

MANAGEMENT CONNECTOR FOR CA SERVICE DESK



- Automatic and manual CA Service Desk incident generation based on Enterprise Manager alerts and job status events
- Fully customizable incident generation via ticket templates
- Automatic alert-to-incident synchronization
- In context launch of CA Service Desk console from Enterprise Manager and vice versa
- Out-of-box ticket templates

As part of an integrated solution for quality IT service management, the Oracle Management Connector for CA Service Desk enables IT organizations to proactively detect and respond to incidents to ensure high quality of service levels are maintained. The Oracle Management Connector for CA Service Desk integrates Oracle Enterprise Manager Grid Control's proactive alert detection and resolution features with CA Service Desk's capabilities to provide a seamless workflow for incident management and resolution – from the creation of CA Service Desk incidents based on alerts to bi-directional console links for incident resolution to automatic incident closure based on the clearing of alerts.

Automatic and manual incident generation

The Oracle Management Connector for CA Service Desk (CA Connector) enables the automatic or manual generation of CA Service Desk incidents (tickets) in response to alerts or job status events detected by Oracle Enterprise Manager Grid Control. In the Enterprise Manager console, administrators use Notification Rules to specify the set of metric alerts and/or job status events for which CA Service Desk incidents should be opened as well as the ticket template used to open the incident. If any of the metrics specified in the notification rule is detected to have crossed its thresholds, an alert is triggered and the CA Connector will automatically generate a CA Service Desk incident with the appropriate fields filled in with details of the alert. For example, if IT organizations require that a CA Service Desk incident be opened for filesystem related alerts, administrators can simply use Enterprise Manager to create notification rules for these filesystem metrics and associate a CA Service Desk ticket template with these metrics. If a filesystem is detected to have crossed its threshold, an alert is triggered and a CA Service Desk incident is automatically generated with details of the alert such as name of the host, filesystem space used, mount point, time the alert triggered, etc.

Once the incident has been created, the CA Connector will continue to keep the incident in synch by updating the CA Service Desk system each time the alert severity changes. For example, if a warning alert on the filesystem metric initially created an incident at “medium” level of urgency, if the alert subsequently changed to critical severity, this change will be communicated from the CA Connector to CA Service Desk which could, in turn, cause the corresponding incident to be upgraded to “high” level of urgency.

For IT organizations that require a manual triage of an alert before an incident is opened for it, the CA Connector also supports the ability to manually generate an incident (ticket)

directly from the Enterprise Manager console. This means a first level operator can use the Enterprise Manager Console to initially investigate the alert, then, if necessary, open an incident (ticket) right within the Console. Relevant information about the alert is automatically carried into the generated incident.

In both scenarios (automatic or manual generation of incidents), the incident ID for the generated incident is tracked and displayed as part of the details of the alert in the Enterprise Manager console. This enables Enterprise Manager administrators to have a complete view of all the actions taken in response to the alert.

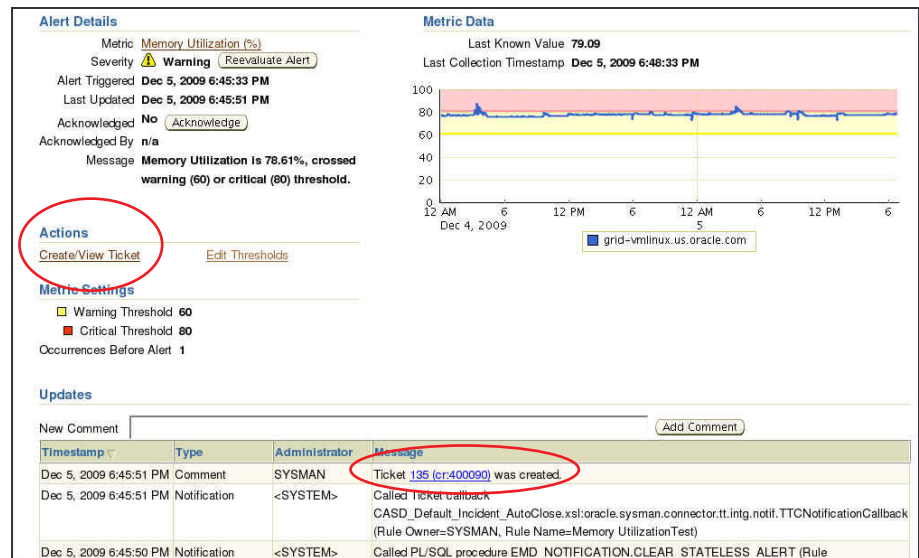


Figure 1: Alert details in the Enterprise Manager console include information about the CA Service Desk incident that was automatically created. Alternatively, the CA Service Desk incident could be manually created directly from the console.

Fully customized incident (ticket) generation via ticket templates

Many IT organizations customize their CA Service Desk installations to support the way they manage incidents. Part of this customization includes defining the valid and required set of fields that make up a CA Service Desk incident (ticket). For example, some IT organizations may require an incident to contain the Affected End User, Incident Area, Priority, Assignee, Severity, and Urgency fields while others may additionally require other fields such as Group and Configuration Item as well. The CA Connector can generate incidents that are compatible with any CA Service Desk implementation by providing the same level of customization via ticket templates.

