

vSphere Host Profiles

ESXi 5.1
vCenter Server 5.1

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see <http://www.vmware.com/support/pubs>.

EN-000795-00

vmware[®]

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

Copyright © 2009–2012 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

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

Contents

About vSphere [®] Host Profiles	5
1 Using Host Profiles in the vSphere Web Client	7
Host Profiles Usage Model in the vSphere Web Client	7
Access Host Profiles in the vSphere Web Client	8
Create a Host Profile in the vSphere Web Client	8
Attach Entities to a Host Profile in the vSphere Web Client	9
Check Compliance in the vSphere Web Client	9
Remediate a Profile in the vSphere Web Client	9
Edit a Host Profile in the vSphere Web Client	10
Duplicate a Host Profile in the vSphere Web Client	12
Copy Settings from Host in the vSphere Web Client	13
Host Profiles and vSphere Auto Deploy in the vSphere Web Client	13
2 Using Host Profiles in the vSphere Client	15
Host Profiles Usage Model	15
Access Host Profiles View	16
Creating a Host Profile	16
Export a Host Profile	17
Import a Host Profile	18
Clone a Host Profile	18
Edit a Host Profile	18
Manage Profiles	21
Checking Compliance	24
Host Profiles and vSphere Auto Deploy	25
Index	29

About vSphere[®] Host Profiles

The *vSphere Host Profiles* documentation provides information about managing host profiles.

The *vSphere Host Profiles* documentation includes information about the following:

- Creating host profiles
- Exporting and importing a host profile
- Editing host profile policies
- Attaching an entity to a host profile
- Applying a host profile to an entity attached to the host profile
- Checking the host profile's compliance to an entity attached to the host profile
- Viewing and updating host customizations

Intended Audience

The *vSphere Host Profiles* documentation is intended for administrators who are familiar with vSphere host configuration.

Using Host Profiles in the vSphere Web Client

1

The host profiles feature creates a profile that encapsulates the host configuration and helps to manage the host configuration, especially in environments where an administrator manages more than one host or cluster in vCenter Server.

Host profiles eliminates per-host, manual, or UI-based host configuration and maintains configuration consistency and correctness across the datacenter by using host profile policies. These policies capture the blueprint of a known, validated reference host configuration and use this to configure networking, storage, security, and other settings on multiple hosts or clusters. You can then check a host or cluster against a profile's configuration for any deviations.

This chapter includes the following topics:

- [“Host Profiles Usage Model in the vSphere Web Client,”](#) on page 7
- [“Access Host Profiles in the vSphere Web Client,”](#) on page 8
- [“Create a Host Profile in the vSphere Web Client,”](#) on page 8
- [“Attach Entities to a Host Profile in the vSphere Web Client,”](#) on page 9
- [“Check Compliance in the vSphere Web Client,”](#) on page 9
- [“Remediate a Profile in the vSphere Web Client,”](#) on page 9
- [“Edit a Host Profile in the vSphere Web Client,”](#) on page 10
- [“Duplicate a Host Profile in the vSphere Web Client,”](#) on page 12
- [“Copy Settings from Host in the vSphere Web Client,”](#) on page 13
- [“Host Profiles and vSphere Auto Deploy in the vSphere Web Client,”](#) on page 13

Host Profiles Usage Model in the vSphere Web Client

You perform host profiles tasks in a certain workflow order.

You must have an existing vSphere installation with at least one properly configured host.

- 1 Set up and configure the host that will be used as the reference host to extract settings for the host profile.
A reference host is the host from which the profile is created.
- 2 Create a profile using the designated reference host.
- 3 Attach a host or cluster to the profile.
- 4 Check the host's compliance to the reference host's profile. If all hosts are compliant with the reference host, they are correctly configured.
- 5 Apply (remediate) the host profile of the reference host to other hosts or clusters of hosts.

Using host profiles is only supported for VMware vSphere 4.0 hosts or later. This feature is not supported for VMware Infrastructure 3.5 or earlier hosts. If you have VMware Infrastructure 3.5 or earlier hosts managed by your vCenter Server 4.0 or later, the following problems can occur if you try to use host profiles for those hosts:

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

As a licensed feature of vSphere, host profiles are only available when the appropriate licensing is in place. If you see errors, ensure that you have the appropriate vSphere licensing for your hosts.

If you want the host profile to use directory services for authentication, the reference host needs to be configured to use a directory service. See the *vSphere Security* documentation.

vSphere Auto Deploy

For hosts provisioned with vSphere Auto Deploy, vSphere Web Client owns the entire host configuration, which is captured in a host profile. In most cases, the host profile information is sufficient to store all configuration information. Sometimes the user is prompted for input when the host provisioned with Auto Deploy boots. See the *vSphere Installation and Setup* documentation for more information on Auto Deploy.

Access Host Profiles in the vSphere Web Client

The Host Profiles main view lists all available profiles. Administrators can also use the Host Profiles main view to perform operations on host profiles and configure profiles.

