

ORACLE®
ENTERPRISE MANAGER **12^c**

An Oracle White Paper

January, 2013

Enterprise Manager 12c: The Nerve Center of Oracle Cloud

| | |
|---|----|
| Executive Overview | 1 |
| Oracle Cloud: Catering to the needs of an Enterprise Ecosystem .. | 2 |
| Managing the Oracle Cloud..... | 4 |
| Management and Monitoring..... | 6 |
| Java Cloud Services Console (Self-Service Management)..... | 8 |
| Infrastructure Performance and Availability Monitoring..... | 9 |
| Service Dashboards and Incident Management | 13 |
| Support Console | 14 |
| Oracle Cloud Operations Lifecycle Management | 16 |
| Conclusion | 18 |
| Appendix..... | 20 |
| Space Management in the Cloud | 20 |
| Cloud Services Compliance Rules | 22 |
| Cloud Operations Responsibilities within EM | 23 |

Executive Overview

Cloud computing is a significant advancement in the delivery of information technology and services. By providing on-demand access to a shared pool of computing resources in a self-service, dynamically scaled and metered manner, Cloud computing offers compelling advantages in cost, speed, and efficiency.

Traditionally deployments require applications to be bound to a particular infrastructure. This results in low utilization, diminished efficiency, and inflexibility. Cloud brings in capabilities to allow applications to be dynamically deployed onto the appropriate infrastructure at runtime. This elastic aspect of Cloud computing allows applications to scale and grow on demand without needing traditional patches or upgrades.

IT departments and infrastructure providers are under increasing pressure to provide computing infrastructure at the lowest possible cost. To do this, they may leverage the concepts of resource pooling, virtualization, dynamic provisioning, utility and commodity computing within the public Cloud or they may create a private Cloud that meets these needs. Customers driven by concerns over security, regulatory compliance, control over Quality of Service (QoS), and long-term costs, will build internal private Clouds. Private Clouds allow internal IT providers and application development teams greater control of data security to meet their governance regulations. There are also a growing number of public Cloud providers that are looking for ways to build a versatile Cloud Infrastructure to support their clientele. However, as the technology matures and these concerns ease, we will see more customers adopting a hybrid Cloud model that makes use of both private and public Clouds using the most suitable of the hybrid strategies.

Oracle offers customers a choice of deploying their applications either in the public cloud or in on-premise private clouds. One such public cloud implementation is Oracle Cloud (formerly known as Oracle Public Cloud). Oracle Cloud offers a portfolio of multiple services in Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) forms. While HCM and CRM are the major SaaS offerings, Java and Database are offered as platform services. Cloud Management can be a complex and multifaceted, involving multifarious processes on tens of thousands of IT assets, housing potentially thousands of tenants. The key goal to managing such a cloud is to offer uninterrupted, agile services to the tenants cost effectively, guaranteeing a high service level.

This whitepaper describes how Enterprise Manager 12c, Oracle's flagship Systems Management product is being used to provide 24x7 management for the Oracle Cloud. The same architecture and principles can be applied to any private or public cloud that is built with Oracle technology.

Oracle Cloud: Catering to the needs of an Enterprise Ecosystem

Why is Cloud important for an enterprise? How does it support the enterprise applications Figure 1 depicts how Cloud strategy fits in and supports an enterprise ecosystem by providing additional deployment choices to enable business agility and flexible cost structure.

Cloud computing has emerged as one of the most important new computing strategies in the enterprise. A combination of new technologies and processes has led to a revolution in the way that computing is developed and delivered to end users. It promises the ability to deliver applications at a lower cost.

Successful Cloud adoption requires businesses to choose the right offering among:

- Broad portfolio of complete and integrated products to build Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).
- Portfolio of Cloud products to build Cloud management layer offering automation, security, and reliability.
- A variety of deployment choices to support the needs of the business and easy migration between the deployment models.
- Support for solutions that enable businesses to adopt cloud at a pace that fits their business. Customers vary widely in terms of how rapidly they wish to move to the Cloud and to what extent they wish to move to the Cloud. Cloud Management challenge is to effectively enable customers to evolve and transform to the Cloud at a pace appropriate for their business.

As organizations adopt Cloud Computing, they will need to define a roadmap that aligns with their own business drivers and clearly identifies their current and future capabilities for delivering IT services. Cloud services and management capabilities need to be identified and prioritized in a Cloud solution portfolio. The ITSO Oracle Practitioner Guide, “A Pragmatic Approach to Cloud Adoption” defines an approach for Cloud adoption and describes the “Cloud Candidate Selection Tool (CCST)” that can be used for this process.

Figure 1 defines a cloud solution portfolio that illustrates the following characteristics:

- A broad spectrum of business applications to support the core business processes and operations. Examples include Sales, Marketing, Financials, Human Capital Management, and Supply Chain Management.
- Platforms and frameworks to develop and run custom processes, applications, and integration components.
- Reliable and Highly Available infrastructure components to support the quality of service requirements of the business.
- Capabilities to support the build-time and runtime cloud management operations including business management, operations management, model management, orchestration, provisioning, security and policy management.

- Choice of architecture in terms of deployment and engineering. Deployment choices should include on-premise and off-premise deployment models. Engineering choices range from best-of-breed infrastructure to optimized best-practice solutions to engineered systems.

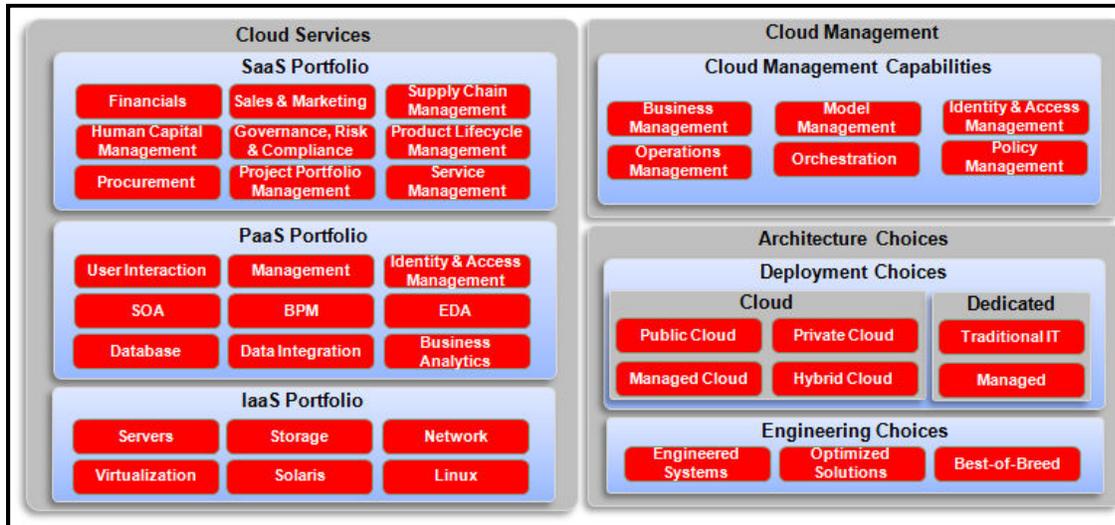


Figure 1 – Cloud Solution Portfolio

The Oracle Cloud is architected to handle the following functional and operational characteristics:

- Thousands of concurrent self-service users
- Tens of thousands of tenants, 25 million users
- Hundreds of thousands service instances
- From one-half-million to one-million infrastructure targets
- More than ten thousand automation jobs per day
- Tens of thousands of page views per second
- Five-Nine (99.999%) availability
- Full disaster recovery
- Water-tight security
- Two minute response commitment to any problem

Therefore, any management solution which manages the Oracle Cloud needs to be architected to ensure the above goals are met.

