

ORACLE®

Интеграция Oracle Internet Directory с Microsoft Active Directory.

Игорь Лукьянов

Старший консультант
Oracle Application Server 10g

Использование интеграции - требования

Для успешной работы Вы должны быть знакомы с управлением инстанса инфраструктуры OAS 10G и иметь его прединсталлированным на одной из поддерживаемых аппаратных платформ и OS. Убедитесь, что инстанс Oracle Internet Directory стартован

Задачи интеграции

1. Конфигурирование профилирующего файла для импорта и интеграции
2. Миграция пользователей Active Directory к Oracle Internet Directory
3. Конфигурирование внешней аутентификации

Конфигурирование профайла для импорта

Положите тестовый профайл activechgimp.map в директорию \$ORACLE_HOME/ldap/odi/conf

Формат файла activechgimp.map:

```
DomainRules CN=Users,DC=ACME,DC=com:cn=Users,dc=ACME,dc=com
AttributeRules ou: : organizationalunit:ou: : organizationalunit objectguid:
:binary:organizationalunit:orclobjectguid: :
organizationalunit:bin2b64(ObjectGUID) cn: : container: cn: :orclContainer
objectguid: :binary:container: orclobjectguid:
:orclContainer:bin2b64(ObjectGUID) dc: : domain: dc: :domain
sAMAccountName,userPrincipalName: : user:orclSAMAccountName:
:orclADUser:toupper
(trunc1(userPrincipalName,'@'))+"$"+sAMAccountname userPrincipalName:
: :user:orclUserPrincipalName: :orclADUser:userPrincipalName
sAMAccountName: : :user:uid: :inetorgperson:sAMAccountName
userPrincipalName: : :user:krbPrincipalName:
```

Конфигурирование профайла для импорта

Формат файла activechgimp.map:

```
:orcluserV2:trunc(userPrincipalName,  
'@')+ '@'+toupper(trunc1(userPrincipalName,'@')) SAMAccountName: :user:sn: : person  
cn: : :person:cn: :person givenName: : :person:displayName: :orclUserV2  
userPrincipalName: : :user:mail: :inetorgperson ObjectGUID: :binary:user:orclObjectGUID:  
:orclADUser:bin2b64(ObjectGUID) ObjectSID: :binary:user:orclObjectSID:  
:orclADUser:bin2b64(ObjectSID) cn: : :group:cn: :groupofuniqueNames SAMAccountName:  
: :group:displayName: :orclgroup Description: : :group:Description: :orclgroup member: :  
:group:uniquemember: :groupofUniqueNames managedby: : :group:owner:  
:orclprivilegeGroup sAMAccountName: : :group:orclSAMAccountName: :orclADGroup  
ObjectGUID: :binary:group:orclObjectGUID: :orclADGroup:bin2b64(ObjectGUID)  
ObjectSID: :binary:group:orclObjectSID: :orclADGroup:bin2b64(ObjectSID) cn: :  
:group:orclisvisible: :orclgroup: 'true'
```

Конфигурирование профайла для импорта

Проверка Domain rules:

CN=Users,DC=acme,DC=com:cn=Users,dc=acme,dc=com

Слева Domain для Microsoft Active Directory

Справа Domain для Oracle Internet Directory

Конфигурирование профайла для импорта

Проверка Attribute rules:

