



# What's New in VMware vSphere™ 5.0 Platform

VMware vSphere 5.0

TECHNICAL WHITE PAPER  
V 1/UPDATED MAY 2011

## Table Of Contents

Introduction .....	3
Virtual Machine Enhancements .....	3
Virtual Machine Scalability and Added Device Support .....	3
Compatibility with Older Versions of VMware Tools and Virtual Hardware .....	3
Improved SSD Handling and Optimization .....	4
New Command-Line Interface .....	4
New “esxcli” Command .....	4
Formatted “esxcli” Command Output .....	5
“esxcli” Command Authentication .....	5
Augmenting “esxcli” with Other Commands .....	5
The “localcli” Command .....	5
ESXi Firewall .....	6
VMware ESXi Firewall GUI .....	6
VMware ESXi Firewall CLI .....	7
Third-Party Interface .....	7
Image Builder .....	7
VIB Packaging Format .....	7
Image Builder Depots and Image Profiles .....	8
Image Builder PowerCLI Interface .....	8
Auto Deploy Server .....	9
How Auto Deploy Works .....	9
Auto Deploy Rules Engine .....	9
Benefits of Auto Deploy .....	10
Auto Deploy and Host Profiles .....	11
vCenter Update Manager .....	11
Improved Integration with vSphere Clusters .....	11
Enhanced Update Manager Download Service .....	11
Update Manager UI Improvements .....	11
Support for VMware ESX/ESXi 4.x to VMware ESXi 5.0 Upgrades .....	11
Improved VMware Tools Upgrade .....	11
Conclusion .....	12

## Introduction

VMware vSphere™ 5.0 (“vSphere”) introduces many improvements and new features to extend the benefits and capabilities of vSphere 4.1. These advancements build on the core capacities in vSphere to provide improved scalability; better performance; and easier provisioning, monitoring and troubleshooting. This paper focuses on the following new features and enhancements:

- Virtual machine enhancements
- Improved SSD handling and optimization
- Command-line enhancements
- VMware® ESXi™ firewall
- vSphere Image Builder
- vSphere Auto Deploy server
- vSphere Host Profiles
- VMware vCenter™ Update Manager

## Virtual Machine Enhancements

vSphere 5.0 provides a significant leap forward in the areas of virtual machine scalability and performance. It offers support for significantly larger virtual machines along with added device support and enhanced backward compatibility for virtual machines running older versions of VMware Tools and virtual hardware.

### Virtual Machine Scalability and Added Device Support

In vSphere 5.0 it is now possible to run practically any workload inside a virtual machine. In addition to its providing support for larger virtual machines, each virtual machine now supports additional capabilities and devices not previously available, including the following:

- Up to 32 virtual CPUs (vCPUs) and up to 1TB of RAM
- Enhanced graphics capabilities, including 3D graphics support that enables a richer desktop experience
- Broader device coverage, including support for 3.0 USB devices, smart card readers and EFI BIOS
- New user interface support for configuring multicore vCPUs
- Support for new guest operating systems including Mac OS X Server v10.6 (“Snow Leopard”)

### Compatibility with Older Versions of VMware Tools and Virtual Hardware

Along with the improvements in scalability and added device support, vSphere 5.0 continues to support hosting virtual machines running prior versions of VMware Tools and older virtual hardware versions. With this support it is not necessary to upgrade all your virtual machines in conjunction with your vSphere 5.0 upgrade. You can continue to run virtual machines with the 4.x version of VMware Tools, and virtual hardware versions 4 and 7, in a fully supported configuration. You are required to upgrade the VMware Tools and virtual hardware version only when necessary to take advantage of the new features and capabilities added in vSphere 5.0.

VERSION	VSPHERE 4.X	VSPHERE 5.0
VMware Tools 4.x	Yes	Yes
VMware Tools 5.0	Yes	Yes
VMFS-3	Yes	Yes
VMFS-5	No	Yes
Virtual hardware <sup>1</sup>	3, 4, 7	4, 7, 8

**Table 1.** vSphere 4.x and vSphere 5.0 Compatibility

## Improved SSD Handling and Optimization

vSphere 5.0 provides new forms of SSD handling and optimization. The VMkernel automatically recognizes and tags SSD devices that are local to an ESXi host or are on the network. In addition, the VMkernel scheduler is modified to allow ESXi swap to extend to local or network SSD devices, which enables memory over commitment and minimizes performance impact.

