
ORACLE®

ORACLE

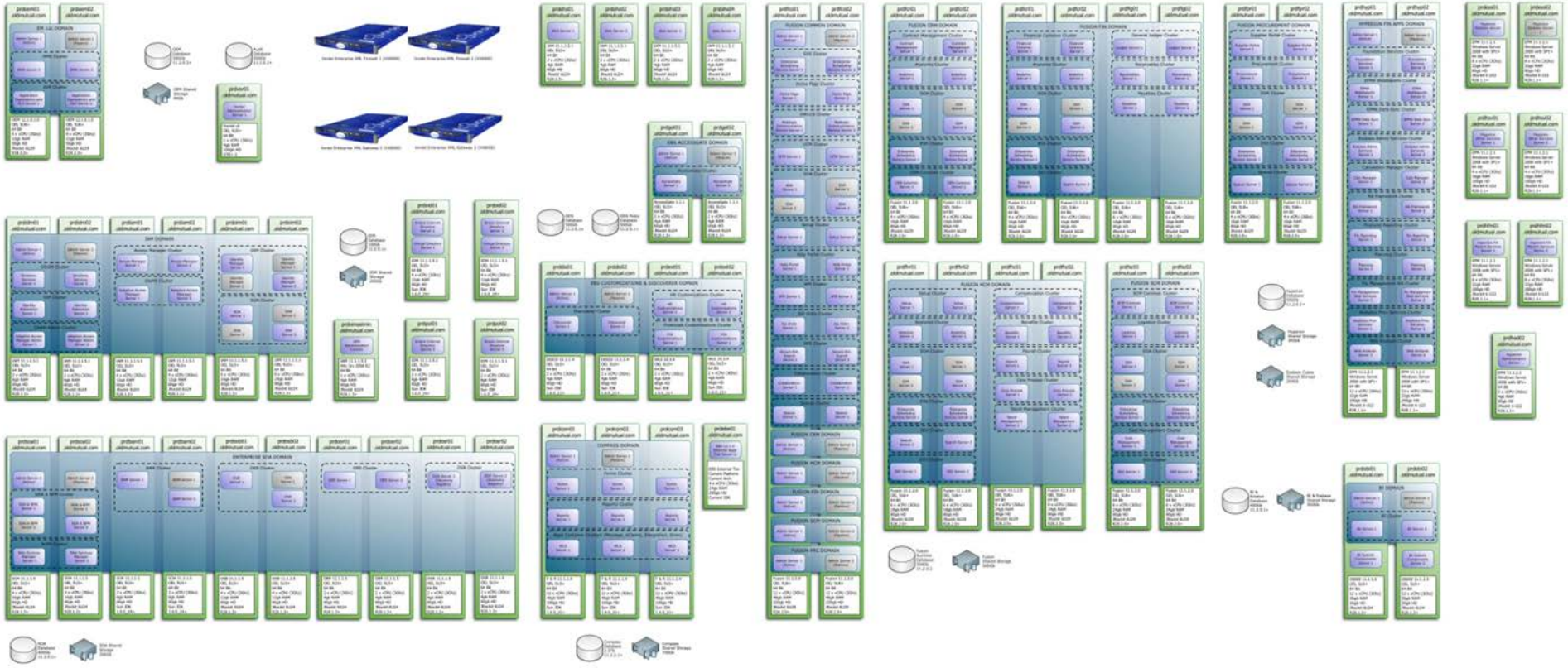
WebLogic Server: Installation Best Practices

Olaf Heimburger, CISSP
Consulting Solution Architect

Safe Harbor Statement

- 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.

The Goal



Planing

Be Prepared for the Future – Avoid Surprises

- Plan for
  - JDK
  - Directory Structure
  - Network Layout
  - AdminServer
  - ManagedServer
  - Clustering
  - JMS
  - Transactional Logs
  - Identity Store
  - Policy Store

JDK Setup

Do you know this?

