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

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.

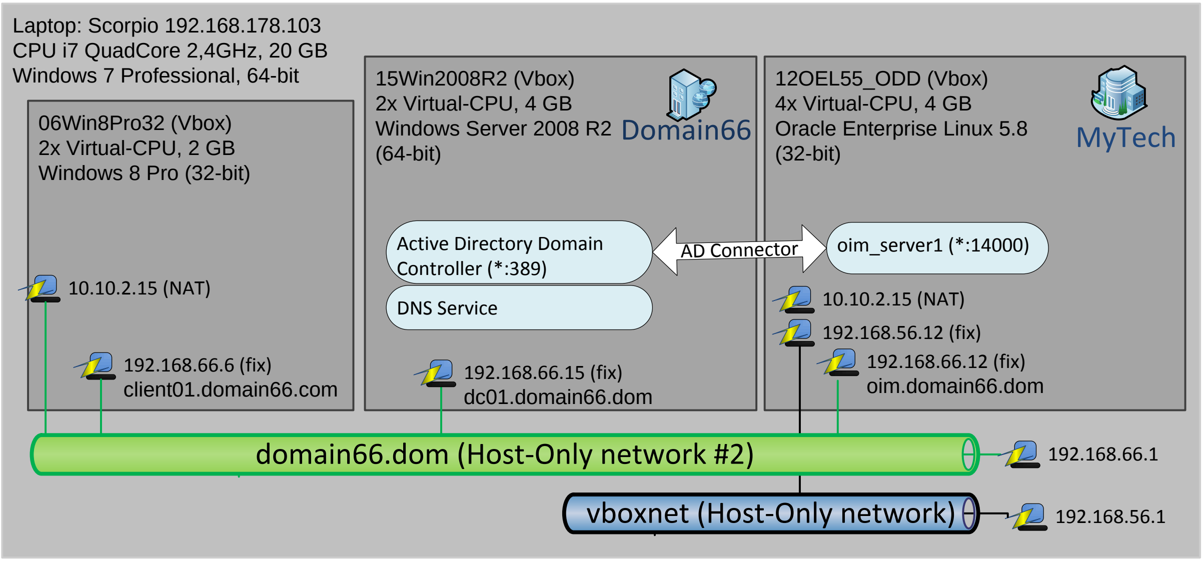


Figure 1. **Technical diagram for the OIM – Active Directory Connector tutorial.**

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-manger_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.

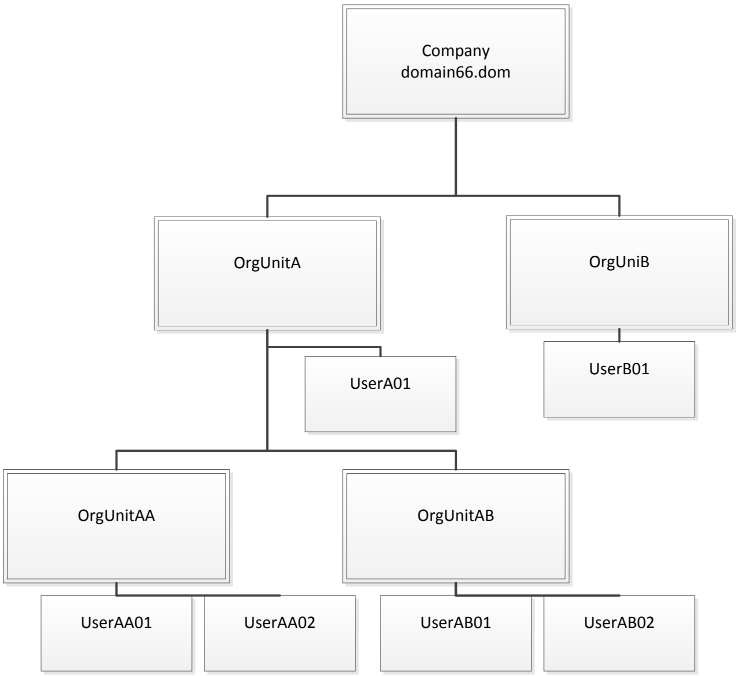


Figure 2. **Organization Diagram of domain66.dom**

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.

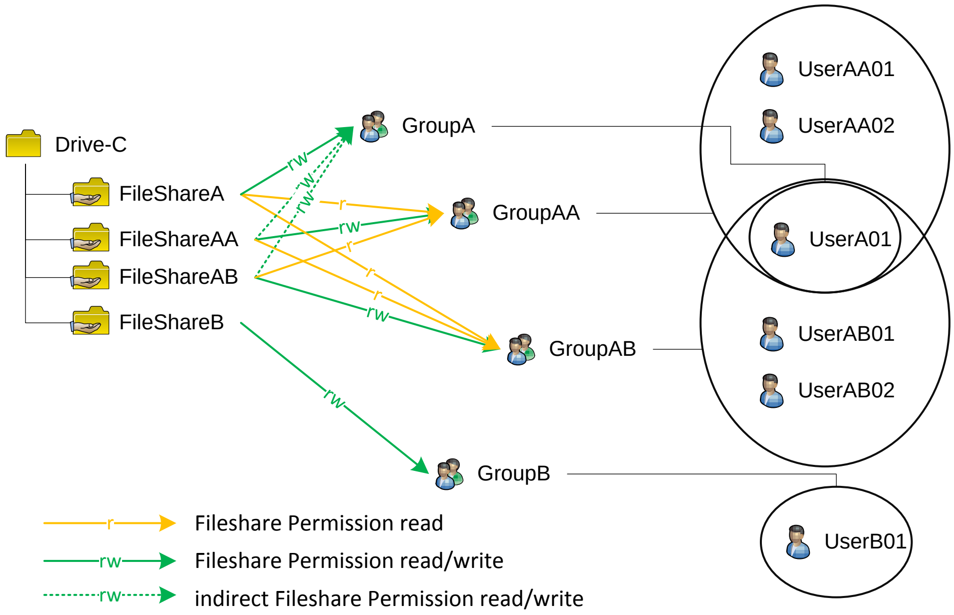


Figure 3. **File Shares and allocation of access rights to groups and users.**

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:

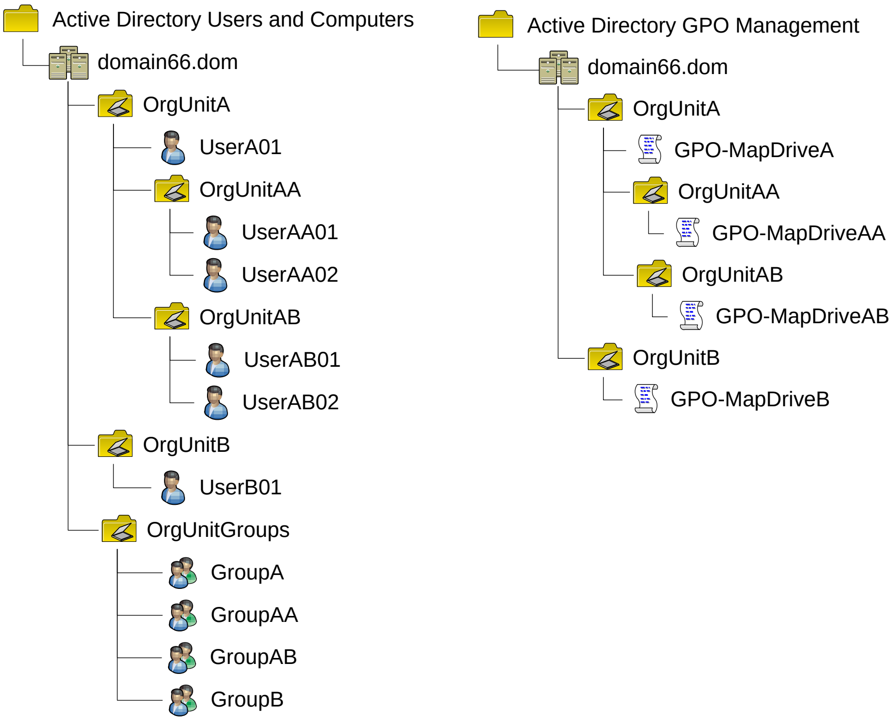


Figure 4. **Active Directory Structure of myCompany.com**

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 Mircosoft 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

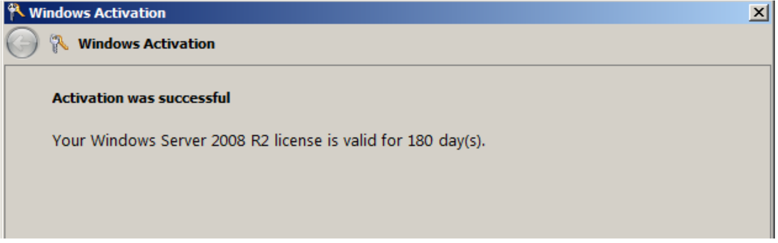
We want to have a scenario with relevance to real life situations; therefore we install Windows Server in the Domain Controller role as a virtual box machine. Thus we can use the Microsoft tools to add users, groups and resources. This will serve as starting point for the OIM AD connector.

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 straight forward, 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 MCTS[1] (in German, also available in English)
- Chapter 14 about AD LDS[2] (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.



Activation was successful

Your Windows Server 2008 R2 license is valid for 180 day(s).

Figure 5. **Message after activation of Windows Server 2008 R2.**

Server is now activated and the evaluation period begins.
31.10.2012 + 180 days = 29.04.2013.

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 book[3] describes this process.

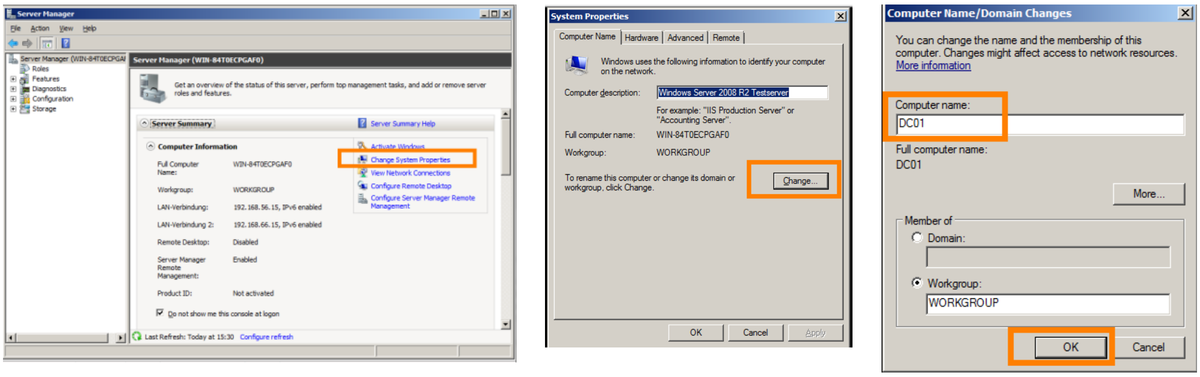
4.3.1 Changing Machine Name

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.

[1] Link to Book: http://www.microsoft-press.de/product.asp?cnt=product&id=ms-5970&titel=Konfigurieren%20von%20Windows%20Server%202008%20Active%20Directory

[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=6f7ede8c914e2e7fad4c26a7a396f5ec&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#mj5eb2021171eea2894fb570f17d033abe



Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.

Computer Information

Full Computer Name: WIN-84T0ECPGAF0

Workgroup: WORKGROUP

LAN-Verbindung: 192.168.56.15, IPv6 enabled

LAN-Verbindung 2: 192.168.66.15, IPv6 enabled

Remote Desktop: Disabled

Server Manager Remote Management: Enabled

Product ID: Not activated

☑ Do not show me this console at logon

Last Refresh: Today at 15:30

Windows uses the following information to identify your computer on the network.

Computer description: Windows Server 2008 R2 Testserver

For example: "IIS Production Server" or "Accounting Server".

Full computer name: WIN-84T0ECPGAF0

Workgroup: WORKGROUP

To rename this computer or change its domain or workgroup, click Change.

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: DC01

Full computer name: DC01

Member of

○ Domain:

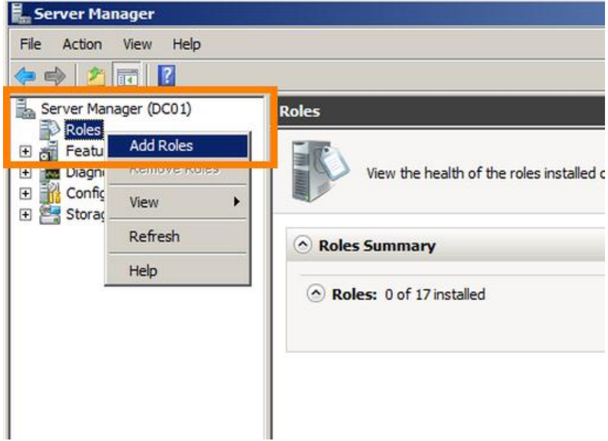
● Workgroup: WORKGROUP

Figure 6. **Changing the computer name of the Windows Server installation.**

We have to restart the Windows Server.

4.3.2 Installing the AD Binaries

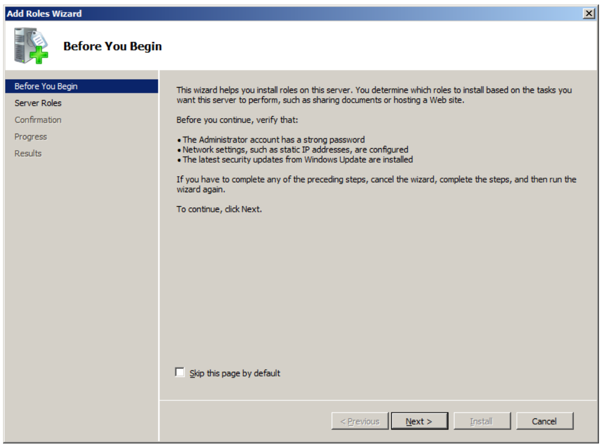
We continue with the installation of the binaries by enabling the server role in the server manager. The installation includes the .Net-Framework. We provide the screens of this process.



View the health of the roles installed c

Roles Summary

Roles: 0 of 17 installed



Before You Begin

This wizard helps you install roles on this server. You determine which roles to install based on the tasks you want this server to perform, such as sharing documents or hosting a Web site.

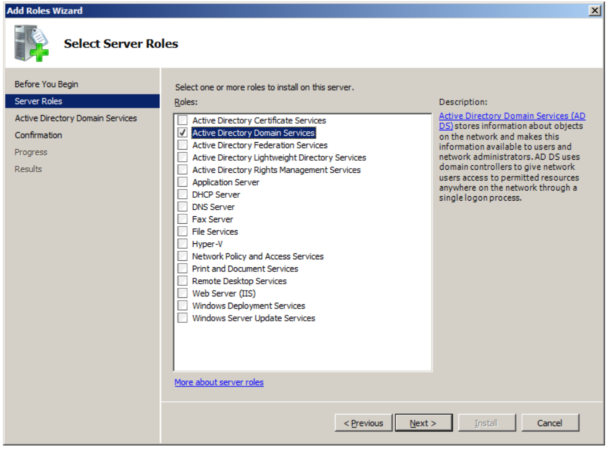
Before you continue, verify that:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The latest security updates from Windows Update are installed

If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

☐ Skip this page by default



Select Server Roles

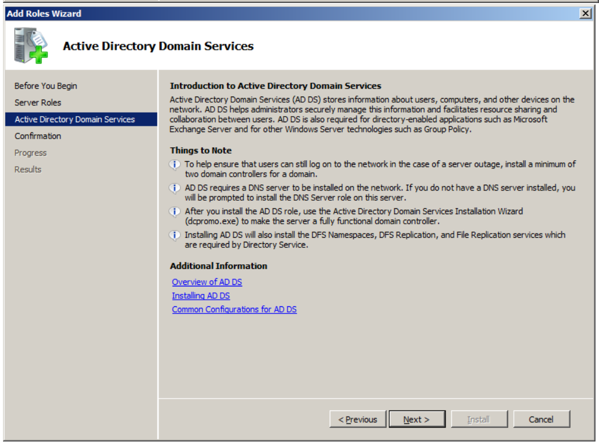
Select one or more roles to install on this server.

Roles:

☐ Active Directory Certificate Services
☑ Active Directory Domain Services
☐ Active Directory Federation Services
☐ Active Directory Lightweight Directory Services
☐ Active Directory Rights Management Services
☐ Application Server
☐ DHCP Server
☐ DNS Server
☐ Fax Server
☐ File Services
☐ Hyper-V
☐ Network Policy and Access Services
☐ Print and Document Services
☐ Remote Desktop Services
☐ Web Server (IIS)
☐ Windows Deployment Services
☐ Windows Server Update Services

Description:

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.



Active Directory Domain Services

Introduction to Active Directory Domain Services

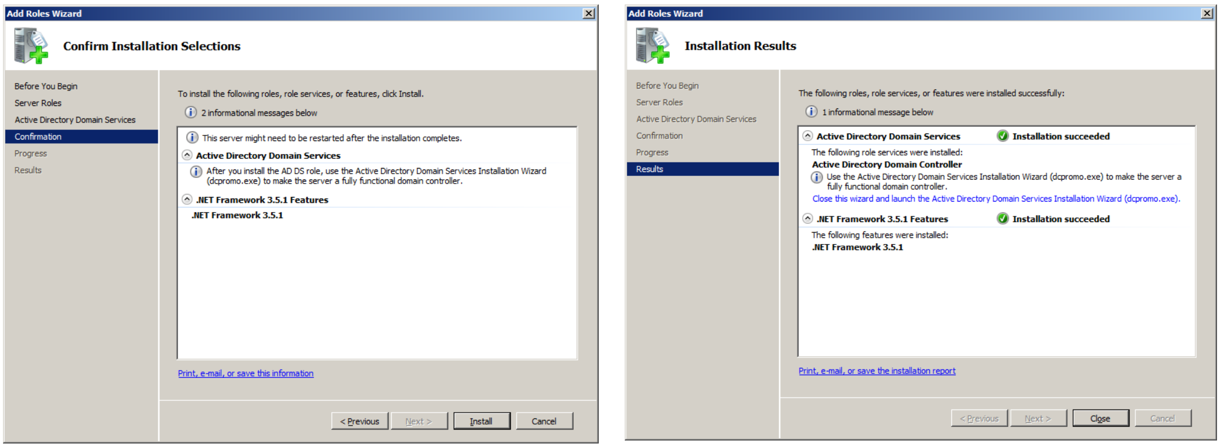
Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users. AD DS is also required for directory-enabled applications such as Microsoft Exchange Server and for other Windows Server technologies such as Group Policy.

Things to Note

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this server.
- After you install the AD DS role, use the Active Directory Domain Services Installation Wizard (dcpromo.exe) to make the server a fully functional domain controller.
- Installing AD DS will also install the DFS Namespaces, DFS Replication, and File Replication services which are required by Directory Service.

Additional Information

Overview of AD DS
Installing AD DS
Common Configurations for AD DS



Confirm Installation Selections

To install the following roles, role services, or features, click Install.

2 informational messages below

This server might need to be restarted after the installation completes.

Active Directory Domain Services

After you install the AD DS role, use the Active Directory Domain Services Installation Wizard (dcpromo.exe) to make the server a fully functional domain controller.

.NET Framework 3.5.1 Features

.NET Framework 3.5.1

Print, e-mail, or save this information

Installation Results

The following roles, role services, or features were installed successfully:

1 informational message below

Active Directory Domain Services — **Installation succeeded**

The following role services were installed:

Active Directory Domain Controller

Use the Active Directory Domain Services Installation Wizard (dcpromo.exe) to make the server a fully functional domain controller.

Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe).

.NET Framework 3.5.1 Features — **Installation succeeded**

The following features were installed:

.NET Framework 3.5.1

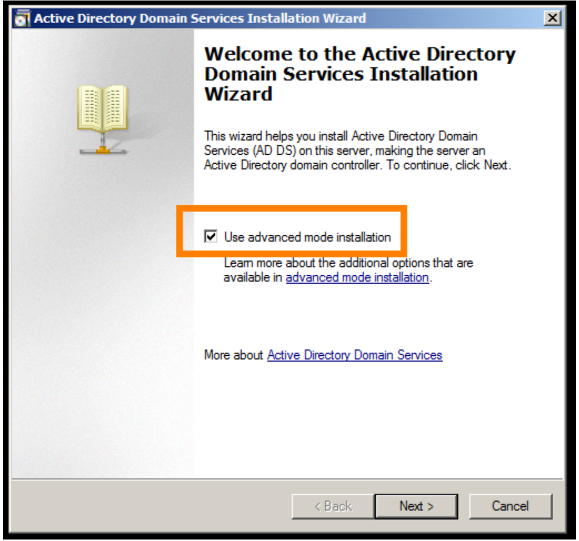
Print, e-mail, or save the installation report

Figure 7. **Installation dialog of the Active Directory binaries.**

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).



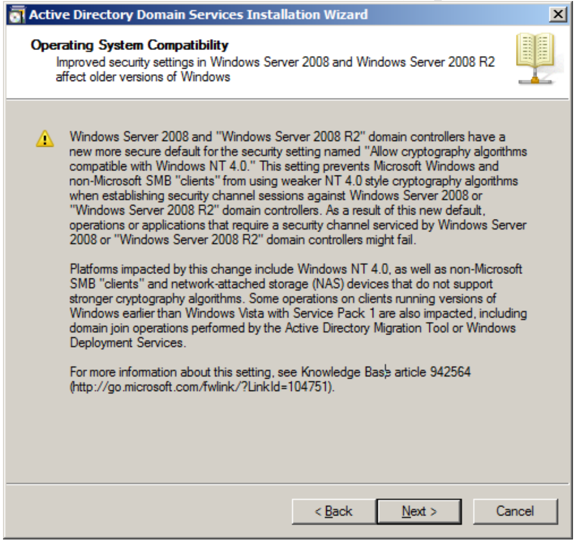
Welcome to the Active Directory Domain Services Installation Wizard

This wizard helps you install Active Directory Domain Services (AD DS) on this server, making the server an Active Directory domain controller. To continue, click Next.

☑ Use advanced mode installation

Learn more about the additional options that are available in advanced mode installation.

More about Active Directory Domain Services



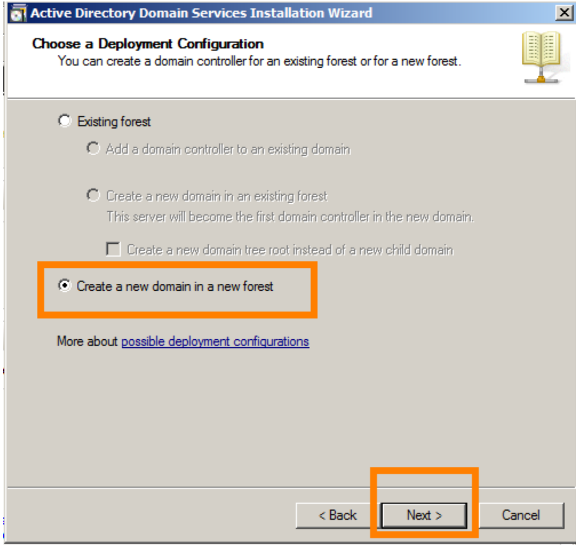
Operating System Compatibility

Improved security settings in Windows Server 2008 and Windows Server 2008 R2 affect older versions of Windows

Windows Server 2008 and "Windows Server 2008 R2" domain controllers have a new more secure default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0." This setting prevents Microsoft Windows and non-Microsoft SMB "clients" from using weaker NT 4.0 style cryptography algorithms when establishing security channel sessions against Windows Server 2008 or "Windows Server 2008 R2" domain controllers. As a result of this new default, operations or applications that require a security channel serviced by Windows Server 2008 or "Windows Server 2008 R2" domain controllers might fail.

Platforms impacted by this change include Windows NT 4.0, as well as non-Microsoft SMB "clients" and network-attached storage (NAS) devices that do not support stronger cryptography algorithms. Some operations on clients running versions of Windows earlier than Windows Vista with Service Pack 1 are also impacted, including domain join operations performed by the Active Directory Migration Tool or Windows Deployment Services.

For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).



Choose a Deployment Configuration

You can create a domain controller for an existing forest or for a new forest.

○ Existing forest

○ Add a domain controller to an existing domain

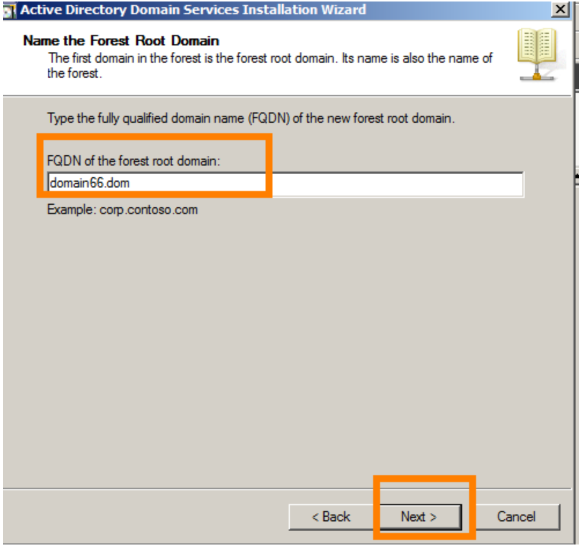
○ Create a new domain in an existing forest

This server will become the first domain controller in the new domain.

□ Create a new domain tree root instead of a new child domain

● Create a new domain in a new forest

More about possible deployment configurations



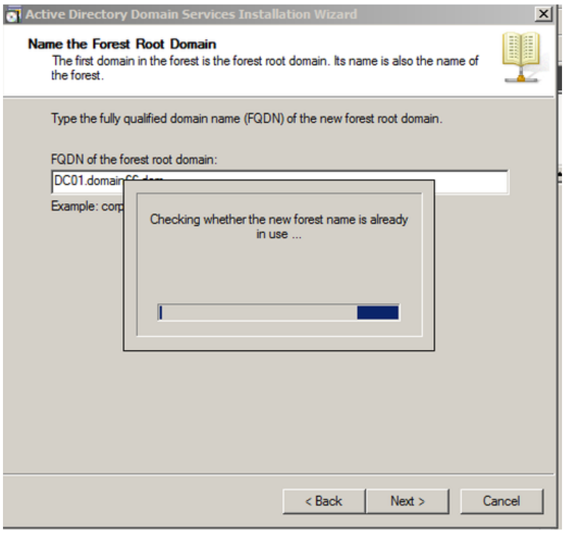
Name the Forest Root Domain

The first domain in the forest is the forest root domain. Its name is also the name of the forest.

Type the fully qualified domain name (FQDN) of the new forest root domain.

FQDN of the forest root domain: domain66.dom

Example: corp.contoso.com



Active Directory Domain Services Installation Wizard

Name the Forest Root Domain

The first domain in the forest is the forest root domain. Its name is also the name of the forest.

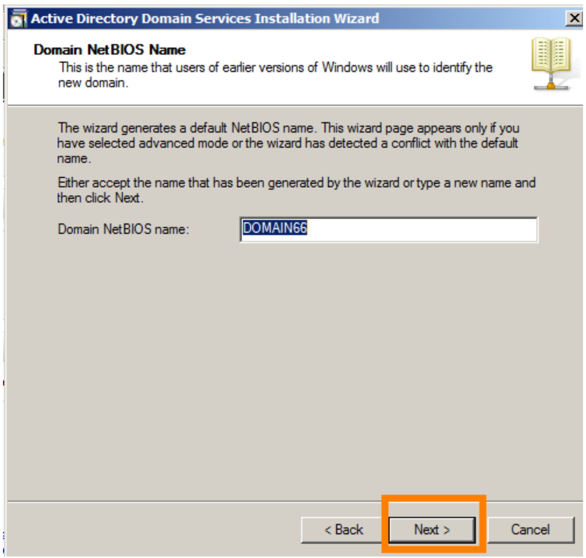
Type the fully qualified domain name (FQDN) of the new forest root domain.

FQDN of the forest root domain: DC01.domain66.dom

Example: corp

Checking whether the new forest name is already in use ...

This may take some mintutes.



Active Directory Domain Services Installation Wizard

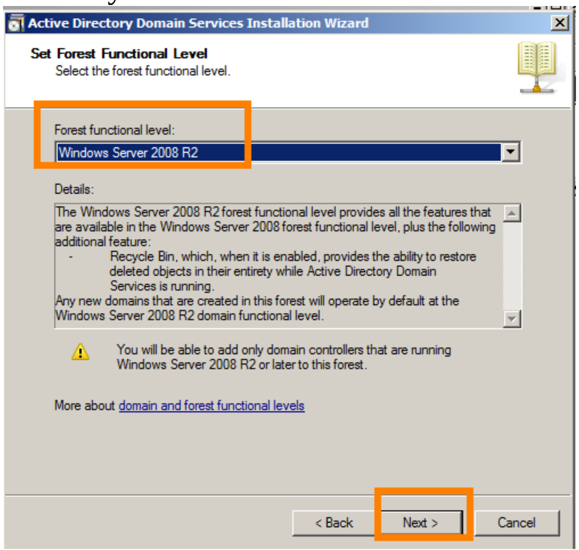
Domain NetBIOS Name

This is the name that users of earlier versions of Windows will use to identify the new domain.

The wizard generates a default NetBIOS name. This wizard page appears only if you have selected advanced mode or the wizard has detected a conflict with the default name.

Either accept the name that has been generated by the wizard or type a new name and then click Next.

Domain NetBIOS name: DOMAIN66



Active Directory Domain Services Installation Wizard

Set Forest Functional Level

Select the forest functional level.