Procedure

- 1 From the vSphere Web Client Home, click **Rules and Profiles**.
- 2 Click **Host Profiles**.

Create a Host Profile in the vSphere Web Client

You create a new host profile by extracting the designated reference host's configuration.

NOTE You can also extract a host profile by navigating to the specific host or cluster.

Prerequisites

Verify that you have a vSphere installation and at least one properly configured host in the inventory.

Procedure

- 1 Navigate to the Host profiles view.
- 2 Click the **Extract Profile from a Host** icon (**+**).
- 3 Select the host with the settings that you want to extract for the new host profile and click **Next**.
The selected host must be a valid host.
- 4 Type the name and enter a description for the new profile and click **Next**.
- 5 Review the summary information for the new profile and click **Finish**.

The new profile appears in the profile list.

Attach Entities to a Host Profile in the vSphere Web Client

Before you can remediate the profile to an entity (host or cluster of hosts), you must attach the entity to the profile or the profile to the entity.

When a host profile is attached to a cluster, the host or hosts within that cluster are also attached to the host profile. However, when the host profile is detached from the cluster, the association between the host or host within the cluster and that host profile remains.

Procedure

- 1 In the Host Profiles main view, select the profile to which you want to add the host or cluster from the profile list.
- 2 Click the **Attach/Detach Hosts and clusters to a host profile** icon ().
- 3 Select the host or cluster from the expanded list and click **Attach**.
The host or cluster is added to the Attached Entities list.
- 4 (Optional) Click **Attach All** to attach all listed hosts and clusters to the profile.
- 5 Click **Next**.
- 6 (Optional) You can update or change the user input parameters for the host profiles policies by customizing the host.
See [“Host Profiles and vSphere Auto Deploy in the vSphere Web Client,”](#) on page 13.
- 7 Click **Finish** to complete attaching the host or cluster to the profile.

Check Compliance in the vSphere Web Client

You can check the compliance of a host or cluster to a profile.

Procedure

- 1 Navigate to a host profile.
- 2 Click the **Check Host Profile Compliance** icon (.

In the **Summary** tab, the compliance status is updated as Compliant, Unknown, or Non-compliant.

A non-compliant status indicates inconsistency between the profile and the host. To resolve this, you should remediate the host.

Remediate a Profile in the vSphere Web Client

Remediate a profile to a host to apply the host profile settings onto the host.

Prerequisites

Verify that the profile is attached to the host and the host is in maintenance mode.

Procedure

- 1 Navigate to the profile you want to remediate to the host.
- 2 Select the **Monitor** tab, then click **Compliance**.
- 3 Right-click the host or hosts that you want remediated and select **All vCenter Actions > Host Profiles > Remediate**

- 4 (Optional) You can update or change the user input parameters for the host profiles policies by customizing the host, and click **Next**.

See [“Host Profiles and vSphere Auto Deploy in the vSphere Web Client,”](#) on page 13 for more information about vSphere Auto Deploy.

- 5 Review the tasks that are necessary to remediate the host profile and click **Finish**.

The compliance status is updated.

Edit a Host Profile in the vSphere Web Client

You can view and edit host profile policies, select a policy to be checked for compliance, and change the policy name or description.

Procedure

- 1 Navigate to the host profile that you want to edit and click the **Manage** tab.
- 2 Click **Edit Host Profile**.
- 3 (Optional) Change the profile name and description and click **Next**.
- 4 Make changes to the profile policies.

See [“Edit a Policy in the vSphere Web Client,”](#) on page 10 for detailed instructions for editing a host profile policy. See [“Disable Host Profile Policy in the vSphere Web Client,”](#) on page 12 for detailed instructions on enabling or disabling a policy from compliance check or remediation.

- 5 (Optional) Customize the hosts.

Make any changes to the available configuration values for this profile.

- 6 Click **Finish**.

The changes are made when the "Update host profile" task is completed in the Recent Tasks status. If you attempt to remediate the profile before the task is complete, the profile configuration does not contain the change.

Edit a Policy in the vSphere Web Client

A policy describes how a specific configuration setting should be applied. You can edit policies belonging to a specific host profile.

When you edit the host profile, you can expand the profile's configuration. Each host profile is composed of several subprofiles that are designated by functional group to represent configuration instances. Each subprofile contains many policies and compliance checks that describe the configuration that is relevant to the profile. You can configure certain subprofiles, example policies, and compliance checks.

Each policy consists of one or more options that contains one or more parameters. Each parameter consists of a key and a value. The value can be one of a few basic types, for example integer, string, string array, or integer array.

