INTRAPACT

THE INFORMATION OFFICE

ADsync Handbuch

11.0

Impressum

ADsync Handbuch Intrapact 11.0, 1. Auflage, 2019.

Dieses Handbuch wurde mit aller Sorgfalt erstellt. Dennoch kann die aktuelle Programmversion von der Beschreibung in diesem Handbuch abweichen. In Beispielen verwendete Namen und Daten sind frei erfunden.

Inhaltsverzeichnis

1. Zusammenfassung

Die Synchronisation der Benutzer aus dem Windows Active Directory (AD) mit der Benutzerverwaltung in den Intrapact Firmen wird über Skripte durchgeführt, die in der jeweiligen Firmendatenbank im Microsoft SQL Server hinterlegt sind.

Diese Skripte bauen eine Verbindung mit Ihrem AD auf und importieren von dort alle Benutzer, Gruppen und Gruppenzuordnungen zu Benutzern, die konfigurierbaren Kriterien entsprechen. Die Verbindung zum AD ist somit eine Einbahnstraße von AD nach Intrapact. Es werden keine Daten von Intrapact ins AD übertragen.

Für die Anbindung ist sowohl die Vollversion von Microsoft SQL Server, als auch die kostenlose Express Edition verwendbar.

Für die periodische Wiederholung des Imports kann die Aufgabenplanung unter Windows oder der SQL Server Agent Dienst verwendet werden.

Wenn Sie alle 3 Synchronisationsbereiche (Benutzer, Gruppen, Gruppenzuordnungen) verwenden, und die Rechtevergabe im Intrapact auf die Gruppen beschränken, dann können Sie eine integrierte Rechtevergabe in den Intrapact-Firmen über das AD steuern. Das heißt, sobald Sie eine Person im AD anlegen und sie den Gruppen zuteilen, ist diese dann ab der nächsten Synchronisation automatisch in der Intrapact-Firma mit den aus den Gruppen abgeleiteten Rechten angelegt, von der aus die Synchronisation gestartet wurde. Das gleiche gilt für Änderungen und für Löschungen.

2. Voraussetzungen

Für die erfolgreiche Implementierung des ADsyncs sind folgende Voraussetzungen zu erfüllen:

- Die AD Anbindung wurde als SQL Server Lösung konzipiert und benötigt daher eine beliebige SQL Server Version ab SQL Server 2008 (Vollversion oder Express Edition)
- Der Zugriff auf das AD erfolgt über eine „Linked Server" Verbindung. Die Berechtigungen dazu müssen vorhanden sein.
- Wenn Fotos aus dem AD importiert werden sollen muss am Server Windows PowerShell zur Verfügung stehen
- Die SQL Server Express Edition besitzt keinen SQL Agent Dienst; deshalb muss einerseits die periodische Wiederholung auf die Windows Aufgabenplanung ausgelagert werden, und andererseits kann die E-Mail-Benachrichtigung über den Importerfolg nur als einfache Textnachricht, also ohne detaillierten Anhang erfolgen, da die Expressedition keine E-Mail Anhänge unterstützt, weil sie dazu einen SQL Agent Dienst benötigen würde.
- Die AD Anbindung wird in jede Firma separat implementiert und kann somit für jede Intrapact Firma getrennt eingestellt werden.
- Im SQL Server müssen die Verwendung von Master..xp_CMDShell und OPENQUERY aktiviert werden

3. Komponenten

Folgende Komponenten müssen in der SQL Server Datenbank einer Firma installiert werden, bzw. werden in späterer Folge einmal automatisch durch ein Setup-Programm installiert:

3.1 Tabelle: kradsettings

In der Tabelle „kradsettings“ werden alle variablen Einstellungen für die AD Synchronisation verwaltet. Diese sind:

