CA Unified Communications Monitor

Understanding Incidents and Incident Responses

Version 3.5

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: What are Incidents?

UC Monitor uses *incidents* to report degraded conditions in VoIP call performance.

Incidents are assigned sequential case numbers and reported on the Incident Report page. An *incident* is a record of information that UC Monitor creates when a threshold is crossed. Thresholds are boundaries of acceptable performance behavior, and exist by default for each monitored call performance metric. Administrators can change thresholds to make them more or less sensitive to performance changes.

UC Monitor creates incident reports, displays them on the Incidents Overview, and launches associated responses. An administrator can configure incident responses for each type of incident:

- Call setup incidents, for Cisco Unified Communications Manager environments only.
- Call quality incidents
- Video quality incidents
- Call server and call server group incidents, for Cisco Unified Communications Manager environments only.

A set of consecutive incidents can represent one extended, degraded state. Depending on the type of metrics, excessive or degraded statistics triggers a call quality incident or a call setup incident. Only one incident is open at a time for a unique Location or voice gateway pair. When an incident is already open for a pair, the incident is updated with the time of the new observation.

Note: Collector incidents are applicable to collector performance and are reported separately. For more information about collector incidents and collector thresholds, see the use case titled "Managing Collectors in Avaya or Cisco Environments" in the UC Monitor bookshelf.

Chapter 2: What are Incident Responses?

Incident responses are associated with specific performance thresholds. You can set up automatic a*ctions f*or each incident response.

- Call Quality incidents can trigger email and SNMP trap actions.
- Call Performance incidents can trigger email, SNMP trap, and traceroute actions.
- Call Setup incidents can trigger email, SNMP, and traceroute actions.
- Call Server incidents can trigger email and SNMP trap actions.
- Call Server Group incidents can trigger email, SNMP, and traceroute actions.
- Collector incidents can trigger traceroute actions.
- Poor Call Quality incidents automatically trigger Call Watch investigations.

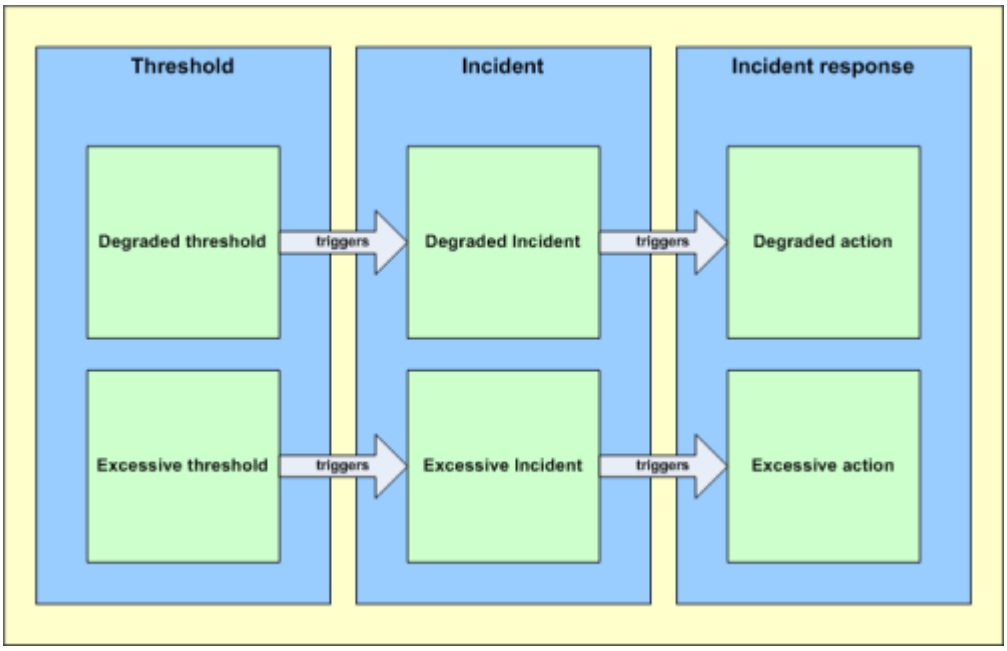
By default, performance thresholds do not trigger actions. When you customize thresholds, you can associate actions to incident responses. The response actions include network-specific parameters, such as email addresses that receive automatic notifications. A UC Monitor administrator can specify one of the following responses for an incident:

- An action that occurs when performance meets or exceeds the degraded threshold
- An action that occurs when performance meets or exceeds the excessive threshold

Important: Understand the difference between expected performance and unusual, or truly degraded, performance. Otherwise, incidents for an actual network anomaly can be lost amid a long series of incidents that are raised continually for normal performance conditions.