Table 1-1. Subset of Host Profile Subprofile Configurations

Sub-Profile Configuration	Example Policies and Compliance Checks	Notes
Memory reservation	Set memory reservation to a fixed value.	
Storage	Configure storage options, including Native Multi-Pathing (NMP), Pluggable Storage Architecture (PSA), FCoE and iSCSI adapters, and NFS storage.	<ul style="list-style-type: none"> ■ Use the vSphere CLI to configure or modify the NMP and PSA policies on a reference host first, and then extract the host profile from that host. If you use the Profile Editor to edit the policies, to avoid compliance failures, make sure that you thoroughly understand interrelationships between the NMP and PSA policies and the consequences of changing individual policies. For information on the NMP and PSA, see the <i>vSphere Storage</i> documentation. ■ Setting values for the Initiator IPv6 Address and Initiator IPv6 Prefix options in a host profile with independent hardware iSCSI adapters has no effect on the HBA because no independent iSCSI HBAs have IPv6 support. ■ Add the rules that change device attributes before extracting the host profile from the reference host. After attaching a host to the host profile, if you edit the profile and change the device attributes (for example, mask device paths or adding SATP rules to mark the device as SSD) you are prompted to reboot the host in order to make the changes. However, after rebooting compliance failures occur because the attributes changed. Because Host Profiles extract device attributes before rebooting, if any changes occur after the reboot, it evaluates and finds those changes, and reports it as non-compliant.
Networking	Configure virtual switch, port groups, physical NIC speed, security and NIC teaming policies, vSphere Distributed Switch, and vSphere Distributed Switch uplink port.	When DHCPv6 is enabled in the networking subprofile, the corresponding ruleset must also be manually turned on in the firewall subprofile.
Date and Time	Configure the time settings and timezone of server.	<p>For the time zone, enter a UTC string. For example, "America/Los_Angeles" for United States Pacific time zone.</p> <p>The default time zone is set to the local time and location of the vSphere Client machine.</p> <p>Network Time Protocol (NTP) should be correctly configured. You can configure the NTP settings on the host's configuration tab. Click Time Configuration, then Properties at the top right of the panel.</p>
Firewall	Enable or disable a ruleset.	
Security	Add a user or a usergroup and set the root password.	

Table 1-1. Subset of Host Profile Subprofile Configurations (Continued)

Sub-Profile Configuration	Example Policies and Compliance Checks	Notes
Service	Configure settings for a service.	
Advanced	Modify advanced options.	<ul style="list-style-type: none"> ■ Host Profiles do not check advanced settings if they are the same as the default settings. vCenter Server only copies the advanced configuration settings that have changed and differ from the default values. In addition, compliance checks are limited to only the settings that are copied. ■ Host Profiles does not support the configuration of PCI devices for virtual machine passthrough on the ESXi host.

Other profile configuration categories include: user group, authentication, kernel module, DCUI keyboard, host cache settings, SFCB, resource pools, login banner, SNMP agent, power system, and CIM indication subscriptions.

Procedure

- 1 Edit the host profile.
- 2 Expand a subprofile until you reach the policy to edit.
- 3 Select the policy.
The policy options and parameters are displayed on the right-hand side of the Edit Host Profile window.
- 4 Make any changes to the policy.

Disable Host Profile Policy in the vSphere Web Client

You can decide whether a host profile policy applied or considered during compliance check.

Procedure

- 1 Edit a host profile.
- 2 Expand the host profile policy configuration settings until you reach the desired policy.
- 3 Disable the checkbox next to a policy to remove it from being applied during remediation or considered during a profile compliance check.

NOTE The check box is enabled by default. If you disable the check box so this policy is not checked for compliance or applied during remediation, the other policies that are enabled will still be applied and checked.

Duplicate a Host Profile in the vSphere Web Client

A host profile duplicate is a copy of an existing host profile.

Procedure

- 1 Navigate to the profile that you want to duplicate.
- 2 Click the **Duplicate Host Profile** icon (.
- 3 Type the name and description for the duplicate host profile and click **Next**.
- 4 Review the summary information for the new profile and click **Finish**.

A clone of the profile appears in the Host Profiles list.

Copy Settings from Host in the vSphere Web Client

If the configuration of the host from which a profile was created changes, you can update the local profile so that the local host configuration matches the host's configuration.

After you create a host profile, you can make incremental updates to the profile. You can make updates using two methods:

- Make the configuration changes to a host in the vSphere Web Client, and copy that host's settings to the profile. The settings within the existing profile are updated to match those of the host.
- Update the profile directly by editing the host profile.

Editing the host profile can be comprehensive and provide more options. Copying settings from a host allows you to validate the configuration before rolling it out to other hosts that are attached to the profile.

Procedure

- 1 Navigate to the host profile.
- 2 Click **Copy Settings from Host**.
- 3 Select the host from which you want to copy the configuration settings.
- 4 Click **OK**.

Host Profiles and vSphere Auto Deploy in the vSphere Web Client

You use host profiles to help vSphere Auto Deploy provision physical ESXi hosts with configuration state information (virtual switches, driver settings, boot parameters, and so on).

