

Ja, wo laufen Sie denn?

LDAP-Integration für SQL*Net



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

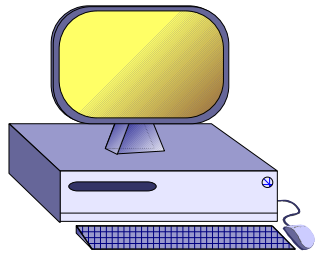
Eigenes Rechenzentrum

Wir sichern Ihre Datenbank

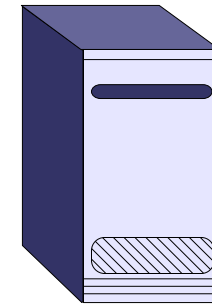
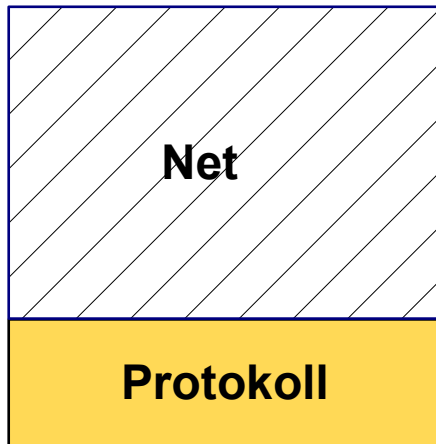
Entwicklung von Software mit Oracle-Werkzeugen
(Forms, Reports, Designer)

Eigenes Java-Framework XCP

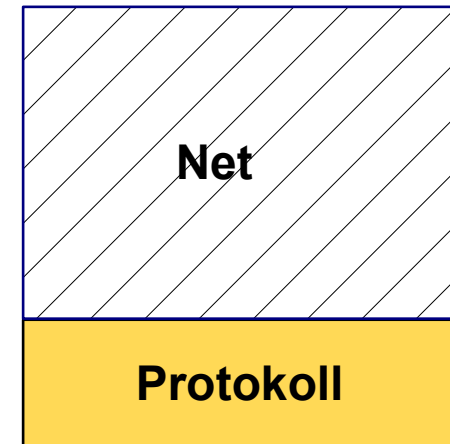
Überblick Oracle SQL*Net



Client



Server



Unterstützte Netzwerk-Protokolle:

TCP/IP

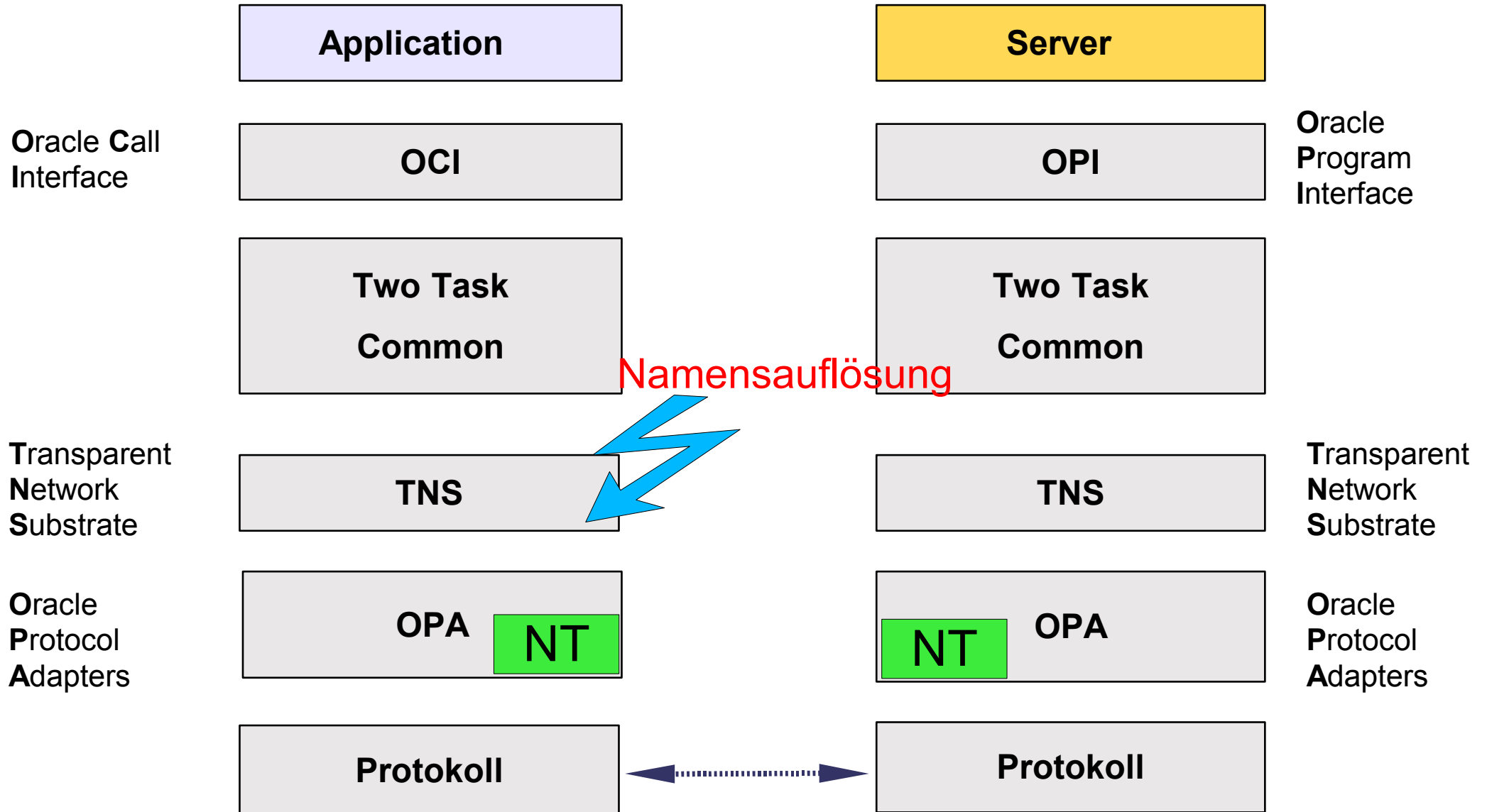
SPX/IPX

DecNet , IBM LU6.2, usw.

Die Oracle-Net-Architektur

Client

Server



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)

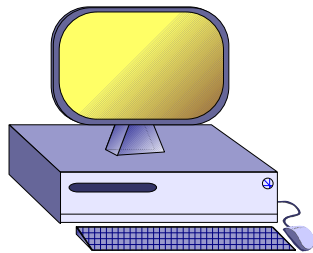
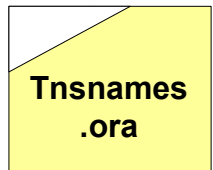
Verzeichnisdienst nutzen

Die wichtigsten Steuerdateien

Default-Verzeichnis \$Oracle_Home/network/admin/

Setzen der default Location mit der TNS_ADMIN-Umgebungsvariable

Client

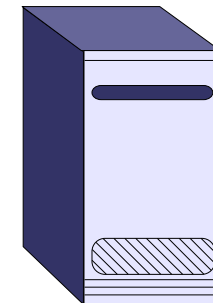


Tnsnames.ora



Sqlnet.ora

Server



listener.ora

Local Naming

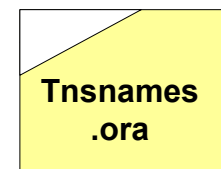
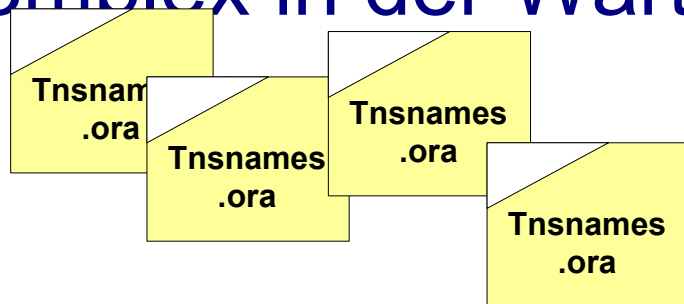
Der TNSalias wird über die Datei tnsnames.ora aufgelöst

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) ← Rechner  
                (HOST = localhost)  
                (PORT = 1521) ← Port Listener  
      )  
    )  
    (CONNECT_DATA =  
      (SERVICE_NAME = gpi) ← 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

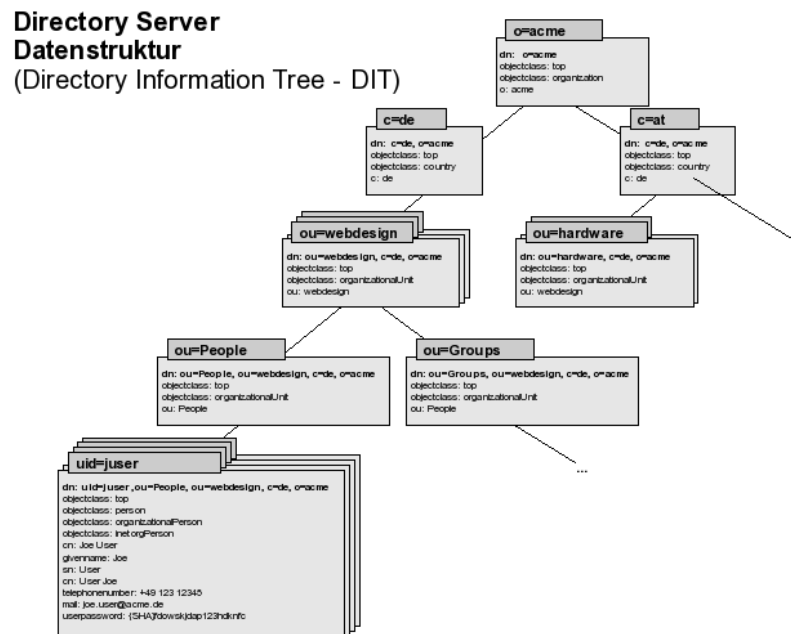
Lightweight Directory Access Protocol (LDAP)

