Best Practices: Server Security Hardening

The following sections explain how to enhance server security by eliminating or controlling individual points of security exposure.

Disable Insecure Services

You should disable non-secure services if you are not using them. For example: TFTP and FTP are not secure protocols. These services are typically used to transfer firmware or software images to and from network devices and Prime Infrastructure. They are also used for transferring system backups to external storage. We recommend that you use secure protocols (such as SFTP or SCP) for such services.

To disable FTP and TFTP services:

Step 1 Log in to Prime Infrastructure with a user ID with administrator privileges.

Step 2 Select **Administration** > **Settings** > **System Settings** > **General** > **Server**.

Step 3 Select the Disable buttons for FTP and TFTP.

Step 4 Restart Prime Infrastructure to apply the updated settings.

Disable Root Access

Administrative users can enable root shell access to the underlying operating system for trouble shooting purposes. This access is intended for Cisco Support teams to debug product-related operational issues. We

recommend that you keep this access disabled, and enable it only when required. To disable root access, run the command **root_disable** from the command line (see How to Connect Via CLI).

During installation, Prime Infrastructure also creates a web root user account, prompting the installer for the password to be used for this account. The web root account is needed to enable first-time login to the Prime Infrastructure server and its web user interface. We recommend that you never use this account for normal operations. Instead, use it to create user IDs with appropriate privileges for day-to-day operations and network management, and administrative user IDs for managing Prime Infrastructure itself. Once these user accounts are created, disable the default "web root" account created at install time, and create user accounts using your administrative user IDs thereafter.

If you forget the shell password, you can recover (and then reset) the shell password by following the steps to recover the administrator password. See Recovering Administrator Passwords on Virtual Appliances . Because recovering the administrator password requires the Prime Infrastructure server to reboot, your system might go down for approximately 20 minutes.

To disable the root accounts:

Step 1 Open a CLI session with the Prime Infrastructure server (seeHow to Connect Via CLI). Do not enter "configure terminal" mode.

Step 2 Disable the web root account by entering the following command:

PIServer/admin# **ncs webroot disable**

Prime Infrastructure disables the web root account.

Step 3 Disable the root shell account by entering the following command at the prompt:

PIServer/admin# **shell disable**

Prime Infrastructure will prompt you for the root shell account password. Enter it to complete disabling of the root shell account.

Use SNMPv3 Instead of SNMPv2

SNMPv3 is a higher-security protocol than SNMPv2. You can enhance the security of communications between your network devices and the Prime Infrastructure server by configuring the managed devices so that management takes place using SNMPv3 instead of SNMPv2.

You can choose to enable SNMPv3 when adding new devices, when importing devices in bulk, or as part of device discovery. See Related Topics for instruction on how to perform each task.

Related Topics

Use SNMPv3 to Add Devices, on page 2
Use SNMPv3 to Import Devices, on page 3
Use SNMPv3 to Run Discovery, on page 3

Use SNMPv3 to Add Devices

To specify SNMPv3 when adding a new device:

Step 1 Select **Inventory** > **Device Management** > **Network Devices**

Step 2 Choose **Add Device**.

Step 3 In the SNMP Parameters area, in Version, select v3.

Step 4 Complete the other fields as appropriate, then click **Add**.

Related Topics

Use SNMPv3 to Import Devices, on page 3
Use SNMPv3 to Run Discovery, on page 3
Use SNMPv3 Instead of SNMPv2, on page 2

Use SNMPv3 to Import Devices

To specify use of SNMPv3 when importing devices in bulk:

Step 1 Select **Inventory** > **Device Management** > **Network Devices**.

Step 2 Choose Bulk Import. The Bulk Import page appears.

Step 3 Download the device add sample template from the “here” link on the Bulk Import page.

Step 4 Edit the template file using any CSV-compatible application. For each row representing a device in the CSV import file:

a) In the snmp version column, enter 3.

b) Enter appropriate values in the snmpv3_user_name, snmpv3_auth_type, snmpv3_auth_password, snmpv3_privacy_type, and snmpv3_privacy_password columns.

c) Complete other columns as appropriate for your devices.

Step 5 Select **Inventory** > **Device Management** > **Network Devices**, then click Bulk Import and import your modified CSV file.

Related Topics

Use SNMPv3 to Add Devices, on page 2
Use SNMPv3 to Run Discovery, on page 3
Use SNMPv3 Instead of SNMPv2, on page 2

Use SNMPv3 to Run Discovery

To specify SNMPv3 as part of device discovery:

Step 1 Select **Inventory** > **Device Management** > **Discovery**. The Discovery Jobs page appears.

