The Active Directory Connector Tutorial

In this tutorial we demonstrate the usage of the Active Directory Connector, which integrates a Microsoft Active Directory into Oracle Identity Manager. The underlying scenario is the integration as a result of a company acquisition. All users of the Active Directory are transferred to OIM, which is then used for user management and provisioning of AD accounts. This tutorial includes the installation and configuration of Windows Server and Active Directory, as well as the installation and configuration of the AD connector. We will create an AD structure, using organizational units, users, groups, GPOs (group policy objects) and directory access writes, to model a non-trivial scenario which emulates a real world installations. While we keep the total system still simple, the complexity is already at a level which reveals usability aspects of the connector, which are beyond a mere technical proving of concept. A conclusion summarizes this work and points to areas of further study.

We use the following software versions:

- Oracle Identity Manager Connector MS AD User Management 11.1.1.5.0
- Oracle Identity and Access Management 11.1.1.5
- Oracle Database 11g, Release 2
- Oracle Virtual Box 4.1.22
- Oracle Enterprise Linux 5.8 (32-bit)
- Microsoft Windows Server 2008 R2 (64-bit)
- Microsoft Windows 8 Professional (32-bit)

1 Contents

The Active Directory Connector Tutorial ............................................................................................................ 1
1 Contents .......................................................................................................................................................... 1
2 Introduction ................................................................................................................................................... 2
3 Technical Overview ...................................................................................................................................... 3
4 Setting up the Company domain66.dom ...................................................................................................... 3
  4.1 Modeling the Company domain66.dom .................................................................................................. 3
  4.2 Setting up Windows Server 2008 R2 ..................................................................................................... 5
  4.3 Configuring the Active Directory .......................................................................................................... 6
    4.3.1 Changing Machine Name ..................................................................................................................... 6
    4.3.2 Installing the AD Binaries .................................................................................................................. 7
    4.3.3 Configuring the AD and DNS ......................................................................................................... 8
    4.3.4 Adding a DNS reverse lookup zone .................................................................................................. 11
  4.4 Configuring the Company domain66 .................................................................................................... 13
  4.5 Joining a domain and testing the client access ..................................................................................... 18
  4.6 Configuring name resolution on Linux ................................................................................................. 20
5 Deploying the AD Connector ....................................................................................................................... 22
  5.1 Creating a Target System User Account for Connector Operations .................................................... 22
  5.2 Installing and Configuring the Connector Server .................................................................................. 23
  5.3 Installing the Connector in Oracle Identity Manager ............................................................................ 24
2 Introduction

One important integration scenario for Oracle Identity Manager (OIM) is connectivity to the Microsoft world. Oracle offers several connectors for this purpose. Among them are the “Active Directory User Management”, the “AD Password Synchronization”, and the “Microsoft Exchange” connectors. They are available at http://www.oracle.com/technetwork/middleware/id-mgmt/downloads/connectors-101674.html.

We want to explore the “Active Directory User Management” connector with an example scenario, where a company named domain66, which was recently acquired by our imaginary company MyTech, needs to be integrated. MyTech is running an OIM system for identity management and resource provisioning. Domain66 uses Microsoft technology and maintains their user base and computer networks in an Active Directory. We want to integrate the AD into the OIM, so that the management of domain66 users and AD accounts will be handled by the OIM. In a first step all domain66 users will be synchronized to OIM and their AD accounts will be managed as resources in OIM. In a second step we look at provisioning new AD accounts to newly created OIM users, as it would be the case for new hires. We will also look at the ongoing task of user attribute reconciliation between the two systems.
3 Technical Overview

The whole scenario will be set up on a single Laptop using Virtual Box, to run the different computer systems as virtual machines. We will use one Oracle enterprise Linux machine for the company MyTech, a Windows 2008 R2 server for the company domain66 and a Windows 8 machine as a test client to connect to the AD. The following diagram illustrates this configuration.

We will use the OIM installation in the virtual machine 11OEL_55ODD which was described in a previous tutorial. (http://weblogic-corner.blogspot.de/2012/11/installation-of-oracle-identity-manager_20.html) The machine is connected to the internet via a virtual NAT network adapter, and to the host computer with the Host-Only network adapter “vboxnet” which remains unused in this scenario. We will make a fresh installation of Windows 2008 R2 server into the virtual machine 15Win2008R2 and connect it to a newly created Host-Only network “domain66.dom”. We will install the Active Directory and a DNS server on this machine. The DNS server handles all requests in the network 192.168.66 of domain66. We will also connect the Linux virtual machine and the Windows client to this network, thus it becomes the basic network for this integration scenario. We will use a Windows 8 Pro client for testing user login and provisioning of shared folders. This client machine will become a member of the AD domain.

4 Setting up the Company domain66.dom

Within this chapter we will model and set up the company domain66.dom. This includes modeling the AD components and resources, installing Windows 2008 R2 Server, installing and configuring the Active Directory and the DNS Server, creating the company structure and users in the AD and testing the setup with a Windows client.

4.1 Modeling the Company domain66.dom

Let’s draw our attention to the structure of the domain66, which is using a Windows Network based on Windows Server 2008 R2 and Active Directory. The Company’s organizational structure is illustrated in the following picture.
It consists of two branches, i.e. OrgUnitA and OrgUnitB. OrgUnitA is further subdivided into OrgUnitAA and OrgUnitAB. The users are allocated to the individual OrgUnits. We use a naming schema that resembles this structure. Every organizational unit has its own file share to share files within that unit. We want all users of one unit to be able to read and write files within this share. Users of neighboring units should have read access. Units that are higher in the hierarchy should have full access on the file shares of the subordinate units. Every user within a sub tree, regardless of its position, should have read access to all the files within that tree. The sub trees of the company’s main branches don’t share any files. On the windows server we will allocate access rights to groups instead of individual users. We will then map the users to the groups. This situation is illustrated in the following picture.

\[\text{Figure 2. Organization Diagram of domain66.dom}\]

