

# Managing Oracle Cloud With Enterprise Manager

## OPERATIONAL MANAGEMENT

ORACLE WHITE PAPER | DECEMBER 2015





## Table of Contents

Executive Summary	2
Operational Management	3
Service Availability Management	3
<b>Availability and Usage Data from Enterprise Manager: Displayed on</b>	
<b>Customer's Cloud Portal</b>	4
<b>Service Dashboards and Incident Management</b>	5
Application Performance Management	10
Cloud Security, Standardization and Risk Management	14
Cloud Operations Automation	16
Enterprise Manager Deployment	18
Conclusion	19
Appendix 1: Glossary of Terms	20
Appendix 2: Cloud Operations Responsibilities within Enterprise Manager	21
Appendix 3: References	23

## Oracle Cloud Operational Summary

**54,000+** Devices  
**700 PB+** Storage



**19** Tier 4 Data Centers  
**New:** Toronto, Frankfurt, Calgary, Munich



**33 Billion+** Transactions/Day



*Managing at scale would not be possible without Oracle Enterprise Manager.*

*Nara Gogineni, Sr. Director, Cloud Operations*

### Executive Summary

Oracle Cloud, the industry's broadest and most integrated public cloud, offers best-in-class services across software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS), and data as a service (DaaS). Enterprise Manager manages and monitors Oracle Cloud to ensure 99.99% availability of Cloud Services.

Enterprise Manager provides an overview of tenant cloud usage, service availability, health of service and service infrastructure on Service Dashboards. It also provides incident and problem management, service life cycle management, gold standards for service configuration, compliance scoring of service/infrastructure vis-à-vis CPU patches and STIG compliance. Additionally operational tasks like management of security certificates and password expiry, monitoring cloud access management and Oracle Cloud service provisioning are automated for Cloud Agility using Enterprise Manager restful APIs and Jython EMCLI. This whitepaper describes how Enterprise Manager 12c, Oracle's flagship Systems and Applications Management product, is being used to provide 24x7 management for the Oracle Cloud. The same

A cloud tenant user gets just a simple portfolio of business application cloud services presented in unified environment providing flexible cloud infrastructure whilst Enterprise Manager obscures the complexity of managing the powerful standards-based cloud platform in 19 worldwide tier 4

architecture and principles can be applied to any private or public cloud that is built with Oracle technology.

## Operational Management

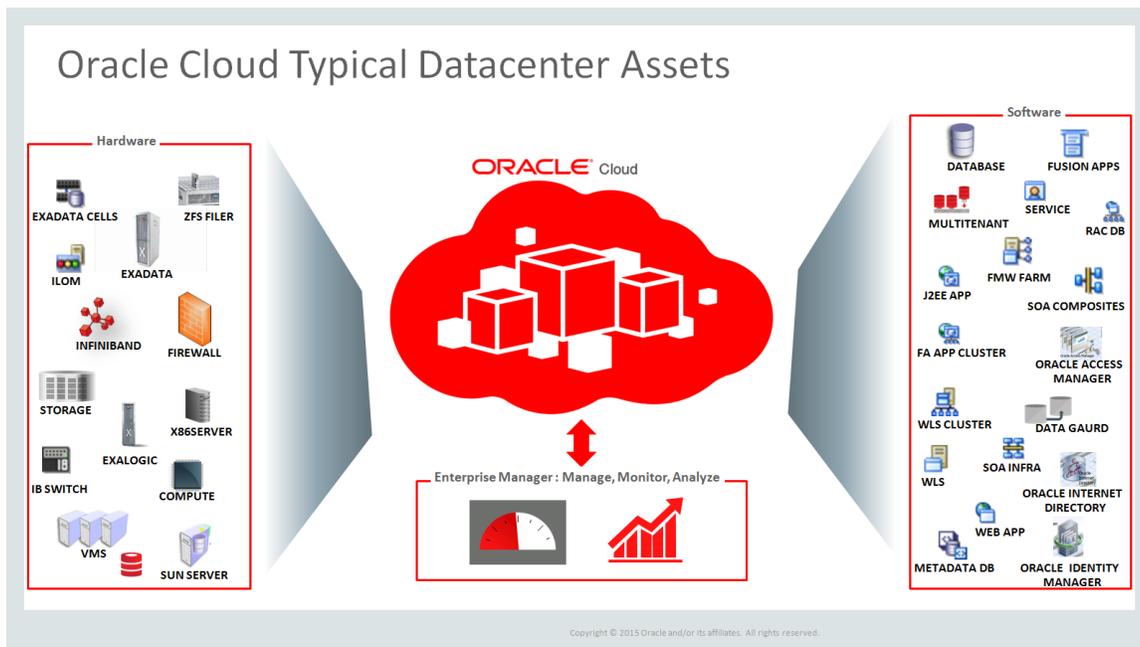
Enterprise Manager has reduced administration and operational management costs by at least 35% for Oracle Cloudops (Cloud Operations team) besides increasing productivity, improving collaboration and simplifying proactive Cloud management. The use of Enterprise Manager in Oracle Cloud management can be briefly categorized as follows:

- » Service Availability Management
- » Application Performance Management
- » Cloud Security, Standardization & Risk Management
- » Cloud Operations Automation

## Service Availability Management

Oracle Cloud Portal shows service status on dashboards via “My Account” pages. The dashboards show uptime and overall outages while displaying a calendar view of service availability. All of this information is provided from Enterprise Manager which monitors the entire cloud infrastructure (Fig 2), including software like J2EE apps, SOA composites, infra DB, FMW clusters, RAC databases and hardware like VMs, storage, filers, engineered systems etc. in addition to all Cloud services.

Fig 2: Oracle Cloud Assets managed by Enterprise Manager



## Availability and Usage Data from Enterprise Manager: Displayed on Customer's Cloud Portal

The current, monthly and yearly usage and availability data for Cloud services is shown to tenants on their Cloud Portal. A planned maintenance window is communicated to Oracle Cloud tenants through Cloud Portal using Enterprise Manager "blackout" functionality. Blackouts (a way to stop monitoring all targets related to services under maintenance) are applied to environments before any service lifecycle management operation (patch, upgrade, or configuration change) is performed on a tenant's service instance. Blackout time periods such as planned maintenance periods, are excluded from service availability metrics. Unplanned outages are shown as Service Incidents.

