Cisco ACE XML Gateway

Installation and Administration Guide

Software Version 5.1

Cisco Systems, Inc. | 170 West Tasman Drive | San Jose, CA 95134-1706 | 800 553-6387

The Cisco ACE XML Gateway is an application oriented networking product.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/)

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes LibCURL. cURL is © 1996 - 2004, Daniel Stenberg, <daniel@haxx.se>. All rights reserved.

This product includes libxslt, the XSLT C library developed for the Gnome project, and libxml2 Libxslt is based on libxml2 the XML C library developed for the Gnome project.

This product includes OpenLDAP Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved.

This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/). [Net-SNMP]

This product includes software developed by the University of California, Berkeley and its contributors.

The regular expression support is based on Henry Spencer's POSIX 1003.2 compliant regex package that has Copyright 1992, 1993, 1994 Henry Spencer. All rights reserved.

AG5.1-070524-0845-a

OL-13877-01

CONTENTS

CHAPTER 1

Introduction

This chapter introduces the Cisco ACE XML Gateway. It covers the following topics:

1.1 About the Cisco ACE XML Gateway

The Cisco ACE XML Gateway, a component of the Cisco Application Control Engine (ACE) family of products, brings application intelligence to the network. It enables efficient deployment of secure, reliable, and accelerated Web service environments based on XML (Extensible Markup Language) and SOAP (Simple Object Access Protocol).

The ACE XML appliances are delivered as rack-mountable and desktop units. The developer's edition of the appliance (or "Gateway-D") is provided in a desktop-style housing. Although functionally similar to the full-sized appliance, the Gateway-D is intended for evaluation, development, and testing settings.

The administration server for an ACE XML implementation is the ACE XML Manager. The ACE XML Manager acts as the development and monitoring point for the system. It serves the web console, the browser-based interface for configuring and monitoring the system.

An ACE XML appliance can operate in the mode of gateway or manager. It can also be set for standalone operation, in which it acts as both gateway and manager. This is the configuration most often used for evaluation and development environments purposes.

This book describes how to install the ACE XML Gateway and Manager appliances in a network and perform their initial configuration. This book assumes that you are familiar with basic network administration. For

example, you should be comfortable adding a new host to a network and setting up its domain name, IP address, and DNS settings. You should be comfortable logging in to a UNIX terminal session, since the initial configuration of the ACE XML appliances is performed from a terminal interface.

This book focuses on appliance-level setup and administration. For information on how to configure the ACE XML Gateway policy—the set of rules and behaviors that controls traffic-handling at the system—see the *Cisco ACE XML Gateway User's Guide*.

Important: Modifying the system in ways other than as described by the Cisco ACE XML Gateway documentation or as directed by Cisco support may lead to an unmaintainable and unsupported system.

In particular, such changes may prevent software updates from working correctly and lead to hardware and software interoperability issues. These types of changes include operating system-level configuration changes, installation of unsupported third-party software, or the use of undocumented operating system tools or commands.

1.2 System Administration Tools

There are two primary user interface environments used to configure and manage the ACE XML Gateway:

- The appliance shell is the command-line interface for use by administrators and installers of the system. This is where you perform the initial configuration of the appliance. You can also manage disk space, start and restart processes, and set up hardware utilization.
- The ACE XML Manager web console is a browser-based interface used for the day-to-day management of the system. Console users develop Gateway policies, deploy them to the ACE XML Gateways, and monitor system and network status.

With a few exceptions, the tasks described in this document are performed from the shell. The Cisco ACE XML Gateway *User's Guide* provides instructions that primarily involve the ACE XML Manager web console.

1.3 Installation and Startup Overview

For each Cisco ACE XML Gateway and Manager appliance to be installed, you will need to take the following steps:

1. Verify serial numbers on the hardware items received.
2. Access the shell using a monitor and keyboard connected to the appliance or the serial port connection from a workstation.

   For instructions, see Chapter 3, "Setting Up the Appliance."
3. Log into the shell as the `root` user.

   For details, see Section 4.3, "Logging In to the Appliance Shell."
4. Change the root password from its default value.
5. Configure network settings, including the IP address of the appliance, hostname, default gateway, and so on.

   For details, see Section 5.3, "Configuring the Appliance."
6. Specify the operating mode of the appliance, either as a gateway, manager, or standalone machine.

   For details, see Section 5.4.1, "Standalone Mode," Section 5.4.2, "Manager Mode," or Section 5.4.3, "Gateway Mode."
7. Ensure that the system clock is correctly set or configure the appliance to use a Network Time Protocol server.

   In most cases, you should not need to set the system clock, as it is preset before delivery. However, if you need to adjust the system time or configure the machine to use an NTP server, see Section 5.5, "Setting the System Clock."
8. Optionally, configure SNMP settings.

   For details, see Chapter 12, "Monitoring the ACE XML Appliance Remotely."
9. Enable the hardware-based SSL acceleration if the appliance is equipped with this option.

   For details, see Section 9.1, "Enabling SSL Acceleration."
10. Set up an nCipher security world hardware keystore if the appliance is equipped with these options.

    For details, see Chapter 7, "Using Hardware Keystores and Security Worlds."
11. Replace the default audit log signing credential.

For details, see Section 8.3, "Changing the Audit Log Signing Credential."

12. When you have completed these tasks for the appliances in your installation, restart all processes in your system.

    For details, see Section 6.3, "Restarting a Cluster."

13. Optionally, use the shell interface to create accounts for additional administrators.

    For details, see Section 11.2, "Creating Appliance User Accounts."

Upon completion of these steps, the ACE XML appliance will be ready for use. By default, the ACE XML Gateway refuses all service traffic addressed to it. To expose services to consumers through the ACE XML Gateway, you must use the ACE XML Manager to develop and deploy a policy. For details, see the *Cisco ACE XML Gateway User's Guide*.

CHAPTER 2

Planning Your Installation

This chapter describes planning considerations for installing Cisco ACE XML Gateway and Manager appliances. It covers these topics:

2.1 Planning Overview

The ACE XML Gateway relies on a variety of agreements, protocols, and physical connections in its daily operations. Implementing the ACE XML Gateway involves configuring the settings on the appliance. In addition to configuration requirements on the appliance itself, installing the appliance usually requires adjustments in the surrounding network, for example, by configuring adjacent firewalls or management hosts.

Before starting your installation, it is recommended that you gather as much information as possible on the target environment. Such advance planning can ease the task of installing and maintaining the appliance.

The ACE XML appliances can be deployed to several types of target environments:

- In a production setting, one or more clusters ACE XML Gateways reside in the network DMZ, often behind a load balancer. In this setting, they receive external requests and communicate with backend servers within and outside the organization.
- In a development setting, the ACE XML Gateway resides within the protected network, where it is used for policy development and testing.

- Each ACE XML Gateway needs to be in the administrative control of a single ACE XML Manager. Gateway policy developers will need access to the manager's web interface. However, the ACE XML Manager should normally be contained within an internal, protected network, and not exposed to external traffic.

2.2 Ports Used by the ACE XML Gateway and Manager

For ACE XML appliances to function properly in your network, you need to ensure that existing network elements, such as internal firewalls, permit the types of traffic used by the appliances.

In particular, the firewalls affected by an ACE XML Gateway and Manager installation may include:

- Firewalls between each ACE XML Gateway and the ACE XML Manager that controls it.
- Firewalls between the ACE XML Manager and the computer used to access the web console.
- Firewalls between the Gateway and the external network.

The following sections list the ports that may need to be opened.

2.2.1 System Traffic Ports

The following ports are used by the ACE XML system for operation purposes (that is, for traffic other than service traffic). This information should be used to configure internal firewalls. The use of a port is implementation-specific. For example, if you do not use NTP, you do not have to configure firewall to permit TCP/UDP traffic on port 123.

The ACE XML Manager uses the following ports and protocols:

- ICMP from anywhere
- TCP on port 22 from anywhere. This port exposes SSH, for administrators who want to start terminal sessions on the ACE XML Manager.
- TCP on port 8243 from anywhere. This port exposes the ACE XML Manager web console for browser access.

  Optionally, you can configure the ACE XML Manager to present its web console on another port.
- UDP on port 53 from anywhere. The ACE XML Manager uses this port to perform DNS lookups.

- UDP on port 161 from anywhere. This port enables the ACE XML Manager to receive SNMP queries.
- UDP on port 514 only from identified ACE XML Gateways. The ACE XML Manager listens on this port to receive syslog information from the Gateways. This information is aggregated to make up the event logs.

On the Gateway, traffic is passed on the following ports and protocols:

- ICMP from anywhere
- TCP on port 22 from anywhere. This port exposes SSH, for the sake of administrators who want to start terminal sessions on the Gateway.
- TCP on port 8200 only from the ACE XML Manager. The Gateway requires this port to be open so that it can receive control messages from its ACE XML Manager.
- UDP on port 53 from anywhere. This port enables the Gateway to perform DNS lookups.
- UDP on port 161 from anywhere. This port enables the Gateway to receive SNMP queries.

Each Gateway sends traffic to its ACE XML Manager on the ports opened on the ACE XML Manager for that purpose. Additionally, the ACE XML Manager and Gateway appliances may generate network traffic on the following ports:

- TCP/UDP on port 123, for Network Time Protocol (NTP).
- TCP on port 25, to send email alerts via SMTP.
- UDP on port 162, for SNMP traps.

2.2.2 Service Traffic Ports

When configuring an external firewall to accommodate an ACE XML installation, in addition to allowing traffic for ports required for system traffic mentioned in Section 2.2.1, "System Traffic Ports," you need to account for service ports in the policy.

The ports used for service traffic vary by policy, but generally include ports 80 and 443, for standard HTTP and HTTPS traffic, respectively.

2.2.3 Considerations for Load Balancers

Best performance can usually be achieved by placing multiple ACE XML Gateways behind one or more load-balancing devices. You do not need to place a load balancer ahead of a dedicated ACE XML Manager appliance or Gateway-D, since they are not usually subject to high volumes of traffic.

The number of load balancers to use depends on the amount of traffic you expect each Gateway to handle, as well as the specifications of the load-balancers. For assistance in determining the number of load-balancers you'll need, contact the manufacturer of the load-balancer.

Load balancers need to be able to monitor the Gateways for availability. The ACE XML Gateway supports application-level monitoring—the load balancer can send an HTTP request to the Gateway and get back an HTML page or SOAP message that indicates the health of the Gateway.

To configure a response to a health check from a load balancer, configure a static response message on a port object in the policy. For more information, see the chapter "Opening Ports on the Gateway" in the Cisco ACE XML Gateway *User's Guide*.

2.3 Appliance Network Interface Considerations

ACE XML appliances use Ethernet for networking communications. They do not support other kinds of networks, such as token ring or PS/2 networks. For full Gigabit Ethernet performance, the cabling that composes your network must be rated at CAT 5e or better. The appliances accept standard RJ-45 Ethernet connectors.

The 1U platform is equipped with four network interfaces on which it can accept service traffic (an additional RJ-45 interface is dedicated to connectivity for the Integrated Lights-Out module). The interfaces can be configured to run at full-duplex 10baseT, 100baseT or gigabit Ethernet speeds.

Although the interfaces can be configured to negotiate this setting automatically, you'll obtain best performance by avoiding the use of auto-negotiation and setting each interface to a specific speed. The reason for this recommendation is that the time required to auto-negotiate bandwidth settings inflicts a small amount of performance overhead. Changing network conditions may cause unnecessary re-negotiation of bandwidth settings, again reducing performance. Problems with other network devices, such as firewalls and routers, may propagate unnecessarily slow performance when using auto-negotiate bandwidth. Theoretically, one malfunctioning router could cause all of the auto-negotiating ACE XML Gateways that work with it to bottleneck all the traffic they handle, potentially reducing bandwidth in zones that have nothing to do with the failed router.

Auto-negotiation can make performance issues harder to track down; conversely, hard-wired bandwidth settings will, in most cases, allow you to identify a malfunctioning router, firewall or ACE XML Gateway quickly.

2.3.1 IP Addresses for Gateways

Depending on the model of the ACE XML appliance, the appliance chassis can have up to five Ethernet ports. The Integrated Lights-Out (iLO) port is for management purposes only, and not intended for service traffic.

Typically, the use of a single interface and IP address is sufficient for handling traffic for the ACE XML Gateway. In some cases, administrators may choose to separate service traffic from ACE XML Manager traffic addressed to the Gateway onto two different Ethernet ports. This is an optional configuration, however, meant to enhance security.

Another configuration option involves having multiple IP addresses associated with a given Gateway interface, and accepting traffic for various services on different virtual hosts. To do so, you will need to specify the addresses in the network configuration of the Gateway appliance, as described in this guide. In the policy, you then associate ports definitions with the additional IP address. For more information on configuring ports, see the *Cisco ACE XML Gateway User's Guide*.

2.3.2 IP Addresses for Managers

Each ACE XML Manager uses only one Ethernet port and one static IP address. On appliance chassis that have multiple physical Ethernet ports, you can use any Ethernet port to connect the ACE XML Manager to the network.

By default, the ACE XML Manager presents the web console on TCP port 8243. However, you can configure the ACE XML Manager to use another port if desired.

For extra security, some network administrators place Manager appliances behind their own firewall. Typically, this firewall resides within the corporate intranet, which is behind the DMZ. The resulting configuration places a minimum of three firewall barriers and at least one Gateway between production Manager appliances and packets arriving from the extranet.

2.3.3 IP Addresses for Gateway-D Appliances

The Ethernet ports, logical ports, and IP address configurations for a Gateway-D are similar to those described for Manager and Gateway appliances. Because a Gateway-D is usually dedicated to development or QA purposes, it is common for such machines to reside behind its own additional firewall—the one that actually creates the QA or Development zone within the DMZ network.

2.4 Obtaining the Root Password

Before starting, you'll need the password for the root account on each appliance to configure the appliance. To obtain this password, contact your Cisco ACE XML Gateway support representative.

CHAPTER 3

Setting Up the Appliance

This chapter describes how to get the ACE XML Gateway appliance ready to install in a network. It covers these topics:

3.1 Installation Overview

The first step in setting up the ACE XML Gateway or ACE XML Manager is to perform the physical installation of the appliance.

The first time you start each ACE XML appliance, you'll need to use a monitor and keyboard connected directly to the appliance to perform the initial configuration of the appliance. Alternatively, you can attach a personal computer or laptop with VT100 compatible terminal emulation software or dumb terminal to the appliance by serial cable.

After the initial configuration, you can perform day-to-day administration tasks from the ACE XML Manager web console or by SSH session on a remote host, as described in Chapter 4, "Accessing the Shell Interface."

As of release 5.1, the Cisco ACE XML Gateway is delivered on the HP ProLiant DL360 G5 server. This guide provides the platform information needed to get the ACE XML Gateway up and running.

For complete information on the server platform, refer to the HP documentation on the HP ProLiant DL360 G5.

3.2 Racking the Appliance

An ACE XML appliance is a key component of your network security infrastructure. As such, its physical as well as network security must be ensured. To prevent unauthorized individuals from tampering with appliances, the appliances should be deployed securely in a lockable cabinet or closet.

The Cisco ACE XML Gateway version 5.1 appliances come in a 1U rack-mountable case with the following dimensions:

- Height: 4.32 cm (1.70 in)
- Depth: 69.22 cm (27.25 in)
- Width: 42.62 cm (16.78 in)

Note: The Gateway-D appliance is intended for desktop placement, and not suitable for rack mounting.

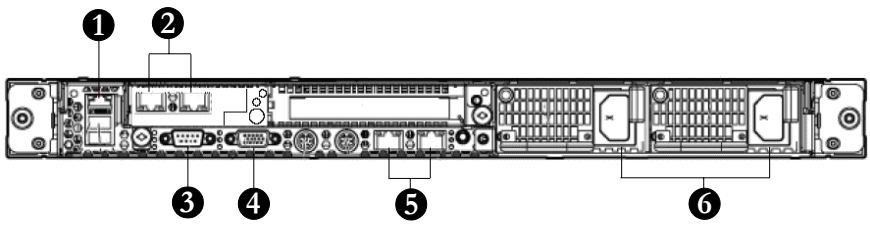
All ACE XML appliances require a properly grounded, three-prong AC connection. Make sure that the rating of the electrical circuit supplying power is adequate to supply power to the rack without overloading. Verify the continuity of ground.

We recommend that you place a surge suppressor or other power conditioner in-line between the ACE XML appliance and the AC wall outlet. To mitigate the effects of power failure, you may wish to also use an uninterruptible power supply (UPS), which provides temporary, battery-powered AC voltage for a fixed period of time (typically, 5 to 30 minutes) in the event of a power failure.

3.3 Back Panel Diagram

The following figure shows the back panel of the ACE XML Gateway and ACE XML Manager.

Figure 3-1: Cisco ACE XML appliance back panel



As highlighted by the callouts in Figure 3-1, the back panel includes the following features:

1. iLO 2 NIC
2. NIC 3 (eth0) and NIC 4 (eth1)
3. Serial connector
4. Video connector
5. Integrated NIC 1 (eth2) and NIC 2 (eth3)
6. Power supply bays 1 and 2

As listed, there are five NIC connectors on the back panel. However, the NIC connector shown as callout 1 in Figure 3-1 is intended for Integrated Lights-Out 2 (iLO 2) connectivity only, and not service traffic.

The iLO module can be used for certain maintenance tasks, such as remotely starting and stopping the appliance. For more information on using the iLO module to access the appliance, contact your Cisco ACE XML Gateway support representative or refer to the HP ProLiant DL360 G5 documentation.

3.4 Prepare the Appliance for Installation

Take the following steps to complete the physical installation of each ACE XML Gateway appliance:

1. Unpack the system.

   Save the packing materials, accessories, and documentation in case you need them later.

2. Install the ACE XML Gateway appliance in its rack.

   Consult the information provided with your rack hardware for detailed mounting instructions.

3. Connect a monitor and keyboard to the appliance or connect to the appliance from a workstation by serial cable.

   You can connect a keyboard and monitor directly to the appropriate connectors on the back panel of the rack-mounted appliance or Gateway-D. The appliances include a console port on the back panel, and USB connectors for input devices such as a keyboard. (The Gateway-D has USB and PS/2 input connectors.)

   Alternatively, connect to the serial port on the appliance by a serial cable from a laptop or personal computer. However, by default, boot messages are printed to the video console output rather than serial output. To have boot messages output to the serial console,

you'll need to access the appliance by video console first to modify the configuration. For more information access, see Section 4.2, "Accessing the Login Prompt by Serial Connection."

4. Connect an Ethernet network cable to the appliance.

   Depending on the model of your appliance, the back panel has up to four Gigabit Ethernet ports that can be used for service traffic. The Gateway-D appliance provides a single Ethernet port.

   Note: To realize full Gigabit Ethernet performance, your network must use CAT 5e Ethernet cable end-to-end.

5. After connecting all other cables, connect the power cables.

   Rack-mounted ACE XML Gateway appliances provide two redundant, hot-swappable power supplies. To help prevent loss of power, you should connect both power supplies to a power source. For initial configuration or testing, you may choose to use the standby power supply only. The Gateway-D appliance provides a single power supply and a single power port.

3.5 Turning on the Power

After connecting the power cables, wait a moment before powering up the appliance. You can then power up the ACE XML Gateway appliance by pressing the power button. The location and appearance of the power button varies by hardware platforms for the ACE XML Gateway appliance:

- On new models of the rack-mounted chassis, the power button is on the right side of the front panel.

  Note: For power button location and other hardware considerations applicable to older models, refer to the documentation provided with your hardware.

- On the Gateway-D, the power switch is towards the top of the front panel.

When powered on, the system begins its start-up sequence. Note that boot sequence output is written to console output only. When complete, the Shell interface login screen appears.

3.6 Next Steps

After accessing the login for the ACE XML Gateway appliance, you can use the Shell interface to configure the basic network settings and operating mode of the appliance.

For information on accessing and getting around the Shell interface, see the next chapter, Chapter 4, "Accessing the Shell Interface."

CHAPTER 4

Accessing the Shell Interface

This chapter provides instruction on accessing the appliance shell menu. It covers these topics:

4.1 About the Shell Interface

The ACE XML Shell interface lets you configure appliance-level settings for the appliance. Once these settings are configured, the appliance can be managed and configured from the ACE XML Manager's web console.

> **Note:** The shell interface should not be confused with the ACE XML Manager web console. The shell is accessed by console connection or client terminal session, while the web console is the browser-based interface for developing a policy.

To perform the initial configuration described in this guide, you will need to access the shell interface on the appliance. To do so, use either a monitor and keyboard attached to the appliance or a computer connected by serial port to the appliance.

After configuring the settings described in this chapter, you will be able to access the shell interface of an appliance using any standard method of establishing a terminal session, either connected by serial connection or over the network with an SSH client, such as PuTTY.

4.2 Accessing the Login Prompt by Serial Connection

Instead of a direct video console connection, you can connect to the appliance using a laptop or personal computer connected by serial cable.

While you can access the appliance operating system by serial connection at any time, in its initial default configuration, the appliance writes boot messages to video console output only. To change this setting, see Section 11.5, "Configuring Serial Console Boot Control."