Managing the Oracle Cloud

A key design goal of Oracle Cloud is to have a highly automated management and monitoring capability so as to ensure the best quality of service and minimize operational costs. Oracle Enterprise Manager Cloud Control 12c (EM) is the Management and Monitoring backplane of Oracle Cloud. It provides the Oracle Cloud operations team a single console to manage the entire cloud infrastructure and applications deployed in Oracle Cloud. Additionally, EM automates a large number of day-to-day operations thereby enabling highly automated, efficient and effective management of the Oracle Cloud environment. EM also powers the self-service Java Service Console that is used by the Cloud Users (Tenant Java Service Administrators) to deploy and manage applications. Oracle Cloud Support analysts use EM as their primary interface to debug and resolve service requests. EM routinely monitors the health of Oracle Cloud components and seamlessly interfaces with My Oracle Support and Tenant Administration System (TAS) to automatically create service requests when the potential problems are detected and close them when the issues are resolved. Oracle Enterprise Manager is Oracle's integrated enterprise IT management solution, which provides the industry's only complete, integrated and business-driven enterprise cloud management solution.

The key capabilities of Enterprise Manager include:

- A complete cloud lifecycle management solution to quickly set up, manage and support enterprise clouds
- Comprehensive, deep and integrated management of the entire Cloud stack - all the way from applications to middleware, database, operating systems and hypervisors to hardware components
- Best service levels for traditional and cloud applications through business-driven application management

EM product architecture comprises the following key components:

- **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 application, J2EE applications). It is a unit that can be monitored and managed individually. There are many different types of targets that Cloud Control can manage. Examples include Host, Database, Listener, ASM, WebLogic Server, Service Bus, SOA applications, J2EE applications, E-Business suite, Siebel, Exadata, Exalogic, VMs, OVM and Fusion Applications.

- **Oracle Management Service (OMS):** Web-based application that orchestrates the Management Agents and the Management Plug-ins to discover service components (called targets), monitor and manage them, and store the collected information in a repository for future reference and analysis. The OMS also renders the user interface for Enterprise Manager Cloud Control and the Java Console.
- **Oracle Management Repository (Repository)** – 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.
- **Self Service Console** – The Self Service Console is a browser based web application that is available to tenants to provision, manage and maintain their applications/infrastructure, review usage/quota, validate availability and chargeback information. This is available for Infrastructure as a Service (IaaS), Platform as a Service (PaaS). Platform as a Service can be further classified into Java as a Service (JaaS) and Database as a Service (DaaS).
- **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.

EM is deployed in Oracle Cloud in a secure, scalable and fault tolerant architecture, with firewalls between the OMR, Oracle Management Service and Agent layers. Multiple OMS instances load balance traffic and provide high availability. Each OMS instance runs on an Exalogic compute node. A highly available RAC database running on Exadata serves as the EM repository. Agents on all Oracle Cloud infrastructures (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. EM 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 traffic analysis allows EM to generate proactive alerts if customers experience performance anomalies.

In Oracle Cloud, the monitoring framework has to manage thousands of servers, databases and middleware instances and integrate with the cloud ecosystems. EM at Oracle Cloud is architected for Cloud-class scale to address the Oracle Cloud requirements:

- Scales to hundreds of thousands of managed services
- Accommodates hundreds of concurrent users, bucketed under multiple administrative roles
- Runs hundreds of concurrent jobs in the Cloud
- Integrates with Oracle Access Manager (OAM) and Identity Management (IDM) systems for security
- Offers a rich automation command line interface and Cloud APIs

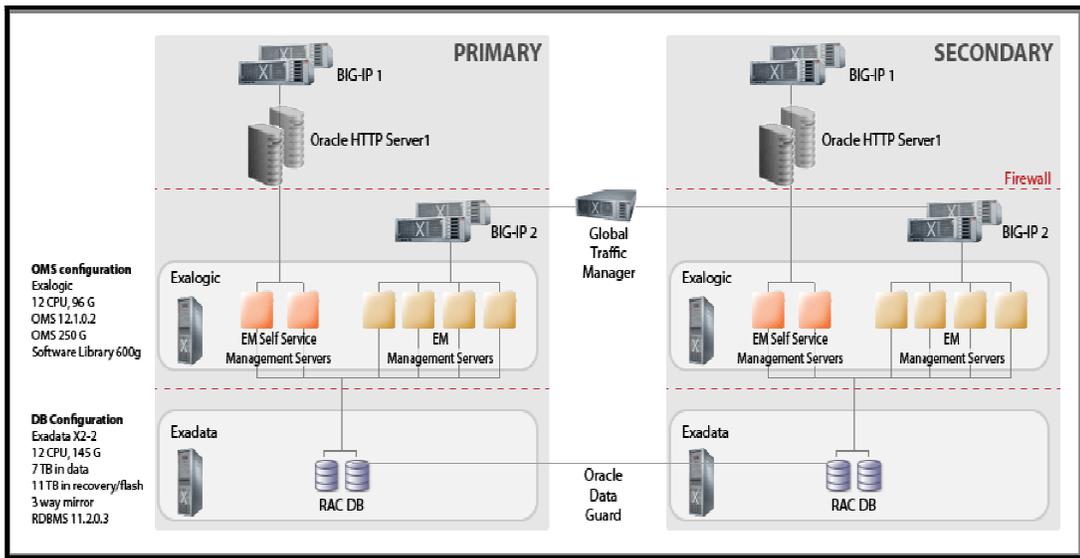


Figure 2 – Enterprise Manager Topology in Oracle Cloud

Management and Monitoring

For Oracle Cloud, there are two key interfaces of Cloud management and monitoring in the Oracle Cloud. They are:

- Java Cloud Service Console via which tenant administrators can deploy/undeploy and monitor availability and key performance metrics of their Java applications in Oracle Cloud
- Enterprise Management Console via which Cloud Operations and Cloud Support staff monitor and manage the entire Cloud infrastructure that includes Cloud services and the Cloud management components.

The two roles are quite distinct (even though it's the same management system that performs both, using a shared repository for its persistence). The figure below captures the key capabilities required from the Cloud management infrastructure to address these use cases.



Figure 3 - Cloud Operational Management Capabilities

In Oracle Cloud, the Administration Group feature of EM is used to define monitoring settings, compliance standards and cloud policies through templates and organize service components in multiple hierarchies, such as Location, Line of Business and Lifecycle status. Enterprise Manager 12c Incident Management system is used to manage SLAs on services by exceptions. Oracle Cloud Administrators review, suppress, escalate and remediate the events/incidents per business needs, and have also integrated with ticketing systems to generate Service Requests for critical events. Three distinct types of users (i.e. Oracle Cloud Operations staff, Java Tenant Administrator and Oracle Support Analysts) use EM daily to perform their tasks. Oracle Cloud operations team uses EM to monitor and manage the Cloud. Unlike Oracle Cloud Operations, Support Analysts do not monitor the Cloud 24*7, they use EM to establish health of Service and Service Components and debug issues that Oracle Cloud customers might report. EM captures the CSI numbers of the customers at the Service/asset level and helps Support analysts identify customer issues quickly. The functions of the three roles described above are represented in *Figure 4* below:

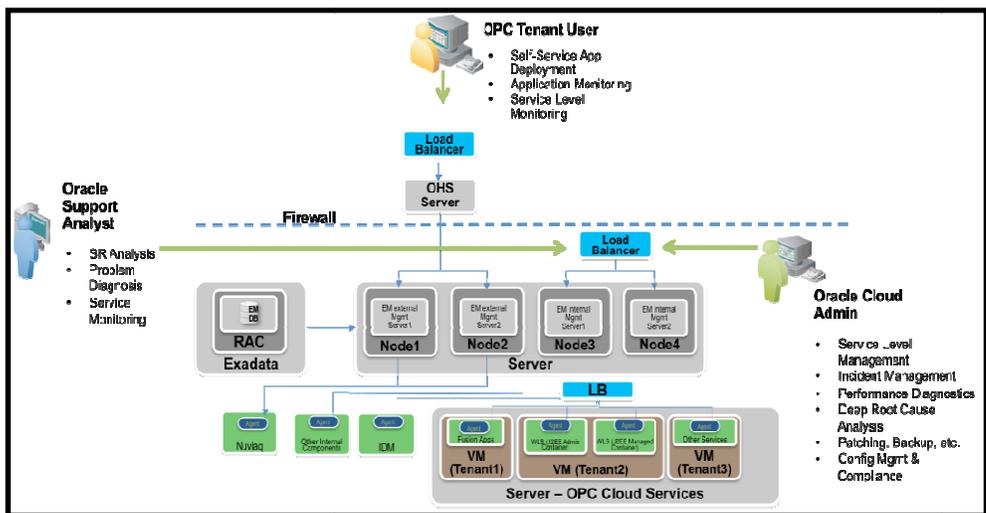


Figure 4 – Role specific functions of EM within Oracle Cloud environment

In order to effectively serve the various roles described above, different OMS instances are assigned to different “roles”. Some of the OMS, front ended by a hardware load balancer, are used by the Oracle Cloud Operations team and the support analysts, while others serve the Tenant Administrators.

