Strategies for Monitoring Large Data Centers with Oracle Enterprise Manager

Ana McCollum
Consulting Product Manager
The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle.
Agenda

- Overview of Oracle Enterprise Manager
- Monitoring Best Practices
- Q&A
Business-Driven IT Management

Business Users and Customers

User Experience

Business Transactions
- WEB PORTAL
- PRODUCT CATALOG
- ORDER ENTRY
- OTHER SERVICES

Business Services

Business-Driven Application Management
- Understand business needs
- Manage from business perspective

Integrated Application-to-Disk & Cloud Management
- Eliminate management silos
- Create agile IT for dynamic business

Integrated Systems Management & Support
- Proactively identify and fix problems
- Maximize business productivity

Oracle
Support

Services Cloud

Integrated Application-to-Disk and Cloud Management

APPLICATIONS
MIDDLEWARE
DATABASES
SERVERS
STORAGE
Business-Driven IT Management

User Experience

Business Transactions
- Web Portal
- Product Catalog
- Order Entry
- Other Services

Business Users and Customers

Business-Driven Application Management
- Understand business needs
- Manage from business perspective

Integrated Application-to-Disk & Cloud Management
- Eliminate management silos
- Create agile IT for dynamic business

Integrated Systems Management & Support
- Proactively identify and fix problems
- Maximize business productivity

Integrated Application-to-Disk and Cloud Management

APPLICATIONS
- Middleware
- Databases
- Servers
- Storage

Services Cloud
- Oracle Support

Integrated Systems Management and Support
Enterprise Manager Monitoring
Fundamental part of *Integrated Application-to-Disk* solution

- Lights-out data center monitoring
  - **Manage by Exception**: continuous monitoring of targets, generation of alerts when exceptions are detected
  - **Metric**: mechanism used to monitor target conditions (availability, performance, etc.)
  - **Alert**: generated when metric crosses its thresholds (warning, critical)
  - **Notifications**: sending of alert information (email, etc.)

- Complete and integrated across stack
  - Entire Oracle stack
  - Heterogeneous infrastructure monitoring by plug-ins
  - Extensible for custom needs

- Manage Many as One
  - Features to setup and monitor many targets as one

- Integrates with third party systems
  - Helpdesks and other management systems
Common Monitoring Questions

What’s the best way to...

- **Set Up Monitoring**
  - Deploy monitoring settings on targets
  - Set up notifications for administrators
  - Assign right level of target privileges to administrators

- **Manage Alerts**
  - Controlling volume of alerts
  - Removing unwanted alerts
  - Automating fix for common alerts
Best Practices for Monitoring the Data Center

Goals:

- **Meet monitoring requirements**
  - Deploy your monitoring standards
  - Alert notifications sent to the appropriate persons
- **Comply with security practices**
  - Follow *Principle of least privilege* when granting target privileges
- **Easy to manage**
  - Infrastructure does not become administrative task
  - ‘Manage many as one’ for managed targets
- **Scalable as enterprise grows**

Strategy:

- Set up monitoring for ‘economies of scale’ by laying the groundwork for monitoring
  - As enterprise grows, minimal effort to monitor new targets or add new Enterprise Manager administrators
- Leverage “Manage Many as One” features
Best Practices: Setting Up Monitoring

4 Step Methodology

1. Organize targets into groups
2. Use Roles to segregate responsibilities
3. Define and enforce monitoring standards
4. Set up notifications using groups
Setting Up Monitoring
STEP 1: Organize targets into Groups

- Plan your group structure
- Considerations:
  - Group together targets monitored in the same way
    - Same monitoring settings due to:
      - Supporting same application
      - Same Deployment type (Production, Development, Test)
    - Visually monitor them together in a dashboard
  - Can have group hierarchies
  - Sample group hierarchy:
    - By Line of Business
    - By Deployment (Prod vs Devt)
    - By Ownership
Setting Up Monitoring
STEP 1: Organize targets into Groups

“Create group based on Production database and host targets in the Finance department”

- Create the group in Enterprise Manager
  - You can search targets by operational criteria (aka target properties)
    - Deployment Type, Line of Business, Location...

