vSphere Host Profiles

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.

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

Contents

About vSphere® Host Profiles

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

The *vSphere Host Profiles* documentation describes how to perform the following:

- Create Host Profiles

- Export and import a Host Profile

- Edit Host Profile policies

- Attach an entity to a Host Profile

- Apply a Host Profile to an entity attached to the Host Profile

- Check the Host Profile's compliance to an entity attached to the Host Profile

- View and update host customizations

Intended Audience

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

Updated Information

This *vSphere Host Profiles* is updated with each release of the product or when necessary.

This table provides the update history of the *vSphere Host Profiles*.

Revision	Description
EN-001347-02	Fixed incomplete sentence in "Edit a Policy in the vSphere Web Client," on page 13.
EN-001347-01	Corrected typo in "Host Profiles and vSphere Auto Deploy in the vSphere Web Client," on page 16 .
EN-001347-00	Initial release.

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 multiple hosts or clusters in vCenter Server.

Host Profiles provide an automated and centrally-managed mechanism for host configuration and configuration compliance. Host Profiles can improve efficiency by reducing reliance upon repetitive, manual tasks. Host Profiles capture the configuration of a pre-configured and validated reference host, store the configuration as a managed object and use the catalog of parameters contained within to configure networking, storage, security and other host-level parameters. Host Profiles can be applied to either individual hosts or to a cluster; applying a Host Profile to a cluster will affect all hosts in the cluster and result in a consistent configuration across all hosts in that cluster.

Host Profiles can be used to validate the configuration of a host by checking compliance of a host or cluster against the Host Profile that is associated with that host or cluster.

This chapter includes the following topics:

Host Profiles Usage Model in the vSphere Web Client

The Host Profile workflow starts with the concept of a reference host; the reference host serves as the template from which the Host Profile is extracted. The designation reference host, and the Host Profile association to that host, persists even after creating the Host Profile. The reference host must be both healthy and available for subsequent usage of the Host Profile.

Before you begin, ensure that you have an existing vSphere enviroment installation with at least one properly and completely configured host.

The sequence required to create a Host Profile from a reference host, apply the Host Profile to a host or cluster and check compliance against the Host Profile is as follows:

1 Set up and configure the reference host.

2 Create a Host Profile from the reference host.

3 Attach other hosts or clusters to the Host Profile.

4 Check the compliance to the Host Profile. If all hosts are compliant with the reference host, they are correctly configured.

5 Apply (remediate).

Host Profiles is supported only for hosts running VMware vSphere 4.0 or later. This feature is not supported for VMware Infrastructure 3.5 or earlier hosts. If you have hosts running VMware Infrastructure 3.5 or earlier, you may attach a Host Profile to these hosts, but remediateion and compliance check will always fail. Additionally, a host that is running VMware Infrastructure 3.5 or earlier cannot be used as a reference host.

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 profie by navigating to the specific host or cluster.

Prerequisites

Verify that you have a working vSphere installation and at least one completely and properly configured host that will act as the reference host.

Procedure

1   Navigate to the Host profiles view.

2   Click the **Extract Profile from a Host** icon (✚).

3   Select the host that will act as the reference host 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

After creating a Host Profile from a reference host, you must attach the host or cluster to the Host Profile.

Prerequisites

The Host Profile must already be extracted from a reference host that is healthy and available.

Procedure

1   From the Profile List in the Host Profiles main view, select the Host Profile to be applied to a host or cluster.

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 16.

7   Click **Finish** to complete attaching the host or cluster to the profile.

Detach Entities From a Host Profile

In order to remove the policy-managed configuration from a host or cluster, that host or cluster must be detached from the Host Profile.

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   From the Profile List in the Host Profiles main view, select the Host Profile to be detached from a host or cluster.

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 **Detach**.

The host or cluster is added to the Attached Entities list.

4   (Optional) Click **Detach All** to detach all listed hosts and clusters from the profile.

5   Click **Next**.

6   Click **Finish** to complete attaching the host or cluster to the profile.

Check Compliance in the vSphere Web Client

You can confirm the compliance of a host or cluster to its attached Host Profile and determine which, if any, configuration parameters on a host are different from those specified in the Host Profile.

Procedure

1   Navigate to a Host Profile.

The **Objects** tab lists all Host Profies, the number or hosts attached to that Host Profile, and summarized results of the last compliance check.

2   Click the **Check Host Profile Compliance** icon (🔴).

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

A non-compliant status indicates a discovered and specific inconsistency between the profile and the host. To resolve this, you should remediate the host. And unknown status indicates that the compliance of the host could not be verified; to resolve the issue, remediate the host through the Host Profile.

