VMware® Host Profiles: Technical Overview

TECHNICAL WHITE PAPER

vmware®

Table of Contents

Introduction

VMware® vSphere™ 4.1 ("vSphere") is the industry's first cloud operating system, transforming datacenters into dramatically simplified environments to enable the next generation of flexible, reliable IT services. vSphere 4.1 delivers new large-scale management features, such as VMware Host Profiles (Host Profiles), that enable efficient operational control and significantly reduce operating costs.

Host Profiles (available through VMware vCenter™ Server) enables you to establish standard configurations for VMware ESX®/ESXi™ hosts and to automate compliance to these configurations, simplifying operational management of large-scale environments and reducing errors caused by misconfigurations. This paper provides a technical overview of Host Profiles and describes how you can use them to automate host configuration and to monitor for configuration compliance.

Host Configuration Management

At the core of VMware vSphere, VMware ESX and VMware ESXi provide the foundation for delivering virtualization-based distributed services to IT environments. VMware ESX/ESXi provides a robust, production-proven virtualization layer that abstracts server hardware resources and allows their sharing by multiple virtual machines.

There are several methods for configuring a VMware ESX/ESXi host today, including:

- Using the vSphere Client, which provides a Windows-based graphical user interface for host configuration
- Using the remote command line interfaces, for command-line–based and scripted configuration

As virtual infrastructures grow, it can become increasingly difficult and time consuming to configure multiple hosts in similar ways. Existing per-host processes typically involve repetitive and error-prone configuration steps. As a result, maintaining configuration consistency and correctness across the datacenter requires increasing amounts of time and expertise, leading to increased operational costs.

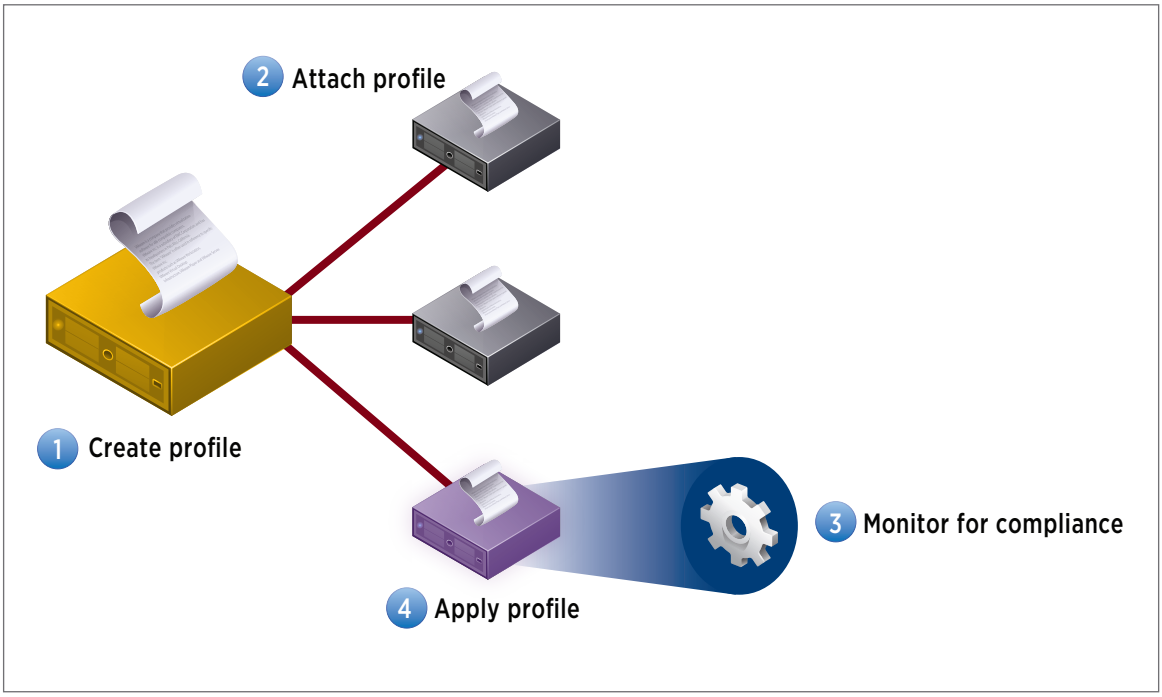
Host Profiles eliminates per-host, manual or UI-based host configuration and maintains configuration consistency and correctness across the datacenter by using Host Profiles policies. These policies capture the blueprint of a known, validated reference host configuration, including the networking, storage, security and other settings. You can then use this profile to:

- Automate host configuration across a large number of hosts and clusters. You can use Host Profiles to simplify the host provisioning process, configure multiple hosts in a similar way, and reduce the time spent on configuring and deploying new VMware ESX/ESXi hosts.
- Monitor for host configuration errors and deviations. You can use Host Profiles to monitor for host configuration changes, detect errors in host configuration, and ensure that the hosts are brought back into a compliant state.

With Host Profiles, the time required to set up, change, audit and troubleshoot configurations drops dramatically due to centralized configuration and compliance checking. Not only does it reduce labor costs, but it also minimizes risk of downtime for applications/virtual machines provisioned to misconfigured systems.

How Does VMware Host Profiles Work?

Host Profiles greatly simplifies the operational management of large deployments by automating host configuration and ensuring compliance.



Host Profiles automates host configuration and ensures compliance in four steps:

1. **Step 1: Create a profile, using the designated reference host.**

   To create a host profile, VMware vCenter Server retrieves and encapsulates the configuration settings of an existing VMware ESX/ESXi host into a description that can be used as a template for configuring other hosts. These settings are stored in the VMware vCenter Server database and can be exported into the VMware profile format (.vpf).

2. **Step 2: Attach a profile to a host or cluster.**

   After you create a host profile, you can attach it to a particular host or cluster. This enables you to compare the configuration of a host against the appropriate host profile.

3. **Step 3: Check the host's compliance against a profile.**

   Once a host profile is created and attached with a set of hosts or clusters, VMware vCenter Server monitors the configuration settings of the attached entities and detects any deviations from the specified "golden" configuration encapsulated by the host profile.

4. **Step 4: Apply the host profile of the reference host to other hosts or clusters of hosts.**

   If there is a deviation, VMware vCenter Server determines the configuration that applies to a host. To bring noncompliant hosts back to the desired state, the VMware vCenter Server Agent applies a host profile by passing host configuration change commands to the VMware ESX/ESXi host agent through the vSphere API.

What Is in a Host Profile?

A host profile is composed of two parts:

- Configuration details – Describes policies that govern how a host configuration should look, including details about each specific configuration setting.
- Compliance details – Describes a set of checks that are performed to ensure that the host is configured as specified in the profile.

These configuration policies are grouped into subprofiles designated by functional groups (e.g., storage, networking, security, etc.). The following table provides examples of some of the key configuration policies and compliance checks encapsulated within a host profile. A full listing with additional details can be found within the Profile Editor.

SUBPROFILES	CONFIGURATION AND COMPLIANCE CHECKS	WHY IS IT IMPORTANT?
Memory Reservation	Service console memory reservation: Validate that <num> bytes of memory are reserved for service console.	If third-party management agents are running within the service console, their performance might depend on the amount of memory reserved for the service console.
Storage	NFS datastore.	It is important to ensure that all the VMware ESX/ESXi servers are configured the same way with respect to storage, so that features such as VMware VMotion™ (VMotion) work across hosts. A compliance failure to the storage subprofile would mean that a particular NFS datastore is not available to the host. Detecting this compliance failure before a VMotion is attempted enables the administrator to take corrective action sooner.
Networking	Virtual switches: Verify that <vswitch> has <nicList> connected (e.g., make sure there are exactly three vSwitches; make sure vSwitch1 is connected to vmnic0 and vmnic1; make sure all network adaptors connected to vSwitch0 are at 1,000Mbps and are running full-duplex). Port groups: Verify that the number of ports on vswitch <vswitch> is <#>. Physical network adaptors. VMware vNetwork Distributed Switch (Distributed Switch).	Early detection of networking misconfiguration can help prevent virtual machine downtime caused by loss of network connectivity. For VMware High Availability (VMware HA) to function, all hosts in the cluster must have compatible networks. It is important to ensure that domain name system (DNS) is fully configured. This includes ensuring proper, consistent configuration for forward lookup and reverse lookup. Otherwise, VMware ESX/ESXi hosts might intermittently disconnect from VMware vCenter, and VMware HA might not work properly.

