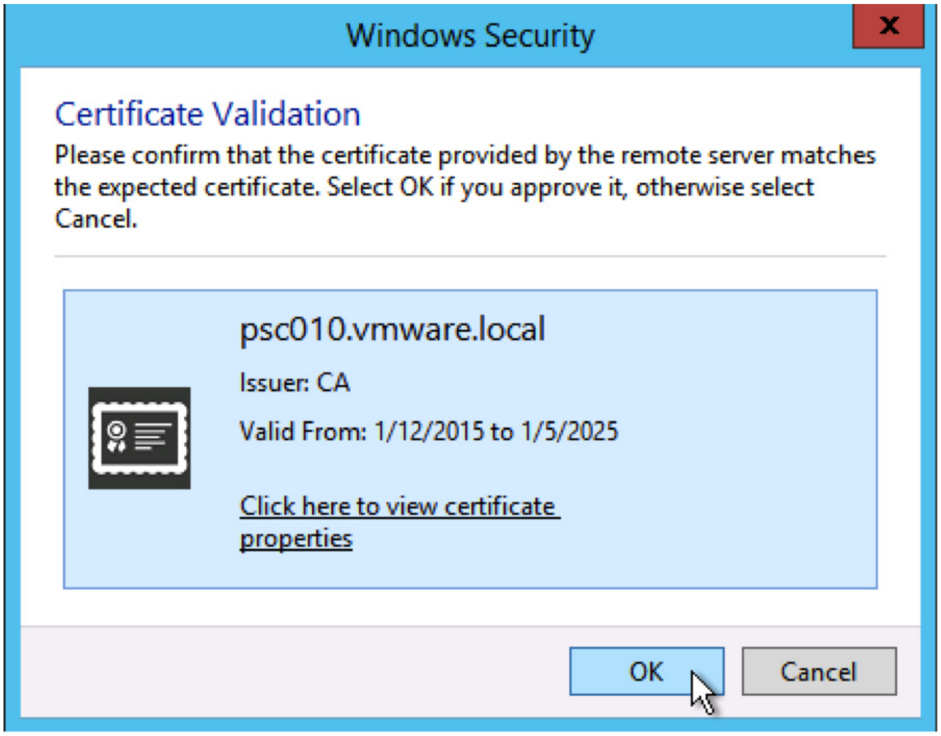
Note: This is the external Platform Services Controller with the vCenter Single Sign-On you want to register with.

vCenter Single Sign-On HTTPS port: 443

vCenter Single Sign-On user name: administrator

vCenter Single Sign-On password: ••••••••

11. Click **OK** to accept the certificate.



Windows Security

Certificate Validation

Please confirm that the certificate provided by the remote server matches the expected certificate. Select OK if you approve it, otherwise select Cancel.

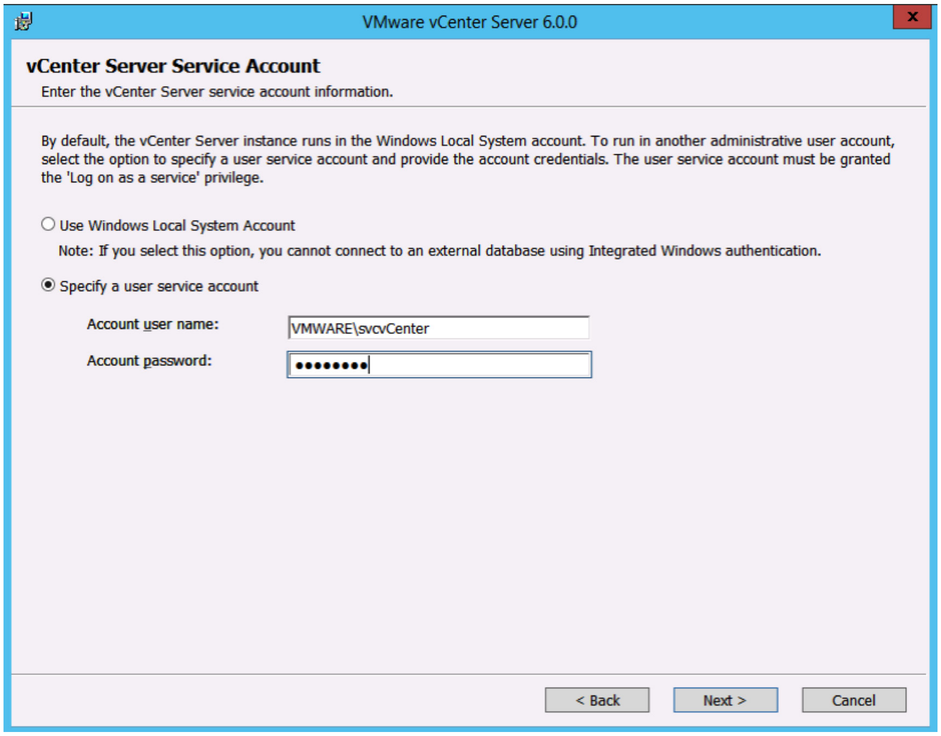
psc010.vmware.local

Issuer: CA

Valid From: 1/12/2015 to 1/5/2025

Click here to view certificate properties

12. Select **Use Windows Local System Account** or enter the service account **user name** and **password**.



VMware vCenter Server 6.0.0

vCenter Server Service Account

Enter the vCenter Server service account information.

By default, the vCenter Server instance runs in the Windows Local System account. To run in another administrative user account, select the option to specify a user service account and provide the account credentials. The user service account must be granted the 'Log on as a service' privilege.

○ Use Windows Local System Account

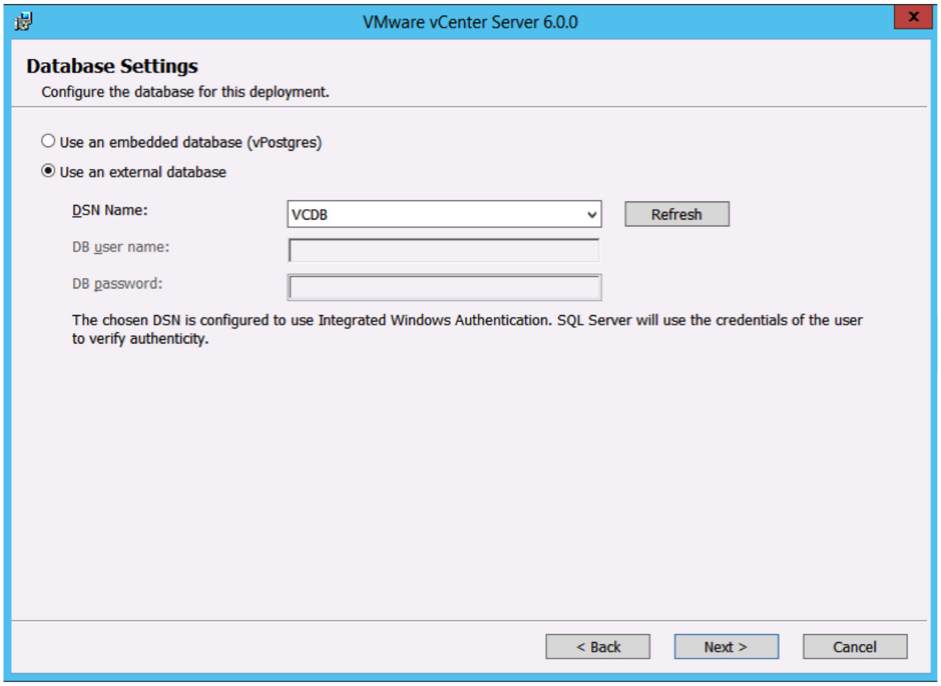
Note: If you select this option, you cannot connect to an external database using Integrated Windows authentication.

● Specify a user service account

Account user name: VMWARE\svcvCenter

Account password: ••••••••

13. Select **Use an embedded database (vPostgres)** or **Use an external database** and enter the server's **DSN Name**. Click **Next**.



VMware vCenter Server 6.0.0

Database Settings

Configure the database for this deployment.

○ Use an embedded database (vPostgres)

● Use an external database

DSN Name: VCDB

DB user name:

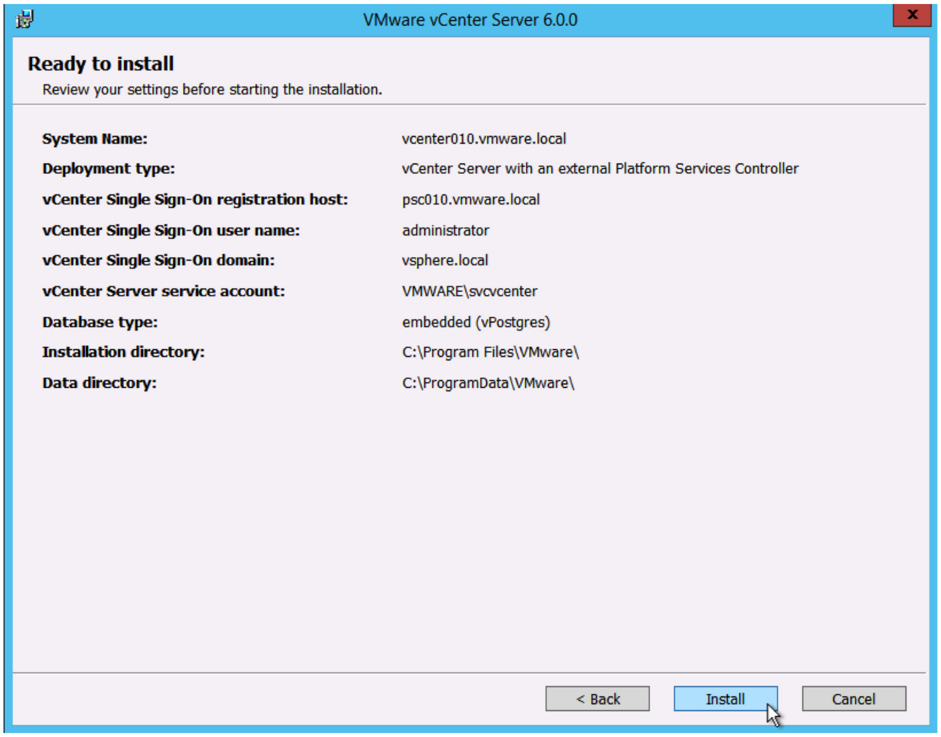
DB password:

The chosen DSN is configured to use Integrated Windows Authentication. SQL Server will use the credentials of the user to verify authenticity.

14. Unless required, leave all ports at their defaults and click **Next**.

15. Unless required, leave the default paths for installation and click **Next**.

16. Review and then click **Install**.



VMware vCenter Server 6.0.0

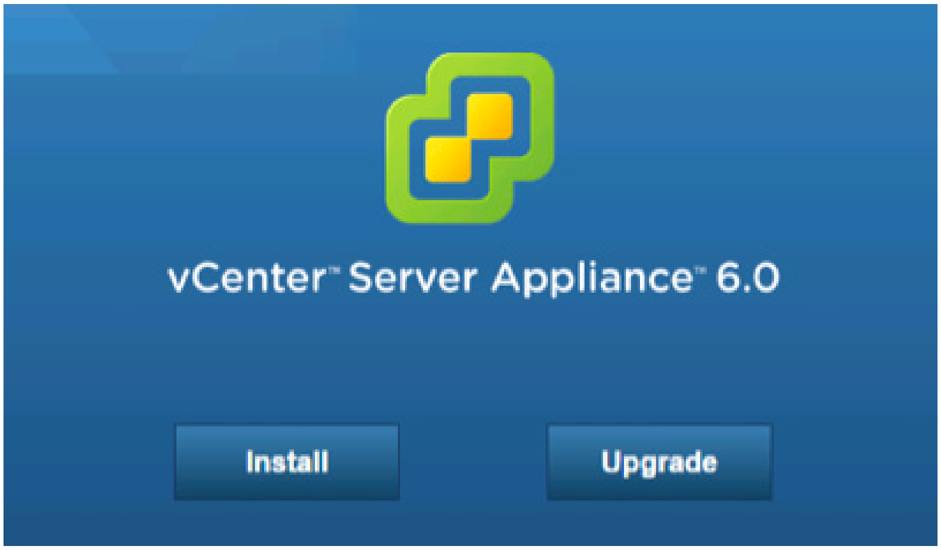
Ready to install

Review your settings before starting the installation.

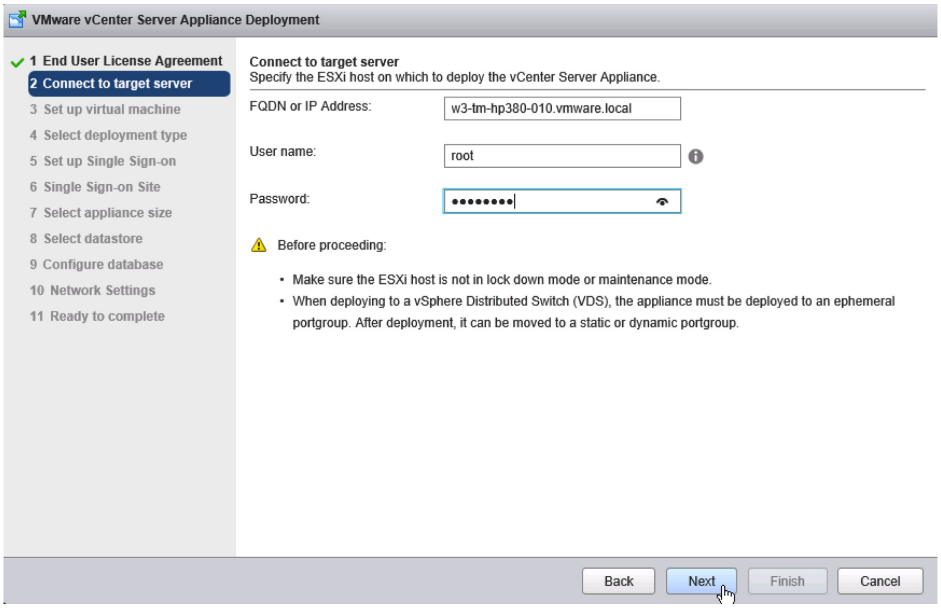
System Name:	vcenter010.vmware.local
Deployment type:	vCenter Server with an external Platform Services Controller
vCenter Single Sign-On registration host:	psc010.vmware.local
vCenter Single Sign-On user name:	administrator
vCenter Single Sign-On domain:	vsphere.local
vCenter Server service account:	VMWARE\svcvcenter
Database type:	embedded (vPostgres)
Installation directory:	C:\Program Files\VMware\
Data directory:	C:\ProgramData\VMware\

vCenter Server Appliance Deployment

1. Mount the ISO image on a PC.
2. Open the vcsa folder and install the plug-in.
3. In the root of the ISO image, double-click the vcsa-setup.html file.
4. Wait until you are prompted to enable the client integration plug-in to run. Click **Install**.



5. Accept the license agreement and click **Next**.
6. Enter a target host, a **user name**, and a **password** on the host with root access.



Connect to target server
Specify the ESXi host on which to deploy the vCenter Server Appliance.

FQDN or IP Address: w3-tm-hp380-010.vmware.local

User name: root

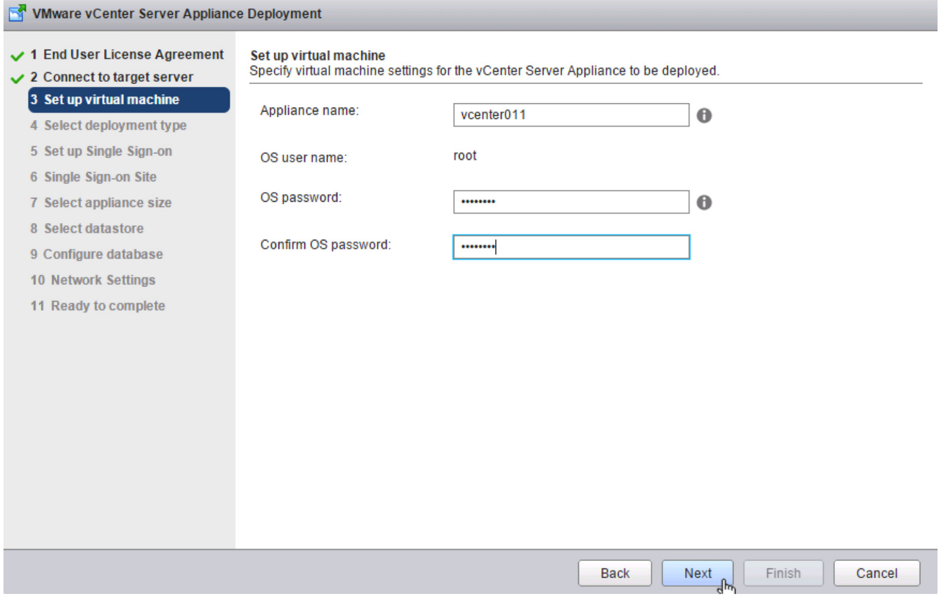
Password: ••••••••

⚠ Before proceeding:

- Make sure the ESXi host is not in lock down mode or maintenance mode.
- When deploying to a vSphere Distributed Switch (VDS), the appliance must be deployed to an ephemeral portgroup. After deployment, it can be moved to a static or dynamic portgroup.

7. Click **Yes** to accept the host's certificate.

8. Enter **Appliance name** and the root **password** you want to assign. Click **Next**.



Set up virtual machine
Specify virtual machine settings for the vCenter Server Appliance to be deployed.

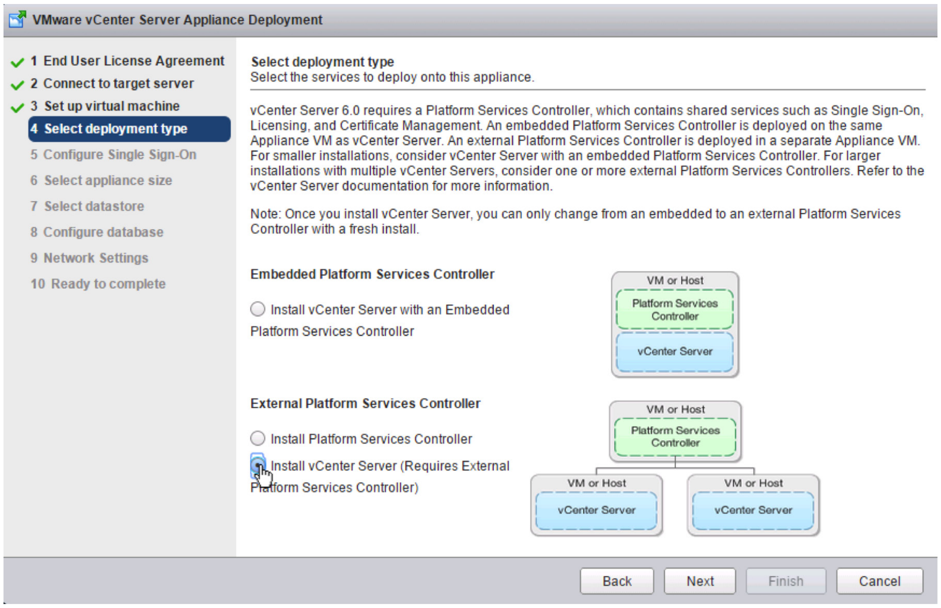
Appliance name: vcenter011

OS user name: root

OS password: ••••••••

Confirm OS password: ••••••••

9. Under **External Platform Services Controller**, select **Install vCenter Server**. Click **Next**.



Select deployment type
Select the services to deploy onto this appliance.

vCenter Server 6.0 requires a Platform Services Controller, which contains shared services such as Single Sign-On, Licensing, and Certificate Management. An embedded Platform Services Controller is deployed on the same Appliance VM as vCenter Server. An external Platform Services Controller is deployed in a separate Appliance VM. For smaller installations, consider vCenter Server with an embedded Platform Services Controller. For larger installations with multiple vCenter Servers, consider one or more external Platform Services Controllers. Refer to the vCenter Server documentation for more information.

Note: Once you install vCenter Server, you can only change from an embedded to an external Platform Services Controller with a fresh install.

Embedded Platform Services Controller

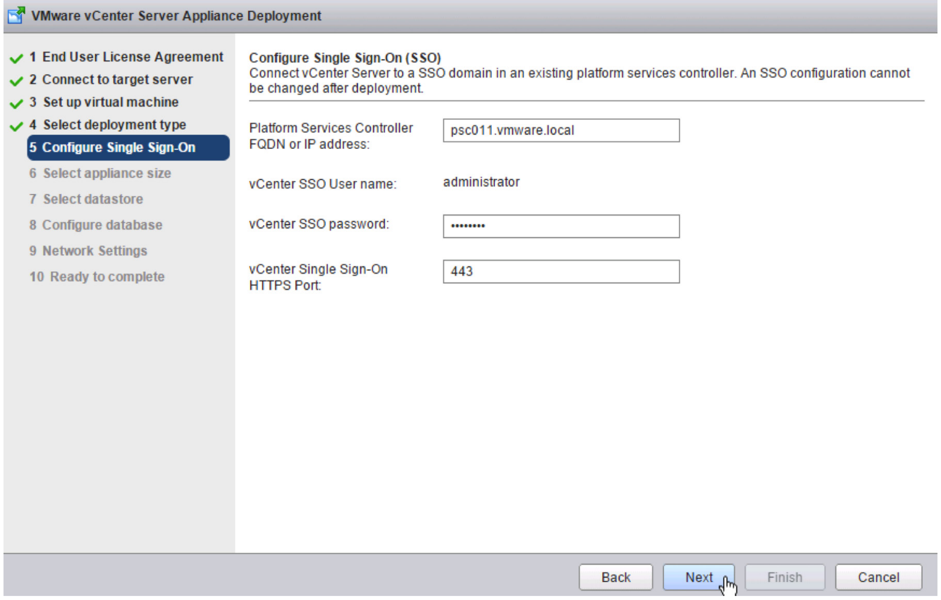
○ Install vCenter Server with an Embedded Platform Services Controller

External Platform Services Controller

○ Install Platform Services Controller

● Install vCenter Server (Requires External Platform Services Controller)

10. Enter the external **Platform Services Controller FQDN** and **vCenter SSO password**. Click **Next**.



Configure Single Sign-On (SSO)
Connect vCenter Server to a SSO domain in an existing platform services controller. An SSO configuration cannot be changed after deployment.

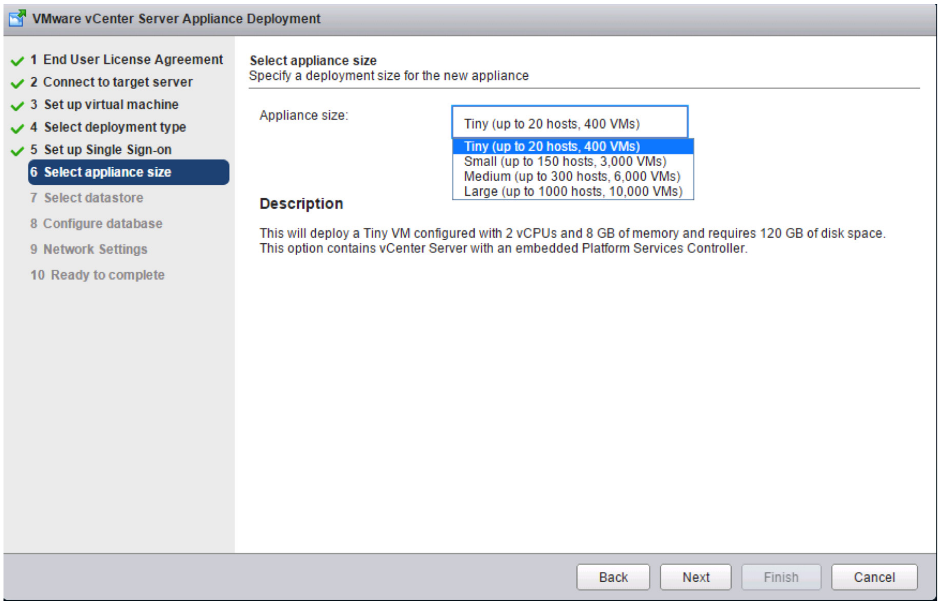
Platform Services Controller FQDN or IP address: psc011.vmware.local

vCenter SSO User name: administrator

vCenter SSO password: ••••••••

vCenter Single Sign-On HTTPS Port: 443

11. Select **Appliance size** from the drop-down list. Click **Next**.


VMware vCenter Server Appliance Deployment
✓ 1 End User License Agreement
✓ 2 Connect to target server
✓ 3 Set up virtual machine
✓ 4 Select deployment type
✓ 5 Set up Single Sign-on
6 Select appliance size
7 Select datastore
8 Configure database
9 Network Settings
10 Ready to complete
Back
Next
Finish
Cancel

Select appliance size
Specify a deployment size for the new appliance

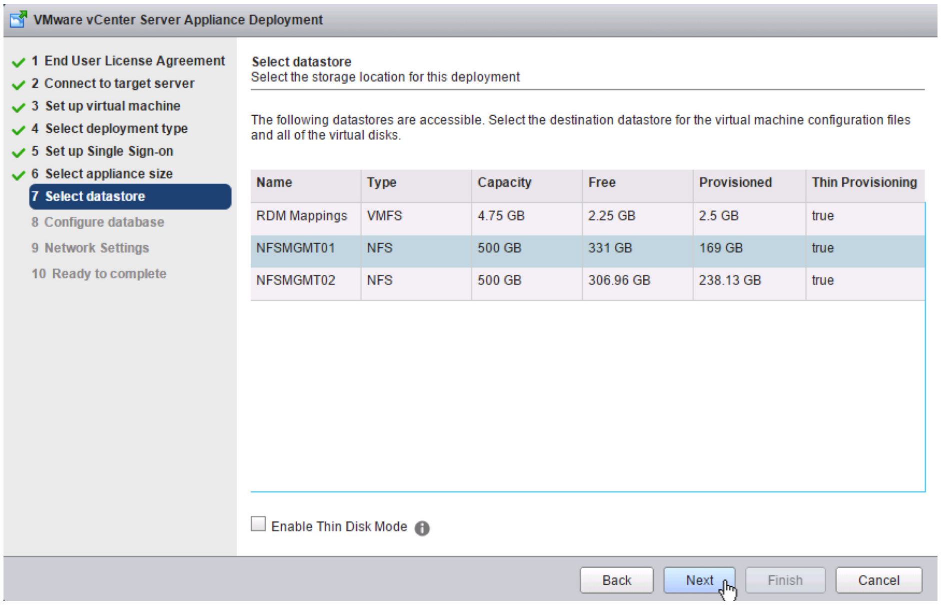
Appliance size: Tiny (up to 20 hosts, 400 VMs)

- Tiny (up to 20 hosts, 400 VMs)
- Small (up to 150 hosts, 3,000 VMs)
- Medium (up to 300 hosts, 6,000 VMs)
- Large (up to 1000 hosts, 10,000 VMs)

Description

This will deploy a Tiny VM configured with 2 vCPUs and 8 GB of memory and requires 120 GB of disk space. This option contains vCenter Server with an embedded Platform Services Controller.

12. **Select datastore** to deploy the appliance on. Click **Next**.


VMware vCenter Server Appliance Deployment
✓ 1 End User License Agreement
✓ 2 Connect to target server
✓ 3 Set up virtual machine
✓ 4 Select deployment type
✓ 5 Set up Single Sign-on
✓ 6 Select appliance size
7 Select datastore
8 Configure database
9 Network Settings
10 Ready to complete
Back
Next
Finish
Cancel

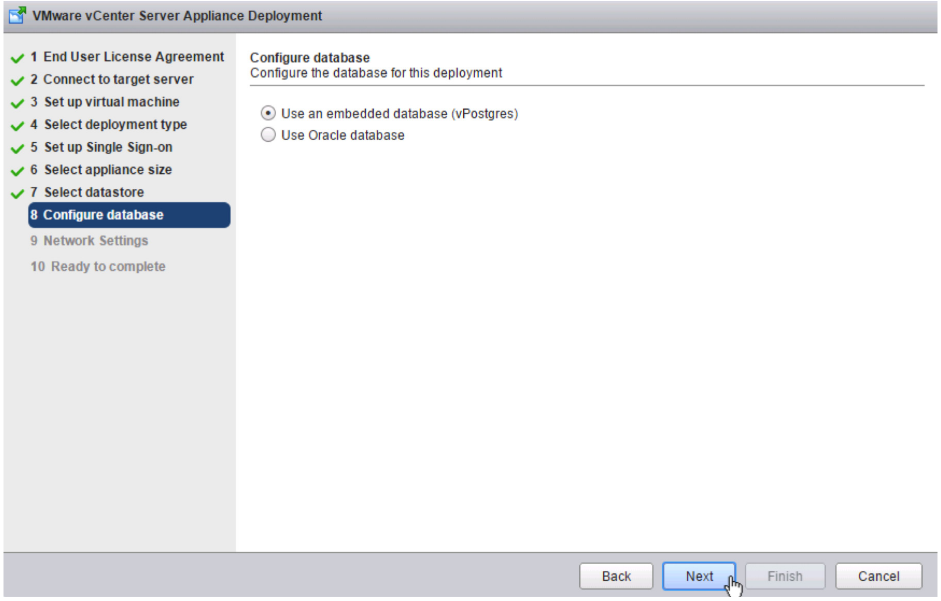
Select datastore
Select the storage location for this deployment

The following datastores are accessible. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Type	Capacity	Free	Provisioned	Thin Provisioning
RDM Mappings	VMFS	4.75 GB	2.25 GB	2.5 GB	true
NFSMGMT01	NFS	500 GB	331 GB	169 GB	true
NFSMGMT02	NFS	500 GB	306.96 GB	238.13 GB	true

☐ Enable Thin Disk Mode

13. Select **Use an embedded database (vPostgres)**, which is recommended, or **Use Oracle database**. Click **Next**.

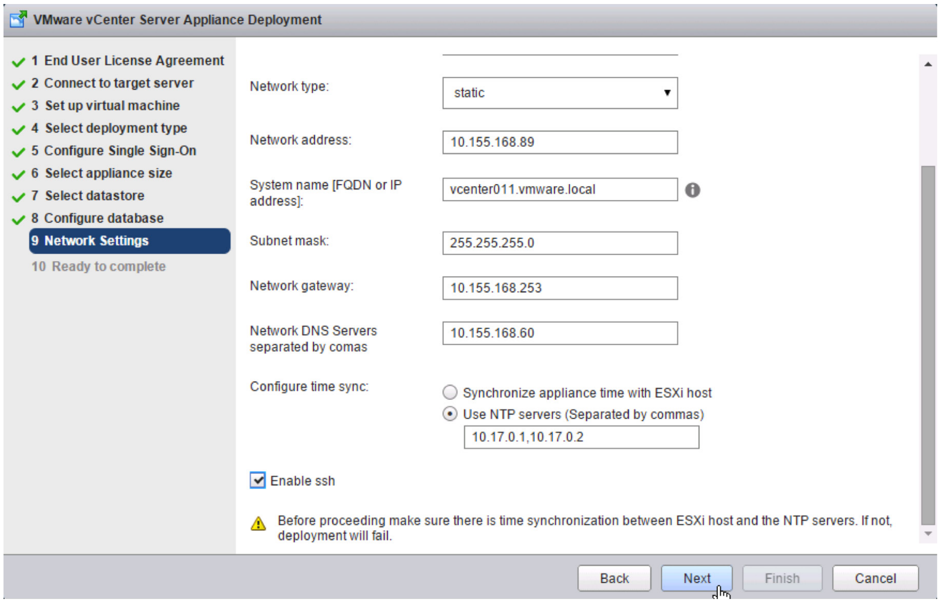


Configure database
Configure the database for this deployment

● Use an embedded database (vPostgres)
○ Use Oracle database

14. Enter **Network settings** and click **Next**.

NOTE: The FQDN or IP address entered here must be resolvable by the DNS server specified or the deployment will fail.



Network type: static

Network address: 10.155.168.89

System name [FQDN or IP address]: vcenter011.vmware.local

Subnet mask: 255.255.255.0

Network gateway: 10.155.168.253

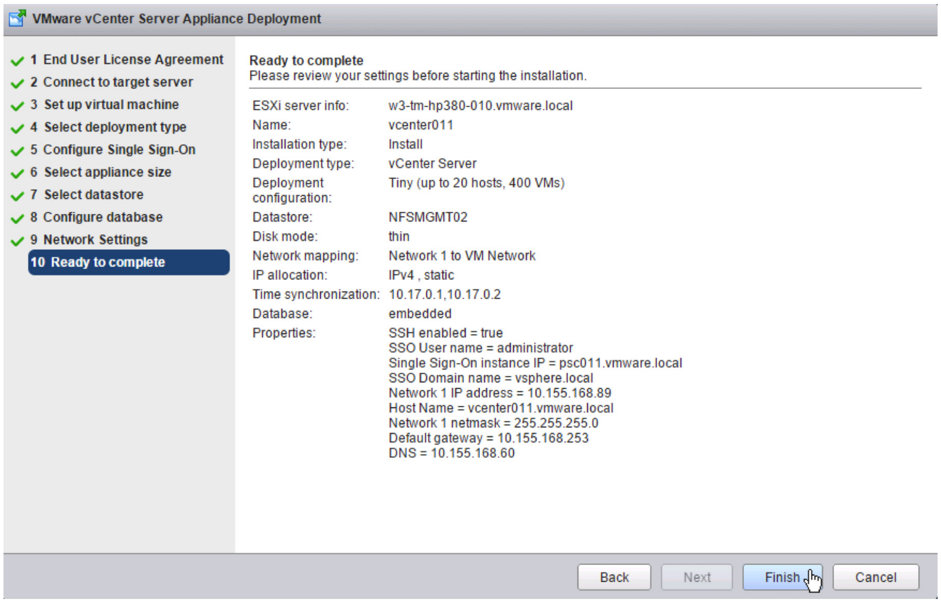
Network DNS Servers separated by comas: 10.155.168.60

Configure time sync:
○ Synchronize appliance time with ESXi host
● Use NTP servers (Separated by commas)
10.17.0.1,10.17.0.2

☑ Enable ssh

⚠ Before proceeding make sure there is time synchronization between ESXi host and the NTP servers. If not, deployment will fail.

15. Review and click **Finish**.

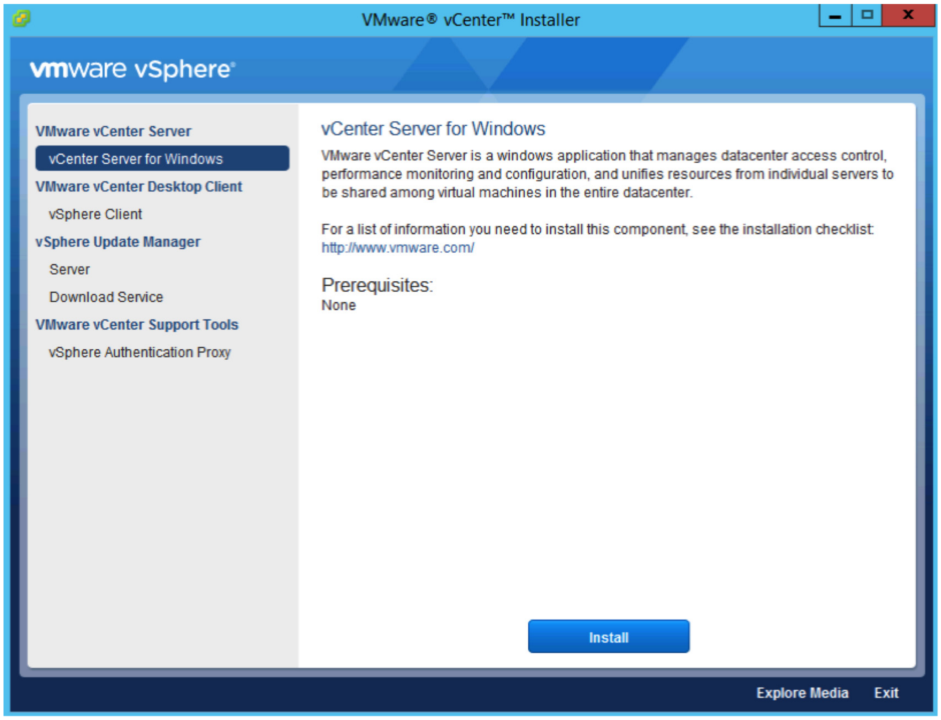

VMware vCenter Server Appliance Deployment
✓ 1 End User License Agreement
✓ 2 Connect to target server
✓ 3 Set up virtual machine
✓ 4 Select deployment type
✓ 5 Configure Single Sign-On
✓ 6 Select appliance size
✓ 7 Select datastore
✓ 8 Configure database
✓ 9 Network Settings
10 Ready to complete
Back
Next
Finish
Cancel

Ready to complete
Please review your settings before starting the installation.

```
ESXi server info:        w3-tm-hp380-010.vmware.local
Name:                    vcenter011
Installation type:       Install
Deployment type:         vCenter Server
Deployment               Tiny (up to 20 hosts, 400 VMs)
configuration:
Datastore:               NFSMGMT02
Disk mode:               thin
Network mapping:         Network 1 to VM Network
IP allocation:           IPv4 , static
Time synchronization:    10.17.0.1,10.17.0.2
Database:                embedded
Properties:              SSH enabled = true
                         SSO User name = administrator
                         Single Sign-On instance IP = psc011.vmware.local
                         SSO Domain name = vsphere.local
                         Network 1 IP address = 10.155.168.89
                         Host Name = vcenter011.vmware.local
                         Network 1 netmask = 255.255.255.0
                         Default gateway = 10.155.168.253
                         DNS = 10.155.168.60
```

Upgrade External vCenter Single Sign-On

1. Back up the vCenter Single Sign-On and vCenter Server machines.
2. Log in to the vCenter Single Sign-On machine.
3. Mount the vCenter Server 6.0 ISO image.
4. If autorun does not start, execute autorun.exe.
5. Select **vCenter Server for Windows** and click **Install**.