The serial connector is a DB-9-type connector. As shown in Figure 3-1, the serial connector appears on the left side of the back panel of the appliance. (Previous models may provide RJ-45 serial ports. However the current and Dell-model platforms only have a single DB-9 connector available for serial connections).

The connecting laptop or personal computer needs to have VT-100-compatible terminal emulation software, such as HyperTerminal or SecureCRT.

Configure the connection to use the following settings:

- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow Control: None

4.3 Logging In to the Appliance Shell

Once you've accessed the appliance shell, follow these steps to install the appliance on your network:

1. Power on the ACE XML Gateway appliance if it is not already running.
2. At the login prompt, enter the username of a user account on the appliance. For most administrative tasks, you need to log in as `root` user.
3. At the password prompt, enter the user's password. If you don't have it, you can obtain the `root` password from your system administrator or from Cisco support.

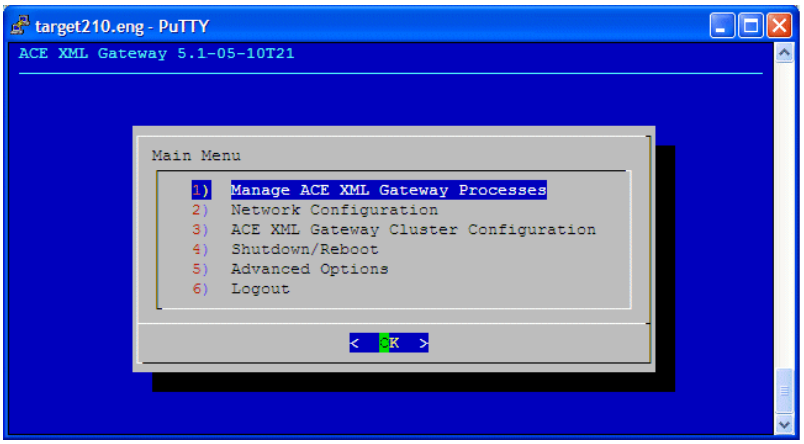
   If this appliance still uses the factory-default password, you are prompted to change the default password. Otherwise, the **Main Menu** appears.

4. If prompted to change the password, choose **OK** to change the password now.

   For security reasons, we recommend that you change the password from its default value. However, the interface does not require you to do so. To bypass changing the password for now, press the escape key.

   After entering a new password or bypassing the password change screen, the **Main Menu** appears, as shown in Figure 4-1.

Figure 4-1: Main Menu



You can now perform the initial set up of the appliance, as described in Chapter 5, "Performing the Initial Configuration."

4.4 Navigating the Administration Interface

The following tips apply to navigating the console menu:

- To select a menu item, type its number. Alternatively, you can use the arrow keys on your keyboard to select menu items.
- Most screens require you to choose **OK** or **Cancel** after entering input.
- To have the system accept your input, select the **OK** item and press the **Enter** key. To exit a screen without making any changes, select the **Cancel** item and press the **Enter** key.

For an overview of the menus in the interface, see Chapter 14, "Shell Menu Reference."

4.5 Accessing the bash Shell

While most administration tasks can be accomplished in the console menu, you may occasionally need to access the bash shell command prompt to accomplish other tasks.

4.5.1 Running bash

To run the bash shell, take the following steps:

1. Log into the ACE XML Shell as the `root` user.

   The **Main Menu** appears.

   For more information, see Section 4.3, "Logging In to the Appliance Shell."

2. Choose **Main Menu > Advanced Options > Run bash**.

The `bash` command prompt appears. You may now use this shell as you would in a typical Linux environment.

4.5.2 Exiting bash

You can exit the `bash` shell by entering the `exit` command. When you do so, the **Advanced Options** menu appears, from where you can return to the main menu or choose other options in the **Advanced Options** menu.

CHAPTER 5

Performing the Initial Configuration

This chapter describes how to configure network settings for a ACE XML Gateway and Manager appliances. It covers these topics:

5.1 Initial Configuration Overview

The initial configuration installs the ACE XML appliance on the network, giving it an IP address and other basic network settings. It also sets the operating mode of the appliance.

The appliance can operate in one of several modes—as a Gateway, Manager, or standalone appliance (in which the appliance acts as both). A Gateway can operate alone or in a cluster. A cluster is a group of Gateways that apply a common policy and that are controlled by a single ACE XML Manager. A Manager can manage one cluster or many, each with a different policy or version of a policy.

When configuring the initial settings for an appliance that will act as a Gateway, you set the IP address of the Manager that will control it. In turn, you must identify the controlled Gateways in the Manager configuration. However, that step is done in the ACE XML Manager web console.

5.2 Before Starting

Before starting the initial configuration procedure, be sure you have the following information:

- IP address and subnet mask to be given to the appliance. The Gateway must be configured with a static IP address. The appliance does not support the use of dynamic IP addressing schemes such as BOOTP or DHCP.
- IP address of the default gateway in the target network.
- IP address of the primary name server for the network to which the appliance is connected.
- The password for the root account on the appliance.

Caution: Make sure you have this information before starting to configure the appliance. Entering incorrect information can render your appliance inoperable.

5.3 Configuring the Appliance

This section describes how to perform the configuration tasks required to set up an ACE XML appliance. They include configuring network settings for the appliance and setting its operating mode, whether it should act as a Manager, Gateway, or both.

While these steps assume that you are configuring the appliance for the first time, any portion of these instructions may be applicable when you want to adjust the appliance's settings or reconfigure it completely.

To perform the initial configuration of the appliance:

1. Log into the Shell interface as `root` user as described in Section 4.3, "Logging In to the Appliance Shell."

   First, you will configure the basic network settings for the appliance, such as hostname and IP address.
2. In the **Main Menu**, choose the **Network Configuration** item.
3. Choose the **Hostname** item from the **Network Configuration** menu.

   The shell prompts you to enter the fully-qualified name of this appliance.
4. In the field, type the fully-qualified hostname for the appliance, such as `xmlgate.example.com`

If a name has been reserved on your network for the use of the ACE XML Gateway appliance, type that name in the field provided. Otherwise, you may enter a placeholder name (but don't use a valid name that belongs to a different appliance in the network!).

When you enter a value, the **Main Menu** appears.

5. Choose the **IP Gateway** item from the **Network Configuration Menu**.

   The **Default IP gateway of this machine** screen appears.

6. Enter the IP address of the default gateway or router that connects this appliance to your network and enter **OK**.

   You may need to consult your local network administrator to obtain the gateway address.

7. In the **Network Configuration** menu, choose the **Name Servers** item to configure the appliance connection for domain name servers.

8. Enter one or more IP addresses for valid DNS servers for the appliance. If entering more than one address, use spaces to separate multiple IP addresses.

   If more than one address is configured, the Gateway will attempt to use the first server for all lookups. If the first server fails to respond after a brief timeout period, the Gateway sends the lookup to the next server in the list.

9. Configure the Ethernet interface 0 by choosing the **Interface eth0** item from the **Network Configuration** menu.

   The shell displays a screen in which you can enable or disable the the specified Ethernet interface.

10. Choose the **enabled** item.

    The shell displays a screen in which to specify one or more IP addresses under which the enabled Ethernet interface is to appear.

11. Enter the IP address to be associated with this interface.

    When entering more than one address, use spaces to separate multiple IP addresses. The first address in the list is the assigned address, and the appliance aliases subsequent addresses in the list to the first IP address in the list.

    Note: Assign only static IP addresses to the network interface. Each address must be a valid static address assigned to the ACE XML appliance by your network administrator. Do not use DHCP or other dynamic addressing schemes to assign

addresses to ACE XML appliances. The Gateway cluster and ACE XML Manager require stable, static IP addresses for correct operation.

12. Enter the netmask that specifies the network and host portions of the IP address you entered. You may need to consult your network administrator to obtain the netmask value to use.

    The shell displays a screen in which you can specify the speed at which this Ethernet port operates.

13. Choose an Ethernet speed or choose the **auto** setting.

    The shell displays the **Ethernet duplex** screen or the **Edit Static Routes** screen.

    In the Ethernet speed screen, choose:

    - **10,** to specify 10baseT
    - **100,** to specify 100baseT
    - **1000** to specify gigabit Ethernet speed
    - **auto** to enable the appliance to configure its Ethernet settings automatically.

    Note: For maximum throughput, do not choose the **auto** setting. For more information on the performance impact of negotiating port speed automatically, see Section 2.3, "Appliance Network Interface Considerations." Also note that to realize full Gigabit Ethernet performance, your network must use CAT 5e Ethernet cable end-to-end.

14. If the shell displays the Ethernet duplex screen, choose a **half-duplex** or **full-duplex** connection.

    The shell displays the **Edit Static Routes** screen.

    If the shell does not display the Ethernet duplex screen, go to the next step.

15. If static routes need to be defined for this appliance, choose **Add new route**. Otherwise, go to the next step.

    Static routes are most commonly needed in a dual-homed appliance configuration, in which the appliance has different separate interfaces on different subnets.

16. Enter a static route in the format specified if needed. If no static routes are required for this appliance, you can skip this step.

When finished, the shell displays the **Edit Static Routes** screen with the new route. If the shell discovers errors in the static route you entered, it displays a screen in which you can make corrections to the route and attempt to enter it again.

To add more static routes, choose the **Add new route** item as necessary to enter all static routes that affect traffic destined for this appliance.

17. When you are finished adding static routes, choose the **Accept settings** item.

    The **Commit the following new settings?** screen appears.

18. To commit the configuration changes, choose **Yes** in the **Commit the following new settings?** screen. To exit the **Network Configuration** menu without changing any settings, choose **No** in the **Commit the following new settings?** screen.

    If you choose **Yes**, the appliance restarts the interface using the new settings, then returns to the **Network Configuration** menu. If the appliance cannot reconfigure the network as your settings specify, it displays an error message, enabling you to check and retry your network settings without restarting the appliance.

19. To enable traffic on another interface, choose the interface item (such as **Interface eth1**) from the **Network Configuration** menu and repeat the steps used to configure the eth0. The specific values you assign for this port's settings may vary according to this appliance's function and its location on your network.

    Note: The Gateway-D appliance provides only one physical Ethernet port.

20. To review your configuration choices, choose the **View Routing Table** item from the **Network Configuration** menu.

    The Kernel IP routing table screen appears. If you cannot see the entire table, you can use the arrow keys on your keyboard to scroll through it.

21. To dismiss the routing table, choose the **Exit** item.

    The **Network Configuration** menu appears.

22. To test your network settings, choose the **Test Network Settings** item from the **Network Configuration** menu.

    The **Network Configuration Tester** checks the basic settings affecting each currently-configured Ethernet interface.

23. To exit the **Network Configuration Tester** screen, press the **Enter** key.

If the appliance's network configuration settings are valid, the **Network Configuration** menu appears.

Otherwise, the **Network Misconfigured** screen appears. In this case, choose **OK** to return to the **Network Configuration** menu and, from there, return to any of the previous screens to correct configuration errors.

24. From the **Network Configuration** menu, choose the **Return to Main Menu** item to continue set the operating mode for the appliance.

25. Now set the operating mode for this appliance by either:

    - Selecting **Yes**, if prompted in the **verify cluster settings** screen to select the operating mode for this appliance.
    - If you are in the **Main Menu**, choose **ACE XML Gateway Cluster Configuration** item.

    The current mode for the appliance is highlighted in the **This machine should act as a** screen. Complete the configuration based on the desired operating mode of the appliance, from these options and by using the instructions at the linked section:

26. In the **This machine should act as a** screen, choose the cluster configuration this appliance is to have:

    - To configure this appliance for Gateway operation:

      a. Choose the **ACE XML Gateway Cluster Member** item.

      b. **Enter** the IP address of the ACE XML Manager appliance that is to control this Gateway.

    Note: For step-by-step instructions on this configuration, see Section 5.4.3, "Gateway Mode."

    - To configure this appliance as a manager, choose the **ACE XML Manager** item. You will need to specify the Gateways in this Manager's control later from the Manager web console, as described in the *User's Guide*.

    Note: For more on this configuration, see Section 5.4.2, "Manager Mode."

    - To configure this appliance as a standalone appliance, choose the **Both Gateway and Manager** item.

    Note: For more on this configuration, see Section 5.4.1, "Standalone Mode."

    - To disable all Gateway and Manager processes until re-enabled explicitly, choose the **Inactive machine** item.

Note: For more on this configuration, see Section 5.4.4, "Inactive Mode."

You are prompted to restart using the new networking settings.

27. It is suggested that you restart the services running on the appliance at this time by clicking **Yes**.

    To exit this screen without restarting, choose **No**. However, you will need to restart the services later to have your changes take effect. To do so, choose the **Main Menu > Manage ACE XML Gateway Processes > Restart All Configured Services** item.

28. If prompted, click **OK** to acknowledge the notice regarding adding Gateways to this Manager. You will need to do so later from the web console.

Congratulations! You have completed the initial configuration of your appliance. You can now put the appliance into service or configure optional features.

5.4 Setting the Operating Mode for the ACE XML Appliance

While performing the initial setup of the appliance, as described in Section 5.3, "Configuring the Appliance," you were prompted to specify the operating mode of the appliance. You can have it act as a Gateway, Manager, or both. This section provides more information on that configuration.

You can access the operating mode settings at any time by selecting **3) ACE XML Gateway Cluster Configuration** in the Main Menu.

The appliance can operate in these modes:

- Standalone Mode
- Manager Mode
- Gateway Mode
- Inactive Mode

5.4.1 Standalone Mode

A single ACE XML appliance can act as both Gateway and Manager. This configuration is useful for evaluation or development purposes.

Note: This section provides details on step 26 in Section 5.3, "Configuring the Appliance." For information on configuring your appliance's network settings,

see the other steps in Section 5.3, "Configuring the Appliance."

To configure the appliance to operate as a standalone appliance:

1. Log into the Shell as the `root` user.

   For more information, see Section 4.3, "Logging In to the Appliance Shell."

2. From the **Main Menu**, **Choose** the ACE XML Gateway **Cluster Configuration** item.

3. Configure the appliance for standalone operation by choosing the **Both Gateway and Manager** item from the **This machine should act as a** screen.

   You are prompted to restart using the new networking settings.

4. It is suggested that you restart the services running on the appliance at this time by clicking **Yes**.

   To exit this screen without restarting, choose **No**. However, you will need to restart the services later to have your changes take effect. To do so, choose the **Main Menu > Manage ACE XML Gateway Processes > Restart All Configured Services** item.

5. If prompted, click **OK** to acknowledge the notice regarding adding Gateways to this Manager. You will need to do so later from the web console.

You've completed the basic configuration of your ACE XML appliance as a standalone appliance. You can now put the appliance into service or configure optional features.

5.4.2 Manager Mode

An ACE XML Manager is the policy development interface and system monitoring point for an ACE XML Gateway implementation. This section describes how to configure an ACE XML appliance that is already running on the network to operate as manager.

Note: This section provides details on step 26 in Section 5.3, "Configuring the Appliance." For information on configuring your appliance's network settings, see the other steps in Section 5.3, "Configuring the Appliance."

To configure the appliance to operate as a Manager:

1. Log into the ACE XML Shell as the `root` user.

   For more information, see Section 4.3, "Logging In to the Appliance Shell."

2. From the **Main Menu**, choose the **ACE XML Gateway Cluster Configuration** item.
3. To configure the appliance for operation as a Manager appliance, choose the **ACE XML Manager** item from the **This machine should act as a** screen.

   Note that you add gateways to this Manager's control later in the ACE XML Manager web console.

   You are prompted to restart using the new networking settings.
4. It is suggested that you restart the services running on the appliance at this time by clicking **Yes**.

   To exit this screen without restarting, choose **No**. However, you will need to restart the services later to have your changes take effect. To do so, choose the **Main Menu > Manage ACE XML Gateway Processes > Restart All Configured Services** item.
5. If prompted, click **OK** to acknowledge the notice regarding adding Gateways to this Manager. You will need to do so later from the web console.

You've completed the basic configuration of your ACE XML appliance as a dedicated Manager appliance. You can now put the appliance into service or configure optional features.

5.4.3 Gateway Mode

A Gateway appliance enforces a collection of rules known as a Gateway policy on message traffic. A clustered Gateway is a member of a *cluster*, which is a group of Gateway appliances that share the same policy and enforce the same rules on all the messages they process. A single ACE XML Manager appliance controls all members of the cluster.

This section describes how to configure an ACE XML appliance as a Gateway appliance. The process of configuring a single Gateway or a cluster of Gateways is similar.

> **Note:** This section provides details on step 26 in Section 5.3, "Configuring the Appliance." For information on configuring your appliance's network settings, see the other steps in Section 5.3, "Configuring the Appliance."

To configure the appliance to operate as a Gateway:

1. Log into the ACE XML appliance Shell as the `root` user.

   For more information, see Section 4.3, "Logging In to the Appliance Shell."

2. From the **Main Menu**, choose the **ACE XML Gateway Cluster Configuration** item.
3. To configure the appliance for Gateway operation, choose the **ACE XML Gateway Cluster Member** item.

   The appliance prompts you to provide the IP address of the ACE XML Manager that is to control this Gateway appliance.
4. Enter the IP address of the ACE XML Manager that will control this ACE XML Gateway.

   The ACE XML Gateway will only accept administrative commands and queries from an ACE XML Manager at the IP address you set here.

   It is important to note that source IP address verification is the primary mechanism that the Gateway uses to authenticate administrative traffic from the Manager. For this reason, you should ensure that access to the administrative port of the Gateway (port 8200, by default) is available only from within a trusted network. If using a hardware-backed keystore, you can further use the steps in Chapter 8, "Using Hardware-Backed Keys for Administrative Communication," to secure the connection with a hardware-backed certificate.
5. It is suggested that you restart the services running on the appliance at this time by clicking **Yes**.

   To exit this screen without restarting, choose **No**. However, you will need to restart the services later to have your changes take effect. To do so, choose the **Main Menu > Manage ACE XML Gateway Processes > Restart All Configured Services** item.

A cluster is a group of Gateways managed by a single Manager instance. If there are multiple Gateways in your deployment, repeat these steps for each Gateway in the cluster. Use the same Manager address for each.

When finished, you can put the appliance into service or configure optional features. Before this Gateway can process service traffic, it needs to be added to the managed cluster configuration of a particular ACE XML Manager. For more information, see the *Cisco ACE XML Gateway User's Guide*.

5.4.4 Inactive Mode

An inactive appliance performs no message-processing functions, either because it's a new appliance that has never been configured or because its message-processing functions are suspended temporarily.

In the latter case, a previously configured appliance can be returned to active service using the **Main Menu > ACE XML Gateway Cluster Configuration** menu.

Note: This section provides details on step 26 in Section 5.3, "Configuring the Appliance." For information on configuring your appliance's network settings, see the other steps in Section 5.3, "Configuring the Appliance."

To configure the appliance to operate as an inactive appliance:

1. Log into the appliance shell as the `root` user.

   For more information, see Section 4.3, "Logging In to the Appliance Shell."

2. From the **Main Menu**, choose the **ACE XML Gateway Cluster Configuration** item.

3. From the operation mode options, configure the appliance as inactive by choosing **Inactive machine**.

   You are prompted to restart with the new networking settings.

4. Restart the services running on the appliance with the new setting at this time by clicking **Yes**. You must restart the appliance to cause the new settings to take effect.

   To exit this screen without restarting, choose **No**. However, you will need to restart the services later to have your changes take effect. To do so, choose the **Main Menu > Manage ACE XML Gateway Processes > Restart All Configured Services** item.

Although it is recommended that you perform the restart now, you may choose to do so later in the configuration process. For example, if you know that you plan to perform other configuration tasks that require a restart, or if you plan to restart all of your network devices at one time, you can defer this task to a more appropriate time.

5.5 Setting the System Clock

Each Manager or Gateway appliance time-stamps the items it enters in its message log or event log. To ensure the accuracy of these timestamps, you must set each ACE XML appliance's system clock.

If there are multiple ACE XML appliances in your deployment, they should all be set to have the same system time. A significant discrepancy between system clocks between appliances in a deployment (that is, of a few minutes or more), can impede the proper operation of the system.

This section describes how to set the time on a ACE XML appliance. You can set the system clock on each ACE XML appliance yourself or synchronize them using a Network Time Protocol (NTP) server.

To ensure consistent timekeeping across appliances, we recommend that ACE XML appliances use NTP to keep their clocks correctly set.

5.5.1 Setting the Clock Manually

To set the system clock on a ACE XML appliance manually:

1. Log into the appliance shell as the `root` user.

   For more information, see Section 4.3, "Logging In to the Appliance Shell."

2. In the **Main Menu**, choose the **Advanced Options** item.

3. In the **Advanced Options** menu, choose **Run bash**.

   The `bash` command prompt appears. You may now use this shell as you would in a typical Linux environment.

4. Use the Linux `date` command to enter the current time.

   For example, the following command sets the system clock to Monday, May 16, 2005 at 5:28 PM, Coordinated Universal Time:

   ```
   date -s "Mon May 16 17:28:00 05"
   ```

   Note: For more information about the `date` command, type `man date` or `info date`.

