Ja, wo laufen Sie denn?

LDAP-Integration für SQL*Net

DOAG
Deutsche ORACLE-Anwendergruppe e.V.

DOAG-Regionaltreffen München/Südbayern

Montag, 12. Februar 2007 um 17:00 Uhr

Agenda

Wer sind Wir?

Überblick SQL*Net

LDAP-Integration

Das `LDAP`-Prinzip

Oracle OID

Active Directory

OpenLDAP

Fazit

Über uns

Oracle Consulting seit Oracle 7.1

IT Service Provider und Remote Backup Dienstleister

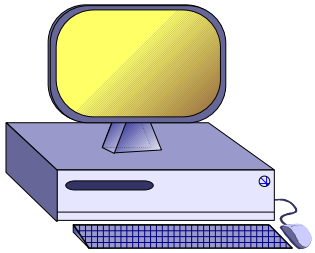
Eigenes Rechenzentrum

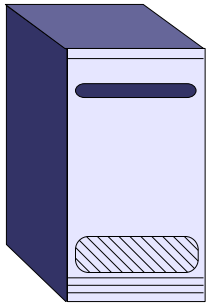
Wir sichern Ihre Datenbank

Entwicklung von Software mit Oracle-Werkzeugen (Forms, Reports, Designer)

Eigenes Java-Framework XCP

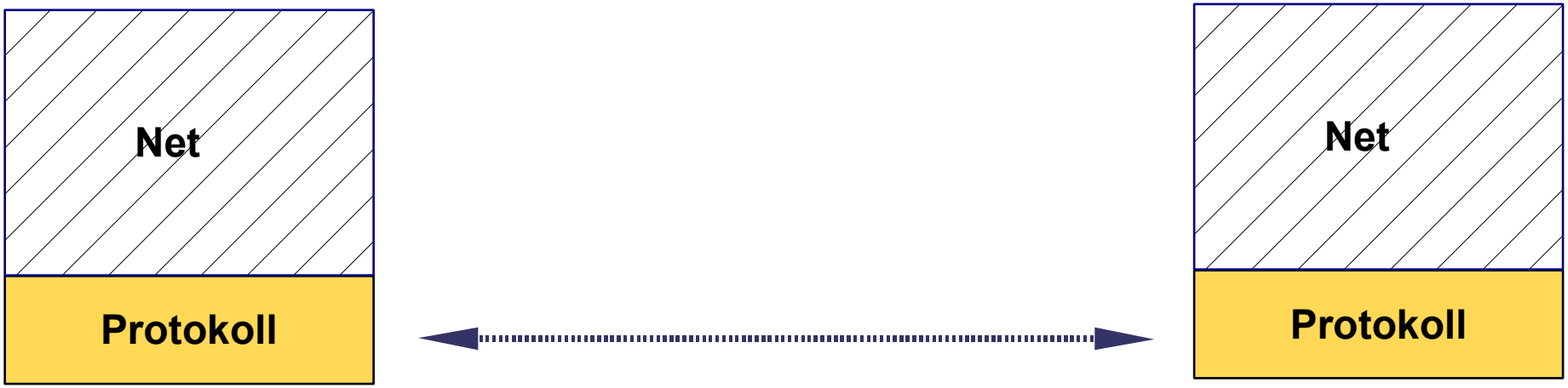
Überblick Oracle SQL*Net





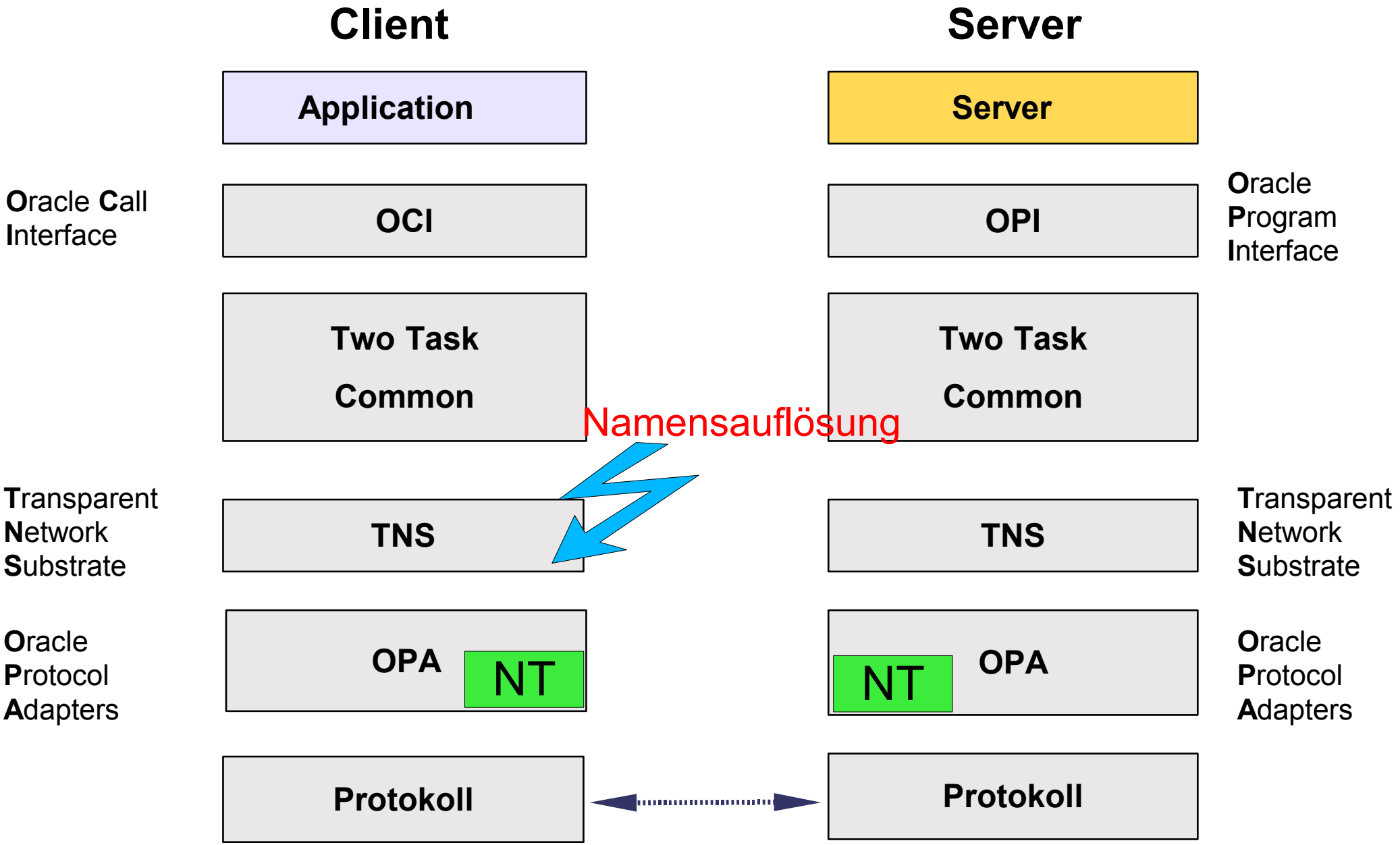
Client

Server



Unterstützte Netzwerk-Protokolle:
TCP/IP
SPX/IPX
DecNet , IBM LU6.2,usw.

Die Oracle-Net-Architektur



Die Konfiguration des Clients

Auswahl der Namensmethode

Host Naming

Netzwerk-Name der DB wird angegeben

Local Naming

TNSAlias Name wird über die TNSNames.ora-Datei ausgewertet

Oracle Name Server (ab 10g nicht mehr unterstützt!)

Rechner-Name, Name und Port des DB Listener wird zentral verwaltet und aufgelöst.

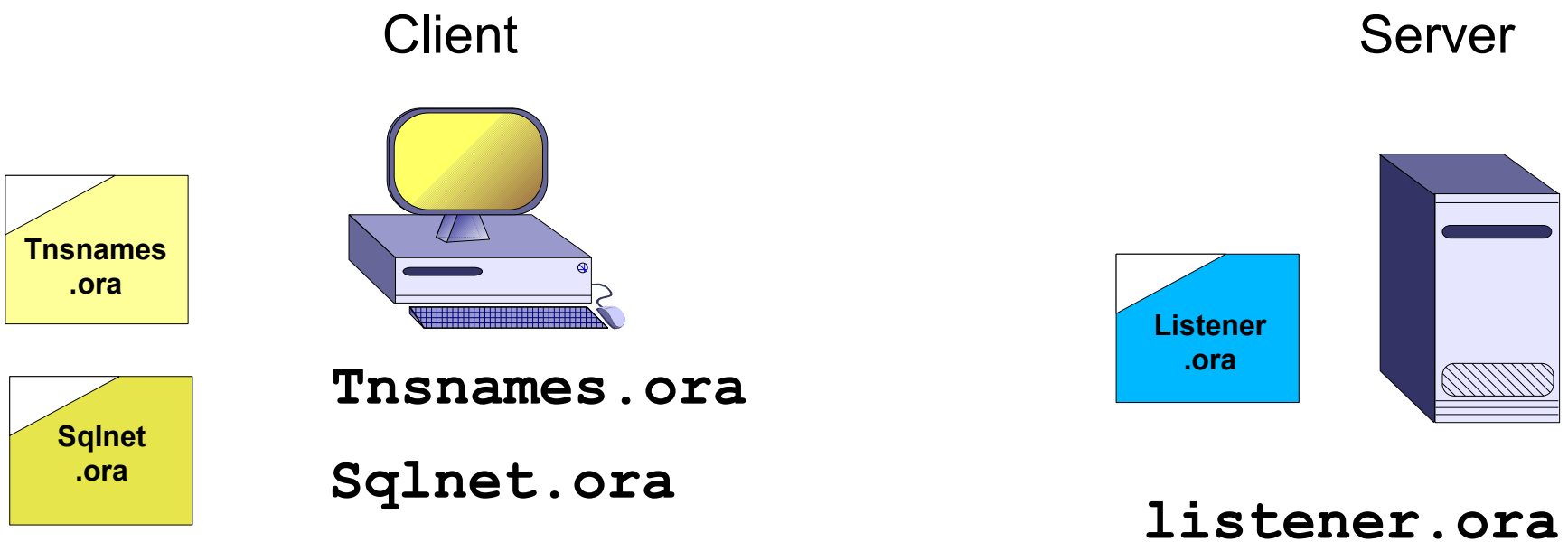
Directory Server (LDAP)

Verzeichnisdienst nutzen

Die wichtigsten Steuerdateien

Default-Verzeichnis $Oracle_Home/network/admin/

Setzen der default Location mit der TNS_ADMIN-Umgebungsvariable



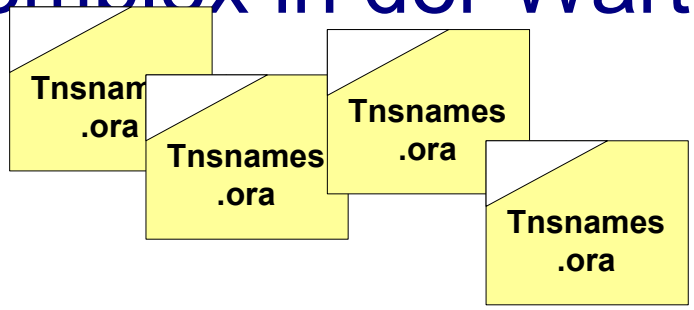
Local Naming

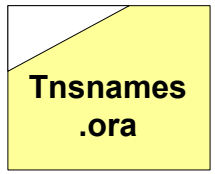
Der TNSalias wird über die Datei tnsnames.ora aufgelöst

Umgebungsvariablen:
Default Alias mit LOCAL setzen

Speicherort der Datei bei mehr als einem Oracle Home über TNS_ADMIN setzen.

Komplex in der Wartung bei vielen Clients





Beispiel Tnsnames.ora

Beispiel für einen Eintrag

TNS Alias

```
GPI.WORLD =
   (DESCRIPTION =
     (ADDRESS_LIST =
       (ADDRESS = (PROTOCOL = TCP)
                  (HOST = localhost)
                  (PORT = 1521)
       )
     )
     (CONNECT_DATA =
       (SERVICE_NAME = gpi)
     )
   )
```

Rechner

Port Listener

Instance Name

SQL*Net im Überblick

SQL*Net ist das Netzwerk-Protokoll der Oracle-Datenbank

Basiert auf vorhandenen Netzwerkprotokollen der Schicht 1 und 2 (TCP/IP)

Konfiguration des Clients meist über die TNSNames.ora-Datei

Häufigste Fehlerursachen

Umgebungsvariablen beachten

Netzwerkstack prüfen!

