Setting up Oracle Identity and Access Management 11gR1 Compact Environment
Version 11.1.1.5.2

# Table of Contents

This compact environment is meant for evaluations and demos. It is not intended for production deployments.

Before downloading product binaries, ensure you have Oracle (https://myprofile.oracle.com/EndUser/faces/profile/createUser.jspx) and Oracle Support (https://support.oracle.com/CSP/ui/flash.html) accounts.

# 1 Description

This document explains how to use the Oracle Identity and Access Management Compact Setup tool on Linux.

The tool performs the following actions:

1   Installs Oracle Identity and Access Management components and dependent products from binaries supplied by the end user.
2   Configures each component to run in a topology optimized for 6GB of RAM. To achieve this, the tool takes the following steps:
   - Reduces the memory footprint of the Oracle Database to about 800 MB.
   - Deploys Oracle Identity and Access Management components to run on the minimum number of servers in one Oracle WebLogic domain.
   - Removes, or does not start, Oracle Fusion Middleware components that are not relevant to the operation of Oracle Identity and Access Management.
3   Integrates Oracle Identity Manager, Oracle Access Manager, and Oracle Internet Directory components to work together.

# 2 System Requirements

The environment requires the following:

1. Platforms supported:
   - Oracle Enterprise Linux 5, x86-64, kernel 2.6.18 or later, oracle-validated setup applied
2. Minimum free disk space:
   - 40 GB (25GB if STAGED_MEDIA is TRUE)
   - 500 MB in /tmp
3. Minimum physical RAM:
   - Bare metal: 6 GB
   - Virtual Box: At least 6718 MB must be allocated to the VM
4. Default ports used:
   - 1521, 3060, 5575, 6501, 7001, 7005, 7499, 7501, and 8899
5. Perl version 5.8.5 or higher installed:
   - Perl downloads are available at http://www.perl.org/get.html
6. UNZIP tool for the destination platform:
   - UNZIP tools are available at https://updates.oracle.com/unzips/unzips.html
7. Network
   - Host name resolution configured to use the hosts file
   - Only one NIC card should be active

# 3 Downloading Product Binaries

To download product binaries:

1. Ensure you have "Oracle" (https://myprofile.oracle.com/EndUser/faces/profile/createUser.jspx) and "Oracle Support" (https://support.oracle.com/CSP/ui/flash.html) accounts.  Oracle users can use their

SSO accounts to download product binaries.  Log in to both accounts to make sure your credentials are valid. *Note*: If you do not have these accounts you will not be able to download required binaries.

2. Create a directory to hold the platform-specific product binaries used during setup.

3. Using your Oracle and Oracle Support accounts, download all required product binaries for the target platform to the download directory created in previous step using the reference information provided in section

# 4   Setting up Environment

Perform these steps:

1. Ensure your Linux environment meets Oracle Database prerequisites. For details on how to configure the Linux environment, refer to section 9, or see http://www.oracle-base.com/articles/11g/OracleDB11gR2InstallationOnEnterpriseLinux5.php#OracleValidatedSetup.

2. Ensure the host name resolution is configured to use the `hosts` file. For details on how to configure this, refer to section 10, or see:
http://download.oracle.com/docs/cd/B28359_01/install.111/b32002/pre_install.htm#BABHFHBA.

3. Ensure the executing user account is a member of the `dba` group. For details on how to configure this, refer to section 11, or see:
http://download.oracle.com/docs/cd/B28359_01/install.111/b32002/pre_install.htm#autoId26.

4. Ensure that any previous setup of the environment is safely stopped and removed before starting a new setup. Refer to section 6 for more information.

5. Unzip `ofm_idm_compact_11.1.1.5.2_generic_disk1of1.zip` in the directory where you want to setup the environment.

6. Navigate to the newly created `idmSetup` subdirectory containing files required by the setup.

7. Update `idmSetup.properties` using the reference information provided in section 7Configuration Properties.  Save a copy of this file in a directory separate from the environment.

8. Execute the command to start the setup:

```
sh idmSetup.sh
```

The script will ask for the password and begin the setup.

*Note*: The full command line with optional parameters is as follows:

```
sh idmSetup.sh [properties-file] [password]
```

The script will take between 60 and 90 minutes (may be 2-3 times longer in VMs) to setup a working environment, depending on the speed of the host machine.