We will use a Windows 2008 Server to setup and manage this structure. The Server will act as a domain controller. Whenever a user logs into the domain, file shares will automatically be mapped to drive letters. Every user will get the file share mapping belonging to it’s
organizational unit. We will use group policy objects (GPOs) to realize this behavior. The resulting LDAP tree of the AD will look like this:

![Active Directory Users and Computers](image1)

![Active Directory GPO Management](image2)

Figure 4. Active Directory Structure of myCompany.com

The figure depicts two trees, one for the management of Users and Computers and one for the management for GPOs. These trees correspond to the Microsoft tools “Server Manager” and “Group Policy Manager”. The first tree shows the allocation of users to their organizational units. We use the separate organizational unit “OrgUnitGroups” to collect all the groups. The allocation of users to groups is not visible in this picture. The second tree contains GPO policies that are used to map drive letters to file shares. They are executed when a user logs on to the domain. Every GPO maps the given drive for all users of the OrgUnit, where the GPO is located. OrgUnitAA and OrgUnitAB are subordinate units and inherit also the GPO of their parent unit, which is GPO-MapDriveA.

Let’s look at an example how all these settings play together. UserAA01 is member of GroupAA. Thus he gets and read/write permission to FileShareAA and read permission to FileShareAB and FileShareA. He belongs to OrgUnitAA which is a child of OrgUnitA. GPO-MapDriveAA is in effect directly and GPO-MapDriveA is also in effect, since it is inherited from the parent OrgUnit. When UserAA01 logs into the domain myCompany.com, FileShareA and FileShareAA are automatically mapped to drive letters.

4.2 Setting up Windows Server 2008 R2

We want to have a scenario with relevance to real life situations; therefore we install Windows Server in the Domain Controller role as a virtual box machine. Thus we can use the Microsoft tools to add users, groups and resources. This will serve as starting point for the OIM AD connector.

The installation and configuration of Windows Server and Active Directory is widely used in the industry and many books are available on this subject. While the installation is easy and straightforward, we consult the book “Windows Server 2008 R2 von Ulrich B. Boddenberg” for some background information. This book in German is freely available on the internet (http://openbook.galileocomputing.de/windows_server_2008).
Other recommended readings covering Windows Server and AD are:

- Konfigurieren von Windows Server 2008 Active Directory, Original Microsoft Training für Examen 70-640 MCTS¹ (in German, also available in English)
- Chapter 14 about AD LDS² (in German, file is saved to D:\15Work\06OracleIdentityManagement\Konfigurieren_von_Windows_Server_2008_Active_Directory_KAPITEL-14.pdf)

We download an evaluation copy of the DVD installer ISO file (7.1). The evaluation period is 180 days, starting from 18.10.2012. During the installation we set the Administrator Password=Welcome1. We also install the language pack for English using the file from (7.2). The server runs without activation for a grace period of 10 days. After that the server still works but shuts itself down every hour and has to be restarted manually.

To activate the server we temporarily add a NAT network adapter in virtual box manager. We configure DHCP and automatic DNS server setting in the network dialog.

In the Control Panel we search for “Activate Windows” and choose “Activate now”

After some seconds we get a success notice.

![Message after activation of Windows Server 2008 R2.](image)

Server is now activated and the evaluation period begins.


We set-up Host-Only Networking and supply a fixed IP address.

### 4.3 Configuring the Active Directory

Now that Windows Server is running we want to install and configure the active directory. The free online book³ describes this process.

#### 4.3.1 Changing Machine Name

In a first step we change the name of the machine to indicate that this is an “Active Directory Domain Controller”. We use the “Computer Name /Domain Changes” dialog to change the computer name to DC01.

---


² Link to PDF Chapter: [http://www.microsoft-press.de/productinfo.asp?replace=false&cnt=productinfo&mode=2&type=2&id=ms-5970&index=2&nr=0&sid=6f7ed8c914e2e7f94d4e266a7a396f5ec&preload=false&page=1&view=fit&Toolbar=1&pagemode=none](http://www.microsoft-press.de/productinfo.asp?replace=false&cnt=productinfo&mode=2&type=2&id=ms-5970&index=2&nr=0&sid=6f7ed8c914e2e7f94d4e266a7a396f5ec&preload=false&page=1&view=fit&Toolbar=1&pagemode=none)

³ Windows Server 2008 R2 von Ulrich B. Boddenberg: Das umfassende Handbuch [http://openbook.galileocomputing.de/windows_server_2008/windows_server_2008_kap_08_003.htm#mj5eb2021171ee2894fb570f17d033abe](http://openbook.galileocomputing.de/windows_server_2008/windows_server_2008_kap_08_003.htm#mj5eb2021171ee2894fb570f17d033abe)
Changing the computer name of the Windows Server installation.

We have to restart the Windows Server.

### 4.3.2 Installing the AD Binaries

We continue with the installation of the binaries by enabling the server role in the server manager. The installation includes the .Net-Framework. We provide the screens of this process.
Installation dialog of the Active Directory binaries.

Figure 7.

The binaries are now installed.

4.3.3 Configuring the AD and DNS

We continue with the “Active Directory Domain Service Installation Wizard” (dcpromo.exe).
This may take some minutes.
Summary:

Configure this server as the first Active Directory domain controller in a new forest.

The new domain name is "domain66.dom". This is also the name of the new forest.

The NetBIOS name of the domain is "DOMAIN66".

Forest Functional Level: Windows Server 2008 R2
Domain Functional Level: Windows Server 2008 R2
Site: Default-First-Site-Name

Additional Options:
Read-only domain controller: "No"
Global catalog: Yes
DNS Server: Yes
Create DNS Delegation: No

Database folder: C:\Windows\NTDS
Log file folder: C:\Windows\NTDS
SYSVOL folder: C:\Windows\SYSVOL

The DNS Server service will be installed on this computer.
The DNS Server service will be configured on this computer.
This computer will be configured to use this DNS server as its preferred DNS server.
The password of the new domain Administrator will be the same as the password of the local Administrator of this computer.

