Internal SNMP Trap Generation

When properly configured, Prime Infrastructure will send SNMP traps to notification receivers, to notify them on the following events, occurring within the Prime Infrastructure system itself:

- Any crash or failure of an internal software process on the Prime Infrastructure server.
- High Availability (HA) state changes, including Registration, Failover, and Failback.
- High CPU, memory or disk utilization.
- CPU, disk, fan, or Power Supply Unit (PSU) failures.
- Backup failure, certification expiry and licenses violations.

This appendix and the following related topics provide reference information on these internal SNMP traps and how to use them to manage Prime Infrastructure.

Related Topics

- About Internal Trap Generation
- Prime Infrastructure SNMP Trap Types
- Generic SNMP Trap Format
- Generic SNMP Trap Format
- Prime Infrastructure SNMP Trap Reference
- Working With Prime Infrastructure Traps

About Internal Trap Generation

You can edit the severity associated with each of these internal SNMP traps. You can also change the threshold limits on CPU, memory and disk utilization traps (these SNMP traps are sent when the system hardware exceeds the configured thresholds).

For other events (such as CPU, disk, fan, and PSU failures, or HA state changes), an SNMP trap is sent as soon as the failure or HA state-change is detected.

SNMP traps are generated based on customized threshold and severities for the following:

- Server Process Failures
- High Availability Operations
- CPU Utilization
- Memory Utilization

- Disk Utilization
- Disk Failure
- Fan Failure
- PSU Failure
- Backup Failure
- Certificate Expiry

Prime Infrastructure does not send SNMPv2 Inform or SNMPv3 notifications.

Prime Infrastructure SNMP Trap Types

The following table lists the SNMP traps that Prime Infrastructure generates for its own functions. The listing is by trap type. The table describes the circumstances under which each trap is generated as well as suggested operational responses (where applicable).

Table A-1 Prime Infrastructure SNMP Trap Types

Trap Type	Trap	Description
Appliance Process Failure	FTP, MATLAB, TFTP	Whenever the FTP, MATLAB, or TFTP process on Prime Infrastructure server fails, the server will generate a failure trap and the server's instance of Health Monitor will try to restart the process automatically. If Health Monitor cannot restart it after 3 tries, the HA server will send another failure trap.
Appliance Process Failure	NMS	Whenever the NMS process on a server starts or fails, the Prime Infrastructure server's Health Monitor thread will generate a corresponding trap. To stop or restart the process, connect to the server via CLI and log in as admin. Then execute the *nms stop* or *nms start* command, as appropriate.
HA Operations	Registration Trigger	Prime Infrastructure generates this trap whenever the primary server initiates HA registration (whether registration fails or succeeds).Once HA registration is triggered, the primary server generates the trap, indicating the start of the operation.
HA Operations	Registration Success	When HA registration is successful, the primary server generates this trap, indicating success.
HA Operations	Registration Failure	When HA registration fails for any reason, the primary or secondary server on which the failure occurred, generates a trap indicating the failure. The trap contains details about the failure. For assistance, contact the Cisco Technical Assistance Center (TAC).
HA Operations	Failover Trigger	This trap is generated whenever the Prime Infrastructure primary server fails and, as part of a failover, the secondary server tries to become active (whether failover fails or succeeds, and whether the secondary server comes up or fails to do so). If the HA configuration (set during registration) has a Manual failover type, users must trigger the failover. Otherwise, the Health Monitor will trigger failover to the secondary server automatically. One trap will be generated to indicate that the failover was triggered. Because the trap is sent before the failover completes, it will not be logged on the secondary server.

Table A-1 Prime Infrastructure SNMP Trap Types (continued)