- Additional tips:
  - Can add new target properties via EMCLI `add_target_property`
  - Can bulk update target properties via EMCLI `set_target_property_value`
Setting Up Monitoring
STEP 1: Organize targets into Groups

- Make the group “privilege-propagating”
  - A privilege on the group that is granted to a user automatically extends to all members of the group
    - Includes subgroups

- Requires:
  - Create Privilege-Propagating Group privilege
  - Full privilege on all targets to be added to the group
  - EMCLI modify_group verb to convert group to privilege propagating group
  - If a group is privilege propagating, all its parent groups must be privilege propagating.
Setting Up Monitoring
4 Step Methodology

Step 1: Organize targets into groups

Step 2: Use Roles to segregate responsibilities

Step 3: Define and enforce monitoring standards

Step 4: Set up notifications using groups
Setting Up Monitoring
STEP 2: Use Roles to segregate responsibilities

- *Who* should do *what* on the targets in the group?
- Map operations on the groups to job responsibilities (Senior Lead, DBA owner, First Line Support, etc.)
- Planning Considerations:
  - For the groups created, who can do these operations on them?
    - Change group membership
    - Grant privileges on the group to other users
  - Who can do these operations on the targets in the group?
    - Add / delete the target from Enterprise Manager
    - Define monitoring settings
    - Define notification settings
    - View / receive notifications for alerts
    - Acknowledge an alert
    - Act on target to resolve alert
    - Blackout target for planned or unplanned downtime
## Setting Up Monitoring

**STEP 2: Use Roles to segregate responsibilities**

Mapping of operations to Enterprise Manager privileges

<table>
<thead>
<tr>
<th>Operations</th>
<th>Enterprise Manager Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>...On the Group:</strong></td>
<td></td>
</tr>
<tr>
<td>• Change group membership</td>
<td></td>
</tr>
<tr>
<td>• Grant privileges on group to users</td>
<td><em>Group Administration</em></td>
</tr>
<tr>
<td><strong>...On the member targets:</strong></td>
<td></td>
</tr>
<tr>
<td>• Delete target from Enterprise Manager</td>
<td><em>Full on group</em></td>
</tr>
<tr>
<td>• Set blackout for planned downtime</td>
<td><em>Operator on group</em></td>
</tr>
<tr>
<td>• Change monitoring settings</td>
<td>• <em>Blackout Target</em></td>
</tr>
<tr>
<td>• Change monitoring configuration</td>
<td>• <em>Manage Target Metrics</em></td>
</tr>
<tr>
<td>• View and acknowledge alerts, Clear alerts</td>
<td>• <em>Configure Target</em></td>
</tr>
<tr>
<td>• View target, receive alerts on target</td>
<td>• <em>Manage Target Alerts</em></td>
</tr>
<tr>
<td></td>
<td><em>View on group</em></td>
</tr>
</tbody>
</table>
Setting Up Monitoring

STEP 2: Use Roles to segregate responsibilities

Examples of common job responsibilities:

**Group Administrator**
- Adds / Deletes target from Enterprise Manager
- Manages group membership
- Grants privilege on group to other users

**Senior Administrator**
- Adds / Deletes target from Enterprise Manager
- Sets up monitoring for targets
- Sets up notification rules for targets

**First Line Support**
- Receives notifications for alerts
- Responds to alerts

**Target Owner**
- Receives alerts and responds to alerts
- Changes monitoring settings for targets
- Perform target maintenance
Setting Up Monitoring
STEP 2: Use Roles to segregate responsibilities

Create roles for each job responsibility

**Group Administrator ROLE**
- “Add Any Target” system privilege
- “Group Administrator” on the group

**Senior Administrator ROLE**
- “Add Any Target” system privilege
- “Full” on the (privilege propagating) group

**First Line Support ROLE**
- “Manage Target Alerts” on the (privilege propagating) group

**Target Owner ROLE**
- “Operator” on the (privilege propagating) group
STEP 2: Use roles to segregate responsibilities

- **Create roles** containing the appropriate **privileges on the privilege propagating group**
- **Examples:**
  - SeniorAdmin Role = `Full` on ‘Production Sales Group’
  - FirstLineSupport Role= `Manage Target Alerts` on ‘Production Sales Group’
- **Grant roles** to administrators who manage the group
- **Don’t** grant privileges on individual member targets
  - Harder to maintain as group grows
Setting Up Monitoring
4 Step Methodology

Step 1: Organize targets into groups

Step 2: Use Roles to segregate responsibilities

Step 3: Define and enforce monitoring standards

Step 4: Set up notifications using groups
Setting Up Monitoring

STEP 3: Define and enforce monitoring standards

- Simplify management of many targets by defining standards for monitoring (set of metrics and thresholds)
  - Monitoring standard for production databases
  - Monitoring standard for test databases
  - etc.