This takes some mintues…

Figure 8. Configuration dialog of the Active Directory.
After the restart the Domain Controller is ready. We start the Server Manager.

4.3.4 Adding a DNS reverse lookup zone

In order to enable DNS reverse lookup, we have to add a new reverse lookup zone.
Figure 9. Dialog to add a reverse lookup zone in the Windows DNS server.

We check with nslookup, if the machine can access it’s own DNS server.

```
C:\Users\Administrator>nslookup dc01.domain66.dom
DNS request timed out.
timeout was 2 seconds.
Server: UnKnown
Address: ::1
Name: dc01.domain66.dom
Address: 192.168.66.15
```

Ok, but we want to avoid the 2 second timeout which is caused by the IPv6 interface. We simply disable IPv6 in the network settings and insert the ip address of the servers network interface as primary DNS server.

Figure 10. Disabling IPv6 and configuring the primary DNS server in Win2008 Server.

Now the DNS lookup works properly and fast.

```
C:\Users\Administrator>nslookup dc01.domain66.dom
Server: dc01.domain66.dom
Address: 192.168.66.15
Name: dc01.domain66.dom
Address: 192.168.66.15
```
4.4 Configuring the Company domain

We already modeled our test company in section 1. Now we want to create this structure in the Active Directory. We will insert the organizational units, users and groups. Then we will configure the file shares, together with their access rights for groups. Finally we will configure the GPOs that will map the drives for the users.

On the Windows Server DC01 we open the Server Manager and create a new organizational unit by using the context menu and new dialog as illustrated below.

![Creating OrgUnitA in the Active Directory.](image1)

In the same manner we create the other OUs. Then we create the users of our company, again using the new dialog of the AD Server Manager, as depicted below.

![Creating UserA01 in the Active Directory.](image2)

We put the users into their corresponding organizational units. After that, we create the groups in the same manner, but they are placed in the OU OrgUnitGroup.
Creating Groups in the Active Directory.

We don’t care about the group scope within this example since we only have a single domain. The group type however needs to be “Security” since we want to use these groups to map access permissions.

In the next step we create the shares for the directories and assign group permissions to them. We open the file explorer and create four directories. Then, for every directory, we open the properties dialog and choose the tab “sharing” to set group permissions. In the file sharing dialog we type in the group name to add, then we choose which permission should be granted for that group.
Setting up File Shares and Permissions.

Now that the File shares are setup and permissions to groups are granted, we have to assign the group membership. We go back to the Server Manager, choose the context menu of the group we want to edit and open the properties dialog. We open the “Members” tab and add users and groups according to the Figure 3.

The only part missing is the configuration of the Group Policy Objects, (GPOs) which will create a drive mapping for the users.

To create a GPO we go to the Group Policy Management feature in the server manager and navigate in the tree of domain66 to OrgUnitA. We want to create a GPO that is mapped to this OU. From the context menu we choose the entry “Create a GPO and link it here...”.
We name it “GPO-MapDriveA”. This creates the GPO under “Group Policy Objects” and a link under OrgUnitA. The scope tab of the detail form tells us that this policy applies to authenticated users of the domain that are located in OrgUnitA or in organizational units down the hierarchy tree. We start the Group Policy Management Editor from the context menu of the GPO.

![Group Policy Editor](image1)

![Group Policy Editor](image2)

Figure 16. Creating a GPO and starting the Group Policy Management Editor.

In the Group Policy Management Editor, we navigate to “User Configuration->Preferences->Windows Settings->Drive Maps” and from the context menu we choose “new->Mapped Drive”, to configure a drive map in this policy. In the dialog, we enter the location of the file share to map and a drive letter. We also want this drive and all drives to be displayed for the user. Then we change to the “Common” tab, choose “item level targeting” and open the Targeting Editor. Here we configure that this drive map is targeted to all users of the domain, where the GPO is valid.
Creating a Drive Map with the Group Policy Management Editor.

We have created a GPO that maps FileShareA to a drive letter, when a domain user belonging to OrgUnitA or any OrgUnit down the tree, i.e. OrgUnitAA and OrgUnitAB, logs in.

In the same manner we create the GPOs GPO-MapDriveAA, GPO-MapDriveAB and GPO-MapDriveB.

Creating Drive Map GPOs for the rest of the File Shares.
The resulting GPO tree in the server manager is given in the following picture.

![Server Manager GPO Tree](http://weblogic-corner.blogspot.com)

**Figure 19. Resulting GPO tree after creating all Drive Mapping GPOs.**

The company domain66 is now setup. When a user logs into the domain from a client machine she gets a drive mappings and access rights on these mappings according to her organizational unit.

Provisioning a new user account would include creating a user in the chosen OrgUnit and adding it to the respective security group.

### 4.5 Joining a domain and testing the client access

In order to test the domain configuration, we boot up a Windows 8 Professional client as a virtual machine and add it to the domain. Then we log on as a domain user, check the mapped drives and test the read and write permissions.

In a first step we configure the network settings. We want to supply a fixed ip address and the address of our DNS server. In the virtual box network setting we verify that the machine is connected to the network 192.168.66. We start the client and log on as local Administrator.

![Network Settings](http://weblogic-corner.blogspot.com)

**Figure 20. Network settings of the Windows 8 client in the virtual box manager.**

Now we change to desktop view and start the control panel and navigate to the network settings. The following picture illustrates the relevant settings of the interface “Ethernet2”
which is connected to the “Virtual Box Host-Only Ethernet Adapter 2”. In the properties dialog we disable IPv6. We only want to use IPv4 addresses to reduce the complexity of the scenario. In the properties dialog for the IPv4 settings we supply a fixed IP address, and the default gateway. We configure the DC01 DNS server as preferred DNS. The alternate DNS server is for name resolution in the internet via the first interface, which is configured as NAT in virtual box. The following picture summarizes these settings.

![Network configuration of the Windows 8 client.](image1)

Figure 21. Network configuration of the Windows 8 client.