Lid	Der Datensatz-Schlüssel. Es darf immer nur 1 Datensatz in der Tabelle sein mit Schlüsselwert = 1
Dtedit	Intrapact-internes Feld
Dtcreation	Intrapact-internes Feld
Luserid	Intrapact-internes Feld
Lcreatorid	Intrapact-internes Feld
Lownerid	Intrapact-internes Feld
Leditid	Intrapact-internes Feld
Lviewid	Intrapact-internes Feld
Xldapstring	Die LDAP-Zeichenfolge, über die das AD durchsucht wird. Beispiel: LDAP://server.local/DC=domain,DC=local Damit werden einmal alle AD-Objekte die sich in der Domäne „domain.local“ des Domaincontrollers „server.local“ befinden für die Auswahl vorgesehen. Diese Auswahl kann dann über die nächsten 2 Filterregeln noch eingeschränkt werden.
Xsqlpersfiltstring	Filterregel für den Personenimport in SQL Notation. Beispiel: l = ''Zürich'' AND department = ''Marketing'' ACHTUNG: jeweils 2 einzelne Hochkommas und nicht 1 Doppelhochkomma! Es werden nur Personen importiert bei denen im AD bei Ort „Zürich“, und in der Abteilung „Marketing“ gespeichert ist. Näheres siehe im Filter-Kapitel weiter unten.
Xsqlgrpfiltstring	Filterregel für den Gruppenimport in SQL Notation. Beispiel: sAMAccountName = ''Intrapact*''

	Es werden nur Gruppen importiert deren Name im AD mit „Intrapact“ beginnt. Näheres siehe im Filter-Kapitel weiter unten.
xinsertgroups	1 = Gruppen sollen aus dem AD übernommen werden, alles andere heißt „nicht übernehmen“.
xinsertmembership	1 = Gruppenzugehörigkeiten von Personen sollen aus dem AD übernommen werden, alles andere heißt „nicht übernehmen“.
xdeactinactmember	1 = Im AD deaktivierte Personen sollen übernommen werden, alles andere heißt „nicht übernehmen“. Dabei wird diese Person auch im Intrapact als deaktiviert gekennzeichnet, und zwar wird in der Tabelle kruser das Feld bdeactivated auf „1“ gesetzt. So eine Person ist nach wie vor in der Benutzerverwaltung sichtbar, behält alle Rechtezuordnungen, kann sich aber nicht mehr anmelden. In der Benutzerverwaltung von Intrapact erhält diese Person einen Haken im Feld „Deaktiviert“. Dort kann man diesen ev. wieder entfernen und die Person ist wieder vollständig aktiv.
xdeldeletedmember	1 = Im AD gelöschte Personen sollen auch im Intrapact als gelöscht markiert werden, alles andere heißt „gelöschte Personen ignorieren und im Intrapact weiter belassen“. Beim Lesen des AD's werden gelöschte Personen nicht mehr in der Ergebnismenge angezeigt, d.h. diese fehlen ganz einfach. Wenn eine Person im AD fehlt, im Intrapact aber noch vorhanden ist, dann ist diese Person ein Löschkanditat. Wenn hier in diesem Feld eine „1“ steht, dann wird die Person in der Tabelle kractor als gelöscht markiert (bdeleted = 1), alle Gruppenzuordnungen werden tatsächlich gelöscht und die Person selber wird in der Tabelle kruser als gelöscht markiert. Dabei wird der Login-Name (strusername) mit einem Präfix aus <**lid-der-person> markiert. Also z. B. wenn Herr Peter Huber den Datensatzschlüssel (= lid) von 147 hat und sein Anmeldename ist „phuber“ dann wird der Anmeldname zu <**147>phuber geändert. Dies zeigt für Intrapact einen gelöschten Benutzer an.
xprimarygroupname	Das Microsoft AD kann auch als Directory-Service für Linux, Unix oder Apple Mac Computer fungieren. In diesem POSIX Standard ist eine sogenannte Hauptgruppenzuordnung (Primary Group) für jede Person notwendig. In einer Windows Domäne braucht man das nicht zwingend. Wenn man jetzt alle Gruppenzuordnungen zu einem User aus dem AD