Fig 3: Oracle Cloud Service Status shown on Service Home Page

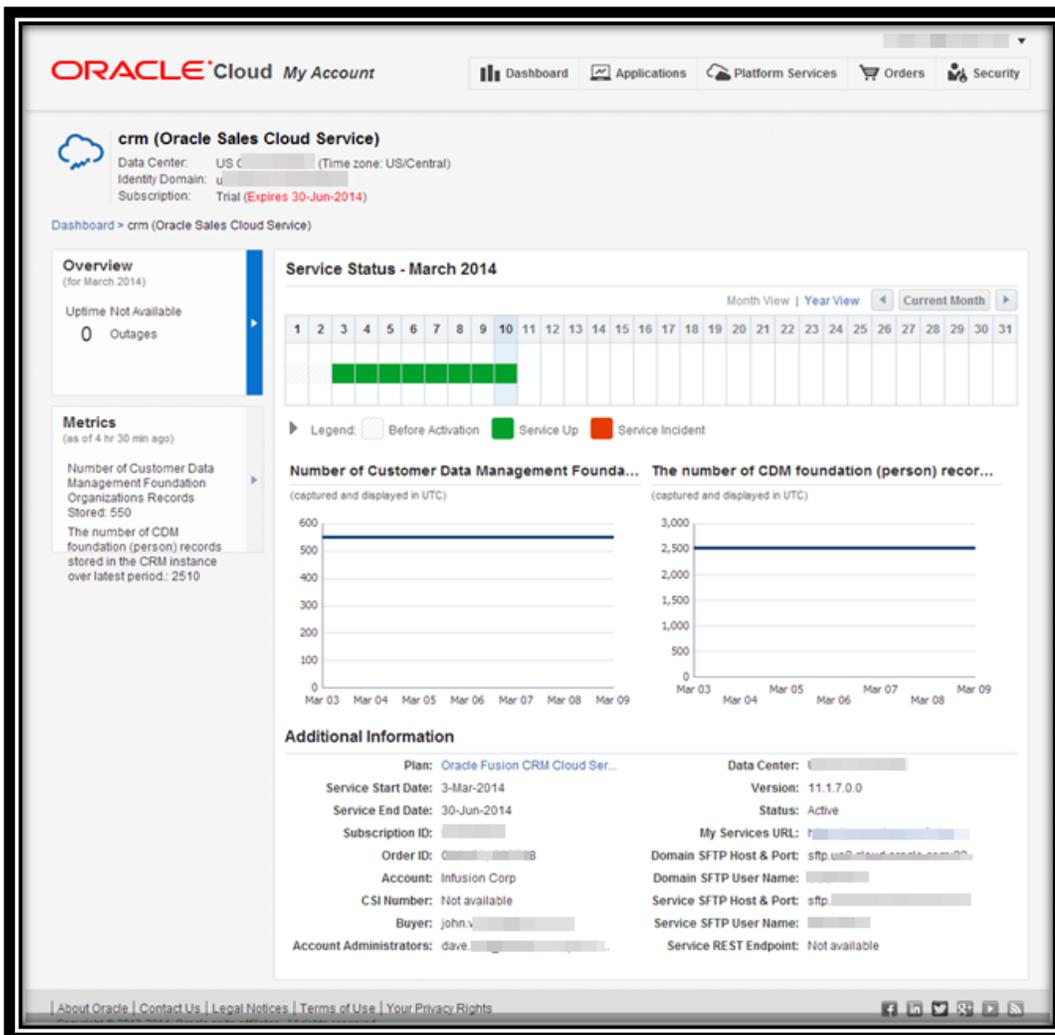
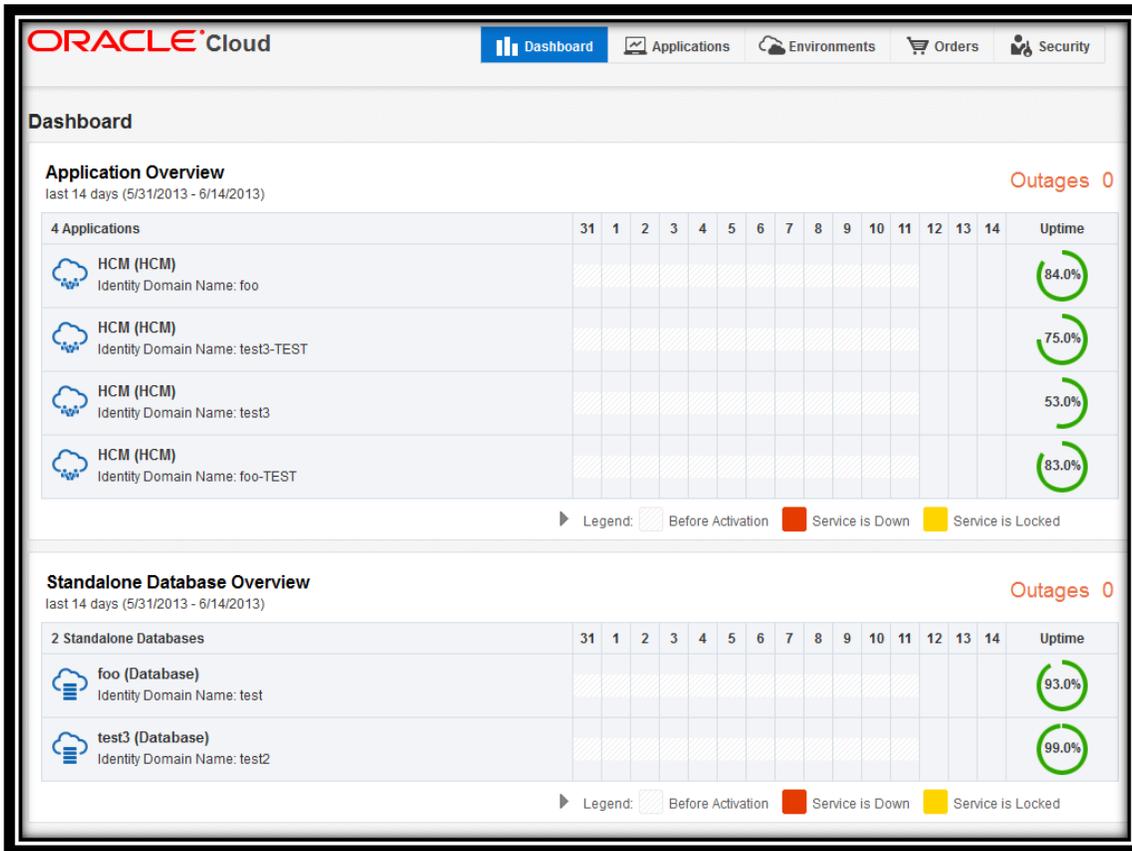


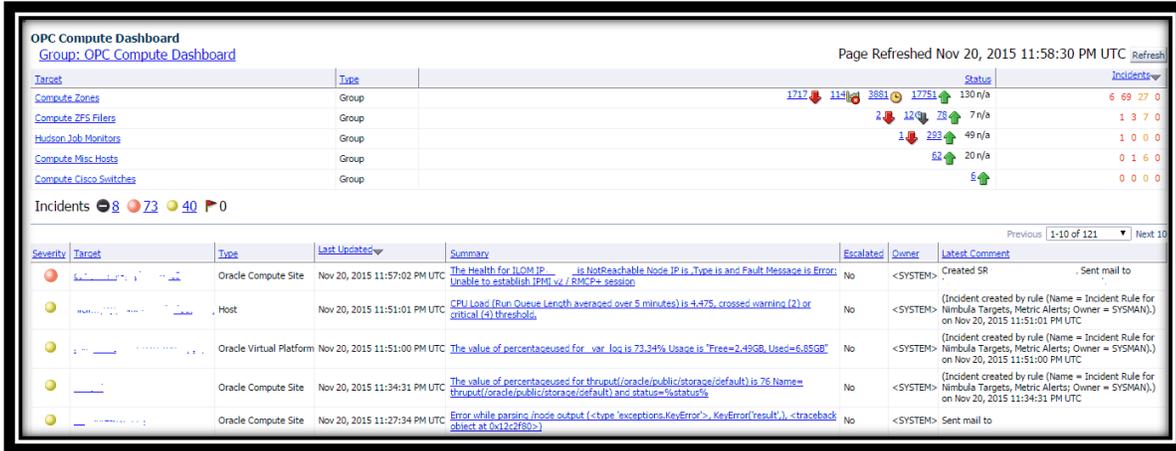
Fig 4: Oracle Cloud Service Availability shown on Service Dashboard



## Service Dashboards and Incident Management

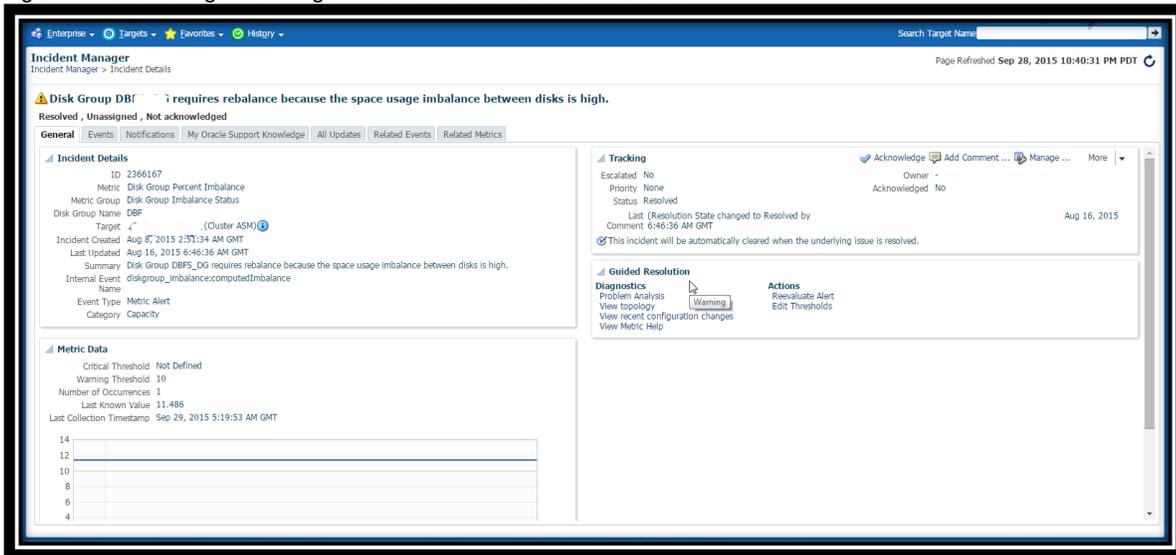
Cloud computing changes the focus to understanding, modeling and monitoring services - not systems - as was with traditional IT. Service Level Management is a key requirement for any Cloud services. All Oracle Cloud Services (SaaS, PaaS, IaaS) are proactively monitored 24x7 by Oracle Cloud Administrators using Enterprise Manager Service and System Dashboards. These dashboards provide a 360 degree view of Cloud services including status, uptime of services, critical incidents on systems that constitute the service, and key performance indicators. Availability status, metric retrieval, service maintenance status (blackout start/stop) and key business metrics on performance and usage are collected by Enterprise Manager and used by Oracle Cloud Operations to proactively manage the health of Cloud services. Service Availability is also checked by Synthetic tests, beacons, which validate Service URLs with login and some key functional flows. The login tests are run at a higher frequency than the functional tests.

Fig 5: Example of Incident Dashboard in Enterprise Manager for Cloud Operations



The Cloud Operations (CloudOps) team manages the infrastructure and application/services incidents using Enterprise Manager Dashboards. Within these dashboards, services are grouped to create logical hierarchies; all incidents within a group are then shown together for ease of management at scale. CloudOps members acknowledge an incident, assign it to themselves and then drill down into incident pages where-in they can triage the issue by reviewing the event that raised the alert, the **metric thresholds** that were exceeded etc. They use guided resolution links to triage/resolve the issue. They can also search the “My Oracle Support Knowledge Base” to find similar issues that other customers may have reported. CloudOps then take the necessary actions to resolve the issue on the system/environment. The alert is closed automatically upon the next test.

