
ORACLE®

Your. Open. World.

Deploying Oracle Enterprise Manager in a Secure Maximum Availability Architecture

Huaqing Wang, Senior Product Manager
Jim Viscusi, Consulting Member of Technical staff
Andrew Bulloch, Director

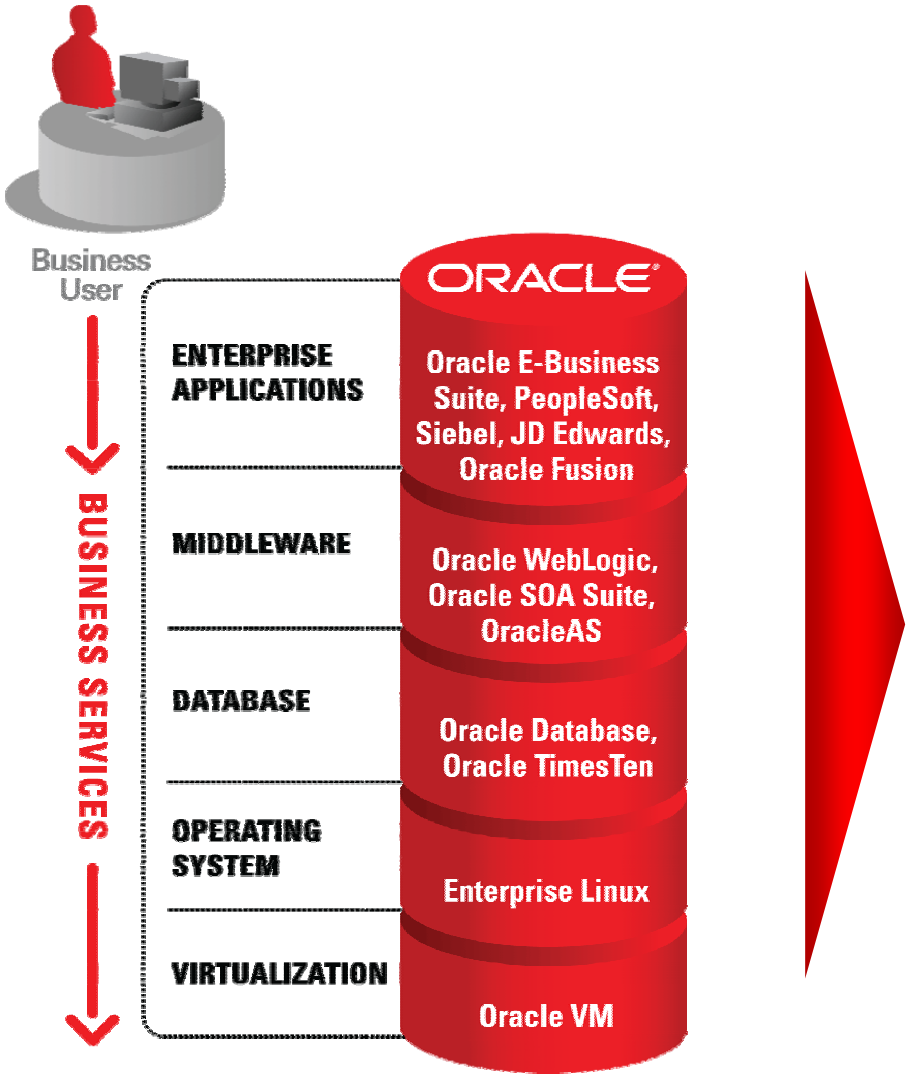
ORACLE

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

Why Oracle Enterprise Manager?

Oracle's Complete Enterprise Software Stack

Built-in & Integrated Manageability

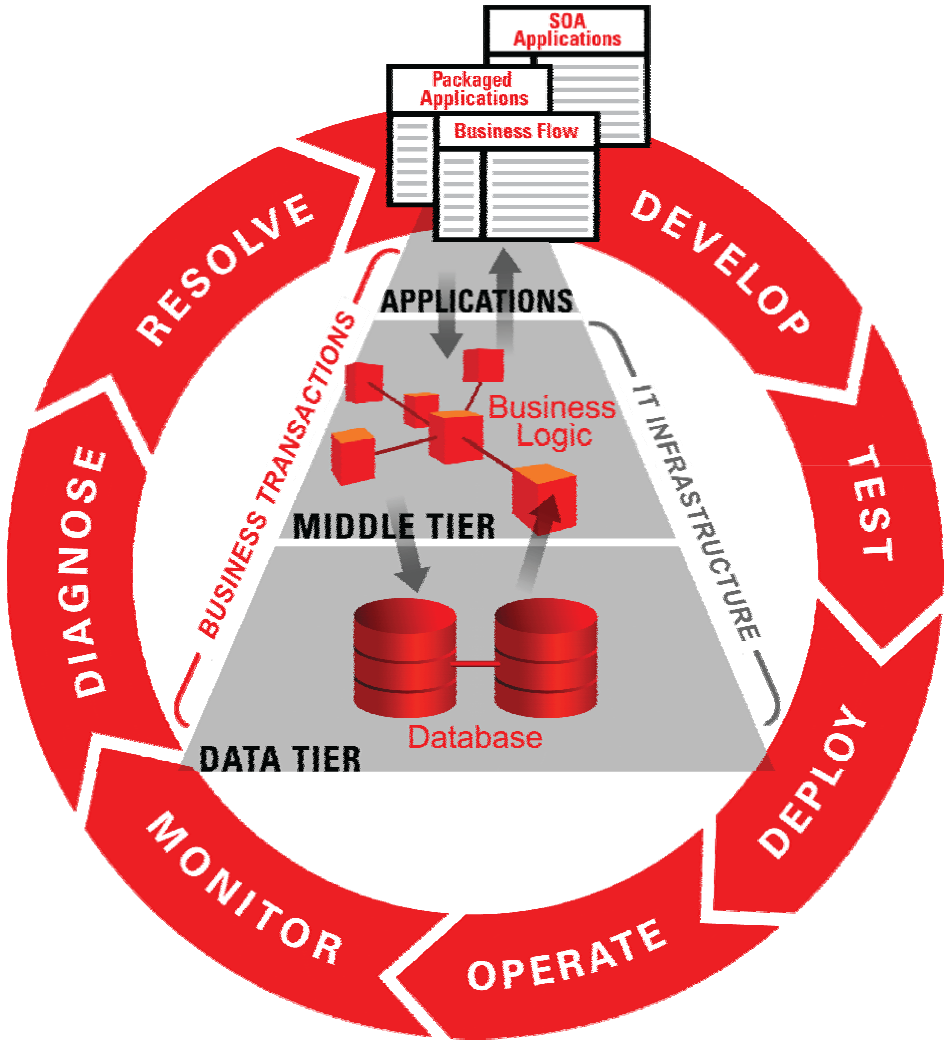


- Leader in the complete enterprise application stack
- Built-in manageability in every tier
- Integrated manageability across the entire stack

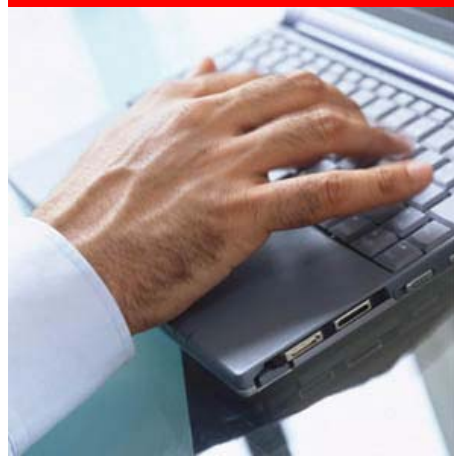
Oracle Enterprise Manager

Increases Business Efficiency

- **Manage applications top-down, from the business perspective** by understanding user experiences and business impact of IT issues
- **Manage entire application lifecycle to increase business agility** with comprehensive application quality management and compliance solutions
- **Reduce operational costs** through intelligent diagnostics and automated IT processes



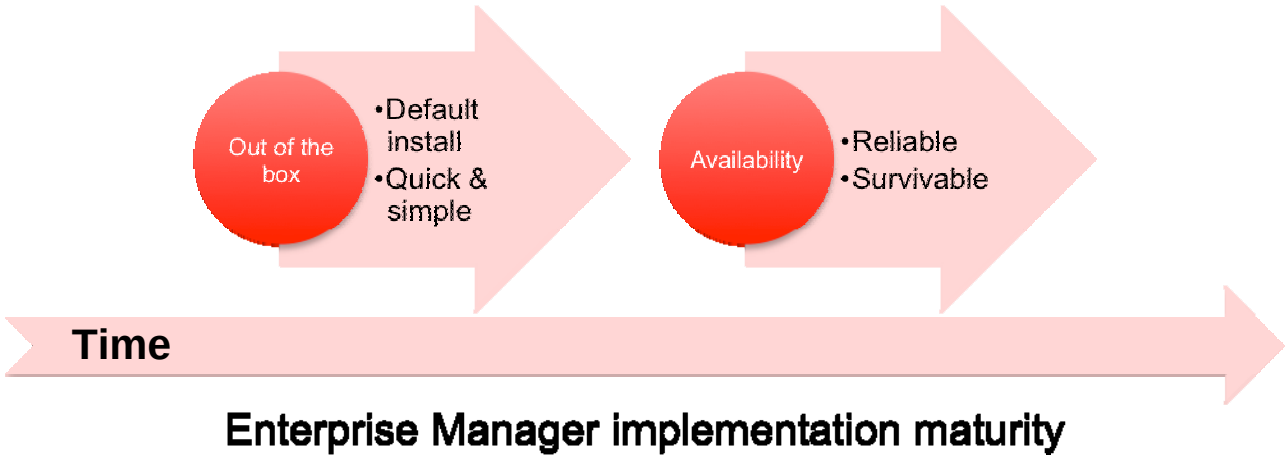
Agenda



- Oracle EM Maximum Availability Architecture (MAA) best practices
- Oracle EM security best practices
- Oracle EM A3 best practices
- Q&A

Best Practices: Deploying Oracle Enterprise Manager in Maximum Availability Architecture

Customer implementations



In this section we want to discuss the key design decisions and alternatives when deploying EM in a highly available manner

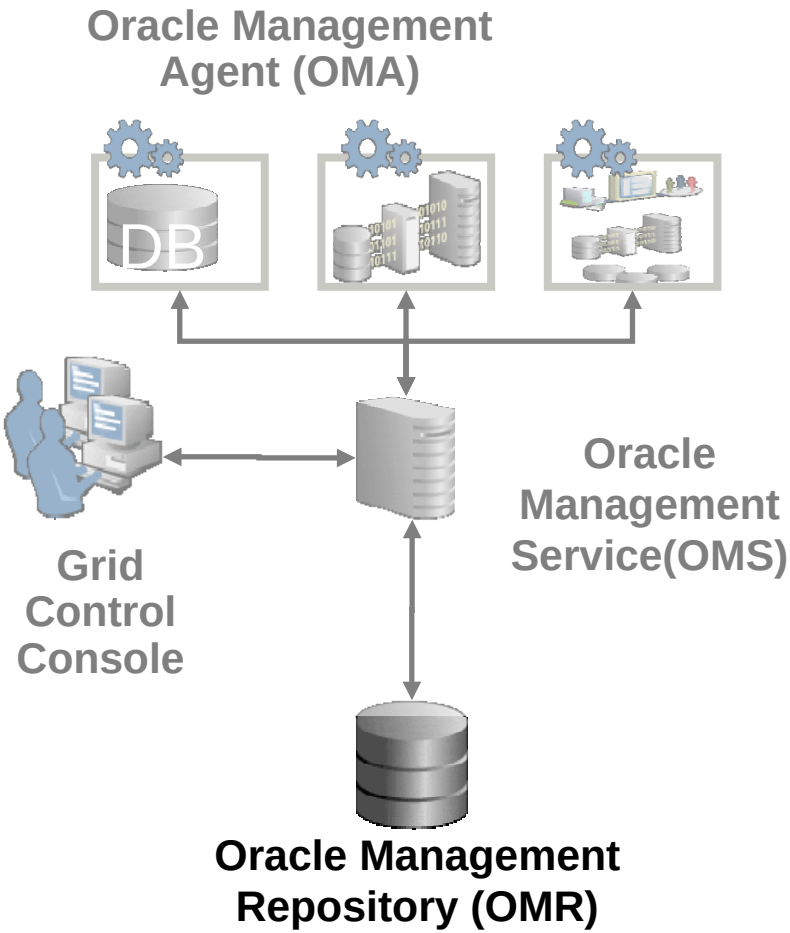
Oracle Enterprise Manager MAA Best Practices

- Degrees of protection
  - Backup and recovery
  - Active/Passive mode
  - Active/Active mode
  - Disaster recovery