Trap Type	Trap	Description
HA Operations	Failover Success	When the triggered failover operation is successful, the secondary server generates a trap indicating success. Users can view the trap in the secondary server's alarm browser.
HA Operations	Failover Failure	When the triggered failover operation fails, a trap will be generated indicating the failure. Users can view the trap in the hm-#-#.log (see Troubleshooting Prime Infrastructure SNMP Traps). The trap contains details about the failure. For assistance, contact Cisco TAC. As with other failure traps, alarms and a “clear” trap are sent if the failure corrects itself.
HA Operations	Failback Trigger	This trap is generated whenever a failback to the primary server is triggered on the secondary server (whether or not the failback is successful). Once the primary server is restored, a user must trigger a failback from the secondary server to the primary server using the **Failback** button on the secondary server Health Monitor web page (there is no automatic Failback option). Once triggered, the secondary server generates the trap indicating the start of the operation.
HA Operations	Failback Success	When the triggered failback operation is successful, the secondary server generates a trap indicating success. Failback success sets the primary server to the ‘Active’ state and the secondary server to the ‘Sync’ state.
HA Operations	Failback Failure	When the triggered failback operation fails, a trap will be generated indicating this failure. Since the failure can occur on either server, the server on which it occurred will generate the trap. Users can view the trap in the hm-#-#.log and on the northbound management server. A failback failure triggers an automatic rollback, in which the secondary server tries to return to its previous ‘Active’ state. Failure of this operation will cause the secondary server to generate an additional trap indicating rollback failure. The failure traps contain details about the failures. For assistance, contact Cisco TAC. As with other failure traps, alarms and a “clear” trap are sent if the failure corrects itself.
Hardware Traps	CPU Utilization	Traps will be sent only when the usage exceeds the preset threshold value for CPU utilization. To view these traps, check the jobs and active sessions for the server that generated the trap.
Hardware Traps	Disk Utilization	Traps will be sent only when the disk usage exceeds the set threshold limit for Disk utilization. To respond, try to free up disk space under the /opt and /localdisk partitions. Do not delete folders under /opt/CSCOlumos without guidance from Cisco TAC.
Hardware Traps	Memory Utilization	Traps will be sent to the SNMP trap receiver, only when memory usage exceeds the set threshold limit for memory utilization.
Hardware Traps	Disk Failure	Traps will be sent to the SNMP trap receiver when disk failure is detected. Contact your local system administrator for corrective action. As with other failure traps, alarms and a “clear” trap are sent if the failure corrects itself.
Hardware Traps	Fan Failure	Traps will be sent to the SNMP trap receiver when fan failure is detected. The bad or missing fan will be identified in the trap or alarm message. Contact your local system administrator for corrective action. As with other failure traps, alarms and a “clear” trap are sent if the failure corrects itself.

Table A-1 Prime Infrastructure SNMP Trap Types (continued)

Trap Type	Trap	Description
Hardware Traps	PSU Failure	Traps will be sent to the SNMP trap receiver when PSU failure is detected. The problematic power supply will be identified in the trap or alarm message. Contact your local system administrator for corrective action. As with other failure traps, alarms and a “clear” trap are sent if the failure corrects itself.
Threshold Traps	Backup Failure	Traps will be sent to the SNMP trap receiver when failure of the daily background task of Prime Infrastructure server backup is detected. The background task runs everyday and takes a backup of the server at the scheduled time. If the backup fails due to insufficient disk space, the event will be processed. If the backup is taken successfully, the alarm will be cleared.
Threshold Traps	Backup Threshold	Informs users when Prime Infrastructure scheduled daily backup has not been taken for a threshold number of days. The default threshold is seven days. If no backup has been taken for seven days, users are notified by this event.
Threshold Traps	Certificate Expiry	Traps will be sent to the SNMP trap receiver when the certificate is about to expire. A critical trap is sent when the certificate is set to expire in 15 days and a major trap is sent when the certificate expiry is in 60 days.
System Traps	Lifecycle	Lifecycle license is used to manage devices. Alarm is generated when the license usage exceeds the configured threshold percentage. By default, traps will be sent when the usage exceeds 80%. However, this can be customized.
System Traps	Data Center	Data Center license is used to manage Data Center devices. Alarm is generated when the license usage exceeds the configured threshold percentage. By default, traps will be sent when the usage exceeds 80%. However, this can be customized.
System Traps	Assurance	Assurance License is used to display the devices that pump NetFlow to Prime Infrastructure . Alarm is generated when the license usage exceeds the configured threshold percentage. By default, traps will be sent when the usage exceeds 80%. However, this can be customized.
System Traps	Collector	Collector License is used to display the volume of NetFlow pumped to Prime Infrastructure . Alarm is generated when the license usage exceeds the configured threshold percentage. By default, traps will be sent when the usage exceeds 80%. However, this can be customized.
System Traps	Lifecycle License	Traps will be sent when the expiry period of the License goes below the threshold limit. By default, traps will be sent when the limit is 30 days. However, you can customize the limit between 1-99 days. This event is considered only when you use Evaluation License.
System Traps	Data Center License	Traps will be sent when the expiry period of the License goes below the threshold limit. By default, traps will be sent when the limit is 30 days. However, you can customize the limit between 1-99 days. This event is considered only when you use Evaluation License.