Fig 6: Incident Manager showing an Incident and its Guided Resolution



Find Once Fix Many - Oracle CloudOps leverage analysis of same/similar Enterprise Manager Incident's occurrence on multiple Service instances to create problem tickets for root cause analysis. Whether they are WLS errors, J2ee deployment failures, failed web services or Synthetic test failures the root cause is analyzed and problem ticket logged to Service development teams. The fix/resolution is applied to fleet of Service pods in the cloud.

## Incident Rules and Rule-Sets

Several Incident Rules are defined by Enterprise Manager Administrators so appropriate Cloud Ops teams get alerts for the services/targets that they manage. In Oracle Cloud the following notification methods are used:

- Email
- Pager
- Raise a Ticket (Service Request)
- No Notification (Only show in Dashboard)

Based on Incident Severity ie “Fatal”, “Critical”, or “Warning” different notification methods are used. Several incidents are shown in the dashboards only, as the dashboards are proactively managed by “24\*7 Eyes on Dashboard teams”. Oracle Cloud incidents are set up to raise tickets for only Fatal alerts.

Fig 7: Incident Rules Sets - Define notifications for different alert types & severity.

The screenshot shows the 'Incident Rules' configuration page. The breadcrumb is 'Incident Rules > View rule set: Notifications Rule set for SaaS DB Hosts Alerts'. The main heading is 'View rule set: Notifications Rule set for SaaS DB Hosts Alerts'. Under the 'General' tab, the following details are visible:

Description	Co-authors	None	
Enabled	Yes	Created By	SYSMAN
Type	Enterprise	Created On	Jan 23, 2014 4:13:01 PM UTC
Applies To	Targets	Last Updated By	SYSMAN
Owner	SYSMAN	Last Updated On	Mar 23, 2015 7:29:54 PM UTC

Below the details, there are tabs for 'Targets' and 'Rules'. The 'Rules' tab is active, showing a list of rules. The instructions say 'Select a rule and click "View" button to view details.' There are two rules listed:

Name	Description	Applies To	Action Summary
Metric Alerts	Metric Alerts	Specific Metric Alert events that match ... <ul style="list-style-type: none"><li>• Severity In (Critical;Warning)</li></ul>	<ul style="list-style-type: none"><li>• Call Autoticketing (Helpcenter/MOS)</li><li>• Create Incident</li></ul>
u02 Filesystem Alert	u02 Filesystem Alert	Specific Metric Alert events	<ul style="list-style-type: none"><li>• Call Autoticketing (Helpcenter/MOS)</li><li>• Create Incident</li></ul>

Above is an example of an Incident Rule set for “SaaS DB Host Alerts”. It has a couple of rules defined within it that indicate what to do when an alert is raised, and specifically what action to perform when a particular filesystem alert is raised.

Fig 8 below is an example of an Incident Rule definition. This is the “Availability” Rule in FA SaaS targets Rule Set.

Fig 9 shows some of the Incident Rule Sets – groups of rules - that Oracle Cloud has configured. In order to standardize on a few set of rules and not have an unmanageable number, the following process was adopted:

- » Create Rules based on Target Type - These rules can be shared across services using the same target type
- » Create Rule-Sets based on Service Type – These rules combine pre-existing rules
- » Exception - Create Rule-Sets based on Teams/notification method – If 1 and 2 don't meet the requirements and this is absolutely needed then create this.

Fig 8: Incident Rule - Define notifications for database Target type & different severities.

The screenshot shows the configuration page for an Incident Rule named 'Database Availability' under the 'Naming Standard' category. The breadcrumb trail is 'Incident Rules > View rule set : Notifications Rule set for SaaS FA targets > Availability'. The rule is currently 'Broken'.

**General Information:**

- Description: Database Availability rule
- Created On: May 9, 2013 4:09:51 AM UTC
- Created By: SYSMAN
- Enabled: Yes
- Broken: No
- Last Updated By: SYSMAN
- Last Updated On: Jun 23, 2015 8:00 AM UTC
- Type: Events

**Selected Events:**

All Target Availability events that match the following conditions:

- Target type In (Database Instance;Listener;Cluster Database)
- Severity In (Clear;Critical;Fatal)

Red arrows point from the text 'Criteria' to these two conditions.

**Actions:**

Order	Condition Summary	Action Summary
1	No additional condition specified	<ul style="list-style-type: none"> <li>Call Autoticketing (Helpcenter/MOS)</li> <li>Create Incident</li> </ul>

A red box highlights the 'Action Summary' column, with a label 'Notification Method' pointing to it.

Fig 9: Some Incident RuleSets defined at Oracle Cloud

The screenshot shows a list of Incident Rules in Oracle Enterprise Manager. The table below represents the data shown in the screenshot.

Name	Description	Order	Enabled
Incident management rule set for all targets	Rule set to create and manage incidents for all targets	1	Yes
Event Management Rule set for Self Update	Rule set to manage Self Update events.	2	No
rbrinega test		3	No
Notifications Rule set for SaaS FA targets	Notifications Rule set for SaaS targets	4	Yes
Notifications Rule set for PaaS targets	Notifications Rule set for PaaS targets to send Emails	5	Yes
Notifications Rule set for IDM SaaS targets	Notifications Rule set for IDM SaaS targets	6	Yes
Notifications Rule set for IDM PaaS targets	Notifications Rule set for IDM PaaS targets	7	Yes
Notifications Rule set for PaaS targets (Java Service)	Notifications Rule set for PaaS targets (Java Service)	8	No
Notifications Rule set for PaaS targets (stage)	Notifications Rule set for PaaS targets to send Emails	9	Yes
Notifications Rule set for Infra team	Notification Rules for Infra team which covers Server, Storage & Network	10	Yes
Auto SR Ruleset For Availability Issues	Incident level Auto SR Ruleset	11	No
Social Cloud Hosts	DevOps Rules for Social Cloud Hosts	13	Yes
Social Cloud CI Application Events	E-mail CI Teams on application events	14	Yes
Social Cloud CI Database Host Events	E-mail CI Database Team on application events	15	Yes
Global /oem Filesystem monitoring	/oem file system monitoring	16	Yes
cloudem-ops-additional-monitoring		17	Yes
Notifications Rule set for SaaS DB Hosts Alerts		18	Yes
Social Cloud Involver Host Events	Involver environment host alerts.	19	No
Auto SR Ruleset	Ruleset to automatically create/update service requests for prod	20	No
Notification Rule Set for PaaS Storage Targets	Notification Rule Set for PaaS Storage Targets	21	Yes

## Monitoring Templates

Oracle Cloud uses monitoring templates extensively to standardize monitoring of key-metrics for each target type. Several Oracle-certified templates are shipped out of the box (see Fig 10). Oracle Cloud has made copies of these templates and edited them to add/remove metric so the alerts are relevant and key to Oracle Cloud's business.

Fig 10: Example of some Oracle Certified Templates that can be used as-is or edited for business metric thresholds

Name	Target Type	Owner	Status			Description
			Pending	Succeeded	Aborted	
Default template for Database Instance	Database Instance	NGOGINEN	0	0	0	Default template for Database Instance
Oracle Certified - Default thresholds for Streams/XS Database Instance	Database Instance	SYSMAN	0	0	0	This template enables streams metric collections and
Oracle Certified - Disable AQ Metrics for SI Databas Database Instance	Database Instance	SYSMAN	0	0	0	This template disables AQ metric collection.
Oracle Certified - Disable Database Usage Tracking Database Instance	Database Instance	SYSMAN	0	0	0	Use this Oracle Certified template to disable the colle
Oracle Certified - Disable Streams/XStream/GG Metr Database Instance	Database Instance	SYSMAN	0	0	0	This template disables streams metric collection
Oracle Certified - Enable AQ Metrics for SI Databasi Database Instance	Database Instance	SYSMAN	0	0	0	This template enables AQ metric collection
Oracle Certified - Enable Database Usage Tracking I Database Instance	Database Instance	SYSMAN	0	0	0	Use this Oracle Certified template to enable the colle
Oracle Certified - Enable Database Usage Tracking I Database Instance	Database Instance	SYSMAN	0	0	0	Use this Oracle Certified template to enable the colle
Oracle Certified - Enable Streams/XStream/GG Metr Database Instance	Database Instance	SYSMAN	0	0	0	This template enables streams metric collection
Oracle Certified-Disable Database Security Configur Database Instance	Database Instance	SYSMAN	0	0	0	Use this Oracle Certified template to disable Security Compliance Standards, Security Reports and in Data
Oracle Certified-Enable Database Security Configur Database Instance	Database Instance	SYSMAN	0	0	0	Use this Oracle Certified template to enable Security Compliance Standards, Security Reports and in Data
Oracle Certified: Disable Database Storage Configur Database Instance	Database Instance	SYSMAN	0	0	0	Use this Oracle Certified template to disable Storage Compliance Standards
Oracle Certified: Enable Database Storage Configur Database Instance	Database Instance	SYSMAN	0	0	0	Use this Oracle Certified template to enable Storage Compliance Standards

## Groups to Manage the Millions of Infrastructure components

In Enterprise Manager Users can define groups of the following types – Dynamic, Regular and Admin. Oracle Cloud uses Dynamic and Regular groups extensively to manage millions of infrastructure components, applications and services. The chart below shows how Oracle Cloud's management tasks are easily performed using Enterprise Manager Groups.