## New Command-Line Interface

vSphere 5.0 introduces a new command-line interface (CLI). A challenge long faced by vSphere administrators has been the need to work with many different command-line tools, each with a unique syntax. In addition, different commands were needed to manage a host locally versus remotely. vSphere 5.0 marks the beginning of efforts by VMware to standardize on a single CLI for both local and remote administration, as well as to help reduce the overall number of CLI tools.

### New “esxcli” Command

The new “esxcli” command provides an intuitive, user-friendly interface that enables real-time discovery of command syntax. While similar in look and feel to its vSphere 4.x predecessor, the new “esxcli” command has an improved syntax and has been extended to include additional functionality not previously available, such as the ability to configure network policies and security policies, manage VIBs, and configure and manage the VMware ESXi firewall.

The “esxcli” command is available on each VMware ESXi host via the VMware ESXi shell. It is also available as part of the optional vCLI package that can be installed on any supported Windows or Linux server, or through the vSphere Management Assistant (vMA).

#### esxcli Command Structure



Example Commands:

```
# esxcli--server 192.168.1.25 storage filesystem list
# esxcli--server 192.168.1.20 --vihost esx01 network ip interface list
```

**Figure 1.** “esxcli” Command

1. VMware ESXi 5.0 supports upgrading virtual hardware version 3 and later

## Formatted “esxcli” Command Output

In addition to providing a consistent look and feel for both local and remote CLI administration, the new “esxcli” command provides the ability to format the command output. Using the “--formatter” option, administrators can choose to have the command output formatted as XML, a key-value pair or a list of comma-separated values. The “esxcli” formatter enhances your ability to parse command output, helping to simplify scripting and improve report generation.

### esxcli Formatter Option

```
# esxcli--formatter=csv --format-param=fields="Name,Mac Address,Enabled"
network ip interface list

Name,MACAddress,Enabled
vmk0,00:1a:64:d0:bf:00,true,
vmk1,00:50:56:71:38:bc,true,
vmk2,00:50:56:79:70:28,true,
vmk3,00:50:56:71:d0:fe,true,
```

Figure 2. “esxcli” Formatter Option

## “esxcli” Command Authentication

Each time you run an “esxcli” command, you must be authenticated. Users can choose to authenticate against an individual VMware ESX® host or a vCenter Server. vSphere 5.0 provides the following options for managing user authentication:

- If you are logged on locally using the VMware ESXi shell, “esxcli” will use the credentials of the logged-in user.
- If you are running commands remotely, you can specify the credentials as part of the command.
- You can save the user’s credentials into a “session file” and provide the name of the session file as a command-line parameter.
- If running commands remotely from a Windows server, you can configure the Windows “—PassThroughAuth.”
- If using the vMA, you can use the “fast pass” authentication.

When working remotely if no authentication credentials are provided with the “esxcli” command, you will be prompted to provide a username and password.

## Augmenting “esxcli” with Other Commands

In vSphere 5.0, the new “esxcli” command replaces the deprecated “esxcfg-” style commands. However, it doesn’t yet provide a comprehensive set of command-line capabilities. The “esxcli” command will continue to be enhanced in future releases and will eventually replace the non-“esxcli” commands. Until that time, you will continue to augment the “esxcli” command with the “vicfg-” commands and other familiar CLI tools such as “vmware-cmd” and “vmkfstools” to troubleshoot and administer your VMware ESXi hosts. Of course, you can also continue to use the vSphere PowerCLI.

## The “localcli” Command

In addition to the new “esxcli” command, a new “localcli” command has been added in vSphere 5.0. The “localcli” command is largely equivalent to the “esxcli” command, with the notable exception that it bypasses the local “hostd” process on the server. The “localcli” command is intended for situations where the VMware ESXi host’s “hostd” daemon becomes unresponsive. It is recommended that you do not use the “localcli” command outside of the direction of VMware global services because it can result in host instability.