VMware® vCenter™ Installer
vmware vSphere
VMware vCenter Server
vCenter Server for Windows
VMware vCenter Desktop Client
vSphere Client
vSphere Update Manager
Server
Download Service
VMware vCenter Support Tools
vSphere Authentication Proxy
Install
Explore Media
Exit

vCenter Server for Windows

VMware vCenter Server is a windows application that manages datacenter access control, performance monitoring and configuration, and unifies resources from individual servers to be shared among virtual machines in the entire datacenter.

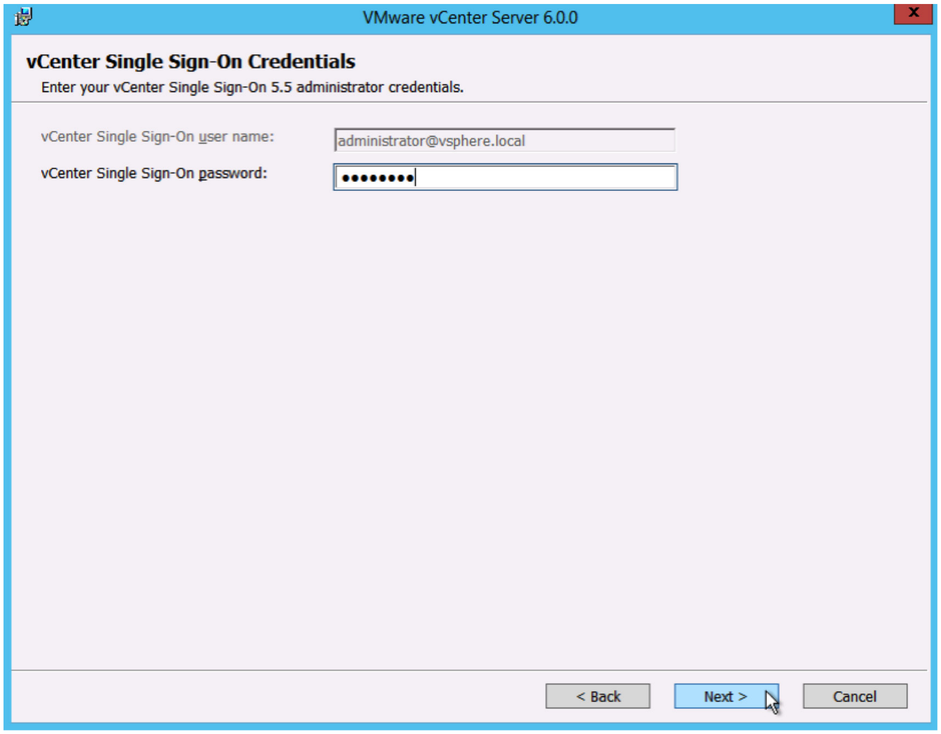
For a list of information you need to install this component, see the installation checklist: http://www.vmware.com/

Prerequisites:
None

6. Click **Next**.

7. Accept the license agreements.

8. Enter the **vCenter Single Sign-On password** for the administrator@vsphere.local account. Click **Next**.



VMware vCenter Server 6.0.0

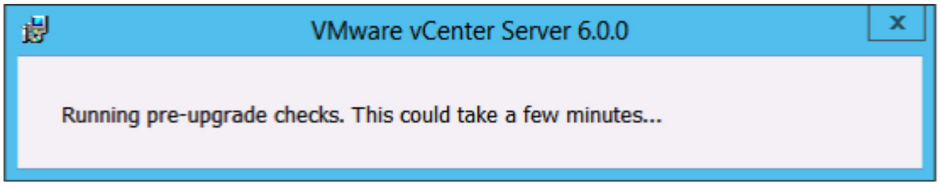
vCenter Single Sign-On Credentials

Enter your vCenter Single Sign-On 5.5 administrator credentials.

vCenter Single Sign-On user name: administrator@vsphere.local

vCenter Single Sign-On password: ••••••••

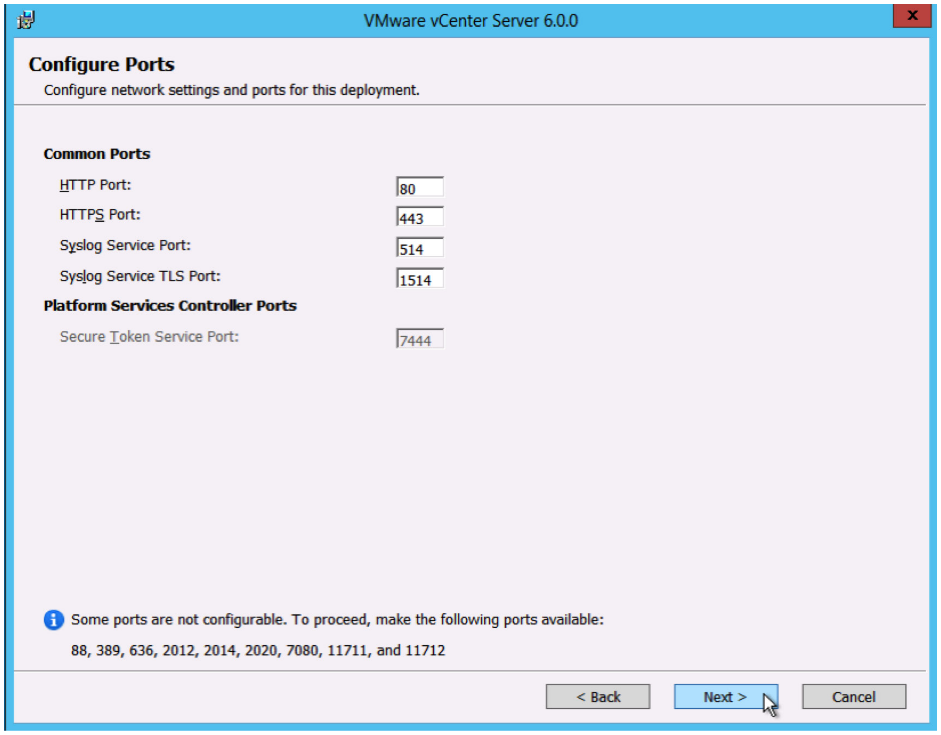
9. Wait for the **pre-upgrade checks** to complete.



VMware vCenter Server 6.0.0

Running pre-upgrade checks. This could take a few minutes...

10. Accept the default ports and click **Next**.



Configure Ports

Configure network settings and ports for this deployment.

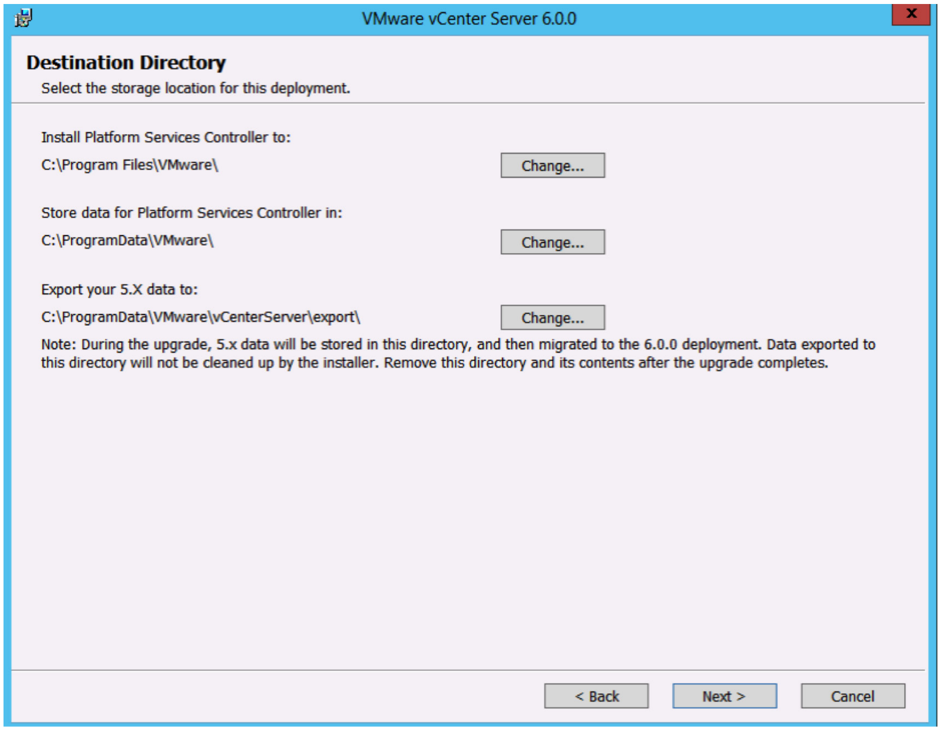
Common Ports

HTTP Port:	80
HTTPS Port:	443
Syslog Service Port:	514
Syslog Service TLS Port:	1514
Platform Services Controller Ports	
Secure Token Service Port:	7444

Some ports are not configurable. To proceed, make the following ports available:

88, 389, 636, 2012, 2014, 2020, 7080, 11711, and 11712

11. Select your installation path or take the defaults. Click **Next**.



Destination Directory

Select the storage location for this deployment.

Install Platform Services Controller to:

C:\Program Files\VMware\

Store data for Platform Services Controller in:

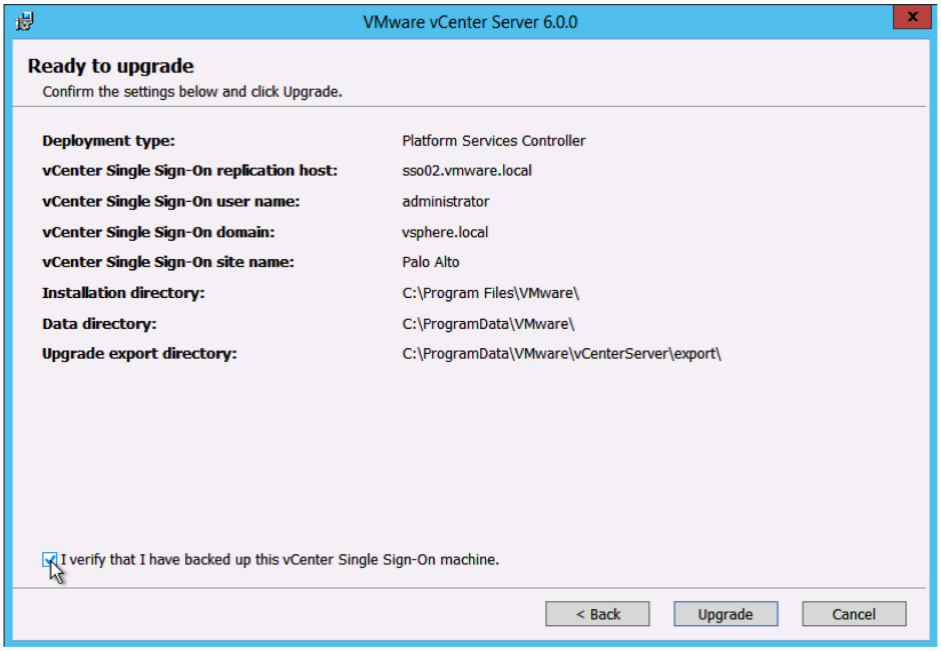
C:\ProgramData\VMware\

Export your 5.X data to:

C:\ProgramData\VMware\vCenterServer\export\

Note: During the upgrade, 5.x data will be stored in this directory, and then migrated to the 6.0.0 deployment. Data exported to this directory will not be cleaned up by the installer. Remove this directory and its contents after the upgrade completes.

12. Check **I verify that I have backed up this vCenter Single Sign-On machine**. Click **Upgrade**.



Ready to upgrade

Confirm the settings below and click Upgrade.

Deployment type:	Platform Services Controller
vCenter Single Sign-On replication host:	sso02.vmware.local
vCenter Single Sign-On user name:	administrator
vCenter Single Sign-On domain:	vsphere.local
vCenter Single Sign-On site name:	Palo Alto
Installation directory:	C:\Program Files\VMware\
Data directory:	C:\ProgramData\VMware\
Upgrade export directory:	C:\ProgramData\VMware\vCenterServer\export\

☑ I verify that I have backed up this vCenter Single Sign-On machine.

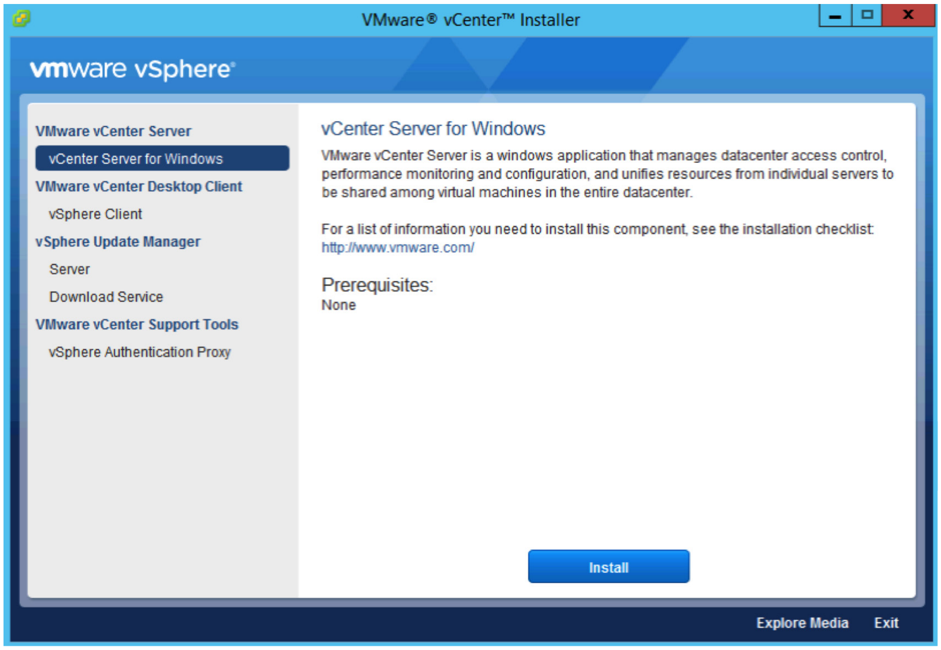
13. Click **Finish**.

14. Log in to the vCenter Server you want to upgrade.

15. Mount the vCenter Server 6.0 ISO image.

16. If autorun does not start, execute autorun.exe.

17. Select **vCenter Server for Windows** and click **Install**.


VMware® vCenter™ Installer
vmware vSphere
VMware vCenter Server
vCenter Server for Windows
VMware vCenter Desktop Client
vSphere Client
vSphere Update Manager
Server
Download Service
VMware vCenter Support Tools
vSphere Authentication Proxy

vCenter Server for Windows

VMware vCenter Server is a windows application that manages datacenter access control, performance monitoring and configuration, and unifies resources from individual servers to be shared among virtual machines in the entire datacenter.

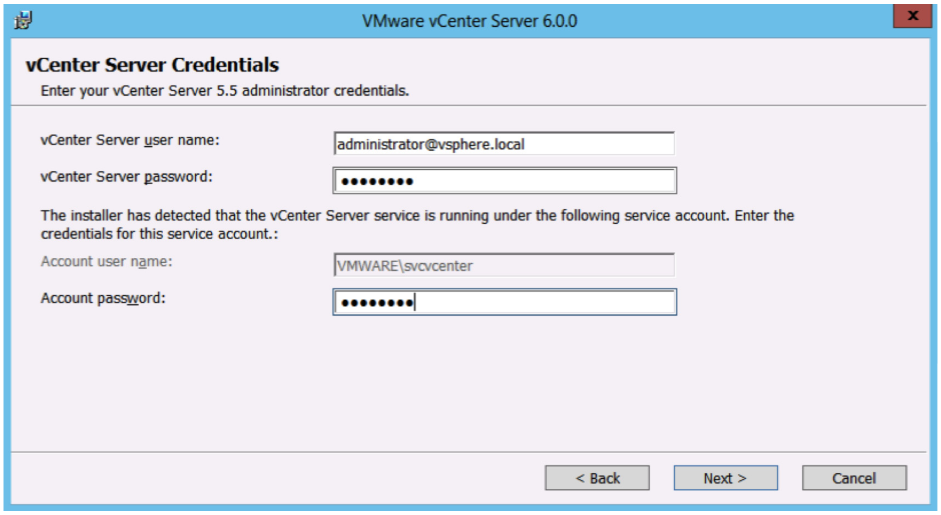
For a list of information you need to install this component, see the installation checklist http://www.vmware.com/

Prerequisites:
None

18. Click **Next**.

19. Accept the license agreements.

20. Enter the **vCenter Server password** for the administrator@vsphere.local account and the **Account password** for the service account (if applicable). Click **Next**.



VMware vCenter Server 6.0.0

vCenter Server Credentials

Enter your vCenter Server 5.5 administrator credentials.

vCenter Server user name: administrator@vsphere.local

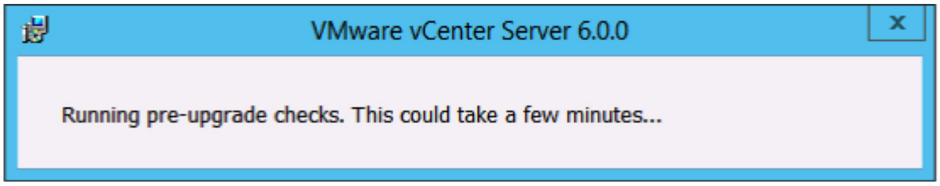
vCenter Server password: ••••••••

The installer has detected that the vCenter Server service is running under the following service account. Enter the credentials for this service account.:

Account user name: VMWARE\svcvcenter

Account password: ••••••••

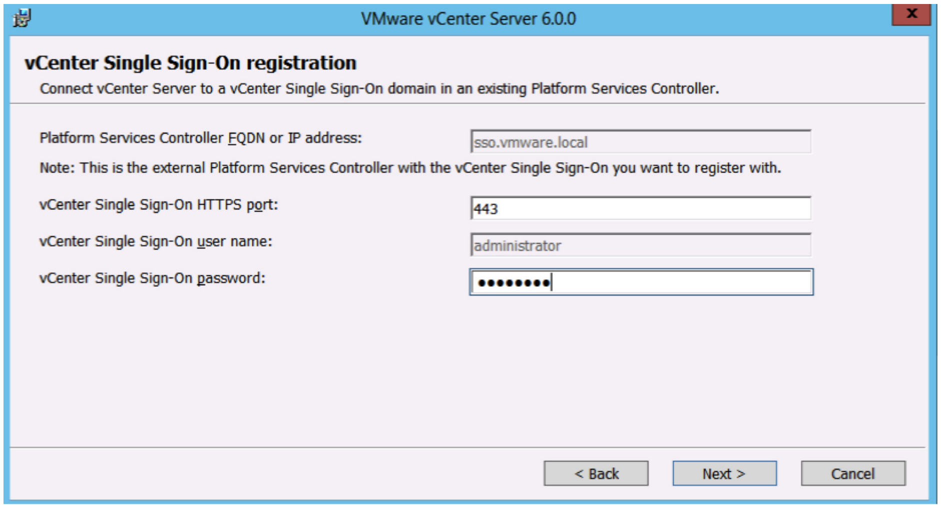
21. Wait for the **pre-upgrade checks** to complete.



VMware vCenter Server 6.0.0

Running pre-upgrade checks. This could take a few minutes...

22. Enter the **vCenter Single Sign-On password** for the administrator@vsphere.local account. Click **Next**.



VMware vCenter Server 6.0.0

vCenter Single Sign-On registration

Connect vCenter Server to a vCenter Single Sign-On domain in an existing Platform Services Controller.

Platform Services Controller FQDN or IP address: sso.vmware.local

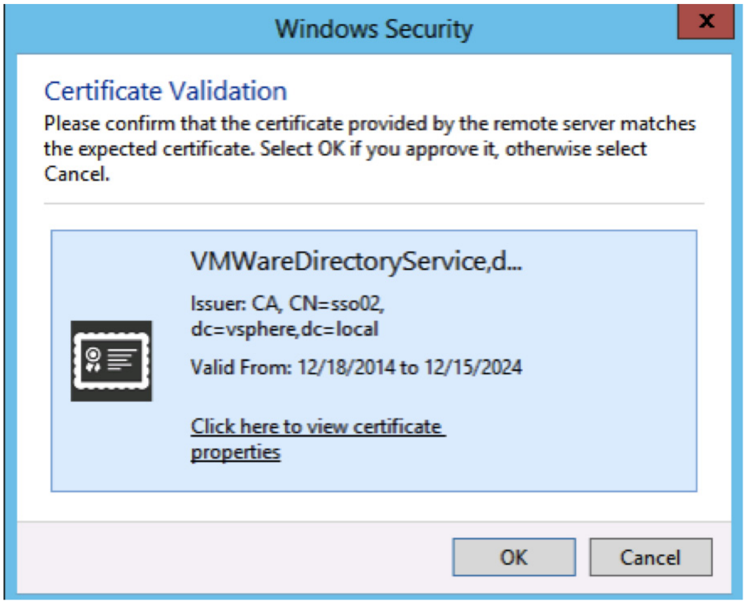
Note: This is the external Platform Services Controller with the vCenter Single Sign-On you want to register with.

vCenter Single Sign-On HTTPS port: 443

vCenter Single Sign-On user name: administrator

vCenter Single Sign-On password: ••••••••

23. Click **OK** to accept the certificate.



Windows Security

Certificate Validation

Please confirm that the certificate provided by the remote server matches the expected certificate. Select OK if you approve it, otherwise select Cancel.

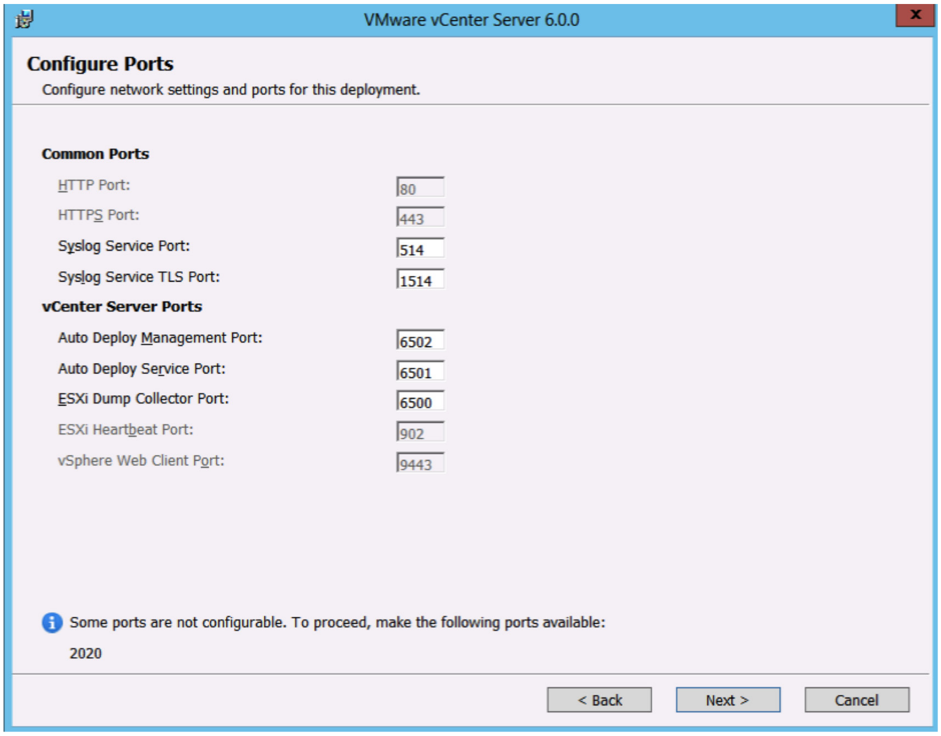
VMWareDirectoryService,d...

Issuer: CA, CN=sso02, dc=vsphere,dc=local

Valid From: 12/18/2014 to 12/15/2024

Click here to view certificate properties

24. Accept the default ports and click **Next**.



VMware vCenter Server 6.0.0

Configure Ports

Configure network settings and ports for this deployment.

Common Ports

HTTP Port:	80
HTTPS Port:	443
Syslog Service Port:	514
Syslog Service TLS Port:	1514

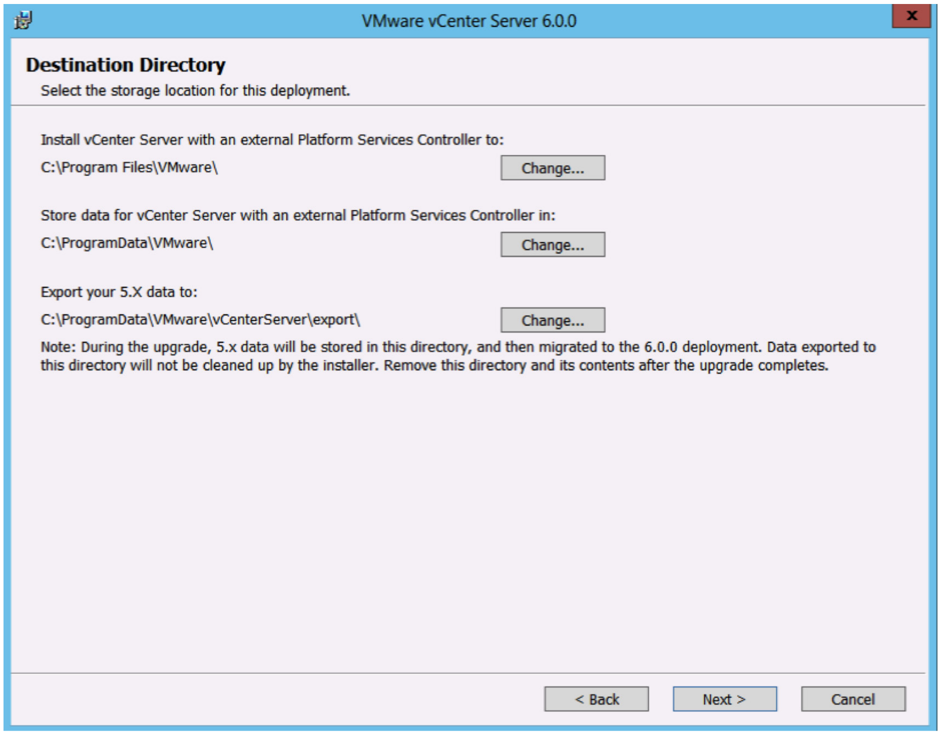
vCenter Server Ports

Auto Deploy Management Port:	6502
Auto Deploy Service Port:	6501
ESXi Dump Collector Port:	6500
ESXi Heartbeat Port:	902
vSphere Web Client Port:	9443

Some ports are not configurable. To proceed, make the following ports available:

2020

25. Accept or change the installation paths as necessary. Click **Next**.



Destination Directory

Select the storage location for this deployment.

Install vCenter Server with an external Platform Services Controller to:

C:\Program Files\VMware\

Store data for vCenter Server with an external Platform Services Controller in:

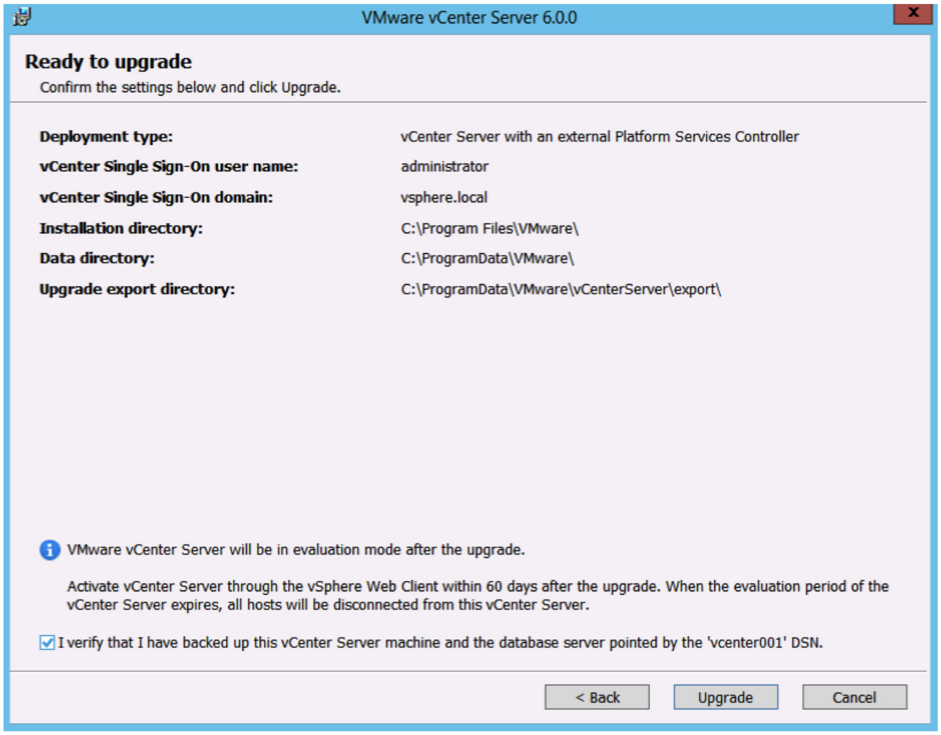
C:\ProgramData\VMware\

Export your 5.X data to:

C:\ProgramData\VMware\vCenterServer\export\

Note: During the upgrade, 5.x data will be stored in this directory, and then migrated to the 6.0.0 deployment. Data exported to this directory will not be cleaned up by the installer. Remove this directory and its contents after the upgrade completes.

26. Check the box to verify that you have backed up the vCenter Server and its database. Click **Upgrade**.



Ready to upgrade

Confirm the settings below and click Upgrade.

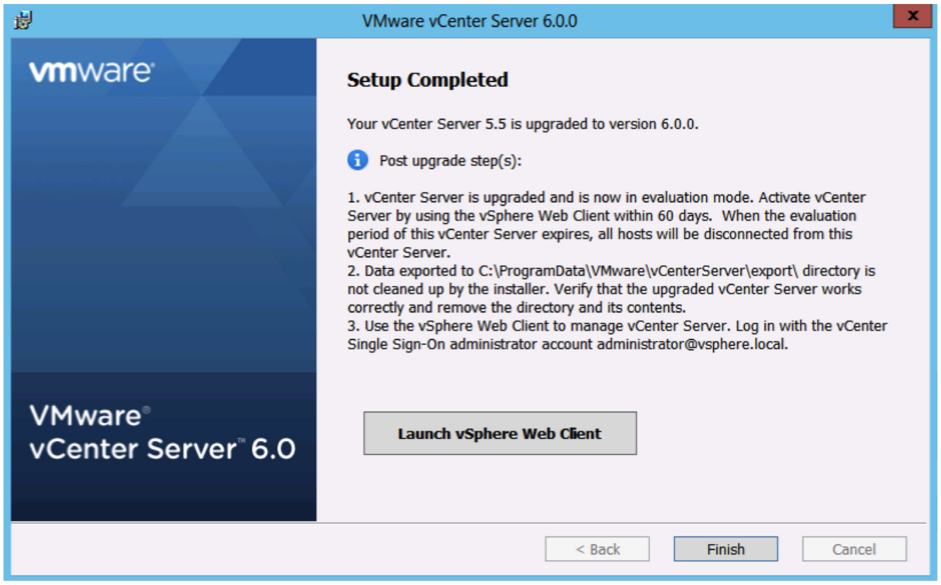
Deployment type:	vCenter Server with an external Platform Services Controller
vCenter Single Sign-On user name:	administrator
vCenter Single Sign-On domain:	vsphere.local
Installation directory:	C:\Program Files\VMware\
Data directory:	C:\ProgramData\VMware\
Upgrade export directory:	C:\ProgramData\VMware\vCenterServer\export\

VMware vCenter Server will be in evaluation mode after the upgrade.

Activate vCenter Server through the vSphere Web Client within 60 days after the upgrade. When the evaluation period of the vCenter Server expires, all hosts will be disconnected from this vCenter Server.

☑ I verify that I have backed up this vCenter Server machine and the database server pointed by the 'vcenter001' DSN.

27. When completed, click **Finish**.


VMware vCenter Server 6.0.0
vmware
VMware® vCenter Server™ 6.0
Launch vSphere Web Client
< Back
Finish
Cancel

Setup Completed

Your vCenter Server 5.5 is upgraded to version 6.0.0.

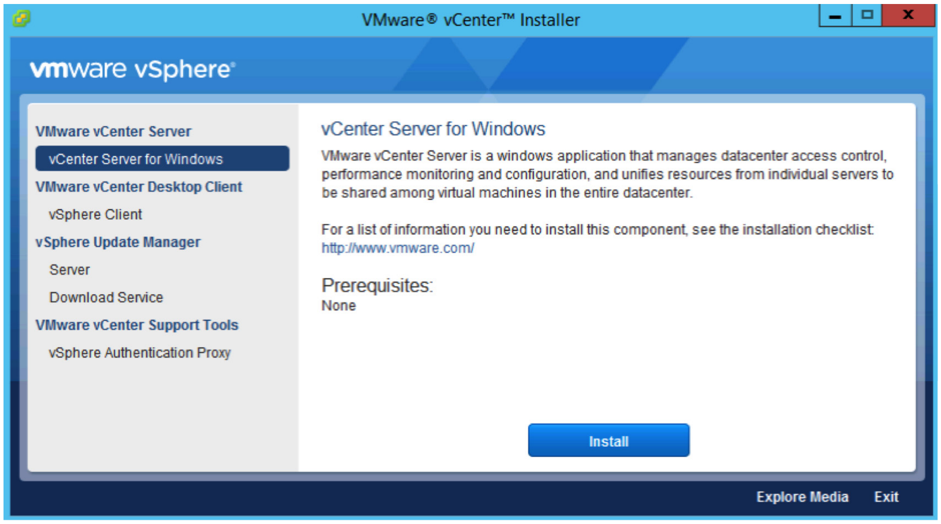
Post upgrade step(s):

1. vCenter Server is upgraded and is now in evaluation mode. Activate vCenter Server by using the vSphere Web Client within 60 days. When the evaluation period of this vCenter Server expires, all hosts will be disconnected from this vCenter Server.
2. Data exported to C:\ProgramData\VMware\vCenterServer\export\ directory is not cleaned up by the installer. Verify that the upgraded vCenter Server works correctly and remove the directory and its contents.
3. Use the vSphere Web Client to manage vCenter Server. Log in with the vCenter Single Sign-On administrator account administrator@vsphere.local.

Fresh vCenter Single Sign-On High Availability Deployment

Windows Deployment

1. Complete steps 1–12 in the "Fresh External Platform Services Controller Deployment" section.
2. Log in to the second Windows Server to become a Platform Services Controller.
3. Mount the vCenter Server 6.0 ISO image.
4. If autorun does not start, execute autorun.exe.
5. Select **vCenter Server for Windows** and click **Install**.


VMware® vCenter™ Installer
vmware vSphere®
VMware vCenter Server
vCenter Server for Windows
VMware vCenter Desktop Client
vSphere Client
vSphere Update Manager
Server
Download Service
VMware vCenter Support Tools
vSphere Authentication Proxy
Install
Explore Media
Exit

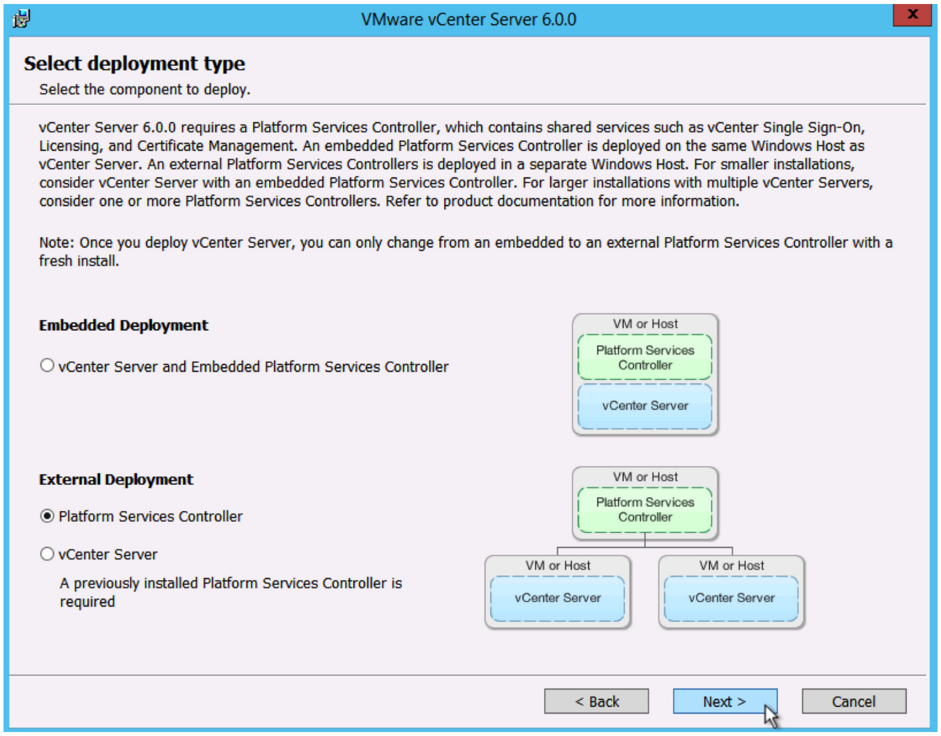
vCenter Server for Windows

VMware vCenter Server is a windows application that manages datacenter access control, performance monitoring and configuration, and unifies resources from individual servers to be shared among virtual machines in the entire datacenter.

