| Figure 1-1 | HTA in a virtual infrastructure | 10 |
| Figure 2-1 | Network topology utilizing Mapped Mode | 14 |
| Figure 2-2 | Network topology utilizing Router Mode | 15 |
| Figure 3-1 | Deploying the OVF template | 18 |
| Figure 3-2 | Static IP Address configuration | 20 |
| Figure 3-3 | HTA Management Console login screen | 21 |
| Figure 3-4 | HTA End-User License Agreement | 22 |
| Figure 3-5 | HTA license installation | 22 |
| Figure 4-1 | HTA Installation Wizard - HTA Host Configuration | 25 |
| Figure 4-2 | HTA Installation Wizard - Network Configuration | 26 |
| Figure 4-3 | HTA Installation Wizard - Finish | 26 |
| Figure 4-4 | HTA Management Console Appliance Dashboard | 27 |
| Figure 5-1 | HTA Installation Wizard - HTA Host Configuration | 29 |
| Figure 5-2 | HTA Installation Wizard - Network Configuration | 30 |
| Figure 5-3 | HTA Installation Wizard - Finish | 31 |
| Figure 5-4 | HTA Management Console Appliance Dashboard | 32 |
| Figure 6-1 | Compliance > Hosts page | 35 |
| Figure 6-2 | Add Host Wizard - Host Login page | 35 |
| Figure 6-3 | Host Login page - Advanced Properties section | 36 |
| Figure 6-4 | Add Host Wizard - Host Details page | 36 |
| Figure 6-5 | Add Host Wizard - Advanced page (ESXi host) | 37 |
| Figure 6-6 | Add Host Wizard - Published IP page | 38 |
| Figure 6-7 | Add Host Wizard - Complete Host Add page | 39 |
| Figure 6-8 | Compliance > Hosts page with added hosts | 39 |
| Figure 6-9 | Compliance > Hosts > Edit Host page - General tab | 40 |
| Figure 6-10 | Compliance > Hosts > Edit Host page - Advanced tab | 41 |
| Figure 6-11 | Compliance > Hosts > Edit Host page - Published IP tab | 41 |
| Figure 6-12 | Compliance > Hosts page with protected hosts | 42 |
| Figure 6-13 | Edit Host (Multiple Hosts) page - General tab | 43 |
| Figure 6-14 | Edit Host (Multiple Hosts) page - Advanced tab | 43 |
| Figure 6-15 | Compliance > Hosts page | 44 |
| Figure 6-16 | Compliance > Hosts page | 44 |
| Figure 6-17 | Add Host Wizard - Host Login page | 45 |
| Figure 6-18 | Add Host Wizard - Host Details page (Nexus) | 45 |
| Figure 6-19 | Add Host Wizard - Published IP page | 46 |
| Figure 6-20 | Add Host Wizard - Complete Host Add page | 47 |
| Figure 6-21 | Compliance > Hosts page with added Nexus host | 47 |
| Figure 6-22 | Compliance > Hosts page | 48 |
| Figure 6-23 | Add Host Wizard - Host Login page | 48 |
| Figure 6-24 | Add Host Wizard - Host Details page (UCS) | 49 |
| Figure 6-25 | Add Host Wizard - Published IP page | 50 |
| Figure 6-26 | Add Host Wizard - Complete Host Add page | 50 |
| Figure 6-27 | Compliance > Hosts page with added UCS Manager host | 51 |
List of Figures

Figure 6-29  HTA-protected virtual infrastructure ................................................................................ 51
Figure 7-1  HTA high availability configuration .................................................................................. 54
Figure B-1  Windows Server 2008 Firewall with Advanced Security Inbound Rules ....................... 66
The HyTrust Appliance (HTA) provides a centralized point of control for hypervisor configuration, compliance, and access management.

This guide describes how to prepare and deploy the HyTrust Appliance (HTA) virtual machine on an ESX or ESXi host.

This guide does not discuss configuration of the HTA. See the HyTrust Appliance Administration Guide for more information.

Audience

This guide is intended for information technology personnel who are reasonably proficient in the following areas:

- Using VMware vSphere, including the ability to install a virtual appliance and configure virtual networks.
- Networking and route configuration.

Document Organization

This guide is organized into the following sections:

- Chapter 1, Installation Overview—Provides an overview of the process required to install the HTA.
- Chapter 2, Selecting the Deployment Architecture—Provides information on the different network deployments supported by the HTA.
- Chapter 3, Installing the Appliance—Describes how to perform the various tasks involved with installing the HTA.
- Chapter 4, Mapped Mode—Provides details on how to configure the HTA for Mapped Mode.
- Chapter 5, Router Mode—Provides details on how to configure the HTA for Router Mode.
- Chapter 6, Post-Installation Tasks—Provides steps on how to verify your HTA network configuration and add an HTA-protected host.
- Chapter 7, High Availability—Describes how to setup and configure two HTAs for high availability.
- Appendix A, Resource Tables and Checklists—Provides various worksheets to use when planning and installing the HTA.
- Appendix B, Configuring the Windows Server 2008 Firewall—Describes how to configure the Windows Server 2008 Firewall for use with the HTA.
- Appendix C, Network Access Requirements—Provides network protocol and port requirements for the HTA.
Document Conventions

The table below summarizes the call-outs and icons used in this guide.

**Call-outs and Icons**

<table>
<thead>
<tr>
<th>Call-out or Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note:</td>
<td>Indicates supporting information to the document text.</td>
</tr>
<tr>
<td>IMPORTANT:</td>
<td>Provides important information that should be highly considered.</td>
</tr>
</tbody>
</table>

The table below summarizes the typographical conventions used in this guide.

**Typographical conventions**

<table>
<thead>
<tr>
<th>Style</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bold</td>
<td>Menu items.</td>
</tr>
<tr>
<td>Italic</td>
<td>Provides emphasis and identifies user interface items and document titles.</td>
</tr>
<tr>
<td>Monospace</td>
<td>Command names, console text, and file names.</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Contains information for which you must supply a value.</td>
</tr>
<tr>
<td></td>
<td>Separates a set of choices from which only one may be chosen.</td>
</tr>
<tr>
<td>( )</td>
<td>Required command parameters that must be specified.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Optional command parameters.</td>
</tr>
</tbody>
</table>

Related References

For more information about the HTA refer to the following resources:

- HyTrust website: [http://www.hytrust.com](http://www.hytrust.com)
- The *HyTrust Appliance Administration Guide*

Contacting HyTrust

If you require additional information or technical support, contact us at:

Phone: (650) 681-8100
Email: info@hytrust.com
Website: [http://www.hytrust.com](http://www.hytrust.com)
CHAPTER

Installation Overview

This chapter contains the following sections:

- Introduction
- System Requirements
- Appliance Installation Overview
- Obtaining the Software

Introduction

Note: All references to hosts or ESX hosts refer to both ESX and ESXi hosts. Other host types which the HTA supports are vSphere vCenter Server, Cisco Nexus 1000V Virtual Supervisor Module (VSM), Cisco Unified Computing System (UCS) Manager, and Cisco Nexus 5000 and 7000 series switches.

The HyTrust Appliance (HTA) offers system managers and administrators an end-to-end virtualization security platform to manage access, standardize and control configuration, and protect a virtual infrastructure within a customer's environment. The HTA is designed to fit easily within the configuration and architecture of most data centers and is installed as a virtual appliance.
The following illustration shows the basic operations of the HTA in a virtual infrastructure environment.

![HTA in a virtual infrastructure](image)

**Figure 1-1**  **HTA in a virtual infrastructure**

The HTA allows corporate users who need to perform management operations on virtual machines and underlying infrastructure to do so using their current identity as defined in a user directory service such as Microsoft Active Directory. With the HTA, users can also continue using the same management client software and other agent programs to which they are accustomed, such as VMware vSphere Client, an SSH client, and web browser applications.

The HTA provides consistent authentication of users across multiple access methods and provides rich authorization and entitlement controls. It also provides a central point for security and compliance administration, policy enforcement, and logging for all accesses and changes made to the virtual infrastructure. HTA administrators can define access control policies based on user roles within an organization and the individual virtual objects (including virtual machines, networks, and storage) and server hosts that users need to access in the course of doing their daily work.

One of the huge benefits of virtualization is the compression of multiple physical layers of systems into a much more manageable, single, logical system. Rather than having physically separated servers and network switches, for example, all of that hardware gets flattened down into a logical representation, making it far easier to perform tasks like backup, disaster recovery, etc. This comes with risk as previously physical components are now logical applications or services running on the host, making it easier to disrupt operations, inadvertently or on purpose. For example, a simple right-click of the mouse on the virtual switch brings up a dialog box to power down the device—presenting a significant risk to organizations that rely on these virtual machines to run core infrastructure including switches, firewalls, mail servers, directory servers, etc.

The HTA can eliminate these risks by providing strict access control over which individual or role is allowed to access the virtual infrastructure, and whether they can make changes. The HTA can granularly determine on a command-by-command basis what tasks each individual is entitled to perform, eliminating the possibility that an individual can shut down pieces of the infrastructure without express permissions.
Additionally, the HTA automatically configures VMware ESX hosts to match customer-defined templates and continually monitors the protected virtual infrastructure to ensure that the ESX host configurations continue to match the defined templates—eliminating guesswork and saving time for the users charged with maintaining the virtual infrastructure.