## ESXi Firewall

vSphere 5.0 now provides a new firewall that protects the management interface of a host running ESXi. This firewall provides similar access control capabilities for the VMware ESXi platform to those available on the VMware ESX platform. However, the technology used to build this firewall is different from the iptables running on a console operating system (OS) in the VMware ESX environment.

In VMware ESXi, the access control capability is provided through a vmknix (VMkernel network adaptor)-level firewall module. This module sits between a vmknix and a virtual switch. It inspects packets against firewall rules. Based on the results, it determines whether to drop or pass packets. The following are key features of the new firewall:

- It is a service-oriented and stateless firewall.
- It supports additional capability to restrict access to services based on IP address and subnet mask.
- The configuration GUI is similar to the VMware ESX firewall.
- The firewall can be configured using the new “esxcli” command-line interface.
- Host Profiles support is provided for this firewall.

The VMware ESXi firewall provides security to the management interface and helps manage firewall rules through a familiar, service-oriented GUI. This familiar GUI and the capability to preserve firewall settings help administrators tremendously during the transition from the VMware ESX to the VMware ESXi platform.

In the following section, higher-level details on firewall GUI, CLI and third-party interface are provided to help administrators understand the firewall rule management and configuration process.

### VMware ESXi Firewall GUI

Similar to the VMware ESX firewall, the VMware ESXi firewall can be managed from the vSphere client's host and cluster view. After selecting the host and choosing the configuration tab, the VI administrator can check different services and firewall settings under the security profile.

Figure 3 shows the screenshot of the security profile of a host, with details on available services and firewall rules. Administrators can start or stop any of these services and also provide access to these services through the firewall parameters.

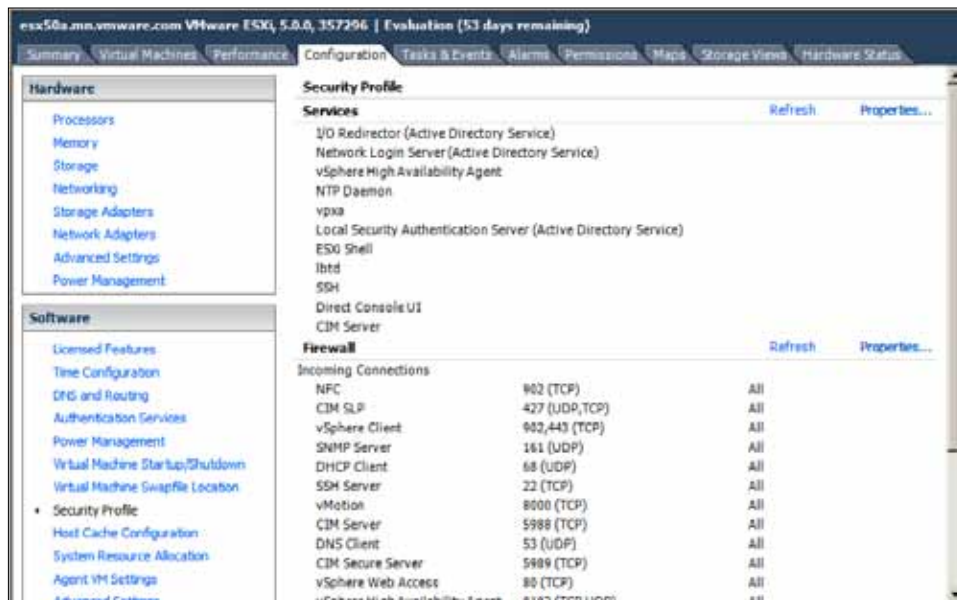
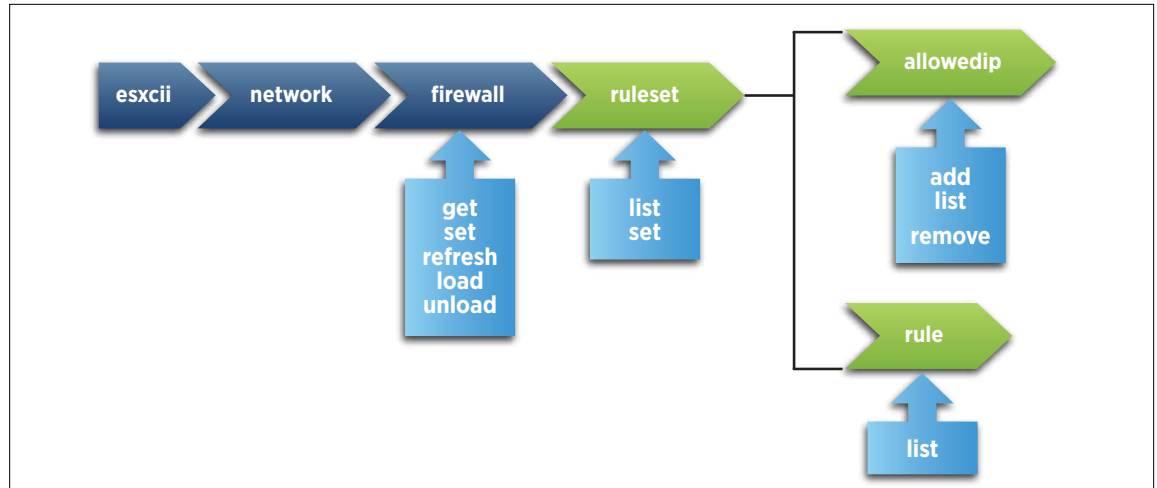


