daccord

Dokumentation

daccord Active Directory Connector

g+h systems

Ihr Kontakt

G+H Systems GmbH
Professionell, effizient und zuverlässig.

Ludwigstraße 8
63067 Offenbach am Main
Deutschland

Telefon: +49 (0) 69 85 00 02 -0
Fax: +49 (0) 69 85 00 02 -51
Email: info@guh-systems.de
Web: www.guh-systems.de

Versionsnachweis

Dieses Dokument wird von der G+H Systems GmbH gepflegt und fortlaufend aktualisiert. Größere Änderungen an Inhalt und Umfang führen zu einer neuen Versionsnummer. Die folgende Liste gibt die Historie dieses Dokumentes wieder.

Version	Datum	Author	Änderungsgrund
1.0	24.04.2014	Leitz, Rene	Initialversion
1.0	19.02.2016	Leitz, René	Finale Version

Rechtliche Hinweise

Die G+H Systems GmbH leistet keinerlei Gewähr bezüglich des Inhaltes oder Gebrauchs dieser Dokumentation. Insbesondere werden keine ausdrücklichen oder stillschweigenden Gewährleistungen hinsichtlich der handelsüblichen Qualität oder Eignung für einen bestimmten Zweck übernommen. Die G+H Systems GmbH behält sich weiterhin das Recht vor, diese Dokumentation zu revidieren und ihren Inhalt jederzeit und ohne vorherige Ankündigung zu ändern.

Des Weiteren übernimmt die G+H Systems GmbH für Software keinerlei Haftung und schließt insbesondere jegliche ausdrücklichen oder impliziten Gewährleistungsansprüche bezüglich der Marktfähigkeit oder der Eignung für einen bestimmten Zweck aus. Außerdem behält sich die G+H Systems GmbH das Recht vor, G+H Software ganz oder teilweise jederzeit inhaltlich zu ändern, ohne dass für die G+H Systems GmbH die Verpflichtung entsteht, Personen oder Organisationen von diesen Überarbeitungen oder Änderungen in Kenntnis zu setzen.

Inhaltsverzeichnis

1 Einleitung

Zur zentralen Ablage und dem performanten Zugriff auf Benutzerdaten und Berechtigungen werden in vielen IT Umgebungen Active Directory Systeme verwendet. Heutzutage bieten viele Anwendungen die Möglichkeit der Integration in ein Active Directory und erlauben damit eine zentrale Administration und Kontrolle dieser Informationen über verschiedenste Anwendungen hinweg.

Der daccord Active Directory Connector bietet über das Lightweight Directory Access Protocol (LDAP) die Möglichkeit zum flexiblen Zugriff auf die hinterlegten Informationen.

Das Lightweight Directory Access Protocol (LDAP) ist ein standardisiertes Zugriffsprotokol. Welche Informationen im Active Directory gespeichert werden, sind im sogenannten „Schema" festgelegt. Dieses kann erweitert werden.

Der daccord Active Directory Connector bietet die Möglichkeit beliebige LDAP-Suchanfragen zu definieren und unterstützt dadurch verschiedene Schematas zum Import der Daten in das daccord System. Dort können die Informationen ausgewertet, aufbereitet und transparent gemacht werden.

Mehr über das Active Directory erfahren Sie hier:
http://de.wikipedia.org/wiki/Active_Directory

Mehr über LDAP erfahren Sie hier:
http://de.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol

Mehr zum daccord System erfahren Sie hier:
http://www.daccord.de/

2 Funktionalität

Der daccord Active Directory Connector ist ein spezieller Connector zum Zugang auf Microsoft Active Directories über LDAP.

Der daccord Active Directory Connector bietet folgende Möglichkeiten zur Auswertung:

- Unterstützung für „Persons" (natürliche Personen), „User" (Benutzerkonten), „Rights" (Berechtigungen) und „Relations" (Berechtigungszuweisungen).
- Unterstützung für „Right Manager" (Berechtigungsverantwortliche) und „Person Manager" (Personenverantwortliche).
- Auswertung von Gruppen in Gruppenmitgliedschaften.
- Maximale Flexibilität durch die Unterstützung beliebiger LDAP-Suchanfragen.
- Unterstützung für verschlüsselte Verbindungen.
- Konvertierung der Daten über XSL-Transformationsdateien.
- Reduzierung der Daten um doppelte Einträge.
- Zusammenführung von Daten zur Unterstützung komplexer Strukturen.

3 Arbeitsweise

Beim Importieren der Informationen aus dem Verzeichnisdienst unterteilt sich die Funktionsweise des daccord Active Directory Connectors in fünf generelle Phasen. Die Festlegung der Funktionsweise des daccord Active Directory Connectors wird über die Konfiguration eines Collectors festgelegt. Dabei wird auch bestimmt welche der nachfolgenden Phasen durchlaufen werden sollen. Die Konfiguration des Collectors kann unter Punkt 5.3 „Einrichten eines neuen Collectors" nachgelesen werden.