- Create Monitoring Templates to encapsulate monitoring standards
  - Monitoring standard for “Production’ systems → put this in one template
  - Monitoring standard for “Test” systems → put in a separate template

- Monitoring Template typically contains complete set of metric settings
  - Specific to a target type
  - Examples:
    - Monitoring Template for production databases
    - Monitoring Template for test databases
Setting Up Monitoring

STEP 3: Define and enforce monitoring standards

- Create monitoring template
  - Senior Administrator creates the template on behalf of the LOB / Team
  - Grant ‘View’ on template to other consumers of the template
  - Grant ‘Full’ on template only to other senior administrators (or role) who are entitled to edit the template

- Apply monitoring templates to groups
  - Apply to highest level in group hierarchy
  - Will apply to the applicable targets in the group / subgroups
  - Example: Database template will only be applied to database targets in group

- Usage Notes:
  - Apply requires at least “Manage Target Metrics”
  - Multiple templates can be applied on a target, potentially overriding metric settings
  - Target can have specific metric settings by setting ‘prevent template override’ flag
Setting Up Monitoring

STEP 3: Define and enforce monitoring standards

- What if I have one monitoring standard for all my targets?
  - Define Monitoring Template
  - Specify it as the ‘Default’ for the target type
  - For targets added in the future, will be used instead of Oracle’s out-of-box monitoring settings

- Enterprise Manager will automatically apply template upon target discovery

- Usage notes:
  - Manually apply template for existing targets
  - Requires Super Administrator privilege to specify template as ‘Default’
Setting Up Monitoring
STEP 3: Define and enforce monitoring standards

- What if I have enterprise-wide settings and application-specific settings for my targets?
  - Use Default Template to specify enterprise-wide settings common to all targets
  - Use another template containing settings specific to application
- Apply to target after discovery
Setting Up Monitoring
4 Step Methodology

Step 1: Organize targets into groups
Step 2: Use Roles to segregate responsibilities
Step 3: Define and enforce monitoring standards
Step 4: Set up notifications using groups
Setting Up Monitoring
STEP 4: Set up notifications using groups

- **Notification Method**: means of sending notifications (e.g. email)
  - You can extend Notification Methods to accommodate custom alert handling: OS Script, PL/SQL, SNMP traps

- **Notification Rule**: when alert occurs, who gets notified and how

- **Use groups as the target for the notification rule**
  - If a target is added to the group, the notification rule will automatically apply to the target
Leveraging your monitoring setup
As your enterprise grows, minimal effort required for target setup

- When new targets are added to Enterprise Manager:
  - Do nothing (if using Default Templates) or apply Template
  - Add to appropriate group
  - … That’s it!

- Results:
  - Targets are monitored according to your standards
  - Notifications for alerts on the targets go to the right administrators
  - Administrators have the right privileges to manage the targets
Common Monitoring Questions

What’s the best way to...

- **Set Up Monitoring**
  - Deploy monitoring settings on targets
  - Set up notifications for administrators
  - Assign right level of target privileges to administrators

- **Manage Alerts**
  - Controlling volume of alerts
  - Removing unwanted alerts
  - Automating fix for common alerts
Managing Alerts

1. Control alerts at the source
   - Was the alert raised prematurely?
     - Are the thresholds too high/low?
     - Review metric trend
     - Adjust thresholds, set number of occurrences
   - Do I care about this condition? If NOT, then:
     - Disable metric collection schedule
       - Note: Other metrics may be impacted
     - For database *alert log* metric, use alert log filters
     - To disable alerting for database TEMP, UNDO tablespaces, see Support Note 816920.1
   - To deploy changed metric settings across targets, use Monitoring Templates
2. Use **Corrective Actions** to auto-resolve alerts

- Tasks that automatically run in response to an alert
- Is the resolution of the alert a repeatable process that can be scripted?
- Usage Notes:
  - Defined for a *metric*
    - Can be same or different for Warning vs Critical severity
    - Can have different tasks based on monitored object
      - Ex: *Filesystem Space Available(%)* can have different corrective actions for /u1 and /u2
  - Set up notifications for corrective action failure
Managing Alerts