Figure 3. Security Profile Screenshot

## VMware ESXi Firewall CLI

For firewall configuration commands, a separate firewall namespace is provided, as shown in Figure 4.



**Figure 4.** “esxcli” Firewall Command Structure

The “get” command (*esxcli network firewall get*) can be used to collect the information about the current firewall settings. The “set” command (*esxcli network firewall set*) enables users to configure firewall rules. Administrators can use this simple and intuitive command interface option to manage firewall rules.

## Third-Party Interface

Administrators who want to define new firewall services can do so through xml description files. Once an xml file with a new service and firewall rule is created under `/etc/vmware/firewall` folder, administrators can run the “esxcli” refresh command to load this new service and firewall configuration. This gives security and VI administrators the ability to create new services and related firewall rules at run time.

## Image Builder

vSphere 5.0 introduces the VMware ESXi Image Builder. The Image Builder is a PowerShell CLI command set that enables customers to customize their VMware ESXi images. With Image Builder, you can create VMware ESXi installation images with a customized set of updates, patches and drivers.

## VIB Packaging Format

The VMware ESXi installation image comprises a series of separately packaged software components referred to as VMware Installation Bundles (VIBs). When a VMware ESXi host is installed, the installer formats the boot device and extracts the VIBs off the installation media onto the boot device (or directly into memory with Auto Deploy). Once the VIBs have been extracted, the host boots and the hypervisor is loaded. A challenge with prior releases of VMware ESXi arose anytime an administrator needed to add or modify one of the VIB components—to add new device drivers for a new network adaptor, for example. vSphere 5.0 addresses this gap by providing users with the Image Builder to customize their VMware ESXi installation images.

## Image Builder Depots and Image Profiles

Using the Image Builder, customers place the VMware ESXi VIBs into software depots. The administrator then uses the Image Builder PowerCLI to combine the VIBs from the separate depots with the default VMware ESXi installation image, to create a custom image profile that can then be used to install their VMware ESXi hosts.

Multiple depots and image profiles can be maintained. For example, a separate image profile can be created for installing VMware ESXi on rackmounted servers while another image profile is used for installing VMware ESXi on blade servers.