- <Sep 11, 2013 2:45:24 AM PDT> <Notice> <Security> <BEA-090898> <**Ignoring the trusted CA certificate "CN=KEYNECTIS ROOT CA,OU=ROOT,O=KEYNECTIS,C=FR". The loading of the trusted certificate list raised a certificate parsing exception PKIX: Unsupported OID in the AlgorithmIdentifier object: 1.2.840.113549.1.1.11**.>
- <Sep 11, 2013 2:45:24 AM PDT> <Notice> <Security> <BEA-090898> <**Ignoring the trusted CA certificate "CN=GeoTrust Primary Certification Authority - G3,OU=(c) 2008 GeoTrust Inc. - For authorized use only,O=GeoTrust Inc.,C=US". The loading of the trusted certificate list raised a certificate parsing exception PKIX: Unsupported OID in the AlgorithmIdentifier object: 1.2.840.113549.1.1.11**.>

JDK Setup

- Use the latest available JDK
- Use a version number neutral path
- Make it part of the ORACLE_HOME
- Add some entropy
  - `-Djava.security.egd=file:/dev/urandom`
- Install the JCE Unlimited Strength Jurisdication Policy Files

WLS Installer

With or without?

- Always use the generic installer
- Allows the same installer on every platform

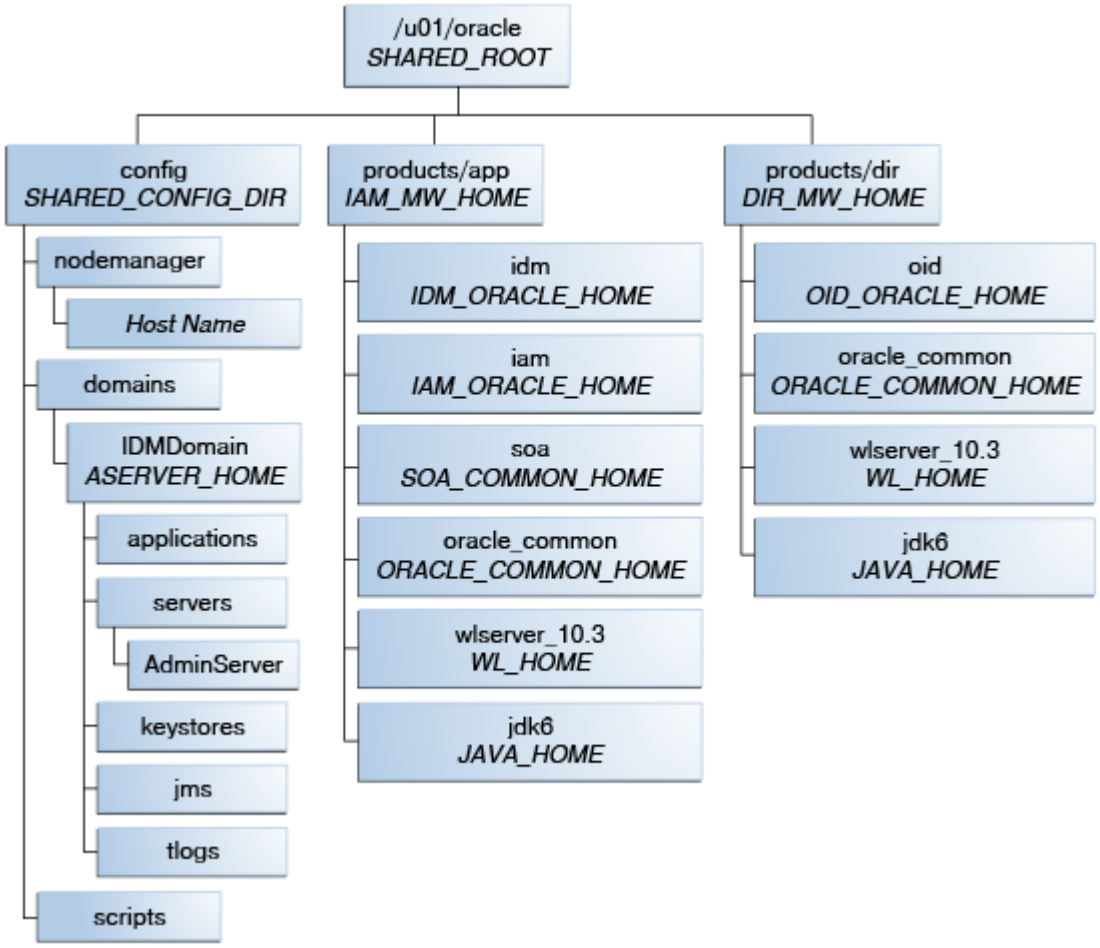
Directory Structure

- Decide on the home structure
- Include the oraInventory, if any.
- Separate binaries from configuration
- Share binaries

Directory Structure

Shared Storage

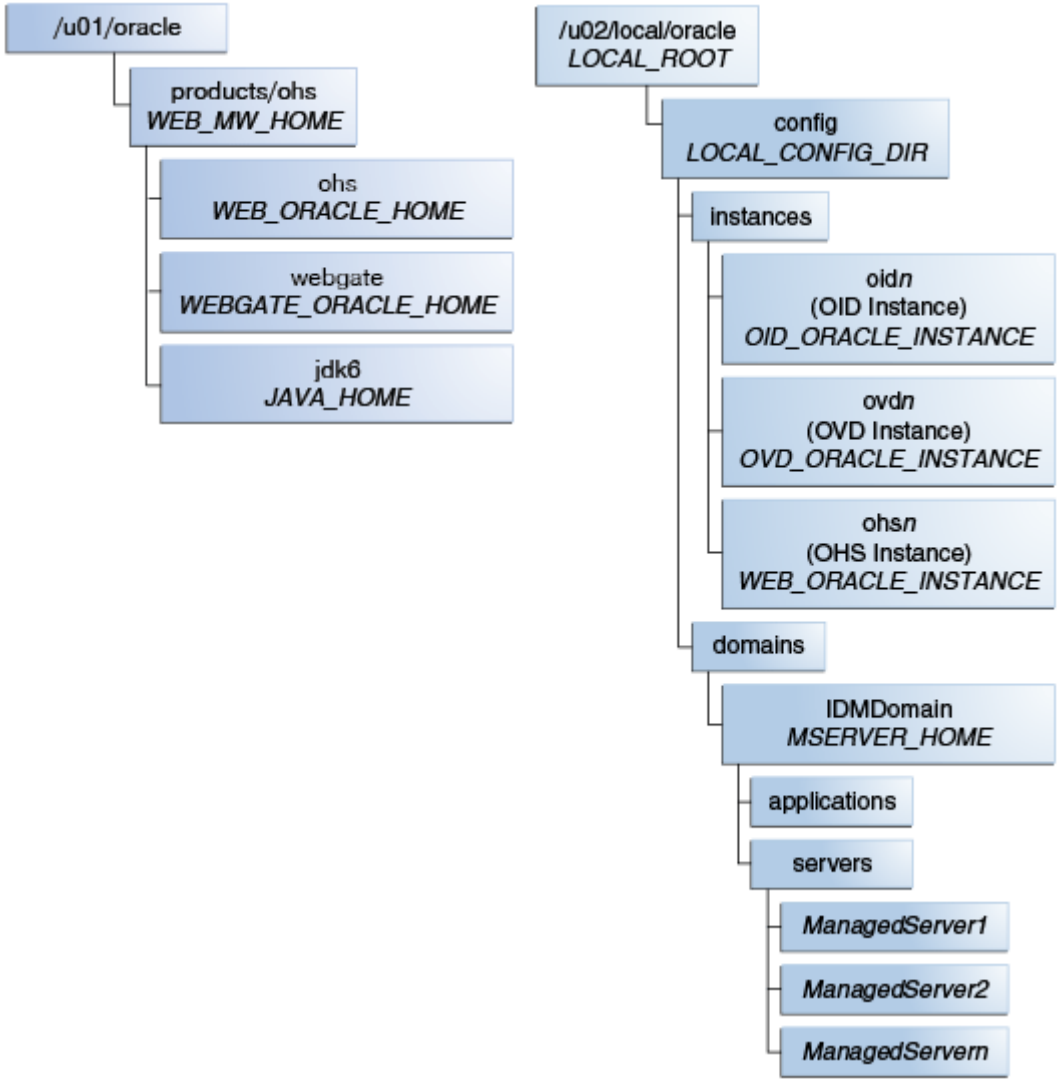
- Common Base
- Shared Everything
- Relies on shared drive performance
- Easy backup
- Easy recovery