Now we want to add this computer to the domain. We open the system properties dialog via the control panel and change its membership from workgroup to a domain.

![Opening the System Properties Dialog in Windows 8.](image2)

Figure 22. Opening the System Properties Dialog in Windows 8.

In the “Domain Changes” dialog we supply the name with which we want to register this computer in the domain and the domain we want to join. In a subsequent dialog we provide the user and password of the domain administrator, which is the user, we use to login to the Windows 2008 Server (Administrator/Welcome1). We receive a welcome message and notice the client machine has to be restarted.
Figure 23. **Adding the Windows 8 Client to the Domain domain66.dom.**

After the restart we can log into the Windows8 client as domain user. We choose UserAA01/Welcome1. We go to the desktop and open the explorer and click on computer. Now we can see that the FileShareA and FileShareAA are maped to drive letters as expected.

Figure 24. **Checking the driver letter mapping for UserAA01.**

We also want to check the permissions. We can read files in FileShareA but cannot create files here. We can read and write files in FileShareAA. This behavior is as expected. Ok.

### 4.6 Configuring name resolution on Linux

We want to use the name resolution of our new DNS server on the Linux side. Here we have three network interfaces, which are eth0, eth1, and eth2. First we create a new network profile, “ADConnector”. The interface eth0 is the NAT-interface for the internet connection. It is configured through DHCP. We have to disable the automatic DNS Server configuration here. We also configure primary and secondary DNS as illustrated below.
Network configuration on Linux to use two DNS servers.

We restart the network and check the DNS resolution.

```
[root@localhost oracle]# /etc/init.d/network restart
[root@localhost oracle]# nslookup dc01.domain66.dom
Server: 192.168.66.15
Address: 192.168.66.15#53
Name: dc01.domain66.dom
Address: 192.168.66.15

[root@localhost oracle]# nslookup www.google.de
Server: 192.168.178.1
Address: 192.168.178.1#53
Non-authoritative answer:
Name: www.google.de
Address: 173.194.44.159
Name: www.google.de
Address: 173.194.44.152
Name: www.google.de
Address: 173.194.44.151
```

In the first request we test the DNS Server of the Windows 2008, which is the primary server and it answers directly. In the second call we check the DNS resolution for the internet which is answered by the Fritzbox router.

We also want the Windows DNS Server to resolve the Linux address of eth2 so we insert a record for it in the Windows DNS Manager.

```
[<root@localhost oracle>]
```

Figure 25.  Network configuration on Linux to use two DNS servers.

Figure 26.  Adding the eth2 interface of the Linux server to the DNS.
We insert a record in the Forward Lookup Zone “domain66.dom” and provide the IP address. We also update the associated pointer record to enable reverse lookup. Now both directions are working from Linux and Windows.

```
root@localhost oracle]# nslookup oim.domain66.dom
Server:         192.168.66.15
Address:        192.168.66.15#53
Name:   oim.domain66.dom
Address: 192.168.66.12

[root@localhost oracle]# nslookup 192.168.66.12
Server:         192.168.66.15
Address:        192.168.66.15#53
12.66.168.192.in-addr.arpa name = oim.domain66.dom.
```

Ok.

5 Deploying the AD Connector.

We will use Oracle Identity Manager Connector MS AD User Management 11.1.1.5.0. We download the software from the download link [http://www.oracle.com/technetwork/middleware/identity-management/downloads/connectors-101674.html](http://www.oracle.com/technetwork/middleware/identity-management/downloads/connectors-101674.html) (see 7.4). We will skip the recommended patch (See 7.5) because we will not be affected by the solved bugs in the context of this tutorial. The list of certified components also recommends patch 13684913 (See 7.6) which we also will skip.

The list of certified components at [http://docs.oracle.com/cd/E22999_01/doc.111/e20347/intro.htm#BABGDDEE](http://docs.oracle.com/cd/E22999_01/doc.111/e20347/intro.htm#BABGDDEE) includes Windows Server 2008 R2 which we will use as a Windows Domain Controller to run the Active Directory.

To deploy the AD Connector, we follow the instructions in [http://docs.oracle.com/cd/E22999_01/doc.111/e20347/deploy.htm#autoId0](http://docs.oracle.com/cd/E22999_01/doc.111/e20347/deploy.htm#autoId0)

5.1 Creating a Target System User Account for Connector Operations

In the Windows Server we create an organizational unit OrgUnitOIM. Here we create the security group OIMGroup. We add this group to the Built-in Group “Konten-Operatoren” (Account Operators). Finally we create a User OIMUser and add this user to the Group OIMGroup. This situation is illustrated in the following figure.

```
Figure 27. OIMUser and its group membership in the Active Directory.
```

We will use this user during the configuration of the AD Connector on the Linux side (see Figure 31).
5.2 Installing and Configuring the Connector Server

We follow the instructions at http://docs.oracle.com/cd/E22999_01/doc.111/e20347/deploy.htm#autoId6. We download the connector server package (7.3) and extract the contents to D:\VirtualBox\GlobalSharedFolder\Connector_Server_111150\Connector_Server_111150. In the feature summary of the server manager we verify that the .NET-Framework is installed. We run the installer from the Windows Server.

We provide the screens of the installer, however there is nothing to choose here.

We locate the Connector Server in the windows services pane and stop it.

We update the key of the connector server to the value “Welcome1”

```
C:\Program Files (x86)\Identity Connectors\Connector Server> ConnectorServer.exe /setkey Welcome1
Key Updated.
```

The key will be updated in encrypted form in the file ConnectorServer.exe.config. We add the section for logging and check the rest of the settings in this file.

```xml
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <connectionStrings>
  <!-- Example connection to a SQL Server Database on localhost. -->
  <add name="ExampleConnectionString" connectionStrings="Data Source=localhost;Initial Catalog=DatabaseName;Integrated Security=True" providerName="System.Data.SqlClient" />
  </connectionStrings>
  <appSettings>
    <add key="connectorserver.port" value="8759" />
    <add key="log4net.config" value="/opt/log4net/log4net.config" />
  </appSettings>
</configuration>
```

We use the default values here.
5.3 Installing the Connector in Oracle Identity Manager

Now we want to install the connector on the Linux side.

