

# Univention Active Directory Connector

Thema:	Installation und Konfiguration des Univention AD Connector.
Datum:	12. August 2008
Seitenzahl:	<a href="#">16</a>
Versionsnummer:	1660
Autoren:	Univention GmbH   <a href="mailto:feedback@univention.de">feedback@univention.de</a>

## Inhaltsverzeichnis

<b>1</b>	<b>Einführung</b>	<b>3</b>
<b>2</b>	<b>Installation</b>	<b>3</b>
2.1	Active Directory . . . . .	3
2.2	Active Directory Benutzer . . . . .	5
2.3	Univention Corporate Server . . . . .	6
<b>3</b>	<b>Funktionsweise</b>	<b>7</b>
3.1	Ablauf der Synchronisation . . . . .	7
<b>4</b>	<b>Mapping Einstellungen</b>	<b>8</b>
<b>5</b>	<b>Details zur vorkonfigurierten Synchronisation</b>	<b>10</b>
5.1	Container und Organisationseinheiten . . . . .	11
5.2	Gruppen . . . . .	11
5.3	Benutzer . . . . .	12
<b>6</b>	<b>Univention Configuration Registry-Variablen</b>	<b>13</b>
6.1	Grundkonfiguration . . . . .	13
6.2	Mapping-Defintion . . . . .	14
6.3	Windows-2000 Synchronisation . . . . .	15
<b>7</b>	<b>Tools</b>	<b>15</b>
7.1	univention-adsearch . . . . .	15
7.2	univention-connector-list-rejected . . . . .	16

## 1 Einführung

Der Univention Active Directory Connector (kurz AD Connector) ermöglicht eine Synchronisation von Verzeichnisdienstobjekten zwischen einem Windows 2000/2003 Server mit Active Directory (AD) und einem Univention Corporate Server (UCS).

Die Synchronisationseinstellungen können dabei individuell festgelegt werden, wodurch der Administrator die Möglichkeit erhält, die Synchronisation genau zu steuern und nur bestimmte Objekte und Attribute zu synchronisieren.

In der Standardeinstellung werden Container, Organisationseinheiten, Benutzer und Gruppen synchronisiert. Die Benutzer nehmen eine Sonderstellung ein, da das Passwort im Active Directory nicht über das LDAP Protokoll abgefragt werden kann. Hierfür wird ein zusätzlicher Dienst auf dem Windows 2003 Server installiert, der diese Passwortsynchronisation ermöglicht. Die Rechner Accounts werden in der Standardkonfiguration nicht synchronisiert, da Windows Rechner nur in einer Domäne sein können und nicht einfach aus einer Active Directory Umgebung in eine Windows NT Domäne, welche durch UCS dargestellt wird, übernommen werden können.

Durch die Möglichkeit in beiden Domänen die gleichen Benutzereinstellungen zu erhalten, können Benutzer transparent auf Dienste beider Umgebungen zugreifen. Nachdem eine Domänen Anmeldung an einer UCS Domäne durchgeführt wurde, ist anschließend eine Verbindung zu einer Dateifreigabe oder einem Exchange Server mit Active Directory ohne erneute Passwortabfrage möglich. Auf den Ressourcen der anderen Domäne finden Benutzer und Administratoren gleichnamige Benutzer und Gruppen vor und können so mit den gewohnten Rechtestrukturen arbeiten.

Der Univention AD Connector kann nur auf einem DC Master oder DC Backup System installiert werden, da nur dort die vollständigen Daten im LDAP vorhanden sind.

Trotz intensiver Tests kann nicht ausgeschlossen werden das die Ergebnisse des Synchronisationsvorgangs den Betrieb einer produktiven Domäne beeinträchtigen. Der Connector sollte daher vorab in einer getrennten Umgebung auf die jeweiligen Anforderungen geprüft werden.

## 2 Installation

### 2.1 Active Directory

Auf dem Active Directory müssen zwei Konfigurationsschritte durchgeführt werden. Zum einen muss ein Zertifikat für den Server erzeugt und exportiert werden, damit eine verschlüsselte Kommunikation stattfinden kann, zum anderen muss der Passwort Dienst installiert und gestartet werden.

### 2.1.1 Zertifikat

Falls der Zertifikatsdienst nicht installiert ist, so kann dieser nachinstalliert werden: Start -> Einstellungen -> Systemsteuerung -> Software -> Windows Komponenten, Zertifikatsdienst auswählen -> Weiter Stammzertifizierungsstelle des Unternehmens wählen -> Weiter, Domänen Namen angeben -> Weiter -> Weiter.