The combination of centralized access control and policies, configuration management, and logging all help to make the HTA a great security and compliance solution for customers. In addition to protecting vCenter Servers and ESX hosts, the HTA also provides protection for the Cisco Nexus 1000V distributed virtual switch (DVS) and Cisco Nexus 5000 and 7000 series switches, and Cisco UCS Manager.

### System Requirements

The ESX host and HyTrust Appliance (HTA) virtual machine requirements depend on the specific load of a protected virtual environment; however, the minimum requirements are as follows:

<table>
<thead>
<tr>
<th>Table 1-1</th>
<th>HTA Minimum System Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource</td>
<td>Minimum Requirement</td>
</tr>
<tr>
<td>Disk Space</td>
<td>30 GB</td>
</tr>
<tr>
<td>Memory</td>
<td>4 GB</td>
</tr>
<tr>
<td>Virtual CPUs</td>
<td>2</td>
</tr>
<tr>
<td>Network</td>
<td>1 physical network interface</td>
</tr>
</tbody>
</table>

In addition to the above requirements, the following are also needed:

- Firefox v3.6+ or Internet Explorer v7+ web browser for display and operation of the HTA Management Console.
- The HTA is a 64-bit virtual appliance, so the server hardware running the VMware ESX on which the HTA is installed must be capable of running 64-bit virtual machines; a 64-bit CPU is required. For Intel CPUs, virtualization acceleration (VT) needs to be enabled in the BIOS.

The HTA is delivered in the Open Virtualization Format (OVF) via a single `.ovf` file that has the appliance description and two virtual machine disk (VMDK) files that contain the appliance software.

**Note:** The HTA is currently compatible with the Enterprise Editions of VMware vSphere 4.0 and above. This includes both ESX and ESXi hosts, and vCenter Server. The HTA also supports and protects Cisco Nexus 1000V VSM, Cisco UCS Manager, and Cisco Nexus 5000 and 7000 series switches.

### Appliance Installation Overview

The following steps provide an overview of the process required to install and configure a virtual HTA:

1. Review the ESX host and other system and environment prerequisites for installing and using an HTA—see System Requirements on page 11.
2. Configure your network infrastructure to support any required VLANs and a physical network topology, or requisition an additional block of IP addresses for Mapped Mode. (Decide on the network configuration you plan to use and configure accordingly—see Chapter 2, Selecting the Deployment Architecture.)

3. For production environments, set up a Microsoft Active Directory (AD) to perform authentication of Administrators and their group information for HTA rules. (Refer to the *HyTrust Appliance Administration Guide* for AD configuration information.)

4. Deploy the HTA as a VMware vSphere virtual machine—see Deploying the OVF Template on page 17. Confirm that the network adapter(s) are properly configured and connected.

5. After editing the necessary settings, power on the HTA virtual machine—see Powering Up the Appliance on page 19.

6. Log into the HTA command line interface (CLI) as ascadminuser and type setup to start the setup process and assign an IP address to the HTA virtual machine—see Configuring the HTA Management Network Interface on page 19.

7. Start the HTA Management Console and run the Install Wizard—see Starting the HTA Management Console on page 20.

8. Optionally, set up the HTA vCenter Server Plugin which allows you to perform HTA operations directly from a vSphere Client accessing a vCenter Server. (Refer to the *HyTrust Appliance Administration Guide* for further details.) You can still use the HTA Management Console.

9. Add vCenter Servers, ESX hosts, Cisco Nexus 1000V switches, a Cisco UCS Manager, and Cisco Nexus 5000 and 7000 series switches which the HTA is to manage and protect—see Adding Your First HTA-Protected Host on page 34.

Refer to the appropriate chapters and sections for step-by-step instructions to perform the tasks described above.

**IMPORTANT:** Use the resource checklist worksheets provided in Appendix A, Resource Tables and Checklists to record network, IP address, AD, and other virtual infrastructure host information that you will need when installing and configuring the HTA and adding protected hosts.

---

**Obtaining the Software**

Log in to the HyTrust website (http://www.hytrust.com) or follow the directions you received from HyTrust Support to obtain the download URL of the HTA OVF file. Download the files to a local drive that is accessible by your virtual infrastructure.

If you wish to enable the HTA Enterprise features, obtain and download the appropriate XML license file to a local drive that is accessible to the HTA Management Console.
Selecting the Deployment Architecture

This chapter contains the following sections:

- Preparation: Network Architecture and Topology
- Network Configuration Considerations

Preparation: Network Architecture and Topology

The HyTrust Appliance (HTA) works by intercepting ESX management requests normally routed directly to ESX hosts or vCenter Servers; the HTA does not intercept any VM guest traffic. The HTA first authenticates and authorizes all users and the operations they want to perform before passing on the request to the requested target. In addition, the HTA allows organizations to create and apply more granular access policies and perform ESX configuration management by applying and monitoring ESX compliance to custom-defined security templates and then remediating deficiencies and discrepancies.

The HTA relies on a customer’s network topology to have visibility to the virtual infrastructure’s management traffic and the ability to intercept it. There are two network configuration options available for installing the HTA: Mapped Mode or Router Mode.

Mapped Mode

When configured to use Mapped Mode, the HTA works as a proxy server and does not require any architectural changes to your virtual infrastructure (VI) network. It works well in both segmented networks or in environments with flat, unstructured network topologies. In Mapped Mode, only Network Connection 1 (eth0) of the HTA is utilized. Each HTA protected host (e.g., vCenter Server, ESX/ESXi host) has a dedicated IP address (called the Published IP or PIP) which management clients use to access the host.

Destination Maps are an out-of-band solution that proxy management traffic within your existing network. The only requirements are as follows:

- The HTA needs to be able to talk to the Service Console (or VMkernel Port for ESXi) of each protected host.
Selecting the Deployment Architecture

Preparation: Network Architecture and Topology

- For each protected host (including a vCenter Server) a new published IP address will be used by end users to access the host.
- The PIP addresses need to be on a subnet local to the HTA Connection 1 (eth0) interface. Do not specify a PIP that belongs to a remote, routed network.

![Figure 2-1 Network topology utilizing Mapped Mode](image)

When a vCenter Server or host is added using Mapped Mode, enter the PIP in the Add Host Wizard, or on the Edit Host page in the Published IP tab. The HTA presents a published IP address for each protected target. The user accesses the protected host by using their PIP through SSH, vSphere Client, web console, etc. as if addressing the host directly. Several thousand IP addresses of protected target hosts may be deployed on the same HTA. Connections to unprotected services are forwarded by the HTA to the protected target. Connections destined to protected services are handled by the HTA.

Due to being out-of-band, Destination Maps do not provide any connection security. Unless there are external routing rules or a firewall, the original IP addresses of the vCenter Server, ESX and ESXi hosts are still available for connections that go around the security the HTA provides. For example, when using the original IP address to access an ESXi host, an administrator can view the web-based Datastore Browser using root credentials of the ESXi host. When available, ESX hosts should be configured to Lock-out Unauthorized Access through the HTA Management Console so that the ESX host denies any traffic that goes around the HTA.

**Router Mode**

The most common deployment method of an in-line configuration is Router Mode. In this configuration, the HTA joins two IPv4 networks, passing information from one network to the other. An example of how Router Mode can be implemented is as follows:

- The NIC for Connection 1 (eth0) is connected to the network from which clients access the virtual infrastructure (typically the internal or corporate LAN segment).
The NIC for Connection 2 (eth1) is connected to the network segment that is to be protected by the HTA (where the vCenter Server and the ESX hosts are located).

Note:
An Enterprise or appropriate evaluation license is required to implement Router Mode. If you are currently using the Community License and want to test Router Mode, contact HyTrust Sales for an evaluation license.

The following table will help you determine the preferred method for installing the HTA.

Table 2-1  HTA network deployment options

<table>
<thead>
<tr>
<th>Network Option</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mapped Mode</td>
<td>Does not require changes to existing routing infrastructure.</td>
<td>Requires management of an additional IP address for each protected host; end users need to change the IP to which they connect their clients; weaker protection against HTA bypass.</td>
</tr>
<tr>
<td>Router Mode</td>
<td>In-line solution guarantees network enforcement.</td>
<td>As a participant in corporate routing fabric, requires more thorough advanced planning; ESX configuration (gateway) needs to be changed out of band.</td>
</tr>
</tbody>
</table>

Network Configuration Considerations

For Mapped Mode, only Connection 1 (eth0) is used. For Router Mode, the most common configuration utilizes Connection 1 and Connection 2 (eth1); however, from the command line interface (CLI), an additional protected network segment can be defined using Connection 3 (eth2).

Connection 1 (eth0) defaults to the HTA Management Console interface and should be connected to your management network. In the case of Router Mode, there is an ingress and egress point that is established (the ingress/egress is eth0/eth1 respectively).

For Router Mode, the default gateway for each host and vCenter Server must be the protected IP address of the HTA (IP assigned to eth1). An additional route should also be defined for unprotected networks to route unprotected traffic to the HTA.
Before you login to the HTA, confirm that all the necessary HTA network adapters in the vSphere Client are connected to the proper network segment and are set to automatically connect at power on. By default, only eth0 is automatically connected. Manual connection of eth1 is required for Router Mode.

