

UCS Windows-Domänen Migration

Thema:	Dokumentation zur Migration bestehender Windows-Domänen.
Datum:	9. Dezember 2010
Seitenzahl:	11
Versionsnummer:	7397
Autoren:	Univention GmbH feedback@univention.de

Inhaltsverzeichnis

1	Einführung	3
2	Durchführung der Migration	3
3	Weiterführende Informationen zur Kontenübernahme	5
3.1	Passwörter	5
3.2	Bereits im UCS-Verzeichnisdienst vorhandene Konten und RIDs	6
4	Datenübernahme	6
4.1	Durchführung der Datenübernahme	6
5	Übernahme von Druckerfreigaben	8
5.1	Voraussetzungen	9
5.2	Druckerdaten lesen	9
5.3	Druckerdaten auf UCS installieren	10
6	Drucker auf dem Samba-Druckserver installieren	10

1 Einführung

Bei der Migration (Übernahme) einer bestehenden Windows NT-Domäne werden mithilfe eines Skriptes alle Benutzer-, Gruppen- und Rechnerkonten sowie die NETLOGON-Freigabe in eine Samba-Domäne übernommen. Abhängig von der Zahl der zu übernehmenden Konten kann die Migration mehrere Stunden dauern. In dieser Zeit sollten die Daten auf dem Windows-PDC nicht verändert werden. Anschließend werden die Windows-basierten Domänencontroller aus dem Netz genommen. Deswegen ist es ratsam, die Migration von Druckerfreigaben (siehe Kapitel 5), die sich auf einem PDC oder BDC befinden, vor der Migration der Domäne durchzuführen. Verzeichnisfreigaben (siehe Kapitel 4) sollten erst nachher übernommen werden, damit die Dateien sofort ihren Benutzern zugeordnet und die Datei-ACLs übertragen werden können.

Alle Einstellungen einschließlich der Benutzer-Passwörter und Benutzernamen bleiben erhalten, so dass für die Anwender die gewohnte Umgebung bestehen bleibt und sie die Migration in der Regel gar nicht bemerken.

Hinweis:

Für die Arbeit unter Linux sind Benutzernamen mit Sonderzeichen nicht empfohlen. Soll von der Möglichkeit Gebrauch gemacht werden, nach der Migration neben Windows auch Linux im Anwenderbereich zu nutzen, sollten alle Benutzernamen mit Sonderzeichen ersetzt werden.

2 Durchführung der Migration

Falls die Migration mit UCS 2.4 durchgeführt werden soll, so wird Samba 3.3 benötigt, da die für die Migration benötigten RPC-Patches in der Standard-Samba-Version von UCS 2.4 Samba 3.5 nicht mehr enthalten sind. Eine Anleitung für die Installation und weitere Hinweise sind in der Univention Support Datenbank (<http://sdb.univention.de/1141>) zu finden.

Wesentlicher Schritt für die Übernahme einer bestehenden Windows NT-Domäne durch einen UCS-Server ist, den Windows NT-PDC durch einen Samba-PDC zu ersetzen.

Dabei ist sicherzustellen, dass sich Windows NT-PDC und Samba-PDC im selben IP-Subnetz befinden.

Die Benutzer-, Gruppen- und Rechnerkonten der Windows NT-Domäne werden standardmäßig in die Container **cn=users,<Basis-DN>**, **cn=groups,<Basis-DN>** und **cn=computers,<Basis-DN>** im UCS-Verzeichnisdienst eingefügt. Über die Univention Configuration Registry-Variablen `samba/defaultcontainer/user`, `samba/defaultcontainer/group` und `samba/defaultcontainer/computer` können andere Container vorgegeben werden. Weitere Hinweise hierzu finden sich im [UCS-Handbuch](#).

Die Übernahme der Windows NT-Domäne wird als Benutzer **root** auf dem Samba-PDC mit folgendem Befehl ausgelöst:

```
univention-pdc-takeover
```

Falls eine Namensauflösung über NetBIOS nicht möglich ist, kann über die Option **-w** die IP-Adresse eines WINS-Servers angegeben werden.