3.1 Import der „User" (Benutzerkonten) und Erzeugung von „Persons" (natürliche Personen)

In dieser Phase wird die konfigurierte LDAP-Suchanfrage zum Holen aller „User" (Benutzerkonten) aus dem Verzeichnisdienst ausgeführt, die Daten ausgewertet und in das daccord System eingelesen. Je nach Konfiguration des Collectors werden die Daten konvertiert und daccord Feldern zugeordnet, um dem übergeordneten daccord-Schema zu entsprechen. Ebenfalls abhängig von der Konfiguration des Collectors können innerhalb dieser Phase auch „Persons" (natürliche Personen) erstellt werden. Diese dienen innerhalb von daccord der Zuordnung mehrerer „User" (Benutzerkonten) zu einer „Person" (natürliche Person).

3.2 Import der „Person Manager" (Personenverantwortliche)

Innerhalb dieser Phase können auf Basis der Informationen aus der Phase 3.1 Zuweisungen verschiedener „Persons" (natürliche Personen) zueinander bis zu einer definierten Hierarchietiefe eingelesen werden.

3.3 Import der „Rights" (Berechtigungen)

Die LDAP-Suchanfrage zum Auslesen aller „Rights" (Berechtigungen) wird innerhalb dieser Phase ausgeführt und die „Rights" aus dem Verzeichnisdienst in das daccord System eingelesen. Je nach Konfiguration des Collectors werden die Daten konvertiert und daccord Feldern zugeordnet, um dem übergeordneten daccord-Schema zu entsprechen.

3.4 Import der „Right Manager" (Berechtigungsverantwortliche)

Auf Basis der Informationen aus der Phase 3.3 können innerhalb dieser Phase Zuweisungen von „Rights" (Berechtigungen) zu „Right Manager" (Berechtigungsverantwortlicher) eingelesen werden.

3.5 Import der „Relations" (Berechtigungszuweisungen)

Über die LDAP-Suchanfrage zum Auslesen der „Relations" (Berechtigungszuweisungen) werden die „Relations" in das daccord System eingelesen. Gruppen in Gruppenmitgliedschaften werden in dieser Phase ausgewertet und ebenfalls in das daccord System eingelesen. Innerhalb dieser Phase ist es über die Konsolidierungsfunktion möglich auch komplexere Strukturen zu verarbeiten. Zusätzlich ist es über die Lieferung bestimmter Informationen und Einhaltung bestimmter XML Strukturen möglich, direkte oder indirekte „Relations" auszuweisen.

4 Voraussetzungen und Vorbereitung

Um den Connector einzurichten, muss die Software über das Kundencenter auf der daccord Website heruntergeladen werden. Um die Daten aus den Microsoft Active Directories auslesen zu können, wird ein Benutzerkonto mit einem Passwort benötigt, das lesenden Zugriff auf die Informationen hat. Des Weiteren muss der Connector das Microsoft Active Directory über eine Netzwerkverbindung erreichen können.

Folgende Schritte sind notwendig um den Connector für die Installation vorzubereiten:

4.1 Herunterladen der daccord Active Directory Connector Software

1. Laden Sie die ZIP-Datei aus dem Kundencenter der daccord Website > Kundencenter > Downloads herunter. Die notwendigen Zugangsdaten erhalten Sie von Ihrem Vertriebskontakt.
2. Entpacken Sie nun die ZIP-Datei auf einer Arbeitsstation.
3. Lokalisieren Sie das daccord Connector Installationsarchiv mit der Dateiendung .DCA.

5 Installation und Konfiguration

Die Abfolge der Installation und Konfiguration ist in folgende Schritte gegliedert:

1. Installation des daccord Active Directory Connectors.
2. Einfügen eines neuen Systems.
3. Einrichten eines neuen Collectors.
4. Konfigurieren des Mappings.
5. Konfigurieren des Convertings.
6. Verwalten des Usermatchings.

5.1 Installation des Connectors

Zunächst muss der daccord Active Directory Connector installiert werden. Dazu folgen Sie bitte den nachfolgenden Schritten:

1. Öffnen Sie das Admin Frontend mit Ihrem Benutzerkonto und Passwort.
2. Wählen Sie Engines > Collector Engines.
3. Markieren Sie eine Engine. Weitere Schaltflächen werden eingeblendet.
4. Wählen Sie die Schaltfläche „Connectors". Die Liste der Connectoren wird angezeigt.
5. Klicken Sie auf „Connector installieren".