For a list of information you need to install this component, see the installation checklist: http://www.vmware.com/

Prerequisites:
None

6. Click **Next**.
7. Accept the license agreements.
8. Under **External Deployment**, select **Platform Services Controller**. Click **Next**.



VMware vCenter Server 6.0.0

Select deployment type

Select the component to deploy.

vCenter Server 6.0.0 requires a Platform Services Controller, which contains shared services such as vCenter Single Sign-On, Licensing, and Certificate Management. An embedded Platform Services Controller is deployed on the same Windows Host as vCenter Server. An external Platform Services Controllers is deployed in a separate Windows Host. For smaller installations, consider vCenter Server with an embedded Platform Services Controller. For larger installations with multiple vCenter Servers, consider one or more Platform Services Controllers. Refer to product documentation for more information.

Note: Once you deploy vCenter Server, you can only change from an embedded to an external Platform Services Controller with a fresh install.

Embedded Deployment

○ vCenter Server and Embedded Platform Services Controller

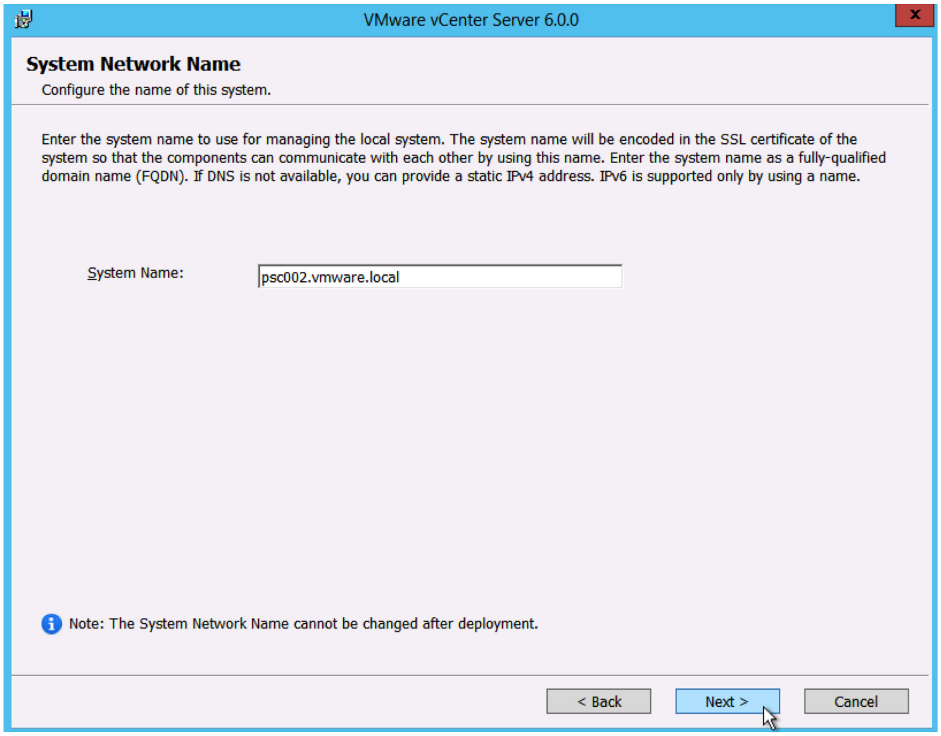
External Deployment

● Platform Services Controller

○ vCenter Server

A previously installed Platform Services Controller is required

9. Verify the **System Name** and click **Next**.



VMware vCenter Server 6.0.0

System Network Name

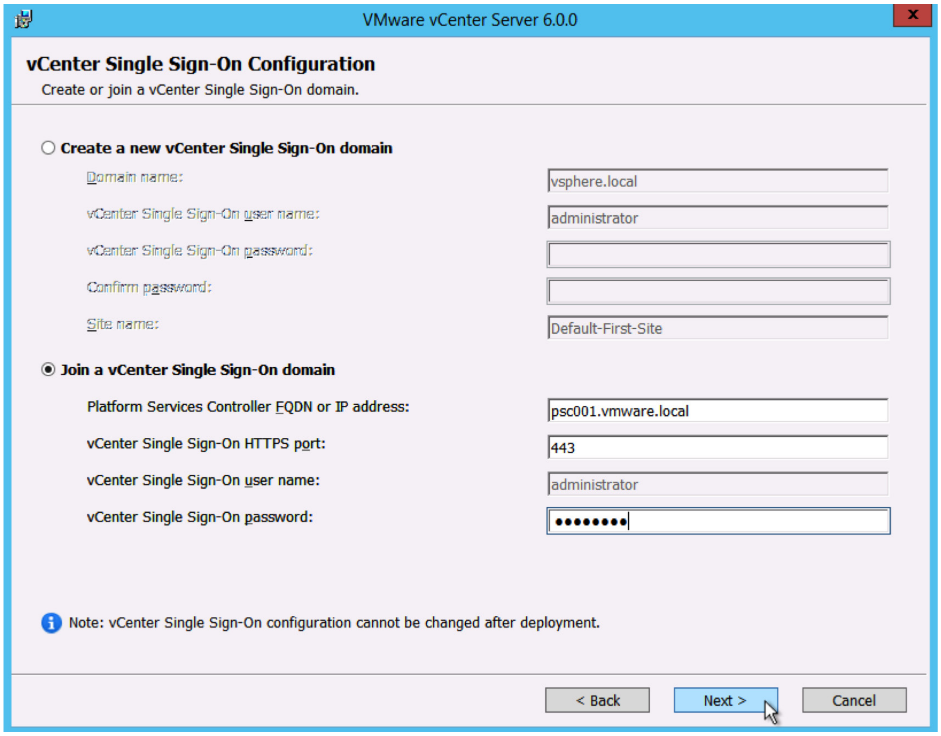
Configure the name of this system.

Enter the system name to use for managing the local system. The system name will be encoded in the SSL certificate of the system so that the components can communicate with each other by using this name. Enter the system name as a fully-qualified domain name (FQDN). If DNS is not available, you can provide a static IPv4 address. IPv6 is supported only by using a name.

System Name: psc002.vmware.local

Note: The System Network Name cannot be changed after deployment.

10. Select **Join a vCenter Single Sign-On domain** and enter the **FQDN** and **password**. Click **Next**.



VMware vCenter Server 6.0

vCenter Single Sign-On Configuration

Create or join a vCenter Single Sign-On domain.

○ **Create a new vCenter Single Sign-On domain**

Domain name: vsphere.local

vCenter Single Sign-On user name: administrator

vCenter Single Sign-On password:

Confirm password:

Site name: Default-First-Site

● **Join a vCenter Single Sign-On domain**

Platform Services Controller FQDN or IP address: psc001.vmware.local

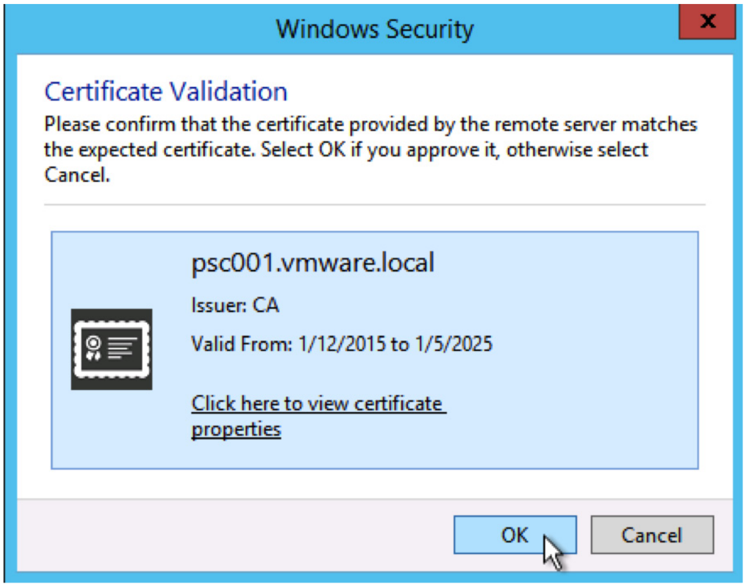
vCenter Single Sign-On HTTPS port: 443

vCenter Single Sign-On user name: administrator

vCenter Single Sign-On password: ••••••••

Note: vCenter Single Sign-On configuration cannot be changed after deployment.

11. Click **OK** to accept the certificate from the Platform Services Controller.



Windows Security

Certificate Validation

Please confirm that the certificate provided by the remote server matches the expected certificate. Select OK if you approve it, otherwise select Cancel.

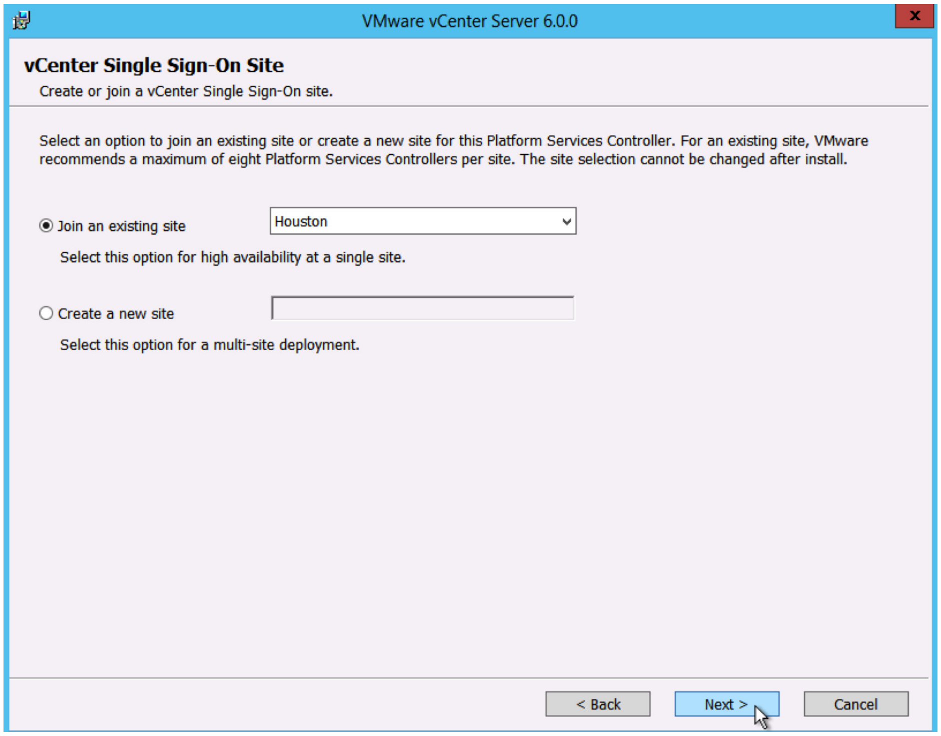
psc001.vmware.local

Issuer: CA

Valid From: 1/12/2015 to 1/5/2025

Click here to view certificate properties

12. Select **Join an existing site** and enter the site. Click **Next**.



VMware vCenter Server 6.0

vCenter Single Sign-On Site

Create or join a vCenter Single Sign-On site.

Select an option to join an existing site or create a new site for this Platform Services Controller. For an existing site, VMware recommends a maximum of eight Platform Services Controllers per site. The site selection cannot be changed after install.

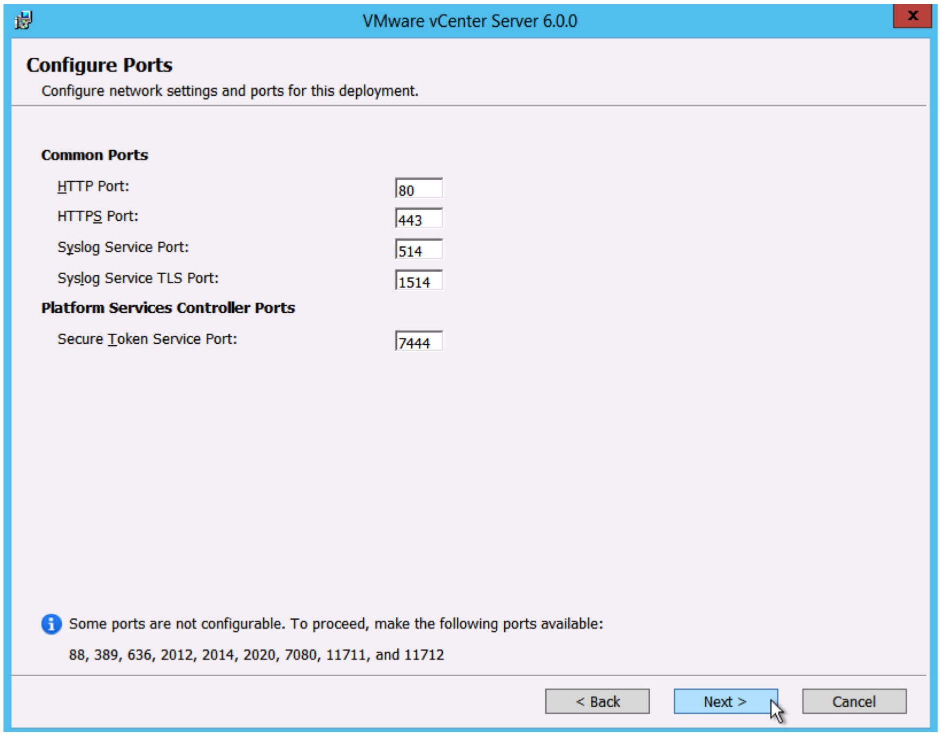
● Join an existing site: Houston

Select this option for high availability at a single site.

○ Create a new site

Select this option for a multi-site deployment.

13. Accept the default ports and click **Next**.



VMware vCenter Server 6.0

Configure Ports

Configure network settings and ports for this deployment.

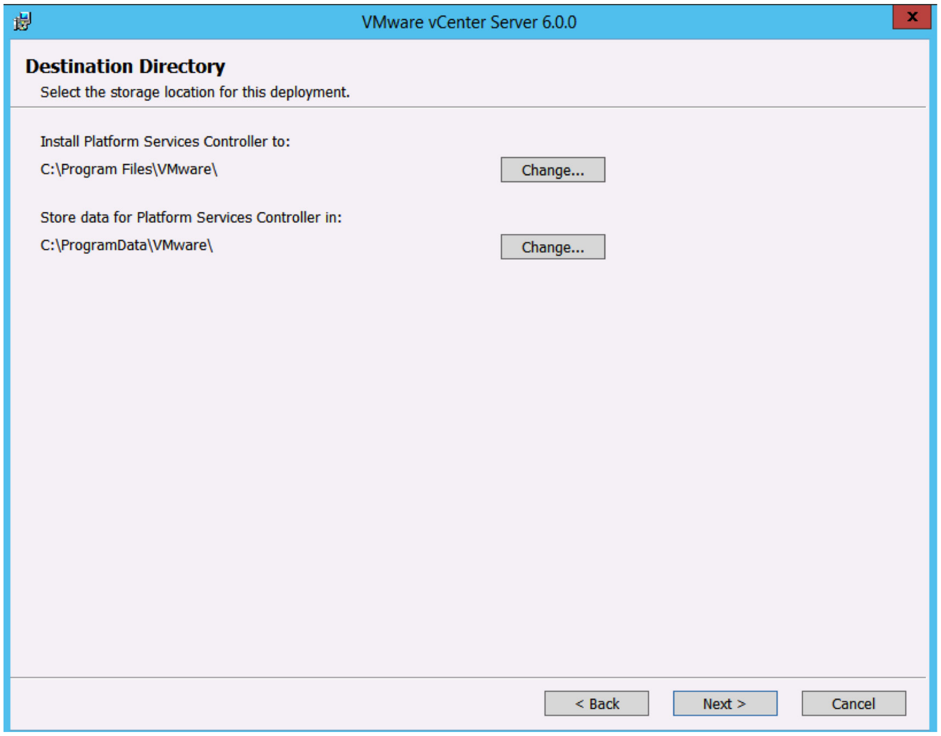
Common Ports

HTTP Port:	80
HTTPS Port:	443
Syslog Service Port:	514
Syslog Service TLS Port:	1514
Platform Services Controller Ports	
Secure Token Service Port:	7444

Some ports are not configurable. To proceed, make the following ports available:

88, 389, 636, 2012, 2014, 2020, 7080, 11711, and 11712

14. Accept or change the installation paths as necessary. Click **Next**.



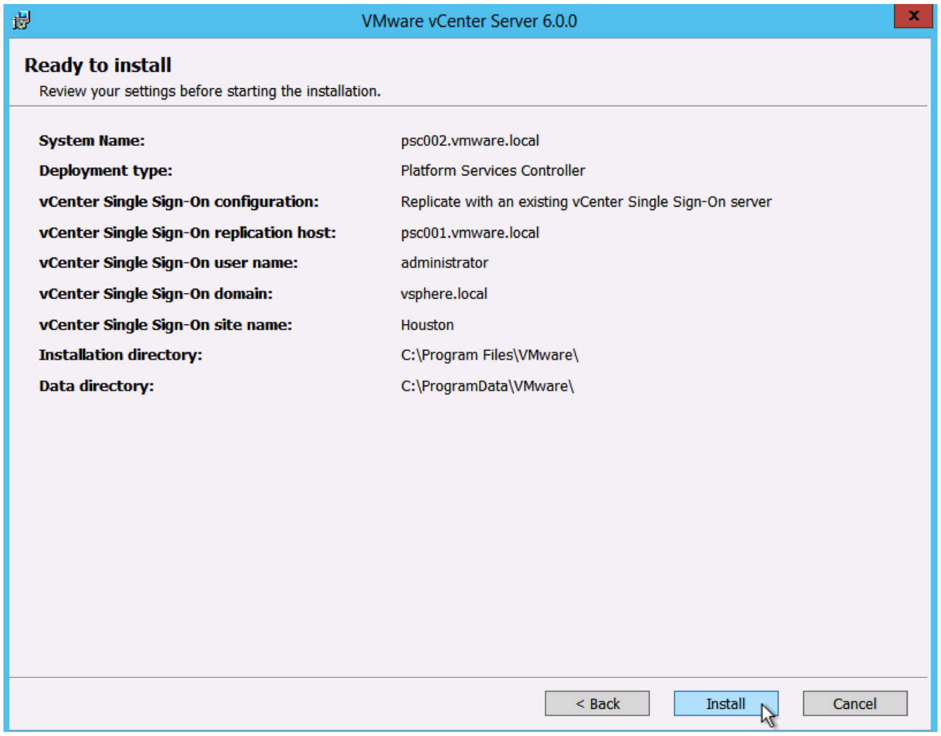
Destination Directory

Select the storage location for this deployment.

Install Platform Services Controller to:
C:\Program Files\VMware\

Store data for Platform Services Controller in:
C:\ProgramData\VMware\

15. Review and click **Install**.



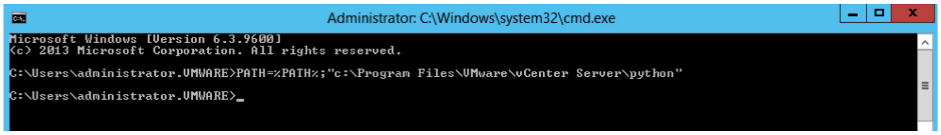
Ready to install

Review your settings before starting the installation.

System Name:	psc002.vmware.local
Deployment type:	Platform Services Controller
vCenter Single Sign-On configuration:	Replicate with an existing vCenter Single Sign-On server
vCenter Single Sign-On replication host:	psc001.vmware.local
vCenter Single Sign-On user name:	administrator
vCenter Single Sign-On domain:	vsphere.local
vCenter Single Sign-On site name:	Houston
Installation directory:	C:\Program Files\VMware\
Data directory:	C:\ProgramData\VMware\

16. Log back in to the first Platform Services Controller.
17. Download the vCenter Single Sign-On high availability configuration scripts from the vCenter Server product download page.
18. Extract the vCenter Single Sign-On high availability scripts to c:\sso-ha.
19. Open a command prompt.
20. Add Python to your path by typing:

```
PATH=%PATH%;%VMWARE_PYTHON_HOME%
```



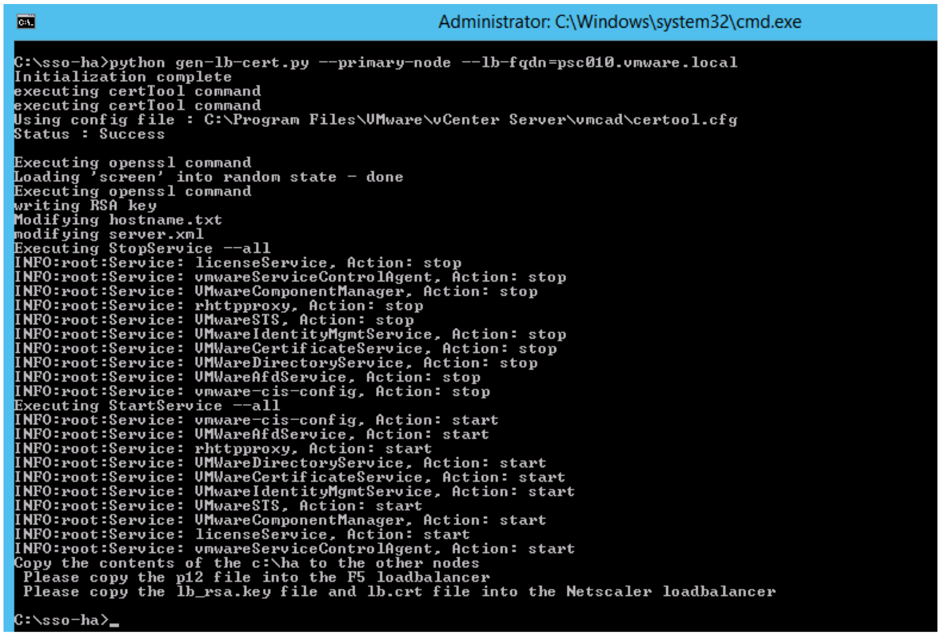
Administrator: C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\administrator.VMWARE>PATH=%PATH%;"c:\Program Files\VMware\vCenter Server\python"

C:\Users\administrator.VMWARE>_
```

21. Change directories to c:\sso-ha.
22. Run:

```
python gen-lb-cert.py --primary-node --lb-fqdn=loadbalancerFQDN
```

where *loadbalancerFQDN* is the FQDN of the load balancer's virtual IP (VIP) used for load-balancing the Platform Services Controllers.



Administrator: C:\Windows\system32\cmd.exe

```
C:\sso-ha>python gen-lb-cert.py --primary-node --lb-fqdn=psc010.vmware.local
Initialization complete
executing certTool command
executing certTool command
Using config file : C:\Program Files\VMware\vCenter Server\vmcad\certool.cfg
Status : Success

Executing openssl command
Loading 'screen' into random state - done
Executing openssl command
writing RSA key
Modifying hostname.txt
modifying server.xml
Executing StopService --all
INFO:root:Service: licenseService, Action: stop
INFO:root:Service: vmwareServiceControlAgent, Action: stop
INFO:root:Service: VMwareComponentManager, Action: stop
INFO:root:Service: rhttpproxy, Action: stop
INFO:root:Service: VMwareSTS, Action: stop
INFO:root:Service: VMwareIdentityMgmtService, Action: stop
INFO:root:Service: VMWareCertificateService, Action: stop
INFO:root:Service: VMWareDirectoryService, Action: stop
INFO:root:Service: VMWareAfdService, Action: stop
INFO:root:Service: vmware-cis-config, Action: stop
Executing StartService --all
INFO:root:Service: vmware-cis-config, Action: start
INFO:root:Service: VMWareAfdService, Action: start
INFO:root:Service: rhttpproxy, Action: start
INFO:root:Service: VMWareDirectoryService, Action: start
INFO:root:Service: VMWareCertificateService, Action: start
INFO:root:Service: VMwareIdentityMgmtService, Action: start
INFO:root:Service: VMwareSTS, Action: start
INFO:root:Service: VMwareComponentManager, Action: start
INFO:root:Service: licenseService, Action: start
INFO:root:Service: vmwareServiceControlAgent, Action: start
Copy the contents of the c:\ha to the other nodes
 Please copy the p12 file into the F5 loadbalancer
 Please copy the lb_rsa.key file and lb.crt file into the Netscaler loadbalancer

C:\sso-ha>_
```

23. Set up your load balancer to balance between the two or more Platform Services Controllers on ports 443, 2012, 2014, 2020, 389, and 636.
    a. An SSL certificate (generated earlier and stored in c:\ha) is required for port 443 only.
    b. For configuration steps for the F5 BIG-IP, see the appendix in this document.
24. Create a forward and reverse DNS entry for the VIP created to load balance the Platform Services Controller traffic.
25. Log in to the second Platform Services Controller.

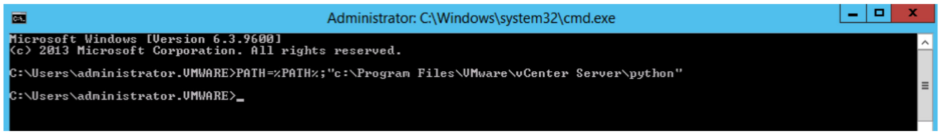
26. Copy the sso-ha and ha folder from the first Platform Services Controller into the c: drive.

27. Copy C:\ProgramData\VMware\vCenterServer\cfg\sso\keys from the first Platform Services Controller to c:\ha\keys.

28. Open a command prompt.

29. Add Python to your path by typing:

```
PATH=%PATH%;%VMWARE_PYTHON_HOME%
```



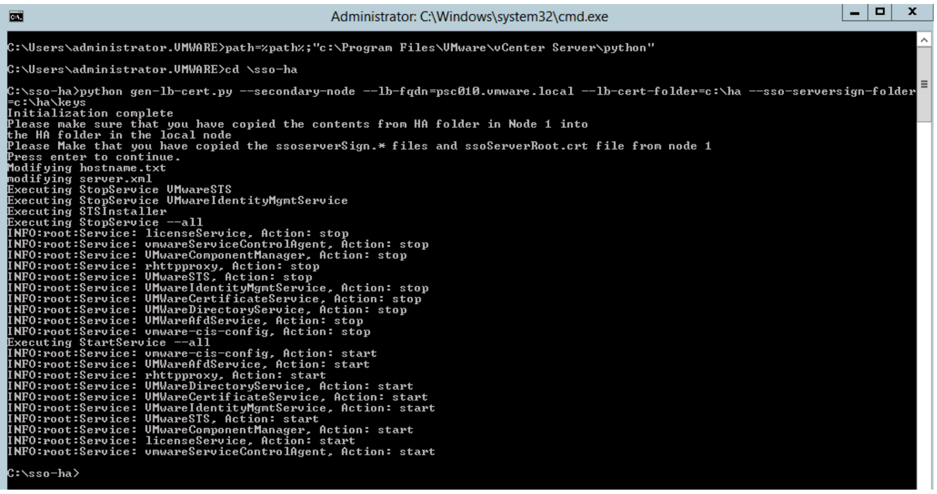
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\administrator.VMWARE>PATH=%PATH%;"c:\Program Files\VMware\vCenter Server\python"

C:\Users\administrator.VMWARE>_
```

30. Change directories to c:\sso-ha.

31. Run:

```
python gen-lb-cert.py --secondary-node --lb-fqdn=loadbalancerFQDN --lb-cert-
folder=C:\ha --sso-serversign-folder=c:\ha\keys\
```

where *loadbalancerFQDN* is the FQDN of the load balancer’s VIP used for load-balancing the Platform Services Controllers.



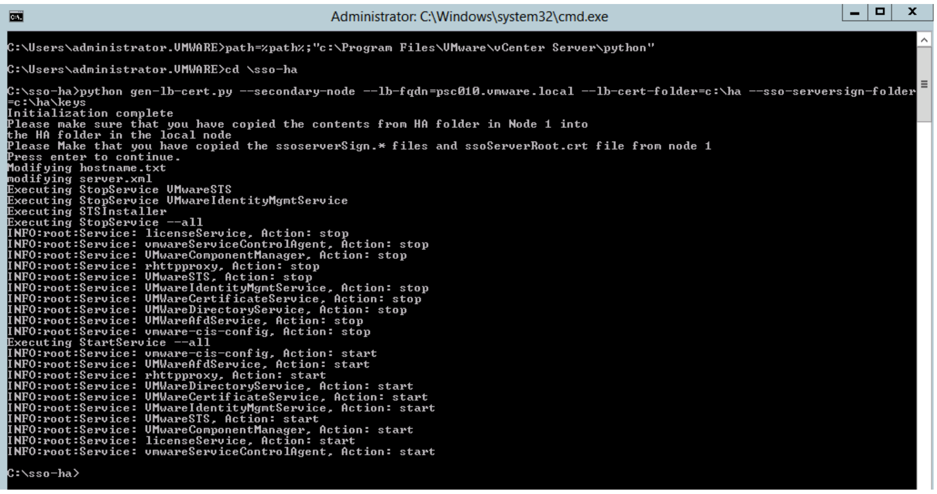
```
C:\Users\administrator.VMWARE>path=%path%;"c:\Program Files\VMware\vCenter Server\python"

C:\Users\administrator.VMWARE>cd \sso-ha

C:\sso-ha>python gen-lb-cert.py --secondary-node --lb-fqdn=psc010.vmware.local --lb-cert-folder=c:\ha --sso-serversign-folder
=c:\ha\keys
Initialization complete
Please make sure that you have copied the contents from HA folder in Node 1 into
the HA folder in the local node
Please Make that you have copied the ssoserverSign.* files and ssoServerRoot.crt file from node 1
Press enter to continue.
Modifying hostname.txt
modifying server.xml
Executing StopService VMwareSTS
Executing StopService VMwareIdentityMgmtService
Executing STSInstaller
Executing StopService --all
INFO:root:Service: licenseService, Action: stop
INFO:root:Service: vmwareServiceControlAgent, Action: stop
INFO:root:Service: VMwareComponentManager, Action: stop
INFO:root:Service: rhttpproxy, Action: stop
INFO:root:Service: VMwareSTS, Action: stop
INFO:root:Service: VMwareIdentityMgmtService, Action: stop
INFO:root:Service: VMWareCertificateService, Action: stop
INFO:root:Service: VMWareDirectoryService, Action: stop
INFO:root:Service: VMWareAfdService, Action: stop
INFO:root:Service: vmware-cis-config, Action: stop
Executing StartService --all
INFO:root:Service: vmware-cis-config, Action: start
INFO:root:Service: VMWareAfdService, Action: start
INFO:root:Service: rhttpproxy, Action: start
INFO:root:Service: VMWareDirectoryService, Action: start
INFO:root:Service: VMWareCertificateService, Action: start
INFO:root:Service: VMwareIdentityMgmtService, Action: start
INFO:root:Service: VMwareSTS, Action: start
INFO:root:Service: VMwareComponentManager, Action: start
INFO:root:Service: licenseService, Action: start
INFO:root:Service: vmwareServiceControlAgent, Action: start

C:\sso-ha>
```

32. Repeat steps 26–32 for any additional Platform Services Controllers.

33. On one Platform Services Controller, update the endpoint URL by running:

```
python lstoolHA.py --hostname=FQDNofLocalMachine --lb-fqdn=loadbalancerFQDN --lb-cert-
folder=C:\ha --user=Administrator@SSODomain --password="password"
```

where *FQDNofLocalMachine* is the FQDN of the machine where the script is being run, *loadbalancerFQDN* is the FQDN of the load balancer’s VIP used for load balancing the Platform Services Controllers, *SSODomain* is the vCenter Single Sign-On domain (by default vsphere.local), and *password* is the password for the vCenter Single Sign-On administrator. The password parameter is optional; if not specified, you will be prompted for it.



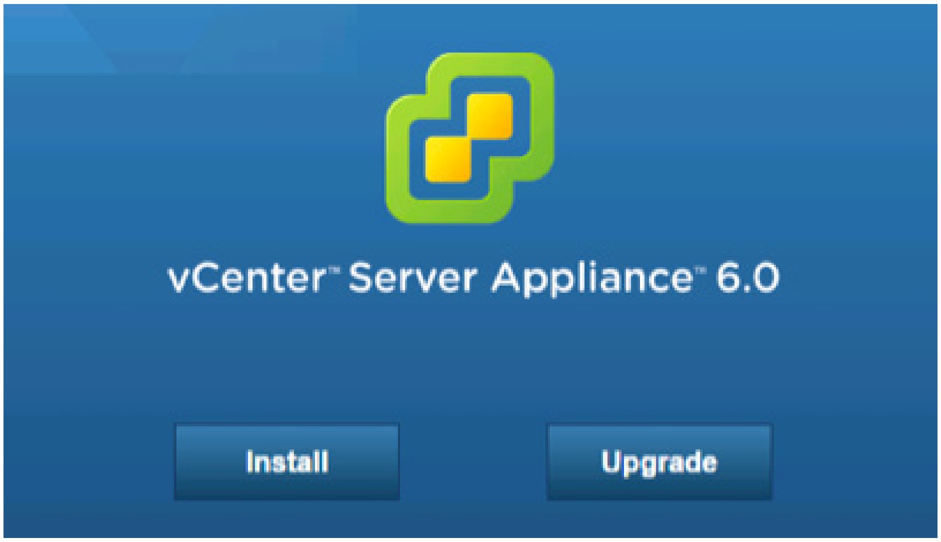
```
C:\Users\administrator.VMWARE>path=%path%;"c:\Program Files\VMware\vCenter Server\python"

C:\Users\administrator.VMWARE>cd \sso-ha

C:\sso-ha>python gen-lb-cert.py --secondary-node --lb-fqdn=psc010.vmware.local --lb-cert-folder=c:\ha --sso-serversign-folder
=c:\ha\keys
Initialization complete
Please make sure that you have copied the contents from HA folder in Node 1 into
the HA folder in the local node
Please Make that you have copied the ssoserverSign.* files and ssoServerRoot.crt file from node 1
Press enter to continue.
Modifying hostname.txt
modifying server.xml
Executing StopService VMwareSTS
Executing StopService VMwareIdentityMgmtService
Executing STSInstaller
Executing StopService --all
INFO:root:Service: licenseService, Action: stop
INFO:root:Service: vmwareServiceControlAgent, Action: stop
INFO:root:Service: VMwareComponentManager, Action: stop
INFO:root:Service: rhttpproxy, Action: stop
INFO:root:Service: VMwareSTS, Action: stop
INFO:root:Service: VMwareIdentityMgmtService, Action: stop
INFO:root:Service: VMWareCertificateService, Action: stop
INFO:root:Service: VMWareDirectoryService, Action: stop
INFO:root:Service: VMWareAfdService, Action: stop
INFO:root:Service: vmware-cis-config, Action: stop
Executing StartService --all
INFO:root:Service: vmware-cis-config, Action: start
INFO:root:Service: VMWareAfdService, Action: start
INFO:root:Service: rhttpproxy, Action: start
INFO:root:Service: VMWareDirectoryService, Action: start
INFO:root:Service: VMWareCertificateService, Action: start
INFO:root:Service: VMwareIdentityMgmtService, Action: start
INFO:root:Service: VMwareSTS, Action: start
INFO:root:Service: VMwareComponentManager, Action: start
INFO:root:Service: licenseService, Action: start
INFO:root:Service: vmwareServiceControlAgent, Action: start

C:\sso-ha>
```

34. Follow the steps to install a new external vCenter Server. When asked for the Platform Services Controller, enter the FQDN of the load balancer's VIP.

vCenter Server Appliance Deployment

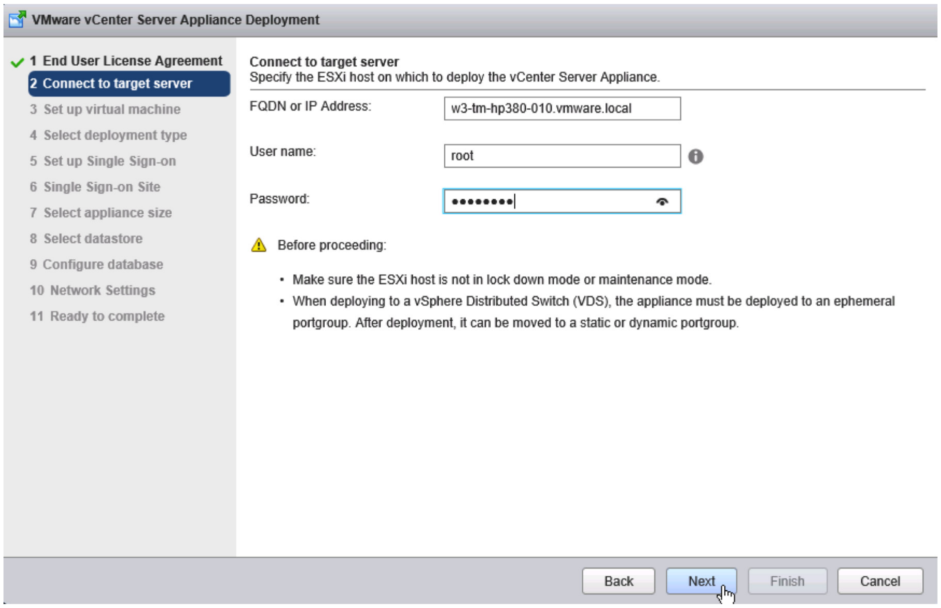
1. Complete steps 1–14 in the "Fresh External Platform Services Controller Deployment" section.