	ausliest erhält man alle Gruppen, wo dieser User drinnen ist (auch Gruppen in Gruppen werden aufgelöst), aber die Primary Group ist nicht Teil dieser Gruppenauflistung, sondern ist ein Spezialfeld im AD, welches nur extrem aufwändig ausgelesen werden kann. Standardmäßig ist die Primary Group immer „Domänen-Benutzer“ und sollte nach Microsoft Regeln auch niemals geändert werden, außer man kennt alle damit verbundenen Seiteneffekte. Der gewünschte Namen kann jedenfalls hier hinterlegt werden.
xlogmode	Was beim AD Import genau gemacht wird, kann in einer LOG-Tabelle (kradlog) mitprotokolliert werden. Dabei gibt es verschiedene Methoden, die durch diesen Parameterwert gesteuert werden: LOG_ONLY: Es wird nur ein „was-wäre-wenn“ Szenario durchgeführt, d.h. es wird alles protokolliert, welche Personen geändert, gelöscht, neu angelegt, Gruppenanlage, etc. werden, aber diese Aktionen werden NICHT durchgeführt. Das heißt, an den Daten in der Datenbank ändert sich nichts, man kann nur sozusagen einen Testlauf machen, was gemacht würde. LOG_OVERWRITE: Die LOG-Tabelle wird gelöscht, dann wird alles ganz normal importiert und das neue LOG ersetzt die alten Daten. LOG_APPEND: Es wird alles ganz normal importiert und das neue LOG wird an die alten Daten unten angehängt. Die LOG-Tabelle wird immer größer und man kann alte Imports später auch noch überprüfen. LOG_OFF: Es wird nur importiert und nichts mitgeschrieben, was gemacht wurde.
xaddall2users	YES: Alle importierten Personen werden zusätzlich in die Intrapact interne Gruppe „Benutzer“ (lid = 4) eingefügt.
xaddthisgroup2admin	Hier kann ein AD Gruppenname angegeben werden, deren Mitglieder alle in die Intrapact interne Gruppe „Administratoren“ (lid = 3) eingefügt werden. Beispiel: Domänen-Admins
xtakeimagesfrom	Im AD können auch Fotos vom Personen (Avatar-Fotos) hinterlegt werden. Dazu gibt es im AD 2 Bereiche:

	„thumbnailPhoto“: Dieses Feld wird von Microsoft intern auch benutzt für die Fotos im Exchange, Outlook, Office, Windows 10 Login-Foto, etc. Dies ist der bevorzugte Weg, denn da sind dann alle Fotos in den Microsoft Produkten und in den Intrapact Firmen gleich. Ein Foto darf im AD hier max. 100kB groß sein, sonst kann man es im AD nicht speichern. Und es wird eina Auflösung von 100px x 100px von Microsoft empfohlen, damit das Foto gut aussieht. „jpegPhoto“: Dieses Feld dient für Fotos, die von Microsoft nicht verwendet werden. Wenn man was getrenntes Eigenes machen will, dann kann man auch dieses Feld verwenden. Hier gibt es die Limits meines Wissens nach nicht, aber man muss sich halt noch mehr selber darum kümmern, dass alles gut aussieht. Es gibt in beiden Varianten keine automatisch Skalierung oder dergl.
xsendlogasmailto	Wenn man hier eine E-Mail Adresse eingibt, dann wird nach dem Import eine Mail an diese Adresse gesendet, mit dem Erfolgsstatus des Imports. Bei einer SQL Server Vollversion mit Anhang, bei einer Expressversion nur eine reine kurze Textnachricht.
xmailprofile	Im SQL Server muss ein E-Mail Profil angelegt werden, über welches der SQL Server dann E-Mails versenden kann. Hier muss der Name des Profils angegeben werden, wenn ein E-Mail Versand gewünscht wird.
xtmpimagepath	Dies ist der Pfad zum Ordner auf der SQL-Server Maschine, in dem die Powershell-Skripts und das temporäre Verzeichnis für den Bilderimport aus dem AD gespeichert werden.

3.2 Tabelle: kradlog

In dieser Tabelle werden alle Informationen gespeichert, was beim Import durchgeführt wurde. Diese Tabelle lässt sich wie eine Liste lesen, d.h. es gibt immer Überschriftzeilen und darunter die Datenzeilen mit der expliziten Aufzählung der Personen, Gruppen, etc. wo Änderungen, Löschungen, Einfügungen gemacht wurden. Der Inhalt dieser Tabelle wird bei der E-Mail Benachrichtigung zum Import als .csv Datei angehängt (nur bei SQL Server Vollversion) und kann über Microsoft Excel geöffnet werden.

3.3 Stored Procedure: GetAllFromAD

Dieses Skript führt den kompletten Import durch. Es ist verschlüsselt abgelegt.

3.4 Stored Procedure: GetADGroups4User

Dieses Skript wird von GetAllFromAD benötigt, um aus dem AD für jeden einzelnen Benutzer alle Gruppenzugehörigkeiten zu lesen. Es ist verschlüsselt abgelegt.