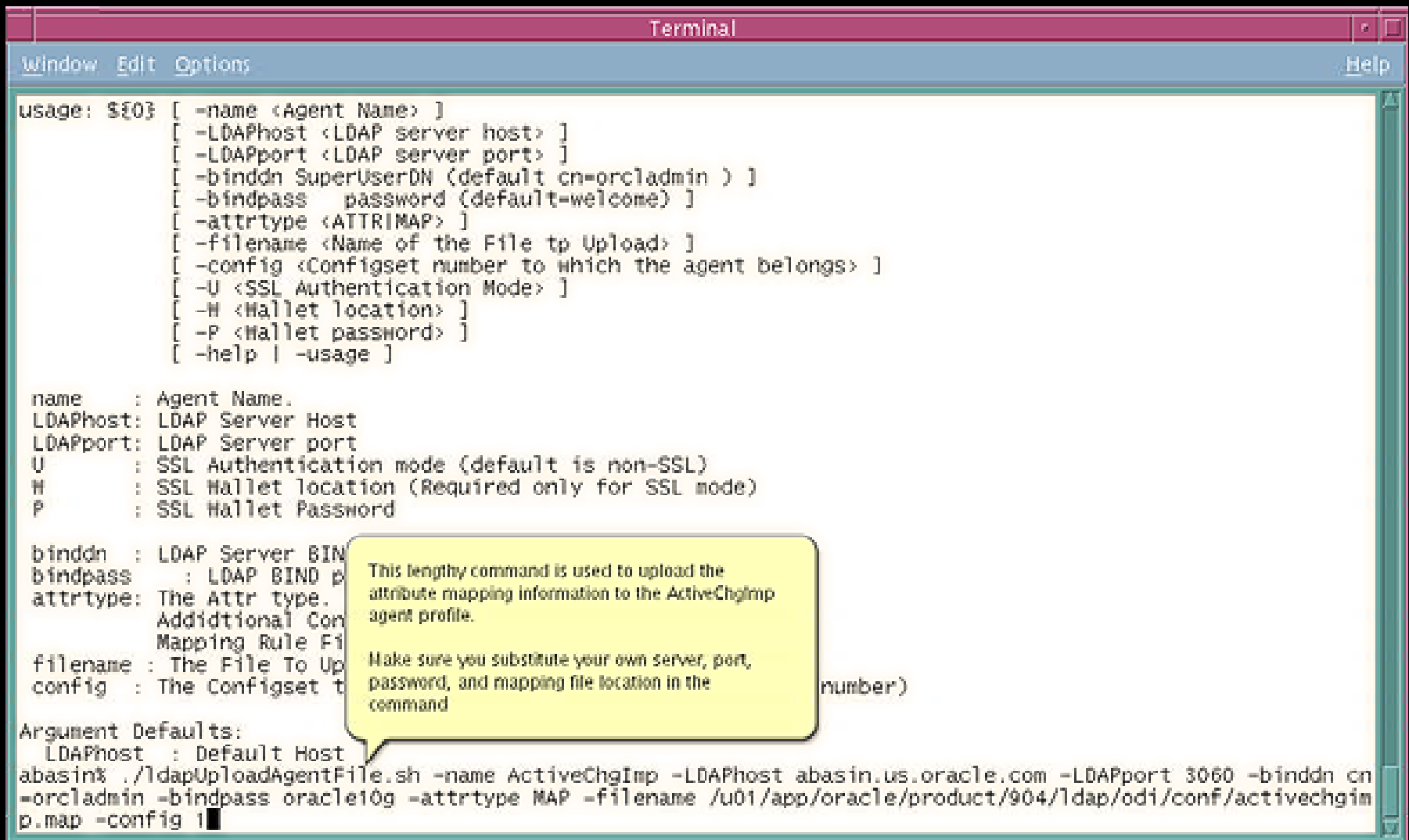
cn::container:cn:orclContainer

Слева объектный класс для Microsoft Active Directory

Справа объектный класс для Oracle Internet Directory

Загрузка профиля для импорта

```
%cd $ORACLE_HOME/ldap/odi/admin
```



```
usage: ${0} [ -name <Agent Name> ]
           [ -LDAPhost <LDAP server host> ]
           [ -LDAPport <LDAP server port> ]
           [ -binddn SuperUserDN (default cn=orcladmin ) ]
           [ -bindpass password (default=welcome) ]
           [ -attrtype <ATTRIMAP> ]
           [ -filename <Name of the File to Upload> ]
           [ -config <Configset number to which the agent belongs> ]
           [ -U <SSL Authentication Mode> ]
           [ -H <Hallet location> ]
           [ -P <Hallet passhord> ]
           [ -help | -usage ]

name      : Agent Name.
LDAPhost  : LDAP Server Host
LDAPport  : LDAP Server port
U         : SSL Authentication mode (default is non-SSL)
H         : SSL Hallet location (Required only for SSL mode)
P         : SSL Hallet Password

binddn    : LDAP Server BIND
bindpass  : LDAP BIND password
attrtype  : The Attr type.
           Additional Configuration
           Mapping Rule File
filename  : The File To Upload
config    : The Configset to which the agent belongs (number)

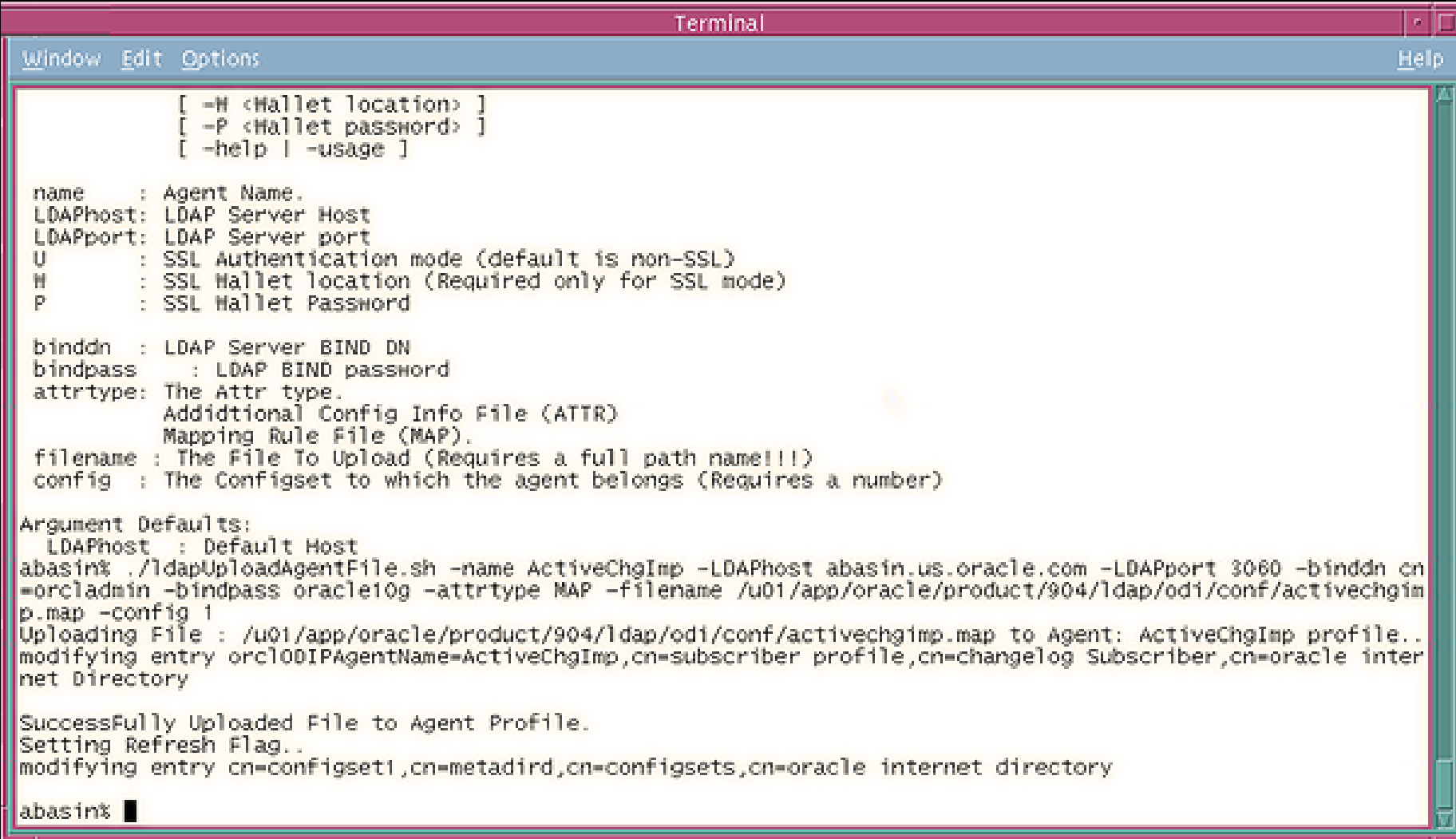
Argument Defaults:
LDAPhost  : Default Host
abasin% ./ldapUploadAgentFile.sh -name ActiveChgImp -LDAPhost abasin.us.oracle.com -LDAPport 3060 -binddn cn
-orcladmin -bindpass oracle10g -attrtype MAP -filename /u01/app/oracle/product/904/ldap/odi/conf/activechgi
p.map -config 1
```

This lengthy command is used to upload the attribute mapping information to the ActiveChgImp agent profile.

