Configuring System Profiles

This section includes the following topics:

System Profile Overview

Prime Network Services Controller provides one default System profile. The System profile includes time zone, DNS domain, DNS Server and NTP Server IP address information that is automatically generated using the data taken from initial Prime Network Services Controller installation. The System profile also contains the following policies: log file, fault, syslog, and core file. You can add and modify DNS server, NTP server, and policy information associated to the default system profile. However, you cannot create a new DNS domain or delete the default System profile.

Note

- Access to a DNS server and an NTP server is required for Prime Network Services Controller to communicate with the Amazon Cloud Provider.
- If you change the fully qualified domain name (FQDN), you must reconfigure Prime Network Services Controller connectivity with the hypervisor.

Policies in System Profiles

You can create multiple policies and assign them to the System profile. To manage policies for the default System profile, choose **Administration > System Profile**.

Note The system profile uses name resolution to resolve policy assignments. For details, see Name Resolution in a Multi-Tenant Environment.

The following policies, which are created under root, are visible in the System profile.:

- Core file
- Fault
- Log file
- Syslog

Policies created under root are visible to both the System profile and the Device profile.

Note You cannot delete existing default policies.

Configuring Policies

Configuring a Core File Policy Profile

You can create and modify the core file policy attributes. For more information on core file policy attributes, see the Core File Attributes Table.

To add, modify, or delete a core file policy:

Procedure

Step 1 Choose **Administration > System Profile > root > Policies > Core File**.

Step 2 In the General tab, do one of the following:

- To add a core file policy, click **Add Core File Policy**. Enter the appropriate information and click **OK**
- To edit a core file policy, select the policy, and then click **Edit**. Edit the appropriate fields and click **OK**.
- To delete a core file policy, select the policy, and then click **Delete**.

Core File Attributes Table

Field	Description
Name	Core file policy name, containing 1 to 32 characters. You can use alphanumeric characters, hyphen (-), underscore (_), and period (.). You cannot change the name after the policy has been saved.
Description	Brief policy description, containing 1 to 256 characters. You can use alphanumeric characters, hyphen (-), underscore (_), and period (.).
Admin State	Indicate whether the administrative state of the policy is to be enabled or disabled.
Hostname/IP Address	Hostname or IP address to use for this policy. If you use a hostname rather than an IP address, you must configure a DNS server in Prime Network Services Controller.
Port	Port number for sending the core dump file. This field is read-only for InterCloud policies.
Protocol	Protocol for exporting the core dump file (tftp only).
Path	Path to use when storing the core dump file on a remote system. The default path is /tftpboot; for example, /tftpboot/*test*, where *test* is the subfolder.

Configuring a Fault Policy

When the system boots up, a default fault policy is created. You can add additional fault policies or modify existing ones. However, you cannot delete the default fault policy. For more information on fault policy attributes, see the Fault Policy Attributes Table.

To add, modify, or delete a fault policy:

Procedure

Step 1 Choose **Administration > System Profile > root > Policies > Fault**.

Step 2 In the General tab, do one of the following:

- To add a fault file policy, click **Add Fault File Policy**. Enter the appropriate information and click **OK**
- To edit a fault file policy, select the policy, and then click **Edit**. Edit the appropriate fields and click **OK**.

- To delete a fault file policy, select the policy, and then click **Delete**.

Fault Policy Attributes Table

Field	Description
Name	Fault policy name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.
Description	Brief policy description.
Flapping Interval	Length of time (in hours, minutes, and seconds) that must elapse before the system allows a fault to change its state. Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, the system does not allow a fault to change its state until this amount of time has elapsed since the last state change. If the condition reoccurs during the flapping interval, the fault returns to the active state. If the condition does not reoccur during the flapping interval, the fault is cleared. What happens at that point depends on the setting in the Clear Faults Retention Action field. The default flapping interval is ten seconds.
Clear Faults Retention Action	Action to be taken when faults are cleared: • retain—Retain the cleared faults. • delete—Delete fault messages as soon as they are marked as cleared.

Field	Description
Clear Faults Retention Interval	How long the system is to retain cleared fault messages: • Forever—The system retains all cleared fault messages regardless of their age. • Other—The system retains cleared fault message for a specified the length of time. In the spinbox that is displayed when you select this option, enter the length of time (in days, hours, minutes, and seconds) that the system is to retain cleared fault messages.