What to do next

To see more detail on compliance failures, select a Host Profile from the **Objects** tab for which the last compliance check produced one or more failures. In order to see specific detail on which parameters differ between the host that failed compliance and the Host Profile, click on the **Monitor** tab and select the Compliance view. Then, expand the object hierarchy and select the failing host. The differing parametersare displayed in the Compliance window, below the hierarchy.

Remediate a Host in the vSphere Web Client

In the event of a compliance failure, use the Remediate function to apply the Host Profile settings onto the host. This action changes all Host Profile managed parameters to the values contained in the Host Profile attached to the host.

Prerequisites

Verify that the profile is attached to the host and the host is in maintenance mode. Since some changes can impact host operation or resource availability, a host must be in maintenance mode to remediate. This ensures that no virtual machines are impacted by any host-level parameter changes.

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 16 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 13 for detailed instructions for editing a Host Profile policy. See "Disable Host Profile Component in the vSphere Web Client," on page 15 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 is applied. You can edit policies belonging to a specific Host Profile.

When you edit the Host Profile, you can expand the Host Profile's configuration hierarchy to see the sub-profile components that comprise the Host Profile. These components are categorized by functional group or resource class to make it easier to find a particular parameter. Each subprofile component contains one or more attributes and parameters, along with the 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

Subprofile 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.	■ Use the vSphere CLI to configure or modify the NMP and PSA policies on a reference host, 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 understand interrelationships between the NMP and PSA policies and the consequences of changing individual policies. For information about the NMP and PSA, see the *vSphere Storage* 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 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 noncompliant.
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, manually turn on the corresponding ruleset in the firewall subprofile.
Date and Time	Configure the time settings and timezone of server.	For the time zone, enter a UTC string. For example, "America/Los_Angeles" for United States Pacific time zone. The default time zone is set to the local time and location of the vSphere Web Client machine. Configure Network Time Protocol (NTP) correctly. You can configure the NTP settings on the host's Configuration tab. Click **Time Configuration**, and then click **Properties** at the top right of the panel.
Firewall	Enable or disable a ruleset.	
Security	Add a user or a user group and set the root password.	

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

Subprofile Configuration	Example Policies and Compliance Checks	Notes
Service	Configure settings for a service.	
Advanced	Modify advanced options.	■ Host Profiles do not check advanced settings if they are the same as the default settings. vCenter Server copies only the advanced configuration settings that have changed and that differ from the default values. In addition, compliance checks are limited to 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 appear on the right side of the Edit Host Profile window.

4   Make changes to the policy.

Disable Host Profile Component in the vSphere Web Client

You can decide whether a Host Profile component is applied or considered during compliance check. This allows administrators to eliminate non-critical attributes from consideration or ignore values that, while part of the Host Profile, are likely to vary between hosts.

Procedure

1   Edit a Host Profile.

2   Expand the Host Profile Component hierarchy until you reach the desired component or component element.

3   Disable the checkbox next to a component 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 component or component element 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 reference host changes, you can update the Host Profile so that it matches the reference host's new configuration.

After you create a Host Profile, you can make incremental updates to the profile. When making changes to a Host Profile, consider the benefits and limitations of the 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. This method allows you to validate the configuration on a single host before rolling it to the other hosts that are attached to the profile.

■   Update the profile directly by editing the Host Profile. This provides the ability to do more comprehensive and immediate remediation of those changes.

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

Host Profiles works with vSphere Auto Deploy to provision physical ESXi hosts have a complete and expected configuration state for virtual switches, driver settings, boot parameters, and so on.

Because hosts that are provisioned with Auto Deploy are considered to be stateless, configuration state information is not stored on the host. Instead, create a reference host and configure it completely with the settings you want. Then, create a Host Profile from this reference host. Next, associate the Host Profile with a new deploy rule using the Auto Deploy rules engine through the PowerCLI. Now, as new hosts are provisioned through Auto Deploy, they will automatically have the Host Profile applied

Remediation for these hosts is the same as statefully deployed hosts; that is, you must place the host into maintenance mode and perform the remediation task. 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 Auto Deploy, 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.

Import a Host Profile in the vSphere Web Client

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

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   Navigate to the Host Profiles view.

2   Click the Import Host Profile icon ( ).

3   Click **Browse** to browse for the VMware Profile Format file to import

4   Enter the **Name** and **Description** for the imported Host Profile, and click **OK**.

The imported profile appears in the profile list.

Export a Host Profile in the vSphere Web Client

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

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   Navigate to the Host Profile you want to export.

2   Right-click the profile and select **All vCenter Actions > Export Host Profile**.

3   Select the location and type the name of the file to export the profile.

4   Click **Save**.

Index