Make sure you substitute your own server, port, password, and mapping file location in the command

Загрузка профайла для импорта

```
%cd $ORACLE_HOME/ldap/odi/admin
```



```
Terminal
Window Edit Options Help

[ -H <Hallet location> ]
[ -P <Hallet passhord> ]
[ -help | -usage ]

name      : Agent Name.
LDAPhost: LDAP Server Host
LDAPport: LDAP Server port
U        : SSL Authentication mode (default is non-SSL)
H        : SSL Hallet location (Required only for SSL mode)
P        : SSL Hallet Password

binddn    : LDAP Server BIND DN
bindpass  : LDAP BIND passhord
attrtype: The Attr type.
          Additional Config Info File (ATTR)
          Mapping Rule File (MAP).
filename : The File To Upload (Requires a full path name!!!)
config   : The Configset to which the agent belongs (Requires a number)

Argument Defaults:
  LDAPhost : Default Host
abasin% ./ldapUploadAgentFile.sh -name ActiveChgImp -LDAPhost abasin.us.oracle.com -LDAPport 3060 -binddn cn
-orcladmin -bindpass oracle10g -attrtype MAP -filename /u01/app/oracle/product/904/ldap/odi/conf/activechgim
p.map -config 1
Uploading File : /u01/app/oracle/product/904/ldap/odi/conf/activechgimp.map to Agent: ActiveChgImp profile..
modifying entry orclODIPAgentName=ActiveChgImp,cn=subscriber profile,cn=changelog Subscriber,cn=oracle inter
net Directory

Successfully Uploaded File to Agent Profile.
Setting Refresh Flag..
modifying entry cn=configset1,cn=metadird,cn=configsets,cn=oracle internet directory

abasin% █
```

Загрузка OID Manager

Под пользователем “orcladmin”:

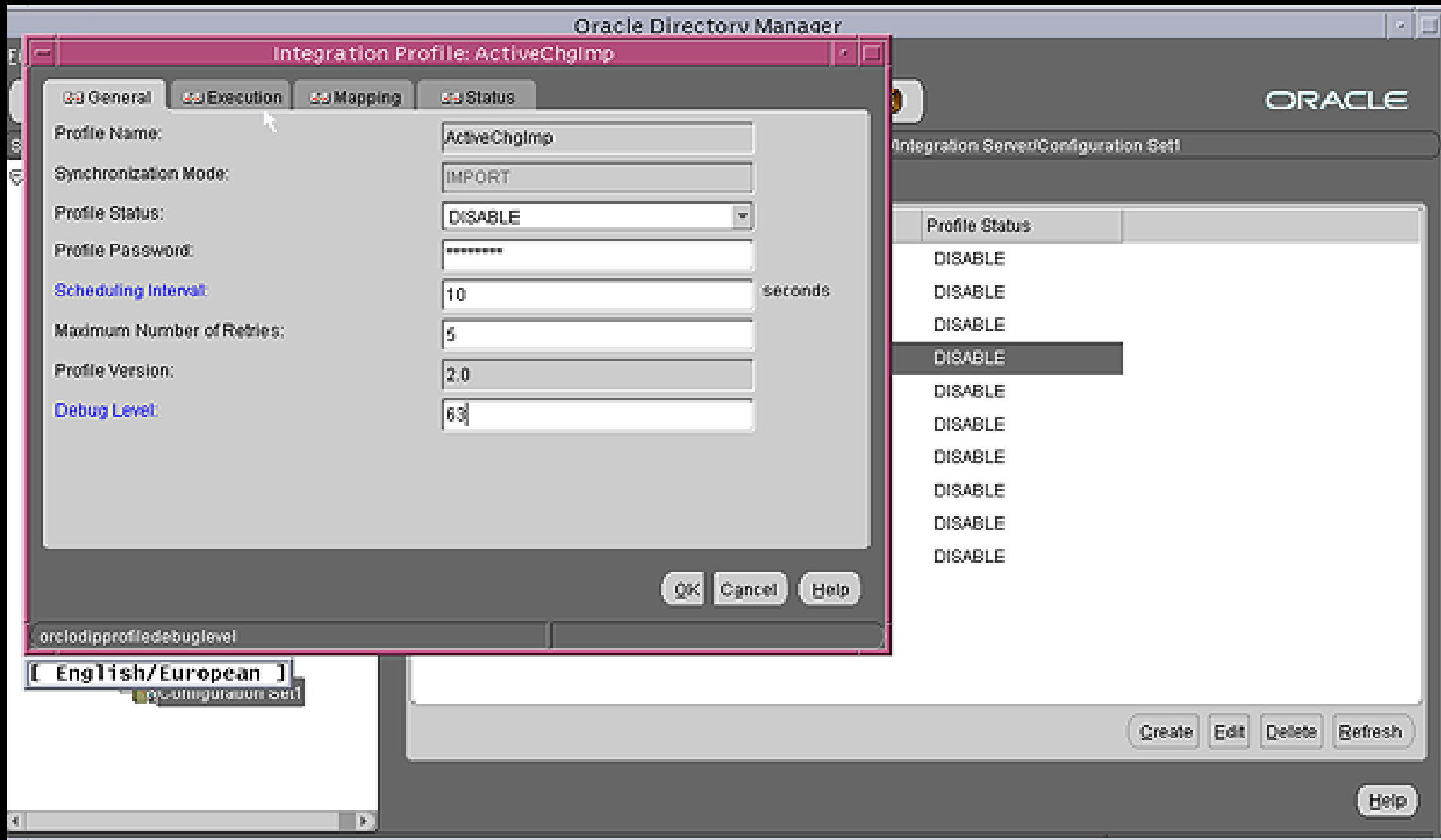
The screenshot displays the Oracle Directory Manager web interface. The left sidebar shows a tree of system objects, with 'Integration Server' and 'Configuration Set1' selected. The main pane shows the 'Integration Profiles' table, which lists various profiles and their synchronization modes. The 'ActiveChgImp' profile is highlighted in blue.