Use the worksheets provided in Appendix A, Resource Tables and Checklists to record network, IP address, and other virtual infrastructure host information needed when configuring the HTA and adding protected hosts.
Installing the Appliance

This chapter contains the following sections:

- Deploying the OVF Template
- Powering Up the Appliance
- Configuring the HTA Management Network Interface
- Starting the HTA Management Console
- Initial Setup and Configuration

Deploying the OVF Template

Before You Begin

Before installing the HyTrust Appliance (HTA), the following should already be in place:

- Virtual infrastructure consisting of installed ESX hosts and, optionally, vCenter Servers.
- Network connectivity and access to the HTA host machine and the infrastructure to secure. The HTA installation requires an ESX host with at least one dedicated network interface (with use of VLANs).
- For Directory Service mode authentication, setup of Microsoft Active Directory with an AD service account and the recommended HyTrust security groups, as described in the HyTrust Appliance Administration Guide.
- Services that virtual infrastructure clients are using should be routable from the appropriate interface. For example, Active Directory, DNS, and RSA services need to be accessible from the HTA.

To install and run the HTA as a virtual appliance, use the vSphere Client application to access either the vCenter Server or the ESX host on which you want to deploy and configure the HTA virtual machine.

Detailed Steps

Perform the following steps to deploy the HTA OVF template:

1. In the vSphere Client, select the ESX host (if standalone) or vCenter Server (if managed) where you want to deploy the HTA OVF file.
2. Choose **File > Deploy OVF Template**. The Deploy OVF Template Wizard appears.

![Deploy OVF Template Wizard](image)

**Figure 3-1 Deploying the OVF template**

3. Select **Deploy from file**. Click Browse and navigate to the virtual appliance OVF file stored on media or a network directory location.

4. Proceed through the remaining steps of the wizard making sure that you set Connection 1 to the network used to access the HTA Management Console. When you reach the end of the wizard, click Finish.

   The vSphere Client now initiates the deployment process on the selected ESX host or vCenter Server resource. As the process continues, its progress is displayed in the vSphere Client Status panel. When finished, the vSphere Client displays the **Create Virtual Machine** completed message in the Recent Tasks display.

5. You can now view the HTA virtual machine default settings and configuration and make any changes through the vSphere Client, such as increasing the memory and virtual CPUs assigned to the HTA, and changing the size of the log disk in the virtual appliance. Confirm that the network adapter(s) are properly configured and connected.

6. Configure the appliance to automatically start on ESX startup. To do that, from the vSphere Client:
   a. Select the ESX host in the object tree.
   b. Select the Configuration tab.
   c. Click the Virtual Machine Start / Shutdown option in the list on the left, and then click Properties in the top right corner of the window.
   d. Select your HTA virtual machine in the list and prioritize its order. Services that support the HTA, such as Active Directory, should have a higher priority. Automatic startup and the proper start order will enable the HTA host ESX protection in the event of a host reboot.
HyTrust Appliance Installation Guide

Installing the Appliance

Powering Up the Appliance

To power up the HTA virtual machine:

1. From the vSphere Client Summary tab view select the HTA virtual machine and click the Power On button, or right-click the HTA virtual machine and select Power On.
2. Open the vSphere Client Console to view the status of the HTA virtual machine as it starts up. (You can also click the Launch Virtual Machine Console Window button to open a popup window to display virtual machine console startup messages.)

After the HTA has completed the boot process, you will be presented with the login screen:

```
Security Appliance - 3.0.2
The management network interface must be configured.
Login as the user "ascadminuser" then type "setup" to configure the management NIC (eth0).
localhost login: _
```

Once the appliance has powered up and completed booting, you must configure the HTA Management network interface.

Configuring the HTA Management Network Interface

The HTA Management network interface (eth0) must be manually configured before you can access the HTA Management Console.

Perform the following to configure the HTA Management network interface:

1. At the vSphere Client console window, log in as the user ascadminuser with the password Pa$$w0rd123!.
2. You are prompted to assign a new password to the local HTA administrator account (ascadminuser). Be sure to keep your new password in a safe and secure place.
3. Start the setup procedure. At the prompt, type:
   ```
   setup
   ```
4. Manually assign a static IP address to the management network interface (eth0) and set the subnet mask, gateway, and DNS server addresses.
5. Save by typing:
   ```
   y
   ```
6. Log out after the network settings have been updated.

Note:
If you choose to deploy the appliance in a Distributed Resource Scheduler (DRS) cluster, make sure that DRS is disabled for the HTA virtual machine by selecting Edit Settings > VMware DRS > Virtual Machine Options. This is required to make sure that the HTA runs only on the ESX where virtual networking is properly configured.

Once the deploy is complete, the HTA appears in the vSphere Client inventory hierarchy for the selected vCenter Server or ESX host.
You now have a static IP address assigned to the HTA Management interface. Take note of the URL address displayed in the console window as shown in the figure below. You will use this URL to access the web-based HTA Management Console.

![Figure 3-2 Static IP Address configuration](image)

**Figure 3-2 Static IP Address configuration**

### Starting the HTA Management Console

You use the web-based HTA Management Console to customize the HTA configuration settings and set up operations for safeguarding your managed virtual infrastructure environment. For example, the HTA Management Console provides menus to set authentication options for users, add vCenter Servers and hosts to the protected infrastructure, define templates and policy checks/tests to enforce security of protected virtual infrastructure, and view and configure logs.

If you have not already done so, confirm that the Network adapter(s) are properly configured and connected to the HTA. Refer to Chapter 2, Selecting the Deployment Architecture to help you determine your preferred deployment method and how to configure the HTA network adapter(s) before you login to the HTA Management Console.

To start the HTA Management Console:

1. Open a web browser and enter the IP address of the HTA Management network interface. For example:
   
   `https://10.223.1.118/asc`

   **Note:** When accessing the HTA for the first time you must use the IP address in the URL. Using the fully qualified domain name (FQDN) is not supported until after you have completed the Installation Wizard in the HTA Management Console.
2. The first time you start up the HTA Management Console you will receive a security exception. You need to manually allow the security exception as the HTA initially ships with a self-signed certificate.

**Note:**
If using Internet Explorer (IE), a security warning window may appear when accessing the HTA Management Console. You must edit the Internet Security properties within IE to remove this warning.

In IE 8+, go to **Tools > Internet Options > Security Tab > Internet > Custom level > Miscellaneous** and enable the *Display mixed content* setting. Restart Internet Explorer for the change to take effect.

In some customer environments, additional modifications to the IE security settings or firewall settings within your corporate network may be required.

---

**Note:**
SSL certificates issued by a trusted authority can be imported at a later time through the HTA Management Console.

3. The login screen appears.

4. Enter the default login username (**superadminuser**) and password (**Pa$$w0rd123!**) to log into the system.

---

**Initial Setup and Configuration**

Initial setup and configuration of the HTA consists of the following operations:

1. Accept the end-user license agreement.
   a. Read the terms of the end-user license agreement (EULA).
   b. Select the *I Accept* checkbox at the bottom.
c. Click Next.

2. If applicable, install a license.
   a. If you have a license file, enter the location of the license file, or click Browse to navigate to it.

   If you do not have a license, the Community License is activated and the HTA will operate with a reduced feature set.

   b. Click Next.

3. Complete the HTA Installation Wizard based on your selected networking mode.
   - To configure the HTA for Mapped Mode networking, see Chapter 4, Mapped Mode.
   - To configure the HTA for Router Mode networking, see Chapter 5, Router Mode.

4. Perform post-installation setup and configuration tasks, see Chapter 6, Post-Installation Tasks.

After finishing the Installation, users can select from the General, Compliance, Policy, Configuration, Maintenance, and Help page options that appear across the top banner of
the HTA Management Console to view and configure other HTA settings. Refer to the
HyTrust Appliance Administration Guide for more information.
Installing the Appliance

Initial Setup and Configuration
This chapter contains the following sections:

- Running the HTA Installation Wizard

Running the HTA Installation Wizard

The HTA Installation Wizard steps you through the following pages to configure the HTA for Mapped Mode.

1. On the HTA Host Configuration page, select Mapped as the Networking Mode and click Next.

![Figure 4-1 HTA Installation Wizard - HTA Host Configuration](image)

*Figure 4-1 HTA Installation Wizard - HTA Host Configuration*
2. The Network Configuration page appears.

![Network Configuration](image)

*Figure 4-2 HTA Installation Wizard - Network Configuration*

3. Specify the network and IP address connection information for the HTA host:
   a. Assign a fully qualified hostname.
   b. Double-check the IP address for Connection 1. This is the management interface (eth0).
   c. Specify the subnet mask (Connection 1: Mask), gateway, and a comma-separated list of DNS servers.
   d. Optionally, select the Enable NTP Servers checkbox and specify the IP address of one or more, comma-separated, NTP servers the HTA should use for time synchronization.

   **Note:** Ensure you use IP addresses for the DNS and NTP servers.

4. Click Next.

![Finish](image)

*Figure 4-3 HTA Installation Wizard - Finish*
5. Click Finish to complete the installation wizard.