# 5  Validating Environment

After completing these steps, all products are installed and configured; in addition, Oracle Access Manager and Oracle Identity Manager are integrated to work together.  Take these steps to validate the integration:

1. Log in to the Oracle Access Manager console by accessing URL `http://<FQDN-HOSTNAME>:7001/oamconsole` with username `OAMMasterAdmin` and password specified during the setup. Check that the following links appear on the login page: **Forgot password**, **Register new account**, and **Track user registration**.

2. From a different browser instance, access the Oracle Identity Manager console by accessing URL `http://<FQDN-HOSTNAME>:7005/oim/faces/pages/Admin.jspx` with username `xelsysadm` and password specified during the setup:
   - Check that the login page is the same one you observed earlier.
   - Click the logout link on the Oracle Identity Manager administration console. You should be redirected to the Oracle Access Manager login page.

# 6  Managing Environment

Once the environment has been setup, managing its lifecycle involves starting, stopping, and removing the environment.

To start the environment, execute command 'sh `start.sh <password>`' from the `idmSetup/bin` directory.  Omit the password if `CACHE_CREDS` was `TRUE`.

To stop the environment, execute command 'sh `stop.sh <password>`' from the `idmSetup/bin` directory. Omit the password if `CACHE_CREDS` was `TRUE`.

*Note:* The password is optional based on whether or not the environment had been created to require passwords (as controlled by the `CACHE_CREDS` setup property).  The script will prompt for the password if it determines the password is required but was not passed in.

To remove the environment, perform these steps:

1. `sh stop.sh <password>` from the `idmSetup/bin` directory
2. `ps -aux | grep idmSetup`, then execute command `kill -9 <pid>` for every process listed
3. Change directory to one level above the  `idmSetup` directory
4. `chmod a+w -R idmSetup`
5. `rm -r -f idmSetup`

# 7 **Configuration Properties**

| Property | Description |
|---|---|
| DOWNLOAD_DIRECTORY | Absolute path to the directory containing downloaded product kits.<br><br>Example: DOWNLOAD_DIRECTORY=/temp/downloadIdm |
| MEDIA_DIRECTORY | Absolute path to the directory to receive setup media generated from downloaded product kits.<br><br>If not specified, the script defaults to the current working directory.<br><br>Example: MEDIA_DIRECTORY=/temp/idmMedia |
| STAGED_MEDIA | Indicates if the script should use existing setup media in MEDIA_DIRECTORY, or generate product setup media from downloaded product kits. Valid values are TRUE and FALSE. Default value is FALSE.<br><br>If set to FALSE, the script generates setup media from downloaded product kits.<br><br>If set to TRUE, the script assumes setup media already exists in MEDIA_DIRECTORY.<br><br>Example: STAGED_MEDIA=FALSE |
| WIPE_MEDIA_DIRECTORY | Indicates if the script should erase existing setup media in MEDIA_DIRECTORY when configured to generate setup media from downloaded product kits (indicated by STAGED_MEDIA=FALSE).<br><br>This property is used to guard against accidental erasure of the setup media. Valid values are TRUE and FALSE. Default value is FALSE.<br><br>If set to TRUE, the script erases setup media in MEDIA_DIRECTORY before proceeding with setup.<br><br>If set to FALSE, the script exits if the setup media already exists in MEDIA_DIRECTORY.<br><br>Example: MEDIA_DIRECTORY=FALSE |
| DB_SID | Indicates the database SID to use. This is an alphanumeric string. Default value is idm.<br><br>Example: DB_SID=idm |
| DB_NAME | Indicates the global database name / database service name to use. This is an alphanumeric string. Default value is idm.oracle.com |