Forest functional level: Windows Server 2008 R2

Details:

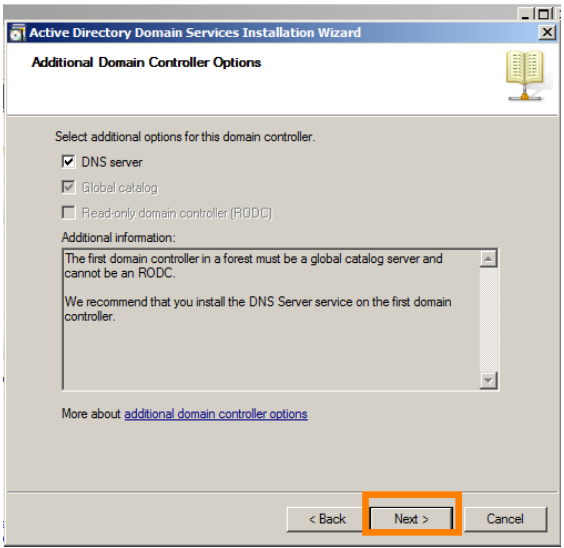
The Windows Server 2008 R2 forest functional level provides all the features that are available in the Windows Server 2008 forest functional level, plus the following additional feature:

- Recycle Bin, which, when it is enabled, provides the ability to restore deleted objects in their entirety while Active Directory Domain Services is running.

Any new domains that are created in this forest will operate by default at the Windows Server 2008 R2 domain functional level.

⚠ You will be able to add only domain controllers that are running Windows Server 2008 R2 or later to this forest.

More about domain and forest functional levels



Active Directory Domain Services Installation Wizard

Additional Domain Controller Options

Select additional options for this domain controller.

☑ DNS server

☑ Global catalog

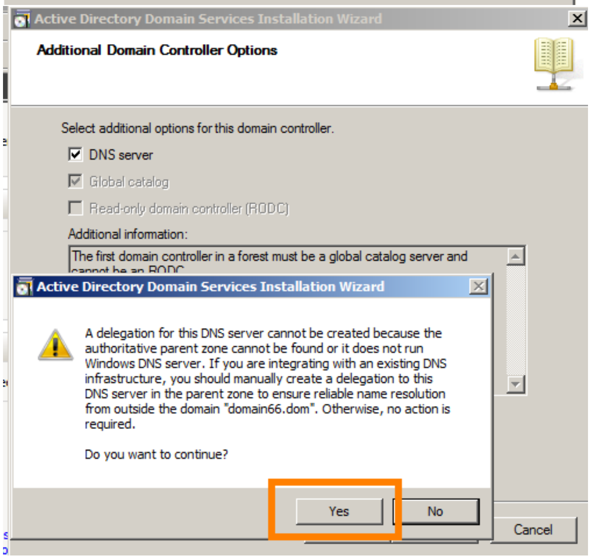
☐ Read-only domain controller (RODC)

Additional information:

The first domain controller in a forest must be a global catalog server and cannot be an RODC.

We recommend that you install the DNS Server service on the first domain controller.

More about additional domain controller options



Active Directory Domain Services Installation Wizard

Additional Domain Controller Options

Select additional options for this domain controller.

☑ DNS server

☑ Global catalog

☐ Read-only domain controller (RODC)

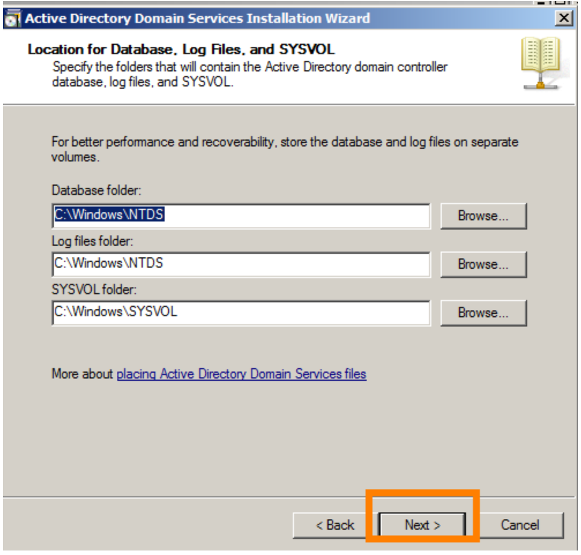
Additional information:

The first domain controller in a forest must be a global catalog server and cannot be an RODC.

Active Directory Domain Services Installation Wizard

⚠ A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "domain66.dom". Otherwise, no action is required.

Do you want to continue?



Active Directory Domain Services Installation Wizard

Location for Database, Log Files, and SYSVOL

Specify the folders that will contain the Active Directory domain controller database, log files, and SYSVOL.

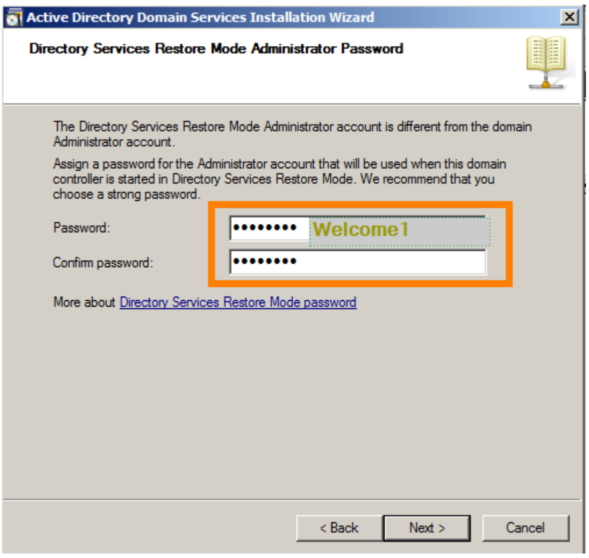
For better performance and recoverability, store the database and log files on separate volumes.

Database folder: C:\Windows\NTDS

Log files folder: C:\Windows\NTDS

SYSVOL folder: C:\Windows\SYSVOL

More about placing Active Directory Domain Services files


Active Directory Domain Services Installation Wizard

Directory Services Restore Mode Administrator Password

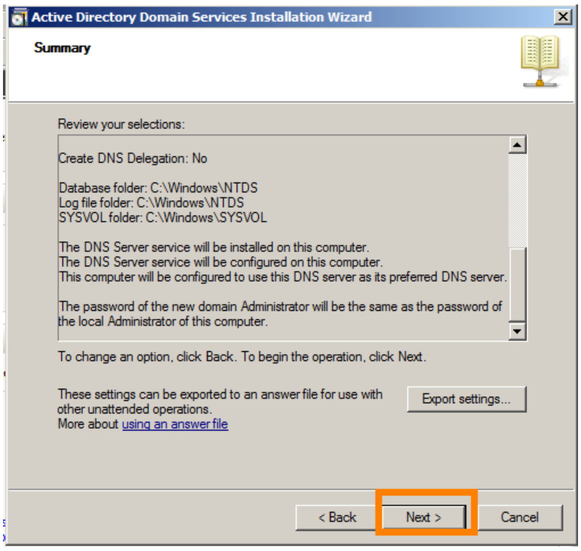
The Directory Services Restore Mode Administrator account is different from the domain Administrator account.

Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password.

Password: •••••••• Welcome1

Confirm password: ••••••••

More about Directory Services Restore Mode password


Active Directory Domain Services Installation Wizard

Summary

Review your selections:

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.

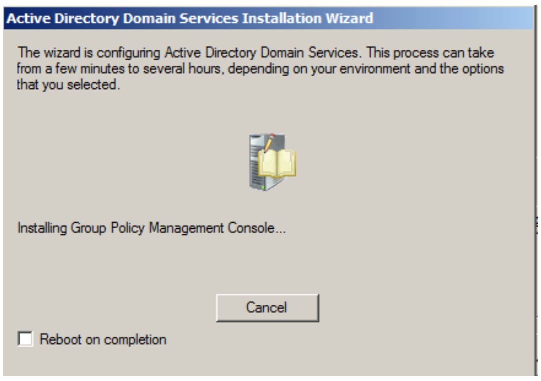
The password of the new domain Administrator will be the same as the password of the local Administrator of this computer.

To change an option, click Back. To begin the operation, click Next.

These settings can be exported to an answer file for use with other unattended operations.
More about using an answer file

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.
```

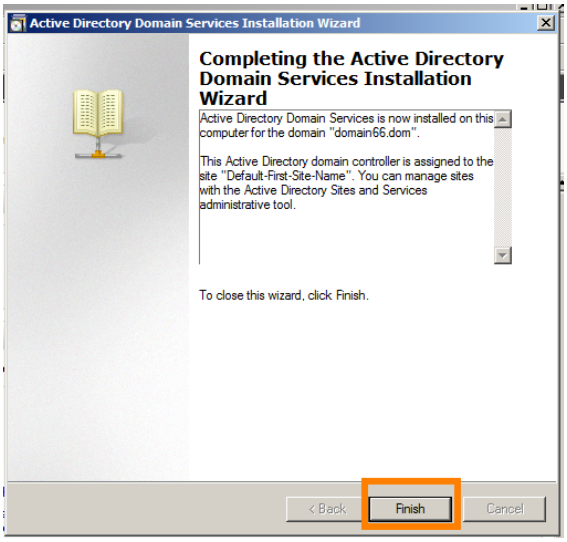

Active Directory Domain Services Installation Wizard

The wizard is configuring Active Directory Domain Services. This process can take from a few minutes to several hours, depending on your environment and the options that you selected.

Installing Group Policy Management Console...

□ Reboot on completion

This takes some mintues…

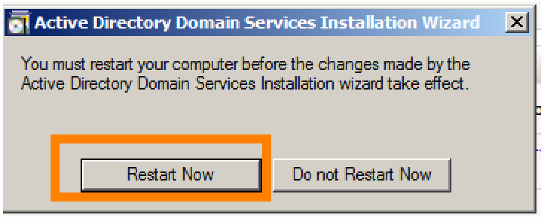

Active Directory Domain Services Installation Wizard

Completing the Active Directory Domain Services Installation Wizard

Active Directory Domain Services is now installed on this computer for the domain "domain66.dom".

This Active Directory domain controller is assigned to the site "Default-First-Site-Name". You can manage sites with the Active Directory Sites and Services administrative tool.

To close this wizard, click Finish.


Active Directory Domain Services Installation Wizard

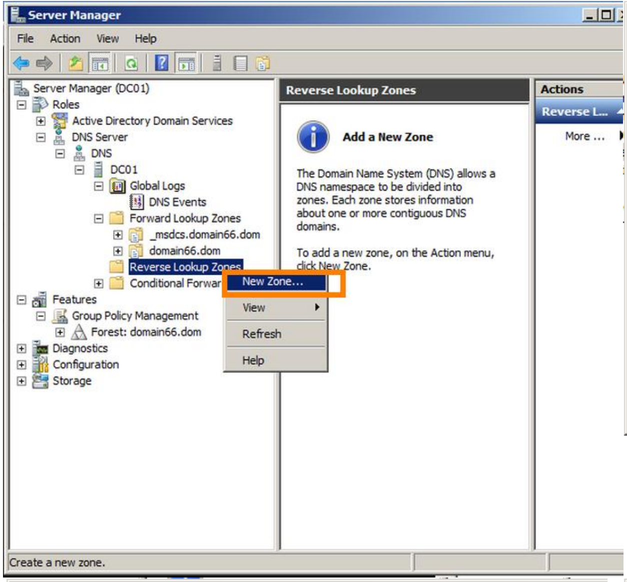
You must restart your computer before the changes made by the Active Directory Domain Services Installation wizard take effect.

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.

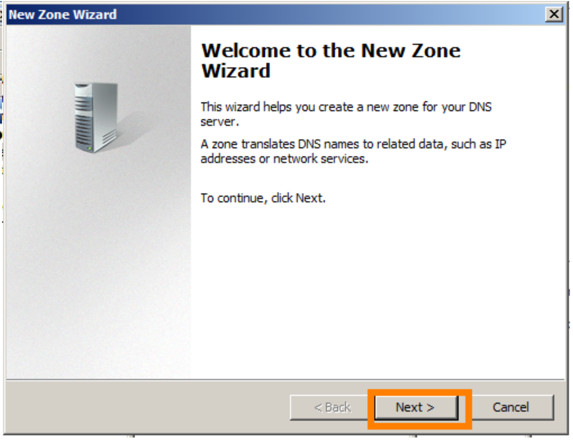


Add a New Zone

The Domain Name System (DNS) allows a DNS namespace to be divided into zones. Each zone stores information about one or more contiguous DNS domains.

To add a new zone, on the Action menu, click New Zone.

Create a new zone.

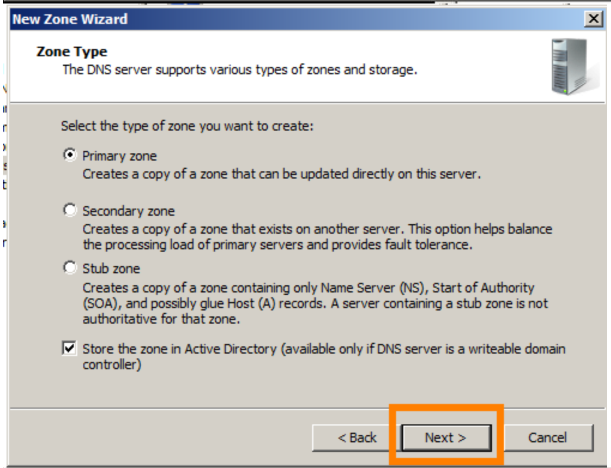


Welcome to the New Zone Wizard

This wizard helps you create a new zone for your DNS server.

A zone translates DNS names to related data, such as IP addresses or network services.

To continue, click Next.



Zone Type

The DNS server supports various types of zones and storage.

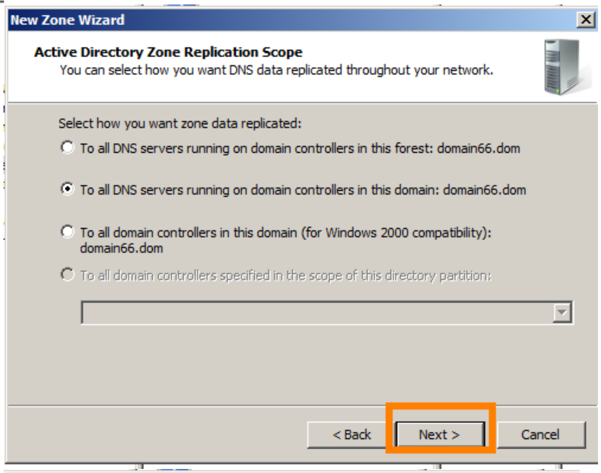
Select the type of zone you want to create:

● Primary zone
Creates a copy of a zone that can be updated directly on this server.

○ Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.

○ Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

☑ Store the zone in Active Directory (available only if DNS server is a writeable domain controller)



Active Directory Zone Replication Scope

You can select how you want DNS data replicated throughout your network.

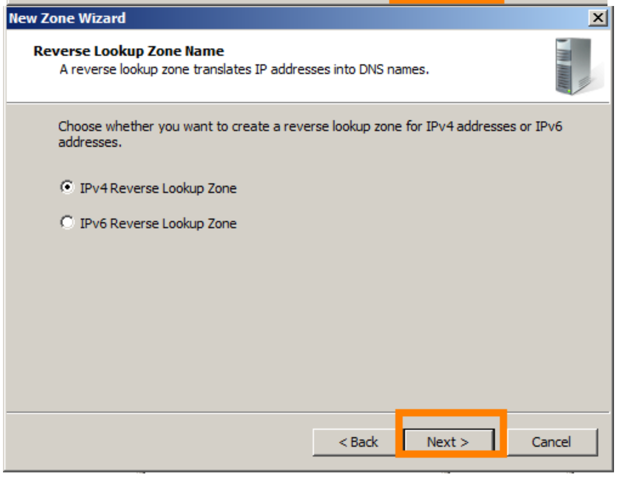
Select how you want zone data replicated:

○ To all DNS servers running on domain controllers in this forest: domain66.dom

● To all DNS servers running on domain controllers in this domain: domain66.dom

○ To all domain controllers in this domain (for Windows 2000 compatibility): domain66.dom

○ To all domain controllers specified in the scope of this directory partition:



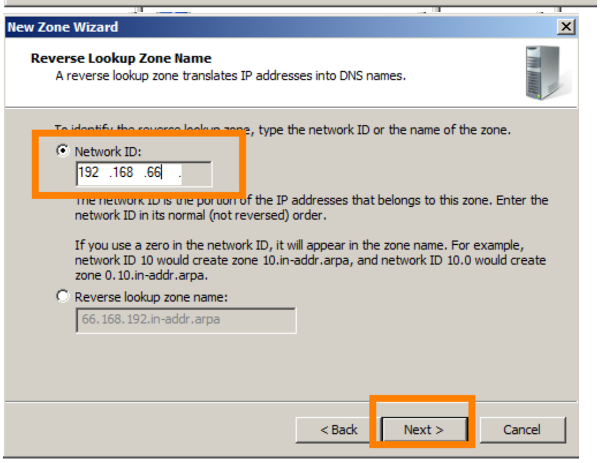
Reverse Lookup Zone Name

A reverse lookup zone translates IP addresses into DNS names.

Choose whether you want to create a reverse lookup zone for IPv4 addresses or IPv6 addresses.

● IPv4 Reverse Lookup Zone

○ IPv6 Reverse Lookup Zone



Reverse Lookup Zone Name

A reverse lookup zone translates IP addresses into DNS names.

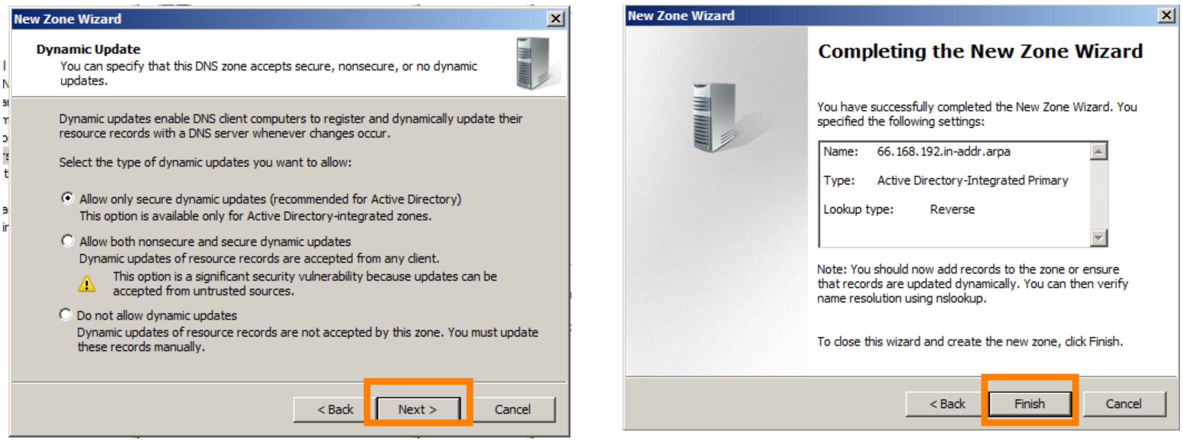
To identify the reverse lookup zone, type the network ID or the name of the zone.

● Network ID:
192 .168 .66 .

The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

○ Reverse lookup zone name:
66.168.192.in-addr.arpa



New Zone Wizard

Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

● Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.

○ Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
This option is a significant security vulnerability because updates can be accepted from untrusted sources.

○ Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

New Zone Wizard

Completing the New Zone Wizard

You have successfully completed the New Zone Wizard. You specified the following settings:

Name: 66.168.192.in-addr.arpa
Type: Active Directory-Integrated Primary
Lookup type: Reverse

Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.

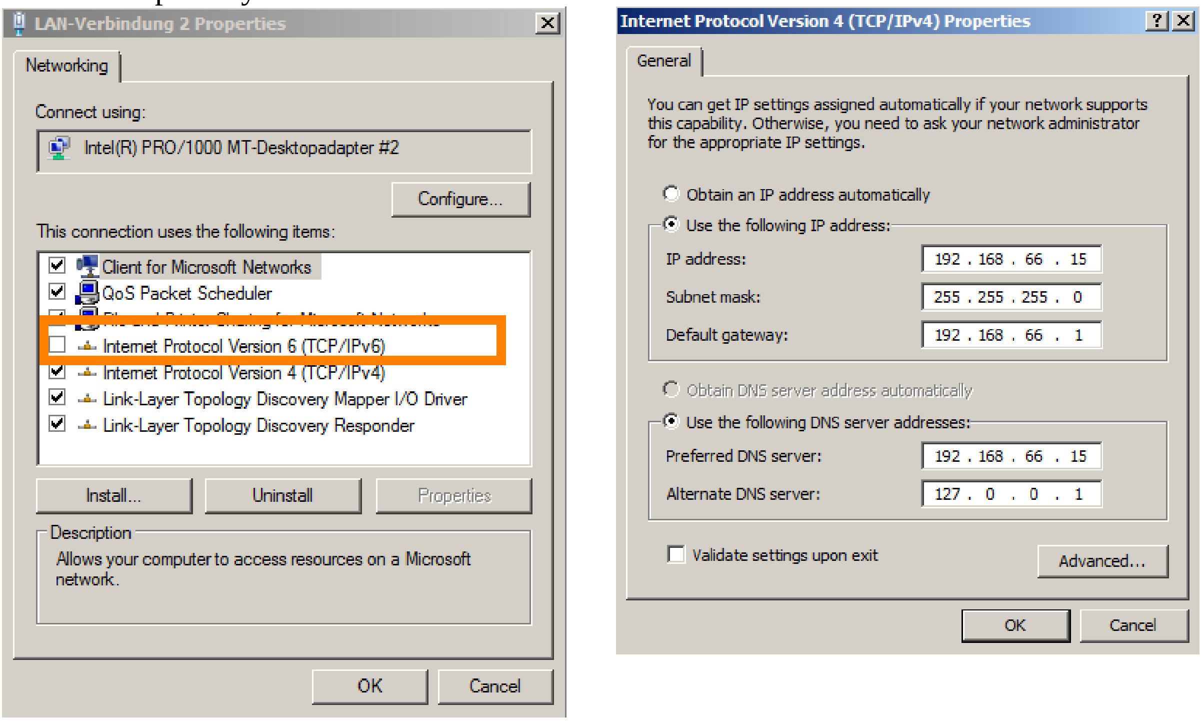
To close this wizard and create the new zone, click Finish.

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.



LAN-Verbindung 2 Properties

Connect using:
Intel(R) PRO/1000 MT-Desktopadapter #2

This connection uses the following items:

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☐ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description
Allows your computer to access resources on a Microsoft network.

Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 66 . 15
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 66 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 66 . 15
Alternate DNS server: 127 . 0 . 0 . 1

☐ Validate settings upon exit

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

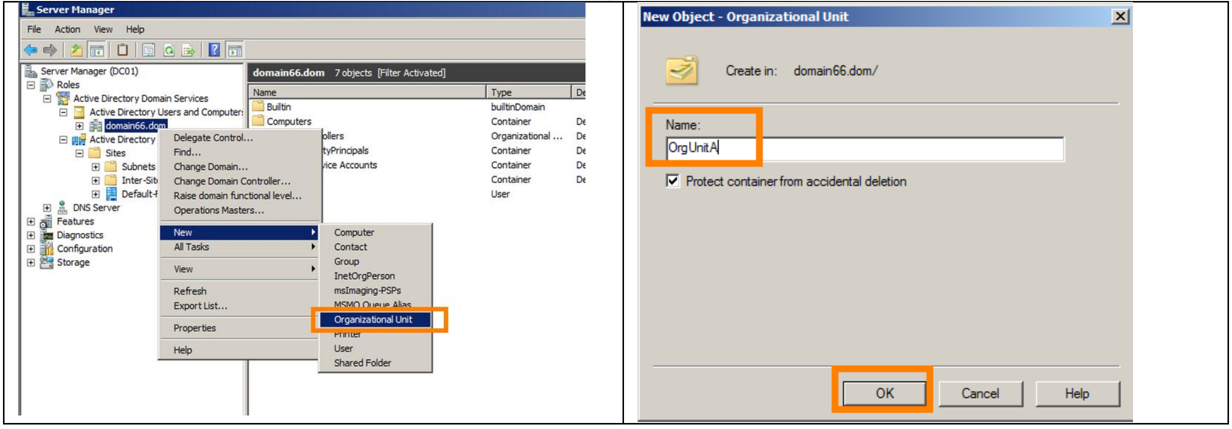
Now the DNS lookup works properly and fast.

```
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 domain66

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.



New Object - Organizational Unit

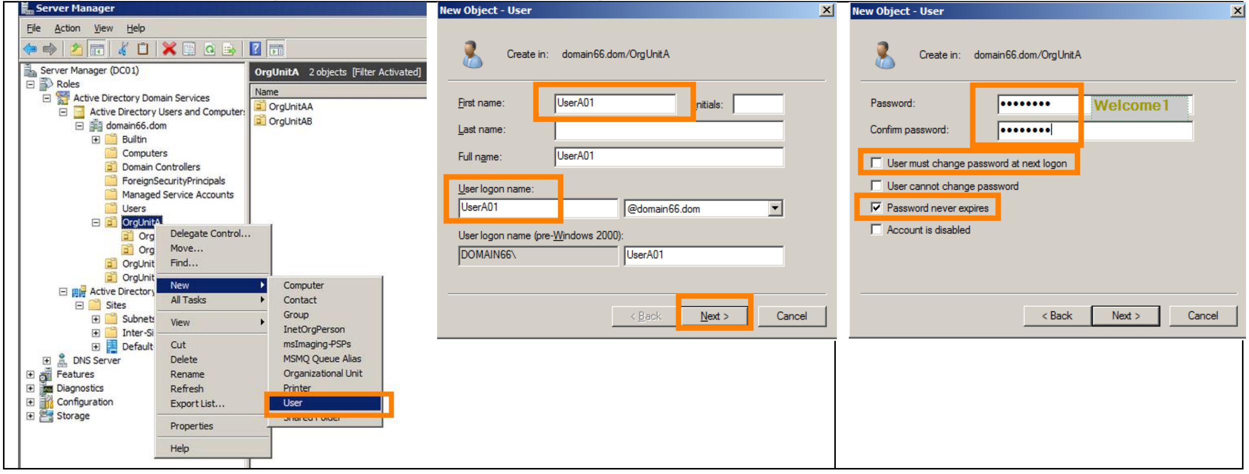
Create in: domain66.dom/

Name: OrgUnitA

☑ Protect container from accidental deletion

Figure 11. **Creating OrgUnitA in the Active Directory.**

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.



New Object - User

Create in: domain66.dom/OrgUnitA

First name: UserA01

Last name:

Full name: UserA01

User logon name: UserA01 @domain66.dom

User logon name (pre-Windows 2000): DOMAIN66\ UserA01

New Object - User

Create in: domain66.dom/OrgUnitA

Password: ••••••••

Confirm password: ••••••••

Welcome1

□ User must change password at next logon

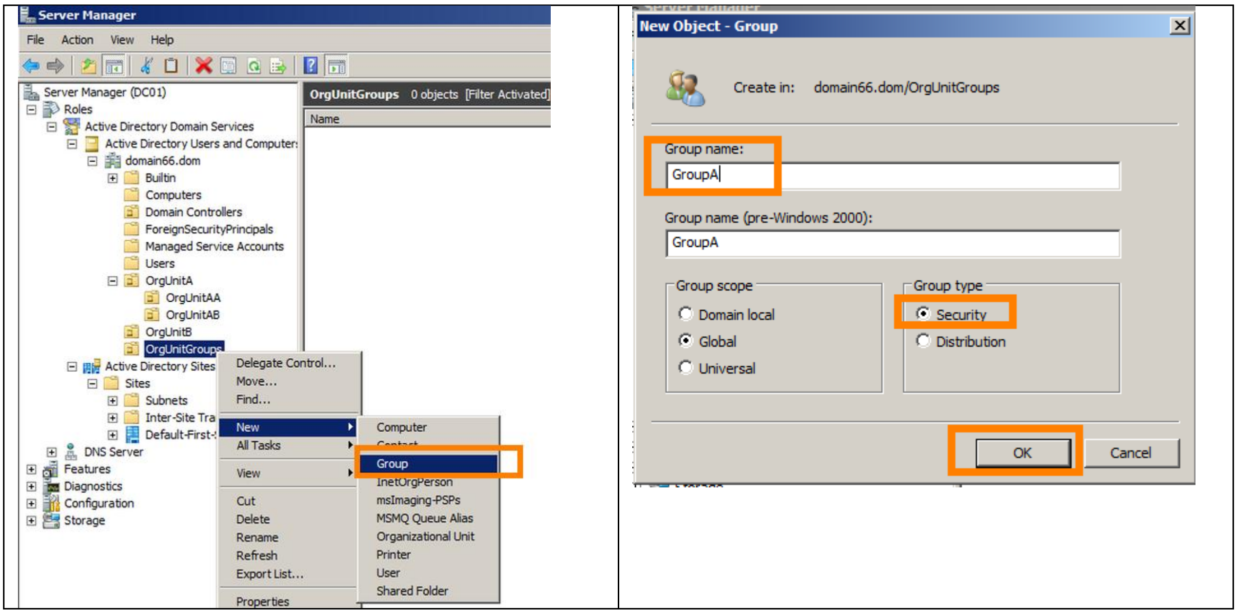
□ User cannot change password

☑ Password never expires

□ Account is disabled

Figure 12. **Creating UserA01 in the Active Directory.**

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.