Java Cloud Services Console (Self-Service Management)

Enterprise Manager powers the Java Cloud Services Console (JCS Console) that allows Oracle Cloud Tenants to monitor and manage their Java Cloud Service (JCS) instances and the J2EE applications. It provides them with all tools for interacting with JCS instances, as well as managing the lifecycle of applications deployed to these instances. EM can handle hundreds of such requests concurrently. Under the covers, EM integrates with Oracle Cloud ecosystems like Oracle Identity Management, My Oracle Support, Oracle E-Business Suite (ERP Global Single Instance), Tenant Administration System and Service Delivery Interface to perform all the orchestration tasks required for application lifecycle management, as well as the data collection for monitoring.

Once a tenant administrator provisions a JCS service and designates one or more service administrators, the Tenant Service Administrator can then monitor availability and performance of their J2EE applications and the WebLogic server/cluster hosting the application. Via the JCS Console, Tenant Service Administrators can perform the following tasks:

- Deploy/undeploy an application
- Start/stop an application
- Monitor application and service instance health and key performance indicators
- View logs
- Receive notifications for current incidents affecting their services

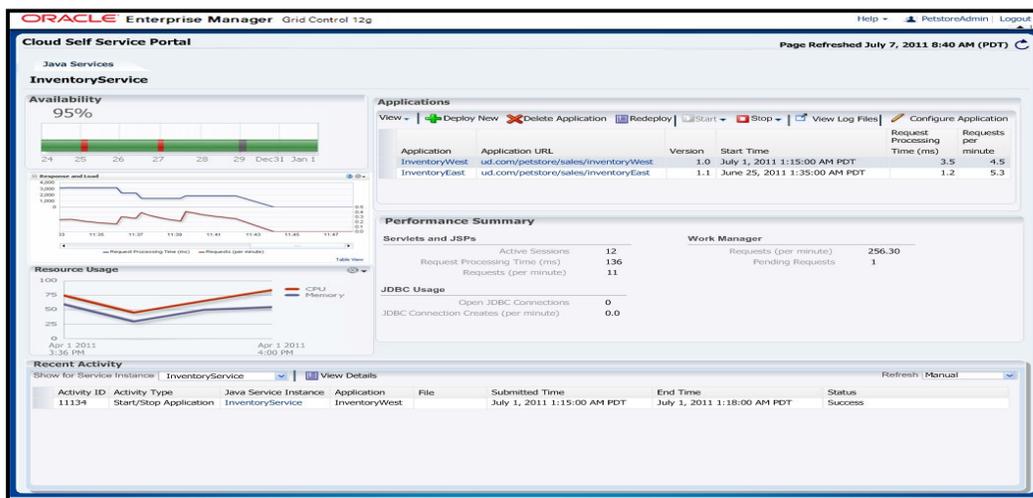


Figure 5- Enterprise Manager Java Console

These capabilities are exposed through the JCS Console and Oracle Cloud APIs (RESTful API, EMCLI) for programmatic access.

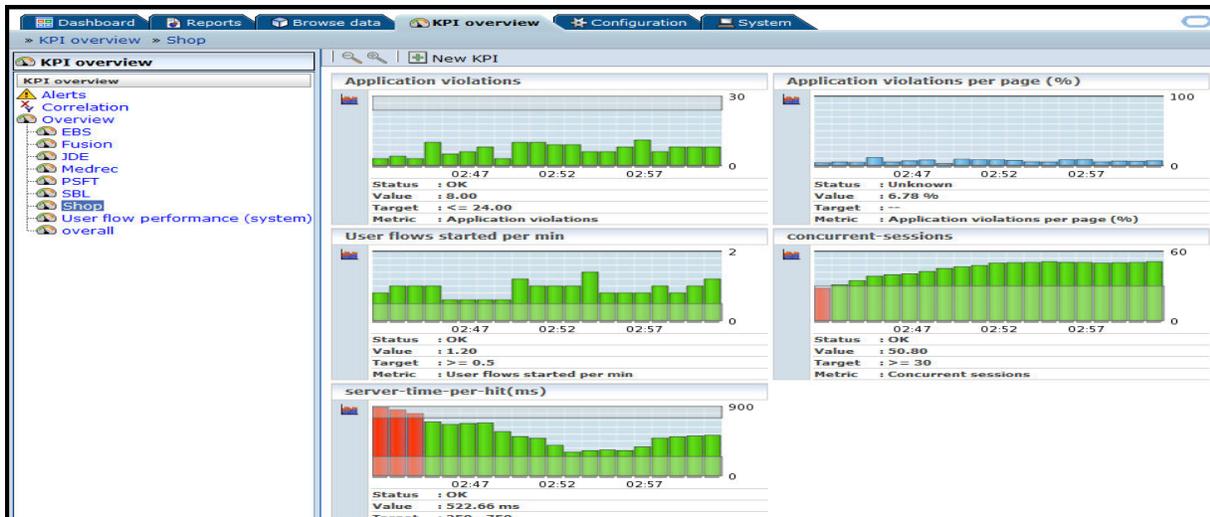
Infrastructure Performance and Availability Monitoring

EM auto-discovery is used at Oracle Cloud to discover Service Components, hardware and software infrastructure of Oracle Cloud. Every Oracle Cloud infrastructure component (Exadata, Exalogic, VM servers, ZFS storage) has an agent deployed on it, allowing these infrastructure components to be discovered by EM and allows deep monitoring and complete administrative control. The process of Agent deployment has been simplified by staging Gold Agent images that are deployed on hydrated Service assemblies (PaaS, SaaS). These Gold Agent images are the latest patched Agent binaries. Agents are deployed and configured as part of a service instance provisioning, thereby allowing a complete end-to-end visibility of all infrastructure and application components, as well as their relationship and association. Using this capability, the Oracle Cloud team can precisely tell which infrastructure components are used to host a particular service instance. This information is also used to perform maintenance impact analysis e.g. if a particular server or storage sub-systems were taken offline for maintenance, which service instance would be impacted. Topology diagrams enable viewing these target relationships for dependency (e.g. which services run on this host?) and usage (e.g. which database is used by which service). For each managed target, EM captures detailed performance and availability metrics, as well as usage metrics essential for metering.

Oracle Cloud also leverages EM's capability to monitor application performance from an end-user perspective. Real-user monitoring complements infrastructure monitoring with measurements of the actual application usage and response, as experienced by the end user. This data is used in several contexts:

- Provides metrics about SaaS application usage (number of login, usage per role, most used functions, bytes transferred, etc) and performance (response time, availability) that can be reported to the end user (via the TAS system and the Cloud UI, see below).
- Provides deep visibility into application performance to the Oracle Cloud operations team, allowing them to quickly detect, isolate and investigate any application performance issue. Charted reports clearly point out the top pages in terms of errors and latency and the top users that are affected.