| | Example: `DB_NAME=idm.oracle.com` |
|---|---|
| `DB_PORT` | Indicates the database port to use. Default value is `1521`.<br><br>Example: `DB_PORT=1521` |
| `DB_CHARSET` | Indicates the character set to use. Default value is `idm`.<br><br>Example: `DB_CHARSET=AL32UTF8` |
| `WLS_STARTUP_DELAY`<br>`WLS_SHUTDOWN_DELAY` | Maximum number of seconds the script should wait for the Oracle Web Logic server to start or stop. While the script detects server up/down conditions, this setting is used to protect against hung server operations. Default value is `420` (start) and `120` (stop).<br><br>When setting the environment on a bare metal host use `420` (start) / `120` (stop) seconds as a starting point. On a slower host, such as virtual machine, adjust the delay to `800` (start) / `240` (stop) seconds.<br><br>Example: `WLS_STARTUP_DELAY=420`<br>Example: `WLS_SHUTDOWN_DELAY=120` |
| `CACHE_CREDS` | Indicates if the environment should require credentials to start and stop Oracle Web Logic and Oracle Database.<br><br>Valid values are `TRUE` and `FALSE`. Default value is `FALSE`.<br><br>Example: `CACHE_CREDS=TRUE` |
| `DEBUG` | Indicates if debug mode should be enabled to generate more verbose output.<br><br>Valid values are `TRUE` and `FALSE`. Default value is `FALSE`.<br><br>Example: `DEBUG=FALSE` |

# 8  Default URLs and Ports

Login credentials and default URLs used by the environment are listed in the following table.

*Note*: <SYS_PW> refers to the password configured during the setup.

| Product and Login Credentials | Console URL |
|---|---|
| | |
| **Oracle WebLogic Server** | |
| WebLogic console (weblogic/<SYS_PW>) | http://<FQDN-HOSTNAME>:7001/console |
| **Oracle Enterprise Manager** | |
| Enterprise Manager (weblogic/<SYS_PW>) | http://< FQDN-HOSTNAME>:7001/em |
| Enterprise Manager Agent | http://< FQDN-HOSTNAME>:5162/emd/main |
| **Oracle Directory Services Manager** | |
| ODSM (orcladmin/<SYS_PW>) | http://< FQDN-HOSTNAME>:7005/odsm/faces/odsm.jspx |

| OID admin account (cn=orcladmin/<SYS_PW>) | |
|---|---|
| **Oracle Identity Federation** | |
| OIF test page | http://< FQDN-HOSTNAME>:7777/fed/user/testspsso |
| **Oracle Identity Navigator** | |
| OINAV (oammasteradmin/<SYS_PW>) | http://< FQDN-HOSTNAME>:7001/oinav |
| **Oracle Access Manager** | |
| OAM Admin (oammasteradmin/<SYS_PW>) | http://< FQDN-HOSTNAME>:7001/oamconsole |
| **Oracle Adaptive Access Manager** | |
| OAAM Admin (oaamadmin/<SYS_PW>) | http://< FQDN-HOSTNAME>:7005/oaam_admin |
| OAAM Server (any username, password 'test') | http://< FQDN-HOSTNAME>:7499/oaam_server |
| **Oracle Identity Manager** | |
| OIM admin console for user and role management activities (xelsysadm/<SYS_PW>) | http://< FQDN-HOSTNAME>:7005/admin/faces/pages/Admin.jspx |
| **Oracle SOA Suite** | |
| SOA Infrastructure (weblogic/<SYS_PW>) | http://< FQDN-HOSTNAME>:7001/soa-infra |
| SOA Worklist (xelsysadm/<SYS_PW>) | http://< FQDN-HOSTNAME>:7001/integration/worklistapp |
| **EM DB Console** (Disabled after the setup) | |
| sys/<SYS_PW> | https://< FQDN-HOSTNAME>:1158/em/console |

The default ports used by the environment are as follows:

| Component | Port |
|---|---|
| Database | EM Console Port: 5500 |
| EM Agent | EM Agent Port: 5162 |
| Oracle Internet Directory | Non-SSL Port: 3060, SSL Port: 3131 |
| Oracle Virtual Directory | Non-SSL Port: 6501, SSL Port: 7501, Admin SSL Port: 8899 |
| Oracle HTTP Server | HTTP Port : 7777, HTTPS Port : 4444, Admin Port : 9999 |

# 9  Meeting Database Prerequisites

A database may not install if the Linux environment is not configured with the required packages. A simple way to install the required packages is to use Oracle's public Yum server.