Directory Structure

Local Storage

- For configuration only
- Best for DMZ
- Rarely for internal parts



Network

- Plan for Server Migration
- Reserve all expected IPs
- Distinguish between External and Internal IPs
- Plan with Load Balancer
- Plan with OHS Front End
- Use Internal Hostnames for Internal IPs
- Use External Hostnames for External IPs

Network

Internal Hostnames and IPs

- All hostnames used by the environment internally
- Hostnames not available for any normal user
- Internal IPs do not resolve to normal users

Network

External Hostnames and IPs

- Hostnames available for all users
- Resolve through DNS

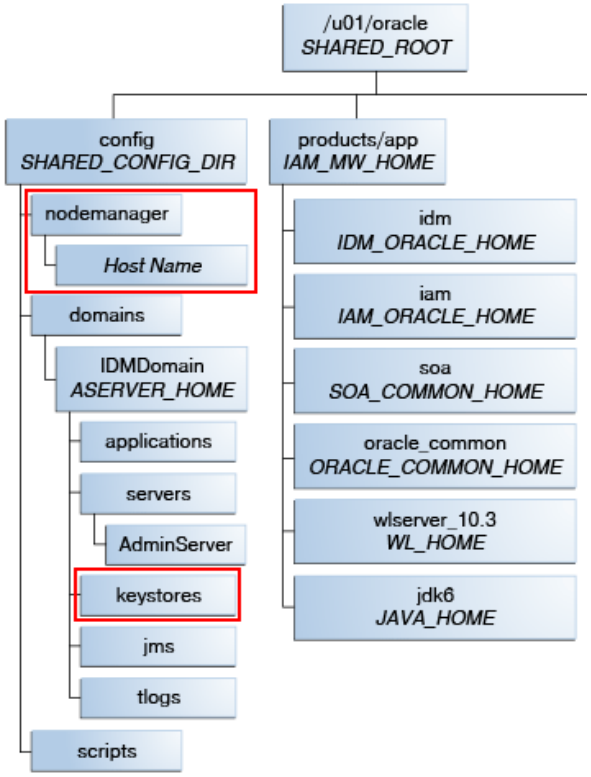
DNS Management

Use A Caching DNS Server

- Avoids Internal hostnames and IP resolution through local files
- One Caching DNS per Environment
  - E.g. dnsmasq
- Configures Internal IPs for Internal Hostnames only
- External IPs in Global DNS only

Nodemanager

- Do not use default structure
- Have configuration separated from binaries
- Use JSSE
- Use separate keystore
- Change default admin user name
  - Do not use „admin“
- Change default password
  - Do not use password of WLS domain admin user

