

ORACLE®



ORACLE<sup>®</sup>

## Incident Management in Enterprise Manager 12.1

Pete Sharman

Principal Product Manager

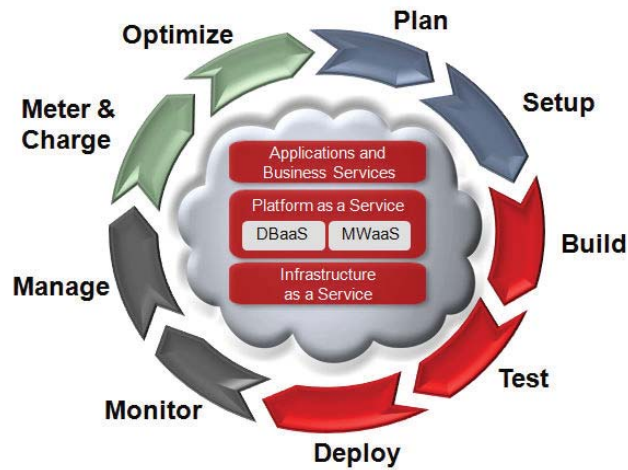
# Agenda

- Introduction to EM 12c
- Overview of Incident Management
- Events, Incidents and Problems
- Incident Rule Sets
- Backward Compatibility / Migration
- Q&A



# Total Cloud Control

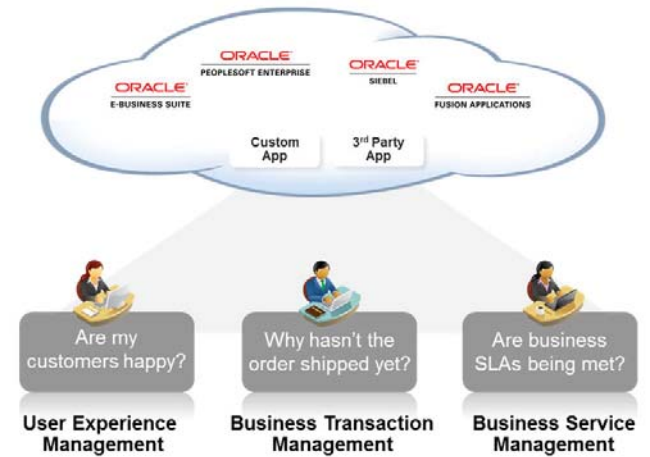
ORACLE®  
ENTERPRISE MANAGER 12<sup>c</sup>



**Complete Lifecycle Management**



**Integrated Cloud Stack Management**



**Business-Driven Application Management**

Self-Service IT

Simple and Automated

Business Driven

ORACLE®

# Enterprise Manager Cloud Control 12c

## Major Themes





# Incident Management

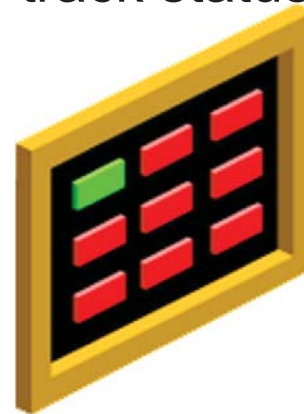
## Overview

- Monitor and resolve service disruptions quickly and efficiently
- Instead of managing numerous discrete events, manage fewer, meaningful incidents:
  - By business priority
  - Across their lifecycle
- Centralized incident console for incident management
- Identify, resolve and eliminate root causes of disruptions