MAA: Backup and Recovery

MAA: Backup And Recovery

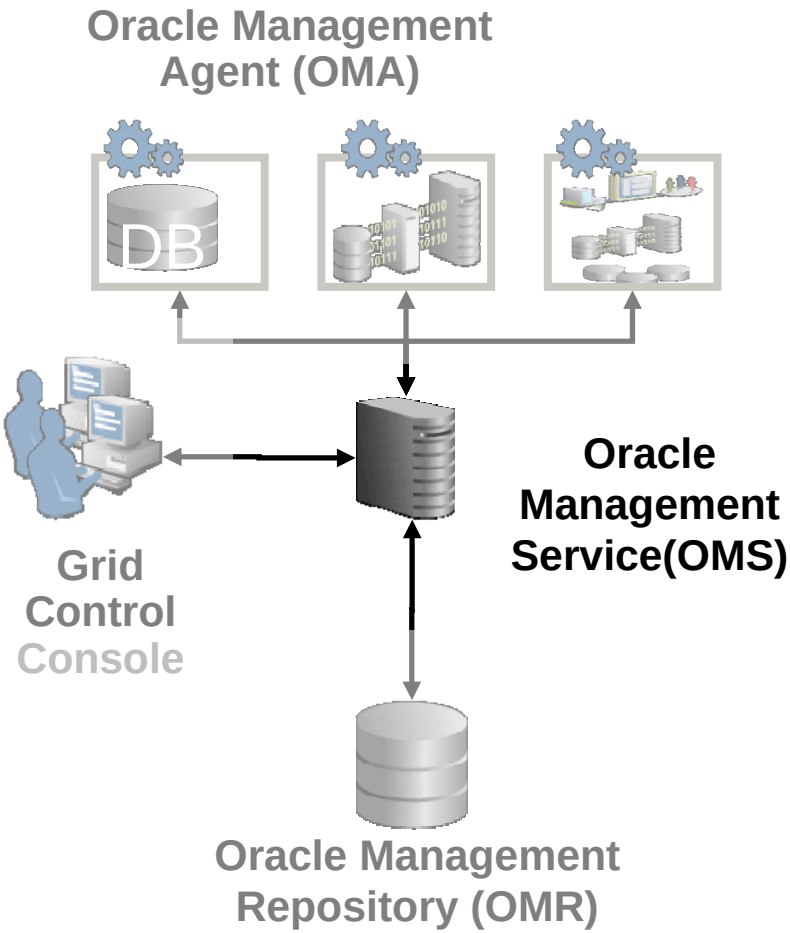
Oracle Management Repository



- Use standard database tools for any database backup and for recovery
- **Case 1:** Full recovery on same host -- No special consideration for EM
  - On new host, modify repository target
- **Case 2:** Partial/Point-in-time recovery – Agent will be the source of truth and state information to resynchronization
  - **emcli resync repos**

MAA: Backup And Recovery

Oracle Management Service



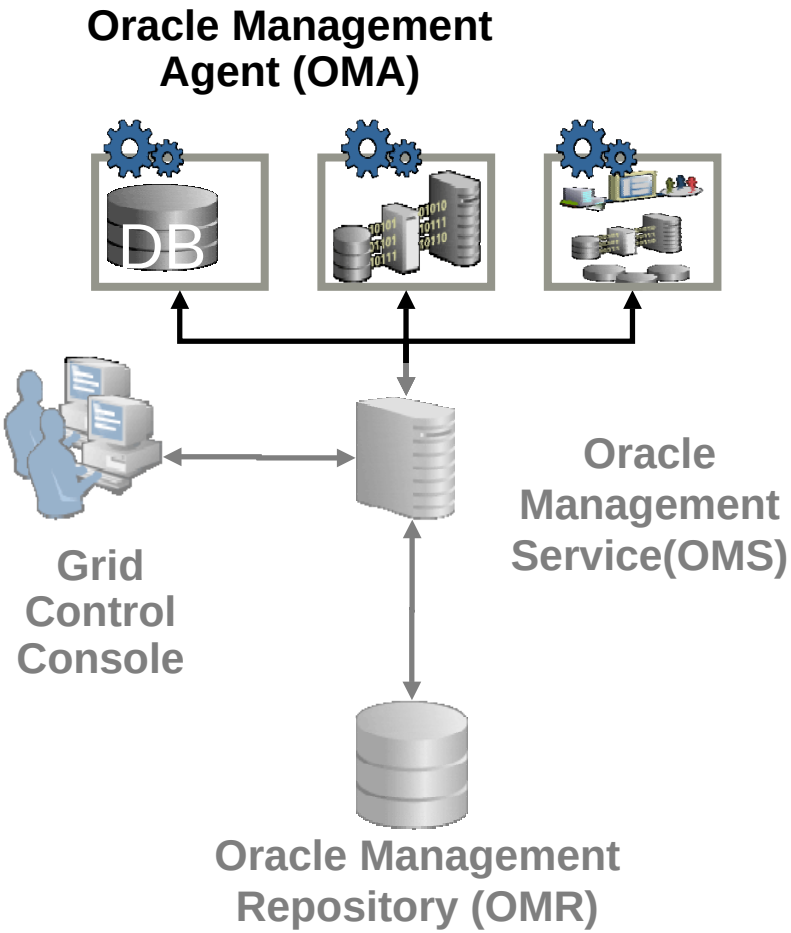
- Oracle Management Service is (mostly) stateless
- Protect /state and /upload directory with some forms of disk mirroring
- Backup OMS config with:
  - **emcli exportconfig**

- **Method 1:** Backup/Restore the software directory structure
  - restore that to the same directory path
- **Method 2:** Reinstall from the original media

- Restore OMS configuration
  - **emcli importconfig**

MAA: Backup And Recovery

Oracle Management Agent

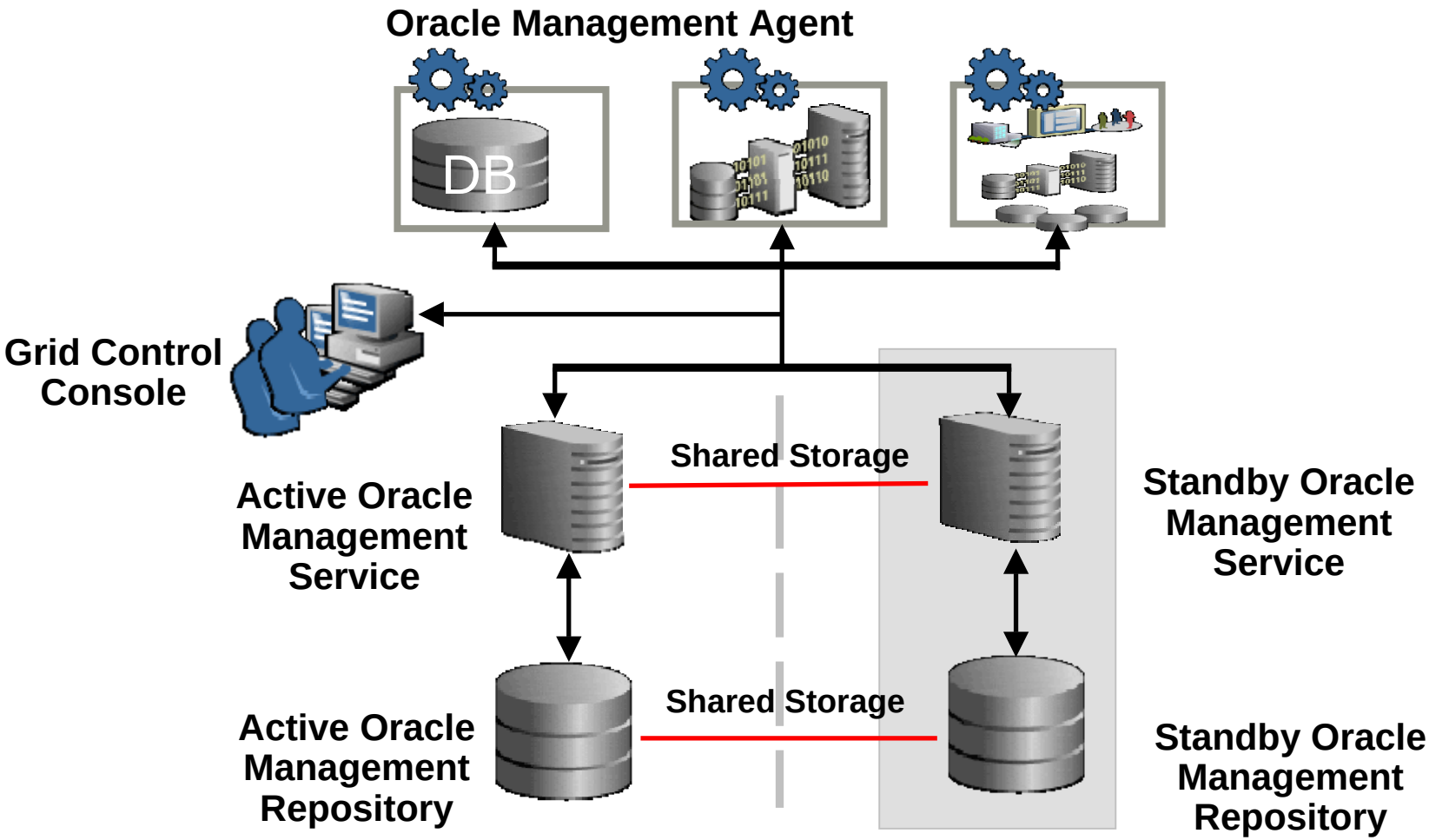


- **Method 1:** Disk backup and restore
- **Method 2:** Reinstall from the original media
- Repository will be considered as the source of truth
  - Rebuild state information from Repository
  - **Emcli resyncagent**

MAA: Active/Passive Mode

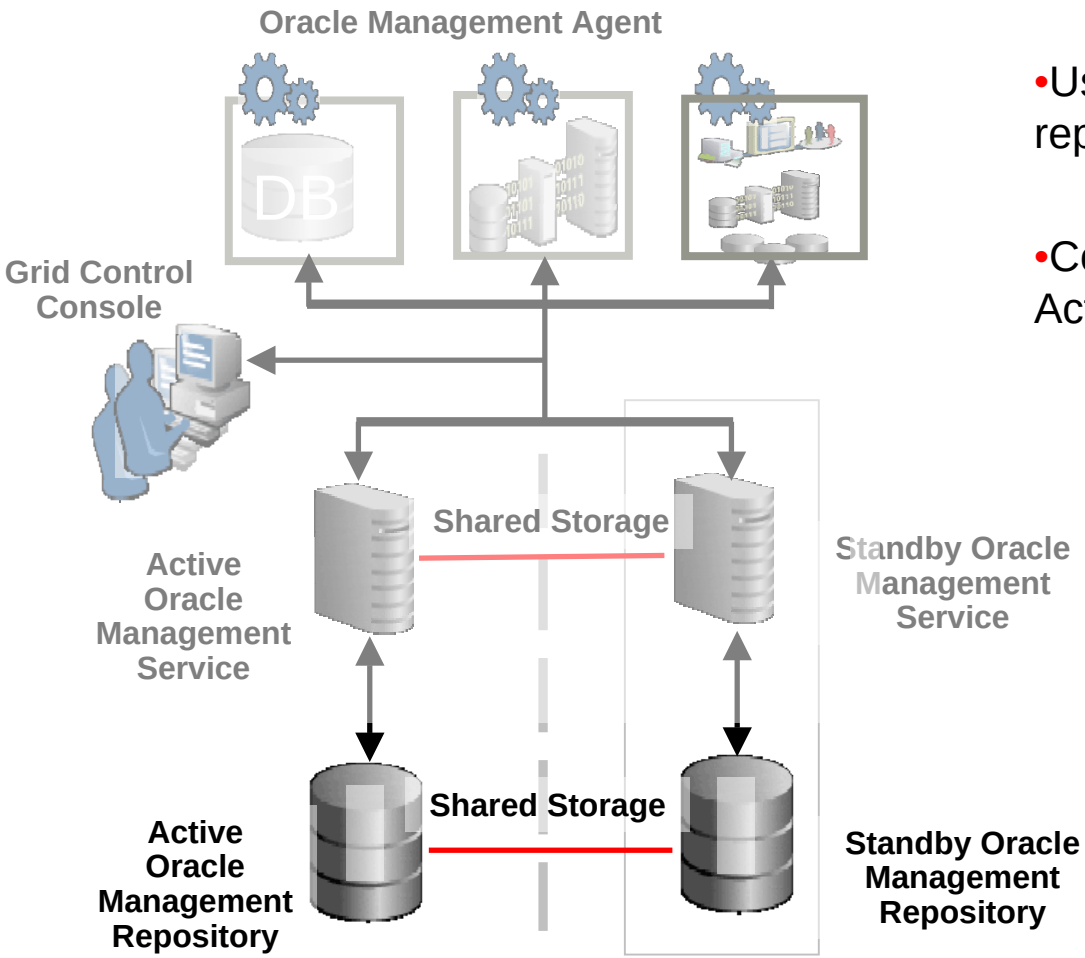
Maximum Availability Architecture

Active/Passive (*blackout* during failover)