TNSPing mit Trace zur Diagnose verwenden

Das LDAP-Prinzip

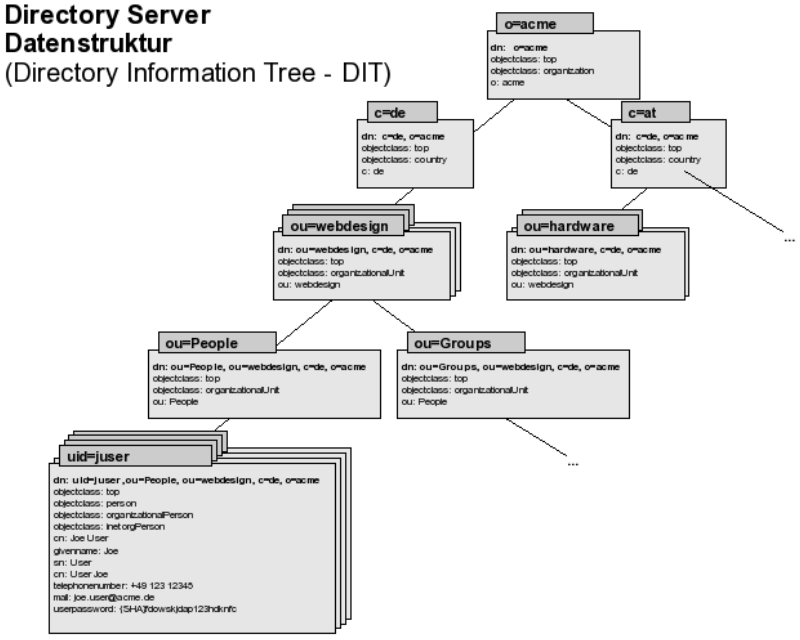
Lightweight Directory Access Protocol (LDAP)

A. Netzwerkprotokoll

B. Verzeichnis

Entstanden als Subset von X.500(DAP) => *lightweight*

Daten werden in einer Baumstruktur abgelegt



LDAP-Eigenschaften

Optimiert für Abfragen

Schema ist flexibel erweiterbar

Komplexe Suchen möglich

Standard nach RFC 4511 (aktuell)

Allerdings hat jeder Hersteller seine eigene Interpretation des Ganzen entwickelt

Wichtige LDAP-Begriffe

Schema

Beschreibt die Struktur der Daten (Format & Beziehungen)
~~~ DML

Objekt

Die einzelnen Knoten im Baum ~~~ ROW

Attribut

Die Werte unter einem Knoten ~~~ COLUMN

Distinguished Name (DN) ~~~ PK

Beschreibt eindeutig jedes Objekt im Baum

Beispiel:

```
uid=juser,ou=People,ou=webdesign,c=de,o=acme
```
~~~

Wichtige LDAP-Begriffe (2)

Organizational Unit

Container für Unterobjekte ~~~ Tablespace

Context

Teilbaum ~~~ SELECT WHERE pid = %d

CN (Common Name)

Name des Objektes ~~~ SELECT name FROM x

RDN (Relative Distinguished Names)

Beschreibt den Pfad

```
CN=NCORA, CN=OracleContext, DC=NCORA, DC=LOCAL
```

Warum LDAP-Integration

LDAP vergleichbar zu DNS

Frei erweiterbar

Plattformübergreifend

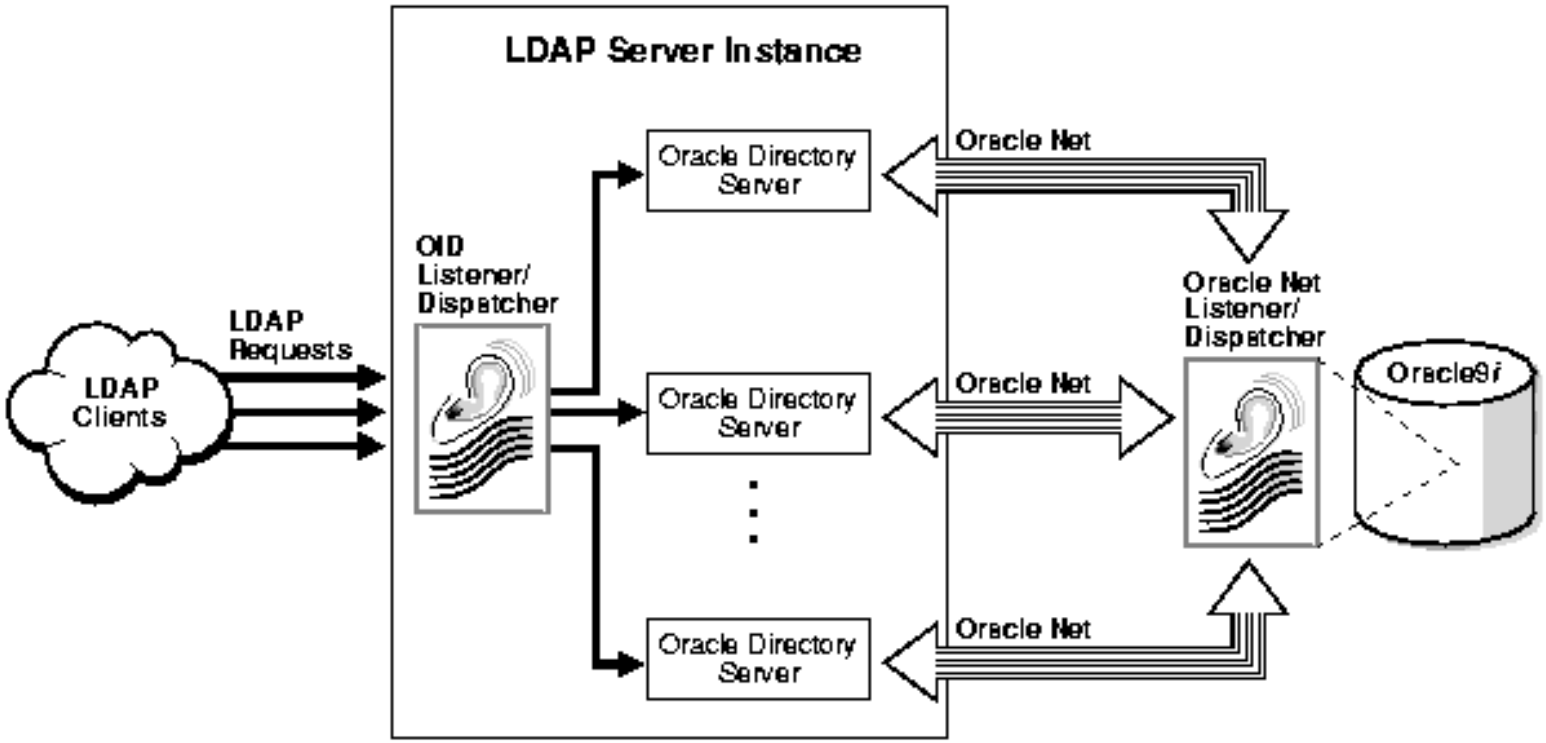
Produktübergreifend

Langjährig erprobt (seit 1993)

Ideal um Informationen wie Benutzerberechtigungen, Namensauflösung, usw. in Netzwerken zu implementieren

Oracle OID - 1

Oracle-Implementierung eines Directory Servers mit LDAP-Abfragemöglichkeiten



Oracle OID - 2

Sehr mächtig aber auch sehr „SCHWERGEWICHTIG“ in der Implementierung

Hochverfügbarkeit möglich, aber aufwändig

Basiert auf der Oracle-Datenbank

Abfragen mit dem LDAP-Protokoll

Active Directory

In Windows-Netzwerken meist hochverfügbar ausgelegt und implementiert

Benutzerverwaltung durch das System bereits sehr hochwertig vorgegeben

Kann um eigene Schematas erweitert werden

Mit etwas Aufwand

Konfigurations-Active-Directory - AD

Ablauf

Installation der MS Administrative Tools für das AD

Anpassung des Active Directory

Schema mit dem Net Configuration Assistant anlegen

Datenbank-Aliase anlegen

SQLNet.ora auf dem Client anpassen

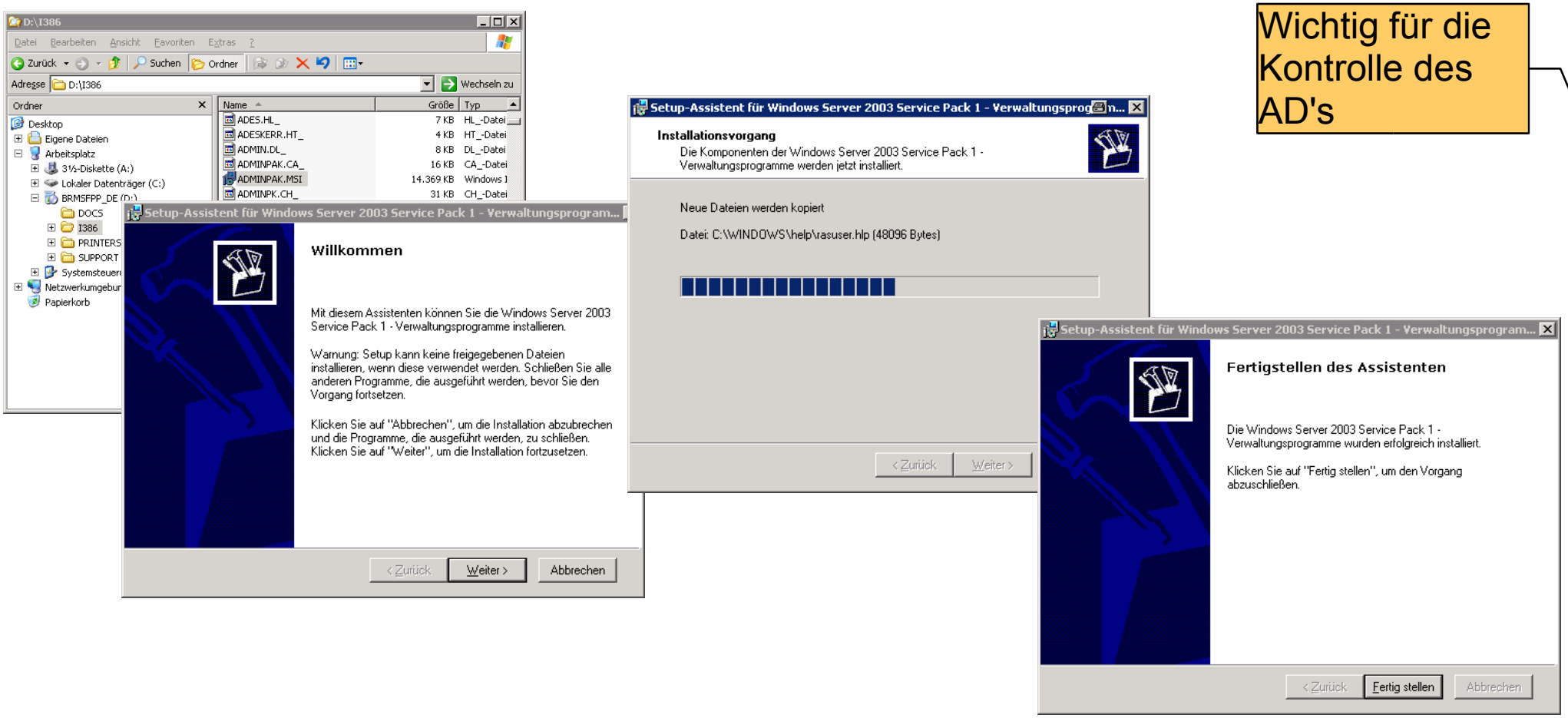
Testen

Installation unter MS Windows Server2003 R2 SP1

MS Administrative Tools für das AD

Installation der Microsoft-Werkzeuge für das AD

Quelle: Adminpack auf der Server Installationscd im Verzeichnis i386 Datei ADMINPAK.MSI

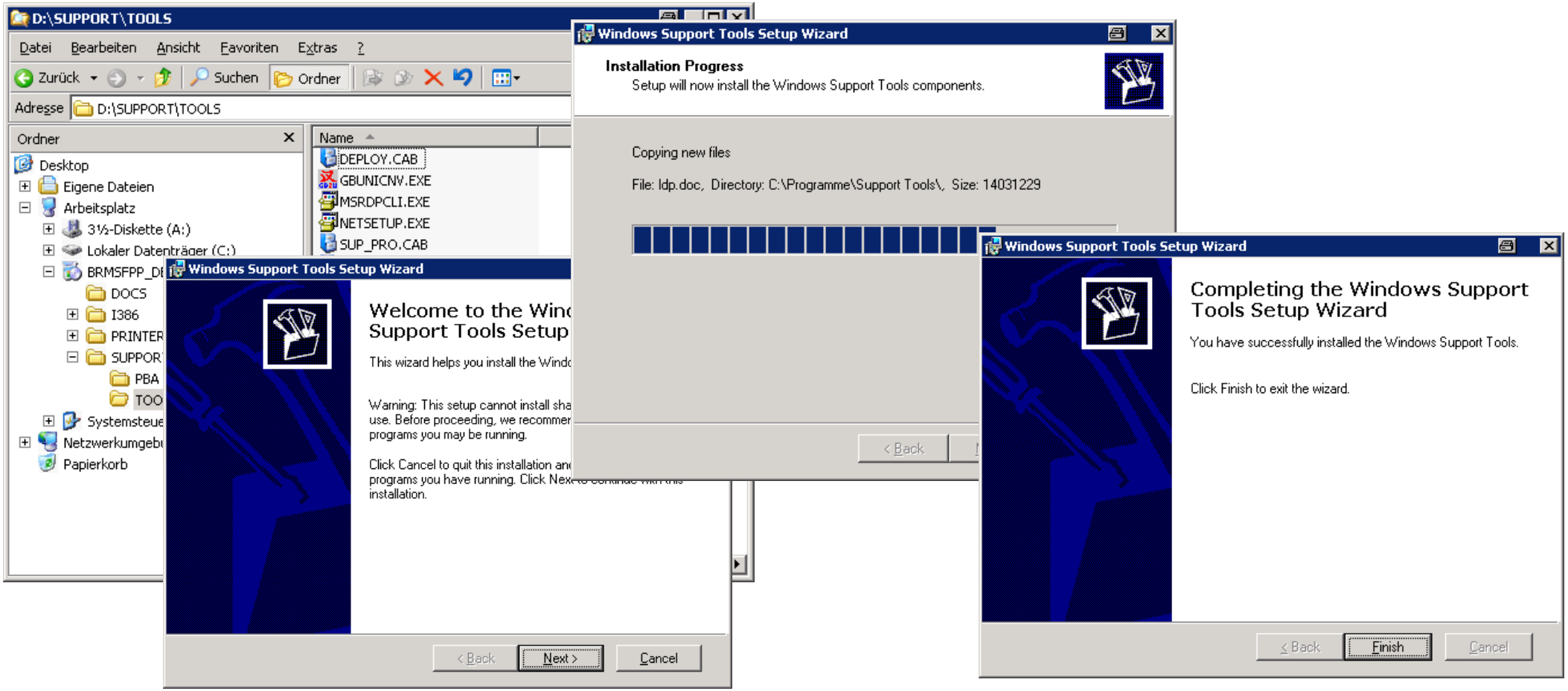


Wichtig für die Kontrolle des AD's

MS Support Tools für das AD

Installation der Support Tools des AD's

Quelle: Adminpack auf der Server Installationscd im Verzeichnis Support\tools Datei SUPTOOLS.MSI



Anpassung des Active Directory (1)