You cannot store configuration state information directly on a host provisioned with Auto Deploy. Instead, you can create a reference host and configure it with the settings you want. You can create a host profile using this reference host. Auto Deploy can remediate the host profile to these hosts so that they are configured with these settings, or you can remediate the host profile using the client.

To remediate a host profile to a host, you must place the host into maintenance mode. The user is prompted to customize the hosts and enter answers for policies that are specified during host profile creation when the host profile is applied.

NOTE If you deploy ESXi through host profiles, configure syslog to store logs on a remote server. See the instructions to set up Syslog from the host profiles interface in the *vSphere Installation and Setup* documentation.

For more information, see about setting up an Auto Deploy reference host in the vSphere Auto Deploy documentation.

Using Host Profiles in the vSphere Client

2

The host profiles feature creates a profile that encapsulates the host configuration and helps to manage the host configuration, especially in environments where an administrator manages more than one host or cluster in vCenter Server.

Host profiles eliminates per-host, manual, or UI-based host configuration and maintains configuration consistency and correctness across the datacenter by using host profile policies. These policies capture the blueprint of a known, validated reference host configuration and use this to configure networking, storage, security, and other settings on multiple hosts or clusters. You can then check a host or cluster against a profile's configuration for any deviations.

This chapter includes the following topics:

- [“Host Profiles Usage Model,”](#) on page 15
- [“Access Host Profiles View,”](#) on page 16
- [“Creating a Host Profile,”](#) on page 16
- [“Export a Host Profile,”](#) on page 17
- [“Import a Host Profile,”](#) on page 18
- [“Clone a Host Profile,”](#) on page 18
- [“Edit a Host Profile,”](#) on page 18
- [“Manage Profiles,”](#) on page 21
- [“Checking Compliance,”](#) on page 24
- [“Host Profiles and vSphere Auto Deploy,”](#) on page 25

Host Profiles Usage Model

You perform host profiles tasks in a certain workflow order.

You must have an existing vSphere installation with at least one properly configured host.

- 1 Set up and configure the host that will be used as the reference host.
A reference host is the host from which the profile is created.
- 2 Create a profile using the designated reference host.
- 3 Attach a host or cluster to the profile.
- 4 Check the host's compliance to the reference host's profile. If all hosts are compliant with the reference host, they are correctly configured.
- 5 Apply the host profile of the reference host to other hosts or clusters of hosts.

Using host profiles is only supported for VMware vSphere 4.0 hosts or later. This feature is not supported for VMware Infrastructure 3.5 or earlier hosts. If you have VMware Infrastructure 3.5 or earlier hosts managed by your vCenter Server 4.0 or later, the following problems can occur if you try to use host profiles for those hosts:

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

As a licensed feature of vSphere, host profiles are only available when the appropriate licensing is in place. If you see errors, ensure that you have the appropriate vSphere licensing for your hosts.

If you want the host profile to use directory services for authentication, the reference host needs to be configured to use a directory service. See the *vSphere Security* documentation.

Hosts Provisioned with vSphere® Auto Deploy

For hosts provisioned with vSphere Auto Deploy, vCenter Server owns the entire host configuration, which is captured in a host profile. In most cases, the host profile information is sufficient to store all configuration information. Sometimes the user is prompted for input when the host provisioned with Auto Deploy boots. The answer file mechanism manages those cases. See the *vSphere Installation and Setup* documentation.

Access Host Profiles View

The Host Profiles main view lists all available profiles. Administrators can also use the Host Profiles main view to perform operations on host profiles and configure profiles.

The Host Profiles main view should be used by experienced administrators who wish to perform host profile operations and configure advanced options and policies. Most operations such as creating new profiles, attaching entities, and applying profiles can be performed from the Hosts and Clusters view.

Procedure

- ◆ Select **View > Management > Host Profiles**.

Any existing profiles are listed on the left side in the profiles list. When a profile is selected from the profile list, the details of that profile are displayed on the right side.

Creating a Host Profile

You create a new host profile by using the designated reference host's configuration.

A host profile can be created from:

- Host Profile main view
- host's context menu

Create a Host Profile from Host Profiles View

You can create a host profile from the Host Profiles main view using the configuration of an existing host.

Prerequisites

You must have a vSphere installation and at least one properly configured host in the inventory.

Procedure

- 1 In the Host Profiles main view, click **Create Profile**.
The Create Profile wizard appears.
- 2 Select the option to create a new profile and click **Next**.
- 3 Select the host you want to designate as the reference host for the new host profile and click **Next**.
The reference host must be a valid host.
- 4 Type the name and enter a description for the new profile and click **Next**.
- 5 Review the summary information for the new profile and click **Finish** to complete creating the profile.

The new profile appears in the profile list.

Create a Host Profile from Host

You can create a new host profile from the host's context menu in the Hosts and Clusters inventory view.

Prerequisites

You must have a vSphere installation and at least one properly configured host in the inventory.