Achtung:

Eine Migration sollte nicht im laufenden Betrieb durchgeführt werden. Zur Erhaltung der Datenkonsistenz sollte sichergestellt sein, dass während des Kopiervorgangs keine Änderungen auf dem Windows-PDC vorgenommen werden.



Das Skript erfordert die Eingabe folgender Parameter:

Parameter	Erklärung
Domainname	Name der Windows-Domäne, die übernommen werden soll, z.B. TESTDOMAIN (Kommandozeilenparameter: -D)
PDC Hostname	Name des Windows NT-PDC, z.B. NT4SERVER (Kommandozeilenparameter: -S)
Administrator-Account	Benutzername eines Benutzers, der in der Windows-Domäne über Administrationsrechte verfügt, z.B. Administrator (Kommandozeilenparameter: -U)
Password	Passwort des oben genannten Benutzers, z.B. geheim (Kommandozeilenparameter: -P)

Das Übernahmeskript stoppt den möglicherweise auf dem Samba-PDC laufenden Samba-Dienst, um Konflikte bezüglich des PDCs der Domäne zu vermeiden. Anschließend versucht das Skript, den primären Domänencontroller für die angegebene Domäne zu erreichen und sich mit dem übergebenen Benutzernamen und dem Passwort zu authentifizieren. Ist das erfolgreich, werden vorhandene Benutzer-, Gruppen- und Rechnerkonten sowie die NETLOGON-Freigabe übernommen. Je nach verfügbarer Netzwerkbandbreite und Menge der zu kopierenden Daten kann der Kopiervorgang längere Zeit in Anspruch nehmen.

Des Weiteren wird der Domänenteil der SID der Windows-Domäne übernommen, indem der Domänenteil der SID der bisherigen Samba-Domäne durch den Domänenteil der SID der Windows-Domäne ersetzt wird.

Außerdem setzt das Skript die Univention Configuration Registry-Variablen `windows/domain` lokal auf den Namen der Windows-Domäne. In der Regel sollte `windows/domain` auch auf allen anderen Samba-Servern dem Namen der Windows-Domäne entsprechen. Da es jedoch Ausnahmen gibt, wird diese Einstellung nur auf dem DC Master automatisch vorgenommen. Die Variable muss auf den anderen Samba-Servern manuell auf den gewünschten Namen gesetzt werden.

Bereits vor der Migration in der Windows-Domäne verwendete Rechnernamen können als NetBIOS-Namen oder NetBIOS-Aliase gesetzt werden.

Bei der Übernahme werden sämtliche von Samba und UCS unterstützten Attribute (z.B. Zeitpunkt der letzten Passwortänderung) übernommen.

Werden Konten aus der Benutzerdatenbank von Windows übernommen, die im UCS-Verzeichnisdienst schon mit gleichem Namen vorhanden sind, haben die Kontoattribute von Windows Vorrang. Das bedeutet unter anderem, dass die Windows-RID übernommen wird,

selbst wenn der Benutzer im UCS-Verzeichnisdienst bereits eine RID hat. Existiert im UCS-Verzeichnisdienst bereits ein Benutzerkonto mit der RID eines Benutzers, der aus der Windows-Domäne übernommen werden soll, erhält der Benutzer aus dem UCS-Verzeichnisdienst eine neue RID.

Wegen des Vorrangs der Attribute der Windows Benutzerdatenbank ist es problemlos möglich, eine Domänenübernahme zu wiederholen.

Zum Abschluss der Übernahme kann der Samba-PDC gestartet werden. Nach Deaktivierung des abzulösenden Windows-PDC kann diese Frage bestätigt werden. Alle anderen Windows-basierten Domänencontroller (BDC) müssen ebenfalls zeitnah aus der Domäne entfernt werden, da Änderungen (z.B. neue Benutzerkonten oder geänderte Passwörter) nicht vom Samba-PDC auf Windows-basierte Domänencontroller repliziert werden können. Für eine Übergangsphase können Änderungen auf allen Samba- und Windows-Domänencontrollern unterbunden werden. Mitgliedsserver können weiter unter Windows betrieben werden.

Da sich die SID der Samba-Domäne geändert hat, müssen bereits installierte Samba-Memberserver neu in die Domäne gejoined werden. Der Join kann über Univention Management Console oder über den Befehl `univention-join` durchgeführt werden. Weitere Informationen können im [UCS-Handbuch](#) nachgeschlagen werden.