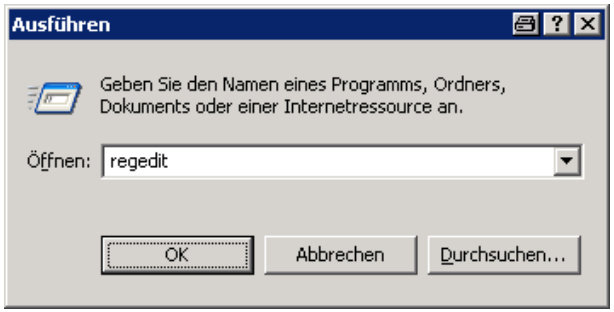
Registry auf dem PDC anpassen

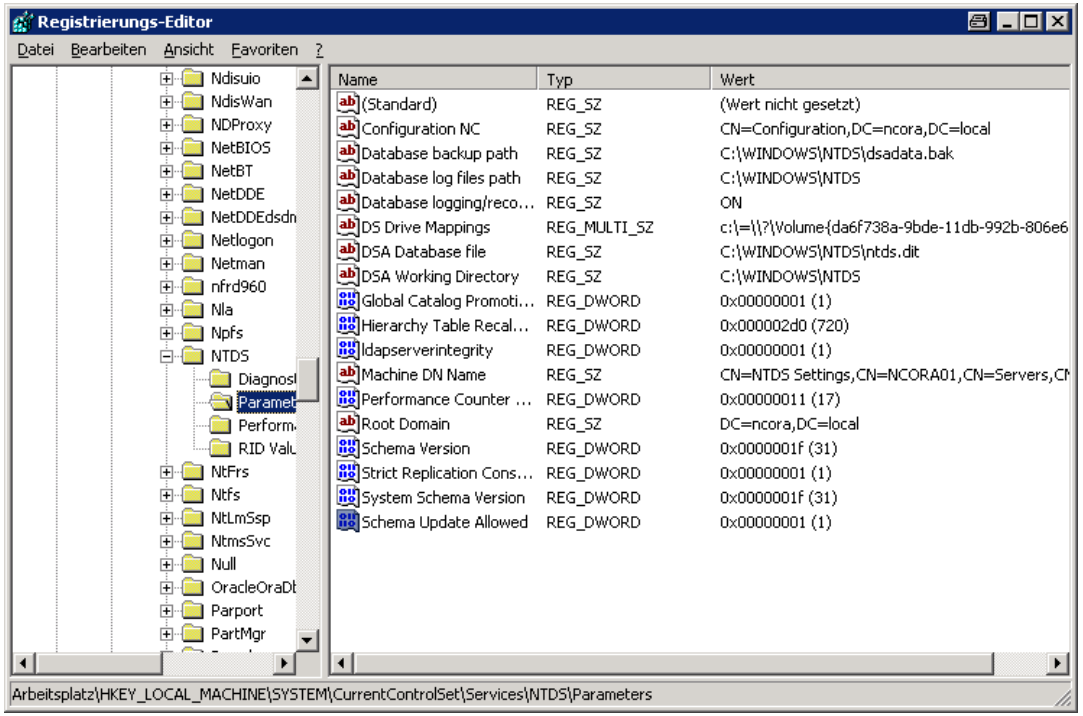
KEY:

```
HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters
```

Neuer Parameter (Typ DWORD) :

```
Schema Update Allowed = 1
```

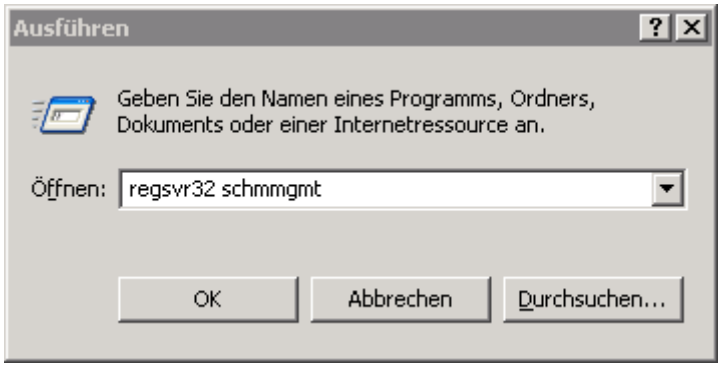




Anpassung des Active Directory (2)

Schema Management registrieren

Befehl




```
Regsvr32 schmmgmt
```

Anpassung des Active Directory (3)

ADSI aktivieren

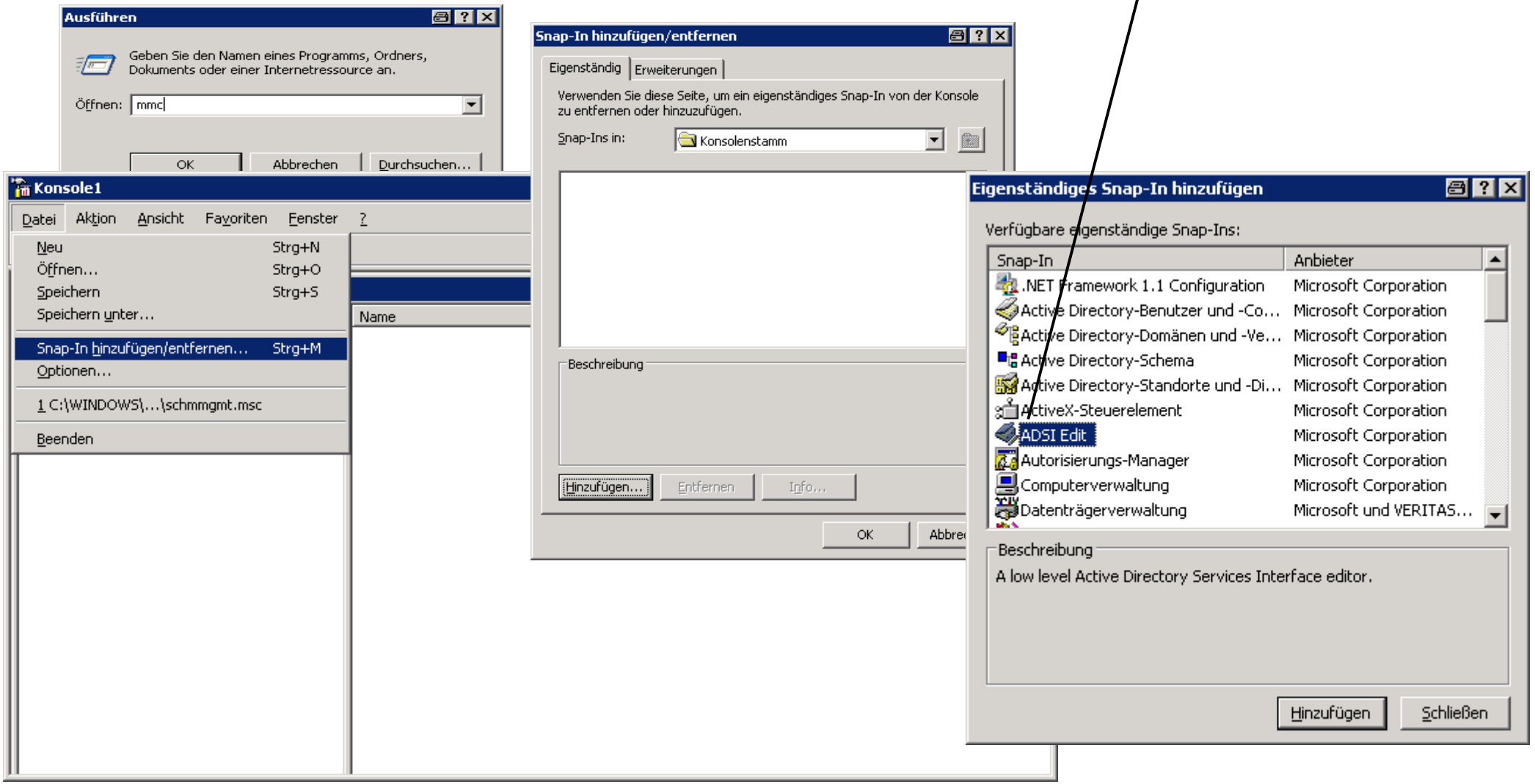
ADSI : Active Directory Server Interface

Skript-Schnittstelle für das AD

Oracle-Werkzeuge verwenden teilweise diese Schnittstelle

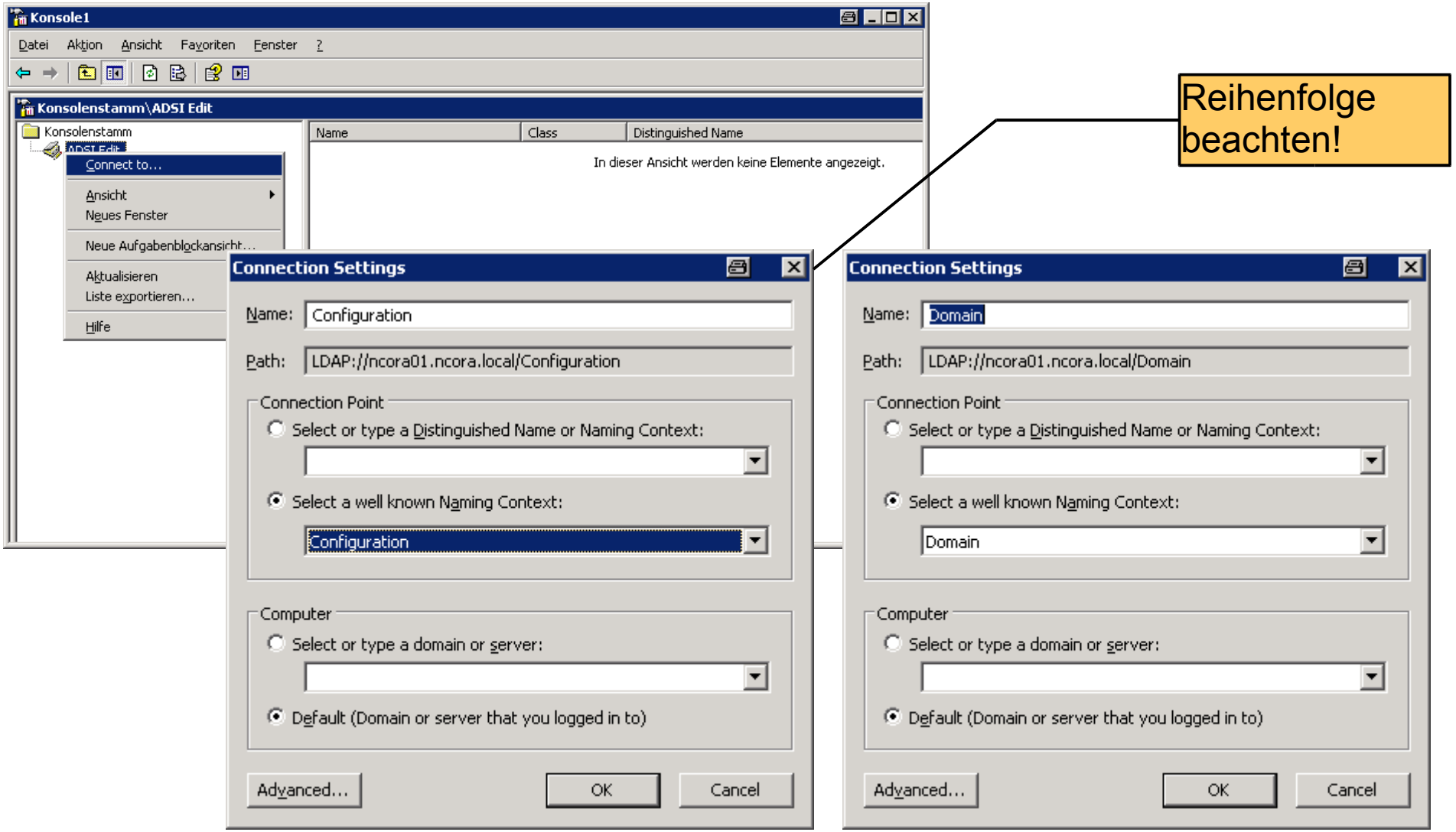
ADSI aktivieren (1)

Snap-In laden



ADSI aktivieren (2)

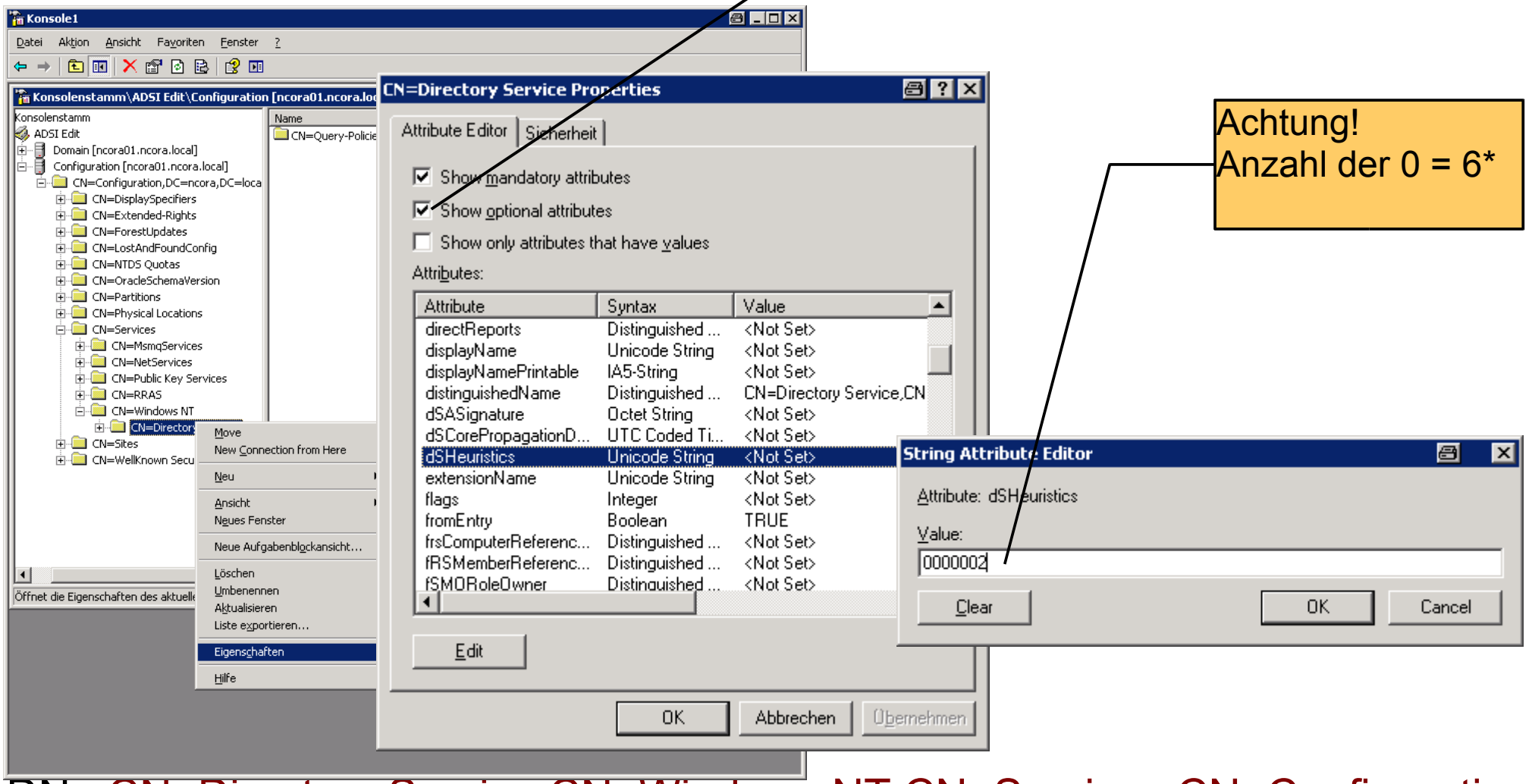
Zum Server verbinden



ADSI aktivieren (3)

Anonymes Browsen des AD wird erlaubt!