New Object - Group

Create in: domain66.dom/OrgUnitGroups

Group name: GroupA

Group name (pre-Windows 2000): GroupA

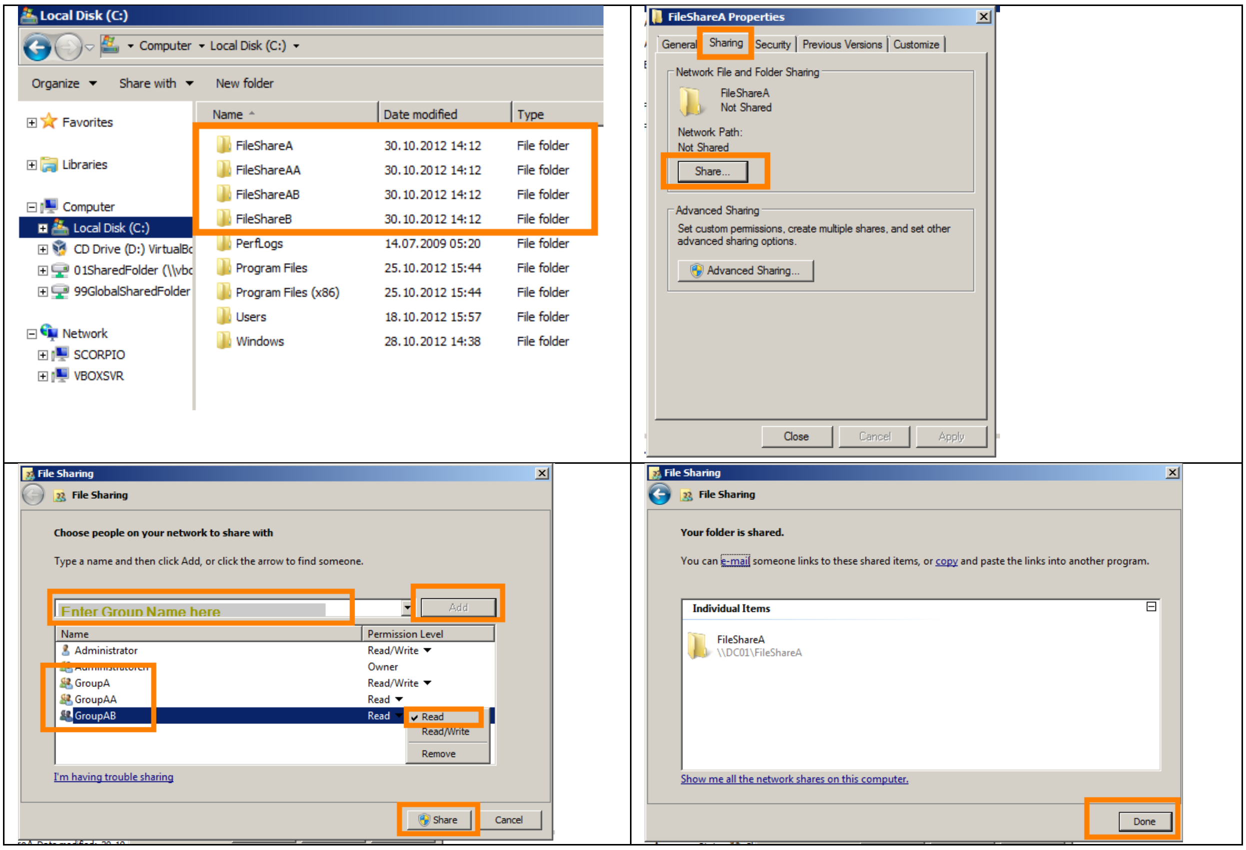
Group scope: ○ Domain local ● Global ○ Universal

Group type: ● Security ○ Distribution

Figure 13. **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.



Name	Date modified	Type
FileShareA	30.10.2012 14:12	File folder
FileShareAA	30.10.2012 14:12	File folder
FileShareAB	30.10.2012 14:12	File folder
FileShareB	30.10.2012 14:12	File folder
PerfLogs	14.07.2009 05:20	File folder
Program Files	25.10.2012 15:44	File folder
Program Files (x86)	25.10.2012 15:44	File folder
Users	18.10.2012 15:57	File folder
Windows	28.10.2012 14:38	File folder

Network File and Folder Sharing
FileShareA
Not Shared
Network Path:
Not Shared

Advanced Sharing
Set custom permissions, create multiple shares, and set other advanced sharing options.

Choose people on your network to share with

Type a name and then click Add, or click the arrow to find someone.

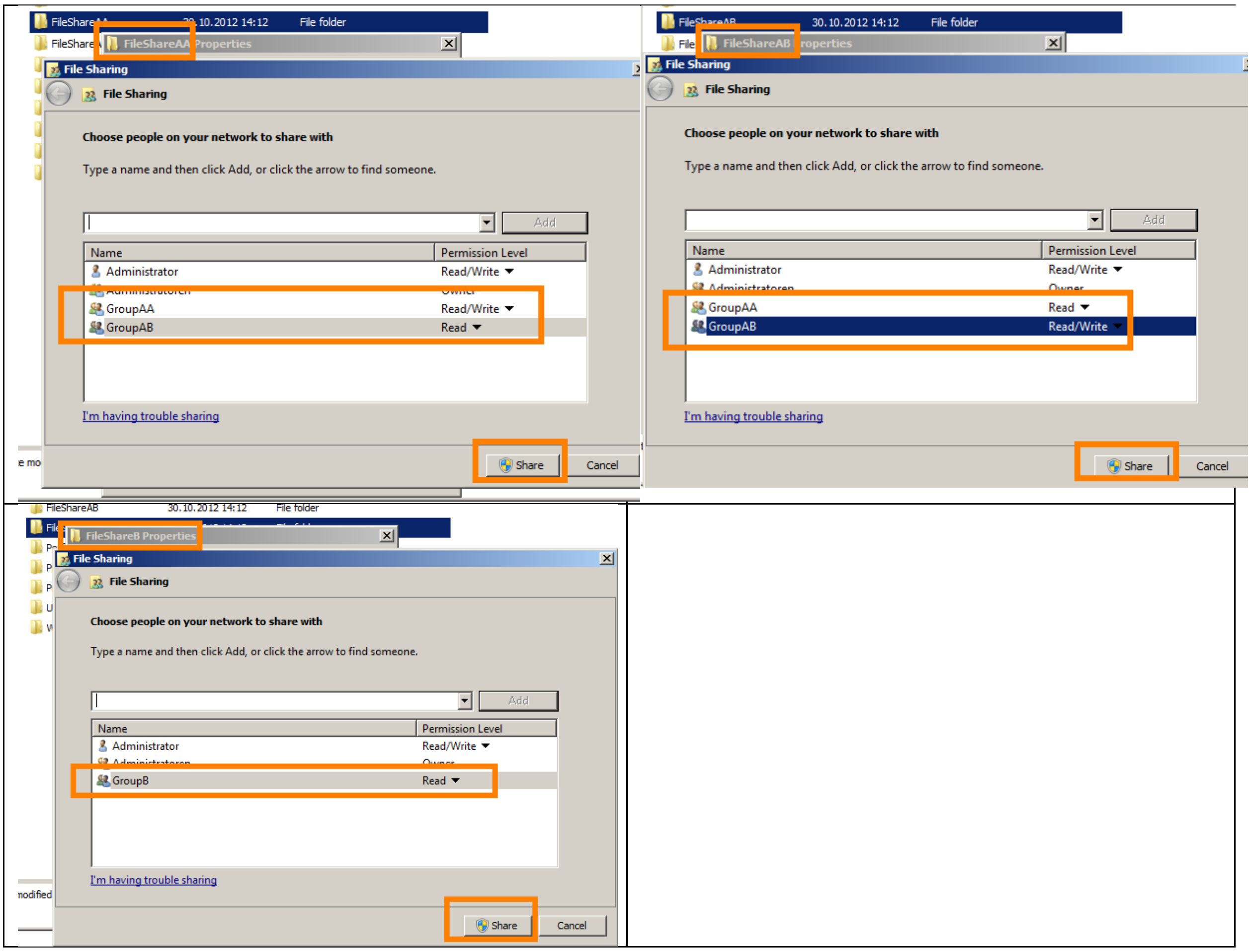
Enter Group Name here

Name	Permission Level
Administrator	Read/Write
Administrators	Owner
GroupA	Read/Write
GroupAA	Read
GroupAB	Read

Your folder is shared.

You can e-mail someone links to these shared items, or copy and paste the links into another program.

Individual Items
FileShareA
\\DC01\FileShareA



FileShareAA Properties

File Sharing

Choose people on your network to share with

Type a name and then click Add, or click the arrow to find someone.

Name	Permission Level
Administrator	Read/Write
Administratoren	Owner
GroupAA	Read/Write
GroupAB	Read

I'm having trouble sharing

FileShareAB Properties

File Sharing

Choose people on your network to share with

Type a name and then click Add, or click the arrow to find someone.

Name	Permission Level
Administrator	Read/Write
Administratoren	Owner
GroupAA	Read
GroupAB	Read/Write

I'm having trouble sharing

FileShareB Properties

File Sharing

Choose people on your network to share with

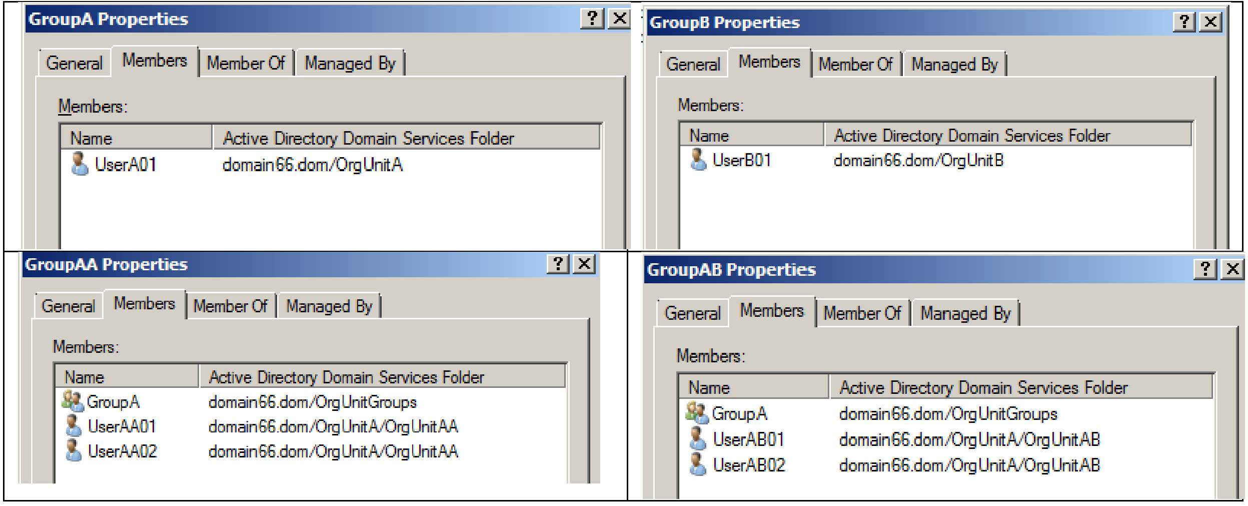
Type a name and then click Add, or click the arrow to find someone.

Name	Permission Level
Administrator	Read/Write
Administratoren	Owner
GroupB	Read

I'm having trouble sharing

Figure 14. **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.



GroupA Properties

Members:

Name	Active Directory Domain Services Folder
UserA01	domain66.dom/OrgUnitA

GroupB Properties

Members:

Name	Active Directory Domain Services Folder
UserB01	domain66.dom/OrgUnitB

GroupAA Properties

Members:

Name	Active Directory Domain Services Folder
GroupA	domain66.dom/OrgUnitGroups
UserAA01	domain66.dom/OrgUnitA/OrgUnitAA
UserAA02	domain66.dom/OrgUnitA/OrgUnitAA

GroupAB Properties

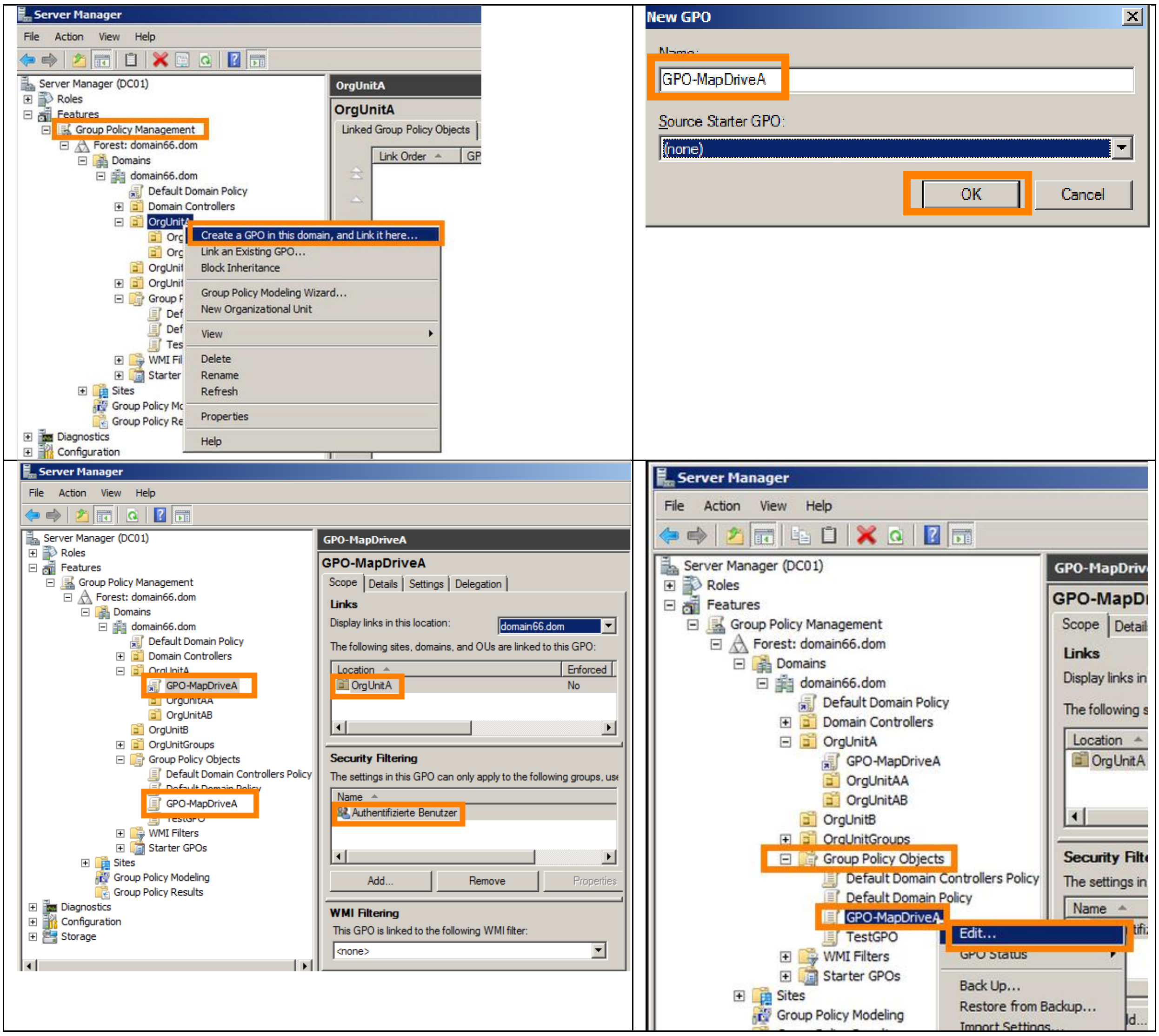
Members:

Name	Active Directory Domain Services Folder
GroupA	domain66.dom/OrgUnitGroups
UserAB01	domain66.dom/OrgUnitA/OrgUnitAB
UserAB02	domain66.dom/OrgUnitA/OrgUnitAB

Figure 15. **Configuring Group Membership in the Active Directory.**

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.



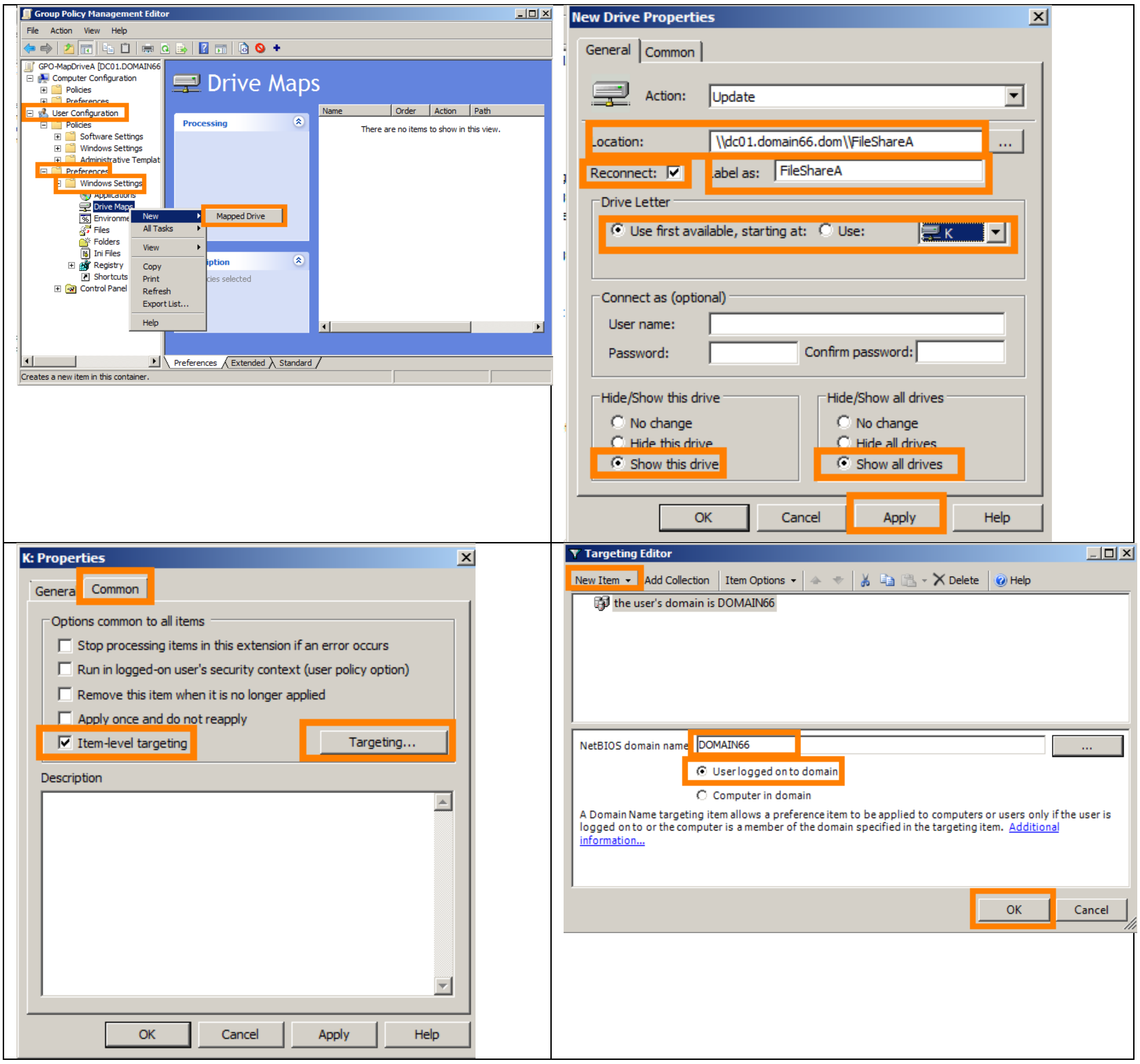
New GPO

Name: GPO-MapDriveA

Source Starter GPO: (none)

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

In the Group Policy Management Editor, we navigate to “User Configuration->Preferences->Windwos 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.



There are no items to show in this view.

Creates a new item in this container.

New Drive Properties — General | Common

Action: Update

Location: \\dc01.domain66.dom\FileShareA

Reconnect: ☑ Label as: FileShareA

Drive Letter: ● Use first available, starting at: ○ Use: K

Connect as (optional): User name: Password: Confirm password:

Hide/Show this drive: ○ No change ○ Hide this drive ● Show this drive

Hide/Show all drives: ○ No change ○ Hide all drives ● Show all drives

OK | Cancel | Apply | Help

K: Properties — General | Common

Options common to all items

- □ Stop processing items in this extension if an error occurs
- □ Run in logged-on user's security context (user policy option)
- □ Remove this item when it is no longer applied
- □ Apply once and do not reapply
- ☑ Item-level targeting — Targeting...

Description

OK | Cancel | Apply | Help

Targeting Editor — New Item | Add Collection | Item Options | Delete | Help

the user's domain is DOMAIN66

NetBIOS domain name: DOMAIN66

● User logged on to domain
○ Computer in domain

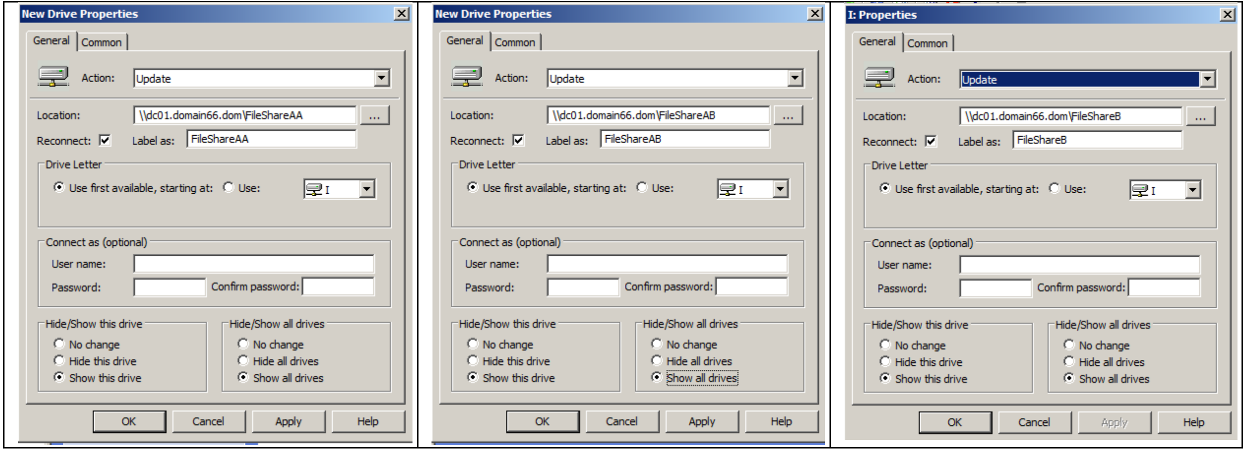
A Domain Name targeting item allows a preference item to be applied to computers or users only if the user is logged on to or the computer is a member of the domain specified in the targeting item. Additional information...

OK | Cancel

Figure 17. **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 users 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.



New Drive Properties — General | Common

Action: Update

Location: \\dc01.domain66.dom\FileShareAA

Reconnect: ☑ Label as: FileShareAA

Drive Letter: ● Use first available, starting at: ○ Use: I

Connect as (optional): User name: Password: Confirm password:

Hide/Show this drive: ○ No change ○ Hide this drive ● Show this drive

Hide/Show all drives: ○ No change ○ Hide all drives ● Show all drives

OK | Cancel | Apply | Help

New Drive Properties — General | Common

Action: Update

Location: \\dc01.domain66.dom\FileShareAB

Reconnect: ☑ Label as: FileShareAB

Drive Letter: ● Use first available, starting at: ○ Use: I

Connect as (optional): User name: Password: Confirm password:

Hide/Show this drive: ○ No change ○ Hide this drive ● Show this drive

Hide/Show all drives: ○ No change ○ Hide all drives ● Show all drives

OK | Cancel | Apply | Help

I: Properties — General | Common

Action: Update

Location: \\dc01.domain66.dom\FileShareB

Reconnect: ☑ Label as: FileShareB

Drive Letter: ● Use first available, starting at: ○ Use: I

Connect as (optional): User name: Password: Confirm password:

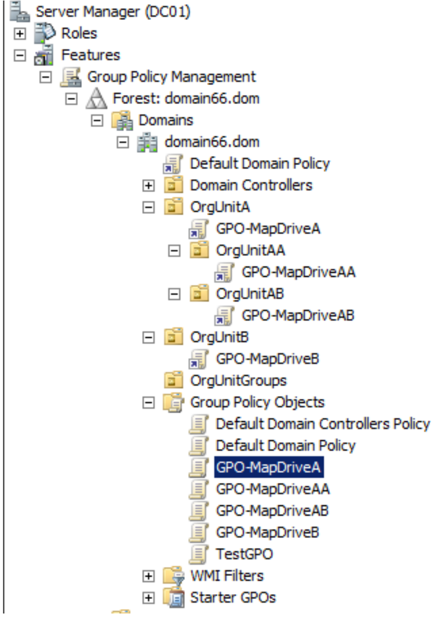
Hide/Show this drive: ○ No change ○ Hide this drive ● Show this drive

