

Univention Active Directory Connector

Thema:	Installation und Konfiguration des Univention AD Connector.	
Datum:	13. Mai 2010	
Seitenzahl:	17	
Versionsnummer:	5455	
Autoren:	Univention GmbH	feedback@univention.de

Inhaltsverzeichnis

1	Einführung Univention Active Directory Connector	3
2	Einrichtung des Univention AD Connectors	3
2.1	Installation des Connectors über Univention Management Console	3
2.2	Grundkonfiguration des Connectors	4
2.3	Import des SSL-Zertifikats des Active Directory	5
2.4	Einrichtung des Passwort-Dienstes auf dem AD-System	5
2.5	Start/Stop des Active Directory Connectors	6
3	Details zur vorkonfigurierten Synchronisation	7
3.1	Container und Organisationseinheiten	7
3.2	Gruppen	7
3.3	Benutzer	9
4	Erweiterung der Mapping-Einstellungen	10
5	Univention Configuration Registry-Variablen	12
5.1	Grundkonfiguration	12
5.2	Mapping-Definitionen	13
5.3	Synchronisation mit Windows 2000	14
6	Besondere Konfigurations-Einstellungen	14
6.1	Einrichtung mit einem abweichenden Active Directory-Benutzer	14
6.2	Installation des Passwort-Dienstes in einem abweichenden Pfad	16
6.3	Synchronisation mehrerer AD-Domänen mit einem UCS-Verzeichnisdienst	16
7	Tools	17
7.1	univention-adsearch	17
7.2	univention-connector-list-rejected	17

1 Einführung Univention Active Directory Connector

Der Univention Active Directory Connector (kurz AD Connector) ermöglicht eine Synchronisation von Verzeichnisdienstobjekten zwischen einem Windows 2000/2003/2008 Server mit Active Directory (AD) und einem Univention Corporate Server.

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-Server installiert, der diese Passwortsynchronisation ermöglicht. Die Rechnerkonten werden in der Standardkonfiguration nicht synchronisiert, da Windows-Rechner nur in eine Domäne eingebunden 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 Domänenanmeldung 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.

2 Einrichtung des Univention AD Connectors

2.1 Installation des Connectors über Univention Management Console

Die Installation erfolgt entweder bei der Installation von UCS oder nachträglich durch Installation des Pakets ***univention-ad-connector***.

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.

2.2 Grundkonfiguration des Connectors

Der Univention Active Directory Connector kann über ein Modul der Univention Management Console konfiguriert werden. Wenn das UMC-Modul nicht verwendet werden soll, kann ein Teil der Konfiguration auch manuell über die entsprechenden Univention Configuration Registry-Variablen vorgenommen werden, die im Text referenziert sind.

Im oberen Teil des Fensters **Active Directory Connector-Status** finden sich drei Angaben, ob der AD-Connector konfiguriert wurde, ob das Zertifikat für die verschlüsselte Kommunikation mit dem Active Directory installiert wurde und der Laufzeit-Status des AD-Connector-Dienstes.

Durch Klick auf **Active Directory Connector einrichten** kann die Konfiguration des AD Connectors begonnen werden.

Im Feld **Rechnername des Active Directory Servers** muss der voll qualifizierte Rechnername des Active Directory Servers angegeben werden. Wenn der Rechnername des AD-Systems für das UCS-System nicht auflösbar sein sollte, muss ggf. für das AD-System ein **DNS Host Record**-Objekt im Univention Directory Manager angelegt werden. (Die Einstellung wird in der Univention Configuration Registry-Variable `connector/ad/ldap/host` gespeichert.)

Die **BasisDN des Active Directorys** kann entweder direkt angegeben werden oder durch Klick auf **[BasisDN ermitteln]** automatisch durch eine LDAP-Abfrage ausgelesen werden.

Im Feld **DN des Replikationsbenutzers** wird die LDAP-DN des Benutzer konfiguriert, der für den Zugriff auf das Active Directory verwendet wird. Die Einstellung wird in der Univention Configuration Registry-Variable `connector/ad/ldap/binddn` gespeichert. Bei Verwendung der Funktion für die automatische Ermittlung der Basis-DN des Active Directory wird das Administrator-Konto für die Basis-DN als Vorgabe eingetragen. Weiterführende Hinweise zum Betrieb des AD Connectors mit einem abweichenden Benutzer finden sich in Kapitel 6.1.1. Das verwendete Kennwort für den Zugriff wird im Feld **Passwort des Replikationsbenutzers** eingetragen und der Dateiname in der Univention Configuration Registry-Variable `connector/ad/ldap/bindpw` gespeichert.