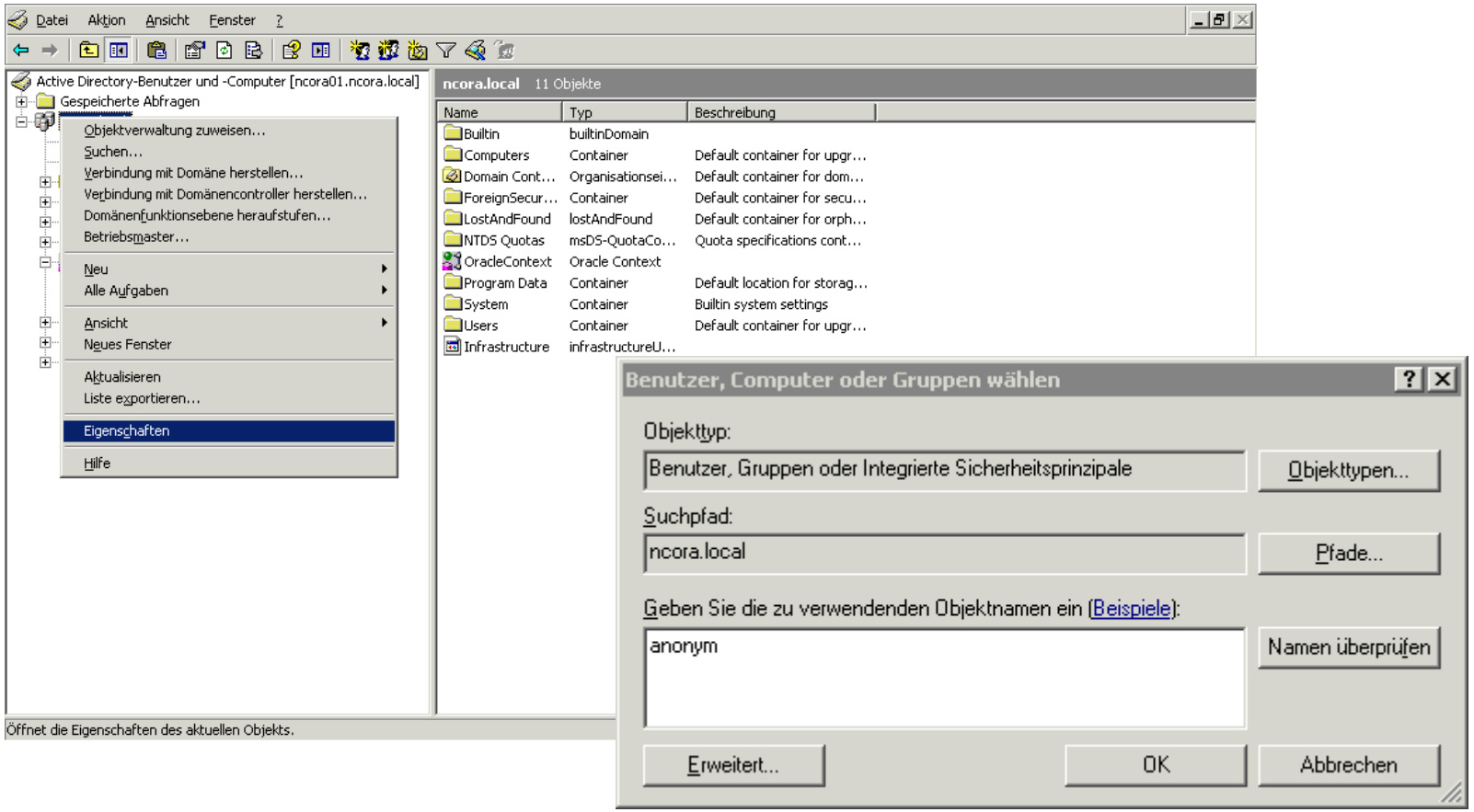
Parameter dSHeuristics anpassen



DN : CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration

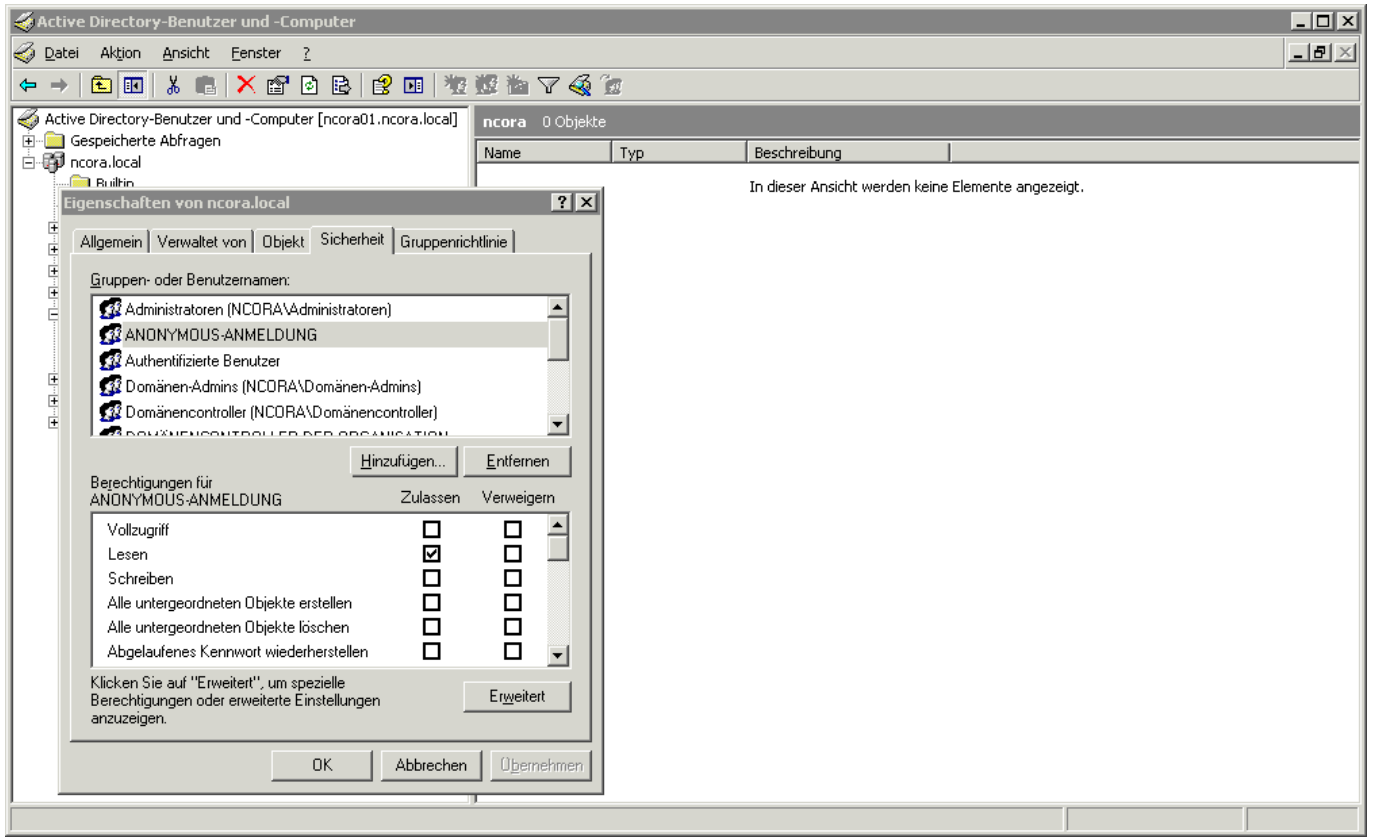
Anpassung des Active Directory (4)

Berechtigungen im AD für den anonymen Zugriff setzen



Anpassung des Active Directory (5)

Berechtigungen im AD für den anonymen Zugriff setzen (rekursiv)

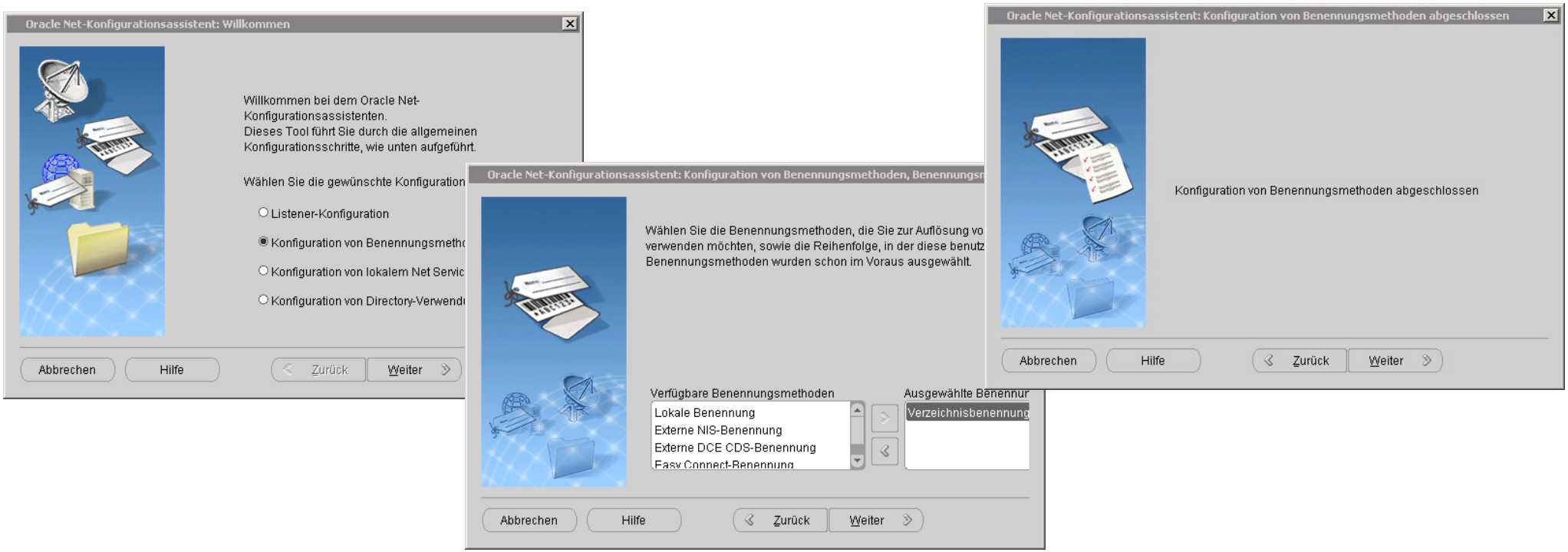


Oracle Net Configuration Assistant

Oracle auf dem Win2003 Server installiert (ohne DB)

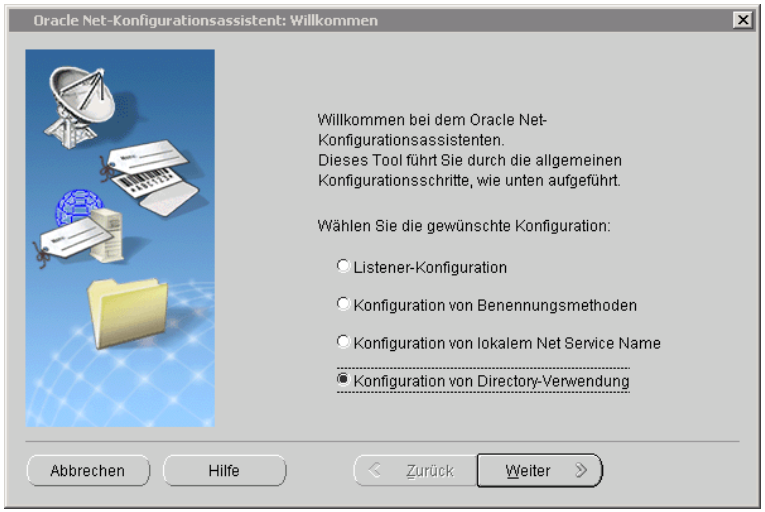
Start vom Oracle NetCa

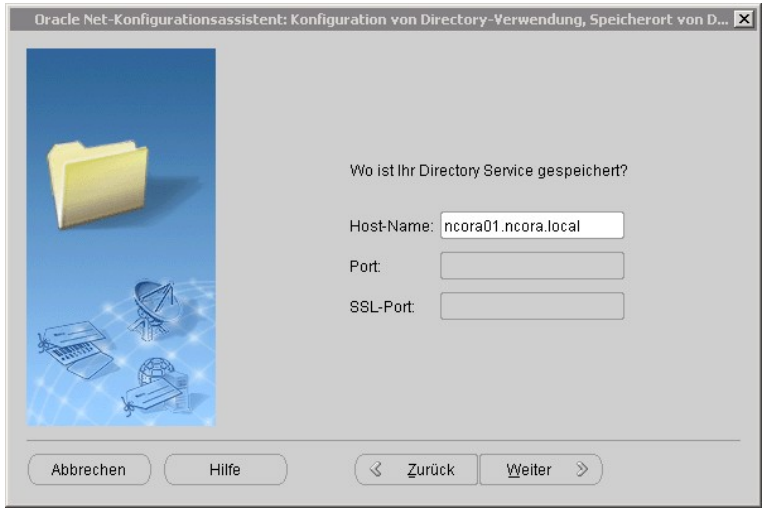
Bennenungsmethode konfigurieren



Oracle Net Configuration Assistant

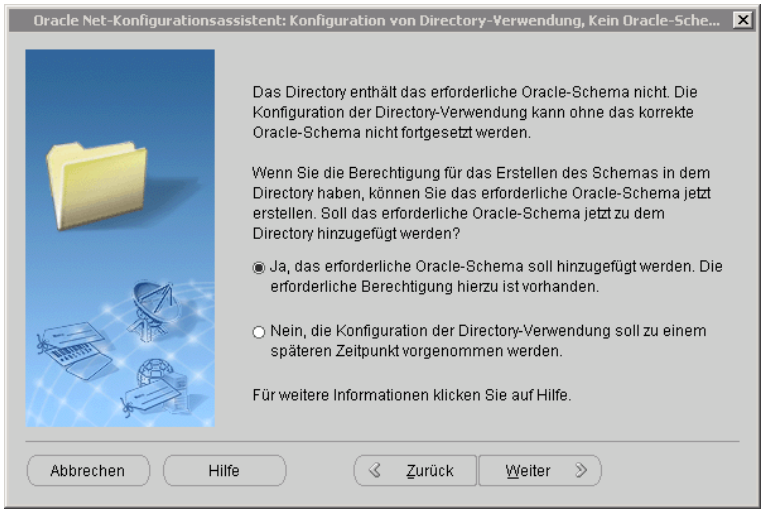
Konfigurations-Directory





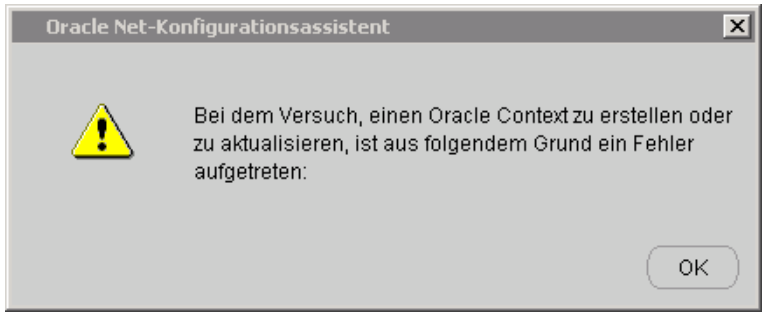
Oracle Net Configuration Assistant (1)