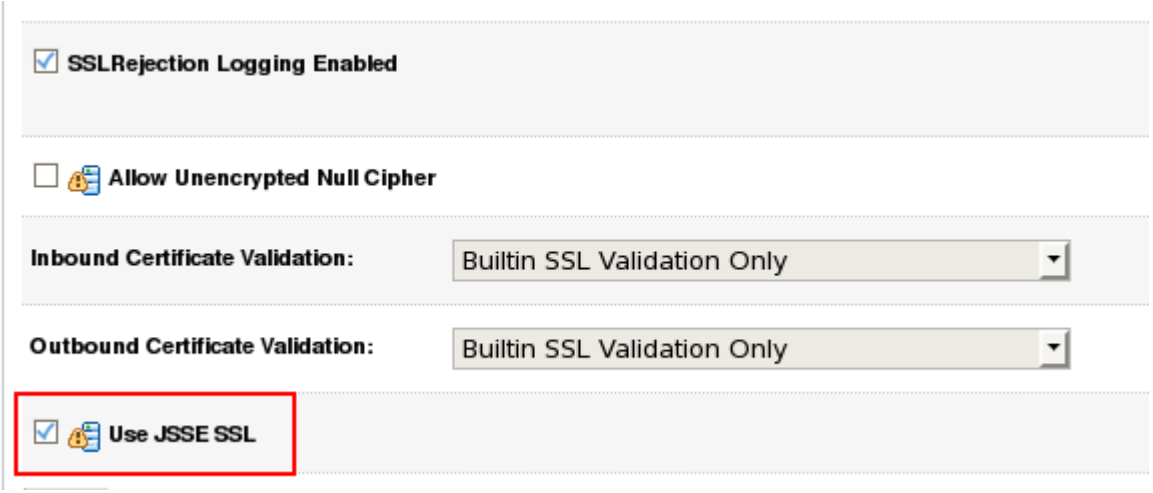


AdminServer

- Configure JSSE
- Avoid Demo Identity and Demo Trust Store
- Plan for OHS integration
- Avoid Network Frontend Setup