Hide/Show all drives: ○ No change ○ Hide all drives ● Show all drives

OK | Cancel | Apply | Help

Figure 18. **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 (DC01)
⊞ Roles
⊟ Features
  ⊟ Group Policy Management
    ⊟ Forest: domain66.dom
      ⊟ Domains
        ⊟ domain66.dom
            Default Domain Policy
          ⊞ Domain Controllers
          ⊟ OrgUnitA
              GPO-MapDriveA
            ⊟ OrgUnitAA
                GPO-MapDriveAA
            ⊟ OrgUnitAB
                GPO-MapDriveAB
          ⊟ OrgUnitB
              GPO-MapDriveB
            OrgUnitGroups
          ⊟ Group Policy Objects
              Default Domain Controllers Policy
              Default Domain Policy
              GPO-MapDriveA
              GPO-MapDriveAA
              GPO-MapDriveAB
              GPO-MapDriveB
              TestGPO
          ⊞ WMI Filters
          ⊞ Starter GPOs
```

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

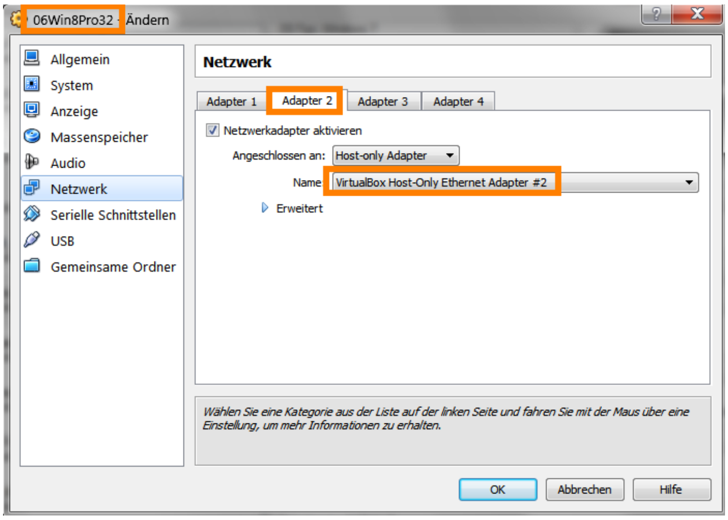
The company domain66 is now setup. When a user logs into the domain from a client machine she gets a drive mappings and access rights on these mappings according to her organizational unit.

Provisioning a new user account would include creating a user in the choosen 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.



06Win8Pro32 - Ändern

Netzwerk

☑ Netzwerkadapter aktivieren

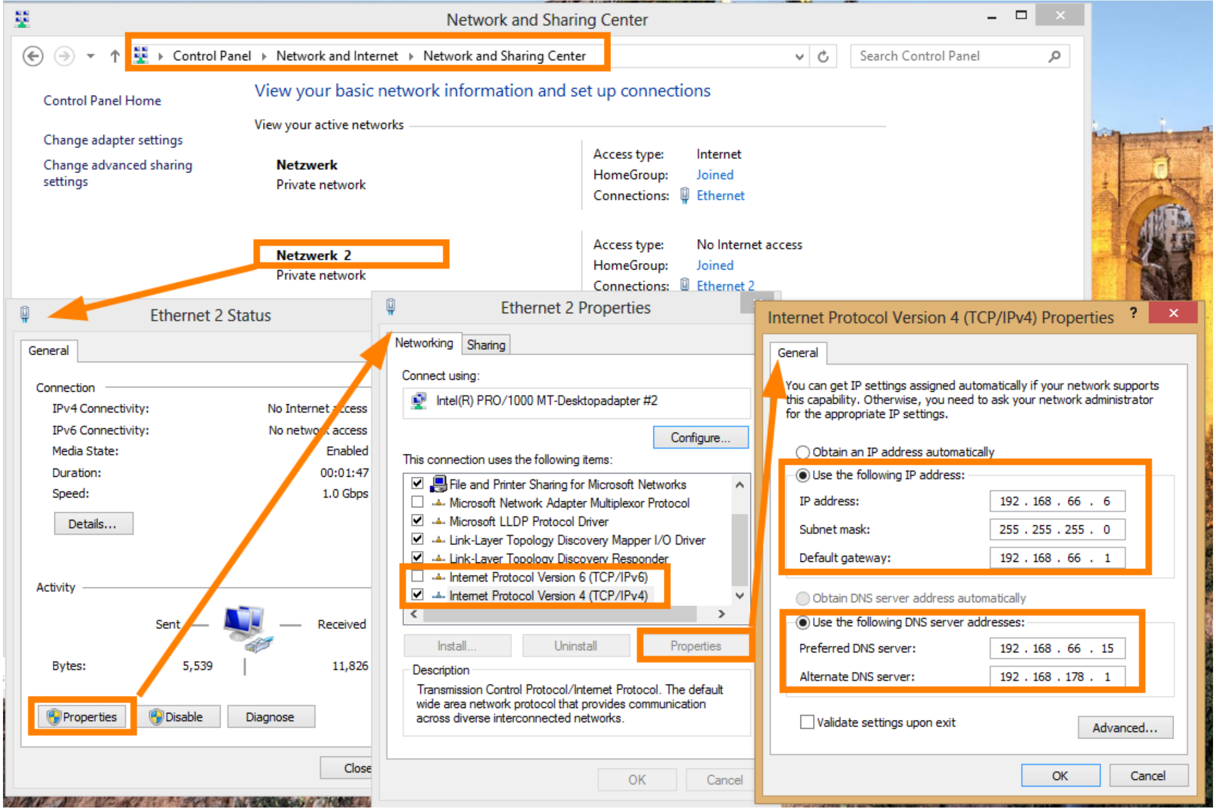
Angeschlossen an: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter #2

Wählen Sie eine Kategorie aus der Liste auf der linken Seite und fahren Sie mit der Maus über eine Einstellung, um mehr Informationen zu erhalten.

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 fix 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 theses settings.



Network and Sharing Center

Control Panel › Network and Internet › Network and Sharing Center

View your basic network information and set up connections

View your active networks

Netzwerk
Private network
Access type: Internet
HomeGroup: Joined
Connections: Ethernet

Netzwerk 2
Private network
Access type: No Internet access
HomeGroup: Joined
Connections: Ethernet 2

Ethernet 2 Status

Connection
IPv4 Connectivity: No Internet access
IPv6 Connectivity: No network access
Media State: Enabled
Duration: 00:01:47
Speed: 1.0 Gbps

Activity
Bytes: Sent 5,539 Received 11,826

Ethernet 2 Properties

Connect using: Intel(R) PRO/1000 MT-Desktopadapter #2

This connection uses the following items:
☑ File and Printer Sharing for Microsoft Networks
□ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder
□ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

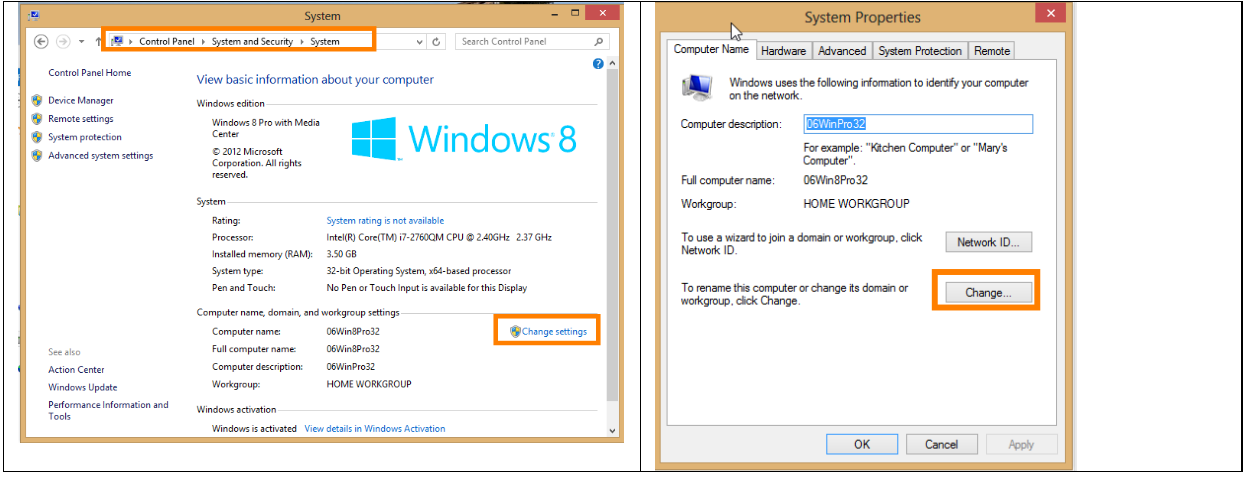
○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 66 . 6
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 66 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 66 . 15
Alternate DNS server: 192 . 168 . 178 . 1

□ Validate settings upon exit

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.



System

Control Panel › System and Security › System

View basic information about your computer

Windows edition
Windows 8 Pro with Media Center
© 2012 Microsoft Corporation. All rights reserved.

System
Rating: System rating is not available
Processor: Intel(R) Core(TM) i7-2760QM CPU @ 2.40GHz 2.37 GHz
Installed memory (RAM): 3.50 GB
System type: 32-bit Operating System, x64-based processor
Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings
Computer name: 06Win8Pro32
Full computer name: 06Win8Pro32
Computer description: 06WinPro32
Workgroup: HOME WORKGROUP

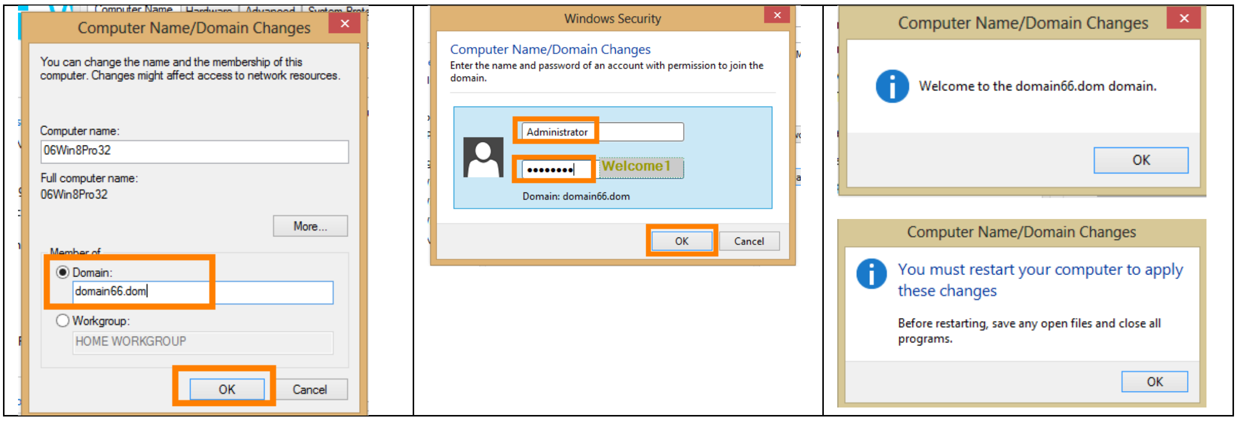
Windows activation
Windows is activated View details in Windows Activation

System Properties

Windows uses the following information to identify your computer on the network.
Computer description: 06WinPro32
For example: "Kitchen Computer" or "Mary's Computer".
Full computer name: 06Win8Pro32
Workgroup: HOME WORKGROUP
To use a wizard to join a domain or workgroup, click Network ID.
To rename this computer or change its domain or workgroup, click Change.

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.



Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: 06Win8Pro32

Full computer name: 06Win8Pro32

Member of

● Domain: domain66.dom

○ Workgroup: HOME WORKGROUP

Windows Security

Computer Name/Domain Changes

Enter the name and password of an account with permission to join the domain.

Administrator

•••••••• Welcome1

Domain: domain66.dom

Computer Name/Domain Changes

Welcome to the domain66.dom domain.

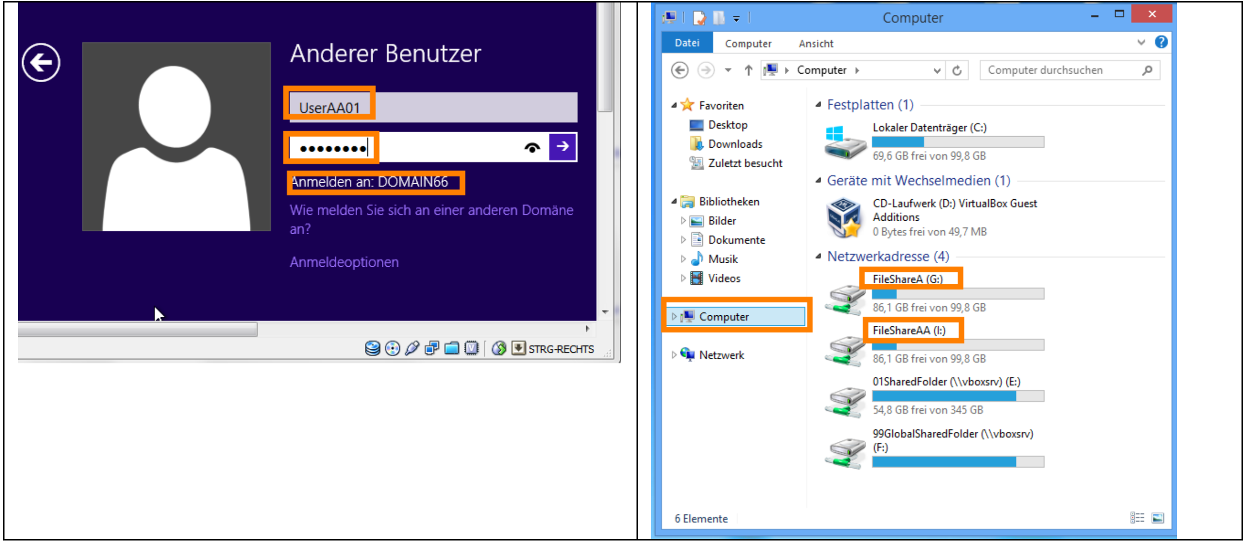
Computer Name/Domain Changes

You must restart your computer to apply these changes

Before restarting, save any open files and close all programs.

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.



Anderer Benutzer

UserAA01

••••••••

Anmelden an: DOMAIN66

Wie melden Sie sich an einer anderen Domäne an?

Anmeldeoptionen

Computer

Festplatten (1)

Lokaler Datenträger (C:) 69,6 GB frei von 99,8 GB

Geräte mit Wechselmedien (1)

CD-Laufwerk (D:) VirtualBox Guest Additions 0 Bytes frei von 49,7 MB

Netzwerkadresse (4)

FileShareA (G:) 86,1 GB frei von 99,8 GB

FileShareAA (I:) 86,1 GB frei von 99,8 GB

01SharedFolder (\\vboxsrv) (E:) 54,8 GB frei von 345 GB

99GlobalSharedFolder (\\vboxsrv) (F:)

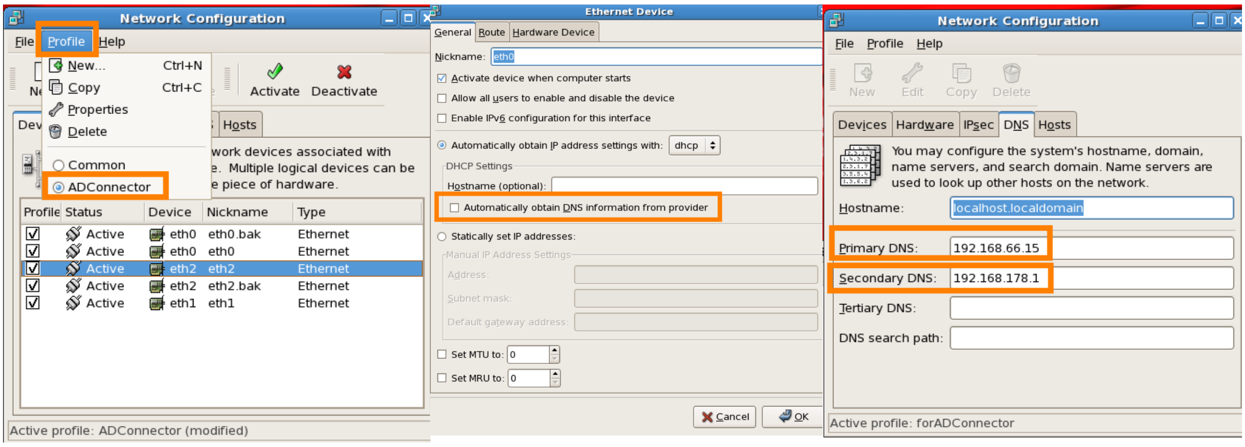
6 Elemente

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. Frist 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
File Profile Help
New... Ctrl+N
Copy Ctrl+C
Properties
Delete
Common
ADConnector
Activate Deactivate
Hosts
work devices associated with
e. Multiple logical devices can be
e piece of hardware.
Ethernet Device
General Route Hardware Device
Cancel OK
Network Configuration
File Profile Help
New Edit Copy Delete
Devices Hardware IPsec DNS Hosts
You may configure the system's hostname, domain, name servers, and search domain. Name servers are used to look up other hosts on the network.

Profile	Status	Device	Nickname	Type
☑	Active	eth0	eth0.bak	Ethernet
☑	Active	eth0	eth0	Ethernet
☑	Active	eth2	eth2	Ethernet
☑	Active	eth2	eth2.bak	Ethernet
☑	Active	eth1	eth1	Ethernet

Active profile: ADConnector (modified)

Nickname: eth0
☑ Activate device when computer starts
☐ Allow all users to enable and disable the device
☐ Enable IPv6 configuration for this interface
● Automatically obtain IP address settings with: dhcp
DHCP Settings
Hostname (optional):
☐ Automatically obtain DNS information from provider
○ Statically set IP addresses:
Manual IP Address Settings
Address:
Subnet mask:
Default gateway address:
☐ Set MTU to: 0
☐ Set MRU to: 0

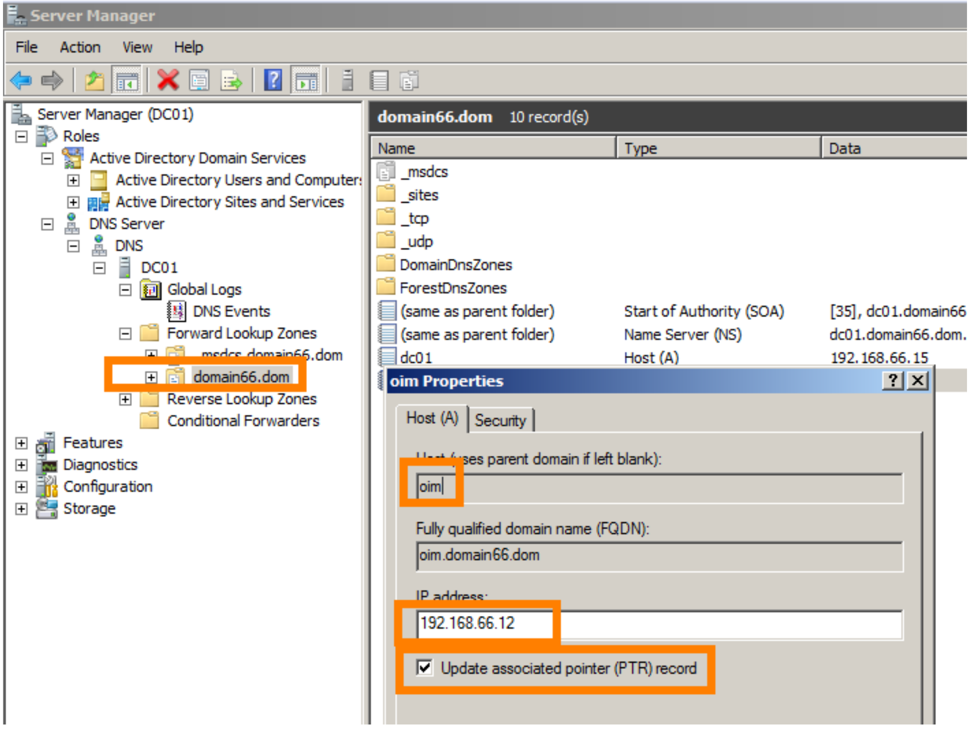
Hostname: localhost.localdomain
Primary DNS: 192.168.66.15
Secondary DNS: 192.168.178.1
Tertiary DNS:
DNS search path:
Active profile: forADConnector

Figure 25. **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.



domain66.dom 10 record(s)

Name	Type	Data
_msdcs		
_sites		
_tcp		
_udp		
DomainDnsZones		
ForestDnsZones		
(same as parent folder)	Start of Authority (SOA)	[35], dc01.domain66
(same as parent folder)	Name Server (NS)	dc01.domain66.dom.
dc01	Host (A)	192.168.66.15

Host (uses parent domain if left blank): oim
Fully qualified domain name (FQDN): oim.domain66.dom
IP address: 192.168.66.12
☑ Update associated pointer (PTR) record

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.

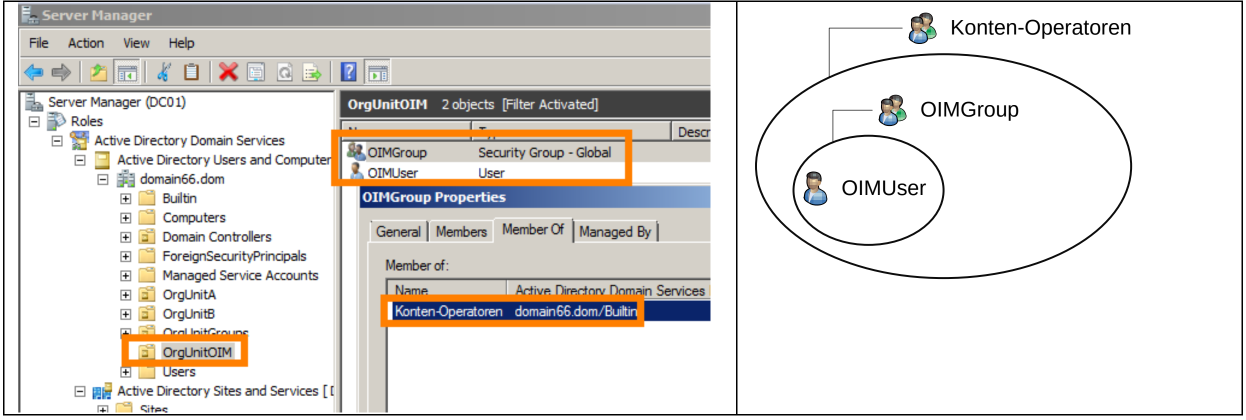
5 Deploying the AD Connector.

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/id-mgmt/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 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

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.



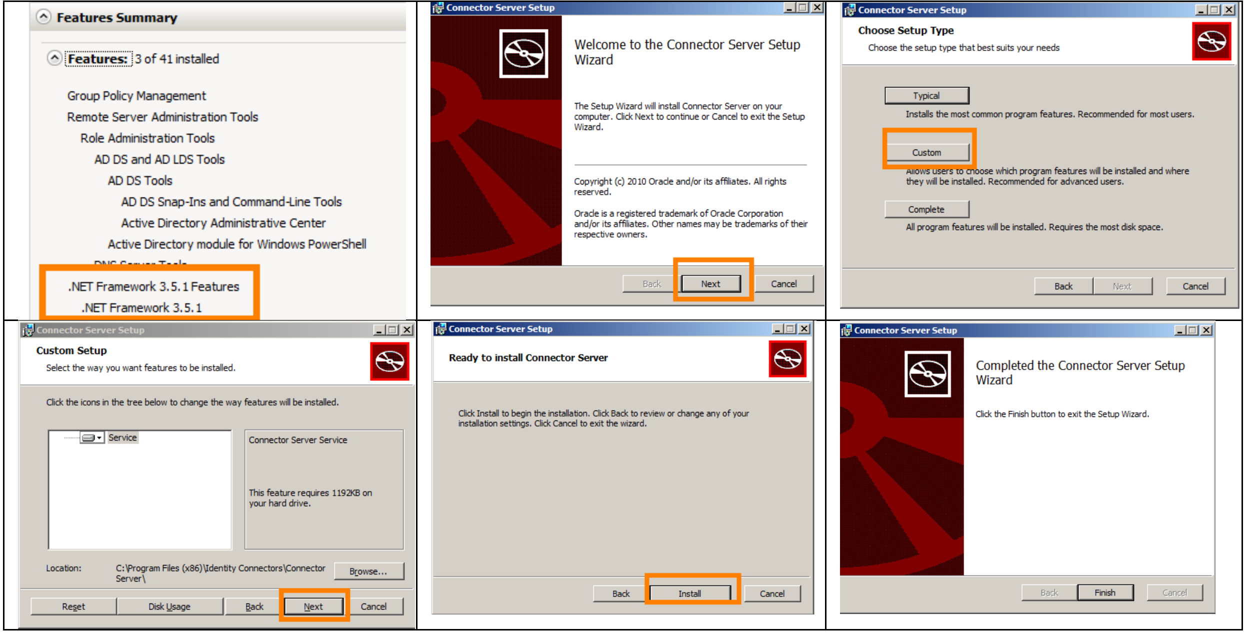
Server Manager
File Action View Help
Server Manager (DC01)
Roles
Active Directory Domain Services
Active Directory Users and Computer
domain66.dom
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
OrgUnitA
OrgUnitB
OrgUnitGroups
OrgUnitOIM
Users
Active Directory Sites and Services
Sites
OrgUnitOIM 2 objects [Filter Activated]
Descr
OIMGroup Security Group - Global
OIMUser User
OIMGroup Properties
General Members Member Of Managed By
Member of:
Name Active Directory Domain Services
Konten-Operatoren domain66.dom/Builtin
Konten-Operatoren
OIMGroup
OIMUser

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:\16VirtualBox\99GlobalSharedFolder\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.



Features Summary

Features: 3 of 41 installed

Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
AD DS Tools
AD DS Snap-Ins and Command-Line Tools
Active Directory Administrative Center
Active Directory module for Windows PowerShell
.NET Framework 3.5.1 Features
.NET Framework 3.5.1

Connector Server Setup

Welcome to the Connector Server Setup Wizard

The Setup Wizard will install Connector Server on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Copyright (c) 2010 Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Connector Server Setup

Choose Setup Type
Choose the setup type that best suits your needs

Typical: Installs the most common program features. Recommended for most users.

Custom: Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users.

Complete: All program features will be installed. Requires the most disk space.

Connector Server Setup

Custom Setup
Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

Connector Server Service

This feature requires 1192KB on your hard drive.

Location: C:\Program Files (x86)\Identity Connectors\Connector Server\

Connector Server Setup

Ready to install Connector Server

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

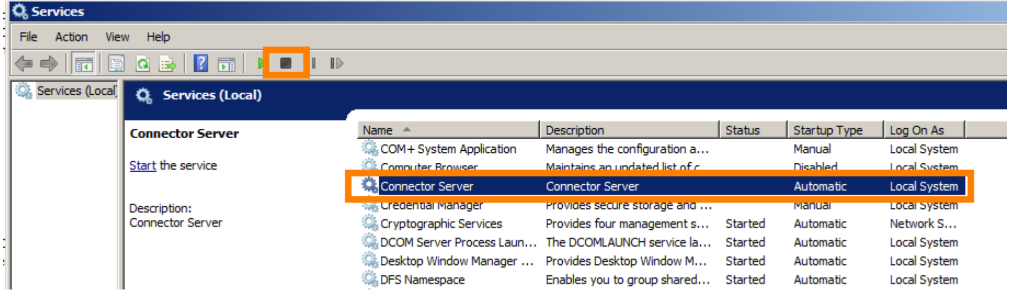
Connector Server Setup

Completed the Connector Server Setup Wizard

Click the Finish button to exit the Setup Wizard.

Figure 28. **Installation of the Connector Server on Windows 2008 Server.**

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



Services (Local)

Connector Server

Start the service

Description:
Connector Server

Name	Description	Status	Startup Type	Log On As
COM+ System Application	Manages the configuration a...		Manual	Local System
Computer Browser	Maintains an updated list of c...		Disabled	Local System
Connector Server	Connector Server		Automatic	Local System
Credential Manager	Provides secure storage and ...		Manual	Local System
Cryptographic Services	Provides four management s...	Started	Automatic	Network S...
DCOM Server Process Laun...	The DCOMLAUNCH service la...	Started	Automatic	Local System
Desktop Window Manager ...	Provides Desktop Window M...	Started	Automatic	Local System
DFS Namespace	Enables you to group shared...	Started	Automatic	Local System

Figure 29. **Stopping the connector server on Winodws.**

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.

C:\Program Files (x86)\Identity Connectors\Connector Server>
```

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

We use the default values here.

```
        <add key="connectorserver.usessl" value="false" />
        <add key="connectorserver.certificatestorename" value="ConnectorServerSSLCertificate" />
        <add key="connectorserver.ifaddress" value="0.0.0.0" />
        <add key="logging.proxy" value="false" />
        <add key="connectorserver.key" value="ir7D3xpnDwzZ53rAikOKdmZ1o5A=" />
    </appSettings>
    <system.diagnostics>
      <trace autoflush="true" indentsize="4">
        <listeners>
          <remove name="Default" />
          <add name="myListener"  type="System.Diagnostics.TextWriterTraceListener"
               initializeData="c:\connectorserver.log"
               traceOutputOptions="DateTime"
            >
             <filter type="System.Diagnostics.EventTypeFilter" initializeData="Information"/>
           </add>
        </listeners>
      </trace>
       <switches>
          <add name="ActiveDirectorySwitch" value="4" />
      </switches>
    </system.diagnostics>
</configuration>
```

This key is updated with the value"Welcome1"

Logging Settings.
0=no logging, 3=info, 4=verbose.

Listing 1. **Changes in the file ConnectorServer.exe.config**

We use the Service Panel to restart the server. We find the logfile at C:\connectorserver.log. Ok.

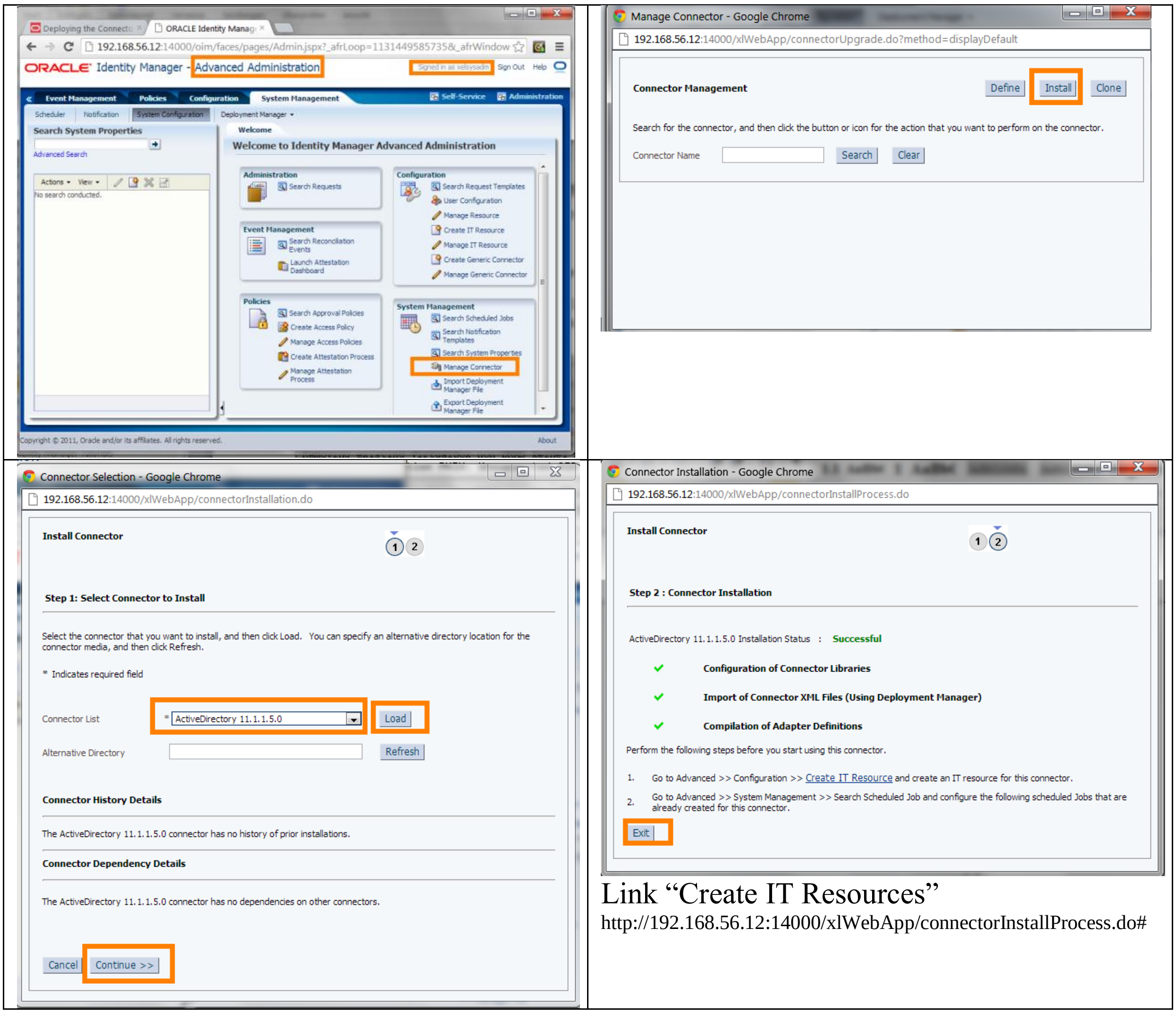
5.3 Installing the Connector in Oracle Identity Manager

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.

```
[oracle@12oel55_odd ConnectorDefaultDirectory]$ pwd
/opt/oracle/Middleware01/Oracle_IDM1/server/ConnectorDefaultDirectory
[oracle@12oel55_odd ConnectorDefaultDirectory]$ cp -r /media/sf_99GlobalSharedFolder/activedirectory-
11.1.1.5.0/  ./activedirectory-11.1.1.5.0
```

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.



192.168.56.12:14000/oim/faces/pages/Admin.jspx?_afrLoop=1131449585735&_afrWindow

Welcome to Identity Manager Advanced Administration

No search conducted.

Copyright © 2011, Oracle and/or its affiliates. All rights reserved.

192.168.56.12:14000/xlWebApp/connectorUpgrade.do?method=displayDefault

Search for the connector, and then click the button or icon for the action that you want to perform on the connector.

192.168.56.12:14000/xlWebApp/connectorInstallation.do

Step 1: Select Connector to Install

Select the connector that you want to install, and then click Load. You can specify an alternative directory location for the connector media, and then click Refresh.

* Indicates required field

Connector List * ActiveDirectory 11.1.1.5.0

Connector History Details

The ActiveDirectory 11.1.1.5.0 connector has no history of prior installations.

Connector Dependency Details

The ActiveDirectory 11.1.1.5.0 connector has no dependencies on other connectors.