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

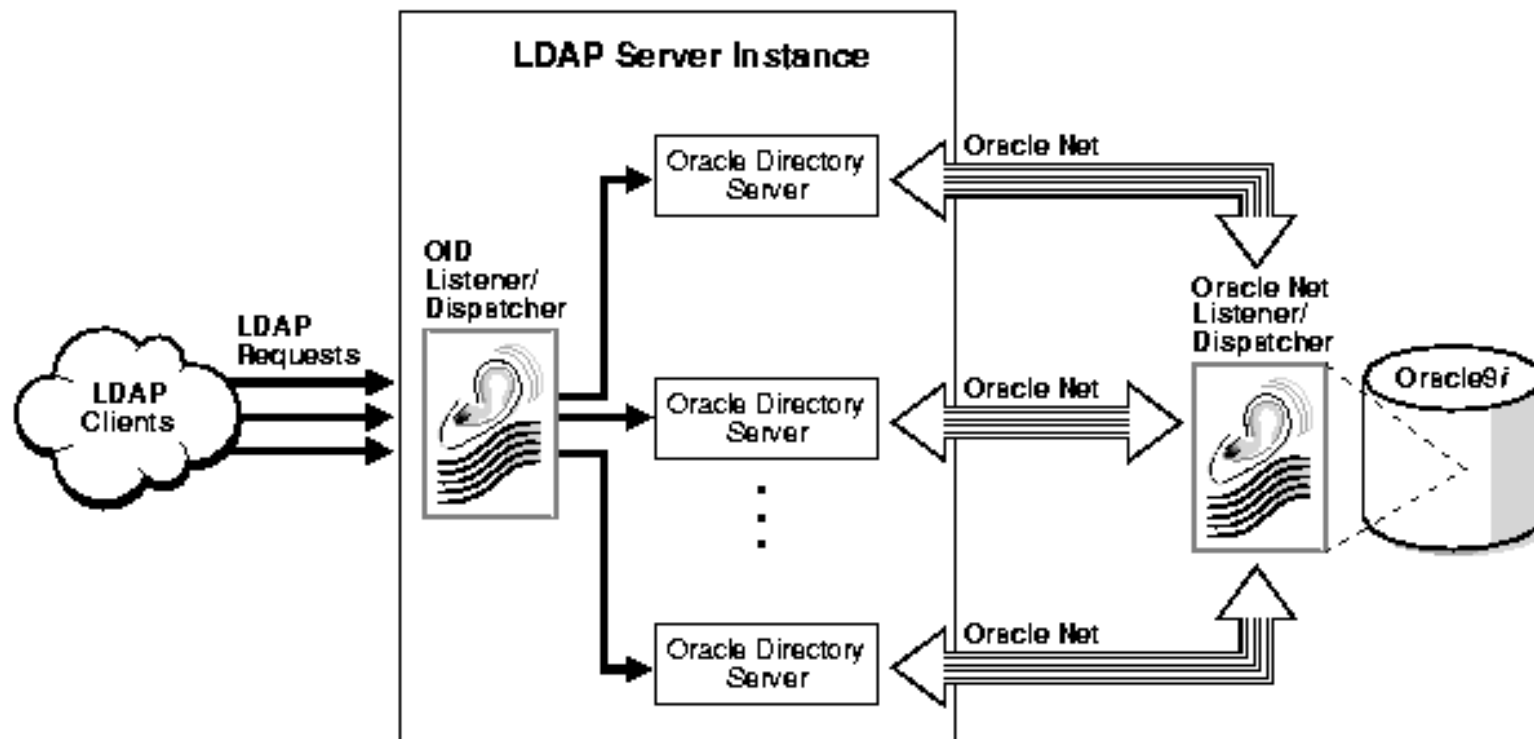
Produktübergreifend

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

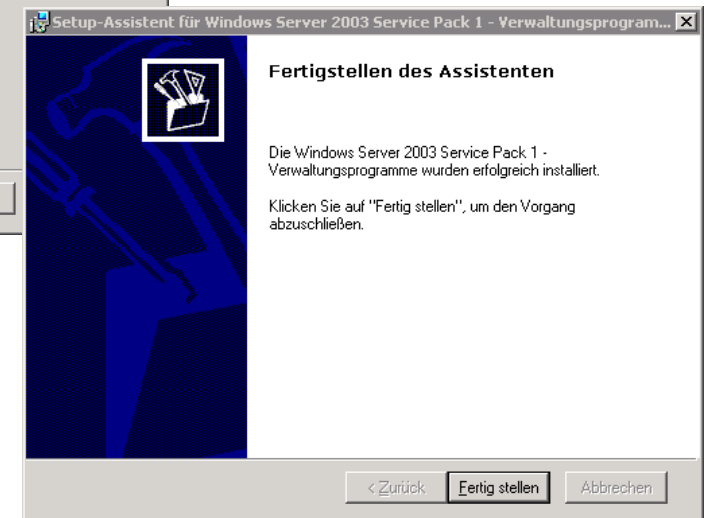
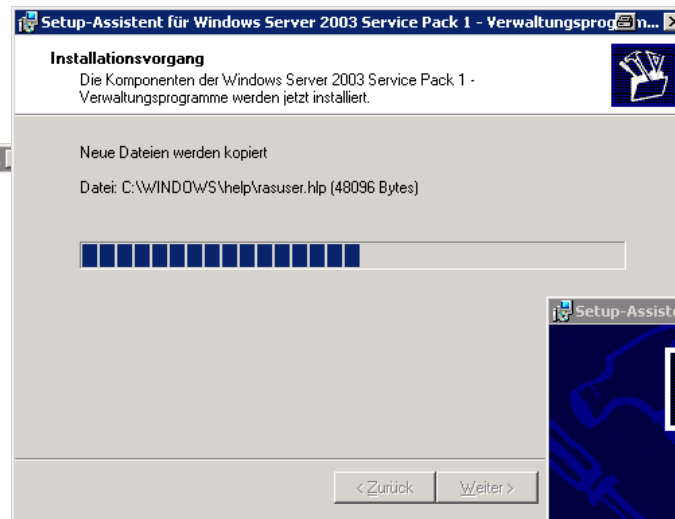
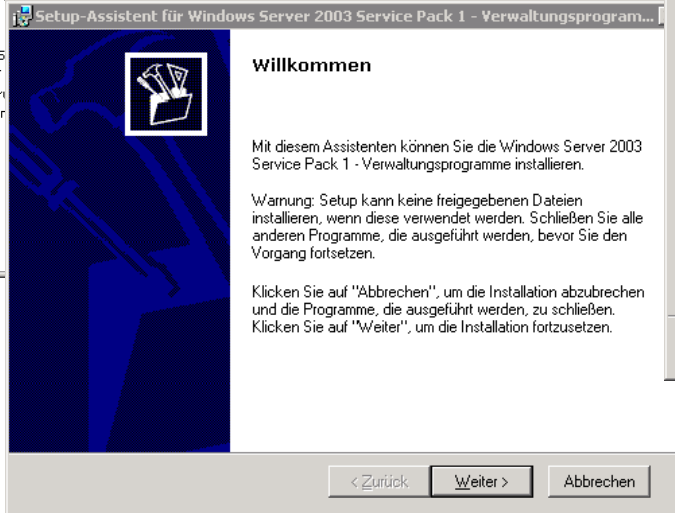
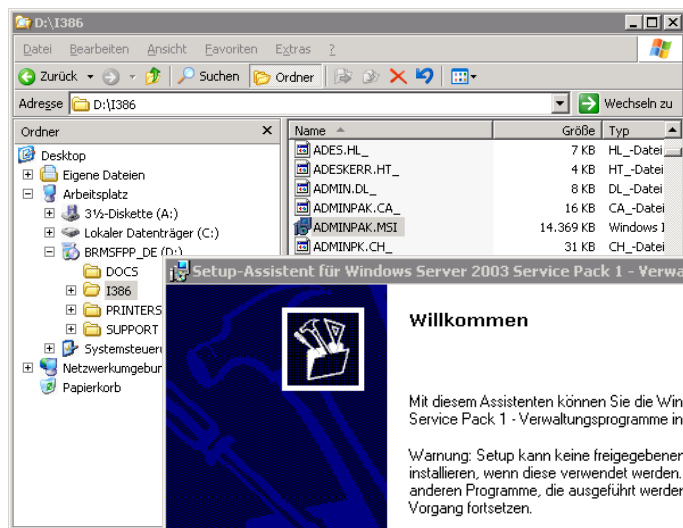
Testen