Table A-1 Prime Infrastructure SNMP Trap Types (continued)

Trap Type	Trap	Description
System Traps	Assurance License	Traps will be sent when the expiry period of the License goes below the threshold limit. By default, traps will be sent when the limit is 30 days. However, you can customize the limit between 1-99 days. This event is considered only when you use Evaluation License.
System Traps	Collector License	Traps will be sent when the expiry period of the License goes below the threshold limit. By default, traps will be sent when the limit is 30 days. However, you can customize the limit between 1-99 days. This event is considered only when you use Evaluation License.

Generic SNMP Trap Format

The following shows the syntax of SNMP trap notifications for Prime Infrastructure:

Component: Component Name, **Server**: Primary, Secondary or Standalone, **Type**: Process, Sync, Activity, etc., **Service**: Service Name, **When**: Phase in the Prime Infrastructure Lifecycle, **State**: HA and HM state of the server, **Result**: Warning, Failure, Success, Information, Exception, **MSG**: Free-form text of the message for a given SNMP Trap

Table A-2 describes possible values for each of the generic trap format attributes.

Table A-2 Values for Generic SNMP Trap Format Attributes

Attribute	Value
Component	Health Monitor or High Availability
Server	From which server (Primary, Secondary or Standalone) was this trap sent?
Type	Which type of action (Process, Sync, Activity, etc.) resulted in this trap?
Service	Which Prime Infrastructure service reported this issue? The possible values include Registration, Failover, Failback, NMS, NCS, Health Monitor, All, Prime Infrastructure, Database, Disk Space, and so on.
When	At what point in the Prime Infrastructure server's life cycle (Startup, Shutdown, etc.) did this happen?
State	What is the server state (Standalone, Failover, Failback, Registration, etc.)?
Result	For which condition is this SNMP trap being reported?
MSG	Freeform text providing more details specific to each SNMP trap.

Prime Infrastructure SNMP Trap Reference

The tables below provide details for each class of SNMP trap notification generated in Prime Infrastructure. The mapped OID for the WCS northbound notification MIB is 1.3.6.1.4.1.9.9.712.1.1.2.1.12. This OID is referenced by Prime Infrastructure's software- and hardware-related traps.The trap OID for the northbound MIB will always be 1.3.6.1.4.1.9.9.712.0.1. For details, consult the listing for CISCO-WIRELESS-NOTIFICATION-MIB.

Table A-3 Appliance Process Failure

Purpose	Informs users that a specific Prime Infrastructure server service is down and that the Health Monitor is attempting to restart it.
When Sent	The trap is sent when Health Monitor tries to restart the process.
OID	1.3.6.1.4.1.9.9.712.1.1.2.1.12
Example	`Component: Health Monitor, Server: Primary, Type: Process, Service: NCS, When: Startup, State: Stand Alone, Result: Warning, MSG: FTP service is down and an attempt will be made to automatically restart the service`
MSG Content	`PI servername: serviceName service is down; an attempt will be made to automatically restart the service.`
Value Type, Range and Constraints	The *servername* parameter in the MSG attribute will take the value of the Prime Infrastructure server's host name. This parameter can take one of the following values: NMS Server, FTP, TFTP or MATLAB.

Table A-4 Failback

Purpose	Informs users that a failback from the secondary server to the primary server has been initiated.
When Sent	This trap is sent when a failback is initiated from the secondary server to the primary server, irrespective of whether the failback operation fails or succeeds.
OID	1.3.6.1.4.1.9.9.712.1.1.2.1.12
Example	`Component: High Availability, Server: Secondary, Type: Process, Service: Database, When: Failback, State: Primary Failback, Result: Failure, MSG: Error in Failback: Failed to recover the primary database using Duplicate DB`

Table A-5 Failover

Purpose	Informs users when the secondary server comes up.
When Sent	When the primary server is down and, as part of failover, the secondary server comes up, traps are generated, irrespective of whether the failover operation fails or succeeds.
OID	1.3.6.1.4.1.9.9.712.1.1.2.1.12
Example	`Component: High Availability, Server: Secondary, Type: Process, Service: Failover, When: Failover, State: Secondary Synching, Result: Success, MSG: Completed failover from primaryAddressInfo to secondaryAddressInfo.`
MSG Content	The primaryAddressInfo and secondaryAddressInfo in the MSG attribute will take the IP address or host name of the servers.