Configuring a Logging Policy

When the system boots up, a default logging policy is created. You can add additional log policies or modify existing ones. However, you cannot delete the default log policy. For more information on logging policy attributes, see the Logging Policy Attributes Tables.

Procedure

Step 1 Choose **Administration > System Profile > root > Policies > Log File**.

Step 2 In the General tab, do one of the following:

- To add a logging file policy, click **Add Logging File Policy**. Enter the appropriate information and click **OK**
- To edit a logging file policy, select the policy, and then click **Edit**. Edit the appropriate fields and click **OK**.
- To delete a logging file policy, select the policy, and then click **Delete**.

Logging Policy Attributes Tables

Field	Description
Name	Logging policy name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.

Field	Description
Description	Brief policy description.
Log Level	One of the following logging severity levels: • debug0 • debug1 • debug2 • debug3 • debug4 • info • warning • minor • major • critical The default log level is info.
Backup Files Count	Number of backup files that are filled before they are overwritten. The range is 1 to 9 files, with a default of 2 files.
File Size (bytes)	Backup file size. The range is 1 MB to 100 MB with a default of 5 MB.

Configuring a Syslog Policy

When the system boots up, a default syslog policy is created. You can add additional syslog policies or modify existing ones. However, you cannot delete the default syslog policy. For more information on syslog policy attributes, see the Syslog Policy Attributes Table.

The syslog message settings that you configure for the System profile apply to Prime Network Services Controller syslog messages only. These settings do not affect other, non-Prime Network Services Controller syslog messages.

To add, modify, or delete a syslog policy:

Procedure

Step 1 Choose **Administration > System Profile > root > Policies > Syslog**.

Step 2 In the General tab, do one of the following:

- To add a syslog policy, click **Add Syslog Policy**. Enter the appropriate information and click **OK**
- To edit a syslog policy, select the policy, and then click **Edit**. Edit the appropriate fields and click **OK**.
- To delete a Syslog policy, select the policy, and then click **Delete**.

Syslog Policy Attributes Table

Field	Description
General Tab	
Name	Policy name.
Description	Brief policy description.
Use Emblem Format	Check the check box to use the EMBLEM format for syslog messages. This option appears only on supported devices.
Continue if Host is Down	Check the check box to continue logging if the syslog server is down. This option only appears on supported devices.
Servers Tab	
Add Syslog Server	Click to add a new syslog server.
Syslog Servers table	List of configured syslog servers.
Local Destinations Tab	
Console	• Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: alert, critical, or emergency. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency.

Field	Description
Monitor	• Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency.
File	• Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency. • File Name—Name of the file to which messages are logged. • Size (bytes)—Maximum size, in bytes, that the file can reach before the system begins to overwrite the messages.

Field	Description
Buffer	Buffer options are not available for InterCloud policies. • Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency. • Buffer Size (Bytes)—In bytes, the size of the buffer for syslog messages. • Wrap to Flash—Indicates whether or not the buffer contents are saved to flash memory when the buffer wraps (becomes full). Check the check box to save the contents to flash memory if the buffer wraps. • Max File Size in Flash (KB)—Maximum size, in kilobytes, that can be used by the syslog buffer. This option is enabled if the Wrap to Flash option is enabled. • Min Free Flash Size (KB)—Minimum size, in kilobytes, that is allocated for the syslog buffer. This option is enabled if the Wrap to Flash option is enabled.
Time Stamp	Check the check box for each of the following options that you want to enable for timestamp display: • Enable Timestamp • Include Year • Include Milliseconds • Show Time Zone • Use Local Time Zone

Adding a Syslog Server to a Syslog Policy

This procedure assumes that you have already created a syslog policy for a Prime Network Services Controller profile. For information on creating a syslog policy for a Prime Network Services Controller profile, see Configuring a Syslog Policy, on page 6. For more information on syslog server attributes see the Syslog Server Attributes Table.

Procedure

Step 1 Choose **Administration > System Profile > root > Policies > Syslog >** syslog-policy.

Step 2 In the Servers tab, click **Add Syslog Server**. Enter the appropriate information and click **OK**.

Step 3 In the Servers tab, do one of the following:

- To add a syslog server, click **Add Syslog Server**. Enter the appropriate information and click **OK**
- To edit a syslog server, select the server, and then click **Edit**. Edit the appropriate fields and click **OK**.
- To delete a syslog server, select the server, and then click **Delete**.