AdminServer

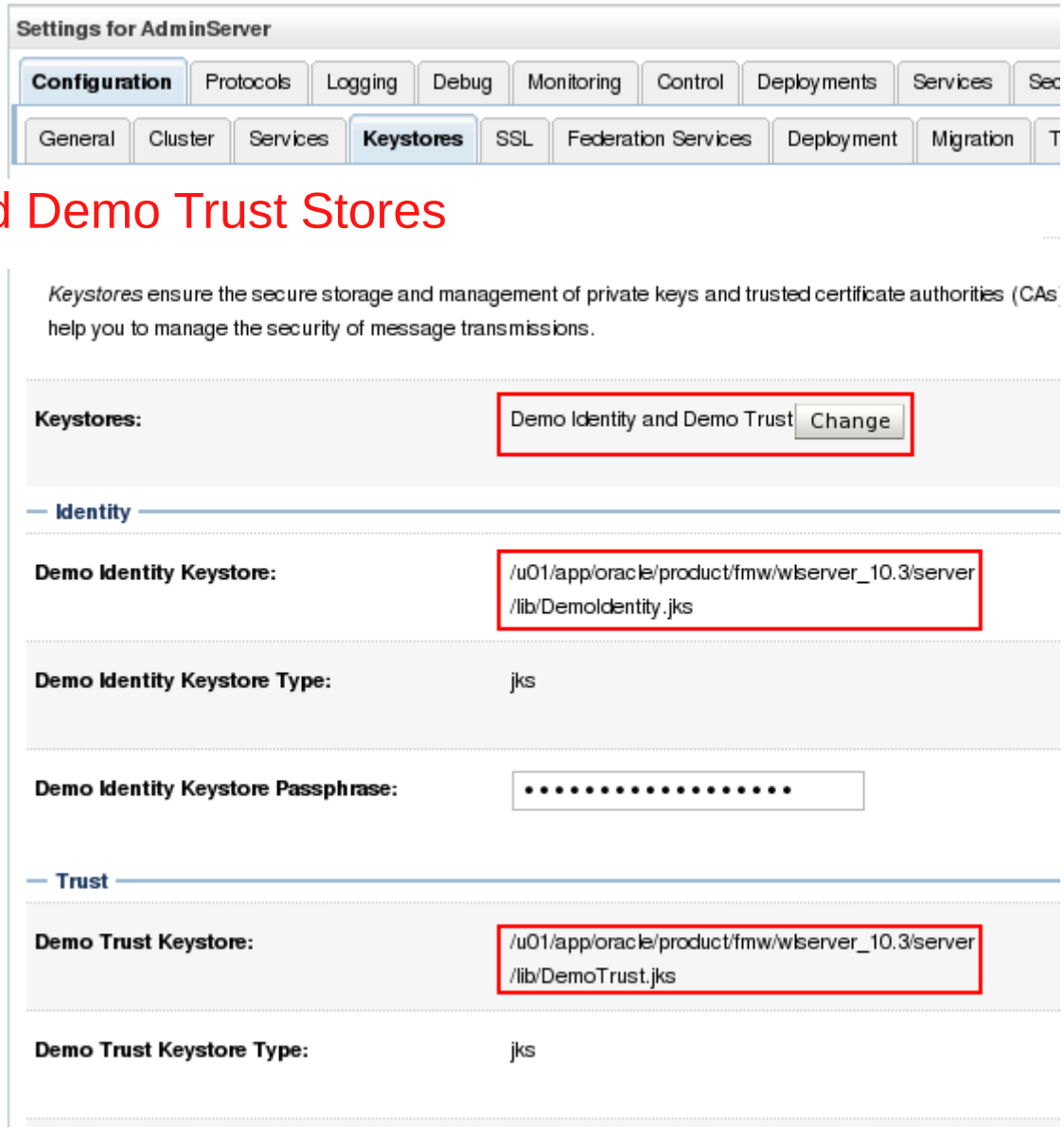
Configure JSSE



- `export CONFIG_JVM_ARGS="-Dweblogic.ssl.JSSEEnabled=true -Dweblogic.security.SSL.enableJSSE=true"`