MAA: Active/Passive Mode

Oracle Management Repository



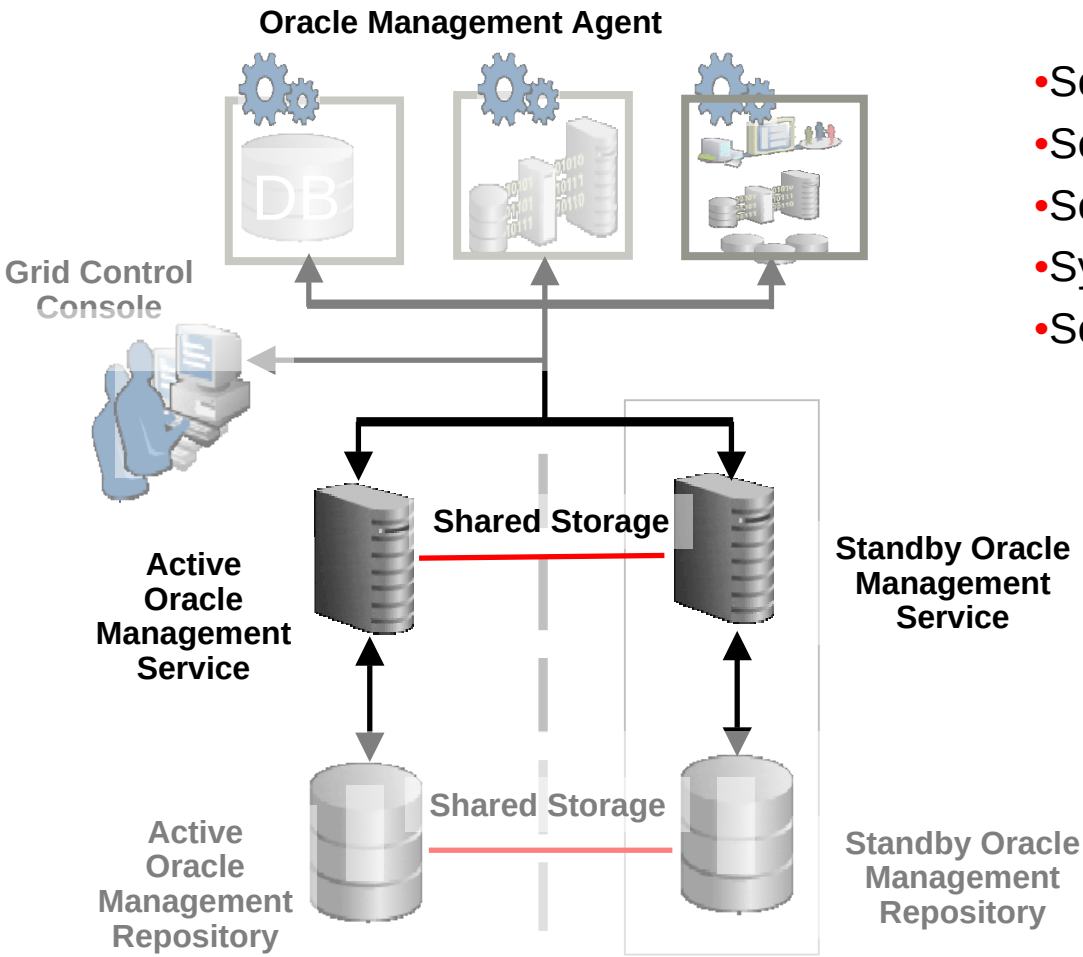
- Use Data Guard for passive repository

  Or

- Configure the database for Active/Passive failover

MAA: Active/Passive Mode

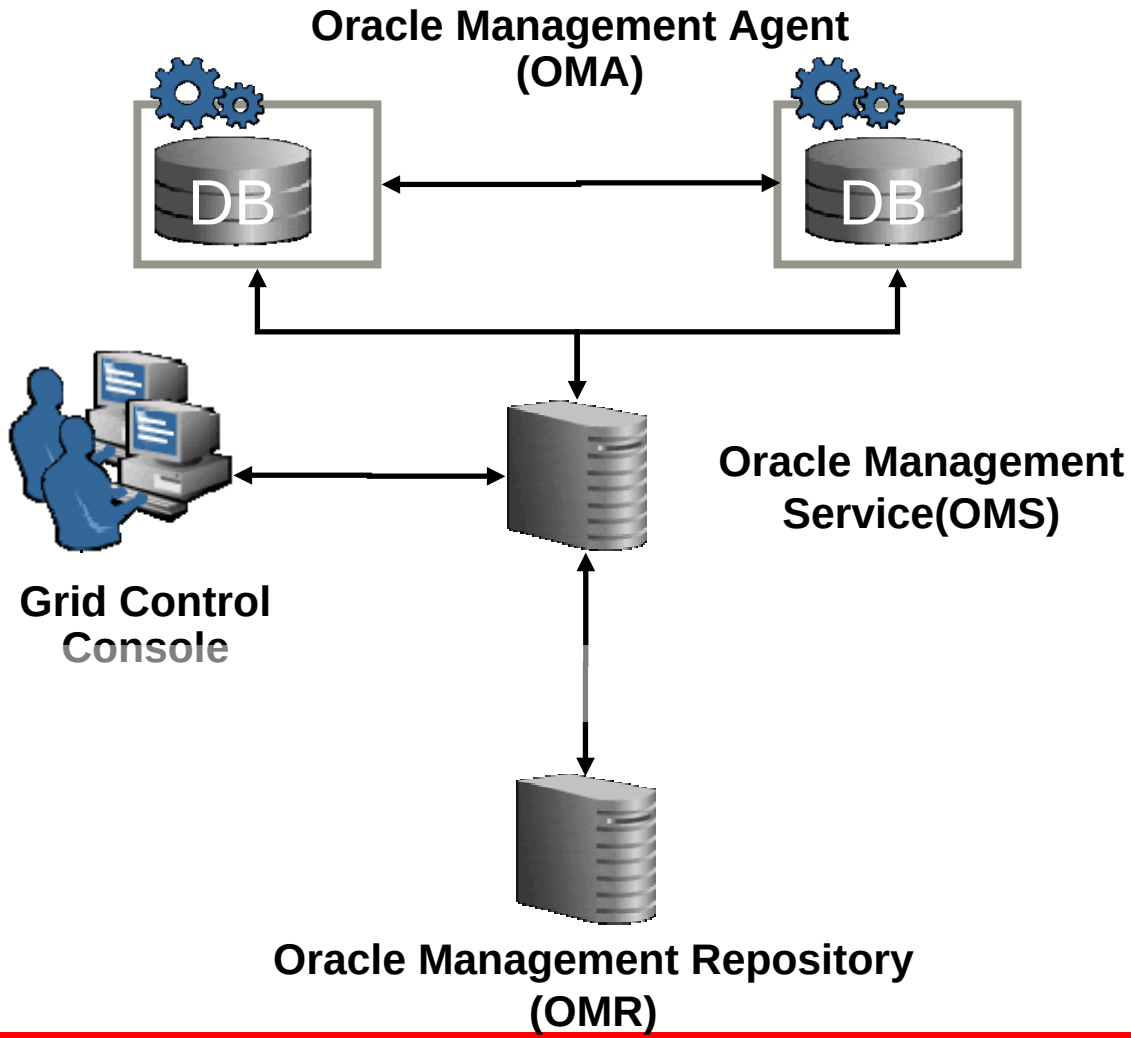
Oracle Management Service



- Setup the virtual hostname/VIP
- Setup shared storage
- Setup operating system
- Synchronize OS user IDs
- Setup shared inventory

MAA: Active/Passive Mode

Oracle Management Agent

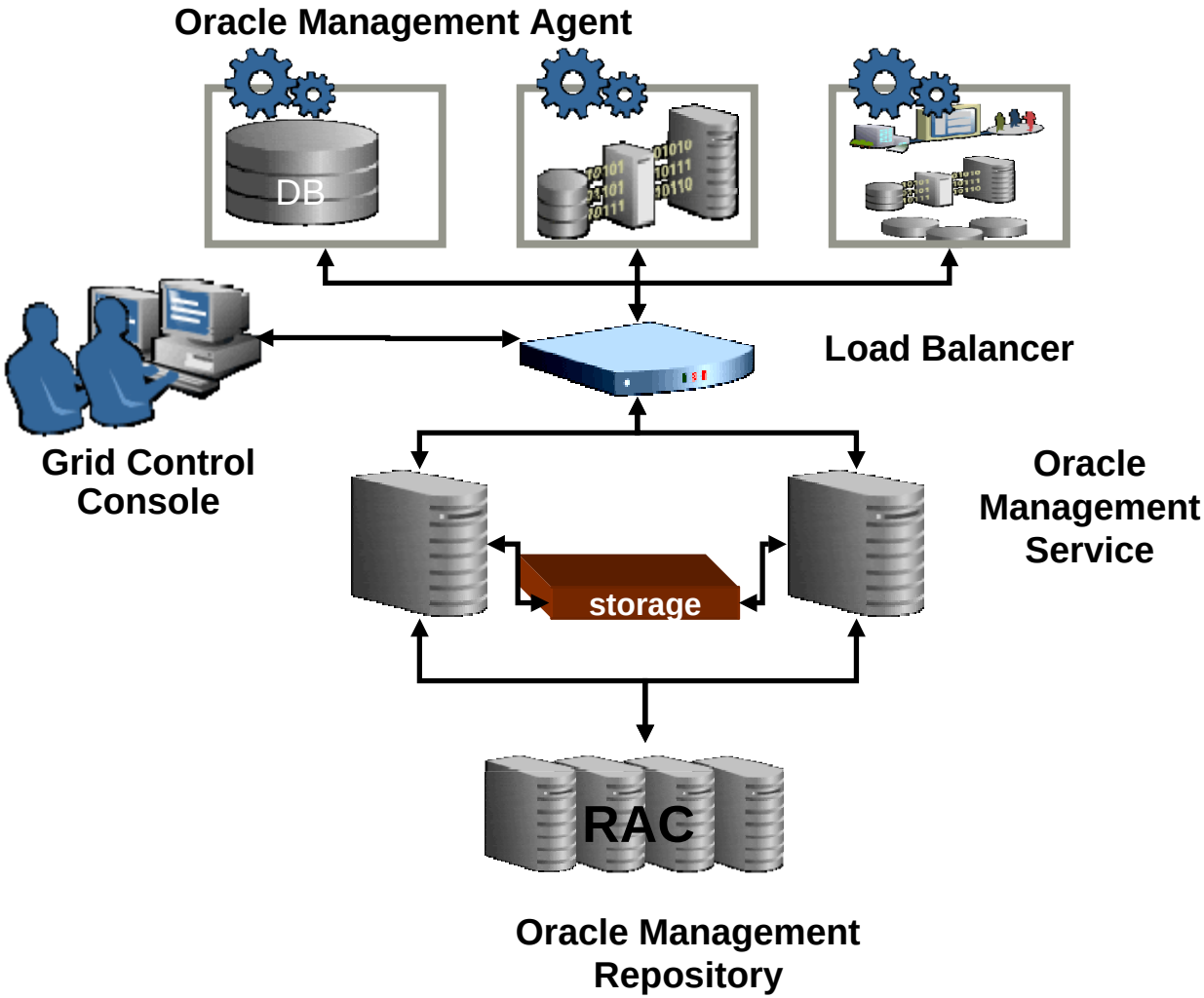


- Install 1 agent per host
- Install the EMCLI
- Install Active/Passive targets using shared storage and clusterware
- Discover targets as normal
- Use EMCLI command relocate target to moving monitoring between agents
- **emcli relocate target**

MAA: Active/Active Mode

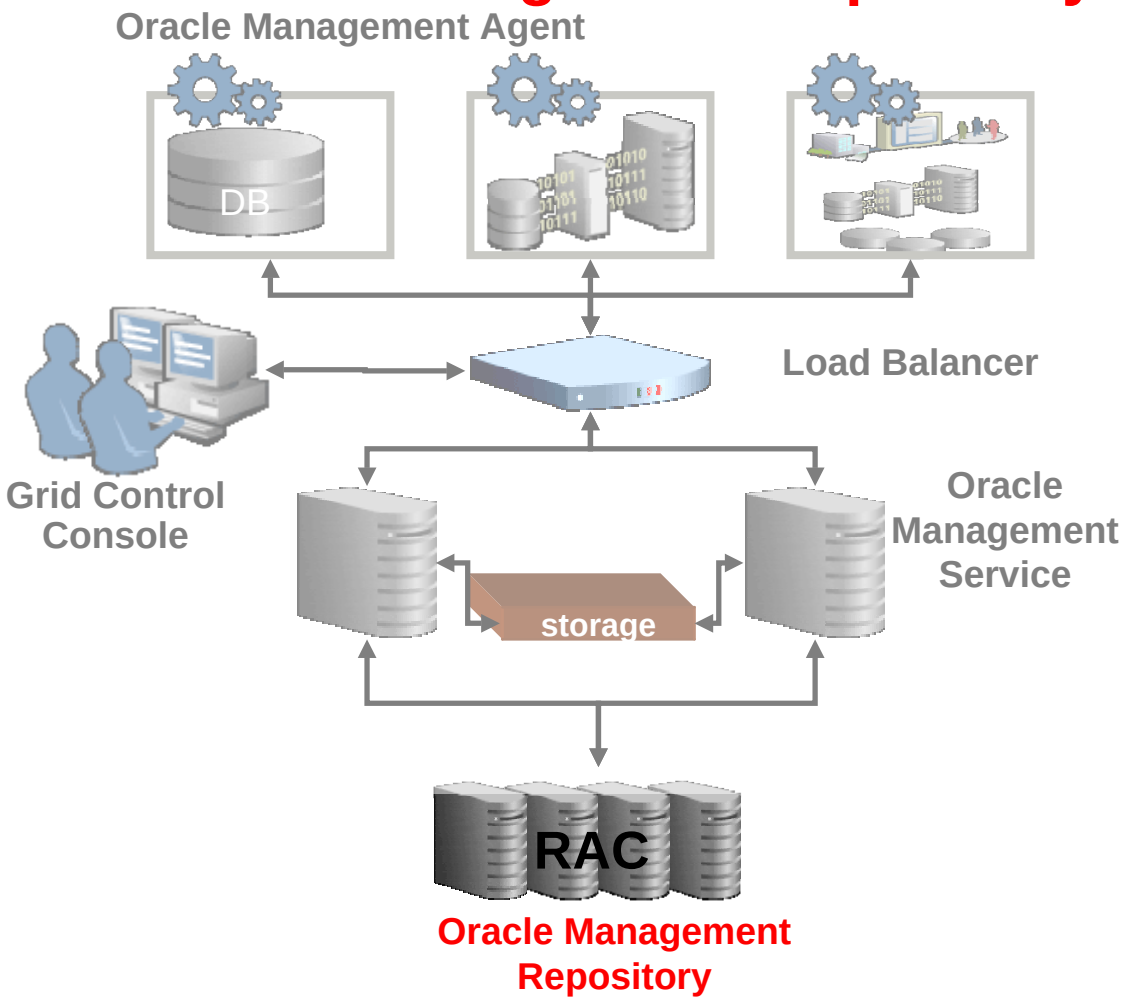
Maximum Availability Architecture

Active/Active Mode (*brownout* during failover)