Sofern in der UCS-Domäne schon vor der Domänen-Übernahme Windows-PCs eingebunden waren, müssen auch diese aufgrund der im Zuge der Übernahme veränderten SID erneut der Domäne beitreten.

Sollte die Übernahme nicht wie gewünscht verlaufen, finden sich in der Datei `/var/log/univention/pdc-takeover.log` Informationen zur Fehlerdiagnose.

3 Weiterführende Informationen zur Kontenübernahme

3.1 Passwörter

Für alle Benutzer, Gruppen und Rechner werden Samba- und POSIX-Konten im UCS-Verzeichnisdienst eingerichtet, für Benutzer außerdem Kerberos-Konten. Wenn unter Windows ein Passwort vorhanden war, wird dieses Passwort als Samba-Passwort gespeichert. Kerberos verwendet das Samba-Passwort in modifizierter Form. Das POSIX-Konto wird zunächst ohne Passwort angelegt, weil das POSIX-Passwort nicht berechnet werden kann. Die Benutzer können sich dennoch über Kerberos an Linux-Systemen anmelden. Wird das Passwort später geändert, wird das geänderte Passwort als Samba-, POSIX- und gegebenenfalls Kerberos-Passwort gespeichert. Dabei ist es unerheblich, ob das Passwort bei der Anmeldung unter Linux oder unter Windows geändert wird.

3.2 Bereits im UCS-Verzeichnisdienst vorhandene Konten und RIDs

Existierten im UCS-Verzeichnisdienst schon vor der Migration entsprechende Benutzer-, Gruppen- oder Rechnerkonten, so werden diesen Konten neue RIDs zugeordnet. Dies hat somit auch eine Änderung der SID (der eindeutigen Bezeichnung eines Windows-Benutzers) zur Folge.

Existierten im UCS-Verzeichnisdienst vor der Migration Konten mit der gleichen RID, aber anderem Namen als in der Windows-Benutzerverwaltung, so erhalten diese Benutzer im UCS-Verzeichnisdienst eine neue RID.

All diese Komplikationen können nur auftreten, wenn in der UCS-Domäne bereits Konten existieren. In der Regel sollten vor der Migration aber nur wenige, automatisch bei der Installation angelegte Konten vorhanden sein.

4 Datenübernahme

Um Daten von Windows-basierten Servern auf Samba-basierte Server zu migrieren, wird auf dem Samba-Server mindestens eine Verzeichnisfreigabe benötigt. Mit einem geeigneten Windows-Werkzeug (z.B. **robocopy**) können die Daten dann vom Windows-Server in die Freigaben auf den Samba-Server kopiert werden. Um die Datenkonsistenz zu gewährleisten, sollte während des Kopiervorgangs nur lesend auf die Daten zugegriffen werden. Anschließend sollten die Windows-Server abgeschaltet oder aus dem Netz genommen werden.

Hinweis:

Es ist möglich, Windows-basierte Mitgliedsserver in eine Samba-Domäne zu integrieren. Befinden sich die benötigten Daten nicht auf einem Domänencontroller, sondern auf einem Mitgliedsserver, ist es also nicht zwingend erforderlich, die Daten zu migrieren.

4.1 Durchführung der Datenübernahme

Für die Migration der Daten von Windows-basierten Servern auf Samba-basierte Server hat sich das Werkzeug **robocopy** ab Version 1.96 bewährt. Es ist im Windows-2000-Professional-Resource-Kit sowie im Windows-2000-Server-Resource-Kit enthalten. Das Programm **scopy** aus dem Windows NT 4.0-Resource-Kit hat sich dagegen nicht als zuverlässig erwiesen. Gegenüber dem Kopieren von Daten mit dem Windows Explorer oder mit gewöhnlichem **copy**-Befehl bietet **robocopy** den Vorteil, dass es Eigentümer und ACLs an Dateien und Verzeichnissen erhalten kann. Voraussetzung ist, dass die Windows-Benutzer in der Samba-Domäne bekannt sind, die Domänenübernahme also bereits durchgeführt wurde.