   The command prompt displays the date you set. The system clock on the ACE XML appliance is now set.

5. To return to the **Advanced Options** menu, type `exit` at the command line and press enter.

Repeat these steps for each Gateway or Manager appliance.

5.5.2 Setting the Clock by a Network Time Server

Although the ACE XML appliance's clock is accurate and stable enough to provide reliable time stamps, all clocks drift to some degree. To enhance consistent timekeeping across the enterprise, you can use a Network Time Protocol (NTP) server to coordinate the system clocks of all computers on the network.

This feature is especially useful when using a syslog aggregator to create one log that reflects the activities of multiple appliances, and it can be critical to the ability to process SOAP headers and other time-sensitive protocols correctly.

ACE XML appliances use version 4.1.2 of the Network Time Protocol. To configure a ACE XML appliance to use an NTP server:

1. Log into the appliance shell as the `root` user.

For more information, see Section 4.3, "Logging In to the Appliance Shell."

2. From the **Main Menu**, choose the **Advanced Options** item.

   The **Advanced Options** menu appears.

3. Choose the **Time Settings** item from the **Advanced Options**.

   The shell displays a screen in which you can specify the NTP servers this appliance is to use.

4. In the field provided, enter the IP addresses or hostnames of one or more NTP servers. By entering multiple servers, you can ensure that if one server is unavailable, an alternate will be used. Use spaces to separate multiple addresses. (To disable use of NTP, remove all information that appears in this field.)

   If there are multiple ACE XML appliances in your deployment, you should set each to have the same NTP servers, to ensure that the appliances remain properly synchronized.

5. Choose **OK** to save the settings.

The appliance attempts to contact the server. If successful, the **Advanced Options** menu appears. If the appliance cannot contact the time server, it displays status messages to this effect. However, you are prompted to save the new settings anyway.

In this case, make sure that the network connection is good. If you know that the connection is good but the appliance cannot connect to the NTP server, check the addresses for errors or verify independently that the specified server is up and running.

On the other hand, if you are configuring an appliance that is not yet on the network, the appliance won't be able to connect to the server even if the address or hostname is correct. In this case, you can choose to save the new settings regardless of the initial failed access attempt.

5.6 Shutting Down and Rebooting

The ACE XML appliance shell provides menu options for shutting down and rebooting the appliance. You should use this method for shutting down the appliance rather than the UNIX `shutdown -h command`, since the `shutdown` command does not remove power to the ACE XML appliance.

Certain types of configuration changes require a reboot. For example, changes to network settings or cluster configurations require that system boot using the new settings. When making multiple changes to the configuration of a ACE XML appliance, it may be more convenient to

reboot the system once after all changes are made, rather than rebooting after every change that requires a reboot. You can use the `Reboot` menu item to reboot the system at your convenience.

5.6.1 Rebooting the ACE XML Appliance

To reboot an ACE XML appliance:

1. Choose the **Shutdown/Reboot** item from the Main Menu.
2. In the **Shutdown/Reboot** screen, choose the **Reboot** item.

   The appliance prompts you to confirm your choice.
3. Confirm the reboot by selecting **Yes** from the confirmation screen. To exit this screen without rebooting, choose the **No** item from the confirmation screen.
4. Choose the **Return to Main Menu** item to exit the page.

5.6.2 Shutting Down the ACE XML Appliance

Take the following steps to shut down a ACE XML appliance safely:

1. Choose the **Shutdown/Reboot** item from the Main Menu.

   The **Shutdown/Reboot** screen appears.
2. Choose the **Shutdown** item from the **Shutdown/Reboot** screen.

   The appliance prompts you to confirm your choice.
3. Confirm the shutdown by choosing **Yes** from the confirmation screen. The appliance shuts down all processes and powers off.

   To exit this screen without shutting down, choose **No**. The appliance returns to the **Shutdown/Reboot** screen.

5.7 Next Steps

After you've completed the steps in this chapter, your ACE XML appliance is functional in a basic configuration as a Manager, Gateway, or standalone appliance.

The remaining sections of this book describe procedures for enabling supplemental configuration options, such as hardware-based keystores, SSL engines, or SNMP.

To configure traffic handling at the Gateway, you can now log into the ACE XML Manager web console, as described in the *Cisco ACE XML Gateway User's Guide*, and start developing the Gateway policy.

CHAPTER 6

Configuring a Gateway Cluster

This chapter describes how to set up a cluster of Gateways. It covers these topics:

6.1 About Gateway Clusters

In a production environment, an ACE XML Gateway is usually deployed within a group of gateways. As a cluster, the gateways run a shared policy and collaborate to handle service traffic. Clustering improves the scalability and reliability of the system. Gateway appliances can be added to the cluster as needed to handle additional workload.

An ACE XML Manager can be used to administer multiple Gateway clusters. In this configuration, each cluster applies a different policy.

There are a few points to note about Gateway clusters:

- If a firewall exists between any of the Gateways and Manager, it needs to permit communication on these ports between the appliances:
  - UDP traffic on port 514. The ACE XML Gateways send syslog information to the ACE XML Manager at runtime for logging purposes over this port.
  - TCP traffic on port 8200. The ACE XML Manager sends configuration information to the Gateways over this port.

  For more information on port use in the system, see Section 2.2, "Ports Used by the ACE XML Gateway and Manager."
- The system clocks of all ACE XML appliances in a cluster (including the ACE XML Manager) must be synchronized. If

using NTP to maintain system clocks, as recommended, the appliances should all rely upon the same NTP servers. For more information, see Section 5.5, "Setting the System Clock."

6.2 Configuring a Cluster

The steps for setting up a cluster of Gateways are as follows:

1. In the appliance shell of each ACE XML Gateway in the cluster, specify the address of the common ACE XML Manager (that is, the address of the Manager that will be administering the cluster).

   For details, see Section 5.4.3, "Gateway Mode."

2. After setting up the ACE XML Manager, access the web console and use the Cluster Management page to configure the Gateways in this Manager's control by IP address.

For more information, see the cluster management information in the *Cisco ACE XML Gateway User's Guide*.

6.3 Restarting a Cluster

The console menu prompts you to restart the processes on the appliance when a restart is needed. Occasionally, you may need to restart the members of a cluster manually.

To restart a cluster system:

1. Shut down processes on all of the ACE XML appliances that compose the cluster.

   From the Main Menu of the appliance shell, choose **Manage ACE XML Gateway Processes > Stop ACE XML Gateway**.

2. First, start up (or restart) processes on the ACE XML Manager.

   From the **Manage ACE XML Gateway Processes** menu, choose the **Start ACE XML Manager** item.

3. Start up processes on each Gateway appliance in the cluster.

   From the **Manage ACE XML Gateway Processes** menu, choose the **Start ACE XML Gateway** item.

For more information, see the *Cisco ACE XML Gateway User's Guide*.

CHAPTER 7

Using Hardware Keystores and Security Worlds

This chapter describes how to set up hardware keystores and nCipher security worlds that use them. It covers these topics:

- Setting Up a Keystore
- Creating a New Security World
- Joining an Existing Security World

7.1 Setting Up a Keystore

The ACE XML appliances can be configured to use the nForce device from nCipher for hardware key storage. The nCipher hardware keystore and security world modules are license-enabled features. If you would like to use an nCipher hardware keystore but do not have a license to do so, please contact your Cisco support representative.

> **Note:** In addition to providing hardware keystores, the nCipher card provides encryption/decryption acceleration. For information on enabling this functionality, see Section 9.1, "Enabling SSL Acceleration."

To use nCipher hardware-based key storage, you need to add the ACE XML appliances to a new or existing nCipher security world. A "security world" is a set of appliances configured to use the hardware-backed keys that nCipher security modules provide. These appliances share secure key information, as well as the set of configuration files and smart cards associated with the keys. When you create the security world, you can set options such as the number of smart cards in the set, whether keys protected by the security world can be recovered.

Each ACE XML appliance that is to use the hardware-backed keys must have an nCipher card pre-installed. The smart cards fit into an nCipher card reader that attaches physically to a port on the appliance. Because smart cards are used only for nCipher administration tasks, such as setting up security worlds or adding appliances to existing security worlds, the card reader need not remain attached to the ACE XML appliance after nCipher administration tasks are complete. Therefore, you can use a single card reader to configure the nCipher functions of multiple ACE XML appliances.

To use a hardware keystore in a clustered environment, you must set up a hardware keystore and a security world that uses it on each ACE XML appliance in the cluster.

Because the initialization process involves changing the settings of hardware switches, you must have physical access to the ACE XML appliances that house the keystore hardware. You'll also need the administrative privileges required to run the terminal-based nCipher software tools that reconfigure the keystore.

Because proper operation of the smart cards is vital to the accessibility of the keystore and security world, it is recommended that you create a backup set of smart cards and keep the backup cards in an off-site location. Accordingly, the examples in this chapter create a set of four cards, any two of which can be used to edit the security world, thus allowing the other two cards to be stored in a safe location.

This guide provides complete, step-by-step descriptions of all tasks related to using nCipher modules with ACE XML appliances. However, you should review the nCipher documentation that accompanied your nCipher-equipped ACE XML appliance for more information about the nCipher system.

7.2 Creating a New Security World

This section describes how to create a new nCipher security world and add a Gateway to it. Subsequently, you can add more Gateways to this security world by following the steps in Section 7.3, "Joining an Existing Security World."

When configuring a new security world, you must specify the number of smart cards to configure (n), and the number of cards that must be physically present (k) to add a new appliance to the security world. In the instructions in this section, the assumption is n=4 and k=2. That is, the security world has four administrator cards, and any two of them must be present to add new modules to the security world.

Note: Before executing any nCipher commands, determine requirements for your IT environment's

security world and see the nCipher documentation for further explanation of the security world options available to you.

7.2.1 Before You Begin

Before configuring the security world, be sure you have the following:

- Physical access to the Gateway and its nCipher card reader.
- The root password for the Gateway.
- Four nCipher smart cards, numbered and labeled. Feel free to use any labeling scheme that is convenient for you.

7.2.2 Creating the New Security World

Take the following steps to create a simple security world having four administrator cards:

1. On the ACE XML appliance, access the `bash` shell as `root` user (from the main menu, choose **Advanced Options > Run bash**).

   For details, see Section 4.5, "Accessing the bash Shell."

2. On the Gateway chassis, move the switch on the nCipher module to the "I" position. (The card may be either on the front or back panel, depending on the appliance model.)

   This action indicates to the nCipher module that you intend to put it into "pre-initialization" mode. However, you will see no additional feedback other than the changed position of the switch. Simply moving the switch does not change the module's mode; you must reset the module to put it into a new mode.

   Important: In the next step, you initialize the nCipher keystore. Doing so destroys stored private keys and the hardware password that protects them. If those keys are important, you should make sure that you have a way to recover them before initializing a previously used keystore. **There is no way to recover the hardware password for the keystore if you lose it or if you erase it by reinitializing the keystore.** Be extremely careful with the hardware password and with keys stored in the keystore.

3. Reset the module by taking one of the following actions:

   - Press the reset button next to the mode switch.

     You may need to use a pen, straight pin, or paper clip to reach the reset button.

or:

- As the `root` user in a terminal session on the ACE XML appliance, execute the following command:

  ```
  /opt/nfast/bin/nopclearfail -ca
  ```

  The `-ca` option specifies that the `nopclearfail` command is to initialize all available nCipher modules. To initialize a particular module specified by its number, use the `-m` and `-c` options instead, as in the following example:

  ```
  /opt/nfast/bin/nopclearfail -c -m 1
  ```

  The `-c` option indicates that the `nopclearfail` command is to clear the nCipher module that the `-m` option specifies. In this example, the options specify that the command is to clear module #1.

The shell indicates successful reset by printing to standard output a line similar to the following:

```
module 1, command , clearunit: OK
```

Also, the blue LED on the nCipher module blinks in single, short flashes. (The nCipher light is next to the three-position, M, I, O, switch on the nCipher card itself.) This feedback occurs whether you use the command line or the hardware reset switch to change the module's mode.

4. To confirm the module's current operating mode, execute the following command from the command line

   ```
   /opt/nfast/bin/enquiry
   ```

   The `enquiry` command summarizes the status of each available nCipher module. If you've switched successfully to pre-initialization mode, a value of `pre-initialization` appears in the `mode` field of the summary for each module you reset.

5. Plug the nCipher card reader into the nCipher PCI card interface on the appliance.

   An LED lights on the card reader to indicate that it is connected. The LED is red if no card is present or the card cannot be read, or green if a valid smart card is present. Do not put a card in the reader yet.

   On older nCipher card readers and ACE XML appliance chassis in which the card is on the back panel, the plug may be too short to reach beyond the lip that extends over the chassis' back panel. If the plug on the nCipher card reader is too short to seat firmly, attach both the male and female gender changers to the plug to extend it.

6. To create the new security world, execute the command:

```
/opt/nfast/bin/new-world -i
              -Q cardsReqd/cardsInSet
                -m moduleNum
```

where:

- *cardsReqd* specifies the number of smart cards that must be physically present in order to edit the security world.
- *cardsInSet* specifies the total number of smart cards in the set.
- *module*N*um* specifies the nCipher module to initialize.

Your new-world command must specify values that describe your particular installation. For example, to initialize four smart cards and require that two be present to edit the security world, you would specify `2` as the `cardsReqd` value and `4` as the `cardsInSet` value, as the following example:

```
/opt/nfast/bin/new-world -i -Q 2/4 -m 1
```

To initialize two smart cards and require only one to be present when editing the security world, substitute `1/2` for the `2/4` value in the example.

The `new-world` utility initializes a single nCipher module at a time. To initialize multiple nCipher modules, run the `new-world` utility once for each module, using the `-m` option to indicate the module that `new-world` is to initialize.

For example, in the preceding command, the `-m 1` argument indicates that `new-world` is to initialize module # 1. For more information, see the nCipher documentation that accompanied your nCipher-equipped ACE XML appliance.

After a few moments, the shell prompts you to insert the first smart card in the set.

7. Insert the card into the card reader, with the chip side up, pushing gently but firmly until the card clicks into place.

   The light on the card reader turns green and the shell prompts you to initialize the card or set its password.

8. If the **Module 1 slot contains an unrecognized card. Overwrite it?** prompt appears, type **yes** and press the **Enter** key.

   The appliance prompts you to set a new password for the card.

   If the unrecognized card prompt does not appear, go on to the next step.

9. Enter the new password for the card and, when prompted, confirm the password. If the second password does not match the first exactly, you are prompted to set the password again.

Important: Do not lose smart card passwords. You'll need them to add other modules to the security world.

The appliance prompts you to remove the card.

10. Remove the card from the reader.
11. Repeat the preceding steps as prompted to set passwords for the remaining cards in the set.

    When you've set passwords for all cards in the set, the console displays the **security world created** message followed by the command-line prompt.
12. To confirm the existence of the new security world, execute the following command line:

    ```
    ls -la /opt/nfast/kmdata/local
    ```

    The shell lists the contents of the specified directory. If the security world was created successfully, the directory contains one world file and at least one module_*X* file, as in the example listing:

    ```
    # ls -la /opt/nfast/kmdata/local
    total 32
    drwxrwsr-x 2 nfast nfast 4096 Jan 24 00:16 .
    drwxrwsr-x 8 nfast nfast 4096 Jan 23 23:09 ..
    -rw-r--r-- 1 root nfast 856 Jan 24 00:16
                          module_XXXX-XXXX-XXXX
    -rw-r--r-- 1 root nfast 16472 Jan 24 00:16
                          world
    ```
13. Disconnect the card reader from the nCipher PCI card.
14. Move the switch on the nCipher module to the "O" position.

    This action indicates to the nCipher module that you intend to put it into "operational" mode.
15. Reset the module by taking one of the following actions:

    - Press the reset button next to the mode switch.

      You may need to use a pen, straight pin, or paper clip to reach the reset button.

    or:

    - As the `root` user in a terminal session on the ACE XML appliance, execute the following command:

      ```
      /opt/nfast/bin/nopclearfail -ca
      ```

      The shell indicates successful reset by printing to standard output a line similar to the following:

      ```
      module 1, command , clearunit: OK
      ```

The `-ca` option specifies that the `nopclearfail` command is to initialize all available nCipher modules. To initialize a particular module specified by its number, use the `-m` and `-c` options instead, as in the following example:

```
/opt/nfast/bin/nopclearfail -c -m 1
```

The `-c` option indicates that the `nopclearfail` command is to clear the nCipher module that the `-m` option specifies. In this example, the options specify that the command is to clear module #1.

When you have reset the nCipher module to enter operational mode, the blue LED on the nCipher module blinks in long flashes.

16. Verify that the module is now operational by executing the following command line:

    ```
    /opt/nfast/bin/enquiry
    ```

    The `enquiry` command summarizes the status of each available nCipher module. If you've switched successfully to operational mode, a value of `operational` appears in the `mode` field of the summary for each module you reset.

17. Exit the `bash` shell.

18. In the **Advanced Options** menu, choose the **SSL Engine Configuration** item.

19. In the **SSL Engine** screen, choose **chil** to enable the nCipher CHIL device.

    The **Advanced Options** menu appears.

20. Choose the **Return to Main Menu** item.

21. In the **Main Menu** menu, choose the **Manage ACE XML Gateway Processes** item.

22. Choose **Restart All Services**.

The shell attempts to restart the appliance in the currently specified configuration, and displays a status screen upon completion of this task.

If the appliance restarted successfully in the new configuration, the nCipher module is now ready for use with the private keys created in this security world. For more information, see the nCipher documentation that accompanied your ACE XML appliance.

7.3 Joining an Existing Security World

This section describes how to add a Gateway to an existing nCipher security world. For general information on security worlds and instructions for creating a security world, see Section 7.2, "Creating a New Security World." Also, see the nCipher documentation that accompanied your ACE XML appliance.

7.3.1 Before You Begin

Before you start to add another ACE XML appliance to a security world, be sure you have the following:

- An ACE XML appliance on which the security world has already been initialized. For more information, see Section 7.2, "Creating a New Security World." The instructions in this section refer to this appliance as the source system.
- A copy of the security world files. This is a directory of files that define security world configuration information. Typically, these files reside in the `/opt/nfast/kmdata` directory of the source system.
- Administrator cards from the existing security world. The number of cards you need from the set depends on how the security world was configured when it was created.
- Physical access to the ACE XML appliance to be added to the security world. The instructions in this section refer to this appliance as the destination system.
- An nCipher card reader attached to the destination system.
- The root passwords for the source and destination systems.

7.3.2 Adding an ACE XML Appliance to the Security World

Adding an ACE XML appliance to an existing nCipher security world involves using files copied from the source appliance to initialize the nCipher card on the destination system, as follows:

1. On the destination system, run the `bash` shell as the `root` user.
2. Move the switch on the nCipher module to the "I" position.
3. Reset the module by taking one of the following actions:
   - Press the reset button next to the mode switch.

     You may need to use a pen, straight pin, or paper clip to reach the reset button.

or:

- Execute the following command line on the destination system:

  ```
  /opt/nfast/bin/nopclearfail -ca
  ```

  The shell indicates successful reset by printing to standard output a line similar to the following:

  ```
  module 1, command , clearunit: OK
  ```

  The `-ca` option specifies that the `nopclearfail` command is to initialize all available nCipher modules. To initialize a particular module specified by its number, use the `-m` and `-c` options instead, as in the following example:

  ```
  /opt/nfast/bin/nopclearfail -c -m 1
  ```

  The `-c` option indicates that the `nopclearfail` command is to clear the nCipher module that the `-m` option specifies. In this example, the options specify that the command is to clear module #1.

When you have reset the nCipher module to enter pre-initialization mode, the blue LED on the nCipher module blinks in short flashes.

4. To confirm the module's current operating mode, execute the following command on the destination system:

   ```
   /opt/nfast/bin/enquiry
   ```

   The `enquiry` command summarizes the status of each available nCipher module. If you've switched successfully to pre-initialization mode, a value of `pre-initialization` appears in the `mode` field of the summary for each module you reset.

5. Plug the nCipher card reader into the nCipher PCI card interface.

   An LED lights on the card reader to indicate that it is connected. The LED is red if no card is present or the card cannot be read. The LED is green if a valid smart card is present. **Do not put a card in the reader yet.**

   On older nCipher card readers and ACE XML appliance chassis in which the card is on the back panel, the plug may be too short to reach beyond the lip that extends over the back of the ACE XML appliance chassis. If the plug on the nCipher card reader is too short to seat firmly, attach both the male and female gender changers to the plug to extend it.

6. On the source system, run `bash` as the `root` user.

   For more information, see Section 4.5, "Accessing the bash Shell."

7. Copy the existing security world files from the source system's `/opt/nfast/kmdata` directory into the same directory path on the destination system.

   You may need to use the `scp` program to copy the data onto the destination system.

8. On the destination system, execute the following command line to add the destination system to the security world:

   ```
   /opt/nfast/bin/new-world -l -s 0 -m 1
   ```

   You are prompted for passwords and smart cards from the administrator card set. Enter passwords and insert cards as directed.