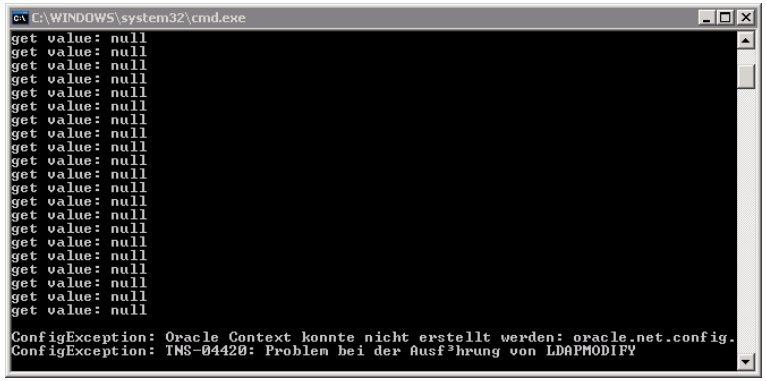
Konfigurations-Directory



Oracle Net Configuration Assistant (2)

Konfigurations-Directory



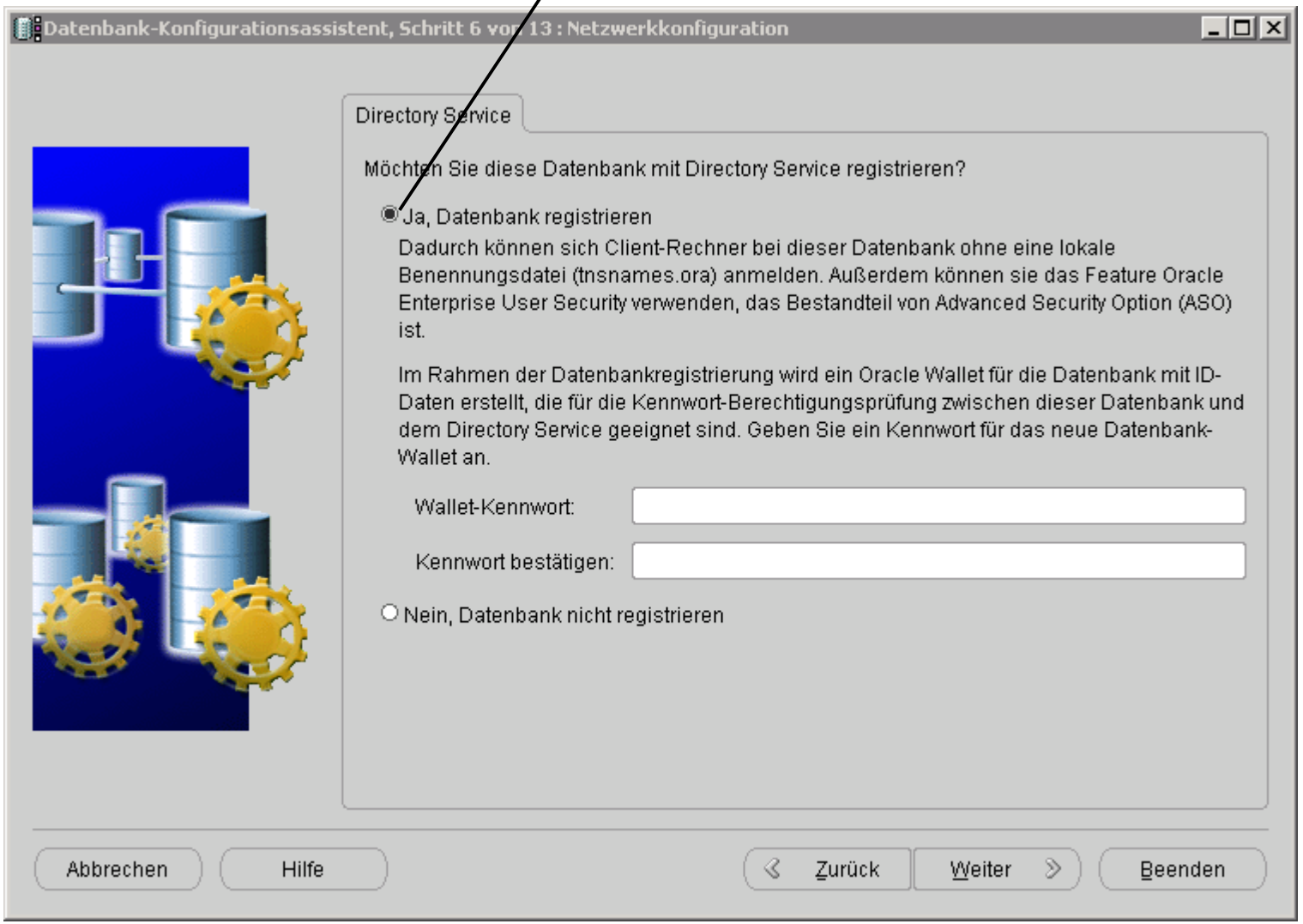


Siehe Metalink ID: Note 361192.91
siehe Treffer 1 unter „Suche: LDAP Windows 2003“

Registrieren bei der Datenbank erstellen

Normale Installation

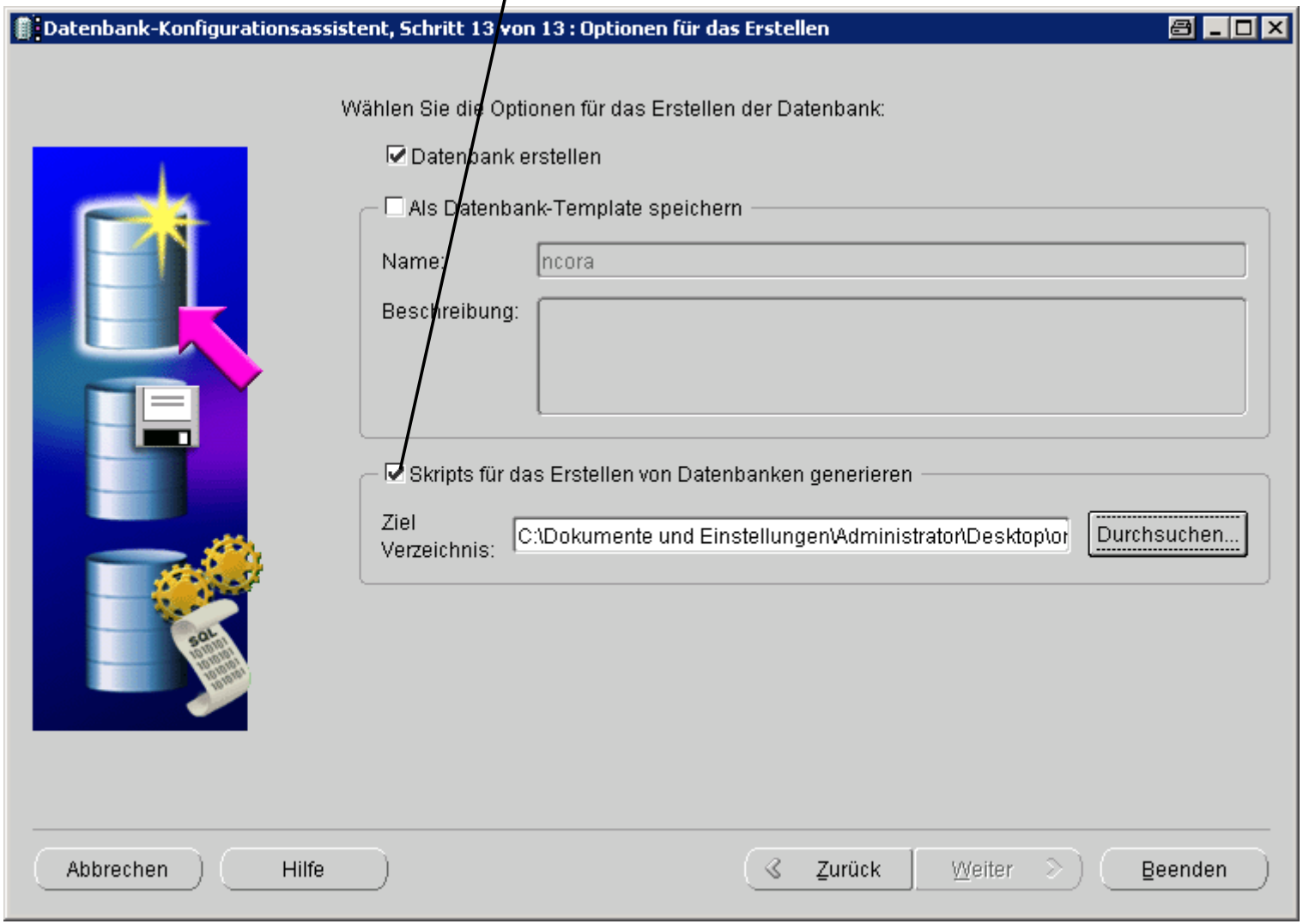
Seite 6:



Registrieren bei der Datenbank erstellen (2)

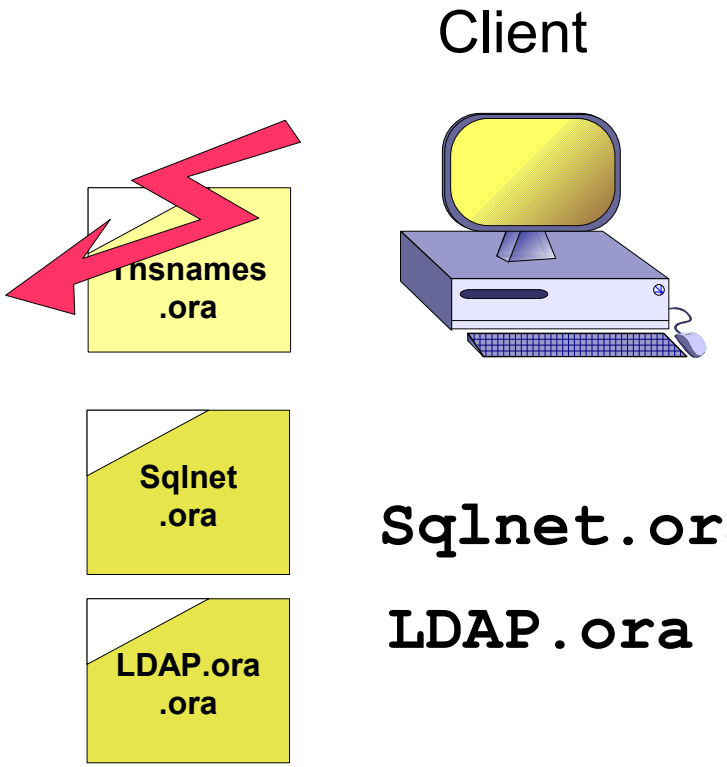
Seite 13:

Wichtig als spätere Dokumentation.