Chapter 3: How Incidents Trigger Responses

UC Monitor creates an incident when it detects a condition on the network that exceeds a threshold. If an action is associated with the threshold condition, UC Monitor launches that action automatically, as shown in the following diagram:



Keep in mind the following details about incidents, incident responses, and actions:

- UC Monitor creates an incident the first time a threshold is crossed.
- UC Monitor creates another incident for the same violation only after the first incident is closed.
- To trigger an incident, a violation must exceed minimum severity and duration criteria.
- A UC Monitor administrator can associate an incident response with the incident type.
- For a few incidents, such as the Abnormal Termination incident, no applicable metrics are monitored for improvement so that the incident can be closed. Therefore, the incident is briefly opened to trigger automatic actions and is then immediately closed. The accompanying email or SNMP trap notification indicates that the incident is open, but in fact closure is pending.

- The traceroute investigation action is configured as an incident response action for call setup or call server group incidents only.

  The results of a traceroute investigation for other types of incidents, such as call quality, are not helpful. Traceroutes begin at the collector, which is located so closely to the call server that little is determined from the route for call traffic.

  For call server group incidents, the collector attempts to run a traceroute to the key phone at the affected Location.

A traceroute investigation can also be launched independently of an incident.

Chapter 4: How Incidents are Closed

An incident remains open until it is automatically closed. For example, the severity of the condition changes, but the metrics still violate the degraded or excessive threshold. The incident is updated to reflect the change in severity, but the incident is not closed.

Incidents are closed when:

- They have been open for 24 hours. If the problem still occurs after 24 hours, a new incident is opened.
- The performance condition that violated the threshold has not been detected for one full clock hour of data collection. A full clock hour is not the same as 60 minutes of time. A full clock hour starts at the beginning of an hour and ends at the beginning of the next hour.

Incident types can change. A call quality threshold violation overrides a call setup violation when they affect the same pair of reporting components. An incident remains open for that pair, but the type of incident changes to call quality when a call quality threshold violation is detected.

Note: You can acknowledge an incident for a degraded performance condition and not be aware that the performance condition has deteriorated further. A degraded incident can change to severe status while still appearing as acknowledged in incident reports. As a best practice, acknowledge only those incidents that you have taken steps to address.

Chapter 5: How Thresholds and Incidents Work Together

The following is a fictitious example of how performance thresholds, incidents, and incident responses work together:

1. A call server cluster at the Austin, TX, network location becomes unavailable due to a LAN connectivity issue.
2. Several users dial out with their IP telephones and are routed to a backup call server cluster in Phoenix.
3. The delay-to-dial tone call setup excessive threshold of 2000 milliseconds is exceeded.
4. UC Monitor creates one call setup incident for all affected telephones at the Austin Location.

   The call setup incident launches two associated incident response actions:

   - Sending an email to notify a network engineer at the Austin location that a call setup threshold was exceeded.
   - Automatically launching a traceroute investigation to the key phone at the Austin Location.
5. The network engineer at the Austin site clicks a link in an email message. The link opens a page of incident reports, where the engineer can quickly drill down to find the affected call server cluster.
6. From the incident report, the engineer can easily access the Investigation Details page. This page allows easy comparison of the baseline route to the current route to find the connectivity issue.

When an incident or Investigations report does not include sufficient information to resolve the problem, the engineer can launch a Call Watch for more information.

Chapter 6: How to Respond to an Incident

Incidents and incident responses are useful for troubleshooting in the following ways:

- Incidents maintain a record of conditions at the time a problem occurs.
- Incident responses automatically gather information that helps you troubleshoot a problem, reducing the mean-time-to-repair (MTTR).

An email about an incident contains a notification that a threshold was crossed. The message also contains a link to the incident report, where you can drill down into detailed information.

Status updates are available for SNMP trap notifications. A UC Monitor administrator can configure them as incident response actions. They also include a notification that performance for a certain component has returned to normal after a recent threshold condition that was also reported. For each incident reported in an incident response email message, one or more links to associated UC Monitor reports are included.

When you receive an notification of an incident (such as an email or an SNMP trap), perform one or more of the following actions to troubleshoot the poor performance.

- Click links provided in the notification to view the relevant incident report.
- Drill down for more information about the incident, such as the status of call servers.
- Click the Related Reports link to an associated investigation report. Review the Traceroute Investigations report to see whether the path of the call setup traffic resembles the one shown in the Baseline Traceroute Details.
- Launch a manual traceroute investigation for more information about the route between the affected endpoint and its call server or voice gateway.
- Initiate a Call Watch for the affected endpoints.
- Acknowledge the incident to reduce its priority and to let other operators know that the issue is addressed.

  Note: You can acknowledge an incident for a degraded performance condition and not be aware that the performance condition has deteriorated further. A degraded incident can change to severe status while still appearing as acknowledged in incident reports. As a best practice, acknowledge only those incidents that you have taken steps to address.