2. Click **Install** to start the installation for the second Platform Services Controller.



3. Accept the license agreement and clic**k Next**.

4. Enter a target host and a **User name** and **Password** on the host with root access.



Connect to target server
Specify the ESXi host on which to deploy the vCenter Server Appliance.

FQDN or IP Address: w3-tm-hp380-010.vmware.local

User name: root

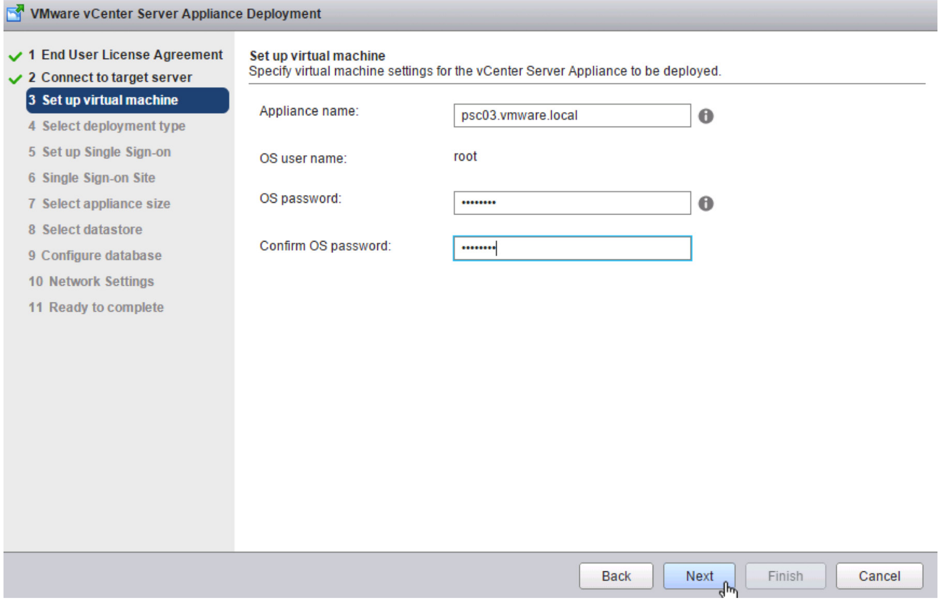
Password: ••••••••

Before proceeding:

- Make sure the ESXi host is not in lock down mode or maintenance mode.
- When deploying to a vSphere Distributed Switch (VDS), the appliance must be deployed to an ephemeral portgroup. After deployment, it can be moved to a static or dynamic portgroup.

5. Click **Yes** to accept the host's certificate.

6. Enter an **Appliance name** and the root **password** you want to assign. Click **Next**.



Set up virtual machine
Specify virtual machine settings for the vCenter Server Appliance to be deployed.

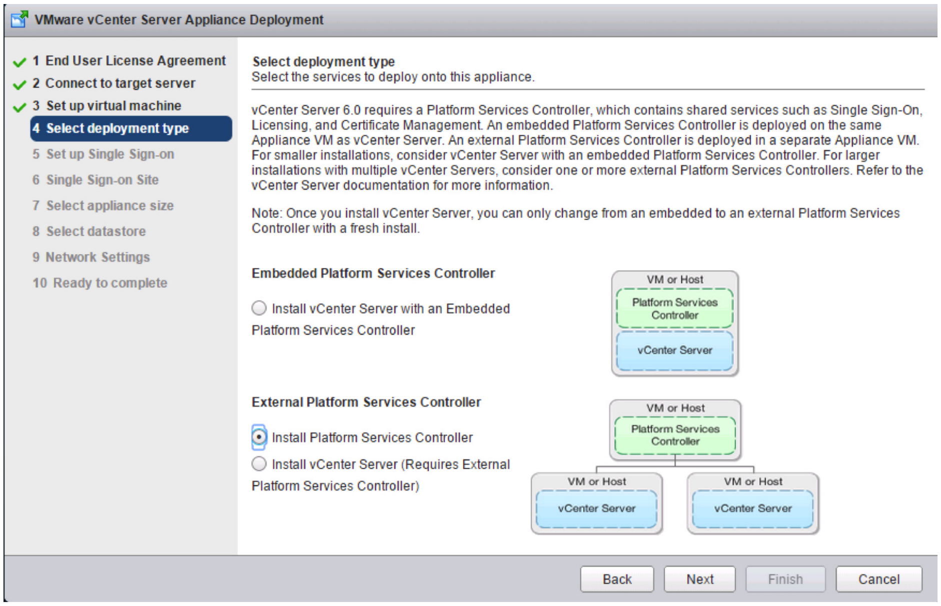
Appliance name: psc03.vmware.local

OS user name: root

OS password: ••••••••

Confirm OS password: ••••••••

7. Under **External Platform Services Controller**, select **Install Platform Services Controller**. Click **Next**.



VMware vCenter Server Appliance Deployment

- ✓ 1 End User License Agreement
- ✓ 2 Connect to target server
- ✓ 3 Set up virtual machine
- 4 Select deployment type
- 5 Set up Single Sign-on
- 6 Single Sign-on Site
- 7 Select appliance size
- 8 Select datastore
- 9 Network Settings
- 10 Ready to complete

Select deployment type
Select the services to deploy onto this appliance.

vCenter Server 6.0 requires a Platform Services Controller, which contains shared services such as Single Sign-On, Licensing, and Certificate Management. An embedded Platform Services Controller is deployed on the same Appliance VM as vCenter Server. An external Platform Services Controller is deployed in a separate Appliance VM. For smaller installations, consider vCenter Server with an embedded Platform Services Controller. For larger installations with multiple vCenter Servers, consider one or more external Platform Services Controllers. Refer to the vCenter Server documentation for more information.

Note: Once you install vCenter Server, you can only change from an embedded to an external Platform Services Controller with a fresh install.

Embedded Platform Services Controller

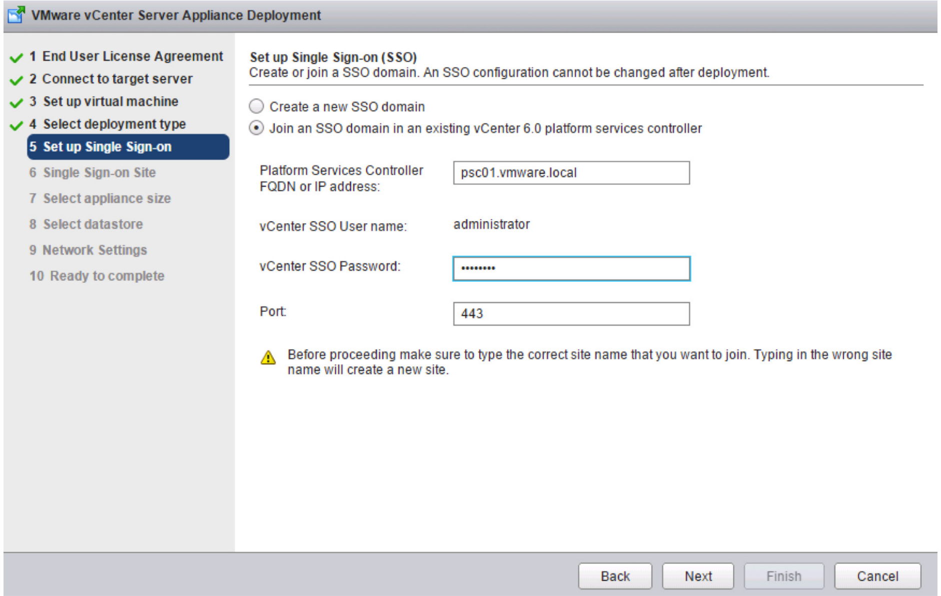
○ Install vCenter Server with an Embedded Platform Services Controller

External Platform Services Controller

● Install Platform Services Controller

○ Install vCenter Server (Requires External Platform Services Controller)

8. Select **Join an SSO domain** and enter the **FQDN** and password. Click **Next**.



VMware vCenter Server Appliance Deployment

- ✓ 1 End User License Agreement
- ✓ 2 Connect to target server
- ✓ 3 Set up virtual machine
- ✓ 4 Select deployment type
- 5 Set up Single Sign-on
- 6 Single Sign-on Site
- 7 Select appliance size
- 8 Select datastore
- 9 Network Settings
- 10 Ready to complete

Set up Single Sign-on (SSO)
Create or join a SSO domain. An SSO configuration cannot be changed after deployment.

○ Create a new SSO domain

● Join an SSO domain in an existing vCenter 6.0 platform services controller

Platform Services Controller FQDN or IP address: psc01.vmware.local

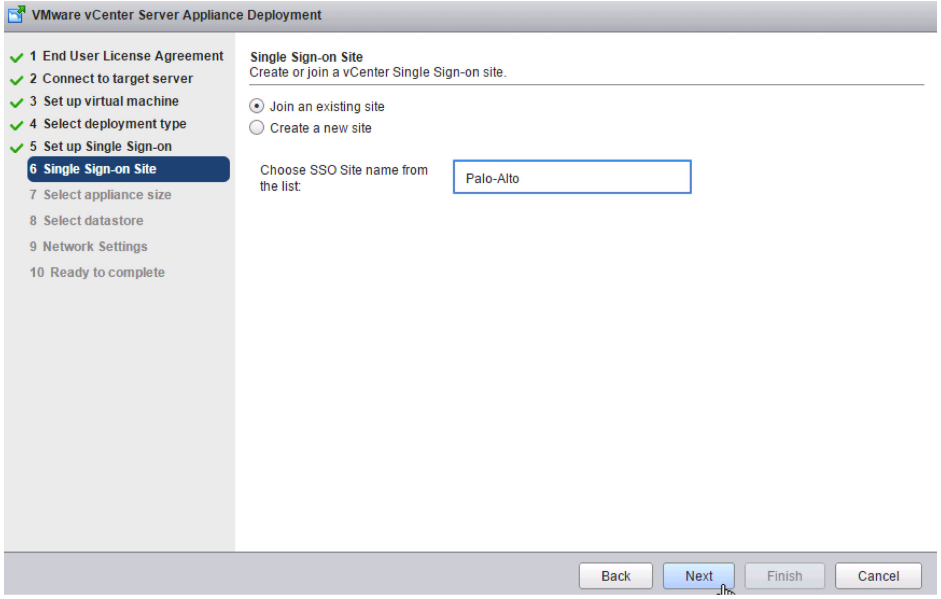
vCenter SSO User name: administrator

vCenter SSO Password: ••••••••

Port: 443

⚠ Before proceeding make sure to type the correct site name that you want to join. Typing in the wrong site name will create a new site.

9. Select **Join an existing site**. Choose the site and click **Next**.



VMware vCenter Server Appliance Deployment

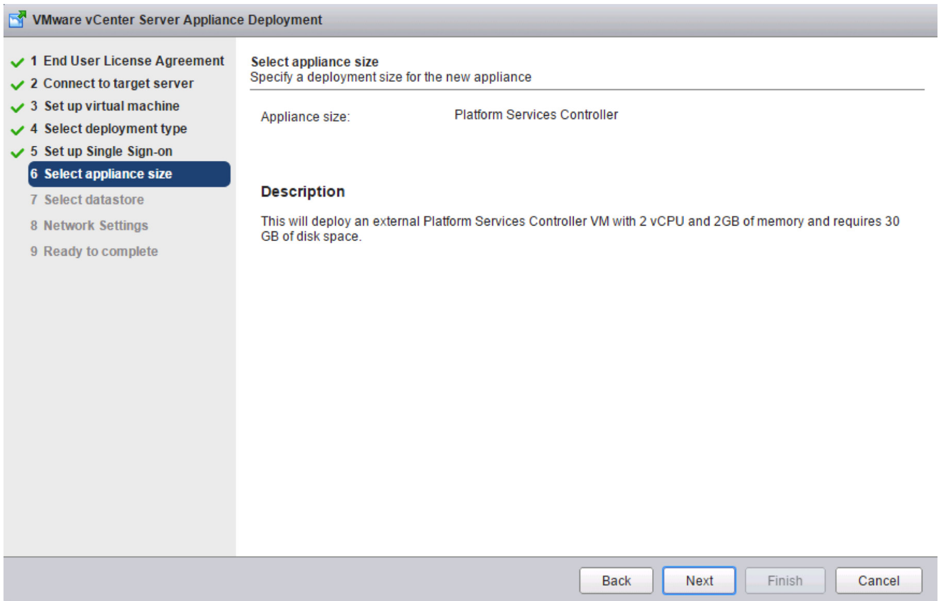
- ✓ 1 End User License Agreement
- ✓ 2 Connect to target server
- ✓ 3 Set up virtual machine
- ✓ 4 Select deployment type
- ✓ 5 Set up Single Sign-on
- 6 Single Sign-on Site
- 7 Select appliance size
- 8 Select datastore
- 9 Network Settings
- 10 Ready to complete

Single Sign-on Site
Create or join a vCenter Single Sign-on site.

● Join an existing site
○ Create a new site

Choose SSO Site name from the list: Palo-Alto

10. Click **Next**. There is only one appliance size for the Platform Services Controller.



VMware vCenter Server Appliance Deployment

- ✓ 1 End User License Agreement
- ✓ 2 Connect to target server
- ✓ 3 Set up virtual machine
- ✓ 4 Select deployment type
- ✓ 5 Set up Single Sign-on
- 6 Select appliance size
- 7 Select datastore
- 8 Network Settings
- 9 Ready to complete

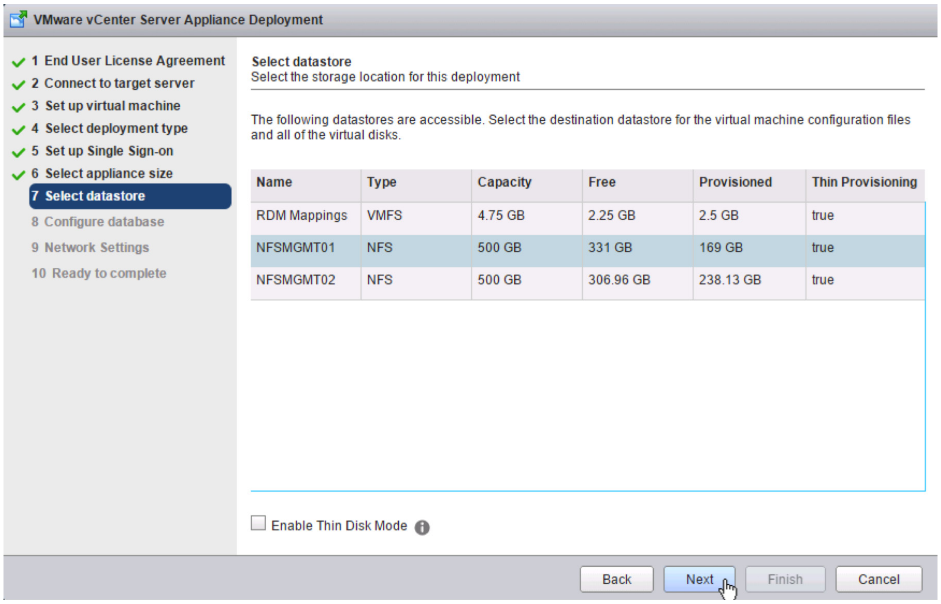
Select appliance size
Specify a deployment size for the new appliance

Appliance size: Platform Services Controller

Description

This will deploy an external Platform Services Controller VM with 2 vCPU and 2GB of memory and requires 30 GB of disk space.

11. Select a datastore to deploy the appliance on and click **Next**.



VMware vCenter Server Appliance Deployment

- ✓ 1 End User License Agreement
- ✓ 2 Connect to target server
- ✓ 3 Set up virtual machine
- ✓ 4 Select deployment type
- ✓ 5 Set up Single Sign-on
- ✓ 6 Select appliance size
- 7 Select datastore
- 8 Configure database
- 9 Network Settings
- 10 Ready to complete

Select datastore
Select the storage location for this deployment

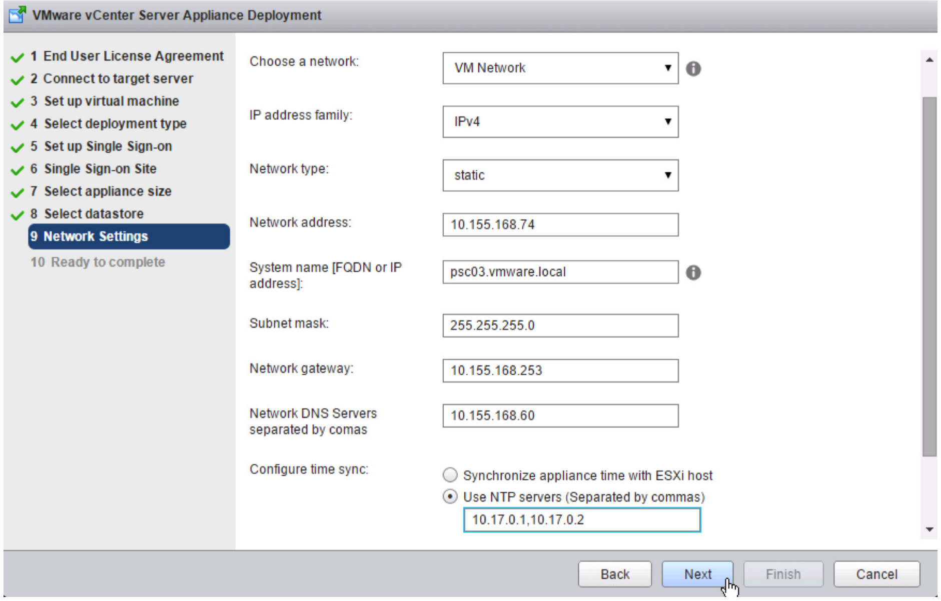
The following datastores are accessible. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Type	Capacity	Free	Provisioned	Thin Provisioning
RDM Mappings	VMFS	4.75 GB	2.25 GB	2.5 GB	true
NFSMGMT01	NFS	500 GB	331 GB	169 GB	true
NFSMGMT02	NFS	500 GB	306.96 GB	238.13 GB	true

☐ Enable Thin Disk Mode

12. Enter **Network Settings** and click **Next**.

NOTE: The FQDN and IP addresses entered here must be resolvable by the DNS server specified or the deployment will fail.

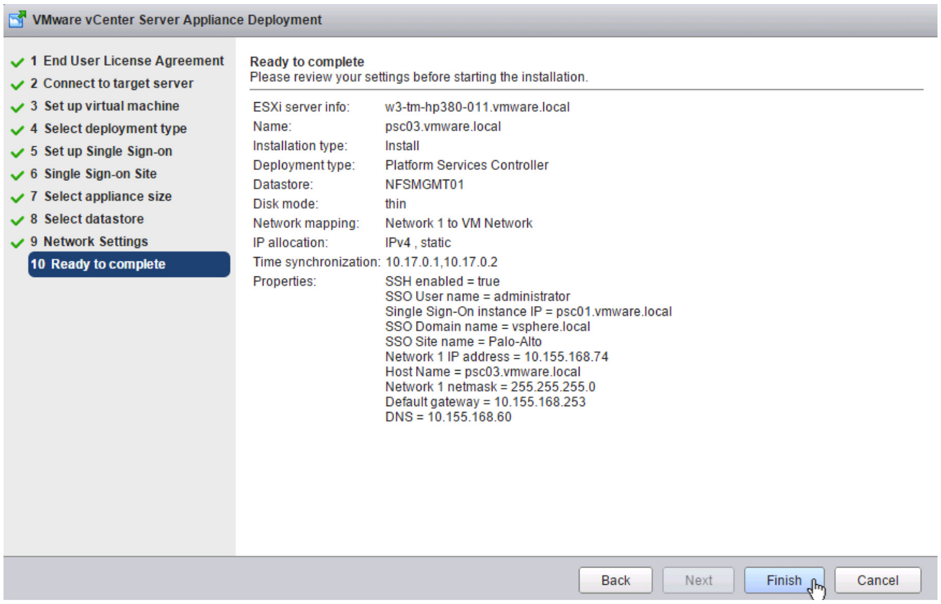


VMware vCenter Server Appliance Deployment

- ✓ 1 End User License Agreement
- ✓ 2 Connect to target server
- ✓ 3 Set up virtual machine
- ✓ 4 Select deployment type
- ✓ 5 Set up Single Sign-on
- ✓ 6 Single Sign-on Site
- ✓ 7 Select appliance size
- ✓ 8 Select datastore
- 9 Network Settings
- 10 Ready to complete

Choose a network:	VM Network
IP address family:	IPv4
Network type:	static
Network address:	10.155.168.74
System name [FQDN or IP address]:	psc03.vmware.local
Subnet mask:	255.255.255.0
Network gateway:	10.155.168.253
Network DNS Servers separated by comas	10.155.168.60
Configure time sync:	○ Synchronize appliance time with ESXi host ● Use NTP servers (Separated by commas) 10.17.0.1,10.17.0.2

13. Review and click **Finish**.



VMware vCenter Server Appliance Deployment
✓ 1 End User License Agreement
✓ 2 Connect to target server
✓ 3 Set up virtual machine
✓ 4 Select deployment type
✓ 5 Set up Single Sign-on
✓ 6 Single Sign-on Site
✓ 7 Select appliance size
✓ 8 Select datastore
✓ 9 Network Settings
10 Ready to complete
Back
Next
Finish
Cancel

Ready to complete
Please review your settings before starting the installation.

ESXi server info: w3-tm-hp380-011.vmware.local
Name: psc03.vmware.local
Installation type: Install
Deployment type: Platform Services Controller
Datastore: NFSMGMT01
Disk mode: thin
Network mapping: Network 1 to VM Network
IP allocation: IPv4 , static
Time synchronization: 10.17.0.1,10.17.0.2
Properties: SSH enabled = true
SSO User name = administrator
Single Sign-On instance IP = psc01.vmware.local
SSO Domain name = vsphere.local
SSO Site name = Palo-Alto
Network 1 IP address = 10.155.168.74
Host Name = psc03.vmware.local
Network 1 netmask = 255.255.255.0
Default gateway = 10.155.168.253
DNS = 10.155.168.60

14. Connect to the first Platform Services Controller via SSH.
15. Type:

```
shell.set --enabled True
```

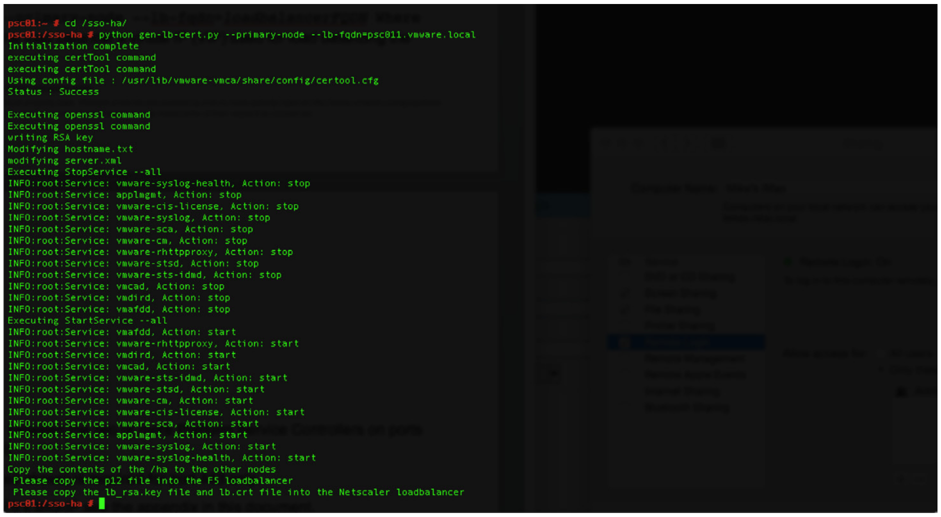
16. Type:

```
shell
```

17. Download the vCenter Single Sign-On high availability configuration scripts from the vCenter Server product download page.
18. Extract the vCenter Single Sign-On high availability scripts to /sso-ha.
19. Change directories to /sso-ha.
20. Run:

```
python gen-lb-cert.py --primary-node --lb-fqdn=loadbalancerFQDN
```

where *loadbalancerFQDN* is the FQDN of the load balancer's VIP used for load-balancing the Platform Services Controllers.



```
psc01:~ # cd /sso-ha/
psc01:/sso-ha # python gen-lb-cert.py --primary-node --lb-fqdn=psc011.vmware.local
Initialization complete
executing certTool command
executing certTool command
Using config file : /usr/lib/vmware-vmca/share/config/certool.cfg
Status : Success

Executing openssl command
Executing openssl command
writing RSA key
Modifying hostname.txt
modifying server.xml
Executing StopService --all
INFO:root:Service: vmware-syslog-health, Action: stop
INFO:root:Service: applmgmt, Action: stop
INFO:root:Service: vmware-cis-license, Action: stop
INFO:root:Service: vmware-syslog, Action: stop
INFO:root:Service: vmware-sca, Action: stop
INFO:root:Service: vmware-cm, Action: stop
INFO:root:Service: vmware-rhttpproxy, Action: stop
INFO:root:Service: vmware-stsd, Action: stop
INFO:root:Service: vmware-sts-idmd, Action: stop
INFO:root:Service: vmcad, Action: stop
INFO:root:Service: vmdird, Action: stop
INFO:root:Service: vmafdd, Action: stop
Executing StartService --all
INFO:root:Service: vmafdd, Action: start
INFO:root:Service: vmware-rhttpproxy, Action: start
INFO:root:Service: vmdird, Action: start
INFO:root:Service: vmcad, Action: start
INFO:root:Service: vmware-sts-idmd, Action: start
INFO:root:Service: vmware-stsd, Action: start
INFO:root:Service: vmware-cm, Action: start
INFO:root:Service: vmware-cis-license, Action: start
INFO:root:Service: vmware-sca, Action: start
INFO:root:Service: applmgmt, Action: start
INFO:root:Service: vmware-syslog, Action: start
INFO:root:Service: vmware-syslog-health, Action: start
Copy the contents of the /ha to the other nodes
 Please copy the p12 file into the F5 loadbalancer
 Please copy the lb_rsa.key file and lb.crt file into the Netscaler loadbalancer
psc01:/sso-ha #
```

21. Set up your load balancer to balance between the two or more Platform Services Controllers on ports 443, 2012, 2014, 2020, 389, and 636.

    a. An SSL certificate (generated earlier) is required for port 443 only.

    b. For configuration steps for the F5 BIG-IP, see the appendix in this document.

22. Create a forward and reverse DNS entry for the VIP created to load-balance the Platform Services Controller traffic.

23. Connect to the second Platform Services Controller via SSH.

24. Copy the /sso-ha and /ha folder from the first Platform Services Controller.

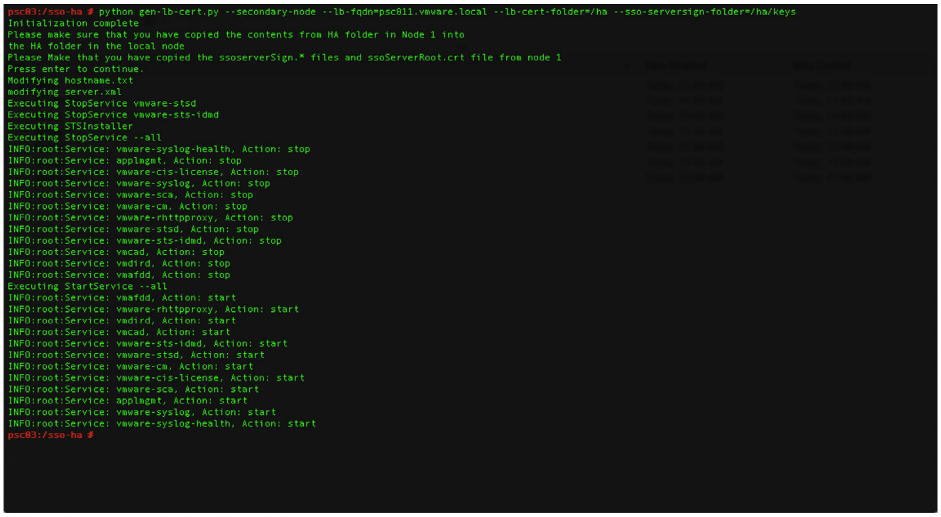
25. Copy /etc/vmware-sso/keys/ from the first Platform Services Controller to /ha/keys.

26. Change directories to /sso-ha.

27. Run:

```
python gen-lb-cert.py --secondary-node --lb-fqdn=loadbalancerFQDN --lb-cert-folder=/ha
--sso-serversign-folder=/ha/keys
```

where *loadbalancerFQDN* is the FQDN of the load balancer's VIP used for load-balancing the Platform Services Controllers.



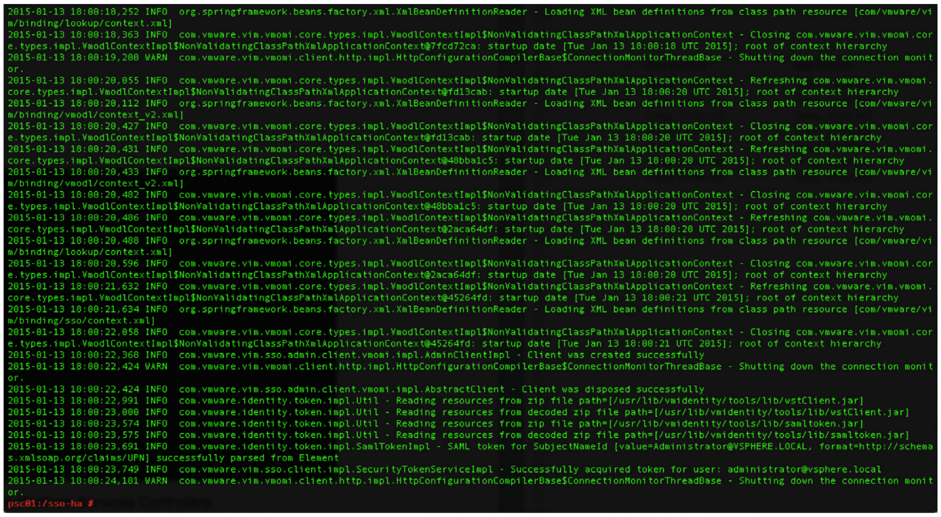
```
psc03:/sso-ha # python gen-lb-cert.py --secondary-node --lb-fqdn=psc011.vmware.local --lb-cert-folder=/ha --sso-serversign-folder=/ha/keys
Initialization complete
Please make sure that you have copied the contents from HA folder in Node 1 into
the HA folder in the local node
Please Make that you have copied the ssoserverSign.* files and ssoServerRoot.crt file from node 1
Press enter to continue.
Modifying hostname.txt
modifying server.xml
Executing StopService vmware-stsd
Executing StopService vmware-sts-idmd
Executing STSInstaller
Executing StopService --all
INFO:root:Service: vmware-syslog-health, Action: stop
INFO:root:Service: applmgmt, Action: stop
INFO:root:Service: vmware-cis-license, Action: stop
INFO:root:Service: vmware-syslog, Action: stop
INFO:root:Service: vmware-sca, Action: stop
INFO:root:Service: vmware-cm, Action: stop
INFO:root:Service: vmware-rhttpproxy, Action: stop
INFO:root:Service: vmware-stsd, Action: stop
INFO:root:Service: vmware-sts-idmd, Action: stop
INFO:root:Service: vmcad, Action: stop
INFO:root:Service: vmdird, Action: stop
INFO:root:Service: vmafdd, Action: stop
Executing StartService --all
INFO:root:Service: vmafdd, Action: start
INFO:root:Service: vmware-rhttpproxy, Action: start
INFO:root:Service: vmdird, Action: start
INFO:root:Service: vmcad, Action: start
INFO:root:Service: vmware-sts-idmd, Action: start
INFO:root:Service: vmware-stsd, Action: start
INFO:root:Service: vmware-cm, Action: start
INFO:root:Service: vmware-cis-license, Action: start
INFO:root:Service: vmware-sca, Action: start
INFO:root:Service: applmgmt, Action: start
INFO:root:Service: vmware-syslog, Action: start
INFO:root:Service: vmware-syslog-health, Action: start
psc03:/sso-ha #
```

28. Repeat steps 24–28 for any additional Platform Services Controllers.

29. On one Platform Services Controller, update the endpoint URL by running:

```
python lstoolHA.py --hostname=FQDNofLocalMachine --lb-fqdn=loadbalancerFQDN --lb-cert-
folder=/ha --user=Administrator@SSODomain --password=password
```

where *FQDNofLocalMachine* is the FQDN of the machine where the script is being run, l*oadbalancerFQDN* is the FQDN of the load balancer's VIP used for load-balancing the Platform Services Controllers, *SSODomain* is the vCenter Single Sign-On domain (by default, vsphere.local), and *password* is the password for the vCenter Single Sign-On administrator. The password parameter is optional; if not specified, you will be prompted for it.