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

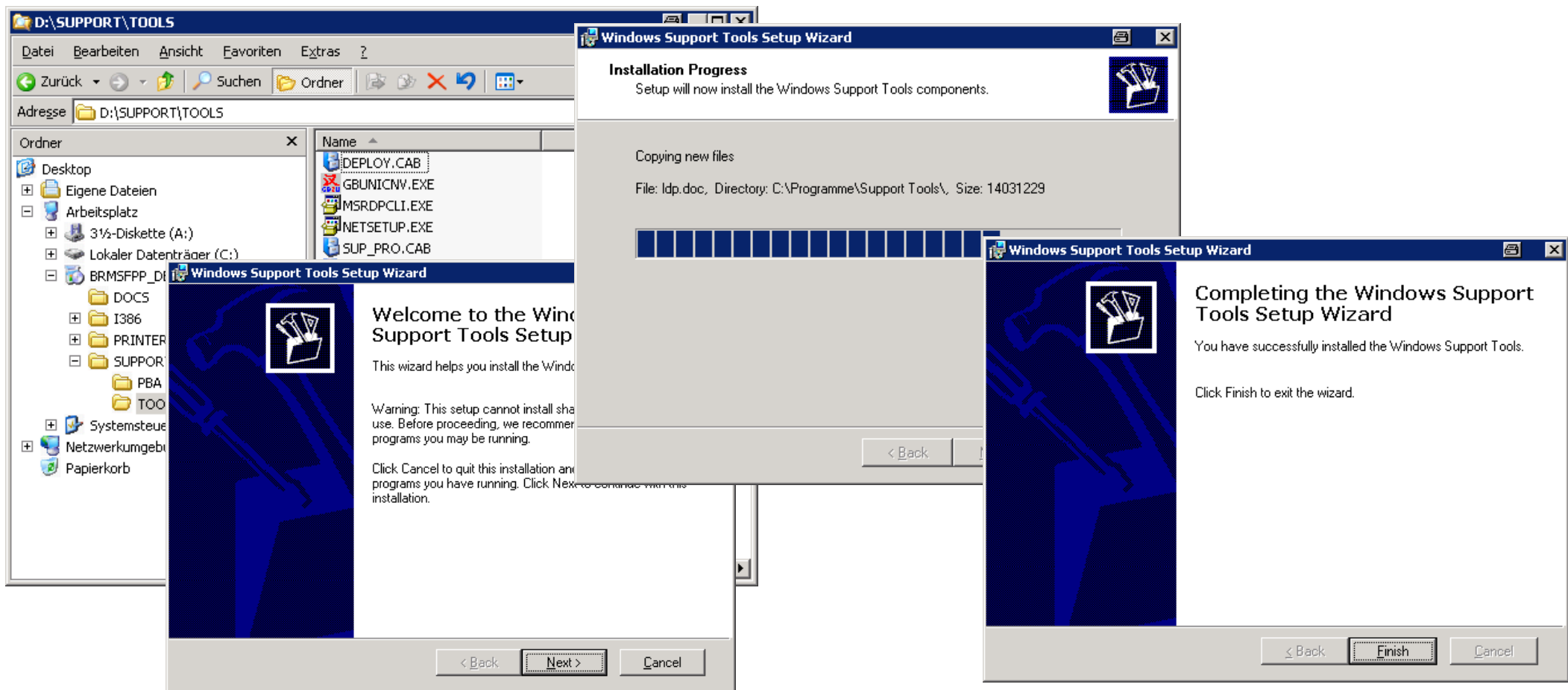


Wichtig für die Kontrolle des AD's

# 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)

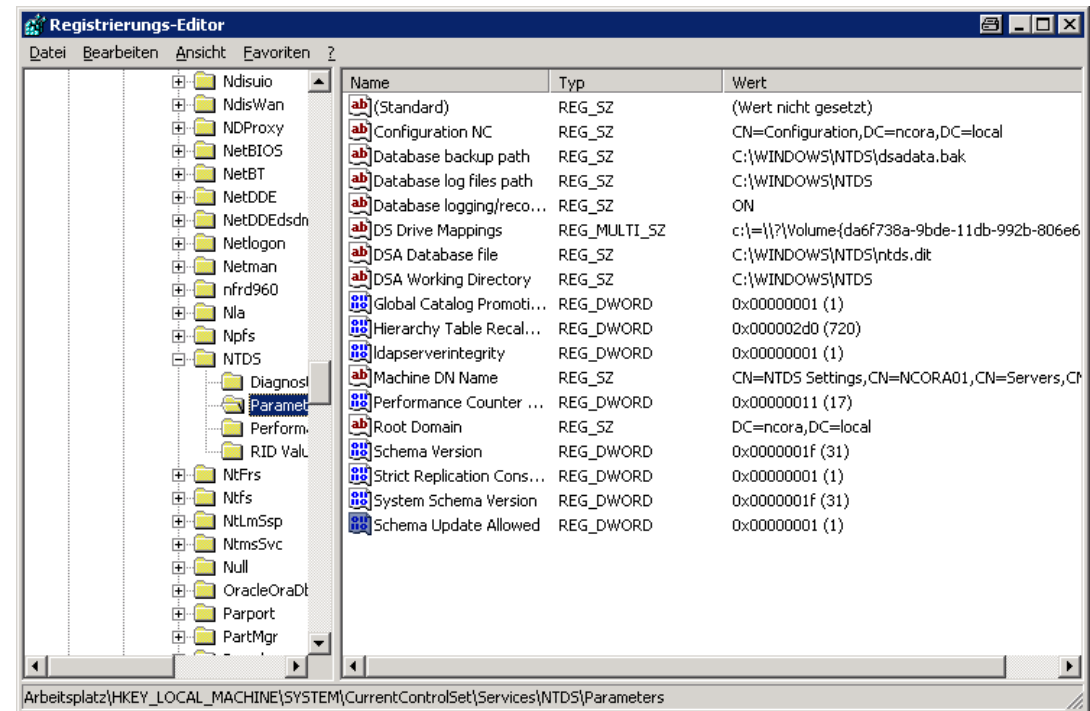
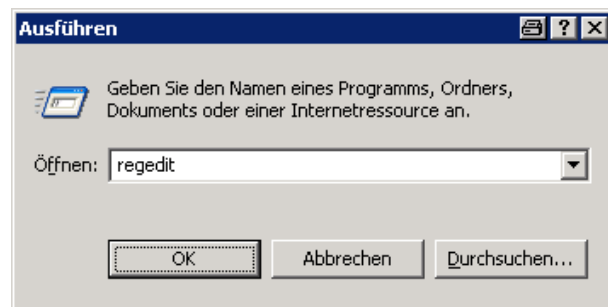
## Registry auf dem PDC anpassen

KEY:

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

Neuer Parameter (Typ DWORD) :

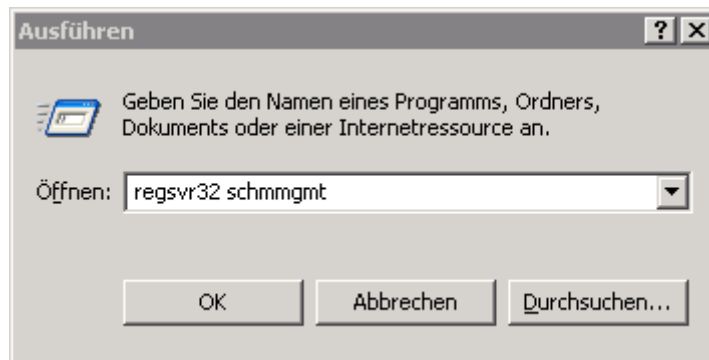
```
Schema Update Allowed = 1
```



# 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

Snap-In unter  
Konsolenstamm

The image shows a sequence of steps to load the ADSI Edit snap-in into the console tree. It includes the 'Ausführen' dialog with 'mmc' entered, the 'Konsole1' window with the 'Snap-In hinzufügen/entfernen...' menu item selected, the 'Snap-In hinzufügen/entfernen' dialog with 'Konsolenstamm' selected, and the 'Eigenständiges Snap-In hinzufügen' dialog with 'ADSI Edit' selected from the list of available snap-ins.

**Ausführen**

Geben Sie den Namen eines Programms, Ordners, Dokuments oder einer Internetressource an.

Öffnen: mmc

OK Abbrechen Durchsuchen...

**Konsole1**

Datei Aktion Ansicht Favoriten Fenster ?

- Neu Strg+N
- Öffnen... Strg+O
- Speichern Strg+S
- Speichern unter...
- Snap-In hinzufügen/entfernen... Strg+M**
- Optionen...
- C:\WINDOWS\... \schmmgmt.msc
- Beenden

**Snap-In hinzufügen/entfernen**

Eigenständig Erweiterungen

Verwenden Sie diese Seite, um ein eigenständiges Snap-In von der Konsole zu entfernen oder hinzuzufügen.

Snap-Ins in: Konsolenstamm

Hinzufügen... Entfernen Info... OK Abbrechen

**Eigenständiges Snap-In hinzufügen**

Verfügbare eigenständige Snap-Ins:

| Snap-In                               | Anbieter                 |
|---------------------------------------|--------------------------|
| .NET Framework 1.1 Configuration      | Microsoft Corporation    |
| Active Directory-Benutzer und -Co...  | Microsoft Corporation    |
| Active Directory-Domänen und -Ve...   | Microsoft Corporation    |
| Active Directory-Schema               | Microsoft Corporation    |
| Active Directory-Standorte und -Di... | Microsoft Corporation    |
| ActiveX-Steuerelement                 | Microsoft Corporation    |
| <b>ADSI Edit</b>                      | Microsoft Corporation    |
| Autorisierungs-Manager                | Microsoft Corporation    |
| Computerverwaltung                    | Microsoft Corporation    |
| Datenträgerverwaltung                 | Microsoft und VERITAS... |

Beschreibung

A low level Active Directory Services Interface editor.

Hinzufügen Schließen

# ADSI aktivieren (2)

## Zum Server verbinden

The screenshot shows the ADSI Edit console window with a context menu open over the 'Configuration' object. Two 'Connection Settings' dialog boxes are overlaid. The left dialog is for the 'Configuration' object, and the right dialog is for the 'Domain' object. A yellow callout box with the text 'Reihenfolge beachten!' (Pay attention to the order!) points to the sequence of dialog boxes.

**Connection Settings (Left):**

- Name: Configuration
- Path: LDAP://ncora01.ncora.local/Configuration
- Connection Point:
  - Select or type a Distinguished Name or Naming Context:
  - Select a well known Naming Context: Configuration
- Computer:
  - Select or type a domain or server:
  - Default (Domain or server that you logged in to)

**Connection Settings (Right):**

- Name: Domain
- Path: LDAP://ncora01.ncora.local/Domain
- Connection Point:
  - Select or type a Distinguished Name or Naming Context:
  - Select a well known Naming Context: Domain
- Computer:
  - Select or type a domain or server:
  - Default (Domain or server that you logged in to)

**Callout Box:** Reihenfolge beachten!

# ADSI aktivieren (3)

Anonymes Browsen des AD wird erlaubt!

## Parameter dSHeuristics anpassen

Ankreuzen!

The screenshot shows the ADSI Edit console with the 'CN=Directory Service Properties' dialog box open. The 'Attribute Editor' tab is active, and the 'dSHeuristics' attribute is selected in the list. The 'String Attribute: Editor' dialog is also open, showing the value '0000002'. A yellow callout box points to the 'dSHeuristics' attribute in the list with the text 'Achtung! Anzahl der 0 = 6\*'. Another yellow callout box points to the 'Show mandatory attributes' and 'Show optional attributes' checkboxes in the 'Attribute Editor' dialog, with the text 'Ankreuzen!'.

| Attribute              | Syntax            | Value                   |
|------------------------|-------------------|-------------------------|
| directReports          | Distinguished ... | <Not Set>               |
| displayName            | Unicode String    | <Not Set>               |
| displayNamePrintable   | IA5-String        | <Not Set>               |
| distinguishedName      | Distinguished ... | CN=Directory Service,CN |
| dSASignature           | Octet String      | <Not Set>               |
| dSCorePropagationD...  | UTC Coded Ti...   | <Not Set>               |
| dSHeuristics           | Unicode String    | <Not Set>               |
| extensionName          | Unicode String    | <Not Set>               |
| flags                  | Integer           | <Not Set>               |
| fromEntry              | Boolean           | TRUE                    |
| frsComputerReferenc... | Distinguished ... | <Not Set>               |
| frsMemberReferenc...   | Distinguished ... | <Not Set>               |
| frsMORoleOwner         | Distinguished ... | <Not Set>               |

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

# Anpassung des Active Directory (4)

## Berechtigungen im AD für den anonymen Zugriff setzen

The screenshot shows the Active Directory console window for the domain 'ncora.local'. The left pane shows the tree structure with 'Benutzer, Computer oder Gruppen wählen' selected. The right pane shows a list of objects in the domain. A dialog box is open in the foreground, allowing the user to select an object type and search for it.

| Name            | Typ                | Beschreibung                   |
|-----------------|--------------------|--------------------------------|
| Builtin         | builtinDomain      |                                |
| Computers       | Container          | Default container for upgr...  |
| Domain Cont...  | Organisationsei... | Default container for dom...   |
| ForeignSecur... | Container          | Default container for secu...  |
| LostAndFound    | lostAndFound       | Default container for orph...  |
| NTDS Quotas     | msDS-QuotaCo...    | Quota specifications cont...   |
| OracleContext   | Oracle Context     |                                |
| Program Data    | Container          | Default location for storag... |
| System          | Container          | Builtin system settings        |
| Users           | Container          | Default container for upgr...  |
| Infrastructure  | infrastructureU... |                                |