AdminServer

Avoid Demo Identity and Demo Trust Stores



AdminServer

Plan for OHS Integration

- ```
  <VirtualHost *:7777>
    ServerName ADMIN.mycompany.com:80
    <Location /console>
     SetHandler weblogic-handler
     WebLogicHost ADMINVHN.mycompany.com
     WeblogicPort 7001
    </Location>
    <Location /odsm>
     SetHandler weblogic-handler
     WebLogicCluster admin1.mycompany.com:7006,admin2.mycompany.com:7006
    </Location>
  </VirtualHost>
  ```
- Enable Weblogic Plugin
  ```

AdminServer

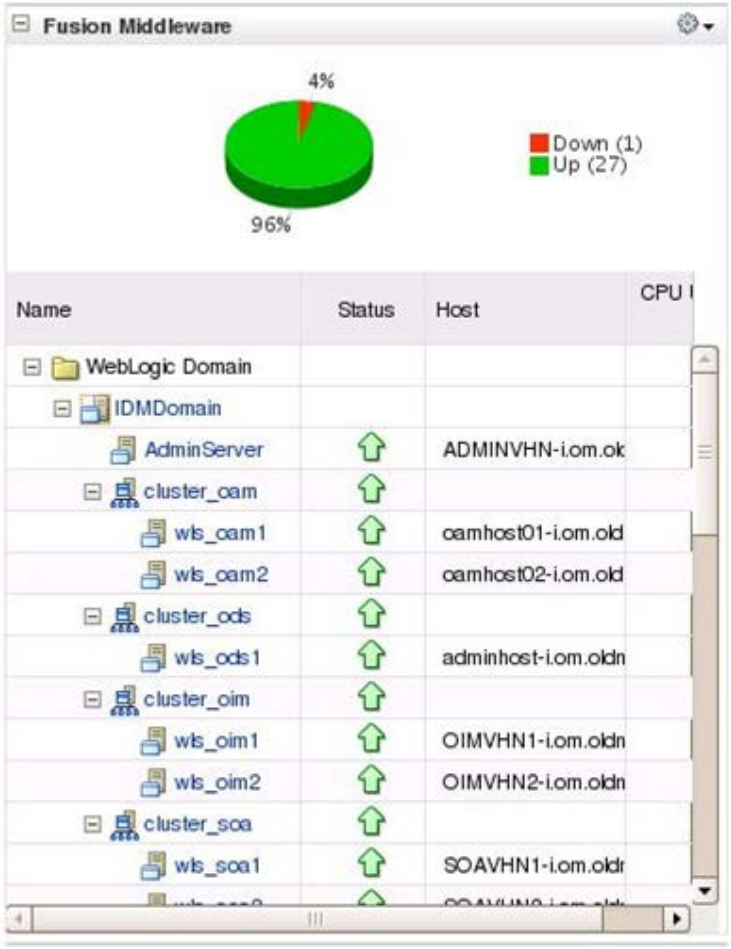
Avoid Network Frontend Setup

ManagedServer

- Put in a Cluster
- Use the correct JMS Distribution Destination type
- Plan for Server Migration

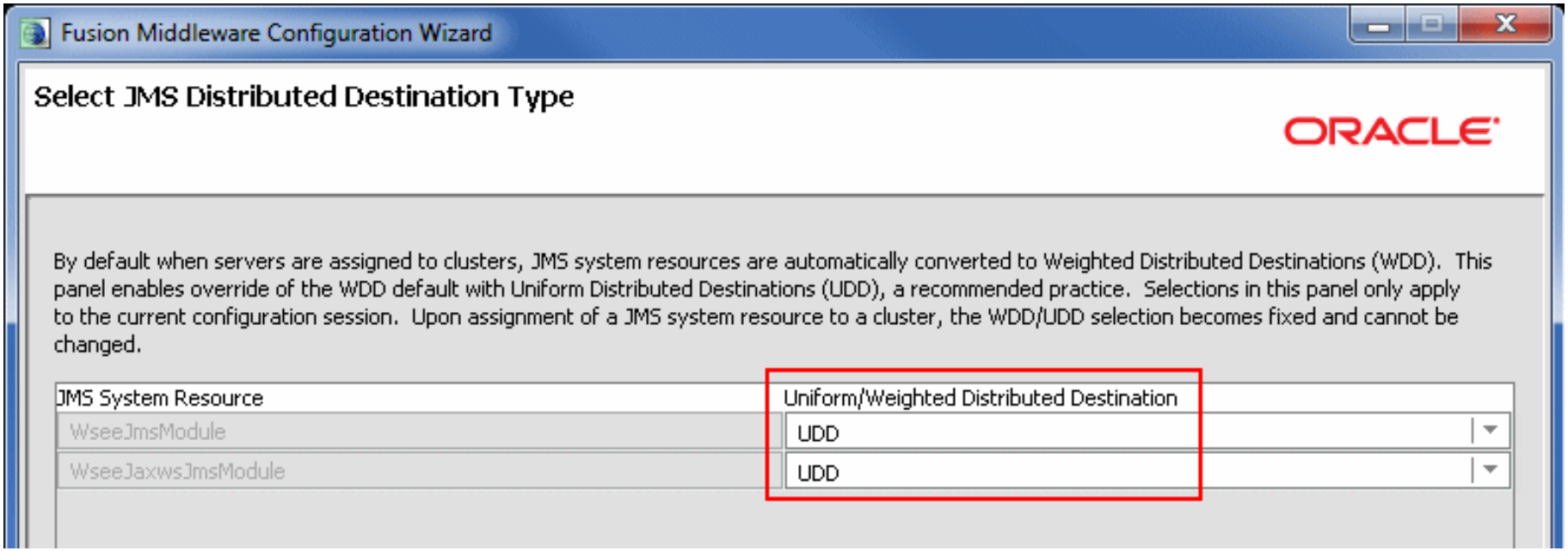
ManagedServer

Put in a Cluster



ManagedServer

Use the Correct JMS Distribution Destination Type



Managed Server

Server Migration: Leasing Table & Data Source

- Leasing Table required
- Data Source *leasing* (*jdbc/leasing*)
  - Multi Data Source for RAC database
  - Targeted to migratable ManagedServers

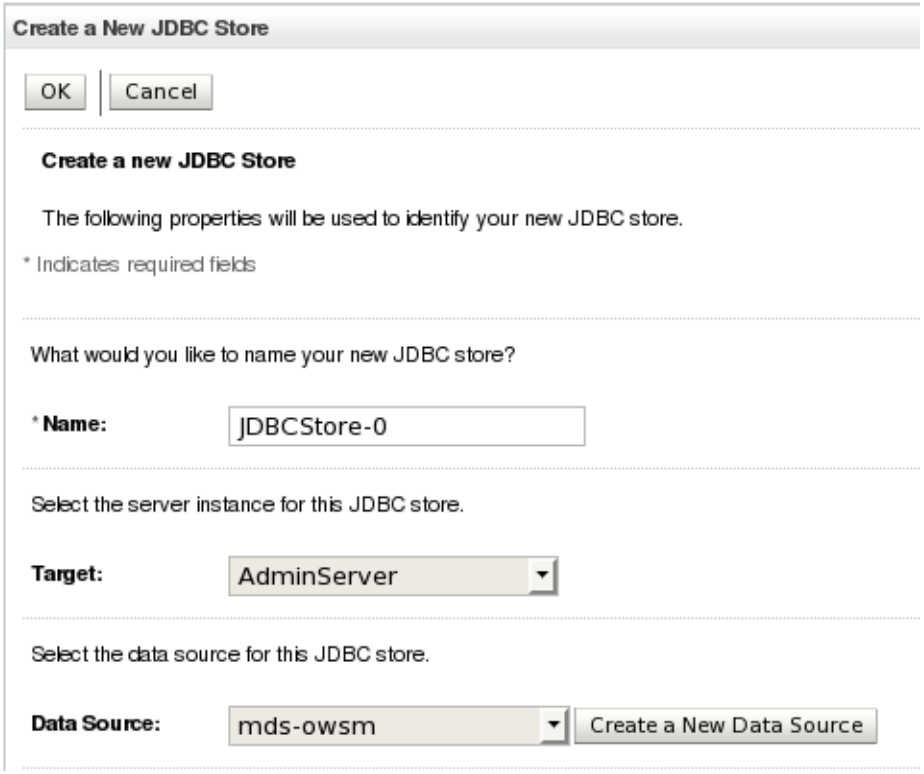
Managed Server

Server Migration: Nodemanager

- File *nodemanager.properties*