MAA: Active/Active Mode

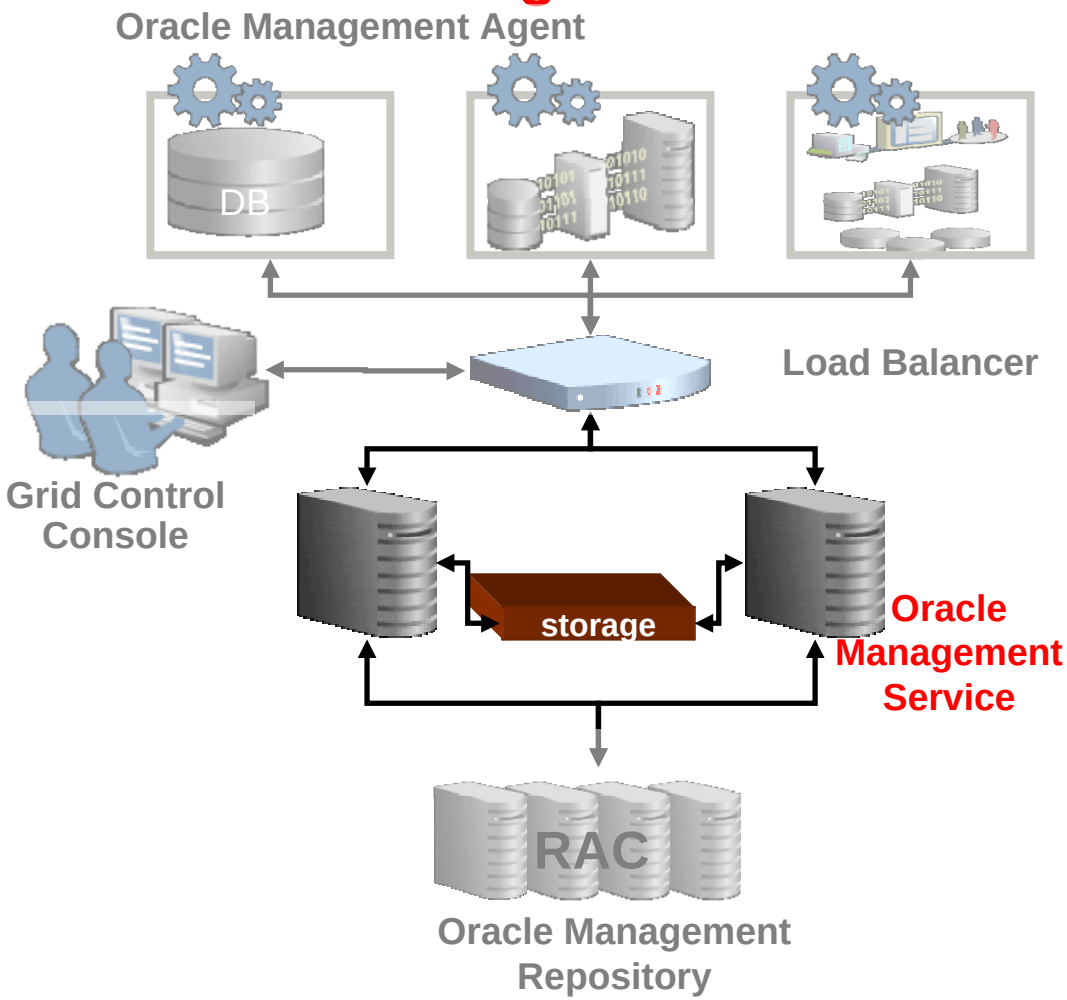
Oracle Management Repository



- Latest certified DB version with RAC
- ASM as storage technology
- Best practices for Database MAA
- Configure Fast Connection Failover

MAA: Active/Active Mode

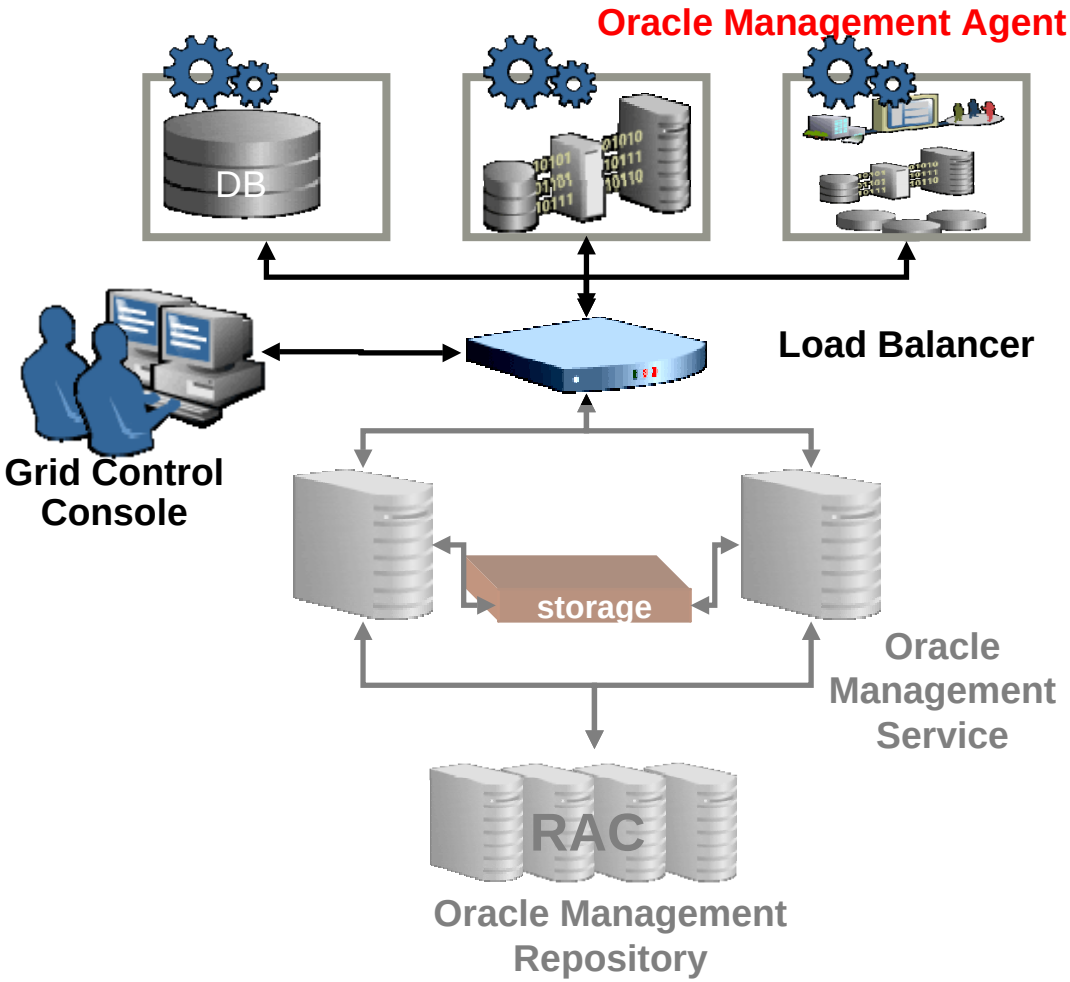
Oracle Management Service



- Appropriate OMS Installation Location (Network Latency)
- Best practices for Application Server MAA
- Configure the shared file system load directory
- Configure connection string

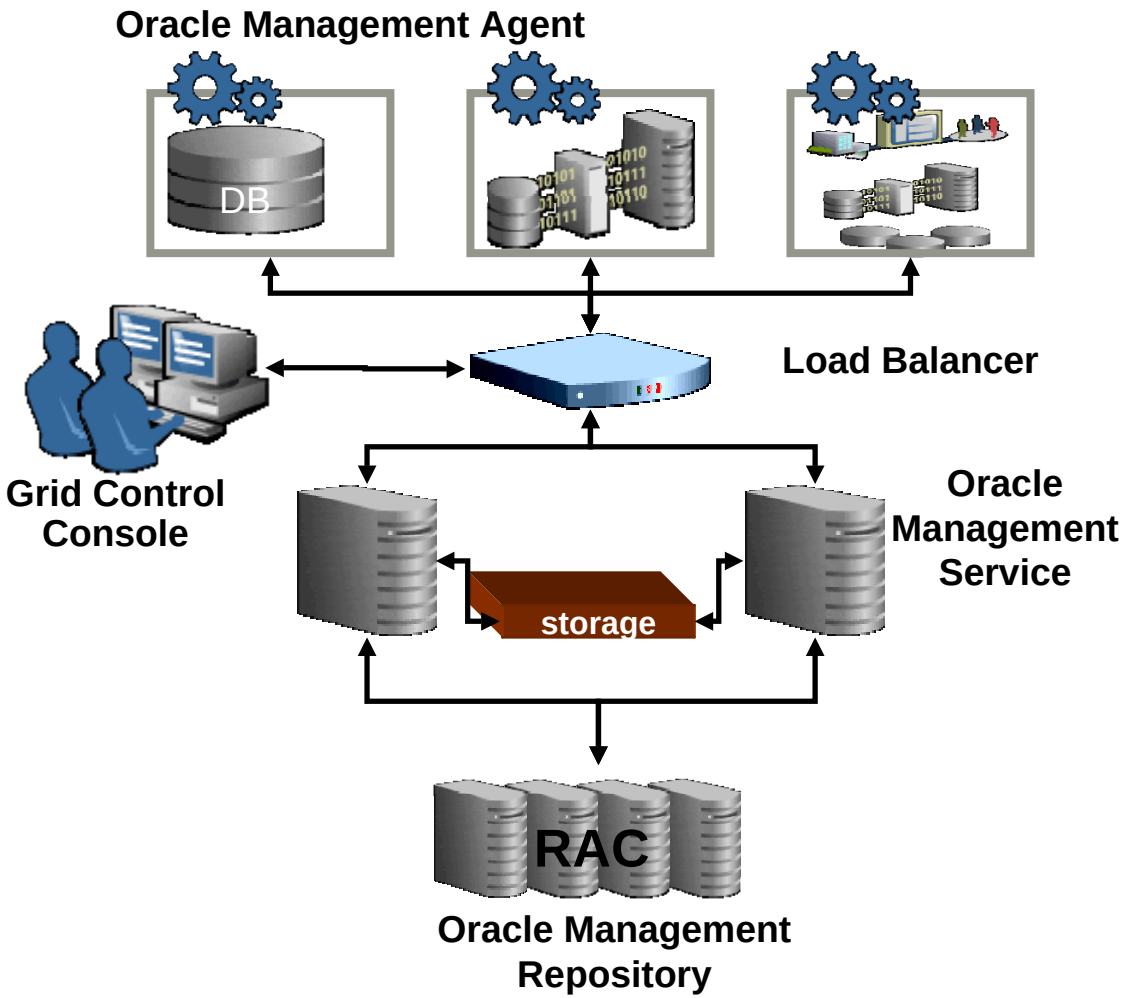
MAA: Active/Active Mode

Oracle Management Agent



- Agent HA feature: watchdog process
- Configure Agent to communicate through SLB
- Configure Agent to allow retrofitting SLB