1. Download and copy the appropriate Yum configuration file, by running the following commands as root:

```
cd /etc/yum.repos.d
wget http://public-yum.oracle.com/public-yum-el5.repo
```

2. Open `public-yum-el5.repo` in a text editor and enable the following sections by changing `enabled=0` to `enabled=1`

```
[el5_uN_base], where N is the highest number available
[el5_oracle_addons]
```

3. Execute the following command:

```
yum install oracle-validated
```

# 10  Configuring Host Name Resolution

A database configuration error may occur if name resolution is not set up. To avoid this error you must ensure that host names are resolved through the `/etc/hosts` file.

1. Verify that the `/etc/hosts` file is used for name resolution. You can do this by checking the `hosts` file entry in the `nsswitch.conf` file as follows:

```
cat /etc/nsswitch.conf | grep hosts
```

The output of this command should contain an entry for files.

2. Verify that the `hosts` file contains the fully qualified host name by using the following command:

```
cat /etc/hosts
```

The output of this command should contain entries for the fully qualified hostname and localhost.

For example:

```
192.168.100.16    myhost.us.example.com myhost
127.0.0.1         localhost.localdomain localhost
```

If the `hosts` file does not contain the fully qualified host name, open the file and make the required changes to the file.

To find out the host name, execute the following command:

```
hostname
```

To find out the fully qualified host name, execute the following command:

```
hostname -f
```

To find out the host IP address, execute the following command:

```
hostname -i
```

# 11  Configuring DBA Group

Verify that the executing user account is a member of the `dba` group. Execute the following command:

Setting up Oracle Identity and Access Management 11gR1 Compact Environment
Version 11.1.1.5.2

```
id -Gn
```

If the output of this command does not contain the `dba` group then perform the following steps:

1. To determine whether the `dba` group exists, enter the following command:

   ```
   grep dba /etc/group
   ```

2. If the `dba` group does not exist, then enter the following command to create it:

   ```
   /usr/sbin/groupadd dba
   ```

3. Enter the following command to add the executing user account to the `dba` group:

   ```
   /usr/sbin/usermod -a -G dba <user-account>
   ```

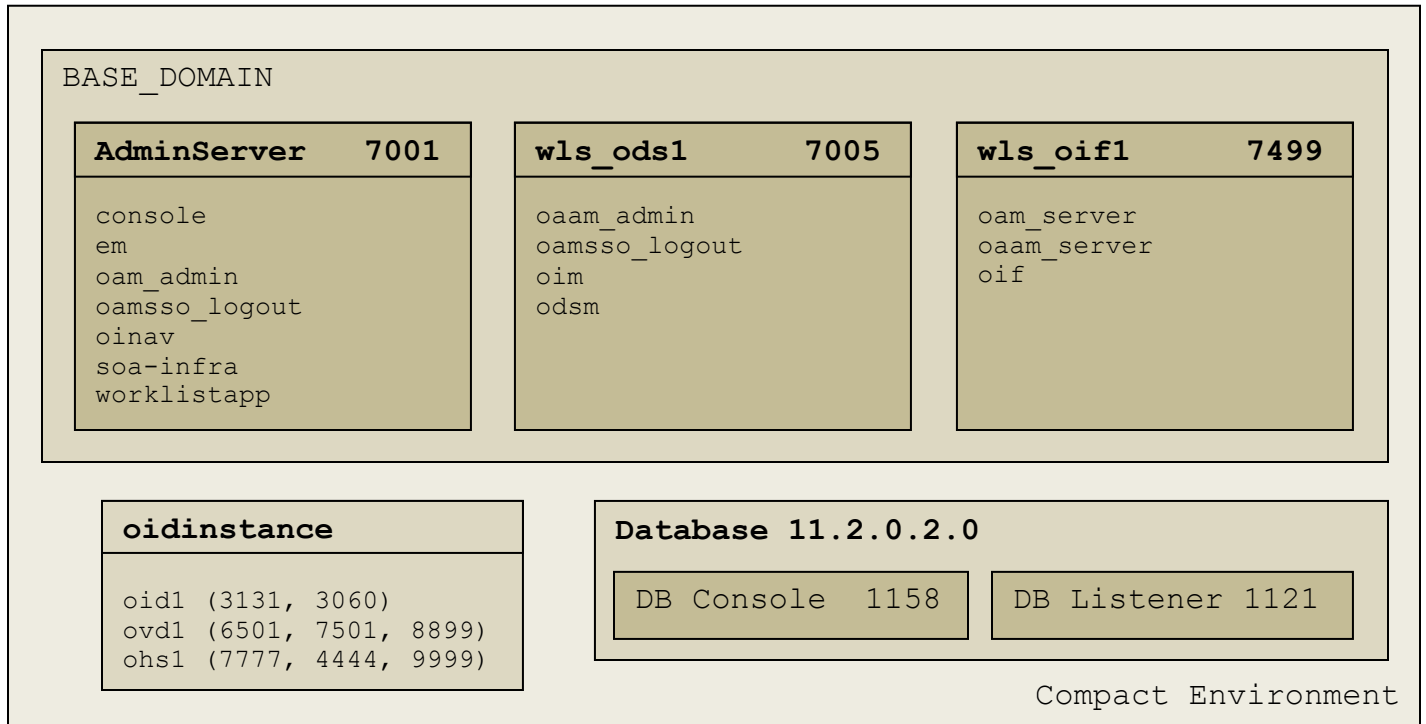   *Note*: `<user-account>` is the executing user's account as reported by the `id` command.