Konfiguration des Clients anpassen

SQLNet.ora und LDAP.ora anpassen



`Sqlnet.ora`

`LDAP.ora`

Konfiguration überprüfen

$ORACLE_HOME/network/admin/

sqlnet.ora

```
NAMES.DIRECTORY_PATH= (LDAP)
```

Verweis auf TNSNames entfällt

ldap.ora

```
DEFAULT_ADMIN_CONTEXT = "DC=ncora,DC=local"

DIRECTORY_SERVER_TYPE = AD
DIRECTORY_SERVERS = (ncora01:389:636)
```

Standardcontext beachten

Servername:<Port>:<SSL-Port>

Testen

TNSPing

```
C:\Dokumente und Einstellungen\Administrator>tnsping ncora

TNS Ping Utility for 32-bit Windows: Version 10.2.0.1.0 - Production on 10-FEB-
2007 18:56:59

Copyright (c) 1997, 2005, Oracle.  All rights reserved.

Parameterdateien benutzt:
C:\oracle\product\10.2.0\db_2\network\admin\sqlnet.ora

Adapter LDAP zur Auflösung des Alias benutzt
Attempting to contact
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=ncora01.ncora.local)(PORT=1521))(CONNECT
_DATA=(SERVICE_NAME=ncora)))
OK (40 ms)

C:\Dokumente und Einstellungen\Administrator>
```

Testen (2)

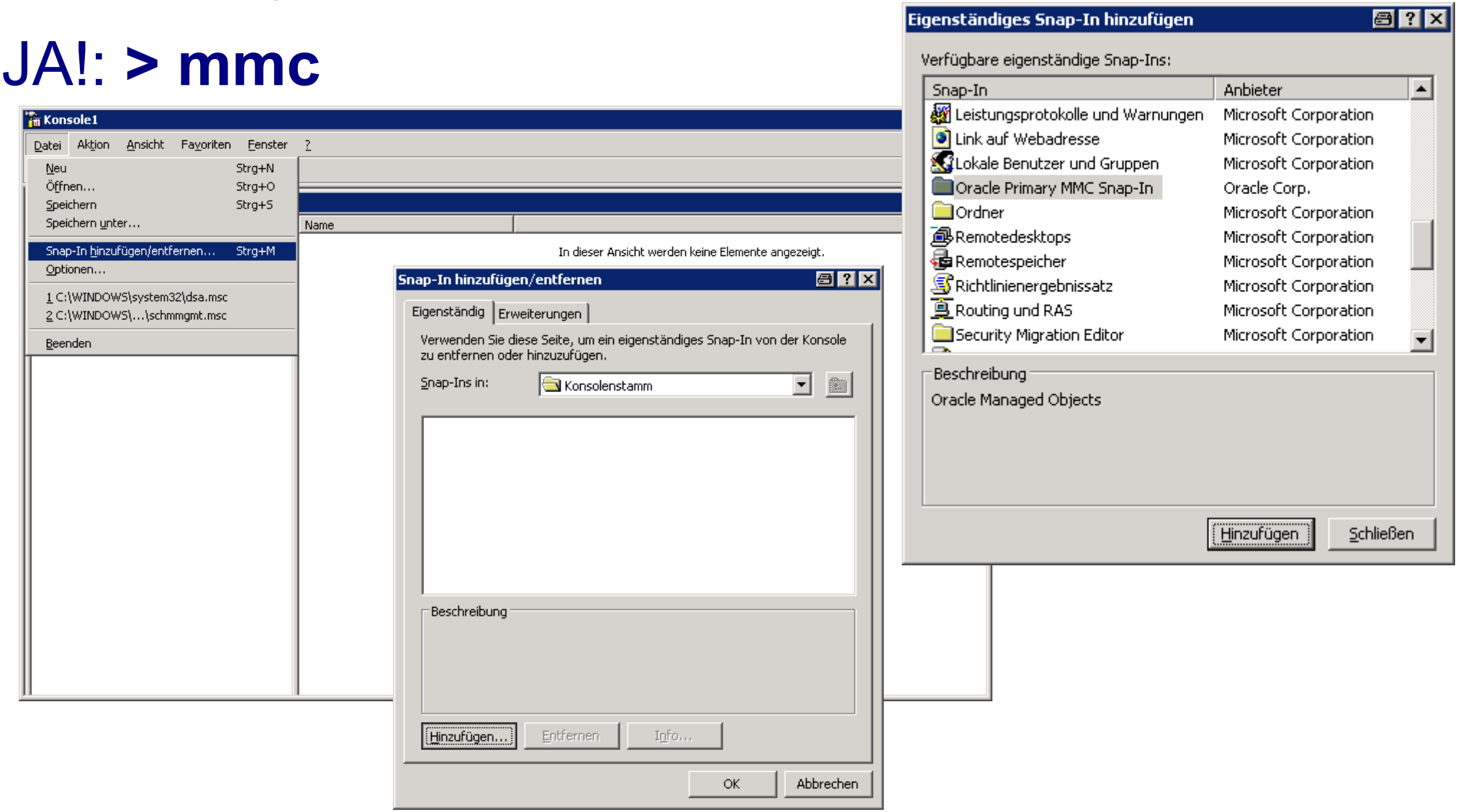
SQL*Plus

```
C:\Dokumente und Einstellungen\Administrator>sqlplus SYSTEM@NCORA

SQL*Plus: Release 10.2.0.1.0 - Production on Sa Feb 10 18:58:46 2007

Copyright (c) 1982, 2005, Oracle.  All rights reserved.

Kennwort eingeben:

Verbunden mit:
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Production
With the Partitioning, OLAP and Data Mining options

SQL> select user from dual;

USER
------------------------------
SYSTEM

SQL>
```

Testen (One last Thing)

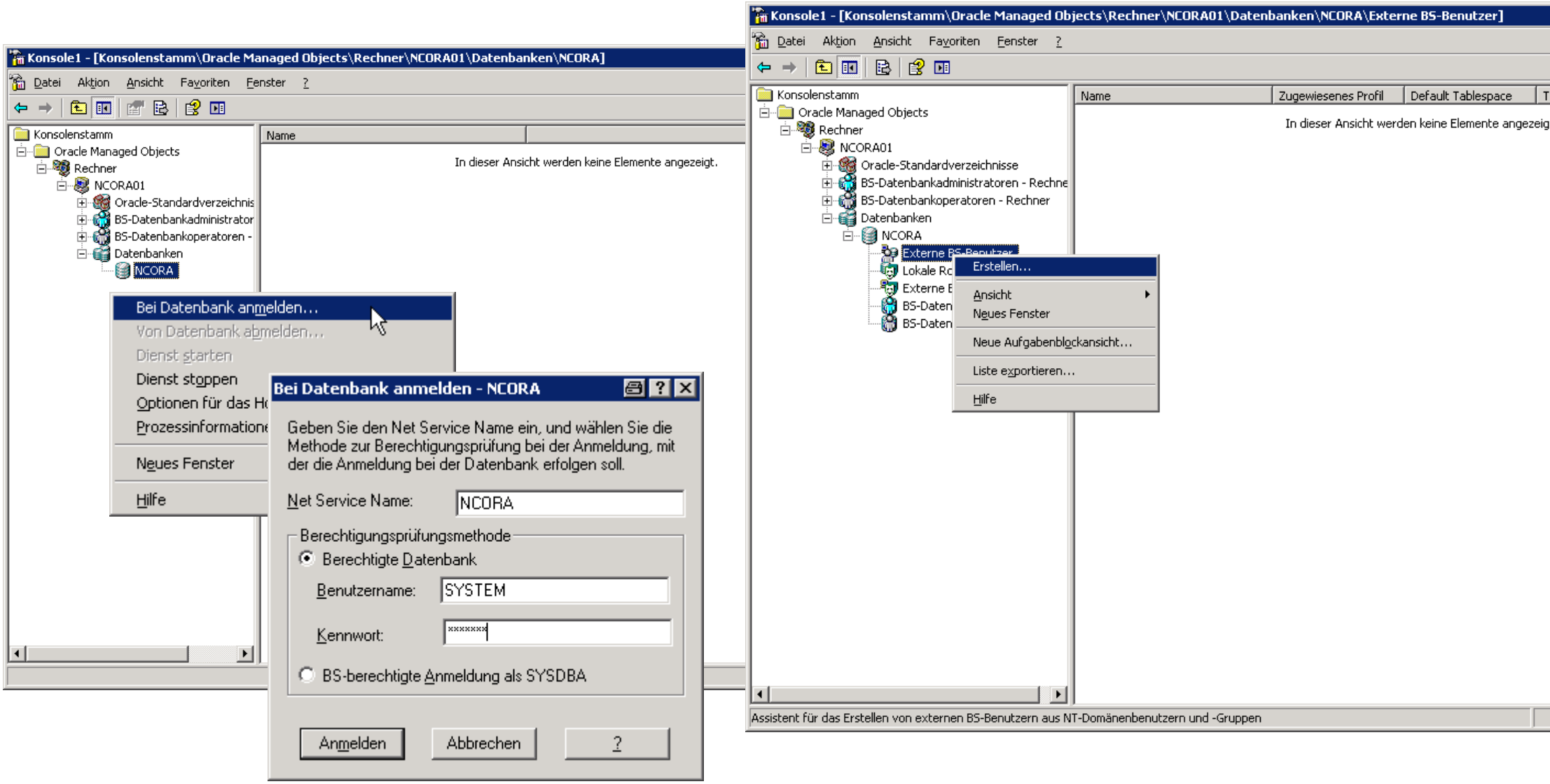
Belohnung des Installationsaufwandes?

JA!: **> mmc**



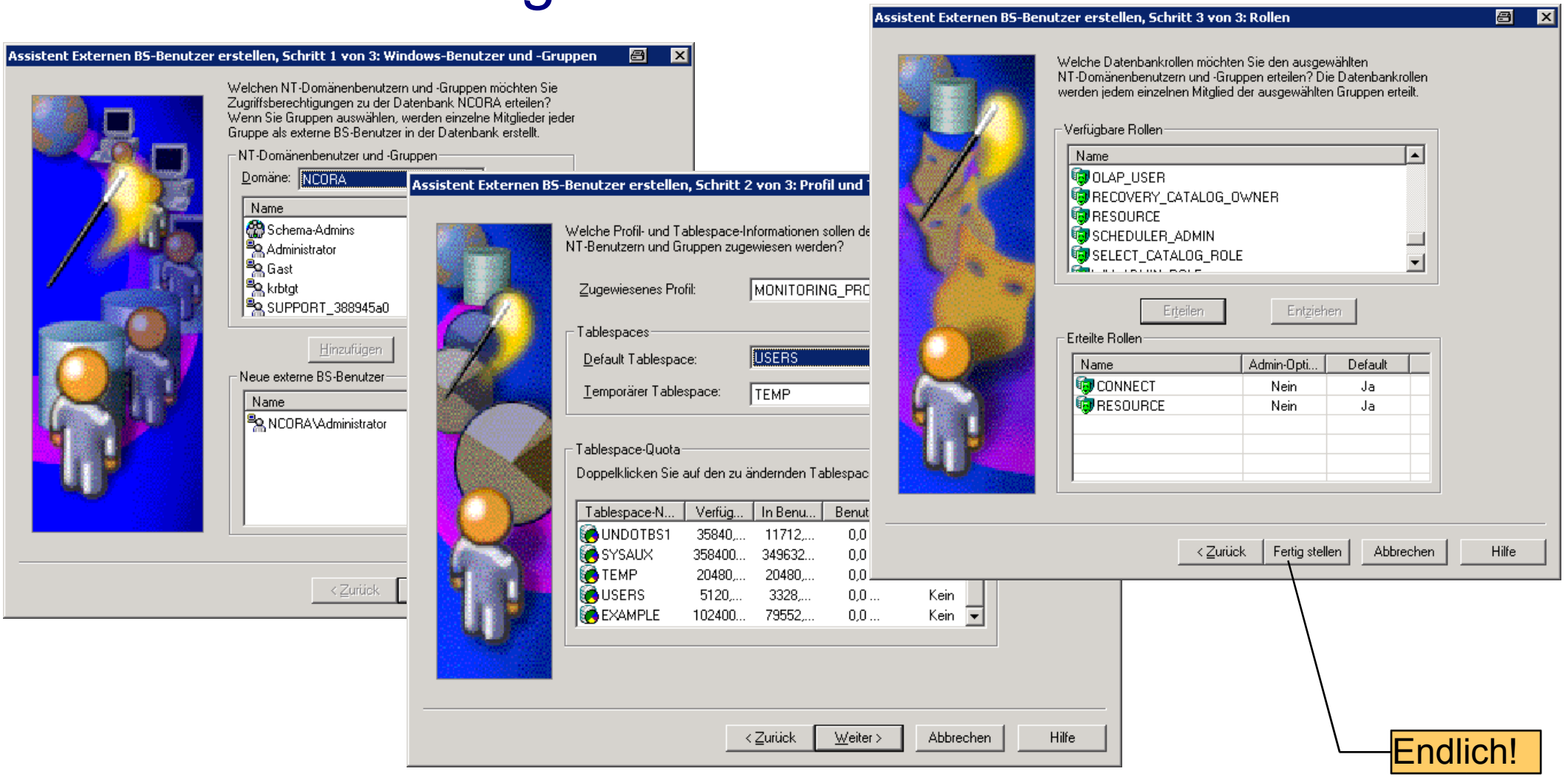
Testen (One last Thing)

Erstmal wieder klicken...



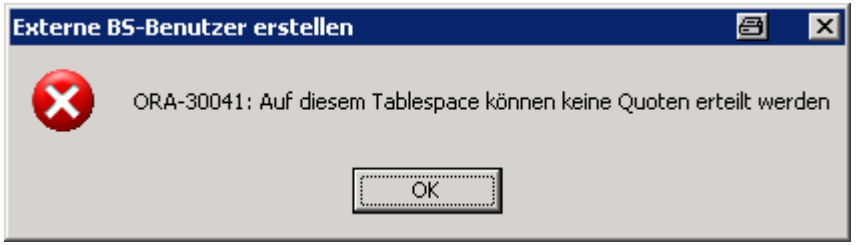
Testen (One last Thing)

Benutzer hinzufügen



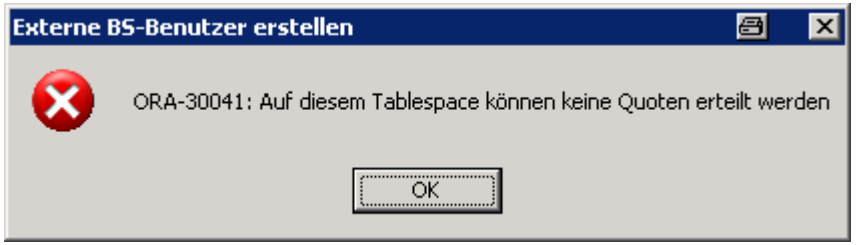
Testen (One last Thing)

Ganz normal.