Profile Name	Synchronization Mode	Profile Status
LdrExport	EXPORT	DISABLE
IplanetExport	EXPORT	DISABLE
TaggedImport	IMPORT	DISABLE
ActiveChgImp	IMPORT	DISABLE
IdmImport	IMPORT	DISABLE
IplanetImport	IMPORT	DISABLE
OracleHRAgent	IMPORT	DISABLE
TaggedExport	EXPORT	DISABLE
ActiveExport	EXPORT	DISABLE
ActiveImport	IMPORT	DISABLE

Buttons at the bottom right: Create, Edit, Delete, Refresh, Help.

Загрузка OID Manager

Конфигурирование General Tab:



Загрузка OID Manager

Конфигурирование Status Tab:

The screenshot displays the Oracle Directory Manager interface. A modal window titled "Integration Profile: ActiveChgImp" is open, showing the "Status" tab. The tab contains the following fields:

- Last Execution Time: October 03, 2003 08:34:12
- Last Successful Execution Time: October 03, 2003 00:00:00
- Synchronization Status: NOT EXECUTED YET
- Synchronization Errors: (Empty list)
- Last Applied Change Number: 2568
- Bootstrap Status: NOT APPLICABLE

At the bottom of the modal window are buttons for "OK", "Cancel", and "Help". Below the modal window, the main interface shows a table with the following data:

Profile Status
DISABLE
DISABLE
DISABLE
DISABLE
DISABLE
DISABLE
DISABLE
DISABLE
DISABLE
DISABLE

At the bottom of the main interface are buttons for "Create", "Edit", "Delete", "Refresh", and "Help".

Получение Last Applied Change Number

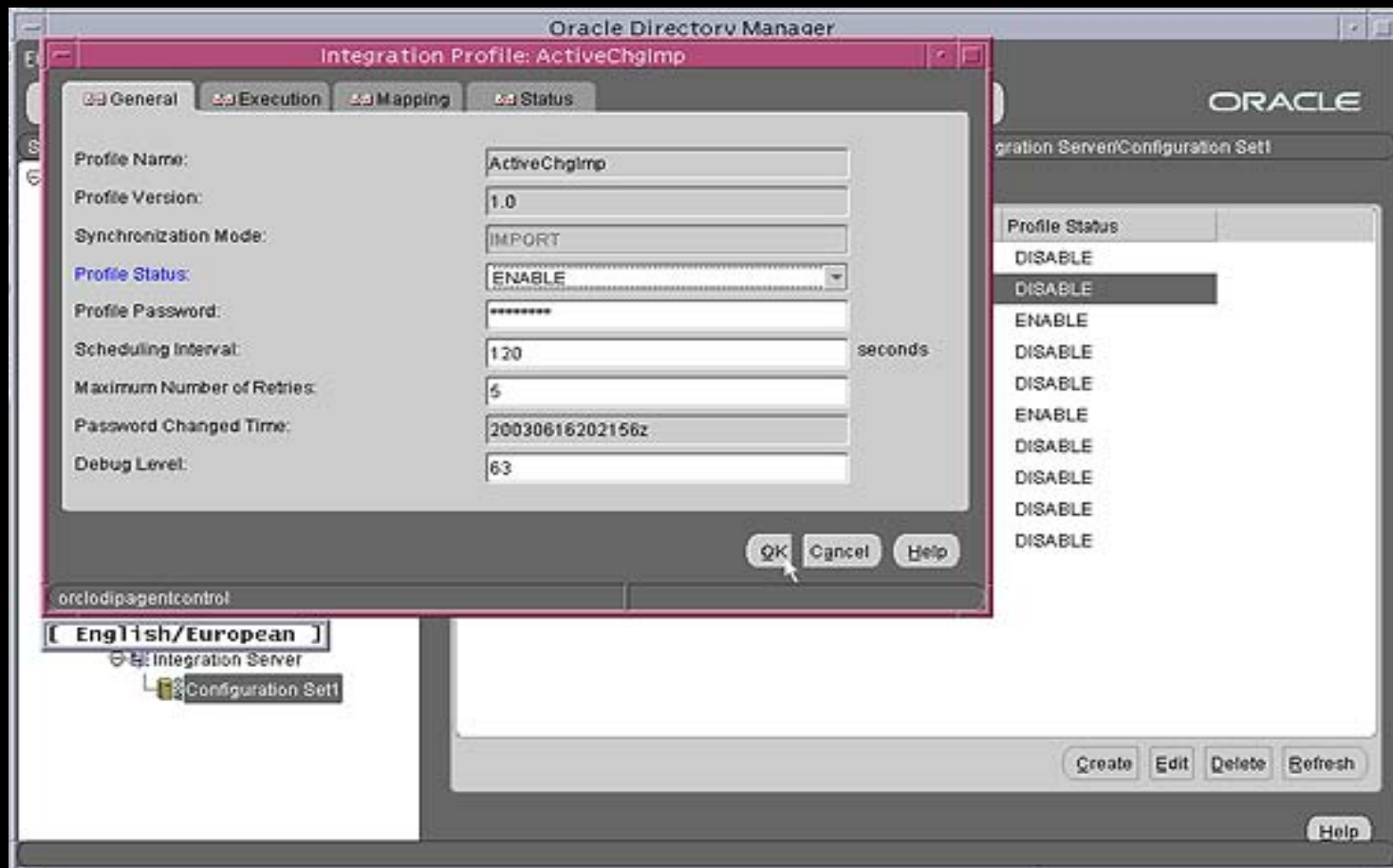
1. Конфигурирование Status Tab: получение last applied change number из Microsoft Active Directory:

```
ldapsearch -p 389 -h AD_Host_name -D  
administrator@acme.com -w admin_password -b "" -s  
base "objectclass=*" highestCommittedUSN
```

2. Конфигурирование Last Successful Execution Time к текущему времени и дате

Запуск Directory Integration and Provisioning сервера. Изменение статуса профиля.

