


You can find the most up-to-date technical documentation on the VMware Web site at:

<http://www.vmwarcae.com/support/>

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)



**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2015 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)



You install or upgrade vCenter Server, like any other network server, on a host machine with a fixed IP address and well-known DNS name, so that clients can reliably access the service.

Assign a static IP address and host name to the Windows server that will host the vCenter Server system. This IP address must have a valid (internal) domain name system (DNS) registration. When you install vCenter Server and the Platform Services Controller, you must provide the fully qualified domain name (FQDN) or the static IP of the host machine on which you are performing the install or upgrade. The recommendation is to use the FQDN.

When you deploy the vCenter Server Appliance, you can assign a static IP to the appliance. This way, you ensure that in case of system restart, the IP address of the vCenter Server Appliance remains the same.

Ensure that DNS reverse lookup returns an FQDN when queried with the IP address of the host machine on which vCenter Server is installed. When you install or upgrade vCenter Server, the installation or upgrade of the Web server component that supports the vSphere Web Client fails if the installer cannot look up the fully qualified domain name of the vCenter Server host machine from its IP address. Reverse lookup is implemented using PTR records.

If you use DHCP instead of a static IP address for vCenter Server, make sure that the vCenter Server computer name is updated in the domain name service (DNS). If you can ping the computer name, the name is updated in DNS.

Ensure that the ESXi host management interface has a valid DNS resolution from the vCenter Server and all vSphere Web Client instances. Ensure that the vCenter Server has a valid DNS resolution from all ESXi hosts and all vSphere Web Clients.

## Verify That the FQDN is Resolvable

You install or upgrade vCenter Server, like any other network server, on a virtual machine or physical server with a fixed IP address and well-known DNS name, so that clients can reliably access the service.

If you plan to use a FQDN, for the virtual machine or physical server on which you install or upgrade vCenter Server, you must verify that the FQDN is resolvable.

### Procedure

- ◆ At the Windows command prompt, run the `nslookup` command.

```
nslookup -nosearch -nodefname your_vCenter_Server_FQDN
```

If the FQDN is resolvable, the `nslookup` command returns the IP address and name of the vCenter Server virtual machine or physical server.



Before you can PXE boot an ESXi host with vSphere Auto Deploy, you must install prerequisite software and set up the DHCP and TFTP servers that Auto Deploy interacts with.

## Prerequisites

- Verify that the hosts that you plan to provision with Auto Deploy meet the hardware requirements for ESXi. See [ESXi Hardware Requirements](#).

---

### Note

You cannot provision EFI hosts with Auto Deploy unless you switch the EFI system to BIOS compatibility mode.

---

- Verify that the ESXi hosts have network connectivity to vCenter Server and that all port requirements are met. See [vCenter Server Required Ports](#).
- If you want to use VLANs in your Auto Deploy environment, you must set up the end to end networking properly. When the host is PXE booting, the UNDI driver must be set up to tag the frames with proper VLAN IDs. You must do this set up manually by making the correct changes in the BIOS. You must also correctly configure the ESXi port groups with the correct VLAN IDs. Ask your network administrator how VLAN IDs are used in your environment.
- Verify that you have enough storage for the Auto Deploy repository. The Auto Deploy server uses the repository to store data it needs, including the rules and rule sets you create and the VIBs and image profiles that you specify in your rules.

Best practice is to allocate 2 GB to have enough room for four image profiles and some extra space. Each image profile requires approximately 350 MB. Determine how much space to reserve for the Auto Deploy repository by considering how many image profiles you expect to use.

- Obtain administrative privileges to the DHCP server that manages the network segment you want to boot from. You can use a DHCP server already in your environment, or install a DHCP server. For your Auto Deploy setup, replace the `gpxelinux.0` file name with `undionly.kpxe.vmw-hardwired`.
- Secure your network as you would for any other PXE-based deployment method. Auto Deploy transfers data over SSL to prevent casual interference and snooping. However, the authenticity of the client or the Auto Deploy server is not checked during a PXE boot.