**Note:** The Finish button is not available until after the Install Wizard completes.

Upon successfully completing the HTA Installation Wizard, the HTA Management Console Appliance Dashboard appears.
Mapped Mode

Running the HTA Installation Wizard
CHAPTER

5

Router Mode

This chapter contains the following sections:

- Running the HTA Installation Wizard

Running the HTA Installation Wizard

The HTA Installation Wizard steps you through the following pages to configure the HTA for Router Mode.

1. On the HTA Host Configuration page, select Router as the Networking Mode and click Next.

![HTA Installation Wizard - HTA Host Configuration](image)

Figure 5-1  HTA Installation Wizard - HTA Host Configuration
2. The Network Configuration page appears.

![Figure 5-2 HTA Installation Wizard - Network Configuration](image)

3. Specify the network and IP address connection information for the HTA host:
   a. Routing Information Protocol (RIP) is a widely deployed interior gateway protocol. If you are deploying in a network where RIP is currently enabled, select the Enable Routing Information Protocol Service checkbox and assign a Router Password. All services running under RIP require the Router Password for remote configuration. (RIPv1 and RIPv2 are supported.)
   b. Assign a fully qualified hostname.
   c. Double-check the IP address for Connection 1. This is the management interface (eth0), which connects to the unprotected network.
   d. Specify the subnet mask (Connection 1: Mask), gateway, and a comma-separated list of DNS servers.
   e. Most configurations will also utilize Connection 2 (eth1), which connects to the HTA-protected network.
   f. Optionally, select the Enable NTP Servers checkbox and specify the IP address (or FQDN) of one or more, comma-separated, NTP servers the HTA should use for time synchronization.

**Note:** Ensure you use IP addresses for the DNS and NTP servers.
4. Click Next.

![HTA Installation Wizard - Finish](image)

*Figure 5-3  HTA Installation Wizard - Finish*

5. Click Finish to complete the installation wizard.

**Note:** The Finish button is not available until after the Install Wizard completes.
Upon successfully completing the HTA Installation Wizard, the HTA Management Console Appliance Dashboard appears.

![HTA Management Console Appliance Dashboard](image)

**Figure 5-4** HTA Management Console Appliance Dashboard
Post-Installation Tasks

This chapter contains the following sections:

- Verifying Network Configuration
- Adding Your First HTA-Protected Host
- Accessing the HTA-Protected Virtual Infrastructure
- Limiting Unauthorized Administrative Access to the HTA

After completing the initial setup and configuration the HyTrust Appliance (HTA) only allows the default, built-in users access. This mode of user authentication is called Demo mode. The HTA also supports performing user authentication via a directory service (e.g., Microsoft Active Directory). This mode of user authentication is called Directory Service mode. The HTA remains in Demo mode until configured to use a directory service.

You may continue to use Demo mode authentication at this time, however, Demo mode is only intended for product evaluation and testing—it is not suitable for production environments.

While in Demo mode, continue to use the superadminuser account to complete the initial configuration of the HTA. Once the HTA has been converted to Directory Service mode, the superadminuser account is no longer available and only directory users with the necessary group membership can access the HTA Management Console and the virtual infrastructure.

If you are deploying the HTA in a production environment, it is recommended that you first convert the HTA to Directory Service mode. Refer to the HyTrust Appliance Administration Guide to complete the conversion prior to adding a vCenter Server.

Verifying Network Configuration

The first thing you need to do after installing the HTA is to verify your network is properly configured by performing the following:

1. Access the HTA web-based management interface using a web browser from a client system.
   a. Enter the URL of the HTA Management Console. For example: https://10.223.1.118/asc
2. Ping the Service Console IP of a target ESX/ESXi host from the HTA terminal window.
3. Ping the Service Console IP of a target ESX/ESXi host from the client system.
Post-Installation Tasks

Adding Your First HTA-Protected Host

4. Ping the vCenter Server IP from the client system.
5. Login with root credentials to the ESX/ESXi host using the vSphere Client from the client system.
6. (ESX hosts only)
   a. Login with root credentials to the web management interface of the ESX host using a web browser from the client system.
   b. Login via SSH to the ESX host using root credentials.
7. Login with Administrator credentials to the vCenter Server using the vSphere Client from the client system.
8. Login with Administrator credentials to the vCenter Server web management interface using a web browser from the client system.

If all of the above work properly, then your network is properly configured and you are ready to access the HTA-protected environment and add your first HTA-protected host.

Adding Your First HTA-Protected Host

The HTA can protect the following types of hosts:

- vCenter Server and its managed ESX hosts—see Adding vCenter Server Managed Hosts
- ESX hosts not managed by vCenter Server—see Adding Unmanaged Hosts
- Cisco Nexus switches—see Adding Cisco Nexus Switches
  - Nexus 1000V Virtual Supervisor Module (VSM) switch
  - Nexus 5000 and 7000 series switches
- Cisco UCS Manager—see Adding Cisco UCS Manager Hosts

Note: A data center with HTA managed hosts will not be fully protected until all the hosts in the data center are protected.

Adding vCenter Server Managed Hosts

Before you can add the vCenter Server managed host(s), you must add the vCenter Server as a host to your HTA-protected environment. Once a vCenter Server is added to the HTA, the HTA will automatically import all the vCenter Server virtualized resources and managed ESX/ESXi hosts.

All vCenter Server managed hosts automatically added to the HTA hosts list will initially show a blocked ( ) icon, indicating that additional configuration is required before the HTA can assess or protect these hosts.

HTA-protected hosts are marked with a yellow shield ( ) icon, indicating that the HTA is controlling all future management communications based on the configured access and segmentation policies.

The following sections describe how to add a vCenter Server and its managed ESX/ESXi hosts (see Add the vCenter Server on page 35), and how to configure vCenter Server managed hosts (see Configure the imported ESX managed hosts on page 39).
Add the vCenter Server

1. From the HTA Management Console, select **Compliance > Hosts** to open the Hosts page.

   ![HyTrust Hosts page](image)

   **Figure 6-1 Compliance > Hosts page**

2. Click Add.

   The Add Host Wizard appears.

   ![HyTrust Add Host Wizard](image)

   **Figure 6-2 Add Host Wizard - Host Login page**

3. On the Host Login page, enter the following:
   a. The fully qualified hostname or IP address of the vCenter Server (or Host).
   b. The administrator User ID and Password for the vCenter Server (or root credentials for a host).

   **Note:** You will not be able to add a host with a password that contains both the left angle bracket (`<`) and the right angle bracket (`>`) characters. However, passwords with either character are supported.
c. Optionally, open the Advanced Properties section (click the triangle or text) to reveal the VI SDK, HTTP, and HTTPS port settings. It is recommended to maintain the default settings.

![Advanced Properties](image)

**Figure 6-3 Host Login page - Advanced Properties section**

d. When finished entering the vCenter Server or ESX host information, click Next. The HTA attempts to automatically detect the host type. Supported host types are vCenter Server, ESX, ESXi, Cisco Nexus 1000V VSM, Cisco UCS Manager, and Cisco Nexus 5000 and 7000 series switches.

4. The Host Details page appears.

![Add Host Wizard](image)

**Figure 6-4 Add Host Wizard - Host Details page**

5. On the Host Details page, enter the following:
   - Friendly Name—A unique name to identify the vCenter Server, or the specified ESX host, in the list of HTA hosts. This does not have to be the same name as used in DNS.

   **Note:** Spaces and special characters are allowed, but the name should not exceed 64 characters.

   - Description—A description for the host.
Post-Installation Tasks
Adding Your First HTA-Protected Host

- Protected—Select this checkbox to have the HTA protect both the vCenter Server, and the ESX hosts it manages. Default is selected.
- Use HTA Service Account—HyTrust recommends selecting this checkbox to use the HTA service account when establishing sessions from the HTA to the vCenter Server. In this mode, only one administrative account is required on the vCenter Server. This configuration, however, is not able to limit the visibility of objects displayed in the vSphere Client.

When the Use HTA Service Account option is deselected, the user accessing the virtual infrastructure via the vSphere Client must have the appropriate administrative privileges configured in the vCenter Server. If the HTA service account is not used, and pass-through mode is utilized, a vCenter Server account must be configured for each user. Limits on viewing objects in the vSphere Client are supported and maintained using the vCenter Server roles and permissions.

- Proceed to Advanced step—Select this checkbox to display advanced configuration options for the host.

6. Click Next.

7. If selected, the Advanced page appears.

The advanced configuration options will vary based on host type. Figure 6-5 shows the options available to an ESXi host.

The following options are available on the Advanced page:
- SSH Port—Enter the port number to use for SSH connections. Default is 22.

Figure 6-5 Add Host Wizard - Advanced page (ESXi host)
Post-Installation Tasks

Adding Your First HTA-Protected Host

Note: SSH can only be enabled for ESXi hosts if Root Password Vaulting is enabled and the Recovery Passcode is set. Refer to the HyTrust Appliance Administration Guide for details on Root Password Vaulting.

- Use HTTPS Secure Port—Enables the HTTPS port.
- HTTP Port—Enter the port number to use for HTTP connections. Default is 80.
- HTTPS Secure Port—Enter the port number to use for HTTPS connections. Default is 443.
- Lock Out Unauthorized Access—(ESX hosts only) Select this option to secure your ESX hosts and reject virtualization management operations not proxied via the HTA. The HTA will configure the ESX host firewall to only allow management traffic proxied by the HTA.