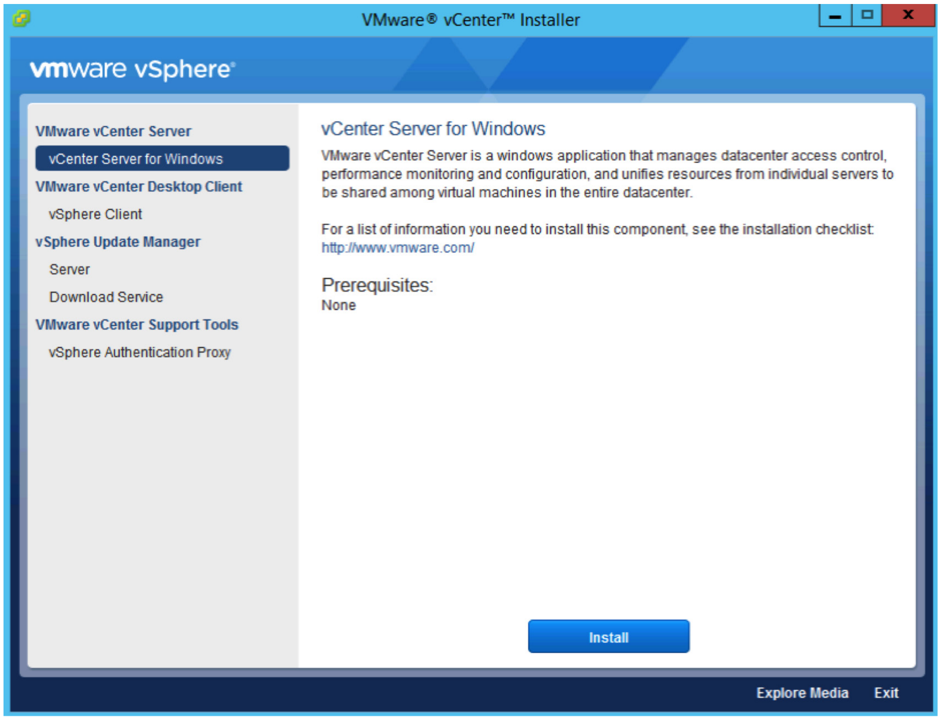


```
2015-01-13 18:00:18,252 INFO  org.springframework.beans.factory.xml.XmlBeanDefinitionReader - Loading XML bean definitions from class path resource [com/vmware/vi
m/binding/lookup/context.xml]
2015-01-13 18:00:18,363 INFO  com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext - Closing com.vmware.vim.vmomi.cor
e.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext@7fcd72ca: startup date [Tue Jan 13 18:00:18 UTC 2015]; root of context hierarchy
2015-01-13 18:00:19,200 WARN  com.vmware.vim.vmomi.client.http.impl.HttpConfigurationCompilerBase$ConnectionMonitorThreadBase - Shutting down the connection monit
or.
2015-01-13 18:00:20,055 INFO  com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext - Refreshing com.vmware.vim.vmomi.
core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext@fd13cab: startup date [Tue Jan 13 18:00:20 UTC 2015]; root of context hierarchy
2015-01-13 18:00:20,112 INFO  org.springframework.beans.factory.xml.XmlBeanDefinitionReader - Loading XML bean definitions from class path resource [com/vmware/vi
m/binding/vmodl/context_v2.xml]
2015-01-13 18:00:20,427 INFO  com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext - Closing com.vmware.vim.vmomi.cor
e.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext@fd13cab: startup date [Tue Jan 13 18:00:20 UTC 2015]; root of context hierarchy
2015-01-13 18:00:20,431 INFO  com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext - Refreshing com.vmware.vim.vmomi.
core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext@48bba1c5: startup date [Tue Jan 13 18:00:20 UTC 2015]; root of context hierarchy
2015-01-13 18:00:20,433 INFO  org.springframework.beans.factory.xml.XmlBeanDefinitionReader - Loading XML bean definitions from class path resource [com/vmware/vi
m/binding/vmodl/context_v2.xml]
2015-01-13 18:00:20,482 INFO  com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext - Closing com.vmware.vim.vmomi.cor
e.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext@48bba1c5: startup date [Tue Jan 13 18:00:20 UTC 2015]; root of context hierarchy
2015-01-13 18:00:20,486 INFO  com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext - Refreshing com.vmware.vim.vmomi.
core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext@2aca64df: startup date [Tue Jan 13 18:00:20 UTC 2015]; root of context hierarchy
2015-01-13 18:00:20,488 INFO  org.springframework.beans.factory.xml.XmlBeanDefinitionReader - Loading XML bean definitions from class path resource [com/vmware/vi
m/binding/lookup/context.xml]
2015-01-13 18:00:20,596 INFO  com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext - Closing com.vmware.vim.vmomi.cor
e.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext@2aca64df: startup date [Tue Jan 13 18:00:20 UTC 2015]; root of context hierarchy
2015-01-13 18:00:21,632 INFO  com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext - Refreshing com.vmware.vim.vmomi.
core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext@45264fd: startup date [Tue Jan 13 18:00:21 UTC 2015]; root of context hierarchy
2015-01-13 18:00:21,634 INFO  org.springframework.beans.factory.xml.XmlBeanDefinitionReader - Loading XML bean definitions from class path resource [com/vmware/vi
m/binding/sso/context.xml]
2015-01-13 18:00:22,058 INFO  com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext - Closing com.vmware.vim.vmomi.cor
e.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext@45264fd: startup date [Tue Jan 13 18:00:21 UTC 2015]; root of context hierarchy
2015-01-13 18:00:22,368 INFO  com.vmware.vim.sso.admin.client.vmomi.impl.AdminClientImpl - Client was created successfully
2015-01-13 18:00:22,424 WARN  com.vmware.vim.vmomi.client.http.impl.HttpConfigurationCompilerBase$ConnectionMonitorThreadBase - Shutting down the connection monit
or.
2015-01-13 18:00:22,424 INFO  com.vmware.vim.sso.admin.client.vmomi.impl.AbstractClient - Client was disposed successfully
2015-01-13 18:00:22,991 INFO  com.vmware.identity.token.impl.Util - Reading resources from zip file path=[/usr/lib/vmidentity/tools/lib/wstClient.jar]
2015-01-13 18:00:23,000 INFO  com.vmware.identity.token.impl.Util - Reading resources from decoded zip file path=[/usr/lib/vmidentity/tools/lib/wstClient.jar]
2015-01-13 18:00:23,574 INFO  com.vmware.identity.token.impl.Util - Reading resources from zip file path=[/usr/lib/vmidentity/tools/lib/samltoken.jar]
2015-01-13 18:00:23,575 INFO  com.vmware.identity.token.impl.Util - Reading resources from decoded zip file path=[/usr/lib/vmidentity/tools/lib/samltoken.jar]
2015-01-13 18:00:23,691 INFO  com.vmware.identity.token.impl.SamlTokenImpl - SAML token for SubjectNameId [value=Administrator@VSPHERE.LOCAL, format=http://schema
s.xmlsoap.org/claims/UPN] successfully parsed from Element
2015-01-13 18:00:23,749 INFO  com.vmware.vim.sso.client.impl.SecurityTokenServiceImpl - Successfully acquired token for user: administrator@vsphere.local
2015-01-13 18:00:24,181 WARN  com.vmware.vim.vmomi.client.http.impl.HttpConfigurationCompilerBase$ConnectionMonitorThreadBase - Shutting down the connection monit
or.
psc01:/sso-ha #
```

30. Follow the steps to install a new external vCenter Server. When asked for the Platform Services Controller, enter the FQDN of the load balancer VIP.

Upgrade of vCenter Single Sign-On High Availability

1. Back up all vCenter Single Sign-On machines.
2. Log in to one of the vCenter Single Sign-On machines in your high availability configuration.
3. Add a host file entry that contains the local machine's IP address and the FQDN of the load balancer's VIP.
4. Mount the vCenter Server 6.0 ISO image.
5. If autorun does not start, execute autorun.exe.
6. Select **vCenter Server for Windows** and click **Install**.


VMware® vCenter™ Installer
vmware vSphere®
VMware vCenter Server
vCenter Server for Windows
VMware vCenter Desktop Client
vSphere Client
vSphere Update Manager
Server
Download Service
VMware vCenter Support Tools
vSphere Authentication Proxy
Install
Explore Media
Exit

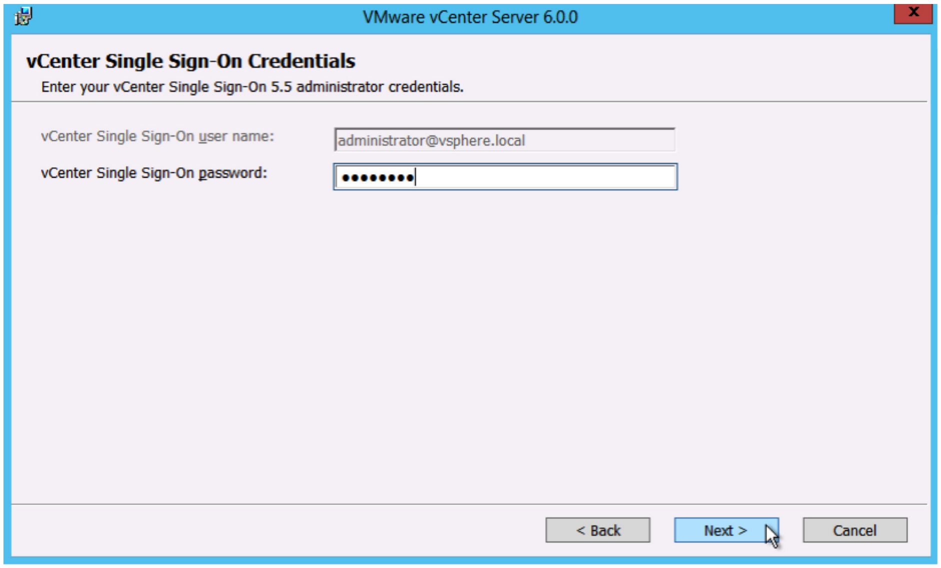
vCenter Server for Windows

VMware vCenter Server is a windows application that manages datacenter access control, performance monitoring and configuration, and unifies resources from individual servers to be shared among virtual machines in the entire datacenter.

For a list of information you need to install this component, see the installation checklist: http://www.vmware.com/

Prerequisites:
None

7. Click **Next**.
8. Accept the license agreements.
9. Enter the **password** for the administrator@vsphere.local account and click **Next**.



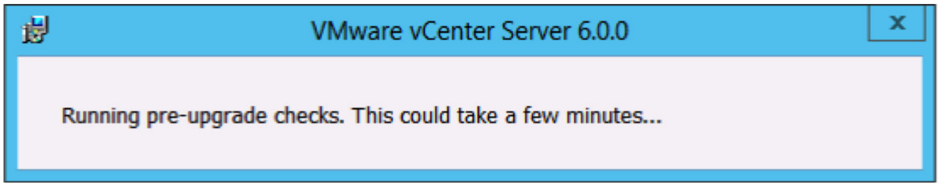
vCenter Single Sign-On Credentials

Enter your vCenter Single Sign-On 5.5 administrator credentials.

vCenter Single Sign-On user name: administrator@vsphere.local

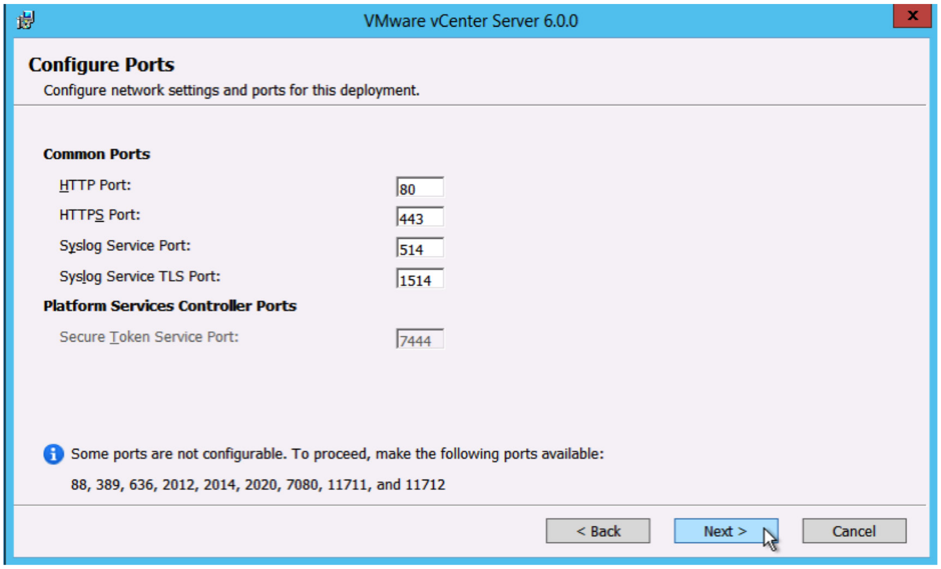
vCenter Single Sign-On password: ••••••••

10. Wait for the **pre-upgrade checks** to complete.



Running pre-upgrade checks. This could take a few minutes...

11. Review the ports and click **Next**.



Configure Ports

Configure network settings and ports for this deployment.

Common Ports

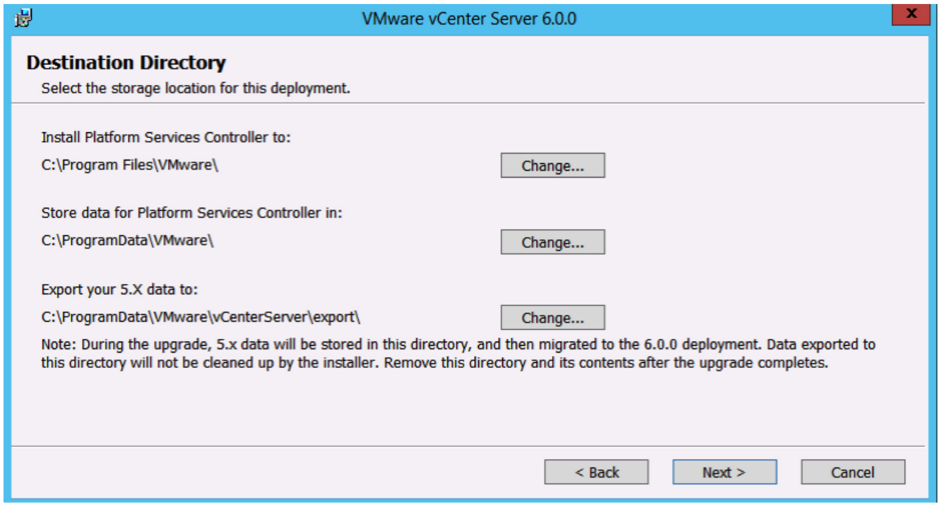
HTTP Port:	80
HTTPS Port:	443
Syslog Service Port:	514
Syslog Service TLS Port:	1514

Platform Services Controller Ports

Secure Token Service Port:	7444

Some ports are not configurable. To proceed, make the following ports available:
88, 389, 636, 2012, 2014, 2020, 7080, 11711, and 11712

12. Choose your installation path or take the defaults. Click **Next**.



Destination Directory

Select the storage location for this deployment.

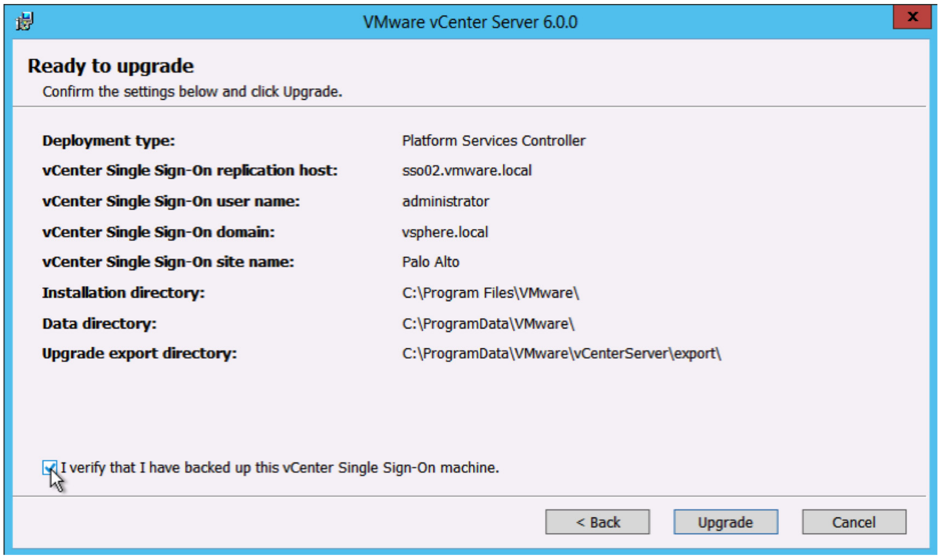
Install Platform Services Controller to:
C:\Program Files\VMware\

Store data for Platform Services Controller in:
C:\ProgramData\VMware\

Export your 5.X data to:
C:\ProgramData\VMware\vCenterServer\export\

Note: During the upgrade, 5.x data will be stored in this directory, and then migrated to the 6.0.0 deployment. Data exported to this directory will not be cleaned up by the installer. Remove this directory and its contents after the upgrade completes.

13. Check **I verify that I have backed up this Single Sign-On machine**. Click **Upgrade**.



Ready to upgrade

Confirm the settings below and click Upgrade.

Deployment type:	Platform Services Controller
vCenter Single Sign-On replication host:	sso02.vmware.local
vCenter Single Sign-On user name:	administrator
vCenter Single Sign-On domain:	vsphere.local
vCenter Single Sign-On site name:	Palo Alto
Installation directory:	C:\Program Files\VMware\
Data directory:	C:\ProgramData\VMware\
Upgrade export directory:	C:\ProgramData\VMware\vCenterServer\export\

☑ I verify that I have backed up this vCenter Single Sign-On machine.

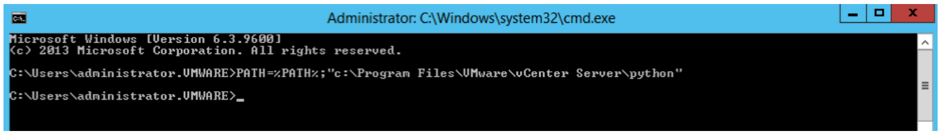
14. Click **Finish**.
15. Remove the host file entry that was added in step 3.
16. Repeat steps 2–15 on the remainder of the vCenter Single Sign-On machines.
17. Download the vCenter Single Sign-On high availability configuration scripts from the vCenter Server product download page.
18. Extract the vCenter Single Sign-On high availability scripts to c:\sso-ha.
19. Create a folder named HA in the root of c:\.
20. Copy rui.crt, rui.p12 from c:\certs\sso to c:\ha and Root64.cer from c:\certs to c:\ha.

21. Rename rui.crt to lb.crt, rui.p12 to lb.p12, and Root64.cer to root.cer.

22. Open a command prompt.

23. Add Python to your path by typing:

```
PATH=%PATH%;%VMWARE_PYTHON_HOME%
```



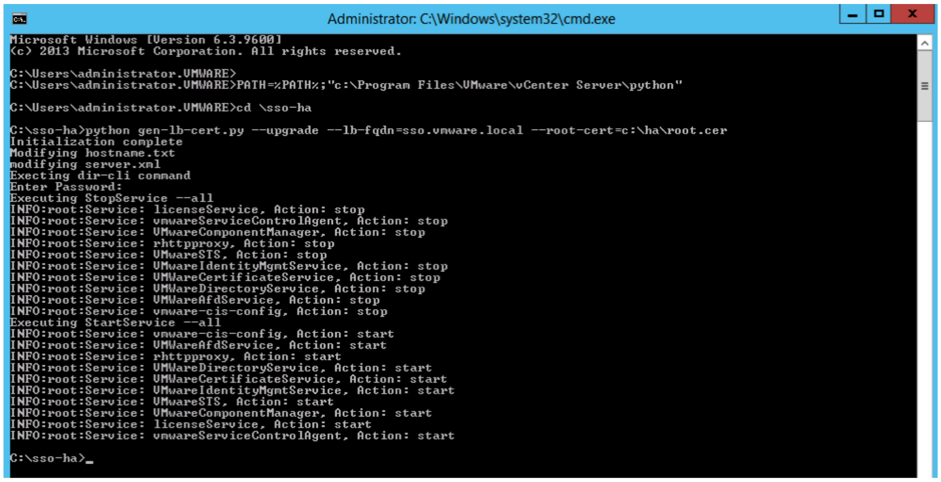
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\administrator.VMWARE>PATH=%PATH%;"c:\Program Files\VMware\vCenter Server\python"

C:\Users\administrator.VMWARE>_
```

24. Change directories to c:\sso-ha.

25. Run:

```
python gen-lb-cert.py --upgrade --lb-fqdn=loadbalancerFQDN --root-cert=c:\ha\root.cer
```

where *loadbalancerFQDN* is the FQDN of the load balancer's VIP used for load-balancing vCenter Single Sign-On.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\administrator.VMWARE>
C:\Users\administrator.VMWARE>PATH=%PATH%;"c:\Program Files\VMware\vCenter Server\python"

C:\Users\administrator.VMWARE>cd \sso-ha

C:\sso-ha>python gen-lb-cert.py --upgrade --lb-fqdn=sso.vmware.local --root-cert=c:\ha\root.cer
Initialization complete
Modifying hostname.txt
modifying server.xml
Execting dir-cli command
Enter Password:
Executing StopService --all
INFO:root:Service: licenseService, Action: stop
INFO:root:Service: vmwareServiceControlAgent, Action: stop
INFO:root:Service: VMwareComponentManager, Action: stop
INFO:root:Service: rhttpproxy, Action: stop
INFO:root:Service: VMwareSTS, Action: stop
INFO:root:Service: VMwareIdentityMgmtService, Action: stop
INFO:root:Service: VMWareCertificateService, Action: stop
INFO:root:Service: VMWareDirectoryService, Action: stop
INFO:root:Service: VMWareAfdService, Action: stop
INFO:root:Service: vmware-cis-config, Action: stop
Executing StartService --all
INFO:root:Service: vmware-cis-config, Action: start
INFO:root:Service: VMWareAfdService, Action: start
INFO:root:Service: rhttpproxy, Action: start
INFO:root:Service: VMWareDirectoryService, Action: start
INFO:root:Service: VMWareCertificateService, Action: start
INFO:root:Service: VMwareIdentityMgmtService, Action: start
INFO:root:Service: VMwareSTS, Action: start
INFO:root:Service: VMwareComponentManager, Action: start
INFO:root:Service: licenseService, Action: start
INFO:root:Service: vmwareServiceControlAgent, Action: start

C:\sso-ha>_
```

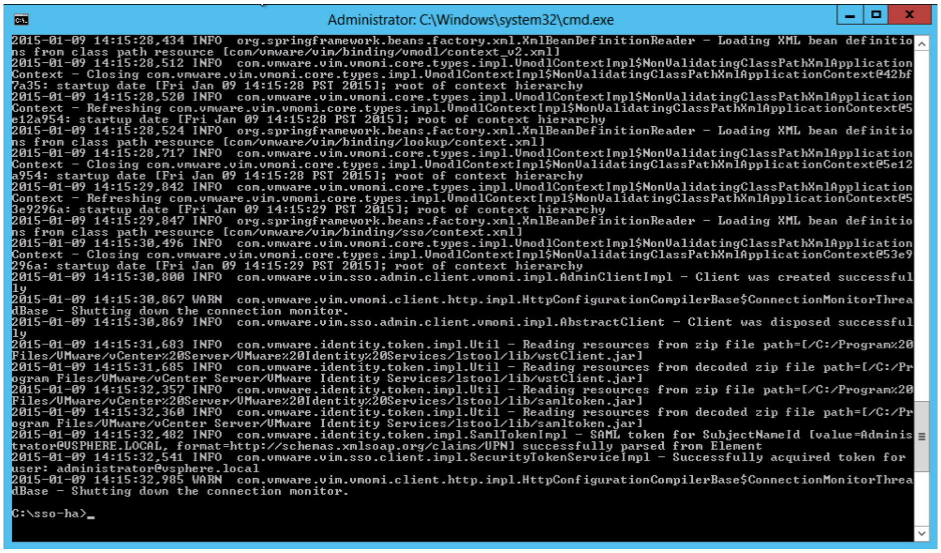
26. When prompted, enter the **password** for the administrator@vsphere.local account.

27. Repeat steps 17–26 on the remaining Platform Services Controllers.

28. On one Platform Services Controller in the site, run:

```
python lstoolHA.py --hostname=FQDNofLocalMachine --lb-fqdn=loadbalancerFQDN --lb-cert-folder=C:\ha --user=Administrator@vsphere.local --password="password"
```

where *FQDNofLocalMachine* is the FQDN of the Platform Services Controller the command is being run on, *loadbalancerFQDN* is the FQDN of the load balancer's VIP used for load-balancing vCenter Single Sign-On, and *password* is the password for the administrator@vsphere.local account. The password parameter is optional; if not specified, you will be prompted for it.

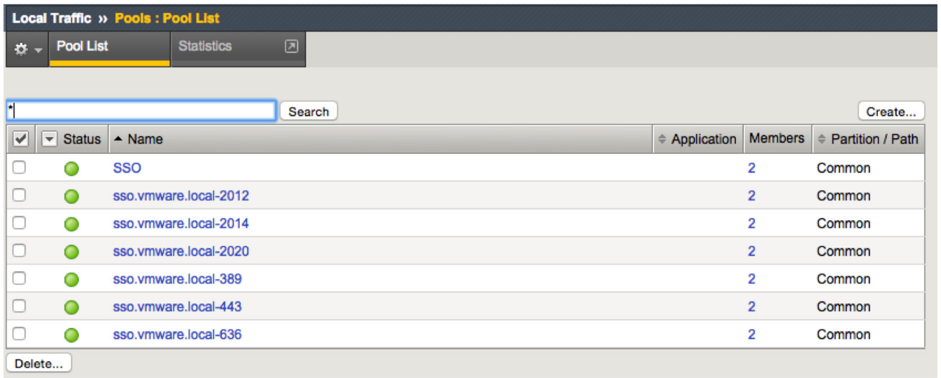


```
2015-01-09 14:15:28,434 INFO  org.springframework.beans.factory.xml.XmlBeanDefinitionReader - Loading XML bean definitio
ns from class path resource [com/vmware/vim/binding/vmodl/context_v2.xml]
2015-01-09 14:15:28,512 INFO  com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplication
Context - Closing com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext@42bf
7a35: startup date [Fri Jan 09 14:15:28 PST 2015]; root of context hierarchy
2015-01-09 14:15:28,520 INFO  com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplication
Context - Refreshing com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext@5
e12a954: startup date [Fri Jan 09 14:15:28 PST 2015]; root of context hierarchy
2015-01-09 14:15:28,524 INFO  org.springframework.beans.factory.xml.XmlBeanDefinitionReader - Loading XML bean definitio
ns from class path resource [com/vmware/vim/binding/lookup/context.xml]
2015-01-09 14:15:28,717 INFO  com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplication
Context - Closing com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext@5e12
a954: startup date [Fri Jan 09 14:15:28 PST 2015]; root of context hierarchy
2015-01-09 14:15:29,842 INFO  com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplication
Context - Refreshing com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext@5
3e9296a: startup date [Fri Jan 09 14:15:29 PST 2015]; root of context hierarchy
2015-01-09 14:15:29,847 INFO  org.springframework.beans.factory.xml.XmlBeanDefinitionReader - Loading XML bean definitio
ns from class path resource [com/vmware/vim/binding/sso/context.xml]
2015-01-09 14:15:30,496 INFO  com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplication
Context - Closing com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl$NonValidatingClassPathXmlApplicationContext@53e9
296a: startup date [Fri Jan 09 14:15:29 PST 2015]; root of context hierarchy
2015-01-09 14:15:30,800 INFO  com.vmware.vim.sso.admin.client.vmomi.impl.AdminClientImpl - Client was created successful
ly
2015-01-09 14:15:30,867 WARN  com.vmware.vim.vmomi.client.http.impl.HttpConfigurationCompilerBase$ConnectionMonitorThrea
dBase - Shutting down the connection monitor.
2015-01-09 14:15:30,869 INFO  com.vmware.vim.sso.admin.client.vmomi.impl.AbstractClient - Client was disposed successful
ly
2015-01-09 14:15:31,683 INFO  com.vmware.identity.token.impl.Util - Reading resources from zip file path=[/C:/Program%20
Files/VMware/vCenter%20Server/VMware%20Identity%20Services/lstool/lib/wstClient.jar]
2015-01-09 14:15:31,685 INFO  com.vmware.identity.token.impl.Util - Reading resources from decoded zip file path=[/C:/Pr
ogram Files/VMware/vCenter Server/VMware Identity Services/lstool/lib/wstClient.jar]
2015-01-09 14:15:32,357 INFO  com.vmware.identity.token.impl.Util - Reading resources from zip file path=[/C:/Program%20
Files/VMware/vCenter%20Server/VMware%20Identity%20Services/lstool/lib/samltoken.jar]
2015-01-09 14:15:32,360 INFO  com.vmware.identity.token.impl.Util - Reading resources from decoded zip file path=[/C:/Pr
ogram Files/VMware/vCenter Server/VMware Identity Services/lstool/lib/samltoken.jar]
2015-01-09 14:15:32,482 INFO  com.vmware.identity.token.impl.SamlTokenImpl - SAML token for SubjectNameId [value=Adminis
trator@VSPHERE.LOCAL, format=http://schemas.xmlsoap.org/claims/UPN] successfully parsed from Element
2015-01-09 14:15:32,541 INFO  com.vmware.vim.sso.client.impl.SecurityTokenServiceImpl - Successfully acquired token for
user: administrator@vsphere.local
2015-01-09 14:15:32,985 WARN  com.vmware.vim.vmomi.client.http.impl.HttpConfigurationCompilerBase$ConnectionMonitorThrea
dBase - Shutting down the connection monitor.

C:\sso-ha>_
```

29. Log in to the load balancer. In this example, we are using an F5 BIG-IP.

30. Create a pool for ports 443, 2012, 2014, 2020, 389, and 636. Set health monitors to use **TCP** and **Load Balancing Method** to **Round Robin**.

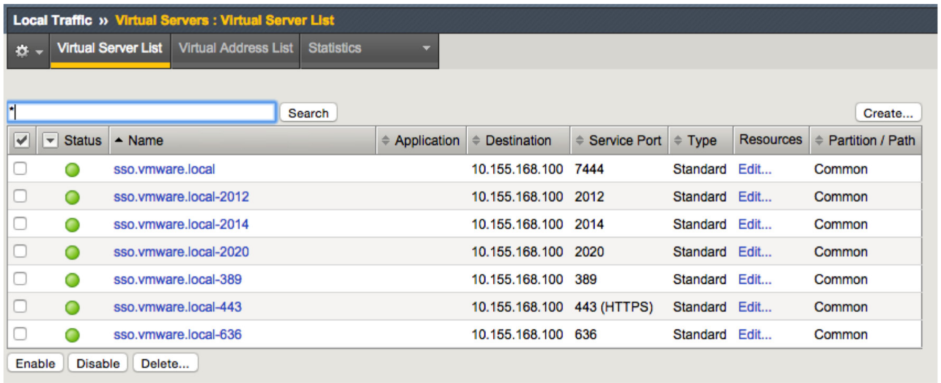
    When complete, the **Pool List** should look like this:



☑	Status	Name	Application	Members	Partition / Path
□	●	SSO		2	Common
□	●	sso.vmware.local-2012		2	Common
□	●	sso.vmware.local-2014		2	Common
□	●	sso.vmware.local-2020		2	Common
□	●	sso.vmware.local-389		2	Common
□	●	sso.vmware.local-443		2	Common
□	●	sso.vmware.local-636		2	Common

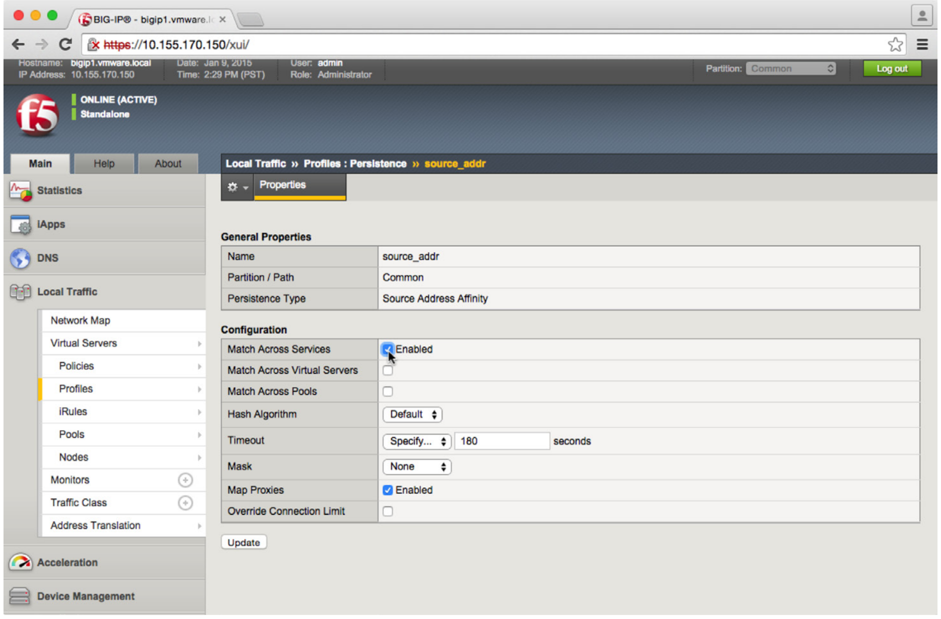
31. Create a virtual server using the same IP address as the original vCenter Single Sign-On high availability virtual server for each of the new pools. Use **TCP** for each virtual server. Set **Source Address Translation** to **Auto Map** and **Default Persistence Profile** to **Source Address**. Assign the client and server SSL profiles created when setting up vCenter Single Sign-On high availability for vCenter Server 5.5 to port 443 only. No other port requires a client or server SSL profile.

    When complete, the **Virtual Server List** should look like this:



☑	Status	Name	Application	Destination	Service Port	Type	Resources	Partition / Path
□	🟢	sso.vmware.local		10.155.168.100	7444	Standard	Edit...	Common
□	🟢	sso.vmware.local-2012		10.155.168.100	2012	Standard	Edit...	Common
□	🟢	sso.vmware.local-2014		10.155.168.100	2014	Standard	Edit...	Common
□	🟢	sso.vmware.local-2020		10.155.168.100	2020	Standard	Edit...	Common
□	🟢	sso.vmware.local-389		10.155.168.100	389	Standard	Edit...	Common
□	🟢	sso.vmware.local-443		10.155.168.100	443 (HTTPS)	Standard	Edit...	Common
□	🟢	sso.vmware.local-636		10.155.168.100	636	Standard	Edit...	Common

32. Edit the **source_addr Persistence Policy** and check the **Match Across Services** box.



General Properties

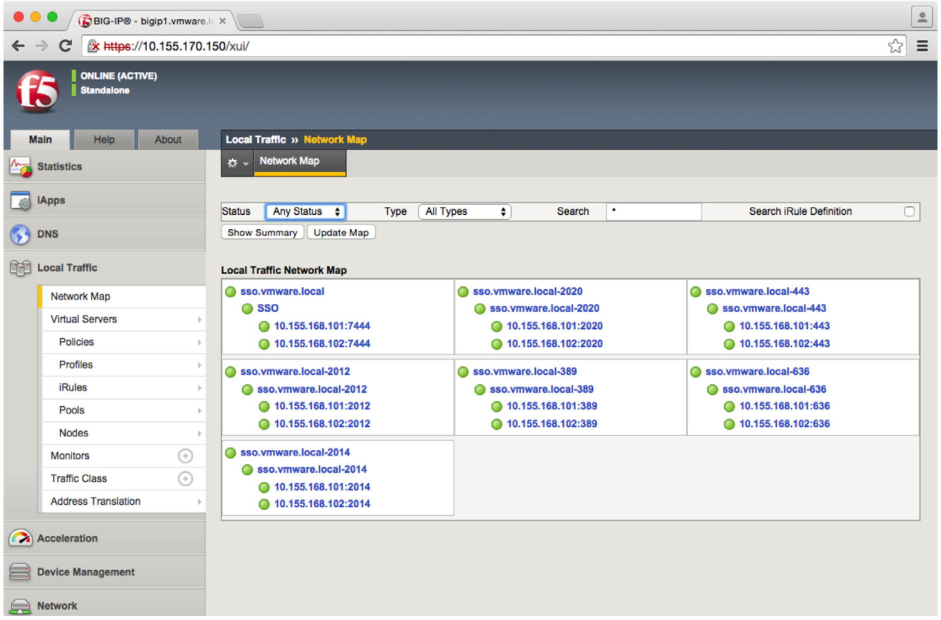
Name	source_addr
Partition / Path	Common
Persistence Type	Source Address Affinity

Configuration

Match Across Services	☑ Enabled
Match Across Virtual Servers	□
Match Across Pools	□
Hash Algorithm	Default
Timeout	Specify... 180 seconds
Mask	None
Map Proxies	☑ Enabled
Override Connection Limit	□

33. View the **Network Map** and verify that all services are up (green).

    For full configuration instructions of the F5 BIG-IP load balancer, see the appendix.



Status: Any Status — Type: All Types — Search: * — Search iRule Definition □

Local Traffic Network Map

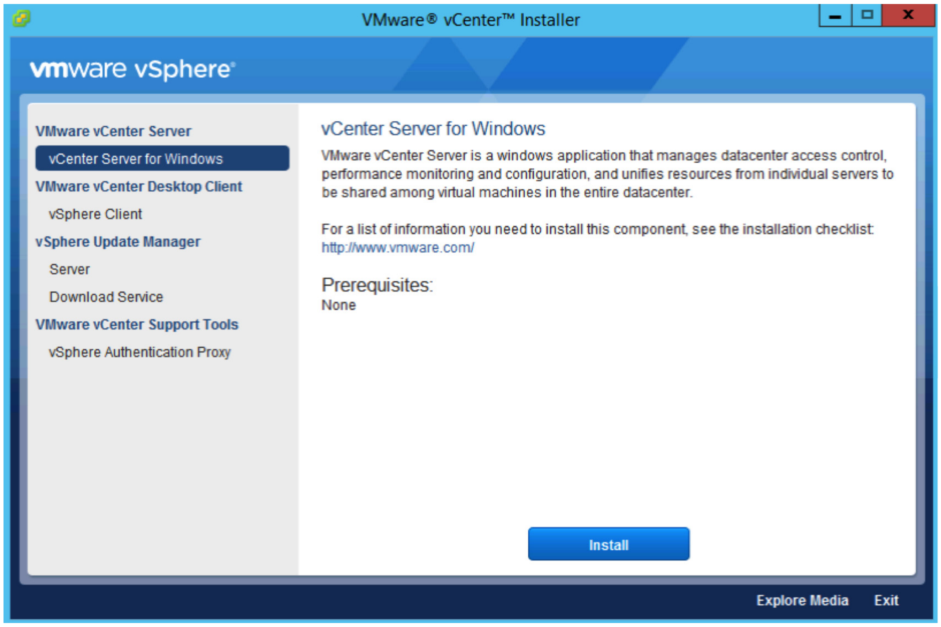
● sso.vmware.local ● SSO ● 10.155.168.101:7444 ● 10.155.168.102:7444	● sso.vmware.local-2020 ● sso.vmware.local-2020 ● 10.155.168.101:2020 ● 10.155.168.102:2020	● sso.vmware.local-443 ● sso.vmware.local-443 ● 10.155.168.101:443 ● 10.155.168.102:443
● sso.vmware.local-2012 ● sso.vmware.local-2012 ● 10.155.168.101:2012 ● 10.155.168.102:2012	● sso.vmware.local-389 ● sso.vmware.local-389 ● 10.155.168.101:389 ● 10.155.168.102:389	● sso.vmware.local-636 ● sso.vmware.local-636 ● 10.155.168.101:636 ● 10.155.168.102:636
● sso.vmware.local-2014 ● sso.vmware.local-2014 ● 10.155.168.101:2014 ● 10.155.168.102:2014		

34. Log in to the vCenter Server you want to upgrade.

35. Mount the vCenter Server 6.0 ISO image.

36. If autorun does not start, execute autorun.exe.

37. Select **vCenter Server for Windows** and click **Install**.


VMware® vCenter™ Installer
vmware vSphere
VMware vCenter Server
vCenter Server for Windows
VMware vCenter Desktop Client
vSphere Client
vSphere Update Manager
Server
Download Service
VMware vCenter Support Tools
vSphere Authentication Proxy
Install
Explore Media
Exit

vCenter Server for Windows

VMware vCenter Server is a windows application that manages datacenter access control, performance monitoring and configuration, and unifies resources from individual servers to be shared among virtual machines in the entire datacenter.