Step 2 Click the Discovery Settings link in the upper right corner of the page. The Discovery Settings page appears.

Step 3 Choose **New** to add new SNMP v3 credentials.

Step 4 Complete the fields as needed.

Step 5 Click **Save** to save the SNMPv3 settings and use them thereafter.

Related Topics

Use SNMPv3 to Add Devices, on page 2
Use SNMPv3 to Import Devices, on page 3
Use SNMPv3 Instead of SNMPv2, on page 2

Authenticate With External AAA

User accounts and password are managed more securely when they are managed centrally, by a dedicated, remote authentication server running a secure authentication protocol such as RADIUS or TACACS+.

You can configure Prime Infrastructure to authenticate users using external AAA servers. You will need to access the **Administration > Users > Users, Roles & AAA** page to set up external authentication via the Prime Infrastructure graphic user interface (GUI). You can also set up external authentication via the command line interface (CLI). See Related Topics for instructions on how to set up AAA using each method.

Related Topics

Set Up External AAA Via GUI, on page 4
Set Up External AAA Via CLI, on page 4

Set Up External AAA Via GUI

To set up remote user authentication via the GUI:

Step 1 Log in to Prime Infrastructure with a user ID that has administrator privileges.

Step 2 Select **Administration > Users > Users, Roles & AAA > TACACS+ or Administration > Users > Users, Roles & AAA > RADIUS**.

Step 3 Enter the TACACS+ or RADIUS server IP address and shared secret in the appropriate fields.

Step 4 Select **Administration > Users > Users, Roles & AAA > AAA Mode Settings**.

Step 5 Set the AAA mode as appropriate.

Related Topics

Authenticate With External AAA, on page 4
Set Up External AAA Via CLI, on page 4

Set Up External AAA Via CLI

To set up remote user authentication via the CLI:

Step 1 Log in to Prime Infrastructure using the command line, as explained in How to Connect Via CLI . Be sure to enter “configure terminal” mode.

Step 2 At the prompt, enter the following command to setup an external TACACS+ server:

PIServer/admin/terminal# aaa authentication tacacs+ server **tacacs**-ip key plain *shared-secret*

Where:

- **tacacs**-ip is the IP address of an active TACACS+ server.
- *shared-secret* is the plain-text shared secret for the active TACACS+ server.

Step 3 At the prompt, enter the following command to create a user with administrative authority, who will be authenticated by the above AAA server:

PIServer/admin/terminal# **username** *username password* **remote role admin email** *emailID*

Where:

- *username* is the name of the user ID.
- *password* is the plain-text password for the user.
- *emailID* is the email address of the user (optional).

Related Topics

Authenticate With External AAA, on page 4
Set Up External AAA Via GUI, on page 4

Enable NTP Update Authentication

Network Time Protocol (NTP) version 4, which authenticates server date and time updates, is an important way to harden server security. Note that you can configure a maximum of three NTP servers with Prime Infrastructure.

To set up authenticated NTP updates:

Step 1 Log in to Prime Infrastructure using the command line, as explained in How to Connect Via CLI .Be sure to enter “configure terminal” mode.

Step 2 At the prompt, enter the following command to setup an external NTPv4 server:

PIServer/admin/terminal# ntp server serverIP userID plain password

Where:

- serverIP is the IP address of the authenticating NTPv4 server you want to use.
- userID is the md5 key id of the NTPv4 server.
- password is the corresponding plain-text md5 password for the NTPv4 server.

  For example: ntp server 10.81.254.131 20 plain MyPassword

Step 3 To ensure that NTP authentication is working correctly, test it by executing the following commands:

- To check the NTP update details: sh run
- To check NTP sync details: sh ntp

Enable OCSP Settings on the Prime Infrastructure Server

Online Certificate Status Protocol (OCSP) enables certificate-based authentication for web clients using OCSP responders. Typically, the OCSP responder's URL is read from the certificate's Authority Information Access (AIA). As a failover mechanism, you can configure the same URL on the Prime Infrastructure server as well

To set up a custom URL of an OCSP responder, follow the steps below.

Step 1 Log in to the Prime Infrastructure server using the command line, as explained in How to Connect Via CLI . Do not enter "configure terminal" mode.