4. Inhalt des Ordners xtmpimagepath auf der SQL Server Maschine

Der Pfad, der im Feld xtmpimagepath gespeichert wird, muss sich auf der SQL Server Maschine befinden. Das heißt, wenn sich Intrapact und der SQL Server auf derselben Maschine befinden, dann ist das ein Pfad innerhalb der Intrapact-Struktur. Wenn der SQL Server auf einer eigenen Maschine betrieben wird, dann muss dieser Pfad auf dem SQL Server angelegt sein, und von diesem schreibend und lesend genutzt werden können. Der nachfolgend genannte Ordner und die 2 Skripts müssen sich dort befinden.

4.1 Ordner „tmpstorage“

Im Ordner < xtmpimagepath>\tmpstorage werden alle Fotos aus dem AD zwischengespeichert. Von dort holt sich dann das SQl-Server Importskript die Dateien ab und fügt sie in die Tabelle „kruserpic“ zur jeweiligen Person ein. Die Fotos haben dazu als folgende Namenskonvention: Loginname.jpg

4.2 Commandline-Skript „ADimport“

In diesem Skript muss der richtige Datenbankname für das AD Importskript angepasst werden. Dieses Skript wird in die Windows Aufgabenplanung eingehängt, damit der AD Import periodisch durchgeführt werden kann. Wird der SQL Server auf einer eigenen Maschine betrieben, und will man die periodische Abholung der Daten aus dem AD über die Windows-Aufgabenplanung erledigen und nicht über den SQL Server Agent Dienst, dann muss der Aufruf dieses Skripts manuell in die Windows Aufgabenplanung eingebaut werden.

4.3 PowerShell-Skript „ps_ADPhotoExport.ps1“

Dieses Skript wird für den Foto-Import aus dem AD benötigt. Es liest die Fotos aus dem AD aus und legt diese im Ordner „tmpstorage“ ab. Wird kein Fotoimport gewünscht, wird dieses Skript nicht benötigt.

5. Anmerkungen zu den Filterregeln

Wenn keine Filterregeln angegeben werden, dann werden alle Personen / Gruppen genommen, die die LDAP-Zeichenfolge liefert. Die Filterregeln gehören nur zu deren weiteren Einschränkung.

Die Filterregeln müssen immer in SQL Notation angegeben werden, wobei bei einfachen Hochkommas diese immer doppelt angegeben werden müssen.

Als Filterfelder können alle „Single-Value" AD-Felder verwendet werden. „Multi-Value" AD-Felder werden von der SQL-Linked-Server Anbindung nicht unterstützt. „Single-Value" Felder sind alle Felder, wo genau 1 Wert drinnen steht, wie z.B. cn (Vollständiger Name), ln (Familienname), l (Ort), usw. „Multi-Value" Felder sind AD-Felder, wo sozusagen mehrere Zeilen, mehrere Werte durch irgendwas getrennt oder ähnliches, drinnen stehen. In der Darstellung (siehe SELFADSI) sieht man meistens, dass es eine Liste ist. So z.B. description (Personenbeschreibung), otherIpPhone (IP Telefonnummern), etc.

Wie die einzelnen Felder heißen findet man am besten auf der SELFADSI Website:

Personen: http://www.selfadsi.org/user-attributes-w2k8.htm

Gruppen: http://www.selfadsi.org/group-attributes-w2k8.htm

Beispiele:

cn <> ''*$''	Importiere nur, wenn der vollständige Name nicht mit $ endet (das sind Systemnamen im AD)
l IN (''Zürich'', ''Bern'', ''Wien'')	Importiere nur, wenn Adressort entweder Zürich, Bern oder Wien ist (das 1. Zeichen ist ein kleines „L", der AD Code für den Adressort)
postalCode = ''4*''	Importiere nur, wenn die Postleitzahl mit 4 beginnt.
sAMAccountName = ''Intrapact_*''	Importiere nur Gruppen, die mit Intrapact_ beginnen
cn <> ''*$'' AND l IN (''Zürich'', ''Bern'', ''Wien'')	Eine Kombination mehrerer Parameter. Hier z.B. Importiere nur, wenn der vollständige Name nicht mit $ endet und wenn Adressort entweder Zürich, Bern oder Wien ist.