Dieses Zertifikat muss exportiert und auf das UCS System kopiert werden: Zertifizierungsstelle -> AD-Domäne -> Eigenschaften -> Zertifikat anzeigen -> Details -> In Datei kopieren -> DER-codiert-binaer X.509.

Dieses Zertifikat sollte anschließend auf dem UCS System mit openssl umgewandelt werden, da dieses im PEM Format benötigt wird:

```
openssl x509 -inform der -outform pem -in <infile.cer> -out <outfile.pem>
```

Der Dateiname des Zertifikates im PEM Format wird anschließend in Univention Configuration Registry gespeichert:

```
univention-config-registry set \  
connector/ad/ldap/certificate=/etc/univention/ad.pem
```

### 2.1.2 Passwort Dienst

Active Directory verbietet die Abfrage von Passwörtern über das LDAP Protokoll, wodurch die Installation eines Paketes auf dem Windows Server benötigt wird. Das Paket heißt **ucs-ad-connector.msi** und findet sich nach der Installation des Pakets **univention-ad-connector** auf dem UCS-System unter `/usr/share/univention-ad-connector/`. Die Installation des Paketes wird durch einen Doppelklick gestartet.

Das Paket wird automatisch in das Windows Verzeichnis `C:\Windows\UCS-AD-Connector` installiert. Zusätzlich wird der Passwort Dienst als Systemdienst in die Windows Umgebung integriert, wodurch der Dienst automatisch oder manuell gestartet werden kann.

Nachdem auf dem UCS System ein Zertifikat für den Rechner erzeugt wurde (siehe Kapitel 2.3.2), sollten die Dateien **private.key** und **cert.pem** aus dem UCS Zertifikatsverzeichnis (`/etc/univention/ssl/<FQDN>`) in das Installationsverzeichnis des Passwort Dienstes kopiert werden.

Anschließend kann der Passwort Dienst über Start -> Verwaltung -> Dienste gestartet werden. Soll der Dienst in einem anderen Verzeichnis installiert werden, so kann dieser nachträglich in ein anderes Verzeichnis kopiert werden. Zunächst sollte der Dienst gestoppt und dann entfernt werden. Dazu können in der DOS Box die folgenden Kommandos eingegeben werden:

```
C:\Windows\AD-Connector\ucs-ad-connector.exe -stop  
C:\Windows\AD-Connector\ucs-ad-connector.exe -remove
```

Anschließend kann das UCS-AD-Connector Verzeichnis verschoben werden und der Dienst neu initialisiert werden.

```
C:\AD-Connector\ucs-ad-connector.exe -install  
C:\AD-Connector\ucs-ad-connector.exe -start
```

## 2.2 Active Directory Benutzer

Neben dem von Haus aus im Active Directory ausreichend privilegierten Benutzer "Administrator" können auch andere Benutzerkonten für den Passwort-Dienst oder den LDAP-Zugriff verwendet werden. Dazu müssen diesen Benutzern ausreichend Berechtigungen zugeordnet werden.

Die Konfiguration in den späteren Kapiteln wird daher exemplarisch am Benutzerkonto "Administrator" durchgeführt, das im Normalfall ausreichende Berechtigungen für den Einsatz des AD-Connectors besitzt. Sind die Berechtigungen jedoch zu umfassend weil z.B. nur eine unidirektionale Synchronisation erfolgen soll, können für den Zugriff auf das LDAP oder den Betrieb des Passwort-Dienstes abweichende Konten als "Replikationsbenutzer" angelegt werden.

### 2.2.1 Benutzerkonto LDAP Replikation

Auf das LDAP eines Active Directory in der Standardkonfiguration (Windows 2003) hat jeder authentifizierte Benutzer ausreichend Leseberechtigung für die Verwendung im AD-Connector. Es können weiterhin Container und Organisationseinheiten sowie alle Benutzer und Gruppen gelesen werden. Schreibberechtigung, die für den Abgleich von UCS-Konten mit AD notwendig sind, haben nur Mitglieder der Gruppe "Administratoren".

In der erweiterten Ansicht des MMC-Plugins **Active-Directory Benutzer und Computer** können die Berechtigungen für einen Replikationsbenutzer über die Eigenschaften von Organisationseinheiten vergeben werden, entzieht man einem zur Replikation angelegten Account die Berechtigungen auf eine Organisationseinheit werden die darunterliegenden Benutzer und Gruppen nicht mehr nach UCS synchronisiert.