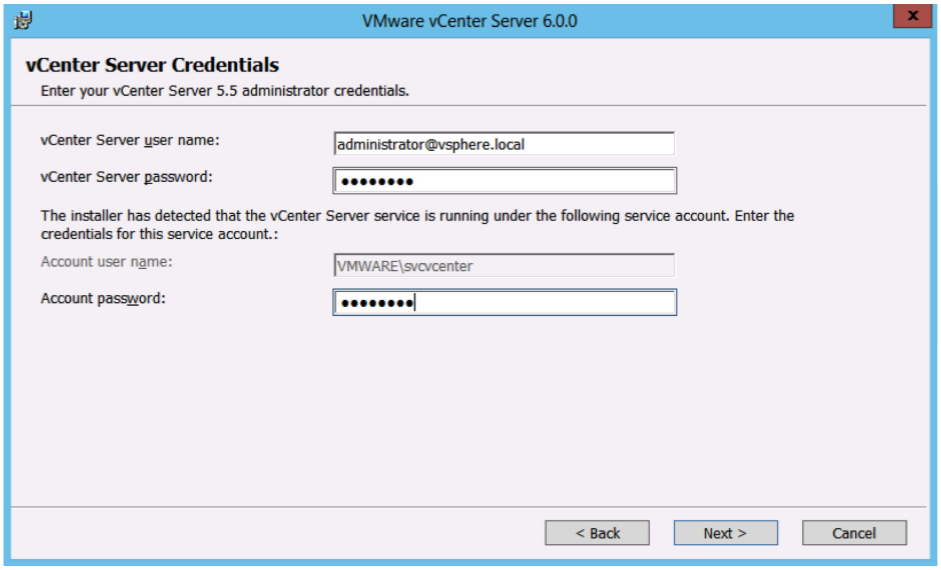
For a list of information you need to install this component, see the installation checklist: http://www.vmware.com/

Prerequisites:
None

38. Click **Next**.

39. Accept the license agreements.

40. Enter the **password** for the administrator@vsphere.local account and the **password** for the service account (if applicable). Click **Next**.



vCenter Server Credentials

Enter your vCenter Server 5.5 administrator credentials.

vCenter Server user name: administrator@vsphere.local

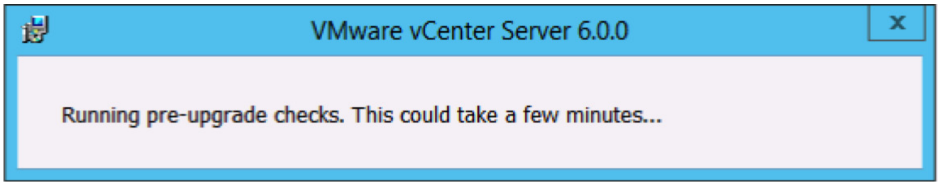
vCenter Server password: ●●●●●●●●

The installer has detected that the vCenter Server service is running under the following service account. Enter the credentials for this service account.:

Account user name: VMWARE\svcvcenter

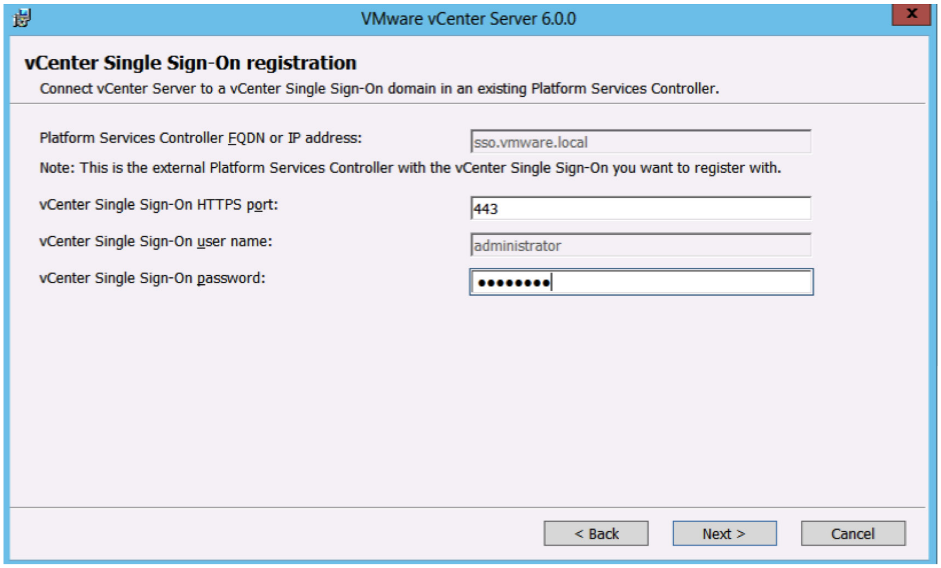
Account password: ●●●●●●●●

41. Wait for the **pre-upgrade checks** to complete.



Running pre-upgrade checks. This could take a few minutes...

42. Enter the **password** for the administrator@vsphere.local account. Click **Next**.



vCenter Single Sign-On registration

Connect vCenter Server to a vCenter Single Sign-On domain in an existing Platform Services Controller.

Platform Services Controller FQDN or IP address: sso.vmware.local

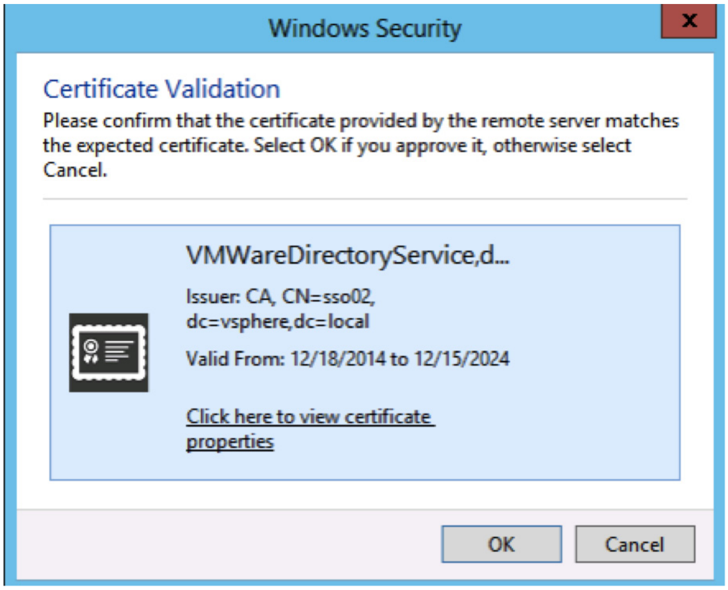
Note: This is the external Platform Services Controller with the vCenter Single Sign-On you want to register with.

vCenter Single Sign-On HTTPS port: 443

vCenter Single Sign-On user name: administrator

vCenter Single Sign-On password: ●●●●●●●●

43. Click **OK** to accept the certificate.



Windows Security

Certificate Validation

Please confirm that the certificate provided by the remote server matches the expected certificate. Select OK if you approve it, otherwise select Cancel.

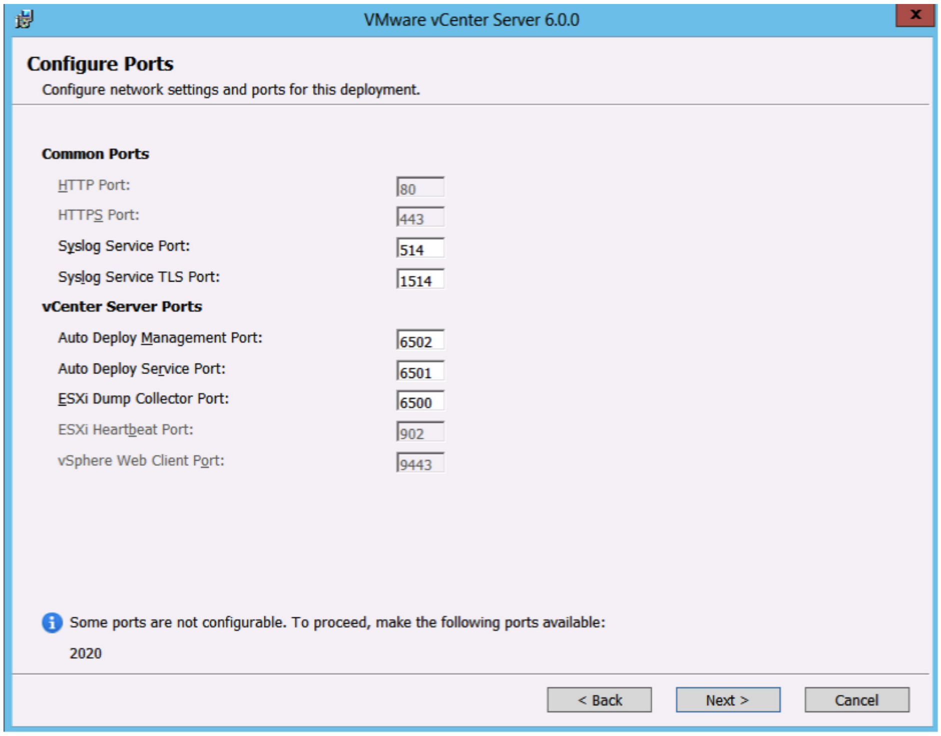
VMWareDirectoryService,d...

Issuer: CA, CN=sso02, dc=vsphere,dc=local

Valid From: 12/18/2014 to 12/15/2024

Click here to view certificate properties

44. Accept the default ports and click **Next**.



VMware vCenter Server 6.0.0

Configure Ports

Configure network settings and ports for this deployment.

Common Ports

HTTP Port: 80
HTTPS Port: 443
Syslog Service Port: 514
Syslog Service TLS Port: 1514

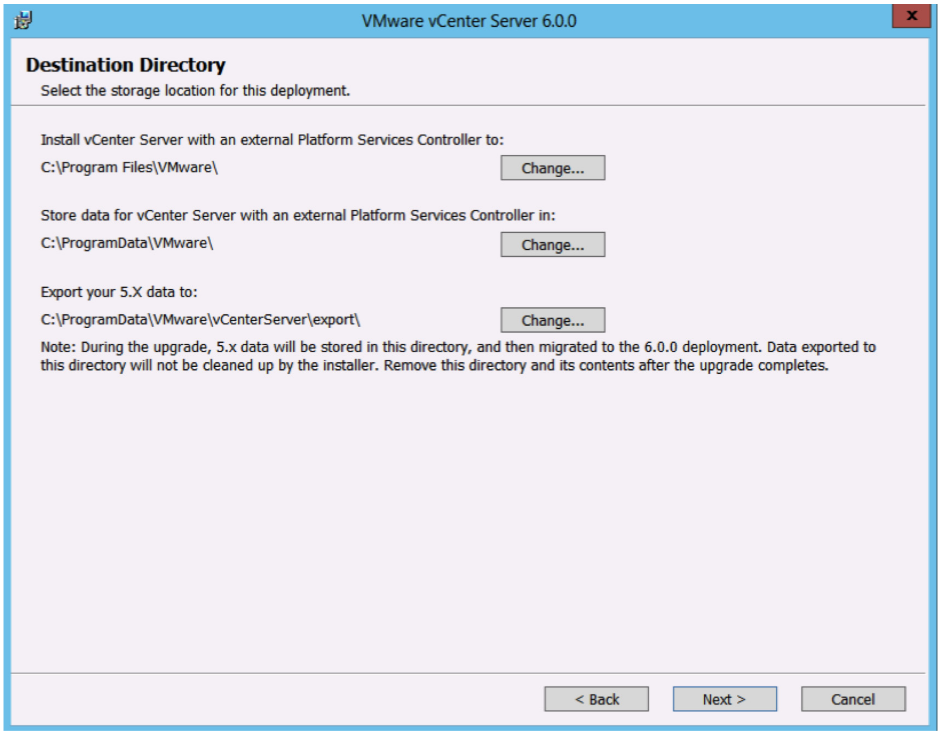
vCenter Server Ports

Auto Deploy Management Port: 6502
Auto Deploy Service Port: 6501
ESXi Dump Collector Port: 6500
ESXi Heartbeat Port: 902
vSphere Web Client Port: 9443

Some ports are not configurable. To proceed, make the following ports available:

2020

45. Accept or change the installation paths as necessary. Click **Next**.



Destination Directory

Select the storage location for this deployment.

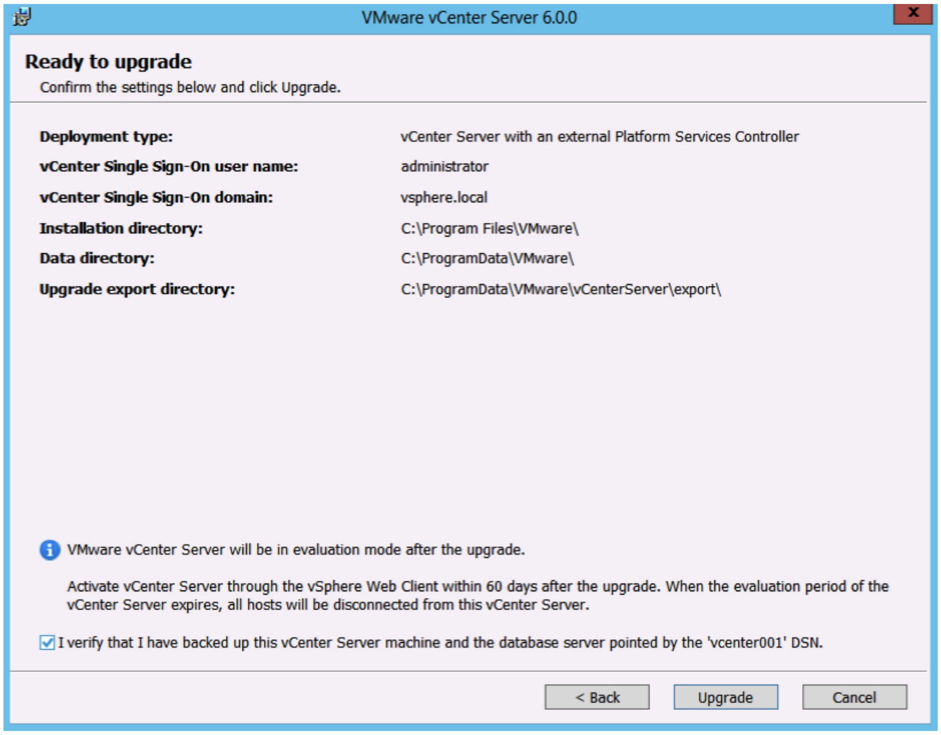
Install vCenter Server with an external Platform Services Controller to:
C:\Program Files\VMware\

Store data for vCenter Server with an external Platform Services Controller in:
C:\ProgramData\VMware\

Export your 5.X data to:
C:\ProgramData\VMware\vCenterServer\export\

Note: During the upgrade, 5.x data will be stored in this directory, and then migrated to the 6.0.0 deployment. Data exported to this directory will not be cleaned up by the installer. Remove this directory and its contents after the upgrade completes.

46. Check the box to verify that you have backed up the vCenter Server and its database. Click **Upgrade**.



Ready to upgrade

Confirm the settings below and click Upgrade.

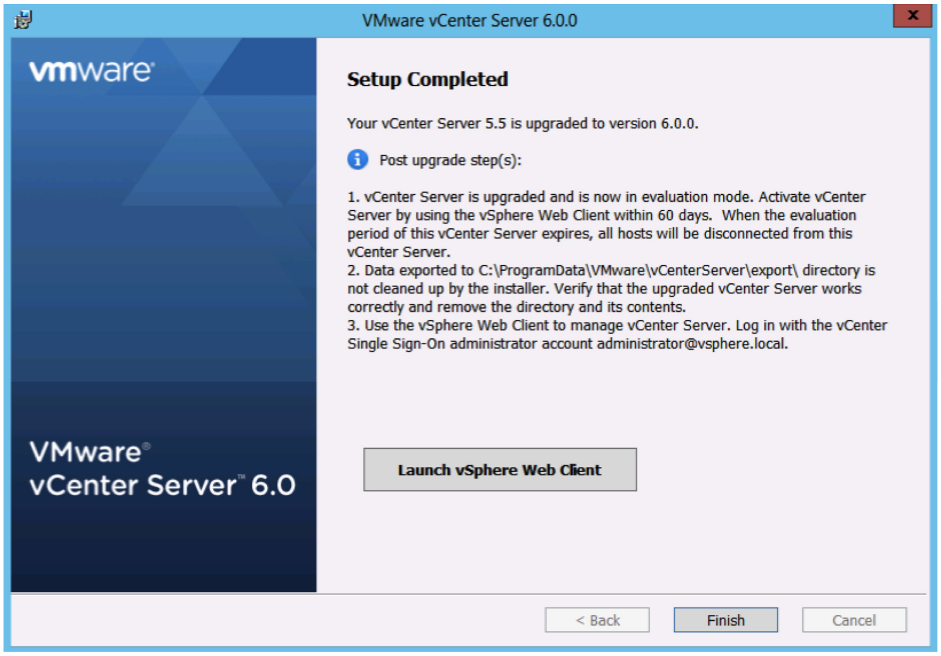
Deployment type:	vCenter Server with an external Platform Services Controller
vCenter Single Sign-On user name:	administrator
vCenter Single Sign-On domain:	vsphere.local
Installation directory:	C:\Program Files\VMware\
Data directory:	C:\ProgramData\VMware\
Upgrade export directory:	C:\ProgramData\VMware\vCenterServer\export\

VMware vCenter Server will be in evaluation mode after the upgrade.

Activate vCenter Server through the vSphere Web Client within 60 days after the upgrade. When the evaluation period of the vCenter Server expires, all hosts will be disconnected from this vCenter Server.

☑ I verify that I have backed up this vCenter Server machine and the database server pointed by the 'vcenter001' DSN.

47. When completed, click **Finish**.



Setup Completed

Your vCenter Server 5.5 is upgraded to version 6.0.0.

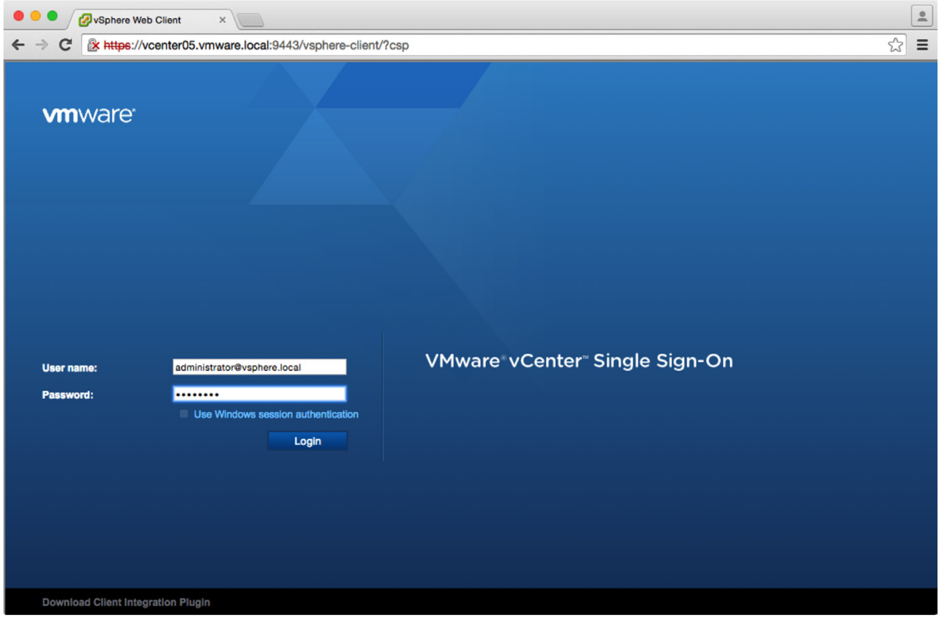
Post upgrade step(s):

1. vCenter Server is upgraded and is now in evaluation mode. Activate vCenter Server by using the vSphere Web Client within 60 days. When the evaluation period of this vCenter Server expires, all hosts will be disconnected from this vCenter Server.
2. Data exported to C:\ProgramData\VMware\vCenterServer\export\ directory is not cleaned up by the installer. Verify that the upgraded vCenter Server works correctly and remove the directory and its contents.
3. Use the vSphere Web Client to manage vCenter Server. Log in with the vCenter Single Sign-On administrator account administrator@vsphere.local.

Postdeployment Steps

Configure Identity Sources

1. Open your Web browser and navigate to https://vcenter:9443, where *vcenter* is the FQDN of the vCenter Server.
2. Log in with **User name** administrator@vsphere.local and the **Password** used during installation.

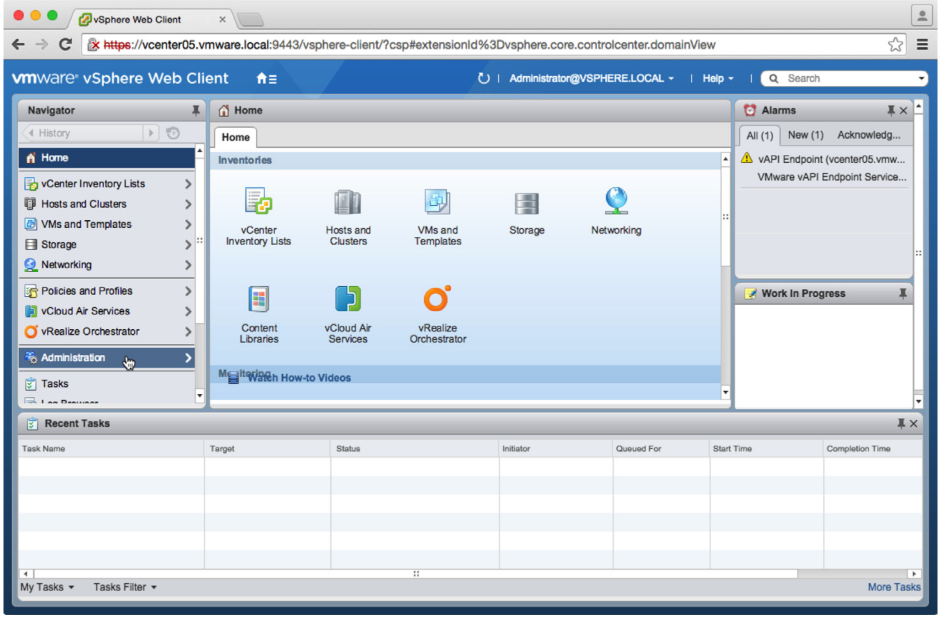

vSphere Web Client
vmware
VMware vCenter Single Sign-On
□ Use Windows session authentication
Login
Download Client Integration Plugin

https://vcenter05.vmware.local:9443/vsphere-client/?csp

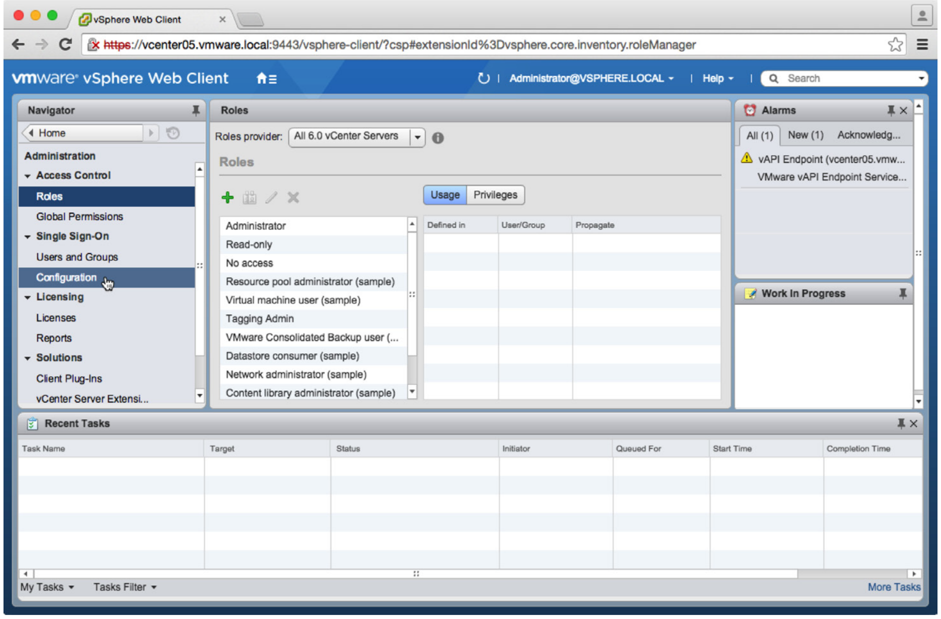
User name: administrator@vsphere.local

Password: ••••••••

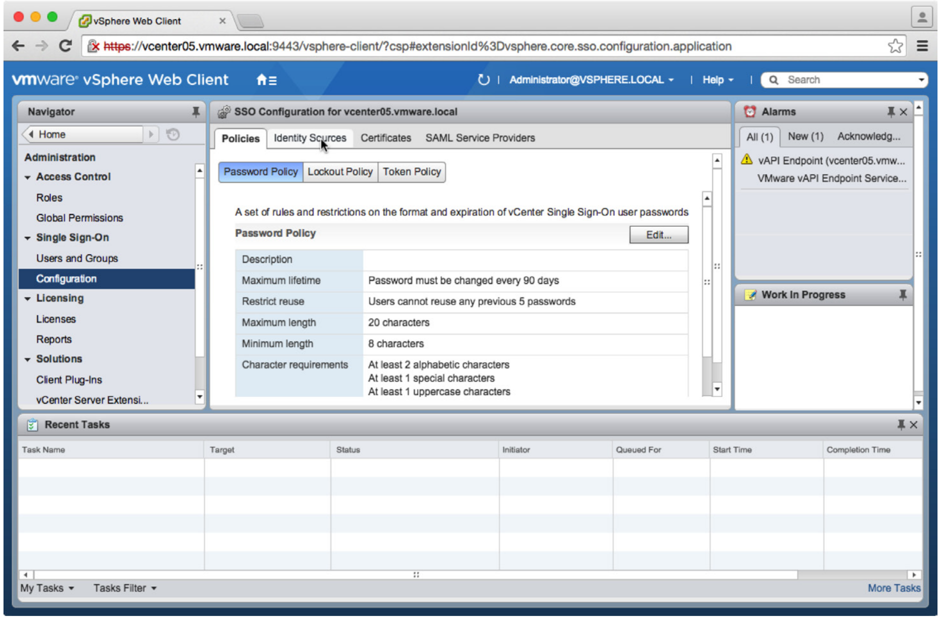
3. Click **Administration** in the left-hand **Navigator** pane.



4. Click **Configuration** under vCenter **Single Sign-On**.



5. Click **Identity Sources**.

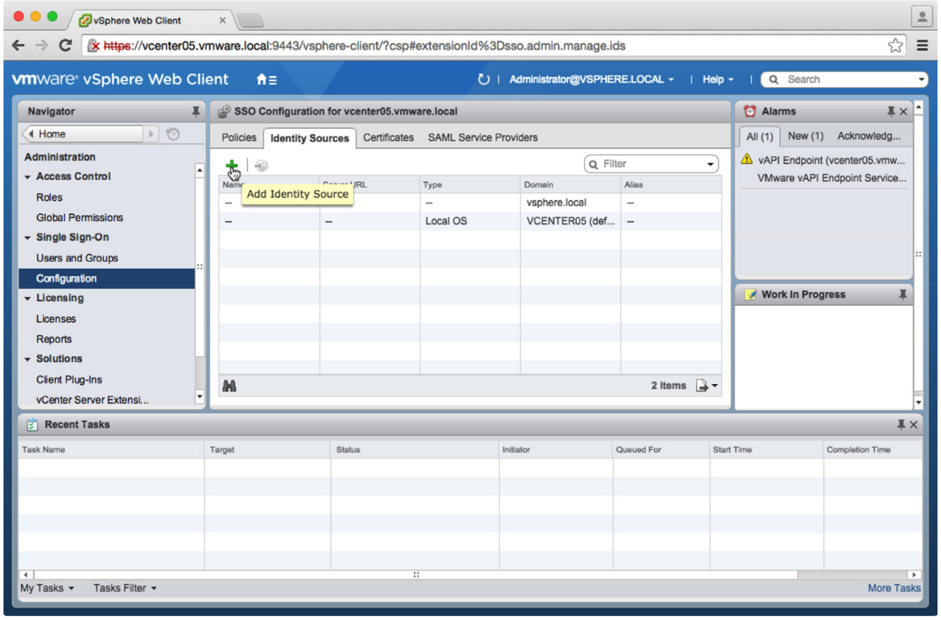


A set of rules and restrictions on the format and expiration of vCenter Single Sign-On user passwords

Password Policy

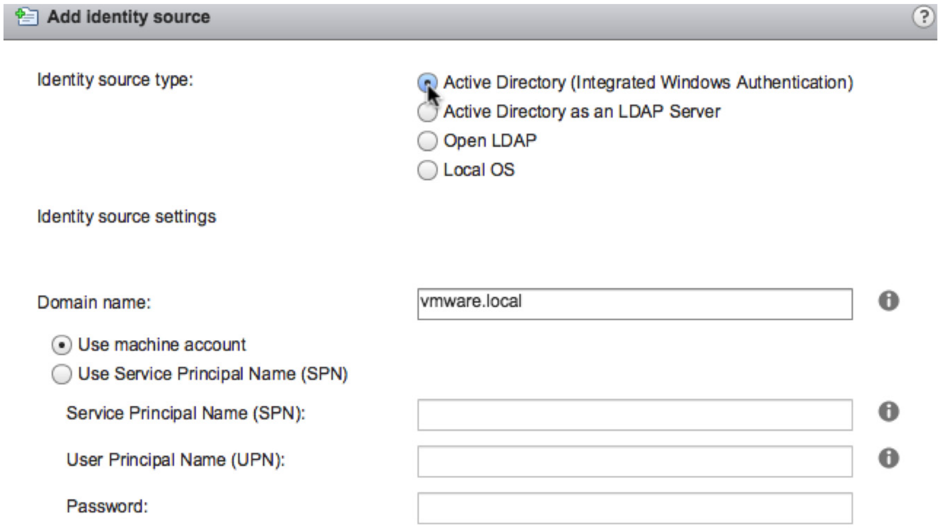
Description	
Maximum lifetime	Password must be changed every 90 days
Restrict reuse	Users cannot reuse any previous 5 passwords
Maximum length	20 characters
Minimum length	8 characters
Character requirements	At least 2 alphabetic characters At least 1 special characters At least 1 uppercase characters

6. Click the **green plus** icon to **Add Identity Source**.



Nam	URL	Type	Domain	Alias
--		--	vsphere.local	--
--	--	Local OS	VCENTER05 (def...	--

7. If using Microsoft Active Directory, select **Active Directory (Integrated Windows Authentication)**. It will autopopulate the root domain in the forest. If using Open LDAP, select and configure it.



Identity source type:

- ● Active Directory (Integrated Windows Authentication)
- ○ Active Directory as an LDAP Server
- ○ Open LDAP
- ○ Local OS

Identity source settings

Domain name: vmware.local

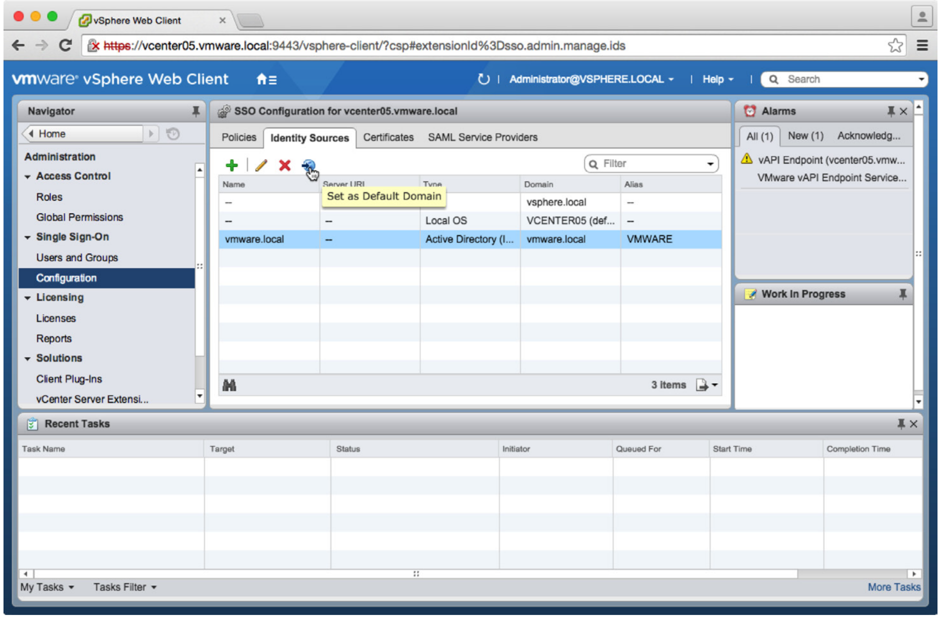
- ● Use machine account
- ○ Use Service Principal Name (SPN)

Service Principal Name (SPN):

User Principal Name (UPN):

Password:

8. Highlight the newly added identity source. Click the **Set as Default Domain** icon.



SSO Configuration for vcenter05.vmware.local

Policies | Identity Sources | Certificates | SAML Service Providers

Set as Default Domain

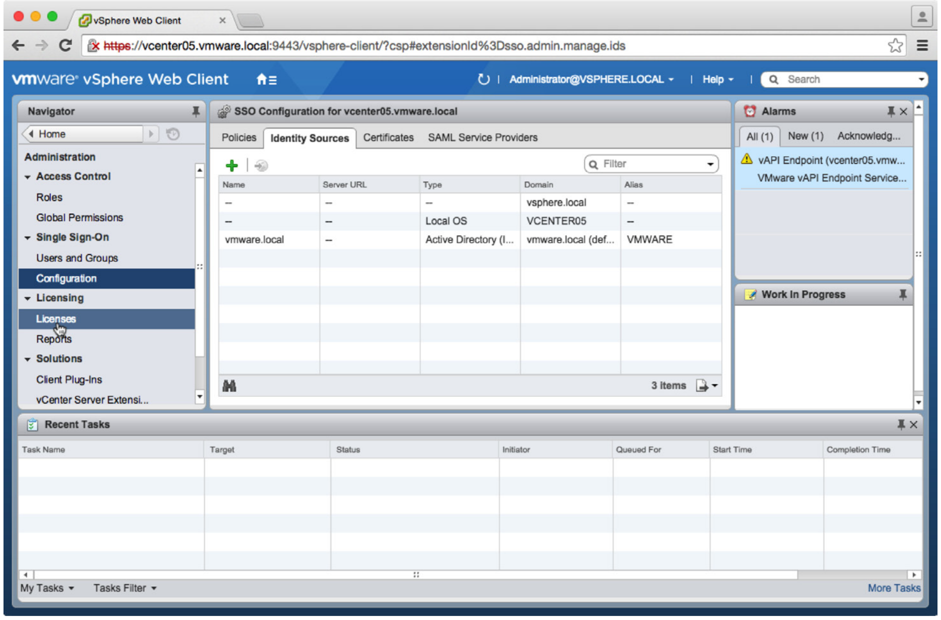
Name	Server URL	Type	Domain	Alias
--			vsphere.local	--
--	--	Local OS	VCENTER05 (def...	--
vmware.local	--	Active Directory (I...	vmware.local	VMWARE

3 items

9. Click **Yes** in the pop-up.

License Management

1. Click **Licenses** in the left-hand **Navigator** pane.



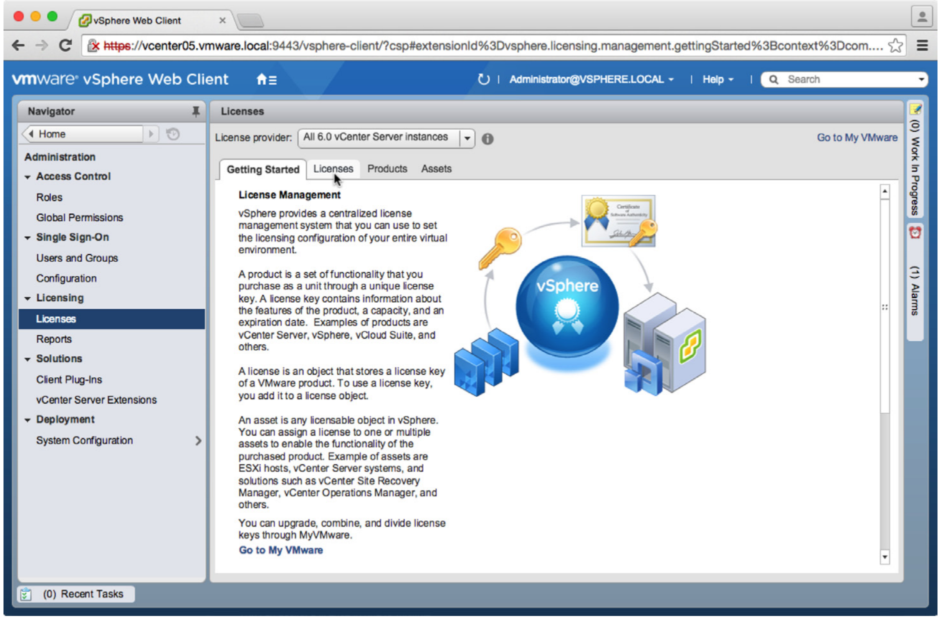
https://vcenter05.vmware.local:9443/vsphere-client/?csp#extensionId%3Dsso.admin.manage.ids

SSO Configuration for vcenter05.vmware.local

Name	Server URL	Type	Domain	Alias
--	--	--	vsphere.local	--
--	--	Local OS	VCENTER05	--
vmware.local	--	Active Directory (I...	vmware.local (def...	VMWARE

3 items

2. Click **Licenses**.



https://vcenter05.vmware.local:9443/vsphere-client/?csp#extensionId%3Dvsphere.licensing.management.gettingStarted%3Bcontext%3Dcom....