Procedure

- 1 In the Host and Clusters view, select the host that you want to designate as the reference host for the new host profile.
The host must be a valid host to use as a reference host.
- 2 Right-click the host and select **Host Profile > Create Profile from Host**.
The Create Profile from Host wizard opens.
- 3 Type the name and enter a description for the new profile and click **Next**.
- 4 Review the summary information for the new profile and click **Finish** to complete creating the profile.

The new profile appears in the host's Summary tab.

Export a Host Profile

You can export a profile to a file that is in the VMware profile format (.vpf).

NOTE When a host profile is exported, administrator and user profile passwords are not exported. This is a security measure and stops passwords from being exported in plain text when the profile is exported. You will be prompted to re-enter the values for the password after the profile is imported and the password is applied to a host.

Procedure

- 1 In the Host Profiles view page, select the profile to export from the profile list.
- 2 Right-click the profile and select the **Export Profile**.
- 3 Select the location and type the name of the file to export the profile.
- 4 Click **Save**.

Import a Host Profile

You can import a profile from a file in the VMware profile format (.vpf).

NOTE When a host profile is exported, administrator and user profile passwords are not exported. This is a security measure and stops passwords from being exported in plain text when the profile is exported. You will be prompted to re-enter the values for the password after the profile is imported and the password is applied to a host.

Procedure

- 1 In the Host Profiles main view, click the **Create Profile** icon.
The Create Profile wizard appears.
- 2 Select the option to import a profile and click **Next**.
- 3 Enter or browse the VMware Profile Format file to import and click **Next**.
- 4 Select a valid host you want to designate as the reference host for the imported profile and click **Next**.
- 5 Type the name, enter a description for the imported profile, and click **Next** when finished.
- 6 Review the summary information for the imported profile and click **Finish** to complete importing the profile.

The imported profile appears in the profile list.

Clone a Host Profile

A host profile clone is a copy of an existing host profile.

Procedure

- 1 In the Host Profiles main view, select the profile to clone.
- 2 Click **Clone Profile**.
- 3 A clone of the profile appears in the Host Profiles view.

Edit a Host Profile

You can view and edit host profile policies, select a policy to be checked for compliance, and change the policy name or description.

Procedure

- 1 In the Host Profiles main view, select the profile to edit from the profile list.
- 2 Click **Edit Host Profile**.
- 3 (Optional) Change the profile name or description in the fields at the top of the Profile Editor.
- 4 Edit the policy.
- 5 (Optional) Enable or disable the policy compliance check.
- 6 Click **OK** to close the Profile Editor.

Edit a Policy

A policy describes how a specific configuration setting should be applied. The Profile Editor allows you to edit policies belonging to a specific host profile.

On the left side of the Profile Editor, you can expand the host profile. Each host profile is composed of several subprofiles that are designated by functional group to represent configuration instances. Each subprofile contains many policies and compliance checks that describe the configuration that is relevant to the profile. You can configure certain subprofiles, example policies, and compliance checks.

Each policy consists of one or more options that contains one or more parameters. Each parameter consists of a key and a value. The value can be one of a few basic types, for example integer, string, string array, or integer array.

Table 2-1. Subset of Host Profile Subprofile Configurations

Sub-Profile Configuration	Example Policies and Compliance Checks	Notes
Memory reservation	Set memory reservation to a fixed value.	
Storage	Configure storage options, including Native Multi-Pathing (NMP), Pluggable Storage Architecture (PSA), FCoE and iSCSI adapters, and NFS storage.	<ul style="list-style-type: none"> ■ Use the vSphere CLI to configure or modify the NMP and PSA policies on a reference host first, and then extract the host profile from that host. If you use the Profile Editor to edit the policies, to avoid compliance failures, make sure that you thoroughly understand interrelationships between the NMP and PSA policies and the consequences of changing individual policies. For information on the NMP and PSA, see the <i>vSphere Storage</i> documentation. ■ Setting values for the Initiator IPv6 Address and Initiator IPv6 Prefix options in a host profile with independent hardware iSCSI adapters has no effect on the HBA because no independent iSCSI HBAs have IPv6 support. ■ Add the rules that change device attributes before extracting the host profile from the reference host. After attaching a host to the host profile, if you edit the profile and change the device attributes (for example, mask device paths or adding SATP rules to mark the device as SSD) you are prompted to reboot the host in order to make the changes. However, after rebooting compliance failures occur because the attributes changed. Because Host Profiles extract device attributes before rebooting, if any changes occur after the reboot, it evaluates and finds those changes, and reports it as non-compliant.
Networking	Configure virtual switch, port groups, physical NIC speed, security and NIC teaming policies, vSphere Distributed Switch, and vSphere Distributed Switch uplink port.	When DHCPv6 is enabled in the networking sub-profile, the corresponding ruleset must also be manually turned on in the firewall subprofile.