SUBPROFILES	CONFIGURATION AND COMPLIANCE CHECKS	WHY IS IT IMPORTANT?
Date and Time	Time settings: Validate that list of NTP servers is <server>. Time zone: Validate that the time zone is set to <time zone>.	VMware ESX/ESXi hosts should have their clocks synchronized for the purpose of keeping coordinated logs for the service console and virtual machines.
Firewall	Firewall configuration: Make sure that incoming traffic is <blocked/not> and outgoing traffic is <blocked/not> by default.	If there are more ports open on the network than the profile allows, it usually indicates the existence of a security hole. *Firewall configuration is not applicable to VMware ESXi hosts.*
Security	n/a	n/a
Service	System services (ntpd, sshd, etc.): Validate that the service <x> is configured with startup policy <automatic / off / on>.	n/a
Advanced	Advanced configuration options.	n/a
User	Users.	If an expected user is missing, that will be flagged as a compliance warning.
User Group	User groups.	If an expected user group is missing, that will be flagged as a compliance warning.

Figure 1. Host Profile Configuration Policies and Compliance Checks

During the creation of a host profile, VMware vCenter Server retrieves and encapsulates the configuration settings of the reference host into the profile. There is a slight variation in how the following settings are handled during the profile creation process:

- Host-specific settings: VMware vCenter Server will not copy host-specific fields (i.e., IP address and hostname) from the reference host into the host profile. Instead, these host-specific fields will have a policy option that instructs VMware vCenter Server to prompt the user to fill in these inputs when a host profile is being applied to a host. The user has the option to change this default setting after the profile is created.

- Advanced configuration settings: VMware vCenter Server will only copy the advanced configuration settings that have changed and differ from the default values. The appropriate default value is determined by the VMware ESX host. Host Profiles will actively filter out advanced options that might be host specific (e.g. Syslog.Local.DatastorePath) and therefore not suitable values to use as templates for other hosts. It will also actively filter out options that are governed by other parts of the host profiles (e.g., Migrate.Enabled). The following is a full listing of advanced settings that Host Profiles does not actively copy into a profile, as of VMware vCenter Server 4.1:
  - `'ScratchConfig.ConfiguredScratchLocation'`
  - `'ScratchConfig.CurrentScratchLocation'`
  - `'Syslog.Local.DatastorePath'`
  - `'Misc.CosCorefile'`
  - `'Misc.SerialPort'`
  - `'Migrate.Enabled,`
  - `'Migrate.vmknic'`
  - `'Mem.HostLocalSwapDirEnabled'`
  - `'Mem.HostLocalSwapDir'`

NOTE: The preceding list indicates only those settings that are not captured during the profile creation/update process; it does not govern which options are applied to a host. The host profile determines which advanced options are set.

- User and user group settings: VMware vCenter Server will not automatically capture user and user groups; this can be enabled using the Profile Editor after the profile has been created.

As illustrated in Figure 1, VMware ESX/ESXi hosts have a wide scope of host configuration parameters. There is an ever-increasing number of configuration parameters for Host Profiles to handle, especially as VMware continually adds features to the VMware ESX/ESXi hypervisor. Therefore, some configuration settings might not be immediately available within Host Profiles. You can continue to use the host configuration page of the vSphere Client or scripts to configure such settings. The following is a list of known limitations for Host Profiles in the VMware vCenter Server 4.1 release:

- Storage: iSCSI HBA and targets, LUN multipathing PSP selection (fixed, round-robin, MRU), configuring storage using Pluggable Storage Architecture
- Networking: static IP routes, IPv6, selecting physical network adaptors based on VLAN
- Security: Tech Support Mode logon banner

This information might change from release to release. You can refer to the release notes for the latest information.

Using Host Profiles

This section describes some of the setup and operation tasks you can perform using Host Profiles — such as creating host profiles, attaching profiles to hosts or clusters, monitoring for compliance, and applying profiles.

Planning Considerations

There are several considerations to take into account before you create a host profile. Getting started with Host Profiles includes the following tasks:

- Determining how many host profiles to create
- Determining which reference host to use
- Determining which entities to attach to the profile

Factor in the following considerations when determining how many host profiles to create, which reference host to use and which entities to attach to the profile:

- Hardware configurations

  As a starting point, group hosts by similar hardware configuration and software version (e.g., same number of vSwitches, network adaptors, VMware ESX/ESXi version, etc.). Ensure that there is at least one additional host of similar hardware, make, model and configuration that can be used to apply a host profile.

  Host Profiles is most appropriate for new installations of similarly configured hosts. However, it also has flexible policy options that enable it to handle slight deviations in the hardware configuration. When choosing a reference host, select the one that has the lowest common denominator of configuration settings. You can apply a profile to a host that has more hardware configurations, but not fewer, than what has been specified in the host profile. For example, if a profile is created from a reference host with only three network adaptors, VMware vCenter Server can still apply the profile to a host that has four network adaptors.

- VMware ESX and ESXi versions

  Host Profiles created from a VMware ESX reference host can be applied to both ESX and ESXi hosts. An ESXi host profile can only be applied to an ESXi host. If you have a mixed cluster of ESX and ESXi hosts, then it is recommended to create a host profile from an ESX host. Host Profiles is able to translate and apply the ESX service console definition to an ESXi VMkernel port for management access, but not vice versa.

  Host Profiles is supported only for VMware vSphere 4.1 hosts. This feature is not supported for VI 3.5 or earlier hosts. If you have VMware Infrastructure 3.5 (VI 3.5) or earlier hosts managed by your VMware vCenter Server 4.1, the following can occur if you try to use Host Profiles for those hosts:

  - You cannot create a host profile that uses a VI 3.5 or earlier host as a reference host.
  - You cannot apply a host profile to any VI 3.5 or earlier hosts. The compliance check fails.
  - While you can attach a host profile to a mixed cluster that contains VI 3.5 or earlier hosts, the compliance check for those hosts fails.

- Configuration maximums

  Configuration scaling maximums should be considered when setting up Host Profiles. For example, Distributed Switches are subject to scalability limits requiring a new profile for every "set" of hosts. Refer to the "Configuration Maximums" document for vSphere 4.1 for the maximum number of hosts per VMware vNetwork Distributed Switch (Distributed Switch) and for the most current scaling information.

- Inventory association

  For easier manageability, attach profiles at the cluster level whenever possible, assuming that all hosts within that cluster share similar configuration settings, rather than at a per-host level. When attaching a host profile to a host or cluster of hosts, note the following constraints around inventory association:

  - A host may have at most one host profile.
  - A cluster may have at most one host profile. All hosts within an attached cluster must be configured according to the host profile.
  - If a host is part of a cluster, the cluster's profile is attached with the host. The host may not have its own profile. If a host leaves the cluster, the cluster's profile will remain attached to the standalone host.
  - A host may be associated with any profile, regardless of location in inventory, subject to cluster restrictions.

- Standardization across multiple VMware vCenter Servers

  Some organizations might have large environments that span across many VMware vCenter Server instances. If you want to standardize on a single host configuration across multiple VMware vCenter Server environments, you can export the host profile out of VMware vCenter Server and have other VMware vCenter Servers import the profile for use in their environments. Host profiles are not replicated, shared or kept in sync across VMware vCenter Servers joined in Linked Mode.

- Maintenance mode prerequisite

  Operational hosts can be used to create Host Profiles or checked for compliance against a known profile. However, Host Profiles can be applied only while hosts are in maintenance mode, requiring virtual machines to be migrated to another host or powered down. Ensure that there is adequate capacity on the additional host to evacuate the workloads running on the ESX hosts that need to be put in maintenance mode to apply the host profile.

Based on these considerations, VMware recommends the following:

- Document your infrastructure configuration. It is extremely helpful to have a record of your virtual infrastructure architecture and VMware ESX/ESXi host configurations. Maintain a separate document to track host-specific configuration values.
- Minimize the number of one-off configurations as much as possible, as this will reduce configuration sprawl. Standardize on a single configuration across multiple VMware vCenter Server instances if possible.
- Group hosts with similar hardware. Create one host profile per such group. If you have a mixed cluster of VMware ESX and ESXi hosts, create a host profile from a VMware ESX host.
- Attach profiles at the cluster level, assuming that all hosts within that cluster share similar configuration settings.
- Ensure that there is adequate capacity on the additional host to evacuate the workloads running on the ESX hosts that need to be put in maintenance mode to apply the host profile.

Additional considerations include:

- Known limitations to Host Profiles

  Check the release notes for known limitations for Host Profiles. There are an ever-increasing number of configuration parameters for Host Profiles to handle, especially as VMware continually adds features to the VMware ESX/ESXi hypervisor from release to release. You can use the vSphere Client or scripts to modify configuration settings that are not captured by Host Profiles.

- Privileges

  Host Profiles privileges control operations related to creating and modifying host profiles. The following privileges are required to use Host Profiles:

PRIVILEGE NAME	CLUSTER COMPLIANCE CHECK
Clear	Clear compliance-related information.
Create	Create a host profile.
Delete	Delete a host profile.
Edit	Edit a host profile.
View	View a host profile.
Host.Config.	Apply a profile to a host. Dynamic privilege checking is done depending on which configuration setting is being changed. For example, networking privileges (i.e., Host.Config.Network) are required to be able to add a virtual switch.