   Note that you can customize the arguments to the `new-world` command. For more information, see the nCipher documentation that accompanied your nCipher-equipped ACE XML appliance.

9. Disconnect the card reader from the nCipher PCI card.

10. Move the switch on the nCipher module to the "O" position.

    This action indicates to the nCipher module that you intend to put it into operational mode. At this point, the blue light on the back of the nCipher card still blinks in short flashes to indicate that the card is still in pre-initialization mode. Simply moving the switch does not change the module's mode; you must reset the module to put it into a new mode.

11. Reset the module by taking one of the following actions:

    - Press the reset button next to the mode switch.

      You may need a pen, straight pin, or paper clip to reach the reset button.

    or:

    - As the `root` user in a terminal session on the ACE XML appliance, execute the following command:

      ```
      /opt/nfast/bin/nopclearfail -ca
      ```

      The shell indicates successful reset by printing to standard output a line similar to the following:

      ```
      module 1, command , clearunit: OK
      ```

      The `-ca` option specifies that the `nopclearfail` command is to initialize all available nCipher modules. To initialize a particular module specified by its number, you can use the `-m` and `-c` options instead, as in the following example:

      ```
      /opt/nfast/bin/nopclearfail -c -m 1
      ```

The `-c` option indicates that the `nopclearfail` command is to clear the nCipher module that the `-m` option specifies. In this example, the options specify that the command is to clear module #1.

When you have reset the nCipher module to enter operational mode, the blue LED on the nCipher module blinks in long flashes.

12. Verify that the module is now operational by executing the following command line:

    ```
    /opt/nfast/bin/enquiry
    ```

    The `enquiry` command summarizes the status of each available nCipher module. If you've switched successfully to operational mode, a value of `operational` appears in the `mode` field of the summary for each module you reset.

13. Exit the `bash` shell.

14. In the **Advanced Options** menu, choose the **SSL Engine Configuration** item.

    The **SSL Engine** screen appears.

15. Choose **chil** to enable the nCipher CHIL device.

    The **Advanced Options** menu appears.

16. Choose the **Return to Main Menu** item.

17. In the **Main Menu** menu, choose the **Manage ACE XML Gateway Processes** item.

    The **Manage ACE XML Gateway Processes** menu appears.

18. Choose the **Restart All Services** item.

    The shell attempts to restart the appliance in the currently-specified configuration, and displays a status screen upon completion of this task.

If the appliance restarted successfully in the new configuration, its nCipher module is now ready for use with the private keys the existing security world provides. For additional information, see the nCipher documentation that accompanied your ACE XML appliance.

CHAPTER 8

Using Hardware-Backed Keys for Administrative Communication

This chapter describes how to substitute the built-in keys with hardware-backed keys to secure administrative communications between the Cisco ACE XML Gateway and Manager. It covers these topics:

8.1 Overview

When the ACE XML Manager establishes an SSL connection with a Gateway to deploy policies or to perform other administrative functions, it presents an X.509 client certificate and expects the Gateway to present its own server certificate in response. The ACE XML Manager also uses a certificate to sign the ACE XML Manager Audit Log, to ensure the integrity of logged information.

For enhanced security, you should replace the default certificates used for these purpose with your own. Each X.509 certificate's unique identity is based on a set of PKI keys. In addition to installing new certificates at initial configuration time, you may choose to install new keys periodically or in response to a possible security breach.

Your certificates can use software- or hardware-based cryptographic keys. The ACE XML system uses software-based keys to implement its default functionality. For greater security, you can use certificates based on keys that a hardware-based keystore generates and protects.

To use hardware-based keys, your ACE XML appliances must be equipped with nCipher hardware-based keystores and you must configure the appliances to use them, as described in Chapter 7, "Using Hardware Keystores and Security Worlds."

While hardware-backed keys are recommended for best security, you can also replace the built-in keys with software-backed key if desired. In general, the procedures for replacing the built in keys with hardware backed keys and software backed keys are very similar. Where the instructions differ, the procedure in this chapter notes differences for installing software-backed keys.

8.2 Installing Hardware-Backed Certificates

Configuring ACE XML appliances to use hardware-based keys for bilateral authentication is a two-part process:

- You must install a new server certificate on each Gateway in a cluster and inform the ACE XML Manager that the Gateway presents this certificate for bilateral authentication.
- You must install a new client certificate on the ACE XML Manager and inform each Gateway in its cluster that the ACE XML Manager presents that certificate for bilateral authentication.

Although the installation procedures are parallel in concept, the details pertinent to each vary slightly. To ensure successful installation, be sure to follow each section's step-by-step instructions carefully.

Note: Installation of each hardware-backed certificate requires you to execute certain commands on the ACE XML Manager appliance, and others on the Gateway appliance. When installing bilateral authentication certificates on a Gateway cluster, you must execute the Gateway-based commands on each Gateway appliance in the cluster.

8.2.1 Before You Begin

Before you begin changing the keys used by administrative certificates, make sure you have met the following prerequisites:

- One or more trusted Certificate Authorities (CAs) must be available for signing administrative certificates. The Manager and Gateway need not use the same CA.
- You must already have configured each ACE XML appliance as a Gateway, Manager, or standalone machine.
- You must already have configured each ACE XML appliance to use an nCipher security world, as described in Chapter 7, "Using Hardware Keystores and Security Worlds."

- You must already have already enabled the use of a hardware-based SSL engine. For details, see Section 9.1, "Enabling SSL Acceleration."

8.2.2 Gateway-to-Manager Authentication

To configure a Gateway machine to use hardware-backed keys in bilateral authentication, complete the following tasks:

- Inform the ACE XML Manager of the CA that signed the certificate that the Gateway presents in bilateral authentication.
- On the Gateway, generate a certificate signing request (CSR).
- Send the CSR to the Gateway's trusted CA for transformation into the Gateway's server certificate.
- Install the server certificate on the Gateway.

The following procedures provide details on these steps

Caution: Before continuing, make sure that message traffic is diverted away from the Gateways to be configured. To do so, take the Gateways offline at the load-balancer that precedes them in your network. If you do not take the Gateways offline, in-progress transactions may be cut off when you perform these steps. Also, stop all Gateway services by setting it to inactive from the appliance shell (that is, from **Network Configuration** > **Cluster Configuration** menu item).

To install a hardware-backed certificate on the Gateway, take the following steps:

1. On the ACE XML Manager machine, run `bash` as the `root` user.
2. Place a copy of the self-signed root certificate of the Gateway's trusted Certificate Authority (CA) in the ACE XML Manager machine's `/usr/local/reactivity/private` directory.

   You can use any means you prefer to copy the file. For example, you can `ssh` to the ACE XML Manager machine from the Gateway's `bash` shell and then use the `scp` command to copy the CA certificate. These instructions refer to this certificate as the Gateway CA certificate.

   Note: All Gateways this Manager controls must present the same Gateway CA certificate. If you need to configure your systems differently, contact Cisco support for assistance. The Gateway and Manager need not use the same CA. However, if you choose not to use the same CA for both sides of bilateral

certificate exchange, take extra care to make sure you install the correct CA certificate on each machine.

3. In the ACE XML Manager shell, change directories to the following directory:

   ```
   cd /usr/local/reactivity
   ```

4. Execute the following command to back up the ACE XML Manager's current database of trusted CAs:

   ```
   mv private/trustkeystore private/trustkeystore.bak
   ```

   This command renames the `trustkeystore` file as the `trustkeystore.bak` file. The `trustkeystore` file is the list of CAs the ACE XML Manager trusts. In the next step, you generate a new `trustkeystore` file.

   Note: In the next example, and in the rest of this chapter, commands longer than a single line wrap to the next line. The backslash character ("\") indicates a line that wraps in this way. When typing these examples (or your own commands) into the `bash` shell, do not include the backslash characters.

5. In the ACE XML Manager shell, execute the following command to generate a new trusted CA database that contains an entry for the newly installed Gateway CA certificate:

   ```
   /usr/java/j2sdk1.4.2_04/bin/keytool \
       -import -trustcacerts -alias ca_cert \
       -keystore private/trustkeystore \
        -storetype jks -file GCACERT.CRT \
       -storepass approuter
   ```

   Where *`GCACERT.CRT`* is the filename of the local copy of the Gateway CA certificate you installed previously.

6. Enter yes in response to the **Trust this certificate?** prompt.

   The new certificate is added to the keystore and the **Certificate was added to keystore** message appears.

7. On the Gateway machine, run bash as the root user.

   The command prompt appears. Subsequent instructions refer to this terminal session as the Gateway shell.

8. In the shell, change directories to:

   ```
   cd /usr/local/reactivity
   ```

9. Execute the following command to back up the Gateway's current administrative server certificate:

   ```
   mv private/server.pem private/server.pem.bak
   ```

Note: To install certificates on a Gateway cluster, you must execute Gateway-based commands (such as this one) on each Gateway machine in the cluster.

10. In the Gateway shell, generate a key and corresponding CSR using one of the following steps, depending on if you are using a hardware-backed or software backed key:

For a hardware-backed key:

- Execute the `generatekey` command to generate a new nCipher-protected private key and corresponding certificate-signing request (CSR) for the Gateway, as follows:

  ```
  /opt/nfast/bin/generatekey --batch embed \
  protect=module recovery=1 size=1024 \
  embedsavefile=private/server.pem \
  x509dnscommon="gatewayhost" \
  x509org="Reactivity" x509locality="Belmont" \
  x509province="California" x509country="US"
  ```

  In your command, replace italicized text with values appropriate for your site. It is suggested that the value of the `x509dnscommon` parameter be the fully-qualified hostname the ACE XML Manager uses to contact the Gateway, although this is not a hard requirement.

  The system writes the CSR into `private/server_req.pem` and the shell displays information about the key generation operation. If successful, **Key successfully generated** appears at the bottom of the listing.

For a software-backed key:

- Enter the following two commands instead of the `generatekey` command:

  ```
  $ openssl genrsa -out server.pem 1024
  $ openssl req -key server.pem \
  -out server_req.pem -new -subj \
  "/CN=gatewayhost/OU=myorgunit/O=Reactivity
  /L=Belmont/ST=California/C=US"
  ```

  In your command, replace italicized text with values appropriate for your site. It is suggested that the CN value be the fully-qualified hostname the Manager uses to contact the Gateway, although this is not a hard requirement.

11. Send the CSR data (the `server_req.pem` file) to the Gateway's trusted CA for transformation into a signed X.509 certificate.

The CA sends a signed certificate in reply. This certificate is the Gateway's server certificate; in other words, it is the certificate the Gateway presents to the ACE XML Manager.

12. If you receive the signed certificate from the CA as the body of an email, place only the certificate contents in a text file:
    - Include the entire `BEGIN CERTIFICATE` line, the entire `END CERTIFICATE` line, and everything in between.
    - On your local file system, save the file using a valid Linux filename, that is, don't use spaces, apostrophes, ampersands, and other unusual characters in this filename.
13. In the Gateway shell, execute the following command to install the signed certificate on the Gateway:

    ```
    $ cat GCERT.CRT >> private/server.pem
    ```

    In your command, replace the *`GCERT.CRT`* with the filename of the signed certificate.

Important: Be sure to use the >> output redirection operator to append the signed certificate to the `server.pem` file. If you replace the file, you will destroy the private key that the `generatekey` tool placed in this file and the keystore will not recognize the certificate as valid. **You cannot recover from this error—you must repeat all the instructions in this section to generate a new key, a new CSR, and a new certificate to install.**

If you completed all of these steps successfully, this Gateway is now configured to use hardware-backed keys for bilateral certificate exchange: the Gateway's hardware-backed administrative certificate is installed, and the Gateway has been informed of the CA to use to validate the certificate the ACE XML Manager presents.

You can now configure other Gateways in the cluster similarly.

8.2.3 Manager-to-Gateway Authentication

To configure a ACE XML Manager to use hardware-backed keys in bilateral authentication, you must complete these tasks:

- Inform the ACE XML Gateways of the CA that signed the certificate the ACE XML Manager presents in bilateral authentication. You must perform this particular step on each ACE XML Gateway in the cluster.
- Generate a certificate signing request (CSR) that utilizes hardware-based keys on the ACE XML Manager.
- Send the CSR to the Manager's trusted CA for transformation into the Manager's client certificate.
- Install the client certificate on the ACE XML Manager.

To install a hardware-backed administrative client certificate on the ACE XML Manager, take the following steps:

1. Before continuing, make sure you have met the prerequisites in Section 8.2.1, "Before You Begin."
2. Place a copy of the self-signed root certificate of the ACE XML Manager's trusted Certificate Authority (CA) in the following directory of each Gateway machine this Manager controls:

   ```
   /usr/local/reactivity/private
   ```

   Use scp or the secure file transfer mechanism you prefer to copy the file. The scp utility would be run from the ACE XML Manager's `bash` shell to copy the ACE XML Manager's CA certificate onto the Gateway machine as follows

   ```
   ssh gatewaymachine -l root
   cd /usr/local/reactivity/private
   scp root@manangername:/pathToMCACert/MCAERT.CRT .
   ```

   In this example, *`MCACERT.CRT`* file is the self-signed root certificate of the CA who signed the certificate the ACE XML Manager presents to the Gateway. Subsequent instructions refer to this certificate as the ACE XML Manager CA certificate. In the example code, this file resides on the *`managername`* computer in the *`pathToMCACert`* directory. The `scp` command copies this file into the `/usr/local/reactivity/private` directory on the *`gatewaymachine`* Gateway appliance.

   The *`MCACERT.CRT`* file must be the PEM-format, self-signed, root certificate of the CA that signs the certificate the ACE XML Manager presents in bilateral certificate exchanges. The Gateway and Manager need not both use the same CA to verify the respective certificates presented to them. However, if you choose not to use the same CA for both sides of the bilateral certificate exchange, be sure to install the correct CA certificate on each machine.
3. On the Gateway machine, run `bash` as the `root` user.
4. In the Gateway shell, execute the following command to set the working directory to the top-level directory:

   ```
   cd /usr/local/reactivity
   ```
5. In the Gateway shell, execute the following command to back up the Manager CA certificate currently installed on the Gateway:

   ```
   mv private/ca.crt private/ca.crt.bak
   ```

   This command line renames the `ca.crt` file as the `ca.crt.bak` file. Shortly, you'll install a new `ca.crt` file.
6. In the Gateway shell, execute the following command to install a new Manager CA certificate on the Gateway:

```
cp MCACERT.CRT private/ca.crt
```

Replace *MCACERT.CRT* with the filename of the local copy of the CA certificate you installed previously.

7. On the Manager appliance, run `bash` as the `root` user.
8. On the Manager shell, change directories as follows:

```
cd /usr/local/reactivity
```

9. In the shell, execute the following command to back up the Manager's current hardware key database:

```
mv private/client.ncipher
                private/client.ncipher.bak
```

This command renames the `client.ncipher` file as `client.ncipher.bak`. This file contains hardware-based private keys the Manager uses to connect to the Gateways it manages. In the next step, you generate a new `client.ncipher` file.

10. In the Manager shell, execute the following command to generate a new nCipher-protected private key for use with the certificate the Manager's Web-based interface presents:

```
bin/ncipherkeytool -genkey -keystore
private/client.ncipher -alias mykey -keyalg RSA
-keysize 1024 -dname "CN=managerhostname,
O=Reactivity,L=Belmont,ST=California,C=US"
```

Replace the *italicized* values for the `CN,O,L, and ST` fields with values that are appropriate for your site. In particular, the `CN=` value must be the fully-qualified hostname of the Manager machine on which you are installing the certificate.

11. In the Manager shell, enter the following command to generate a CSR based on the new nCipher-protected private key:

```
bin/ncipherkeytool -certreq -keystore
private/client.ncipher -alias mykey -file client.req
```

The system writes the CSR into the `client.req` file. If you like, you can inspect this file to ensure that it contains a valid certificate signing request.

12. Send the CSR data (the `client.req` file) to the Manager's trusted CA for transformation into a signed X.509 certificate.

Keep in mind that this certificate is the Manager's client certificate, that is, the one the Manager presents to Gateways.

13. When you receive the signed certificate from the CA as an email, paste only the certificate contents into a text file:

- Include the entire `BEGIN CERTIFICATE` line, the entire `END CERTIFICATE` line, and everything in between.
- On your local file system, save the file using a valid Linux filename: don't use spaces, apostrophes, ampersands, and other unusual characters in this filename.

14. In the Manager shell, execute the following command to install the Manager's trusted CA certificate in the Manager's nCipher-protected keystore:

```
bin/ncipherkeytool -import -trustcacerts \
   -keystore private/client.ncipher -alias ca_cert \
   -file MCACERT.CRT
```

When you type this command, replace the *`MCACERT.CRT`* parameter with the filename of the local copy of the Manager CA certificate you installed previously.

The Shell prompts you to confirm the operation. Its output looks similar to the following:

```
Owner: EMAILADDRESS=name@example.com,
  CN=Some CA, OU=Engineering, O="Beagle, Inc.",
  L=Belmont,  ST=California, C=US Issuer:
  EMAILADDRESS=name@example.com, CN=Some CA,
  OU=Engineering, O="Beagle, Inc.", L=Belmont,
  ST=California, C=US Serial number: 0
Valid from: Thu Dec 09 20:31:59 UTC 2004
     until: Wed Dec 09 20:31:59 UTC
  2009
Certificate fingerprints:
           MD5:  XX:   hellip  :XX
           SHA1: XX:   hellip  :XX
Trust this certificate? [no]:
```

Note that the Gateway and Manager need not use the same CA to verify the respective certificates presented to them. However, if you choose not to use the same CA for both sides of the bilateral certificate exchange, take extra care to make sure you install the correct CA certificate on each machine.

15. In the Manager shell, enter `yes` to trust this certificate.

The shell adds the new certificate to the keystore and displays the **Certificate was added to keystore** message.

16. In the Manager shell, enter the following command to install the new Manager client certificate in the Manager's nCipher keystore:

```
bin/ncipherkeytool -import  \
     -keystore private/client.ncipher \
     -alias mykey -file MCERT.CRT
```

When you type this command, replace the *MCERT.CRT* parameter with the filename of a local copy of the signed X.509 certificate the Manager's trusted CA returned in response to your certificate signing request.

If the ncipherkeytool command installed the manager's client certificate successfully, the shell displays the **Certificate reply was installed in keystore** message.

17. To make the Manager's Web interface present the new client certificate:

    a. Open for editing the following Manager properties file: `/usr/local/reactivity/config/webapp.properties`

    b. Change the following line:

    ```
    ssl.client.keystore=
       /usr/local/reactivity/private/client.p12
    ```

    to:

    ```
    ssl.client.keystore=
       /usr/local/reactivity/private/client.ncipher
    ```

    c. Change the following line:

    ```
    ssl.client.storetype=pkcs12
    ```

    to:

    ```
    ssl.client.storetype=ncipher.sworld
    ```

18. In the Manager shell, execute the following command to set agateway as the owner and group of the webapp.properties file:

    ```
    chown agateway:agateway
       /usr/local/reactivity/config/webapp.properties
    ```

19. Verify the ownership change by typing the following command:

    ```
    ls -la /usr/local/reactivity/config
    ```

    The shell lists the contents of the `config` directory. In the listing, the owner and group assigned to the `webapp.properties` file should be agateway, as displayed in the following:

    ```
    -rw-r--r-- 1 agateway agateway 2874 Feb 8 00:34
                    webapp.properties
    ```

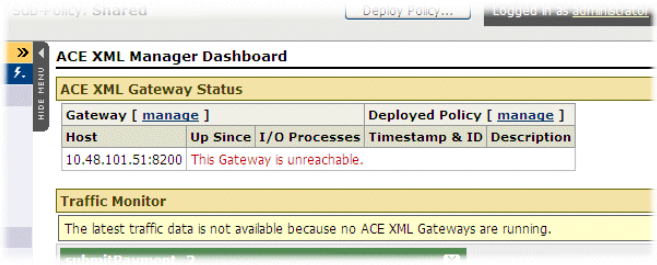
Once you complete these steps, the Manager uses hardware-backed keys for bilateral certificate exchange. If you also configured all Gateways that this Manager controls, the Manager and Gateways can now use their newly installed hardware-backed certificates for bilateral authentication.

8.2.4 Testing Hardware-Based Certificates

After configuring the Manager and Gateways as previously described, you can test the installation by viewing the event log in the Manager web console. Navigating to the event log requires the Manager to perform bilateral certificate exchange with each managed Gateway to retrieve the entries in the log.

Once you log into the Manager's web console, make sure that the Dashboard does not display warnings indicating that the Manager cannot contact any Gateway cluster members, such as the one in Figure 8-1.

Figure 8-1: Unreachable Gateway



If you replace the certificates without completing other parts of the installation process correctly, you may be able to log into the Manager web console or establish terminal sessions with the Manager or Gateways while still not having a fully functional installation. Assuming the Gateway was configured correctly prior to installation of the hardware-based keys, errors loading a certificate or reading the keystore may prevent the Gateway from starting successfully. If you see this message, you may be able to discern the problem by examining the Event Log.