192.168.56.12:14000/xlWebApp/connectorInstallProcess.do

Step 2 : Connector Installation

ActiveDirectory 11.1.1.5.0 Installation Status : Successful

✓ Configuration of Connector Libraries

✓ Import of Connector XML Files (Using Deployment Manager)

✓ Compilation of Adapter Definitions

Perform the following steps before you start using this connector.

1. Go to Advanced >> Configuration >> Create IT Resource and create an IT resource for this connector.
2. Go to Advanced >> System Management >> Search Scheduled Job and configure the following scheduled Jobs that are already created for this connector.

Link “Create IT Resources”
http://192.168.56.12:14000/xlWebApp/connectorInstallProcess.do#

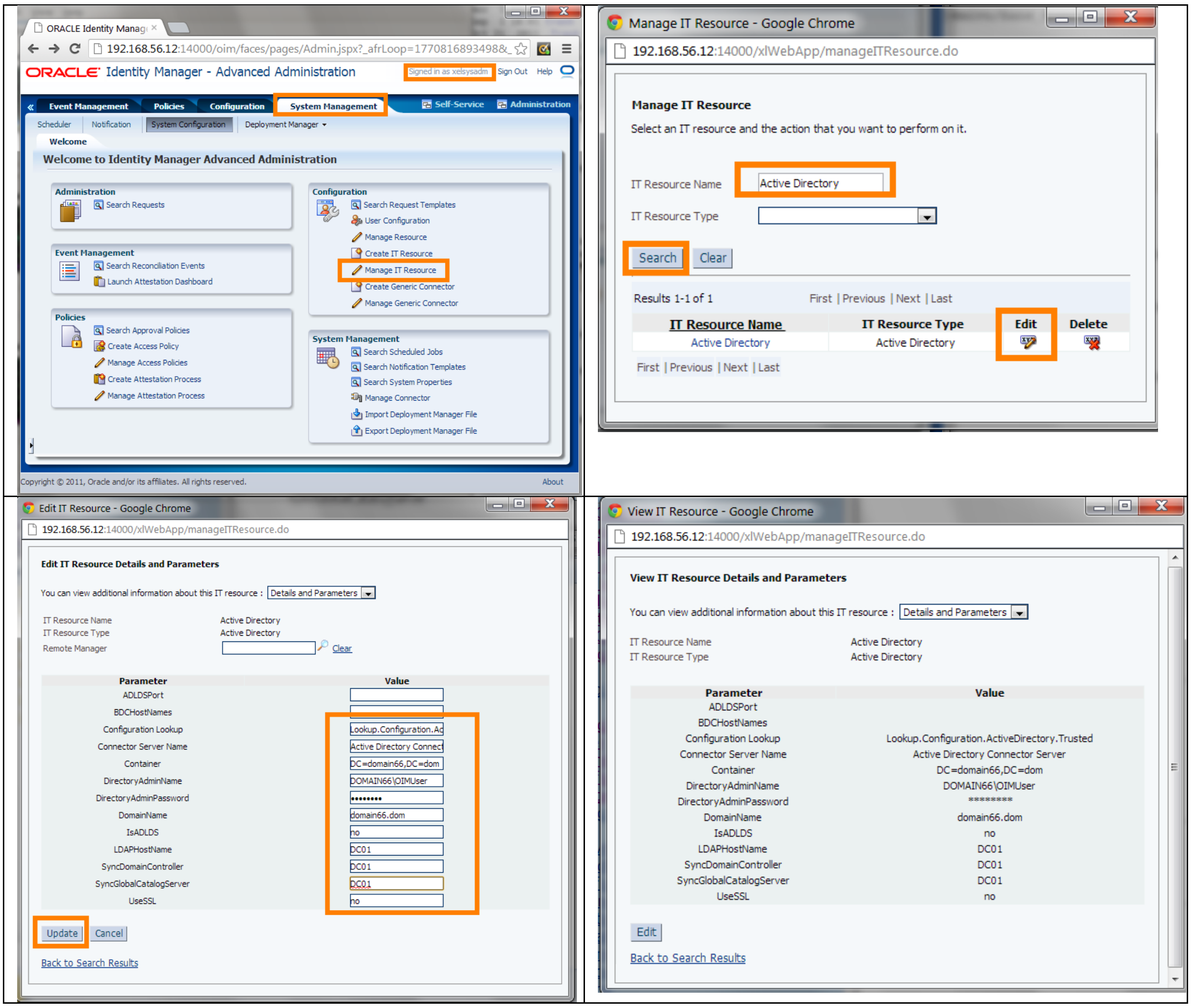
Figure 30. **Installation of the AD Connector in OIM.**

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#BABCFEGF
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
[oracle@12oel55_odd bin]$
```

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.


ORACLE Identity Manag
192.168.56.12:14000/oim/faces/pages/Admin.jspx?_afrLoop=1770816893498&_
ORACLE Identity Manager - Advanced Administration
Signed in as xelsysadm
Sign Out
Help
Event Management
Policies
Configuration
System Management
Self-Service
Administration
Scheduler
Notification
System Configuration
Deployment Manager
Welcome
Welcome to Identity Manager Advanced Administration
Administration
Search Requests
Event Management
Search Reconciliation Events
Launch Attestation Dashboard
Policies
Search Approval Policies
Create Access Policy
Manage Access Policies
Create Attestation Process
Manage Attestation Process
Configuration
Search Request Templates
User Configuration
Manage Resource
Create IT Resource
Manage IT Resource
Create Generic Connector
Manage Generic Connector
System Management
Search Scheduled Jobs
Search Notification Templates
Search System Properties
Manage Connector
Import Deployment Manager File
Export Deployment Manager File
Copyright © 2011, Oracle and/or its affiliates. All rights reserved.
About
Manage IT Resource - Google Chrome
192.168.56.12:14000/xlWebApp/manageITResource.do
Search
Clear
First | Previous | Next | Last
Edit IT Resource - Google Chrome
192.168.56.12:14000/xlWebApp/manageITResource.do
Update
Cancel
Back to Search Results
View IT Resource - Google Chrome
192.168.56.12:14000/xlWebApp/manageITResource.do
Edit
Back to Search Results

Manage IT Resource

Select an IT resource and the action that you want to perform on it.

IT Resource Name: Active Directory
IT Resource Type:

Results 1-1 of 1

IT Resource Name	IT Resource Type	Edit	Delete
Active Directory	Active Directory	✎	✗

Edit IT Resource Details and Parameters

You can view additional information about this IT resource : Details and Parameters

IT Resource Name: Active Directory
IT Resource Type: Active Directory
Remote Manager:

Parameter	Value
ADLDSPort	
BDCHostNames	
Configuration Lookup	Lookup.Configuration.Ac
Connector Server Name	Active Directory Connect
Container	DC=domain66,DC=dom
DirectoryAdminName	DOMAIN66\OIMUser
DirectoryAdminPassword	••••••••
DomainName	domain66.dom
IsADLDS	no
LDAPHostName	DC01
SyncDomainController	DC01
SyncGlobalCatalogServer	DC01
UseSSL	no

View IT Resource Details and Parameters

You can view additional information about this IT resource : Details and Parameters

IT Resource Name: Active Directory
IT Resource Type: Active Directory

Parameter	Value
ADLDSPort	
BDCHostNames	
Configuration Lookup	Lookup.Configuration.ActiveDirectory.Trusted
Connector Server Name	Active Directory Connector Server
Container	DC=domain66,DC=dom
DirectoryAdminName	DOMAIN66\OIMUser
DirectoryAdminPassword	********
DomainName	domain66.dom
IsADLDS	no
LDAPHostName	DC01
SyncDomainController	DC01
SyncGlobalCatalogServer	DC01
UseSSL	no

Figure 31. **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.

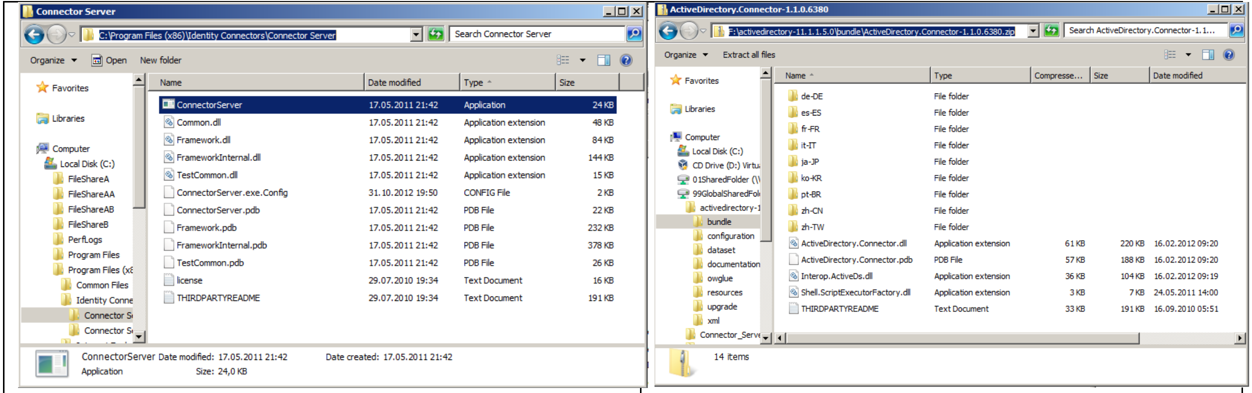
We provide the following values:

Configuration Lookup	`Lookup.Configuration.ActiveDirectory.Trusted (identity reconciliation)`
Connector Server Name	`Active Directory Connector Server (default)`
Container	`DC=domain66,DC=dom`
DirectoryAdminName	`DOMAIN66\OIMUser`
DirectoryAdminPassword	`Welcome1`
DomainName	`domain66.dom`
isADLDS	`No`
LDAPHostName	`DC01`
SyncDomainController	`DC01`
SyncGlobalCatalogServer	`DC01`
UseSSL	`no`

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

C:\Program Files (x86)\Identity Connectors\Connector Server

Name	Date modified	Type	Size
ConnectorServer	17.05.2011 21:42	Application	24 KB
Common.dll	17.05.2011 21:42	Application extension	48 KB
Framework.dll	17.05.2011 21:42	Application extension	84 KB
FrameworkInternal.dll	17.05.2011 21:42	Application extension	144 KB
TestCommon.dll	17.05.2011 21:42	Application extension	15 KB
ConnectorServer.exe.Config	31.10.2012 19:50	CONFIG File	2 KB
ConnectorServer.pdb	17.05.2011 21:42	PDB File	22 KB
Framework.pdb	17.05.2011 21:42	PDB File	232 KB
FrameworkInternal.pdb	17.05.2011 21:42	PDB File	378 KB
TestCommon.pdb	17.05.2011 21:42	PDB File	26 KB
license	29.07.2010 19:34	Text Document	16 KB
THIRDPARTYREADME	29.07.2010 19:34	Text Document	191 KB

ConnectorServer Date modified: 17.05.2011 21:42 Date created: 17.05.2011 21:42
Application Size: 24,0 KB

ActiveDirectory.Connector-1.1.0.6380

F:\activedirectory-11.1.1.5.0\bundle\ActiveDirectory.Connector-1.1.0.6380.zip

Name	Type	Compresse...	Size	Date modified
de-DE	File folder			
es-ES	File folder			
fr-FR	File folder			
it-IT	File folder			
ja-JP	File folder			
ko-KR	File folder			
pt-BR	File folder			
zh-CN	File folder			
zh-TW	File folder			
ActiveDirectory.Connector.dll	Application extension	61 KB	220 KB	16.02.2012 09:20
ActiveDirectory.Connector.pdb	PDB File	57 KB	188 KB	16.02.2012 09:20
Interop.ActiveDs.dll	Application extension	36 KB	104 KB	16.02.2012 09:19
Shell.ScriptExecutorFactory.dll	Application extension	3 KB	7 KB	24.05.2011 14:00
THIRDPARTYREADME	Text Document	33 KB	191 KB	16.09.2010 05:51

14 items

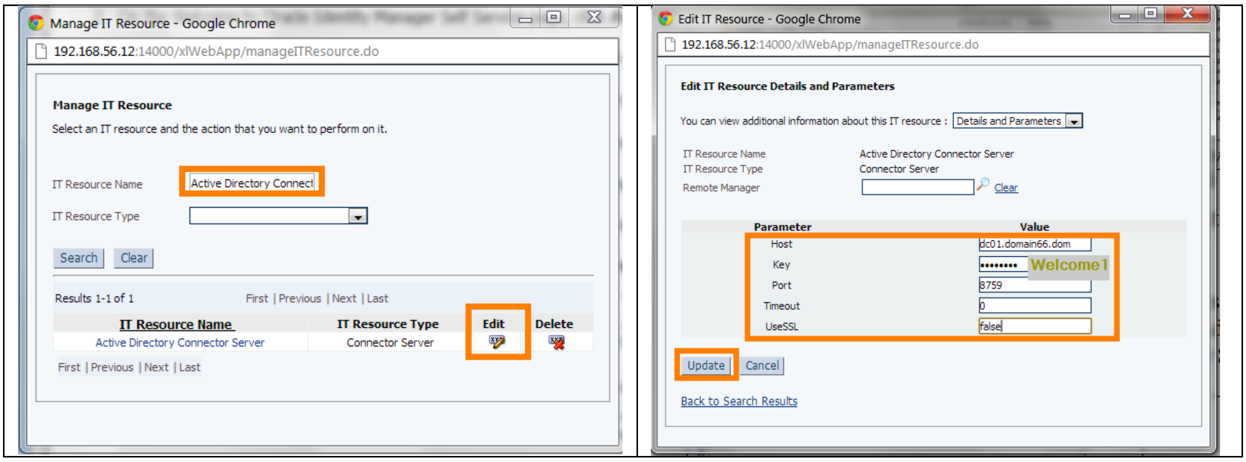
Connector Server Home

Active Directory Connector bundle

Figure 32. **The Connector Server Home and the AD Connector bundle before copying.**

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.



Manage IT Resource - Google Chrome

192.168.56.12:14000/xlWebApp/manageITResource.do

Manage IT Resource

Select an IT resource and the action that you want to perform on it.

IT Resource Name: Active Directory Connect
IT Resource Type:

Search Clear

Results 1-1 of 1 First | Previous | Next | Last

IT Resource Name	IT Resource Type	Edit	Delete
Active Directory Connector Server	Connector Server		

First | Previous | Next | Last

Edit IT Resource - Google Chrome

192.168.56.12:14000/xlWebApp/manageITResource.do

Edit IT Resource Details and Parameters

You can view additional information about this IT resource : Details and Parameters

IT Resource Name: Active Directory Connector Server
IT Resource Type: Connector Server
Remote Manager: Clear

Parameter	Value
Host	dc01.domain66.dom
Key	•••••••• Welcome1
Port	8759
Timeout	0
UseSSL	false

Update Cancel

Back to Search Results

Figure 33. **Configuring the details for the AD Connector resource in OIM.**

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@12oe155_odd bin]$ pwd
```

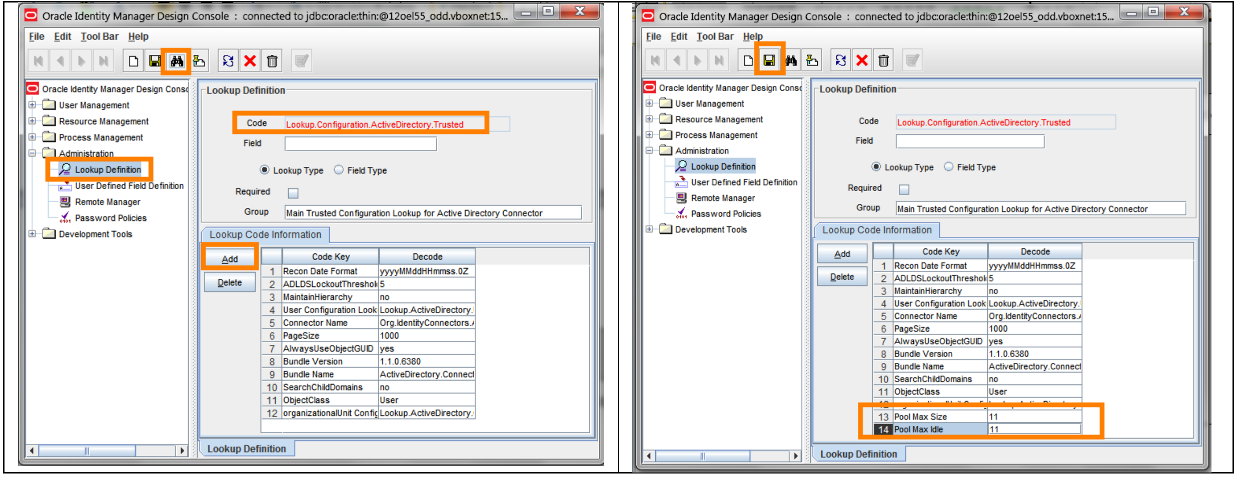
```
/opt/oracle/Middleware01/Oracle_IDM1/server/bin
[oracle@12oel55_odd bin]$ ./PurgeCache.sh All
[Enter the admin username:]xelsysadm
[Enter the admin password:]
[Enter the service url : (i.e.: t3://oimhostname:oimportno)]t3://localhost:14000
PurgeCache Login Success...
Purging the cache categories:[All] is successful
```

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.

```
C:\Users\uScorpio>d:
D:\>cd D:\10Oracle\04OIM\Oracle_IDM1\designconsole
D:\10Oracle\04OIM\Oracle_IDM1\designconsole>xlclient.cmd
```

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.



Lookup Definition

Code: Lookup.Configuration.ActiveDirectory.Trusted

Field:

● Lookup Type ○ Field Type

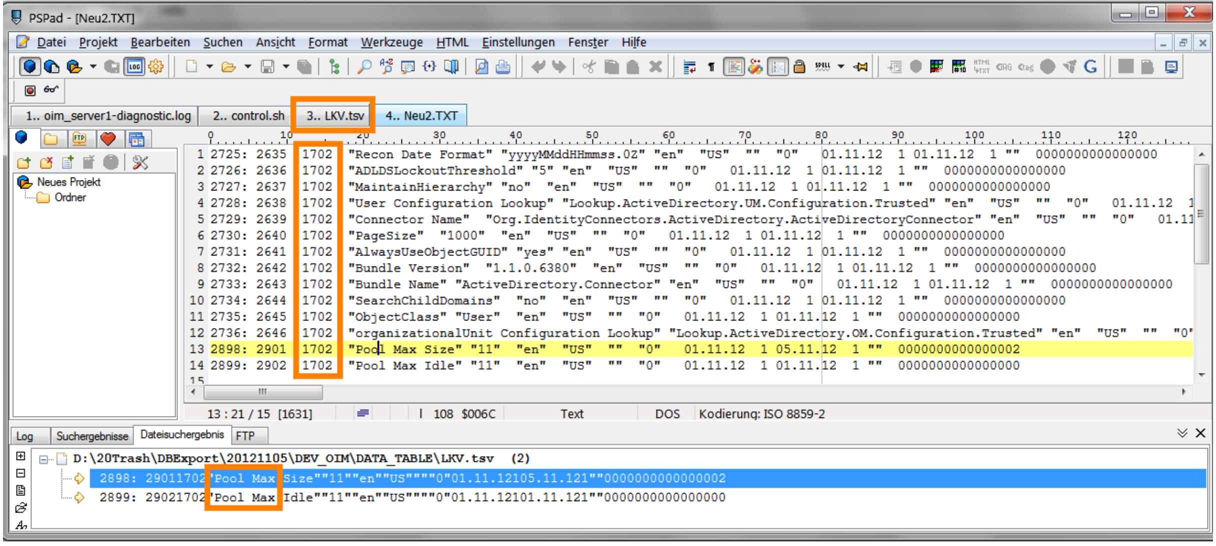
Required □

Group: Main Trusted Configuration Lookup for Active Directory Connector

	Code Key	Decode
1	Recon Date Format	yyyyMMddHHmmss.0Z
2	ADLDSLockoutThreshol	5
3	MaintainHierarchy	no
4	User Configuration Look	Lookup.ActiveDirectory.
5	Connector Name	Org.IdentityConnectors.A
6	PageSize	1000
7	AlwaysUseObjectGUID	yes
8	Bundle Version	1.1.0.6380
9	Bundle Name	ActiveDirectory.Connect
10	SearchChildDomains	no
11	ObjectClass	User
12	organizationalUnit Config	Lookup.ActiveDirectory.
13	Pool Max Size	11
14	Pool Max Idle	11

Figure 34. **Configuring connection pool parameters for the AD Connector in the Design Console.**

A search in the exported data base 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.



```
2725: 2635  1702  "Recon Date Format" "yyyyMMddHHmmss.0Z" "en"  "US"  ""  "0"   01.11.12  1 01.11.12  1 ""  0000000000000000
2726: 2636  1702  "ADLDSLockoutThreshold" "5" "en"  "US"  ""  "0"   01.11.12  1 01.11.12  1 ""  0000000000000000
2727: 2637  1702  "MaintainHierarchy" "no"  "en"  "US"  ""  "0"   01.11.12  1 01.11.12  1 ""  0000000000000000
2728: 2638  1702  "User Configuration Lookup" "Lookup.ActiveDirectory.UM.Configuration.Trusted" "en"  "US"  ""  "0"   01.11.12  1
2729: 2639  1702  "Connector Name"  "Org.IdentityConnectors.ActiveDirectory.ActiveDirectoryConnector" "en"  "US"  ""  "0"   01.11
2730: 2640  1702  "PageSize"  "1000"  "en"  "US"  ""  "0"   01.11.12  1 01.11.12  1 ""  0000000000000000
2731: 2641  1702  "AlwaysUseObjectGUID" "yes" "en"  "US"  ""  "0"   01.11.12  1 01.11.12  1 ""  0000000000000000
2732: 2642  1702  "Bundle Version"  "1.1.0.6380"  "en"  "US"  ""  "0"   01.11.12  1 01.11.12  1 ""  0000000000000000
2733: 2643  1702  "Bundle Name" "ActiveDirectory.Connector" "en"  "US"  ""  "0"   01.11.12  1 01.11.12  1 ""  0000000000000000
2734: 2644  1702  "SearchChildDomains"  "no"  "en"  "US"  ""  "0"   01.11.12  1 01.11.12  1 ""  0000000000000000
2735: 2645  1702  "ObjectClass" "User"  "en"  "US"  ""  "0"   01.11.12  1 01.11.12  1 ""  0000000000000000
2736: 2646  1702  "organizationalUnit Configuration Lookup" "Lookup.ActiveDirectory.OM.Configuration.Trusted" "en"  "US"  ""  "0"
2898: 2901  1702  "Pool Max Size" "11"  "en"  "US"  ""  "0"   01.11.12  1 05.11.12  1 ""  0000000000000002
2899: 2902  1702  "Pool Max Idle" "11"  "en"  "US"  ""  "0"   01.11.12  1 01.11.12  1 ""  0000000000000000
```

13 : 21 / 15 [1631] 108 $006C Text DOS Kodierung: ISO 8859-2

```
D:\20Trash\DBExport\20121105\DEV_OIM\DATA_TABLE\LKV.tsv  (2)
    2898: 29011702"Pool Max Size""11""en""US""""0"01.11.12105.11.121""0000000000000002
    2899: 29021702"Pool Max Idle""11""en""US""""0"01.11.12101.11.121""0000000000000000
```

Figure 35. **Searching the property Max Pool Size in the exported OIM database.**

The entry in the LKU table corresponding to the key 1702 is:

```
1702 "1""Main Trusted Configuration Lookup for Active Directory Connector" "0"
             "Lookup.Configuration.ActiveDirectory.Trusted" "" 01.11.12 1 01.11.12 1 "" 0000000000000000
```

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.

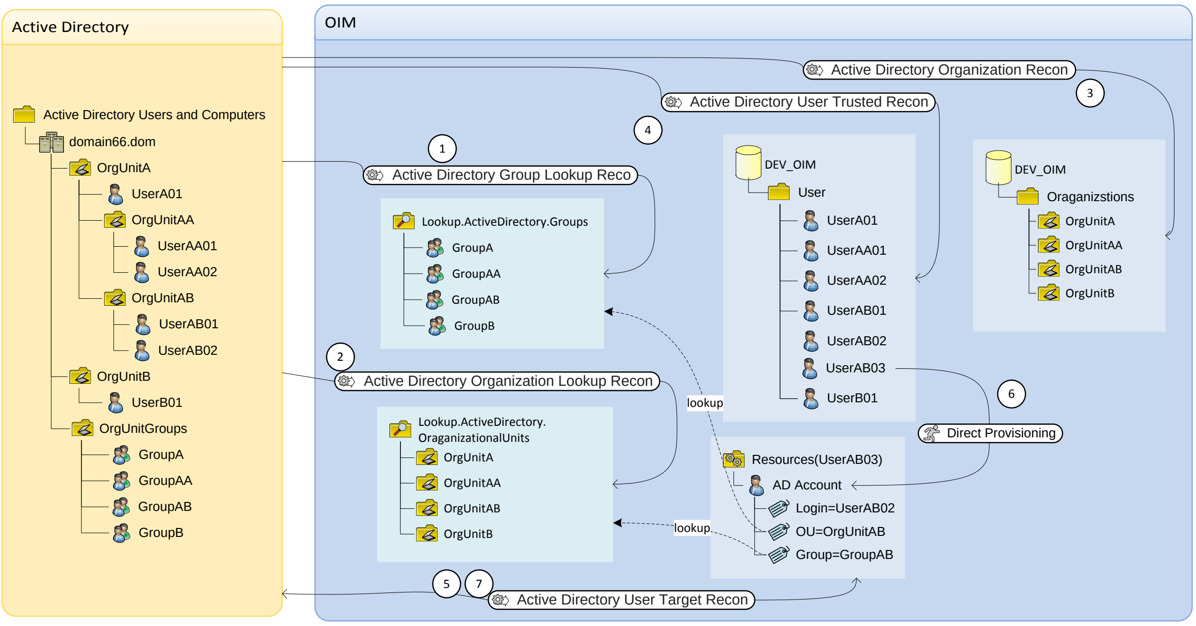
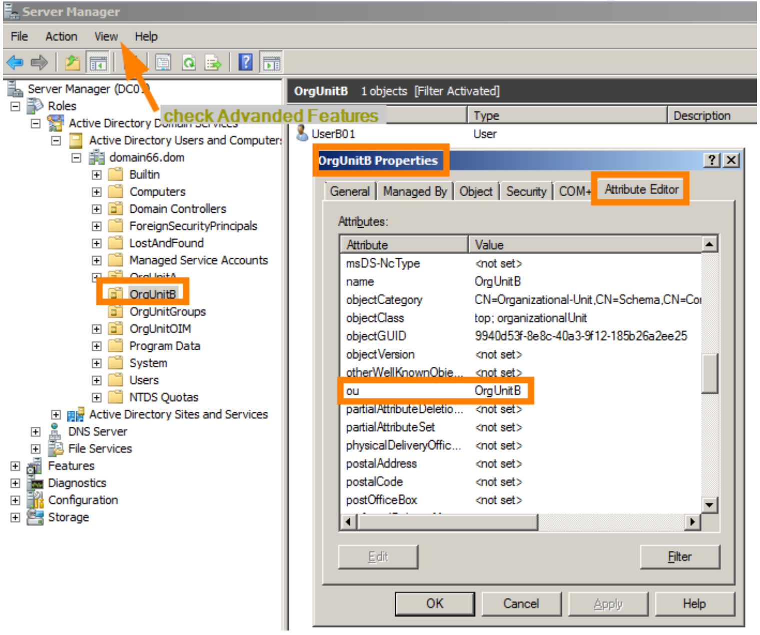


Figure 36. **Overview of the integration of company domain66 into the OIM.**

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.

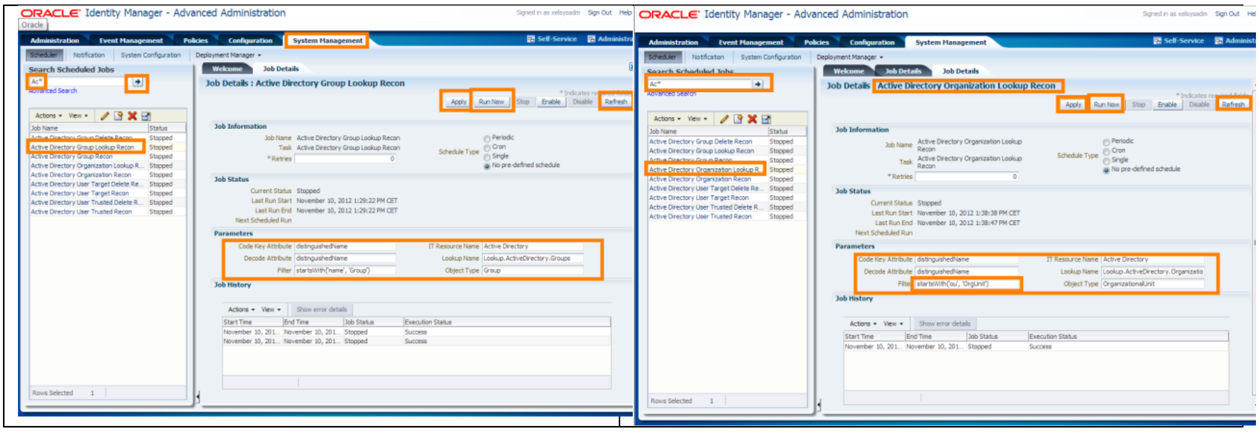


check Advanded Features

Attribute	Value
msDS-NcType	<not set>
name	OrgUnitB
objectCategory	CN=Organizational-Unit,CN=Schema,CN=Co
objectClass	top; organizationalUnit
objectGUID	9940d53f-8e8c-40a3-9f12-185b26a2ee25
objectVersion	<not set>
otherWellKnownObje...	<not set>
ou	OrgUnitB
partialAttributeDeletio...	<not set>
partialAttributeSet	<not set>
physicalDeliveryOffic...	<not set>
postalAddress	<not set>
postalCode	<not set>
postOfficeBox	<not set>

Figure 37. **Using the Attribute Editor in Windows 2008 Server to find the attribute names for the filter expressions.**

The following pictures illustrate the settings for group and organization lookup reconciliation.