We follow the instructions at http://docs.oracle.com/cd/E22999_01/doc.111/e20347/deploy.htm#autoId9.

We install from the package activedirectory-11.1.1.5.0.zip (see 7.4). We copy the package to the shared folder at D:\16VirtualBox\99GlobalSharedFolder\activedirectory-11.1.1.5.0.

On Linux, we copy the media contents to its target location.

In the next step we should login to the OIM console with a User described in ( "Creating the User Account for Installing Connectors" ), however this link is invalid.

Instead this link http://docs.oracle.com/cd/E21764_01/doc.1111/e14308/conn_mgmt.htm#autoId5 says that a user of the SYSTEM ADMINISTRATORS group is fine.

So we login with user xelsysadm/welcome1X at the URL http://192.168.56.12:14000/oim.

We provide the screens for the installation.
Now we are instructed to purge the OIM server cache as described in http://docs.oracle.com/cd/E22999_01/doc.111/e20347/deploy.htm#BABCFE

We provide the commands in the following box.

```
[oracle@12oel55_odd bin]$ pwd
/opt/oracle/Middleware01/Oracle_IDM1/server/bin
[oracle@12oel55_odd bin]$ export WL_HOME=/opt/oracle/Middleware01/wlserver_10.3
[oracle@12oel55_odd bin]$ ./PurgeCache.sh All
[Enter the admin username]: xelsysadm
[Enter the admin password]: welcome1X (not shown in the shell)
[Enter the service url : (i.e.: t3://oimhostname:oimportno)] t3://localhost:14000
PurgeCache Login Success...
Purging the cache categories:
All is successful
```

In the next step we configure the IT resources for the target system as described in http://docs.oracle.com/cd/E22999_01/doc.111/e20347/deploy.htm#autoId11.

We are still logged in with the user xelsysadm on the “Advanced Administration” page.
Configuring the IT resources for the target system to connect to the AD.

We set up a configuration for identity reconciliation (trusted source reconciliation) first.

We provide the following values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connector Server Name</td>
<td>Active Directory Connector Server (default)</td>
</tr>
<tr>
<td>Container</td>
<td>DC=domain66,DC=dom</td>
</tr>
<tr>
<td>DirectoryAdminName</td>
<td>DOMAIN66\OIMUser</td>
</tr>
<tr>
<td>DirectoryAdminPassword</td>
<td>Welcome1</td>
</tr>
<tr>
<td>DomainName</td>
<td>domain66.dom</td>
</tr>
<tr>
<td>isADLDS</td>
<td>No</td>
</tr>
<tr>
<td>LDAPHostName</td>
<td>DC01</td>
</tr>
<tr>
<td>SyncDomainController</td>
<td>DC01</td>
</tr>
<tr>
<td>SyncGlobalCatalogServer</td>
<td>DC01</td>
</tr>
<tr>
<td>UseSSL</td>
<td>No</td>
</tr>
</tbody>
</table>

Ok.
5.4 Installing the Connector in the Connector Server

We now configure the Windows side and follow the instructions from http://docs.oracle.com/cd/E22999_01/doc.111/e20347/deploy.htm#autoId12. In a first step we shut down the connector server and copy the content of the distribution media F:\activedirectory-11.1.1.5.0\bundle\ActiveDirectory.Connector-1.1.0.6380.zip to the connector server home at C:\Program Files (x86)\Identity Connectors\Connector Server.

![Connector Server Home and Active Directory Connector bundle](image)

After copying the bundle files directly into the connector server home, we restart the connector server via the services pane.

We continue with the configuration of the IT resources for the connector server. We login again in the OIM Administration Console and go to Advanced->Manage IT Resources dialog as before. We search for “Active Directory Connector Server” and click edit.

![Configuring the details for the AD Connector resource in OIM](image)

The AD connector is now installed and configured. We continue with the post installation activities.

5.5 Post installation steps

The post installation steps are documented at http://docs.oracle.com/cd/E22999_01/doc.111/e20347/deploy.htm#autoId15. We want purge the server cache and modify connection pool definitions. The rest of the activities is optional. We purge the server cache on the Linux machine again, as already done before in 5.3.

```
/oracle@12oel55_odd bin]$ pwd
```
Now we want to modify the settings for the connection pool, just to test the installation. We open the Design Console and login as xelsysadm/welcome1X.

Listing 2. Starting the Design Console from the Windows command prompt.

In the design console we add the properties “Pool Max Idle” and “Pool Max Size” and define the value 11. We are satisfied with the default values for the rest of the properties.

A search in the exported database reveals that the parameters are inserted in the data table LKV. OIM represents sets, e.g. to define system property values, in two tables. The LKU table holds keys, that identify a set, and the LKV table defines the members of a set. The following picture shows the result of the search for the string “Pool Max” in the exported OIM database. There are two occurrences in the file LKV.tsv. If we filter for the LKU-Key 1702, we get all the members of that set, which matches exactly the property set that we modified with the Design Console.

The entry in the LKU table corresponding to the key 1702 is:
It contains the Lookup Definition Code "Lookup.Configuration.ActiveDirectory.Trusted", which we used for searching in the Design Console. When the AD connector is installed, it uses the OIM Administration Lookup tables to store its configuration data. These values can be modified using the Design Console.

6 Integrating domain66 into the OIM

The AD connector is installed and configured to operate between the AD of the Windows Server and the OIM on the Linux machine. Now we want to integrate the users of domain66 into the OIM. Therefore we have to configure and run several scheduled task in OIM. The following picture summarizes this process.

Figure 36. Overview of the integration of company domain66 into the OIM.