Sind solche eingeschränkten Leserechte definiert, können "rejects" entstehen, wenn nicht alle Bedingungen an Benutzer und Gruppen für die Synchronisation erfüllt werden können. Ein typischer Grund ist eine Primäre Gruppe in einem für den Connector nicht mehr lesbaren Container. Wird beispielsweise der Lesezugriff auf den Standard-Gruppencontainer unterbunden, können AD-Benutzer mit der dort liegenden primären Gruppe "Domänen-Benutzer" nicht mehr in UCS angelegt werden. Es sollte dann eine andere primäre Gruppe in AD zugeordnet oder die Gruppe verschoben werden.

Um unnötige "rejects" zu vermeiden sollten im UCS-Mapping entsprechende Einschränkungen definiert werden, damit der Connector nicht versucht Bereiche zum AD zu synchronisieren in die er keinen Schreibzugriff hat. Im einfachsten Fall, dem "nur-Lesen"-Zugriff auf AD, kann für alle Objekte in der UCS Mapping-Definition der `sync_mode` auf `read` gesetzt werden (siehe Kapitel 4).

## 2.2.2 Benutzerkonto Passwort Dienst

Der Passwort Dienst, auf den der AD-Connector zugreift, benötigt für den lesenden Zugriff auf die SAM-Datenbank deutlich mehr Privilegien als ein Standardbenutzer. Wird für den LDAP-Zugriff auf das AD ein abweichender Benutzer mit deutlich eingeschränkten Rechten verwendet, kann dieser nicht ebenfalls für den Betrieb des Passwort Dienstes eingesetzt werden.

Nach der Installation wird der Passwort Dienst als lokaler Systemdienst gestartet und ist zunächst keinem Benutzerkonto zugeordnet. Soll ihm ein eigener Benutzer zugeordnet werden kann das dazu angelegte Benutzerkonto in die Gruppe der Administratoren aufgenommen werden, um alle benötigten Privilegien zu erhalten. Zusätzlich muss er lesend auf das Installationsverzeichnis `C:\Windows\UCS-AD-Connector` und schreibenden Zugriff auf die darin liegenden Dateien `copypwd.txt` und `copypwd.in.txt` sowie die Logdatei haben.

Manuelles Starten des Dienstes ist für einen abweichenden Benutzer möglich, wenn er in den lokalen Sicherheitsrichtlinien die Berechtigung zur lokalen Anmeldung und das Debugging von Programmen erhält. Leider werden diese Berechtigungen nicht in ausreichender Form angewandt wenn das Programm automatisch als Dienst gestartet wird.

## 2.3 Univention Corporate Server

### 2.3.1 Installation

Die Installation erfolgt entweder bei der Installation von UCS oder nachträglich mit dem Befehl:

```
apt-get install univention-ad-connector
```

Die Basiskonfiguration erfolgt über Univention Configuration Registry. Die zwingend zu setzenden Variablen (eine vollständige Liste finden Sie in Kapitel 6):

- `connector/ad/ldap/host`  
Diese Variable enthält den FQDN des Active Directory Servers, z.B. `w2k3.ad.univention.de`.
- `connector/ad/ldap/base`  
Die Basis DN des Active Directory Servers, z.B. `dc=ad,dc=univention,dc=de`.
- `connector/ad/ldap/binddn`  
Mit diesem LDAP Benutzer nimmt der Univention AD Connector Änderungen im LDAP des Active Directory vor, z.B. `cn=Administrator,cn=users,dc=ad,dc=univention,dc=de`
- `connector/ad/ldap/bindpw`  
Die Datei, die das Passwort des `connector/ad/ldap/binddn` Benutzers enthält, z.B. `/etc/univention/ad.secret`.

- `connector/ad/ldap/certificate`  
Das Zertifikat im PEM Format des Windows Servers, siehe Kapitel [2.1.1](#), z.B. `/etc/univention/ad.pem`.
- `connector/ad/windows_version`  
Die Art der LDAP-Datenbankzugriffe unterscheidet sich zwischen Windows 2000 und Windows 2003. Um gegen ein AD aus Windows 2000 synchronisieren zu können, muss diese Univention Configuration Registry-Variable auf **win2000** konfiguriert werden.

### 2.3.2 Zertifikat

Auf dem UCS System muss ein Zertifikat für eine verschlüsselte Kommunikation mit dem Passwort Dienst auf dem Active Directory erzeugt werden. Dazu kann entweder ein Memberserver mit dem Univention Directory Manager Webfrontend angelegt werden, wodurch automatisch ein Zertifikat erzeugt wird, oder es wird mit dem Kommandozeilen-tool `univention-certificate` manuell ein Zertifikat erzeugt. Das fertige Zertifikat liegt anschließend im Verzeichnis `/etc/univention/ssl/<FQDN>`. Die beiden Dateien `private.key` und `cert.pem` müssen in das Installationsverzeichnis des Passwort Dienstes auf dem Windows Server (siehe Kapitel [2.1.2](#)).