Die Datenübernahme wird folgendermaßen durchgeführt: Zunächst sollten mit Univention Directory Manager auf dem Samba-Server, auf den Daten kopiert werden sollen, Samba-Freigaben für die zu migrierenden Windows-Dateien eingerichtet werden. Es empfiehlt sich, die Freigaben auf EXT3- oder XFS-Partitionen einzurichten.

Wie unten beschrieben sollte das Programm **robocopy** auf dem Windows-Server, von dem aus die Daten kopiert werden sollen, für jede Freigabe aufgerufen werden. Es sollte dabei ein Benutzerkonto verwendet werden, das über Leserechte für das Quellverzeichnis und Schreibrechte für das Zielverzeichnis verfügt.

```
robocopy <Quellverzeichnis> <Zielverzeichnis> /E /Z /SEC \
/SECFIX /TIMFIX /R:<Wiederholungen> /W:<Sekunden> /V /NP \
/LOG:<Dateiname>
```

UNC-Pfadangaben sind zulässig. Pfade mit Sonderzeichen müssen in Anführungsstriche gesetzt werden. Die Parameter und Optionen haben folgende Bedeutung:

Parameter/Option	Erklärung
Quellverzeichnis	Verzeichnis auf dem Windows-Server, das kopiert werden soll
Zielverzeichnis	Verzeichnisfreigabe auf dem Samba-Server, in die kopiert werden soll, anzugeben als UNC-Pfad (<code>\\Server\Freigabe</code>)
/E	kopiert rekursiv auch leere Unterverzeichnisse
/Z	erlaubt den Neustart von robocopy , wenn es abgebrochen wurde
/SEC	kopiert auch Sicherheitsinformationen (ACLs)
/SECFIX	kopiert auch Sicherheitsinformationen (ACLs), die im Zielverzeichnis schon vorhanden sind
/TIMFIX	passt die Dateizeiten an
/R:<Wiederholungen>	Anzahl der Versuche im Falle eines Fehlers, die betreffende Operation zu wiederholen
/W:<Sekunden>	Zeit in Sekunden, die zwischen zwei Wiederholungsversuchen gewartet wird
/V	erhöht die Anzahl der Ausgaben des Programms
/NP	unterdrückt die Anzeige eines Fortschrittsbalkens
/LOG:<Dateiname>	gibt ein Protokoll in die mit Dateiname bezeichnete Datei auf dem Windows-Server aus

Beispiel:

Auf einem Windows NT-Server existiert auf Laufwerk **H:** ein Verzeichnis **user-homes** mit den Heimatverzeichnissen der Windows-Benutzer, das auf den Samba-Server migriert werden soll. Hierzu muss in Univention Directory Manager eine Verzeichnisfreigabe mit Verzeichnisbesitzer **Administrator** und **Samba-Schreibzugriff** eingerichtet werden. Der Freigabe sollte ein Name, z.B. **win-homes**, erteilt werden. Die übrigen Parameter können nach Bedarf angepasst oder auf den voreingestellten Werten belassen werden.

Hinweis:

Die Samba-Freigabe **homes** nimmt eine Sonderstellung ein, da sie immer das Linux-Heimatverzeichnis des jeweiligen Benutzers freigibt. Wenn anstelle der Samba-Freigabe **win-homes** die Samba-Freigabe **homes** verwendet wird, werden die Verzeichnisse also in das Linux-Heimatverzeichnis des Benutzers kopiert, der den Befehl unter Windows ausführt.

Anschließend sollte als Benutzer **Administrator** an der Windows-Kommandozeile folgender

Befehl eingegeben werden:

```
robocopy h:\user-homes \\ucs-samba-server\win-homes /E \  
/Z /SEC /SECFIX /TIMFIX /R:10 /W:10 /V /NP \  
/LOG:robocopy.log
```

Achtung:

Je nach verfügbarer Netzwerkbandbreite und Menge der zu kopierenden Daten kann der Kopiervorgang längere Zeit in Anspruch nehmen. Zur Erhaltung der Datenkonsistenz ist unbedingt sicherzustellen, dass während des Kopiervorgangs nicht mit den Daten gearbeitet wird, beziehungsweise nur lesend auf die Daten zugegriffen wird.