Management Tasks	Oracle Cloud Grouping
Monitoring, Notification	Apply monitoring templates to groups based on target type, Or groups based on target type and a Service
Problem Analysis	Dynamic groups Ex : Target type=pod and Group=PaaS Target type=PBCS Service, lifecycle status=prod

Compliance	Group of databases of SaaS Service
Reporting	Group of groups for executive reports
Dashboards	Group of all targets of a particular service
Service Maintenance	Maintenance window patching of multiple services and blackouts, Patching selective group of hosts, Patching selective group of Agents
Jobs	Selective group of hosts, group of databases used to perform shell or sql jobs on

Most Oracle Cloud Dashboards and Reports are based on “Groups of Services” or “Groups of Groups of Services”.

## Application Performance Management

Oracle Cloud teams rely on Enterprise Manager for troubleshooting issues with Cloud services. From analyzing performance issues in the application or techstack to capturing diagnostic dumps, Oracle Cloud support and operations users use Enterprise Manager with personalized home pages. Fig 11 to 14 show some of the popular home pages that Oracle Cloud ops teams use.

Fig 11: Oracle Cluster Database Home Page

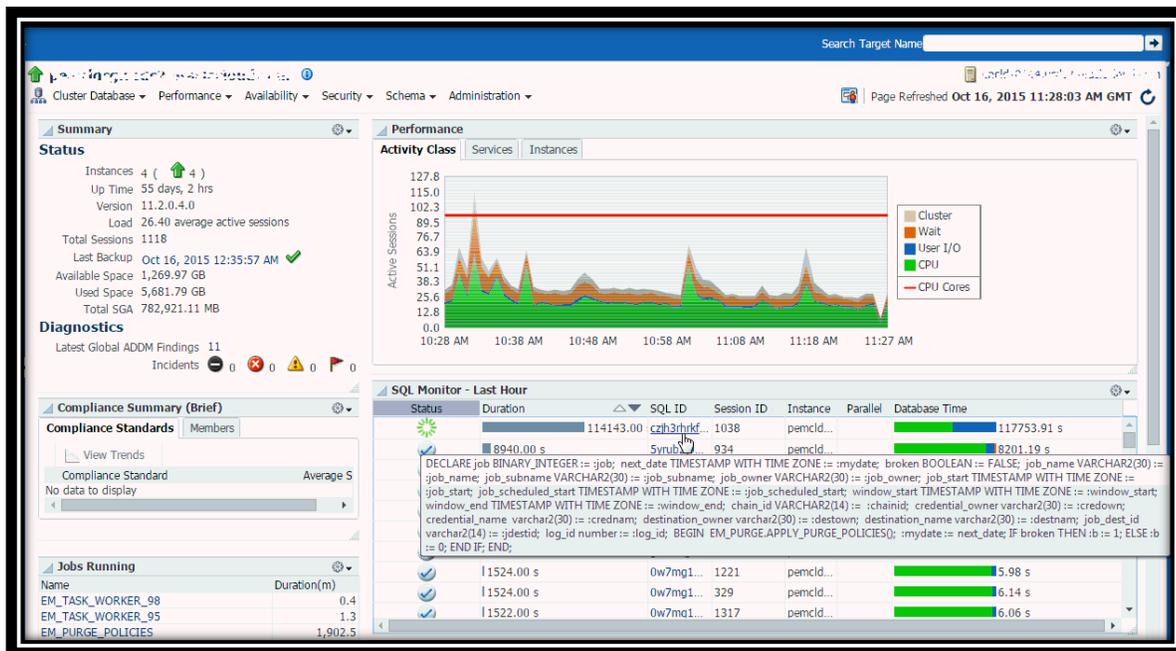


Fig 12: Oracle Fusion Middleware Home Page

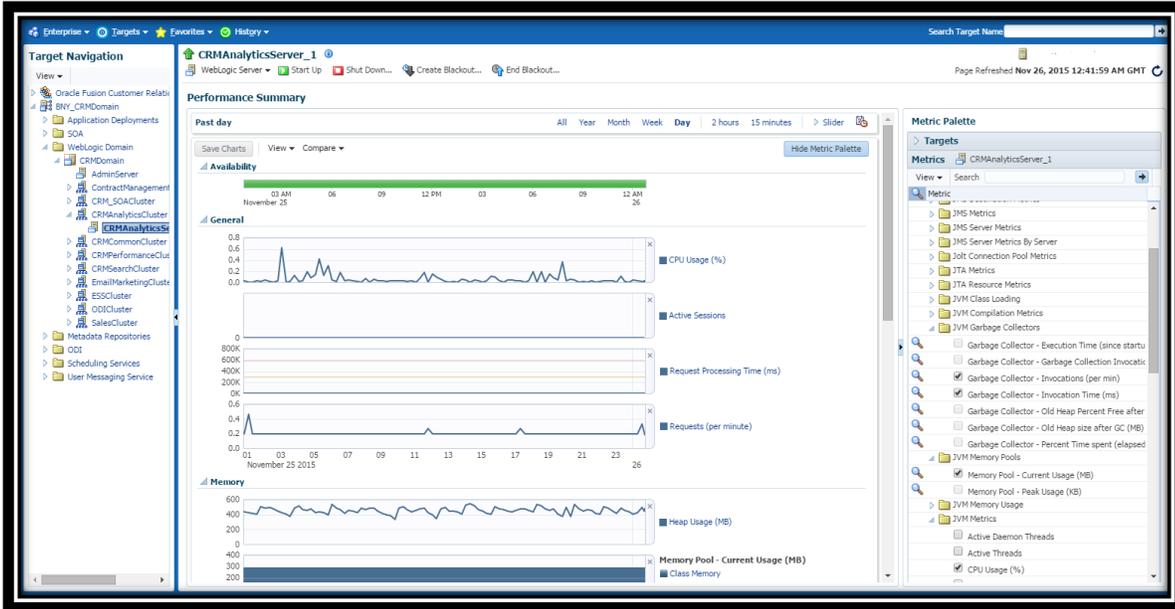


Fig 13: Oracle Fusion Applications Home Page

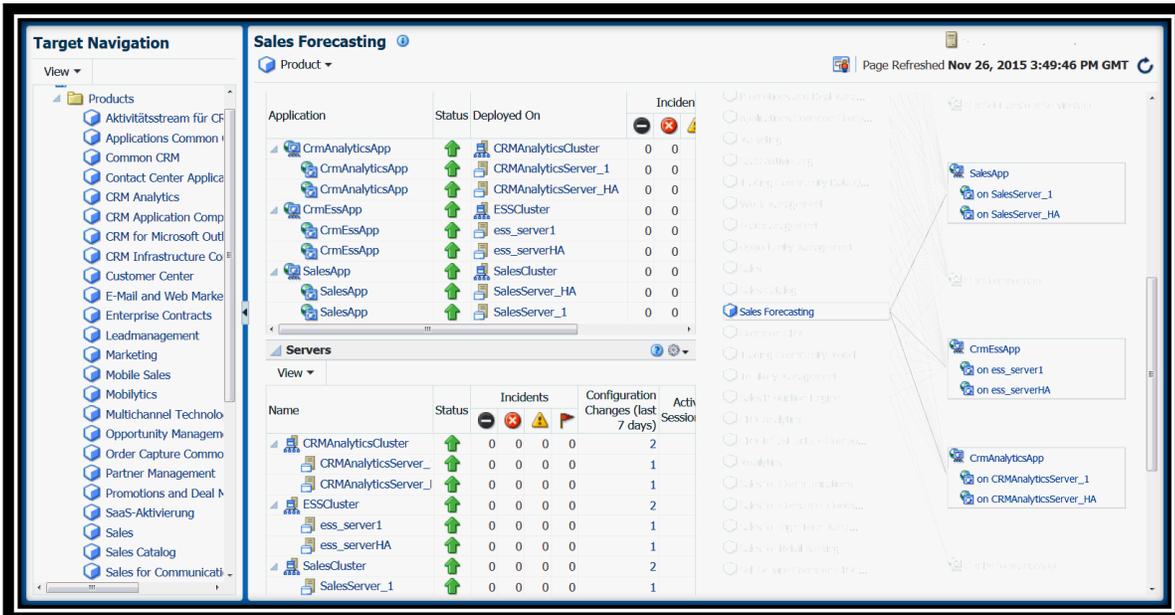
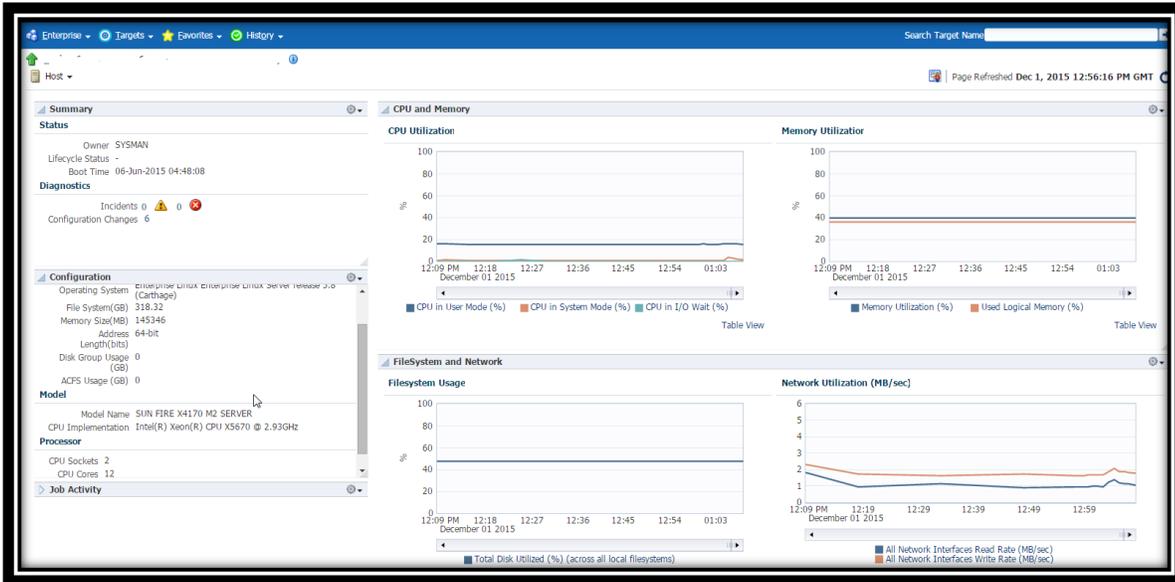