# Incident Management

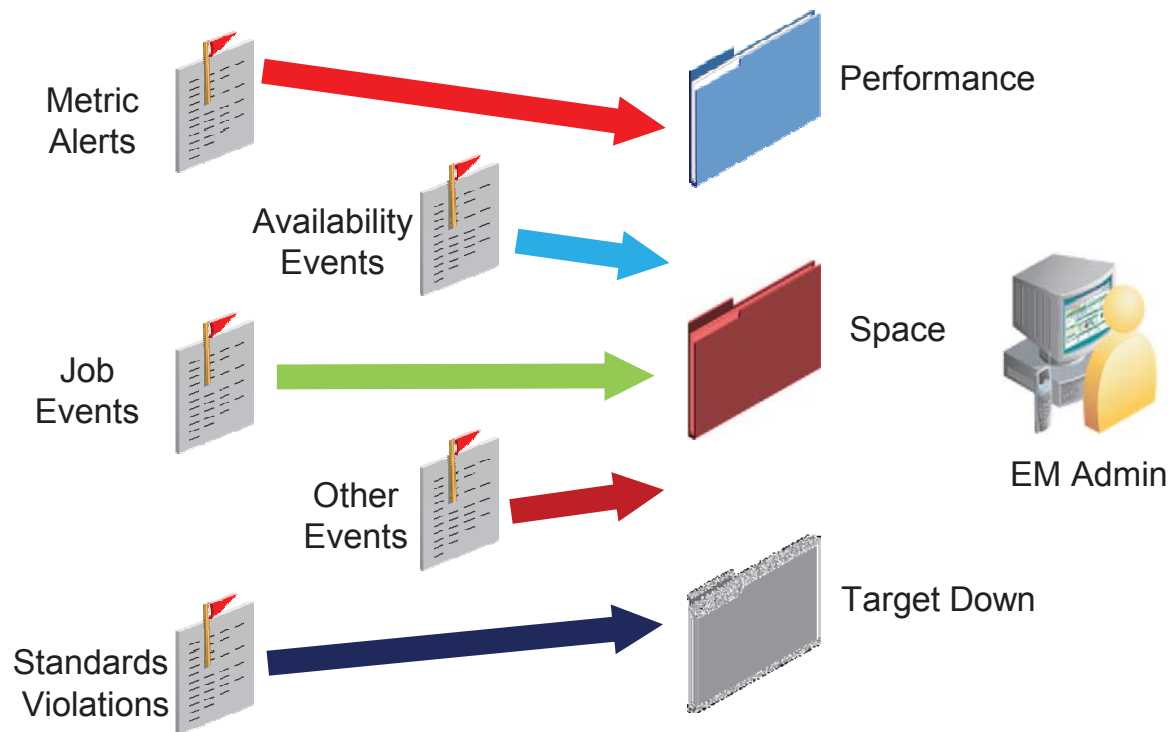
## Overview

- Integrated Oracle expertise to accelerate incident and problem diagnosis and resolution
- Support for incident lifecycle operations
  - Assign, acknowledge, prioritize, track status, escalate, suppress



# Incident Management

## Events and Incidents



- Manage by incidents
  - Significant events
  - Combination of events related to the same issue (e.g., events raised from database, host, storage indicating lack of space)

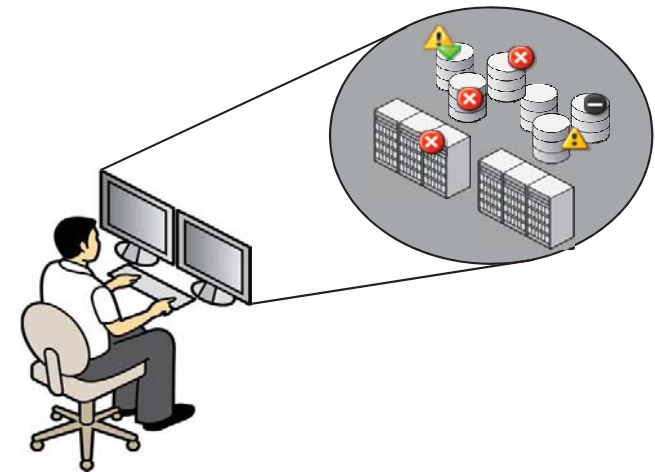


# Incident Management

## Events





Significant occurrences in IT infrastructure detected and raised by Enterprise Manager. Events have:

- Entity on which the event is raised (target, job, etc.)
- Type
- Severity
- Message
- Timestamp
- Category