On the left side we see the AD tree of domain66.dom as configured previously. As a precondition we have to populate the lookup maps for groups and organizations in the OIM with the values from the AD. The AD connector uses these lookup maps during provisioning and reconciliation operations. Therefore, in step 1 and step 2 we run the scheduled jobs for “AD Group Lookup Recon” and “AD Organization Lookup Recon”. We want create all AD users and organizations as users and organizations in OIM. This is done in step 3 and step 4 with the scheduled tasks “AD Organization Recon” and “AD User Trusted Recon”. In this step the AD serves as trusted source, however we only use these scheduled tasks to initially create the users in the OIM. Subsequent user management will be done with the OIM, which becomes the trusted source for identities for both companies, domain66 and MyTech. Now all users exist in the OIM, however without any AD accounts. In step 5 we configure and run the scheduled job “AD Users Target Recon”. Thus all AD accounts are created in the resource section of the matched OIM users. In step 6 we create a new user in OIM and provision an AD account using “Direct Provisioning” of the OIM. This results in the creation of a user in the AD. In step 7 we setup the scheduled job “AD User Target Recon” to synchronize any changes that are made to user’s attributes. This job should be configured to run on a regular basis.
6.1 Scheduled Tasks for Lookup Field Synchronization

There are two scheduled tasks for lookup field synchronization, one for groups, and the other for organizations. The configuration is documented at http://docs.oracle.com/cd/E22999_01/doc.111/e20347/using_conn.htm#autoId4.

Before running the jobs, we check the configurations. We login to the OIM Console and open the job detail pages for the scheduled tasks “Active Directory Group Lookup Recon” and “Active Directory Organization Lookup Recon”. OIM console -> Advanced -> System Management -> Scheduler. We enter “Active*” in the search field and get a list of all Active Directory Scheduled Jobs. We verify that the values in the parameter section correspond to the documentation. We don’t want to get all the groups available in the AD, only those relevant for us. Therefore we apply the filter: “startsWith('name', 'Group')”, thus only the groups we created ourselves in the AD will be fetched. For the lookup of OrganizationalUnits we use the filter “startsWith('ou', 'OrgUnit’)” to fetch only the OrgUnits we have created according to our naming schema.

The filter syntax is documented at http://docs.oracle.com/cd/E22999_01/doc.111/e20347/using_conn.htm#CHDJFDBI. We use the attribute names “name” and “ou” in the filter expression. We get these names from the Attribute Editor in Windows 2008 Server as depicted below.

![Using the Attribute Editor in Windows 2008 Server to find the attribute names for the filter expressions.](image)

The following pictures illustrate the settings for group and organization lookup reconciliation.
We run the Group Lookup Reconciliation by pressing run, and after a while, refresh. The job status is indicated as successful in the history field.

We can see the effect of this action in the Design Console. The attribute map for the code Lookup.ActiveDirectory.Groups gets populated.

We also run the Organization Lookup Recon task and check the attribute map in the Design Console.
Running the Active Directory Organization Lookup Recon scheduled task.

The Lookup Field definitions are now synchronized between AD and OIM.

We take a snapshot of the Linux machine at this point.

<table>
<thead>
<tr>
<th>Sicherheitspunkt 10</th>
<th>System started.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Scheduled Jobs for Active Directory Group and Organization Lookup Recon run.</td>
</tr>
<tr>
<td></td>
<td>Used Filters:</td>
</tr>
<tr>
<td></td>
<td>startsWith('name', 'Group')</td>
</tr>
<tr>
<td></td>
<td>startsWith('ou', 'OrgUnit')</td>
</tr>
</tbody>
</table>

Ok.

### 6.2 Configure and run organization reconciliation

Now we want to import all relevant organizational units from the AD to OIM. This is a prerequisite for importing the AD users. We follow the instruction at http://docs.oracle.com/cd/E22999_01/doc.111/e20347/using_conn.htm#autoId15.

In a first step we check the Configuration Lookup Parameter of the IT Resource. We open the “Manage IT resource dialog” in the OIM Console as depicted below.

Next, we check that the configuration lookup parameter is set to Lookup.Configuration.ActiveDirectory.Trusted. Thus we make sure that we run the adapter in the trusted source reconciliation mode. In this mode we run the AD Organization Recon task with the parameter “Resource Object Name = Xellerate Organization”. Furthermore we configure the filter with the value `startsWith('ou', 'OrgUnit')` to reconcile only the relevant subset of organizational units.
Step 1: Running the AD Organization Recon Task in identity management mode.

Then we change the configuration lookup parameter of the IT Resource to Lookup.Configuration.ActiveDirectory. Thus we switch the adapter to provisioning mode. We change the parameter “Resource Object Name = AD Organizational Unit” and clear the last token filed. Then we run the task again.

Step 2: Running the AD Organization Recon Task in provisioning mode.

As a result the AD OrgUnits are reconciled to OIM and the resources “AD Organizational Unit” and “Xellerate Organization” are provisioned to the OUs, which we can see in the administration pane of the OIM Console.

AD OrgUnits in OIM as a result of the reconciliation process.

We switch the configuration lookup parameter back to Lookup.Configuration.ActiveDirectory.Trusted to run in trusted source mode again. We check the events that were created with these two runs.
Events created during Organization Reconciliation.

Now we have created the OrgUnits from the AD as OIM organizations. In the next step we want to create the AD users in OIM. Since they are created in their corresponding organizational units, we needed to create these organizations in OIM first.

6.3 Configure and run user trusted reconciliation

Now we open the job detail tab for “Active Directory User Trusted Recon” and configure the settings for trusted user reconciliation. We only want run this task once to create all relevant users of the domain66 in the OIM. We need to run the connector in “Identity Management” mode so we check that the IT resource “Active Directory” is set to “Lookup.Configuration.ActiveDirectory.Trusted” Then we edit some attributes as depicted below, e.g. we set the filter to “startsWith('sAMAccountName', 'User')”. Then we run the job.

Running the AD User Trusted Recon job to create the AD users in OIM.