Fig 14: Host Home Page



Using JVM Diagnostics (JVMD) Cloud operations users drill into problems such as stuck threads and thread locks and do deeper analysis to identify which Java method is stuck in the thread stack, or which database-SQL threads are stuck on in the case of database wait events. They can perform live thread analysis as the problem is happening, or analyze the trace JVM activity for a particular point in time (from historical monitored data). With JVMD CloudOps users establish cross-tier correlation between JVMD and Database Diagnostics. Administrators can drill down from a JVM thread in a DB Wait State to the associated Oracle database session (Fig 15), or reverse drill up from the SQL query to the associated JVM and related WebLogic Server targets.

Fig 15: JVM Diagnostics Home Page

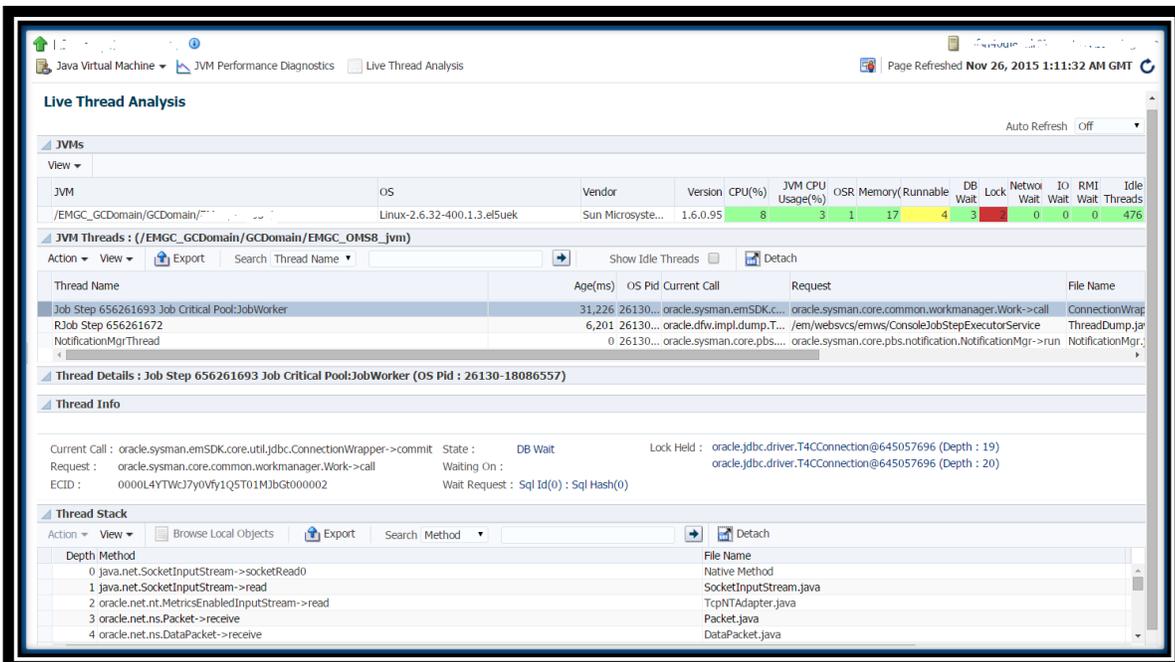
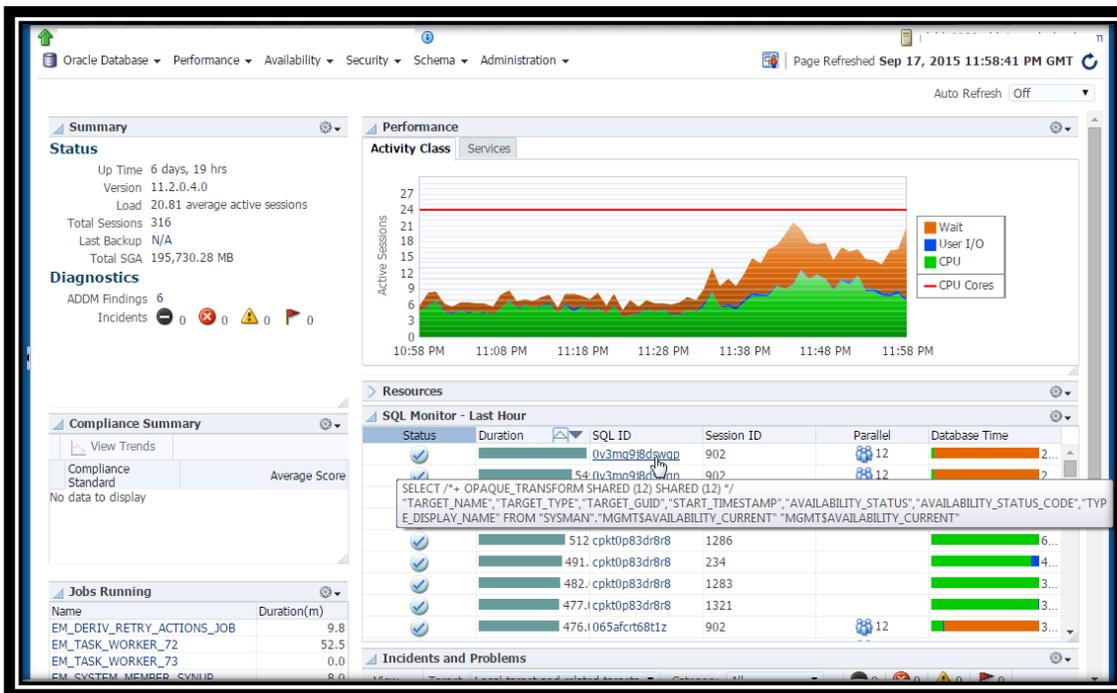


Fig 15 to 17 show how from analyzing memory usage and memory release patterns between garbage collections to identifying the java method/sql that is causing the anomaly, CloudOps users can identify performance issues and better develop plans for optimized performance. Generating Diagnostic Snapshots (Fig 16) also enables teams to gather all relevant diagnostic details for poor-performing services to share with development teams. Tuning the heap size for a service instance is performed using similar analysis.

Fig 16: JVM Threads State on a 24 hour timescale



Fig 17: Database Wait and Sql-Session details with ability to drill down to tune sql execution plan



## Cloud Security, Standardization and Risk Management

Oracle Cloud operations use Enterprise Manager to mitigate risk in the Oracle Cloud by:

- » Standardizing on templates, roles, credentials and notification rules
- » Automating provisioning/operational flows for Cloud services
- » Controlled access and secure install
- » Compliance dashboards/reporting and managing compliance scores
- » Configuration drift checks

Oracle Cloud monitoring is standardized using out of the box Oracle-certified monitoring templates for different infrastructure types. Cloud Enterprise Manager Administrators update/edit these templates per Oracle Cloud requirements for new monitoring metrics and/or custom monitoring metrics (metric extensions). For example, all Cloud services host, storage and database instances are monitored with the same monitoring templates.

Compliance standards/rules are also added to the templates and applied to each new service target. Compliance rules are enabled to mitigate risks against security breaches that often happen owing to faulty configuration such as default passwords, relaxed file permissions, or an open port. CloudOps teams review compliance scores and compliance dashboards, and plan maintenance activities to ensure patch compliance for all service components (Fig 18-20).