Ticket templates are customer-defined files that specify how (incident) ticket fields should be filled based on attributes of Enterprise Manager alerts. In a ticket template, administrators specify the fields of the ticket that should be pre-filled and the values assigned to those fields. The values for the ticket fields can either be:

- **Derived values based on the alert.** This means the values for the ticket fields are based on the values of the Enterprise Manager alert. For example, administrators can

assign the alert message to the ‘Summary’ field of the ticket, and the metric name, target name and metric alert severity fields to the ‘Description’ field of the ticket. If the target type of the target on which the alert occurred is ‘Database’, then the ticket ‘Incident Area’ field could be set to ‘Database’ and the ‘Group’ field could be set to DBA group.

- **Operational values based on target properties.** Each target in Enterprise Manager has a set of target properties that can be used to associate business and/or operational attributes to the target. For example, you can use the ‘Contact’ property to specify the administrator who owns the target, or the ‘Deployment Type’ property to specify how the target is being used – Production, Test, Stage, etc. To support other operational requirements, you can also add additional target properties as well (e.g. “Asset ID” or “Application Supported”, etc.). Any of these target properties can be used in the ticket template and be mapped to the appropriate CA Service Desk incident field.
- **Constant values for specific fields.** This means the values of the ticket fields are predefined constant values recognized in the CA Service Desk system. For example, administrators can set the ‘Incident Area’ ticket field to ‘Infrastructure Servers’ if they have configured Enterprise Manager to open (incident) tickets for database and application server alerts. They can also set the ‘Reported By’ field to ‘Enterprise Manager’ to indicate that the source of the ticket is an Enterprise Manager alert.

To facilitate the definition of templates for a specific CA Service Desk installation, the CA Connector installation offers a couple of out-of-box templates based on the default CA Service Desk configuration. Administrators can easily use these out-of-box templates as a basis for their own custom templates that fit their operational needs. Administrators can create as many ticket templates as required, for example, a Production Database template, a Test Database template, and a Development Database Template, and assign different alert-to-ticket mappings in each of these templates. Once these custom templates have been defined and registered in Enterprise Manager, they are available for any administrator to use in notification rules.

Advanced Notification Methods

Name	Type	Description	Support Repeat Notifications	Assign Method to Rule
No notification methods found.				

Repeat Notifications

Notifications can be sent repeatedly for all Metric alerts and Availability states (Target Down, Agent Unreachable, Metric Error Detected) specified in this rule. The repeat notifications will stop only when the alert is acknowledged or has cleared or the maximum number of repeat notifications has been reached.

Send Repeat Notifications

Use Global Repeat Notification Settings Override Global Repeat Notification Settings

Repeat notifications will not be sent for this rule until a Super Administrator enables the feature.

Repeat Frequency (minutes)

Maximum Repeat Notifications

Clear Alert

Select Clear to permanently clear metric alerts which are not cleared automatically by agents using metric evaluation but require administrator to manually clear them. For example, database Alert Log entries generates metric alerts which are not cleared by agent.

Clear Alert

Ticketing

Template

General Availability Metrics Policies Jobs Actions

Figure 2: In a notification rule, the appropriate ticket template can be chosen for the targets and alerts selected in the rule.

Bi-directional console launch for incident resolution

After the incident is created, the incident ID and a link to the CA Service Desk web console UI is available as part of the alert details in the Enterprise Manager console. This provides an easy way for administrators to logon to the CA Service Desk console to perform actions such as further annotate the incident with suggestions for a fix or determine the progress that has been made thus far. Likewise, in the CA Service Desk console, a link to the alert details page in the Enterprise Manager console is provided, allowing service desk analysts to quickly access Enterprise Manager's features to resolve the alert. For example, if an incident was opened for a database down alert, the service desk analyst can quickly link back from the CA Service Desk console to the Enterprise Manager console to restart the database. This minimizes the need to have service desk analysts install specific toolsets for repair actions. Once the repair action has been performed, Enterprise Manager will detect that the alert condition has been cleared and the CA Connector can be configured to automatically close or resolve the incident associated with the alert. This bi-directional workflow thus streamlines the incident resolution process to promote quick time to resolution.

The screenshot displays the CA Service Desk web console interface. At the top, it shows the incident ID '135' and the title '135 Incident Detail'. Below this, there are several sections of information:

- Affected End User:** Administrator, Incident Area: Open, Status: Open, Priority: 5.
- Reported By:** ServiceDesk, Assignee: ServiceDesk, Group: ServiceDesk, Configuration Item: ServiceDesk.
- Severity:** Urgency, Impact: None, Active?: YES.
- Problem:** Call Back Date/Time, Root Cause.
- Change:** Caused by Change Order, Outage Start Time, Outage End Time.
- Summary Information:**
 - Summary:** Memory Utilization is 78.61%, crossed warning (60) or critical (80) threshold. Total Activity Time: 00:00:00.
 - Description:** Ticket created by EM CASD Connector. Incident Priority: 0.

At the bottom of the summary information, there is a detailed description of the alert, including the EM User (SYSMAN), Alert Information, Target Type (Host), Target Name (grid-vmlinux.us.oracle.com), Metric Column (Memory Utilization (%)), Metric Name (Load), Severity (Warning), Collection Time (2009-12-05 18:45:33.0), Target Host (grid-vmlinux.us.oracle.com), Notification Rule (Memory UtilizationTest), and a URL linking back to the Enterprise Manager console.

Figure 3: Information about the alert is passed to the CA Service Desk incident. A link back to the Enterprise Manager console is also provided.

Learn More

For more information about this and other Oracle Management Connectors, visit <http://www.oracle.com/technology/products/oem/extensions/index.html>

To learn more about Oracle Enterprise Manager Grid Control, visit www.oracle.com/enterprise_manager

Copyright © 2010, Oracle. All rights reserved.

This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor is it subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle, JD Edwards, and PeopleSoft are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.