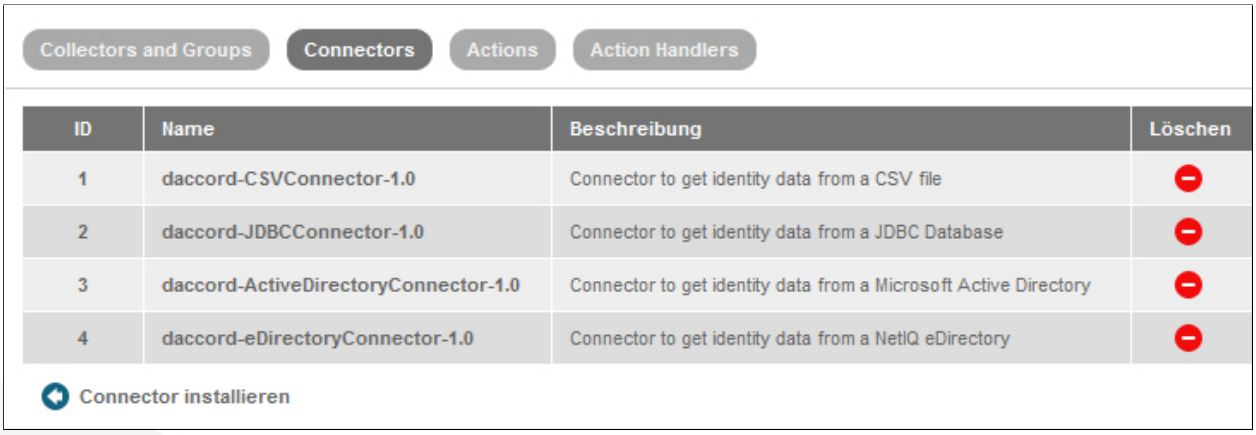

Abbildung 1: Connector installieren

5.2 Einfügen eines „Systems"

Die Daten aus dem Active Directory werden über den daccord Active Directory Connector in das zentrale daccord System übertragen. Dazu muss innerhalb von daccord zunächst ein „System" angelegt werden, welches später das Active Directory System in den Auswertungen repräsentiert. Um das „System" anzulegen, führen sie bitte folgende Schritte aus:

1. Wählen Sie im Reiter „Systemkonfiguration" die Schaltfläche „Systeme"
2. Klicken Sie auf „System hinzufügen"

Abbildung 2: System hinzufügen

3. Legen Sie das neue System mit den folgenden Parametern an:

Parameter	Beschreibung
Name	Vergeben Sie hier einen eindeutigen Namen für dieses System, z.B. „Active Directory". ***Hinweis:*** *Der definierte Name kann jederzeit geändert werden.*
Beschreibung	Vergeben Sie hier eine Beschreibung des Systems.
Request-System-ID	Bestimmt die Zuordnungs-ID des Systems zu einem externen Antragssystem.

Tabelle 1: Konfiguration eines Systems

5.3 Einrichten eines neuen Collectors im Admin Frontend

Jedes an daccord angeschlossene Zielsystem benötigt mindestens einen Collector, der wie folgt eingerichtet wird:

1. Wählen Sie Engines > Collector Engines.

2. Klicken Sie auf die Schaltfläche „Collectors and Groups".

3. Optional kann zur besseren Übersicht eine Collector Group, z.B. Active Directory Collectors angelegt werden. Dies macht insbesondere Sinn, wenn mehrere Active Directory Systeme an daccord angeschlossen werden sollen:

   a. Klicken Sie dazu in der Zeile „Alle Collectoren" und der Spalte „Aktionen" auf den grünen Kreis mit dem Plus-Zeichen „Collector Group hinzufügen".

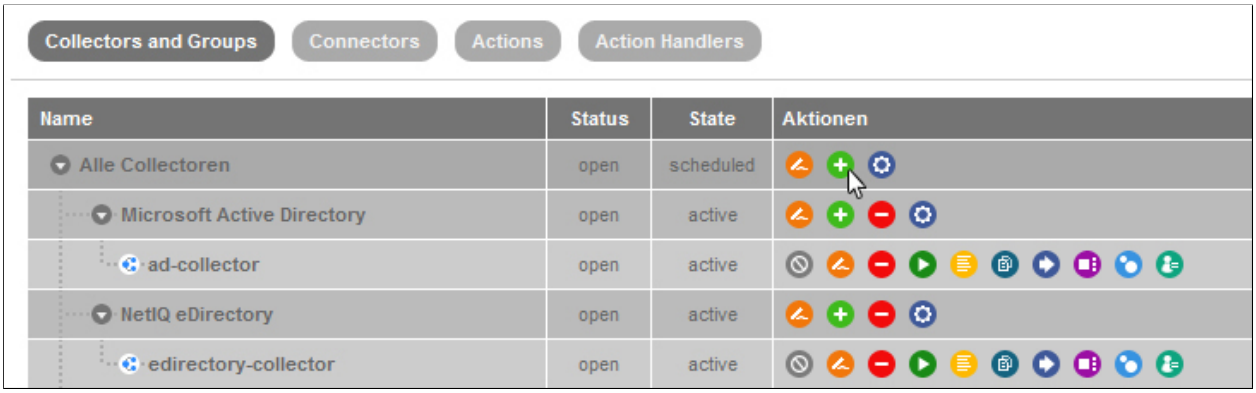

Abbildung 3: Collector Group hinzufügen

   b. Es öffnet sich ein Fenster, in dem Sie der Collector Group einen Namen und eine Beschreibung hinzufügen können, z.B. „Microsoft Active Directory".