This data also provides reports about SaaS application and usage, to be used for capacity planning, performance improvements, usage tracking, etc. These configurable reports allow application performance to be analyzed along many dimensions. *Figure 6* provides a sample illustration of the graphics they contain:



2

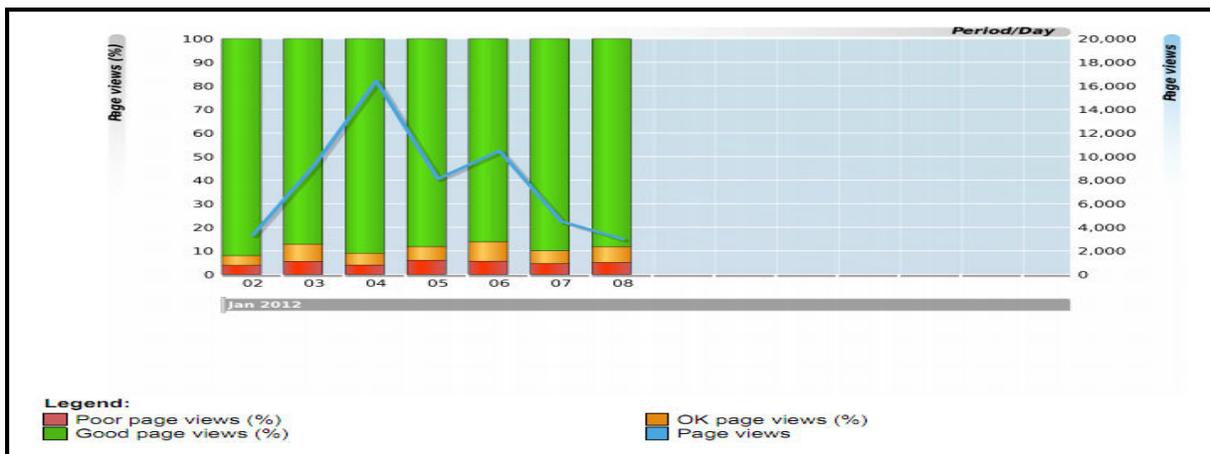


Figure 6- Reports on Real User Experience

With additional client-side JavaScript instrumentation, Real-user monitoring can be used in collaboration between Oracle Cloud customers and Oracle Cloud operators to diagnose performance issues and pinpoint the source (client side, CDN, 3rd party site, Oracle Cloud infrastructure) without requiring any additional software download or configuration by the client.

Also, EM Beacons are used for proactively monitoring network and business transaction flows via synthetic transactions. Beacons are placed outside Oracle Cloud firewall to simulate user access to PaaS Service (Oracle WebLogic Server). For SaaS Services, beacons are defined to simulate key business transactions to validate availability and performance latency. These are run at a scheduled frequency and reported on Service Availability reports.

Standardized monitoring templates for metric thresholds and metric frequency are applied to every monitored Oracle Cloud component. These thresholds enable administrators to measure against business SLAs to ensure optimal performance. The metrics captured by EM get published to the TAS (Tenant Administration System) via RESTful web services. This information is rendered to Cloud UIs, so tenants have transparency and visibility on usage, statistics and availability of their Oracle Cloud services. The metrics that get published vary based on the service type. Examples include:

- For Java Service - number of active sessions, heap and CPU usage per server, number of applications deployed, disk usage, etc
- For DB Service – Space usage, total number of objects, amount of data transferred, etc
- For Fusion HCM service – Business metrics such as number of Goals, number of performance documents, number of completed 360 degree feedback, etc

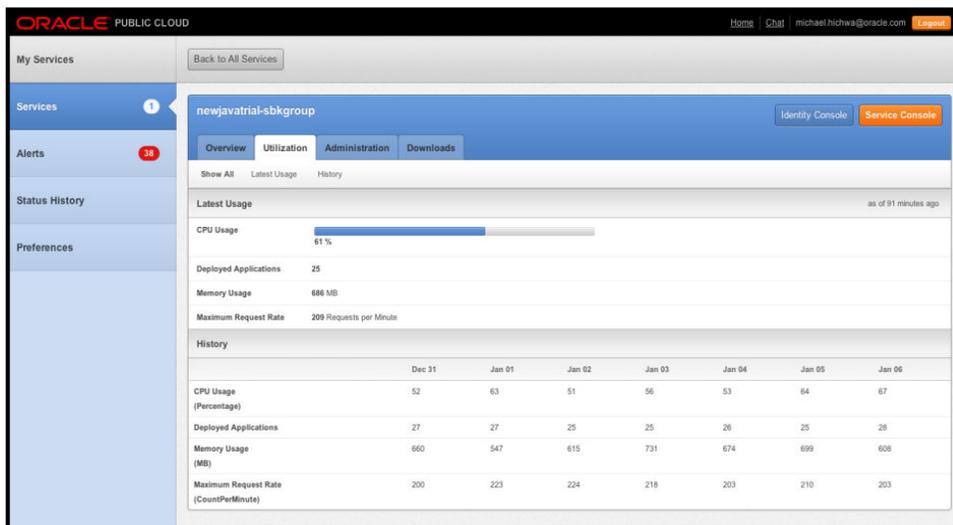


Figure 7– EM Metrics published in TAS

EM’s Web services also provide TAS with historical availability information for the last 90 days. A schedule of planned maintenance window is communicated to Oracle Cloud Tenants through Cloud UI, using EM blackout functionality. Blackouts are applied to environments before any change management (patch, upgrade, config change) is performed on a customer’s Service Instance. Blackout periods are excluded from Service availability definition.

Oracle Cloud makes extensive use of Oracle’s Engineered Systems for redundancy, reliability and performance. Exadata is used for database services, while Exalogic is used for SaaS (Oracle Fusion Applications) and PaaS (Java) services. The management of Engineered Systems is indeed

special, because they are managed vertically as a unit by administrators with specialized skills in managing multiple stack components. For Exadata, EM offers a schematic view of hardware components of the Database Machine for example; compute nodes, Exadata storage cells, Infiniband switches, ILOM (Lights out monitoring), etc. Oracle Cloud Operations monitor critical hardware metrics and view aggregated alerts and faults from all Exadata components on one dashboard. For Exalogic, EM integrates with Exalogic Control to provide deep management of the infrastructure layer.