- oidctl connect=iasdb server=odisrv instance=10 config=1 flags="port=3060" start



Грантирование прав доступа для Active Directory Group синхронизации

Используйте для этого grantrole.ldif – файл:

```
#ldapmodify -p oid_portnum -h oid_host_name -D  
"cn=orcladmin" -w orcladmin_pass -f ./grantrole.ldif
```

Миграция учетных записей пользователей из Microsoft Active Directory к Oracle Internet Directory.

Каждая учетная запись пользователя должна быть смигрирована:

1. Создаем backup всех пользователей из Microsoft Active Directory в Idif-текстовый файл:

```
Idifde -f OUTPUT.LDF -d "cn=users,dc=acme,dc=com"
```

2. Сдвигаем OUTPUT.LDF на сервер, где работает Oracle Internet Directory.
3. Правим файл: Idf2ldf.properties в директории \$ORACLE_HOME/ldap/odi/samples:

Миграция учетных записей пользователей из Microsoft Active Directory к Oracle Internet Directory.

```
%cd $ORACLE_HOME/ldap/odi/samples
```

```
%cp ldf2ldf.properties ldf2ldfad.properties
```

```
%chmod 777 ldf2ldf.properties
```

В файле ldf2ldf.properties делаем изменения:

1. odip.bootstrap.srctype = LDIF
2. odip.bootstrap.srcurl = /u01/OUTPUT.LDF
3. odip.bootstrap.desttype = LDIF
4. odip.bootstrap.desturl = /u01/oid.ldif

Миграция учетных записей пользователей из Microsoft Active Directory к Oracle Internet Directory.

5. odip.bootstrap.mapfile =
 \$ORACLE_HOME/ldap/odi/conf/activechgimp.map
6. odip.bootstrap.logfile =
 \$ORACLE_HOME/ldap/odi/log/bootstrap.log
7. odip.bootstrap.logseverity =
 \$ORACLE_HOME/ldap/odi/log/bootstrap.log
8. odip.bootstrap.tracefile =
 \$ORACLE_HOME/ldap/odi/log/bootstrap.trc

Миграция учетных записей пользователей из Microsoft Active Directory к Oracle Internet Directory.

Создаем новый LDIF-файл для загрузки в Oracle Internet Directory:

```
% dipassistant bootstrap -cfg  
/u01/app/oracle/product/904/ldap/odi/samples/ldf2ldfad.p  
roperties
```

Добавляем содержимое из LDIF-файла в Oracle Internet Directory:

```
%ldapadd -p port_num -h host_name -D "cn=orcladmin" -w  
password -c -f /u01/oid.ldif
```

Миграция учетных записей пользователей из Microsoft Active Directory к Oracle Internet Directory.

Создаем новый LDIF-файл для загрузки в Oracle Internet Directory:

```
% dipassistant bootstrap -cfg  
/u01/app/oracle/product/904/ldap/odi/samples/ldf2ldfad.p  
roperties
```

Добавляем содержимое из LDIF-файла в Oracle Internet Directory:

```
%ldapadd -p port_num -h host_name -D "cn=orcladmin" -w  
password -c -f /u01/oid.ldif
```

Установка внешней аутентификации для Oracle Internet Directory

Установка внешней аутентификации для Oracle Internet Directory производится через запуск конфигурационного скрипта

```
$ORACLE_HOME/ldap/admin/oidspadi.sh
```

Установка фильтра аутентификации

```
(&(objectclass=inetorgperson)(cn=orcladmin)
```

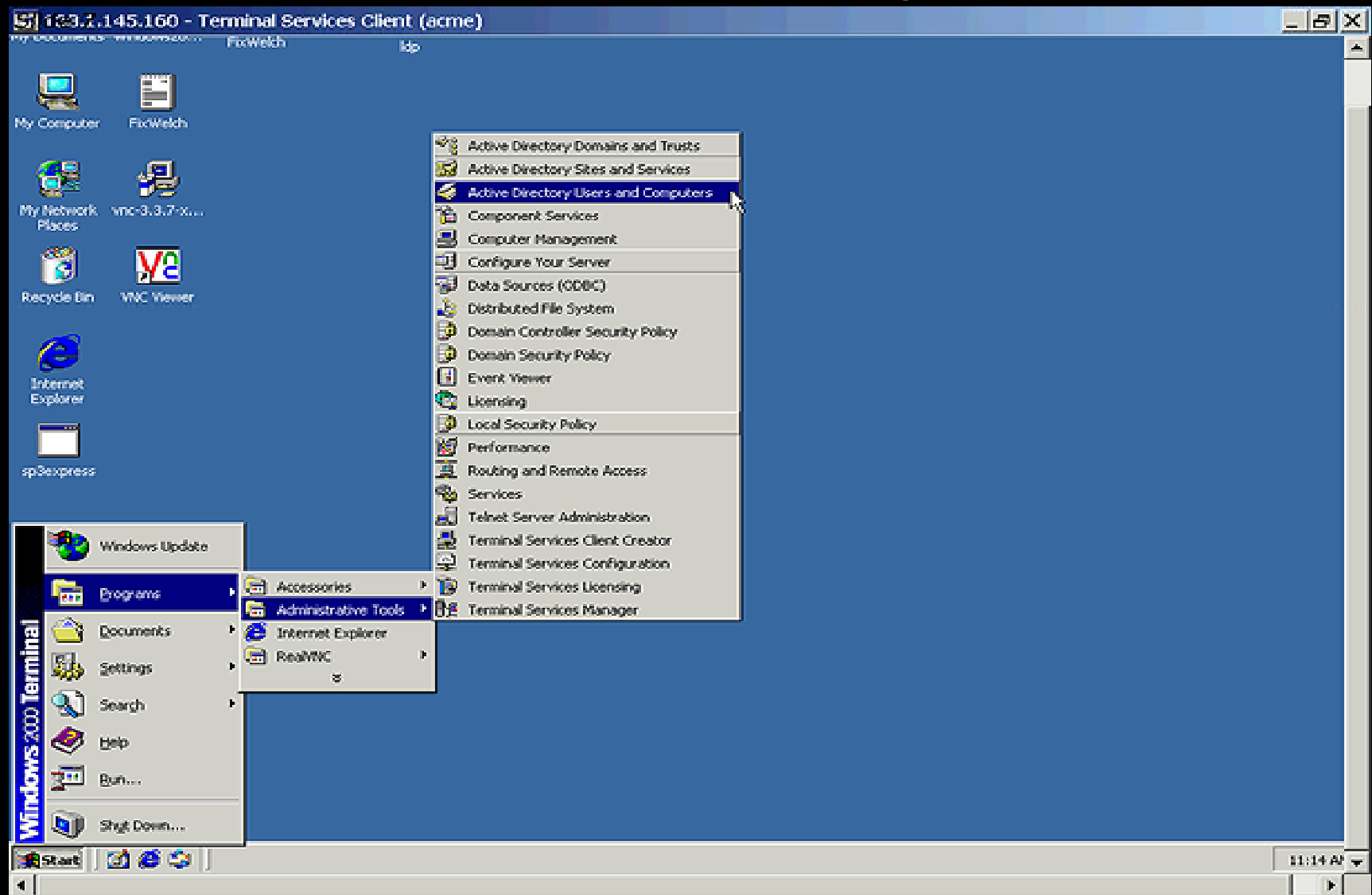
Исключение пользователей из внешней аутентификации:

```
(|(cn=orcladmin)(cn=portal)
```