Fig 18: Compliance Summary for Oracle Cloud Services

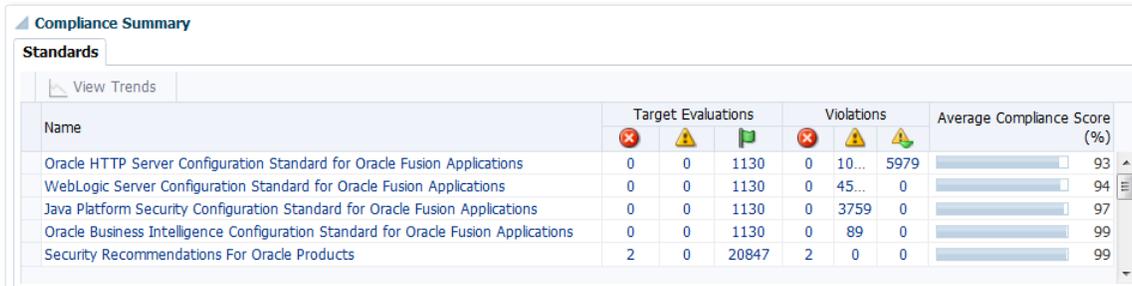


Fig 19: Custom Compliance Standards defined by CloudOps

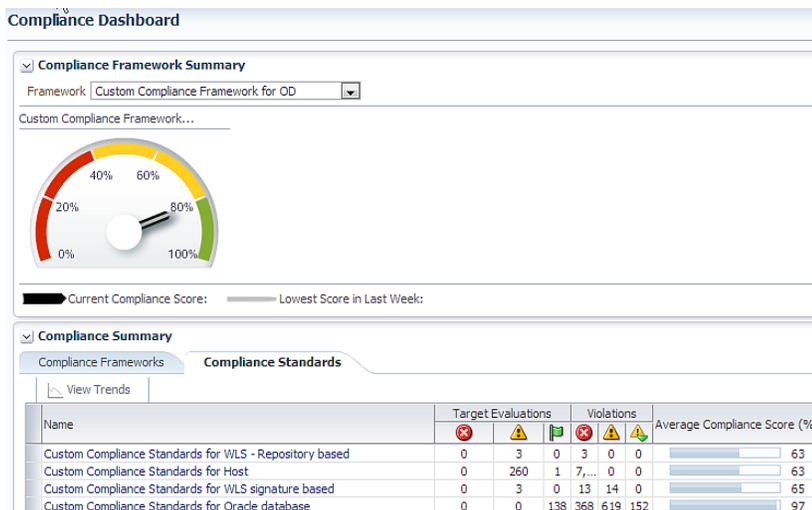
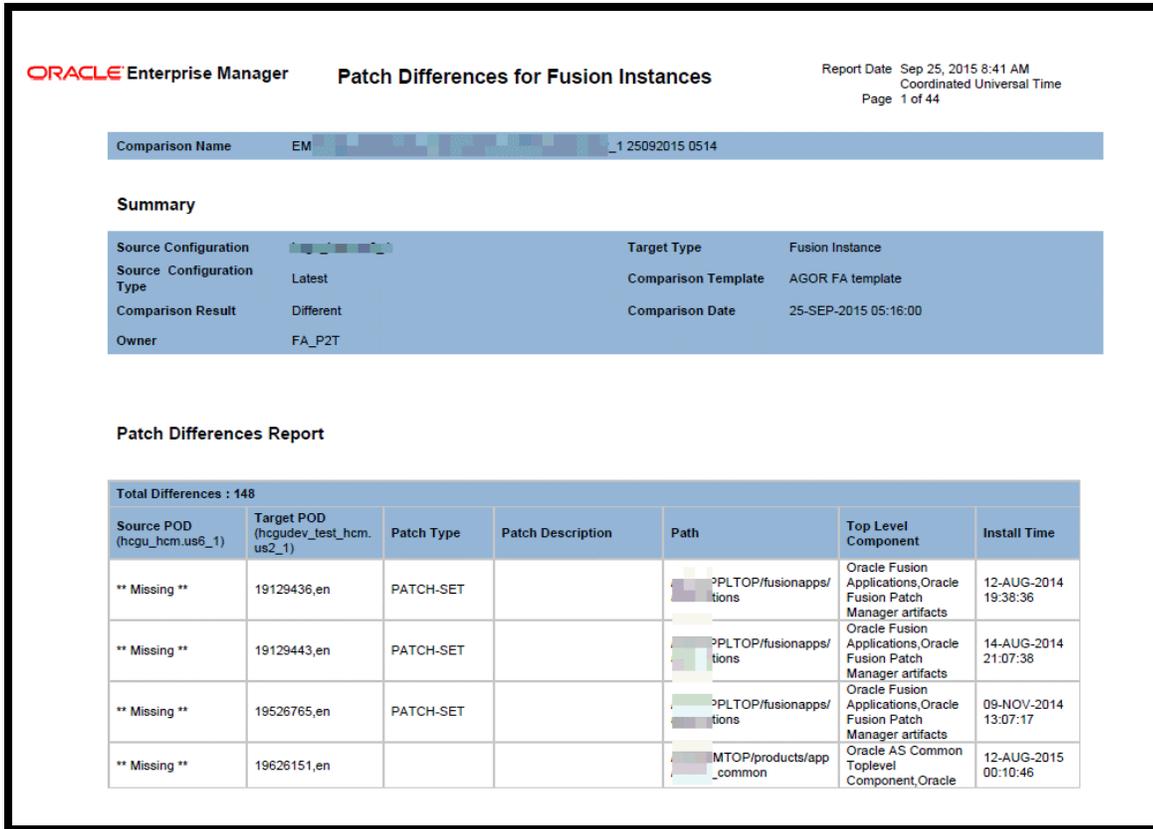


Fig 20: Report of Patch Compare of a Tenant Pod with Gold Baseline



Changes to configurations, files and file attributes across the IT infrastructure are common, but the few that impact file or configuration integrity are often hidden within a large volume of daily changes. These changes can reduce security posture and in some cases may be leading indicators of a breach in progress. Some of the values monitored for unexpected changes to files or configuration items include:

- » Credentials
- » Privileges and security settings
- » Content
- » Core attributes and size
- » Hash values
- » Configuration values

Access to Enterprise Manager is managed by authenticating against corporate LDAP servers with single-sign-on. No local accounts are created in Enterprise Manager. Roles have been pre-created for different user categories by assigning only necessary fine-grained privileges. The roles are marked external and get authorized externally in corporate Oracle Identity Management (IDM). Named Credentials are used to delegate access to Service targets. Enterprise Manager is installed and configured to use custom certificates.

## Cloud Operations Automation

Cloud Devops leverage Enterprise Manager to automate several Cloud Operations Management tasks for Cloud agility, predictability and reliability. Cloud services provisioning flows and maintenance tasks have been automated to ensure best and secure practices/steps are followed.

Some of the Enterprise Manager extensibility features like metric extensions, custom plug-ins, service beacons, custom configurations, custom compliance rules, jobs, deployment procedures, EMCLI commands and Rest APIs are used by Devops to automate Cloud operation tasks like those shown in (Fig 21)

- » Automated Cloud inventory and asset management
- » Scheduled backups and periodic purges
- » Management of scheduled downtime through blackouts
- » Data promotion from test to production instance
- » Compliance and security policy management
- » Fleet certificate management
- » Service health checks post Service maintenance

Fig 21: Example of Some Cloud Operation tasks using Enterprise Manager

<b>Custom Jobs, MEs created to automate Cloud Maintenance Workflows</b>	
Service Provisioning in EM	FA Post Provisioning tasks
FA Prod to Test	Tenant User Management
FA System Accounts Management	Certificates Monitoring & Renewal
FA DR Procedure	FA Health Checks
FA DR DB replication	Import User Sql Job
FA Pod Certification DP	LCM Purge
PBCS Daily Diagnostics	OID Check accounts
PBCS Restart Services	PBCS Health check
Check Root Access	RMAN Run for FA
Check Space Fleet (ZFS)	Patchset Upgrade

Fig 22 shows some examples of Cloud business reports created for line managers. These reports contain custom business metrics defined as metric extensions (ME) in Enterprise Manager. Some of the MEs that Devops have created are track certificate expiry of SaaS and PaaS fleet instances; monitor LDAP bind check; account expiration monitoring for SaaS instances accounts; monitor send mail queue; and log filtering.

**Business Report on pulse of Shared IDM For Devops Line-Management**

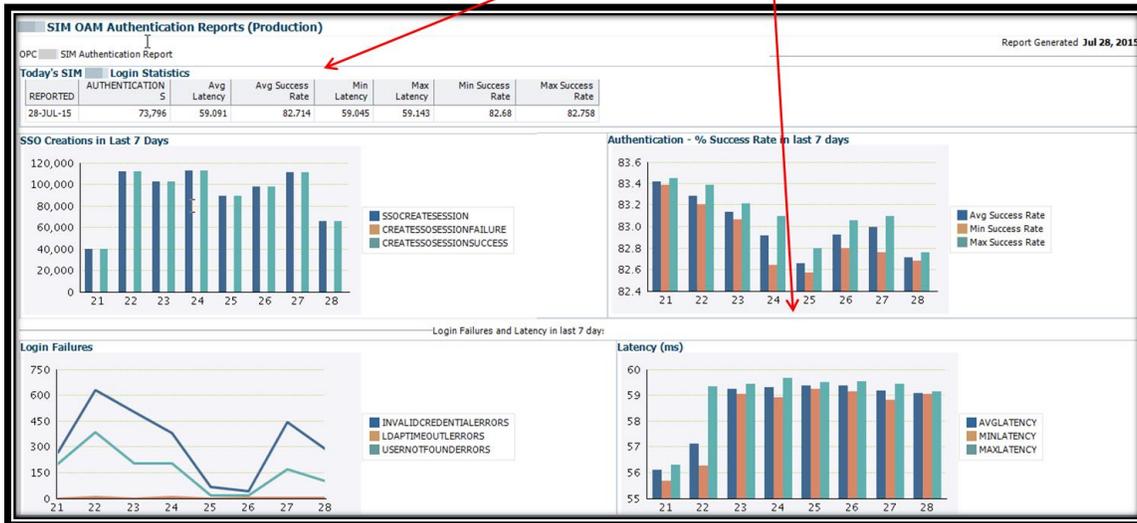


Fig 22: Reports based off of Custom Business Metric defined by Cloud DevOps

All Cloud services create a monitoring metadata plug-in in Enterprise Manager to define their business metrics as part of the onboarding process. Fig 23 shows an example of several tasks that have been automated for the service provisioning flow for all Cloud services scripted using EMCLI Jython commands.