6. Master..xp_CMDShell und OPENQUERY Aktivierung

Das Importskript verwendet Teile im SQL Server, die standardmäßig nicht unbedingt aktiviert sind. Diese können im SQL Server mit folgenden Befehlen aktiviert werden:

OPENQUERY, OPENROWSET:

```
sp_configure 'show advanced options', 1;
RECONFIGURE;
GO
sp_configure 'Ad Hoc Distributed Queries', 1;
RECONFIGURE;
GO
```

Aufruf von externen Skripts (z.B. Powershell) aus SQL Skripts heraus:

```
-- To allow advanced options to be changed.
EXEC sp_configure 'show advanced options', 1;
GO
-- To update the currently configured value for advanced options.
RECONFIGURE;
GO
-- To enable the feature.
EXEC sp_configure 'xp_cmdshell', 1;
GO
-- To update the currently configured value for this feature.
RECONFIGURE;
GO
```

7. Ablauf des AD Imports

Der AD-Import wird normalerweise automatisch über die Windows Aufgabenplanung oder den SQL Server Agent Dienst gestartet. Alle vom Skript zusätzlich benötigten Zwischentabellen, Views, etc. werden dynamisch angelegt und verwendet.

Der Import läuft in 3 Abschnitten ab, wobei als erstes die Daten aus dem AD in Zwischentabellen gelesen werden, danach werden diese Daten in die entsprechenden Intrapact-Tabellen, mit eventueller LOG-Datei Mitschrift, eingepflegt, und zum Abschluss kann eine Statusmeldung des Imports mit eventuellem LOG-Datei Anhang per Mail an eine definierte Person versendet werden.

7.1 Ablauf des 1. Abschnitts

1. Es wird überprüft, ob der AD-Zugriff als LinkedServer angelegt ist. Falls nicht, wird dieser automatisch erstellt. Je nach Berechtigungsstruktur am SQL Server kann es sein, dass der Linked Server noch manuell im SQL Server Management Studio nachbearbeitet werden muss, damit er alle Zugriffsrechte hat, und zwar in der jeweiligen Datenbank, unter Serverobjekte -> Verbindungsserver -> ADSI mit Rechtsklick auf „Eigenschaften“ gehen und dort dann den Abschnitt „Sicherheit“ im linken Menübaum wählen. Dort gehört eventuell „In folgendem Sicherheitskontext verwenden:“ ausgewählt, und ein Domainbenutzer („domainname\benutzername“) mit seinem Kennwort eingetragen, der vollen Zugriff auf das AD hat.

2. Das AD vor Windows Server 2008 ließ eine maximale Anzahl von 1000 Objekten pro Abfrage zu. Ab Version Windows Server 2008 kann man nur mehr maximal 901 Objekte pro Abfrage abfragen. Da es aber durchaus Firmen mit mehr als 901 Mitarbeiter gibt, wird im 2. Schritt automatisch eine Abfrage generiert (Abfrage: „adViewMembers“ unter den Sichten in der Datenbank), die jeweils eine eigene Abfrage startet pro 1. Zeichen des Loginnamens. Dieses darf numerisch (0 bis 9) oder ein Buchstabe des Alphabets (A bis Z) sein. Umlaute dürfen auch sein, da die Sortierreihenfolge des SQL Servers z.B. bei einer Abfrage nach allen Personen, die mit „O“ beginnen, auch alle Personen, die mit „Ö“ beginnen, liefert. Zusammengefasst heißt das, pro Anfangsbuchstabe des Loginnamens werden max. 901 Personen übernommen; also max. 901 Personen, die mit „A“ beginnen, max. 901 Personen, die mit „B“ beginnen, usw.

   Im 2. Schritt werden jetzt auf diese Art und Weise alle Personen, die der LDAP-Zeichenfolge und der Personen-Filterregel aus der Tabelle „kradsettings“

entsprechen, in die temporäre Zwischentabelle „kruseradimport“, mit allen benötigten AD-Feldern, importiert.

3. Analog Punkt 2 wird im 3. Schritt der gleiche Vorgang mit den Gruppen durchgeführt. Es wird die Abfrage „adViewGroups“ generiert, und alle Gruppen, die der LDAP-Zeichenfolge und der Gruppen-Filterregel aus der Tabelle „kradsettings“ entsprechen, in die temporäre Zwischentabelle „krusergroupadimport“, mit allen benötigten AD-Feldern, importiert.