Note: Lock Out mode is not available for ESXi hosts. If you wish to enforce Lock Out functionality on ESXi hosts, configure Root Password Vaulting. Refer to the HyTrust Appliance Administration Guide.

To lock out access to the vCenter Server, you must manually configure the firewall rules on the Windows Server 2008 virtual machine running the vCenter Server—see Appendix B, Configuring the Windows Server 2008 Firewall.

- Golden Host—(ESX hosts only) Select this option to designate this host as the master for network configuration. Only one host can enable this option.
- Additional Host Consoles—View, add, or edit additional fully qualified domain names or IP addresses assigned to the host.

Review the information on the Advanced page for accuracy before clicking Next to continue.

8. If using Mapped Mode, the Published IP (PIP) page appears.

Figure 6-6 Add Host Wizard - Published IP page

The following fields are available:

- Published Hostname/IP—The hostname/IP address to use to route all traffic to this host.
- Published IP Mask—The subnet mask to use to route all traffic to this host.
Click Next to continue.

9. The HTA Add Host Wizard now indicates it has all the information needed to add the host(s).

![Add Host Wizard - Complete Host Add page](image)

**Figure 6-7** Add Host Wizard - Complete Host Add page

10. Click Finish.

Once you have successfully added a vCenter Server it will appear on the Hosts page along with its managed hosts.

![Compliance > Hosts page with added hosts](image)

**Figure 6-8** Compliance > Hosts page with added hosts

**Note:**

In larger environments, the add host process can take several minutes, so it may take some time before the hosts appear in the list.

As shown in Figure 6-8, the vCenter Server is now protected, as indicated by the yellow shield (🛡️) icon.

However, each imported vCenter Server managed host requires additional configuration before the HTA can protect it, as indicated by the blocked (🔒) icon.

**Configure the imported ESX managed hosts**

1. On the Host page (**Compliance > Hosts**), click on a blocked hostname.
2. On the General tab, specify the root administrator credentials (User ID and Password) for the selected host.

![General tab of HyTrust Hosts](image)

**Figure 6-9 Compliance > Hosts > Edit Host page - General tab**

**Note:** If this ESX or ESXi host is hosting the HTA virtual appliance, select the HTA checkbox to protect it.

3. If needed, change the assigned security template (default template chosen by host type).
4. Open the Advanced tab, review the settings, and, if needed, update the advanced HTA configuration settings for the selected host.

![HyTrust Appliance Installation Guide](image)

**Figure 6-10** Compliance > Hosts > Edit Host page - Advanced tab

5. If using Mapped Mode, select the Published IP tab and specify the Published IP address and Mask that clients will use to route management traffic to the HTA.

![HyTrust Appliance Installation Guide](image)

**Figure 6-11** Compliance > Hosts > Edit Host page - Published IP tab

6. Once you are finished editing the host configuration, click OK to save your changes.

7. Repeat for each blocked host.
After completing this process for each host, all hosts on the Hosts page should now be protected.

![HyTrust Hosts](image)

**Figure 6-12   Compliance > Hosts page with protected hosts**

You can sort the list by Hosts, Host Type, Patch Level, or Default Template. Sorting is accomplished by clicking on the appropriate column headers.

Now that all hosts are protected, all future communications to them go through the HTA.

If you are utilizing the Destination Map feature, you can login to your ESX host (using its Published Hostname/IP address) from any client to confirm proper network connectivity.

In Router Mode, you can login directly to the Host using the real IP address to confirm proper network connectivity.

**Note:** If you are still in Demo mode, you will need to use the Demo mode username (superadminuser) and password (Pa$$word123!).

You are now ready to create and deploy access policies. Refer to the *HyTrust Appliance Administration Guide* for details.

### Configuring multiple ESX or ESXi hosts

To configure multiple ESX or ESXi hosts at the same time, also called batch edit:

1. Place a checkbox next to each host you want to configure.

**Note:** Multiple host edit is only supported for hosts of the same type (e.g., ESXi only) that share the same root credentials.
2. Click the Add button. The Edit (Multiple Host) page appears.

![Edit Host (Multiple Hosts) page - General tab](image1)

*Figure 6-13  Edit Host (Multiple Hosts) page - General tab*

3. Open the Advanced tab and make any necessary changes.

![Edit Host (Multiple Hosts) page - Advanced tab](image2)

*Figure 6-14  Edit Host (Multiple Hosts) page - Advanced tab*

4. Once you are finished configuring the hosts, click OK to save your changes.

You are now ready to create and deploy access policies. Refer to the *HyTrust Appliance Administration Guide* for details.
Adding Unmanaged Hosts

To add unmanaged ESX hosts (i.e., ESX hosts that are not managed by a vCenter Server):

1. From the HTA Management Console, select **Compliance > Hosts** to open the Hosts page.

2. Click Add.

   The HTA Add Host Wizard appears. This wizard sequences through a series of steps to specify an individual ESX host to add (or choose a vCenter Server to add the collection of hosts it manages).

3. Complete the Add Host Wizard.

   You are now ready to create and deploy access policies. Refer to the *HyTrust Appliance Administration Guide* for details.

Adding Cisco Nexus Switches

1. From the HTA Management Console, select **Compliance > Hosts** to open the Hosts page.

2. Click Add.
The Add Host Wizard appears.

![Add Host Wizard - Host Login page](image)

**Figure 6-17 Add Host Wizard - Host Login page**

3. On the Host Login page, enter the following:
   a. The fully qualified hostname or IP address of the Nexus host.
   b. The administrator User ID and Password for the Nexus host.

   **Note:** You will not be able to add a host with a password that contains both the left angle bracket (<) and the right angle bracket (>) characters. However, passwords with either character are supported.

c. Click Next.

4. The Host Details page appears.

![Add Host Wizard - Host Details page (Nexus)](image)

**Figure 6-18 Add Host Wizard - Host Details page (Nexus)**

5. On the Host Details page, enter the following:
Post-Installation Tasks
Adding Your First HTA-Protected Host

- Friendly Name—A unique name to identify the Nexus host in the list of HTA hosts. This does not have to be the same name as used in DNS.

**Note:**
Spaces and special characters are allowed, but the name should not exceed 64 characters.

- Description—A description for the host.
- Protected—Select this checkbox to have the HTA protect the Nexus host. Default is selected.
- Use HTA Service Account—HyTrust recommends selecting this checkbox to use the HTA service account when establishing sessions from the HTA to the Nexus host.

  When the Use HTA Service Account option is deselected, the user accessing the virtual infrastructure via the Nexus host must have the appropriate administrative privileges configured. If the HTA service account is not used, and pass-through mode is utilized, a Nexus account must be configured for each user.

6. Click Next.
7. If using Mapped Mode, the Published IP (PIP) page appears.

![Add Host Wizard - Published IP page](image)

Figure 6-19   Add Host Wizard - Published IP page

The following fields are available:
- Published Hostname/IP—The hostname/IP address to use to route all traffic to this host.
- Published IP Mask—The subnet mask to use to route all traffic to this host.

Click Next to continue.
8. The HTA Add Host Wizard now indicates it has all the information needed to add the host(s).

\[Image: HyTrust Add Host Wizard - Complete Host Add page\]

Note: In larger environments, the add host process can take several minutes, so it may take some time before the hosts appear in the list.

A yellow shield (🛡️) icon next to the Nexus host indicates it is now protected.

9. Click Finish.

Once you have successfully added a Nexus host it will appear on the Compliance > Hosts page.

\[Image: Compliance > Hosts page with added Nexus host\]

Adding Cisco UCS Manager Hosts

Prerequisites

If using SSL, you must perform the following before you can add a Cisco UCS Manager host:

1. Import the SSL Certificate using the HTA Management Console—refer to Managing Certificates in the HyTrust Appliance Administration Guide.
Post-Installation Tasks

Adding Your First HTA-Protected Host

2. By default the HTA only accepts SSL version 3; however, SSL version 2 is required for compatibility with Cisco USC Manager hosts. Configure the HTA to accept SSL version 2 by running the following command as ascadminuser:

   asc certs -ssl 2

3. Restart Tomcat by running the following command as ascadminuser:

   asc service -n tomcat6

Steps

1. From the HTA Management Console, select Compliance > Hosts to open the Hosts page.

   ![Compliance > Hosts page](Figure 6-22)

2. Click Add.

   The Add Host Wizard appears.

   ![Add Host Wizard - Host Login page](Figure 6-23)

3. On the Host Login page, enter the following:
   a. The fully qualified hostname or IP address of the UCS Manager host.
   b. The administrator User ID and Password for the UCS Manager host.
Note: You will not be able to add a host with a password that contains both the left angle bracket (<) and the right angle bracket (>) characters. However, passwords with either character are supported.

c. If not using SSL, open the Advanced Properties section and deselect the Use VI SDK Secure Port and Use HTTPS Secure Port settings.

Figure 6-24 Advanced Properties section - Disable SSL

d. Click Next.

4. The Host Details page appears.

Figure 6-25 Add Host Wizard - Host Details page (UCS)

5. On the Host Details page, enter the following:
   - Friendly Name—A unique name to identify the UCS Manager host in the list of HTA hosts. This does not have to be the same name as used in DNS.

   Note: Spaces and special characters are allowed, but the name should not exceed 64 characters.