Job Details : Active Directory Group Lookup Recon

Job Information
Job Name: Active Directory Group Lookup Recon
Task: Active Directory Group Lookup Recon
* Retries: 0
Schedule Type: ○ Periodic ○ Cron ○ Single ● No pre-defined schedule

Job Status
Current Status: Stopped
Last Run Start: November 10, 2012 1:29:22 PM CET
Last Run End: November 10, 2012 1:29:22 PM CET
Next Scheduled Run:

Parameters
Code Key Attribute: distinguishedName
Decode Attribute: distinguishedName
Filter: startsWith('name', 'Group')
IT Resource Name: Active Directory
Lookup Name: Lookup.ActiveDirectory.Groups
Object Type: Group

Job History

Start Time	End Time	Job Status	Execution Status
November 10, 201...	November 10, 201...	Stopped	Success
November 10, 201...	November 10, 201...	Stopped	Success

Job Details Active Directory Organization Lookup Recon

Job Information
Job Name: Active Directory Organization Lookup Recon
Task: Active Directory Organization Lookup Recon
* Retries: 0
Schedule Type: ○ Periodic ○ Cron ○ Single ● No pre-defined schedule

Job Status
Current Status: Stopped
Last Run Start: November 10, 2012 1:38:38 PM CET
Last Run End: November 10, 2012 1:38:47 PM CET
Next Scheduled Run:

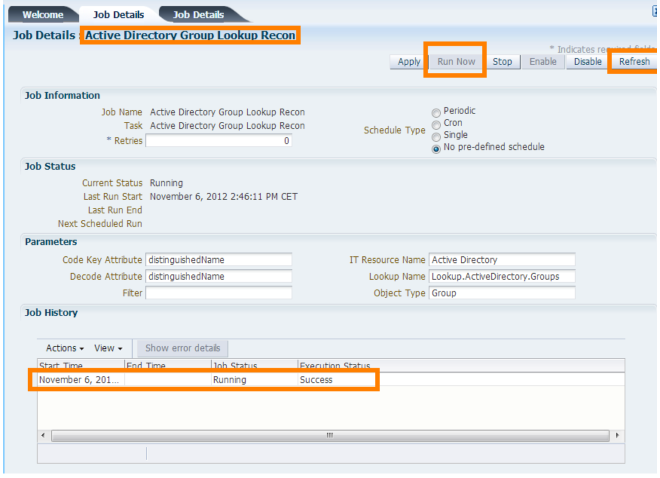
Parameters
Code Key Attribute: distinguishedName
Decode Attribute: distinguishedName
Filter: startsWith('ou', 'OrgUnit')
IT Resource Name: Active Directory
Lookup Name: Lookup.ActiveDirectory.Organizatio
Object Type: OrganizationalUnit

Job History

Start Time	End Time	Job Status	Execution Status
November 10, 201...	November 10, 201...	Stopped	Success

Figure 38. **Checking the Lookup Field configuration for Groups and Organization 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.



Job Details : Active Directory Group Lookup Recon

Job Information
Job Name: Active Directory Group Lookup Recon
Task: Active Directory Group Lookup Recon
* Retries: 0
Schedule Type: ○ Periodic ○ Cron ○ Single ● No pre-defined schedule

Job Status
Current Status: Running
Last Run Start: November 6, 2012 2:46:11 PM CET
Last Run End:
Next Scheduled Run:

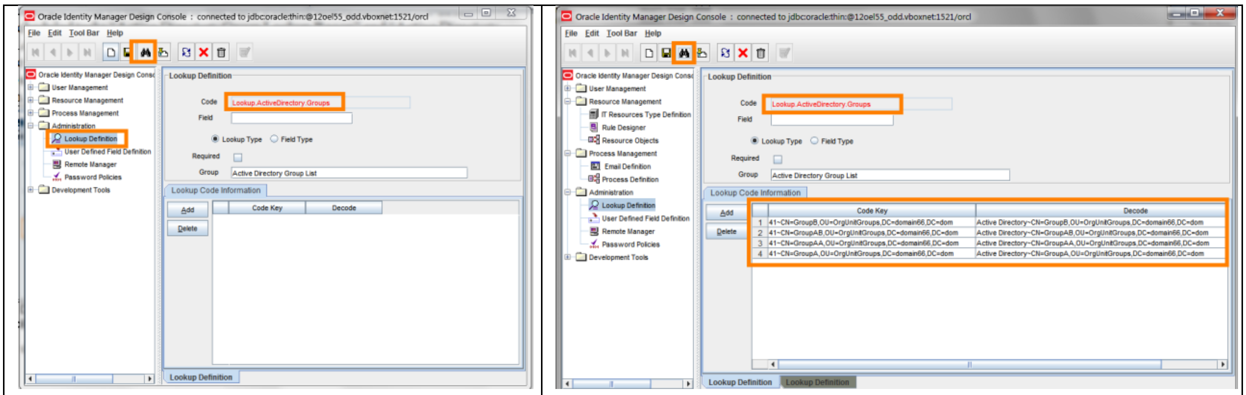
Parameters
Code Key Attribute: distinguishedName
Decode Attribute: distinguishedName
Filter:
IT Resource Name: Active Directory
Lookup Name: Lookup.ActiveDirectory.Groups
Object Type: Group

Job History

Start Time	End Time	Job Status	Execution Status
November 6, 201...		Running	Success

Figure 39. **Running the Active Directory Group Lookup Recon scheduled task.**

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



Oracle Identity Manager Design Console : connected to jdbc:oracle:thin:@12oel55_odd.vboxnet:1521/orcl

Lookup Definition
Code: Lookup.ActiveDirectory.Groups
Field:
● Lookup Type ○ Field Type
Required □
Group: Active Directory Group List

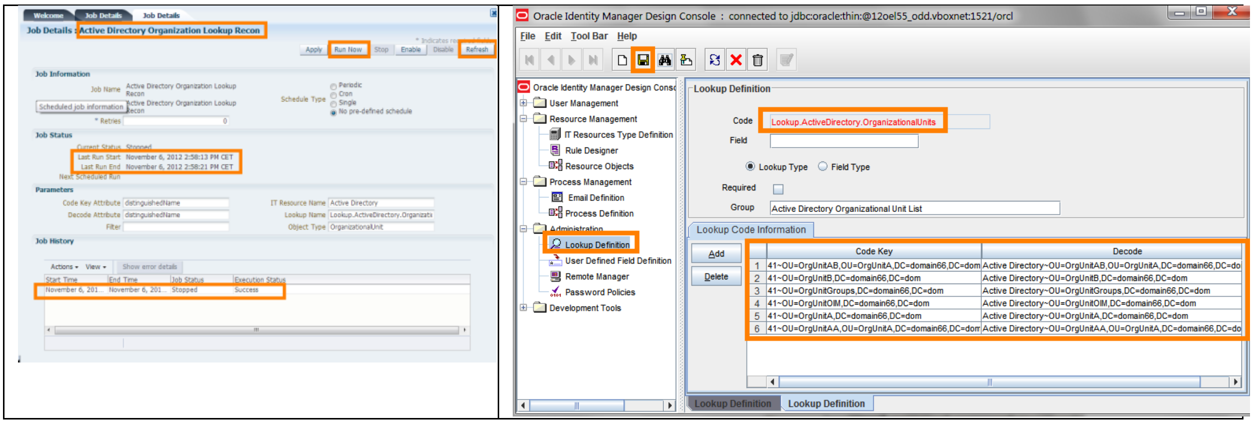
Lookup Code Information

	Code Key	Decode
1	41~CN=GroupB,OU=OrgUnitGroups,DC=domain66,DC=dom	Active Directory~CN=GroupB,OU=OrgUnitGroups,DC=domain66,DC=dom
2	41~CN=GroupAB,OU=OrgUnitGroups,DC=domain66,DC=dom	Active Directory~CN=GroupAB,OU=OrgUnitGroups,DC=domain66,DC=dom
3	41~CN=GroupAA,OU=OrgUnitGroups,DC=domain66,DC=dom	Active Directory~CN=GroupAA,OU=OrgUnitGroups,DC=domain66,DC=dom
4	41~CN=GroupA,OU=OrgUnitGroups,DC=domain66,DC=dom	Active Directory~CN=GroupA,OU=OrgUnitGroups,DC=domain66,DC=dom

Before running Group Lookup Recon After running Group Lookup Recon

Figure 40. **Running Group Lookup Recon task populates the attribute map with values.**

We also run the Organization Lookup Recon and check the attribute map in the Design Console.



Job Details : Active Directory Organization Lookup Recon

Job Information

Job Name: Active Directory Organization Lookup Recon
Task: Active Directory Organization Lookup Recon
* Retries: 0
Schedule Type: ● No pre-defined schedule

Job Status

Current Status: Stopped
Last Run Start: November 6, 2012 2:58:13 PM CET
Last Run End: November 6, 2012 2:58:21 PM CET
Next Scheduled Run

Parameters

Code Key Attribute: distinguishedName
Decode Attribute: distinguishedName
Filter:
IT Resource Name: Active Directory
Lookup Name: Lookup.ActiveDirectory.Organizati
Object Type: OrganizationalUnit

Job History

Start Time	End Time	Job Status	Execution Status
November 6, 201...	November 6, 201...	Stopped	Success

Lookup Definition

Code: Lookup.ActiveDirectory.OrganizationalUnits
Field:
● Lookup Type ○ Field Type
Required □
Group: Active Directory Organizational Unit List

Lookup Code Information

	Code Key	Decode
1	41~OU=OrgUnitAB,OU=OrgUnitA,DC=domain66,DC=dom	Active Directory~OU=OrgUnitAB,OU=OrgUnitA,DC=domain66,DC=do
2	41~OU=OrgUnitB,DC=domain66,DC=dom	Active Directory~OU=OrgUnitB,DC=domain66,DC=dom
3	41~OU=OrgUnitGroups,DC=domain66,DC=dom	Active Directory~OU=OrgUnitGroups,DC=domain66,DC=dom
4	41~OU=OrgUnitOIM,DC=domain66,DC=dom	Active Directory~OU=OrgUnitOIM,DC=domain66,DC=dom
5	41~OU=OrgUnitA,DC=domain66,DC=dom	Active Directory~OU=OrgUnitA,DC=domain66,DC=dom
6	41~OU=OrgUnitAA,OU=OrgUnitA,DC=domain66,DC=dom	Active Directory~OU=OrgUnitAA,OU=OrgUnitA,DC=domain66,DC=do

Figure 41. **Running the Active Directory Organization Lookup Recon scheduled task.**

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

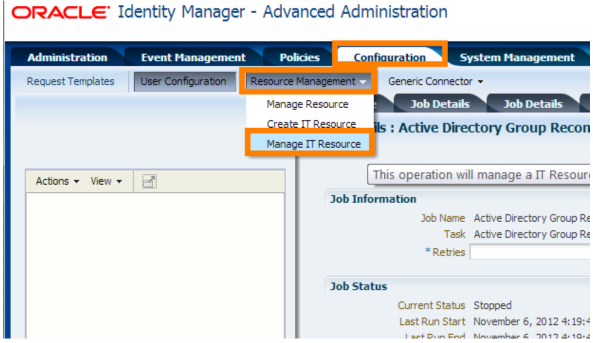
We take a snapshot of the Linux machine at this point.

Sicherheitspunkt 10	System started. Scheduled Jobs for Active Directory Group and Organization Lookup Recon run. Used Filters: startsWith('name', 'Group') startsWith('ou', 'OrgUnit')

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.



ils : Active Directory Group Recon

This operation will manage a IT Resour

Job Information

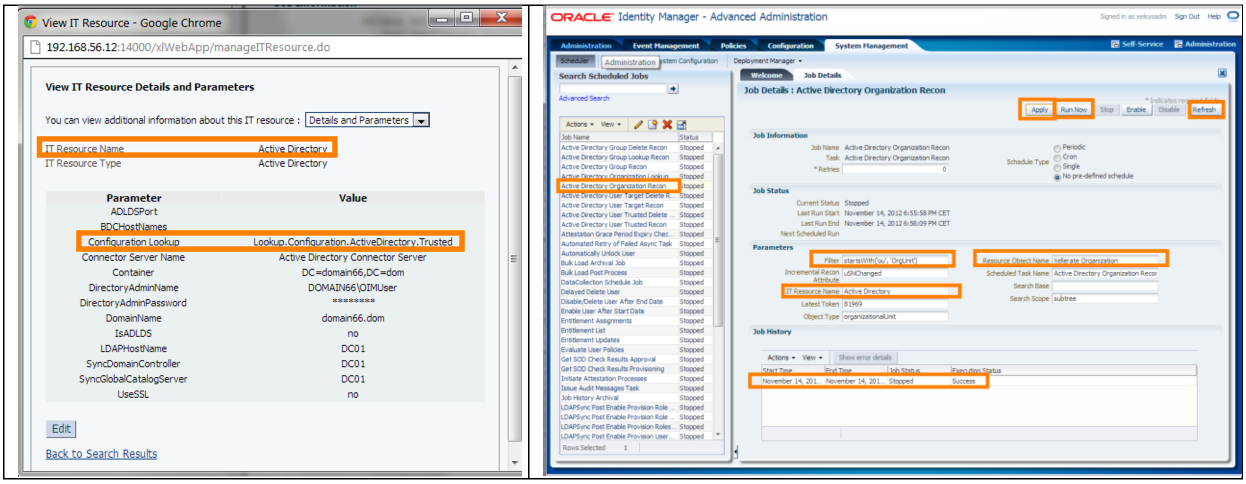
Job Name: Active Directory Group Re
Task: Active Directory Group Re
* Retries

Job Status

Current Status: Stopped
Last Run Start: November 6, 2012 4:19:4
Last Run End: November 6, 2012 4:19:4

Figure 42. **Opening the dialog to manage IT Resources in the OIM Console.**

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.



View IT Resource Details and Parameters

You can view additional information about this IT resource : Details and Parameters

IT Resource Name	Active Directory
IT Resource Type	Active Directory

Parameter	Value
ADLDSPort	
BDCHostNames	
Configuration Lookup	Lookup.Configuration.ActiveDirectory.Trusted
Connector Server Name	Active Directory Connector Server
Container	DC=domain66,DC=dom
DirectoryAdminName	DOMAIN66\OIMUser
DirectoryAdminPassword	********
DomainName	domain66.dom
IsADLDS	no
LDAPHostName	DC01
SyncDomainController	DC01
SyncGlobalCatalogServer	DC01
UseSSL	no

Search Scheduled Jobs

Job Name	Status
Active Directory Group Delete Recon	Stopped
Active Directory Group Lookup Recon	Stopped
Active Directory Group Recon	Stopped
Active Directory Organization Lookup	Stopped
Active Directory Organization Recon	Stopped
Active Directory User Target Delete R...	Stopped
Active Directory User Target Recon	Stopped
Active Directory User Trusted Delete ...	Stopped
Active Directory User Trusted Recon	Stopped
Attestation Grace Period Expiry Chec...	Stopped
Automated Retry of Failed Async Task	Stopped
Automatically Unlock User	Stopped
Bulk Load Archival Job	Stopped
Bulk Load Post Process	Stopped
DataCollection Schedule Job	Stopped
Delayed Delete User	Stopped
Disable/Delete User After End Date	Stopped
Enable User After Start Date	Stopped
Entitlement Assignments	Stopped
Entitlement List	Stopped
Entitlement Updates	Stopped
Evaluate User Policies	Stopped
Get SOD Check Results Approval	Stopped
Get SOD Check Results Provisioning	Stopped
Initiate Attestation Processes	Stopped
Issue Audit Messages Task	Stopped
Job History Archival	Stopped
LDAPSync Post Enable Provision Role ...	Stopped
LDAPSync Post Enable Provision Role ...	Stopped
LDAPSync Post Enable Provision Roles...	Stopped
LDAPSync Post Enable Provision User...	Stopped

Rows Selected 1

Job Details : Active Directory Organization Recon

Job Information
Job Name: Active Directory Organization Recon
Task: Active Directory Organization Recon
*Retries: 0
Schedule Type: ○ Periodic ○ Cron ○ Single ● No pre-defined schedule

Job Status
Current Status: Stopped
Last Run Start: November 14, 2012 6:55:58 PM CET
Last Run End: November 14, 2012 6:56:09 PM CET
Next Scheduled Run:

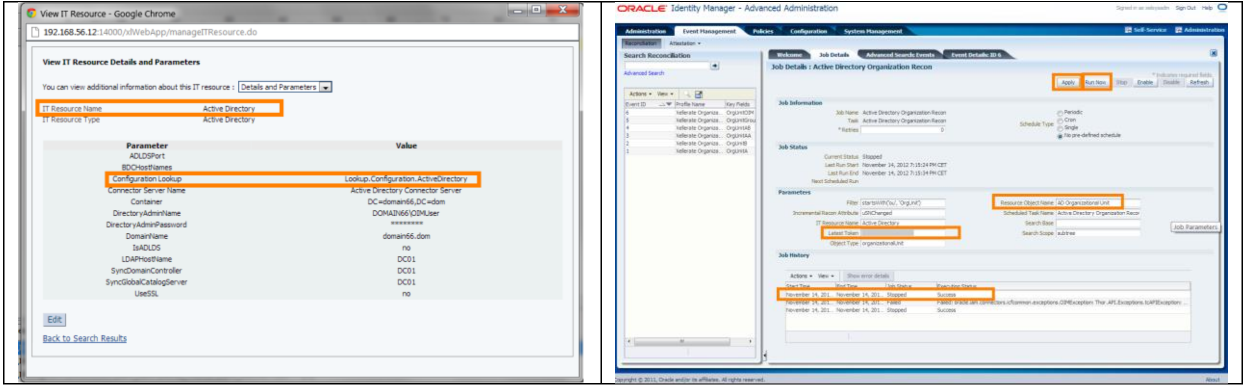
Parameters
Filter: startsWith('ou', 'OrgUnit')
Incremental Recon Attribute: uSNChanged
IT Resource Name: Active Directory
Latest Token: 81969
Object Type: organizationalUnit
Resource Object Name: Xellerate Organization
Scheduled Task Name: Active Directory Organization Recon
Search Base:
Search Scope: subtree

Job History

Start Time	End Time	Job Status	Execution Status
November 14, 201...	November 14, 201...	Stopped	Success

Figure 43. **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.



View IT Resource Details and Parameters

You can view additional information about this IT resource : Details and Parameters

IT Resource Name	Active Directory
IT Resource Type	Active Directory

Parameter	Value
ADLDSPort	
BDCHostNames	
Configuration Lookup	Lookup.Configuration.ActiveDirectory
Connector Server Name	Active Directory Connector Server
Container	DC=domain66,DC=dom
DirectoryAdminName	DOMAIN66\OIMUser
DirectoryAdminPassword	********
DomainName	domain66.dom
IsADLDS	no
LDAPHostName	DC01
SyncDomainController	DC01
SyncGlobalCatalogServer	DC01
UseSSL	no

Job Details : Active Directory Organization Recon

Job Information
Job Name: Active Directory Organization Recon
Task: Active Directory Organization Recon
*Retries: 0
Schedule Type: ○ Periodic ○ Cron ○ Single ● No pre-defined schedule

Job Status
Current Status: Stopped
Last Run Start: November 14, 2012 7:15:24 PM CET
Last Run End: November 14, 2012 7:15:34 PM CET
Next Scheduled Run:

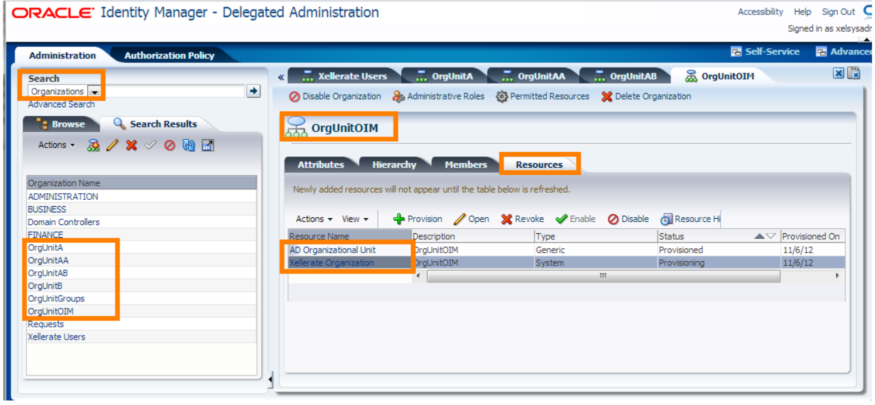
Parameters
Filter: startsWith('ou', 'OrgUnit')
Incremental Recon Attribute: uSNChanged
IT Resource Name: Active Directory
Latest Token:
Object Type: organizationalUnit
Resource Object Name: AD Organizational Unit
Scheduled Task Name: Active Directory Organization Recor
Search Base:
Search Scope: subtree

Job History

Start Time	End Time	Job Status	Execution Status
November 14, 201...	November 14, 201...	Stopped	Success
November 14, 201...	November 14, 201...	Failed	Failed: oracle.iam.connectors.icfcommon.exceptions.OIMException: Thor.API.Exceptions.tcAPIException: ...
November 14, 201...	November 14, 201...	Stopped	Success

Figure 1. **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.



Organization Name
ADMINISTRATION
BUSINESS
Domain Controllers
FINANCE
OrgUnitA
OrgUnitAA
OrgUnitAB
OrgUnitB
OrgUnitGroups
OrgUnitOIM
Requests
Xellerate Users

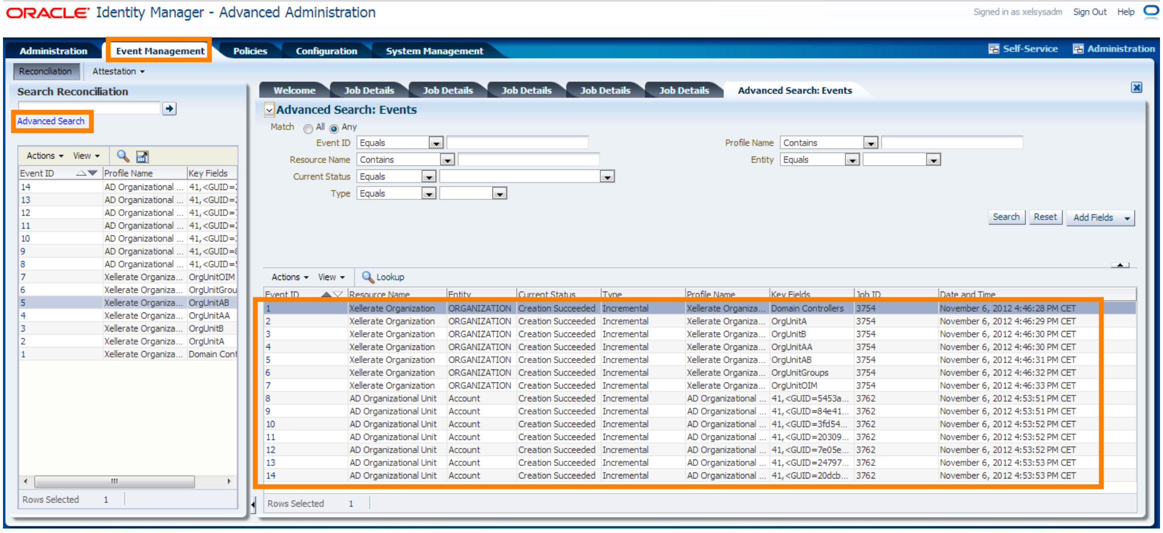
OrgUnitOIM

Newly added resources will not appear until the table below is refreshed.

Resource Name	Description	Type	Status	Provisioned On
AD Organizational Unit	OrgUnitOIM	Generic	Provisioned	11/6/12
Xellerate Organization	OrgUnitOIM	System	Provisioning	11/6/12

Figure 2. **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 where created with these two runs.



Search Reconciliation

Event ID	Profile Name	Key Fields
14	AD Organizational ...	41,<GUID=
13	AD Organizational ...	41,<GUID=
12	AD Organizational ...	41,<GUID=
11	AD Organizational ...	41,<GUID=
10	AD Organizational ...	41,<GUID=
9	AD Organizational ...	41,<GUID=
8	AD Organizational ...	41,<GUID=
7	Xellerate Organiza...	OrgUnitOIM
6	Xellerate Organiza...	OrgUnitGrou
5	Xellerate Organiza...	OrgUnitAB
4	Xellerate Organiza...	OrgUnitAA
3	Xellerate Organiza...	OrgUnitB
2	Xellerate Organiza...	OrgUnitA
1	Xellerate Organiza...	Domain Cont

Rows Selected 1

Advanced Search: Events

Match ○ All ● Any

Event ID	Equals	
Resource Name	Contains	
Current Status	Equals	
Type	Equals	
Profile Name	Contains	
Entity	Equals	

Event ID	Resource Name	Entity	Current Status	Type	Profile Name	Key Fields	Job ID	Date and Time
1	Xellerate Organization	ORGANIZATION	Creation Succeeded	Incremental	Xellerate Organiza...	Domain Controllers	3754	November 6, 2012 4:46:28 PM CET
2	Xellerate Organization	ORGANIZATION	Creation Succeeded	Incremental	Xellerate Organiza...	OrgUnitA	3754	November 6, 2012 4:46:29 PM CET
3	Xellerate Organization	ORGANIZATION	Creation Succeeded	Incremental	Xellerate Organiza...	OrgUnitB	3754	November 6, 2012 4:46:30 PM CET
4	Xellerate Organization	ORGANIZATION	Creation Succeeded	Incremental	Xellerate Organiza...	OrgUnitAA	3754	November 6, 2012 4:46:30 PM CET
5	Xellerate Organization	ORGANIZATION	Creation Succeeded	Incremental	Xellerate Organiza...	OrgUnitAB	3754	November 6, 2012 4:46:31 PM CET
6	Xellerate Organization	ORGANIZATION	Creation Succeeded	Incremental	Xellerate Organiza...	OrgUnitGroups	3754	November 6, 2012 4:46:32 PM CET
7	Xellerate Organization	ORGANIZATION	Creation Succeeded	Incremental	Xellerate Organiza...	OrgUnitOIM	3754	November 6, 2012 4:46:33 PM CET
8	AD Organizational Unit	Account	Creation Succeeded	Incremental	AD Organizational ...	41,<GUID=5453a...	3762	November 6, 2012 4:53:51 PM CET
9	AD Organizational Unit	Account	Creation Succeeded	Incremental	AD Organizational ...	41,<GUID=84e41...	3762	November 6, 2012 4:53:51 PM CET
10	AD Organizational Unit	Account	Creation Succeeded	Incremental	AD Organizational ...	41,<GUID=3fd54...	3762	November 6, 2012 4:53:52 PM CET
11	AD Organizational Unit	Account	Creation Succeeded	Incremental	AD Organizational ...	41,<GUID=20309...	3762	November 6, 2012 4:53:52 PM CET
12	AD Organizational Unit	Account	Creation Succeeded	Incremental	AD Organizational ...	41,<GUID=7e05e...	3762	November 6, 2012 4:53:52 PM CET
13	AD Organizational Unit	Account	Creation Succeeded	Incremental	AD Organizational ...	41,<GUID=24797...	3762	November 6, 2012 4:53:53 PM CET
14	AD Organizational Unit	Account	Creation Succeeded	Incremental	AD Organizational ...	41,<GUID=20dcb...	3762	November 6, 2012 4:53:53 PM CET

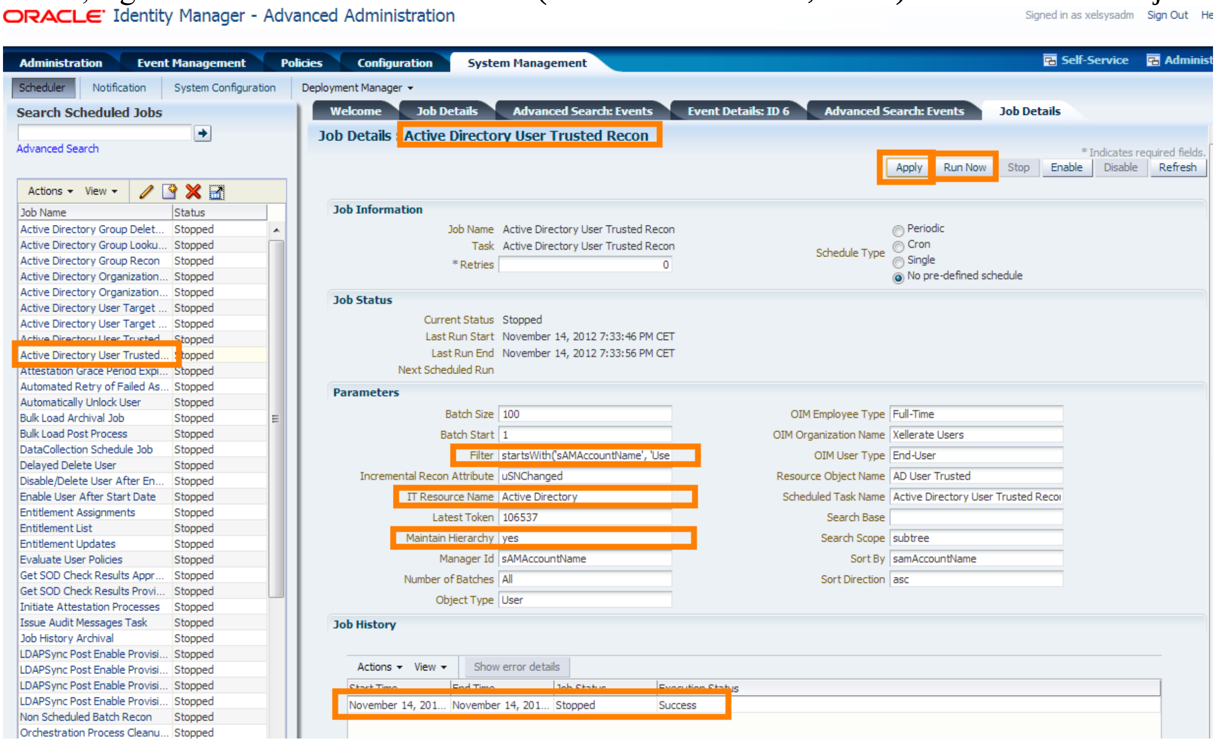
Rows Selected 1

Figure 3. **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 Diretory" 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.