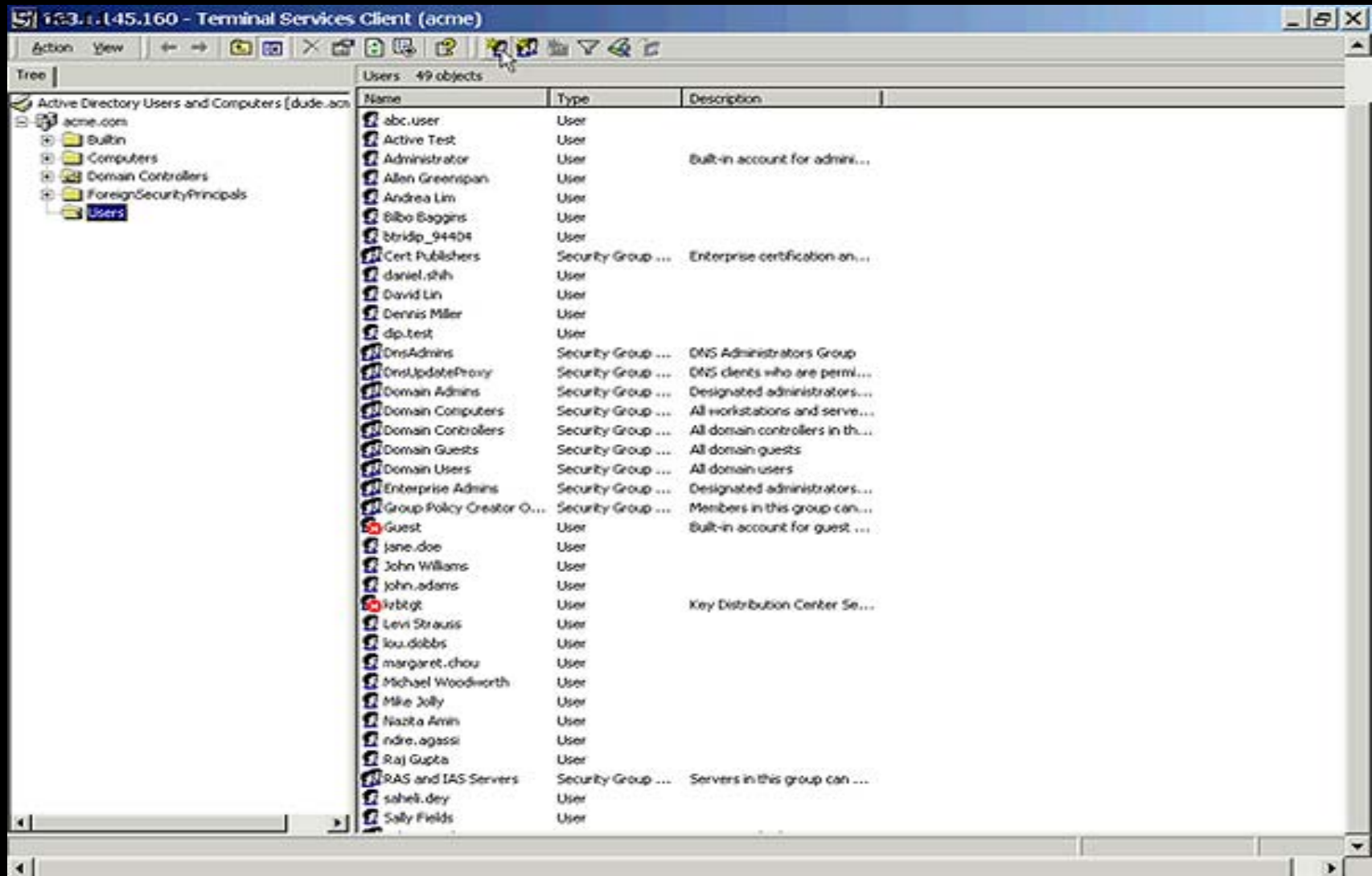
Аутентификация пользователей AD против AD, и пользователей OID против OID:

```
(!(objectclass=orclADUser)
```