Table A-6 CPU Utilization

Purpose	Informs users that CPU utilization has crossed the set threshold limit.
When Sent	After the CPU utilization crosses the set threshold, the trap is generated on the next polling cycle. The system poller job runs every 5 minutes. A trap is also generated when the threshold limit is changed on the Prime Infrastructure Event Configuration web page.
OID	.1.3.6.1.4.1.9.9.712.0.1.
Example	`CPU Utilization is at 85% and has violated threshold limit of 80%.`
Value Type, Range and Constraints	All percentage ranges are from 1 to 99. Do not enter the percentage character ("%") when specifying a threshold limit.
Wire Format	`[OctetString] applicationSpecificAlarmID=Appliance_CPU, lastModifiedTimestamp=12 Jun 2014 11:12:32 UTC, alarmCreationTime=12 Jun 2014 11:12:32 UTC, ownerID=, eventCount=1, mayBeAutoCleared=false, instanceId=8178170, severity=4, eventType=APPLIANCE_CPU_VIOLATED_THRESHOLD, previousSeverity=CLEARED, category=System(17), transientNameValue={}, source=CPU, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=Component: Appliance, Server: primary, Type: Hardware, Message: CPU Utilization is at 3% and has violated threshold limit of 1%, isAcknowledged=false, displayName=NMS:192.168.115.141`
Constraints and Caveats	Traps are not generated if the issue is resolved before the next polling cycle.

Table A-7 Disk Utilization

Purpose	Informs users that disk utilization has crossed the set threshold limit.
When Sent	After the disk utilization crosses the set threshold, the trap is generated on the next polling cycle. The system poller job runs every 5 minutes. A trap is also generated when the threshold limit is changed on the Prime Infrastructure Event Configuration web page.
OID	.1.3.6.1.4.1.9.9.712.0.1

Examples	`PI opt disk volume utilization is at 85% and has violated threshold limit of 0%`
	`PI opt disk volume is within the recommended disk usage range, less than 80% used`
	`PI local disk volume utilization is at 85% and has violated threshold limit of 80%`
	`PI local disk volume is within the recommended disk usage range, less than 80% used`

Value Type, Range and Constraints	All percentage ranges are from 1 to 99. Do not enter the percentage character ("%") when specifying a threshold limit.
Wire Format	`[OctetString] applicationSpecificAlarmID=LocaldiskDiskSpace,reportingEntityAddress=10.77.240.246,lastModifiedTimestamp=Sun Mar 23 08:44:06 UTC 2014, alarmCreationTime=2014-03-14 13:29:31.069, eventCount=1, mayBeAutoCleared=false, instanceId=483484, severity=1, eventType=NCS_LOW_DISK_SPACE, authEntityId=93093, previousSeverity=MAJOR, category=System(17), transientNameValue={}, source=10.77.240.246, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=PI localdisk volume is within the recommended disk usage range, less than 70% used., isAcknowledged=false, authEntityClass=983576643, displayName=NCS 10.77.240.246`
Constraints and Caveats	Traps are not generated if the issue is resolved before the next polling cycle.

Table A-8 Memory Utilization

Purpose	Informs users that memory utilization has crossed the set threshold limit.
When Sent	After the memory utilization crosses the set threshold, the trap is generated on the next polling cycle. The system poller job runs every 5 minutes. A trap is also generated when the threshold limit is changed on the Prime Infrastructure Event Configuration web page.
OID	.1.3.6.1.4.1.9.9.712.0.1.
Examples	`Memory Utilization is at 85% and has violated threshold limit of 80%.`
Value Type, Range and Constraints	All percentage ranges are from 1 to 99. Do not enter the percentage character ("%") when specifying a threshold limit.
Wire Format	`[OctetString] applicationSpecificAlarmID=Appliance_MEMORY, lastModifiedTimestamp=12 Jun 2014 11:12:32 UTC, alarmCreationTime=12 Jun 2014 11:12:32 UTC, ownerID=, eventCount=1, mayBeAutoCleared=false, instanceId=8178171, severity=4, eventType=APPLIANCE_MEM_VIOLATED_THRESHOLD, previousSeverity=CLEARED, category=System(17), transientNameValue={}, source=MEMORY, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=Component: Appliance, Server: primary, Type: Hardware, Message: MEMORY Utilization is at 38% and has violated threshold limit of 1%, isAcknowledged=false, displayName=NMS:192.168.115.141`
Constraints and Caveats	Traps are not generated if the issue is resolved before the next polling cycle.