Einige Active Directory-Verzeichnisdienst-Internas unterscheiden sich zwischen Windows 2000 und Windows 2003/2008. Im Eingabefeld **Version des Windows-Servers** wird die verwendete Variante konfiguriert. (Univention Configuration Registry-Variable `connector/ad/windows_version`)

Einige Gruppennamen werden abhängig von der Installationssprache des Servers im Active Directory anders gespeichert. Unter **Verwendete Sprache für das Gruppen-Mapping** kann die verwendete Lokalisierung ausgewählt werden. Weitere Hinweise finden sich in Kapitel 3.2. (Univention Configuration Registry-Variable `connector/ad/mapping/group/language`)

Der AD Connector kann in verschiedenen Modi betrieben werden, die unter **Synchronisationsmodus des Active Directory Connectors** ausgewählt werden können. Neben einer bidirektionalen Synchronisation kann auch einseitig in Richtung AD oder UCS-Verzeichnisdienst repliziert werden. (Univention Configuration Registry-Variable `connector/ad/mapping/syncmode`)

In **Polling-Intervall (in Sekunden)** kann festgelegt werden wie lange nach einem Lauf ohne Änderungen gewartet wird, bis eine erneute Anfrage gestellt wird. (Univention Configuration Registry-Variable `connector/ad/poll/sleep`)

Unter **Wiederholungsintervall für abgelehnte Objekte** wird festgelegt nach wievielen Synchronisations-Intervallen zurückgehaltene Änderungen nachträglich eingespielt werden. (Univention Configuration Registry-Variable `connector/ad/retryrejected`)

Der **Debug-Level des Active Directory Connectors** konfiguriert wieviele Debug-Informationen in die Datei `/var/log/univention/connector.log` protokolliert werden. Mit der Voreinstellung (1) werden nur Fehler und Warnungen aufgezeichnet. Mit **Debug-Ausgaben für Funktionen ausgeben** kann ausserdem festgelegt werden, ob für Funktionsaufrufe weiterer Debug-Output hinzugefügt wird. (Univention Configuration Registry-Variable `connector/ad/level` und Univention Configuration Registry-Variable `connector/ad/function`)

Nach einem Klick auf **Änderungen speichern** wird die Konfiguration in Univention Configuration Registry übernommen. Änderungen werden erst nach einem Neustart des Univention AD Connectors übernommen, siehe Kapitel 2.5.

2.3 Import des SSL-Zertifikats des Active Directory

Auf dem Active Directory-System muss nun ein SSL-Zertifikat erzeugt und exportiert werden, damit eine verschlüsselte Kommunikation stattfinden kann. Erzeugt wird das Zertifikat mit dem Zertifikatsdienst des Active Directory.

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.

Nun muss das SSL-AD-Zertifikat in das UCS-System importiert werden. Dies erfolgt durch einen Klick auf **Active Directory-Zertifikat hochladen**. Hierbei öffnet sich ein Fenster, in dem unter **Durchsuchen** eine Datei ausgewählt und mit **Hochladen** bestätigt wird. Nach einem Klick auf **Speichern** wird das hochgeladene Zertifikat für den AD Connector verfügbar gemacht. Der genaue Speicherort wird in der Univention Configuration Registry-Variable `connector/ad/ldap/certificate` festgehalten.

2.4 Einrichtung des Passwort-Dienstes auf dem AD-System

Active Directory verbietet die Abfrage von Passwörtern über das LDAP-Protokoll, was die Installation eines Paketes auf dem Windows Server erfordert.

Der Univention Active Directory Connector unterstützt mit den in UCS 2.3 ausgelieferten Paketen nur die Passwortsynchronisation mit Windows-Servern für 32-Bit-Intel-Systeme. Für die Passwort-Synchronisation mit 64-Bit-Varianten wie Windows 2008 R2 oder Windows 2003 R2 steht eine Testversion eines 64-Bit-kompatiblen Passwortsynchronisationsdienstes bereit. Die Einrichtung wird unter <http://sdb.univention.de/1131> beschrieben.