**Benutzer, Computer oder Gruppen wählen**

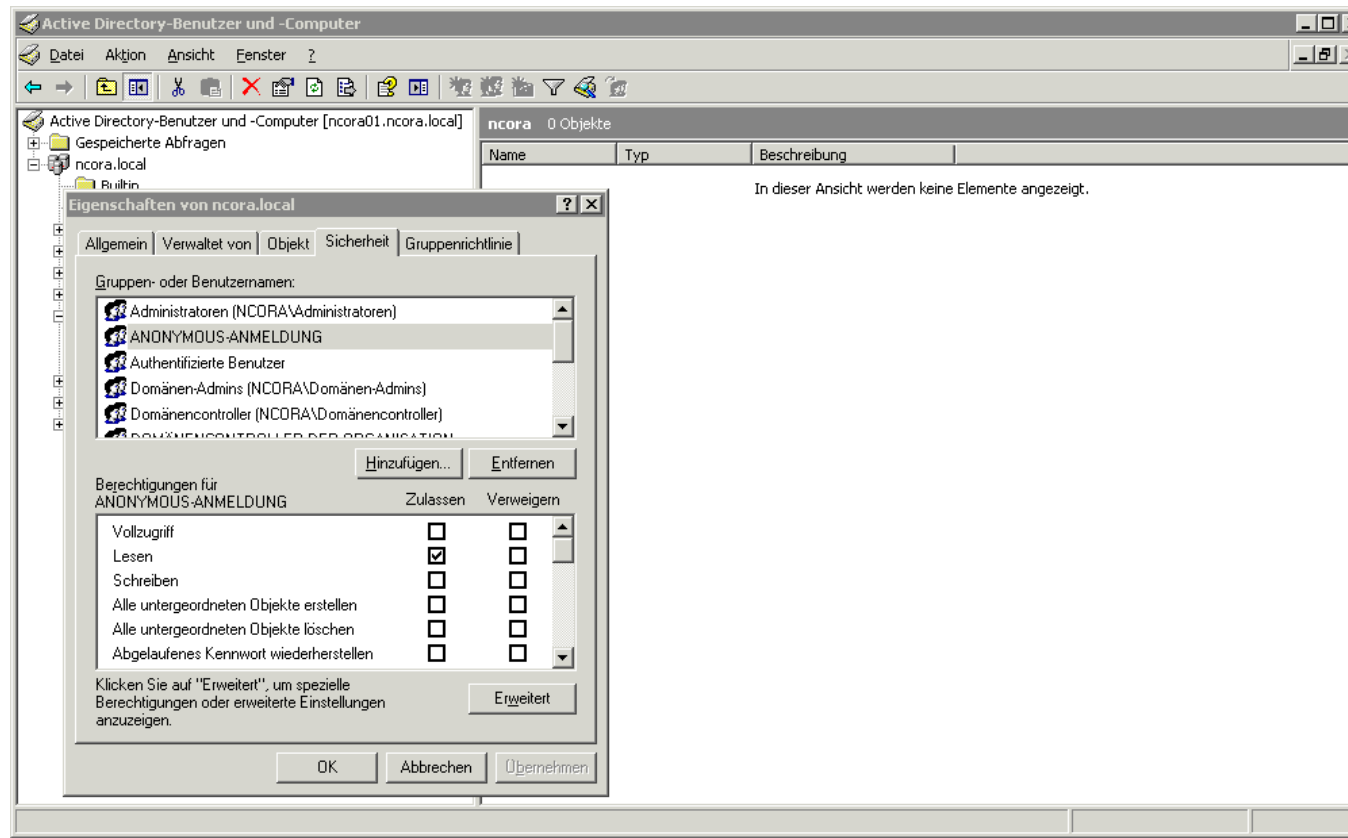
Objekttyp:  
Benutzer, Gruppen oder Integrierte Sicherheitsprinzipale

Suchpfad:  
ncora.local

Geben Sie die zu verwendenden Objektnamen ein (Beispiele):  
anonym

# Anpassung des Active Directory (5)

## Berechtigungen im AD für den anonymen Zugriff setzen (rekursiv)

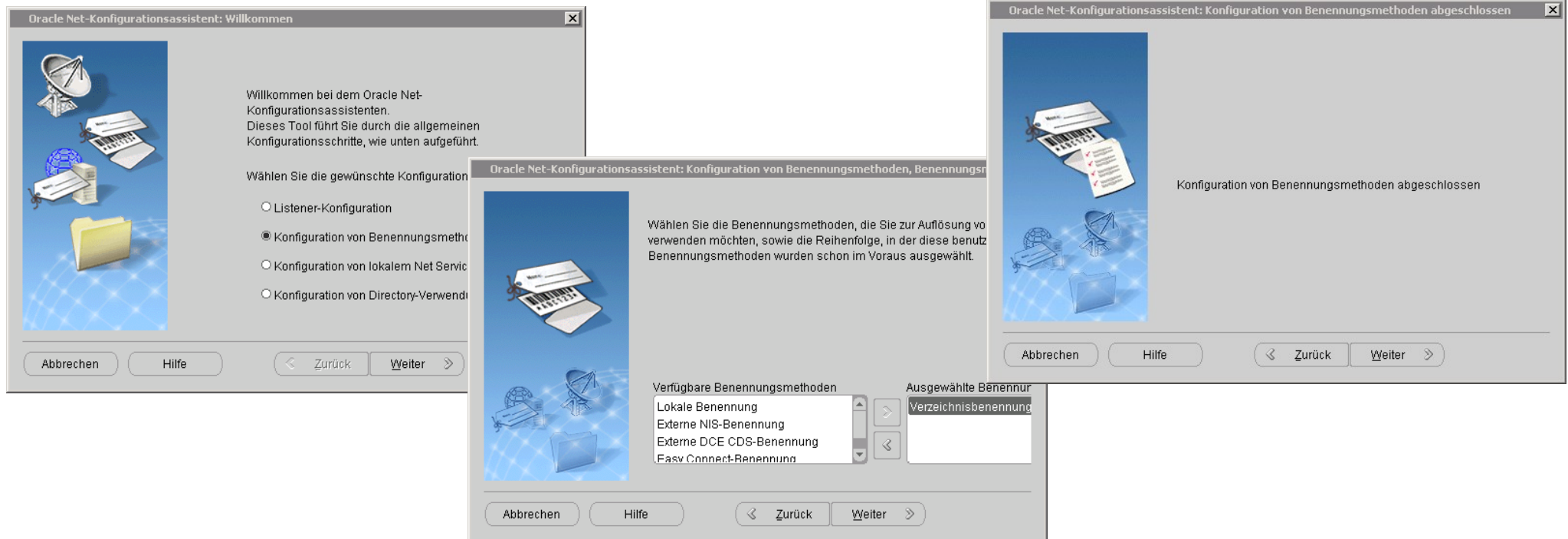


# Oracle Net Configuration Assistant

Oracle auf dem Win2003 Server installiert (ohne DB)

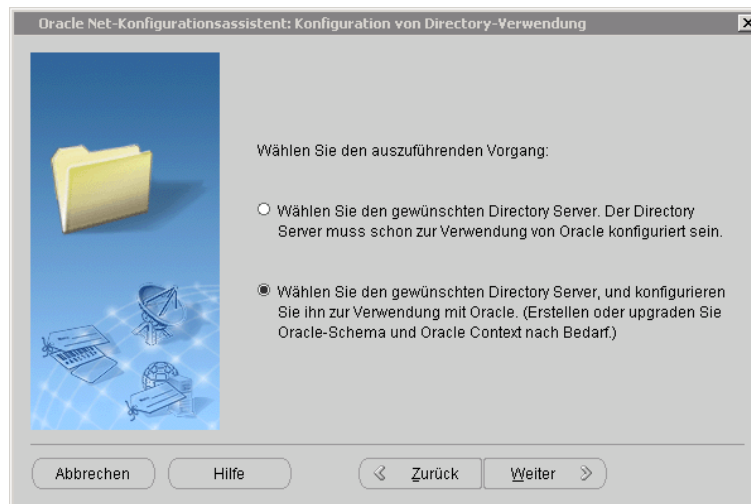
Start vom Oracle NetCa

Benennungsmethode konfigurieren



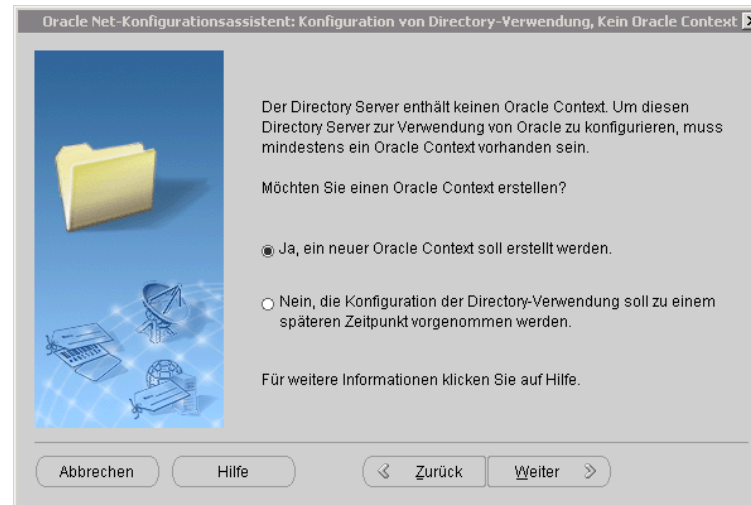
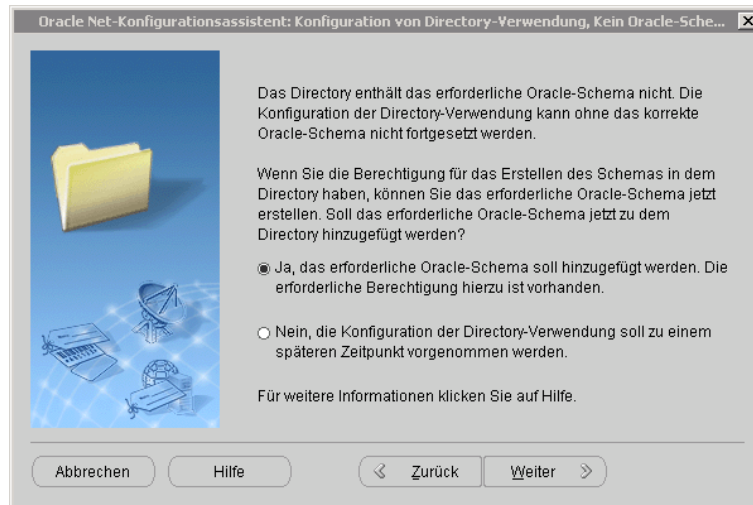
# Oracle Net Configuration Assistant