### 2.3.3 Dienst

Der Univention AD Connector Dienst kann mit dem Befehl `/etc/init.d/univention-ad-connector start` gestartet und mit dem Befehl `/etc/init.d/univention-ad-connector stop` gestoppt werden.

## 3 Funktionsweise

### 3.1 Ablauf der Synchronisation

Nach dem erstmaligen Start der Dienste wird die Initialisierung vorgenommen. Dabei werden alle Einträge aus dem UCS gelesen und entsprechend dem eingestellten Mapping in AD-Objekte umgewandelt und auf UCS Seite hinzugefügt, bzw., falls bereits vorhanden, modifiziert. Anschließend werden alle Objekte aus dem AD gelesen und in UCS-Objekte umgewandelt und entsprechend hinzugefügt bzw. modifiziert. Solange noch Änderungen vorliegen, werden die Verzeichnisdienstserver weiter abgefragt.

Sobald keine Änderungen mehr vorliegen, wird für eine bestimmte Zeit gewartet, bis der Univention AD Connector wieder im Active Directory bzw. im lokalen OpenLDAP abfragt. Diese Zeit kann mit der Univention Configuration Registry-Variable `connector/ad/poll/sleep` definiert werden. Die verwendete Einheit ist Sekunden, nach der Installation ist dieser Wert auf fünf Sekunden eingestellt.

Sollte ein Objekt nicht synchronisiert werden können, so wird dieses Objekt „rejected“. Beim Starten des Univention AD Connectors wird versucht, diese Objekte wieder einzuspielen. Zusätzlich wird nach einigen Durchläufen erneut versucht, diese Objekte wieder einzuspielen. Mit der Univention Configuration Registry-Variable `connector/ad/retryrejected` kann dieser Zyklus gesteuert werden. In der Voreinstellung werden zehn Zyklen benötigt, bevor die Objekte zurückgespielt werden.

Log- und Statusmeldungen werden in den Dateien

```
/var/log/univention/connector-status.log
/var/log/univention/connector.log
/var/log/univention/connector-tracebacks.log
```

angezeigt. Der Debug Level kann mit der Univention Configuration Registry-Variable `connector/debug/level` verändert werden.

Die DNSs der nicht synchronisierten Objekte können über das Skript `univention-connector-list-rejected` abgefragt werden. Dazu ist es empfehlenswert den Connector anzuhalten. Für diese Objekte finden sich allgemeine Hinweise (abhängig vom Debug-Level) in der Datei `connector.log` sowie genauere Fehlermeldungen, die durch die LDAP-Zugriffe auf Active Directory oder den Univention Directory Manager generiert wurden, in der Datei `connector-tracebacks.log`.

## 4 Mapping Einstellungen

Die Definition der zu synchronisierenden Objekte und Attribute wird in der Datei `/etc/univention/connector/ad/mapping.py` angegeben. Die Datei ist direkt in der Skriptsprache **Python** geschrieben, wodurch sehr flexible Definitionen möglich sind. Die Verwaltung dieser Datei erfolgt über Univention Configuration Registry, so dass Änderungen grundsätzlich am zugehörigen Template (`/etc/univention/connector/ad/mapping`) vorgenommen werden sollten. Das Template wertet für einige Standardoptionen Univention Configuration Registry-Variablen aus, so dass ein direkter Eingriff nicht immer notwendig ist. Die existierenden Univention Configuration Registry-Variablen werden in Kapitel 6.2 beschrieben.

Mit der Variable `global_ignore_subtree` wird eine Liste von zu ignorierenden Bereichen angegeben. Dabei können die Univention Configuration Registry-Variablen gemäß dem Template Mechanismus verwendet werden, z.B.:

```
global_ignore_subtree=[ 'cn=univention,@\%@ldap/base@%\%@',
                       'cn=System,@\%@connector/ad/ldap/base@%\%@' ]
```

Durch diese Angaben wird der Container `cn=univention` auf UCS Seite und auf Active Directory Seite der Container `cn=System` mit allen Unterobjekten ignoriert.

In dem Dictionary `ad_mapping` werden alle weiteren Mapping Optionen definiert. Dabei wird als Key immer ein eindeutiger Name vergeben, z.B. `user`. Als Wert wird diesem Key ein `univention.connector.property` Objekt übergeben. Dieses Objekt hat die folgenden Eigenschaften:

**ucs\_module** Das Univention Directory Manager Modul, welches für die Bearbeitung des Objektes verwendet wird. Eine Liste aller möglichen Module kann mit dem Befehl `univention-directory-manager help` ausgegeben werden.