Nachdem alle weiterhin benötigten Freigaben eines Windows-Servers in Verzeichnisse auf dem Samba-Server kopiert worden sind, sollte der Windows-Server abgeschaltet oder aus dem Netz genommen werden.

Sollen die Daten weiterhin unter dem Namen des Windows-Servers verfügbar sein, muss die Univention Configuration Registry-Variable `samba/netbios/aliases` des Samba-Servers auf den Namen des Windows-Servers konfiguriert werden und der Samba-Dienst neu gestartet werden.

Für die Auflösung des Namens über DNS muss ein Alias-Record in Univention Directory Manager eingerichtet werden.

Nach kurzer Zeit sollten die Freigaben wieder unter dem als NetBIOS-Alias eingerichteten Namen des Windows-Servers und außerdem unter dem Namen des Samba-Servers in der Netzwerkumgebung der Windows-Clients sichtbar sein.

Hinweis:

Die Übertragung der ACLs von Windows nach Samba/Linux ist nicht in allen Fällen in einer Form möglich, dass sie hinterher exakt den unter Windows bestehenden ACLs entsprechen. Dies liegt an den unterschiedlichen Verfahren zur Rechteverwaltung mit unterschiedlichen Rechteklassen. Es ist deshalb notwendig, die wesentlichen ACLs manuell zu prüfen und gegebenenfalls zu korrigieren.

5 Übernahme von Druckerfreigaben

Windows NT stellt bei Druckerfreigaben im Netzwerk auf Wunsch Druckertreiber zur automatischen Installation auf Windows-Clients zur Verfügung. Um diese Funktionalität nach der Migration unverändert nutzen zu können, müssen die Druckerfreigaben inklusive der dazugehörigen Treiberdateien auf den Samba-Druckerserver migriert werden.

Achtung:

Falls sich die zu migrierenden Druckerfreigaben auf dem Windows-PDC befinden, sollte die Druckerübernahme vor der Domänenübernahme durchgeführt werden, da der Windows-PDC nach der Domänenübernahme nicht mehr aktiviert werden sollte.



Hinweis:

univention-winprinters ist eine Migrationshilfe, um von bestehenden Windows-Clients weiterhin zu drucken, ohne dass dort die Einstellungen geändert werden müssen. Allerdings können die migrierten Drucker nicht sofort von einem Linux-Arbeitsplatz aus verwendet werden, weil sie nach der Migration über **smb** angesprochen werden.

Sollen die Drucker auch unter Linux verwendet werden, so muss in Univention Directory Manager eine Druckerfreigabe mit dem passenden Druckermodell angelegt werden. Es existiert dann eine Freigabe für den Drucker, die bei der Migration automatisch erstellt wurde und den Drucker unter Windows zur Verfügung stellt, und eine von Hand eingetragene Freigabe, die den Drucker unter Linux bereitstellt. Wenn nur eine Freigabe pro Drucker gewünscht ist, sollte eine Druckerfreigabe mit dem passenden Druckermodell angelegt werden und der Drucker auf den Windows-Rechnern als Netzwerkdrucker mit Postscript-Treibern konfiguriert werden.

5.1 Voraussetzungen

Das Paket **univention-winprinters** muss auf dem Samba-Druckserver installiert sein.

Außerdem muss auf dem Windows-Server mindestens ein Drucker freigegeben sein. Die Groß- und Kleinschreibung in Druckernamen wird beachtet. Druckernamen, die Sonderzeichen wie Umlaute oder Leerzeichen enthalten, werden als Samba-Namen übernommen (siehe auch das Druckdienste-Kapitel im [UCS-Handbuch](#)).