While viewing the **Event Log**, look for **Notice**, **Warning** or **Alert** messages that indicate problems with the hardware keystore or other problems starting up.

In order to populate the **Event Log** with entries, the Manager must perform bilateral certificate exchange with each of the Gateways in its cluster as a prerequisite to polling them for new events to enter in the log. Therefore, if you can view an **Event Log** configured at **Notice** level or higher, and it contains no errors related to certificates, hardware keystores, or communications between the Manager and its Gateway cluster, the hardware-backed certificates used for bilateral certificate exchange are installed correctly.

8.3 Changing the Audit Log Signing Credential

The Console Audit Log is a ACE XML Manager web console page that shows the administrative-level changes affecting the system, such as policy deployment, changes to the current policy, changes to the user privileges of administrative accounts, and so on. In addition to the change made, the audit log shows who made the changes.

The audit log uses a PKI credential to authenticate processes before allowing them to edit and sign the audit log. This section describes how to substitute hardware-backed keys in place of the software-based keys that this credential uses normally.

Before completing these procedures, you must:

- Enable the use of the hardware-based SSL engine. For details, see Section 9.1, "Enabling SSL Acceleration."
- Add the ACE XML appliance to an nCipher security world.

To change the audit log signing credential:

1. On the Manager machine, log into the appliance shell as the `root` user.
2. Choose the **Manage ACE XML Gateway Processes** menu item.
3. In the **Manage ACE XML Gateway Processes** menu, choose **Stop ACE XML Manager**.

   The ACE XML appliance shuts down the Manager process and displays a status screen indicating the success of this operation.
4. Press the **Enter** key to dismiss the status screen.
5. In the **Manage ACE XML Gateway Processes** menu, choose **Return to Main Menu**.
6. Choose the **Advanced Options** item from the **Main Menu**.
7. Choose the **Run bash** item from the **Advanced Options** menu.
8. At the `bash` command prompt, change directories to the following directory:

   ```
   cd /usr/local/reactivity
   ```
9. To generate a new nCipher-protected keystore and self-signed certificate for audit log signing, execute the following command:

   ```
   $ bin/ncipherkeytool -genkey
      -keystore private/auditlog.ncipher
      -alias client -keyalg RSA -keysize 1024
      -dname "CN=auditlog"
   ```

To verify success of this command, list the contents of the `/usr/local/reactivity/private` directory to verify the presence of a newly-created `auditlog.ncipher` file. For example, you might use the following command to do so:

```
ls -lt private
```

10. Back up the current audit log certificate by entering the command:

    ```
    $ mv private/auditlog.crt private/auditlog.crt.bak
    ```

    This command renames `auditlog.crt` as `auditlog.crt.bak`. To verify the operation, list the contents of the `private` directory. If the rename operation succeeded, this directory contains an `auditlog.crt.bak` file and no `auditlog.crt` file.

11. Execute the following command to extract the new audit log certificate from the keystore for log verification utility use:

    ```
    $ bin/ncipherkeytool -export -rfc
         -keystore private/auditlog.ncipher
         -alias client -file private/auditlog.crt
    ```

    The shell displays the **Certificate stored in file <private/auditlog.crt>** message.

12. Edit `/usr/local/reactivity/config/webapp.properties` as follows:

    a. Change `p12` to `ncipher` in the following line.

    ```
    audit.log.private.key.pcks12=
         /usr/local/reactivity/private/auditlog.p12
    ```

    to:

    ```
    audit.log.private.key.pcks12=
      /usr/local/reactivity/private/auditlog.ncipher
    ```

    b. Change `pkcs12` to `ncipher.sworld` in the following line:

    ```
    audit.log.signing.keystore.type=pkcs12
    ```

    to:

    ```
    audit.log.signing.keystore.type=ncipher.sworld
    ```

13. In the Manager shell, execute the following command to set `agateway` as the owner and group of `webapp.properties`:

    ```
    chown agateway:agateway
        /usr/local/reactivity/config/webapp.properties
    ```

14. Confirm the file ownership change by executing the following command to view the owner and group assigned to the `webapp.properties` file:

    ```
    ls -la /usr/local/reactivity/config
    ```

The shell lists the contents of the `config` directory. In this listing, the owner and group assigned to the `webapp.properties` file should be agateway, as in following example:

```
-rw-r--r-- 1 agateway agateway 2874 Feb 8 00:34
            webapp.properties
```

15. Reset the audit log signing state by entering the following command:

    ```
    $ rm auditlogs/audit.console.current
    ```

    This command removes the current audit log. In a subsequent step, you'll generate a new audit log signed with the hardware-based certificate.

16. Exit the `bash` shell.

17. In the **Advanced Options** menu, choose the **Return to Main Menu** item.

18. Choose the **Manage ACE XML Gateway Processes** menu item.

19. Choose **Start ACE XML Manager**.

    The ACE XML appliance attempts to restart the Manager process and displays a status screen indicating the status of the operation.

20. Press the **Enter** key to dismiss the status screen.

    The **Manage ACE XML Gateway Processes** menu reappears.

21. Log into the ACE XML Manager web console (not the appliance shell) as a user with administrator role.

    The **Dashboard** appears.

22. Click the **Reports and Tools > Event Log** link.

    The **Event Log** should display the following message:

    A "/usr/local/reactivity/auditlogs/audit.console.current" not found. This file should only be missing on newly installed ACE XML Manager web consoles.

In the previous step, you removed the `audit.console.current` file, so this error message is to be expected. The ACE XML Manager writes a new log file in place of the file you removed, so you won't see this message on subsequent logins.

CHAPTER 9

Configuring Advanced Options

This chapter describes advanced set up options available with the ACE XML appliances. It covers these topics:

- Enabling SSL Acceleration
- Using Actional Looking Glass

9.1 Enabling SSL Acceleration

SSL-related operations are processing-intensive. Your appliance may be equipped with an SSL acceleration card that can offload SSL-related tasks from the Cisco ACE XML Gateway and improve system performance.

The ACE XML Gateway appliance supports the Cavium Nitrox XL Accelerator and nCipher CHIL® (hardware crypto hook) engine module.

> **Note:** The nCipher card can act as a hardware-based key store as well as an SSL accelerator. For information on using the nCipher device for hardware key storage, see Chapter 7, "Using Hardware Keystores and Security Worlds."

If your ACE XML appliance is configured with an SSL accelerator card, enable it as follows:

1. Log into the appliance shell as the `root` user.

   The **Main Menu** appears.

   For more information, see Section 4.3, "Logging In to the Appliance Shell."

2. From the **Main Menu**, choose **Advanced Options > SSL Engine Configuration**.

3. In the **SSL Engine** screen, choose one of the following options to enable it:

- **cavium**, to enable the Cavium Nitrox XL Security Accelerator device.
- **chil**, to enable the nCipher CHIL® device.

Choosing **none** disables SSL acceleration.

Note: If one of these items does not appear on the SSL Engine screen, your Gateway may not be licensed for SSL acceleration. For more information, contact Cisco support.

4. Click **OK** to accept the new settings.

The **Main Menu** appears. The ACE XML appliance now uses the enabled SSL accelerator.

9.2 Using Actional Looking Glass

Actional Looking Glass is a web service management solution that enables users to visualize, understand, monitor, and manager Web services networks.

The ACE XML Gateway has an Actional Ghost Agent that allows the services presented through the Gateway to be visible to Actional Looking Glass server. The system works with Actional Looking Glass version 6.0.

To use Actional with the system, connect each ACE XML Gateway in your deployment to the central Actional server, as described here.

If any network firewalls exist between the ACE XML appliances and Actional systems, be sure to permit traffic on the port appropriate for Actional. The Actional agent listens on port 8260 for connections from the central Actional system.

When enabled, the Agent publishes the following URLs:

- http://<*xml-gateway*>:8260/lgagent
- http://<*xml-gateway*>:8260/appsrv

To connect the ACE XML Gateway to Actional Looking Glass:

1. From the Main Menu of the appliance shell, choose **Advanced Options > Traffic Management**.
2. On the **Management Adapters** screen, choose the **Actional Looking Glass** item.

Note: If the **Actional Looking Glass** item does not appear on the **Management Adapters** screen, the Actional Management module may not be

license-enabled on your Gateway. For more information, contact Cisco support.

A message appears that changing this option requires a restart of the Gateway.

3. Choose **OK** to continue. Choose **Cancel** to stop the procedure for now.
4. Enter the IP address of your Actional central server.

This configures and starts the Actional Ghost Agent on the Gateway. The Gateway is now accessible from the Actional solution.

CHAPTER 10

Separating Traffic On Network Interfaces

This chapter describes how to separate traffic on different network interfaces. It covers these topics:

10.1 Overview

Depending on the platform chassis, the ACE XML appliance may have from one to four Ethernet interfaces that can handle service traffic. By default, the XML Gateway is configured to handle all traffic balanced on its built-in network interfaces, and not to separate traffic by type.

However, for security reasons, you may wish to isolate different classes of traffic on different physical network interfaces. For example, you may wish to separate administrative traffic from service-related traffic.

This chapter describes how to configure the network interfaces on the appliance, particularly for the purpose of having traffic separated by interface.

Traffic can be separated only if the messages have distinguishing features that are evident to the interface, and which can be used as a basis for the separation. For example, since communication with the ACE XML Manager takes place on port 8243, it's possible to have such traffic handled on a specific network interface. Source IP address can also be used as a distinguishing feature.

For configuration modifications such as having the `eth0` port on an appliance dedicated to administrative traffic and `eth1` to production traffic, you will need to configure the physical interfaces of the appliance as well as make policy changes in the XML Manager web console.

10.2 Configuring Physical Network Interfaces on the Appliance

The first step in configuring traffic separation over different network interfaces is to enable the interface on the appliance and give it its own IP address. These steps should be performed on each appliance in your installation, including the XML Manager and all XML Gateways.

To configure Ethernet interface on the appliance:

1. While logged into the ACE XML appliance's shell interface as `root` user, choose the **Network Configuration** item from the **Main Menu**.
2. In the **Network Configuration** screen, choose a network interface to configure, such as **Interface eth0** or **Interface eth1**.

   The shell displays a screen in which you can enable or disable the specified ethernet interface.
3. Choose the **enabled** item.

   The shell displays a screen in which to specify the IP address of the enabled Ethernet interface.
4. Enter the IP address for this interface.

   The address must be a valid IP address. You cannot use DHCP or other dynamic addressing schemes with the appliance. The Gateway cluster and ACE XML Manager depend on stable, static IP addresses for correct functioning.
5. Enter the netmask value for the IP address.

   The shell displays a screen in which you can specify the speed at which this Ethernet port is to operate.
6. Choose an Ethernet speed from:

   - **Auto** for automatic negotiation of duplex setting.

   Note: For maximum throughput, avoid the **auto** selection. For more information on how auto-negotiating port speed affects performance, see Section 2.3, "Appliance Network Interface Considerations."

   - **10** to specify 10baseT
   - **100** to specify 100baseT, or
   - **1000** to specify gigabit Ethernet speed.

Note: To realize full Gigabit Ethernet performance, your network must use CAT 5e Ethernet cable from end-to-end.

7. If you specified an Ethernet speed of 10 or 100, the script asks you to select whether the connection is half-duplex or full-duplex. Choose either **half** or **full** for the connection from the **Ethernet duplex** menu.
8. If static routes affect traffic destined for this Gateway, choose the **Add new route** item and enter a static route in the format indicated.

   A static route allows the Gateway to exchange traffic on multiple networks, but not itself act as an IP router. A static route is sometimes needed for a dual-homed appliance.

   If the route configuration is successful, the shell displays the **Edit Static Routes** screen with the new route added. If the shell discovers errors in the static route you entered, it displays a screen in which you can make corrections to the route and attempt to enter it again.

   To add more static routes, choose **Add new route** as necessary to add all static routes that affect traffic destined for this Gateway.
9. When finished adding static routes, choose **Accept settings**.
10. To commit the configuration changes, choose **Yes** in the **Commit the following new settings** screen. To exit without changing any settings, choose **No**.

    If you chose **Yes**, the Gateway restarts the interface using the new settings and returns you to the Network Configuration menu. If the Gateway cannot reconfigure the network as the settings require, it displays an error message, enabling you to check and retry your network settings without restarting the appliance.
11. If you have just configured `eth0`, repeat the process to configure `eth1` with a different IP address.

    After configuring the second interface, you can configure traffic destined for the IP addresses in the Manager web console, as described in the following section.

10.3 Assigning Traffic to Network Interfaces

After associating different IP addresses with particular interfaces, you can assign traffic to the interfaces from the Manager web console. While the details of using the Manager web console are outside the scope of this document, the general steps for completing the configuration are listed.

10.3.1 Assigning Administrative Traffic to an Interface

To have administrative traffic handled on a specific interface, perform the following steps:

1. Click the **Cluster Management** link in the navigation menu of the Manager web console.
2. Click the **edit** link next to the cluster you want to configure.

   If additional clusters have not been defined in this Manager, only one cluster will be shown on the Cluster Management page, the "Default Cluster."
3. For the **Manager HTTPS Port** setting, choose the IP address for the interface on which you want to handle administrative traffic. Each IP address configured for the appliance interfaces should be listed in the drop-down menu.
4. Click the **Restart the ACE XML Manager** button to have the Manager restart with the new setting.

10.3.2 Assigning Service Traffic to an Interface

The preceding steps describe how to assign XML Gateway administrative traffic to an interface. You can similarly assign service traffic to particular interfaces, as follows:

1. Open the configuration page for a port object (accessed by clicking the **Open HTTP(S) Ports** menu option).
2. In the **Listen For** option, choose the option labelled **requests to specific IP addresses**.
3. In the IP addresses text box, type the IP address of the interface on which the Gateway should listen for traffic to the port.

   The port can then be assigned to particular service proxies and handlers, which causes traffic for those services to be handled at the interface.
4. When finished, deploy the policy to have your changes take effect.

For more information, see the *Cisco ACE XML Gateway User's Guide*.

CHAPTER 11

Miscellaneous Administrative Tasks

This chapter describes various system maintenance and setup tasks you may need to perform. It covers these tasks:

11.1 Obtaining Version Information

Every ACE XML appliance has a version number that identifies the appliance's software with a particular release. This information is often required when contacting Cisco support or to ensure that all appliances in a cluster are running the same software version.

To obtain version information from the ACE XML appliance:

1. Log into the appliance shell as the `root` user.
2. In the **Main Menu**, choose the **Advanced Options** menu item.

   The **Advanced Options** menu appears.
3. Choose the **Version Information** menu item.

The release identifier string appears as a banner at the top of the screen. In the center of the screen, the appliance displays version numbers of the currently-installed Gateway software, operating system kernel, Tarari

XML coprocessor card firmware (this option information refers to a hardware add-on option that is no longer available), and nForce hardware keystore card firmware.

11.2 Creating Appliance User Accounts

There are several types of user accounts in the system. Manager user accounts provide access to the ACE XML Manager web console interface.

Another type of user account is used for accessing the ACE XML appliance command-line environment. These accounts, called operating system accounts, enable access to terminal sessions on the appliance, whether locally using a console connected to the appliance or remotely using secure shell (SSH).

Each ACE XML appliance includes the built-in `root` account. The `root` user has broad privileges for performing operations on the ACE XML appliance. For security purposes, it is essential that access to the `root` account is controlled carefully. You can create additional login accounts to allocate limited administrative privileges to the appliance. User accounts also make it easier to audit configuration changes.

There are two types of user accounts for the appliance:

- Developer users access the appliance to install SDK extension
- Operator users access the appliance to roll and retrieve log files

Notice that the privileges in either case are very restrictive. For example, the menu-driven Shell interface is not available for either type of user. In both cases, they are restricted to the tasks listed.

11.2.1 Steps for Creating the Account

To create a new login account on the ACE XML appliance:

1. Log into the appliance shell as the `root` user.
2. In the **Main Menu**, choose the **Advanced Options** item.
3. Choose the **Run Bash** option on the **Advanced Options** page.
4. At the `bash` prompt, create one of the two user types as follows:
   - To create an operator user, enter the following command:

     ```
     reactivity-operator-add [username]
                             "[description]"
     ```

     where:

     - *`[username]`* is the login name of the new operator user.

- *[description]* is a brief description of the account's purpose.

• To create a developer user, enter the following command:

```
reactivity-developer-add [username]
                         "[description]"
```

where:

- *[username]* is the login name of the new user.
- *[description]* is a brief description of the account.

Be sure to enclose the description with the double-quote character (") to ensure that the shell reads it correctly.

You are prompted for a password.

5. Enter a password for the new account.
6. Confirm the password by entering it a second time.

The new user can now log in to the shell interface. Type `exit` to return to the administration menu.

11.3 Backing Up and Restoring the System

Working policies are extremely valuable documents, often the result of many hours of planning and configuration. They also contain important and sensitive information about your network. You should treat them with the same care that you use with any other sensitive, mission-critical data, including having a backup and disaster recovery plan.

There are two approaches to backing up a system:

- By archiving individual policies and storing them offline. This captures policy changes made in the Manager interface, but excludes configuration settings made on the appliance directly.
- By backing up the state of the appliance with the backup command. This produces an archive file that contains the system state of the appliance, including configuration settings, policy, log files, and so on.

Most people will choose to do both, storing individual policies as needed, and maintaining a regular schedule of system backups. Archiving individual policies can be accomplished from the ACE XML Manager web console. (For instructions on doing so, see the chapter "Exporting a Policy to a File" in the Cisco ACE XML Gateway *User's Guide*.) This section describes how to back up the entire system.

To back up a system or restore an appliance based on a previously saved backup, use the backup command on the appliance. The backup command is available on both Gateway systems and the Manager.

When you run the command, it examines the files on the appliance for any differences to the original state, excluding those that are runtime-process-oriented. This information is written to an archive file, which you can move to an appropriate storage medium for backup or disaster recovery purposes.

11.3.1 Backing Up a System

The backup utility makes it possible to restore a system to a previously captured state. The backup utility saves the state of an appliance by recognizing changes that have been made to the system from its initial state and saving those changes to an archive. When that backup is restored on an appliance, the system is restored to the saved state.

> **Note:** Restoration from a backup file is intended to occur only on an ACE XML appliance with an empty configuration. Restoration may not work on an appliance that is not in that state.

System features saved by the backup utility include the policy state, the system's network configuration, and log information—essentially, any file created or modified since system installation, including scripts or data files.

There are some types of system changes or features that are not backed up by the backup/restore utility. For instance, it does not incorporate information that is specifically runtime-oriented, such as active process information. It also excludes certain types of system changes, such as software updates, hotfixes, or certified extensions installed by RPM. On the other hand, SDK extensions you have created and installed yourself are backed up. You will need to restore these items separately, before using the backup and restore process.

The result of the backup operation is an archive file that contains new or changed files. Note that if you do not remove this archive file, it will be included in the next backup operation. It is therefore advised that after saving the backup file to a storage medium you remove the original from the appliance filesystem.

Before running the backup command, you should ensure that a sufficient amount of free space is available on the appliance for the backup process to work. The exact amount varies depending on the size of your policy, log files, and so on. In general, however, to back up everything except log files, you will need to have about 50 MB of free disk space on the appliance. If backing up event logs, audit logs, or traffic logs, you will

need to have the amount of free disk space equal to the size of the logs. Therefore, if backing up the entire system, you will need 50MB plus the total size of the logs.

> **Note:** The backup operation does not itself check for sufficient disk space before starting. If the space is not available, the operation will not succeed.

To back up the system:

1. Access the appliance shell on the ACE XML appliance you want to backup.
2. Choose **Advanced Options > Run Bash**.
3. Use the `backup` command to generate the backup file, as follows:

   ```
   backup -all <filename>
   ```

   Where filename is the name of the `tgz` file that will contain the backup archive. For example:

   ```
   backup -all applianceBackup.tgz
   ```

   The `-all` switch causes all data to be backed up, including network and Gateway configuration settings, the policy filestore, and log files. Alternatively, you can just specify a subset of the data to be backed up by using a command switch, such as:

   ```
   backup -filestore applianceBackup.tgz
   ```

   The *filestore* switch causes all data except log information to be backed up. To back up only log data, use either the `-userlog` (for the event log), `-auditlog`, or `-traffic` switches.

   If you do not specify a switch with the command, only the network and Gateway configurations are backed up.

   > **Note:** Enter `backup -h` to see all available options for the command. Notice the `-e` and `-l` switches. They cause command operation errors to be printed to standard error output. In general, you shouldn't have to use these options unless directed to do so by Cisco support.

After the process is finished creating the backup artifacts, you can use the scp (secure copy) utility to copy the archive to an off-box location. Generally, after copying the archive elsewhere, you should remove the backup archive from the appliance. If you do not, it will be included in the next backup archive you create.

11.3.2 Restoring a System

Restoration from a backup file is intended to occur only on an ACE XML appliance with an initial, empty configuration. Restoration may not work on an appliance that already contains a populated policy or that may have other changes from its initial state. It should, however, contain the same software version, hotfixes, and SDK extensions as the system used to generate the backup. These items should be separately installed before running the backup restore command.