Table A-9 Disk Failure

Purpose	Informs users that a drive is missing or bad.
When Sent	Once a disk drive issue is detected, a trap will be generated on the next polling cycle. The system poller job runs every 5 minutes.
OID	.1.3.6.1.4.1.9.9.712.0.1
Example	`Component: Appliance, Server: Standalone, Type: Hardware, Message: A problem was detected in the RAID device. A rebuild is in progress. Device at enclosure 252 slot ZERO is bad or missing. Drive0 is missing or bad.`
Constraints and Caveats	Traps are not generated if the issue is resolved before the next polling cycle. If the drive is unplugged at the time of system restart, the trap is generated.

Table A-10 Fan Failure

Purpose	Informs users when a fan fails.
When Sent	When a fan fails, a trap is generated on the next polling cycle. The system poller job runs every 5 minutes.
OID	.1.3.6.1.4.1.9.9.712.0.1

Table A-10 Fan Failure (continued)

Example	`Fan is either bad or missing.`
Wire Format	`[OctetString] applicationSpecificAlarmID=Appliance_Fan1, lastModifiedTimestamp=Sun Apr 13 15:24:11 IST 2014, alarmCreationTime=Sun Apr 13 15:24:11 IST 2014, ownerID=, eventCount=1, mayBeAutoCleared=false, instanceId=2875873, severity=4, eventType=APPLIANCE_FAN_BAD_OR_MISSING, previousSeverity=CLEARED, category=System(17), transientNameValue={}, source=Fan1, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=Fan is either bad or missing, isAcknowledged=false, displayName=NMS: 10.77.240.246`
Constraints and Caveats	Traps are not generated if the issue is resolved before the next polling cycle, or the fan is unplugged at the time of system restart.

Table A-11 PSU Failure

Purpose	Informs users that a power supply unit is unplugged.
When Sent	When a power supply is unplugged, a trap is generated on the next polling cycle. The system poller job runs every 5 minutes.
OID	.1.3.6.1.4.1.9.9.712.0.1
Example	`Component: Appliance, Server: Standalone, Type: Hardware, Message: Power supply: PSx is either bad or missing.`
Wire Format	`[OctetString] applicationSpecificAlarmID=Appliance_PS1, lastModifiedTimestamp=19 Aug 2015 01:41:26 UTC, alarmCreationTime=19 Aug 2015 01:41:26 UTC, ownerID=, eventCount=1, mayBeAutoCleared=false, instanceId=1424089, severity=4, eventType=APPLIANCE_POWER_SUPPLY_BAD_OR_MISSING, previousSeverity=CLEARED, category=System(17), transientNameValue={}, source=x.x.x.x, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=Component: Appliance, Server: Standalone, Type: Hardware, Message: Power supply: PSx is either bad or missing, isAcknowledged=false, displayName=NMS:x.x.x.x`
Constraints and Caveats	If the PSU is unplugged, a Power Supply alarm will be seen in Prime Infrastructure and a trap will be sent. If the PSU is unplugged at the time of system shutdown, and Prime Infrastructure is not up till restart, an alarm will not be generated.