## Konfigurations-Directory



# Oracle Net Configuration Assistant (1)

## Konfigurations-Directory





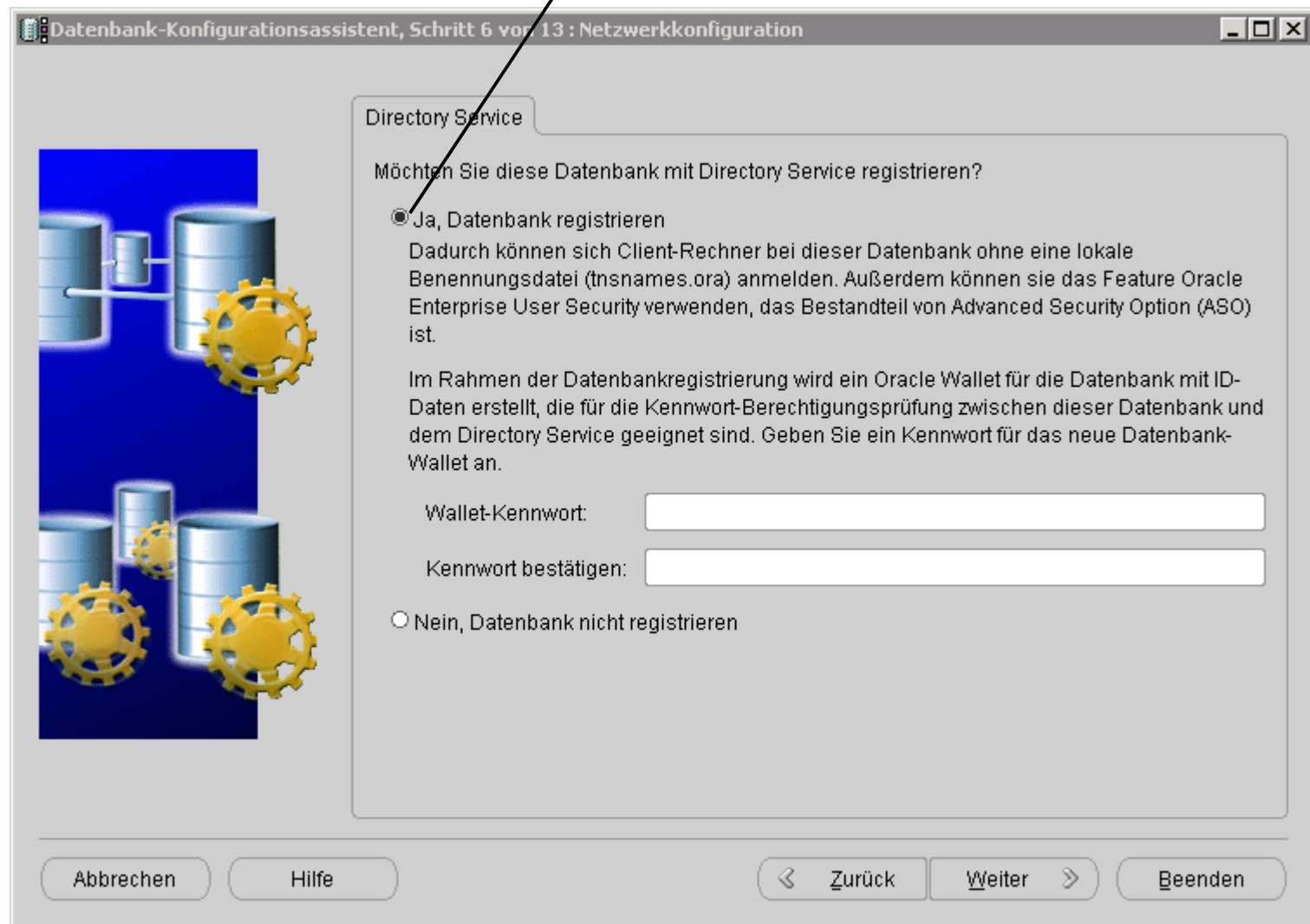


# Registrieren bei der Datenbank erstellen

Normale Installation

Seite 6:

Wenn alles geklappt hat!



Datenbank-Konfigurationsassistent, Schritt 6 von 13 : Netzwerkconfiguration

Directory Service

Möchten Sie diese Datenbank mit Directory Service registrieren?

Ja, Datenbank registrieren

Dadurch können sich Client-Rechner bei dieser Datenbank ohne eine lokale Benennungsdatei (tnsnames.ora) anmelden. Außerdem können sie das Feature Oracle Enterprise User Security verwenden, das Bestandteil von Advanced Security Option (ASO) ist.

Im Rahmen der Datenbankregistrierung wird ein Oracle Wallet für die Datenbank mit ID-Daten erstellt, die für die Kennwort-Berechtigungsprüfung zwischen dieser Datenbank und dem Directory Service geeignet sind. Geben Sie ein Kennwort für das neue Datenbank-Wallet an.

Wallet-Kennwort:

Kennwort bestätigen:

Nein, Datenbank nicht registrieren

Abbrechen Hilfe Zurück Weiter Beenden

# Registrieren bei der Datenbank erstellen (2)

Seite 13:

Wichtig als spätere Dokumentation.

Datenbank-Konfigurationsassistent, Schritt 13 von 13 : Optionen für das Erstellen

Wählen Sie die Optionen für das Erstellen der Datenbank:

- Datenbank erstellen
- Als Datenbank-Template speichern
- Skripts für das Erstellen von Datenbanken generieren

Name:

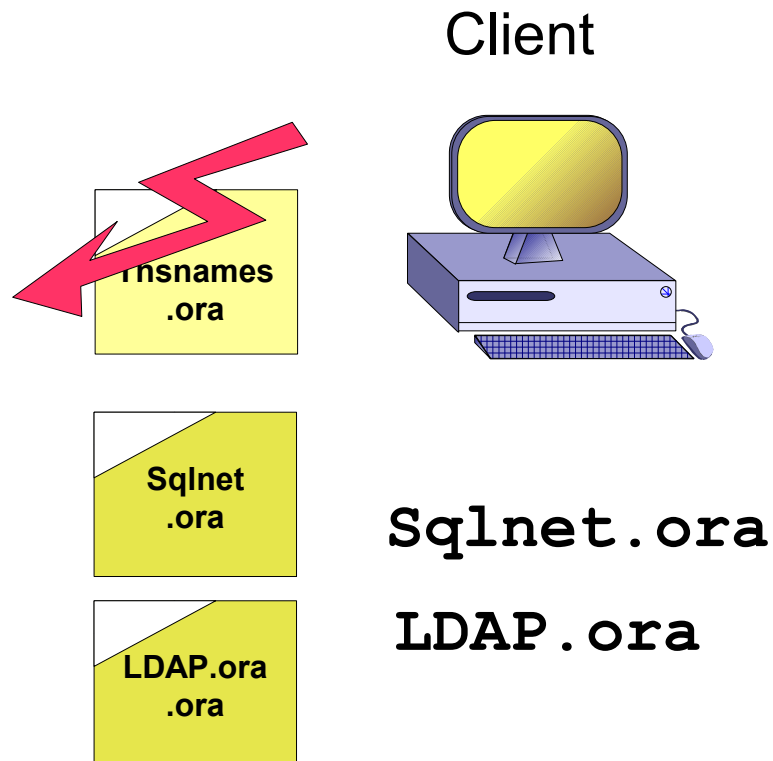
Beschreibung:

Ziel Verzeichnis:

Abbrechen Hilfe Zurück Weiter Beenden

# Konfiguration des Clients anpassen

## SQLNet.ora und LDAP.ora anpassen



# Konfiguration überprüfen

`$ORACLE_HOME/network/admin/  
sqlnet.ora`

Verweis auf TNSNames  
entfällt

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

`ldap.ora`

Standardcontext  
beachten

```
DEFAULT_ADMIN_CONTEXT = "DC=ncora,DC=local"  
  
DIRECTORY_SERVER_TYPE = AD  
DIRECTORY_SERVERS = (ncora01:389:636)
```

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;