# 12  Environment Architecture

This compact form factor of the environment is achieved by way of optimizing the setup and configuration of the components that make up the Identity & Access Management environment:

1   The database is configured to require the smallest amount of memory necessary to support a simple environment capable of running a demo. To achieve this goal the database is configured to run in about 800MB of RAM.  The actual amount of memory (+ 150MB) is specified in `idmSetup/scripts/sql/optimize.sql`.
2   The OID and OVD applications are started
3   The Identity Management 11gR1  11.1.1.5.0 domain is deployed using three servers:
    * Admin server running the WLS Console and FMW Control applications
    * Wls_oif1 server running the OIF application
    * Wls_ods1 server running the ODSM application for administering OID and OVD
4   The Identity and Access Management 11.1.1.5.0 domains extends the Identity Management 11.1.1.5.0 domain to leverage the existing server footprint without starting additional WLS servers:
    * The OAM application is deployed to the wls_oif1 server
    * The OAAM Admin application is deployed to the Admin server
    * The OAAM Server application is deployed to the wls_oif1 server
    * The OIM application is deployed to wls_ods1
    * The SOA components as required by OIM is deployed to the Admin server

Figure 1: Functional Topology illustrates functional components present in the environment.

```
 BASE_DOMAIN

   ┌──────────────────────────┐  ┌──────────────────────────┐  ┌──────────────────────────┐
   │ AdminServer     7001     │  │ wls_ods1        7005     │  │ wls_oif1        7499     │
   ├──────────────────────────┤  ├──────────────────────────┤  ├──────────────────────────┤
   │ console                  │  │ oaam_admin               │  │ oam_server               │
   │ em                       │  │ oamsso_logout            │  │ oaam_server              │
   │ oam_admin                │  │ oim                      │  │ oif                      │
   │ oamsso_logout            │  │ odsm                     │  │                          │
   │ oinav                    │  │                          │  │                          │
   │ soa-infra                │  │                          │  │                          │
   │ worklistapp              │  │                          │  │                          │
   └──────────────────────────┘  └──────────────────────────┘  └──────────────────────────┘

   ┌──────────────────────────┐  ┌───────────────────────────────────────────────────────┐
   │ oidinstance              │  │ Database 11.2.0.2.0                                     │
   ├──────────────────────────┤  │  ┌──────────────────────┐  ┌──────────────────────┐    │
   │ oid1 (3131, 3060)        │  │  │ DB Console   1158    │  │ DB Listener 1121     │    │
   │ ovd1 (6501, 7501, 8899)  │  │  └──────────────────────┘  └──────────────────────┘    │
   │ ohs1 (7777, 4444, 9999)  │  │                                                         │
   └──────────────────────────┘  └───────────────────────────────────────────────────────┘
                                                              Compact Environment
```