Syslog Server Attributes Table

Field	Description
Server Type	One of the following server types: • primary • secondary • tertiary
Hostname/IP Address	Hostname or IP address where the syslog file resides. **Note** If you use a hostname, you must configure a DNS server.

Field	Description
Severity	One of the following severity levels: • emergencies (0) • alerts (1) • critical (2) • errors (3) • warnings (4) • notifications (5) • information (6) • debugging (7)
Forwarding Facility	One of the following forwarding facilities: • auth • authpriv • cron • daemon • ftp • kernel • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7 • lpr • mail • news • syslog • user • uucp

Field	Description
Admin State	Administrative state of the server: disabled or enabled.
Port	Port to use to send data to the syslog server. The default port selection is 514 for UDP. This option is not available for InterCloud policies.
Protocol	Protocol to use: TCP or UDP (default). This option is not available for InterCloud policies.
Use Transport Layer Security	Check the check box to use Transport Layer Security. This option is available only for TCP. This option is not available for InterCloud policies.
Server Interface	Interface to use to access the syslog server.

Modifying the Default System Profile

You can add and modify DNS server, NTP server, and policy information associated to the default system profile. However, you cannot create a new DNS domain or delete the default System profile.

Procedure

Step 1 Choose **Administration > System Profile > root > Profile > default**.

Step 2 In the General tab, update the information as required:

Field	Description
Name	Default profile name (read-only).
Description	Brief profile description.
Time Zone	Available time zones. The default time zone is UTC.

Step 3 In the Policy tab, update the information as required:

Field	Description
DNS Servers	
Add DNS Server	Click to add a new DNS server.
Delete	Deletes the DNS server selected in the DNS Servers table.
Up and down arrows	Changes the priority of the selected DNS server. Prime Network Services Controller uses the DNS servers in the order in which they appear in the table.
DNS Servers table	Identifies the DNS servers configured in the system.
NTP Servers	
Add NTP Server	Click to add a new NTP server.
Delete	Deletes the NTP server selected in the NTP Servers table.
Up and down arrows	Changes the priority of the selected NTP server. Prime Network Services Controller uses the NTP servers in the order in which they appear in the table.
NTP Servers table	Identifies the NTP servers configured in the system.
DNS Domains	
Edit	Edits the DNS domain selected in the DNS Domains table. The default DNS domain cannot be deleted. **Caution** Changing the DNS domain will cause a loss of connectivity that results in an error message, your session closing, and then the display of a new Prime Network Services Controller certificate. This situation occurs when the Prime Network Services Controller hostname, Prime Network Services Controller domain name, or both have changed. If this occurs, reconfigure connectivity with your hypervisor. For more information, see Configuring VM Managers.
DNS Domains	Identifies the default DNS domain name and domain configured in the system.
Other Options	

Field	Description
Syslog	The syslog policies associated with this profile can be selected, added, or edited. Click the Resolved Policy field to review or modify the specified policy.
Fault	The fault policies associated with this profile can be selected, added, or edited. Click the Resolved Policy field to review or modify the specified policy.
Core File	The core file policies associated with this profile can be selected, added, or edited. Click the Resolved Policy field to review or modify the specified policy.
Log File	The log file policies associated with this profile can be selected, added, or edited. Click the Resolved Policy field to review or modify the specified policy.

Step 4 Click **Save**.

Editing a DNS Domain

Caution Changing the DNS domain will cause a loss of connectivity that results in an error message, your session closing, and then the display of a new Prime Network Services Controller certificate. This situation occurs when the Prime Network Services Controller hostname, domain name, or both have changed. If this occurs, reconfigure connectivity with the hypervisor. For more information, see Configuring VM Managers.

Procedure

Step 1 Choose **Administration > System Profile > root > Profile > default**.
Step 2 Click the **Policy** tab.
Step 3 In the DNS Domains table, select the domain that you want to edit, then click **Edit**.
Step 4 In the Edit DNS Domains dialog box, edit the Domain Name field as required, then click **OK**.
Step 5 Click **Save**.

Adding an NTP Server

You can specify a maximum of four NTP servers for the System profile. Use the up and down arrows to arrange the servers from highest to lowest priority, with the highest priority server at the top of the list.

Procedure

Step 1 Choose **Administration > System Profile > root > Profile > default**.

Step 2 In the Policy tab, do one of the following:

- To add an NTP server, click **Add NTP Server**. Enter the appropriate information, click **OK**, and then click **Save**.
- To delete an NTP server, select the server, and then click **Delete**.