4. Im 4. Schritt werden dann zu jeder Person alle Gruppen aus dem AD gelesen, in die sie eingeordnet ist. Dazu wird für jede Person die Stored Procedure „GetADGroups4User“ aufgerufen, welche aus dem AD für die jeweilige Person die Gruppen in eine temporäre Zwischentabelle liest, dabei auch Gruppen in Gruppen auflöst, und das Ergebnis davon dann in die weitere temporäre Zwischentabelle „krgroupuseradimport“ einfügt.

7.2 Ablauf des 2. Abschnitts

1. Es wird überprüft, ob die LOG-Tabelle existiert. Wenn nicht, wird diese automatisch angelegt.

2. Aus der Tabelle „krcompprops“ wird die letzte Replikations-ID ausgelesen, um 1 erhöht und wieder zurückgespeichert. Die Replikations-ID ist eine eindeutige Importnummer und wird bei den Datenänderungen im Intrapact immer mitgespeichert. Dadurch kann man sehen, wann ein Datensatz (Benutzer, Gruppen) zuletzt durch einen AD-Import geändert wurde.

3. Nur wenn in den „kradsettings“ die Deaktivierung von Personen erlaubt wurde, wird folgendes gemacht:

   Es werden alle im AD deaktivierten Personen ermittelt, welche im Intrapact noch nicht deaktiviert sind. Nur wenn die jeweilige Person eine alte Replikations-ID hat wird das „bdeactivated“-Feld in der Tabelle „kruser“ auf „1“ gesetzt und sie somit auch im Intrapact deaktiviert. Am Vorhandensein einer Replikations-ID erkennt man nämlich, dass diese Person aus dem AD angelegt wurde, und nicht manuell im Intrapact erfasst wurde. Manuell erfasste Personen werden bei Deaktivierungen und Löschungen nicht berücksichtigt, da sie ja nicht aus dem AD angelegt wurden. Deaktivierte Personen im AD erkannt man, dass im „userAccountControl“ Feld des AD das 2. Bit gesetzt ist (userAccountControl & 2 = 2).

4. Nur wenn in den „kradsettings“ die Löschung von Personen erlaubt wurde, wird folgendes gemacht:

Es werden alle im Personen ermittelt, welche aus dem AD nicht mehr importiert wurden, und im Intrapact aber noch vorhanden sind. Nur wenn die jeweilige Person eine alte Replikations-ID hat wird die Löschmarkierung durchgeführt. Dabei wird das „bdeleted"-Feld in der Tabelle „kractor" auf „1" gesetzt, der Loginname (strusername) in der Tabelle „kruser" erhält ein Präfix von „<**lid_des_users>", und aus der Tabelle „krgroupusers" werden alle Gruppenzuordnungen dieser Person gelöscht. Sollte diese Person wiederkehren können sich die Gruppenzuordnungen ja geändert haben.

Durch diese Maßnahmen ist diese Person im Intrapact nicht mehr sichtbar.

5. Im Schritt 5 wird geprüft, ob es Personen gibt, die im Intrapact als gelöscht markiert sind, jetzt aber im Import wieder vorhanden sind. Das sind die sogenannten Rückkehrer.
   Durch die Übernahme von Altdaten kann es noch sein, dass eine Person mehrfach als gelöscht markiert in der Datenbank vorhanden ist, da sie im alten System jedes Mal neu angelegt wurde, wenn sie nach einer Löschung im Import wieder vorhanden war.
   Im neuen System wird deshalb bei Rückkehrern immer der letzte Datensatz dieser Person (der Datensatz mit der höchsten lid) wieder reaktiviert, das heißt, es wird das „bdeleted"-Feld in der Tabelle „kractor" auf „0" gesetzt, der Präfix von „<**lid_des_users>" vom Loginname (strusername) in der Tabelle „kruser" entfernt. Prophylaktisch werden auch die Gruppenzuordnungen nochmals gelöscht, weil sie ja aus Altlasten stammen könnten. Danach ist der User wieder sichtbar und erhält die Gruppenzuordnungen dann neu in einem der weiteren Schritte zugeteilt.

6. Im Schritt 6 wird jetzt bei allen in der temporären Importtabelle, und gleichzeitig auch in der kruser-Tabelle mit Replikations-ID vorhandenen Benutzern überprüft, ob es Änderungen bei Datenfeldern gegeben hat (Name, Straße, PLZ, Ort, usw.). Dort, wo es welche gibt, werden diese mit den Daten aus dem AD korrigiert.