**sync\_mode** Der zu verwendene Synchronisationsmodus. Mögliche Werte sind `read`, `write`, `sync` und `none`. Bei `read` werden die Objekte vom Active Directory zum UCS repliziert. Bei `write` werden Objekte vom UCS zum Active Directory repliziert, mit `sync` werden die Daten synchronisiert und mit `none` werden keine Änderungen durchgeführt. Im vordefinierten Mapping wird der globale Sync-Mode aus der Univention Configuration Registry-Variablen `connector/ad/mapping/syncmode` verwendet.

**scope** Scope gibt die Suchtiefe für die LDAP Suchen an. Mögliche Werte sind `sub`, `one`, `base`.

**con\_search\_filter** Der LDAP Suchfilter, mit dem die Objekte im Active Directory identifiziert werden.

**match\_filter** Der LDAP Suchfilter, mit dem die Objekte im UCS identifiziert werden.

**ignore\_filter** Hier kann ein Filter für Objekte angegeben werden, die ignoriert werden sollen.

**ignore\_subtree** Diese Liste von Containern wird ignoriert, die Unterobjekte werden ebenfalls nicht beachtet.

**con\_create\_objectclass** Eine Liste von Objektklasse, die auf Active Directory Seite verwendet wird.

**dn\_mapping\_function** Eine Liste von Funktionen, die bei der Umwandlung der DN von Active Directory nach UCS und umgekehrt aufgerufen werden. Benötigt wird diese Einstellung z.B. bei Benutzern, da auf UCS Seite mit dem Attribut `uid` und auf Active Directory Seite mit dem Attribut `cn` in der DN gearbeitet wird.

**attributes** Ein Dictionary mit `univention.connector.attribute` Objekten, die bei der Erzeugung und bei einer Änderung direkt durchgearbeitet werden.

**ucs\_create\_functions** Eine Liste von Funktionen, die nach dem Anlegen des Objekts ausgeführt werden.

**post\_con\_modify\_function** Eine Liste von Funktionen, die nach dem Modifizieren eines Objektes im Active Directory ausgeführt werden.

**post\_ucs\_modify\_functions** Eine Liste von Funktionen, die nach dem Modifizieren eines Objektes im UCS ausgeführt werden.

**post\_attributes** Ein Dictionary von Attributen, die nicht während des Anlegens eines Objekts, sondern erst in einem zweiten Schritt geändert werden können.

**mapping\_table** Ein Dictionary, dessen Keys den attribut-Keys entsprechen. Dem Key wird eine Liste von String-Tupeln zugeordnet, die jeweils UCS und AD Bezeichner enthalten. Wird während der Synchronisation ein UCS-Objekt aus dieser Liste gefunden, wird der entsprechende AD-Wert gesetzt und umgekehrt. Wird z.B. beim Mapping der Gruppennamen verwendet.

**position\_mapping** Weist einen Untercontainer in UCS einem Unterordner in AD zu. Sollte mit Sorgfalt verwendet werden, falls es gleichnamige Container auf der jeweils anderen Seite gibt. Z.B. sollte für Gruppen der UCS-Container cn=groups nicht auf den Standard-AD-Container cn=users gemappt werden, da dieser Container unter UCS bereits existiert. Gruppen, die unter UCS unter cn=users angelegt werden liegen dann nicht innerhalb dieses Bezuges und können Fehler verursachen.

## 5 Details zur vorkonfigurierten Synchronisation

Die Synchronisation erfolgt grundsätzlich unter Ausschluss durch entsprechende Filter ignorierte Container. Das sind folgende Untercontainer der LDAP-Basis:

Auf UCS-Seite:

```
cn=univention
cn=policies
cn=shares
cn=printers
cn=networks
cn=kerberos
cn=dhcp
cn=dns
cn=computers
```

Auf AD-Seite:

```
cn=System
cn=Builtin
cn=ForeignSecurityPrincipals
```

```
ou=Domain Controllers  
cn=Program Data
```

## 5.1 Container und Organisationseinheiten

Die strukturierenden Elemente werden zusammen mit ihrer Beschreibung synchronisiert. Zusätzlich ignoriert werden auf beiden Seiten die Container `cn=mail` und `cn=kerberos`. Bei Containern sind einige Besonderheiten auf AD-Seite zu beachten. Active Directory bietet im „Manager für Benutzer und Gruppen“ keine Möglichkeit, Container anzulegen, zeigt diese im erweiterten Modus aber an (Menü „Ansicht; Option „Erweiterte Funktionen“).