   - Description—A description for the host.
   - Protected—Select this checkbox to have the HTA protect the UCS Manager host. Default is selected.
Post-Installation Tasks

Adding Your First HTA-Protected Host

- Use HTA Service Account—HyTrust recommends selecting this checkbox to use the HTA service account when establishing sessions from the HTA to the UCS Manager host.

When the Use HTA Service Account option is deselected, the user accessing the virtual infrastructure via the UCS Manager host must have the appropriate administrative privileges configured. If the HTA service account is not used, and pass-through mode is utilized, a UCS Manager account must be configured for each user.

6. Click Next.
7. If using Mapped Mode, the Published IP (PIP) page appears.

![Published IP page](image1)

**Figure 6-26 Add Host Wizard - Published IP page**

The following fields are available:
- Published Hostname/IP—The hostname/IP address to use to route all traffic to this host.
- Published IP Mask—The subnet mask to use to route all traffic to this host.

Click Next to continue.

8. The HTA Add Host Wizard now indicates it has all the information needed to add the host(s).

![Complete Host Add page](image2)

**Figure 6-27 Add Host Wizard - Complete Host Add page**

9. Click Finish.
Once you have successfully added a UCS Manager host it will appear on the Compliance > Hosts page.

![Compliance > Hosts page with added UCS Manager host](image)

**Note:**
In larger environments, the add host process can take several minutes, so it may take some time before the hosts appear in the list.

A yellow shield (🛡️) icon next to the UCS Manager host indicates it is now protected.

### Accessing the HTA-Protected Virtual Infrastructure

When a user attempts to establish a session with an ESX host or a vCenter Server, in an HTA-protected environment, the HTA intercepts the request. The HTA authenticates the user against a combination of the policy data stored locally and the central user directory or Active Directory (AD). In addition, the HTA performs an authorization check to determine if the user is allowed to login to the target.

![HTA-protected virtual infrastructure](image)

The HTA forwards the request to the intended ESX host only if authentication and authorization at the HTA-level is successful.

Authentication for the user (including session ID) lasts for the duration of the session. Once the session is established, authorization of the user to perform a particular operation, including AD group membership, can occur on multiple occasions per session.

After the HTA authenticates the user and authorizes the request, it sends the request to the target object. The HTA uses a special service account when forwarding requests to the
target. Further explanation regarding the authentication and authorization process using
the vSphere Client and SSH can be found in the HyTrust Appliance Administration Guide.

Limiting Unauthorized Administrative Access to the HTA

The following configuration steps are required to mitigate the risk of unauthorized
administrative access to the HTA:

1. Apply the CoreAppliance RuleSet to the HTA virtual machine and restrict membership
   in the CoreAppliance security group.
2. Setup and configure SNMP to monitor HTA reboots and implement change control.
3. Change the HTA virtual machine boot order to boot from the disk first (not CD, etc.).

Refer to the appropriate sections in the HyTrust Appliance Administration Guide for details
on how to perform these tasks.
High Availability

This chapter contains the following sections:

- Overview
- Setup and Configuration
- HA Systems Boot Order
- HA CLI Commands

Overview

An Enterprise or appropriate evaluation license is required to configure the HTA for high availability (HA).

HTA HA requires a second HTA virtual machine (matching the specifications listed in Table 1-1) installed on a different host from the primary HTA.

Using the HTA HA option, two HTA instances are installed on separate hosts. During HTA HA setup, the administrator joins and establishes a relationship between the two HTA instances, assigning one HTA as primary and the other HTA as secondary. Each HTA instance uses a network connection (eth2) to monitor the health of the other HTA and synchronizes all current database and configuration information at a default interval of 10 minutes.

Note: For maximum HA protection, it is recommended that each HTA instance be in a separate cluster, have its own separate storage, and use a dedicated network link (eth2) connecting them to each other.

When configuring the secondary HTA, two static IP addresses are assigned. Manually assign a static IP address to its management network interface (eth0). Once you assign the static IP address, subnet mask, gateway, and DNS server you are prompted to specify the network settings for the HA services on the Connection 3 (eth2) interface.

Note: The HTA Management Console is not available on the secondary HTA.

Client traffic is only routed through the primary HTA.
On failover, the primary HTA management interface settings are transferred to the secondary HTA, which becomes the primary HTA. Client traffic is then routed to the new primary HTA (which was originally configured as the secondary HTA). This is referred to as HA promotion and demotion.

**IMPORTANT:** Do not attempt to promote the original primary HTA if it fails. After the secondary HTA becomes the primary HTA, install a fresh secondary HTA, configure it, and join it to the newly promoted primary HTA.

The following illustration shows the HTA HA configurations for both Mapped Mode and Router Mode.

![HTA HA Configuration in Mapped Mode](image1)

![HTA HA Configuration in Router Mode](image2)

**Figure 7-1**  
HTA high availability configuration

During normal operation, all client requests destined for the HTA or the protected infrastructure are routed to the primary HTA. When both HTA instances are running, the secondary HTA periodically monitors the health of the primary HTA and synchronizes its data and configuration information with the primary HTA.
Administrators can use the HTA HA command line interface (CLI) command (asc ha) to configure and monitor the HA (e.g., checking status, setting the synchronization and timeout intervals, forcing immediate synchronization, or initiating the failover process)—see HA CLI Commands on page 58.

As long as the primary HTA remains healthy, it continues to process client access requests. However, if a problem is detected on the primary HTA, and automatic failover is active on both the primary and secondary HTAs, the secondary HTA will automatically promote itself to become the new primary HTA. The duration of time from when the secondary detects a problem and when automatic failover occurs is based on the timeout interval.

An Administrator can manually promote or demote an HTA using the asc ha --mode command—see HA CLI Commands on page 58.

**Setup and Configuration**

It is important to have the proper measures (i.e., notifications) in place to alert an HTA administrator well in advance of a failover event so he can try to determine the root cause of the issue. Refer to the Appliance Configuration chapter (Configuration Notifications section) in the HyTrust Appliance Administration Guide for more information on configuring HTA notifications.

In the unlikely event that services cannot be restored on the primary HTA after an automatic failover occurs, an HTA administrator can install and join a new secondary HTA to the newly promoted primary HTA to restore the HA structure.

Once the HTA administrator verifies that everything is working properly, he can remove the failed HTA from the vCenter Server inventory since it can no longer be used.

---

**Note:**

HTA HA is only supported when the management interface (eth0) and the HA interface (eth2) are on different subnets. This requirement applies to both Mapped Mode and Router Mode deployments.

---

**Default Configuration**

The default HTA HA configuration is automatic failover with a default poll (health check) interval of 5 minutes, and a default timeout of 30 minutes (1800 seconds), as shown in the table below.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failover Mode</td>
<td>Automatic</td>
<td>The secondary HTA will automatically promote itself to the primary HTA when the timeout clock expires.</td>
</tr>
<tr>
<td>Poll Interval (health check)</td>
<td>5 minutes</td>
<td>The health check polling interval time period between primary and secondary HTAs.</td>
</tr>
<tr>
<td>Poll Interval (data sync)</td>
<td>10 minutes</td>
<td>The data synchronization period between nodes.</td>
</tr>
<tr>
<td>Timeout</td>
<td>30 minutes (1800 seconds)</td>
<td>The minimum time threshold before an automatic failover event occurs.</td>
</tr>
</tbody>
</table>
If the secondary HTA determines during one of its health checks that the primary HTA is not healthy, the timeout clock starts. If during the timeout period, a subsequent health check determines the primary HTA is healthy, the timeout clock resets; otherwise, when the timeout clock expires the secondary HTA will automatically promote itself and become the primary HTA.

It is recommended that you configure both email (SMTP) and SNMP notifications when using HA. HA details are also logged in the `/var/log/asc/htcli.log` file. Refer to the *HyTrust Appliance Administration Guide* for details on configuring SMTP and SNMP notifications.

Primary HTA Setup

**Prerequisites**

Complete the initial HTA setup on an ESX or ESXi host for the primary HTA:

- Edit the HTA virtual machine settings using the vSphere Client and select the Network Connection 3 (eth2) Device Status checkboxes *Connected* and *Connect at power on*.
- Assign an IP address to network Connection 1 (eth0)—see Configuring the HTA Management Network Interface on page 19.
- Complete the HTA Management Console Installation Wizard—see Starting the HTA Management Console on page 20 and Initial Setup and Configuration on page 21.

**Steps**

1. Confirm that the primary HTA is powered on and finishes booting.
2. From the vSphere Client, open up the HTA console window and login using the *ascadminuser* credentials.

   **Note:** The *ascadminuser* password was modified during initial HTA setup.

3. Start the HA setup procedure. From the HTA command line interface, type:
   ```
   hasetup
   ```
4. At the *Please specify network settings for the Connection 1 (eth0) interface* prompts, confirm the settings assigned to the HTA. Press Enter each time when prompted to maintain the current setting.
5. After confirming the settings for IP, subnet mask, gateway, and DNS server, type:
   ```
   y
   ```
   to proceed to the next step.
6. At the *Deploy as primary (production) or secondary (standby)* prompt, type:
   ```
   pri
   ```
7. At the *Please specify network settings for High Availability services on Connection 3 (eth2) interface* prompt, enter a different IP address and subnet mask for Connection 3 (eth2) on the primary HTA.
8. To save your settings, type:
   ```
   y
   ```
9. Logout.