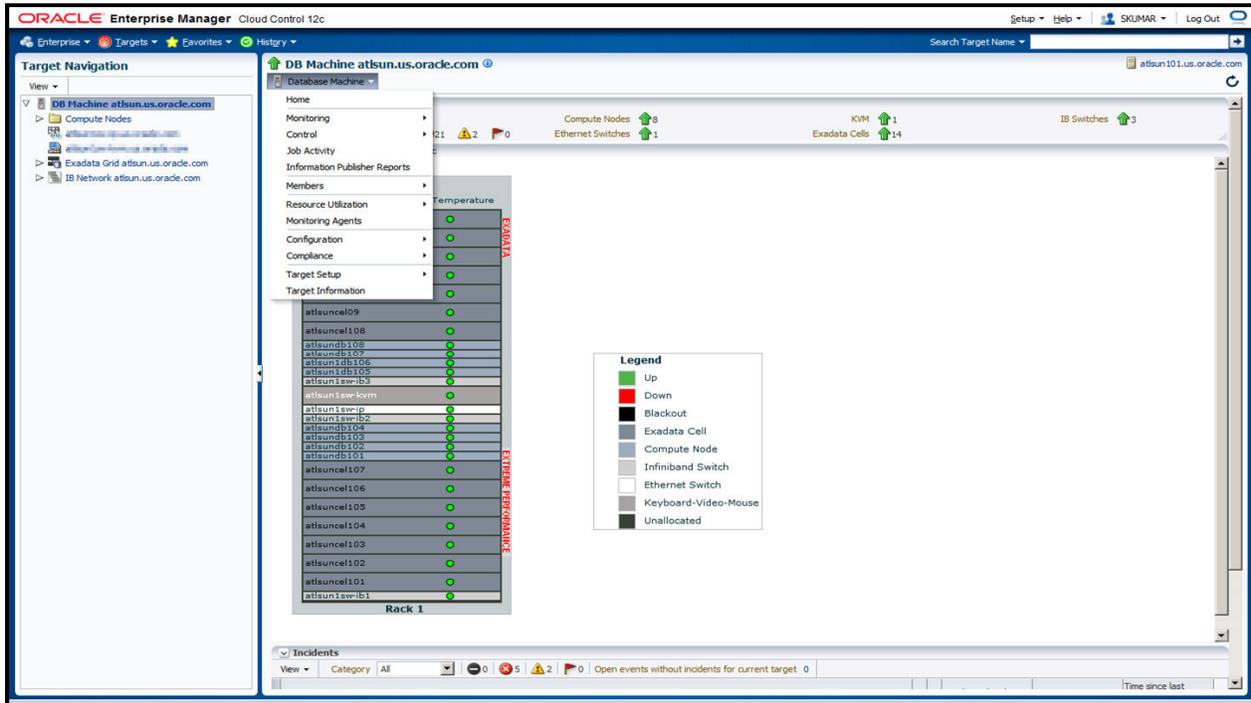


Figure 8 – Exadata Database machine schematic

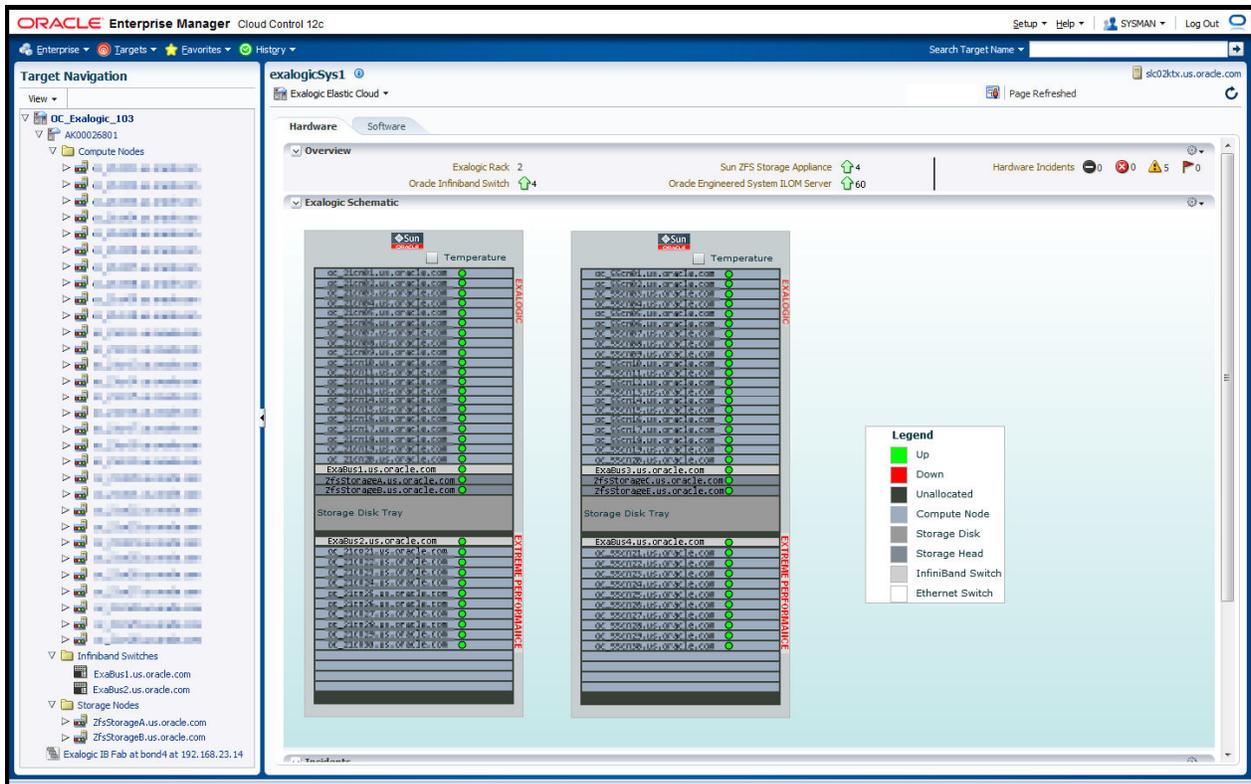


Figure 9– Exalogic schematic

Service Dashboards and Incident Management

Cloud computing changes the focus on understanding, modeling, and monitoring services, not systems as was with traditional IT. Service Level Management is a key requirement for any Cloud services. For the cloud to operate non-disruptively, the services need constant monitoring. All Oracle Cloud Services (SaaS and PaaS) are proactively monitored, 24x7, by Oracle Cloud Administrators using EM Service and System Dashboards. These dashboards provide 360 degree view of the 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 some key performance metrics, usage metrics and business metrics are provided to TAS for Oracle Cloud SaaS and PaaS services metering and capacity planning.

| Group: Cloud9 Servers | | | | | | |
|--|-------|------------------|-----------|-------------------------------------|-------------------------|--|
| Target | Type | Status | Incidents | Run Queue Length (5 minute average) | Logical Free Memory (%) | |
| Cloud Infrastructure Servers | Group | 4 2 33 | 0 0 3 0 | | | |
| All Cloud Servers | Group | 49 52 124 330 | 0 3 60 0 | | | |
| Database Service Servers | Group | 1 25 | 0 0 1 0 | | | |
| SaaS Servers | Group | 43 | 0 1 11 0 | | | |
| Java Service Servers | Group | 5 | 0 0 0 0 | | | |

Incidents

| Severity | Target | Type | Last Updated | Status | Summary |
|----------|----------------------------|------|-------------------------|--------|--|
| | [redacted] | Host | Dec 17, 2011 5:27:45 AM | New | Agent is Unreachable (REASON = unable to connect to the agent. [Connection timed out]). Host is unreachable (REASON = Ping tim |
| | [redacted] | Host | Dec 23, 2011 2:42:02 PM | New | Agent is Unreachable (REASON = unable to connect to the agent. [Connection timed out]). Host is unreachable (REASON = Ping tim |
| | [redacted] | Host | Dec 17, 2011 5:22:52 AM | New | Agent is Unreachable (REASON = unable to connect to the agent. [Connection timed out]). Host is unreachable (REASON = Ping tim |
| | [redacted] | Host | Dec 17, 2011 5:24:48 AM | New | Agent is Unreachable (REASON = unable to connect to the agent. [Connection timed out]). Host is unreachable (REASON = Ping tim |
| | [redacted] | Host | Dec 17, 2011 5:24:48 AM | New | Agent is Unreachable (REASON = unable to connect to the agent. [Connection timed out]). Host is unreachable (REASON = Ping tim |
| | [redacted] | Host | Dec 17, 2011 5:25:49 AM | New | Agent is Unreachable (REASON = unable to connect to the agent. [Connection timed out]). Host is unreachable (REASON = Ping tim |
| | [redacted] | Host | Dec 17, 2011 5:28:49 AM | New | Agent is Unreachable (REASON = unable to connect to the agent. [Connection timed out]). Host is unreachable (REASON = Ping tim |
| | [redacted] | Host | Dec 30, 2011 7:10:22 PM | New | Filesystem / has 9.87% available space, fallen below warning (10 |

Figure 10– Incident Dashboard

The ability to drill down into the incidents from the Service Dashboard facilitates faster debugging and resolution. EM detects Incidents that impact the health and availability of any of the Oracle Cloud Services and automatically files a My Oracle Support Service Request (SR) to notify the operations and the support team of the problem. Detailed diagnostics and configuration information of the underlying system, including application to infrastructure dependency mapping, is packaged and attached to the Service Request (using EM’s Automatic Diagnostic Repository (ADR) functionality) to enable problem diagnostics. In addition, EM also notifies TAS of the outage and this information is notified to the tenant through the Cloud UI.