7. Im Schritt 7 werden jetzt alle neuen Personen (also in der temporären Tabelle vorhanden, und im Intrapact noch nicht vorhanden sind), die aber keine Rückkehrer sind, angelegt. Dazu werden sie in die Tabellen „kractor" und „kruser" eingetragen. Die Zuordnung zu den Gruppen erfolgt erst zu einem späteren Zeitpunkt.

8. Im Schritt 8 werden alle Gruppen, die nicht mehr aus dem AD im Import vorhanden sind, aber im Intrapact noch mit einer Replikations-ID bestehen, sozusagen vom AD abgehängt. Das heißt, diese Gruppen werden nicht gelöscht, sondern es wird nur die Replikations-ID in der Tabelle „krusergroup", und das „bimported" Feld in der Tabelle „krgroupusers" geleert. Dadurch verhält sich diese Gruppe ab jetzt wie eine manuell im Intrapact angelegte Gruppe und die Zuordnungen gehen nicht verloren.

9. Im Schritt 9 wird überprüft, ob es Gruppen gibt, die im Import vorhanden sind, aber im Intrapact als manuell angelegte Gruppen vorhanden sind (eventuell irgendwann

zuvor einmal durch Punkt 8 entstanden und jetzt wieder vorhanden, also „Gruppen-Rückkehrer“). Bei diesen wird die Replikations-ID in der Tabelle „krusergroup“ wieder gefüllt, und das „bimported“ Feld in der Tabelle „krgroupusers“ wieder auf „1“ gesetzt. Dadurch ist es ab jetzt wieder eine AD-Gruppe.

10. Im Schritt 10 werden alle neu hinzukommenden Gruppen importiert. Eine Gruppen-Änderung gibt es nicht, da der Gruppenname gleichzeitig das Schlüsselfeld ist, ist eine Namensänderung der Gruppe gleichzeitig eine Löschung der alten gruppe und eine Neuanlage der neuen Gruppe.

11. Im Schritt 11 werden alle Personen-/Gruppenbeziehungen, die noch nicht im Intrapact vorhanden sind, in die Tabelle „krgroupusers“ eingefügt.

12. Im Schritt 12 werden, falls in den „kradsettings“ festgelegt, alle Personen zur Intrapact-Internen Gruppe „Benutzer“ (lid = 4), und alle Personen aus der in den „kradsettings“ definierten Administratorengruppe in die Intrapact interne Gruppe „Administratoren“ (lid = 3) hinzugefügt.

13. Im Schritt 13 werden, falls in den „kradsettings“ ein AD-Feld für den Fotoimport definiert ist, die Mitarbeiterfotos in die Tabelle „kruserpic“ importiert. Dazu muss es im Basisordner (<Laufwerk>:\Intrapact\org\<Firmenname>) der jeweiligen Intrapactfirma im Ordner „tasks“ das Powershell-Skript „ps_ADPhotoExport.ps1“ geben. Dieses exportiert alle Fotos aus dem AD in den Ordner „tasks\tmpstorage“, wobei der Dateiname gleich dem Loginnamen der Person ist. Für alle im Intrapact vorhandenen Personen wird dann überprüft, ob ein Foto vorhanden ist, und wenn ja, wird es in die Tabelle „kruserpic“ importiert. Dabei werden keinerlei Anpassungen an den Fotos gemacht. Es obliegt dem Systemadministrator im AD richtig dimensionierte Fotos zu hinterlegen.

7.3 Ablauf des 3. Abschnitts

Zum Abschluss wird überprüft, ob in den „kradsettings“ eine E-Mail Adresse hinterlegt ist, an die ein LOG des Imports gemailt werden soll. Ist diese vorhanden, wird bei einer SQL Server Express Edition ein einfacher Text, und bei einer SQL Server Vollversion ein Text mit dem Inhalt der LOG-Tabelle im csv-Format als Anhang versendet.

Um die Mailfunktion nutzen zu können, muss am SQL Server die Datenbank-Mailfunktion aktiviert sein. Diese muss von einem SQL Server Administrator installiert und aktiviert werden.

Danach müssen die benötigten Parameter in der Tabelle „kradsettings“ eingetragen werden.