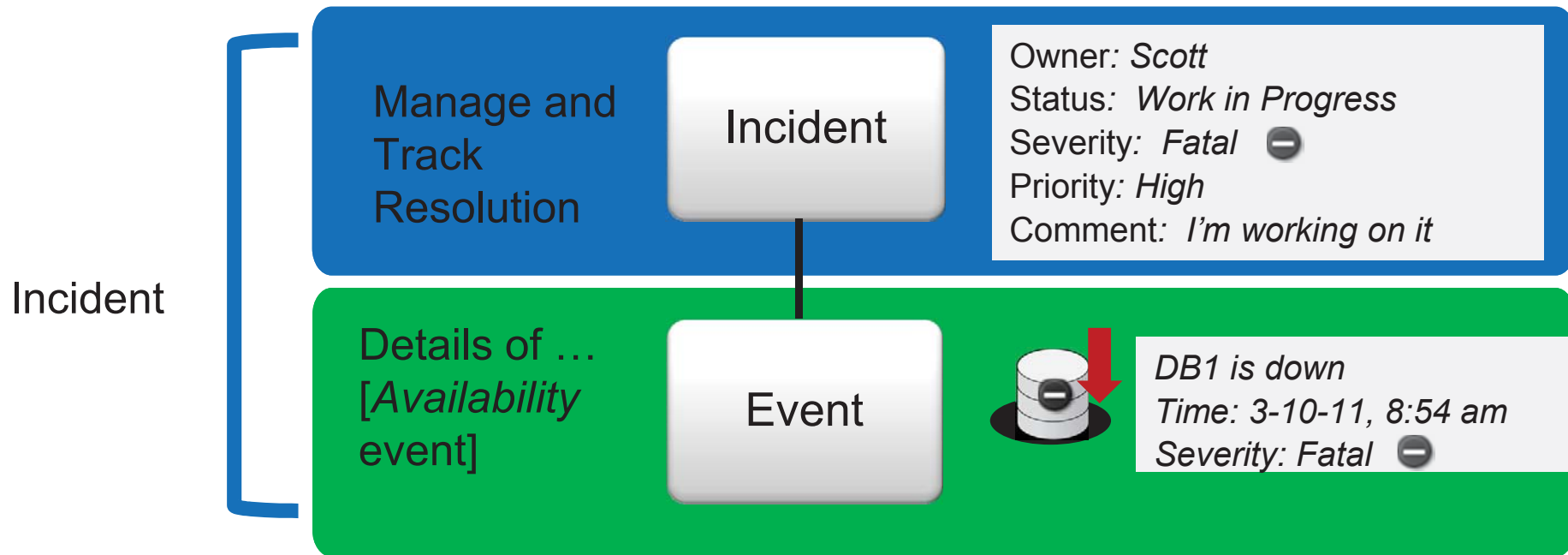
# Incident Management

## Events

- Event Types:
  - Target Availability
  - Metric Alert / Evaluation Error
  - Job Status Change
  - Compliance Standard Violation Event
  - High Availability
  - Connector External Class
  - User reported event
- Event Severities
  - Fatal 
  - Critical 
  - Warning 
  - Advisory 
  - Informational