### Besonderheiten

- Active Directory kann keine Organisationseinheiten unterhalb von Containern anlegen, daher werden so in UCS erstellte OUs und die darunterliegenden Objekte nicht synchronisiert.
- Unter AD gelöschte Container oder Organisationseinheiten werden unter UCS rekursiv gelöscht, das bedeutet, dass evtl. nicht synchronisierte Unterobjekte, die in AD nicht zu sehen sind, ebenfalls entfernt werden.

## 5.2 Gruppen

Gruppen werden anhand des Gruppennames synchronisiert, dabei findet eine Berücksichtigung der primären Gruppe eines Benutzers statt (die unter AD nur am Benutzer im LDAP hinterlegt wird). Gruppenmitglieder, die im anderen System z.B. aufgrund von Ignore-Filtern kein Gegenstück haben, werden ignoriert (bleiben also Mitglied der Gruppe). Zusätzlich wird die Beschreibung der Gruppe synchronisiert.

Der Connector ignoriert Samba-Gruppen vom Typ „5: Eine Synchronisation von SID oder RID findet nicht statt.“

### Besonderheiten

- Unter AD wird der „Prä-Windows 2000 Name“ (LDAP-Attribut `SamAccountName`) verwendet, daher kann eine Gruppe in der AD-Konfiguration mit anderem Namen erscheinen als unter UCS.
- Neu angelegte oder verschobene Gruppen werden immer im gleichen Untercontainer auf der Gegenseite angelegt. Existieren während der Initialisierung gleichnamige Gruppen in unterschiedlichen Containern, werden die Mitglieder synchronisiert, nicht jedoch die Position im LDAP. Wird eine solche Gruppe auf einer Seite verschoben ist der Zielcontainer auf der anderen Seite identisch, so dass sich die DNs der Gruppen ab diesem Zeitpunkt nicht mehr unterscheiden.

- Bestimmte Gruppennamen werden anhand einer mapping-table umgesetzt, so dass z.B. die UCS-Gruppe „Domain Users“ mit der AD-Gruppe „Domänen-Benutzer“ synchronisiert wird. Dieses Mapping kann in englischsprachigen AD-Domänen dazu führen, dass die deutschsprachigen Gruppen angelegt werden und sollte in diesem Fall deaktiviert werden. Dazu kann die Univention Configuration Registry-Variable `connector/ad/mapping/group/language` verwendet werden (siehe auch Kapitel 6.2).

Die vollständige Tabelle ist:

<b>UCS-Gruppe</b>	<b>AD-Gruppe</b>
Domain Users	Domänen-Benutzer
Domain Admins	Domänen-Admins
Windows Hosts	Domänencomputer

- Die Repräsentation von Gruppen in Gruppen unterscheidet sich zwischen AD und UCS. Sind unter UCS Gruppen Mitglieder von Gruppen, so können diese Objekte nicht immer auf AD-Seite synchronisiert werden und erscheinen in der Liste der zurückgewiesenen Objekte. Verschachtelte Gruppen sollten daher aufgrund der in Active Directory vorliegenden Einschränkungen immer nur dort zugewiesen werden.
- Active Directory limitiert Suchergebnislisten bei Abfragen auf maximal 1000 Objekte. Während der eigentlichen Synchronisation umgeht der Connector auch bei vielen Änderungen dieses Limit durch die Abfrage von Teilbereichen. In einigen Situationen kann diese Grenze dennoch erreicht werden. Wenn eine Gruppe für mehr als 1000 Benutzer als primäre Gruppe zugewiesen wurde, führt dieses Limit zu einem Reject der Gruppe. Das ist bei großen Active Directory Umgebungen häufig für die Gruppe „Domain Users“ der Fall. In Active Directory sollte daher die „MaxPageSize“ erhöht werden (siehe <http://support.microsoft.com/kb/315071>).

### 5.3 Benutzer

Benutzer werden wie Gruppen anhand des Benutzernamens bzw. anhand des AD-Prä-Windows 2000 Namen synchronisiert. Direkt übermittelt werden die Attribute Vorname, Nachname, primäre Gruppe (sofern auf der anderen Seite vorhanden), Organisation, Beschreibung, Straße, Stadt, PLZ, Profilpfad, Anmeldeskriptpfad, Deaktivierung eines Kontos und Kontoablaufdatum. Indirekt werden zusätzlich Passwort, Passwortablaufdatum und „Ändern des Passwortes beim nächsten Login“ synchronisiert. Vorbereitet aber auf Grund unterschiedlicher Syntax in der Konfiguration auskommentiert sind erste Mail-Adresse und Telefonnummer.

Ausgenommen werden die Benutzer root und Administrator.