4. Klicken Sie in der Zeile „Alle Collectoren" (bzw. alternativ in der Zeile der entsprechenden Collector Group, die Sie unter Punkt 5.4.3 eingerichtet haben und der Spalte „Aktionen" auf den blauen Kreis mit dem Zahnrad-Symbol „Collector verwalten".

5. Es öffnet sich ein Dialog. Klicken Sie hier bitte auf „Collector hinzufügen".

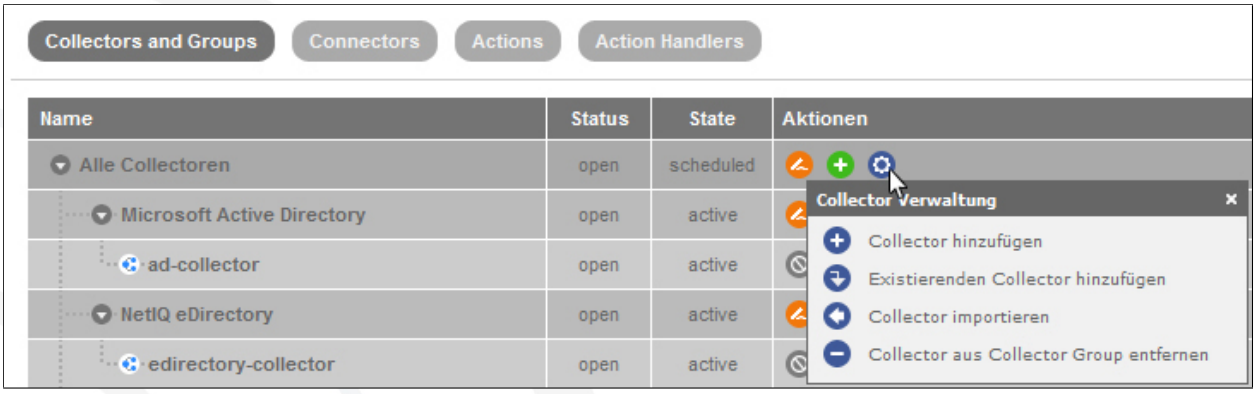

Abbildung 4: Collector hinzufügen

6. Konfigurieren Sie den Collector mit folgenden Parametern:

Parameter	Beschreibung
Name	Vergeben Sie hier einen eindeutigen Namen für diesen Collector, z.B. „Active Directory Collector". ***Hinweis:*** *Der definierte Name kann nachträglich nicht geändert werden.*
System	Wählen Sie hier das unter Punkt 5.2. „Einfügen eines Systems" angelegte System aus.
Zeitsteuerung	Geben Sie hier die zeitliche Steuerung des Collectors im CRON-basiertem Format an.
Log Level	Geben Sie hier den Detailierungsgrad der Ausgaben in den Logdateien an.
Status	Wählen Sie hier den Ausführungszustand des Collectors aus. ***Hinweis:*** *Ein Collector im Status deaktiviert wird nicht ausgeführt.*
Modus	Wählen Sie hier den Verarbeitungsmodus des Collectors aus. ***Hinweis:*** *Collectoren im Mode „Entwicklung" dienen zur Vorbereitung und führen keine Datenbankveränderungen durch.*
„User"-Knoten	Geben Sie hier die Bezeichnung für den XML-Knoten an, welcher zur eindeutigen Identifizierung eines Benutzerdatensatzes dient.
„Right"-Knoten	Geben Sie hier die Bezeichnung für den XML-Knoten an, welcher zur eindeutigen Identifizierung eines Rechtedatensatzes dient.
Schwellenwert (Add)	Wählen Sie hier einen prozentualen Wert an ADD Operationen aus, die als gültig akzeptiert werden. ***Hinweis:*** *Wird dieser Wert überschritten, wird von einer fehlerhaften Lieferung ausgegangen und keine Verarbeitung durchgeführt.*
Schwellenwert (Delete)	Wählen Sie hier einen prozentualen Wert an DELETE Operationen aus, die als gültig akzeptiert werden. ***Hinweis:*** *Wird dieser Wert überschritten, wird von einer fehlerhaften Lieferung ausgegangen und keine Verarbeitung durchgeführt.*