3. Clear old log-based alerts regularly
   - Think about operational practice for regularly clearing old, resolved alerts
   - Automate using duration-based notification rules
     - Tip: Create a separate notification rule for this
     - Do not combine with rules for sending notifications
   - Manually via EMCLI
     - `clear_stateless_alerts`
       - Bulk clears stateless alerts for a target
Managing Alerts

Auto-clearing log-based alerts using notification rules

First specify the duration-based condition… (“Alert Log” alerts opened for at least 30 days)
Managing Alerts

Auto-clearing log-based alerts using notification rules

Then choose ‘Clear Alert’ action
Managing Alerts

4. Perform proactive monitoring using the System Dashboard

- Shows overall health of your group using universal colors of alarm
- Use System Dashboard at any level in group hierarchy:
  - Highest level – visibility into status/performance of ALL targets
  - Lower level – details of alerts for specific group
Managing Alerts

System Dashboard

- Include metrics showing overall health
- To help triage/assign the alert, add operational data using target properties (e.g. Contact, Application Supported, etc.)
- Latest comment for alert is shown. Use this to:
  - Display ticket ID
  - Show alert ownership
More Monitoring Tips in the Appendix

Refer to Appendix for information on additional topics:
- Choosing metrics and thresholds for alerting
- Customizing email to add more operational context
- Practices for setting up notification rules
- Sending alert reminders using repeat notifications
- Escalations through email
- Did my fix resolve the alert?
- Is this old alert still valid?
- Are my targets following my monitoring standards?
- Do I have correct notification coverage for my target's alerts?
- Changing dbsnmp credentials across many databases
Benefits: Enterprise Manager Monitoring
Enabling value through best practices

- Minimal effort to scale as enterprise grows
- Reduce manual tasks
  Improve administrator productivity
- Flexible to meet monitoring and security requirements
- Enables IT to meet service goals
- Standardized approach to monitoring
- Manage More with Less
## Additional Oracle Enterprise Manager Sessions

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00 a.m.</td>
<td><strong>Oracle WebLogic Server Management for Oracle DBAs</strong></td>
<td>• Marriott Marquis, Salon 9</td>
</tr>
<tr>
<td></td>
<td><strong>Enabling Database as a Service Through Agile Self-Service Provisioning</strong></td>
<td>• Moscone S. Room 102</td>
</tr>
<tr>
<td></td>
<td><strong>Reduce TCO with Oracle Application Management Pack for Oracle E-Business Suite</strong></td>
<td>• Moscone W L2, Rm 2024</td>
</tr>
<tr>
<td>10:30 a.m.</td>
<td><strong>Best Practices for Managing Your PeopleSoft Applications</strong></td>
<td>• Marriott Hotel, Golden Gate A</td>
</tr>
<tr>
<td></td>
<td><strong>Oracle Enterprise Manager Grid Control Deployment Best Practices</strong></td>
<td>• Moscone S. Room 102</td>
</tr>
<tr>
<td></td>
<td><strong>Managing Sun SPARC Servers with Oracle Enterprise Manager Ops Center</strong></td>
<td>• Moscone S. Room 252</td>
</tr>
<tr>
<td></td>
<td><strong>Heterogeneous Data Masking: Oracle, SQL Server, and DB2 Database Best Practices</strong></td>
<td>• Moscone S. Room 306</td>
</tr>
<tr>
<td>12:00 p.m.</td>
<td><strong>Scalable Enterprise Data Processing for the Cloud with Oracle Grid Engine</strong></td>
<td>• Moscone S. Room 310</td>
</tr>
<tr>
<td></td>
<td><strong>Spot Problems Before Your Users Call: User Experience Monitoring for Oracle Apps</strong></td>
<td>• Marriott Hotel, Golden Gate A</td>
</tr>
<tr>
<td></td>
<td><strong>Reduce Problem Resolution Time with Oracle Database 11g Diagnostic Framework</strong></td>
<td>• Moscone S. Room 102</td>
</tr>
</tbody>
</table>
## Additional Oracle Enterprise Manager Sessions