Also, the appliance should be in the same operating mode as the system used to generate the backup file. That is, if the source system was configured in standalone mode, the target system should be configured for standalone mode as well.

After ensuring these prerequisites, restore the system as follows:

1. Access the appliance shell on the ACE XML appliance on which you want restore the system.
2. Choose **Advanced Options > Run Bash**.
3. Use the `backup` script to restore the system from the backup file. The file should be either on the system or a disk location accessible from the appliance operating system.

   For example:

   ```
   backup -restore <filename>
   ```

   Where filename is the name of the `tgz` file that was previously saved with the `backup` script. For example:

   ```
   backup -restore -verbose applianceBackup.tgz
   ```

   The `-verbose` switch enables error messages that occur during the backup or restoration process to be printed to the screen.

   Note: Enter `backup -h` to see a full list of options. To have errors in the operation printed to the screen, use the `-e` or `-l` switch.

The system reads the file and overwrites the current system with the appliance state represented in the file. After the changes are applied, the appliance reboots. After is has restarted, the system contains the state restored from the backup archive.

11.4 Applying an Update

Cisco occasionally issues updates to the ACE XML Gateway and Manager software. These updates typically include security enhancements, new features or feature enhancements, and bug fixes.

Contact your Cisco support representative or check the Cisco support web site for information about software updates.

11.4.1 Update Steps

Each software update includes specific installation instructions tailored to that release. Because the specifics of upgrading may change from release to release, you should work with your Cisco support representative when performing any update.

In general, the update process consists of the following steps:

1. Get the update files

   When an update for your software is available, you can obtain the needed files from Cisco support. In most cases the update package consists of an automated install package and installation instructions.

2. Read the update instructions thoroughly

   Be sure to read thoroughly the instructions that accompany the update package. The details of upgrading may vary from release to release, depending on the features affected by the update.

3. Prepare the Gateway instance

   Before applying an update, it's a good idea to back up important files to ensure that you don't lose working policies, needed resources, or user accounts.

   You should perform such backups not only on the ACE XML Manager, but also on each Gateway. See Section 11.3, "Backing Up and Restoring the System," for details on backing up important files.

4. Apply the update to all ACE XML Gateway and Manager appliances. See the documentation that accompanies the update package for any special instructions.

If for any reason you need to restore your ACE XML Gateway instance to a previous version of its system software, Cisco-distributed updates include instructions for performing such rollbacks.

11.5 Configuring Serial Console Boot Control

By default, most ACE XML appliances are designed to support serial console access, with connection settings of 9600 bps, 8 data bits, no parity, and 1 stop bit.

By default, however, boot messages go to video console rather than to the serial console. You can change the configuration so that boot messages go to serial console as follows:

1. Log in to the appliance shell as the `root` user.
2. In the **Main Menu**, choose the **Advanced Options** item.
3. Choose the **Boot Settings** item from the **Advanced Options**.
4. Have boot output directed to serial console at startup by choosing the **Serial Port** item.

   Note: To use a keyboard, monitor, and mouse attached directly to the ACE XML appliance or through a KVM switch, choose the **Console** item.

   The shell displays the **Advanced Options** screen. You must reboot the appliance to cause the new settings to take effect.
5. From the **Advanced Options**, choose **Return to Main Menu**.
6. From the **Main Menu**, choose the **Shutdown/Reboot** item.
7. In the **Shutdown/Reboot** screen, choose **Reboot**.
8. The shell prompts you to confirm your choice. Choose **Yes** to restart the appliance with the new settings.

When connecting a serial cable to the ACE XML appliance, be sure to connect it to the serial interface for the appliance and not for any cards that may be installed in the appliance.

The nCipher card shipped with ACE XML appliances has its own serial port, used only for nCipher card readers. It does not support terminal sessions.

11.6 Recovering from Low Disk Space

If the appliance shuts down unexpectedly, it could be due to lack of disk space. By default, log files are not removed from the appliance. It's possible for the log files to eventually consume the available disk space on the appliance.

The appliance may also shut down if use of RAM resources are exceeded. In this case, however, the Gateway recovers by itself.

Gateways are designed to shut down when available disk space is less than 10 percent of total disk space. The Manager, however, does not have this protection mechanism and will operate until it is out of space. Therefore, you should be sure to monitor Manager disk space regularly.

If the appliance shuts down due to lack of disk space, you will need to free disk space on the affected appliance before it can be restarted.

To recover an appliance that has shut down due to lack of disk space:

1. Connect to the appliance using SSH and log in as root user.

   Note that the appliance can continue to accept SSH connections even though disk space has caused other processes to shut down.

2. From the **Main menu**, choose **Advanced Options > Run Bash**
3. You can confirm that the disk space is low using the `df` command, which displays used and free disk space.
4. Use `scp`, `cp`, or any other tool to remove log files from the disk.
5. Return to the menu by entering `exit` in the Bash shell and then select the appropriate menu option for returning to the Main menu.
6. Restart the appliance by choosing one of the following from **Manage ACE XML Gateway Processes** menu:
   - **Start ACE XML Gateway**
   - **Start ACE XML Manager**
   - **Restart All Configured Services** (if you choose this option with Gateways operating in your environment, the Gateways are restarted, which may result in dropped network traffic.)

To prevent unexpected shutdowns in the future, consider using a script that automatically moves logs off disk at regular intervals.

As a backup to such an approach, you can also enable automatic log file deletion. To do so, access the **Gateway Advanced Settings** page in the Manager Web console. This page is accessible from the **System Management** page.

On the page, enable the option labelled **Delete old log files when total message log disk usage exceeds**. Note that if the configured threshold is exceeded, the information in the deleted log files is lost.

For more information, see the online help available from that page in the Manager.

11.7 Changing the MTA Postmaster Address

The ACE XML Gateway can receive SMTP traffic for certain types of services. Specifically, it can process and validate ebXML content passed as email attachments. To use ebXML service processing at the Gateway, you configure an ebXML-based service definition in the Manager web console.

> **Note:** The Gateway's SMTP server never acts as a relay. It accepts incoming messages only for local addresses and it accepts outgoing messages only from the Gateway. Periodically, the SMTP server attempts to resend messages that suffered transient failures. The MTA does not support SMTP over SSL or TLS within SMTP.

If an ebXML service is added to the policy, the appliance opens port 25 to handle SMTP traffic. Thereafter, it's possible for the ACE XML Gateway MTA to receive email in its postmaster mailbox.

The postmaster address is a standard administrative address for MTA's (as required by the SMTP protocol). It does not affect incoming or outgoing gateway traffic.

If desired, you can modify the address so that mail to the postmaster is sent to another location, or keep the default, in which case the postmaster mailbox is the root user's mailbox on the ACE XML Gateway.

To change the existing address:

1. Log in to the shell interface of the Gateway appliance as the `root` user.
2. In the **Main Menu**, choose the **Advanced Options** item.
3. In the **Advanced Options**, choose **MTA Configuration**.
4. Choose the Configure postmaster address item.
5. Enter the email address to which administrative information should be addressed.
6. When finished, you can return to the **Advanced Options** menu from the **MTA Menu**.

Repeat these steps for each Gateway in the cluster.

CHAPTER 12

Monitoring the ACE XML Appliance Remotely

This chapter describes how to monitor the system using SNMP and syslog. It covers these topics:

12.1 About Appliance Monitoring

The event log viewer in the ACE XML Manager provides extensive information on the activities and conditions of the ACE XML appliances. For most purposes, it acts as the primary monitoring and troubleshooting tool for your deployment.

However, certain events may need to be monitored from external tools as well. For example, it may be useful to have information on the health of the ACE XML appliance or on failure of service transactions appear in an SNMP management system.

The ACE XML XML Gateway integrates with syslog and SNMP network management tools, so that you can view system status and activity information from these monitoring tools.

12.2 SNMP and ACE XML Appliances

The Simple Network Management Protocol (SNMP) is a widely used technology for monitoring resources on a network. The ACE XML appliance includes an SNMP agent that can provide information to an SNMP network management system (NMS). Versions 4.0 and later of the ACE XML XML Gateway support SNMP version 3, version 2c, and version 1.

The ACE XML Gateway includes a vendor-specific SNMP MIB that defines the properties available for SNMP monitoring, including properties representing its operational status, workload, and disk utilization. In addition to appliance state properties, the Gateway can provide SNMP systems with information on service activity, including service errors or successful transactions.

> **Note:** This chapter describes how to use SNMP for internal system monitoring. For information on using SNMP to monitor service activity, see the *Cisco ACE XML User's Guide*.

SNMP information is available in two forms: as queriable properties and as traps. A queriable property is a system value that is returned in response to an SNMP query, while a trap is an agent-initiated alerts sent to a management system.

The SNMP implementation of ACE XML appliances is based on the open source package, NET-SNMP package. If new to SNMP, refer to the NET-SNMP Web site (http://net-snmp.sourceforge.net/) for additional background information.

While you can retrieve SNMP queries to the ACE XML appliance without any special configuration requirements, to use advanced SNMP features, such as traps or encryption, you'll need to configure a few SNMP-related settings. This chapter describes the SNMP support, traps, and other SNMP configuration options relevant to the system.

SNMP Daemon

The SNMP daemon is enabled and running on the ACE XML appliances by default. The SNMP daemon listens for and responds to SNMP requests on the conventional port number for SNMP, port 161. You can query the appliance from an NMS or set up polling without any special configuration steps needed on the appliance.

Community Name

By default, the ACE XML system uses the community name `reactivity`. Traps are sent with a community name `public`.

12.3 ACE XML Appliance MIB

The MIB for the ACE XML appliance is located at the following location of the appliance filesystem:

/etc/reactivity/snmp/REACTIVITY-MIB.txt

The MIB contains the following managed objects. Note that the objects fall into three categories: platform, software, and traps.

Object	Description
`platform`	Information on the ACE XML appliance hardware platform.
`platformDescr`	A description of the platform running the ACE XML system, including the underlying operating system and processor.
`storage`	Information about hard drives on the appliance.
`diskUtilization`	The amount of storage used, as a percentage of the total hard drive capacity. In general, disk usage should not exceed 90%. If it does, a trap will be generated. You can remedy excessive disk utilization by moving backup log files off the appliance. It may be necessary to change backup procedures in order to remove log files more frequently.
`diskStatus`	The current state of the hard drive, with possible values of `ok(1)`, `failure(2)`, or `not Available(4)`. If `diskStatus` reports a failure, contact Cisco support.
`load`	The load average indicates the workload applicable to the CPU. Roughly speaking, it's the average number of active processes over the measured span. This includes processes that are waiting for I/O. A trap is sent for this property when one of the load values reaches 80. A high value, such as 70 or 80, may indicate that the Gateway is being sent more message traffic than it can process reliably. To resolve the problem, reconfigure load-balancers to spread traffic across more Gateway instances or add more Gateway instances to the cluster that is being overwhelmed.
`loadAverage1Min`	Average number of processes in the schedule queue for the one-minute period preceding the SNMP request.

Object			Description
	loadAverage5Min		Average number of processes in the schedule queue for the five-minute period preceding the SNMP request.
	loadAverage15Min		Average number of processes in the schedule queue for the fifteen-minute period preceding the SNMP request.
temperature			Information regarding the temperature of the hardware appliance, based on several internal sensors.
	temperatureStatus		A consolidated status of underlying hardware temperature sensors. Not all possible temperature sensors may be available in a given system, depending on its model. The status represents potential problems with a temperature of any device or card the platform supports. Possible values are `ok (1)`, `warning (2)`, `critical (3)`, `not available (4)`. If any sensor registers a value outside of its normal range of tolerance, this value reports `warning` or `critical`. In this case, verify that nothing is interrupting the airflow through the device and that the room temperature where the device is installed is not too hot. Otherwise contact Cisco support.
	temperatureStatus Message		Error messages of all reported failures.
devices			Third party devices installed on the ACE XML appliance.
	cryptoAccelerator		Information on cryptographic accelerator devices on the ACE XML appliance. **Note**: Not all objects in this category are available with the Cavium Nitrox XL Accelerator.
		cryptoInstalled	Whether a third party cryptographic acceleration is installed on the system.
		cryptoVendor	Third-party vender of the cryptographic acceleration card.
		cryptoVersion	Version of the cryptographic acceleration card.
		cryptoSerialNumber	Serial number of the cryptographic acceleration card. This value is not available for the Cavium Nitrox XL Accelerator.

Object		Description
	cryptoStatus	Status of the cryptographic acceleration card. Possible values of `ok (1)`, `warning (2)`, `failure (3)`, or `not Available (4)`. In the event of a `warning` or `failure` report on this value, contact Cisco support.
	statusMessage	Error messages of all reported failures
xmlAccelerator		Information on XML accelerator devices on the ACE XML appliance. **Note**: This object is deprecated. It applies to an XML accelerator hardware add-on card that is no longer available with the ACE XML Gateway appliance.
	xmlAccInstalled	Whether an XML accelerator card is installed, with possible values of `yes (1)`, and `no (2)`. **Note**: This object is deprecated. It applies to an XML accelerator hardware add-on card that is no longer available with the ACE XML Gateway appliance.
	xmlAccVendor	The vendor of the XML accelerator card installed on the system, if present. **Note**: This object is deprecated. It applies to an XML accelerator hardware add-on card that is no longer available with the ACE XML Gateway appliance.
	xmlAccVersion	Version of XML accelerator card. **Note**: This object is deprecated. It applies to an XML accelerator hardware add-on card that is no longer available with the ACE XML Gateway appliance.
	xmlAccSerialNumber	Serial number of XML acceleration card. **Note**: This object is deprecated. It applies to an XML accelerator hardware add-on card that is no longer available with the ACE XML Gateway appliance.
	xmlAccStatus	Status of XML acceleration card. Possible values of `ok (1)`, `warning (2)`, `failure (3)`, `not Available (4)`. In the event of a `warning` or `failure` report on this value, contact Cisco support. **Note**: This object is deprecated. It applies to an XML accelerator hardware add-on card that is no longer available with the ACE XML Gateway appliance.

Object		Description
	xmlAccStatus Message	Status message of XML acceleration card. **Note**: This object is deprecated. It applies to an XML accelerator hardware add-on card that is no longer available with the ACE XML Gateway appliance.
software		Information on the software currently installed on the ACE XML appliance.
	buildNumber	Deprecated. The release identifier is authoritative.
	versionString	The system version of the ACE XML Gateway software.
	releaseIdentifier	The release identifier string associated with the currently installed software and firmware. This is the same value as the "System Version" ID at the top of the System Management page in the console. You may need to provide this information when working with Cisco support to diagnose a problem.
	status	Status of various processors in the system.
		coreProcess — Status of the main process that controls the Gateway system. Possible values of up(1), if the Gateway process is running, or down(2), if it is not. This value does not report status of the Manager process. If this object reports down, contact Cisco support.
		ioProcesses — Status of the I/O processes that the Gateway uses to process requests and responses. This status reports up(1) when all Gateway I/O processes are up. If any I/O process is down, then this status reports somedown(2). You can identify which processes are down by examining the downProcesses element. If all Gateway I/O processes are down, this object reports alldown(3). This value does not report the status of any process on the Manager. Note that you can stop and start I/O processes in the System Management page of the ACE XML Manager web console. If an I/O process is down unexpectedly, contact Cisco support.

Object			Description
	downProcesses		Names of Gateway I/O processes that are down. If this node is empty, all Gateway I/O processes are up. This value does not report the status of any process on the Manager.
	processing		Information related to message processing.
		notificationTrapMessage	The message delivered with an SNMP trap generated for service handling.
traps			SNMP traps used by the Gateway to report conditions that require attention.
	diskUsageNotification		Disk space available to Gateway is below acceptable minimum. The ACE XML appliance sends this trap when the disk is more than 90% full. We recommend that you respond quickly to this notification. If the disk becomes too full to permit normal operation, the ACE XML Gateway shuts itself down and permits no traffic to flow. The precise amount of time you have depends on the amount of logging data your Gateway records, the overall size of your disk array, and whether resources are being consumed at a rate greater than normal due to an attack. For information on recovering from this condition, see Section 11.6, "Recovering from Low Disk Space." You can remedy excessive disk utilization by moving backup log files off the appliance. It may be necessary to change backup procedures in order to remove log files more frequently.
	diskFailureNotification		A disk on the ACE XML appliance has failed. If this trap is generated, contact Cisco support.

Object	Description
cpuOverloadNotification	One or more CPU load averages has exceeded the maximum value that guarantees reliable operation of the ACE XML appliance. The trap is sent when any of the monitored CPU load averages reports a value of 80 or greater. Upon CPU overload, the ACE XML appliance logs the error and shuts down. If configured as a Gateway, the appliance attempts to restart. This notification may indicate that the ACE XML Gateway is being sent more legitimate message traffic than it can process reliably. To resolve the problem, reconfigure load-balancers to spread traffic across more Gateway instances or add more Gateway instances to the cluster that is being overwhelmed.
temperatureAlert Notification	The temperature of an internal device, such as a CPU, is outside of its corresponding tolerance range. It is important to respond immediately to this notification by making a physical inspection of the appliance. Verify that nothing is interrupting the airflow through the device and that the room temperature where the device is installed is not too hot. Otherwise, contact Cisco support.
coreDownNotification	The core ACE XML Gateway or Manager process is down. This trap is sent whenever the core process goes down, including during scheduled shutdowns and restarts of the Manager or Gateway that the administrator initiates in the Web-based or Shell interfaces. When an unscheduled shutdown of the Gateway's core process occurs, the Gateway attempts to restart this process automatically; even if it succeeds in doing so, any unscheduled shutdown of the core process indicates the presence of a serious problem. In contrast, the Manager does not attempt to restart its core process after an unscheduled shutdown. If you experience an unexplained shutdown of the core process on an ACE XML Gateway or Manager, contact Cisco support for assistance.

Object	Description
ioProcessesDown Notification	One or more I/O processes is down. Inspect the downProcesses element for a listing of processes that are down. Stopped I/O processes can be restarted from the System Administration page of the ACE XML Manager console. If an I/O process is down unexpectedly, contact Cisco support.
xmlAcceleratorStatus Notification	This notification is sent when the XML processing accelerator module is installed and is malfunctioning. Problems that cause this trap to be sent may range from out-of-bounds operating temperature to complete failure of the module. As a first step in diagnosing the problem, examine other traps to discern the context of the failure, and examine the performance statistics of the Gateway. If you need help to isolate and resolve the problem, contact your Cisco support representative. If necessary, you can disable the XML accelerator and run the Gateway without it until you resolve the problem.
cryptoAcceleratorStatus Notification	The cryptographic accelerator module is installed and is malfunctioning. Problems that cause this trap to be sent may range from out-of-bounds operating temperature to complete failure of the module. If the cryptographic accelerator fails, the Gateway logs an error upon attempting any operation that requires a key the cryptomodule manages or an SSL connection the cryptomodule accelerates. In this event, contact Cisco support.
softwareNotificationTrap	This notification is generated for message traffic activity at the ACE XML Gateway. The appropriate remediation for this trap varies depending on the source condition. A service definition in a policy may be set to emit traps for any activity, in which case the trap is sent for successful request and response processing. However, it is usually use to indicate a service error, which may stem from such conditions as server not available or client authentication failure.

12.4 Configuring SNMP Settings

These instructions describe how to configure SNMP behavior for the ACE XML appliance. Both ACE XML Manager and Gateway produce SNMP information. Therefore, these steps should be performed on each Gateway and Manager in your deployment.

From the appliance configuration pages, `root` users can access SNMP settings by navigating to the **Main Menu > Advanced Options > SNMP Configuration** menu.

From there, you can specify security settings for SNMP access, a username/password for SNMP Version 3 access, and the trap destination. The following sections more instructions for using the configuration screen.

12.4.1 Security Settings

By default, the Gateway does not impose any special security requirements for SNMP access, other than the community string which can act as a shared secret. For additional security, you may choose to apply a password requirement to SNMP access or encrypt SNMP-related traffic.

Username/password access is a feature of SNMP version 3. To use it, therefore, you will need to use an NMS that can act as a version 3 SNMP user.

To configure security settings, from the Shell interface, go to **Main Menu > Advanced Options > SNMP Configuration > Security** screen.

The options for SNMP security are:

- **No Authentication**. The ACE XML appliance does not authenticate SNMP requests. This is the default. It permits requests in the form of unauthenticated version 1 and version 2c requests that supply the appropriate community string. If a version 3 user has been configured (as described in Section 12.4.2, "SNMP Version 3 User Settings"), version 3-style requests with the appropriate username and password will also be accepted, but are not required.
- **Authentication Only**. Only requests that supply the correct username and password are accepted. For information on configuring these settings, see Section 12.4.2, "SNMP Version 3 User Settings". For an example of this type of request, see Section 12.5.2, "Sample Request with Authentication (Version 3)."
- **Authentication and Privacy (Encryption)**. SNMP requests are authenticated and encrypted. The requests must provide the configured username and password combination and pass phrase

for the version 3 user. For an example of this type of request, see Section 12.5.3, "Sample Request with Authentication and Privacy (Version 3)."

From the **Security** menu, choose the option desired. For version 3 authenticated access, choose **Authentication Only** or **Authentication and Privacy**.