Fig 23: Automation Example: Service Provisioning

**SERVICE: PRIMARY SITE SETUP FLOW**

- 1 •Create VMs
- 2 •Deploy Agents on VMs
- 3 •Discover and Promote Targets
- 4 •Set Global Target Properties
- 5 •Set Monitoring Templates
- 6 •Set Compliance Standards
- 7 •Create Beacons
- 8 •Register with External Systems

**SERVICE: SECONDARY SITE SETUP FLOW**

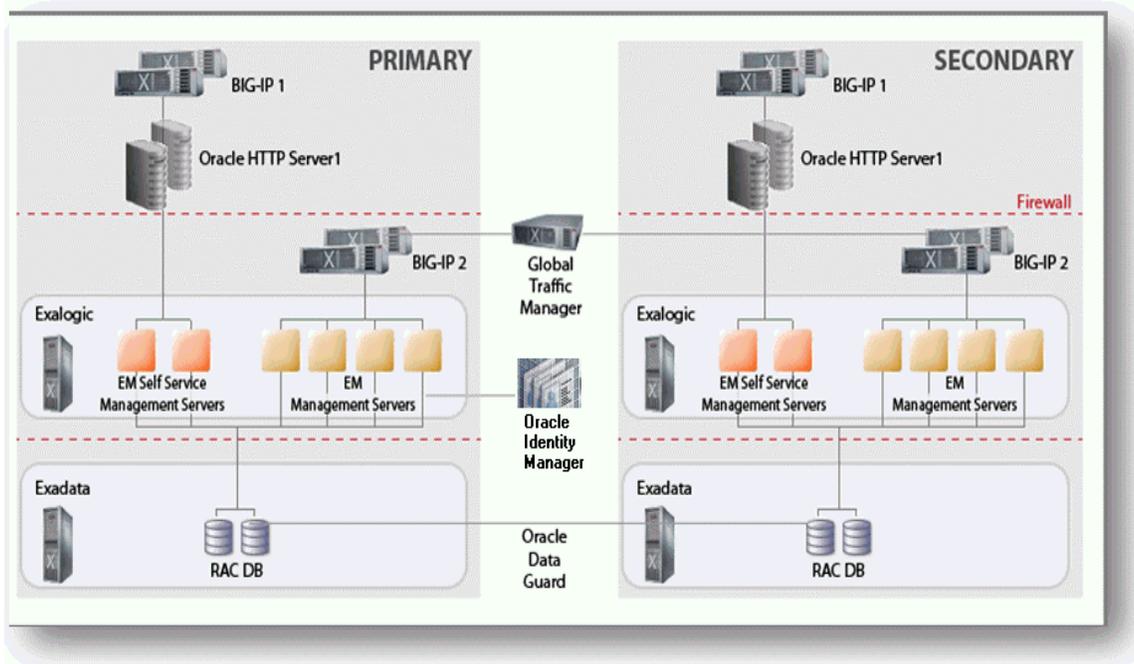
- 1 •Create VMs
- 2 •Deploy Agents on VMs
- 3 •Siteguard - DR Orchestration
- 4 •Configure DB-DataGaurd
- 5 •Application: Storage Replication
- 6 •Discover and Promote Targets
- 7 •Set Monitoring Templates
- 8 •Set Compliance Standards
- 9 •Set in Blackout
- 10 •Register with External Systems

## Enterprise Manager Deployment

Enterprise Manager is deployed into Oracle Cloud in a secure, scalable and fault tolerant architecture, with firewalls between the Oracle Management Repository (OMR), Oracle Management Server and Management Agent layers. Multiple OMS instances (6) load balance traffic and also provide high availability. Each OMS instance runs on an Exalogic compute node. A highly available 4-node RAC database running on Exadata serves as the OMR.

Management Agents deployed to all Oracle Cloud infrastructure components (Exadata servers, Exalogic servers, Oracle VM, ZFS storage, Infiniband, network, BigIP, Linux and Solaris servers, IDM, OAM and OHS servers) monitor the infrastructure and all service components.

Fig 24: Typical Deployment of Enterprise Manager at Oracle Cloud



- » Current versions Enterprise Manager 12.1.0.5 RDBMS 11.2.0.4
- » Exadata: X4-2 (2\*16) 32CPU thread, 240G RAM for Enterprise Manager repository
- » Enterprise Manager Repository: 6.5TB, FRA 11T(3way redundancy)
- » OMS : SUN FIRE X4170 M2 (2\*12) 24 Core, 140G, 700G disk for shared library
  - » Repository Backups
    - RMAN. daily incremental and level0 (fullbackup) on every Sunday. Plus archivelog backups for every 2 hrs to free up space in Flash (reco DG)
    - Backup copied from ASM to NFS. One week backups on ASM and on NFS, and 15days backups on tape
    - FRA ~11T. Guaranteed Restore points (GRP) used during Upgrades/Maintenance
  - » OMS Backups
    - Binary Install, Software Library, EMKey \$ORACLE\_HOME/sysman/config/emkey.ora
    - OMS Configuration from all OMSes \*\* Before and After every maintenance \$ORACLE\_HOME/bin/emctl exportconfig oms
  - » Agent Backups

- Recoverable from the OMS. Backup emd.properties file for changes.

Enterprise Manager also gathers monitoring data by sniffing traffic flowing into Oracle Cloud. This functionality uses a network tap that allows for data collection without imposing any overhead on the user transactions. Real User Experience Insight (RUEI) provides this real user traffic analysis, enabling Enterprise Manager to generate proactive alerts for customer experience performance anomalies for SaaS or PaaS services.

In Oracle Cloud, the monitoring framework has to manage thousands of servers, applications, databases and middleware instances and integrate with the Cloud ecosystems. Enterprise Manager at Oracle Cloud is architected for Cloud-class scale and agility and integrated with Oracle Access Manager (OAM) and Identity Management (IDM) systems for security.

## Conclusion

---

*Oracle Cloud is efficiently managed by Enterprise Manager which provides complete, integrated and business-driven enterprise cloud management solution. Enterprise Manager scales to manage:*

*Thousands of concurrent self-service users*

*Tens of thousands of tenants, 25 million cloud users*

*Hundreds of thousands Service Instances*

*7 Million+ Infrastructure targets*

*2 Million + automation job executions per day*

*11 Million+ Synthetic tests per day*

*3 Million+ events processed/day*

*Tens of thousands of Compliance Evaluations per day*

*Five-Nine (99.999%) availability*

*Full disaster recovery*

---

## Appendix 1: Glossary of Terms

- » Oracle Management Agent (OMA): A lightweight Java-based component that is deployed on each monitored host. It is responsible for managing and monitoring all the service components running on those hosts, communicating and uploading service health and other vital metric data to the Oracle Management Service. Agents also perform operations against the service components (targets) as fixit jobs, scheduled jobs or tasks by Oracle Cloud Operations staff.
- » Targets: These are service components (hardware infrastructure, software infrastructure, SOA applications, J2EE applications). Each target is a unit that can be monitored and managed individually. There are many different types of targets that Cloud Control can manage including Host, Database, Listener, ASM, WebLogic Server, Service Bus, SOA applications, J2EE applications, E-Business Suite, Seibel, Exadata, Exalogic, VMs, OVM and Fusion Applications.
- » Oracle Management Service (OMS): A Web-based application that orchestrates with the Management Agents and the Management Plug-ins to discover service components (targets), monitor and manage targets, and store the collected information in the Management Repository for future reference and analysis. OMS also renders the user interface for Enterprise Manager Cloud Control and the Java Console.
- » Oracle Management Repository (Repository, OMR) – The Oracle Management Repository is used as a persistent data store. Examples of the information stored in the repository include user information, job definitions, monitoring and alerting settings and all configuration and monitoring data related to targets. Scheduled database jobs aggregate and analyze the information collected by the Management Agents and uploaded to the repository.
- » Oracle Software Library – The software library is a file system repository that stores software entities such as software patches, virtual appliance images, reference gold images, application software, and their associated directive scripts. The software library is accessed by the OMS and is used extensively by the Cloud Control framework for features such as self-update and agent-push.
- » Console – The console is a browser-based Web application that is the main user interface for Cloud Control. This console allows the administrator to monitor, manage and report on the Cloud Control targets that have been setup.
- » Enterprise Manager Command Line Interface (EMCLI) – EMCLI allows users to access Cloud Control functionality either interactively from a command line, or as part of a script. This allows Cloud Control operations to be integrated with complex business processes without user interaction.
- » RestAPI – Restful interface for external system integrations (examples Availability, Blackout, Job submission)
- » CloudOps – Oracle Cloud teams that are managing Cloud Services Operations
- » Cloud Support – Oracle Cloud teams working on Customer reported issues through Service Requests in My Oracle Support.
- » Target – An entity that can be monitored /managed. It can be an infrastructure, techstack or application layer component.
- » Enterprise Manager gathers 2 sets of data statistics of a target.
  - Metric: Interesting aspect that helps establish the business health and availability of a target. Different metric are captured at varying frequency (from a minute to several hours).
  - Configuration Data: Interesting informational aspects that are useful to define the signature of the target and any changes on it. This is captured once in 24 hours

## Appendix 2: Cloud Operations Responsibilities within Enterprise Manager

The Cloud Operations Enterprise Management team consists of members located around the globe. This allows for “follow the sun” coverage 24 hrs a day, 365 days a year. Each region’s team members are on call during their work day and responsible for taking Severity 1(S1) Enterprise Manager Alerts and addressing issues via the standard support queue. Like any operations team, weekdays and weekend duties are scheduled in a Monthly Operations Roster.