Table A-12 Identify Services Engine down

Purpose	Informs users when an ISE is unreachable.
When Sent	When an ISE is down or unreachable, the trap is generated via polling. **Note** This is a system generated trap. Hence it does not have any corresponding OID.
Example	`Identity services engine` *`ISEIPAddress`* `is unreachable.`

Table A-13 License violation

Purpose	Informs users when the number of devices Prime Infrastructure is actually managing exceeds the number of devices it is licensed to manage.
When Sent	At 2:10AM, on the day following the completion of the job that added the extra devices to Prime Infrastructure inventory **Note** This is a system generated trap. Hence it does not have any corresponding OID.
Example	`Number of managed devices N is greater than licensed devices N. Please purchase and install a license that will cover the number of managed devices, or remove unused devices from the system.`

Table A-14 Prime Infrastructure does not have enough disk space for backup

Purpose	Informs users when Prime Infrastructure does not have sufficient space in the specified directory to perform a backup.
When Sent	Whenever Prime Infrastructure runs a server backup job and the backup repository specified (or "defaultrepo") is 100 percent full. The trap is generated after the job completes. **Note** This is a system generated trap. Hence it does not have any corresponding OID.
Example	`Prime Infrastructure with address localIPAddress does not have sufficient disk space in directory directoryName for backup. Space needed: Needed GB, space available Free GB.`

Table A-15 Prime Infrastructure email failure

Purpose	Informs users that an attempt to send an email notification has failed.
When Sent	This trap is generated by polling when Prime Infrastructure attempts to send an email notification to an invalid user, or email notification is enabled without specifying the email server in Prime Infrastructure. **Note** This is a system generated trap. Hence it does not have any corresponding OID.
Example	`Prime Infrastructure with address localIPAddress failed to send email. This may be due to possible SMTP misconfiguration or network issues.`

Table A-16 Northbound OSS server unreachable

Purpose	Informs users that a northbound notification server is unreachable.
When Sent	This trap is generated by polling when a destination northbound notification server is down or unreachable.
OID	.1.3.6.1.4.1.9.9.712.0.1
Example	`Northbound notification server OSSIPAddress is unreachable. NCS alarms will not be processed for this server until it is reachable.`

Working With Prime Infrastructure Traps

The following sections explain how to configure and use Prime Infrastructure trap notifications.

Related Topics

- Configuring Notifications
- Port Used To Send Traps
- Configuring Email Notifications for SNMP Traps
- Viewing Events and Alarms for SNMP Traps
- Filtering Events and Alarms for SNMP Traps
- Purging Alarms for SNMP Traps
- Troubleshooting Prime Infrastructure SNMP Traps

Configuring Notifications

For Prime Infrastructure to send northbound SNMP trap notifications, you must configure the correct settings on both the Prime Infrastructure Event Notification and Notification Receivers pages. Once configured, traps will be generated based on the values associated with the Threshold and Severity for the following SNMP Events:

- Appliance Process Failure
- HA Operations
- CPU, disk and memory utilization
- Disk, fan and PSU Failure
- Backup failure, certification expiry and licenses violations

You can edit the threshold and severity associated with each event, and enable or disable trap generation for the associated event.

Step 1 Log in to Prime Infrastructure using a user ID with root domain privileges.

Step 2 Select **Administration > Settings > System Settings > Alarms and Events > System Event configuration**.

Step 3 For each SNMP event you want to configure:

a. Click on the row for that event.

b. Set the **Event Severity** level to Critical, Major, or Minor, as needed.

c. For the CPU, disk, memory utilization, life cycle, data center, assurance, and collector traps: Enter the **Threshold** percentage (from 1-99). These events will send the associated SNMP traps when the utilization exceeds the threshold limit. You cannot set thresholds for events for which the threshold setting is shown as NA. These events send traps whenever the associated failure is detected.

d. For backup threshold, certificate expiry, certificate expiry (critical), lifecycle license, data center license, assurance license, and collector license trap: Enter the **Threshold** in days (from x-y, where x is the minimum value and y is the maximum value in days).

e. Set the **Event Status** to Enabled or Disabled. If set to Enabled, the corresponding trap will be generated for this event.

f. For the CPU, disk, memory utilization, enter the **Create and Clear Alarm Iteration** value. The default value is two. The first polling after setting the iteration value will take two times the iteration value entered in minutes. All the future polling will take 20 minutes only.

   The default polling time is 20 minutes.

Step 4 When you are finished, click **Save** to save your changes.

Related Topics

- Configuring Notification Receivers

Configuring Notification Receivers

Once you have enabled trap notifications and customized their severities and thresholds, you must configure one or more Notification Receivers to receive the traps.

When you add a Notification Receiver, remember to select the **System** checkbox as one of the Criteria and, set the Severity to the highest severity set under the severity level configured for each trap on the Event Notifications page.