Search Scheduled Jobs

Job Name	Status
Active Directory Group Delet...	Stopped
Active Directory Group Looku...	Stopped
Active Directory Group Recon	Stopped
Active Directory Organization...	Stopped
Active Directory Organization...	Stopped
Active Directory User Target ...	Stopped
Active Directory User Target ...	Stopped
Active Directory User Trusted ...	Stopped
Active Directory User Trusted...	Stopped
Attestation Grace Period Expi...	Stopped
Automated Retry of Failed As...	Stopped
Automatically Unlock User	Stopped
Bulk Load Archival Job	Stopped
Bulk Load Post Process	Stopped
DataCollection Schedule Job	Stopped
Delayed Delete User	Stopped
Disable/Delete User After En...	Stopped
Enable User After Start Date	Stopped
Entitlement Assignments	Stopped
Entitlement List	Stopped
Entitlement Updates	Stopped
Evaluate User Policies	Stopped
Get SOD Check Results Appr...	Stopped
Get SOD Check Results Provi...	Stopped
Initiate Attestation Processes	Stopped
Issue Audit Messages Task	Stopped
Job History Archival	Stopped
LDAPSync Post Enable Provisi...	Stopped
LDAPSync Post Enable Provisi...	Stopped
LDAPSync Post Enable Provisi...	Stopped
LDAPSync Post Enable Provisi...	Stopped
Non Scheduled Batch Recon	Stopped
Orchestration Process Cleanu...	Stopped

Job Details : Active Directory User Trusted Recon

* Indicates required fields.

Job Information

Job Name Active Directory User Trusted Recon
Task Active Directory User Trusted Recon
* Retries 0

Schedule Type ○ Periodic ○ Cron ○ Single ● No pre-defined schedule

Job Status

Current Status Stopped
Last Run Start November 14, 2012 7:33:46 PM CET
Last Run End November 14, 2012 7:33:56 PM CET
Next Scheduled Run

Parameters

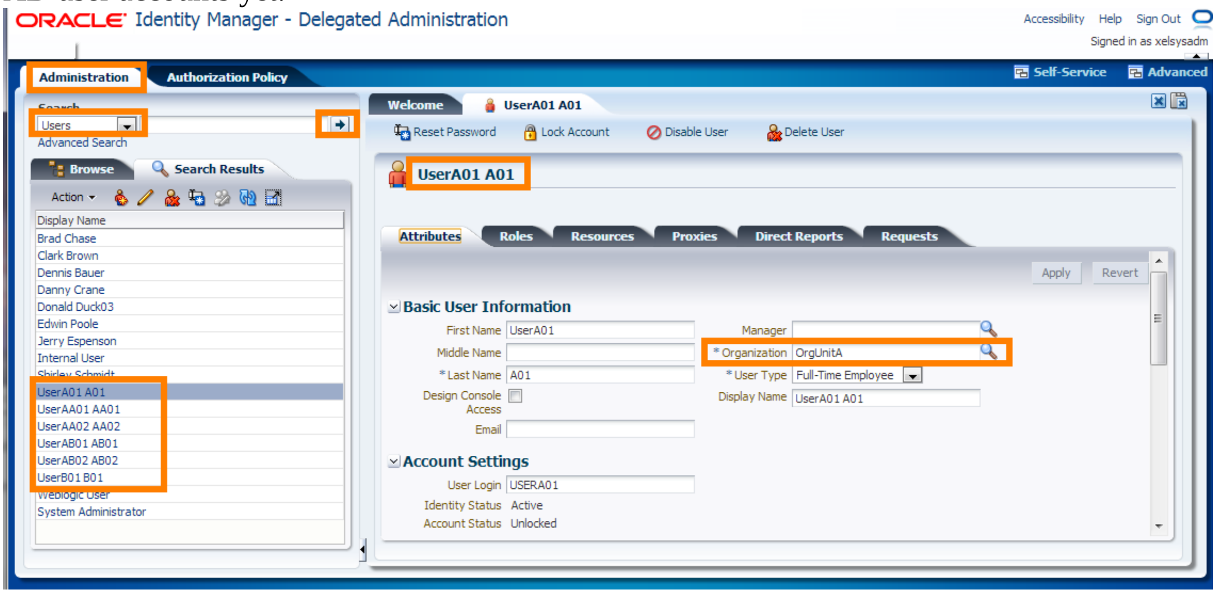
Batch Size	100	OIM Employee Type	Full-Time
Batch Start	1	OIM Organization Name	Xellerate Users
Filter	startsWith('sAMAccountName', 'Use	OIM User Type	End-User
Incremental Recon Attribute	uSNChanged	Resource Object Name	AD User Trusted
IT Resource Name	Active Directory	Scheduled Task Name	Active Directory User Trusted Recoı
Latest Token	106537	Search Base	
Maintain Hierarchy	yes	Search Scope	subtree
Manager Id	sAMAccountName	Sort By	samAccountName
Number of Batches	All	Sort Direction	asc
Object Type	User		

Job History

Start Time	End Time	Job Status	Execution Status
November 14, 201...	November 14, 201...	Stopped	Success

Figure 4. **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. The resources tab however is still empty, which means that these users are not connected to any AD user accounts yet.



Display Name
Brad Chase
Clark Brown
Dennis Bauer
Danny Crane
Donald Duck03
Edwin Poole
Jerry Espenson
Internal User
Shirley Schmidt
UserA01 A01
UserAA01 AA01
UserAA02 AA02
UserAB01 AB01
UserAB02 AB02
UserB01 B01
Weblogic User
System Administrator

UserA01 A01

Basic User Information

First Name	UserA01	Manager	
Middle Name		* Organization	OrgUnitA
* Last Name	A01	* User Type	Full-Time Employee
Design Console Access	□	Display Name	UserA01 A01
Email			

Account Settings

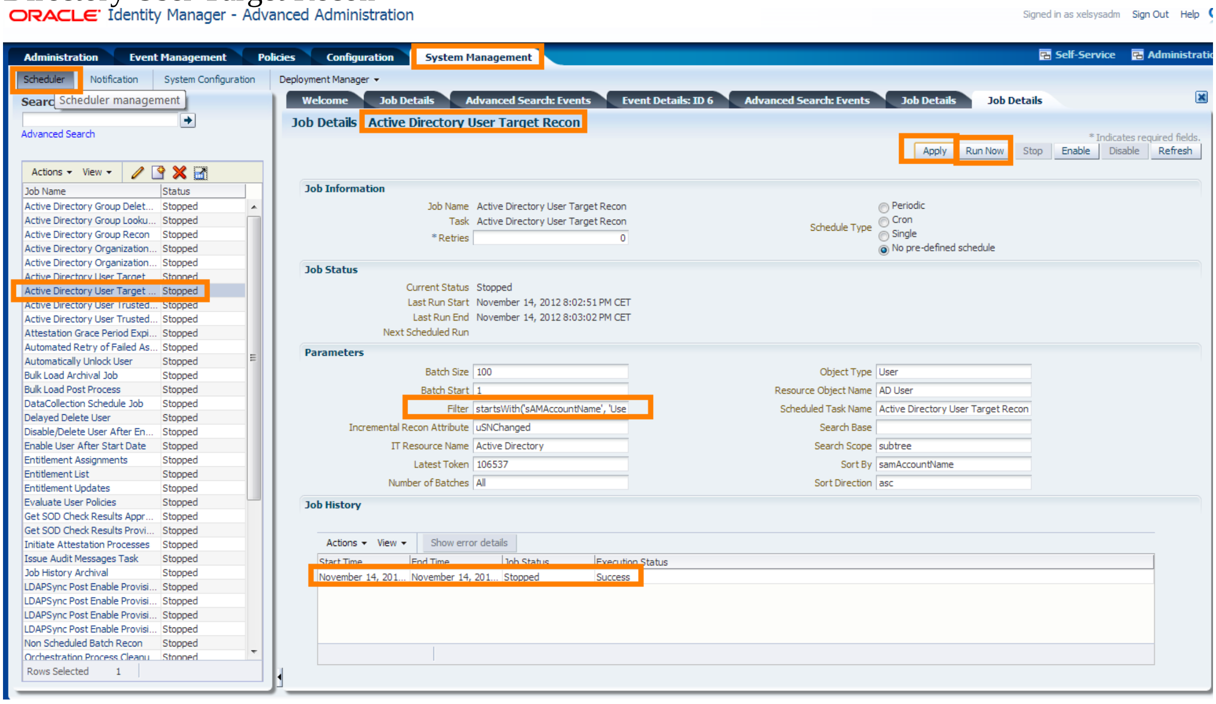
User Login	USERA01
Identity Status	Active
Account Status	Unlocked

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”



Job Name	Status
Active Directory Group Delet...	Stopped
Active Directory Group Looku...	Stopped
Active Directory Group Recon	Stopped
Active Directory Organization...	Stopped
Active Directory Organization...	Stopped
Active Directory User Target	Stopped
Active Directory User Target ...	Stopped
Active Directory User Trusted...	Stopped
Active Directory User Trusted...	Stopped
Attestation Grace Period Expi...	Stopped
Automated Retry of Failed As...	Stopped
Automatically Unlock User	Stopped
Bulk Load Archival Job	Stopped
Bulk Load Post Process	Stopped
DataCollection Schedule Job	Stopped
Delayed Delete User	Stopped
Disable/Delete User After En...	Stopped
Enable User After Start Date	Stopped
Entitlement Assignments	Stopped
Entitlement List	Stopped
Entitlement Updates	Stopped
Evaluate User Policies	Stopped
Get SOD Check Results Appr...	Stopped
Get SOD Check Results Provi...	Stopped
Initiate Attestation Processes	Stopped
Issue Audit Messages Task	Stopped
Job History Archival	Stopped
LDAPSync Post Enable Provisi...	Stopped
LDAPSync Post Enable Provisi...	Stopped
LDAPSync Post Enable Provisi...	Stopped
LDAPSync Post Enable Provisi...	Stopped
Non Scheduled Batch Recon	Stopped
Orchestration Process Cleanu...	Stopped

Rows Selected 1

Job Details Active Directory User Target Recon

Job Information

Job Name	Active Directory User Target Recon	Schedule Type	○ Periodic ○ Cron ○ Single ● No pre-defined schedule
Task	Active Directory User Target Recon		
* Retries	0		

Job Status

Current Status	Stopped
Last Run Start	November 14, 2012 8:02:51 PM CET
Last Run End	November 14, 2012 8:03:02 PM CET
Next Scheduled Run	

Parameters

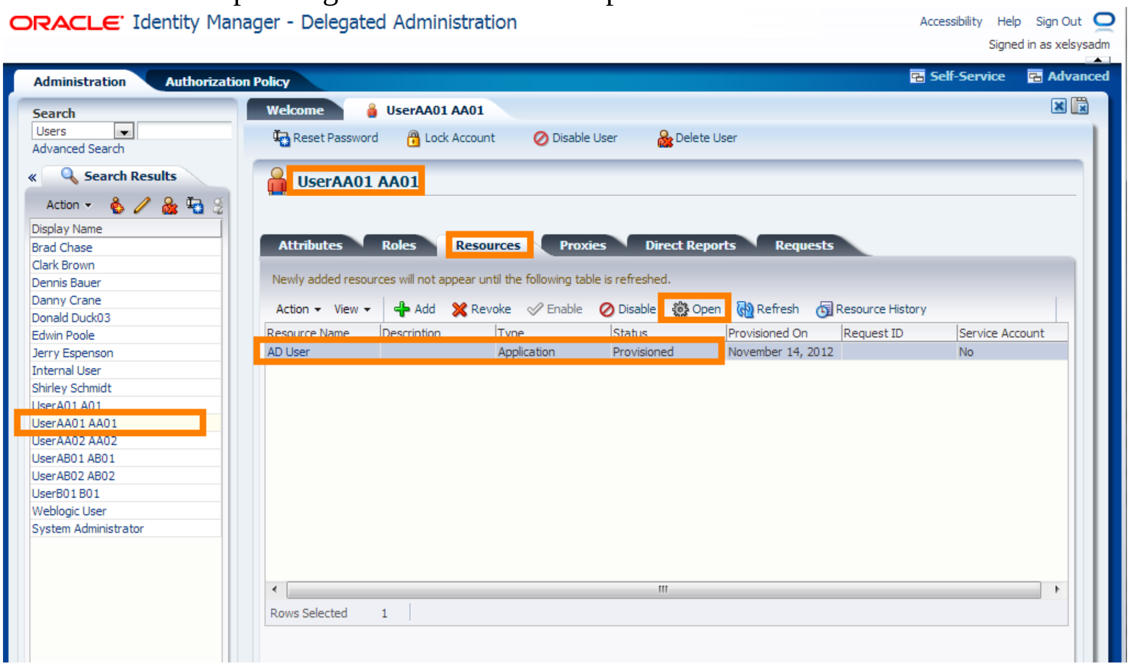
Batch Size	100	Object Type	User
Batch Start	1	Resource Object Name	AD User
Filter	startsWith('sAMAccountName', 'Use	Scheduled Task Name	Active Directory User Target Recon
Incremental Recon Attribute	uSNChanged	Search Base	
IT Resource Name	Active Directory	Search Scope	subtree
Latest Token	106537	Sort By	samAccountName
Number of Batches	All	Sort Direction	asc

Job History

Start Time	End Time	Job Status	Execution Status
November 14, 201...	November 14, 201...	Stopped	Success

Figure 6. **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.



ORACLE Identity Manager - Delegated Administration

Signed in as xelsysadm

Search: Users

Display Name: Brad Chase, Clark Brown, Dennis Bauer, Danny Crane, Donald Duck03, Edwin Poole, Jerry Espenson, Internal User, Shirley Schmidt, UserA01 A01, UserAA01 AA01, UserAA02 AA02, UserAB01 AB01, UserAB02 AB02, UserB01 B01, Weblogic User, System Administrator

UserAA01 AA01

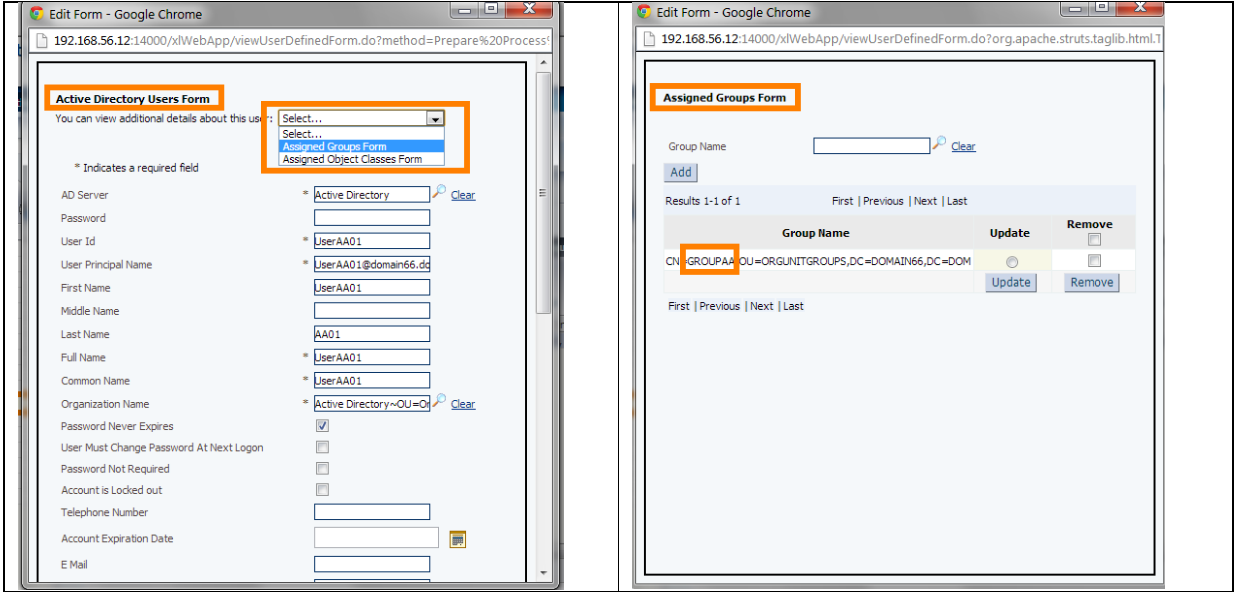
Newly added resources will not appear until the following table is refreshed.

Resource Name	Description	Type	Status	Provisioned On	Request ID	Service Account
AD User		Application	Provisioned	November 14, 2012		No

Rows Selected 1

Figure 7. **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.



Edit Form - Google Chrome

192.168.56.12:14000/xlWebApp/viewUserDefinedForm.do?method=Prepare%20Process

Active Directory Users Form

You can view additional details about this us: Select...

Select...
Assigned Groups Form
Assigned Object Classes Form

* Indicates a required field

AD Server *	Active Directory
Password	
User Id *	UserAA01
User Principal Name *	UserAA01@domain66.dc
First Name	UserAA01
Middle Name	
Last Name	AA01
Full Name *	UserAA01
Common Name *	UserAA01
Organization Name *	Active Directory~OU=Or
Password Never Expires	☑
User Must Change Password At Next Logon	□
Password Not Required	□
Account is Locked out	□
Telephone Number	
Account Expiration Date	
E Mail	

Edit Form - Google Chrome

192.168.56.12:14000/xlWebApp/viewUserDefinedForm.do?org.apache.struts.taglib.html.T

Assigned Groups Form

Group Name

Results 1-1 of 1

Group Name	Update	Remove □
CN=GROUPAA OU=ORGUNITGROUPS,DC=DOMAIN66,DC=DOM	○	□

Figure 8. **“AD Users Form” and “Assigned Groups Form” showing the details of the provisioned users account.**

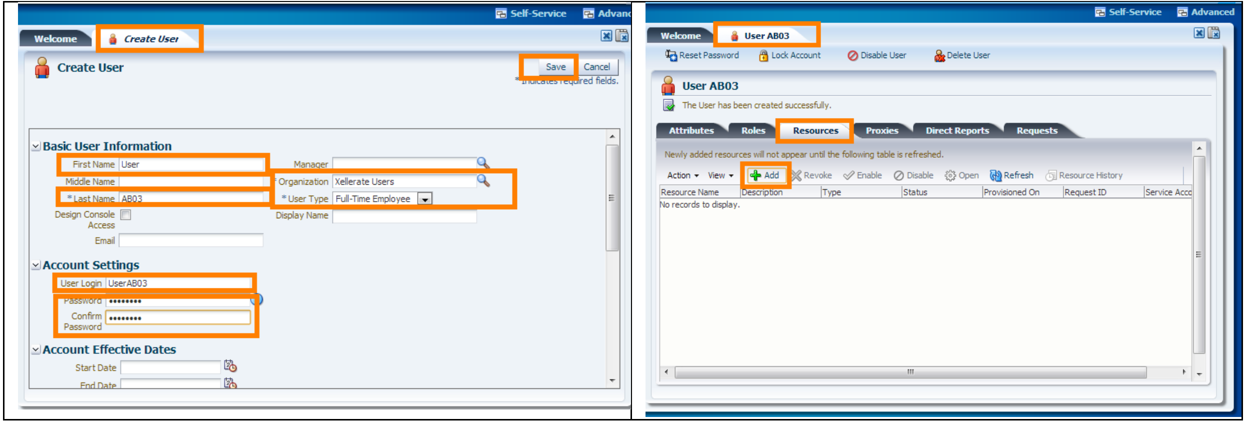
If we would change some of these attributes in the “AD Users Form” or in the Active Directory directly, this would be reconciled by the next run of the scheduled job. Further tests reveal that the job "AD User Target Recon" updates attributes of this resource in both directions, depending on the newer 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".



Create User

* Indicates required fields.

Basic User Information

First Name: User
Middle Name:
* Last Name: AB03
Design Console Access: □
Email:
Manager:
* Organization: Xellerate Users
* User Type: Full-Time Employee
Display Name:

Account Settings

User Login: UserAB03
Password: ••••••••
Confirm Password: ••••••••

Account Effective Dates

Start Date:
End Date:

User AB03

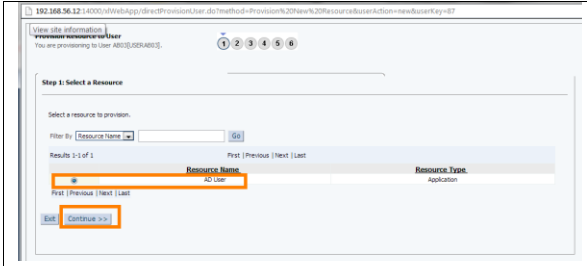
The User has been created successfully.

Newly added resources will not appear until the following table is refreshed.

Resource Name	Description	Type	Status	Provisioned On	Request ID	Service Acco
No records to display.						

Figure 9. **Creating a new user in OIM and starting the resource provisioning.**

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.



192.168.56.12:14000/xlWebApp/directProvisionUser.do?method=Provision%20New%20Resource&userAction=new&userKey=87

Provision Resource to User
You are provisioning to User AB03[USERAB03].

Step 1: Select a Resource

Select a resource to provision.

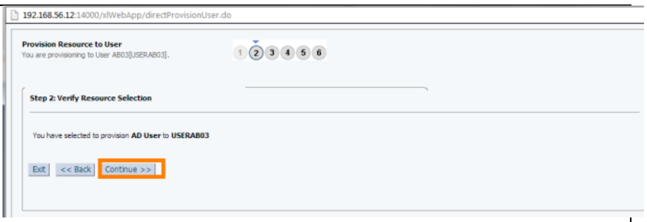
Filter By: Resource Name

Results 1-1 of 1 First | Previous | Next | Last

	Resource Name	Resource Type
●	AD User	Application

First | Previous | Next | Last

We select the Resource.



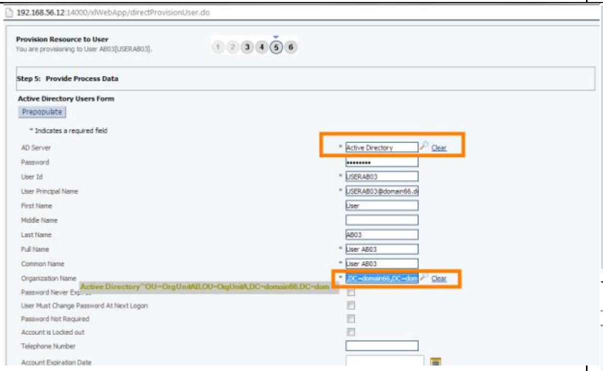
192.168.56.12:14000/xlWebApp/directProvisionUser.do

Provision Resource to User
You are provisioning to User AB03[USERAB03].

Step 2: Verify Resource Selection

You have selected to provision **AD User** to **USERAB03**

We check the confirmation page.



192.168.56.12:14000/xlWebApp/directProvisionUser.do

Provision Resource to User
You are provisioning to User AB03[USERAB03].

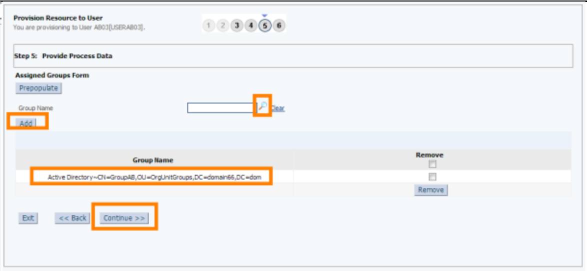
Step 5: Provide Process Data

Active Directory Users Form

* Indicates a required field

AD Server: * Active Directory
Password: ••••••••
User Id: * USERAB03
User Principal Name: * USERAB03@domain66.d
First Name: User
Middle Name:
Last Name: AB03
Full Name: * User AB03
Common Name: * User AB03
Organization Name: * ,DC=domain66,DC=dom
Active Directory~OU=OrgUnitAB,OU=OrgUnitA,DC=domain66,DC=dom
Password Never Expires: □
User Must Change Password At Next Logon: □
Password Not Required: □
Account is Locked out: □
Telephone Number:
Account Expiration Date:

We provide additonal values and choose the OrgUnit.



Provision Resource to User
You are provisioning to User AB03[USERAB03].

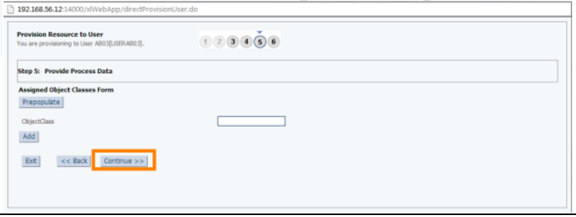
Step 5: Provide Process Data

Assigned Groups Form

Group Name:

Group Name	Remove □
Active Directory~CN=GroupAB,OU=OrgUnitGroups,DC=domain66,DC=dom	□

We add the membership to GroupAB



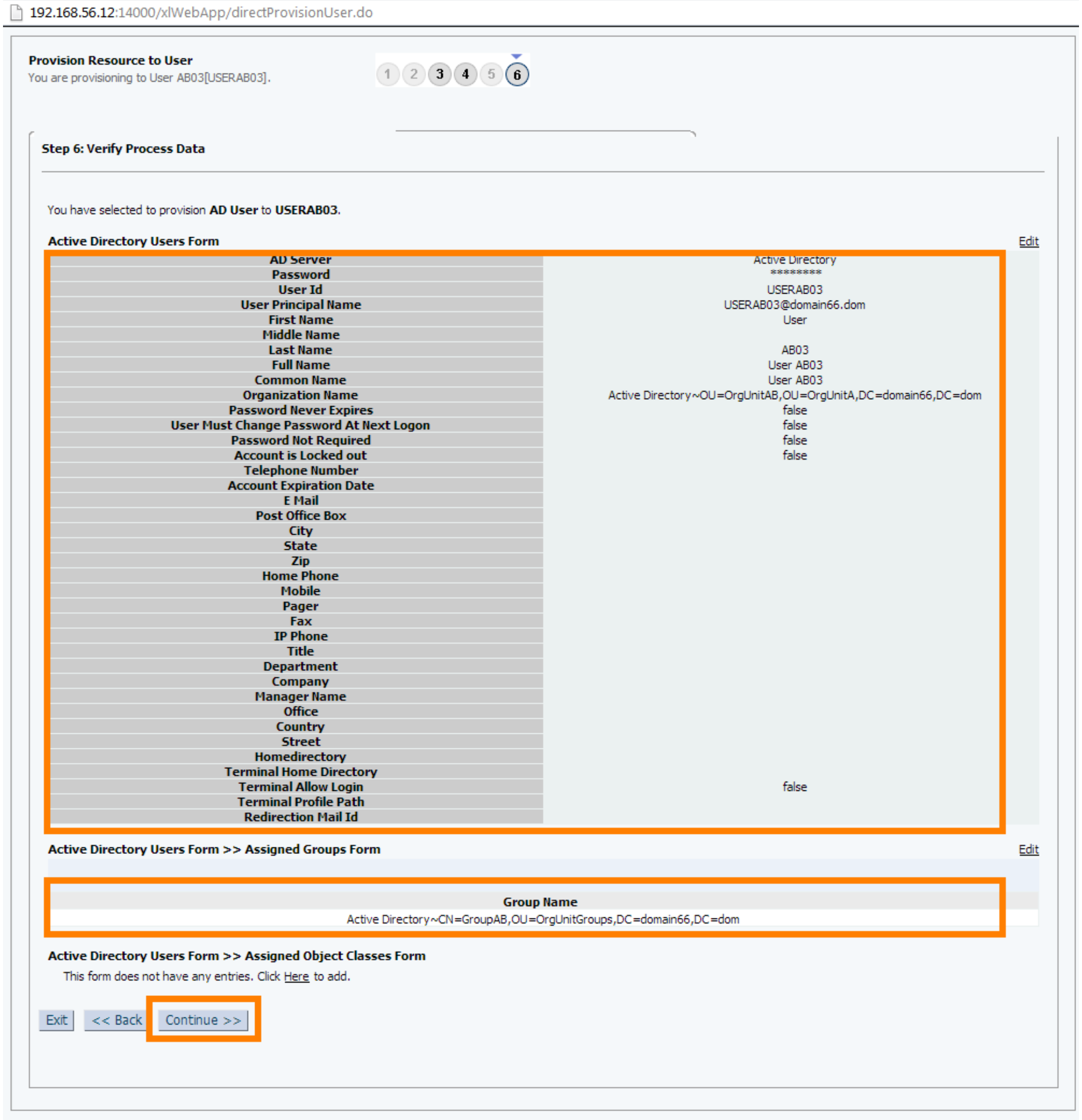
192.168.56.12:14000/xlWebApp/directProvisionUser.do

Provision Resource to User
You are provisioning to User AB03[USERAB03].

Step 5: Provide Process Data

Assigned Object Classes Form

ObjectClass:



Provision Resource to User

You are provisioning to User AB03[USERAB03].

Step 6: Verify Process Data

You have selected to provision **AD User** to **USERAB03**.