Nach Auswahl von **Download des .msi-Pakets und UCS-Zertifikats** öffnet sich ein neues Browser-Fenster, in dem drei Dateien zum Download angeboten werden: ***ucs-ad-connector.msi***, ***private.key*** und ***cert.pem***.

ucs-ad-connector.msi ist die Installations-Datei für den Passwortdienst, der durch einen Doppelklick gestartet werden kann. Die Installation ist in der Regel schnell abgeschlossen und erfolgt ohne weitere Benutzerinteraktion.

Das Paket wird automatisch in das 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.

Die Dateien ***private.key*** und ***cert.pem*** beinhalten unter UCS erzeugte SSL-Zertifikate für die gesicherte Kommunikation. Sie müssen ebenfalls in das Installationsverzeichnis des Passwort-Dienstes kopiert werden.

Anschließend kann der Passwort-Dienst über **Start -> Verwaltung -> Dienste** gestartet werden.

In einer Standard-Installation unter Windows 2008 blockiert die Windows-Firewall die Zugriffe auf den AD Connector. Diese muss entweder in der **Systemsteuerung** deaktiviert werden oder Port 6670/TCP freigegeben werden.

Unter Windows 2008 werden standardmässig keine LAN-Manager-Hashwerte (auch bekannt als NTLM-Hashes) mehr gespeichert. Da diese für den Betrieb mit dem UCS AD Connector jedoch zwingend benötigt werden, muss diese Funktion über eine Richtlinie wieder aktiviert werden. Hierzu ist im Gruppenrichtlinienverwaltungs-Editor unter **Computerkonfiguration -> Richtlinien -> Windows-Einstellungen -> Sicherheitseinstellungen -> Lokale Richtlinien -> Sicherheitsoptionen** die Einstellung **Netzwerksicherheit: Keine LAN-Manager-Hashwerte für nächste Kennwortänderung speichern** auf **Deaktiviert** zu setzen.

2.5 Start/Stop des Active Directory Connectors

Abschließend kann der Connector über **Active Directory Connector starten** gestartet werden und bei Bedarf über **Active Directory Connector beenden** angehalten werden. Alternativ kann ein Starten/Stoppen auch über Kommandozeile durch die Befehle `/etc/init.d/univention-ad-connector start` und `/etc/init.d/univention-ad-connector stop` erfolgen.