Table 2-1. Subset of Host Profile Subprofile Configurations (Continued)

Sub-Profile Configuration	Example Policies and Compliance Checks	Notes
Date and Time	Configure the time settings and timezone of server.	<p>For the time zone, enter a UTC string. For example, "America/Los_Angeles" for United States Pacific time zone.</p> <p>The default time zone is set to the local time and location of the vSphere Client machine.</p> <p>Network Time Protocol (NTP) should be correctly configured. You can configure the NTP settings on the host's configuration tab. Click Time Configuration, then Properties at the top right of the panel.</p>
Firewall	Enable or disable a ruleset.	
Security	Add a user or a usergroup and set the root password.	
Service	Configure settings for a service.	
Advanced	Modify advanced options.	<ul style="list-style-type: none"> ■ Host Profiles do not check advanced settings if they are the same as the default settings. vCenter Server only copies the advanced configuration settings that have changed and differ from the default values. In addition, compliance checks are limited to only the settings that are copied. ■ Host Profiles does not support the configuration of PCI devices for virtual machine passthrough on the ESXi host.

Other profile configuration categories include: user group, authentication, kernel module, DCUI keyboard, host cache settings, SFCB, resource pools, login banner, SNMP agent, power system, and CIM indication subscriptions.

Procedure

- 1 Open the Profile Editor for the profile to edit.
- 2 On the left side of the Profile Editor, expand a subprofile until you reach the policy to edit.
- 3 Select the policy.

On the right side of the Profile Editor, the policy options and parameters are displayed on the **Configuration Details** tab.

- 4 Select a policy option from the drop-down menu and set its parameter.
- 5 Click **OK** when you are finished editing the profile.

NOTE The change is made when the "Update host profile" task is completed in the Recent Tasks status. If you attempt to apply the profile before the task is complete, the profile configuration does not contain the change.

- 6 (Optional) If you make a change to a policy, but want to revert back to the default option, click **Revert** and the option is reset.

Enable Compliance Check

You can decide whether a host profile policy is considered during compliance check.

Procedure

- 1 Open the Profile Editor for a profile and navigate to the policy you wish to enable for compliance check.
- 2 On the right side of the Profile Editor, select the **Compliance Details** tab.
- 3 Enable the check box for the policy.

NOTE The check box is enabled by default. If you disable the check box so this policy is not checked for compliance, the other policies that are enabled for compliance check will still be checked.

Manage Profiles

After you create a host profile, you can manage the profile by attaching a profile to a particular host or cluster and then applying that profile to the host or cluster.

You can associate a profile and a host or cluster either by attaching the profile to the host or cluster, or by attaching the host or cluster to the profile. You can then apply the profile to the host or cluster.

NOTE A host profile must have a valid reference host associated with it before you can manage the profile.

Attaching Host or Cluster Entities to a Host Profile

If you want to set up a host to use the same configuration as a reference host, you can attach the host to a profile. You can also attach a cluster to a profile.

Profiles can also be attached to a cluster. In order to be compliant, all hosts within an attached cluster must be configured according to the profile. Hosts are not automatically configured in accordance to the host profile that is attached with the cluster when it is added to the cluster. When a host is added to a cluster that is attached to a profile, the host is automatically attached to the profile.

You can attach a host or cluster to a profile from:

- Host Profiles main view
- Host's context menu
- Cluster's context menu
- Cluster's Profile Compliance tab

Attach Entities from the Host Profiles View

Before you can apply the profile to an entity (host or cluster of hosts), you need to attach the entity to the profile or the profile to the entity.

You can attach a host or cluster to a profile from the Host Profiles main view.

When a host profile is attached to a cluster, the host or hosts within that cluster are also attached to the host profile. However, when the host profile is detached from the cluster, the association between the host or host within the cluster and that host profile remains.

Procedure

- 1 In the Host Profiles main view, select the profile to which you want to add the host or cluster from the profile list.
- 2 Click the **Attach Host/Cluster** icon.

- 3 Select the host or cluster from the expanded list and click **Attach**.
The host or cluster is added to the Attached Entities list.
- 4 Click **OK** to close the dialog.

Attach Profiles from the Host

Before you can apply the profile to a host you need to attach the host to the profile or the profile to the host.

You can attach a profile to a host from the host's context menu in the Hosts and Clusters inventory view.

When a host profile is attached to a cluster, the host or hosts within that cluster are also attached to the host profile. However, when the host profile is detached from the cluster, the association between the host or host within the cluster and that host profile remain.

Procedure

- 1 In the Host and Clusters view, select the host to which you want to attach a profile.
- 2 Right-click the host and select **Host Profile > Manage Profile**.

NOTE If no host profiles exist in your inventory, a dialog appears asking if you want to create and attach the host to this profile.

- 3 In the Attach Profile dialog, select the profile to attach to the host and click **OK**.
The host profile is updated in the **Summary** tab of the host.

Applying Profiles

To bring a host to the desired state as specified in the profile, apply the profile to the host.