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

Step 2 Select **Administration > Settings > System Settings > Alarms and Events > Notification Receivers.**

Step 3 From the **Select a command** drop-down list, choose **Add Notification Receiver**, then click **Go**.

Step 4 Complete at least the following fields:

a. **IP Address or DNS name**: Enter the IPv4 or IPv6 address of the server or DNS name of the server on which the receiver will run.

b. **Server Name**: Enter the host name of the server on which the receiver will run.

c. Under **Criteria - Category**, select at least the **System** checkbox.

d. Under **Criteria - Severity**, select the highest **Severity Level** that you set when you configured the trap notifications themselves.

   For example: If you selected “Critical” as the **Event Severity** for a PSU failure, select “Critical” as the value in this field.

   Alternatively: Select **All** to receive all traps, regardless of severity.

Step 5 When you are finished, click Save.

Related Topics

- Configuring Notifications
- Port Used To Send Traps
- Configuring Email Notifications for SNMP Traps
- Viewing Events and Alarms for SNMP Traps
- Filtering Events and Alarms for SNMP Traps
- Purging Alarms for SNMP Traps
- Troubleshooting Prime Infrastructure SNMP Traps

Port Used To Send Traps

Prime Infrastructure sends traps to notification receivers on port 162. This port cannot be customized at present. The northbound management system has to register itself through the Notification Receiver web page (see Configuring Notification Receivers).

Configuring Email Notifications for SNMP Traps

You can configure Prime Infrastructure to send email notification for alarms and events generated in response to SNMP traps. All of these alarms and events are considered part of the System event category. You can also customize the severity level for which such notifications will be sent.

Note that, for these email notifications to be sent, the Prime Infrastructure administrator must configure at least a primary SMTP email server.

Step 1 Log in to Prime Infrastructure.

Step 2 Select **Monitor > Monitoring Tools > Alarms and Events**.

Step 3 Click **Email Notification** tab. Prime Infrastructure displays the first Email Notification Settings page.

Step 4 In the **Alarm Category** column, click on the **System** category's name. Prime Infrastructure displays a second Email Notification Settings page.

Step 5 Under **Send email for the following severity levels**, select all of the severity levels for which you want Prime Infrastructure to send email notifications.

Step 6 In **To**, enter the email address to which you want Prime Infrastructure to send email notifications. If you have multiple email addresses, enter them as a comma-separated list.

Step 7 Click **Save**. Prime Infrastructure displays the first Email Notification Settings page.

Step 8 In the **Enable** column, make sure System is selected, then click **Save**.

Related Topics

- Configuring Email Server Settings

Configuring Email Server Settings

To enable Prime Infrastructure to send email notifications, the system administrator must configure a primary SMTP email server (and, preferably, a secondary email server).

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

Step 2 Select **Administration > Settings > System Settings > Mail and Notification > Mail Server Configuration**.

Step 3 Under **Primary SMTP Server**, complete the **Hostname/IP**, **User Name**, **Password** and **Confirm Password** fields as appropriate for the email server you want Prime Infrastructure to use. Enter the IP address of the physical server. You cannot enter a virtual IP address in the Hostname/IP field, and the IP address cannot be behind a load balancer.

Step 4 (Optional) Complete the same fields under **Secondary SMTP Server**.

Step 5 Under **Sender and Receivers**, enter a legitimate email address for the Prime Infrastructure server.

Step 6 When you are finished, click **Save**.

Related Topics

- Viewing Events and Alarms for SNMP Traps
- Filtering Events and Alarms for SNMP Traps
- Purging Alarms for SNMP Traps
- Troubleshooting Prime Infrastructure SNMP Traps
- Configuring Notifications
- Port Used To Send Traps
- Configuring Email Notifications for SNMP Traps

Viewing Events and Alarms for SNMP Traps

Events and Alarms for all of Prime Infrastructure's internal SNMP traps fall under the System category. You can view them in the Prime Infrastructure Alarms and Events dashboard.

Step 1 Log in to Prime Infrastructure.

Step 2 Select **Monitor** > **Monitoring Tools** > **Alarms and Events**.

Filtering Events and Alarms for SNMP Traps

You can use the Prime Infrastructure Filter feature to narrow the display of alarms to just those in the System category, or use a combination of criteria and operators to focus the list on very specific alarms. The following sections explain how to do this.