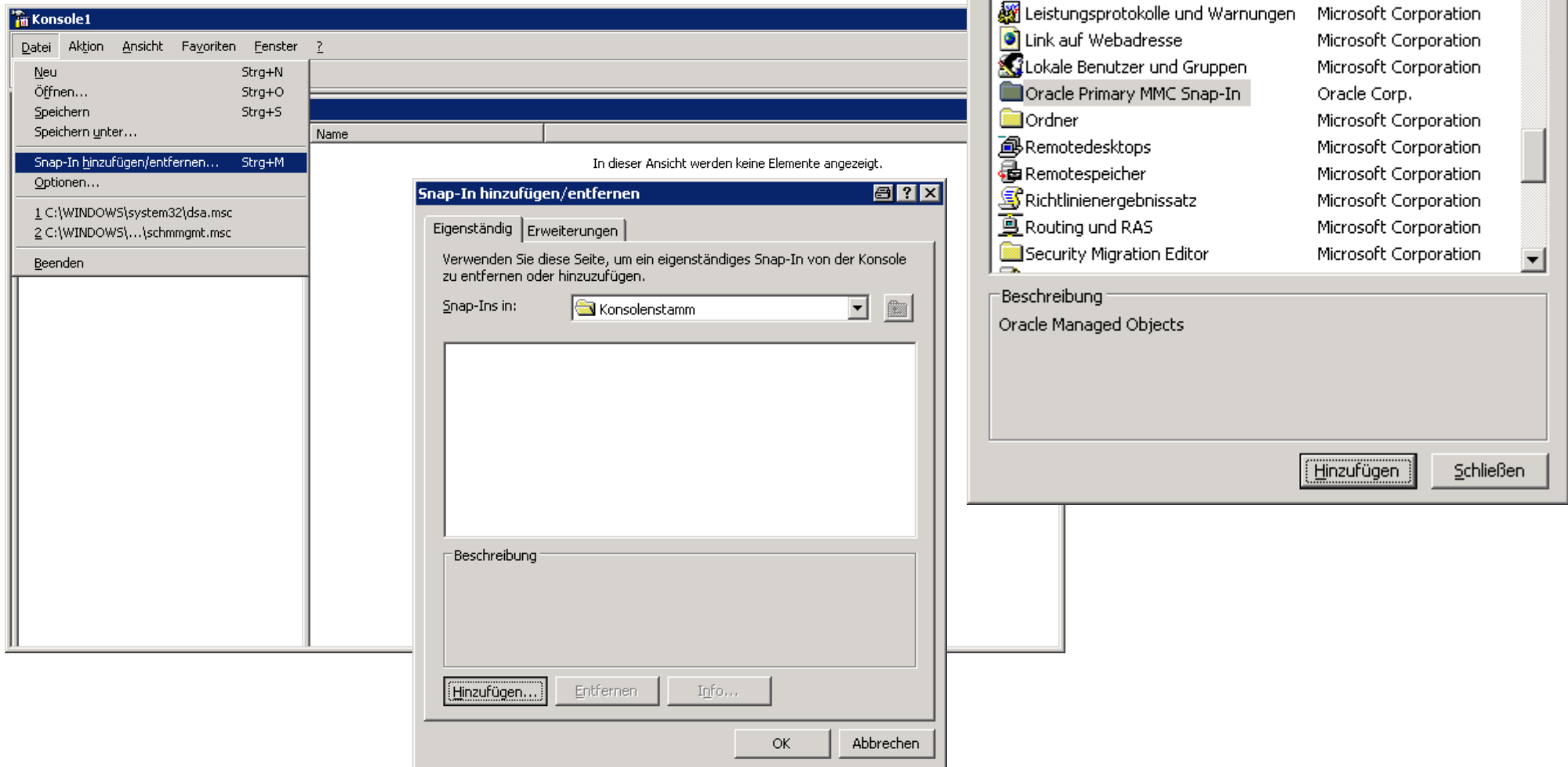
USER
-----
SYSTEM

SQL>
```

# Testen (One last Thing)

Belohnung des Installationsaufwandes?

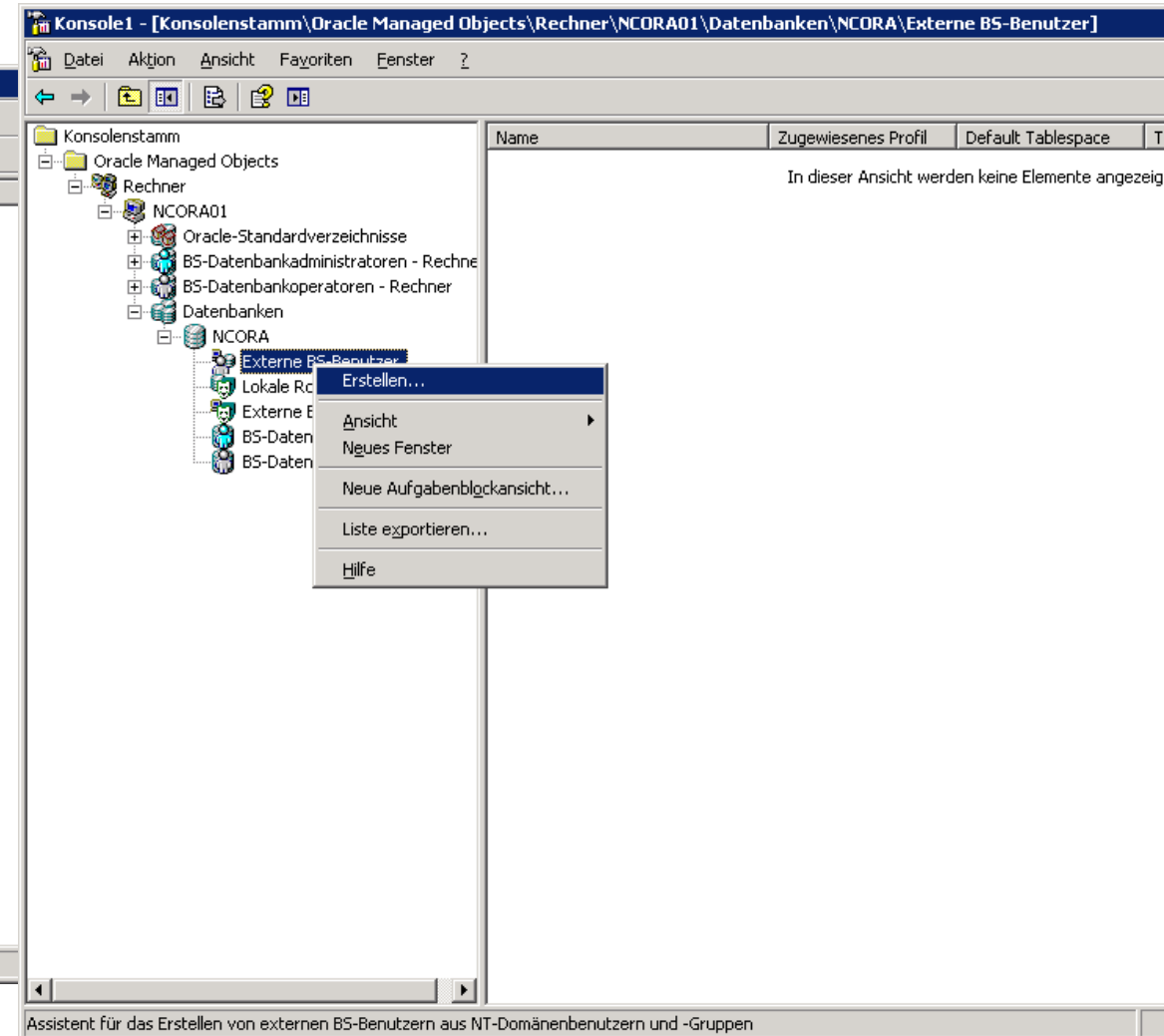
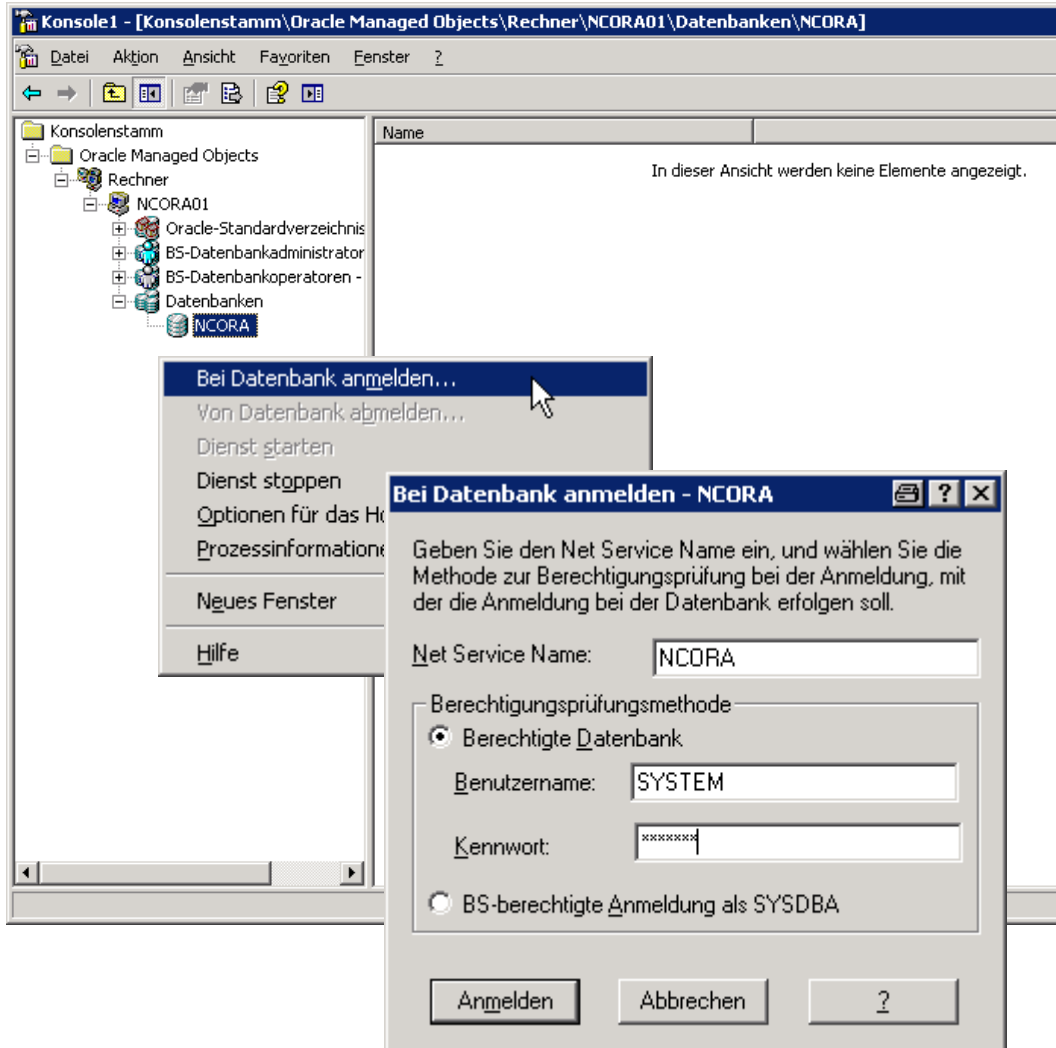
JA!: > mmc





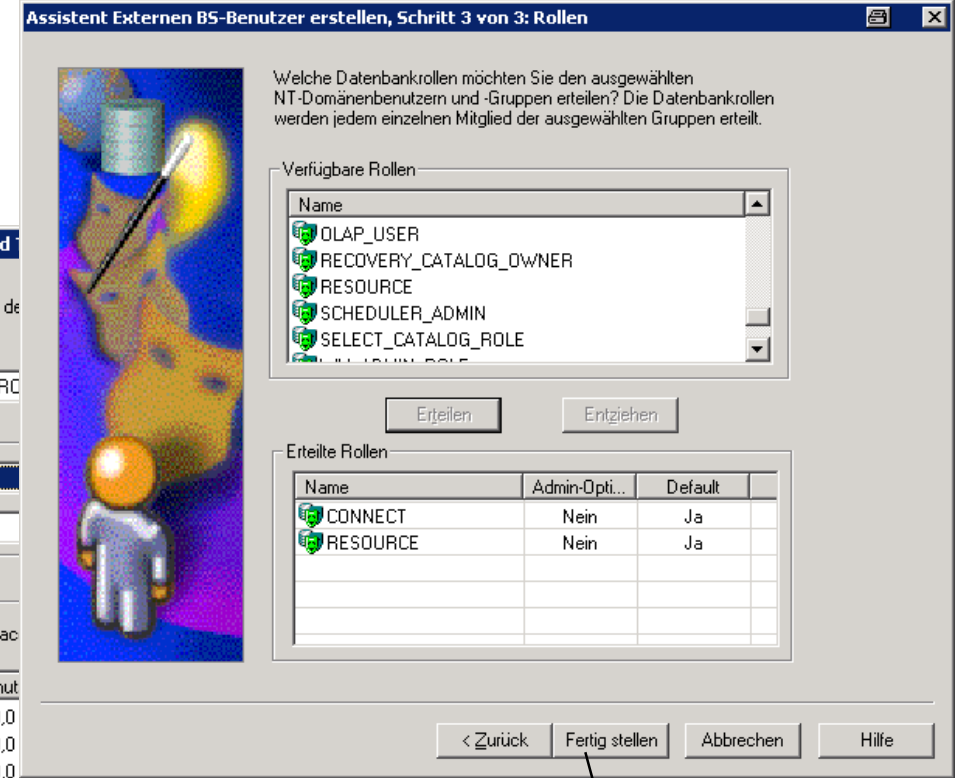
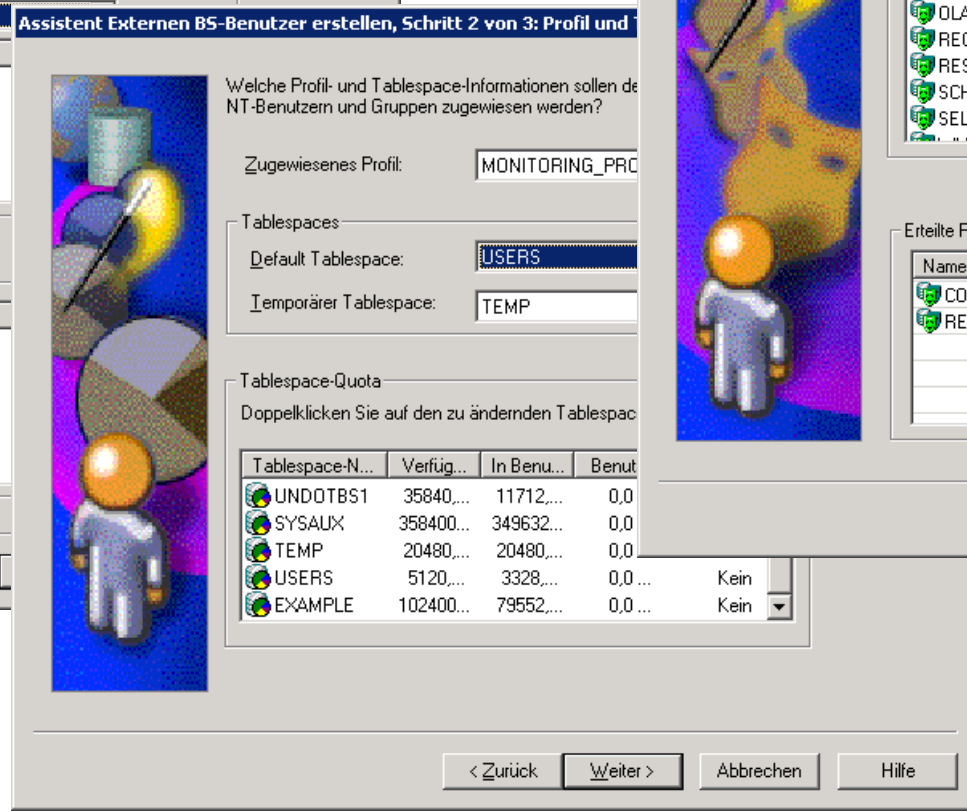
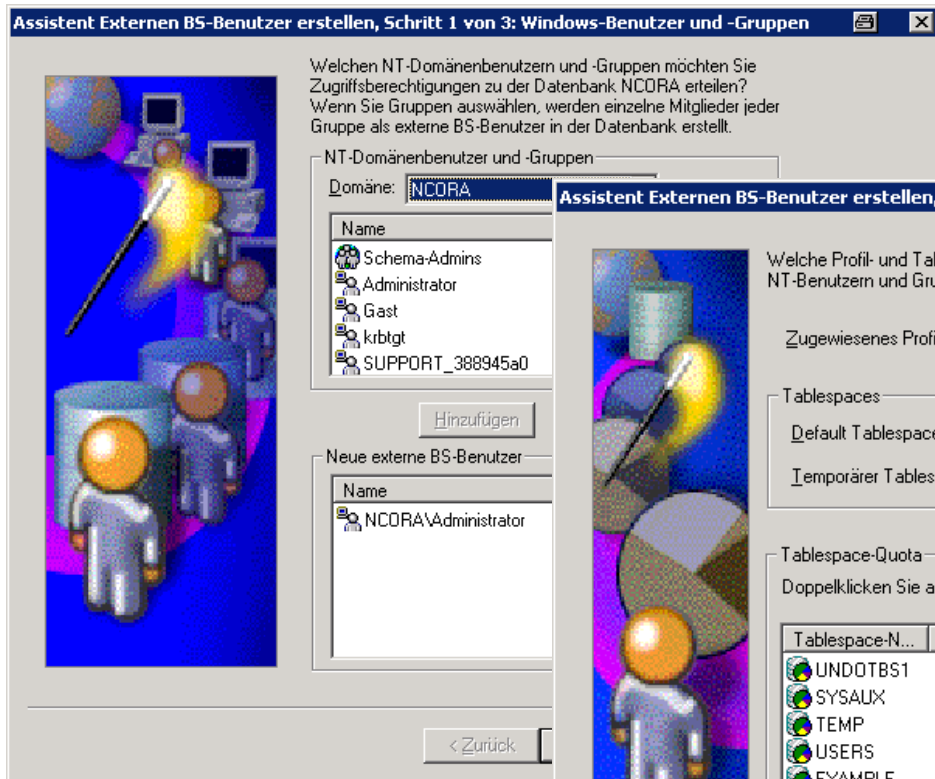
# Testen (One last Thing)

Erstmal wieder klicken...



# Testen (One last Thing)

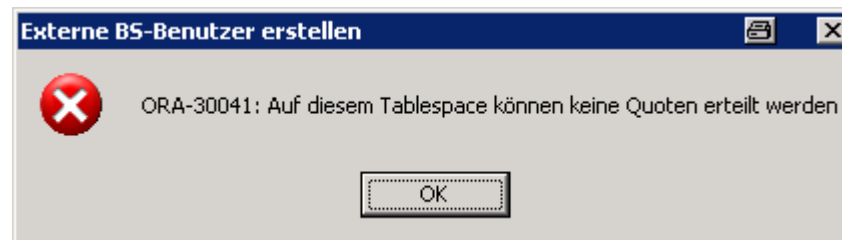
## Benutzer hinzufügen



Endlich!

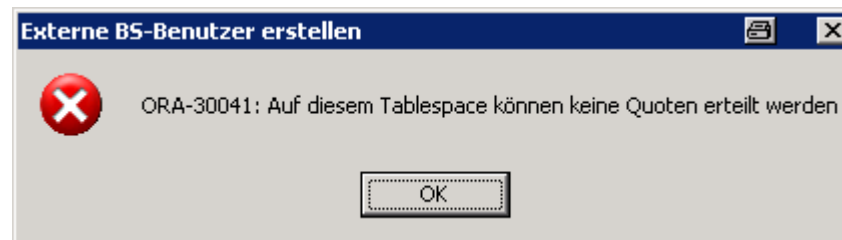
# Testen (One last Thing)

Ganz normal.

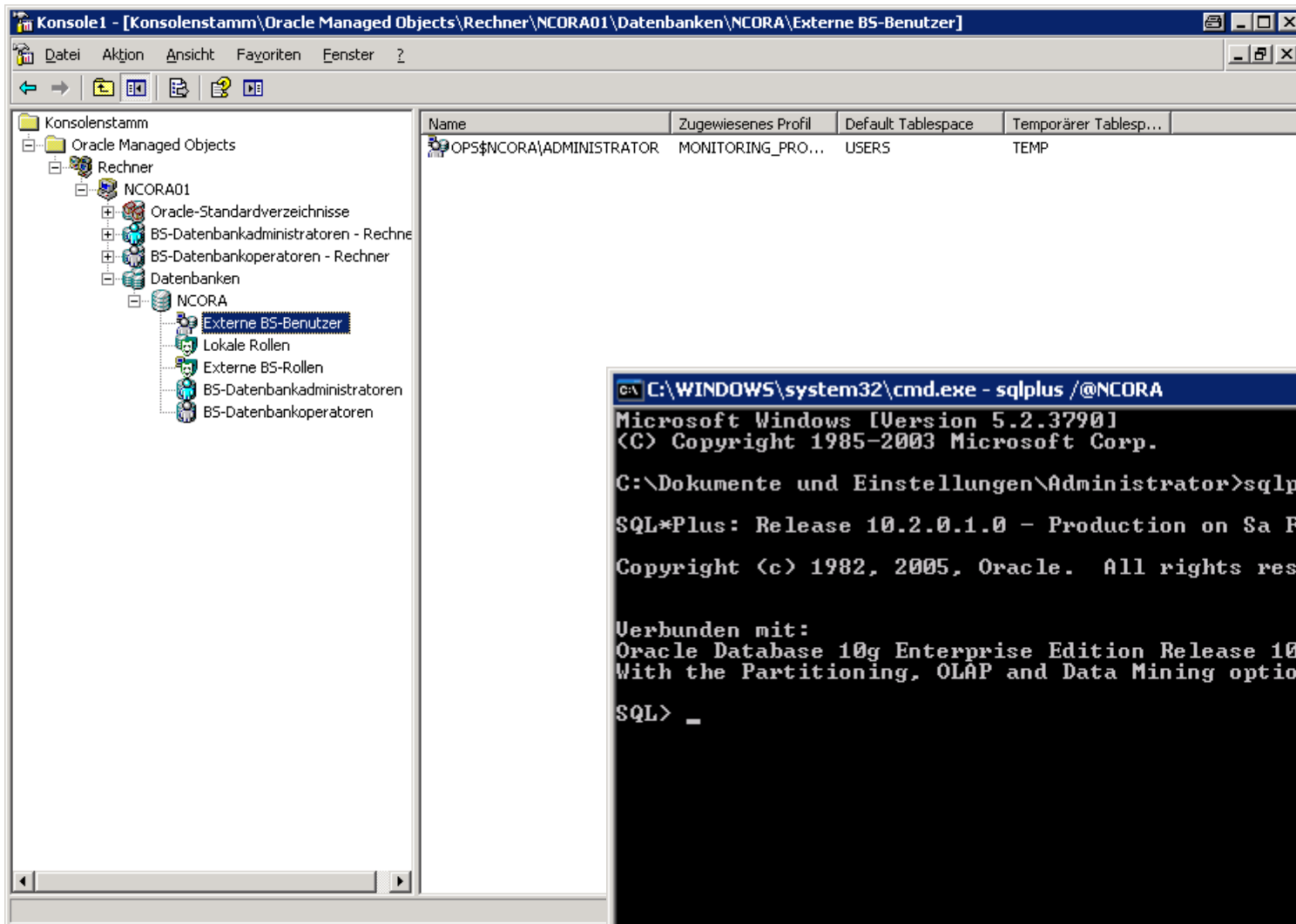


# Testen (One last Thing)

Ganz normal #2.



# Testen (One really last Thing)



Konsole1 - [Konsolenstamm\Oracle Managed Objects\Rechner\NCORA01\Datenbanken\NCORA\Externe BS-Benutzer]

Oracle Managed Objects

- Rechner
  - NCORA01
    - Oracle-Standardverzeichnisse
    - BS-Datenbankadministratoren - Rechner
    - BS-Datenbankoperatoren - Rechner
    - Datenbanken
      - NCORA
        - Externe BS-Benutzer**
        - Lokale Rollen
        - Externe BS-Rollen
        - BS-Datenbankadministratoren
        - BS-Datenbankoperatoren

| Name                     | Zugewiesenes Profil | Default Tablespace | Temporärer Tablesp... |
|--------------------------|---------------------|--------------------|-----------------------|
| OPS\$NCORA\Administrator | MONITORING_PRO...   | USERS              | TEMP                  |

```
C:\WINDOWS\system32\cmd.exe - sqlplus /@NCORA
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Dokumente und Einstellungen\Administrator>sqlplus /@NCORA
SQL*Plus: Release 10.2.0.1.0 - Production on Sa Feb 10 19:11:23 2007
Copyright (c) 1982, 2005, Oracle. All rights reserved.