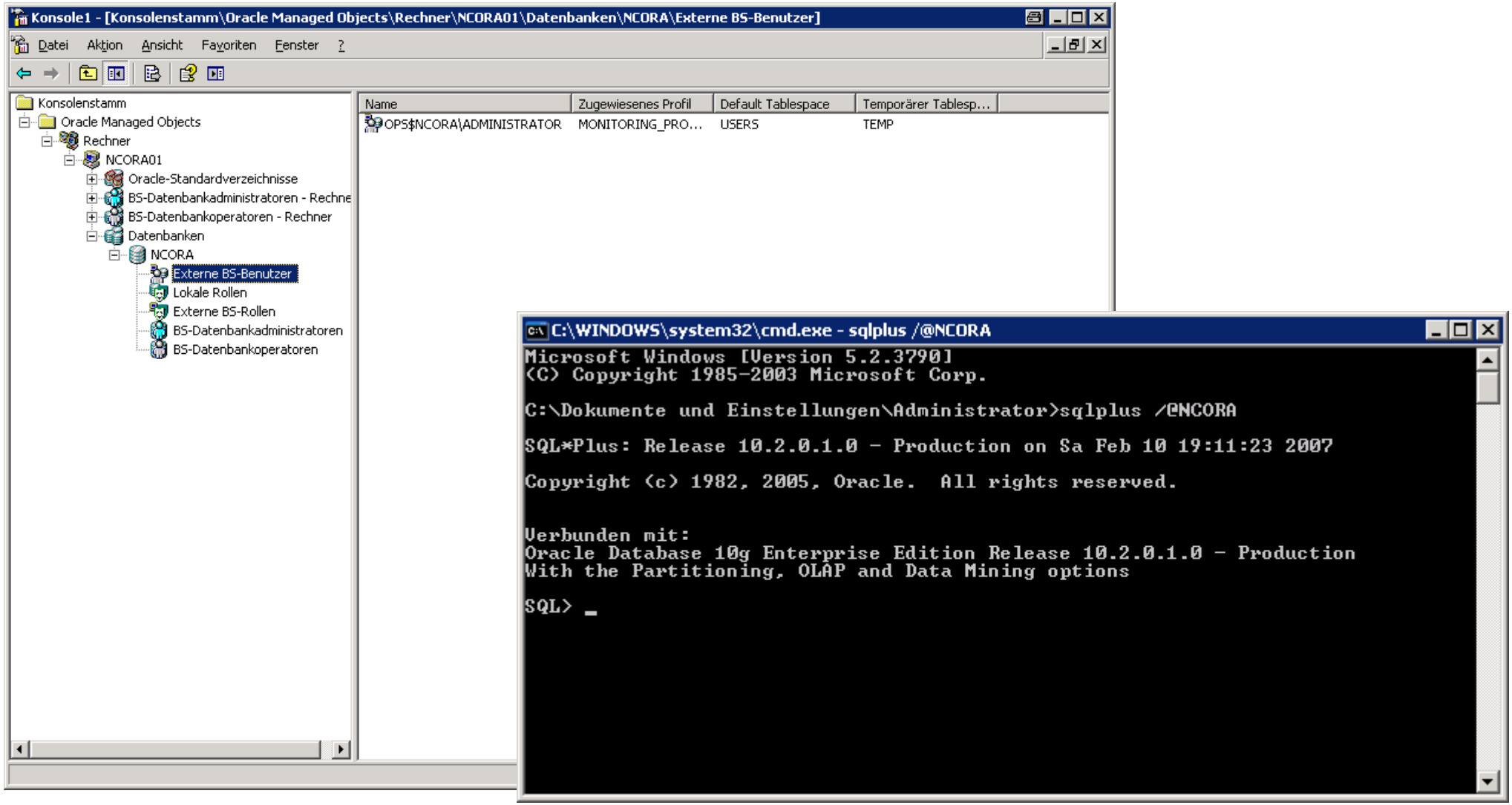


Testen (One last Thing)

Ganz normal #2.

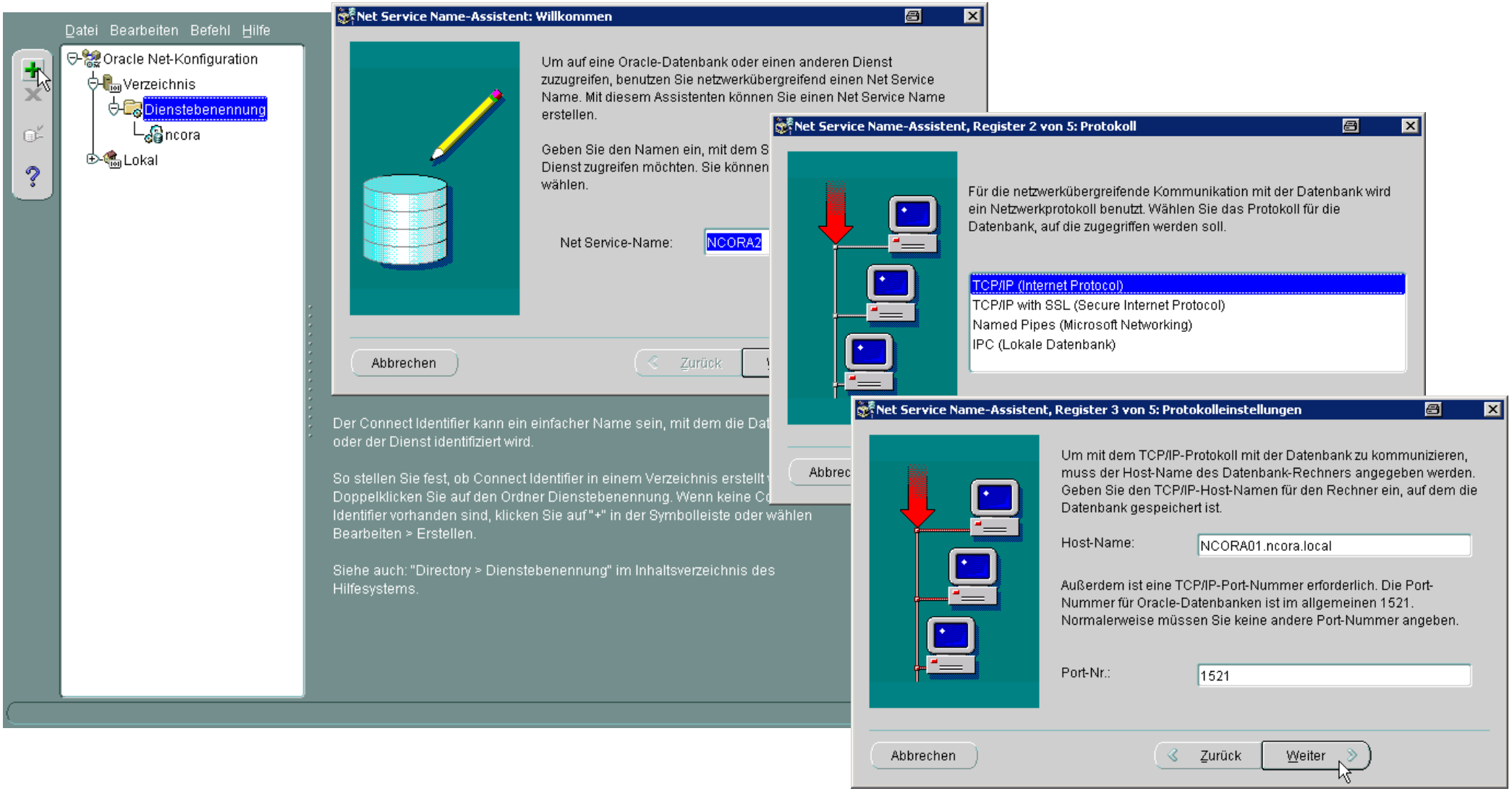


Testen (One really last Thing)

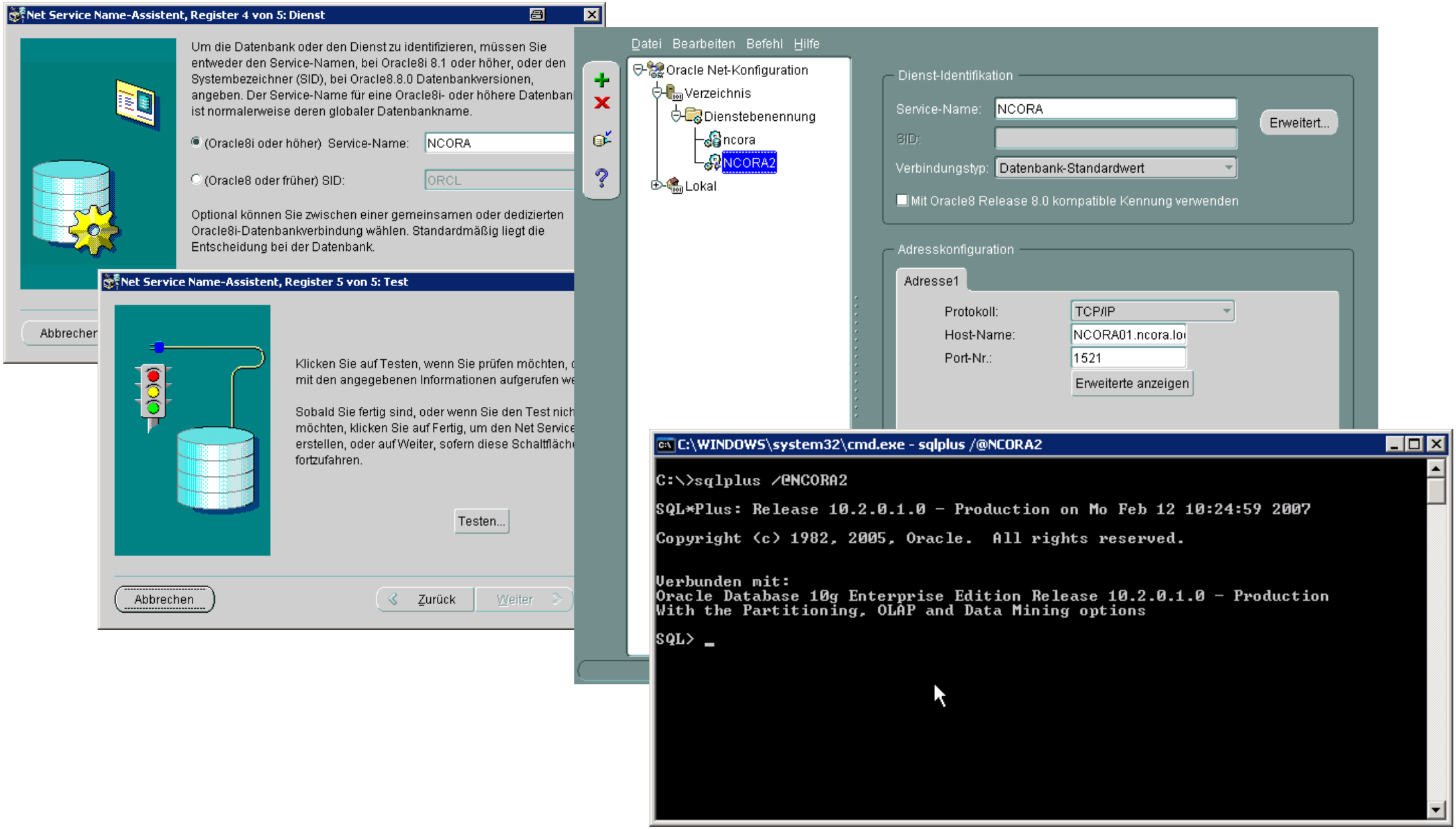


Datenbanken nachträglich hinzufügen

Oracle Net Manager



Datenbanken nachträglich hinzufügen (2)



AD-Integration-Fazit

Durchaus machbar

Praktisch gerade für kleinere Organisationen

Sicherheit vom geänderten AD muss noch im Detail geprüft werden

OpenLDAP

Open-Source-Referenzimplementierung des LDAPv3 Standards

Einfache Installation unter Linux

Mit Linux „Bordmitteln“ redundant auslegbar

Konfiguration OpenLDAP

Ablauf

Installation

Schema anlegen

DB-Aliase konfigurieren

SQLNet.ora auf dem Client anpassen

Testen

OpenLDAP installieren

Grundinstallation

Debian 3.1

```
~ # apt-get install slapd ldap-utils
```

/etc/ldap/slapd.conf

slappasswd

```
# slappasswd
New password:
Re-entssword:
{SSHA}4rNn65PM2DsXsLcLeLU3N+5nC0g2vuRC
```

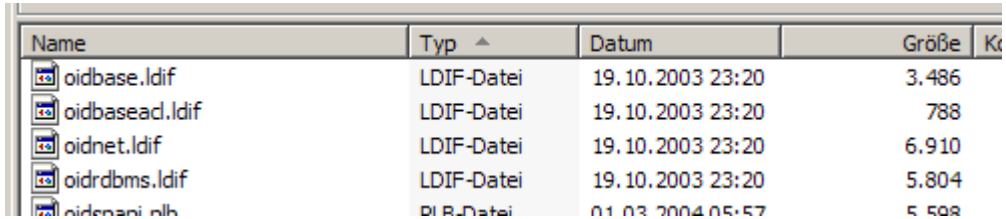
Base DN anpassen

```
# The base of your directory in database #1
suffix          "dc=nci,dc=local"

rootdn          "cn=admin,dc=nci,dc=local"
rootpw          {SSHA}4rNn65PM2DsXsLcLeLU3N+5nC0g2vuRC
```

Oracle-Schema anlegen

Oracle-*.ldif-Dateien vom OID auswerten

IAS-10g-9-0-4-2\Disk2\stage\Components\oracle.oid.server\9.0.4.0.0\1\DataFiles



Name	Typ	Datum	Größe
oidbase.ldif	LDIF-Datei	19.10.2003 23:20	3.486
oidbaseacl.ldif	LDIF-Datei	19.10.2003 23:20	788
oidnet.ldif	LDIF-Datei	19.10.2003 23:20	6.910
oidrdbms.ldif	LDIF-Datei	19.10.2003 23:20	5.804

Problem: .ldif-Format unterschiedlich zu OpenLDAP

Oracle-Schema anlegen

Über die IAS Installation suchen

Oracle-*.ldif-Dateien vom OID auswerten

```
oidbase.ldif
oidnet.ldif
oidrdbms.ldif
```

LDIF-Format für das OID erzeugen

```
#! /usr/bin/perl -w
#
# ldif2schema - convert Oracle Internet Directory schema extension
# ldif files to OpenLDAP schema files
#

while(<>) {
    chomp;
    s/DistinguishedNameMatch/distinguishedNameMatch/;
    if (s/^attributetypes:\s+//) {
        print "attributetype $_\n\n";
    }
    if (s/^objectclasses:\s+//) {
        print "objectClass $_\n\n";
    }
}
```

```
# for i in *.ldif; do ./convert.pl < $i > `basename $i .ldif`.schema; done
```

Oracle-Schema anlegen (Vergleich)

OID-Format:

```
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: ( 2.16.840.1.113894.7.1.1 NAME 'orclVersion' EQUALITY
caseIgnoreMatch SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' SINGLE-VALUE )
```

OpenLDAP-Format:

```
attributetype ( 2.16.840.1.113894.7.1.1 NAME 'orclVersion' EQUALITY
caseIgnoreMatch SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' SINGLE-VALUE )
```

Oracle-Schemas anlegen

Schema-Definition einbinden

/etc/ldap/slapd.conf

```
include         /etc/openldap/schema/oidbase.schema
include         /etc/openldap/schema/oidnet.schema
include         /etc/openldap/schema/oidrdbms.schema
```