After enabling authentication, you will also need to configure the username and password and, if encryption is enabled, the passphrase for accessing the system, as described in the following section.

12.4.2 SNMP Version 3 User Settings

If using version 3 user authentication (which is enabled as described in Section 12.4.1, "Security Settings") you will need to provide the username and password required to authenticate requests for SNMP information. There are no credentials configured for SNMP users by default on a newly installed system.

To configure the user settings for SNMP authentication:

1. In the **SNMP Configuration** screen of the appliance shell, choose the **Version 3 User** item.
2. In the **Enter user name** screen, type the username of users authorized to access SNMP information.
3. Enter the password for user authentication.

   For security reasons, no on-screen feedback appears while you type the password and pass phrase as required by the next several steps. Type carefully; if you do not enter each password or pass phrase the same way twice, you'll be prompted to re-enter it.
4. Confirm the password by re-entering it.
5. In the **Please enter the new SNMP V3 User pass phrase** screen, enter a pass phrase for authenticated access.

   This pass phrase is a shared secret used for ensuring the privacy (encryption) of communication between the Gateway and SNMP user. You do not need to set a pass phrase if using authentication only.

   For security reasons, no user feedback appears on the screen as you type the pass phrase.
6. When prompted, retype the pass phrase.
7. In the **User configuration has been changed** screen, click **OK** or press the **Enter** key.

The user settings are configured and the **SNMP Configuration** screen appears.

12.4.3 Configuring ACE XML Appliance Traps

To enable trap production by the Gateway, you need to specify the destination Network Management System (NMS) by IP address or hostname. These steps should be taken on each appliance in the system.

To configure the trap destination:

1. From the **SNMP Configuration** menu of the appliance shell, choose the **Traps** item.
2. Enter the hostname or IP address of the destination system. Note that only a single destination system is permitted.

   The **Enter community string to send traps with** screen appears.
3. Enter the community string you want to accompany the traps. By default, the trap community string is `public`, which most management systems are configured to accept by default. If desired, enter another and click OK.
4. Enter `1` or `2` to specify the SNMP version, depending on what the NMS is able to accept:
   - An SNMP Version 1 NMS reports feedback only when queried.
   - An SNMP Version 2 NMS reports feedback continuously.

   The **SNMP Traps are reconfigured** screen appears.
5. Click **OK** or press the **Enter** key.

   The **SNMP Configuration** screen appears.

   You may now choose another SNMP configuration option or exit to the **Advanced Options** screen.

Note the following OIDs apply to the traps generated by the ACE XML appliance:

- `snmp.trap.oid [=.1.3.6.1.4.1.9.9.147.2.0.7]` – Object Identifier (OID) of the trap sent by the Gateway.
- `snmp.trap.message.oid [=.1.3.6.1.4.1.9.9.147.1.1.1.2.1.9.1]` – Object Identifier (OID) that identifies data belonging to the SNMP trap message sent by the Gateway.

12.5 SNMP Monitoring Example

To view the information available from the MIB, use the `snmpwalk` command. The `snmpwalk` command queries each object in the MIB, returning the value of each from the system targeted by the query, using the SNMP GETNEXT request. It's useful as a first-line test of the operability of the SNMP daemon on an appliance.

12.5.1 Sample Request (Version 1 or 2)

For SNMP version 1, the command is issued in the following form:

snmpwalk -v 1 -c reactivity -m /path/to/REACTIVITY-MIB.txt host_name_or_ip REACTIVITY-MIB::reactivity

For example:

[root@mini root]# snmpwalk -v 1 -c reactivity -m /etc/reactivity/snmp/REACTIVITY-MIB.txt localhost REACTIVITY-MIB::reactivity

To get the value of a specific object in the MIB, rather than the entire tree, you can use the `snmpget` command and pass the name of the managed object, such as:

snmpget -v 1 -c reactivity -m /etc/reactivity/snmp/REACTIVITY-MIB.txt sf4200.eng.example.com REACTIVITY-MIB::diskUtilization

This query return a value in the following form:

REACTIVITY-MIB::diskUtilization.0 = INTEGER: 22

12.5.2 Sample Request with Authentication (Version 3)

For authenticated, version 3 SNMP access, you need to supply a username and password combination when invoking snmpwalk instead of a community string. Before this is possible, you need to specify the username/password to use in the SNMP configuration settings as described in Section 12.4.2, "SNMP Version 3 User Settings."

Once you have done so, you can query the system as follows:

snmpwalk -v 3 -u v3user -l authNoPriv -a MD5 -A swordfish mini.eng.example.com .1.3.6.1.4.1.14709

In this command example, the username is v3user with a password of swordfish and authentication protocol of MD5. Also note that instead of querying by MIB name, the request used the common OID for the MIB, 1.3.6.1.4.1.14709. You can similarly query any MIB object by OID value rather than symbolic name.

12.5.3 Sample Request with Authentication and Privacy (Version 3)

If authentication and privacy are enabled, in the command, you will additionally need to supply the passphrase you have configured in the SNMP configuration settings:

snmpwalk -v 3 -u v3user -l authPriv -a MD5 -A swordfish -x DES -X swordfish mini.eng.example.com .1.3.6.1.4.1.14709

In this case, the passphrase, swordfish, is passed with the -X switch.

12.5.4 Sample Output

While the output from the snmpwalk command will vary from system to system, it will likely appear similar to the following:

Listing 12-1: Sample snmpwalk Output

```
REACTIVITY-MIB::platformDescr.0 = STRING: Linux
mini.eng.example.com 2.4.21-47.ELsmp #1 SMP Wed Jul 5
       20:38:41 EDT 2006 i686
REACTIVITY-MIB::diskUtilization.0 = INTEGER: 9
REACTIVITY-MIB::diskStatus.0 = INTEGER: ok(1)
REACTIVITY-MIB::loadAverage1Min.0 = STRING: 0.16
REACTIVITY-MIB::loadAverage5Min.0 = STRING: 0.05
REACTIVITY-MIB::loadAverage15Min.0 = STRING: 0.01
REACTIVITY-MIB::temperatureStatus.0 = INTEGER: ok(1)
REACTIVITY-MIB::temperatureStatusMessage.0 = STRING:
REACTIVITY-MIB::cryptoInstalled.0 = INTEGER: yes(1)
REACTIVITY-MIB::cryptoVendor.0 = STRING: ncipher
REACTIVITY-MIB::cryptoVersion.0 = STRING:  version string
       2.23.2cam4, 2.18.13cam1 built on Jun 28 2004 15:29:08
REACTIVITY-MIB::cryptoSerialNumber.0 = STRING: 2778-2DAF-B7B9
REACTIVITY-MIB::cryptoStatus.0 = INTEGER: ok(1)
REACTIVITY-MIB::statusMessage.0 = STRING: ok
REACTIVITY-MIB::xmlAccInstalled.0 = INTEGER: yes(1)
REACTIVITY-MIB::xmlAccVendor.0 = STRING: Tarari
REACTIVITY-MIB::xmlAccVersion.0 = STRING: Driver=3.1.2
CPP=00000003
       CPC=0004023d
REACTIVITY-MIB::xmlAccSerialNumber.0 = STRING: 04430008
REACTIVITY-MIB::xmlAccStatus.0 = INTEGER: ok(1)
REACTIVITY-MIB::xmlAccStatusMessage.0 = STRING: ok
REACTIVITY-MIB::buildNumber.0 = STRING: Release_Build832 832
REACTIVITY-MIB::versionString.0 = STRING: 5.0.1
REACTIVITY-MIB::releaseIdentifier.0 = STRING: 5.0.1-2007-01-26T20
REACTIVITY-MIB::coreProcess.0 = INTEGER: up(1)
REACTIVITY-MIB::ioProcesses.0 = INTEGER: somedown(2)
REACTIVITY-MIB::downProcesses.0 = STRING: reactor
```

12.6 SNMP Trap Example

An SNMP trap is an alert initiated by the managed agent (the Gateway, in this case) and sent to a monitoring system to notify the recipient of a condition or event that requires attention.

There are two types of traps that can be sent from the system:

- Service activity-related traps provide information on service activity, such as a server unavailable error, authentication failure, or even a successful service transaction through the Gateway.
- Appliance condition traps provide information on machine-level conditions for each appliance in the deployment, such as CPU utilization or temperature alerts.

Accordingly, there are two places where SNMP settings are configured, in the appliance configuration screens and in the Manager web console. Service-related traps are configured in the Manager web console. For more information on using service traps, see the *Cisco ACE XML Gateway User's Guide*.

By default, traps have the community string `public`.

The freely available NET-SNMP package includes a trap listener, snmptrapd, which you can use for trap production testing on the appliance.

Example traps from the appliance are shown in the following listing.

Listing 12-2: Trap Output Example

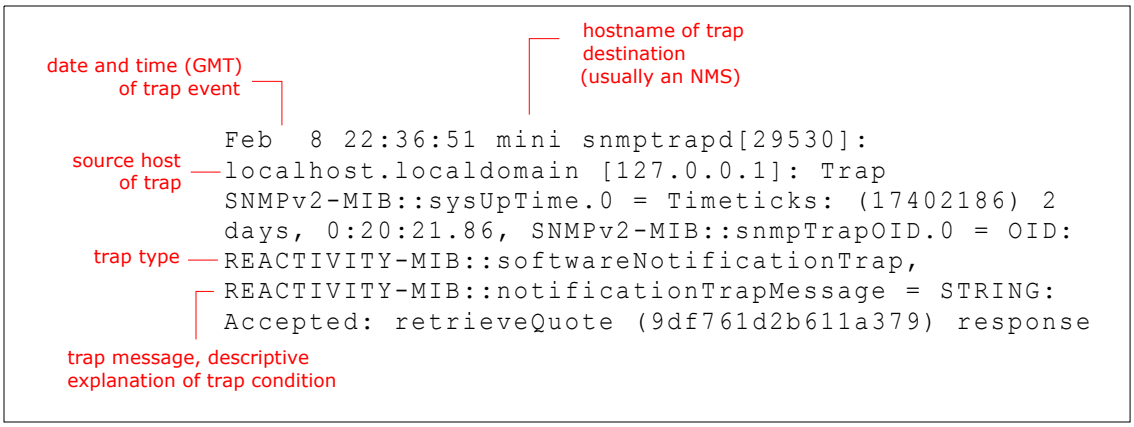
```
Feb  8 22:36:51 mini snmptrapd[29530]: localhost.localdomain
[127.0.0.1]: Trap SNMPv2-MIB::sysUpTime.0 = Timeticks: (17402186)
2 days, 0:20:21.86, SNMPv2-MIB::snmpTrapOID.0 = OID:
REACTIVITY-MIB::softwareNotificationTrap,
REACTIVITY-MIB::notificationTrapMessage = STRING: Accepted:
retrieveQuote (9df761d2b611a379) response

Feb  8 22:36:56 mini snmptrapd[29530]: localhost.localdomain
[127.0.0.1]: Trap SNMPv2-MIB::sysUpTime.0 = Timeticks: (17402678)
2 days, 0:20:26.78, SNMPv2-MIB::snmpTrapOID.0 = OID:
REACTIVITY-MIB::softwareNotificationTrap,
REACTIVITY-MIB::notificationTrapMessage = STRING: Denied:
retrieveQuote (9df761d2b611a379): -1 Validation Error Actor:
internal-firewall The message was found to be invalid.

Feb  9 00:11:01 target203 snmptrapd[2223]: 10.50.1.203:
Enterprise Specific Trap (60) Uptime: 5:24:33.98,
REACTIVITY-MIB::ioProcesses = INTEGER: somedown(2),
REACTIVITY-MIB::downProcesses = STRING: http-server reactor
```

The example shows three traps, reporting a successful service transaction, a service failure (invalid request), and down processes. Figure 12-1 shows the parts of a trap.

Figure 12-1: Trap format



12.7 Timeliness of MIB Results

SNMP requests to the ACE XML appliance return cached information rather than real-time results. The ACE XML appliance updates this cached information every ten minutes. Thus, it is possible that the results of SNMP requests may not always reflect the up-to-the minute status of the appliance.

For example, if you shut down the gateway process and then immediately get the value of the `software.status.coreProcess` object, you might not get the `down(2)` result you would expect. Subsequently, if you restart this process and get the value of this trap immediately after doing so, you may not get the `up(1)` result you would expect.

To obtain up-to-the minute status information, use the web console or Shell interfaces to the ACE XML appliance. For less timely needs, simply retry your SNMP request after about ten minutes. By then, the cached result that the appliance reports will likely reflect the machine's current status.

12.8 Monitoring the System with Syslog

The ACE XML system uses `syslog` internally to aggregate logging messages generated by the ACE XML Gateways. The ACE XML Gateways send information about traffic handling and other events to the ACE XML Manager via `syslog`.

> **Note:** The `syslog` implementation used by the ACE XML Gateways system is UDP-based. UDP is a best-effort delivery protocol—it does not guarantee message delivery. Therefore, it's possible to lose events between the Gateway and Manager in a busy network or in other unusual network conditions.

In addition to sending syslog events to the Manager, the ACE XML Gateway can be configured to send the events to other destinations as well. The destination host should be a syslog server or any host on which the syslog daemon is running. Syslog messages from the ACE XML Gateways are sent via UDP. Therefore, any firewalls between the Gateways and syslog destination should be configured to permit UDP traffic from the Gateway.

The syslog information generated by the Gateway and subject to forwarding to a syslog destination can be found in the following file: `/var/log/reactivity/user`. This file contains the information that normally appears in the event log viewer for Gateway events. Note that the Gateway maintains another syslog-formatted log file, `internal`. However, this file is used for internal debugging only and its use for syslog forwarding is not supported.

12.8.1 Configuring an Additional syslog Destination

To configure an additional syslog host, modify the following configuration file on each XML Gateway: `/etc/syslog.conf`

> **Caution:** Before attempting to adjust any settings in the `/etc/syslog.conf` file, consult Cisco ACE XML Gateway support.

Notice the following three lines at the end of the file:

```
# uncomment this line if you would like  /
                  XML Firewall event logs to be
# additionally sent to a remote logging server
#local0.* @myloghost.mydomain.com
```

To configure a remote syslog server, uncomment the final line and replace the placeholder destination with the location, by IP address or hostname, of your destination syslog host.

Be careful not to modify other syslog settings in this file. By default, each logging entry in the `/etc/syslog.conf` file begins with the '-' character, which instructs `syslog` not to synchronize the log file after each logging message. This configuration option is important. If you remove the '-' character, `syslog` attempts to synchronize the corresponding log file after each message is logged. On a busy Gateway, such frequent attempts to synchronize the log files can cause the Gateway to lose event log information.

12.8.2 ACE XML Gateway Syslog Format

The destination syslog system will usually need to process the log events received from the ACE XML Gateway in some way.

A sample syslog event generated by the Gateway is:

```
Sep 25 20:48:17 rg450 approuter[12199]: 1159217297224
[core /network/input 0A0064C6014C5B378A02317CB9C6792B
D] Successfully received message
```

The log entry can best be understand by considering its fields individually:

- `Sep 25 20:48:17`

  The first segments is a timestamp that conforms to syslog format. It is accurate to the second, but contains no year or time zone information. The Gateway always uses GMT as the time zone.

- `rg450`

  The hostname of the particular Gateway appliance that generated this event.

- `approuter[12199]`

  This segment is the name of the process that generated the event, and its Unix process ID. This is not likely to be useful to an external system.

- `1159217297224`

  The timestamp generated by the Gateway itself. It is expressed as the number milliseconds since the Unix epoch, Jan 1 1970 0:00 GMT. Where possible, this time value should be used instead of the syslog-generated timestamp as it is more precise and does not leave the year or time zone up to interpretation.

- `[core /network/input 0A0064C6014C5B378A02317CB9C6792B D]`

  The segment contains information about the event generated by the Gateway. Breaking it down:

  – `core`

    The name of the component in the Gateway which generated the event.

- `/network/input`

  The event category. This describes what part of message processing was executing when the event was generated.

- `0A0064C6014C5B378A02317CB9C6792B`

  A unique ID for the SOAP message the Gateway is processing. You may have many syslog events describing the same SOAP message, and so many events with the same unique ID. This ID is globally unique across all Gateways. You can confidently use it as the primary key in a table of messages, for instance. It is always a string of hex digits. Note that syslog events that describe things other than message processing, like system startup, may have some shorter text string in this field. Also not that requests and responses that are part of the same SOAP transaction will have different IDs.

- `D`

  This is the level of the event. The possible levels, from lowest to highest priority, are:

  - D: Debug
  - I: Info
  - N: Notice
  - W: Warning
  - E: Error
  - A: Alert

- Successfully received message

  A textual description of what occurred. There is no set format for this field—the text varies depending on the type of log event.

The sample shows debug-level event showing internal message exchange. Of more interest to a monitoring system will likely be information on traffic activity. The following shows the syslog event for a message that was successfully processed by the Gateway.

```
'Password Validation', access OK for 'retrieveQuote':
HTTP POST SOAP request (SOAPAction:
"http://oakinsurance.com/order/retrieveQuote") for
/service/order from 10.0.101.198
```

Note the following information in the sample:

- Password Validation

  This is the name of the authentication rule in the Gateway policy which allowed the message to proceed.

- retrieveQuote

  This is the name of the particular SOAP call in the Gateway policy that the message is being sent to.

- 10.0.101.198

  This is the IP address of the system that sent the SOAP message.

A successful message transaction generates at most one Notice-level event, as represented by this sample. If the Gateway rejects the message or otherwise discovers something wrong with the message, it may log one or more Warning-level events. Note that warning-level events are used to indicate problems with messages, not with the Gateway's operation. If a problem occurs with the Gateway itself, the event is logged at the Error or Alert level.

CHAPTER 13

Using the Command Line Interface (CLI)

This chapter describes the ACE XML system command-line interface. It covers these topics:

13.1 About the CLI

The ACE XML appliance includes a command-line interface (CLI) that enables you to perform many common administrative operations from the ACE XML Manager command line.

The capabilities provided by the CLI compose a subset of the functionality available in the ACE XML Manager web console, the interface for administering the system. The CLI is useful as an alternative to using the web console when you want to perform management operations quickly, particularly if already working in the ACE XML Manager web console environment.

More significantly, the CLI gives administrators a mechanism for executing administrative operations from scripts. Scripting CLI commands can significantly ease the process of deploying policies from a test environment to production.

Many of the commands in the CLI are intended to facilitate this process. For example, the CLI includes commands for compiling and deploying policies, renaming policy artifacts, and replacing certificates (since production security certificates normally differ from those used in a development or testing environment).

Note: It's possible for a policy to be edited by a CLI command at the same time as a Manager user is editing the policy in the ACE XML Manager web

console. The changes made by the CLI command are not immediately reflected in the policy as it appears in the ACE XML Manager web console. Console users must log out of the console and then log back in to see the effects of the command. In general, use care to avoid conflicts between multiple console users, including CLI users.

13.1.1 Command Summary

The following table provides an overview of the commands in the ACE XML Gateway CLI.

Command	Description
`compile`	Tags the head policy, compiles it, and places the result in the compiled policies directory.
`crl_status`	Reports the revoked security certificates known to the Gateway.
`deploy`	Tags the working policy in the ACE XML Manager and deploys to a given ACE XML Gateway.
`exportppf`	Exports the current working policy to a named file.
`getdeployed`	Retrieves the ID of the deployed policy.
`renamecert`	Renames the specified certificate.
`renamehandler`	Renames the specified handler.
`replacecert`	Replaces the named certificate.
`replacepkcs12key`	Replaces the named key using a PKCS12 file.
`replacekeyandcert`	Replaces the named key using separate key and certificate files.
`setserverhostname`	Changes the hostname used to address the given back-end HTTP server.
`setserverport`	Changes the port number used to address the given back-end HTTP server.
`sethttpport`	Changes the port number for the given HTTP port object (used to listen for incoming requests).

Command	Description
`sethttphostname`	Changes the hostname for the given HTTP port object (used to listen for incoming requests).
`sethandlerloglevel`	Changes the message logging level for the given handler.
`translate`	Translates the format of the policy to the latest version.
`validity`	Checks the working policy in the ACE XML Manager for validity problems and reports them to standard output.
`version`	Retrieves the product version.

Section 13.3, "Command Reference," provides more information on the commands.

13.1.2 Understanding Configuration Data

Before using the CLI commands to work with policies, it's a good idea to become acquainted with how configuration settings are kept in the ACE XML Manager. A policy is the set of configuration settings that control how traffic is passed through the ACE XML Gateway. It defines the handlers, services descriptors, access rules, and other behaviors and rules relating to service traffic.

The ACE XML appliance stores a policy in two forms:

- Working policy. The working draft of the policy in the ACE XML Manager. A working policy cannot be deployed until compiled.
- Compiled policy. Compiled policies are available for error checked and converted to the runtime format, suitable for deploying to ACE XML Gateways.

Many of the commands in the CLI require you to pass as an argument the path to the filestore you want to affect with the command. Since an ACE XML Manager can administer multiple ACE XML Gateway clusters, there may be multiple filestores on the Manager.

