Configuring System Profiles

This section includes the following topics:

Profiles

Prime Network Services Controller profiles are configurable.

Prime Network Services Controller provides default profiles. Default profiles are system generated and can be modified, but they cannot be deleted. You can add new policies to a profile, including DNS and NTP policies, or assign existing policies to the a profile.

The Prime Network Services Controller profile includes the DNS domain name that specified at boot configuration. That domain is displayed in the Prime Network Services Controller instance. New DNS domains cannot be created. However, the domain name description can be modified.

Prime Network Services Controller does not support the creation of additional Prime Network Services Controller profiles.

Policies in System Profiles

You can create multiple policies and assign them to the System profile. Policies for the System profile are created and deleted on the **System Profile** tab. Policies can be assigned to the System profile. System profile uses name resolution to resolve policy assignments. For details, see Name Resolution in a Multi-Tenant Environment.

The following policies created under root only, in the Device Policies area, will be 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.

DNS server, NTP server and domain names can be assigned as inline policies. A time zone setting can also be assigned to the profile.

When the system boots up, the following policies already have existing default policies:

- Fault policy
- Log File
- Syslog policy

The default policies cannot be deleted but may be modified.

Configuring Policies

Configuring a Core File Policy

Adding a Core File Policy to the System Profile

Procedure

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

Step 2 In the General tab, click **Add Core File Policy**.

Step 3 In the Add Core File Policy dialog box, complete the following fields, then click **OK**:

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.

Field	Description
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.

Editing a Core File Policy for a System Profile

Procedure

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

Step 2 In the General tab, click the core file policy you want to edit, then click **Edit**.

Step 3 In the Edit dialog box, modify the following fields as appropriate, then click **OK**:

Field	Description
Name	Name of the core file policy (read-only).
Description	Brief policy description.
Admin State	Administrative status of the policy: enabled or disabled.
Hostname	Hostname or IP address. **Note** If you use a hostname, you must configure a DNS server.
Port	Port number to use when exporting the core dump file. This field is read-only for InterCloud policies.
Protocol	Protocol used to export the core dump file (tftp only).
Path	Path to use when storing the core dump file on the remote system. The default path is /tftpboot. To specify a subfolder under tftpboot, use the format /tftpboot/*folder* where *folder* is the subfolder.

Deleting a Core File Policy from the System Profile

Procedure

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

Step 2 In the General tab, click the core file policy you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Configuring a Fault Policy

Adding a Fault Policy to the System Profile

When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

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

Step 2 In the General tab, click **Add Fault Policy**.

Step 3 In the Add Fault Policy dialog box, provide the information as described in the following table, then click **OK**:

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.

Field	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.
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.

Editing a Fault Policy for a System Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

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

Step 2 In the General tab, select the fault policy you want to edit, then click **Edit**.

Step 3 In the Edit Fault Policy dialog box, modify the fields as needed by using the information in the following table, then click **OK**.

Field	Description
Name	Policy name (read-only).
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 recurs during the flapping interval, the fault returns to the active state. If the condition does not recur during the flapping interval, the fault is cleared. The next action depends on the setting in the Clear Faults Retention Action field. The default flapping interval is ten seconds.
Clear Faults Retention Action	Available fault retention actions: • retain—The system retains fault messages. • delete—The system deletes fault messages when they are marked as cleared.
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.

Deleting a Fault Policy from the System Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

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

Step 2 In the General tab, select the fault policy you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Configuring a Logging Policy

Adding a Logging Policy to the System Profile

When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

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

Step 2 In the General tab, click **Add Logging Policy**.

Step 3 In the Add Logging Policy dialog box, complete the following fields:

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.
Description	Brief policy description.

Field	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.

Step 4 Click **OK**.

Editing a Logging Policy for System Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

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

Step 2 In General tab, select the logging policy that you want to edit, then click **Edit**.

Step 3 In the Edit Log File Policy dialog box, modify the information as required by using the information in the following table, then click **OK**.

Field	Description
Name	Logging policy name (read-only).
Description	Brief policy description.
Log Level	One of the following logging 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.

Deleting a Logging Policy from the System Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

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

Step 2 In the General tab, select the logging policy you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Configuring a Syslog Policy

Adding a Syslog Policy to the System Profile

When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

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.

Procedure

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

Step 2 In the General tab, click **Add Syslog Policy**.

Step 3 In the Add Syslog Policy dialog box, provide the information as described in the following table, then click **OK**.