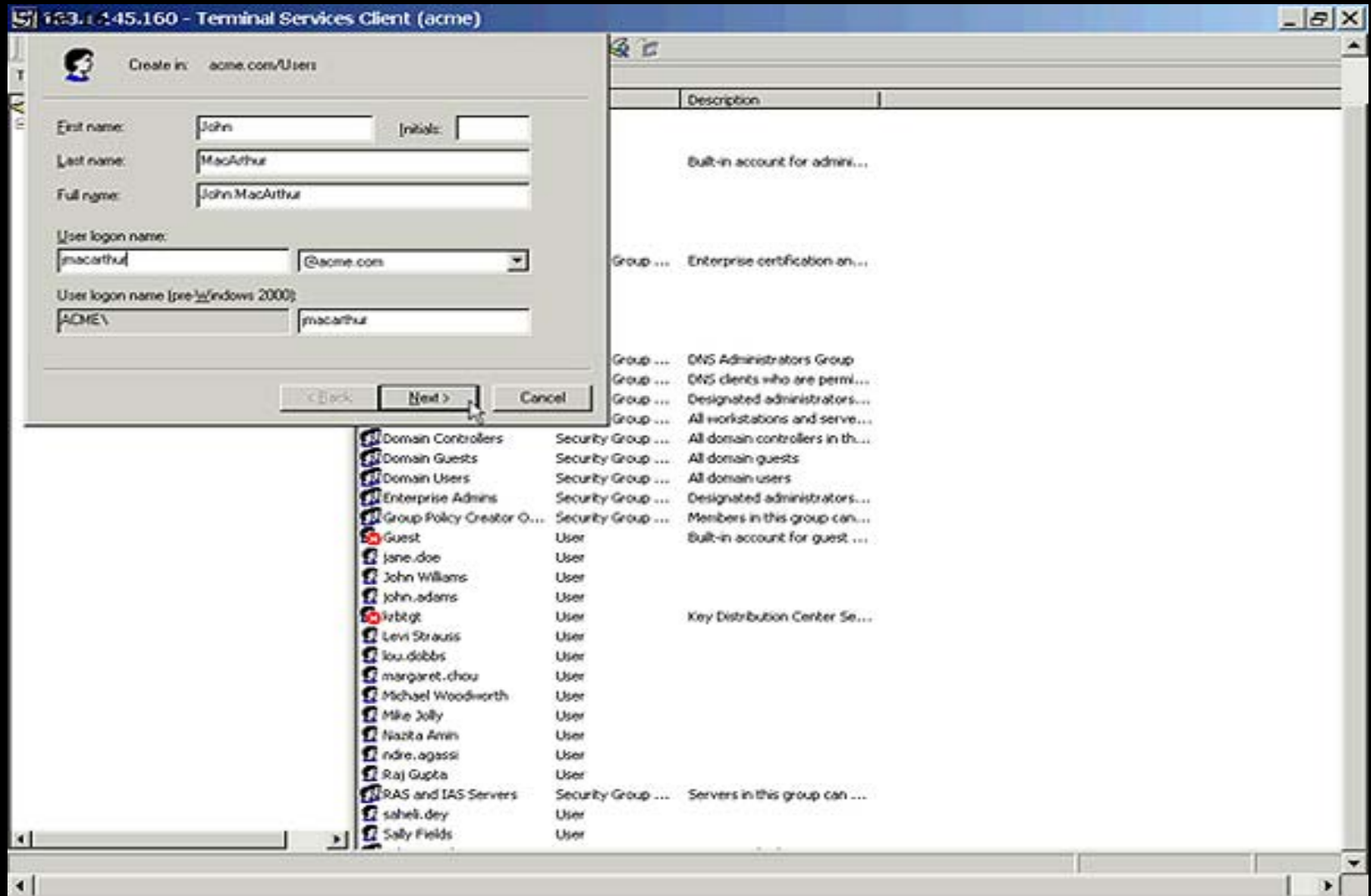
Создание нового пользователя в Microsoft Active Directory



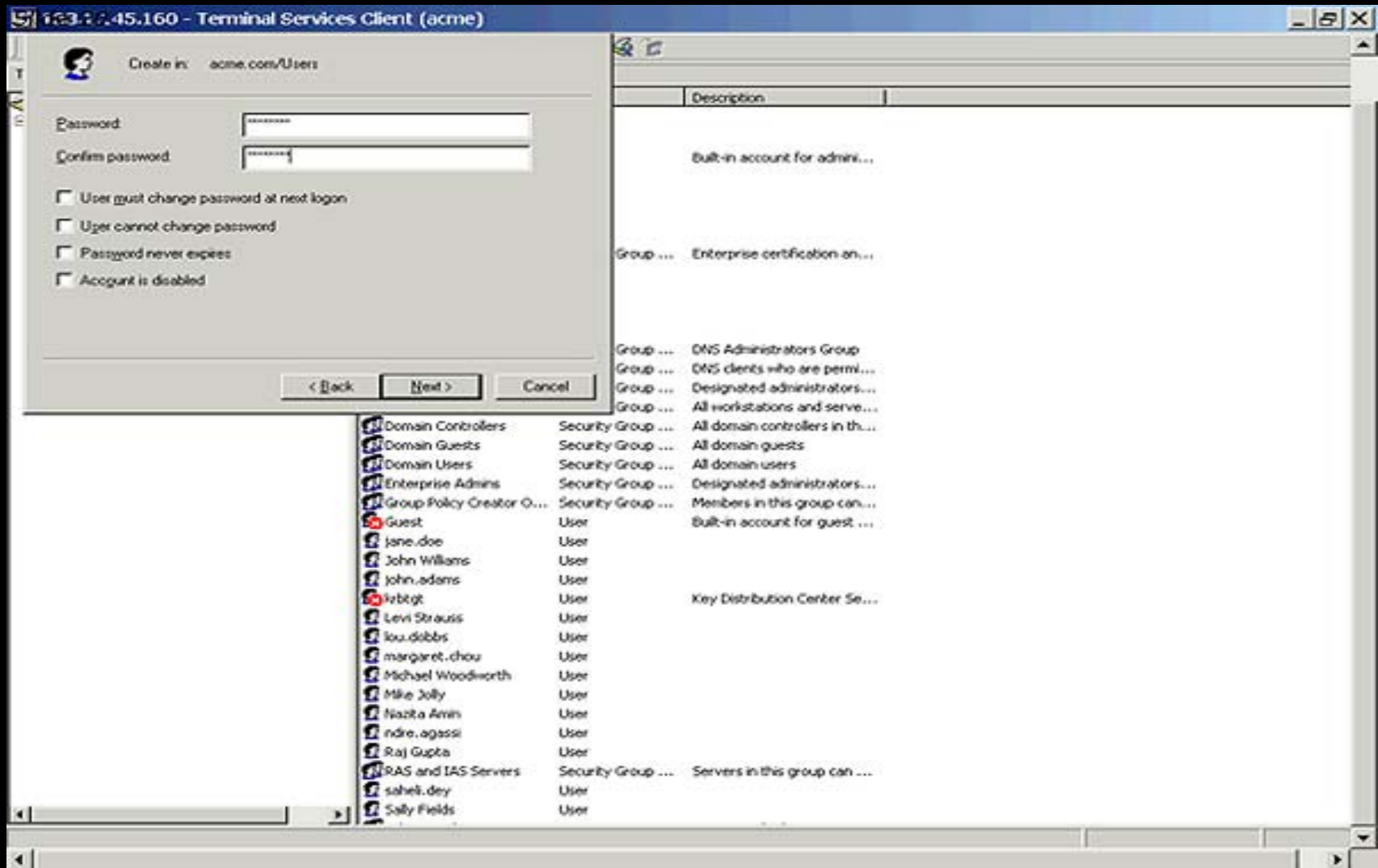
Создание нового пользователя в Microsoft Active Directory