5.2 Druckerdaten lesen

Um die Druckerdaten mit Namen, Treibern und Einstellungen von dem Windows-Server auszu-lesen, muss auf dem UCS-Server der Befehl

```
get_winprinters --nt4_server=<nt-server-name> \  
                [ --nt4_domain=<nt-server-domain> ] \  
                [ --nt4_ipaddr=<nt-ipaddr> ]
```

einggegeben werden, wobei ein Benutzername mit Administrationsrechten und das dazugehörige Passwort der Windows-Domäne abgefragt werden. Für diesen Befehl werden keine **root**-Rechte auf dem UCS-Server benötigt. Die Parameter haben folgende Bedeutung:

Variable	Erklärung
nt-server-name	Name des Windows-Druckerservers
nt-server-domain	Name der Windows-Domäne (nur nötig, falls nicht automatisch erkannt)
nt-ipaddr	IP-Adresse des Windows-Druckerservers (nur nötig, falls nicht automatisch erkannt)

Das Skript erstellt für jeden Drucker ein Debian-Paket mit dem Namen **winprt-*<Druckername>*.deb** im aktuellen Verzeichnis (Bsp. **winprt-hp-color-laserjet.deb**). Diese Pakete können kopiert, archiviert oder lokal weiterverwendet werden.

5.3 Druckerdaten auf UCS installieren

Über die Univention Management Console können die benötigten Debian-Pakete auf dem Samba-Druckerserver installiert werden. Dabei setzen sich die Paketnamen aus dem Präfix "winprt" und dem Suffix "<druckername>.deb" zusammen.

Achtung:

Installieren bedeutet hier nicht, dass die entsprechenden Drucker installiert werden, sondern dass die Dateien aus dem Paket in das Verzeichnis `/var/lib/winprt-data/` kopiert werden.



Um zu prüfen, ob die Drucker korrekt migriert wurden, kann als Benutzer **root** mit dem Befehl

```
list_winprinters
```

(ohne Parameter) eine Auflistung aller übernommenen Drucker vorgenommen werden.

6 Drucker auf dem Samba-Druckserver installieren

Mit folgendem Befehl werden die übernommenen Drucker auf dem System installiert:

```
put_winprinters \
  --samba_hostname=<samba-printserver-hostname> \
  [--ldap_binddn=<ldap-binddn>] \
  [--ldap_bindpwf=<ldap-bindpw-file>] \
  [--ldap_position=<ldap-position-dn>] \
  <Druckername>
```

Dabei wird der Benutzername eines **Printer Admins** oder eines Administrators mit entsprechendem Passwort abgefragt. Die Parameter haben folgende Bedeutung:

Parameter	Erklärung
samba-printserver-hostname	Rechnername des Samba-Servers, auf dem die Druckerfreigaben eingerichtet werden sollen.
Druckername	Name(n) von einem oder mehreren Druckern wie von list_winprinters angezeigt.
ldap-binddn	DN des Benutzers, mit dessen Rechten die Druckerfreigaben im UCS-Verzeichnisdienst eintragen werden sollen. Diese und die folgende Angabe sind nicht erforderlich, wenn put_winprinters als root auf dem DC Master aufgerufen wird.
ldap-bindpw-file	Relativer oder absoluter Pfad einer Datei, die das Passwort des oben genannten Benutzers enthält.
ldap-position	Position im UCS-Verzeichnisdienst, an dem die Daten für den installierten Drucker gespeichert werden sollen.

Mit dem folgenden Befehl werden z.B. alle Drucker auf dem Samba-Druckserver **ucs-print01** installiert. Die Daten werden dabei unter dem Container (**cn=printers, dc=firma**) gespeichert. Der LDAP-Schreibzugriff erfolgt im Beispiel ebenfalls als Benutzer **Administrator** mit dem Passwort, das aus der Datei **passwort** im aktuellen Verzeichnis ausgelesen wird. Es empfiehlt sich, diese Datei nur temporär mit einem Editor in einem beliebigen Verzeichnis anzulegen und nach der Verwendung durch **put_winprinters** sofort wieder zu löschen.

```
put_winprinters --samba_hostname=ucs-print01 \  
--ldap_binddn=uid=Administrator, cn=users, dc=firma, dc=com \  
--ldap_bindpwf=passwort \  
--ldap_position=cn=printers, dc=firma \  
\$(list_winprinters)
```

Die migrierten Drucker können über **Univention Directory Manager → Drucker → Suchen** angezeigt werden. Ihnen sollte jeweils der Druckerhersteller **misc** und das Druckermodell **smb** zugeordnet sein. Zur Administration der Drucker steht außerdem das **CUPS**-Webinterface (<http://<druckerserver>:631>) zur Verfügung. Unter Windows sind die Drucker über die Netzwerkumgebung zugänglich.