**On-Call Responsibilities:** The on call person is responsible for the following specific to ensuring Enterprise Manager is healthy and available during their rotation:

- » Metric collection clean up
- » Remove decommissioned targets
- » Apply/Audit Template apply to production targets
- » Clean up Security Policy violations
- » Promote new targets (databases, Exadata, Exalogic etc) via service requests
- » Review and address Alerts in the console and work with target owners to clear
- » Review and work with Job owners to clean up all broken jobs (removing if applicable)
- » Ensure all Agents are Up and uploading data
- » Ensure all Enterprise Manager DBMS processes are running successfully and within threshold
- » Create accounts for Cloud Operations and Cloud Support
- » Manage Enterprise Manager site backup
- » Ensure Cloud Enterprise Manager executive dashboards are accessible
- » Ensure Cloud Enterprise Manager interfaces with other Cloud eco-systems like TAS, SDI, MOS are operational
- » From an on-call queue perspective, the Enterprise Manager team member would be responsible for ensuring that the queue is clean, all SRs are updated and SRs are closed in a timely fashion.

**Oracle Cloud Enterprise Manager Team Responsibilities:** Oracle Cloud Enterprise Manager Team manages and maintains the following:

- » Oracle Management Server – The Cloud Enterprise Manager team is solely responsible for applying patches to the OMR database and the OMS mid-tiers. As well, no team members outside of the Enterprise Manager team are permitted to start or stop any component of the Enterprise Manager infrastructure. This also includes adjusting of OMS parameters.
- » Oracle Management Agent – The Cloud Enterprise Manager team is solely responsible for the gold-agent image installation for automated provisioning and patching of Agents for **all** targets in the cloud. As the Agent is a critical part of the monitoring solution, the Enterprise Manager team owns the OS user credentials for the Agent. They also own the tuning of any Agent properties in “emd.properties” file. The Cloud Enterprise Manager team receives P1 alert notifications for Agent down/unreachable alerts in their console.
- » Target Discovery– This is mostly automated for PaaS and SaaS services. Only new infrastructure components (Exadata, Exalogic, ZFS Filers etc) must be explicitly discovered. This is initiated by an SR being opened by the Cloud Capacity team to the Enterprise Manager Services queue. Once the target is discovered, target properties are updated, standard template is automatically applied and the target is then added to the proper notification group and service management groups.
- » Template Collections – As templates drive all standard metrics and metric extensions (ME) implementation, it is critical that they are administered properly and maintained. The creation of the templates is driven by standard metrics that are reviewed and signed off by the Cloud Operations target owners (i.e. Database Admins and Fusion Apps Service admins, sysadmins, storage admins). The templates agreed upon by

target owners are uploaded to the template collections and applied through groups by Enterprise Manager Administrators. Whenever new Service-targets are discovered, they receive the “baseline” metrics required and agreed to by the CloudOps team.

- » Incident Notification Rule Sets – These are the core rules that are used to notify Cloud Enterprise Manager and Cloud Operations team members of incidents (fatal/non-fatal) on targets they manage. The management of these rules by the Cloud Enterprise Manager team is to ensure that all required alerts are sent to the appropriate Cloud Service operations team.
- » Master Notification Groups – These are the groups that drive all notifications to the target owners for SaaS (FA HCM, FA CRM), PaaS (Platform as a Service), DBaaS (Database as a Service), and Infrastructure (Physical/Virtual server, storage, network) targets. Adding targets and removing targets from these groups is what drives target notifications. Therefore, the administration of these groups is limited to the Cloud Enterprise Manager team. At the provisioning of service/infrastructure components, EMCLI scripts, written by the Enterprise Manager team, run and add targets to appropriate groups.
- » Group Dashboards – The Cloud Enterprise Manager team is responsible to create the group dashboards for SaaS, PaaS, DBaaS, and other systems.
- » Service SLA and Reporting – Cloud Service PM define Services and their SLAs. Cloud Enterprise Manager team owns set up of SLA for all Cloud Services (definition of components, key components, key performance indicators and SLAs) within Enterprise Manager. The Cloud Enterprise Manager team is also responsible to manage Service dashboards and IP reports showing health/performance/SLA of Services and Infrastructure of Oracle Cloud.

#### **Oracle Cloud Operations (aka Target Owners) Responsibilities** (i.e. PaaS, IaaS and SaaS Admins):

- » Target Discovery– Most target discovery in Oracle Cloud is automated at the provisioning of the service. Only Infrastructure components are discovered using Enterprise Manager Discovery wizards. The Infrastructure team members notify the Enterprise Manager team that new targets require discovery via a P2 service request (SR) to the Cloud Enterprise Manager queue. This SR is actioned by the Cloud Enterprise Manager team member and the target is then discovered with assistance by the target owner.
- » Metric Extensions (ME) Creation/Administration– All MEs are created and maintained by the target owner. This includes the writing of the code as well as the implementation of the ME on a given target. Once the target owner is confident that the ME is working properly, they would then open an SR to the Cloud Enterprise Manager Services queue, requesting that the ME be added to the standard template and applied to all target types that apply, if required. The Enterprise Manager team also writes MEs to meet some of their monitoring requirements.
- » Dashboards – The Oracle Cloud Operations team is responsible for maintaining the dashboards 24\*7 for all groups (SaaS, PaaS, and IaaS) and ensuring that all raised incidents are assigned and addressed in a timely manner. Incidents can be Critical, Fatal or Warning severity. The team responds to fatal events at the highest priority as these are usually availability issues.
- » Job Queue – All custom jobs and the code creation for those jobs is the responsibility of the target owners. This includes troubleshooting of jobs when they are broken. Cloud Operations have several fix-it jobs on Service or Service components to address incidents and availability issues. Cloud Enterprise Manager team can be requested to support via the Enterprise Manager Services queue. Cloud Enterprise Manager team also creates jobs for task automation.
- » Reports Creation - All reports required by a Cloud Operations team member (target owners) are created and maintained by the team member. This includes the maintenance of the code and addressing of errors seen on a report. There are some reports that are administered by the Enterprise Manager team but for the most part, reports are created by the target owner.

It is critical that all members of the team that administer Enterprise Manager full time as well as the target owners understand what they are responsible for and that those responsibilities are taken seriously. This is essential in meeting Service SLAs and to handling issues proactively, ensuring the streamlining and standardization of processes and reducing operational cost of cloud management.



## Appendix 3: References

1. [MOS Note 1553342.1 - Oracle Enterprise Manager 12c Configuration Best Practices](#)
2. [MOS Note 1929586.1 – Patch Set and Critical patch Update](#)
3. [MAA Best Practices Document](#)
4. [Whitepaper: Deploying a highly available Oracle Enterprise Manager 12c](#)
5. [Whitepaper: Strategies for Scalable, Smarter Monitoring using Oracle Enterprise Manager Cloud Control 12c](#)
6. [Patching Agent : Follow Blog: Simplified Agent and Plug-in Deployment](#)
7. [Website: Cloud.oracle.com](#)
8. [Enterprise Manager Cloud Control Advance Installation guide](#)



**Oracle Corporation, World Headquarters**

500 Oracle Parkway  
Redwood Shores, CA 94065, USA

**Worldwide Inquiries**

Phone: +1.650.506.7000  
Fax: +1.650.506.7200

CONNECT WITH US

-  [blogs.oracle.com/oracle](http://blogs.oracle.com/oracle)
-  [facebook.com/oracle](http://facebook.com/oracle)
-  [twitter.com/oracle](http://twitter.com/oracle)
-  [oracle.com](http://oracle.com)

**Integrated Cloud Applications & Platform Services**

Copyright © 2015, Oracle and/or its affiliates. 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 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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0615

White Paper Title : Oracle Cloud Management by Enterprise Manager  
December 2015

Author: Akshai Duggal

Contributing Authors: [Rajiv Maheshwari, Courtney Llamas, Venkat Karpuram, Narayan Sangam, Rajesh Kadam, Virender Katoch, Neelima Bawa, Jonathan Cohen]