Parameter	Beschreibung
„User" Verarbeitung	Bestimmt, ob der Collector „User" (Benutzerkonto) verarbeitet. ***Hinweis:*** *Wenn Sie „Ja, nur ergänzend" wählen, werden keine neuen „User" (Benutzerkonten) erstellt, sondern nur Informationen zu vorhandenen „User" hinzugefügt.*
„Persons" Verarbeitung	Bestimmt, ob der Collector „Persons" (natürliche Personen) verarbeitet. ***Hinweis:*** *Wenn Sie „Ja, nur ergänzend" wählen, werden keine neuen „Persons" (natürliche Personen) erstellt, sondern nur Informationen zu vorhandenen „Persons" hinzugefügt.*
„Rights" Verarbeitung	Bestimmt, ob der Collector „Rights" (Berechtigungen) verarbeitet. ***Hinweis:*** *Wenn Sie „Ja, nur ergänzend" wählen, werden keine neuen „Rights" (Berechtigungen) erstellt, sondern nur Informationen zu vorhandenen „Rights"hinzugefügt.*
„Relations" Verarbeitung	Bestimmt, ob der Collector „Relations" (Berechtigungszuweisungen) verarbeitet. ***Hinweis:*** *Wenn Sie „Ja, nur ergänzend" wählen, werden keine neuen „Relations" (Berechtigungszuweisungen) erstellt, sondern nur Informationen zu vorhandenen „Relations"hinzugefügt.*
„Person Manager" Verarbeitung	Bestimmt, ob der Collector „Person Manager" (Personenverantwortliche) verarbeitet. ***Hinweis:*** *Wenn Sie „Ja, nur ergänzend" wählen, werden keine neuen „Person Manager"-Zuweisungen erstellt, sondern nur Informationen zu vorhandenen „Person Manager"-Zuweisungen hinzugefügt.*
„Right Manager" Verarbeitung	Bestimmt, ob der Collector „Right Manager" (Berechtigungsverantwortlicher) verarbeitet. ***Hinweis:*** *Wenn Sie „Ja, nur ergänzend" wählen, werden keine neuen „Right Manager"-Zuweisungen erstellt, sondern nur Informationen zu vorhandenen „Right Manager"-Zuweisungen hinzugefügt.*
Historien Speicherung	Bestimmt, ob der Collector eine Historie der Veränderungen in der Datenbank ablegt. ***Hinweis:*** *Wenn Sie „Ja, nur die Änderungen" wählen, werden nur die Informationen zu den geänderten Datenfeldern festgehalten.*

Parameter	Beschreibung
„User" Neuzuordnung	Bestimmt, ob durch diesen Collector eine erneute Zuordnung von „Users" zu natürlichen Personen durchgeführt werden soll. ***Hinweis:*** *Wenn Sie „Ja, nur nicht zugeordnete User" wählen, wird versucht, für diejenigen „User", die keiner natürlichen Person zugeordnet werden konnten erneut eine Zuordnung herzustellen.Wenn Sie „Ja, alle User" wählen, wird für alle „User" eine erneute Zuordnung versucht.*
Connector	Wählen Sie hier den Namen des Connectors aus, den Sie unter Punkt 5.1 "Installation des Connectors" definiert haben.
Connector-Modus	Wählen Sie hier den Kommunikationsmodus des Collectors. ***Hinweis:*** *Im indirekten Modus wird ein Polling-Verfahren zur Entgegennahme der Antwort eingesetzt. Im direkten Modus wird von dem Connector die Antwort direkt erwartet.*
Connector-Anfragen	Wählen Sie hier die maximale Anzahl an Versuchen aus, um die Daten im Polling-Verfahren vom Connector zu erfragen. ***Hinweis:*** *Diese Information wird nur benötigt, wenn Sie als Connector-Modus den „indirekten Kommunikationsmodus" gewählt haben.*
Connector-Wartezeit	Wählen Sie hier die Wartezeit in Sekunden zwischen den Anfrageversuchen im Polling-Verfahren aus. ***Hinweis:*** *Diese Information wird nur benötigt, wenn Sie als Connector-Modus den „indirekten Kommunikationsmodus" gewählt haben.*
LDAP Host	Geben Sie hier die IP Adresse oder den DNS-Namen des Microsoft Active Directory Servers an. (z.B. ldap.mydomain.de).
Sichere Verbindung	Wählen Sie aus, ob die Verbindung über einer sichere Verbindung (SSL) hergestellt werden soll.
Schlüsselspeicherdatei	Wählen Sie die Java Schlüsselspeicherdatei für die SSL-Verbindung aus. Diese Datei muss über die „Collector Datei Verwaltung" hochgeladen worden sein. ***Hinweis:*** *Diese Information wird nur benötigt, wenn eine sichere Verbindung hergestellt werden soll.*
LDAP Port	Geben Sie hier den Kommunikationsport des Microsoft Active Directory Servers an. (z.B. „389" oder „636").
Verzeichnisdienstbenutzer	Geben Sie hier den Benutzer zur Anmeldung am Microsoft Active Directory an. (z.B. „CN=user,dc=company,dc=local").