- Set up a remote Syslog server. See the *vCenter Server and Host Management* documentation for Syslog server configuration information. Configure the first host you boot to use the remote Syslog server and apply that host's host profile to all other target hosts. Optionally, install and use the vSphere Syslog Collector, a vCenter Server support tool that provides a unified architecture for system logging and enables network logging and combining of logs from multiple hosts.
- Install ESXi Dump Collector, set up your first host so that all core dumps are directed to ESXi Dump Collector, and apply the host profile from that host to all other hosts. See [Configure ESXi Dump Collector with ESXCLI](#).
- Verify that the Auto Deploy server has an IPv4 address. Auto Deploy does not support a pure IPv6 environment end-to-end. The PXE boot infrastructure does not support IPv6. After the deployment you can manually reconfigure the hosts to use IPv6 and add them to vCenter Server over IPv6. However, when you reboot a stateless host, its IPv6 configuration is lost.

## Procedure

- 1 Install vCenter Server or deploy the vCenter Server Appliance.  
The Auto Deploy server is included with the management node.
- 2 Configure the Auto Deploy service startup type.
  - a Log in to your vCenter Server system by using the vSphere Web Client.
  - b On the vSphere Web Client Home page, click **Administration**.
  - c Under **System Configuration** click **Services**.
  - d Select **Auto Deploy**, click the **Actions** menu, and select **Edit Startup Type**.
    - On Windows, the Auto Deploy service is disabled. In the Edit Startup Type window, select **Manual** or **Automatic** to enable Auto Deploy.
    - On the vCenter Server Appliance, the Auto Deploy service by default is set to **Manual**. If you want the Auto Deploy service to start automatically upon OS startup, select **Automatic**.
- 3 Configure the TFTP server.
  - a In a vSphere Web Client connected to the vCenter Server system, go to the inventory list and select the vCenter Server system.
  - b Click the **Manage** tab, select **Settings**, and click **Auto Deploy**.
  - c Click **Download TFTP Boot Zip** to download the TFTP configuration file and unzip the file to the directory in which your TFTP server stores files.

- 4 Set up your DHCP server to point to the TFTP server on which the TFTP ZIP file is located.
  - a Specify the TFTP Server's IP address in DHCP option 66, frequently called next-server.
  - b Specify the boot file name, which is `undionly.kpxe.vmw-hardwired` in the DHCP option 67, frequently called `boot-filename`.
- 5 Set each host you want to provision with Auto Deploy to network boot or PXE boot, following the manufacturer's instructions.
- 6 Locate the image profile that you want to use and the depot in which it is located.

In most cases, you point to an image profile that VMware makes available in a public depot. If you want to include custom VIBs with the base image, you can use the vSphere ESXi Image Builder to create an image profile and use that image profile.
- 7 Write a rule that assigns an image profile to hosts.
- 8 **(Optional)** If you set up your environment to use Thumbprint mode, you can use your own Certificate Authority (CA) by replacing the OpenSSL certificate `rbd-ca.crt` and the OpenSSL private key `rbd-ca.key` with your own certificate and key file.
  - On Windows, the files are in the SSL subfolder of the Auto Deploy installation directory. For example, on Windows 7 the default is `C:\ProgramData\VMware\VMware vSphere Auto Deploy\ssl`.
  - On the vCenter Server Appliance, the files are in `/etc/vmware-rbd/ssl/`.

By default, vCenter Server 6.0 and later uses vSphere Certificate Authority.

When you start a host that is set up for Auto Deploy, the host contacts the DHCP server and is directed to the Auto Deploy server, which provisions the host with the image profile specified in the active rule set.

## What to do next

- Install vSphere PowerCLI. See [Install vSphere PowerCLI and Prerequisite Software](#).
- Use the vSphere PowerCLI cmdlets to define a rule that assigns an image profile and optional host profile to the host.
- **(Optional)** Configure the first host that you provision as a reference host. Use the storage, networking, and other settings you want for your target hosts to share. Create a host profile for the reference host and write a rule that assigns both the already tested image profile and the host profile to target hosts.
- If you want to have Auto Deploy overwrite existing partitions, set up a reference host to do auto partitioning and apply the host profile of the reference host to other hosts. See [Consider and Implement Your Partitioning Strategy](#).

- If you have to configure host-specific information, set up the host profile of the reference host to prompt for user input. See [Host Customization in the vSphere Web Client](#).