3 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
```

3.1 Container und Organisationseinheiten

Container und Organisationseinheiten 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 **Ansicht → 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.

3.2 Gruppen

Gruppen werden anhand des Gruppennamens 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.

Besonderheiten

- Unter AD wird der **Prä-Windows 2000 Name** (LDAP-Attribut **SamAccountName**) verwendet, daher kann eine Gruppe im Active Directory mit anderem Namen erscheinen als unter UCS.
- Der Connector ignoriert Gruppen, die im Univention Directory Manager unter **Samba Gruppentyp** als **Bekannte Gruppe** konfiguriert wurden. Eine Synchronisation von SID oder RID findet nicht statt.
- Gruppen, die im Univention Directory Manager unter **Samba Gruppentyp** als **Lokale Gruppe** konfiguriert wurden, werden vom Connector als **globale Gruppen** in das Active Directory synchronisiert.
- 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-Tabelle 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 5.2).

Die vollständige Tabelle ist:

UCS-Gruppe	AD-Gruppe
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.
- Wird im Univention Directory Manager eine globale Gruppe A als Mitglied einer anderen globalen Gruppe B aufgenommen, so erscheint diese Mitgliedschaft aufgrund von AD-internen Beschänkungen unter Windows 2000/2003 nicht im Active Directory. Wird Gruppe A anschließend umbenannt, geht die Gruppenmitgliedschaft in Gruppe B verloren. Mit Windows 2008 besteht diese Einschränkung nicht mehr, dort können im Active Directory auch globale Gruppen verschachtelt 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>).

3.3 Benutzer

Benutzer werden wie Gruppen anhand des Benutzernamens bzw. anhand des AD-Prä-Windows 2000 Namens synchronisiert. Direkt übermittelt werden die Attribute **Vorname**, **Nachname**, **primäre Gruppe** (sofern auf der anderen Seite vorhanden), **Organisation**, **Beschreibung**, **Straße**, **Stadt**, **PLZ**, **Profilpfad**, **Anmeldeskriptpfad**, **Deaktiviert** und **Kontoablaufdatum**. Indirekt werden zusätzlich **Passwort**, **Passwortablaufdatum** und **Ändern des Passwortes beim nächsten Login** synchronisiert. Vorbereitet, aber auf Grund unterschiedlicher Syntax in der Mapping-Konfiguration auskommentiert, sind **Primäre 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 der Benutzer-Option **Passwort-Ändern beim nächsten Login** erfolgt UCS-seitig nur auf Samba-Ebene. Wird das Ändern des Passworts durch Univention Directory Manager ausgelöst, das Passwort dann aber im Active Directory geändert, werden die Ablaufdaten bzgl. des Kerberos- und Posix- Kennworts nicht geändert, so dass der User z. B. bei Thin Client-Anmeldung sein Passwort erneut ändern muss.
- Bei der erstmaligen Synchronisation wird der 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 UCS-Verzeichnisdienst mehr hat und 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, das 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-Seite schon vor der Rückübertragung der Operation erneut eingetragen, so wird er nach der Rückübertragung gelöscht. Das Auftreten dieses Verhaltens ist abhängig von dem eingestellten Polling-Intervall 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.

4 Erweiterung der 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 Änderung 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 5.2 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 modules` 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 bidirektional synchronisiert und mit `none` werden keine Änderungen durchgeführt. Im vordefinierten Mapping wird der globale Sync-Mode aus der Univention Configuration Registry-Variable `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 abgearbeitet werden.

ucs_create_functions Eine Liste von Funktionen, die nach dem Anlegen eines Objekts in UCS 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-Verzeichnisdienst 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 das entsprechende AD-Attribut gesetzt und umgekehrt. Wird z.B. beim Mapping der Gruppennamen verwendet.

position_mapping Weist einem Untercontainer in UCS einen 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 Univention Configuration Registry-Variablen

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

5.1 Grundkonfiguration

- `connector/ad/ldap/base`
Die LDAP-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 in der Univention Configuration Registry-Variable `connector/ad/ldap/binddn` gespeicherten Benutzers enthält, z.B. `/etc/univention/ad.secret`. Die Datei sollte genau eine Zeile enthalten.
- `connector/ad/ldap/certificate`
Dateiname mit vollem Pfad, in der das von Active Directory exportierte Zertifikat abgelegt ist (zur verschlüsselten Übertragung der Passwörter). Das Zertifikat wird im PEM-Format gespeichert.
- `connector/ad/ldap/host`
Diese Variable enthält den FQDN des Active Directory Servers, z.B. `w2k3.ad.univention.de`.
- `connector/ad/ldap/port`
Die Portnummer des LDAP-Dienstes des Active Directory-Servers, voreingestellt ist 389.

- `connector/ad/ldap/ssl`
Wird die Konfigurationsoption auf **no** gesetzt, wird für den Zugriff auf das Active Directory auf die SSL-Verschlüsselung verzichtet. Dies kann notwendig sein, wenn auf dem Active Directory Server kein Zertifikatsdienst installiert werden kann.
- `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 fünf 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 in `/var/log/univention/connector.log` auszugebenden Debug-Informationen. 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.

5.2 Mapping-Definitionen

- `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** (bidirektionale 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**. Bei der Installation des Pakets **univention-ad-connector-exchange** wird der Wert 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. Bei der Installation des Pakets **univention-ad-connector-exchange** wird der Wert auf **true** gesetzt.

- `connector/ad/mapping/group/language`
Definiert, welche Abbildung 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**.
- `connector/password/service/encoding`
Der Passwortdienst unter Windows benötigt den Benutzernamen bei der Passwortänderung im iso8859-Format. Mit dieser Variable kann das Encoding gesetzt werden. Abweichungen von der Voreinstellung (iso8859-15) sollten nur in Sonderfällen nötig sein.

5.3 Synchronisation mit Windows 2000

- `connector/ad/windows_version`
Die Art der LDAP-Datenbankzugriffe unterscheidet sich zwischen Windows 2000 und Windows 2003/2008. 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 Synchronisation von Beschreibungen im Windows 2000 Modus deaktiviert. Wird diese Univention Configuration Registry-Variable auf **true** gesetzt, werden Beschreibungen für Benutzer dennoch, soweit möglich, synchronisiert.

6 Besondere Konfigurations-Einstellungen

In diesem Kapitel werden werden einige weiterführende Konfigurationsschritte besprochen, z.B. der Betrieb des AD Connectors mit einem Nicht-Administrator-Benutzer.

6.1 Einrichtung mit einem abweichenden 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 ausreichende Berechtigungen zugeordnet werden.

Die Konfiguration in diesem Dokument wird 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-Verzeichnis oder den Betrieb des Passwort-Dienstes abweichende Konten als "Replikationsbenutzer" angelegt werden.

6.1.1 Benutzerkonto für LDAP Replikation

In der Standardkonfiguration eines Active Directory-Verzeichnisses auf Basis von Windows 2003 verfügt jeder authentifizierte Benutzer über ausreichende Leseberechtigung für die Verwendung des AD-Connectors. Es können 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. Soll z.B. ein rein lesender Zugriff auf AD erfolgen, so reicht es aus durch Setzen des `sync_mode` auf `read` einen lesenden Zugriff zu konfigurieren. (siehe Kapitel 4).

6.1.2 Benutzerkonto für den 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 Zugriff auf das Installationsverzeichnis `C:\Windows\UCS-AD-Connector` und schreibend 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.

6.2 Installation des Passwort-Dienstes in einem abweichenden Pfad

Soll der Passwort-Dienst in einem anderen Verzeichnis als der Installationsvorgabe 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 Windows-Eingabeaufforderung die folgenden Kommandos eingegeben werden:

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

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

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

6.3 Synchronisation mehrerer AD-Domänen mit einem UCS-Verzeichnisdienst

Es besteht die Möglichkeit mehrere getrennte Active Directory-Domänen in eine gemeinsame UCS-Domäne zu synchronisieren. Damit können beispielsweise mehrere Domänen eines Forests synchronisiert werden. Pro AD-Domäne kann eine OU (Organisational Unit) im LDAP definiert werden, unter der die Objekte der jeweiligen Domäne synchronisiert werden.

Für die mehrfache Replikation werden mehrere Connector-Instanzen parallel gestartet. Jede Connector-Instanz wird dabei mit einer eigenständigen Konfigurationsbasis betrieben. Um eine neue Instanz zu erzeugen, muss das Skript `prepare-new-instance` aufgerufen werden, z.B.:

```
/usr/share/univention-ad-connector/scripts/prepare-new-instance \
-a create -c connector2
```

Dieses Skript erzeugt dann ein weiteres Init-Skript für die zweite Connector-Instanz (`/etc/init.d/univention-ad-connector2`), ein Konfigurationsverzeichnis `/etc/univention/connector2` mit einer Kopie der Mapping-Einstellungen der Connector-Hauptinstanz (diese kann ggf. angepasst werden) und eine Reihe interner Laufzeitverzeichnisse.

Die zusätzlichen Connector-Instanzen werden in der Univention Configuration Registry-Variable `connector/listener/additionalbasenames` registriert.

Erfolgt eine Synchronisation von Univention Corporate Server in Richtung Active Directory, so muss nach dem Anlegen einer weiteren Connector-Instanz die Replikation des Listener-Moduls neu angestoßen werden. Hierzu muss der Befehl

```
univention-directory-listener-ctrl resync ad-connector
```

aufgerufen werden. Diese Änderung kann gerade bei grossen Verzeichnisdiensten einige Zeit in Anspruch nehmen und sollte nach Möglichkeit in einem Wartungsfenster erfolgen.

Die zum Univention AD Connector gehörigen Kommandozeilenwerkzeuge wie z.B. `univention-adsearch` unterstützen mit dem Parameter `-c` die Angabe einer Connector-Instanz.

Die Konfiguration weiterer Connector-Instanzen wird nicht über das Univention Management Console-Modul abgedeckt.

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 weiterhin in einem LDAP-Unterbaum vorgehalten). Als erste Option erwartet das Skript einen LDAP-Filter, die 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, wird eine entsprechende Fehlermeldung (Sizelimit Exceeded) angezeigt..

7.2 univention-connector-list-rejected

Listet die DNs nicht synchronisierter Objekte auf. Zusätzlich wird, sofern zwischengespeichert, die korrespondierende DN im jeweils anderen LDAP-Verzeichnis 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  
/var/log/univention/connector-tracebacks.log
```