Related Topics

- Filtering for SNMP Traps Using Quick Filters
- Filtering for SNMP Traps Using Advanced Filters

Filtering for SNMP Traps Using Quick Filters

Prime Infrastructure's Quick Filters allow you to quickly focus on the data inside a table by applying a filter for a specific table column or columns.

Step 1 Log in to Prime Infrastructure.

Step 2 Select **Monitor** > **Monitoring Tools** > **Alarms and Events**.

Step 3 From the **Show** drop-down list, select **Quick Filter**. Prime Infrastructure displays a table header listing fields on which you can perform a quick filter, including **Severity**, **Message**, and **Category**.

Step 4 In the **Category** field, enter **System**. Prime Infrastructure displays only System alarms.

Step 5 To clear the Quick Filter, click the funnel icon shown next to the **Show** box.

Filtering for SNMP Traps Using Advanced Filters

Prime Infrastructure's Advanced Filter allows you to narrow down the data in a table by applying a filter combining multiple types of data with logical operators (such as “Does not contain”, “Does not equal”, “Ends with”, and so on). For example, you can choose to filter the table of alarms based on the Category, then further reduce the data by filtering on Severity (as shown in the steps below). You can also save an Advanced Filter for later re-use.

Step 1 Log in to Prime Infrastructure.

Step 2 Select **Monitor > Monitoring Tools > Alarms and Events**.

Step 3 From the **Show** drop-down list, select **Advanced Filter**. Prime Infrastructure displays a table header showing criteria for the first rule in the filter.

Step 4 Complete the first rule as follows:

a. In the first field, select **Category** from the drop-down list.

b. In the second field, select **Contains** from the drop-down list.

c. In the third rule field, enter **System**.

d. Click **Go**. Prime Infrastructure displays only System alarms.

Step 5 Click the plus sign icon to add another rule, then complete the second rule as follows:

a. In the first field, select **Severity** from the drop down list

b. In the second field, select **equals (=)** from the drop-down list.

c. In the third rule field, select **Major** from the drop-down list.

d. Click **Go**. Prime Infrastructure displays only System alarms with Major Severity.

Repeat this step as needed.

Step 6 To save the Advanced filter, click the **Save** icon and supply a name for the filter.

Step 7 To clear the Advanced Filter, click **Clear Filter.**

Related Topics

- Purging Alarms for SNMP Traps
- Troubleshooting Prime Infrastructure SNMP Traps
- Configuring Notifications
- Port Used To Send Traps
- Configuring Email Notifications for SNMP Traps
- Viewing Events and Alarms for SNMP Traps
- Filtering Events and Alarms for SNMP Traps

Purging Alarms for SNMP Traps

You can remove an alarm from the list of alarms by changing its status to Acknowledged or Cleared. No e-mails will be generated for these alarms.

Step 1 Log in to Prime Infrastructure.

Step 2 Select **Monitor > Monitoring Tools > Alarms and Events**.

Step 3 Select an alarm, then choose **Change Status > Acknowledge** or **Change Status > Clear**.

Troubleshooting Prime Infrastructure SNMP Traps

If you are having trouble with Prime Infrastructure's internal traps and related notifications, check the following:

Step 1 Ping the notification receiver from the Prime Infrastructure server, to ensure that there is connectivity between Prime Infrastructure and your management application.

Step 2 Check if any firewall ACL settings are blocking port 162, and open communications on that port if needed.

Step 3 Log in to Prime Infrastructure with a user ID that has administrator privileges. Select **Administration > Settings > Logging** and download the log files. Then compare the activity recorded in these log files with the activity you are seeing in your management application:

- ncs_nb.log: This is the log of all the northbound SNMP trap messages Prime Infrastructure has sent. Check for messages you have not received.
- ncs-#-#.log: This is the log of other recent Prime Infrastructure activity. Check for hardware trap messages you have not received.
- hm-#-#.log: This is the complete log of Health Monitor activity. Check for recent messages about High Availability state-changes and application-process failures that you have not received.

The messages you see in these logs should match the activity you see in your management application. If you find major differences, open a support case with Cisco Technical Assistance Center (TAC) and attach the suspected log files with your case.

Related Topics

- Prime Infrastructure SNMP Trap Types
- Prime Infrastructure SNMP Trap Reference
- Working With Prime Infrastructure Traps