Support Console

EM is the primary console used by Oracle Cloud support analysts to diagnose and resolve problems reported by the Cloud tenants. In order to facilitate this, EM keeps a complete mapping of the managed targets (Cloud Service components), the Oracle Cloud service type it belongs to (e.g. Fusion CRM, Java Service or Database Service), service instance owner, and Tenant Customer Support Identifiers (CSI). Using this information and the Cloud Support Home page, a support analyst can quickly identify the service instance belonging to a given tenant. EM allows drill down to individual service components to identify the root cause of incident and help remedy the problem. The information flow between Enterprise Manager, the Support Analyst and the Tenant is shown below:

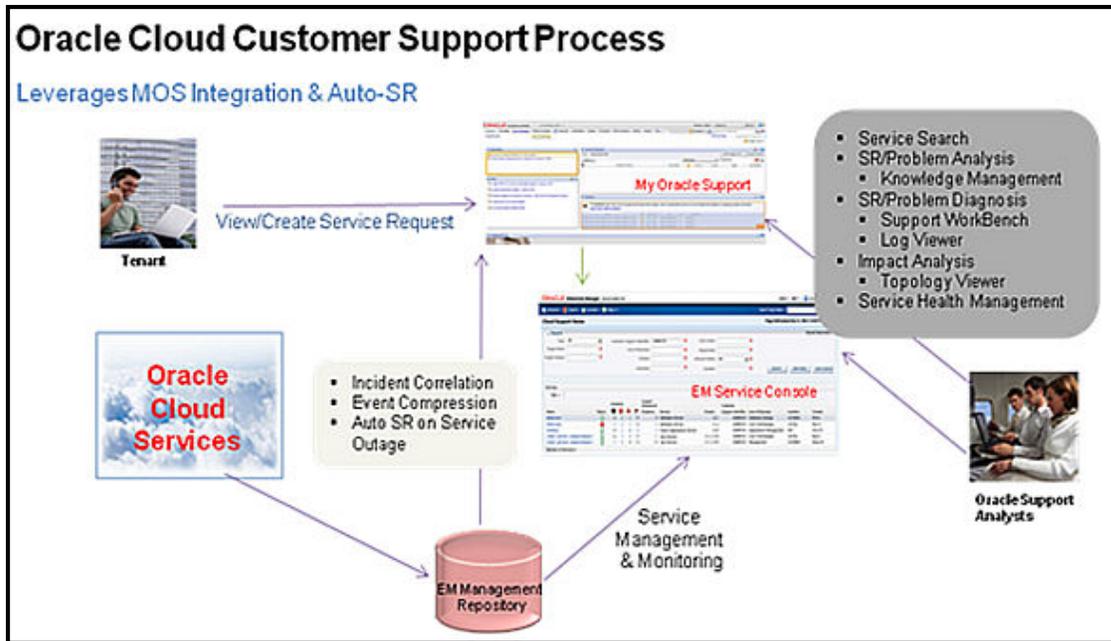


Figure 10– Support Process for Oracle Cloud

The Cloud Support Console is specifically designed to facilitate support of the Cloud environments. In the above figure, we see that:

- In Step 1, the SR is automatically filed by EM, corresponding to the specific CSI
- In Step2, the SR is attended to by the Support Analyst. Features for the Support Analyst include:
 - Tailored views for support analysts
 - Search Services and their incidents using business parameters (e.g. customer name, subscription id)
 - Service instance health and incidents across service types (e.g. Fusion Apps, Java, and DB Services)
 - Launch points for common actions and diagnostics
 - Package diagnostics, configuration, dependency data to attach to SR
 - Drill-down to topology views for impact analysis
- In Step 3, the tenant tracks, reviews and validates the SR from time-to-time till closure.
- The following snapshot of the Support Console shows the richness:

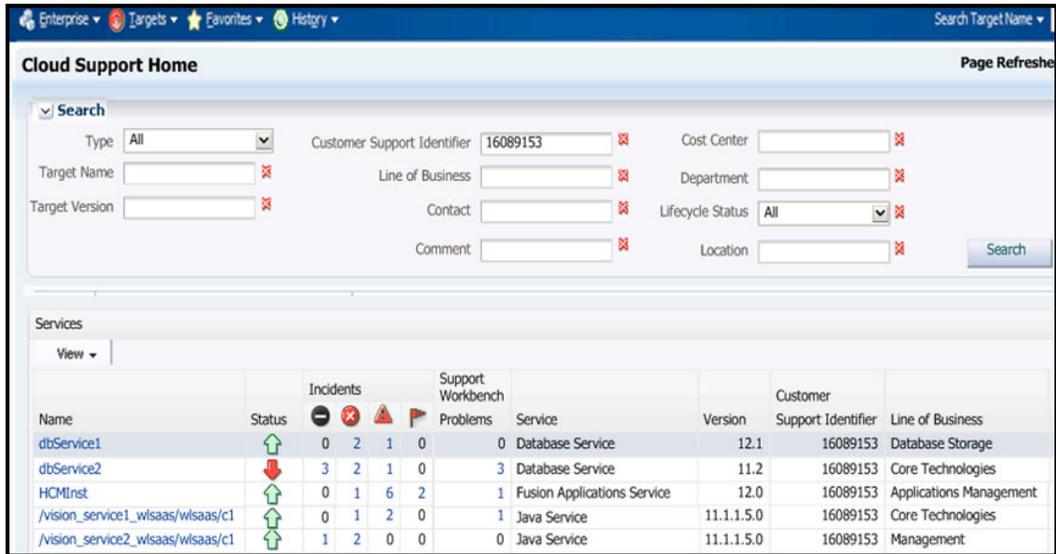


Figure 11 – Support Console

Oracle Cloud Operations Lifecycle Management

On a day-to-day basis, Oracle Cloud administrators need to perform repetitive tasks such as backup, patching, log cleanup, etc. Usually these tasks are mundane and time-consuming, hence needing as much hands-off automation as possible.

Had it not been for automation tools, the bulk of time in managing a cloud would be spent behind mundane, repetitive, administrative tasks such as patching. Experiences from customers indicate for example, that without Enterprise Manager, administrators spend hundreds of person-hours to apply quarterly patches to databases.

Administrators leverage EM to automate several Cloud Operations Management tasks like:

- 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
- Patch automation and management

Enterprise Manager comes with an automation framework comprising Jobs and Deployment Procedures (discussed earlier) that lets administrators define these repetitive actions and schedule them as needed. EM's task automation framework is scalable, carries functions such as ability to

schedule, resume and retry which are of paramount importance in conducting mass operations in an enterprise scale cloud. Oracle Cloud operations team extensively uses this framework to automate a larger number of periodic operations e.g. backups, log rotation and purges, etc. The task automation is also used for adhoc management and maintenance operations as well. Change management for cloud scale environments are performed by using EM's task management framework to manage-many-as-one (Groups/Systems) functionality. The task automation verbs are also exposed through the EMCLI interface. Oracle Cloud administrators make extensive use of EMCLI for large scale operations on thousands of tenant services.

EM's blackout functionality is extensively used to schedule and manage planned management operations. Oracle Cloud operations teams defines blackout on the affected Service components – both for periodic as well as adhoc operations – in EM, which subsequently notifies TAS so that affected tenant/user can be alerted of the upcoming planned/scheduled maintenance.

Configuration Compliance is another very important aspect of managing the cloud. We often see news reports on how the securities of certain clouds have been breached. The security breaches often happen owing to faulty configuration such as default passwords, relaxed file permissions, or an open port. Compliance inherently demands certain disciplines that may get submerged in the entropy of cloud. To manage compliance, Oracle Cloud administrators have created gold baselines and gather configuration collections in EM for all Oracle Cloud systems. Any deviations from the baselines triggers compliance violation notifications, alerting administrators to resolve the issue before it creates risk in the environment. Starting from the top level the hierarchy contains Compliance Frameworks, Compliance Standards and Compliance Rules. Compliance Frameworks aggregate the compliance scores of Compliance Standards which may be for different target types. Compliance Standards contain one or more Compliance Rules but are specific to a single target type. Compliance Rules are responsible for executing a single and specific validation of a target and reporting conformance.