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thursday, Sept. 23</td>
<td>1:30 p.m. - Patching Enterprise-wide Databases: Automation Techniques and Real-World Insights</td>
<td>Moscone S. Room 310</td>
</tr>
<tr>
<td></td>
<td>1:30 p.m. - Managing User Experience: Lessons from eBay</td>
<td>Marriott Hotel, Golden Gate A</td>
</tr>
<tr>
<td></td>
<td>1:30 p.m. - Deep Java Diagnostics and Performance Tuning: Expert Tips and Techniques</td>
<td>Marriott Marquis, Salon 9</td>
</tr>
<tr>
<td></td>
<td>1:30 p.m. - Oracle Enterprise Manager Configuration Management Unleashed: Top 10 Expert Tips</td>
<td>Marriott Marquis, Salon 6</td>
</tr>
<tr>
<td></td>
<td>1:30 p.m. - Oracle Enterprise Manager Security Best Practices</td>
<td>Moscone S. Room 102</td>
</tr>
<tr>
<td></td>
<td>3:00 p.m. - The X-Files: Managing the Oracle Exadata and Highly Available Oracle Databases</td>
<td>Moscone S. Room 102</td>
</tr>
<tr>
<td></td>
<td>3:00 p.m. - Monitoring and Diagnosing Oracle RAC Performance with Oracle Enterprise Manager</td>
<td>Moscone S. Room 310</td>
</tr>
</tbody>
</table>
## Oracle Enterprise Manager Hands On Labs

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00 - 10:00 a.m.</td>
<td><strong>Database Performance Diagnostics and Tuning</strong></td>
<td>Marriott Hotel, Salon 12/13, YB Level</td>
</tr>
<tr>
<td>10:30 - 11:30 a.m.</td>
<td><strong>Oracle Fusion Middleware Management</strong></td>
<td>Marriott Hotel, Salon 12/13, YB Level</td>
</tr>
<tr>
<td>DEMO TITLE</td>
<td>LOCATION</td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>---------------------------</td>
<td></td>
</tr>
<tr>
<td>Oracle Real Application Testing: Database Replay</td>
<td>Moscone West</td>
<td></td>
</tr>
<tr>
<td>Oracle Real Application Testing: SQL Performance Analyzer</td>
<td>Moscone West</td>
<td></td>
</tr>
<tr>
<td>Self-Managing Database: Automatic Performance Diagnostics</td>
<td>Moscone West</td>
<td></td>
</tr>
<tr>
<td>Self-Managing Database: Automatic Fault Diagnostics</td>
<td>Moscone West</td>
<td></td>
</tr>
<tr>
<td>Self-Managing Database: Automatic Application and SQL Tuning</td>
<td>Moscone West</td>
<td></td>
</tr>
<tr>
<td>Application Quality Management: Application Testing Suite</td>
<td>Moscone South - S022</td>
<td></td>
</tr>
<tr>
<td>Real User Monitoring with Oracle Enterprise Manager</td>
<td>Moscone South - S021</td>
<td></td>
</tr>
<tr>
<td>Siebel CRM Application Management</td>
<td>Moscone South - S024</td>
<td></td>
</tr>
<tr>
<td>Real User Monitoring with Oracle Enterprise Manager</td>
<td>Moscone West</td>
<td></td>
</tr>
<tr>
<td>Oracle WebLogic Server Management and Java Diagnostics</td>
<td>Moscone West</td>
<td></td>
</tr>
<tr>
<td>SOA Management with Oracle Enterprise Manager</td>
<td>Moscone West</td>
<td></td>
</tr>
<tr>
<td>Oracle Business Transaction Management</td>
<td>Moscone West</td>
<td></td>
</tr>
<tr>
<td>Push Button Provisioning and Patch Automation</td>
<td>Moscone West</td>
<td></td>
</tr>
<tr>
<td>Smart Configuration Management</td>
<td>Moscone West</td>
<td></td>
</tr>
<tr>
<td>Oracle Enterprise Manager Ops Center</td>
<td>Moscone West</td>
<td></td>
</tr>
<tr>
<td>Managing the Enterprise Private Cloud</td>
<td>Moscone West</td>
<td></td>
</tr>
<tr>
<td>System Management, My Oracle Support, and Oracle Enterprise Manager</td>
<td>Moscone West</td>
<td></td>
</tr>
<tr>
<td>Self Managing Database: Change Management for DBAs</td>
<td>Moscone West</td>
<td></td>
</tr>
<tr>
<td>Oracle Enterprise Manager: Complete Datacenter Management</td>
<td>Moscone West</td>
<td></td>
</tr>
<tr>
<td>Self-Managing Database: Data Masking for DBAs</td>
<td>Moscone West</td>
<td></td>
</tr>
</tbody>
</table>
Appendix
Setting up Monitoring: Tips and Traps
Choosing metrics and thresholds for alerting