Figure 2. Host Profile Privileges

The vSphere Client will not show selection for host profiles if the administrator does not have the right privilege. In addition, the user must have privileges related to the configuration and maintenance of the VMware ESX/ESXi hosts. For example, if a user does not have network configuration privileges (i.e., Host.Config.Network) and tries to apply a host profile, VMware vCenter Server will generate an error, indicating lack of sufficient privileges, and will not allow the user to proceed with the profile application process. Refer to the Basic System Administration guide for additional details on privileges required for host configuration.

Monitoring for Configuration Compliance

Maintaining visibility and control in an environment that is flexible and changes rapidly is critical. Checking compliance on a regular basis ensures that the host or cluster continues to be correctly configured. Once you have attached a profile to a host or cluster, you can check the compliance status from various places in the vSphere Client:

- Host Profiles main view — displays compliance status of hosts and clusters listed by profile
- Host Summary tab — displays compliance status of the selected host
- Cluster Profile Compliance tab — displays compliance status of the selected cluster and all the hosts within the selected cluster

For day-to-day monitoring and operational tasks, VMware recommends using the Cluster Profile Compliance tab. When you select a cluster from the VMware vCenter inventory panel, the Profile Compliance tab displays host profile compliance information about the hosts within the selected cluster, as well as compliance against specific cluster requirements and settings.

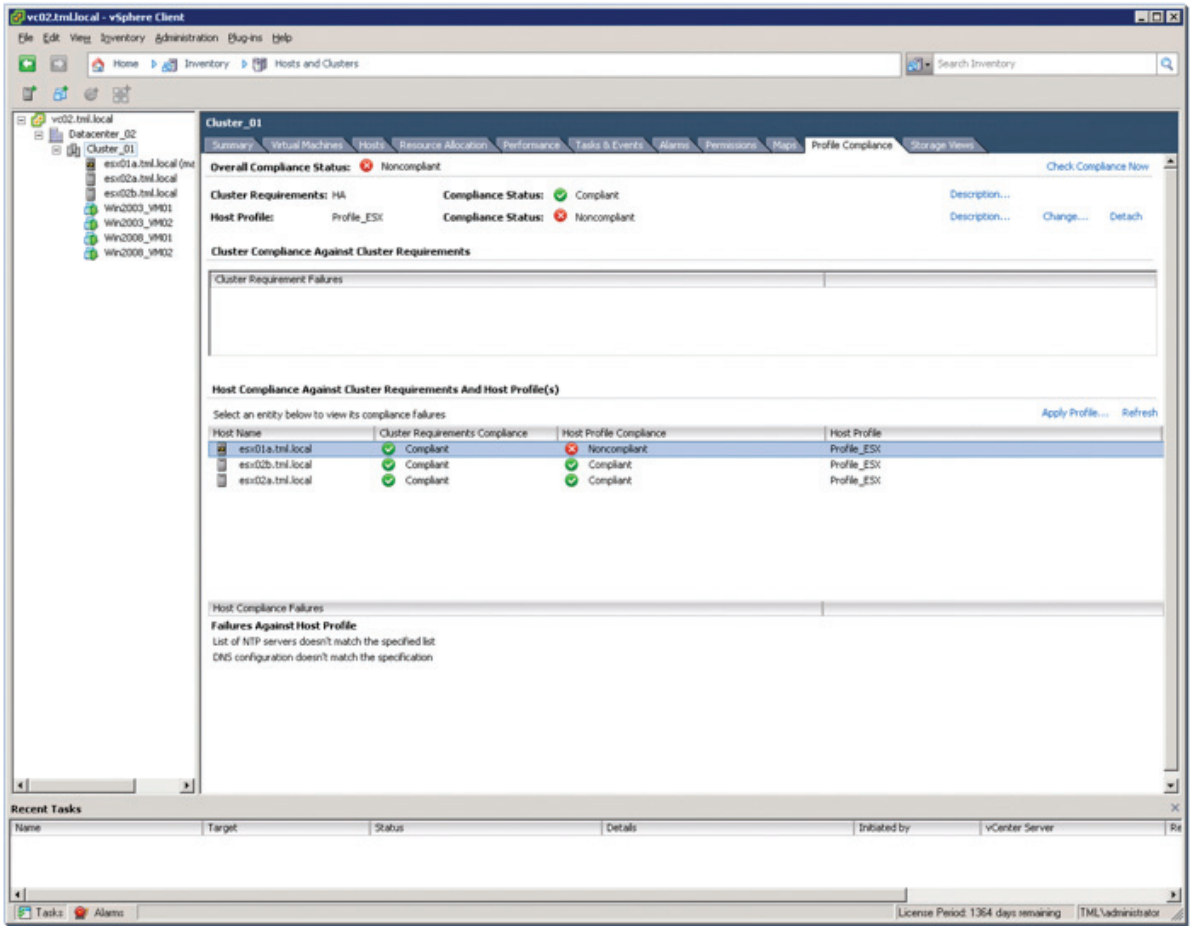


Figure 3. Cluster Profile Compliance Tab

A base set of host compliance checks is generated from the description for how hosts are configured. In addition, the following built-in cluster-level compliance checks occur with or without a host profile attached to the cluster.

CLUSTER REQUIREMENT	CLUSTER COMPLIANCE CHECK
VMware Distributed Resource Scheduler (VMware DRS)	• Validate that VMotion network adaptor speed is at least 1,000Mbps. • Validate that VMotion is enabled. • Validate that at least one shared datastore exists.
VMware Distributed Power Management (VMware DPM)	• Validate that power management is supported on the host.
VMware High Availability (VMware HA)/ VMware Fault Tolerance (VMware FT)	• Validate that fault tolerance logging is enabled. • Validate that fault tolerance logging network adaptor speed is at least 1,000Mbps. • Validate that all the hosts in the cluster have the same build for fault tolerance. • Validate that the host hardware supports fault tolerance.

Figure 4. Built-in Cluster Compliance Checks

You can monitor profile compliance of standalone hosts that are not part of a cluster by selecting the host from the VMware vCenter inventory panel and viewing the Host Summary page, or the Host Profiles main page.

A host will show as noncompliant if the host configuration is different or drifts from the desired configuration defined by the attached profile. When a host shows up as noncompliant, you must verify whether the host configuration deviation is the result of an authorized and intentional configuration change. To understand which specific configurations violated the compliance check, you can review the "Host Compliance Failures" and "Cluster Requirement Failures" sections for more details. For example, if a virtual switch is missing a physical network adaptor (according to the compliance checks), the error will indicate the name of the physical network adaptor that is missing, as well as the name of the virtual switch on which the error occurred. If the change was authorized and intentional, you might want to update the host profile. Otherwise, if you want to override the change, you can use Host Profiles to bring the host back to a desired state of configuration by simply applying the host profile.

In addition to the Profile Compliance page, several built-in alarms and scheduled tasks further simplify ongoing compliance monitoring.

- **Scheduled tasks for checking compliance:** You can schedule the "Check compliance of a profile" task to run once in the future or multiple times, at a recurring interval. This task checks that a host's configuration matches the configuration specified in a host profile. By default, this interval is set to check once a day.
- **Alarm triggers for checking compliance:** You can set the following alarms to alert you on various events.
  - Alarm Settings → Alarm Type: "Hosts" → "Monitor for specific events" → Triggers: "Host profile applied", "Host compliant with profile", "Host noncompliant with profile"
  - Alarm Settings → Alarm Type: "Clusters" → "Monitor for specific events" → Triggers: "Cluster compliance checked"

Automating Host Configuration

Host Profiles enables you to automate host configuration across a large number of hosts and clusters. In one click, you can instruct VMware vCenter Server to apply a host profile, at which point it configures each host to match the desired configuration state. Host Profiles simplifies the host provisioning process and drastically reduces the time spent on configuring and deploying new VMware ESX/ESXi hosts.

Before a profile can be applied to a host, the host must be placed in maintenance mode. Virtual machines that are running on a host entering maintenance mode must be migrated to another host (either manually or automatically by VMware DRS) or shut down. It is possible to make some simple configuration changes (e.g., date and time settings) using the host configuration page in the vSphere Client without requiring the host to be put in maintenance mode. However, as a precaution, Host Profiles requires hosts to be in maintenance mode for all host configuration changes, to ensure that there is no data loss or loss of service.

NOTE: If you have VMware HA-enabled clusters, placing the hosts in maintenance mode is sufficient; there is no need to suspend the Host Monitoring feature before applying the host profile.