#### Besonderheiten

- Benutzer werden ebenfalls anhand des Namens identifiziert, so dass für Benutzer, die vor der ersten Synchronisation auf beiden Seiten angelegt wurden, hinsichtlich der Position im LDAP das gleiche Verhalten gilt wie bei Gruppen.

- Die Synchronisation des Passwortablaufdatums und des Passwort-Änderns beim nächsten Login erfolgt UCS-seitig nur auf Samba-Ebene. Wird das Ändern des Passworts durch den UCS-Admin ausgelöst, die Änderung aber gegen AD vorgenommen, werden die Ablaufdaten bzgl. des Kerberos- und Posix- Kennworts nicht geändert, so dass der User z.B. am Thin Client sein Passwort erneut ändern muss.
- Bei der erstmaligen Synchronisation wird der LDAP-Benutzer 'Administrator' aus der Gruppe 'Domain Admins' entfernt, da der AD-Administrator meist nicht Mitglied in dieser Gruppe ist. Dies hat zur Folge, dass 'Administrator' keine Schreibrechte im LDAP mehr hat und kann umgangen werden, indem vor der Synchronisation ein weiterer Benutzer in der Gruppe 'Domain Admins' hinzugefügt wird, der später für die Administration genutzt werden kann.
- Es kann vorkommen, dass ein unter AD anzulegender Benutzer, dessen Passwort zurückgewiesen wurde, nach sofortigem erneuten Anlegen aus AD gelöscht wird. Grund dafür ist, dass AD diesen Benutzer zunächst anlegt und nach dem Abweisen des Passwortes sofort wieder löscht. Werden diese Operationen nach UCS übertragen, werden sie auch wieder zurück nach AD übermittelt. Wurde der Benutzer auf AD vor der Rückübertragung der Operation erneut eingetragen, so wird er nach der Rückübertragung gelöscht. Das Auftreten dieses Verhaltens ist abhängig von den eingestellten Ruhezeiten des Connectors.
- AD und UCS legen neue Benutzer per Voreinstellung in eine bestimmte primäre Gruppe (meist „Domain Users“ bzw. „Domänen Benutzer“). Während der ersten Synchronisation von UCS nach AD werden die Benutzer daher immer in dieser Gruppe Mitglied.

## 6 Univention Configuration Registry-Variablen

Zur Konfiguration auf UCS-Seite stehen einige Univention Configuration Registry-Variablen zur Verfügung. Diese werden bei einem Neustart des Connectors ausgewertet.

### 6.1 Grundkonfiguration

- `connector/ad/ldap/base`  
LDAP-Basis von Active Directory.
- `connector/ad/ldap/binddn`  
BIND-DN des in Active Directory zu verwendenden Accounts.
- `connector/ad/ldap/bindpw`  
Datei mit vollem Pfad, in der das gegen Active Directory zu verwendende Passwort gespeichert ist. Die Datei sollte genau eine Zeile enthalten.
- `connector/ad/ldap/certificate`  
Datei mit vollem Pfad, in der das von Active Directory exportierte Zertifikat abgelegt ist (zur verschlüsselten Übertragung der Passwörter).

- `connector/ad/ldap/host`  
FQDN des Active Directory-Servers.
- `connector/ad/ldap/port`  
LDAP-Port des Active Directory-Servers, voreingestellt ist 389.
- `connector/ad/listener/dir`  
Verzeichnis, in dem die von UCS nach Active Directory zu übertragene Objekte liegen, voreingestellt ist `/var/lib/univention-connector/ad`. In diesem Pfad legt das zugehörige Listener-Modul die Änderungen ab, er sollte daher nicht geändert werden.
- `connector/ad/poll/sleep`  
Zeit in Sekunden, die nach einem Lauf ohne Änderungen gewartet wird, bis erneut angefragt wird. Lokal wird dabei nur nach neuen Dateien im oben genannten Verzeichnis gesucht, auf Active Directory-Seite wird eine LDAP-Anfrage gestellt. Je niedriger diese Zeit, desto höher die Replikationsgeschwindigkeit und die unnötige Systemlast. Voreingestellt sind 5 Sekunden.
- `connector/ad/retryrejected`  
Anzahl der Anfragen ohne neue Änderungen, nach der versucht wird, zurückgehaltene Änderungen nachträglich einzuspielen. Voreingestellt ist 10. Dieses Verhalten kann in der Datei `/var/log/univention/connector-status.log` nachvollzogen werden.
- `connector/debug/level`  
Bestimmt die Auszugebenden Debug-Informationen in `/var/log/univention/connector.log`. Voreingestellt ist 1, so dass Warnungen und Fehler protokolliert werden. Kann bis 4 erhöht werden.
- `connector/debug/function`  
Voreingestellt ist 0. Auf 1 gesetzt werden Funktionsaufrufe als zusätzliche Debug-Information protokolliert.

