vSphere Host Profiles

Update 1
VMware vSphere 6.0
VMware ESXi 6.0
vCenter Server 6.0

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.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
14 FEB 2018	Minor changes.
04 SEP 2017	Corrected information about setting the **Is Shared Clusterwide** in Configure Storage Host Profiles.
EN-001800-03	Corrected information about configuring time settings in Edit a Policy.
EN-001800-02	Added a note in Chapter 1 Using Host Profiles that states host profiles extracted from ESXi 6.0 hosts are not compatible with ESXi 5.5 or earlier hosts.
EN-001800-01	Added Reference Host Independence to describe the reference host independence feature.
EN-001800-00	Initial release.

Using Host Profiles

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.

Note After upgrading to vSphere 6.0, host profiles previously extracted from ESXi 5.5 hosts should function. However, host profiles extracted from ESXi 6.0 hosts are not compatible with ESXi 5.5 or earlier hosts.

This chapter includes the following topics:

- Host Profiles Usage Model
- Reference Host Independence
- Access Host Profiles
- Create a Host Profile
- Attach Entities to a Host Profile
- Detach Entities From a Host Profile
- Check Compliance
- Remediate a Host
- Edit a Host Profile
- Duplicate a Host Profile
- Copy Settings from Host

- Host Profiles and vSphere Auto Deploy
- Import a Host Profile
- Export a Host Profile

Host Profiles Usage Model

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.

Before you begin, ensure that you have an existing vSphere environment 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).

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.

Reference Host Independence

A dedicated reference host is not required to be available to perform host profile tasks.

When you create a host profile, you extract the configuration information from a specified ESXi reference host. In previous releases, vSphere required that the reference host be available for certain Host Profiles tasks, such as editing, importing, and exporting. In vSphere 6.0, a dedicated reference host is no longer required to be available to perform these tasks.

For host profile tasks that require a reference host, an ESXi host that is compatible to the host profile is assigned as the role of reference host.

In some cases, a compatible host is not available to validate the host profile during these tasks. If you made small changes to the host profile that do not require validation, you can choose to skip the validation. If you choose to skip the host validation, a warning displays indicating that no valid reference host is associated with the profile. You can then proceed and complete the task.

Due to the introduction of this feature, users can no longer edit or change the reference host from the vSphere Web Client. The reference host selection occurs at runtime, without notifying users, in the vCenter Server for on-going tasks.

Access Host Profiles

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 **Policies and Profiles**.

2   Click **Host Profiles**.

Create a Host Profile

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 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.

Note   Host profiles do not capture offline or unpresented devices. Any changes made to offline devices after extracting a host profile will not make a difference to the compliance check results.

Attach Entities to a Host Profile

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

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.

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

Detach Entities From a Host Profile

In order to disassociate a 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 detaching the host or cluster to the profile.

Check Compliance

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 Profiles, 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.

Note   Host profiles do not capture offline or unpresented devices. Any changes made to offline devices after extracting a host profile will not make a difference to the compliance check results.

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 parameters are displayed in the Compliance window, below the hierarchy.

Remediate a Host

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.

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 **Host Profiles > Remediate**

> **Note** Certain Host Profile policy configurations require that the host be rebooted after remediation. In those cases, you are prompted to place the host into maintenance mode.

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 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

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 for detailed instructions for editing a Host Profile policy. See Disable Host Profile Component 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

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.

Note Currently, there is no way to remove or replace policy options policies, or sub-profiles that are deprecated in this release. Metadata is added to these deprecated policies that allows old host profiles to continue working but will extract new host profiles with only non-deprecated parts of a host profile.

Table 1-1. Subset of Host Profile Subprofile Configurations

Component Categories	Configuration Settings	Notes and Examples
Advanced Configuration Settings	Advanced Options, Agent VM , DirectPath I/O , Hosts file, Power Ssytem, System Image Cache	■ 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.
CIM Indication Subscriptions	CIM-XML Indication Subscriptions	
General System Settings	Console, Core Dump, Device Alias, Host Cache, Kernel Module, Management Agent, System Resource Pool, System Swap, vFlash Host Swap Cache	For Date and Time Configuration: ■ 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 **Manage** tab. Click **Settings** then **Time Configuration** (under System). Click **Edit** to configure the time settings .
Networking	vSwitch, 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.

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

Component Categories	Configuration Settings	Notes and Examples
Security	Firewall, Security Settings, Service	
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. ■ 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.

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.

Configure Storage Host Profiles

When you use storage devices that are not shared across a cluster, but that the vSphere storage stack cannot detect as local, compliance failures might occur when you apply a host profile.

To resolve the compliance failures caused by using unshared storage devices, use the upgraded Pluggable Storage Architecture (PSA) and Native Multipathing Plug-In host profile policies.

Note ESXi diagnostic data that you obtain by running the `vm-support` command contains host profiles information which includes storage host profiles, PSA, NMP, and Virtual Volumes data. No sensitive information, such as passwords, is collected.

Prerequisites

Extract a host profile from a reference host. See Create a Host Profile for instructions.

Procedure

1   For SAS devices that are not detected as local, select **Storage configuration > Pluggable Storage Architecture configuration > PSA device sharing > *name of device***.

2   For each device not shared across the cluster, disable **Device is shared clusterwide**.

    The **Is Shared Clusterwide** value for PSA devices helps you determine which devices in the cluster should be configured by a host profile. Correctly setting this value for devices in the cluster eliminates compliance errors due to non-shared devices.

    By default, this value is populated to reflect the **Is Local** setting for the device. For example, a device with **Is Local** set to **True**, this setting is disabled by default. This setting allows storage host profiles to ignore these devices during compliance checks.

    You can find the Is Local setting for the device by running the command `esxcli storage core device list` in the ESXi Shell. For more information on this command and identifying disks or LUNs, see http://kb.vmware.com/kb/1014953.

3   For SAN boot LUN devices shared across the cluster but logically local to the host, disable the **Is Shared Clusterwide** on the reference host. You must set the value to *False* before extracting the host profile from the reference host. When applying the host profile to the target host, the boot device settings for the remote boot LUN device are copied from the reference host into the target host. Select **Storage configuration > Pluggable Storage Architecture configuration > Host boot device configuration** and verify that this LUN is correctly captured.

4   Remediate the profile to the reference host for the changes in the sharing state to take effect on the reference host.

    If you must re-extract the profile (for example, if you attach more shared SAN boot LUNs to your cluster), you do not need to reconfigure sharing for devices that you previously configured.

Disable Host Profile Component

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

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

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

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. 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

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

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 **Export Host Profile**.

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

4   Click **Save**.