If we go to the “Administration” page and search for all users we can see that our users from domain66 are now created in OIM and also have the correct organization attribute.
resources tab however is still empty, which means that these users are not connected to any AD user accounts yet.

![Image](http://weblogic-corner.blogspot.com)

**Figure 5. Newly created Users as a result of the trusted user reconciliation.**

While these users now exist in OIM, they cannot login because their passwords were not synchronized from the AD. This connector cannot propagate password changes from AD to OID. This can be accomplished with the “Microsoft AD Password Synchronization Connector”.

6.4 Configure and run user target reconciliation

We now want to match the AD-Accounts to the newly created users in OIM and therefore configure user target reconciliation. We need to run the connector in “Provisioning” mode, so we verify that the IT resource “Active Directory” is set to “Lookup.Configuration.ActiveDirectory”. We open the scheduled task tab for “Active Directory User Target Recon”.

![Image](http://weblogic-corner.blogspot.com)
Running the user target reconciliation to create AD account resources for the newly created OIM users.

If we check the Resource section of a user, e.g. UserAA01 as in the following picture, we can see that the corresponding AD User account is provisioned.

The AD User accounts are now provisioned to the newly created OIM users.

In the “Resources” tab we can open the “Users Form” dialog and check the attributes. We also check the assigned groups by selecting the “Assigned Groups Form” in the dropdown box.

If we would change some of these attributes in the “AD Users Form” or in the Active Directory directly, this would be reconciled by the next run of the scheduled job. Further tests reveal that the job "AD User Target Recon" updates attributes of this resource in both directions, depending on the newer change date. Changing an Attribute in the OIM Users Form directly changes these attributes in the AD. Disabling and enabling of the resource in OIM also takes effect immediately in the AD. The Job "Active Directory User Target Delete Recon" is used to revoke the resource in OIM when an AD User was deleted.
Up to now the users of the company domain66 are fully integrated within the OIM. We now want to see how we can create new users in OIM and provision an AD account to it.

6.5 Executing direct user provisioning.

We will create a new OIM User UserAB03 and provision an AD account to it. In the OIM console we change to “Administration” and choose “Create User”.

![Creating a new user in OIM and starting the resource provisioning.](http://weblogic-corner.blogspot.com)

After providing the required user attributes we save it and turn to the “Resources” tab. There are no resources provisioned yet. We press “add” to provision a new AD Account. This will open the “Provision Resource to User” dialog.

![We check the confirmation page.](http://weblogic-corner.blogspot.com)

We select the Resource.

![We add the membership to GroupAB](http://weblogic-corner.blogspot.com)

We provide additional values and choose the OrgUnit.
We check the summary and provision the account.

Figure 10. Steps of the “Provision Resource to User” dialog in OIM.

We provide the basic user information, the organization and group assignments and create the user. The summary page displays all attributes that can be set in the users form. Note that the dialog skips step 3 and 4. If we check the Active Directory in the Server Manager of Windows 2008, we find the UserAB03 in the correct OrgUnit.

Figure 11. Verifying the creation of AD UserAB03 with the Server Manager of Windows.
Now we want to start the Windows 8 client and login as the newly provisioned UserAB03. Since our Windows client is a member of the AD domain, we can directly login from there.

![Login Screenshot](image)

Figure 12. Checking login and permissions for UserAB03 with the Windows 8 client.

We change to the desktop and open the explorer. We can see that FileShareAB is already mapped to drive I:, as expected, according to the GPOs of the domain. We check write permissions to FileShareAB by creating a text file with notepad. We can also open and read FileShareAA via the network, as expected, according to the group membership. But we don’t have read access to FileShareB, as expected, due to the missing group membership of GroupB.

Summing up, during the provisioning of an AD account in OIM, we created a new user account in the AD. By providing OrgUnit and Group memberships we created drive mappings and enforced access permissions, according to the policies of the AD.

7 Downloads

The following sections list the software download that were used during this work.

7.1 Windows Server 2008 R2 DE-X64

<table>
<thead>
<tr>
<th>Link</th>
<th>File</th>
<th>MDS</th>
<th>Notes</th>
</tr>
</thead>
</table>
7.2 Windows Server 2008 R2 Service Pack 1 User Interface Language Packs (EN)

File D:\01Downloads\Windows6.1-KB2483139-x64-en-US.exe
MD5 f70b8ca16eb79240bdf14d2b9f3f4e
Notes

7.3 Connector Server 11.1.1.5.0

File D:\01Downloads\Connector_Server_111150.zip
MD5 258675d766210b0924aa9ab09e111542 (unknown by Google)
Notes

7.4 Oracle Identity Manager Connector MS AD User Management 11.1.1.5.0

File D:\01Downloads\activedirectory-11.1.1.5.0.zip
MD5 65b18f6a39d709a1cac49446a2d7f1e8
Notes Please apply AD connector patch 14190610 after downloading from MOS (My Oracle Support) if you are using this connector against OIM 11.1.2.0 or above.

7.5 AD Connector Patch 14190610: MERGE LABEL REQUEST ON TOP OF 11.1.1.5.0

Link [https://support.oracle.com/epmos/faces/PatchResultsNDetails?_adf.ctrl-state=vrt360o47f_9&releaseId=17111150&requestId=15273691&patchId=14190610&languageId=0&platformId=2000&_afrLoop=457977425119592](https://support.oracle.com/epmos/faces/PatchResultsNDetails?_adf.ctrl-state=vrt360o47f_9&releaseId=17111150&requestId=15273691&patchId=14190610&languageId=0&platformId=2000&_afrLoop=457977425119592)
File D:\01Downloads\p14190610_111150_Generic.zip
MD5 e998966bc093ee3d301c6cd6156e5e3cd
Notes MD5 from Website MD5 E99896BC093EE3D301C6CD6156E5E3CD matches, Ok.