Summary: Active/Active Mode

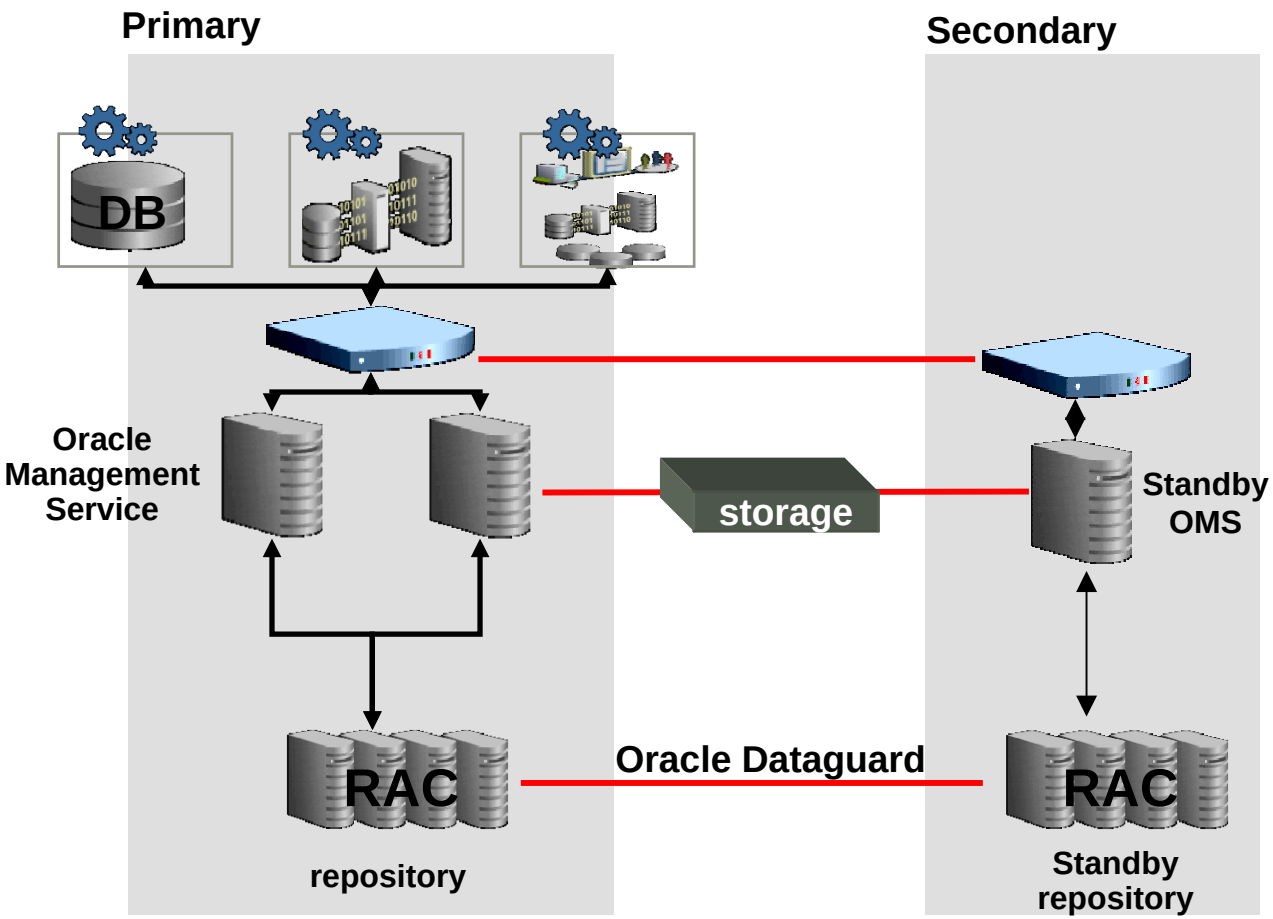


- MAA Solution combines redundancy at all tiers
  - Agent ←→ Multiple OMS using Load Balancer
  - OMS ←→ Multiple RAC Nodes using SQL*Net
  - Repository: RAC and Hardware
- Reliable and scalable
- Automated operations
- No perceived loss of service

MAA: Disaster Recovery

Maximum Availability Architecture

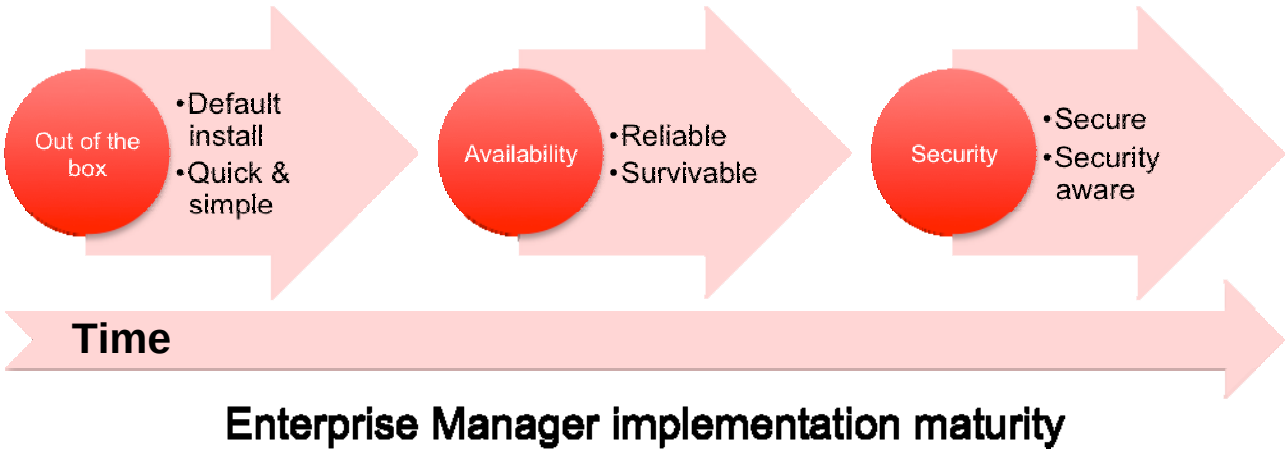
Disaster Recovery



- Physical standby database
- Fast Start Failover and the Oracle observer
- Data Guard Broker for management
- Redundant OMS
- Extend FCF/ONS to automate connection switchover

Best Practices: Deploying Oracle Enterprise Manager securely and/or in a secure environment

Customer implementations



In this section we want to discuss the key design decisions and alternatives when deploying EM in a secure way and in secured environments

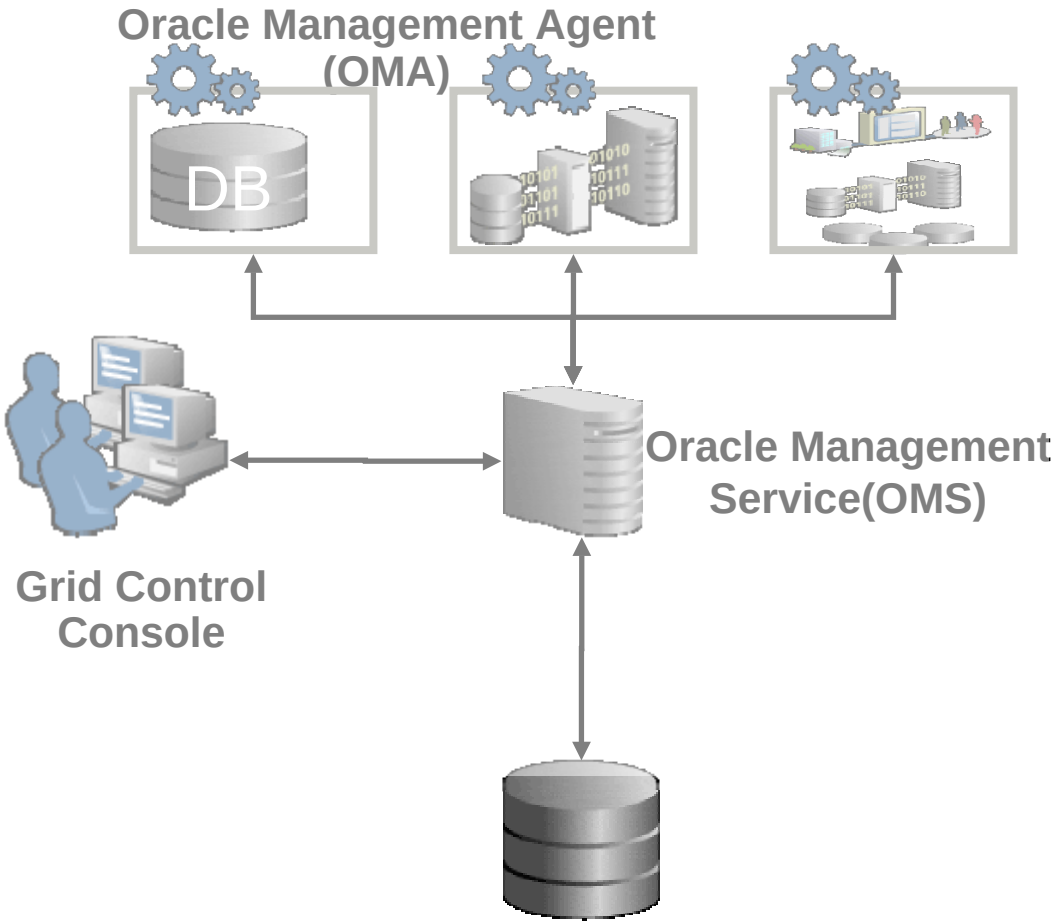
Oracle Enterprise Manager Security Best Practices

- Let’s break this wide ranging topic down into three areas
  - Secure individual Enterprise Manager components
  - Secure communication between Enterprise Manager components and managed targets
  - Firewalls, deploying EM in a secure environment

Security: Securing individual Oracle Enterprise Manager Components

Deploying Secure Enterprise Manager

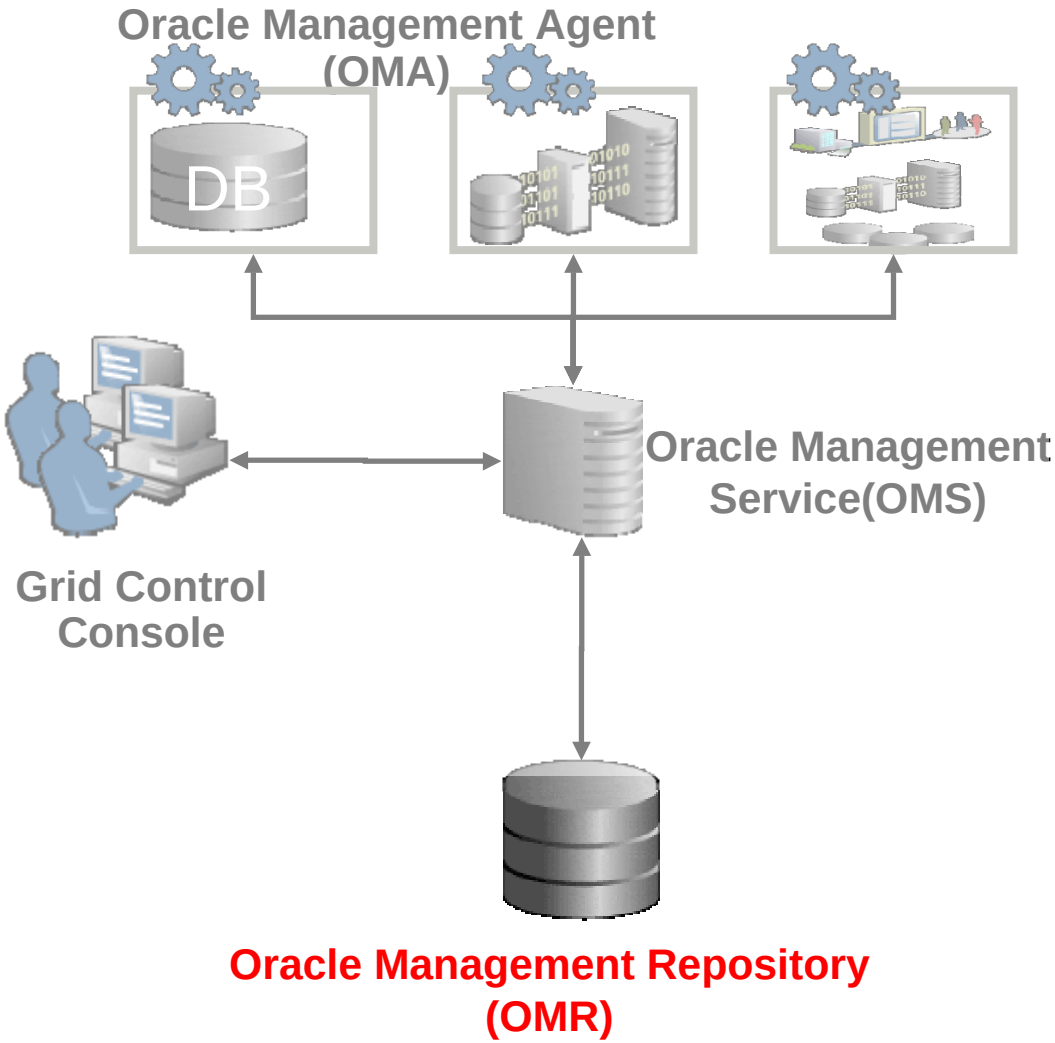
Oracle Management Repository



- Follow best practices for securing the Oracle Database (e.g. Oracle Database Security Guide)
  - Revoke EXECUTE on UTL_FILE, UTL_TCP, etc
  - Ensure well-known accounts locked down
  - Shut off XDB as it's not required
  - One exception is enforcement of resource limits !
- Enable password profile for EM users
  - enforce some complexity & ageing
  - MGMT_VIEW should be exempt
  - exercise caution with lock out !