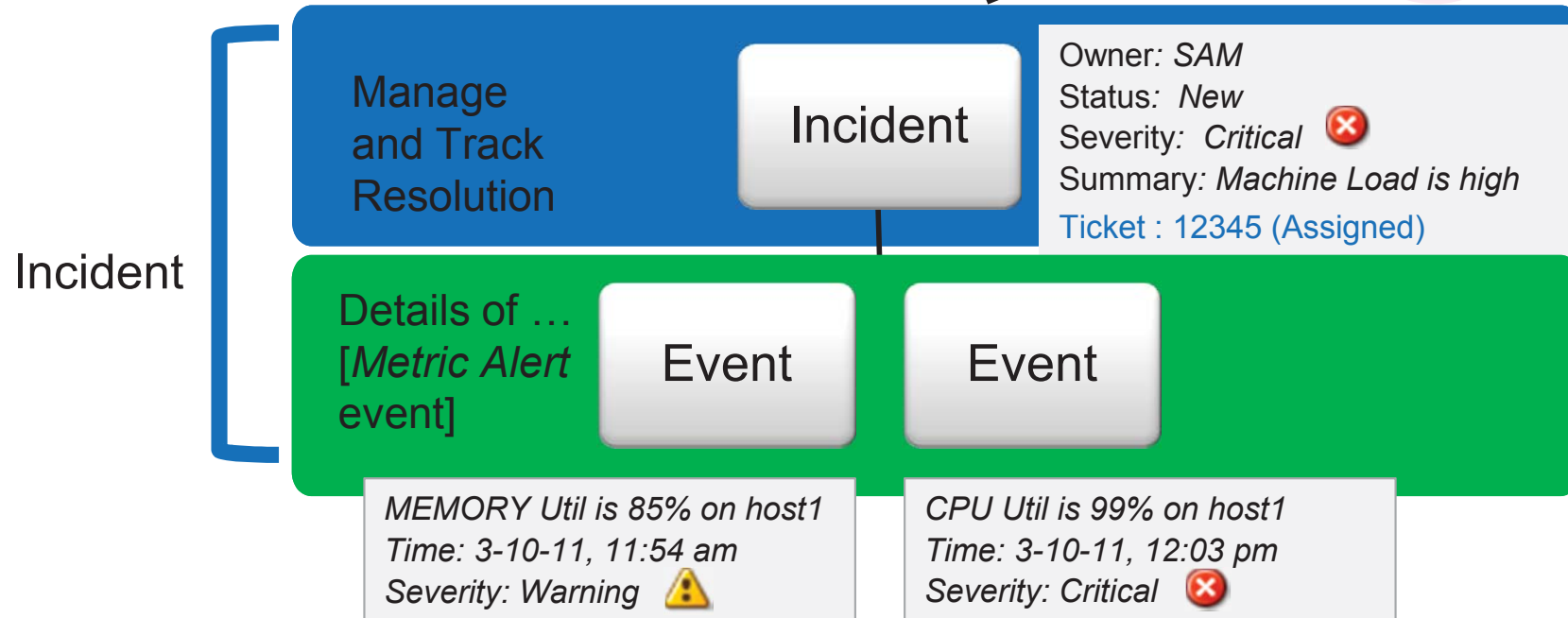
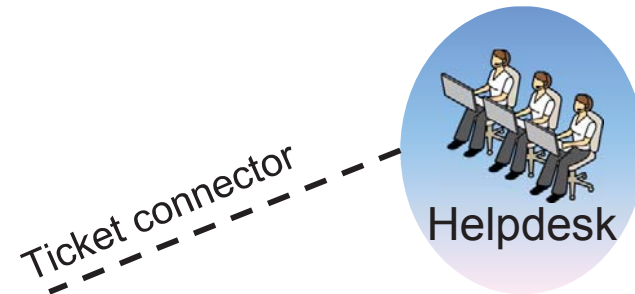
# Incident Management