LDAP-Daemons neustarten

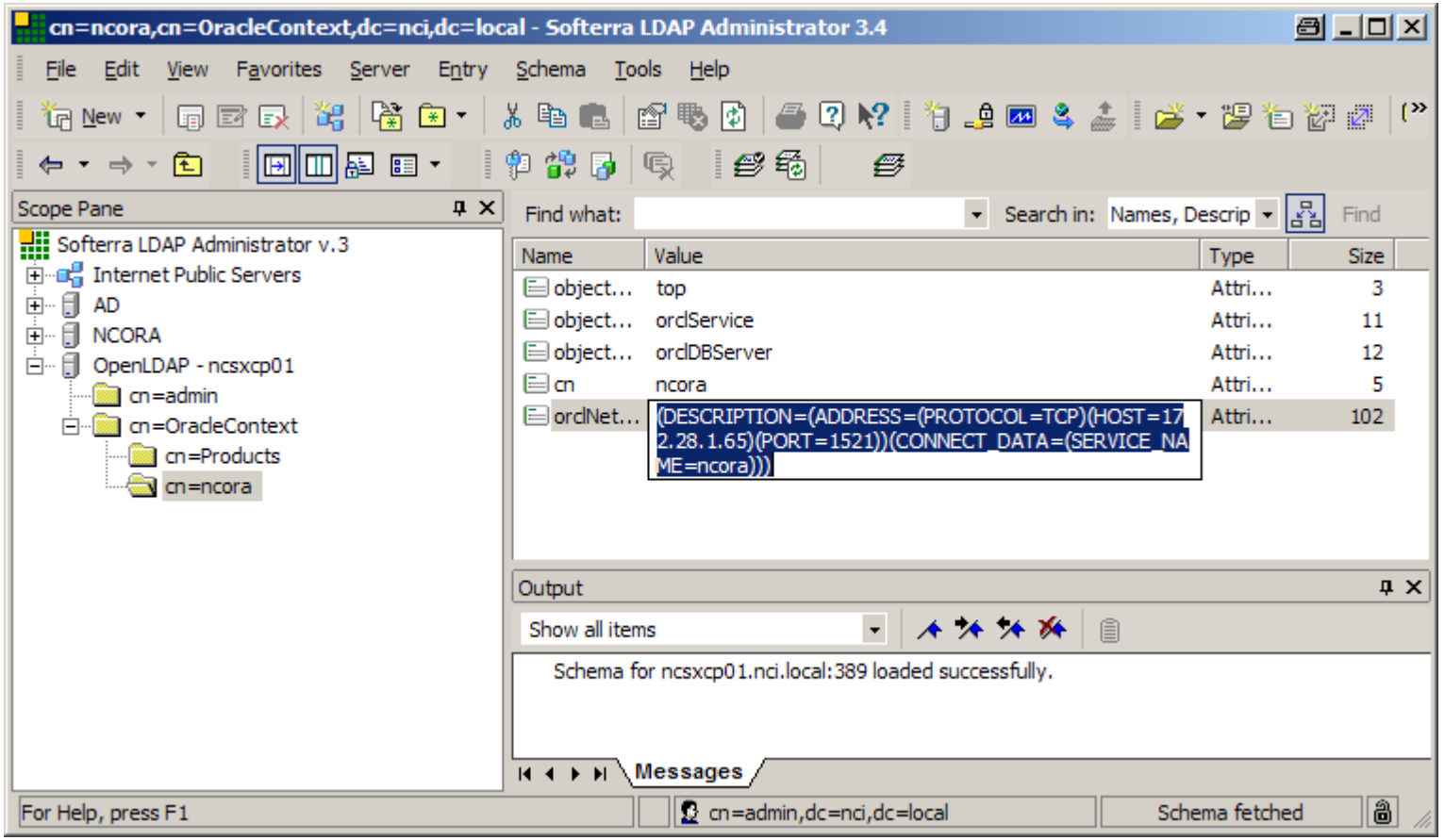
```
# /etc/init.d/slapd restart
Stopping OpenLDAP: slapd.
Starting OpenLDAP: running BDB recovery, slapd.
```

Oracle-Context & -Eintrag anlegen

Per LDIF anlegen

```
dn: CN=OracleContext,DC=nci,DC=local
objectClass: top
objectClass: orclContext
cn: OracleContext


dn: CN=Products,CN=OracleContext,DC=nci,DC=local
objectClass: top
objectClass: orclContainer
cn: Products


dn: CN=ncora,CN=OracleContext,DC=nci,DC=local
objectClass: top
objectClass: orclService
objectClass: orclDBServer
cn: ncora
orclNetDescString:
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=ncora01.ncora.local)(PORT=1521))(CONNECT
_DATA=(SERVICE_NAME=ncora)))
```

Überprüfen, ob der Eintrag existiert



Prüfen und testen

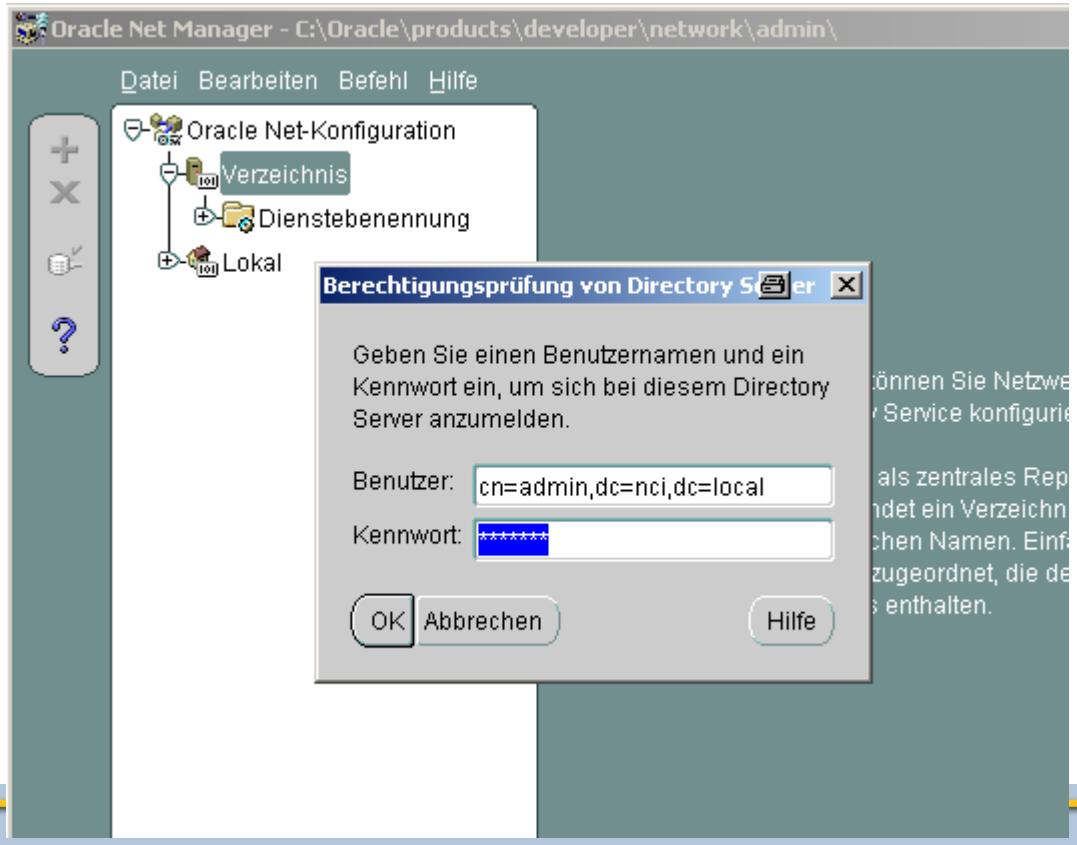
LDAP Search

```
ldapsearch -H ldap://172.28.1.54 -x -b "dc=nci,dc=local" "(objectclass=*)"
```

Auf die Reihenfolge der Parameter achten!

Net Manger

cn=admin,dc=nci,dc=local



Einträge ändern / hinzufügen

Über LDIF-Datei

-a
für neue Einträge!

```
ldapmodify -D "cn=admin,dc=nci,dc=local" -W -x -f tns_eintrag.ldif
```

```
dn: CN=oradev,CN=OracleContext,DC=nci,DC=local
cn: oradev
objectClass: top
objectClass: orclService
objectClass: orclDBServer
orclNetDescString:
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.3.23)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=DEV)))
orclNetDescName:  CN=ncora2,CN=OracleContext,DC=nci,DC=local
orclOracleHome: /home/oracle
orclSID: ncora
orclSystemName:  ncora
orclVersion: 10101
```

Einträge löschen

ldapdelete

```
ldapdelete -D "cn=admin,dc=nci,dc=local" -W -x
"CN=ncora2,CN=OracleContext,DC=nci,DC=local"
```

Einträge aus TNSNames.Ora importieren

Lösung A:

```
namesctl dump_ldap -f names.ldif
```

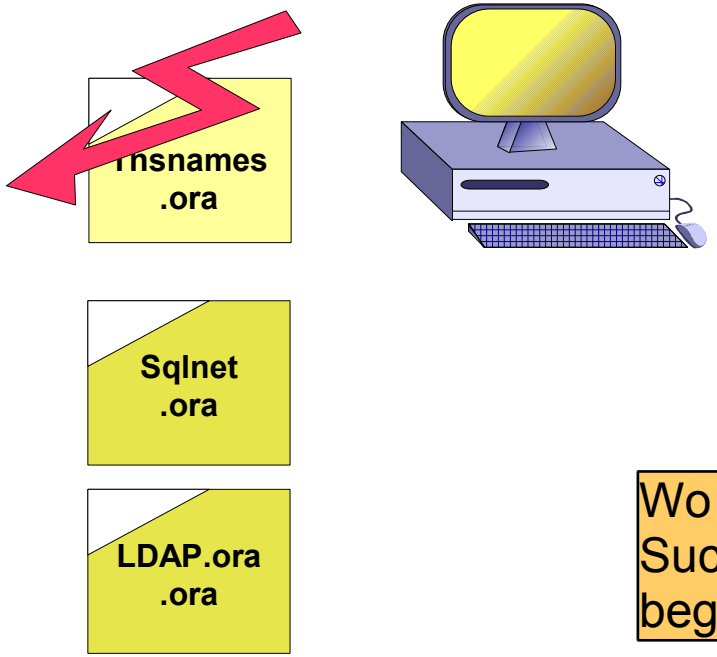
Lösung B:

Manuelles Erstellen der LDIF-Dateien

Erstellen einer Appliance

Den Client konfigurieren

SQLNET.ora und LDAP.ora anpassen



Sqlnet.ora

```
NAMES.DIRECTORY_PATH= (LDAP)
```

LDAP.ora

```
DIRECTORY_SERVERS= (192.168.2.17:389:636)

DIRECTORY_SERVER_TYPE = OID

DEFAULT_ADMIN_CONTEXT="dc=nci,dc=local"
```

Wo soll mit der Suche begonnen werden!

Testen

tnsping

```
H:\>tnsping ncora

TNS Ping Utility for 32-bit Windows: Version 9.0.1.4.1 - Production on 10-
FEB-2007 20:31:44

Copyright (c) 1997 Oracle Corporation.  All rights reserved.

Parameterdateien benutzt:
C:\Oracle\product\developer10g\network\admin\sqlnet.ora

Adapter LDAP zur Auflösung des Alias benutzt
Attempting to contact
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=172.28.1.65)(PORT=1521))(CONNECT_
DATA=(SERVICE_NAME=ncora)))
OK (20 msec)
```

Log überprüfen

tail -f /var/log/syslog (beim tnsping)

```
Feb 10 19:57:40 ncsxcp01 slapd[18669]: conn=64 fd=13 ACCEPT from
IP=172.28.1.20:1739 (IP=0.0.0.0:389)
Feb 10 19:57:40 ncsxcp01 slapd[18669]: conn=64 op=0 BIND dn="" method=128
Feb 10 19:57:40 ncsxcp01 slapd[18669]: conn=64 op=0 RESULT tag=97 err=0
text=
Feb 10 19:57:40 ncsxcp01 slapd[18669]: conn=64 op=1 SRCH
base="cn=ncora,cn=OracleContext,dc=nci,dc=local" scope=0 deref=2
filter="(objectClass=*)"
Feb 10 19:57:40 ncsxcp01 slapd[18669]: conn=64 op=1 SRCH attr=objectclass
orclNetDescString orclNetDescName orclVersion
Feb 10 19:57:40 ncsxcp01 slapd[18669]: conn=64 op=1 SEARCH RESULT tag=101
err=0 nentries=1 text=
Feb 10 19:57:40 ncsxcp01 slapd[18669]: conn=64 op=2 UNBIND
Feb 10 19:57:40 ncsxcp01 slapd[18669]: conn=64 fd=13 closed
```

```
Log einschalten mit :
/etc/syslog.conf =>>
        local4.debug    /var/log/slapd.log

kill -<HUP ID> <id von syslogd>

/etc/ldap/slapd.conf  ==>
loglevel            296
```

kill -l | grep HUP
=> ID für ein -HUP
(je nach OS!)

Testen (2)

sqlplus

```
H:\>sqlplus SYSTEM@ncora

SQL*Plus: Release 9.0.1.4.0 - Production on Sa Feb 10 20:32:56 2007

(c) Copyright 2001 Oracle Corporation.  All rights reserved.

Kennwort eingeben:

Verbunden mit:
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Production
With the Partitioning, OLAP and Data Mining options

SQL>
```

Zusammenfassung

Mit LDAP zentral und einfach den Zugriff auf die Datenbank in Unternehmen verwalten

Mit dem ActiveDirectory eine perfekte Integration in eine Windows-Umgebung realisieren

Beutzerberechtigung auch für Lesezugriffe wünschenswert

Mit OpenLDAP eine einfach Lösung betreiben

Verwendetes OID-Schema ist nur ein Auszug

Net Manager funktioniert nicht

Eigene Software zur Verwaltung verwenden

Ausblick

Test mit Windows-Longhorn-Server

Übernahme des kompletten OID-Schemas

Problem: Clientsoftware erwartet ursprüngliches Schema

Wrapper & Hilfsskripte

Out-Of-The Box (mit eigener Oberfläche)

Oracle SQL*Net

Kontakt:
Gunther Pippèrr
Sebastian Roth

gunther@pipperr.de

http://www.pipperr.de

Ihr Ansprechpartner für:
- Oracle Workshops und Training
- Oracle-Projekte mit Forms/Reports
- Java- und XML-Projekte
- Schnittstellen-Entwicklung
- Oracle-Lizenzen
- Remote Wartung und Administration
- Oracle Security

Quellen

Oracle Metalink/Tahiti (Suchfunktion benutzen!)

Oracle Whitepaper (September 2004)

Links

http://dizwell.com/prod/node/23

http://dizwell.com/prod/node/87

http://dizwell.com/prod/node/88

http://dizwell.com/prod/node/505

http://home.nc.rr.com/jtlayton/oid2openldap.html

http://www.softerra.com

http://notepad-plus.sf.net