  - `Interface: eth0`
    `NetMask: 255.255.255.0`
    `UseMacBroadcast=true`
- Verify startup output
  - `StateCheckInterval=500`
    `eth0=*,NetMask=255.255.248.0`
    `UseMACBroadcast=true`

JMS

- Plan for hot backups
- Use JDBC store for JMS storage



Transaction Logs

- Plan for hot backups
- Use JDBC store for Transaction Logs
  -
```
<server>
 <transaction-log-jdbc-store>
  <data-source>MyDataSource</data-source>
  <prefix-name>TLOG_MS1</prefix-name>
  <create-table-ddl-file>myDDL/myCreateTable.sql</create-table-ddl-
file>
  <max-retry-seconds-before-tlog-fail>120</max-retry-seconds-before-
tlog-fail>
 </transaction-log-jdbc-store>
</server>
```

- Globally-Scoped DataSource
- One JDBC TLOG per server
- Not shared between servers

Miscellaneous

- Install Oracle Application Development Runtime
- Externalize Identity Store
  - OVD
  - OID
  - OUD
- Externalize Single Sign-On
  - OAM
    - Username/Password
    - Kerberos (Windows Native Authentication / SPNEGO)
    - Secure Token Service
    - SAML (w/ OIF)
    - Strong Authentication with Oracle Adaptive Access Manager

Hardware and Software

ORACLE®

Engineered to Work Together


ORACLE®