## Incidents with One Event



# Incident Management

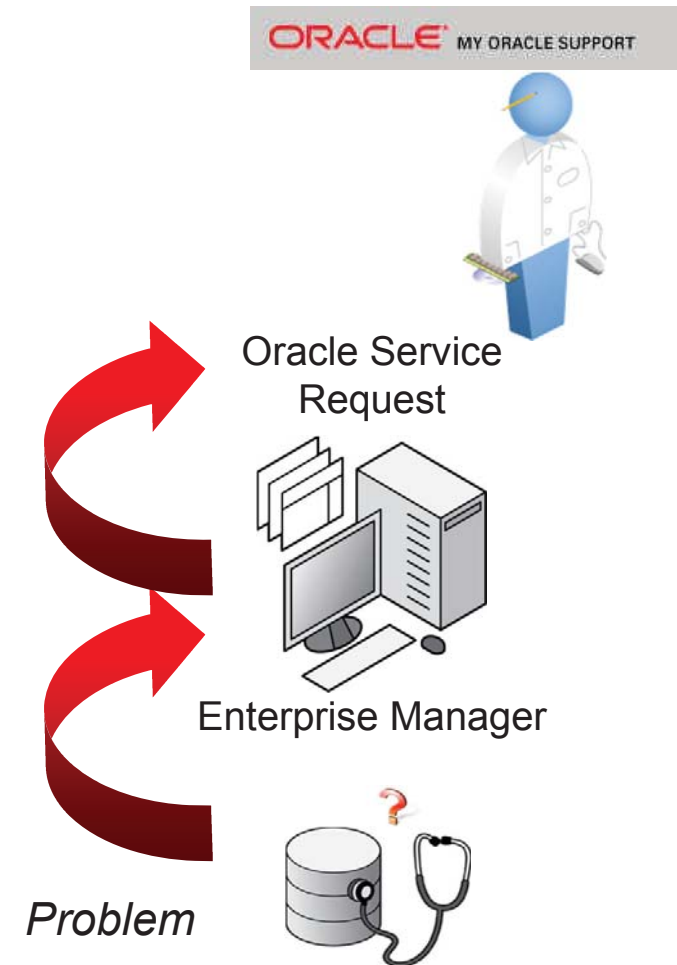
## Incidents with Multiple Events



# Incident Management

## Problems

- Underlying root cause of incidents
- Facilitate resolution of Oracle software 'problems'
  1. Auto-creation of problem based on ADR incidents
  2. Package diagnostic data
  3. Open Oracle SR