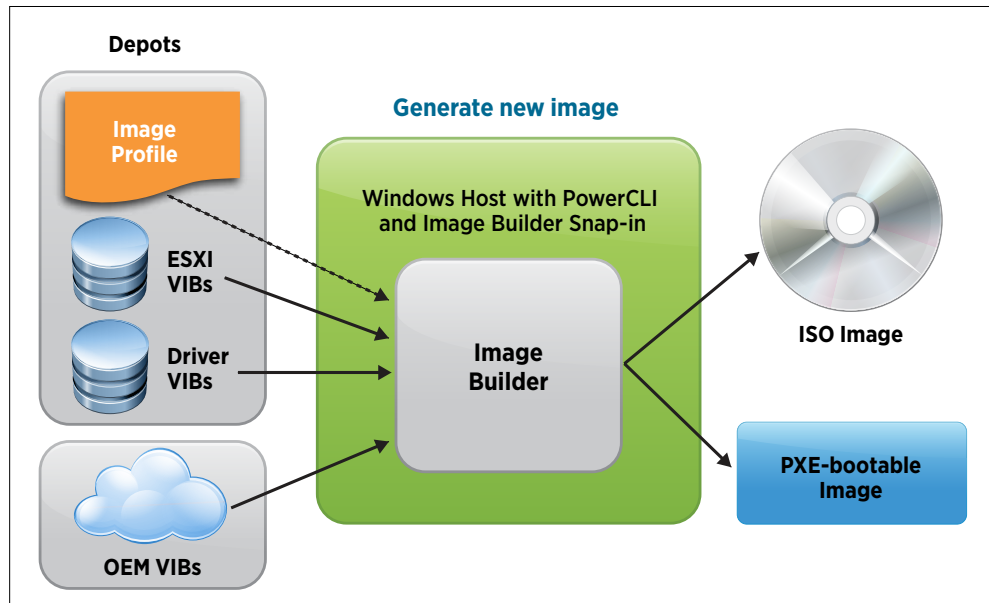


Figure 5. Image Builder

## Image Builder PowerCLI Interface

Image Builder uses a PowerCLI interface to define and manage the depots and create the image profiles. In addition to identifying the VIBs that make up your image profile, Image Builder also enables you to define relationships between the various VIB components, helping you ensure that dependencies are met and components are installed in the desired order.

The Image Builder PowerCLI snap-in is included with PowerCLI.

### Auto Deploy PowerCLI Commands

```
PowerCLI C:\> Connect-VIServer 192.168.1.20

PowerCLI C:\> Get-EsxImageProfile MyProfile | format -list

PowerCLI C:\> Add-EsxSoftwarePackage --ImageProfile MyProfile --SoftwarePackage
new-package

PowerCLI C:\> Export-EsxImageProfile --ImageProfile MyProfile --ExportToBundle
--FilePath "C:\ESXiImages"
```

Figure 6. Image Builder PowerCLI Commands



## Auto Deploy Server

The vSphere Auto Deploy server simplifies the deployment of VMware ESXi hosts in your environment. Using the Auto Deploy server, you can provision hundreds of physical hosts with VMware ESXi software. You can specify the image to deploy and the host to provision with the image. Optionally, you can specify Host Profiles to apply to the host, and a location for each host.

### How Auto Deploy Works

When a physical host setup for Auto Deploy is turned on, Auto Deploy uses a PXE boot infrastructure in conjunction with vSphere Host Profiles to provision and customize that host. No state is stored on the host itself. Instead, the Auto Deploy server manages state information for each host.

When a physical host is booted, it PXE boots over the network where a DHCP server assigns an IP address and redirects the host to a TFTP server, which directs the host to perform an HTTP boot from the Auto Deploy server. The Auto Deploy server then streams the VMware ESXi software image into memory on the target host. Once the entire image is resident in memory, VMware ESXi boots up and contacts the VMware vCenter Server, where Host Profiles can be used to automatically configure the host. Once the host has been configured, it is placed into the proper VMware vCenter cluster or folder and is available to host virtual machines.