Primary HTA HA setup is now complete. Next, you must install and configure a second HTA instance and join the two HTAs to create an HTA HA cluster.
It is recommended that you use an isolated HA network to establish the Connection 3 (eth2) connection between the primary and secondary HTAs. For example, you can use the vSphere Client to create and configure a virtual network connection for the two HTA instances to use. Since the primary and secondary HTAs are on separate hosts, creating a new VLAN for HTA HA and trunking the physical switches that support the virtual infrastructure to handle the new VLAN is required. The eth0 and eth2 IP addresses must not be on the same subnet.

**Secondary HTA Setup**

1. From the vSphere Client, deploy a second HTA on a different ESX or ESXi host from the primary HTA—see Deploying the OVF Template on page 17.
2. Power on the secondary HTA—see Powering Up the Appliance on page 19.

<table>
<thead>
<tr>
<th>Note:</th>
<th>Before you login to the secondary HTA, go to Edit Settings for the HTA within the vSphere Client to confirm that Network Connection 3 (eth2) is connected to the proper network segment and the Device Status checkboxes <strong>Connected</strong> and <strong>Connect at power on</strong> are selected.</th>
</tr>
</thead>
</table>
3. From the vSphere Client, open up the HTA console window and login using the asadminuser credentials.

   Before you can proceed, a new password must be assigned to the secondary HTA local administrator account (asadminuser). Be sure to keep your new password in a safe and secure place.

<table>
<thead>
<tr>
<th>Note:</th>
<th>The asadminuser account is a local administrator account on each HTA, so the credentials for this account on the primary HTA and secondary HTA are independent.</th>
</tr>
</thead>
</table>
4. Start the HA setup procedure. From the HTA command line interface, type:

   hasetup

5. At the **Please specify network settings for the Connection 1 (eth0) interface** prompt, manually assign a static IP address, subnet mask, gateway, and DNS server to the management network interface of the secondary HTA.
6. Once you have assigned the static IP address, subnet mask, gateway, and DNS server, type:

   y

   to save the results and proceed to the next step.
7. At the **Deploy as primary (production) or secondary (standby)** prompt, type:

   sec

8. At the **Please specify network settings for High Availability services on Connection 3 (eth2) interface** prompt, enter an IP address and subnet mask for Connection 3 (eth2) of the secondary HTA.
9. To save your settings, type:

   y
10. At the **Join a primary appliance by specifying its (eth2) IP address and asadminuser password** prompt, specify the IP address and asadminuser password of the primary HTA.
High Availability

HA Systems Boot Order

Note: Make sure to use the new password (not the default) for the primary HTA ascadminuser account which was changed during setup.

This process may take several minutes as the secondary HTA establishes communication with the primary HTA.

If successful, the secondary HTA updates and displays the HyTrust High Availability (HA) System status as Enabled and the Mode as Secondary. The HA status is also updated on the primary HTA and shows the Mode as Primary after you refresh the CLI command window.

Note: The Last Sync date displayed in the CLI command window is in UTC.

11. After the HA system status updates, you can logout.

HA Systems Boot Order

Anytime you have to shutdown or restart the primary HTA, or after successfully completing the setup of both HTA HA systems, perform the following steps to boot the HTA HA systems (i.e., systems are synced):

1. Perform a clean shutdown of the secondary HTA.
2. Perform a clean shutdown of the primary HTA.
3. Start the primary HTA.
4. Start the secondary HTA after the primary has finished booting. (This is required to prevent automatic take-over.)

HA CLI Commands

All HTA HA operations are performed using the HTA CLI asc ha command. Using the vSphere Client, you can open the HTA console window and execute HTA CLI commands to perform HTA HA operations. For example, you can run the asc ha --status command from either the primary or secondary HTA to retrieve updated status for both HTAs in the cluster.

You can obtain help on the syntax of all HTA HA CLI commands and options using the following command:

```
asc ha --help
```

The following table provides a description of the most common HTA HA command options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d or --disband</td>
<td>Disconnect the HTA from the HA cluster. This can be run from the primary or secondary node.</td>
</tr>
<tr>
<td>Syntax:</td>
<td>asc ha --disband</td>
</tr>
</tbody>
</table>
**High Availability**

**HA CLI Commands**

**HyTrust Appliance Installation Guide**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| `-f` or `--failover` | Set the failover mode to either manual or automatic. In automatic failover mode the secondary can assume primary functions if the primary node has been offline for the specified timeout interval. Syntax:  
  
  \[ asc ha --failover \{auto|manual\} \]  
  
  Examples:  
  
  - To enable automatic failover:  
    \[ asc ha --failover auto \]  
  - To disable automatic failover:  
    \[ asc ha --failover manual \]  
| `--haclean`        | Clean old HyTrust HA sync data, keeping only the three most recent data sets. Syntax:  
  
  \[ asc ha --haclean \]  
| `-i` or `--interval` | Set the data synchronization period between nodes, in minutes, between 2 and 1440. The default is 10. Syntax:  
  
  \[ asc -i <minutes> \]  
  
  Example:  
  
  \[ asc -i 30 \]  
| `-j` or `--join`   | Join two nodes to create a HA cluster. This command can be run from either the primary or secondary node. Syntax:  
  
  \[ asc ha --join \{IP\} --password <Password> --mode <Mode> \]  
  
  Where:  
  
  - IP—The IP address of the remote HTA node (not the one you are running the command on).  
  - Password—The `ascadminuser` password of the HTA node specified by `IP`.  
  - Mode—The mode for this HTA node. Valid values are `primary` or `secondary`.  
  
  Example:  
  
  \[ asc ha --join 10.1.10.45 --password Pa$$w0rd123! --mode secondary \]
### Table 7-2  Most common HTA HA command options (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-o</code> or <code>--mode</code></td>
<td>Set the mode to primary (production) or secondary (standby). Changing the operational mode of an HA node will trigger a failover event. Syntax: asc ha --mode {primary</td>
</tr>
<tr>
<td><code>-p</code> or <code>--password</code></td>
<td>The password of the remote node. Required when joining a HA cluster. Optionally, the password can be supplied via the HTHAPW environment variable</td>
</tr>
<tr>
<td><code>-s</code> or <code>--sync</code></td>
<td>View the current configuration and operational state of the HA cluster. Syntax: asc ha --sync</td>
</tr>
<tr>
<td><code>--sshkeytest</code></td>
<td>Test the network connection between the two HTA HA nodes and verify the SSH keys. Syntax: asc ha --sshkeytest</td>
</tr>
<tr>
<td><code>-t</code> or <code>--status</code></td>
<td>View the current configuration and operational state of the HA cluster. Syntax: asc ha --status</td>
</tr>
<tr>
<td><code>-u</code> or <code>--timeout</code></td>
<td>Set the primary node monitoring minimum time threshold, in minutes, before an automatic failover event occurs. The minimum value is 10. Syntax: asc ha --timeout &lt;minutes&gt; Example: asc ha --timeout 10</td>
</tr>
</tbody>
</table>
Resource Tables and Checklists

This appendix contains the following sections:

- HTA Host and Appliance
- Protected Hosts
- Active Directory
- HyTrust High Availability

You should use the tables and checklists in this appendix to document the information required when planning and installing the HyTrust Appliance (HTA). You can reference this information as you set up and configure the HTA.

HTA Host and Appliance

<table>
<thead>
<tr>
<th>Table A-1</th>
<th>HTA Host and Appliance checklist</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Resource</strong></td>
<td><strong>Value</strong></td>
</tr>
<tr>
<td><strong>ESX Server for HTA</strong></td>
<td></td>
</tr>
<tr>
<td>ESX/ESXi FQDN</td>
<td></td>
</tr>
<tr>
<td>Service Console IP</td>
<td></td>
</tr>
<tr>
<td>Service Console Subnet Mask</td>
<td></td>
</tr>
<tr>
<td>Service Console Gateway</td>
<td>(in Router Mode: gateway = Connection 2 IP of HTA)</td>
</tr>
<tr>
<td>Host Type and Version (e.g., ESXi 4.1)</td>
<td></td>
</tr>
<tr>
<td>Root Password</td>
<td></td>
</tr>
<tr>
<td>Network separation method (physical, VLAN, tagged VLAN)</td>
<td></td>
</tr>
</tbody>
</table>
Note: The HTA does not support hosts with passwords that contains both the “<” and the “>” characters. However, passwords that have either character are supported.

Table A-2  Protected Hosts checklist

<table>
<thead>
<tr>
<th>Resource</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server to Protect</td>
<td></td>
</tr>
<tr>
<td>Server Name</td>
<td></td>
</tr>
<tr>
<td>Server IP</td>
<td></td>
</tr>
<tr>
<td>Server Subnet Mask</td>
<td></td>
</tr>
<tr>
<td>Service Gateway</td>
<td></td>
</tr>
<tr>
<td>(in Router Mode: gateway = Connection 2 IP of HTA)</td>
<td></td>
</tr>
<tr>
<td>Server VLAN ID</td>
<td></td>
</tr>
<tr>
<td>Server Version (e.g., vCenter Server 4.1)</td>
<td></td>
</tr>
<tr>
<td>Windows Server Edition</td>
<td></td>
</tr>
<tr>
<td>Administrator account &amp; password (Local or AD account)</td>
<td></td>
</tr>
<tr>
<td>vCenter Server Services credentials (Log On As)</td>
<td></td>
</tr>
</tbody>
</table>
Active Directory

Refer to the HyTrust Appliance Administration Guide for information on AD configuration.