Parameter	Beschreibung
Verzeichnisdienstpasswort	Geben Sie hier das Passwort des Microsof Active Directory Benutzers an.
Zeitüberschreitung	Wählen Sie den Wert für die Zeitüberschreitung der Verbindung in Millisekunden aus.
Anzahl der Ergebnisse pro Seite	Geben Sie hier an wieviele Datensätze bei einer LDAP-Abfrage pro Ergebnisseite geliefert werden. ***Hinweis:*** *(Der maximale Wert ist 1000 Datensätze.)*
LDAP Basis DN	Geben Sie hier den Einstiegspunkt der LDAP-Suche zur Abfrage der jeweiligen Daten an. (z.B. „OU=users,DC=company,DC=DE"). ***Hinweis:*** *(Gültig für „User", „Rights" und „Relations".)*
LDAP Filter	Geben Sie hier den LDAP-Suchfilter zur Abfrage der jeweiligen Daten an. (z.B. „(objectClass = Person)"). ***Hinweis:*** *(Gültig für „User", „Rights" und „Relations".)*
LDAP Suchbereich	Wählen Sie hier den Bereich der Suche ab der LDAP Basis DN aus. ***Hinweis:*** *(Gültig für „User", „Rights" und „Relations".)*
LDAP Attribute	Geben Sie hier eine kommagertrennte Liste an auszulesenden LDAP-Attributen an. (z.B. "cn,sn,givenname"). ***Hinweis:*** *(Gültig für „User", „Rights" und „Relations".)*
Konvertierungsdatei	Wählen Sie hier die XSL-Datei zur Konvertierung der Daten aus. Diese Datei muss über die "Collector Datei Verwaltung"hochgeladen worden sein. ***Hinweis:*** *(Gültig für „User", „Rights" und „Relations".)*
Duplikatsprüfung	Wählen Sie hier „Ja" aus, wenn die einzulesenden Daten doppelte Einträge enthalten, welche entfernt werden müssen. ***Hinweis:*** *(Gültig für „User", „Rights" und „Relations".)*

Parameter	Beschreibung
Zuordnungsursprung	Wählen Sie aus, über welches Objekt die Benutzer-Rechte-Beziehungen ausgelesen werden soll. (z.B. Gruppenmitgliedschaft aus dem Gruppenobjekt). ***Hinweis:*** *(Gültig für „Relations".)*

Tabelle 2: Konfiguration eines Collectors

5.4 Mapping Konfiguration

Um die ausgelesenen Daten in die richtigen Datenbankfelder der daccord Datenbank zu übertragen, müssen die Felder miteinander verknüpft werden, also das so genannte Mapping für „User" (Benutzerkonten) und „Rights" (Berechtigungen) durchgeführt werden.

Klicken Sie in der Zeile des Collectors auf den lilafarbenen Kreis, „Mappings". Wählen Sie nun, ob Sie die Mappings für „User" (Benutzerkonten) oder „Rights" (Berechtigungen) administrieren wollen.

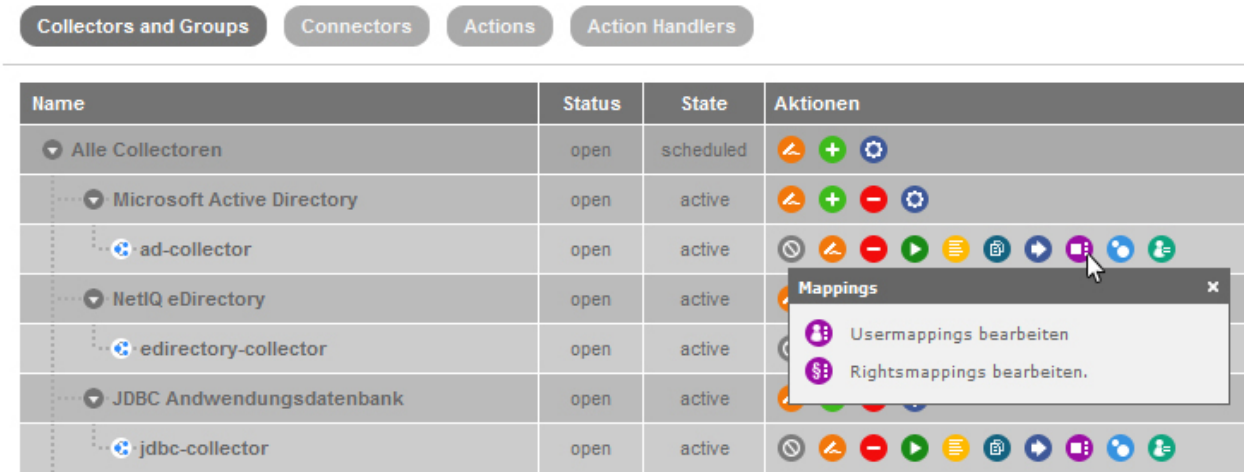

Abbildung 5: Mapping konfigurieren

Die Konfiguration des Mapping ist eine allgemeine Konfigurationstätigkeit für Connectoren und ist in der daccord Systemdokumentation erläutert.

5.5 Converting Konfiguration

Um die ausgelesenen Daten in ein geeignetes, auswertbares Format zu bringen, können diese vor dem Import über sogenannte „Scripts" in das geeignete Format konvertiert werden. Um vorhandene „Scripts" zu bearbeiten oder neue „Scripts" zu erstellen wählen Sie im Reiter „Systemkonfiguration" die Schaltfläche „Scripts".

Um das Converting zu konfigurieren, klicken Sie in der Zeile des Collectors auf den hellblauen Kreis, „Convertings". Wählen Sie nun, ob Sie die Convertings für „User" (Benutzerkonten) oder „Rights" (Berechtigungen) administrieren wollen.

Die Konfiguration des Converting ist eine allgemeine Konfigurationstätigkeit für Connectoren und ist in der daccord Systemdokumentation erläutert.