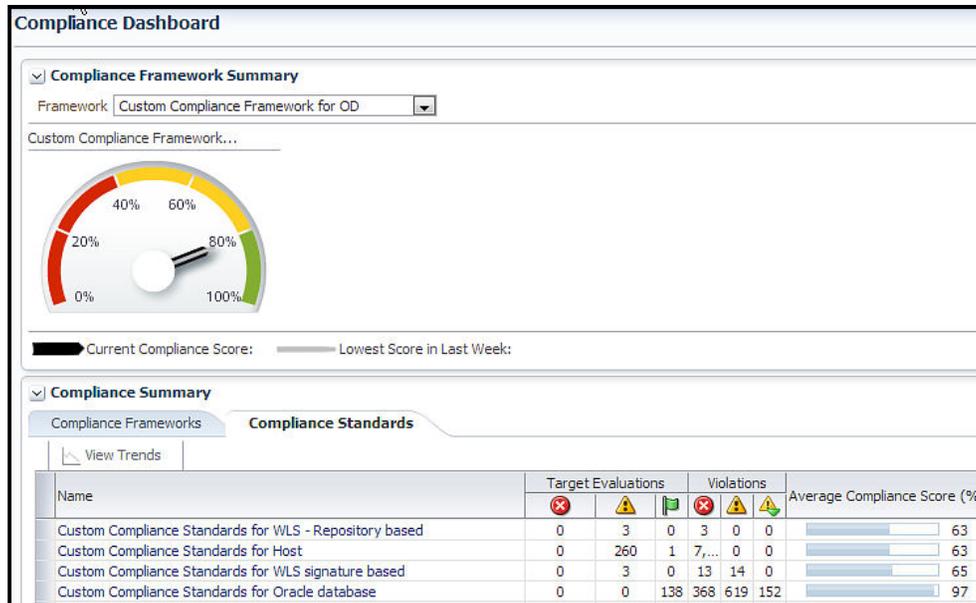


Figure 12-Compliance Frameworks

EM provides a comprehensive toolset to administrators to help them understand the exact nature of configuration drift, its source and the remedy and present the consolidated reports to compliance officers and auditors. The Fusion Applications stack is a complex stack comprising multiple components. If there is a minor configuration drift detecting that could be like finding a needle in a haystack. The sophisticated configuration comparison capability can compare multiple application pods (across test, dev and production lifecycles) and help detect deviations with ease.

Finally, the built-in integration between Enterprise Manager and My Oracle Support (MOS) allows Oracle Cloud administrators to get Patch advisories on all Oracle software deployed as part of Oracle Cloud and ensure CPUs (Critical Patch Updates) are applied to all Oracle Cloud systems.

Conclusion

Oracle Cloud is an extremely demanding environment in terms of scalability, security and agility. It is an environment where Enterprise Manager 12c's Application to Disk management capabilities are put to a real test. The true enterprise-class characteristic of the cloud management platform is evidenced by the following Oracle Cloud statistics of September, 2012:

- 5,622 concurrent self-service users
- 31,518 tenants, 25 million users
- 506,947 service instances
- 598,810 targets
- 9,243 automation jobs per day

- 125,983,703 page views per day

As cloud computing gains popularity, it is expected that more clouds with similar SLA demands will emerge. Implementers can gain from the experience to gain maximum return from their cloud with minimum cost.

Appendix

In this section some of the Oracle Cloud EM use cases are detailed.

Space Management in the Cloud

Cloud computing requires a better understanding of the elasticity characteristics of deployed applications, workloads and the cloud platform. Wikipedia defines Cloud Computing – “via dynamic (“on-demand”) provisioning of resources on a fine-grained, self-service basis near real-time [32], without users having to engineer for peak loads”. [Intrinsic to the definition of cloud computing is that resources can be dynamically scaled up and out, on demand. Since a cloud platform does not have infinite resources, the way to efficiently provide and provision for instantaneous elasticity is by using EM to manage inventory, auto-provision, perform continuous capacity management and report on service usage.

In Oracle Cloud the following space management processes are automated using EM.

Scale Up

Oracle Cloud uses EM to monitor the space usage of every service through metrics for service components (targets) like database, FMW, Fusion Apps, J2EE apps etc. The gathered information (every 15 minutes) is rolled up per hour, per day, per week, per month. This rolled up data is presented to Tenants through Oracle Cloud UIs. Based on utilization data and business needs, tenants can decide to Scale up from Small to Medium or Small to Enterprise.

Scale Out

Oracle Cloud offers customers to scale out and add more hardware/software infrastructure like hosts and web servers to the existing Service clusters. This allows tenants to manage their user growth and business needs. EM has automated workflows/jobs to provision additional WebLogic servers and VMs to a tenant’s service thereby guaranteeing instantaneous elasticity.

Capacity Planning

The size of Oracle Cloud, elasticity needs and instant provisioning times require Oracle Cloud operations to have stair step capacity available and a process of continuum capacity planning. A pool of SaaS and PaaS assemblies are hydrated and retained. When a tenant requests a service, one of the pre-hydrated slots gets a “personality” assignment. The number of hydrated assemblies is assessed and a new one is created to fill the slot of the one recently provisioned for a tenant. Capacity needs to be reviewed and planned from business, service, and service components perspectives. EM gathers inventory, quotas, service level performance metric data,

workload metric data, processor, I/O and memory analysis and real time page hits information. All this data is mined to generate capacity reports targeted to predict peak usage needs to ensure cloud infrastructure components can meet that need. The goal is to optimize and ensure just enough capacity is made available.

Cloud Capacity Management Process Flow

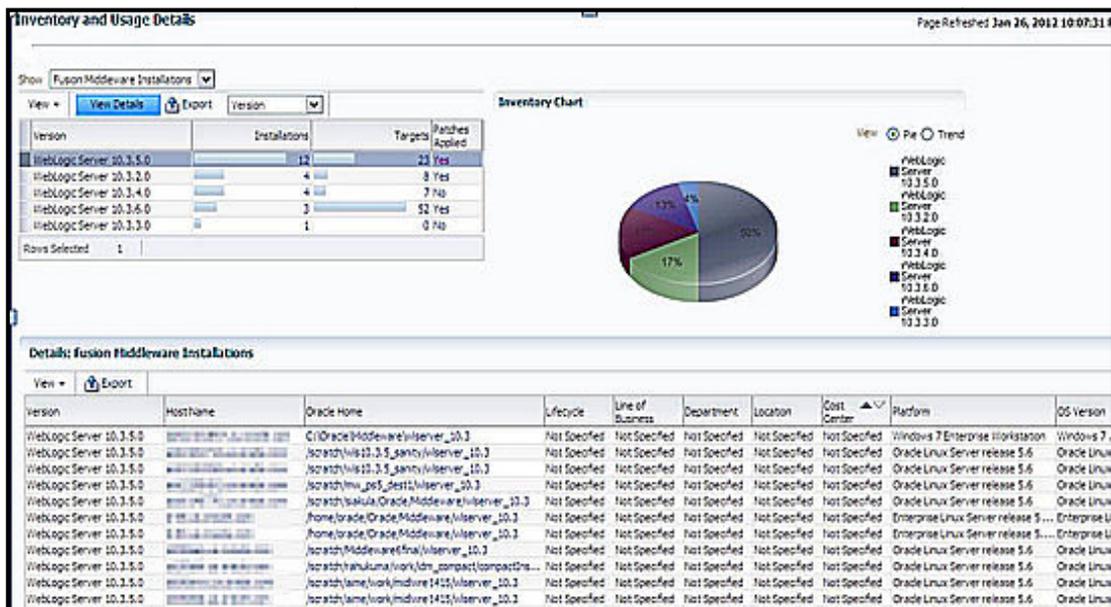


Figure 13-Inventory and usage reporting



Figure 14-Cloud capacity trending

Since Oracle Cloud Services are on shared infrastructure using multitenant model, it makes capacity modeling and planning much more complex. Auto provisioning makes some aspects of capacity planning convoluted and intricate as pools of hydrated assemblies are pre-prepared and staged (VMs and storage with application software all installed). Considering that cost is a core driver for leveraging cloud computing for tenants, it is paramount that only essential resources are purchased, deployed and locked in.

Cloud Services Compliance Rules

All Cloud Services are proactively checked for Compliance against pre-defined security and configuration standards. These standards are defined in EM as compliance rules and all environments are checked periodically. Violations to the compliance checks are raised as alerts/incidents. Incident notification rules are setup to notify the appropriate target owners. For example, for SaaS (Fusion Apps Service) the following security and configuration compliance checks are enabled:

- Security Recommendations for Oracle Products
- Java Virtual Machine Configuration Standard for Fusion Applications
- Java Platform Security Configuration Standard for Fusion Applications
- Oracle HTTP Server Configuration Standard for Fusion Applications
- WebLogic Server Configuration Standard for Fusion Applications
- Certificate Validation Standard for Fusion Applications

Critical configuration settings that ensure an optimum execution of a SaaS instance are set as standards in “Java Virtual Machine Configuration Standard for Fusion Applications” and “Oracle HTTP Server Configuration Standard for Fusion Applications”. For example below are some of the JVM configurations that are defined for validation.