## 6.2 Mapping-Defintion

- `connector/ad/mapping/syncmode`  
Definiert den Synchronisations-Modus, unterstützt werden die Werte **read** (nur lesend von Active Directory nach UCS), **write** (nur schreiben von UCS nach Active Directory) oder **sync** (Bidirectionale Synchronisation). Voreingestellt ist **sync**.
- `connector/ad/mapping/user/primarymail`  
Definiert, ob die primäre Mailadresse an Benutzerobjekten von UCS mit dem Attribut **mail** in Active Directory synchronisiert werden soll. Da **mail** ein multivalue ist kann es zu Problemen bei der Synchronisation kommen, default ist daher **false**. Wird mit Installation der Exchange-Erweiterung auf **true** gesetzt.
- `connector/ad/mapping/group/primarymail`  
Definiert, ob die primäre Mailadresse an Gruppenobjekten von UCS mit dem Attribut **mail** in Active Directory synchronisiert werden soll. Da **mail** ein multivalue ist kann es zu Problemen bei der Synchronisation kommen, default ist daher **false**.

Active Directory benötigt ggf. die Exchange-Erweiterung für diese Option. Wird mit Installation der Exchange-Erweiterung auf **true** gesetzt.

- `connector/ad/mapping/group/language`  
Definiert, ob das Mapping von Standard-Gruppennamen zwischen UCS (Gruppennamen sind immer englisch) und Active Directory genutzt werden soll. Voreingestellt ist das Mapping auf ein deutschsprachiges Active Directory über den Wert **de**.

### 6.3 Windows-2000 Synchronisation

- `connector/ad/windows_version`  
Die Art der LDAP-Datenbankzugriffe unterscheidet sich zwischen Windows 2000 und Windows 2003. Um gegen ein Active Directory aus Windows 2000 synchronisieren zu können, muss diese Univention Configuration Registry-Variable auf **win2000** konfiguriert werden.
- `connector/ad/mapping/user/win2000/description`  
Aufgrund von Einschränkungen im Betrieb mit Windows 2000 Server kann der Connector keine Objektbeschreibungen in Active Directory leersetzen. Daher wird die Synchronisations von Beschreibungen im Windows 2000 Modus deaktiviert. Wird diese Univention Configuration Registry-Variable auf **true** gesetzt werden Beschreibungen für Benutzer dennoch, soweit möglich, synchronisiert.
- `connector/ad/mapping/group/win2000/description`  
Aufgrund von Einschränkungen im Betrieb mit Windows 2000 Server kann der Connector keine Objektbeschreibungen in Active Directory leersetzen. Daher wird die Synchronisations von Beschreibungen im Windows 2000 Modus deaktiviert. Wird diese Univention Configuration Registry-Variable auf **true** gesetzt werden Beschreibungen für Gruppen dennoch, soweit möglich, synchronisiert.

## 7 Tools

Mit dem AD Connector werden zur Diagnose folgende Tools installiert:

### 7.1 univention-adsearch

Ermöglicht die einfache LDAP-Suche im Active Directory. Verwendet werden immer die über Univention Configuration Registry vorgegebenen Werte für AD Server und AD Account. In AD gelöschte Objekte werden immer mit angezeigt (diese werden in AD in einen Subtree im LDAP gehalten). Als erste Option erwartet das Skript einen LDAP-Filter, zweite Option kann eine Liste der anzuzeigenden LDAP-Attribute sein.

Beispiel:

```
univention-adsearch cn=administrator cn,givenName
```

AD beschränkt die Anzahl der Ergebnisse auf maximal 1000 Ergebnisse (Sizelimit) . Sollte die Suchmaske mehr Einträge zurückliefern erhalten Sie eine entsprechende Fehlermeldung (Sizelimit Exceeded).

## 7.2 univention-connector-list-rejected

Listet die DNs nicht synchronisierter Objekte auf. Zusätzlich wird, sofern zwischengespeichert, die korrespondierende DN im anderen LDAP angegeben. Abschließend gibt `lastUSN` die ID der letzten von AD synchronisierten Änderung an.

Dieses Skript liefert evtl. eine Fehlermeldung oder unvollständige Ausgaben wenn der AD Connector in Betrieb ist.

Zur Fehlersuche bei Synchronisationsproblemen finden sich entsprechende Meldungen in folgenden Dateien:

```
/var/log/univention/connector.log  
/var/log/univention/connector-status.log
```