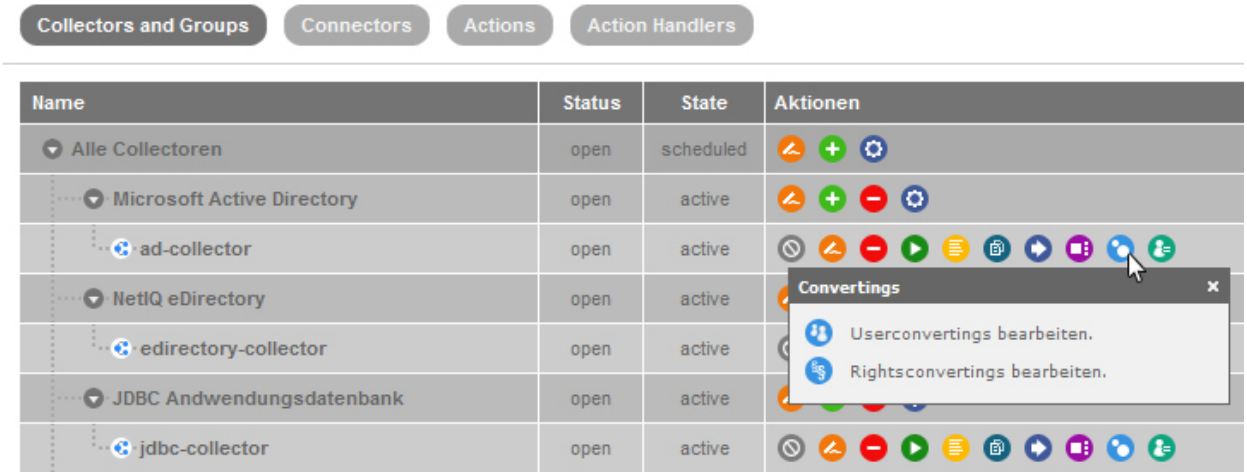

Abbildung 6: Converting konfigurieren

5.6 Usermatching Verwaltung

Die Konfiguration einer Matching Regel für die Zuweisung der „User" (Benutzerkonten) zu einer „Person" (natürliche Person) können Sie unter Beachtung der folgenden Schritte durchführen:

Klicken Sie in der Zeile des Collectors auf den blau-grünen Kreis mit dem Benutzersymbol, „Usermatchings".

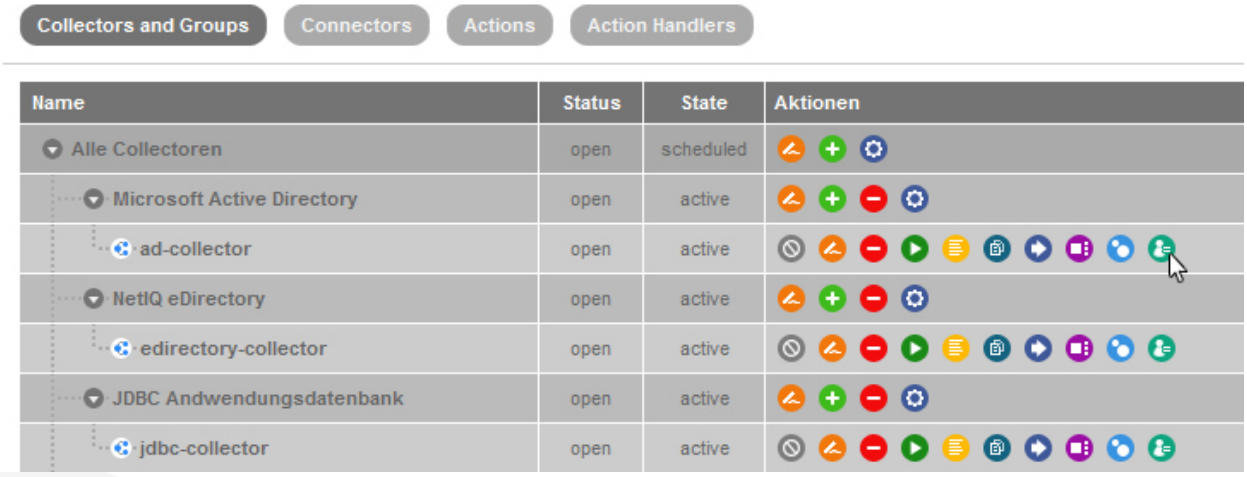

Abbildung 7: Usermatching verwalten

Die Konfiguration des Usermatching ist eine allgemeine Konfigurationstätigkeit für Connectoren und ist in der daccord Systemdokumentation erläutert.