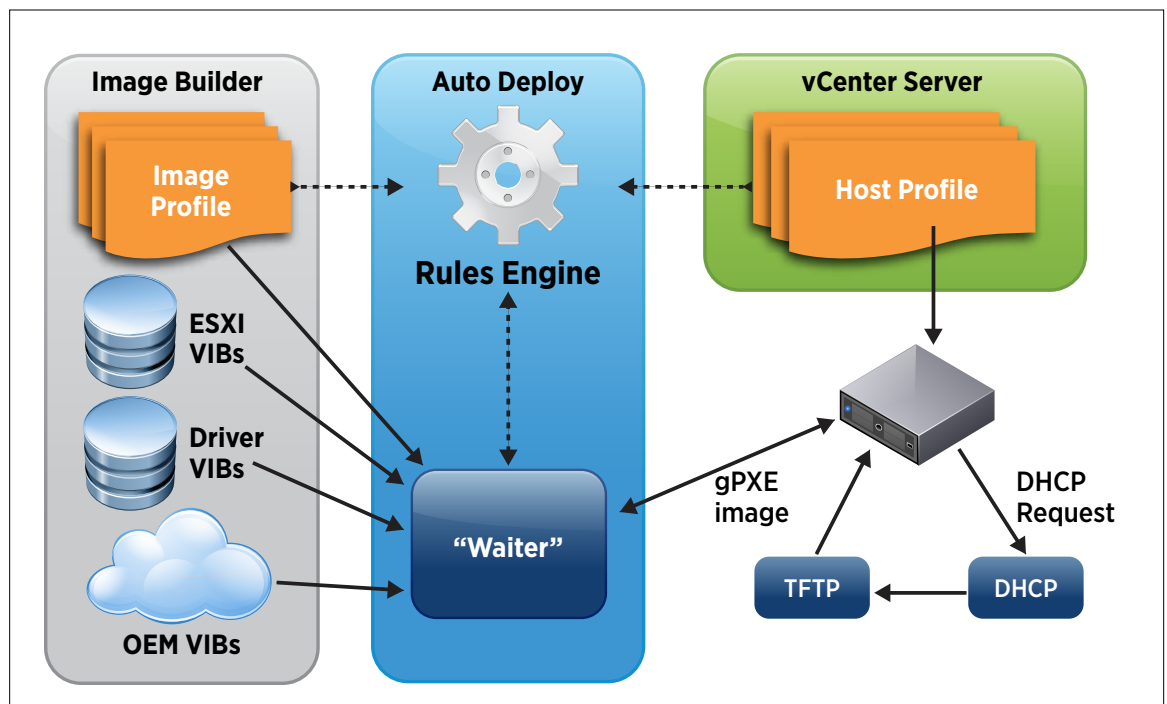


Figure 7. Auto Deploy Architecture

### Auto Deploy Rules Engine

The Auto Deploy server uses a rules engine to identify which image and which Host Profile to deliver to which host. Administrators use the Auto Deploy PowerCLI to define the rules that assign image profiles and Host Profiles to the hosts.

**Auto Deploy PowerCLI Commands**

```
PowerCLI C:\> Connect-VIServer 192.168.1.20

PowerCLI C:\> Add-EsxSoftwareDepot C:\ESXiImages\ESXi-Image1.zip

PowerCLI C:\> New-DeployRule --Name "Host-Group1" --Item "Image1-Profile" --Pattern
"ipv4 192.168.1.30 - 192.168.1.50"

PowerCLI C:\> Add-DeployRule Host-Group1
```

**Figure 8.** Auto Deploy PowerCLI Commands

As part of the HTTP boot request, the VMware ESXi host provides the Auto Deploy server with information about the server, including the type of hardware (make/model) and its TCP/IP configuration. The Auto Deploy server rules engine compares this information against the predefined rules to identify the proper image and Host Profiles for the host.

With Auto Deploy, you can maintain multiple rule sets to account for many different types of server hardware in your environment. Each time the server boots, the rules engine will ensure that the proper image is deployed, based on the hardware characteristics of the server.

## Benefits of Auto Deploy

The Auto Deploy server provides many benefits:

Decouples the VMware ESXi host from the physical server and eliminates the boot disk	Because the host image is loaded over the network directly into host memory, there is no longer a need for a dedicated boot device for each host. In an environment with hundreds of hosts, this can result in a significant savings in terms of disk space as well as improve system reliability through the elimination of rotating media.
Makes it easy to (re)deploy large numbers of VMware ESXi hosts	Auto Deploy provides for a flexible deployment framework that can be used to install small as well as large numbers of hosts.
Facilitates VMware ESXi host recovery	Because the VMware ESXi host image is decoupled from the physical server, it also simplifies recovery of VMware ESXi hosts. If you have a hardware failure, simply boot the host image from a new server.
Eliminates configuration drift	Auto Deploy works directly with both the Image Builder and Host Profiles when deploying and configuring VMware ESXi hosts. Every host reboot is like a fresh install.
Simplifies patching and updating	With Auto Deploy, patching is as simple as updating the Host Profile image using Image Builder and rebooting your VMware ESXi host.