- Default thresholds may over-alert
  - Some defaults designed for PRODUCTION use cases
  - Use template with adjusted thresholds to apply to DEV and TEST

- Choose metrics for alerting carefully:
  - Time-based metrics superior for performance
  - Base resource consumption (CPU, I/O, Memory)
  - Workload or application-specific metrics or health checks

- Threshold values
  - Use metric history to analyze value ranges
  - Be conservative with critical thresholds:
    - Reserve CRITICAL for high signal of serious problem
Database Performance Metrics

- **#1 Metric: Average Active Sessions**
  - Measures active load on database instance
  - Sudden high spikes usually mean severe performance issue

- **Use Adaptive Thresholds:**
  - Sets thresholds automatically and adjusts for workload cycles
  - Warn at 0.99 significance (measured sample statistic)
  - Critical at 0.9999 significance (estimated high significance value)

- **11g: New Adaptive Thresholds user interface**
  - Supports threshold “what-if” analysis over recent history
  - Organizes metrics into Classes
  - Located under “Baseline Metric Thresholds” in Grid/Database Control
Setting Up Monitoring: Beyond the Basics

Additional tips for setting up notifications

- Customize email format to add more operational context
  - Add target properties (Line of Business, Owner, Contact..) in the email to provide additional operational information
- Practices for setting up Notification Rules
  - Designate users (Senior Administrators) to create rules on behalf of the team
  - Common use cases
    - Rules for production targets different than rules for non-production targets
    - Separate rules by Line-of-Business / team
    - Use naming convention (e.g. include team name in rule)
      - Facilitates searching for rules
Setting Up Monitoring: Beyond the Basics

Additional tips for setting up notifications

• Send alert reminders using Repeat Notifications
  – Set the global defaults to the least frequent interval used and use this in most rules
    • Example: Global setting: Repeat every 30 minutes up to a max of 3 repeats
  – For rules that include important targets or critical alerts, set to higher repeat frequency
    • Example: For target down rule(s): repeat every 5 minutes up to a max of 10 repeats
  – Usage Note: Users need to ‘acknowledge’ the alert in the Enterprise Manager console to stop repeat notifications
    • Remember to provide “Manage Target Alerts” privilege to your operators
Setting Up Monitoring: Beyond the Basics

Additional tips for setting up notifications

- Escalate unattended, important alerts via email
  - Send email to different person (e.g. manager level) if alert is open too long
  - To set up this rule:
    - Create new notification rule and put a ‘duration condition’ associated with the alert
    - Rule action: Send email to the manager
Notification Rule for Alert Escalation via E-mail

In Metrics tab, define duration condition for the alert…
(Apply rule if alert opened > 12 hours and not acknowledged)

.. then in Actions tab, send email to the manager
Managing Alerts: Other Tips

- How do I know if my fix resolved the alert?
  - Use ‘Reevaluate Alert’ feature
  - Alternative to waiting for next metric evaluation
  - Causes the agent to reevaluate the metric alert
  - Current severity will be provided
  - Usage: requires 10.2.0.5 agent or higher
Managing Alerts: Other Tips

- Is this alert still valid?
  - Enterprise Manager does not change the alert triggered date
  - Validation shown in the Console
    - Last Collected Value
    - Last Collected Timestamp
Monitoring: Ongoing Maintenance

- Are my targets still following my monitoring standards?
  - Generate report using *Monitoring Template Comparison* reporting element and/or
  - Use “Compare Settings” feature in Monitoring Templates page
  - Shows differences between monitoring template and target’s settings
Monitoring: Ongoing Maintenance

Report using the Monitoring Template Comparison element

Differences are highlighted
Monitoring: Ongoing Maintenance

- Do I still have correct notification coverage for my target?
  - Notification Rule Coverage report (per target)
  - For each metric contained in a rule:
    - Alert severities covered
    - Rule(s), if any
    - Type of notification
    - Shows alert-able metrics *not* covered in any rule
    - Potential missed notification
What’s the easiest way to change monitoring credentials (e.g. dbsnmp) across many databases?

- EMCLI `update_db_password`
  - Changes password associated with the user in Enterprise Manager and database target
  - Changes the password across all features that use it:
    - Preferred credentials, Corrective Actions, Jobs, User-defined metrics, target monitoring credentials
  - Usage tip: Blackout the target during this operation to avoid metric collection errors due to invalid password
ORACLE IS THE INFORMATION COMPANY