You can apply a profile to a host from:

- Host Profiles main view
- Host's context menu
- Cluster's Profile Compliance tab

If the profile is not applied, or configured to what is specified in the profile, it will cause the compliance status for the profile to fail the next time a compliance check is performed. You fix this by applying the profile to the host.

Apply a Profile from the Host Profiles View

You can apply a profile to a host from the Host Profiles main view.

Prerequisites

The profile must be attached to the host and the host must be in maintenance mode before a profile is applied to it.

Procedure

- 1 In the Host Profiles main view, select the profile you want to apply to the host.
- 2 Select the **Hosts and Clusters** tab.
The list of attached hosts are shown under Entity Name.
- 3 Click **Apply Profile**.
In the Profile Editor, you might be prompted to enter the required parameters needed to apply the profile.
- 4 Enter the parameters and click **Next**.

- 5 Continue until all the required parameters are entered.
- 6 Click **Finish**.

Compliance Status is updated.

Apply a Profile from the Host

You can apply a profile to a host from the host's context menu.

Prerequisites

The host must be in maintenance mode before a profile is applied to it.

Procedure

- 1 In the Host and Clusters view, select the host to which you want to apply a profile.
- 2 Right-click the host and select **Host Profile > Apply Profile**.
- 3 In the Profile Editor, enter the parameters and click **Next**.
- 4 Continue until all the required parameters are entered.
- 5 Click **Finish**.

Compliance Status is updated.

Change Reference Host

The reference host configuration is used to create the host profile.

You can perform this task from the Host Profiles main view or from the host's context menu.

Prerequisites

The host profile must already exist.

Procedure

- 1 In the Host Profiles main view, right-click the profile you wish to change the reference host and select **Change Reference Host**.
- 2 Expand the inventory list and select the host you want to use as the new reference host for the profile.
- 3 Click **Update**.

The **Reference Host** is updated.

- 4 Click **OK**.

The Summary tab for the host profile lists the updated reference host.

Manage Profiles from a Cluster

You can create a profile, attach a profile, or update reference hosts from the cluster's context menu.

Procedure

- ◆ In the Hosts and Clusters view, right-click a cluster and select **Host Profile > Manage Profile**. Depending on your host profile setup, one of the following results occurs:

Profile Status and Task	Result
If the cluster is not attached to a host profile and no profile exist in your inventory, create a profile.	a A dialog box opens asking if you would like to create a profile and attach it to the cluster. b If you select Yes , the Create Profile wizard opens.
If the cluster is not attached to a host profile and one or more profiles exist in your inventory, attach a profile.	a The Attach Profile dialog opens. b Select the profile you want to attach to the cluster and click OK .
If the cluster is already attached to a host profile, detach a profile or attach to a different profile.	In the dialog box, click Detach to detach the profile from the cluster or Change to attach a different profile to the cluster.

Updating Profiles From the Reference Host

If the configuration of the host from which a profile was created (the reference host) changes, you can update the local profile so that the local host configuration matches the reference host's configuration.

Once you create a host profile, you might need to make incremental updates to the profile. You can do this using two methods:

- Make the configuration changes to the reference host in the vSphere Client, then update the profile from the reference host. The settings within the existing profile are updated to match those of the reference host.
- Update the profile directly using the Profile Editor.

While updating the profile from the Profile Editor can be more comprehensive and provide more options, updating the profile from the reference host allows you to validate the configuration before rolling it out to other hosts that are attached to the profile.

Updating the profile from the reference host is performed from the Host Profiles main view.

Procedure

- ◆ In the Host Profiles main view, right-click the profile you want to update and select **Update Profile From Reference Host**.

Checking Compliance

Checking compliance ensures that the host or cluster continues to be correctly configured.

After a host or cluster is configured with the reference host profile, a manual change, for example, can occur, making the configuration incorrect. Checking compliance on a regular basis ensures that the host or cluster continues to be correctly configured.

Check Compliance from the Host Profiles View

You can check the compliance of a host or cluster to a profile from the Host Profiles main view.

Procedure

- 1 From the Host Profiles list, select the profile that you want to check.

- 2 In the **Hosts and Clusters** tab, select the host or cluster from the list under Entity Name.
- 3 Click **Check Compliance Now**.

The compliance status is updated as Compliant, Unknown, or Non-compliant.

If the compliance status is Non-compliant, you can apply the the profile to the host.

Check Compliance from Host

After a profile has been attached to a host, run a compliance check from the host's context menu to verify the configuration.

Procedure

- 1 In the Host and Clusters view, select the host on which you want to run the compliance check.
- 2 Right-click the host and select **Host Profile > Check Compliance**

The host's compliance status is displayed in the host's **Summary** tab.

If the host is not compliant, you must apply the profile to the host.

Check Cluster Compliance

A cluster may be checked for compliance with a host profile or for specific cluster requirements and settings.