### Auto Deploy and Host Profiles

The Auto Deploy server uses Host Profiles to configure the VMware ESXi hosts after they have been installed and booted. To accommodate configuring VMware ESXi hosts deployed with Auto Deploy, several significant improvements have been made to Host Profiles in vSphere 5.0. Most notably, Host Profiles have been extended to include additional configuration settings not in earlier versions, such as support for iSCSI, FCoE, storage multipathing, individual device settings and kernel module settings. In addition, for host-specific configuration attributes Host Profiles now enables creating a per-host answer file. The answer file is used to store host-specific attributes that are not shared with other hosts. This facilitates the automated deployment of hosts using Auto Deploy, because the host-specific settings can be applied using the answer file, and the remaining shared configuration can then be applied using the Host Profile.

## vCenter Update Manager

The vCenter Update Manager has been further optimized in vSphere 5.0.

### Improved Integration with vSphere Clusters

The new Update Manager includes improved integration with vSphere clusters. Update Manager now monitors the cluster's available capacity and uses the information on spare capacity, to optimize the number of hosts that can be patched simultaneously. This enables more optimal patching of clusters, with no risk of virtual machine downtime. In the case where maintenance windows are limited and virtual machine downtime is not critical, Update Manager is now able to patch an entire cluster in unison, enabling rapid and simultaneous patching of all hosts in a cluster.

### Enhanced Update Manager Download Service

Update Manager 5.0 also provides more flexibility in configuring the Update Manager Download Service (UMDS). Users can now define multiple URLs from which the host can download updates. In addition, administrators can now filter the updates that get downloaded to include only those patches/updates that are applicable to their environment.

### Update Manager UI Improvements

The Update Manager Utility has also been improved to make it easier to update and manage the Update Manager configuration itself. With the new Update Manager Utility, users can now change the Update Manager database password and configure proxy authentication, as well as manage SSL certificates.

### Support for VMware ESX/ESXi 4.x to VMware ESXi 5.0 Upgrades

Update Manager 5.0 also provides support for upgrading VMware ESX/ESXi 4.x hosts to VMware ESXi 5.0. Administrators can use Update Manager to expedite the migration of existing VMware ESX/ESXi 4.x hosts to VMware ESXi 5.0, including migrating third-party components such as Cisco Nexus 1000V and EMC PowerPath.

### Improved VMware Tools Upgrade

In addition to facilitating the upgrade of VMware ESX/ESXi hosts, Update Manager also facilitates the updating of VMware Tools running inside virtual machines by allowing the update to be scheduled in advance and performed at a convenient time without requiring the administrator to be present for the update.

# Conclusion

vSphere 5.0 continues to build on the rich set of capabilities provided in vSphere 4.1. vSphere 5.0 supports virtual machines with up to 32 vCPUs and 1TB of RAM, making it possible to virtualize even the biggest workloads. Along with the impressive virtual machine size, vSphere 5.0 further extends the features and capabilities of the virtual machine to include support for 3D graphics, USB 3.0 devices, and smart card readers. vSphere 5.0 provides a new and improved command-line interface that for the first time provides a consistent command structure for both local and remote management of VMware ESXi hosts. The new services-based firewall improves the security of the VMware ESXi host and offers an improved user experience. The new Image Builder puts an end to the challenge of customizing VMware ESXi installation images by providing a PowerCLI snap-in, enabling administrators to create and maintain customized installation images. The Auto Deploy server streamlines the deployment and configuration of large numbers of VMware ESXi hosts by leveraging the PXE-based network boot infrastructure to deploy VMware ESXi on the fly. To support Auto Deploy, vCenter Host Profiles have been updated to include additional configuration parameters such as iSCSI, FCoE, multipathing and kernel-level settings. In addition, Host Profiles now includes support for per-host answer files that can be used together with Auto Deploy to apply host-specific settings. Finally, the new vSphere 5.0 Update Manager also includes many improvements and enhancements to greatly improve your ability to upgrade, patch and maintain your hosts as well as upgrade the virtual machine hardware and the VMware Tools running inside your virtual machines.