The working and compiled policies are kept in the following location on the ACE XML Manager file system:

`var/lib/reactivity/console_documents/cluster<num>/filestore`

Where *`cluster<num>`* is the directory name appropriate for the cluster you want to affect with the CLI command.

Note that the directory names of clusters are named with a prefix of "cluster" followed by an arbitrary number. To correlate a cluster as it is identified in the web console to a directory name, inspect the `cluster.properties` file in the cluster directory. It includes a name field that indicates the web console name for the cluster to which this policy corresponds.

You can use the `grep` command to retrieve this name. From the `/var/lib/reactivity` directory, run the following command:

```
grep "name=" /console_documents/*/ cluster.properties
```

The command returns the cluster name as it appears in the policy.

In the path passed in command arguments, replace *`cluster<num>`* with the directory name appropriate for the cluster you want to affect with the CLI command.

When using CLI commands to operate on the policy, keep in mind that operations that change policy artifacts, such as renaming handlers, are applied to the working policy, that is, the filestore contents. The policy must be compiled and deployed before the changes you perform with the CLI commands can be applied to traffic that passes through the Gateways managed by the ACE XML Manager.

Since the CLI commands operate on the same filesystem data as the web console, you'll need to perform the CLI commands as the same user on the appliance, which is user `agateway`. When running the command as `root` user, you should sudo as `agateway` to issue the command.

If the ACE XML Manager web console is open when a CLI command is invoked that modifies a policy, the changes made by the command are not immediately reflected in the console. In general, it's recommended that you use CLI commands only when the web console is not in use.

13.2 Using the Command-Line Interface

The CLI commands are available from the Bash command line on the ACE XML appliance.

> **Note:** For instructions on accessing the shell, see Section 4.5, "Accessing the bash Shell."

From the `usr/local/reactivity` directory on the ACE XML appliance, issue a CLI command in the following form:

```
# sudo -u agateway ./scripts/cli <command> <arg1> <arg2>
```

For example, to view the release version of the software, enter the following command:

```
# sudo -u agateway ./scripts/cli version
```

For a list of available commands, enter:

```
# sudo -u agateway ./scripts/cli
```

You can get usage information on a particular command by entering it without arguments. For example:

```
# sudo -u agateway ./scripts/cli sethttpport
```

13.3 Command Reference

This section provides information on the commands in the ACE XML Gateway CLI. It provides sample invocations of each command and output.

13.3.1 version

Prints the version number and release identifier of the ACE XML Manager software, in the form:

<version number>-<release identifier>

The release identifier can help with troubleshooting; when contacting customer support, you will often be asked for the release identifier number.

Also, it can help you ensure that all Gateway instances in a cluster are consistent in terms of their release version.

example

```
# sudo -u agateway ./scripts/cli version
  4.2-2005-04-09TOO
```

13.3.2 getdeployed

Retrieves the identifier, author, and compile date of the active policy on a specified Gateway. The policy author is the ACE XML Manager web console user who deployed the policy. An identifier is simply a unique identifier for the policy generated internally by the ACE XML Manager.

You can use this command to ensure that all ACE XML Gateways in a cluster are using the same policy.

format

```
getdeployed <host> <port>
```

options

- `host` is the IP address or hostname of the ACE XML Gateway.

- `port` is the port number on which the Gateway listens for Manager traffic, 8200, by default.

example

```
# sudo -u agateway ./scripts/cli getdeployed localhost 8200
Current policy version: ee579c2426064759
Policy author: administrator
Policy compiled on: Sat May 28 19:29:21 UTC 2005
```

13.3.3 compile

Compiles the working policy in the ACE XML Manager, tagging it with a description you specify, and places the result in the directory:

`var/lib/reactivity/console_documents/cluster<num>/filestore`

Where `cluster<num>` is the internal identifier for the cluster filestore. For more information, see Section 13.1.2, "Understanding Configuration Data."

This command is generally intended for testing purposes. In most cases, you would use `deploy`, which both compiles and deploys a policy.

format

`compile <filestore> <description>`

options

- `filestore` is the folder that contains the working policy to be compiled.
- `description` is a brief description of this version of the policy

13.3.4 deploy

Compiles the current working policy in the filestore, tags it with a description, and deploys to the specified Gateway.

Note: Note that CLI-based deployment circumvents approval requirements that may be enabled in the ACE XML Manager, which are applicable to Manager-based deployment.

format

`deploy <filestore> <host> <port> <description>`

options

- `filestore` is the folder that contains the working policy. For more information, see Section 13.1.2, "Understanding Configuration Data."

- `host` is the IP address or hostname of the ACE XML Gateway to which you want to deploy the compiled policy.
- `port` is the port number on which the Gateway listens for Manager traffic, 8200, by default.
- `description` is a required description of the policy.

example

```
# sudo -u agateway ./scripts/cli deploy
var/lib/reactivity/console_documents/cluster25233/filestore
10.0.101.72 8200 myPolicy
```

13.3.5 validity

Checks the working policy for validity problems and reports them to standard output. Examples of the types of problems this command may report include:

- expired certificate
- use of noNamespace schemas in SOAP messages
- other missing or corrupted resources

format

```
validity <filestore>
```

options

- `filestore` is the folder that contains the working policy. For more information, see Section 13.1.2, "Understanding Configuration Data."

13.3.6 exportppf

Exports the current working policy to a PPF file. PPF is ACE XML Gateways's Portable Policy Format. You can use a PPF file to archive a policy to backup media or to transfer a policy from one Manager to another.

As a command argument, specify the name of the file to which the policy will be written. If a file with the same name already exists, the file is overwritten.

The output PPF file is written to the current directory. From there, you can move it to another machine using `scp` (secure copy) or the ftp client available on ACE XML systems.

format

```
exportppf <filestore> <outputfile>
```

options

- `filestore` is the folder that contains the working policy. For more information, see Section 13.1.2, "Understanding Configuration Data."
- `outputfile` is the filename to which the policy is written.

example

```
# sudo -u agateway ./scripts/cli exportppf
/var/lib/reactivity/console_documents/cluster25325/filestore
myPPFFilestore.ppf
```

13.3.7 crl_status

Reports the CRL status of the ACE XML Gateway. The CRL, or certificate revocation list, shows the revoked certificates known to the Gateway.

format

`crl_status <host> <port>`

options

- `host` is the IP address or host name of the ACE XML Gateway for which you want to view a report.
- `port` is the port on which the Gateway listens for Manager traffic, typically `8200`.

example

```
# sudo -u agateway ./scripts/cli crl_status
10.0.101.73 8200
<crlstatus><crl><certid>...</certid><server>10.0.10
1.73</server><status>Fri Jun 24 14:59:22 UTC
2005...</status></crl></crlstatus>
```

13.3.8 translate

When updates occur to the ACE XML Gateway product, it's possible that changes are introduced to the filestore XML format. Normally, such changes are handled transparently, as a result of the product upgrade process and by importing PPF files.

This command lets you perform the operation explicitly, translating the XML format of the working policy to the latest version. It is intended primarily for use by the product updater.

format

`translate <filestore>`

options

- `filestore` is the folder that contains the working policy. For more information, see Section 13.1.2, "Understanding Configuration Data."

example

```
# sudo -u agateway ./scripts/translate
console_documents_filestore
```

13.3.9 replacecert

Replaces a certificate of a given filestore with another certificate. The certificate should be uploaded to the file system of the ACE XML Manager on which you are working before running this command.

format

`replacecert <filestore> <certResourceName> <certificate>`

options

- `filestore` is the folder that contains the working policy. For more information, see Section 13.1.2, "Understanding Configuration Data."
- `certResourceName` is the symbolic name of the certificate resource that you want to replace.
- `certificate` is the certificate file you want to use to replace the current certificate.

13.3.10 replacepkcs12key

Replaces the named key using a PKCS12 file. The PKCS12 file should be uploaded to the file system of the ACE XML Manager on which you are working before running this command.

format

`replacepkcs12key <filestore> <keyName> <pkcs12File> <password>`

options

- `filestore` is the folder that contains the working policy. For more information, see Section 13.1.2, "Understanding Configuration Data."
- `keyName` is the name of the key that you want to replace.
- `pkcs12File` is the PKCS12 file with the key that you want to use to replace the current key.
- `password` is the string used to encrypt the key.

13.3.11 replacekeyandcert

Replaces the named key using separate key and certificate files.

format

```
replacekeyandcert <filestore> <keyName> <keyFile> <password>
```

options

- `filestore` is the folder that contains the working policy. For more information, see Section 13.1.2, "Understanding Configuration Data."
- `keyName` is the name of the key that you want to replace.
- `keyFile` is the new key file you want to use.
- `certFile` is the new certificate that you want to use.
- `password` is the string used to encrypt the key.

13.3.12 renamecert

Renames the specified certificate.

format

```
renamecert <filestore> <oldCertName> <newCertName>
```

options

- `filestore` is the folder that contains the working policy. For more information, see Section 13.1.2, "Understanding Configuration Data."
- `oldCertName` is the name of the certificate that you want to rename.
- `newCertName` is the new name for the certificate.

13.3.13 renamehandler

Renames a specified handler. If more than one handler with the same name exists in the filestore, an error message appears that indicates the number of occurrences of the named handler.

format

```
renamehandler <filestore> <oldHandlerName> <newHandlerName>
```

options

- `filestore` is the folder that contains the working policy. For more information, see Section 13.1.2, "Understanding Configuration Data."

- `oldHandlerName` is the name of the handler that you want to rename.
- `newHandlerName` is the new name for the handler.

example

```
# sudo -u agateway ./scripts/cli renamehandler
var/lib/reactivity/console_documents/cluster25233/filestore
oldname newname
```

13.3.14 setserverhostname

Changes the hostname for a given back-end HTTP server. This value is used to address outgoing request traffic to the server.

format

`setserverhostname <filestore> <serverName> <newHost>`

options

- `filestore` is the folder that contains the working policy. For more information, see Section 13.1.2, "Understanding Configuration Data."
- `serverName` is the name of the HTTP that you want to modify. This is the symbolic name of the server used in the ACE XML Manager.
- `newHost` is the new host name for the HTTP server.

example

```
# sudo -u agateway ./scripts/cli setserverhostname
var/lib/reactivity/console_documents/cluster25233/filestore
erpserver server2
   Found one HTTPServer named: 'erpserver'
   Server hostname set
```

13.3.15 setserverport

Changes the port for the given back-end HTTP server. This value is used to address outgoing request traffic to the server.

format

`setserverport <filestore> <serverName> <newPort>`

options

- `filestore` is the folder that contains the working policy. For more information, see Section 13.1.2, "Understanding Configuration Data."

- `serverName` is the name of the HTTP that you want to modify. This is the logical name of the server, as it is known in the policy.
- `newPort` is the new HTTP port number to which to address traffic to the server.

example

```
# sudo -u agateway ./scripts/cli setserverport
var/lib/reactivity/console_documents/cluster25233/filestore
erpserver 81
Found one HTTPServer named: 'erpserver'
Server port set
```

13.3.16 sethttpport

Changes the HTTP port number for a port object. A port object defines the port number, along with other listening port attributes, on which handlers listen for incoming traffic.

format

`sethttpport` *`<filestore> <portName> <newPortNumber>`*

options

- `filestore` is the folder that contains the working policy. For more information, see Section 13.1.2, "Understanding Configuration Data."
- `portName` is the logical name of the port object, as it is known in the policy.
- `newPortNumber` is the new port number on which the named port object listens for incoming traffic.

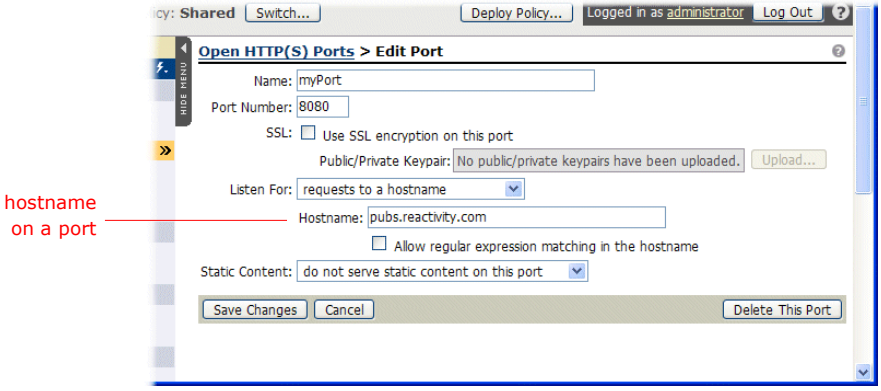
example

```
# sudo -u agateway ./scripts/cli sethttpport
var/lib/reactivity/console_documents/cluster25233/filestore
myHandlerPort 8181
   Found one HTTPPort named: 'myHandlerPort'
   Port set
```

13.3.17 sethttphostname

The `sethttphostname` command lets you change the hostname on which the port object listens. (Figure 13-1 shows the equivalent setting in the ACE XML Manager web console.)

Figure 13-1: Hostname port attribute



format

```
sethttphostname <filestore> <portName>
<newHostname>
```

options

- `filestore` is the folder that contains the working policy. For more information, see Section 13.1.2, "Understanding Configuration Data."
- `portName` is the logical name of the port object, as it is known in the policy.
- `newHostName` is the new hostname on which the port object listens for incoming traffic.

example

```
# sudo -u agateway ./scripts/cli sethttphostname
var/lib/reactivity/console_documents/cluster25233/filestore
myPort docs.example.com
Found one HTTPPort named: 'myHandlerPort'
Hostname set
```

13.3.18 sethandlerloglevel

Changes the message logging level for the given handler.

format

```
sethandlerloglevel <filestore> <handlerName>
<level>
```

options

- `filestore` is the folder that contains the working policy. For more information, see Section 13.1.2, "Understanding Configuration Data."

- `handlerName` is the logical name of the handler object, as it is known in the policy.
- `level` is the new log level, with the following options:
  - `debug` for logging of inbound and outbound message bodies.
  - `full` for logging of outbound message bodies only.
  - `stats` log statistics only, no message content.

CHAPTER 14

Shell Menu Reference

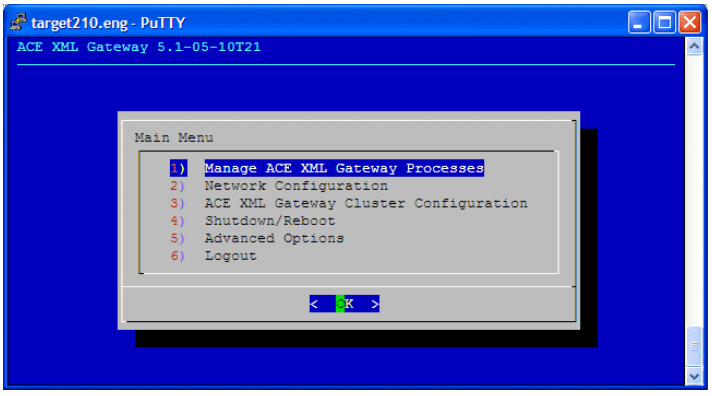
The chapter provides an overview of the menus in the Shell interface. It covers these topics:

- Main Menu
- Manage ACE XML Gateway Processes Menu
- Network Configuration Menu
- ACE XML Gateway Cluster Configuration Menu
- Shutdown/Reboot Menu
- Advanced Options Menu

14.1 Main Menu

The main page of the console menu appears as shown in Figure 14-1.

Figure 14-1: Main Menu



Note: For information on logging into the Shell interface, see Chapter 4, "Accessing the Shell Interface."

This menu has these items:

- **Manage ACE XML Gateway Processes** displays the current operational status of the appliance, whether running or stopped. It also allows you to stop or start those processes.
- **Network Configuration** contains the network settings for this ACE XML appliance.
- **ACE XML Gateway Cluster Configuration** contains settings that control the operation mode of the appliance, whether it should act as a Manager, Gateway, or a standalone appliance.
- **Shutdown/Reboot** shuts down or reboots this appliance. This option is the recommended method for shutting down and rebooting the system. Note that the `shutdown -h` shell command does not remove power to the system.
- **Advanced Options** contains administrative settings for the ACE XML appliance, including SSL engine settings, Netegrity server settings, the `root` password, SNMP settings, and more. It also lets you access the bash shell on the appliance.
- **Logout** logs out of the Shell Interface.

14.2 Manage ACE XML Gateway Processes Menu

Use the **Manage ACE XML Gateway Processes** menu to display and change the operating status of the ACE XML Gateway and Manager. The menu has these items:

- **Display Current Status** lists the operational status for the Gateway and Manager. Each process is shown with a status of "running" or "stopped".
- **Restart All Configured Services** restarts all currently enabled processes immediately.
- **Stop ACE XML Gateway** halts the primary traffic listening process on the Gateway. If you choose this option, the option changes to **Start Gateway**.

Note: This item does not appear if the ACE XML appliance has never been configured, if the appliance is configured as a dedicated Manager, or if the appliance is configured as an inactive appliance; that is, the appliance must already be configured as a Gateway in order for this menu item to appear.

- **Stop ACE XML Manager** halts the Manager process. If chosen, the option changes to **Start ACE XML Manager**.

  Note: This item does not appear if the ACE XML appliance has never been configured, if the appliance is configured as a dedicated Gateway, or if the appliance is configured as an inactive appliance. The appliance must be configured as a Manager in order for this menu item to appear.

- **Return to Main Menu** displays the **Main Menu**.

14.3 Network Configuration Menu

This menu contains the network settings for the ACE XML appliance, such as its host name, IP address, name servers it may use, and the configuration of its Ethernet interfaces.

The Network Configuration menu has these items:

- **Hostname** is the fully-qualified domain name of this ACE XML appliance.
- **IP Gateway** identifies the IP address of the default TCP/IP gateway in the appliance's subnet.
- **Name Servers** specifies by IP address domain name servers (DNS) that resolve IP addresses for this ACE XML appliance.
- **Interface eth0** sets parameters for the network interface, including its IP address, netmask, speed (10baseT, 100baseT, Gigabit, or auto), duplex (half, full, or auto), and static routes.

  Your appliance may have anywhere from one to four network interfaces. Menu options for configuring the other interfaces have similar labels. For example, the second interface would be labeled **Interface eth1**, the third would be **Interface eth2**, and so on.

- **View Routing Table** displays the IP routing table, as if you executed the shell's `route` command, passing no arguments.
- **Test Network Settings** tests the validity of this appliance's current network settings, such as whether Ethernet interfaces are enabled, whether the current IP settings are well-formed and whether DNS servers and other ACE XML appliances can be pinged successfully.
- **Return to Main Menu** exits the **Network Configuration** page and returns to the **Main Menu**.

14.4 ACE XML Gateway Cluster Configuration Menu

Use this option to configure the operating mode of the appliance, either as a Manager, Gateway, both (standalone), or inactive.

This menu has these items:

- **ACE XML Gateway Cluster Member** sets the operating mode for this appliance as a Gateway, either operating as a single Gateway or within a cluster. If you choose this option, there must be at least one other ACE XML appliance in your system, the ACE XML Manager. To configure this mode, you need to set the IP address of the ACE XML Manager that is to control this Gateway appliance.
- **ACE XML Manager** sets the operating mode for this appliance as an ACE XML Manager. A Manager appliance inspects, configures, and controls all Gateway appliances configured as members of its cluster.
- **Both Gateway and Manager** configures the appliance to act as both Manager and Gateway. This configuration is known as a standalone mode.
- **Inactive Machine** disables all non-console activity.

14.5 Shutdown/Reboot Menu

This menu item enables you to turn off the appliance safely, reboot it, or return to the **Main Menu**.

- To reboot the appliance, choose the **Reboot** item.
- To shut down the appliance, choose the **Shutdown** item.

14.6 Advanced Options Menu

The **Advanced Options** menu provides version information and other configuration options, such as hardware acceleration for SSL, configuration of SNMP monitoring, and Netegrity registration options. This menu has these items:

- **Time Settings** enables or disables the use of one or more Network Time Protocol servers.
- **SSL Engine Configuration** enables or disables a hardware-based SSL accelerator.

- **Boot Settings** configures the logging destination of boot messages. The appliance can be configured to send boot messages to an attached video monitor (the default) or to the serial port.
- **Netegrity Configuration** configures the appliance to work with a specified Netegrity SiteMinder or TrafficMinder server.

  For more information, see the tech note titled *Using Netegrity Authentication Sources*.
- **Change root Password** changes the root password for this ACE XML appliance. Specifying a secure root password for each of your ACE XML appliances is essential to protecting the security of your network.
- **SNMP Configuration** configures SNMP settings for this ACE XML appliance.

  For more information, see Chapter 12, "Monitoring the ACE XML Appliance Remotely."
- **Version Information** provides version numbers of the currently-installed Gateway software, operating system kernel, and other components of the system.
- **MTA Configuration** configures the message transfer agent (MTA) that supports ebXML messages.
- **Traffic Management** enables use of optional Actional Looking Glass management adapters for monitoring the Gateway.
- **Run Bash** suspends the appliance shell temporarily and runs the `bash` shell.
- **Return to Main Menu** exits the **Advanced Options** page and returns to the **Main Menu**.

CONTENTS