Figure 13. Description of AD Connector Patch 14190610
7.6  AD Connector Patch 13684913

Link  https://support.oracle.com/epmos/faces/PatchResultsNDetails?_adf.ctrl-state=vt360bo47l_9&releaseId=19800111152&requestId=14605415&patchId=13684913&languageId=0&platformId=2000&_afrLoop=458761440548960
File  D:\01Downloads\p13684913_111152_Generic.zip
MDS  8f89313c6355ecab71fc408a6ba50192
Notes  8F89313C6355ECAB71FC408A6BA50192 from oracle website matches, ok.

Figure 14.  Description of Patch 13684913

8  Miscellaneous

Contained in this chapter are some additional articles explored during the course of the tutorial, which might of interest.

8.1  AD Connector Modes

The AC Connector can be configured into one of two modes, which are Identity reconciliation and Account Management. The following table contains a mode comparison.

<table>
<thead>
<tr>
<th>Operation modes</th>
<th>Identity Reconciliation</th>
<th>Account Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synonyms</td>
<td>trusted source reconciliation; authoritative source reconciliation</td>
<td>target resource management</td>
</tr>
<tr>
<td>Operations</td>
<td>trusted source reconciliation</td>
<td>Provisioning, Target resource reconciliation</td>
</tr>
<tr>
<td>Purpose</td>
<td>AD is the trusted source to create OIM Users, Groups and Organizations</td>
<td>OIM is the source to provision and update User accounts in AD</td>
</tr>
<tr>
<td>Lookup Definitions</td>
<td>Active Directory Group Lookup Recon</td>
<td>Active Directory Organization Lookup Recon</td>
</tr>
<tr>
<td>Scheduled Jobs for Groups</td>
<td>Active Directory Group Recon, Active Directory Group Delete Recon,</td>
<td></td>
</tr>
<tr>
<td>Scheduled Jobs for Organizations</td>
<td>Active Directory Organization Recon</td>
<td>Active Directory Organization Delete Recon</td>
</tr>
<tr>
<td>Scheduled Jobs for Users</td>
<td>Active Directory User Trusted Recon, Active Directory User Trusted Delete Recon,</td>
<td>Active Directory User Target Recon, Active Directory User Target Delete Recon,</td>
</tr>
</tbody>
</table>
8.2 Analysis of Database Content

Since some of the configuration information is stored in xml files and other parts are stored in the database, we export the database content into text files for analysis purposes. We run 4 four exports and store the results in separate folders.

![Separate folders for the Database export.](image)

We start the SQL Developer, connect to the database and export the schemas separately.

![Exporting the data of the DEV_MDS Database Schema.](image)

Now we can analyze the data of the tables or use a search tool to find expressions within these files easily. Here is a screen shot, using PSPad for searching the string UserAA in the
DEV_OIM Schema.

Figure 17. Example for searching in the exported database table.

The demonstrated analysis method enables full text search through the database content. However it is only practical for small databases.

8.3 Starting and Stopping the Scheduler

The scheduler can be started and stopped. This will impact all scheduled tasks. To check the status login to http://192.168.56.12:14000/SchedulerService-web

Figure 18. Checking that status of the scheduler via the web interface.

8.4 Snapshots during the Installation of Windows Server 2008 R2

As a recommended practice we take virtual machine snapshots at distinct point in the installation process. Thus we can recover to the last snapshot if we run into problems.

Sicherheitspunkt 1 Installation Server 2008 R2
Administrator/Welcome1
Host-Only Network, feste IP=192.168.56.15
Guest Additions

Sicherheitspunkt 2 Installation of Winows Updates. Up to 18.10.2012

Sicherheitspunkt 3 English Language Pack
Host-Only Network, fix IP=192.168.66.15 (additional network)
NAT-network disabled, (no internet connection)

Sicherheitspunkt 4 Changing Computer Name to AD01
Installation of Active Directory Domain Controller and DNS Server.
Domain Name = domain66.com
8.5 Updating the virtual box guest additions on Linux.

We need to update the virtual box guest additions, since we have updated virtual box in the meantime.

```
[root@12oel55_odd VBOXADDITIONS_4.1.22_80657]# pwd
/media/VBOXADDITIONS_4.1.22_80657
[root@12oel55_odd VBOXADDITIONS_4.1.22_80657]#
Verifying archive integrity... All good.
Uncompressing VirtualBox 4.1.22 Guest Additions for Linux..........
VirtualBox Guest Additions installer
Removing installed version 4.1.16 of VirtualBox Guest Additions...
Removing existing VirtualBox DRMS kernel modules [ OK ]
Removing existing VirtualBox non-DRMS kernel modules [ OK ]
Building the VirtualBox Guest Additions kernel modules
Building the main Guest Additions module [ OK ]
Building the shared folder support module [ OK ]
Building the OpenGL support module [ OK ]
Doing non-kernel setup of the Guest Additions [ OK ]
You should restart your guest to make sure the new modules are actually used
Installing the Window System drivers
Installing X.Org 7.1 modules [ OK ]
You may need to restart the hal service and the Window System (or just restart
the guest system) to enable the Guest Additions.
Installing graphics libraries and desktop services components [ OK ]
```

Ok.

9 Conclusion

In this tutorial we demonstrated the configuration and usage of the OIM AD connector in a company acquisition scenario. The Active Directory based user management of our example company domain66 was integrated into Oracle Identity Manager. The connector’s scheduled jobs were used for an initial integration of all domain66 users. Subsequent steps demonstrated the provisioning of AD accounts to new users and the reconciliation of changed attributes of existing users. The installation and configuration of Windows Server, Active Directory and a DNS server, as well as the initial modeling and setup of the company domain66 was included in this tutorial. The OIM installation was based on the virtual machine of a previous tutorial. While this work elucidates the general idea of AD connector usage, additional topics have to be considered for a productive scenario in the real world. These include the usage of SSL secured communication and password synchronization, which was omitted in this work. Furthermore, a real world scenario would most probably use a high-availability configuration of the OIM and several replicated AD instances. Some fields for further investigation might be the reconciliation of deleted users, as well as extending the connector’s functionality to include custom fields.