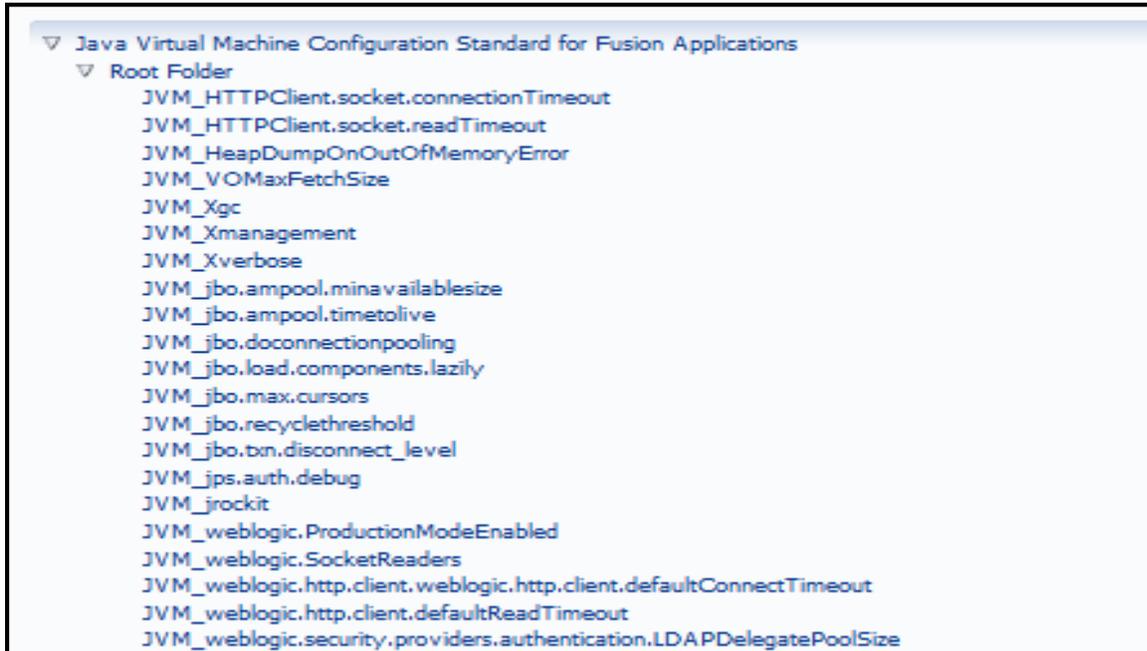


Figure 15-JVM configuration details

If any Fusion Applications Instance deviates from the configurations defined as standards, due to any change/patching activity, it is immediately brought to the notice of the target owners by an EM incident. At which time the Cloud Operations team can choose to a) request for a change to the Compliance Standard or b) update the instance and fix the violations.

As shown for Fusion Applications, similarly standards are defined for other services i.e. PaaS (Java as a Service) and DaaS (Database as a Service). All Oracle Cloud infrastructure is also validated with security and configuration compliance checks.

Cloud Operations Responsibilities within EM

The Cloud Operations Enterprise Management team consists of members located around the globe. This allows for regional 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) EM 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 SR request
- 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 EM DBMS processes are running successfully and within threshold
- Create accounts for Cloud Operations and Cloud Support
- Manage EM site backup
- Ensure Cloud EM executive dashboards are accessible
- Ensure Cloud EM interfaces with other Cloud eco-systems like TAS, SDI, MOS are operational

From an on-call queue perspective, the EM 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 EM Team Responsibilities: Oracle Cloud Enterprise Manager team manages and maintains the following:

- Oracle Management Server – The Cloud EM team is solely responsible for applying patches to the OMR database and the OMS mid-tiers. As well, no team members outside of the EM team are permitted to start or stop any component of the EM infrastructure. This also includes adjusting of OMS parameters.
- Oracle Management Agent – The Cloud EM team is solely responsible for the installation, patching, starting or stopping of Agents for **all** targets in the enterprise. As the Agent is the most critical part of the monitoring solution, the EM team owns the OS user credentials for the Agent. They are responsible for Agent patching and maintaining Agent gold images for new Agent deployment. This includes the adjustment of any settings in the “emd.properties” file for all Agents. The Cloud EM team receives P1 alert notifications for Agent down/unreachable alerts in the console to ensure proactive monitoring.
- Target Discovery– This is mostly automated for PaaS and SaaS services. Only new infrastructure (Exadata, Exalogic, ZFS Filers etc) are discovered. This is initiated by an SR being opened by the Cloud Capacity team to the EM 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 by the EM team member.
- Admin Group Management – The Cloud EM team is responsible to define the Admin Group hierarchy for each of their EM sites using the 7 first class target properties. Updates to the Admin Group tree are only performed by Cloud EM team. EM team generates a report once a week for an exclusion list of targets not in any Admin group.

- **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 Admins, WebLogic server admins, sysadmins, storage admins). The templates agreed upon by target owners are uploaded to the template collections and attached to the Admin group leaf node by EM administrators. Therefore, when new targets are discovered, they receive the “baseline” metrics required and agreed to by the target owners.
- **Incident Notification Rule Sets** – These are the core rules that are used to notify Cloud EM and Cloud Operations team members of incidents (fatal/non-fatal) on targets they manage. The management of these rules by the Cloud EM team is to ensure that all required alerts are sent to the appropriate target owner/teams mail lists. The target owners (Cloud Operations) can create their own notification rules but would not be able to edit or administer the Incident Notification rules defined by EM Admin.
- **Master Notification Groups** – These are the groups that drive all notifications to the target owners for SaaS (FA HCM, FA CRM), JaaS (Java as a Service), DaaS (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 EM team. At the provisioning of service/infrastructure components, EMCLI scripts written by EM team run and targets are added to appropriate groups. The Cloud Operations team members (target owners) can create their own groups but are not permitted to update or edit the Master Notification Groups. These are also the groups used to audit the application of templates for the on-call person in the Cloud EM team.
- **Group Dashboards** – Cloud EM team is responsible to create the group dashboards for SaaS, PaaS, DaaS, and other systems. These are used by Cloud Operations (Service target owners) to address incidents using EM Incident Management console.
- **Service SLA and Reporting** – Cloud PM define Services and their SLAs. Cloud EM team owns setting up for all Cloud Services (definition of components, key components, key performance indicators and SLAs) within EM. The Cloud EM 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, DaaS 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 EM Discovery screens. The Infrastructure team members notify the EM team that new targets require discovery. This is done via a P2 SR to the Cloud Enterprise Manager queue. This SR is actioned by the Cloud EM 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 EM Services queue, requesting that the ME be added to the standard template and applied to all target types that apply, if required. In some cases, a ME is specific to a target and therefore, wouldn't need to be added to the Master Template. EM Team also writes MEs to meet some of their monitoring requirements. Some examples are monitor certificate expiry of SaaS and PaaS fleet instances, monitor LDAP bind check, monitor NFS availability, account expiration monitoring for SaaS instances accounts, monitor send mail queue, etc.

- Dashboards – Oracle Cloud Operations team is responsible to man the Groups (SaaS, PaaS, DaaS) dashboards 24*7 and ensure 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 usually they are 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 EM team can be requested to support via the EM Services queue. Cloud EM team may also write jobs.
- Inventory Errors– On some targets there are issues with the agent reading the oraInventory file. For the most part, this is due to permissions issues and managed by the target owners. The review and setting of file/directory permissions to ensure that the EM agent OS user can read the inventory files is the responsibility of the target owner. This is critical to ensure proper configuration management.
- Reports Creation- All required reports 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 EM team but for the most part, reports are created by the target owner.

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



Oracle is committed to developing practices and products that help protect the environment

Enterprise Manager 12c: The Nerve
Center of Oracle Cloud
January, 2013
Author: Akshai Duggal
Contributing Authors: Sudip Datta,
Nara Gogineni, Martin Pena

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

Copyright © 2013, 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.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices.

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. UNIX is a registered trademark licensed through X/Open Company, Ltd. 1010

Hardware and Software, Engineered to Work Together