License provider: All 6.0 vCenter Server instances

License Management

vSphere provides a centralized license management system that you can use to set the licensing configuration of your entire virtual environment.

A product is a set of functionality that you purchase as a unit through a unique license key. A license key contains information about the features of the product, a capacity, and an expiration date. Examples of products are vCenter Server, vSphere, vCloud Suite, and others.

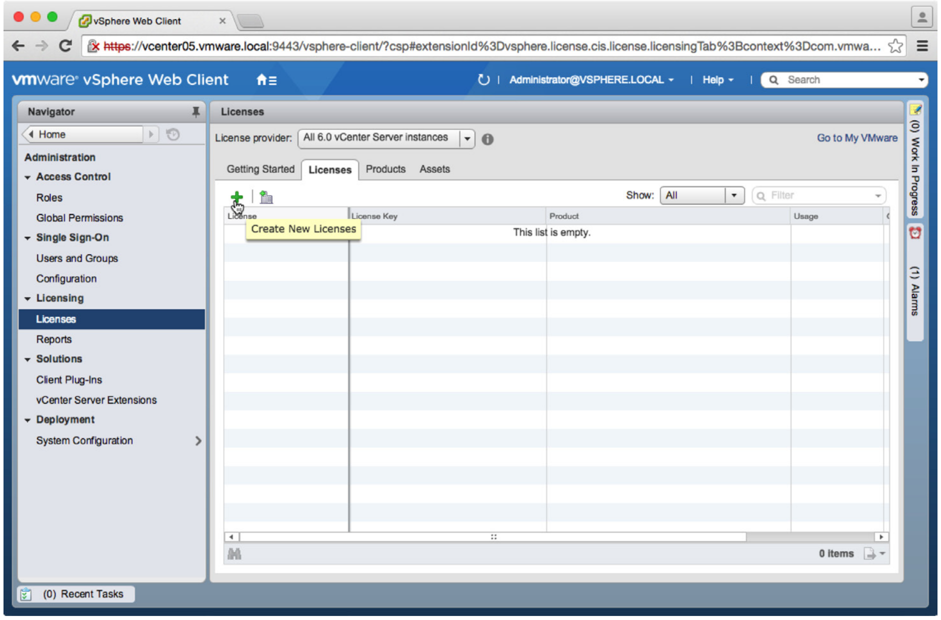
A license is an object that stores a license key of a VMware product. To use a license key, you add it to a license object.

An asset is any licensable object in vSphere. You can assign a license to one or multiple assets to enable the functionality of the purchased product. Example of assets are ESXi hosts, vCenter Server systems, and solutions such as vCenter Site Recovery Manager, vCenter Operations Manager, and others.

You can upgrade, combine, and divide license keys through MyVMware.

Go to My VMware

3. Click the **green plus** icon to add your licenses.



License provider: All 6.0 vCenter Server instances

Show: All

Create New Licenses

License	License Key	Product	Usage

This list is empty.

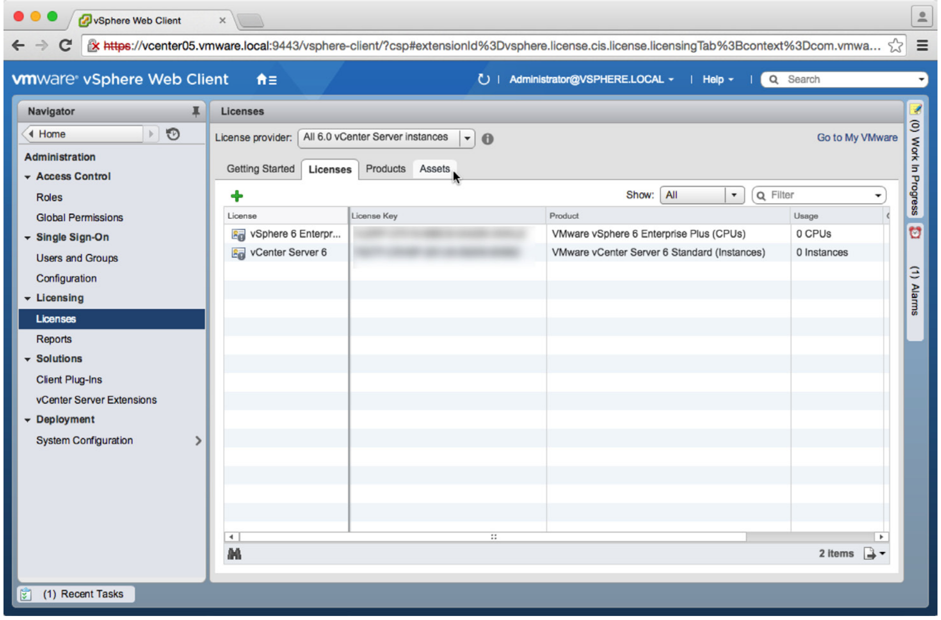
0 items

4. Enter your license keys, one per line, and click **Next**.

5. Give each license a descriptive name and click **Next**.

6. Click **Finish**.

7. Click **Assets**.



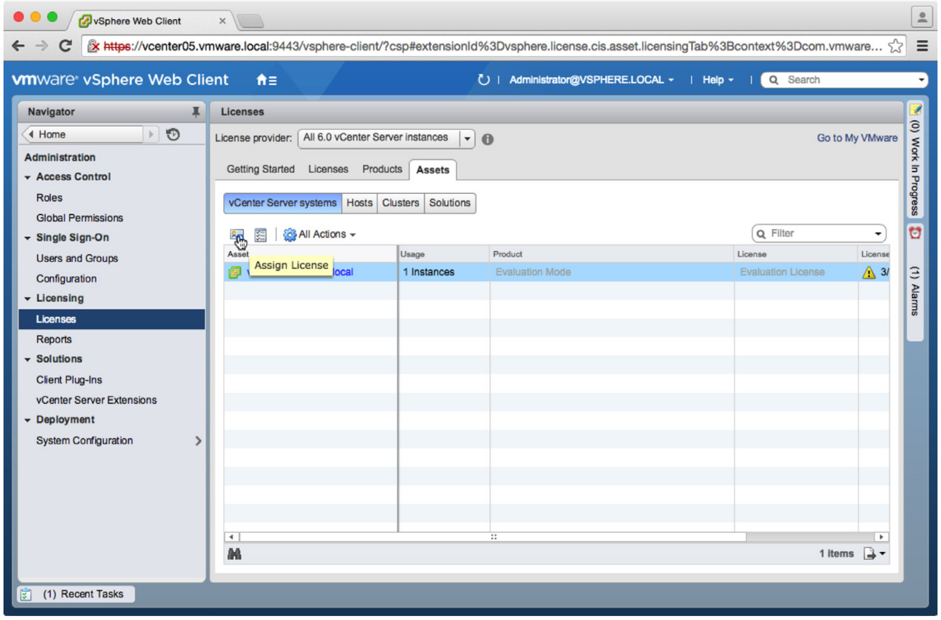
License provider: All 6.0 vCenter Server instances

Show: All

License	License Key	Product	Usage
vSphere 6 Enterpr...	[redacted]	VMware vSphere 6 Enterprise Plus (CPUs)	0 CPUs
vCenter Server 6	[redacted]	VMware vCenter Server 6 Standard (Instances)	0 Instances

2 items

8. Highlight **vCenter Server systems** in evaluation mode and click the **Assign License** icon.

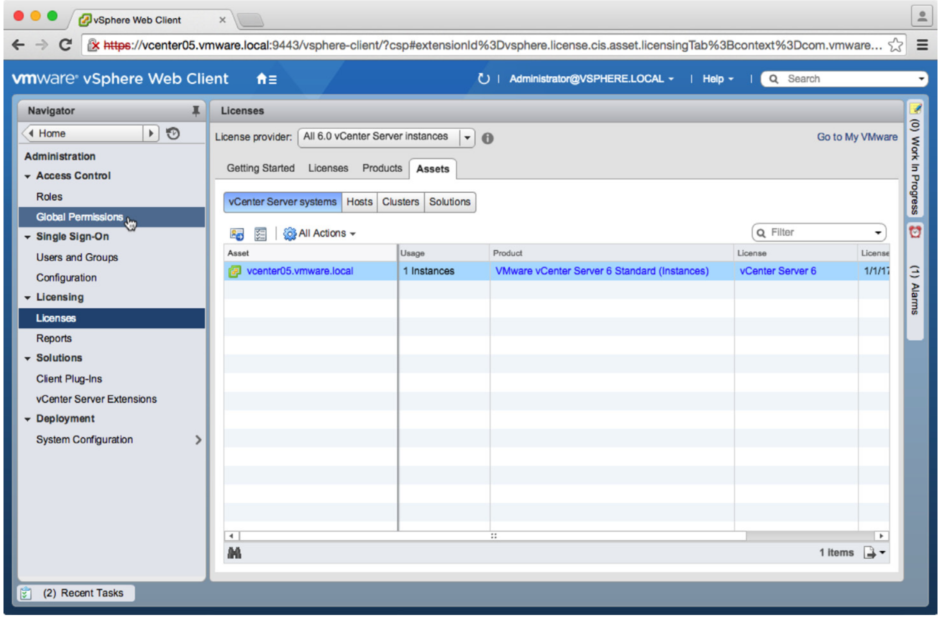


Asset	Usage	Product	License	License
ocal	1 Instances	Evaluation Mode	Evaluation License	3/

9. Select the vCenter Server license entered earlier and click **OK**.

Global Permissions

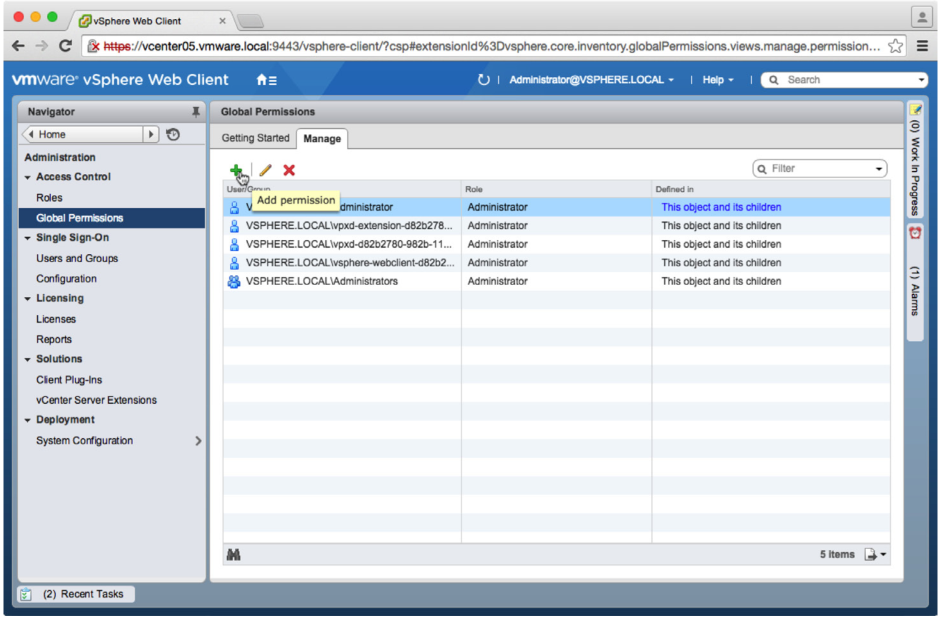
1. Click **Global Permissions** in the left-hand **Navigator** pane.



Asset	Usage	Product	License	License
vcenter05.vmware.local	1 Instances	VMware vCenter Server 6 Standard (Instances)	vCenter Server 6	1/1/17

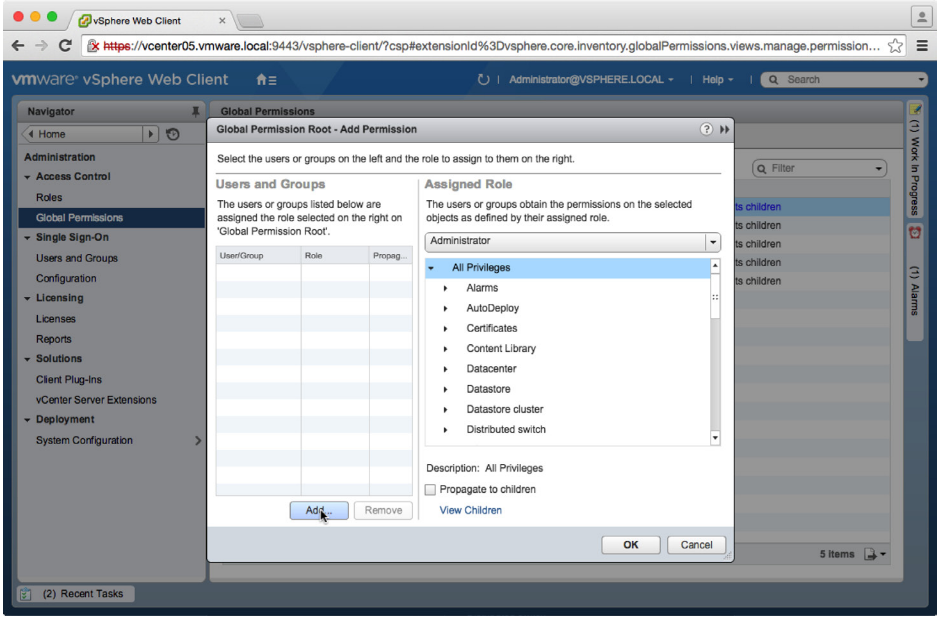
2. Click **Manage**.

3. Click the **green plus** icon to add a permission.



User/Group	Role	Defined in
V dministrator	Administrator	This object and its children
VSPHERE.LOCAL\vpxd-extension-d82b278...	Administrator	This object and its children
VSPHERE.LOCAL\vpxd-d82b2780-982b-11...	Administrator	This object and its children
VSPHERE.LOCAL\vsphere-webclient-d82b2...	Administrator	This object and its children
VSPHERE.LOCAL\Administrators	Administrator	This object and its children

4. Click **Add**.



Global Permission Root - Add Permission

Select the users or groups on the left and the role to assign to them on the right.

Users and Groups

The users or groups listed below are assigned the role selected on the right on 'Global Permission Root'.

User/Group	Role	Propag...

Add... Remove

Assigned Role

The users or groups obtain the permissions on the selected objects as defined by their assigned role.

Administrator

- All Privileges
  - Alarms
  - AutoDeploy
  - Certificates
  - Content Library
  - Datacenter
  - Datastore
  - Datastore cluster
  - Distributed switch

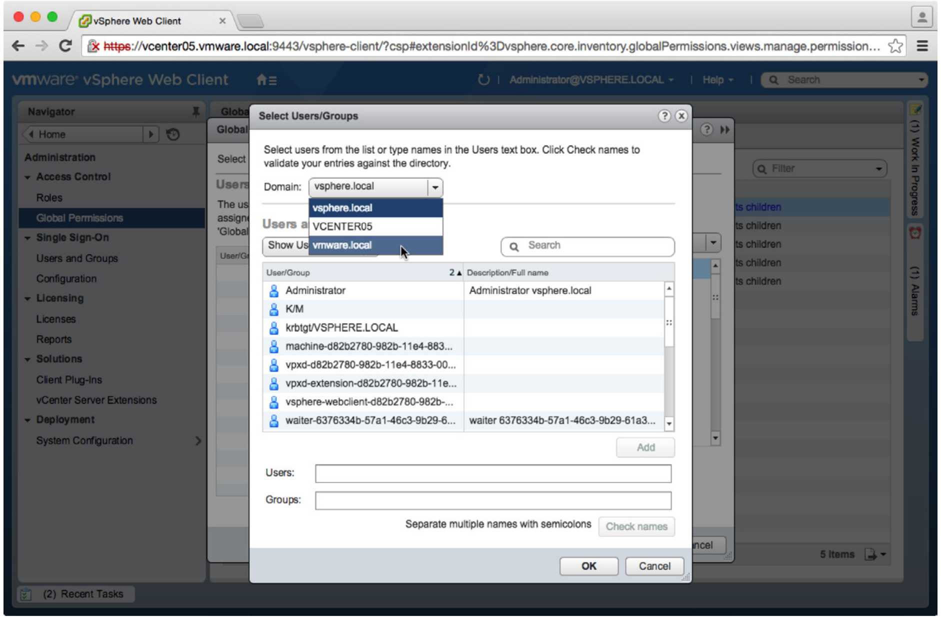
Description: All Privileges

□ Propagate to children

View Children

OK Cancel

5. Select your Active Directory domain or other identity source you added earlier.



https://vcenter05.vmware.local:9443/vsphere-client/?csp#extensionId%3Dvsphere.core.inventory.globalPermissions.views.manage.permission…

Select Users/Groups

Select users from the list or type names in the Users text box. Click Check names to validate your entries against the directory.

Domain: vsphere.local

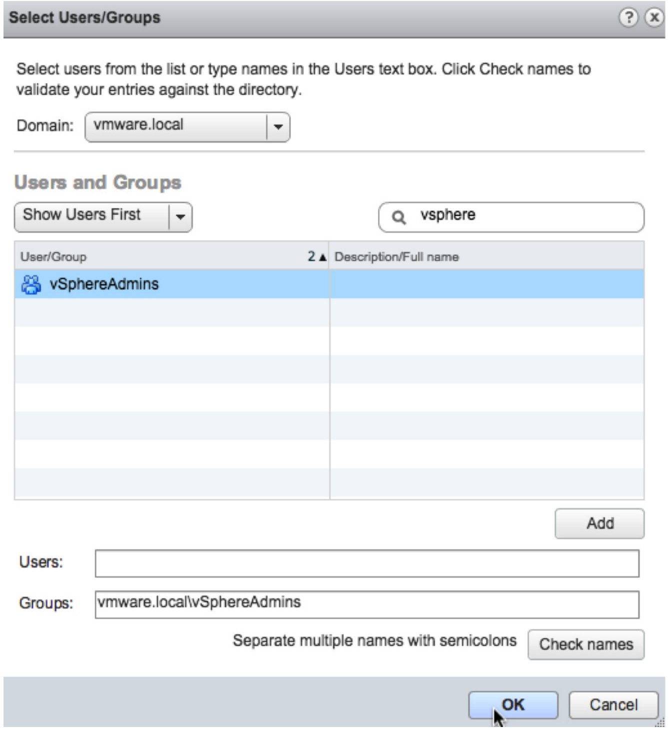
User/Group	Description/Full name
Administrator	Administrator vsphere.local
K/M	
krbtgt/VSPHERE.LOCAL	
machine-d82b2780-982b-11e4-883...	
vpxd-d82b2780-982b-11e4-8833-00...	
vpxd-extension-d82b2780-982b-11e...	
vsphere-webclient-d82b2780-982b-...	
waiter-6376334b-57a1-46c3-9b29-6...	waiter 6376334b-57a1-46c3-9b29-61a3...

Users:

Groups:

Separate multiple names with semicolons

6. Add your vSphere Administrators group or users. Click **OK**.



Select Users/Groups

Select users from the list or type names in the Users text box. Click Check names to validate your entries against the directory.

Domain: vmware.local

Users and Groups

Show Users First

vsphere

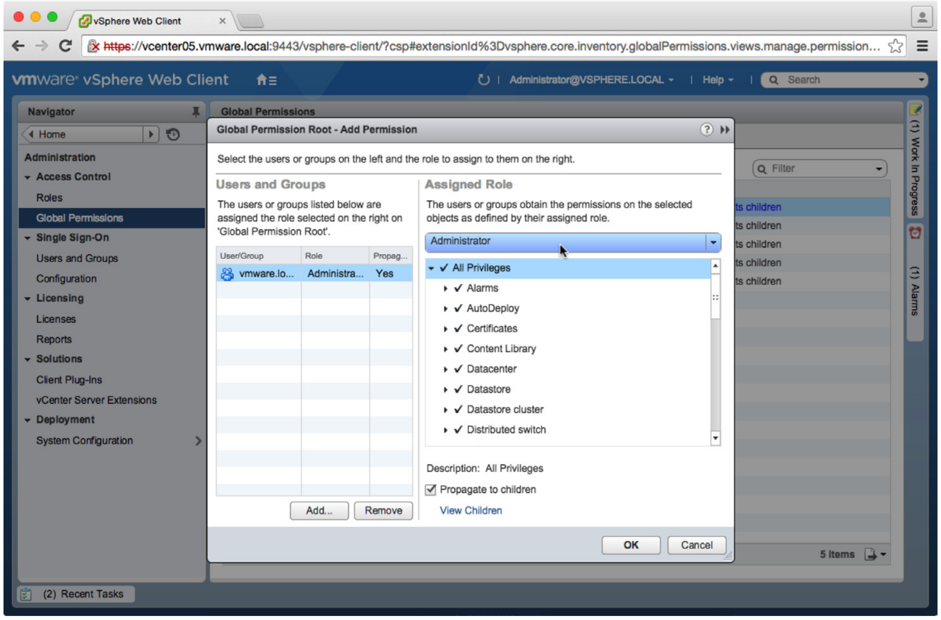
User/Group	Description/Full name
vSphereAdmins	

Users:

Groups: vmware.local\vSphereAdmins

Separate multiple names with semicolons

7. Ensure that the **Administrator** role is selected and **Propagate to children** is checked. Click **OK**.



https://vcenter05.vmware.local:9443/vsphere-client/?csp#extensionId%3Dvsphere.core.inventory.globalPermissions.views.manage.permission...

Global Permission Root - Add Permission

Select the users or groups on the left and the role to assign to them on the right.

Users and Groups

The users or groups listed below are assigned the role selected on the right on 'Global Permission Root'.

User/Group	Role	Propag...
vmware.lo...	Administra...	Yes

Assigned Role

The users or groups obtain the permissions on the selected objects as defined by their assigned role.

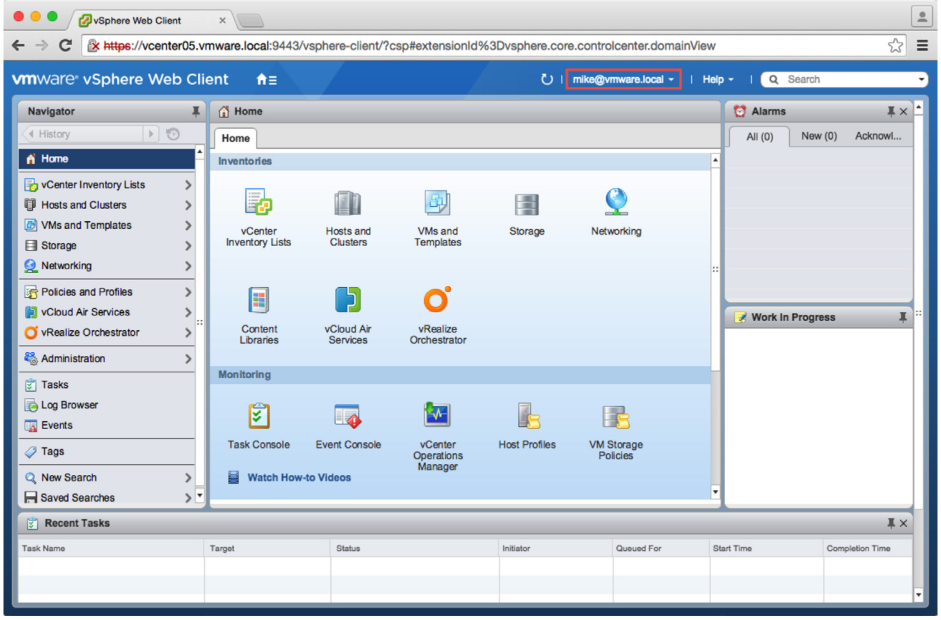
Administrator

- ✓ All Privileges
  - ✓ Alarms
  - ✓ AutoDeploy
  - ✓ Certificates
  - ✓ Content Library
  - ✓ Datacenter
  - ✓ Datastore
  - ✓ Datastore cluster
  - ✓ Distributed switch

Description: All Privileges

☑ Propagate to children

8. You can now log out and back in to vSphere Web Client as an **Administrator** you just added.



https://vcenter05.vmware.local:9443/vsphere-client/?csp#extensionId%3Dvsphere.core.controlcenter.domainView

mike@vmware.local

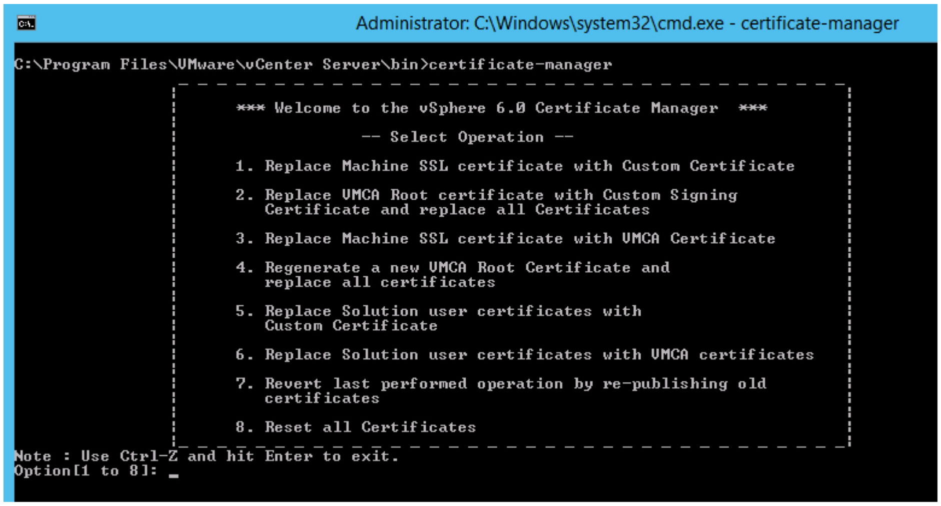
Certificate Management

In most cases, certificate replacement in vSphere 6.0 is not necessary. This is because the Platform Services Controller contains the VMware Certificate Authority (VMCA), which issues certificate authority (CA) signed certificates with a validity period of 10 years.

These certificates are issued to solution users—the users created when a solution such as vCenter Server, vCenter Inventory Service, and so on, is registered with vCenter Single Sign-On—and are utilized as certificate endpoints. These users are issued certificates instead of individual services. This enables the services associated with a solution user to utilize the same certificate, substantially reducing the number of certificates required to manage in the environment.

ESXi hosts are also issued certificates from the VMCA when the hosts are added to the vCenter Server inventory or when vCenter Server is upgraded.

When certificates must be changed—such as when making the VMCA a subordinate of an existing enterprise CA or when generating new solution user certificates after the VMCA mode has changed—the certificate manager utility can be used.


Administrator: C:\Windows\system32\cmd.exe - certificate-manager

```
C:\Program Files\VMware\vCenter Server\bin>certificate-manager
                 _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
                |                                                                   |
                |      *** Welcome to the vSphere 6.0 Certificate Manager  ***      |
                |                                                                   |
                |                   -- Select Operation --                          |
                |                                                                   |
                |      1. Replace Machine SSL certificate with Custom Certificate   |
                |                                                                   |
                |      2. Replace VMCA Root certificate with Custom Signing         |
                |         Certificate and replace all Certificates                  |
                |                                                                   |
                |      3. Replace Machine SSL certificate with VMCA Certificate     |
                |                                                                   |
                |      4. Regenerate a new VMCA Root Certificate and                |
                |         replace all certificates                                  |
                |                                                                   |
                |      5. Replace Solution user certificates with                   |
                |         Custom Certificate                                        |
                |                                                                   |
                |      6. Replace Solution user certificates with VMCA certificates |
                |                                                                   |
                |      7. Revert last performed operation by re-publishing old      |
                |         certificates                                              |
                |                                                                   |
                |      8. Reset all Certificates                                    |
                |_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _|
Note : Use Ctrl-Z and hit Enter to exit.
Option[1 to 8]: _
```

Make the VMCA a Subordinate Certificate Authority

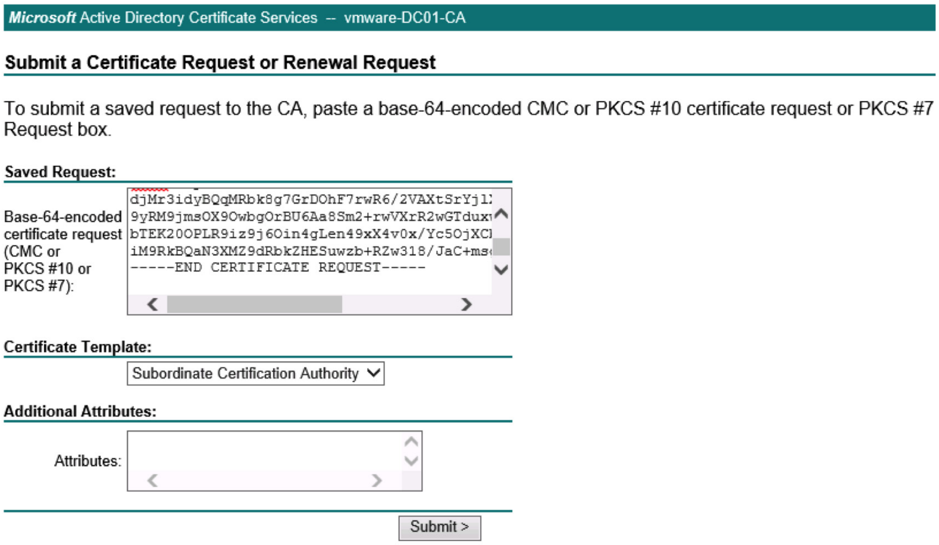
1. Log in to the Platform Services Controller.

2. Using openssl, generate a certificate request.

```
openssl genrsa -out c:\certs\psc001.key 2048
openssl req -new -key c:\certs\psc001.key -out c:\certs\psc001.csr
```

   a. Answer questions to build the request.

   b. Submit the request to a CA. Use the subordinate CA template for the request.



Microsoft Active Directory Certificate Services -- vmware-DC01-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
djMr3idyBQqMRbk8g7GrDOhF7rwR6/2VAXtSrYj1
9yRM9jmsOX9OwbgOrBU6Aa8Sm2+rwVXrR2wGTdux
bTEK20OPLR9iz9j6Oin4gLen49xX4v0x/Yc5OjXC
iM9RkBQaN3XMZ9dRbkZHESuwzb+RZw318/JaC+ms
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Subordinate Certification Authority

Additional Attributes:

Attributes:

c. Download the certificate in Base 64 format; save it to c:\certs.

3. Wait at least 24 hours before continuing. The VMCA requires that the certificate have a valid date of at least 24 hours prior.

4. Run certificate-manager from c:\program files\vmware\vCenter Server\bin for Windows installs or /usr/lib/vmware-vmca/bin/certificate-manager for vCenter Server Appliance.

5. Choose option 2: **Replace VMCA Root certificate with Custom Signing Certificate and replace all Certificates**.

6. Enter the administrator@vsphere.local password.

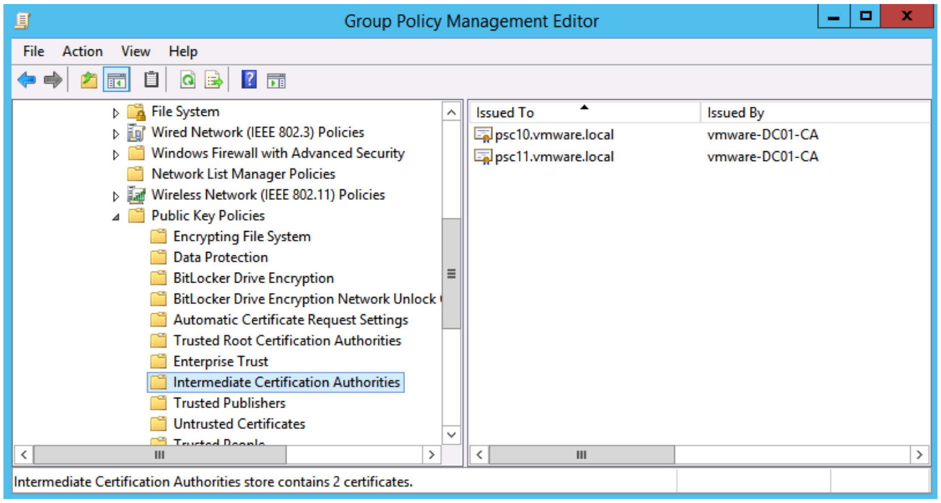
7. Answer all questions as you did earlier when creating the certificate request.

8. When asked to provide a valid custom certificate for root, enter the path to the certificate obtained earlier.

9. When asked to provide a valid custom key for root, enter the path to the .key file generated with openssl earlier.

10. Enter **Y** to continue to replace the certificate.

11. Add the certificate to a Windows Group policy as an intermediate CA. This will enable client machines —such as those using vSphere Web Client—to trust the certificates issued by the VMCA.



Group Policy Management Editor
File
Action
View
Help
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Encrypting File System
Data Protection
BitLocker Drive Encryption
BitLocker Drive Encryption Network Unlock
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Trusted People

Issued To	Issued By
psc10.vmware.local	vmware-DC01-CA
psc11.vmware.local	vmware-DC01-CA

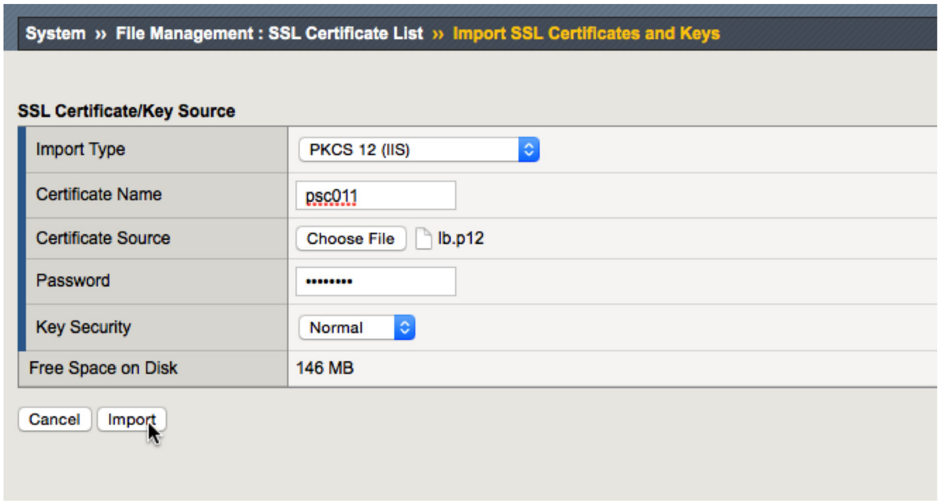
Intermediate Certification Authorities store contains 2 certificates.

Appendix

Configure the F5 BIG-IP Load Balancer

1. Download the lb.p12 file from the ha folder of one of the Platform Services Controllers.
2. Log in to the F5 BIG-IP configuration Web page.
3. Click **System**.
4. Open **File Management**, **SSL Certificate List**.
5. Click **Import**.
6. For **Import Type**, select **PKCS 12**. Provide a descriptive **Certificate Name**. Browse for the **Certificate** downloaded earlier. Enter **changeme** for the **Password**. Click **Import**.