The Apply Profile wizard might prompt you to enter additional host-specific information, such as IP address or host name, before the profile is applied. VMware vCenter will show a detailed list of actions (i.e., what will be added, removed, modified) that will be performed on the host to configure it, allowing you to review this before applying the configuration to the host. Always double-check to make sure that you have entered these fields correctly.

If a host has more configuration elements than what is specified in the host profile, in most cases, Host Profiles will take care of removing elements as necessary (e.g., networks, NFS datastores). Users and user groups are an exception to this, since an administrator might not want to remove all users from the host. Therefore, Host Profiles cannot be used to automate the removal of users and user groups from each host.

Once the profile is applied, the host settings will match those specified in the host profile.

NOTE: Some host configuration changes, such as modifying service console memory reservations, will require a reboot.

In a scenario where the user has entered an invalid configuration setting in the Apply Profile wizard or within the profile itself, VMware vCenter Server tries to configure as much as possible to get the host to the desired configuration state; it then generates an error message that tells the user what settings it was unable to apply. The user can then make the necessary adjustments and try to reapply the profile to configure the remaining settings. VMware vCenter Server will make only the changes required to bring the host to the desired configuration. In other words, it will proceed with the remainder of the configuration from the point where it had generated the error. Host Profiles will not roll back the host to the previous configuration.

Because applying profiles requires user interaction to review the changes and might prompt the user for additional input (e.g., unique static IP address for each host), VMware vCenter Server does not offer the capability for scheduling an “Apply Profile” task to run at a designated time in the future.

Making Incremental Changes to an Existing Host Profile

Once you have created a host profile, you might find it necessary to make incremental updates to it in order to reflect changes in your business compliance and configuration policies. There are two methods for doing this:

1. **Update profile using the vSphere Client** – Make the configuration change on the reference host using the host configuration page in the vSphere Client; update the profile from the reference host; then apply the update to the other hosts to which the host profile is attached. This method enables you to verify that the changes were properly made on the one host, before rolling out the changes more widely across the environment. This is the recommended method for making basic changes to an existing host profile.
2. **Update profile using the Profile Editor** – Make the configuration change in the host profile using the Profile Editor; then apply the edited host profile to the hosts to which the host profile is attached. In general, use this method only if you intend on using the advanced profile policy options. These advanced policy options are available only through the Profile Editor; they are not available through the host configuration page in the vSphere Client.

Depending on your host profile setup, you can use one of the following suggested approaches for automating host configuration changes across a set of hosts or clusters.

SCENARIO	SUGGESTED METHOD
If no profile exists in your inventory	Create and apply profile: 1. Set up and configure the host that will be used as the reference host. 2. Create profile using the designated reference host. 3. Attach profile to hosts or clusters. 4. Apply the profile.
If the profile exists in your inventory and you want to propagate a basic configuration change across the environment Examples: • Update DNS Settings • Update NTP Settings • Add new Virtual Switch • Add new Port Groups • Configure hosts to use Distributed Switch • Configure hosts to use NAS storage	Update profile using the vSphere Client: 1. Identify the profile's reference host. • If the profile does not have a reference host in the environment (i.e., profile was imported), change its reference host. 2. Change setting on reference host using the vSphere Client. 3. Update profile from reference host. 4. Apply the profile.
If the profile exists in your inventory and you want to propagate an advanced configuration change across the environment, which relates to changing host profile defaults or handling variations in the underlying hardware configuration Examples: • Disable compliance checks • Enable compliance check for users and user groups • Customize network configurations • Customize network duplex settings • Handle host-specific settings • Allow exceptions in host configuration variability • Use one profile across both VMware ESX and VMware ESXi	Update profile using the Profile Editor: 1. Edit profile using Profile Editor. 2. Apply the profile.

Figure 5. Procedures for Applying a Host Profile

The following figure shows how the subprofile categories map to the categories listed on the Host Configuration page in the vSphere Client.

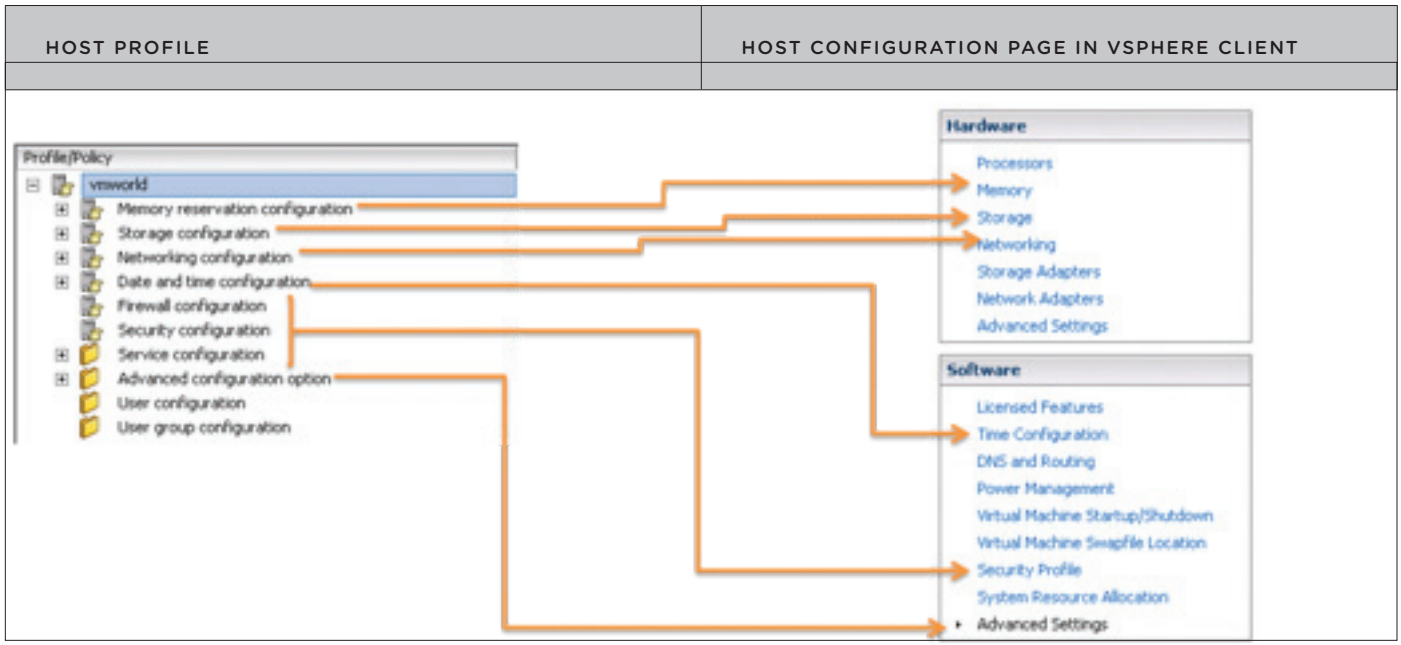


Figure 6. Comparing Host Profile Categories to Host Configuration Page

The following section provides example workflows that address common settings that might need modification after the initial creation of a host profile. These settings can be easily modified using the host configuration page within the vSphere Client and then updating the host profile from the reference host.

Use Case 1: Using Host Profiles to Update DNS Configuration

If you introduce a new domain name system (DNS) server to your environment, you might want to update the hosts so that they are able to leverage it. Host Profiles can automatically apply these DNS changes across a specified set of hosts, and ensure that the hosts remain in compliance with the list of DNS servers.

Once you have identified the reference host of the host profile you would like to change, use the following procedure:

1. Ensure that the reference host is compliant with the host profile.
2. Change DNS configuration on the reference host using the vSphere Client.
    a. Select the reference host from the inventory panel.
    b. Click the Configuration tab, and click **DNS and Routing**.
    c. On the right of the window, click **Properties**.
    d. In the DNS Configuration tab, enter values for the Name and Domain fields.
    e. Choose to use a DNS server address. Specify the domains in which to look for hosts. Click **OK**.

3. Update the profile from the reference host.
    a. In the Host Profiles main view, select the profile to update.
    b. Right-click the profile, and select **Update Profile from Reference Host**.
    c. <Optional> Review the updated DNS change in the host profile to confirm that it was accurately captured. From the Profile Editor, select **Profile > Networking configuration > DNS configuration**. View the default compliance checks.
4. Apply profile to the attached entities.
    a. Select the **Hosts and Clusters** tab. The list of attached hosts is shown under Entity Name.
    b. Click **Apply Profile**.

Use Case 2: Using Host Profiles to Update NTP Settings

VMware ESX/ESXi hosts should have their clocks synchronized for the purpose of keeping coordinated logs for the service console and virtual machines. This is most efficiently done using an NTP server.