Procedure

- 1 In the Host and Clusters view, select the cluster on which you want to run the compliance check.
- 2 In the Profile Compliance tab, click **Check Compliance Now** to check the cluster's compliance with both the host profile that is attached to this cluster and the cluster requirements, if any.
 - The cluster is checked for compliance with specific settings for hosts in the cluster, such as DRS, HA, and DPM. For example, it may check if vMotion is enabled. The compliance status for the cluster requirements is updated. This check is performed even if a host profile is not attached to the cluster.
 - If a host profile is attached to the cluster, the cluster is checked for compliance with the host profile. The compliance status for the host profile is updated.
- 3 (Optional) Click **Description** next to the Cluster Requirements for a list of the specific cluster requirements.
- 4 (Optional) Click **Description** next to Host Profiles for a list of the specific host profile compliance checks.
- 5 (Optional) Click **Change** to change the host profile that is attached to the cluster.
- 6 (Optional) Click **Remove** to detach the host profile that is attached to the cluster.

If the cluster is not compliant, the profile must be applied separately to each host within the cluster.

Host Profiles and vSphere Auto Deploy

Host profiles are used to help vSphere Auto Deploy provision physical ESXi hosts with configuration state information (virtual switches, driver settings, boot parameters, and so on).

Configuration state information cannot be stored directly on a host provisioned with Auto Deploy. Instead, you can create a reference host and configure it with the settings you want. Then, create a host profile using this reference host. Auto Deploy can apply the host profile to these hosts so they are configured with these settings, or you can apply the host profile using the client.

To apply a host profile to a host, the host must be placed into maintenance mode. The user is prompted to type answers for policies that are specified during host profile creation when the host profile is applied.

A host provisioned with Auto Deploy can be rebooted while the host profile is attached to the host. After rebooting, values stored in the answer file help the host provisioned with Auto Deploy to apply the profile. An answer file is created that contains a series of key value pairs for the user input options.

The answer file contains the user input policies for a host profile. The file is created when the profile is initially applied to a particular host.

NOTE If you deploy ESXi through host profiles, configure syslog to store logs on a remote server. See "Set up Syslog from the Host Profiles Interface" in the *Installation and Setup* documentation for instructions.

See "Setting up an Auto Deploy Reference Host" in the vSphere Auto Deploy documentation for more information.

Check Answer File Status

The answer file status indicates the state of the answer file. The status of an answer file can be complete, incomplete, missing, or unknown.

Prerequisites

The answer file status can only be checked when the host profile is attached to a host.

Procedure

- ◆ In the host profiles view, click **Check Answer File**.

The Answer File Status for the host profile is updated. The status indicates one of the following states:

Incomplete	The answer file is missing some of the required user input answers.
Complete	The answer file has all of the user input answers needed.
Unknown	The host and associated profile exist but the status of the answer file is not known. This is the initial state of an answer file.

Update Answer File

You can update or change the user input parameters for the host profiles policies in the answer file.

Procedure

- 1 Right-click the host entity and select **Update Answer File**.
- 2 When prompted, enter or change the user input parameter, and click **Next**.
- 3 Click **Update** when finished entering changes.

Import Answer File

You can import a previously exported answer file to associate with a host profile.

Prerequisites

The imported answer file must be associated with at least one host.

Procedure

- 1 Right-click the host entity and select **Import Answer File**.
- 2 Select the answer file to import.

Export Answer File

You can export an answer file so that it can be imported and used by another host profile.

The answer file might contain sensitive information such as passwords and IP addresses. If exported, this information is vulnerable to unauthorized access. During the export process all passwords are removed from the answer file. When the answer file is imported, the password information must be re-entered.

Procedure

- 1 Right-click the host entity and select **Export Answer File**.
- 2 Select the location to save the answer file.

Index

A

answer file, update **26**
Auto Deploy **13, 25**

C

clusters, managing profiles from **24**
compliance checks, host profiles **12, 21**
creating, host profiles **8, 16, 17**

D

disabling, host profile policy **12**

E

editing
 host profile policies **10, 19**
 host profiles **10, 18**
enabling, host profile policy compliance checks **21**
exporting, host profiles **17**

H

host, reference **23**
host profile, attaching entities **21**
host profiles
 accessing **8, 16**
 applying profiles **22, 23**
 attaching entities from host **22**
 attaching entities from Host Profile view **21**
 attaching hosts or clusters to a host profile **9**
 checking compliance **9, 24, 25**
 creating **16**
 creating from host **17**
 creating from host profile view **8, 16**
 disabling policy **12**
 editing a policy **10, 19**
 editing profiles **10, 18**
 enabling policy compliance checks **21**
 exporting **17**
 importing profiles **18**
 managing profiles **21**
 remediate profiles **9**
 updating from reference host **13, 24**
 usage model **7, 15**
host profiles, cloning profiles **18**
host profiles, duplicating profiles **12**
host profiles,import answer file **26**

I

importing host profile **18**

P

profiles, managing **24**

R

reference host **23**

U

using host profiles **7**