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

# Datenbanken nachträglich hinzufügen

## Oracle Net Manager

Oracle Net-Konfiguration

- Verzeichnis
- Dienstbenennung**
- ncora
- Lokal

Net Service Name-Assistent: Willkommen

Um auf eine Oracle-Datenbank oder einen anderen Dienst zuzugreifen, benutzen Sie netzwerkübergreifend einen Net Service Name. Mit diesem Assistenten können Sie einen Net Service Name erstellen.

Geben Sie den Namen ein, mit dem Sie auf den Dienst zugreifen möchten. Sie können ihn auch aus einer Liste wählen.

Net Service-Name:

Abbrechen Zurück

Net Service Name-Assistent, Register 2 von 5: Protokoll

Für die netzwerkübergreifende Kommunikation mit der Datenbank wird ein Netzwerkprotokoll benutzt. Wählen Sie das Protokoll für die Datenbank, auf die zugegriffen werden soll.

- TCP/IP (Internet Protocol)**
- TCP/IP with SSL (Secure Internet Protocol)
- Named Pipes (Microsoft Networking)
- IPC (Lokale Datenbank)

Abbrechen

Net Service Name-Assistent, Register 3 von 5: Protokolleinstellungen

Um mit dem TCP/IP-Protokoll mit der Datenbank zu kommunizieren, muss der Host-Name des Datenbank-Rechners angegeben werden. Geben Sie den TCP/IP-Host-Namen für den Rechner ein, auf dem die Datenbank gespeichert ist.

Host-Name:

Außerdem ist eine TCP/IP-Port-Nummer erforderlich. Die Port-Nummer für Oracle-Datenbanken ist im allgemeinen 1521. Normalerweise müssen Sie keine andere Port-Nummer angeben.

Port-Nr.:

Abbrechen Zurück Weiter

Der Connect Identifier kann ein einfacher Name sein, mit dem die Datenbank oder der Dienst identifiziert wird.

So stellen Sie fest, ob Connect Identifier in einem Verzeichnis erstellt sind. Doppelklicken Sie auf den Ordner Dienstbenennung. Wenn keine Connect Identifier vorhanden sind, klicken Sie auf "+" in der Symbolleiste oder wählen Sie Bearbeiten > Erstellen.

Siehe auch: "Directory > Dienstbenennung" im Inhaltsverzeichnis des Hilfesystems.

# Datenbanken nachträglich hinzufügen (2)

Net Service Name-Assistent, Register 4 von 5: Dienst

Um die Datenbank oder den Dienst zu identifizieren, müssen Sie entweder den Service-Namen, bei Oracle8i 8.1 oder höher, oder den Systembezeichner (SID), bei Oracle8.8.0 Datenbankversionen, angeben. Der Service-Name für eine Oracle8i- oder höhere Datenbank ist normalerweise deren globaler Datenbankname.

(Oracle8i oder höher) Service-Name:

(Oracle8 oder früher) SID:

Optional können Sie zwischen einer gemeinsamen oder dedizierten Oracle8i-Datenbankverbindung wählen. Standardmäßig liegt die Entscheidung bei der Datenbank.

Abbrechen

Net Service Name-Assistent, Register 5 von 5: Test

Klicken Sie auf Testen, wenn Sie prüfen möchten, ob die mit den angegebenen Informationen aufgerufen werden kann.

Sobald Sie fertig sind, oder wenn Sie den Test nicht durchführen möchten, klicken Sie auf Fertig, um den Net Service Name zu erstellen, oder auf Weiter, sofern diese Schaltfläche verfügbar ist, um fortzufahren.

Testen...

Abbrechen Zurück Weiter

Oracle Net-Konfiguration

Verzeichnis

- Dienstebenenennung
  - ncora
    - NCORA2**
- Lokal

Dienst-Identifikation

Service-Name:

SID:

Verbindungstyp:

Mit Oracle8 Release 8.0 kompatible Kennung verwenden

Adresskonfiguration

Adresse1

Protokoll:

Host-Name:

Port-Nr.:

```
C:\WINDOWS\system32\cmd.exe - sqlplus /@NCORA2

C:\>sqlplus /@NCORA2

SQL*Plus: Release 10.2.0.1.0 - Production on Mo Feb 12 10:24:59 2007

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

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

SQL> _
```

# 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 | K... |
|----------------|------------|------------------|-------|------|
| oidbase.ldif   | LDIF-Datei | 19.10.2003 23:20 | 3.486 |      |
| oidbasead.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 |      |
| oidnami.nlh    | LDIF-Datei | 01.03.2004 05:57 | 5.598 |      |

Problem: .ldif-Format unterschiedlich zu OpenLDAP

# Oracle-Schema anlegen

Oracle-\*.ldif-Dateien vom OID auswerten

LDIF-Format für das OID erzeugen

Über die IAS  
Installation  
suchen

oidbase.ldif  
oidnet.ldif  
oidrdbms.ldif

```
#!/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

The screenshot shows the Softerra LDAP Administrator 3.4 interface. The left pane displays the directory tree with 'cn=ncora' selected under 'cn=OracleContext'. The main pane shows a table of LDAP entries with the following data:

| Name      | Value                                                                                                  | Type     | Size |
|-----------|--------------------------------------------------------------------------------------------------------|----------|------|
| object... | top                                                                                                    | Attri... | 3    |
| object... | ordService                                                                                             | Attri... | 11   |
| object... | ordDBServer                                                                                            | Attri... | 12   |
| cn        | ncora                                                                                                  | Attri... | 5    |
| ordNet... | (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=172.28.1.65)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=ncora))) | Attri... | 102  |

The value for 'ordNet...' is highlighted in a blue box. Below the table, the 'Output' pane shows the message: 'Schema for ncsxcp01.nci.local:389 loaded successfully.' The status bar at the bottom indicates 'cn=admin,dc=nci,dc=local' and 'Schema fetched'.

# Prüfen und testen

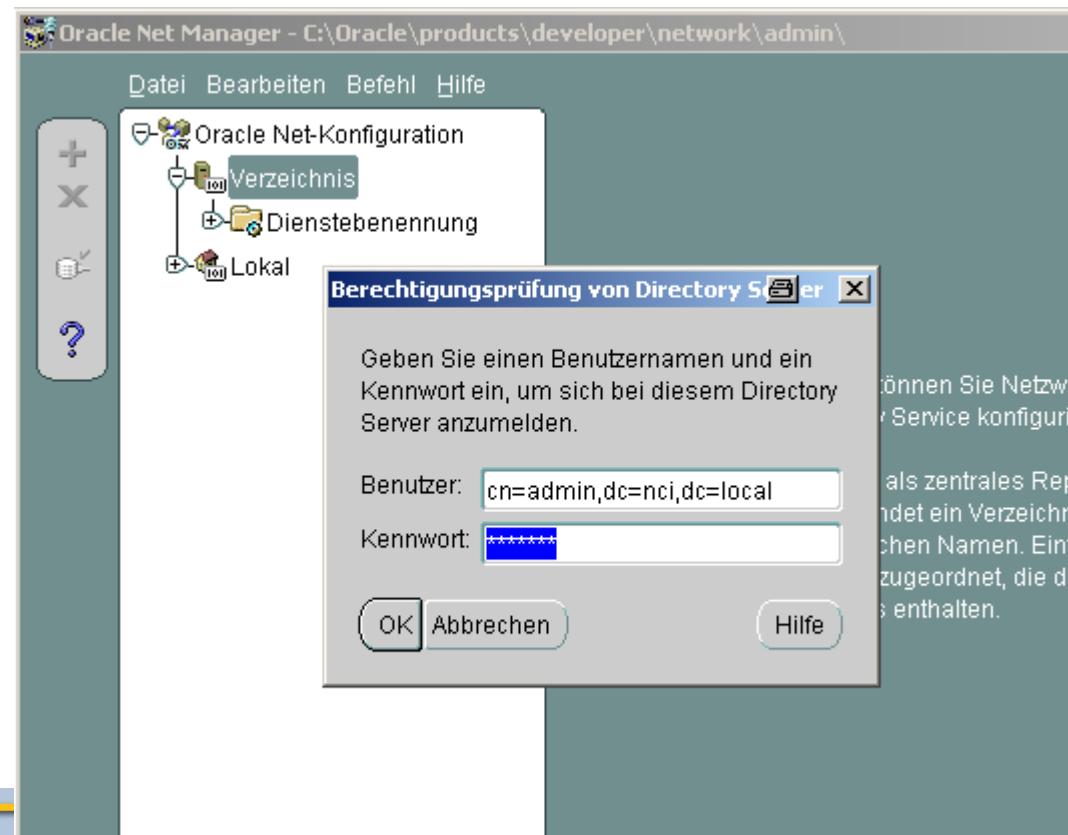
## LDAP Search

```
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

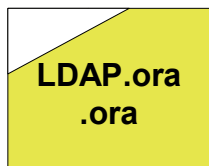
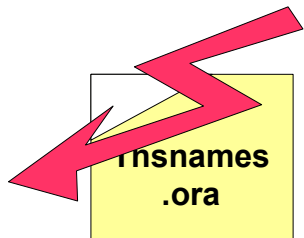
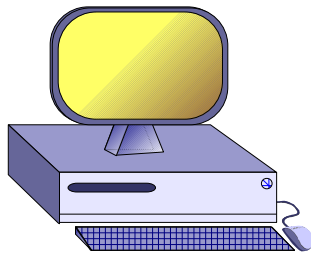
### Sqlnet.ora

```
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"
```

Client



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 tnspring)

```
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
```

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

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

kill -<HUP ID> <id von syslogd>

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



# 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

Benutzerberechtigung auch für Lesezugriffe wünschenswert

Mit OpenLDAP eine einfache 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](mailto: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>