Host Profiles can be used to create a standard policy for ensuring that NTP server addresses are the same for all the hosts in the network. If you need to update NTP settings after you have created a host profile, use the following procedure:

1. Identify the reference host and ensure that it is compliant with the host profile.
2. Change NTP configuration on the reference host, using the vSphere Client.
3. Update the profile from the reference host.
    a. In the Host Profiles main view, select the profile to update.
    b. Right-click the profile, and select **Update Profile from Reference Host**.
    c. <Optional> Review the updated NTP change in the host profile to confirm that it was accurately captured. From the Profile Editor, select **Profile > Date and Time configuration**. View the default compliance checks.
4. Apply the profile to the attached entities.

Use Case 3: Using Host Profiles to Add a New Virtual Switch

Host Profiles can simplify the process of adding a new virtual switch to a large set of hosts. For example, an administrator might want to add a new virtual switch with the name **vSwitch15**, to have numPorts = **64**, and **vmnic1** to be connected to it.

Option 1: Update the profile, using the vSphere Client.

1. Identify the reference host and ensure that it is compliant with the host profile.
2. Add a virtual switch to the reference host, using the vSphere Client.
3. Update the profile from the reference host.
    a. In the Host Profiles main view, select the profile to update.
    b. Right-click the profile, and select **Update Profile from Reference Host**.
    c. <Optional> Review the updated networking change in the host profile to confirm that it was accurately captured. From the Profile Editor, select **Profile > Networking configuration**. View the default compliance checks.
4. Apply the profile to the attached entities.

Option 2: Update the profile, using the Profile Editor.

1. Open the profile, using Profile Editor.
2. Add a new vSwitch to the host profile.
    a. Expand out to: **Networking Configuration > vSwitch**.
    b. Right-click on the **vSwitch** folder, and select **Add Profile**.
    c. Enter name as **vSwitch15**.
    d. Configure the link configuration.
    i. On the "Configuration Details" tab under Link Configuration, click **Edit to configure** "which physical NICs should be connected to this vSwitch."
        ii. Enter **vmnic1** in the **Names of Nics to attach** field.
    e. Configure the number of ports.
        i. Expand out vSwitch15. Click on **Number of ports**.
        ii. Select **Number of ports on the vSwitch for the fixed configuration** option from the drop-down menu. Enter **64** in the Number of ports with which to configure this switch" field.
3. Apply the profile to the attached entities.

Use Case 4: Using Host Profiles to Add New Port Groups

Port groups are important particularly for VMotion. They make it possible to specify that a given virtual machine must have a particular type of connectivity on every host on which it might run.

Assume an administrator has provisioned a new network for a set of virtual machines to use. The administrator can create a new virtual machine port group on the host that represents the new network. However, if VMotion is in use, the same virtual machine port group must be created on all the hosts that can host the virtual machines connected to the new network. Host Profiles enables the administrator to manage this change easily.

Once you have identified the reference host of the host profile you would like to change, use the following procedure:

1. Ensure that the reference host is compliant with the host profile.
2. Using the host configuration page within the vSphere Client, add a port group to the reference host and configure the necessary port group parameters.
3. Update the profile from the reference host.
    a. In the Host Profiles main view, select the profile to update.
    b. Right-click the profile and select **Update Profile from Reference Host**.
    c. <Optional> Review the updated networking change in the host profile to confirm that it was accurately captured. From the Profile Editor, select **Profile > Networking configuration**. View the default compliance checks.
4. Apply the profile to the attached entities.

Once you apply the profile, a new virtual port group will be created on the specified hosts.

Use Case 5: Using Host Profiles to Configure Hosts to Use VMware vNetwork Distributed Switch

Host Profiles can be used to capture the vNetwork Standard Switch (vSS) and vNetwork Distributed Switch configuration of a VMware ESX host, and then apply and propagate that configuration to a number of other VMware ESX or ESXi hosts.

Host Profiles is the preferred and easiest method for deploying a Distributed Switch across a large population of hosts. The following use case assumes that you are starting with a population of hosts, each with a single Standard Switch.

Migrate reference host to Distributed Switch.

1. Create Distributed Switch (without any associated hosts).
2. Create Distributed Virtual Port Groups on Distributed Switch to match existing or required environment.
3. Add host to Distributed Switch and migrate vmnics to dvUplinks and Virtual Ports to DV Port Groups.
4. Delete Standard Switch from host.

At the completion of Step 4, we will have a single host with its networking environment completely migrated to Distributed Switch. The following three steps allow us to create a host profile of this migrated host and then apply it to a number of hosts in one step (Step 7).

5. Create host profile of Reference Host.
6. Attach and apply the host profile to the candidate hosts.
7. Migrate virtual machine networking for virtual machines and take the hosts out of Maintenance Mode.

Variation on Using Host Profiles for Migration

The previously outlined process can be time consuming for a large number of virtual machines. An alternative method, which reduces the per–virtual machine edit process but requires a reapplication of a modified host profile, is as follows:

1. Retain the Standard Switch on each host (and, therefore, the Port Groups) during migration, using Host Profiles. Do not perform Step 4 (so you create a host profile of a host with a Standard Switch and a Distributed Switch and then apply that profile to the hosts).
2. Right-click on the Distributed Switch and select **Migrate Virtual Machine Networking**... and then migrate all virtual machines for each Port Group in one step per Port Group.
3. Delete the Standard Switch from the host profile using the edit **host profile** function (or just delete the Standard Switch from the reference host and create a fresh host profile).
4. Reapply this host profile to the hosts in the cluster.

NOTE: Because we already have migrated the virtual adaptors, we would not need to reenter any of the IP addresses.

For a detailed, screen-by-screen walkthrough of this use case, refer to the VMware vSphere 4.1 Evaluator's Guide. For additional details on using Host Profiles to migrate hosts to vDS, refer to VMware vSphere 4.1: Deployment Methods for the vNetwork Distributed Switch.

Use Case 6: Using Host Profiles to Configure Hosts to Use NAS Storage

You can use Host Profiles to prepare your VMware ESX/ESXi hosts to use a newly added NAS storage device.

1. Identify the reference host and ensure that it is compliant with the host profile.
2. Add an NFS-based datastore on the reference host, using the vSphere Client.
    a. Because NFS requires network connectivity to access data stored on remote servers, before configuring NFS you must first configure networking to make sure you have at least one vmknic. To mount an NFS datastore, the Add Storage wizard guides you through the following configuration steps:
        i. Select the host from the inventory panel.
        ii. Click the Configuration tab and click **Storage** in the Hardware panel.
        iii. Click **Add Storage**.
        iv. Select Network File System as the storage type and click **Next**.
        v. Enter the server name, the mount point folder name, and the datastore name. Click **Next**.
        vi. In the Network File System Summary page, review the configuration options and click **Finish**.

3. Update the profile from the reference host.
    a. In the Host Profiles main view, select the profile to update.
    b. Right-click the profile and select **Update Profile from Reference Host**.
    c. <Optional> Review the updated storage change in the host profile to confirm that it was accurately captured. From the Profile Editor, select **Profile > Storage configuration**. View the default compliance checks.
4. Apply the profile to the attached entities.

Advanced Profile Editing and Customization

Profile policies describe how the configuration settings should be applied to the VMware ESX/ESXi hosts. The default settings used by Host Profiles might not be applicable to certain user scenarios, in which case you can use the Profile Editor to customize the profile policies to fit your particular environment. The Profile Editor allows you to:

- Change the profile name or description.
- View and edit the host profile policies.
- Enable and disable compliance checks.
- Leverage advanced policy options.

Unless you must change the default host profile policies, enable or disable compliance checks, or leverage the advanced policy options, it is generally recommended that you make the configuration changes on the reference host, using the host configuration page in the vSphere Client, rather than editing the profile directly using the Profile Editor.

Here are a couple of general tips when editing a host profile:

- To experiment with a host profile, it is safest to create a duplicate profile and to work with the copy. A duplicate can be created by exporting the profile to be duplicated and importing it back into VMware vCenter Server with a new name.
- If you intend to do an in-place update of the host profile, it is suggested that you keep a backup copy of the original. A rudimentary way to back up the host profile is to export it.

Customizing Compliance Details

During the initial profile creation process, Host Profiles generates a set of compliance checks by default. Users can use the Profile Editor to disable any of the compliance checks.

Use Case 1: Disabling Default Compliance Checks

Users can edit host profiles to disable compliance checks that do not apply to their environment.

1. Open the Profile Editor by selecting the profile and clicking **Edit Profile**.
2. Navigate to the policy you wish to disable.
3. Click on the **Compliance Details** tab.
4. Uncheck the box next to the specific compliance check you want to disable.
5. Apply the profile to the attached entities.

Use Case 2: Enabling Compliance Check for Users and User Groups

For compliance monitoring, you can use Host Profiles to ensure that the list of VMware ESX/ESXi users on the hosts stays the same. Host Profiles will flag any user removals (but not user additions) on a host as a compliance failure. This is useful for security purposes in preventing unauthorized user removals.