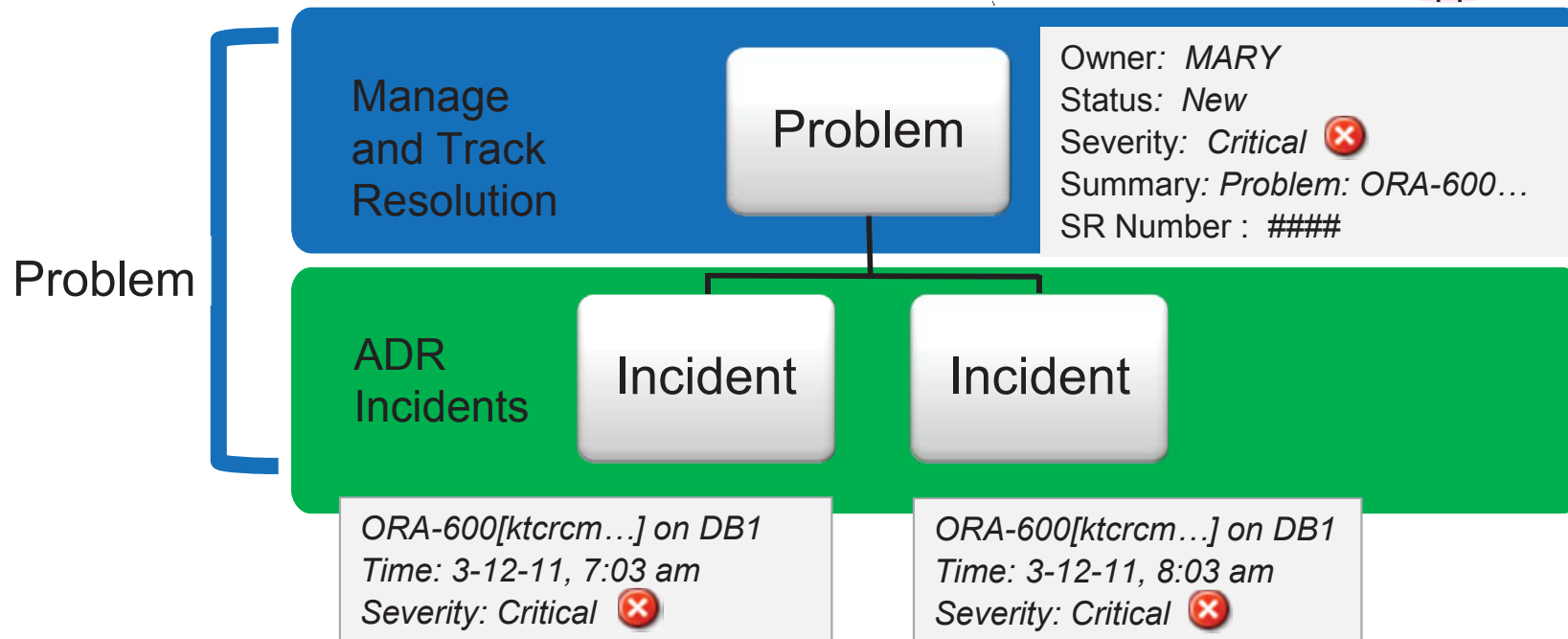
# Incident Management

## Problems

- ADR incident generates one Enterprise Manager incident per occurrence
  - Multiple ADR incidents with the same problem signature (e.g. same root cause) generate one problem object
- Manage Problem in Incident Manager
  - Track status (assign ownership, etc.)
  - View diagnostic information (via Support Workbench)
  - Open Oracle SR (via Support Workbench)
  - Status of diagnostic activity visible in UI: SR #, Bug # etc

# Incident Management

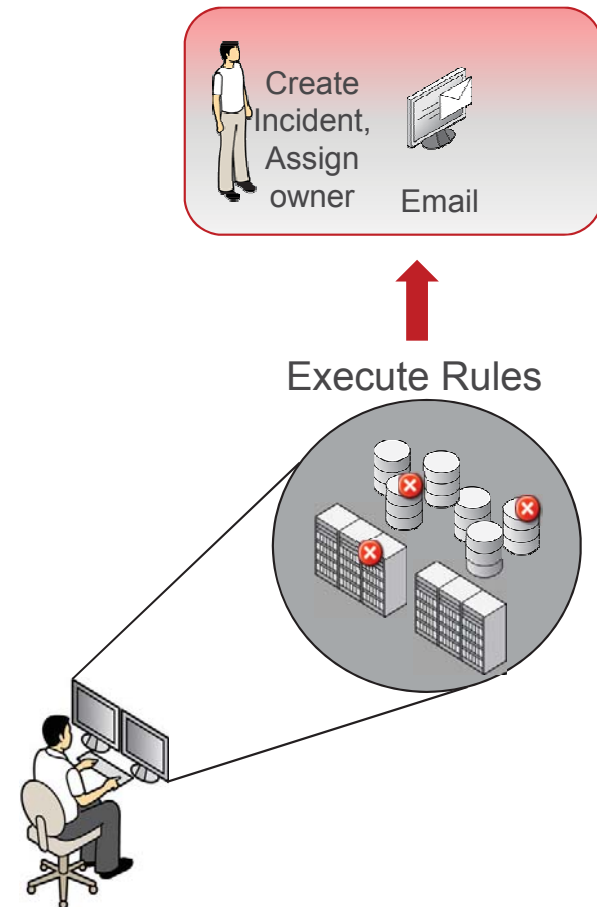
## Incidents and Problems



# Incident Management

## Incident Rule Sets

- Replace notification rules
- Automate actions related to events, incidents, problems
  - Creation of incident based on an event
  - Notification actions (including ticketing)
  - Operations to manage incident workflow (assign owner, set priority, escalate, etc.)







# Incident Management

## Incident Rule Sets

- Rule set - Set of one or more rules that apply to a common set of objects: targets (e.g. groups), jobs, etc.
- Logically combine different rules relating to the same object into one manageable unit
- Rules within a rule set are executed in specified order
- Rule sets are also executed in specified order
- Out-of-box rule sets for incident creation, event deletion
  - Can't be edited, only disabled



# Incident Management

## Incident Rule Sets

- Rule – instructions within a rule set that automate actions on events or incidents or problems
  - Operates on *incoming* events or incidents or problems
- Rule consists of:
  - 1.Criteria: events/incidents/problems on which rule applies
  - 2.Action(s): ordered set of one or more operations on the specified events/ incidents/ problems. Each action can be executed based on additional conditions.