**Figure 1: Functional Topology**

The setup process is illustrated by Figure 2: Lifecycle Process. Note that Product Binaries as downloaded in Step 1, and derived Product Media as extracted from Product Binaries in step 2, can be created once and then used to create multiple environments. For example, staged product media can be saved to a portable disk and used in setting up different environments.
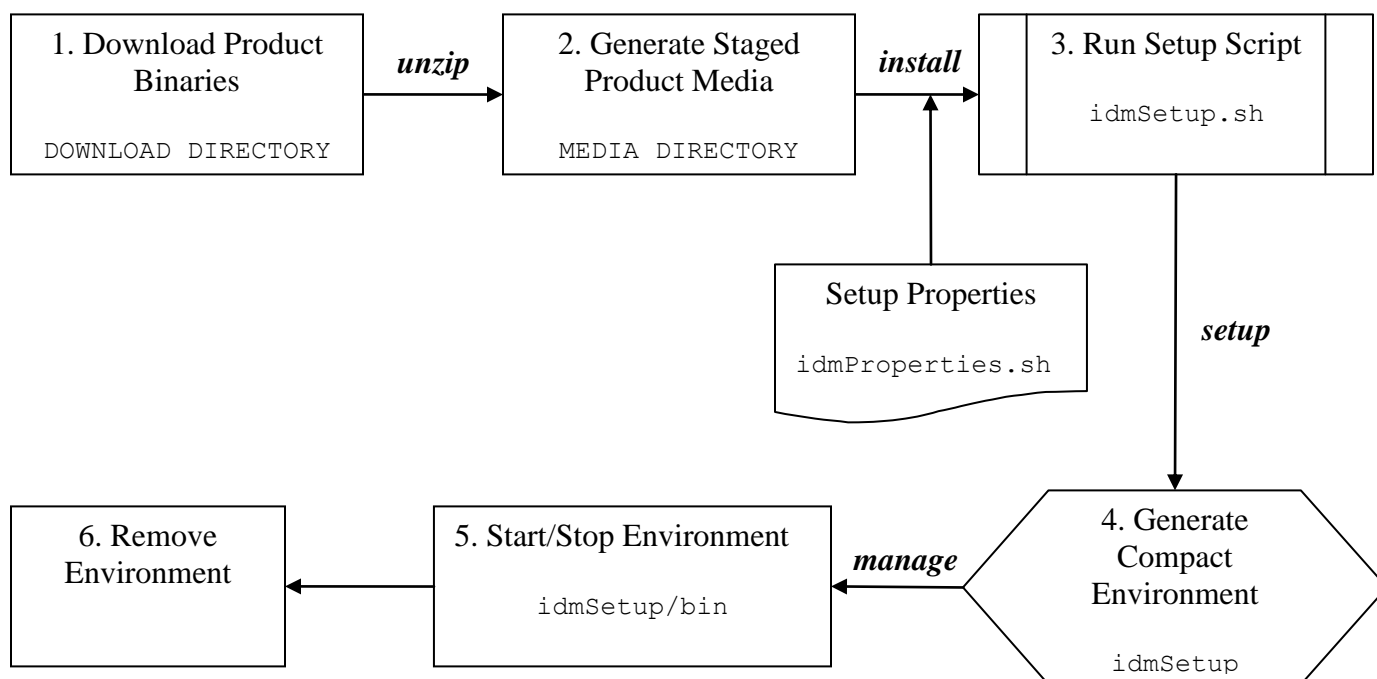
**Figure 2: Lifecycle Process**

Figure 3: IAM/IDM domain **Directory Structure** describes the directory structure used by the compact environment:

```
idmSetup
    bin......................Scripts to manage environment
    binaries.................Product media w/o using MEDIA_DIRECTORY
    config...................Temporary configuration files
    config-templates.........Configuration templates
    logs.....................Setup logs
    runtime..................Runtime environment
        db...................Database runtime
        jrockit..............Jrockit runtime
        wlshome..............Middleware home
            Oracle_IDM1.........IAM (OAM, OAAM, OIM, SOA)
            Oracle_MGMT_IDM1....IDM (OID, OVD)
            IDM_MGMT............OID instance
            user_projects.......WLS domain (base_domain)
            wlserver_10.3.......WLS runtime
```

**Figure 3:** IAM/IDM domain **Directory Structure**

# 13  Product Download Locations

The following table lists download locations for Linux binaries.