During the profile creation process, Host Profiles does not automatically capture user and user group configurations from the reference host. Administrators will need to enable this setting in the Profile Editor before using it.

1. Open the Profile Editor by selecting the profile and clicking **Edit Profile**.
2. Right-click on Users, and select **Add User**.

   NOTE: The box to enable the compliance check does not appear immediately after you add a new user/user group. It will appear only after you have saved the profile.
3. Save profile and close the Profile Editor.
4. Reopen the Profile Editor. Check the box next to the compliance check. Close Profile Editor.
5. Apply the profile to the attached entities.

Given a list of required users and user groups that should be present on each host, Host Profiles can detect which hosts are missing the required users/groups, and then automatically create those users/groups on those hosts. Host Profiles cannot be used to detect unauthorized creation of new users and user groups. It also cannot be used to automate the removal of users and user groups from each host.

Customizing Configuration Details

Host Profiles provides a number of advanced policy options to provide maximal flexibility when configuring VMware ESX/ESXi hosts and to address specific configuration requirements. With the vSphere Client or scripts, users would have to specify explicitly how the hosts should be configured. With Host Profiles, users can simply specify the configuration they want instead of specifying how to do it, and VMware vCenter Server will intelligently determine how best to get to that desired configuration.

For example, networking configuration using the vSphere Client would require users to specify that vmnic0 should be connected to vSwitch0. In contrast, Host Profiles enables the user to express how many network adaptors should be connected to the vSwitch, rather than worrying about which network adaptors should be connected to which vSwitch. During the configuration process, Host Profiles can instruct VMware vCenter Server to automatically pick up free network adaptors and assign them to a particular virtual switch. VMware vCenter Server would automatically translate the “Any 2 NICs” policy option into “vmnic0 and vmnic1” and configure the host appropriately.

Allowing VMware vCenter Server to determine the best configuration not only increases configuration flexibility across different hardware types, but it also reduces the potential risk of user-introduced misconfiguration errors.

Host Profiles offers the following policy option types:

CONFIGURATION DETAILS: HOW SHOULD THIS SETTING BE CONFIGURED?

1. Use a fixed configuration.
2. Ask the user how it should be configured.
3. Have VMware vCenter determine the best configuration, based on specified conditions.
  a. Specify one criterion.
  b. Specify multiple criteria.
4. Disregard this setting.

Figure 7. Summary of Policy Option Types

Depending on the configuration selections, the exact wording of the policy options in the Profile Editor might vary. The following chart describes each of these policy option types in more detail.

POLICY OPTION TYPE	DESCRIPTION + EXAMPLE UI WORDING	EXAMPLE
1. Use a fixed configuration.	Other hosts using this host profile will get the same settings and the same instances (i.e., networks, datastores). This is the default setting in most cases. This might appear in the UI as: • "Use a fixed configuration option." • "Apply the specified configuration." • "Always create."	This is the default setting in most cases.
2. Ask the user how it should be configured.	Before applying a profile, the Apply Profile wizard will prompt the user to enter the desired configuration values. The profile will not be applied until the user finishes providing all the requested information designated by this policy option. This might appear in the UI as: • "Ask for specific configuration values at apply time." • "Prompt the user for x if no default is available."	This typically is used for host-specific fields, such as IP address and host name.
3. Have VMware vCenter determine the best configuration, based on specified conditions.	User specifies one criterion, and VMware vCenter determines the best configuration, based on that criterion. This policy option enables the user to specify exceptions in host configuration variations and helps determine whether the profile can be applied to the host. This might appear in the UI as: • "Choose x with y criteria." • "Create if."	The user can choose one specific criterion to allow VMware vCenter Server to choose which physical network adaptors should be connected to a particular vSwitch; e.g., "Choose physical network adaptors with the given link state." This is also useful in enabling exceptions to host configuration variations; e.g., "Create if product family matches <ESX / embedded ESXi>.
	User specifies multiple criteria, and VMware vCenter Server determines the best configuration, based on multiple criteria. This might appear in the UI as: • Compose one or more policy options for the result.	The user can combine multiple criteria to allow VMware vCenter Server to choose which physical network adaptors should be connected to a particular vSwitch. The policy criteria might be any combination of name, link state, cardinality, bandwidth, and duplexity.
	Use the default values. This might appear in the UI as: • "Use default values."	n/a

POLICY OPTION TYPE	DESCRIPTION + EXAMPLE UI WORDING	EXAMPLE
4. Disregard this setting.	This policy option instructs the user to pick another policy option if he desires a change to be made. Otherwise, choosing this setting will instruct VMware vCenter Server to disregard altogether and leave the settings as is. This might appear in the UI as: • "User must explicitly choose the policy option."	n/a

Figure 8. Details and Examples of Policy Option Types That Specify How a Setting Should Be Configured

The following section provides example workflows that address settings that can only be specified using the Profile Editor. These settings provide greater flexibility in configuration management than what the host configuration page in the vSphere Client provides.

Use Case 1: Customizing Network Configurations

Using Host Profiles policies provides greater configuration flexibility. Policies allow you to specify what to do instead of how to do it, so the configuration does not have to be a set of exact values. For example, say you want two network adaptors to connect to vSwitch0. Instead of specifying to connect vmnic0 and vmnic1 to vSwitch0, you can configure a policy to connect two network adaptors to vSwitch0. Then when VMware vCenter Server applies the profile, it will assign two free network adaptors to the vSwitch.

The following table describes the various options for determining how a physical network adaptor should be connected to a particular vSwitch.

POLICY OPTION	DESCRIPTION
Choose physical network adaptors with the specified name.	Attaches <list of specified Network Adaptors> to this virtual switch. This is the default and has the same behavior as configuring networking using the host configuration page in the vSphere Client.
Choose physical network adaptors operating at higher than a minimum bandwidth and duplexity criteria.	Attaches physical network adaptors that operate at higher than the specified minimum bandwidth and duplexity.
Choose physical network adaptors with the given link state.	Attaches physical network adaptors with the given link state.
Choose physical network adaptors with the specified cardinality.	Selects a number of network adaptors that pass the other policy options. This policy option is used last if it is one of multiple criteria within a composite option.
Compose one or more policy options for the result.	Allows the user to specify any combination of name, minimum bandwidth, duplexity, link state, and cardinality.

Figure 9. Policy Options for Connecting Physical Network Adaptors to Virtual Switches

Option 1: Specify one criterion.
In the case where a user does not care which network adaptors are connected, but wants to make sure two network adaptors are connected to vSwitch15, use the following procedure:

1. Edit the profile using the Profile Editor.
    a. Select **Networking configuration**.
    b. On the Configuration Details tab under Link Configuration, click **Edit** to specify "Which physical NICs should be connected to this vSwitch?"

    (NOTE: Alternatively, you can use the tree navigation on the left to expand out to: "Profile" > Networking configuration > vSwitch > "vSwitch0" > Link Configuration > Physical network adaptors.)

    c. Select **Choose physical NICs with the specified cardinality** from the drop-down menu.
    d. Enter in "= 2": This instructs VMware vCenter Server to connect the first two network adaptors that satisfy the other criteria. If there are no other criteria, the first two available network adaptors will be selected.
    e. Click **OK**.
2. Apply the profile to the attached entities.

During the actual application of the profile, free network adaptors will be picked and assigned to the virtual switch. If the required number of network adaptors is not found, an error will be raised during application of the profile.

Option 2: Combine multiple criteria.
User specifies multiple criteria, and VMware vCenter Server determines the best configuration, based on all of the criteria specified. The user can select the "compose one or more policy options for the result" option to allow VMware vCenter Server to choose which physical network adaptors should be connected to a particular vSwitch, based on the policy criterion specified. The policy criteria might be any combination of name, link state, cardinality, bandwidth, and duplexity.

NOTE: You may combine only those criteria that relate to a similar configuration area. For example, the criteria for controlling Port Group virtual switch selection policy may use only other criteria used to configure Port Group virtual switch selection.

In the case where a user wants to specify a combination of name, link state, cardinality, bandwidth, and duplexity when determining which physical network adaptors to connect to a particular vSwitch, use the following procedure:

1. Edit the profile using the Profile Editor.
    a. Select **Networking configuration**.
    b. On the Configuration Details tab under Link Configuration, click **Edit** to specify "Which physical NICs should be connected to this vSwitch?"

    (NOTE: Alternatively, you can use the tree navigation on the left to expand out to: "Profile" > Networking configuration > vSwitch > "vSwitch0" > Link Configuration > Physical network adaptors.)

    c. Select **Compose one or more policy options for the result** from the drop-down menu.
    d. Select all of the check boxes and fill in the additional requested information.

    NOTE: The "Choose physical NICs with the specified cardinality" option is considered last if it is one of multiple criteria specified. It will select only network adaptors that pass the other specified criteria.

    e. Click **OK**.
2. Apply the profile to the attached entities.