Deploying Secure Enterprise Manager

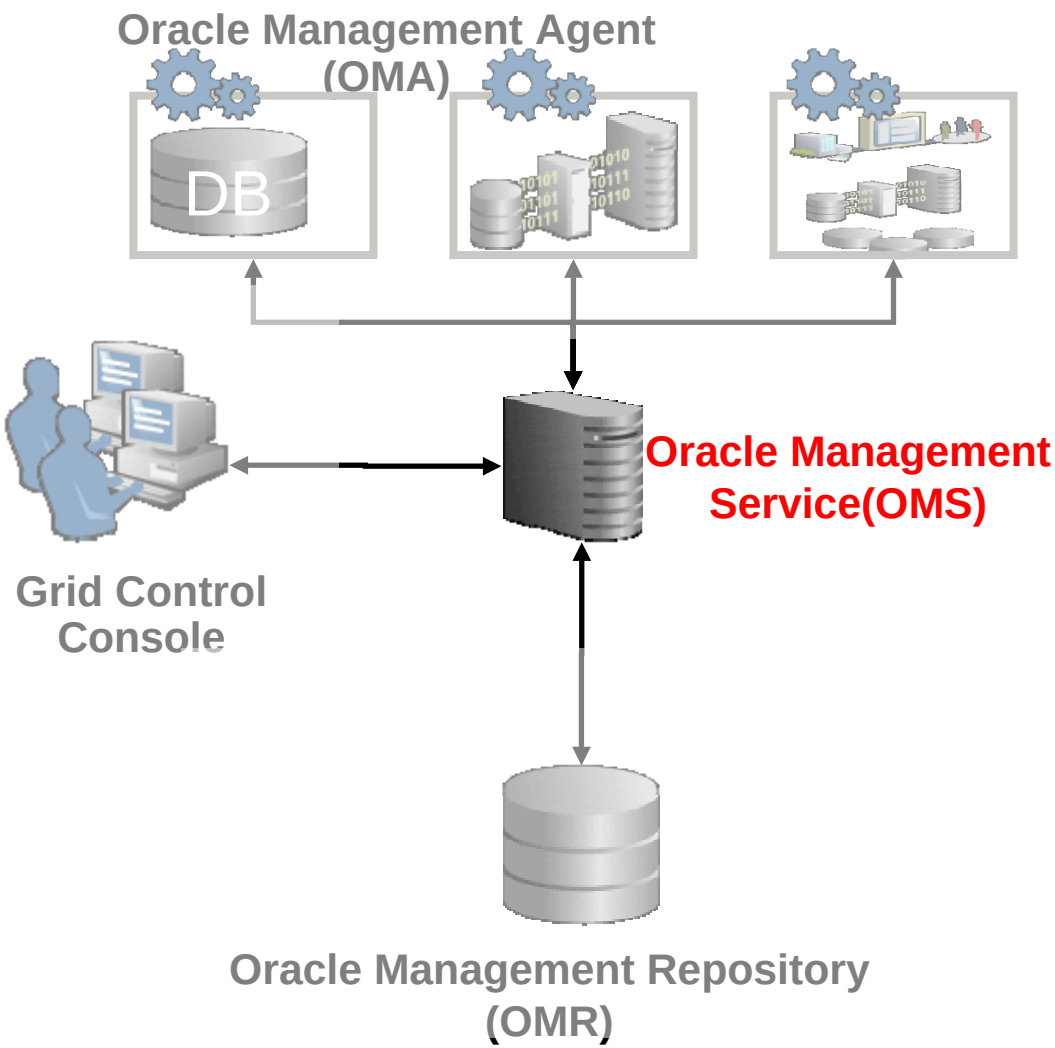
Oracle Management Repository



- Restrict access to the repository host
  - Restrict network access to the repository host
  - Disable remote login
  - For extra paranoia you can restrict listener in-bound connections on a defined IP range
- Enabled auditing
  - Ensure audit_file_dest has restricted permissions to prevent sys users from modifying audit data
  - Audit all SYS operations (audit_sys_operations=true)
  - Supplement this with application logging (more later)

Deploying Secure Enterprise Manager

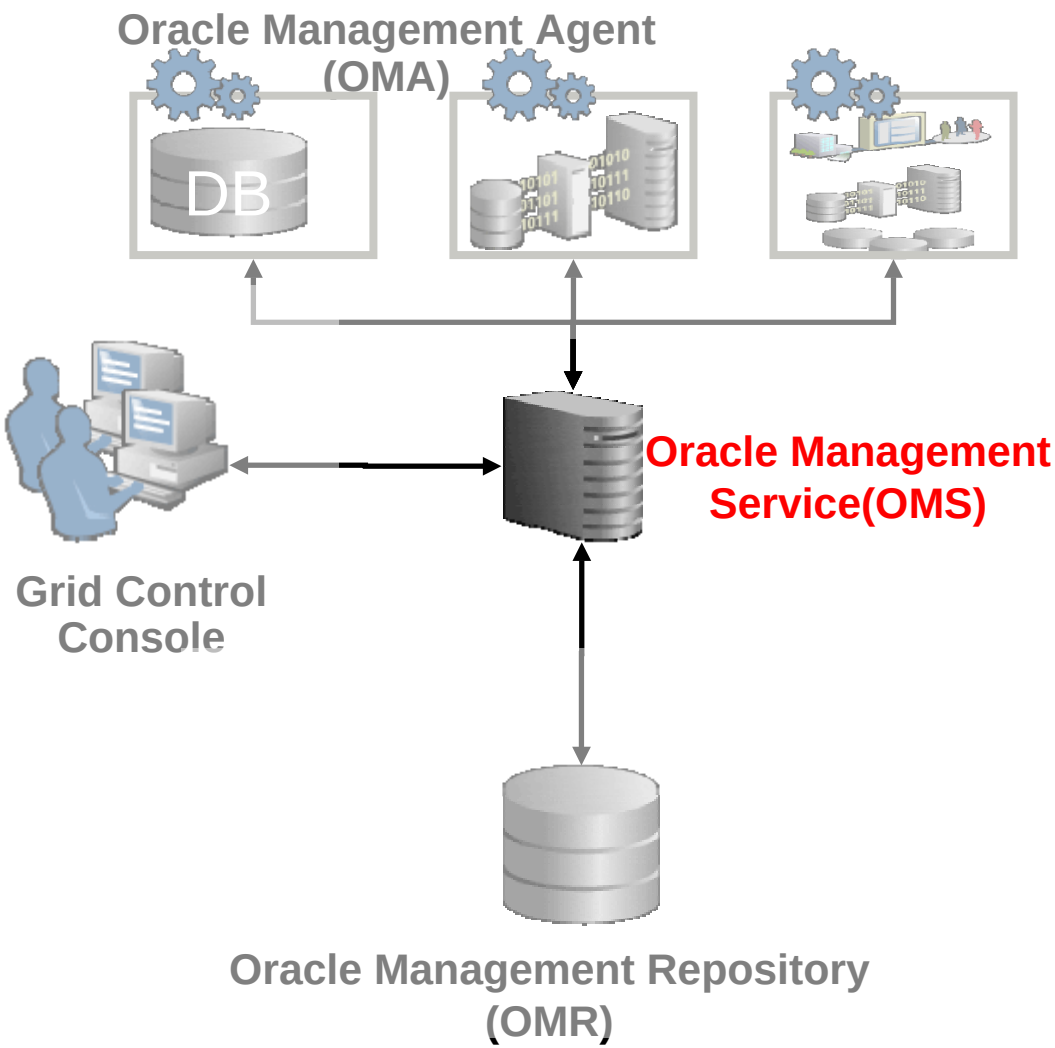
Oracle Management Service



- Follow best practices for securing Oracle Application Server
  - Stop non-essential services in the OMS home
  - Apply CPU patches to the OMS tier AS home
- Remove all un-secured services from OMS machines (httpd, portmap, etc)
- Restrict access to all un-secured console URLs
  - Ensure you run the OMS in 'secure lock' mode
  - Modify OHS configuration to prevent un-secure access to UI console through an OMS

Deploying Secure Enterprise Manager

Oracle Management Service



- Stop SYSMAN being the enterprise login for all DBA's !!
- Prevent SYSMAN from logging into the Console :

```
delete from
mgmt_created_users
where user_name =
'SYSMAN'
```

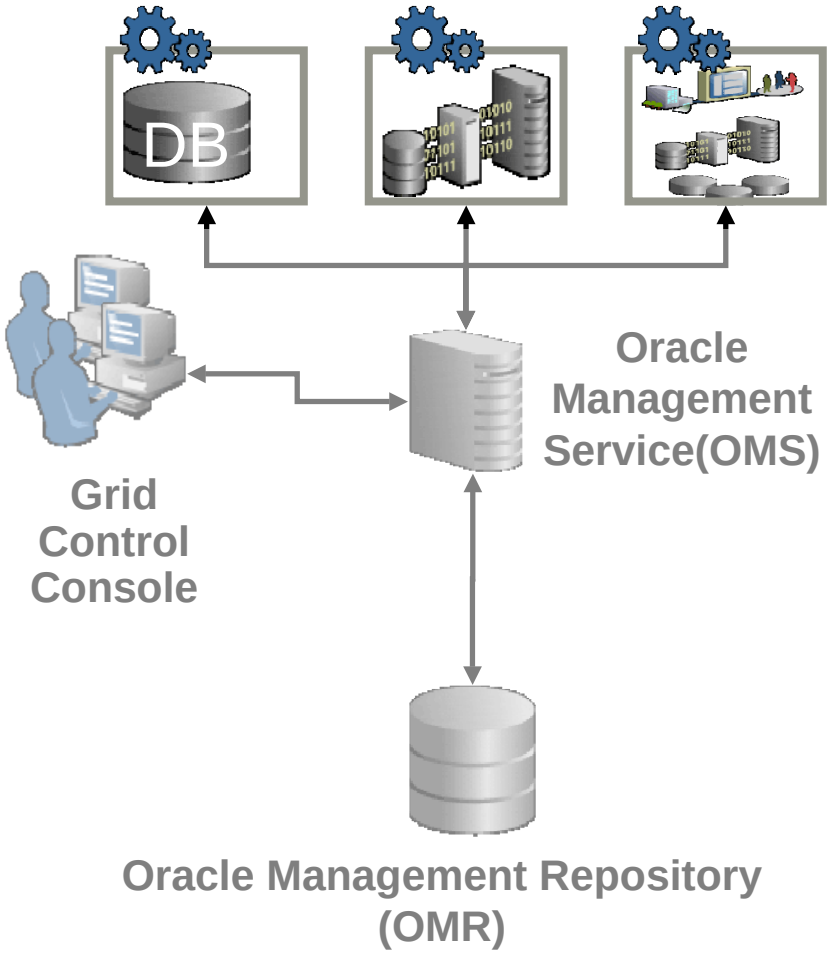
- Unlock the account using the following :

```
insert into
mgmt_created_users
(user_name,
system_user)  values
('SYSMAN', 1)
```

Deploying Secure Enterprise Manager

Oracle Management Agent

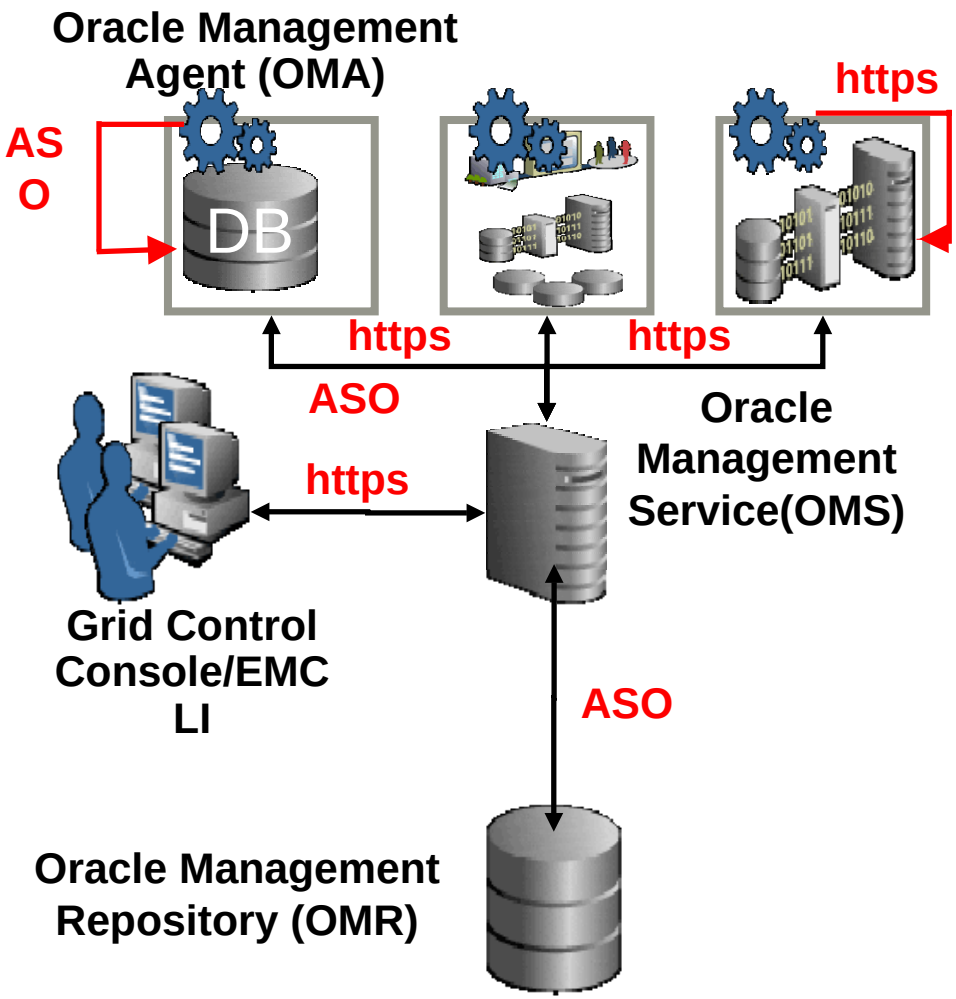
Oracle Management Agent (OMA)



- Use one-time registration passwords with a reasonable expiry date
  - Prevents un-authorised agents and systems being incorporated
- Ensure that agents are secured when communicating with the OMS
- Install the latest CPU when available
  - Agent homes are based on DB RSF's so may also be subject to published CPU's
- Support only impersonation based access to this account post-install
  - For patching this needs to be suspended
  - Next release addresses this in patch process

Deploying Secure Enterprise Manager

Securing communication between EM components



- Secure transport between OMS & Repository DB and OMS and managed targets
  - Enable Advanced Security Option(ASO) between OMS and OMR
  - Enable ASO between OMS and Oracle Database targets managed by EM
- All OMS-OMA communication should run in secure-lock mode
- Secure Grid Control Console communication with OMS
- Use a certificate from well-known CA(Certification Authority)
  - Be wary of certificate lifetime
  - Next release will also address certificate replacement