☐ Verify AD service can be routed to Network Connection 1 of the HTA
☐ Create HTA service account
☐ Create 17 unique HyTrust Security Groups

<table>
<thead>
<tr>
<th>Table A-2</th>
<th>Protected Hosts checklist (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource</td>
<td>Value</td>
</tr>
<tr>
<td>VMware VirtualCenter Server (vpxd.exe)</td>
<td></td>
</tr>
<tr>
<td>VMware VirtualCenter Management Webservices (vctomcat)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ESX Server(s) to Protect</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESX/ESXi FQDN</td>
</tr>
<tr>
<td>Service Console IP</td>
</tr>
<tr>
<td>Service Console Subnet Mask</td>
</tr>
<tr>
<td>Service Console Gateway</td>
</tr>
<tr>
<td>(in Router Mode: gateway = Connection 2 IP of HTA)</td>
</tr>
<tr>
<td>Host Type and Version (e.g., ESXi 4.1)</td>
</tr>
<tr>
<td>Root Password</td>
</tr>
<tr>
<td>Service Console VLAN ID or NIC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table A-3</th>
<th>Active Directory checklist</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource</td>
<td>Value</td>
</tr>
<tr>
<td>Root Domain Name</td>
<td></td>
</tr>
<tr>
<td>Preferred Global Catalog</td>
<td></td>
</tr>
<tr>
<td>Domain Controller Name</td>
<td></td>
</tr>
<tr>
<td>DNS Server IP</td>
<td></td>
</tr>
<tr>
<td>HTA Service Account Name and credentials</td>
<td></td>
</tr>
</tbody>
</table>

HyTrust High Availability

Optional

☐ Locate second host to install secondary HTA
☐ Verify network connectivity of Host to Public and Protected network segments
Create isolated VLAN for HyTrust HA and create necessary vSwitch for Network connection 3 (eth2)

**Table A-4  HyTrust High Availability checklist**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection 1 of Primary HTA</td>
<td></td>
</tr>
<tr>
<td>■ IP</td>
<td></td>
</tr>
<tr>
<td>■ Subnet Mask</td>
<td></td>
</tr>
<tr>
<td>■ Gateway</td>
<td></td>
</tr>
<tr>
<td>■ DNS Server</td>
<td></td>
</tr>
<tr>
<td>■ VLAN ID</td>
<td></td>
</tr>
<tr>
<td>Connection 3 of Primary HTA</td>
<td></td>
</tr>
<tr>
<td>■ IP</td>
<td></td>
</tr>
<tr>
<td>■ Subnet Mask</td>
<td></td>
</tr>
<tr>
<td>Connection 1 of Secondary HTA</td>
<td></td>
</tr>
<tr>
<td>■ IP</td>
<td></td>
</tr>
<tr>
<td>■ Subnet Mask</td>
<td></td>
</tr>
<tr>
<td>■ Gateway</td>
<td></td>
</tr>
<tr>
<td>■ DNS Server</td>
<td></td>
</tr>
<tr>
<td>■ VLAN ID</td>
<td></td>
</tr>
<tr>
<td>Connection 3 of Secondary HTA</td>
<td></td>
</tr>
<tr>
<td>■ IP</td>
<td></td>
</tr>
<tr>
<td>■ Subnet Mask</td>
<td></td>
</tr>
</tbody>
</table>
Configuring the Windows Server 2008 Firewall

This appendix describes how to configure the Windows Server 2008 Firewall to work with the HyTrust Appliance (HTA). For details on configuring other Firewalls, refer to the appropriate documentation.

This appendix contains the following sections:
- **View and Modify Inbound Rules**

### View and Modify Inbound Rules

Configuring the Windows Server 2008 Firewall to work with the HTA requires you to use the Windows Server 2008 Firewall advanced configuration utility to change its Inbound Rules.

Perform the following steps:

1. Open the Start menu and select **Administrative Tools > Windows Firewall and Advanced Security**.
2. Click Inbound Rules in the left pane to view the current inbound firewall rules.
3. Locate the Remote Desktop (TCP-In) rule and confirm that it is disabled.
   - If it is enabled, select it and click the Disable Rule button in the Action pane on the right. (You could also right-click on it and choose Disable Rule from the context pop-up.)
4. Locate the VMware vCenter Server - HTTP rule.
   a. Select it and click the Properties button in the Action pane (or right-click on it and choose Properties from the context pop-up) to open its properties dialog.
   b. Click the Scope tab.
   c. In the Remote IP address section, select These IP addresses, and click the Add button.
   d. Select This IP address or subnet, enter the IP address of the HTA in the field, and click OK.
   e. Click OK in the Properties dialog to apply the changes.
   f. Repeat for the following rules:
View and Modify Inbound Rules

- VMware vCenter Server - HTTPS
- VMware vCenter Server - Web Services HTTPS
- VMware vCenter Server Web Services HTTP

You should now have all the necessary rules configured properly.

![Inbound Rules Table]

Figure B-1 Windows Server 2008 Firewall with Advanced Security Inbound Rules

Now, authentication and authorization to the vCenter Server can only be accomplished via the HTA.
## Network Access Requirements

This appendix describes the HyTrust Appliance (HTA) network protocol and port requirements.

The following tables list the required network protocol ports needed while implementing network access restrictions when deploying the HTA.

### Table C-1 HTA inbound traffic requirements

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Protocols</th>
<th>Ports</th>
<th>Interfaces</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>TCP</td>
<td>80</td>
<td>All</td>
<td>Including custom HTTP ports referenced in the HTA configuration.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>TCP</td>
<td>443</td>
<td>All</td>
<td>Including custom HTTPS ports referenced in the HTA configuration.</td>
</tr>
<tr>
<td>Ping</td>
<td>ICMP</td>
<td>Types 8, 11</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>Route Discovery</td>
<td>TCP, UDP</td>
<td>179, 2602, 2604</td>
<td>All</td>
<td>Only required for HTA Router Mode deployments. Route discovery services are disabled by default.</td>
</tr>
<tr>
<td>SNMP v2c</td>
<td>TCP, UDP</td>
<td>161</td>
<td>Network 1</td>
<td>SNMP is disabled by default.</td>
</tr>
<tr>
<td>SSH</td>
<td>TCP</td>
<td>22</td>
<td>All</td>
<td>Including custom SSH ports referenced in the HTA configuration.</td>
</tr>
<tr>
<td>vCenter Server Forwards</td>
<td>TCP, UDP</td>
<td>1–65535</td>
<td>All</td>
<td>vCenter Server plugins and Windows Server can require additional forwards in this port range.</td>
</tr>
<tr>
<td>vSphere</td>
<td>TCP, UDP</td>
<td>902, 903</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>Service Name</td>
<td>Protocols</td>
<td>Ports</td>
<td>Interfaces</td>
<td>Comments</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------</td>
<td>----------------</td>
<td>------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Active Directory</td>
<td>TCP, UDP</td>
<td>88, 389, 636</td>
<td>All</td>
<td>Active Directory communications LDAP and LDAPS.</td>
</tr>
<tr>
<td>DNS</td>
<td>TCP, UDP</td>
<td>53</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>TCP</td>
<td>80</td>
<td>All</td>
<td>Including custom HTTP ports referenced in the HTA configuration.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>TCP</td>
<td>443</td>
<td>All</td>
<td>Including custom HTTPS ports referenced in the HTA configuration.</td>
</tr>
<tr>
<td>Ping</td>
<td>ICMP</td>
<td>Types 8, 11</td>
<td>All</td>
<td></td>
</tr>
<tr>
<td>Route Broadcast</td>
<td>TCP, UDP</td>
<td>179, 2602, 2604</td>
<td>All</td>
<td>Only required for HTA Router Mode deployments.</td>
</tr>
<tr>
<td>SMTP</td>
<td>TCP</td>
<td>25</td>
<td>All</td>
<td>Required for sending SNMP alerts.</td>
</tr>
<tr>
<td>SNMP v2c Trap</td>
<td>TCP, UDP</td>
<td>162</td>
<td>All</td>
<td>SNMP alerts are disabled by default.</td>
</tr>
<tr>
<td>SSH</td>
<td>TCP</td>
<td>22</td>
<td>All</td>
<td>Including custom SSH ports referenced in the HTA configuration.</td>
</tr>
<tr>
<td>Syslog</td>
<td>TCP, UDP</td>
<td>514, 10514</td>
<td>All</td>
<td>Including custom Syslog ports referenced in the HTA configuration.</td>
</tr>
<tr>
<td>vCenter Server Forwards</td>
<td>TCP, UDP</td>
<td>1–65535</td>
<td>All</td>
<td>vCenter Server plugins and Windows Server can require additional forwards in this port range.</td>
</tr>
<tr>
<td>vSphere</td>
<td>TCP, UDP</td>
<td>902, 903</td>
<td>All</td>
<td></td>
</tr>
</tbody>
</table>