Use Case 2: Customizing Network Duplex Settings

Use the following procedure to set up networks automatically with a different duplex setting (e.g., 100 full duplex rather than 100 half):

1. Create the profile.
2. Edit the profile, using the Profile Editor.
    a. In the Profile Editor, select **Profile > Networking configuration > Physical NIC configuration > Physical network adaptor**.
    b. Under "How should the physical NIC be configured," select **Fixed physical NIC configuration** in the drop-down menu.
    c. Check the box for **Flag indicating if NIC should be duplex** and fill in the fields **Name of the physical NIC to configure** and **Link speed in Mbps**.
3. Apply the profile to the attached entities.

This will maintain the desired network duplex settings specified within the host profile.

Use Case 3: Handling Host-Specific Settings (i.e., IP Address, Host Name)

If the reference host is using DHCP, the profile that was created from the reference host will also use DHCP. If the reference host uses static IP addresses, the profile will, by default, use the policy option that prompts the user for the IP address at application time.

As a best practice, VMware recommends using a static IP address to simplify client access. If the reference host is using a static IP address, the profile will instruct VMware vCenter Server to prompt the user to enter host-specific configuration settings (i.e., IP address and host name) before the profile can be applied to other hosts. The user has the option to change this default setting, using the Profile Editor. For example, you can edit the profile to instruct VMware vCenter Server to use DHCP to configure IP addresses, instead of prompting the user to enter static IP addresses.

The following options are available for handling host-specific fields, accessible from the Profile Editor in the following locations:

- IP Address
    - In the Profile Editor, select **Profile > Networking configuration > "Port group" > Service Console > IP Address Settings**.
- Host Name
    - In the Profile Editor, select **Profile > Networking configuration > DNS Configuration > Host Name**.

POLICY OPTION	DESCRIPTION
Apply a specified IP configuration.	Use the specified IP address and subnet mask stored in the host profile. This requires that the IP address be specified in the profile. By doing this, the profile can be used only on that particular host.
User-specified IP address to be used while applying the configuration.	Unconditionally prompts the user at application time for an IP address and subnet. If a value is already available on the host, that value will be shown to the user. User can choose to retain the value shown or change it.
Use DHCP to configure IP address.	Assign IP address using DHCP.
Prompt the user for IP address if no default is available.	Prompt the user at application time for an IP address and subnet if there is not already one specified for the host. <default>

Figure 10. Policy Options for IP Address Fields

POLICY OPTION	DESCRIPTION
User-specified host name to be used while applying the configuration.	Ask the user during profile application. This means that the user wants to specify or confirm the host name every time the profile is applied. If the value is found in the system, VMware vCenter Server will show the current value and ask the user to confirm, or ask the user for the value.
Obtain host name from DHCP.	Assign host name using DHCP.
Prompt the user for host name if default is not available.	Prompt the user at application time for a host name if there is not already one specified for the host. <default>

Figure 11. Policy Options for Host Name Fields

To enable DHCP to configure all IP addresses, instead of prompting the user to enter static IP addresses, use the following procedure:

1. Edit the profile using the Profile Editor.
    a. In the Profile Editor, select **Profile > Networking configuration > "Port group" > Service Console > IP Address Settings**.
    b. Under "How should the IP Address be configured," select "**Use DHCP to configure IP address**" in the drop-down menu.
    c. Repeat for each port group listed in the networking configuration if desired.
2. Apply the profile to the attached entities.

Use Case 4: Allowing Exceptions in Host Configuration Variability

The "Create if" policy option allows the user to specify conditions to control whether or not the profile will be used. This policy option enables you to create one flexible profile that can be applied to different types of servers, allow for exceptions in host configuration variations, and help validate whether the profile can be applied to the host.

If you want to use the same profile for a variety of host configurations, you can customize the host profile to use "Create if" policies. This allows you to deal with variations in hardware configuration. For example, if you have hardware with a variation of two to four network adaptors, you can create three separate profiles, or just one profile using the "Create if" policy. This policy enables you to specify different network adaptor counts for different hardware types (e.g., create the virtual switch only if number of network adaptors >= 3). VMware vCenter Server will check at profile application time to determine whether the virtual switch gets created.

As an example, you could specify the following:

- vSwitch 0 = always create
- vSwitch 1 = create if vmnic1 exists

This enables you to deal with variability where you might have host A with one virtual switch and host B with two virtual switches. With the "Create if" policy in place, you can ensure that the profile does not fail to apply.

To use this setting, use the following procedure:

1. Edit the profile using the Profile Editor.
    a. In the Profile Editor, select **Profile > Networking Configuration > vSwitch > "vSwitch1**."
    b. Select "**Determine when the vSwitch will be created**."
    c. Select "**Create if the link specification results in a certain minimum number of physical NICs**." Specify one (1) as the minimum number. Specify that vSwitch be connected to vmnic0 in the link profile. If the link profile yields vmnic1, this profile will be used. If not, the profile will be discarded.
2. Apply the profile to the attached entities.

Use Case 5: Using One Flexible Profile Across Both VMware ESX and ESXi

Special handling is needed to allow the same host profile to be used to manage a service console-managed VMware ESX Server (hereafter referred to as "ESX") and a service console-less ESX (referred to as "ESXi"). The lack of a service console in VMware ESXi introduces differences in how the host is configured for networking. The configuration differences derive primarily from by which network interface the system is managed. The management interface is the network interface through which all VMware management tools interface with the system; it includes the vSphere Client, VI CLI, and VI API.

The differences in networking between ESX and ESXi are caused by how management network traffic is partitioned. In ESX, management network traffic is partitioned from the rest of the VMkernel services because the management traffic must be directed to the service console. In ESXi, there is no service console, so the management traffic is directed to the VMkernel, where the rest of the services (NFS, iSCSI, VMotion) reside as well. The implication of this difference leads to a number of complications when trying to describe a common network topology between ESX and ESXi. The complications are directional, meaning there are different problems when trying to apply certain ESX-specific network configurations to ESXi, and vice versa.

Host Profiles handles the differences in network topologies and constraints by following a conservative and predictable approach. The following principles underpin the policies used in Host Profiles:

- A host profile created for ESX can be safely applied to another ESX host if the hardware configuration and software version are sufficiently similar.
- A host profile created for ESXi can be safely applied to another ESXi host if the hardware configuration and software version are sufficiently similar.
- Repeated application to the reference host from which the profile was created will not alter the host.
- Repeated successful application of a host profile to any host will not alter the host.

The following principles are to be followed when mapping a configuration created for ESX to an ESXi host, and vice versa:

- Ensure that the network interface for the management network exists even if it requires creating duplicate configuration entities/IP addresses.
- Fail the attempt to apply the profile where ambiguity exists that might cause the management network to fail to be created. Let the user edit the profile manually to ensure that the host profile is doing the correct mapping.

The following table describes how Host Profiles handles the vswif and vmknic devices that it encounters in ESX and ESXi network configurations:

SOURCE OF PROFILE	NETWORK DEVICE	HOW DEVICE IS MANIFESTED WHEN PROFILE IS APPLIED		COMMENTS
		ESX	ESXi	
ESX	vswif	Create identical vswif.	Create analogous vmknic, adding a "Management" tag to the vmknic.	vswif can only be used for management network functionality.
ESX	vmknic with or without tags	Create identical vmknic with same tags.	Create identical vmknic with same tags.	vmknic on ESX not used for management networking. Used for VMkernel services only. Therefore, the tags are not modified.

SOURCE OF PROFILE	NETWORK DEVICE	HOW DEVICE IS MANIFESTED WHEN PROFILE IS APPLIED		COMMENTS
		ESX	ESXi	
ESXi	vmknic with or without tags	Fail to apply by default due to ambiguity.	Create identical vmknic with same tags.	Could be used for either management network functionality or VMkernel services. In the case of ESX, where an explicit choice must be made, fail by default to apply the profile until user clarifies the desired applicability to ESX.

Figure 12. Expected Behavior When Using Profiles Across ESX and ESXi

This section describes best practices that help prevent some of the problems when trying to use Host Profiles across both ESX and ESXi.