Security: Configure Enterprise Manager for Firewalls

Configuring Enterprise Manager for Firewalls

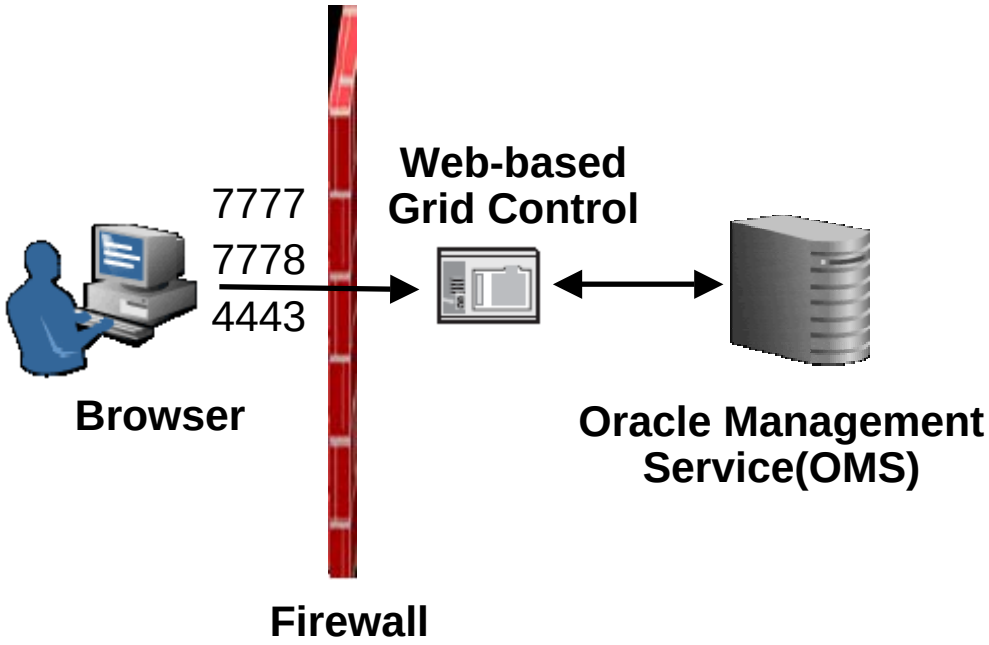
- Firewalls are commonplace in most mature and modern IT infrastructures
- Two areas where EM and Firewalls will interact
  - Enterprise Manager needs to navigate through them when EM components are separated by firewalls
  - Enterprise Manager needs to communicate with managed targets that are themselves behind or protected by firewall
- Enterprise Manager 10g is designed to cope with both these cases *but*….
- …this is one of the least understood areas when deploying EM in a secure environment

Configuring Enterprise Manager for Firewalls

- Lot's of different permutations with EM when dealing with Firewalls….
  - Firewall between your browser and the Grid Grid Control
  - Configuring OMA on a host protected by a firewall
  - Configuring OMS on a host protected by a firewall
  - Firewalls between OMS and OMR
  - Firewalls between the Grid Control and a managed database target
  - Firewalls used with multiple OMS
  - Configuring firewalls to allow ICMP and UDP for Beacons
  - …….
- Let's take a tour through some of these

Configure EM For Firewalls

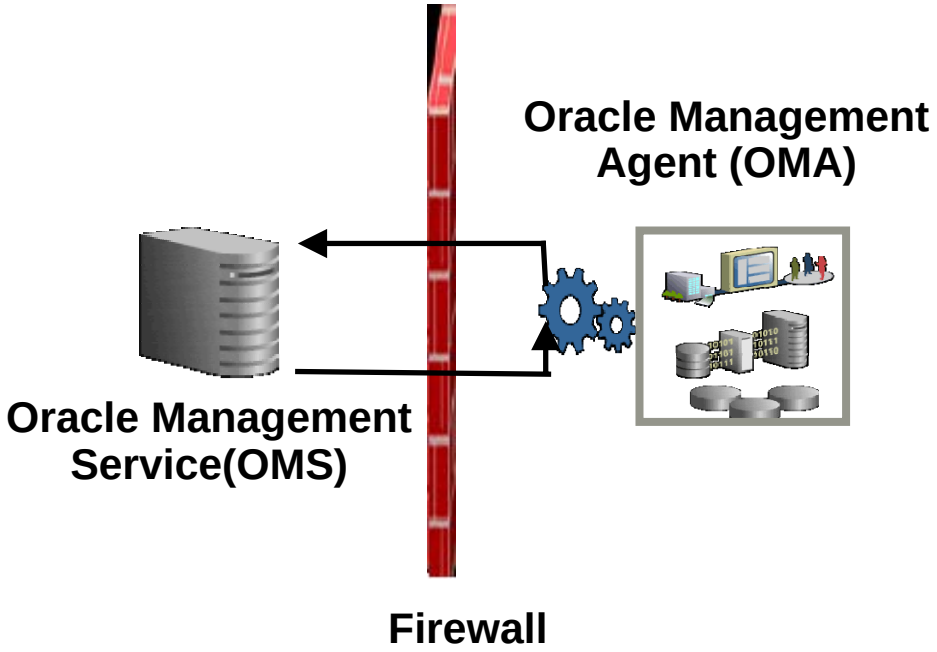
Firewall between browser and Grid Control Console



- Configure the firewall to allow the Grid Control Console to receive HTTP traffic over port 7778
  - Or 7777 if you're using the Web Cache in the OMS home
- If the EM Console has been secured (as mentioned earlier), configure the firewall to allow https traffic over port 4443

Configure EM For Firewalls

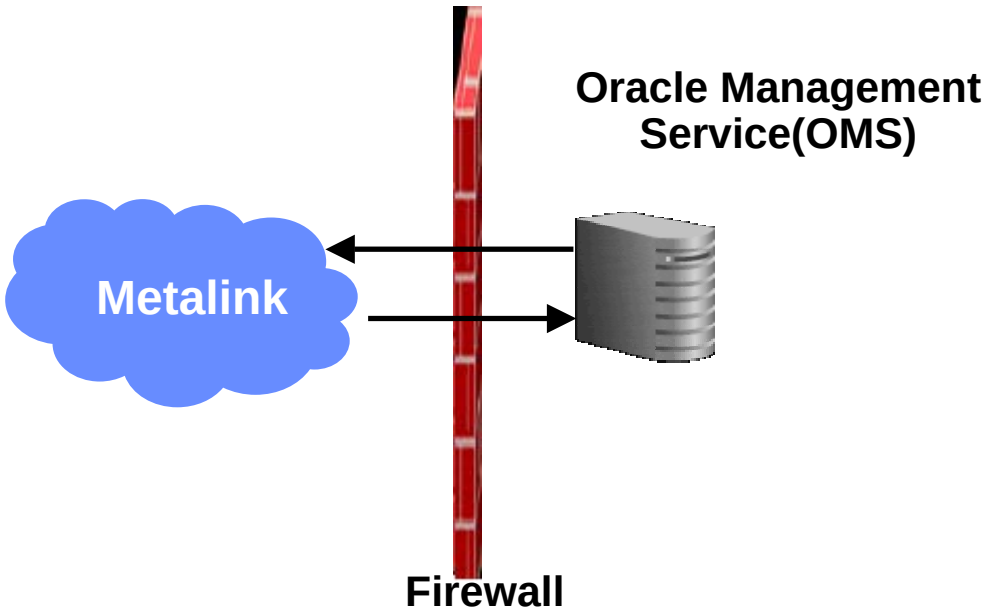
Configuring OMA on a host protected by a firewall



- Configure Oracle Management Agent to use a proxy server
  - Using settings in emd.properties
  - REPOSITORY_PROXYHOST
  - REPOSITORY_PROXYPORT, etc
- Configure the firewall to allow inbound communication from the OMA to the OMS
  - Port 1159 (by default)
  - Port range 4898-4989 (if non-default)
- Configure the firewall to allow outbound communications from the OMS to OMA
  - Port 3872 (default)
  - Port 1830-1849 (if non-default)

Configure EM For Firewalls

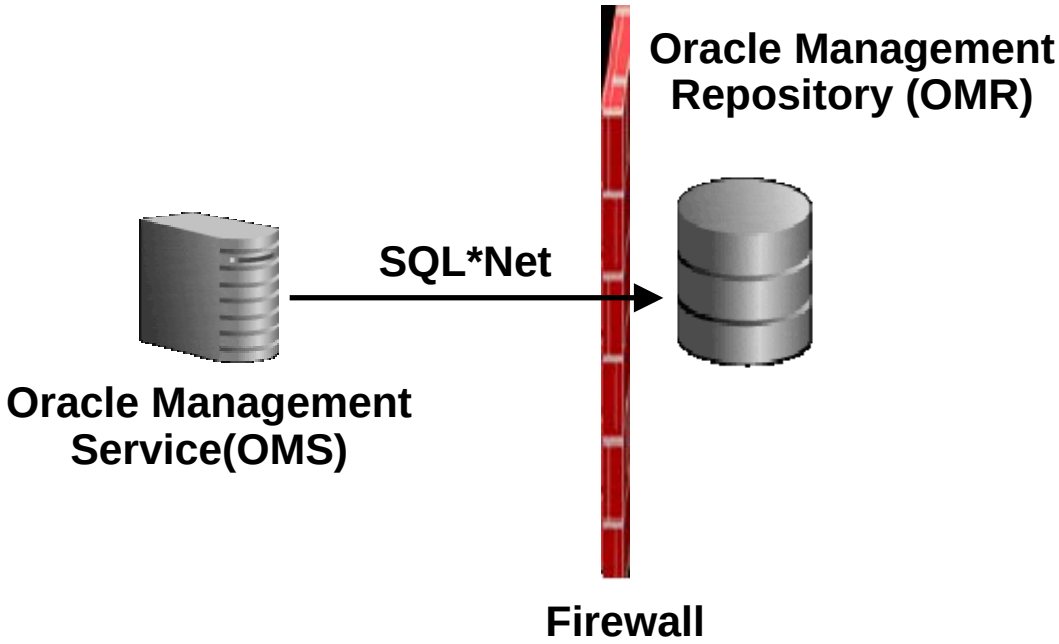
Configuring OMS on a host protected by a firewall



- Link out to Metalink is required to obtain critical patch updates or retrieve patches
- Configure Oracle Management Service to use a proxy server
  - Use settings in emoms.properties
  - PROXYHOST
  - PROXYPORT
- “DontProxyfor” property allows for a mix with some targets/agents behind a firewall and some not
- Configure the firewall to allow punch through to Metalink
- You’ll receive a warning on the EM Console homepage if Metalink data is stale

Configure EM For Firewalls

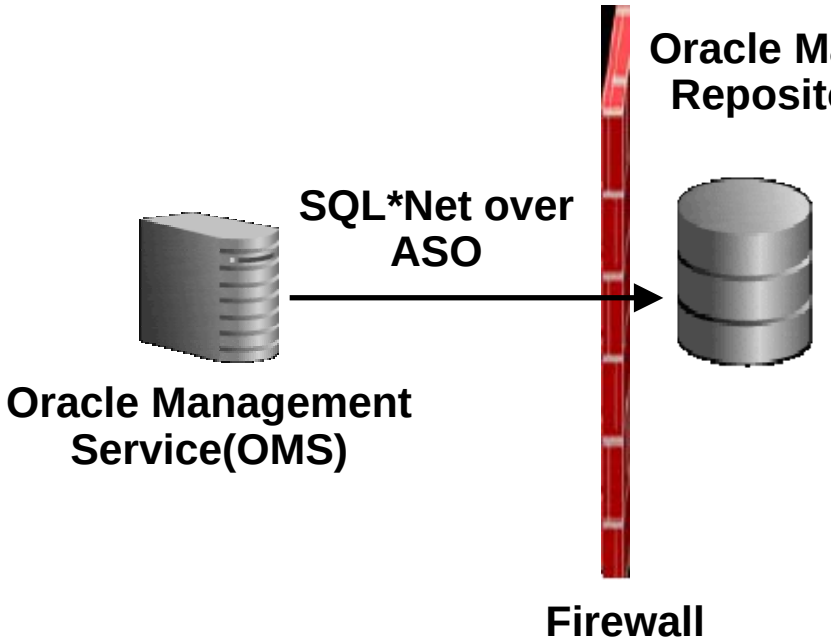
Firewall between OMS and OMR



- Configure the firewall to allow Oracle Net traffic flow
  - Some vendors firewalls can be configured to recognise Oracle*Net traffic
  - Otherwise, define an ACL that allows traffic flow between the subnet hosting the OMS and the subnet hosting the repository
- Secure connections by using features of ASO
  - DB side configuration using ASO in sqlnet.ora