Step 2 At the prompt, enter the following command to enable client certificate authentication:

PIServer/admin# **ocsp responder custom enable**

Step 3 At the prompt, enter the following command to set the custom OCSP responder URL:

PIServer/admin# **ocsp responder set url** *Responder#URL*

Where:

- *Responder#* is the number of the OCSP responder you want to define (e.g., 1 or 2).
- *URL* is the URL of the OCSP responder, as taken from the client CA certificate.

  Note that there should be no space between the *Responder#* and *URL* values.

Step 4 To delete an existing custom OCSP responder defined on the Prime Infrastructure server, use the following command:

PIServer/admin# **ocsp responder clear url** *Responder#*

If you do not already know the number of the OCSP responder you want to delete, use the **show security-status** command to view the OCSP responders currently configured on the server. For details, see Check On Server Security Status, on page 8.

Set Up Local Password Policies

If you are authenticating users locally, using Prime Infrastructure's own internal authentication, you can enhance your system's security by enforcing rules for strong password selection.

Note that these policies affect only the passwords for local Prime Infrastructure user IDs. If you are authenticating Prime Infrastructure users via a centralized or remote AAA server, you can enforce similar protections using the functions of the AAA server.

To enforce local password policies:

Step 1 Log in to Prime Infrastructure with a user ID that has administrator privileges.

Step 2 Select **Administration > Users > Users, Roles & AAA > Local Password Policy**.

Step 3 Select the check boxes next to the password policies you want to enforce, including:

- The minimum number of characters passwords must contain.
- No use of the username or “cisco” as a password (or common permutations of these).
- No use of “public” in root passwords.
- No more than three consecutive repetitions of any password character.
- Passwords must contain at least one character from three of the following character classes: upper case, lower case, digit, and special character.
- Whether the password must contain only ASCII characters.
- Minimum elapsed number of days before a password can be reused.
- Password expiration period.
- Advance warnings for password expirations.

If you enable any of the following password policies, you can also specify:

- The minimum password length, in number of characters.
- The minimum elapsed time between password re-uses.
- The password expiry period.
- The number of days in advance to start warning users about future password expiration.

Step 4 Click **Save**.

Disable Individual TCP/UDP Ports

The following table lists the TCP and UDP ports Prime Infrastructure uses, the names of the services communicating over these ports, and the product’s purpose in using them. The “Safe” column indicates whether you can disable a port and service without affecting Prime Infrastructure’s functionality.

Table 1: Prime Infrastructure TCP/UDP Ports

Port	Service Name	Purpose	Safe?
21/tcp	FTP	File transfer between devices and server	Y
22/tcp	SSHD	Used by SCP, SFTP, and SSH connections to and from the system	N
69/udp	TFTP	File transfer between devices and the server	Y
80/tcp	HTTP	Provisioning of Nexus devices	Y
162/udp	SNMP-TRAP	To receive SNMP Traps	N
443/tcp	HTTPS	Primary Web Interface to the product	N
514/udp	SYSLOG	To receive Syslog messages	N

Port	Service Name	Purpose	Safe?
1522/tcp	Oracle	Oracle/JDBC Database connections: These include both internal server connections and for connections with the High Availability peer server.	N
8082/tcp	HTTPS	Health Monitoring	N
8087/tcp	HTTPS	Software updates on HA Secondary Systems	N
9991/udp	NETFLOW	To receive Netflow streams (enabled if Assurance license installed)	N
9992/tcp	PI Tomcat Process	Lync Monitoring in Assurance	N
61617/tcp	JMS (over SSL)	For interaction with remote Plug&Play Gateway server	Y

Check On Server Security Status

Prime Infrastructure administrators can connect to the server via CLI and use the **show security-status** command to display the server's currently open TCP/UDP ports, the status of other services the system is using, and other security-related configuration information. For example:

Step 1 Log in to Prime Infrastructure using the command line, as explained in Connecting Via CLI . Do not enter "configure terminal" mode.

Step 2 Enter the following command at the prompt:

PIServer/admin# **show security-status**

Depending on your settings, you will see output like the following:

Open TCP Ports : 21 22 80 443 1522 8082 9992 11011:11014 61617

Open UDP Ports : 69 162 514 9991

FIPS Mode : disabled

TFTP Service : enabled

FTP Service : enabled

JMS port (61617) : enabled

Root Access : disabled

Client Auth : enabled

OCSP Responder1 : http://10.77.167.65/ocsp

OCSP Responder2 : http://10.104.178.99/ocsp