SCENARIO	PROCEDURE
When starting a new VI deployment with mixed ESX and ESXi hosts	Use an ESX host as the reference host for the host profile. Create the host profile from the ESX host and apply it to ESX and ESXi. Continue to partition the management network traffic from the rest of the network services. Partitioning the management network traffic is generally good practice in and of itself and avoids the redundant IP address issue that might prevent the host from utilizing all its physical network interfaces.
When adding an ESXi host to a VI deployment that previously contained only ESX hosts	In this scenario, the host profile would have been created from an ESX host. There should be no problems, as the network device mapping from ESX to ESX is relatively straightforward.
When adding an ESX host to a VI deployment that previously contained only ESXi hosts	In this scenario, the host profile would have been created from an ESXi host. There are a number of possible options for handling this scenario: 1. If the user understands the desired network mapping to ESX and how to make it work in Host Profiles, edit the profile accordingly. Remove the restriction preventing the profile from being applied to ESX. Apply the profile to ESX. 2. Try to recreate the profile, using ESX as the reference host. Recreating a host profile can involve manually configuring the new ESX host directly. Alternatively, the host profile could be applied to configure the ESX host. To do this: 1. Temporarily remove the restriction preventing the profile from being applied to ESX. 2. Apply the profile created from ESXi to the ESX host. 3. Reinstate the restriction preventing the profile from being applied to ESX if desired. 4. Verify the configuration of the ESX host, fixing network configuration directly on the host as necessary. After the ESX host is configured appropriately, create a new host profile from the host. Reattach hosts attached to the old host profile with the new host profile.

Figure 13. Handling Profiles for ESX and ESXi

Users always have the option of keeping ESX and ESXi hosts managed by different host profiles. This is the most straightforward approach, although this might make it more difficult to interchange ESX and ESXi hosts, and in cases where there are mixed clusters of ESX and ESXi.

Figure 14 shows a profile created from ESXi, applicable only to ESXi.

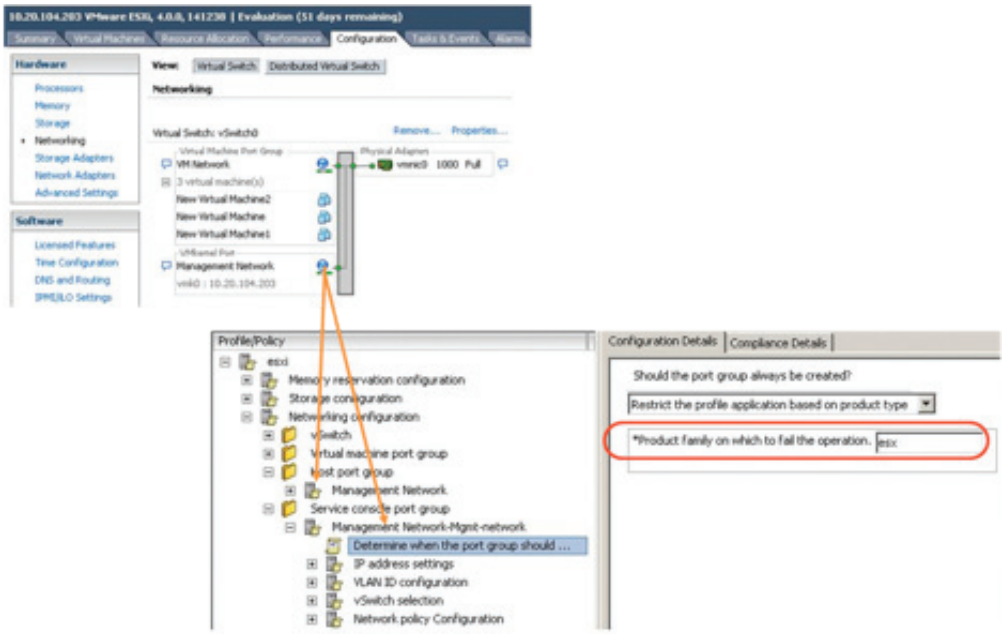


Figure 14. Profile Created from ESXi, Applicable Only to ESXi

Figure 15 shows a profile created from ESX, applicable to both ESX and ESXi.

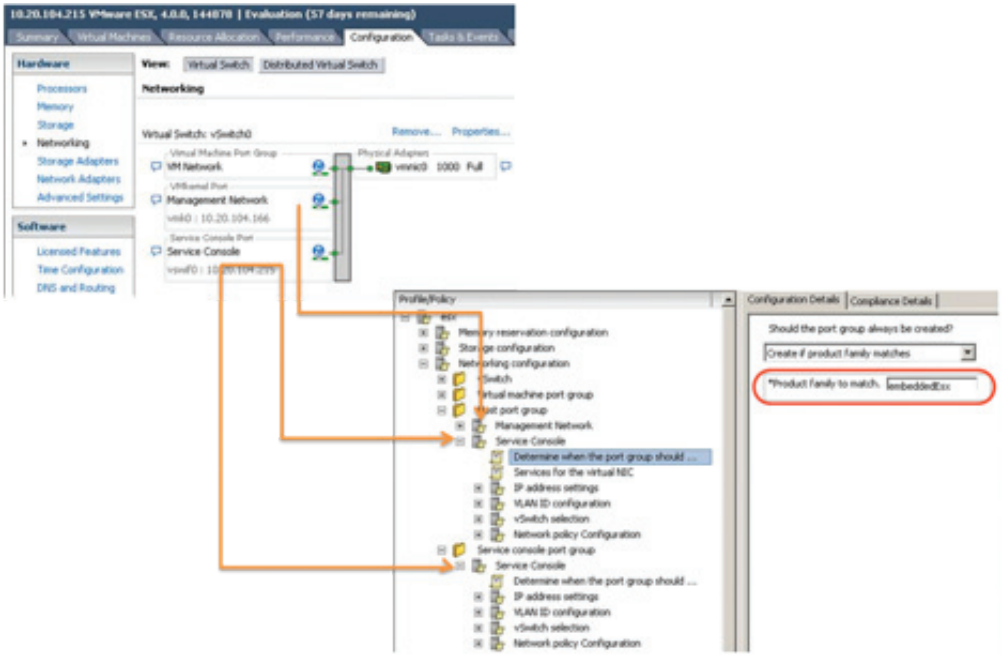


Figure 15. Profile Created from ESX, Applicable to Both ESX and ESXi

VMware vSphere 4.1 PowerCLI Cmdlets for Host Profiles

VMware vSphere PowerCLI provides an easy-to-use Windows PowerShell interface to the vSphere APIs. vSphere PowerCLI contains a number of PowerShell cmdlets that enable you to perform various administration tasks on VMware vSphere components.

The release of vSphere PowerCLI with VMware vSphere 4.1 includes support for Host Profiles cmdlets. Some common tasks for which vSphere PowerCLI can be used to perform with Host Profiles include:

- Create profiles
- Attach profiles
- Check compliance
- Apply profiles
- Export/import profiles
- Delete profiles

For detailed examples and additional information about VMware vSphere PowerCLI cmdlets for Host Profiles, refer to the VMware vSphere PowerCLI documentation.

Troubleshooting

If you are having trouble with Host Profiles, consider the following:

- Verify that all prerequisites are met.
- As a licensed feature of VMware vSphere, Host Profiles is only available when the appropriate licensing is in place. If you see errors, ensure that you have the appropriate VMware vSphere licensing for your hosts.
- Host Profiles will check compliance only for hosts that are powered-on. If you try to check compliance against powered-off hosts in the cluster, you might receive an error message: “an error occurred while communicating with a remote host.”

If you cannot resolve the problem, contact VMware for support.

Summary

Host Profiles greatly simplifies host configuration management and enables centralized compliance monitoring and reporting against desired host configurations. Provisioning is already much simpler in a virtualized environment. With VMware vSphere 4.1, VMware has made it even simpler for VMware ESX/ESXi hosts to be provisioned and configured with Host Profiles — so that adding capacity to your datacenter becomes a trivial, fairly automatic task. With Host Profiles, the time required to set up, change, audit and troubleshoot configurations drops dramatically due to centralized configuration and compliance checking. Host Profiles not only reduces labor costs, but it also minimizes risk of downtime for applications/virtual machines provisioned to misconfigured systems.

Resources

- *vSphere 4.1: ESX/ESXi Configuration Guide*
  http://www.vmware.com/pdf/vsphere4/r41/vsp_41_esx_server_config.pdf
- *VMware vNetwork Distributed Switch: Migration and Configuration*
  http://www.vmware.com/resources/techresources/10050
- *Management of VMware ESXi*
  http://www.vmware.com/resources/techresources/1010
- *VMware Infrastructure 3 Security Hardening*
  http://www.vmware.com/resources/techresources/726
- *Virtual Networking Concepts*
  http://www.vmware.com/resources/techresources/997
- *VMware vSphere PowerCLI*
  http://www.vmware.com/support/developer/windowstoolkit
- *Host Profile API Code Samples*
  http://communities.vmware.com/docs/DOC-10720

Providing Feedback

VMware appreciates your feedback on the material included in this guide. In particular, we would be grateful for any guidance on the following topics:

- How useful was the information in this guide?
- What other specific topics would you like to see covered?
- Overall, how would you rate this guide?

Please send your feedback to tmfeedback@vmware.com, with "VMware Host Profiles: Technical Overview" in the subject line. Thank you for your help in making this guide a valuable resource.

vmware

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