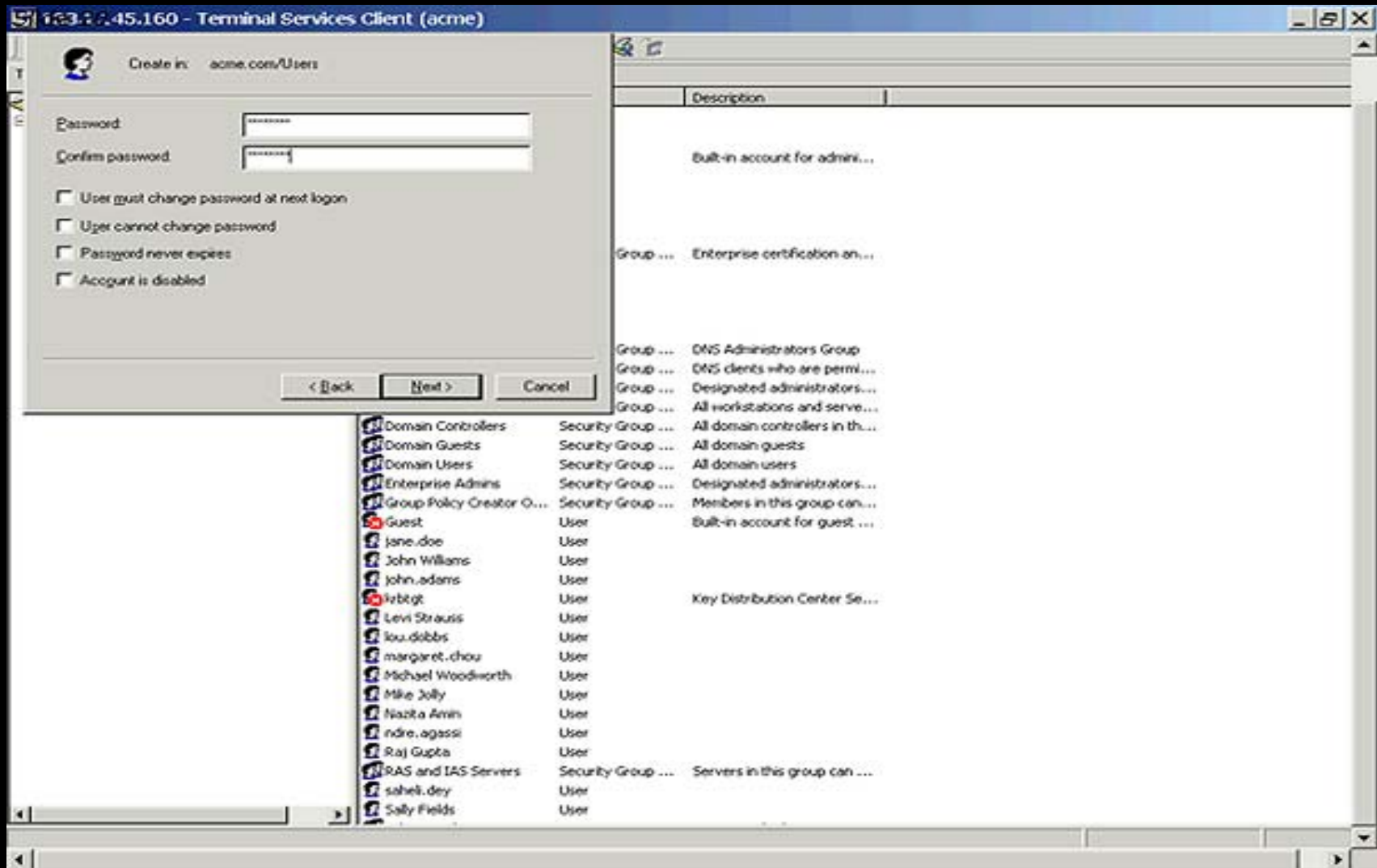
Создание нового пользователя в Microsoft Active Directory



Создание нового пользователя в Microsoft Active Directory



Создание нового пользователя в Microsoft Active Directory



Проверка свойств User Subscriber Контейнера

1. Запустите Oracle Internet Directory Manager под пользователем “orcladmin”.
2. В навигационном окне откройте:
“Entry Management” -> “dc=domain” -> “cn=users”
3. Убедитесь, что пользователь был создан успешно.
Тоже самое можно проверить через службу DAS:
<http://hostname.domain:httpportnum/oiddas>, при попытке
логина любым пользователем Microsoft Active
Directory.

A large, stylized graphic in the background consisting of a grey 'Q' and 'A' with a red ampersand in the center. The text 'Вопросы' and 'Ответы' is overlaid on the ampersand.

Вопросы Ответы

ORACLE®