| Product | Download Location (Linux x86-64) |
|---|---|
| Oracle Database 11*g* Release 2 (11.2.0.2.0) | https://updates.oracle.com/download/10098816.html<br><br>Select "Linux X86-64" and download the first two binaries as shown below:<br><br>p10098816_112020_Linux-x86-64_1of7.zip<br>p10098816_112020_Linux-x86-64_2of7.zip |
| Oracle WebLogic Server 11*g* Release 1 (10.3.5)<br><br>http://www.oracle.com/technetwork/middleware/weblogic/downloads/wls-main-097127.html | http://download.oracle.com/otn/nt/middleware/11g/wls/1035/wls1035_generic.jar |
| Oracle JRockit JDK for Java Version 6<br><br>http://www.oracle.com/technetwork/middleware/jrockit/downloads/index.html | http://download.oracle.com/otn/bea/jrockit/jrockit-jdk1.6.0_26-R28.1.4-4.0.1-linux-x64.bin |
| Oracle Fusion Middleware Repository Creation Utility 11*g* Release 1 (11.1.1.5.0) | http://download.oracle.com/otn/linux/middleware/11g/111150/ofm_rcu_linux_11.1.1.5.0_disk1_1of1.zip |
| Oracle Identity Management 11*g* Release 1 (11.1.1.2.0)<br><br>http://www.oracle.com/technetwork/middleware/downloads/oid-11g-161194.html | http://download.oracle.com/otn/linux/middleware/11g/ofm_idm_linux_11.1.1.2.0_64_disk1_1of1.zip |
| Oracle Identity Management 11*g* Release 1 Patch Set 4 (11.1.1.5.0) | https://updates.oracle.com/download/12395123.html<br><br>Select "Linux X86-64" and click Download.<br><br>p12395123_111150_Linux-x86-64.zip |
| Oracle Identity and Access Management 11*g* Release 1 (11.1.1.5.0)<br><br>http://www.oracle.com/technetwork/middleware/downloads/oid-11g-161194.html | http://download.oracle.com/otn/nt/middleware/11g/111150/ofm_iam_generic_11.1.1.5.0_disk1_1of1.zip |
| Oracle SOA Suite Release 11*g* Release 1 (11.1.1.5.0)<br><br>http://www.oracle.com/technetwork/middleware/soasuite/downloads/index.html | http://download.oracle.com/otn/nt/middleware/11g/111150/ofm_soa_generic_11.1.1.5.0_disk1_1of2.zip<br><br>http://download.oracle.com/otn/nt/middleware/11g/111150/ofm_soa_generic_11.1.1.5.0_disk1_2of2.zip |
| Oracle Identity Manager 11*g* Release 1 Bundle Patch 2 (11.1.1.5.2) | https://updates.oracle.com/download/13399365.html<br><br>Select "Generic Platform" and click Download.<br><br>p13399365_111150_Generic.zip |

| Oracle Access Manager 11*g* Release 1 Bundle Patch 2 (11.1.1.5.2) | https://updates.oracle.com/download/13115859.html<br><br>Select "Generic Platform" and click Download.<br><br>p13115859_111150_Generic.zip |
|---|---|

# 14 Release Notes

**11.1.1.5.2 Release Notes**
Added the following features:

1. Support user-specified directory to receive product media generated from downloaded product binaries.
2. Support setup from staged product media.
3. Support operation of Oracle WebLogic and Oracle Database without credentials.
4. Optimize start/stop scripts to automatically detect Oracle WebLogic Server up/down conditions.
5. Optimize server restarts to speed up setup time by 25%.
6. Enhance pre-requisites
   - Ensure correct version of PERL.
   - Ensure user is a member of the dba group and is not root.
   - Ensure the machine is configured to use host name resolution.
   - Ensure free HD requirements check reflects location of the installation media directory.
   - Ensure sufficient free HD space on /tmp to account for JROCKIT requirements.
7. Enhance script robustness by exiting upon detecting an unrecoverable error.
8. Log the entire setup process to a log file.
9. Documented functional and directory topology.
10. Apply OAM BP02 and OIM BP02 patches.

**11.1.1.5.0 Release Notes**
Initial Release