Configure EM For Firewalls

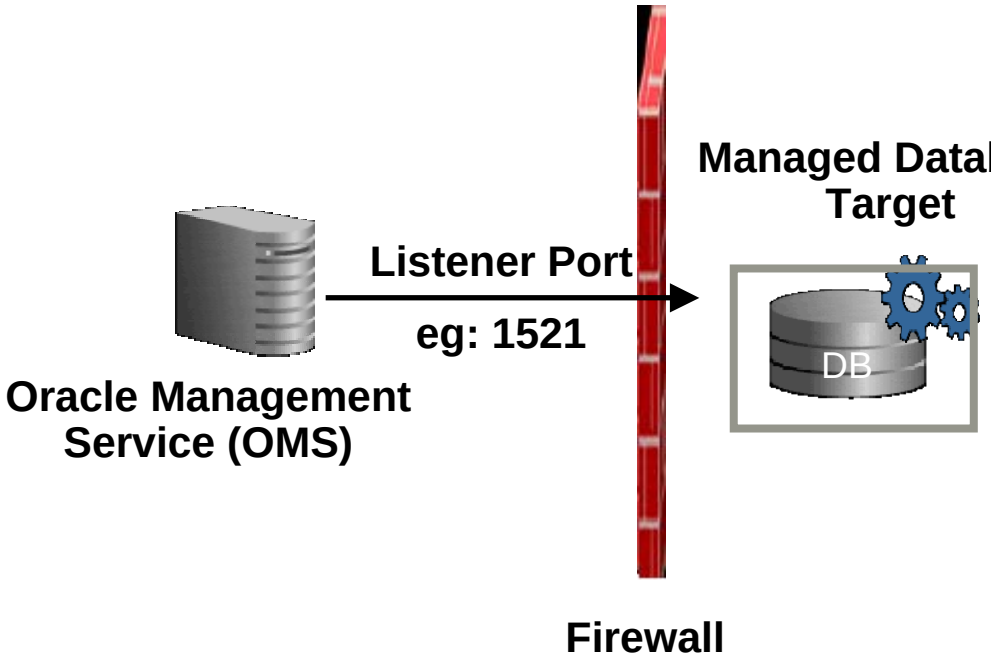
Firewall between OMS and OMR *with ASO*



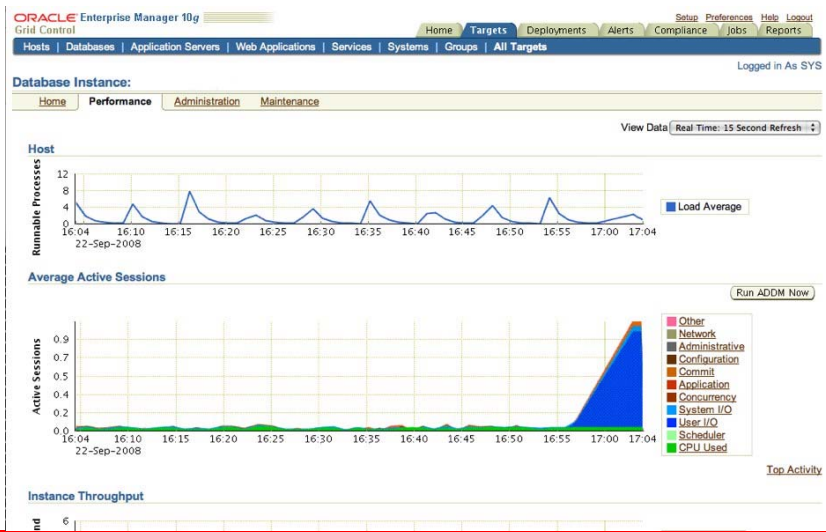
- Secure connections by using features of ASO
- DB side configuration using ASO in sqlnet.ora
  - sqlnet.encryption_server=requested
  - sqlnet.crypto_seed='abcdefg12345'
- OMS side configuration in emoms.properties
  - oracle.sysman.emRep.dbConn.\ enableEncryption=true
  - oracle.net.encryption_client=requested
- You'll know when it's got a typo :-
  - ORA-12645: Parameter does not exist

Configure EM For Firewalls

Firewall between Grid Control and DB Targets

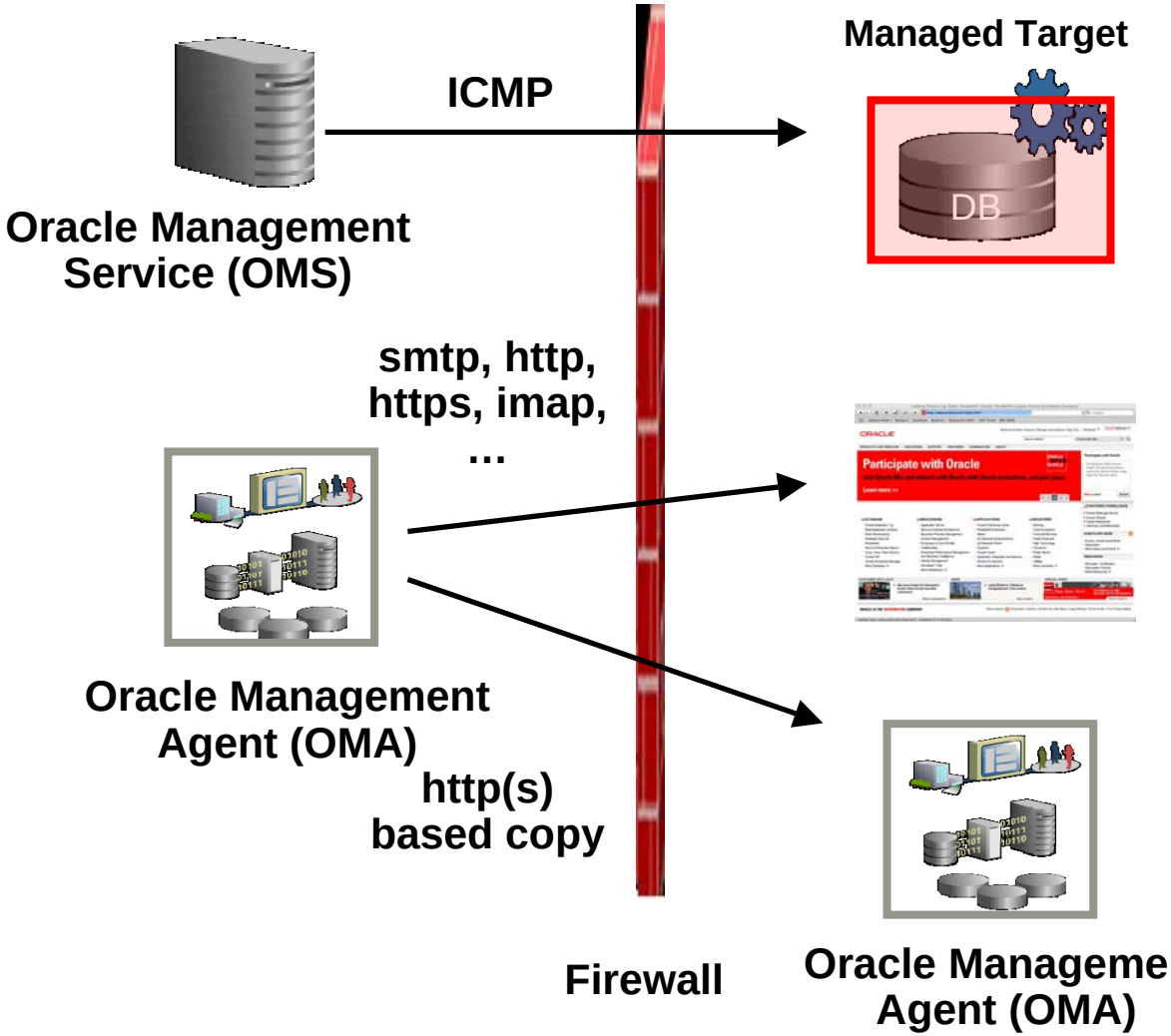


- For administrative operations, configure the firewall to allow the OMS to communicate with the database through Oracle Listener Port
  - Configure the firewall to allow Oracle Net firewall proxy access if allowed
  - Or again, configure the firewall with an ACL to allow this communication to take place



Configure EM For Firewalls

Some other requirements to cater for…



- Deterministic analysis of root of a target down state
- Any OMS may contact any Agent to determine availability
  - Important in multi-OMS environments
- Beacons can run service tests on 14 different protocols – cater for them in your design
- Cloning requires point-to-point communication between agents

Best Practices for Firewall implementations

- If at all possible, get firewalls into first design of the solution
  - Carefully analyse your protocol requirements between EM and the Managed Targets in your environment
  - Consider placement of OMS's when laying down your EM topology
- Work closely with the network team on design of groups and ACL's for groups of targets, it'll save both teams a resource headache

Security:
Authentication,Authorization and Audit

Deploying Secure Enterprise Manager

Authentication

- Complex password and periodical password change
- Reduce the number of super users
- Enable auditing for Logon and Logoff operations
- Do not set preferred credentials for group/common accounts
- Use impersonation based access to targets

Deploying Secure Enterprise Manager

Authentication

- Simplified SYSMAN/DBSNMP password change process
- Ability to change database target credentials on both target and Enterprise Manager simultaneously
- Special character support in username and password
- GUI support to change password during grace period or after password is expired.
- Support for SSO registration using osso.conf file
- Support for registering SSO authentication over https
- EMCLI Support for enabling SSO users as EM users
- GUI Support for sudo/PowerBroker setting
- sudo/PowerBroker support for UDM, Monitoring Template and Corrective Action

Deploying Secure Enterprise Manager

Authorization

- Make sure the privileges/roles are granted only when needed – Principle of Least Privileges
- Grant roles to users instead of granting privileges to enable Role Based Access Control (RBAC)
- Monitor the privileges grants on a regular basis and also keep track of which users exercise what privileges by enabling auditing.

- New fine-grained privileges
  - Blackout target
  - Configure target
  - Manage target metrics
- Enable the support of privilege propagation group

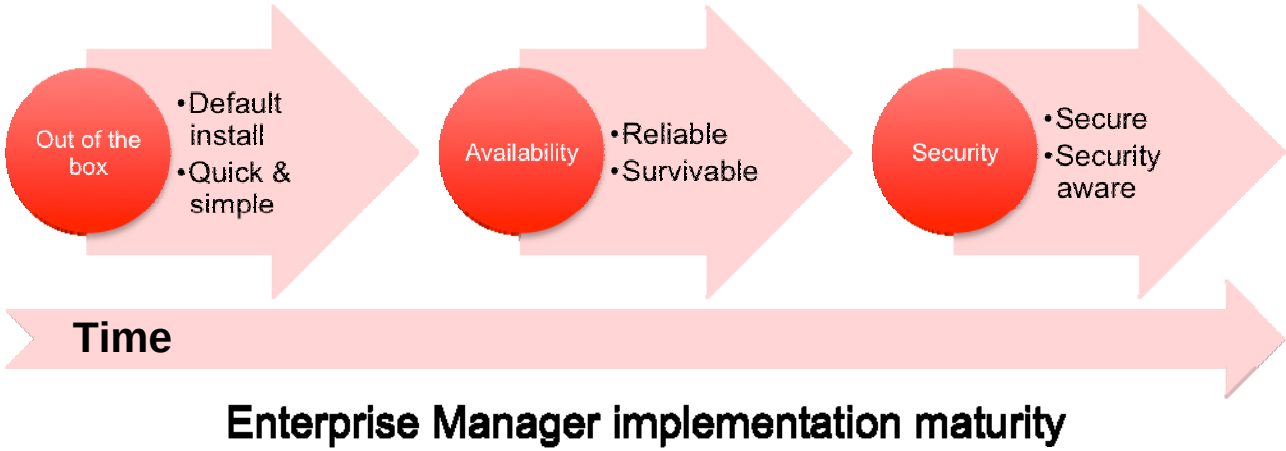
Deploying Secure Enterprise Manager

AUDIT

- Enable auditing all operations
- Monitor audit log and externalize the audit data from the repository to an external store

- Audit data
  - ODL Compliance
- EMCLI Verbs to Configure Oracle Enterprise Manager audit system
- Support for Audit externalization/export service

What you should take away from today



- An understanding of the options available when configuring EM in a highly available fashion
- An understanding of the many aspects of security that can affect an EM implementation

HA Sessions, Labs and Demos

Thu, Sep 25

- 9:00 am - Oracle Secure Backup, Moscone South 102
- 10:30 am - Streams Replication, Moscone South 102
- 12:00 pm - Rolling Database Upgrades, Moscone South 103
- 1:30 pm - Streams Performance, Moscone South 102
- 3:00 pm - Oracle Grid Computing, Moscone South 303
- 3:00 pm - E-Business Suite R12 MAA, Moscone West 2007
- 3:00 pm - Siebel MAA, Moscone South 308
- 3:00 pm - Fusion SOA HA & Scalability, Marriott Salon 14/15

Hands On Labs - Thu, Sep 25

- 10:30 - 11:30 am, 12:00 - 1:00 pm - Active Data Guard, Marriott Golden Gate A3

DEMOgrounds, Mon-Thu

- Active Data Guard, Streams, Oracle Secure Backup, RMAN/Flashback, MAA

Enterprise Manager Sessions, Labs, Demos

Thu, Sep 25

- 9:00 am – Oracle Database 11g Shock Upgrades, Moscone South 301
- 10:30 am – Integrating 40 Data Centers in Three Years, Moscone South 303
- 12:00 pm – Application Testing Best Practices, Moscone South 303
- 1:30 pm – Proactive Performance Monitoring with Baselines & Adaptive Threshold, Moscone South 303
- 3:00 pm - Oracle Grid Computing, Moscone South 303
- 3:00 pm – Coping with virtualization, Moscone South 301

Hands On Labs - Thu, Sep 25

- 12:00 - 1:00 pm, SOA Management and Java Application Diagnostics
- 1:30 – 2:30pm, Database Performance Diagnostics and Tuning
- 3:00 – 4:00 pm, Lowering Management Costs via Configuration Management and Provisioning Automation

DEMOgrounds, Mon-Thu, Moscone West Hall

- Complete Data Center Management
- Oracle Real Application Testing
- Self-Managing Database
- Changing Management and Data Masking for DBAs
- Application Quality Management
- Managing Configuration Complexity
- Complete Provisioning of The Oracle Software Stack

For More Information

search.oracle.com

or

oracle.com

ORACLE IS THE INFORMATION COMPANY