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 is supported for ASA 1000Vs. It is not supported for VSGs or InterCloud policies.
Continue if Host is Down	Check the check box to continue logging if the syslog server is down. This option is supported for ASA 1000Vs. It is not supported for VSGs or InterCloud policies.
Servers Tab	

Field	Description
Add Syslog Server	Click to add a new syslog server.
Syslog Servers table	List of configured syslog servers.
Local Destinations Tab	
Console area	• 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.
Monitor area	• 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.

Field	Description
File area	- 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 area	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.

Editing a Syslog Policy for the System Profile

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.

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

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

Step 2 In the General tab, select the syslog policy you want to edit, then click **Edit**.

Step 3 In the Edit Syslog Policy dialog box, update the information as required by using the information in the following table, then click **OK**.

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 is supported for ASA 1000Vs. It is not supported for VSGs or InterCloud policies.
Continue if Host is Down	Check the check box to continue logging if the syslog server is down. This option is supported for ASA 1000Vs. It is not supported for VSGs or InterCloud policies.
Servers Tab	
Add Syslog Server	Click to add a new syslog server.
Syslog Servers table	List of configured syslog servers.
Local Destinations Tab	
Console area	• 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 area	• 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 area	• 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 area	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.

Deleting a Syslog Policy from a System Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

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

Step 2 In the General tab, click the syslog policy you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Adding a Syslog Server to the System Profile

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 Adding a Syslog Policy to the System Profile, on page 10.

Procedure

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

Step 2 In the Servers tab, click **Add Syslog Server**.

Step 3 In the Add Syslog Server dialog box, provide the information as described in the following table, then click **OK**:

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.
Severity	One of the following severity levels: • emergencies (0) • alerts (1) • critical (2) • errors (3) • warnings (4) • notifications (5) • information (6) • debugging (7)

Field	Description
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
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.

Field	Description
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.

Editing a Syslog Server for the System Profile

Procedure

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

Step 2 In the General tab, select the syslog policy with the syslog server that you want to edit, then click **Edit**.

Step 3 In the Edit Syslog Policy dialog box, click the **Servers** tab.

Step 4 Select the syslog server that you want to edit, then click **Edit**.

Step 5 In the Edit Syslog Server dialog box, edit the information as required, using the information in the following table, and then click **OK**:

Field	Description
Server Type	One of the following server types: primary, secondary, or 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: enabled or disabled.
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. It is not available for InterCloud policies.
Server Interface	Interface to use to access the syslog server. If the syslog server is for a device instead of the System profile, keep the following in mind: • This option applies to ASA 1000V only. Enter the data interface name specify in the edge firewall. • Use the device CLI to configure a route through the management interface. • This option is not available for InterCloud policies.

Deleting a Syslog Server from a System Profile

Procedure

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

Step 2 In the General tab, select the syslog policy with the server you want to delete, then click **Edit**.

Step 3 In the Edit Syslog Policy dialog box, click the **Servers** tab.

Step 4 In the Servers table, select the syslog server you want to delete, then click **Delete**.

Step 5 When prompted, confirm the deletion.

Step 6 Click **OK** or **Apply** to apply the change to the syslog policy.

Configuring the Default Profile

Editing the System Default 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.

Field	Description
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. The VM Manager Extension file must be exported again and installed on vCenter. To continue, accept the Prime Network Services Controller certificate and log into Prime Network Services Controller again.
DNS Domains	Identifies the default DNS domain name and domain configured in the system.
Other Options	
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.

Field	Description
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**.

Configuring a DNS Server

Adding a DNS Server

You an specify a maximum of four DNS 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 Click the **Policy** tab.

Step 3 In the DNS Servers area, click **Add DNS Server**.

Step 4 In the Add DNS Server dialog box, enter the DNS server IP address, then click **OK**.

Step 5 Click **Save**.

Deleting a DNS Server

Procedure

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

Step 2 Click the **Policy** tab.

Step 3 In the **DNS Servers** area, select the DNS server you want to delete, then click **Delete**.

Step 4 When prompted, confirm the deletion.

Step 5 Click **Save** to save your changes.

Configuring an NTP Server

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, click **Add NTP Server**.

Step 3 In the Add NTP server dialog box, enter the hostname or IP address of the NTP server, then click **OK**.

Step 4 Click **Save**.

Deleting an NTP Server

Procedure

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

Step 2 Click the **Policy** tab.

Step 3 In the NTP Servers area, click the server that you want to delete, then click **Delete**.

Step 4 When prompted, confirm the deletion.

Step 5 Click **Save**.

Configuring a DNS Domain

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. Prime Network Services Controller domain name, or both have changed. The VM Manager Extension file must be exported again and installed on vCenter. To continue, accept the Prime Network Services Controller certificate and log into Prime Network Services Controller again.

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**.