# Incident Management

## Incident Rule Sets

RULE CRITERIA	RULE CONDITION	RULE ACTION
CPU Util(%), Tablespace Used(%) metric alert events of warning or critical severity	--	Create Incident
Incidents of warning or critical severity	If severity = critical If severity = warning	Notify by page Notify by email
Incidents open for more than 7 days		Set escalation level to 1

# Incident Management

## Incident Rule Sets

Rule Set: *Rule Set for PROD-GROUP*

Applies to: *PROD-GROUP*

Type: *Enterprise*

RULE#1: Target down rule

**Criteria:** *DB and WLS down availability event*

**Action:** *Create incident, Set Priority = High*

RULE#2: Email and Pager rule

**Criteria:** *All Incidents with severity= Fatal, Critical or Warning*

**Action #1:** *If severity = Warning, email*

**Action #2:** *If severity = Fatal or Critical, page*



# Incident Management

## Rule Set Recommendations

- For rule sets that operate on targets, use groups as the target for the rule set
- Put together all rules that pertain to group members in the same rule set
- Leverage the execution order of rules within the rule set



# Incident Management

## Rule Set Recommendations

- Use rules on *events* to
  - Create incidents for the alerts/events you manage in Enterprise Manager
  - Create incidents and create tickets on the incidents if you use trouble ticketing systems integrated with Enterprise Manager
  - Send events to third party management systems
  - Only notify on events but not create incidents – adhoc usage



# Incident Management

## Rule Set Recommendations

- Use rules on *incidents*
  - Automate management of incident workflow (assign owner, set priority, escalation levels, etc.) and send notifications
  - Create tickets based on incident conditions e.g., create a ticket if incident is escalated to level 2
- Use rules on *problems*
  - Automate management of problem workflow (assign owner, set priority, escalation levels etc.) and send notifications



# Incident Management

## Prioritization of Rules and Notifications

- Under heavy load, more important events and incidents are processed ahead of others
- Processing priority based on:
  - Lifecycle Status of the target
    - 1. Mission Critical - highest priority
    - 2. Production
    - 3. Stage
    - 4. Test
    - 5. Development - lowest priority
  - Type of event/incident
    - Availability events/incidents – highest priority
    - All events/incidents (warning, critical severities)
    - All events (informational) – lowest priority





# Incident Management

## Backward Compatibility

- Existing notification methods (PL/SQL, OS scripts, SNMP traps) will continue to work in Enterprise Manager Cloud Control 12.1
- To leverage new features, create new versions of these notification methods
  - Use new event model
- Existing notification rules will be migrated to incident rule sets

# Incident Management

## Notification Rule - Incident Rule Set Mapping

### 11.1 Notification Rule

Notification Rule : *Rule for PROD-GROUP*  
Applies to: *PROD-GROUP*  
Target Type: DB

Availability tab  
**Criteria:** *DB down*

Metrics tab  
**Criteria:** *Selected metrics, severities*

**Action:** *email user1 and user2*

### 12.1 Incident Rule set

Rule Set: *Rule for PROD-GROUP*  
Applies to: *PROD-GROUP*  
Type: *Enterprise*

Event Rule#1: "Target Availability" rule  
**Criteria:** *Event Type = Target Availability  
Target Type = "DB"  
Target Status = "Down"*  
**Action:** *email user1 and user2 and  
Create Incident*

Event Rule#2: "Metric Alert" rule  
**Criteria:** *Event Type = Metric Alert  
Target Type = "DB"  
Metric Alert specific criteria*  
**Action:** *email user1 and user2 and  
Create Incident*

# New Features in 12cR2

## Incident Management Related



- Incident Rules
  - Support for Lifecycle Status as criteria for targets in rule set
- Incident Manager
  - Support for bulk operations: Acknowledge, Suppress, Clear, Comment, Set Status, Escalate, Prioritize, Assign
  - Quick access to target information

Target information available

The screenshot displays the Oracle Incident Management interface. A table lists several incidents, including 'The J2EE Application is down' and 'The WebLogic Server is down'. A 'Target Information' popup window is open, showing details for the target '/ess\_soa\_WLS\_SOAWC/WLS\_SOAWC/soa\_server1/default'. The popup includes fields for 'Down Since', 'Availability (%)', 'Version', 'Oracle Home', 'Middleware Home', 'Domain Home', 'Agent', 'Host', and 'Member of'. A red arrow points from the 'Target Information' link in the 'Incident Details' section of the table to the popup window.

# Q&A

# Hardware and Software

ORACLE®

# Engineered to Work Together

ORACLE®

ORACLE®