Active Directory Users Form

AD Server	Active Directory
Password	********
User Id	USERAB03
User Principal Name	USERAB03@domain66.dom
First Name	User
Middle Name	
Last Name	AB03
Full Name	User AB03
Common Name	User AB03
Organization Name	Active Directory~OU=OrgUnitAB,OU=OrgUnitA,DC=domain66,DC=dom
Password Never Expires	false
User Must Change Password At Next Logon	false
Password Not Required	false
Account is Locked out	false
Telephone Number	
Account Expiration Date	
E Mail	
Post Office Box	
City	
State	
Zip	
Home Phone	
Mobile	
Pager	
Fax	
IP Phone	
Title	
Department	
Company	
Manager Name	
Office	
Country	
Street	
Homedirectory	
Terminal Home Directory	
Terminal Allow Login	false
Terminal Profile Path	
Redirection Mail Id	

Active Directory Users Form >> Assigned Groups Form

Group Name
Active Directory~CN=GroupAB,OU=OrgUnitGroups,DC=domain66,DC=dom

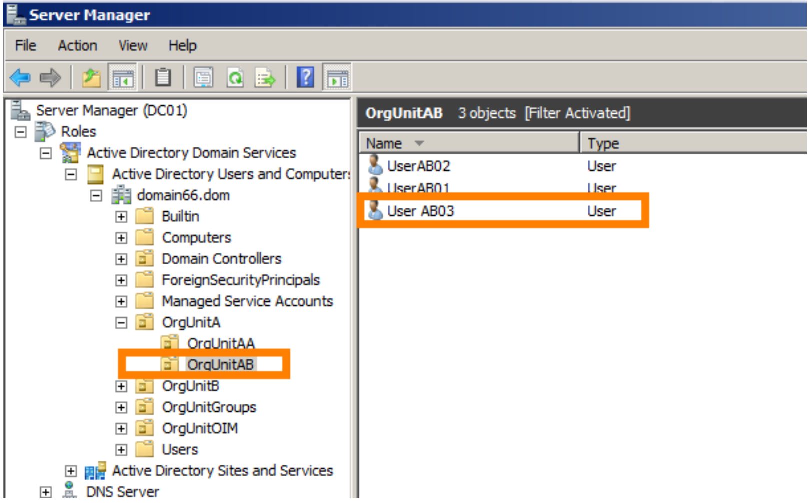
Active Directory Users Form >> Assigned Object Classes Form

This form does not have any entries. Click Here to add.

We ceck the summary and provision the account.

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

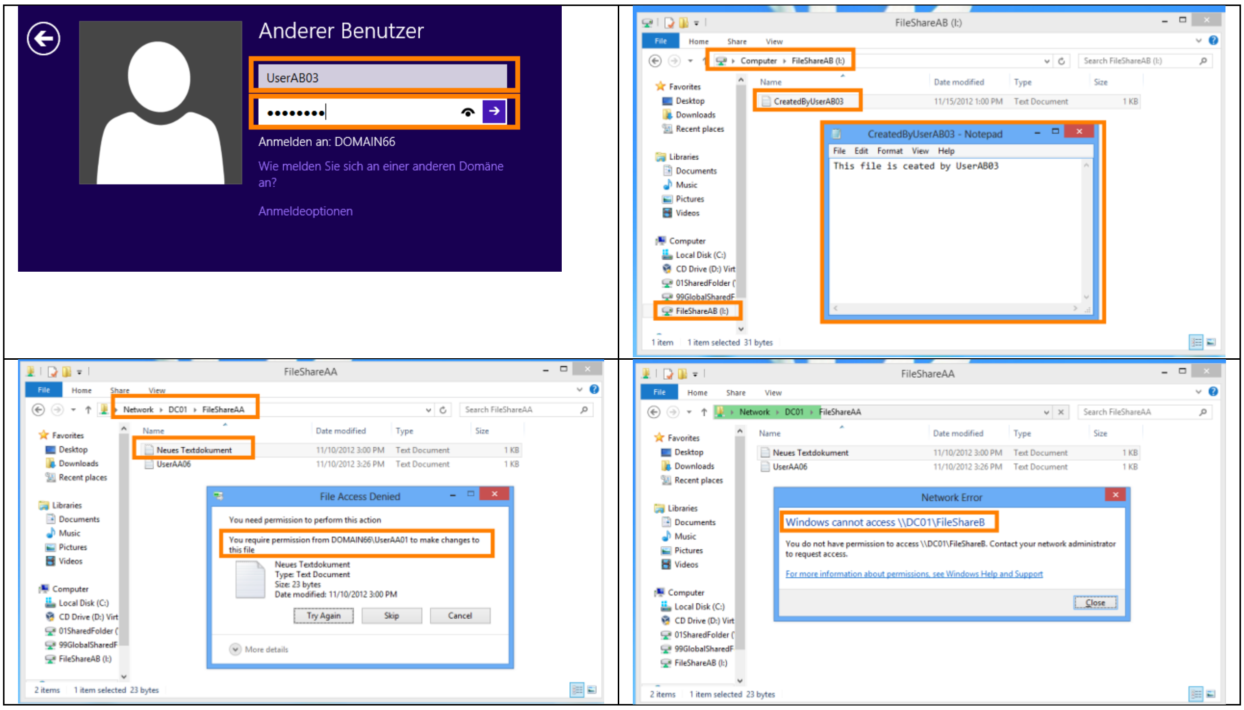
We provide the basic user information, the organization and group assignments and create the user. The summary page displays all attributes that can be set in the users form. Note that the dialog skips step 3 and 4. If we check the Active Directory in the Server Manager of Windows 2008, we find the UserAB03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



Name	Type
UserAB02	User
UserAB01	User
User AB03	User

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.



Anderer Benutzer

UserAB03

••••••••

Anmelden an: DOMAIN66

Wie melden Sie sich an einer anderen Domäne an?

Anmeldeoptionen

FileShareAB (I:)

Computer ▸ FileShareAB (I:)

Name	Date modified	Type	Size
CreatedByUserAB03	11/15/2012 1:00 PM	Text Document	1 KB

CreatedByUserAB03 - Notepad

```
This file is ceated by UserAB03
```

1 item 1 item selected 31 bytes

FileShareAA

Network ▸ DC01 ▸ FileShareAA

Name	Date modified	Type	Size
Neues Textdokument	11/10/2012 3:00 PM	Text Document	1 KB
UserAA06	11/10/2012 3:26 PM	Text Document	1 KB

File Access Denied

You need permission to perform this action

You require permission from DOMAIN66\UserAA01 to make changes to this file

Neues Textdokument
Type: Text Document
Size: 23 bytes
Date modified: 11/10/2012 3:00 PM

Network Error

Windows cannot access \\DC01\FileShareB

You do not have permission to access \\DC01\FileShareB. Contact your network administrator to request access.

For more information about permissions, see Windows Help and Support

2 items 1 item selected 23 bytes

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

Link	http://www.microsoft.com/de-de/download/details.aspx?id=19994
File	D:\01Downloads\7601.17514.101119-1850_x64fre_server_eval_de-de-GRMSXEVAL_DE_DVD.iso
MD5	e2508890839735dcfce216d17eefae2e (unknown by Google)
Notes	The evaluation periode is 180 days, starting from 18.10.2012.

7.2 Windows Server 2008 R2 Service Pack 1 User Interface Language Packs (EN)

Link	http://www.microsoft.com/en-us/download/details.aspx?id=2634
File	D:\01Downloads\Windows6.1-KB2483139-x64-en-US.exe
MD5	f70b8ca16eb79240bdf14d2fb9ff3f4e
Notes	

7.3 Connector Server 11.1.1.5.0

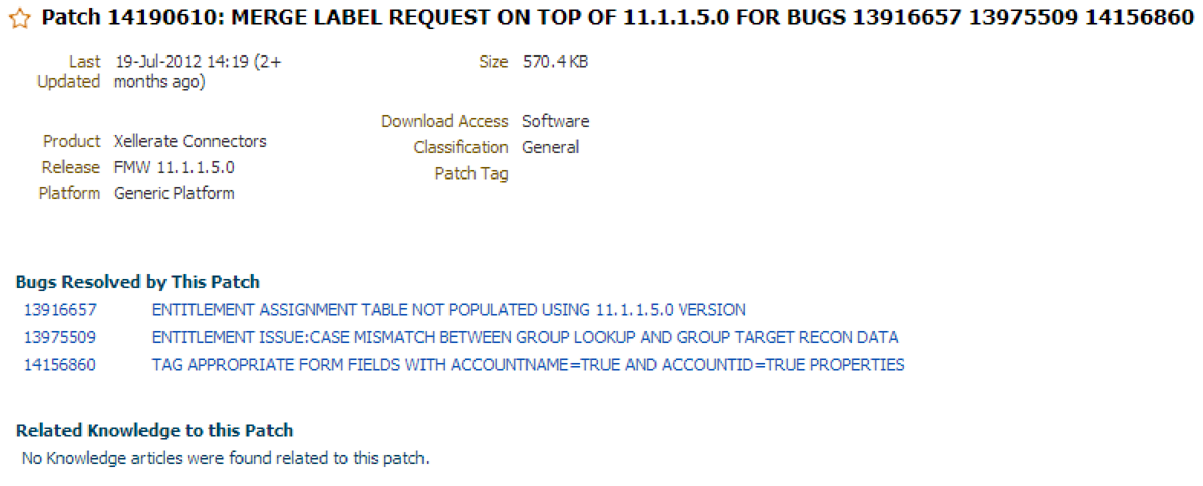
Link	http://www.oracle.com/technetwork/middleware/id-mgmt/downloads/connectors-101674.html
File	D:\01Downloads\Connector_Server_111150.zip
MD5	258675d766210b0924aa9ab09e111542 (unknown by Google)
Notes	

7.4 Oracle Identity Manager Connector MS AD User Management 11.1.1.5.0

Link	http://www.oracle.com/technetwork/middleware/id-mgmt/downloads/connectors-101674.html
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 Connetctor Patch 14190610: MERGE LABEL REQUEST ON TOP OF 11.1.1.5.0

Link	https://support.oracle.com/epmos/faces/PatchResultsNDetails?_adf.ctrl-state=vf360o47f_9&releaseId=17111150&requestId=15273691&patchId=14190610&languageId=0&platformId=2000&_afrLoop=457977425119592
File	D:\01Downloads\p14190610_111150_Generic.zip
MD5	e99896bc093ee3d301c6cd6156e5e3cd
Notes	MD5 from Website MD5 E99896BC093EE3D301C6CD6156E5E3CD matches, Ok.



☆ **Patch 14190610: MERGE LABEL REQUEST ON TOP OF 11.1.1.5.0 FOR BUGS 13916657 13975509 14156860**

Last Updated 19-Jul-2012 14:19 (2+ months ago)
Size 570.4 KB

Download Access Software
Product Xellerate Connectors
Classification General
Release FMW 11.1.1.5.0
Patch Tag
Platform Generic Platform

Bugs Resolved by This Patch

13916657	ENTITLEMENT ASSIGNMENT TABLE NOT POPULATED USING 11.1.1.5.0 VERSION
13975509	ENTITLEMENT ISSUE:CASE MISMATCH BETWEEN GROUP LOOKUP AND GROUP TARGET RECON DATA
14156860	TAG APPROPRIATE FORM FIELDS WITH ACCOUNTNAME=TRUE AND ACCOUNTID=TRUE PROPERTIES

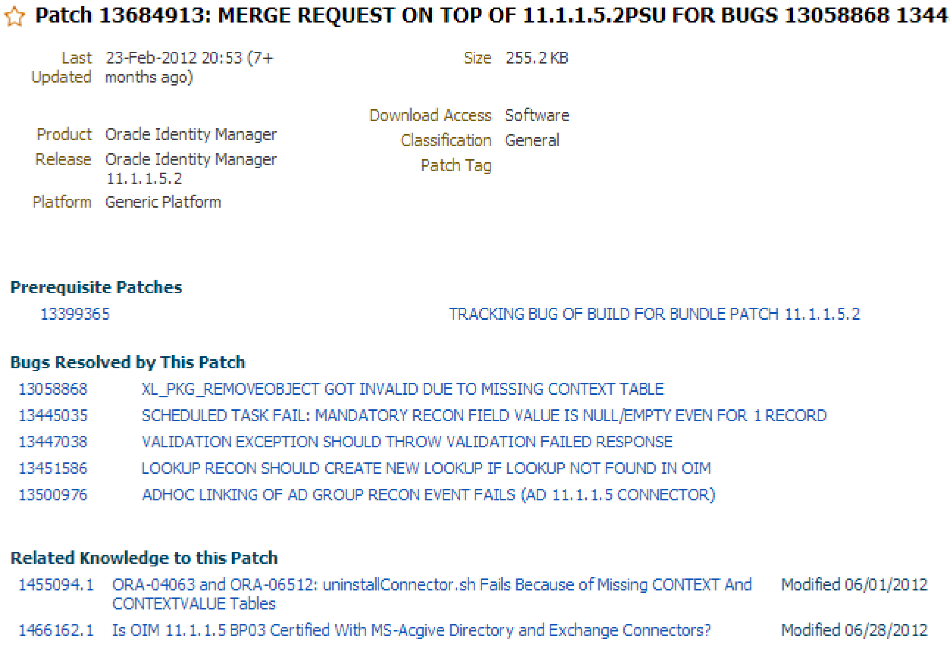
Related Knowledge to this Patch

No Knowledge articles were found related to this patch.

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=vf360o47f_9&releaseId=19800111152&requestId=14605415&patchId=13684913&languageId=0&platformId=2000&_afrLoop=458761440548960
File D:\01Downloads\p13684913_111152_Generic.zip
MD5 8f89313c6355ecab71fc408a6ba50192
Notes MD5 8F89313C6355ECAB71FC408A6BA50192 from oracle website matches, ok.



☆ **Patch 13684913: MERGE REQUEST ON TOP OF 11.1.1.5.2PSU FOR BUGS 13058868 13445035 13447038**

Last Updated 23-Feb-2012 20:53 (7+ months ago)
Size 255.2 KB

Product Oracle Identity Manager
Release Oracle Identity Manager 11.1.1.5.2
Platform Generic Platform
Download Access Software
Classification General
Patch Tag

Prerequisite Patches

13399365	TRACKING BUG OF BUILD FOR BUNDLE PATCH 11.1.1.5.2

Bugs Resolved by This Patch

13058868	XL_PKG_REMOVEOBJECT GOT INVALID DUE TO MISSING CONTEXT TABLE
13445035	SCHEDULED TASK FAIL: MANDATORY RECON FIELD VALUE IS NULL/EMPTY EVEN FOR 1 RECORD
13447038	VALIDATION EXCEPTION SHOULD THROW VALIDATION FAILED RESPONSE
13451586	LOOKUP RECON SHOULD CREATE NEW LOOKUP IF LOOKUP NOT FOUND IN OIM
13500976	ADHOC LINKING OF AD GROUP RECON EVENT FAILS (AD 11.1.1.5 CONNECTOR)

Related Knowledge to this Patch

1455094.1	ORA-04063 and ORA-06512: uninstallConnector.sh Fails Because of Missing CONTEXT And CONTEXTVALUE Tables	Modified 06/01/2012
1466162.1	Is OIM 11.1.1.5 BP03 Certified With MS-Acgive Directory and Exchange Connectors?	Modified 06/28/2012

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.

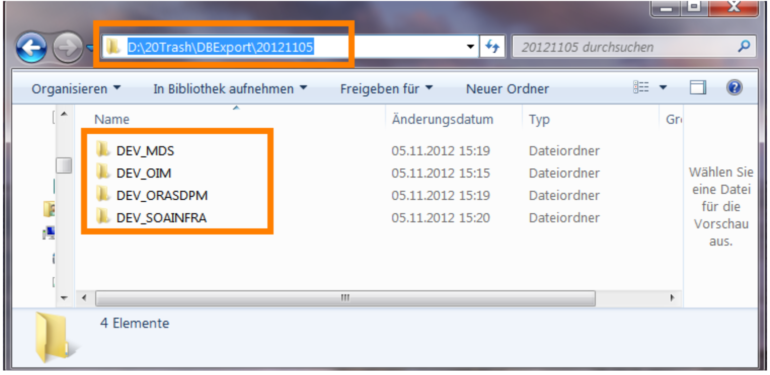
8.1 AD Connector Modes

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.

Operation modes	Identity Reconciliation	Account Management
Synonyms	trusted source reconciliation; authoritative source reconciliation	target resource management
Operations	trusted source reconciliation	Provisioning, Target resource reconciliation
Purpose	AD is the trusted source to create OIM Users, Groups and Oragnizations	OIM is the source to provision and update User accounts in AD
Lookup Definitions	Active Directory Group Lookup Recon Active Directory Organization Lookup Recon	
Scheduled Jobs for Groups		Active Directory Group Recon, Active Directory Group Delete Recon,
Scheduled Jobs for Organizations		Active Directory Organization Recon Active Directory Organization Delete Recon
Scheduled Jobs for Users	Active Directory User Trusted Recon, Active Directory User Trusted Delete Recon,	Active Directory User Target Recon, Active Directory User Target Delete Recon,

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 data base content into text files for analysis purposes.
We run 4 four exports and store the results in separate folders.



D:\20Trash\DBExport\20121105

20121105 durchsuchen

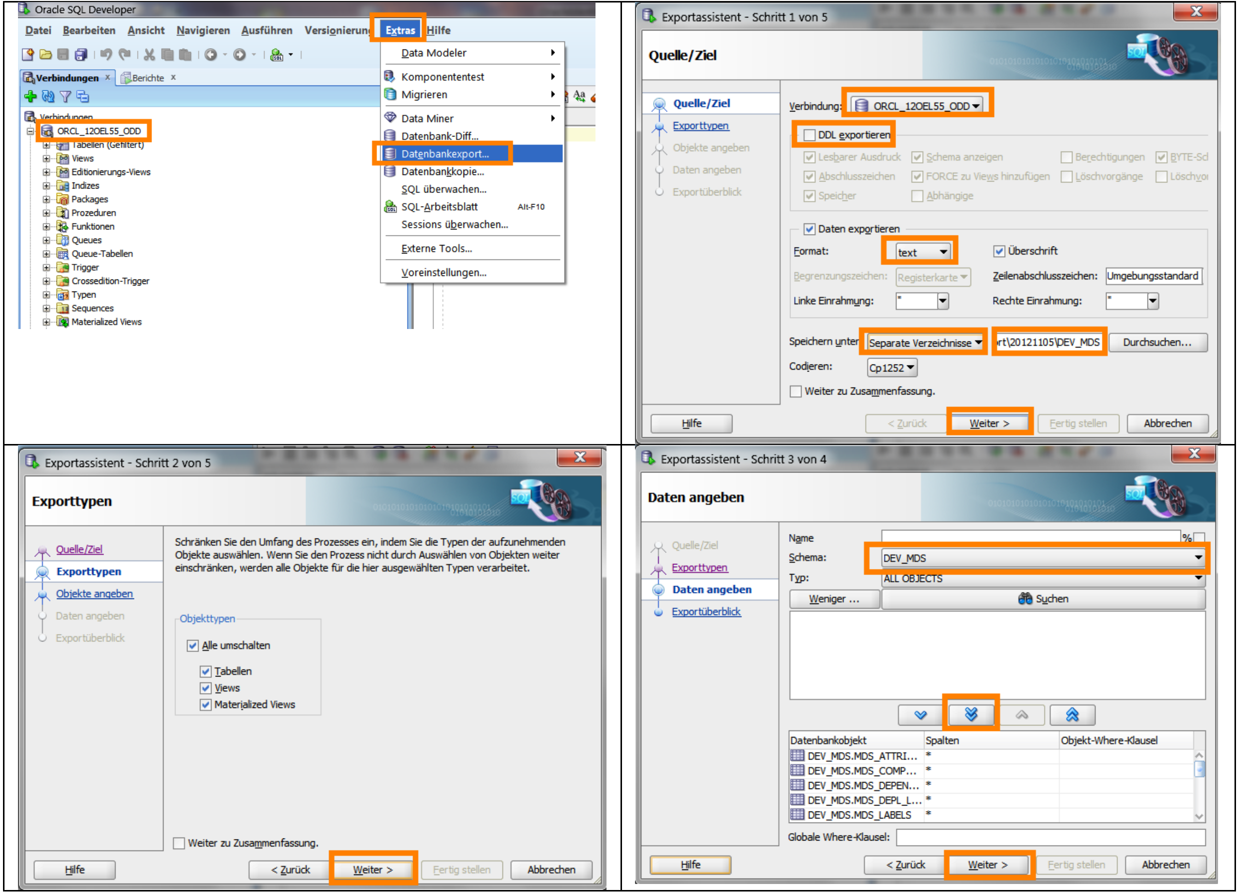
Name	Änderungsdatum	Typ
DEV_MDS	05.11.2012 15:19	Dateiordner
DEV_OIM	05.11.2012 15:15	Dateiordner
DEV_ORASDPM	05.11.2012 15:19	Dateiordner
DEV_SOAINFRA	05.11.2012 15:20	Dateiordner

Wählen Sie eine Datei für die Vorschau aus.

4 Elemente

Figure 15. **Separate folders for the Database export.**

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



Exportassistent - Schritt 1 von 5

Quelle/Ziel

Verbindung: ORCL_12OEL55_ODD

□ DDL exportieren

☑ Lesbarer Ausdruck ☑ Schema anzeigen □ Berechtigungen ☑ BYTE-Sd
☑ Abschlusszeichen ☑ FORCE zu Views hinzufügen □ Löschvorgänge □ Löschvor
☑ Speicher □ Abhängige

☑ Daten exportieren

Format: text ☑ Überschrift

Begrenzungszeichen: Registerkarte Zeilenabschlusszeichen: Umgebungsstandard

Linke Einrahmung: " Rechte Einrahmung: "

Speichern unter: Separate Verzeichnisse rt\20121105\DEV_MDS Durchsuchen...

Codieren: Cp1252

□ Weiter zu Zusammenfassung.

Exportassistent - Schritt 2 von 5

Exporttypen

Schränken Sie den Umfang des Prozesses ein, indem Sie die Typen der aufzunehmenden Objekte auswählen. Wenn Sie den Prozess nicht durch Auswählen von Objekten weiter einschränken, werden alle Objekte für die hier ausgewählten Typen verarbeitet.

Objekttypen

☑ Alle umschalten

☑ Tabellen
☑ Views
☑ Materialized Views

□ Weiter zu Zusammenfassung.

Exportassistent - Schritt 3 von 4

Daten angeben

Name: %

Schema: DEV_MDS

Typ: ALL OBJECTS

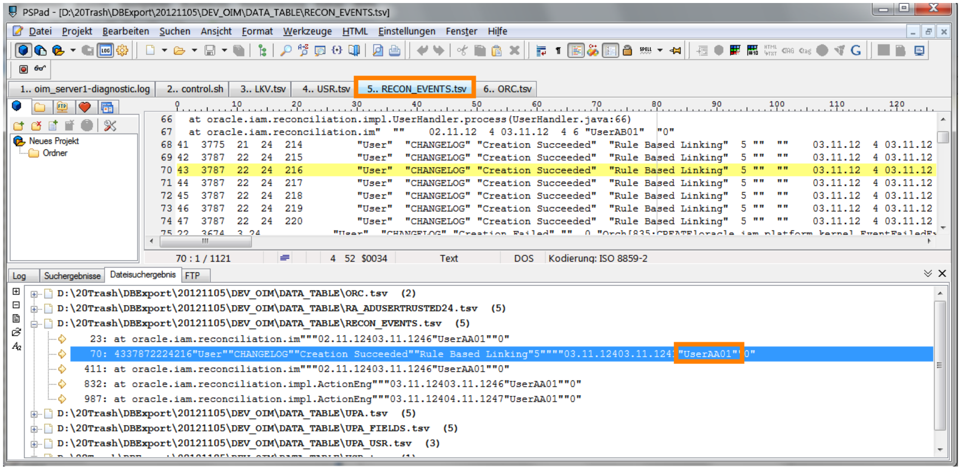
Datenbankobjekt	Spalten	Objekt-Where-Klausel
DEV_MDS.MDS_ATTRI...	*	
DEV_MDS.MDS_COMP...	*	
DEV_MDS.MDS_DEPEN...	*	
DEV_MDS.MDS_DEPL_L...	*	
DEV_MDS.MDS_LABELS	*	

Globale Where-Klausel:

Figure 16. **Exporting the data of the DEV_MDS Database Schema.**

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.


PSPad - [D:\20Trash\DBExport\20121105\DEV_OIM\DATA_TABLE\RECON_EVENTS.tsv]
Datei Projekt Bearbeiten Suchen Ansicht Format Werkzeuge HTML Einstellungen Fenster Hilfe
1.. oim_server1-diagnostic.log
2.. control.sh
3.. LKV.tsv
4.. USR.tsv
5.. RECON_EVENTS.tsv
6.. ORC.tsv
Neues Projekt
Ordner
Log
Suchergebnisse
Dateisuchergebnis
FTP

```
66  at oracle.iam.reconciliation.impl.UserHandler.process(UserHandler.java:66)
67  at oracle.iam.reconciliation.im"  ""    02.11.12  4 03.11.12  4 6 "UserAB01"  "0"
68 41  3775  21  24  214        "User"  "CHANGELOG" "Creation Succeeded"  "Rule Based Linking"  5 ""  ""   03.11.12  4 03.11.12
69 42  3787  22  24  215        "User"  "CHANGELOG" "Creation Succeeded"  "Rule Based Linking"  5 ""  ""   03.11.12  4 03.11.12
70 43  3787  22  24  216        "User"  "CHANGELOG" "Creation Succeeded"  "Rule Based Linking"  5 ""  ""   03.11.12  4 03.11.12
71 44  3787  22  24  217        "User"  "CHANGELOG" "Creation Succeeded"  "Rule Based Linking"  5 ""  ""   03.11.12  4 03.11.12
72 45  3787  22  24  218        "User"  "CHANGELOG" "Creation Succeeded"  "Rule Based Linking"  5 ""  ""   03.11.12  4 03.11.12
73 46  3787  22  24  219        "User"  "CHANGELOG" "Creation Succeeded"  "Rule Based Linking"  5 ""  ""   03.11.12  4 03.11.12
74 47  3787  22  24  220        "User"  "CHANGELOG" "Creation Succeeded"  "Rule Based Linking"  5 ""  ""   03.11.12  4 03.11.12
75 22  3674  3 24          "User"  "CHANGELOG" "Creation Failed" ""  0 "Orch[835:CREATEloracle.iam.platform.kernel.EventFailedEx

70 : 1 / 1121     4  52  $0034     Text     DOS   Kodierung: ISO 8859-2
```

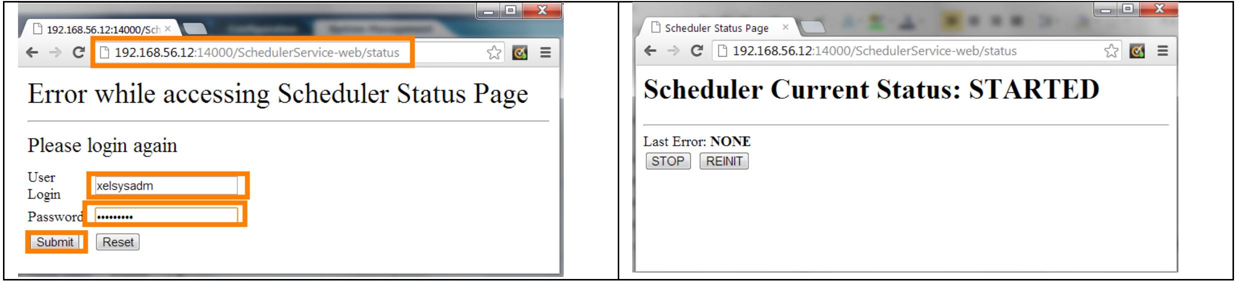
```
D:\20Trash\DBExport\20121105\DEV_OIM\DATA_TABLE\ORC.tsv  (2)
D:\20Trash\DBExport\20121105\DEV_OIM\DATA_TABLE\RA_ADUSERTRUSTED24.tsv  (5)
D:\20Trash\DBExport\20121105\DEV_OIM\DATA_TABLE\RECON_EVENTS.tsv  (5)
    23: at oracle.iam.reconciliation.im"""02.11.12403.11.1246"UserAA01""0"
    70: 4337872224216"User""CHANGELOG""Creation Succeeded""Rule Based Linking"5""""03.11.12403.11.124"UserAA01""0"
    411: at oracle.iam.reconciliation.im"""02.11.12403.11.1246"UserAA01""0"
    832: at oracle.iam.reconciliation.impl.ActionEng"""03.11.12403.11.1246"UserAA01""0"
    987: at oracle.iam.reconciliation.impl.ActionEng"""03.11.12404.11.1247"UserAA01""0"
D:\20Trash\DBExport\20121105\DEV_OIM\DATA_TABLE\UPA.tsv  (5)
D:\20Trash\DBExport\20121105\DEV_OIM\DATA_TABLE\UPA_FIELDS.tsv  (5)
D:\20Trash\DBExport\20121105\DEV_OIM\DATA_TABLE\UPA_USR.tsv  (3)
```

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


192.168.56.12:14000/Sch
192.168.56.12:14000/SchedulerService-web/status
Submit
Reset
Scheduler Status Page
192.168.56.12:14000/SchedulerService-web/status
STOP
REINIT

Error while accessing Scheduler Status Page

Please login again

User Login: xelsysadm

Password: ••••••••

Scheduler Current Status: STARTED

Last Error: NONE

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
Sicherheitspunkt3	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]# sh ./VBoxLinuxAdditions.run
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 DKMS kernel modules           [  OK  ]
Removing existing VirtualBox non-DKMS 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  ]
Setting up the Window System to use the Guest Additions    [  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 componen[  OK  ]
 [root@12oel55_odd VBOXADDITIONS_4.1.22_80657]#
```

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.