NOTE: If you want to use a custom password when running the gen-lb-cert.py --primary-node command on the first Platform Services Controller to generate the certificates, add the following: --password=yourPassword.

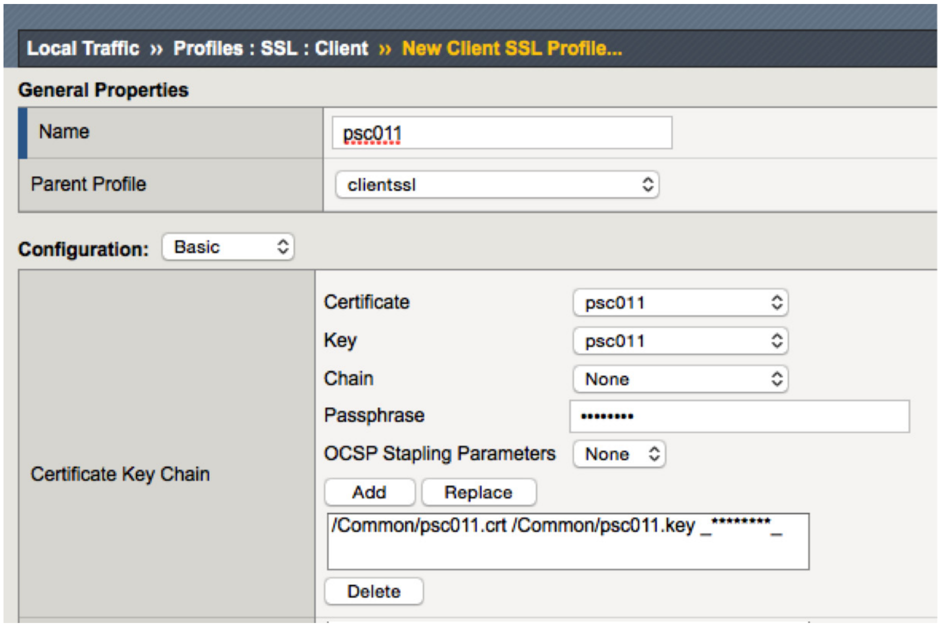


System » File Management : SSL Certificate List » Import SSL Certificates and Keys

SSL Certificate/Key Source

Import Type	PKCS 12 (IIS)
Certificate Name	psc011
Certificate Source	Choose File lb.p12
Password	••••••••
Key Security	Normal
Free Space on Disk	146 MB

7. Click **Local Traffic**.
8. Open **Profiles**, **SSL**, **Client**.
9. Click **Create**.
10. Provide a descriptive **Name**.
    a. Click **Custom**.
    b. Choose the **Certificate** and **Key** installed earlier.
    c. Enter the **Passphrase** for the certificate.
    d. Click **Add**.
    e. Scroll to the bottom and click **Finished**.



Local Traffic » Profiles : SSL : Client » New Client SSL Profile...

General Properties

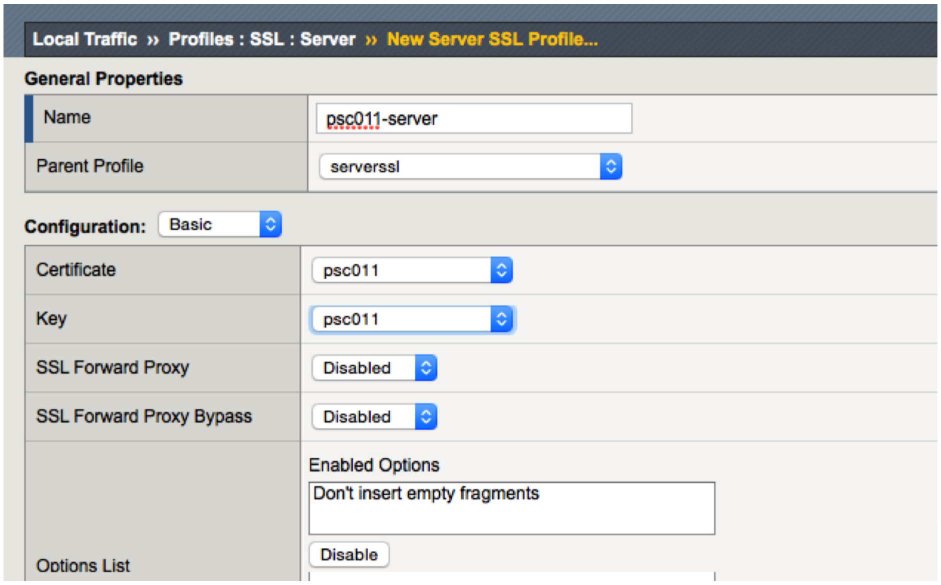
Name	psc011
Parent Profile	clientssl

Configuration: Basic

Certificate Key Chain	Certificate	psc011
	Key	psc011
	Chain	None
	Passphrase	••••••••
	OCSP Stapling Parameters	None

/Common/psc011.crt /Common/psc011.key _********_

11. Open **Profiles**, **SSL**, **Server**.
12. Click **Create**.
13. Provide a descriptive **Name**.
    a. Click **Custom**.
    b. Choose the **Certificate** and **Key** installed earlier.
    c. Click **Add**.
    d. Scroll to the bottom and click **Finished**.



Local Traffic » Profiles : SSL : Server » New Server SSL Profile...

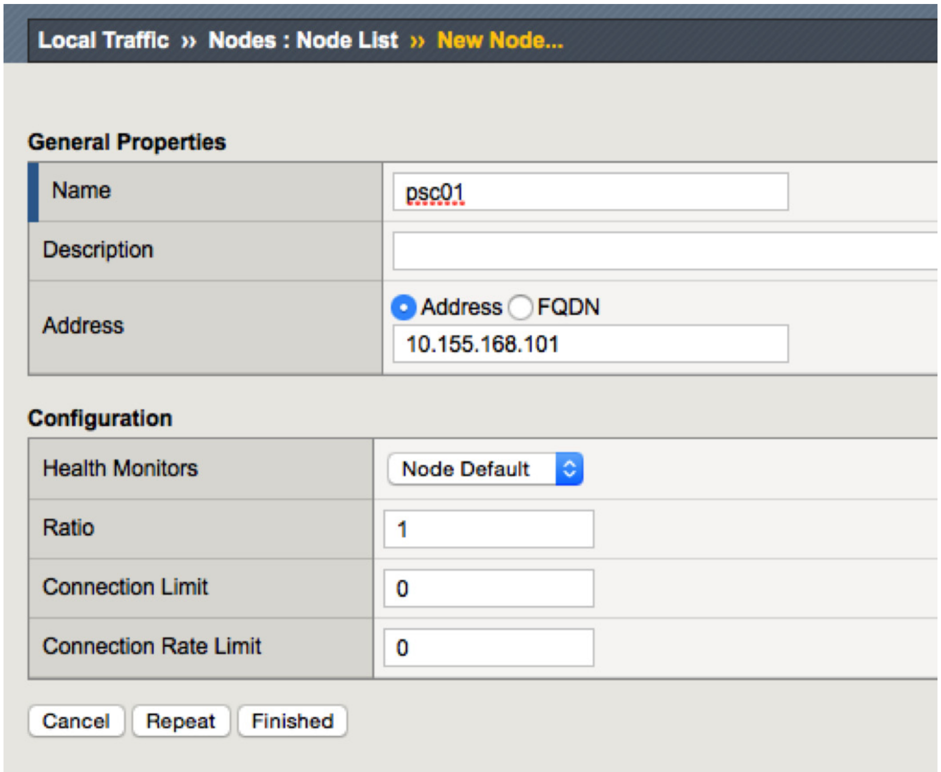
General Properties

Name	psc011-server
Parent Profile	serverssl

Configuration: Basic

Certificate	psc011
Key	psc011
SSL Forward Proxy	Disabled
SSL Forward Proxy Bypass	Disabled
Options List	Enabled Options Don't insert empty fragments

14. Open **Nodes**, **Node List**.
15. Click **Create**.
16. Add all Platform Services Controllers as a node. Use **Repeat** to speed up the process.



Local Traffic » Nodes : Node List » New Node...

General Properties

Name	psc01
Description	
Address	● Address ○ FQDN 10.155.168.101

Configuration

Health Monitors	Node Default
Ratio	1
Connection Limit	0
Connection Rate Limit	0

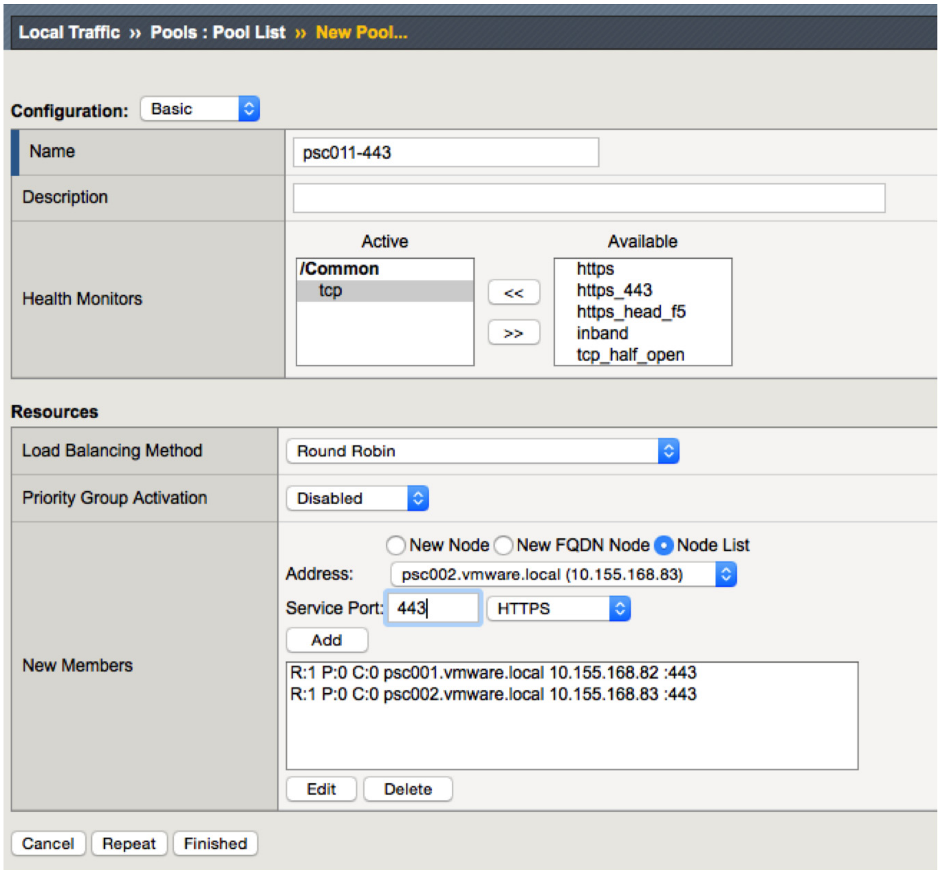
17. Open **Pools**, **Pool List**.

18. Click **Create**.

19. Create six pools, one each for port 443, 2012, 2014, 2020, 389, and 636.

    a. All pools have the same **Configuration**, **tcp** for monitoring, and **Round Robin** for **Load Balancing Method**.

    b. Use **Repeat** to save time: Remove the existing members from the list.



Local Traffic » Pools : Pool List » New Pool...

Configuration: Basic

Name	psc011-443
Description	
Health Monitors	Active: /Common tcp Available: https https_443 https_head_f5 inband tcp_half_open

Resources

Load Balancing Method	Round Robin
Priority Group Activation	Disabled
New Members	○ New Node ○ New FQDN Node ● Node List Address: psc002.vmware.local (10.155.168.83) Service Port: 443 HTTPS R:1 P:0 C:0 psc001.vmware.local 10.155.168.82 :443 R:1 P:0 C:0 psc002.vmware.local 10.155.168.83 :443

20. Open **Virtual Servers**, **Virtual Server List**.

21. Click **Create**.

22. All virtual servers—except the one for port 443—have the same configuration.

    a. Provide a descriptive **Name**.

    b. Enter the **Destination Address**.

    c. For **Service Port**, enter **443**.

    d. For **SSL Profile (Client)**, select the client profile created earlier.

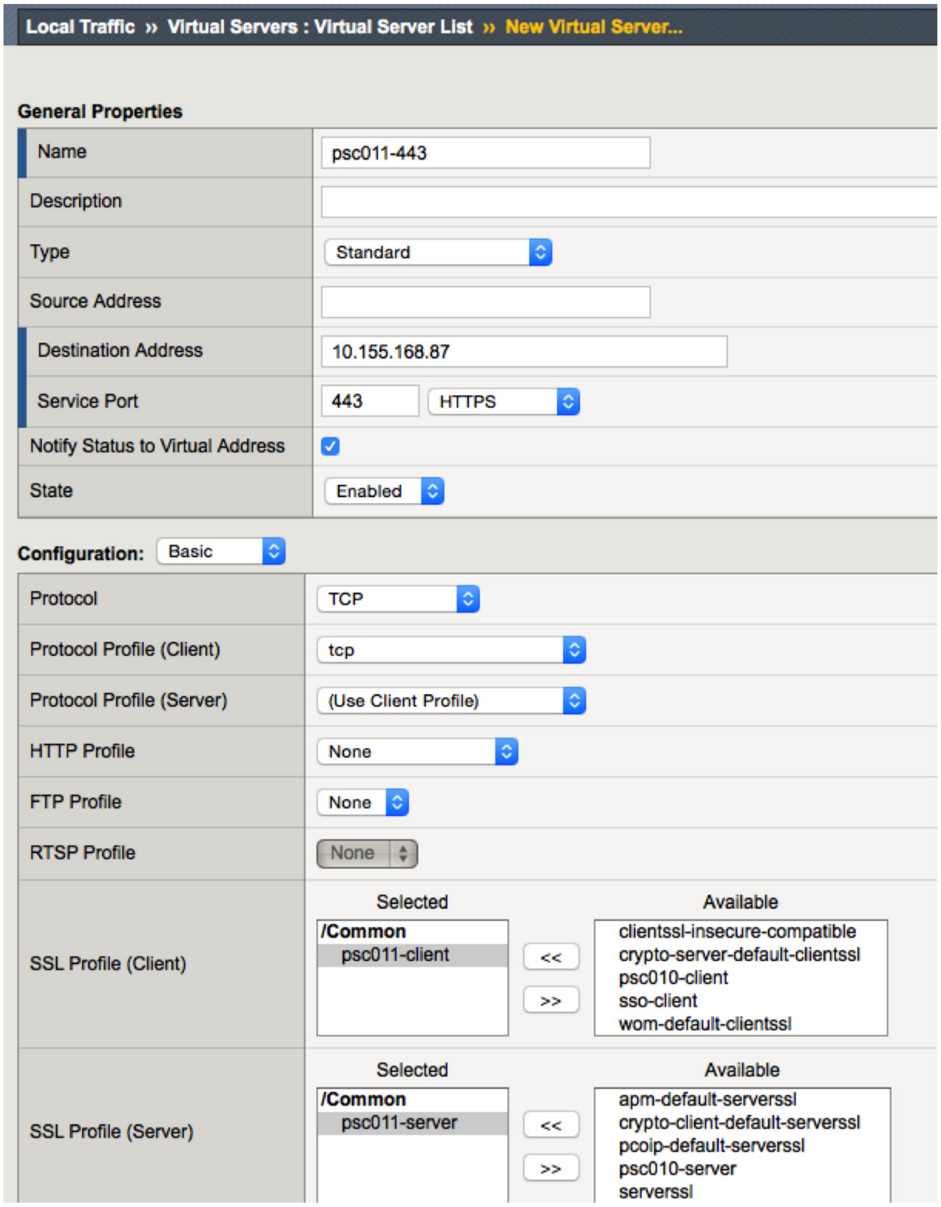
    e. For **SSL Profile (Server)**, select the client profile created earlier.

    f. For **Source Address Translation**, select **Auto Map**.

    g. For the **Default Pool**, select the pool created for port 443.

    h. For the **Default Persistence Profile**, select s**ource_addr**.

    i. Click **Finished**.



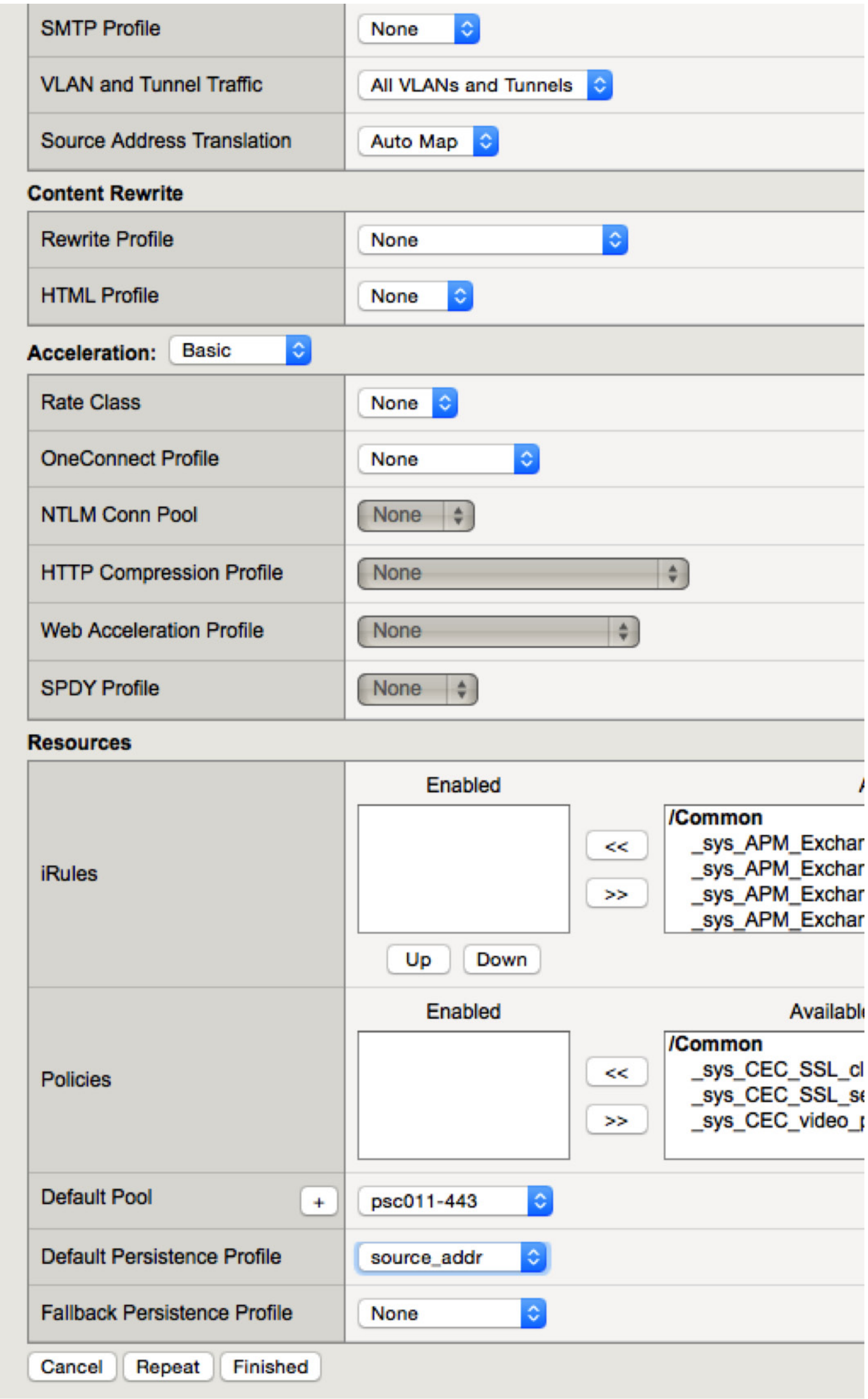
Local Traffic » Virtual Servers : Virtual Server List » New Virtual Server...

General Properties

Name	psc011-443
Description	
Type	Standard
Source Address	
Destination Address	10.155.168.87
Service Port	443 HTTPS
Notify Status to Virtual Address	☑
State	Enabled

Configuration: Basic

Protocol	TCP		
Protocol Profile (Client)	tcp		
Protocol Profile (Server)	(Use Client Profile)		
HTTP Profile	None		
FTP Profile	None		
RTSP Profile	None		
SSL Profile (Client)	Selected /Common psc011-client	<< >>	Available clientssl-insecure-compatible crypto-server-default-clientssl psc010-client sso-client wom-default-clientssl
SSL Profile (Server)	Selected /Common psc011-server	<< >>	Available apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl psc010-server serverssl



SMTP Profile	None
VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	Auto Map

Content Rewrite

Rewrite Profile	None
HTML Profile	None

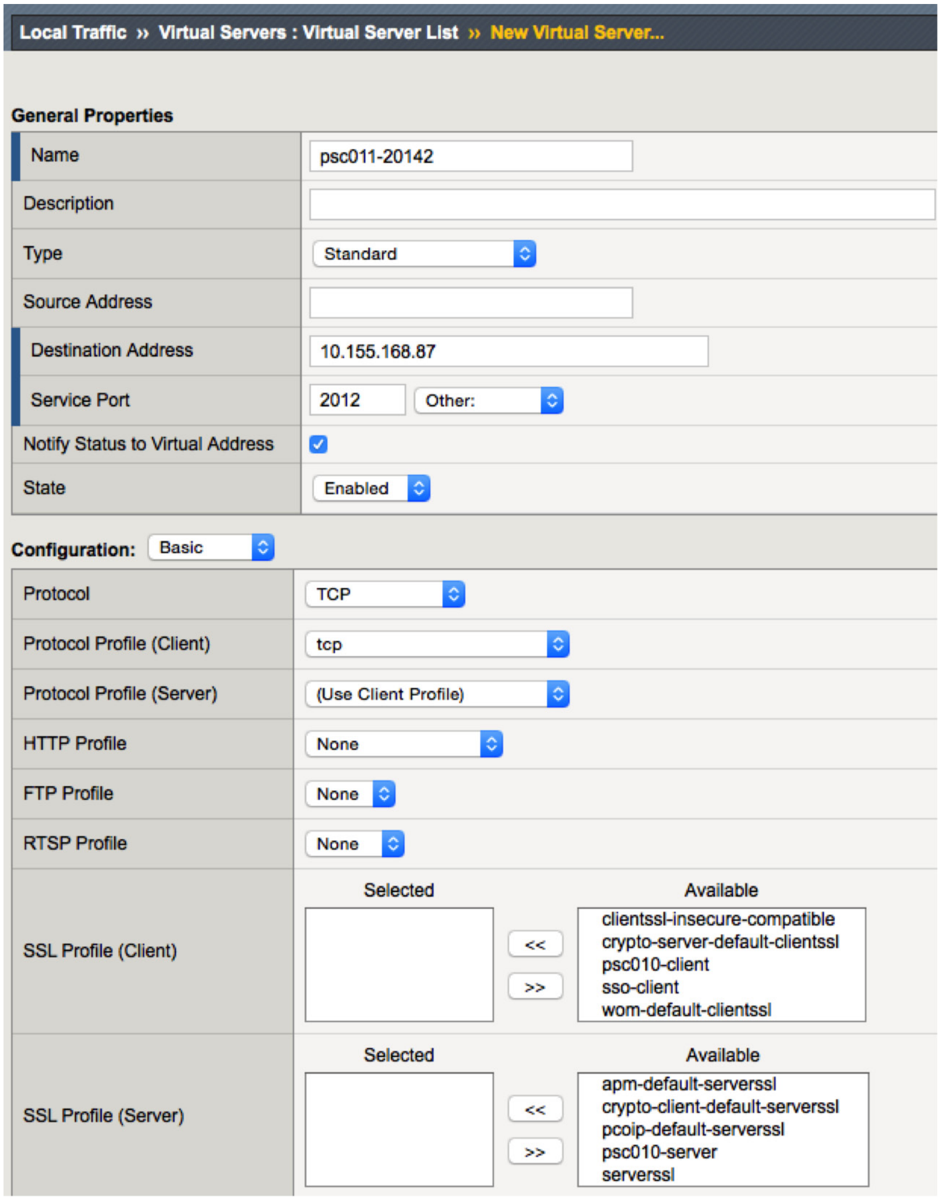
Acceleration: Basic

Rate Class	None
OneConnect Profile	None
NTLM Conn Pool	None
HTTP Compression Profile	None
Web Acceleration Profile	None
SPDY Profile	None

Resources

iRules	Enabled: (empty) Available: /Common _sys_APM_Exchar _sys_APM_Exchar _sys_APM_Exchar _sys_APM_Exchar
Policies	Enabled: (empty) Availabl: /Common _sys_CEC_SSL_cl _sys_CEC_SSL_se _sys_CEC_video_p
Default Pool	psc011-443
Default Persistence Profile	source_addr
Fallback Persistence Profile	None

23. Repeat step 22 for all other ports: 2012, 2014, 2020, 389, and 636. All settings are the same, except there is no **SSL Profile (Client)** or **SSL Profile (Server)** and the **Service Port** and **Default Pool** should match. For example, if the **Service Port** is 2012, the **Default Pool** should be the pool set up for port 2012.



Local Traffic » Virtual Servers : Virtual Server List » New Virtual Server...

General Properties

Name	psc011-20142
Description	
Type	Standard
Source Address	
Destination Address	10.155.168.87
Service Port	2012 Other:
Notify Status to Virtual Address	☑
State	Enabled

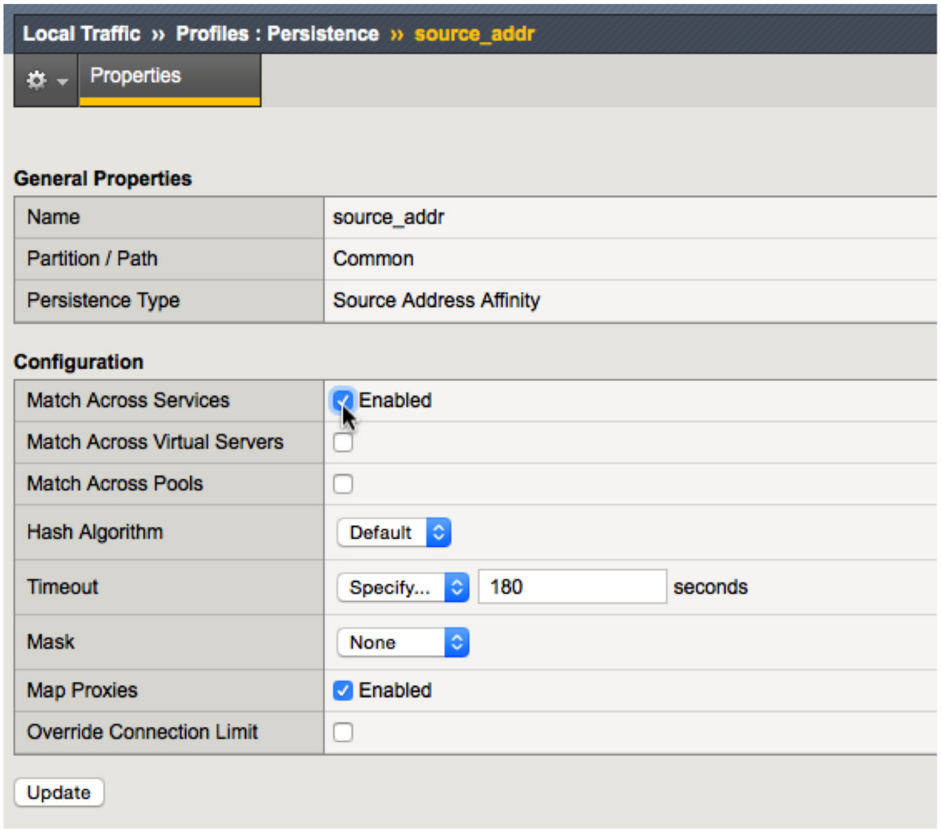
Configuration: Basic

Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	None
FTP Profile	None
RTSP Profile	None
SSL Profile (Client)	Selected: Available: clientssl-insecure-compatible crypto-server-default-clientssl psc010-client sso-client wom-default-clientssl
SSL Profile (Server)	Selected: Available: apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl psc010-server serverssl

24. Open **Profiles**, **Persistence**.

25. Click **source_addr**.

26. Check **Match Across Services** and click **Update**.



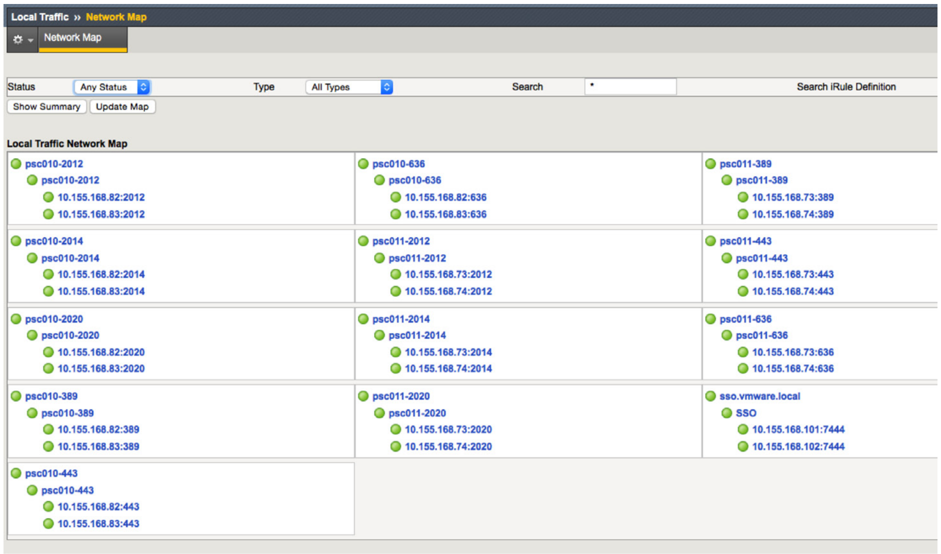
General Properties

Name	source_addr
Partition / Path	Common
Persistence Type	Source Address Affinity

Configuration

Match Across Services	☑ Enabled
Match Across Virtual Servers	□
Match Across Pools	□
Hash Algorithm	Default
Timeout	Specify... 180 seconds
Mask	None
Map Proxies	☑ Enabled
Override Connection Limit	□

27. After both Platform Services Controller nodes have been installed and configured, click **Network Map** and verify that all services are up (green).



Status: Any Status   Type: All Types   Search: *   Search iRule Definition

Local Traffic Network Map

```
● psc010-2012
    ● psc010-2012
        ● 10.155.168.82:2012
        ● 10.155.168.83:2012
● psc010-2014
    ● psc010-2014
        ● 10.155.168.82:2014
        ● 10.155.168.83:2014
● psc010-2020
    ● psc010-2020
        ● 10.155.168.82:2020
        ● 10.155.168.83:2020
● psc010-389
    ● psc010-389
        ● 10.155.168.82:389
        ● 10.155.168.83:389
● psc010-443
    ● psc010-443
        ● 10.155.168.82:443
        ● 10.155.168.83:443
● psc010-636
    ● psc010-636
        ● 10.155.168.82:636
        ● 10.155.168.83:636
● psc011-2012
    ● psc011-2012
        ● 10.155.168.73:2012
        ● 10.155.168.74:2012
● psc011-2014
    ● psc011-2014
        ● 10.155.168.73:2014
        ● 10.155.168.74:2014
● psc011-2020
    ● psc011-2020
        ● 10.155.168.73:2020
        ● 10.155.168.74:2020
● psc011-389
    ● psc011-389
        ● 10.155.168.73:389
        ● 10.155.168.74:389
● psc011-443
    ● psc011-443
        ● 10.155.168.73:443
        ● 10.155.168.74:443
● psc011-636
    ● psc011-636
        ● 10.155.168.73:636
        ● 10.155.168.74:636
● sso.vmware.local
    ● SSO
        ● 10.155.168.101:7444
        ● 10.155.168.102:7444
```

Scripted vCenter Server Installations

vCenter Server Appliance can be deployed via custom JSON files from a command line. The ISO ships with examples for deploying an embedded (vCenter Server and Platform Services Controller), management (vCenter Server), and Platform Services Controller appliance.

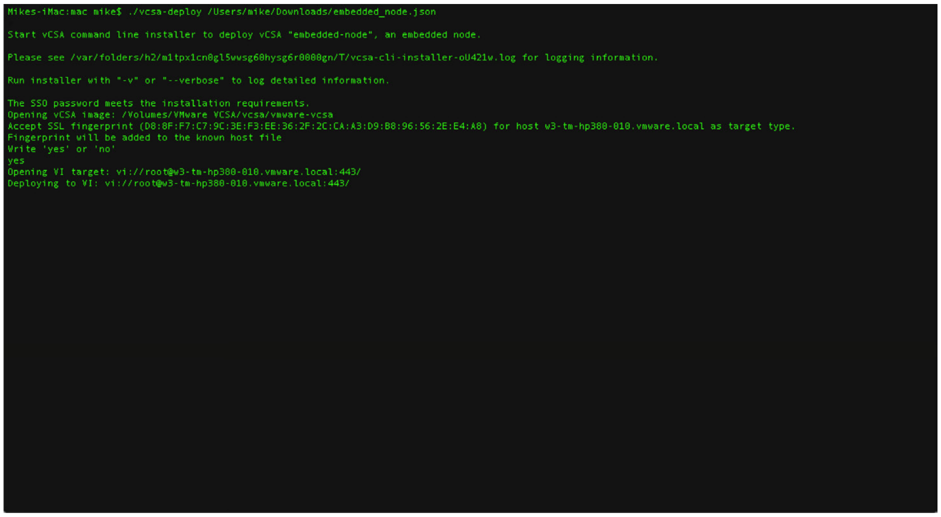
There are command-line utilities for 64-bit Linux, Mac OS X, and Windows.

The following is a sample embedded JSON file:

```
{
  “__comments”:
  [
    “Will deploy an embedded VCSA to host 10 in the MGMT Cluster”
  ],

  “deployment”:
  {
    “esx.hostname”:”w3-tm-hp380-010.vmware.local”,
    “esx.datastore”:”NFSMGMT01”,
    “esx.username”:”root”,
    “esx.password”:”VMware1!”,
    “deployment.option”:”tiny”,
    “deployment.network”:”VM Network”,
    “appliance.name”:”embedded-node”,
    “appliance.thin.disk.mode”:true
  },

  “vcsa”:
  {

    “system”:
    {
      “root.password”:”VMware1!”,
      “ssh.enable”:true
    },

    “sso”:
    {
      “password”:”VMware1!”,
      “domain-name”:”vsphere.local”,
      “site-name”:”PaloAlto”
    }
  }
}
```

To deploy vCenter Server Appliance from this file, save it on your local system. From a command line, navigate to the utilities folder for your OS. For example, on Mac OS X, this is /Volumes/VMware VCSA/vcsa-cli-installer/mac. Now run vcsa-deploy followed by the full path to the custom JSON file. For example:

```
./vcsa-deploy /Users/mike/Downloads/embedded_node.json
```



```
Mikes-iMac:mac mike$ ./vcsa-deploy /Users/mike/Downloads/embedded_node.json

Start vCSA command line installer to deploy vCSA "embedded-node", an embedded node.

Please see /var/folders/h2/m1tpx1cn0gl5wwsg60hysg6r0000gn/T/vcsa-cli-installer-oU421w.log for logging information.

Run installer with "-v" or "--verbose" to log detailed information.

The SSO password meets the installation requirements.
Opening vCSA image: /Volumes/VMware VCSA/vcsa/vmware-vcsa
Accept SSL fingerprint (D8:8F:F7:C7:9C:3E:F3:EE:36:2F:2C:CA:A3:D9:B8:96:56:2E:E4:A8) for host w3-tm-hp380-010.vmware.local as target type.
Fingerprint will be added to the known host file
Write 'yes' or 'no'
yes
Opening VI target: vi://root@w3-tm-hp380-010.vmware.local:443/
Deploying to VI: vi://root@w3-tm-hp380-010.vmware.local:443/
```

References

vSphere 6.0 Documentation Center
http://pubs.vmware.com/vsphere-60

Additional Resources

VMware vSphere 6.0 Feature Walkthroughs
http://featurewalkthrough.vmware.com/#!/vsphere-6-0

VMware Mobile Knowledge Portal
http://www.vmwaremkp.com

About the Author

Mike Brown is a senior technical marketing manager in the Integrated Systems Technical Marketing group. Mike has worked in the IT industry for more than 17 years. His focus is on reference architectures for VMware vCloud Suite® and the software-defined data center (SDDC) as well as VMware vCenter Server, VMware vCenter Single Sign-On, and VMware vSphere Web Client. Mike has multiple industry certifications, including VMware Certified Design Expert (VCDX).

Follow Mike on the vSphere Blog and on Twitter @vMikeBrown.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com