6 Erweiterte Konfiguration

6.1 Import von „Person Manager" (Personenverantwortliche)

Über den daccord Active Directory Connector ist es möglich Zuordnungen zwischen verschiedenen „Persons" (natürliche Personen) automatisiert aus Microsoft Active Directories auszulesen und im daccord System zu hinterlegen. „Person Manager" (Personenverantwortlicher) haben anschließend die Möglichkeit über das User Frontend die „User" (Benutzerkonten) und „Rights" (Berechtigungen) der ihnen zugewiesenen „Persons" einzusehen und zu kontrollieren. Diese Funktion wird häufig zur Abbildung der Vorgesetztenstruktur verwendet.
Um diesen Import zu ermöglichen, ist die Lieferung bestimmter Informationen und Einhaltung vorgegebener XML-Strukturen notwendig. Folgende Punkte sind dabei zu beachten:

1. Die Zuordnung wird nur nach einem erfolgreichen „User"-Import durchgeführt.
2. Der Collector muss hinsichtlich der Verarbeitung von „Person Manager" (Personenverantwortliche) konfiguriert sein.
3. Der Collector verarbeitet alle Datensätze, die einen Knoten „managerid" beinhalten.
4. Der Inhalt des Knotens „userid" innerhalb des gefundenen Datensatzes wird verwendet um den relevanten „User" und dessen zugeordnete „Person" zu finden.
5. Der Inhalt des Knotens „managerid" innerhalb des gefundenen Datensatzen wird verwendet, um den verantwortlichen „User" und dessen zugeordnete „Person" zu finden.
6. Sollte es sich nicht um die selbe „Person" handeln, wird die Zuordnung hergestellt.

Hinweis: *Sollte der jeweilige Verzeichnisdienst die Informationen nicht im benötigten Format liefern, dann können die Daten über eine XSL-Transformationsdatei umgewandelt werden.*

6.2 Import von „Right Manager" (Berechtigungsverantwortliche)

Über den daccord Active Directory Connector ist es möglich Zuordnungen von „Persons" (natürliche Personen) zu „Rights" (Berechtigungen) automatisiert aus Active Directory Systemen auszulesen und im daccord System zu hinterlegen. „Right Manager" (Berechtigungsverantwortlicher) haben anschließend die Möglichkeit über das User Frontend die ihnen zugeordneten „Rights" und diejenigen „User" (Benutzerkonten), die diese „Rights" besitzen, einzusehen und zu kontrollieren.
Um diesen Import zu ermöglichen, ist die Lieferung bestimmter Informationen und Einhaltung vorgegebener XML-Strukturen notwendig. Folgende Punkte sind dabei zu beachten:

1. Die Zuordnung wird nur nach einem erfolgreichen „Rights"-Import durchgeführt.
2. Der Collector muss hinsichtlich der Verarbeitung von „Right Manager" (Berechtigungsverantwortlicher) konfiguriert sein.
3. Der Collector verarbeitet alle Datensätze, die einen Knoten „managerid" beinhalten.
4. Der Inhalt des Knotens „rightid" innerhalb des gefundenen Datensatzes wird verwendet um das relevante „Right" zu finden.
5. Der Inhalt des Knotens „managerid" innerhalb des gefundenen Datensatzen wird verwendet um den verantwortlichen „User" und dessen zugeordnete „Person" (natürliche Person) zu finden und die Zuordnung herzustellen.

Hinweis: *Sollte der jeweilige Verzeichnisdienst die Informationen nicht im benötigten Format liefern, dann können die Daten über eine XSL-Transformationsdatei umgewandelt werden.*

6.3 Einrichten einer verschlüsselten Verbindung

Es besteht die Möglichkeit die Kommunikation des daccord Active Directory Connectors zum Microsoft Active Directory über eine verschlüsselte Verbindung abzusichern. Diese Konfiguration verhindert das Auslesen von sensiblen Informationen während der Kommunikation.

Um die verschlüsselte Verbindung zu ermöglichen, gehen Sie bitte folgendermaßen vor:

1. Stellen Sie den Parameter „Sichere Verbindung" in der Collector Konfiguration auf „Ja" ein.

2. Stellen Sie den Parameter „LDAP Port" in der Collectorkonfiguration auf den verschlüsselten Port des Active Directory Systems ein.

3. Exportieren Sie den „Public Key" des Microsoft Active Directory Servers in ein Java Schlüsselspeicherdatei. ***Hinweis:*** *Innerhalb des heruntergeladenen Installationspaketes befindet sich eine Java Anwendung „exportCertificates" zum Export von Zertifikaten in einen Java Schlüsselspeicher. Lesen Sie dazu bitte die Anweisungen in der zugehörigen Readme-Datei.*

4. Fügen Sie die erzeugte Schlüsselspeicherdatei über die „Collector Datei Verwaltung" dem Collector als Ressourcen-Datei hinzu.

5. Wählen Sie beim Parameter „Schlüsselspeicherdatei" in der Collectorkonfiguration die Datei aus.

7 Inbetriebnahme

Als erste Initialbefüllung werden alle Daten ohne Differenzbildung aus dem Active Directory System ausgelesen und in die daccord Datenbank übertragen. Gehen Sie wie folgt vor, um den Collector zur Initialbefüllung zu starten:

1. Klicken Sie in der Zeile des Collectors auf den grünen Kreis mit dem Start-Symbol „Collector ausführen".
2. Es öffnet sich ein Dialog. Wählen Sie bitte „Collector INITIAL starten".

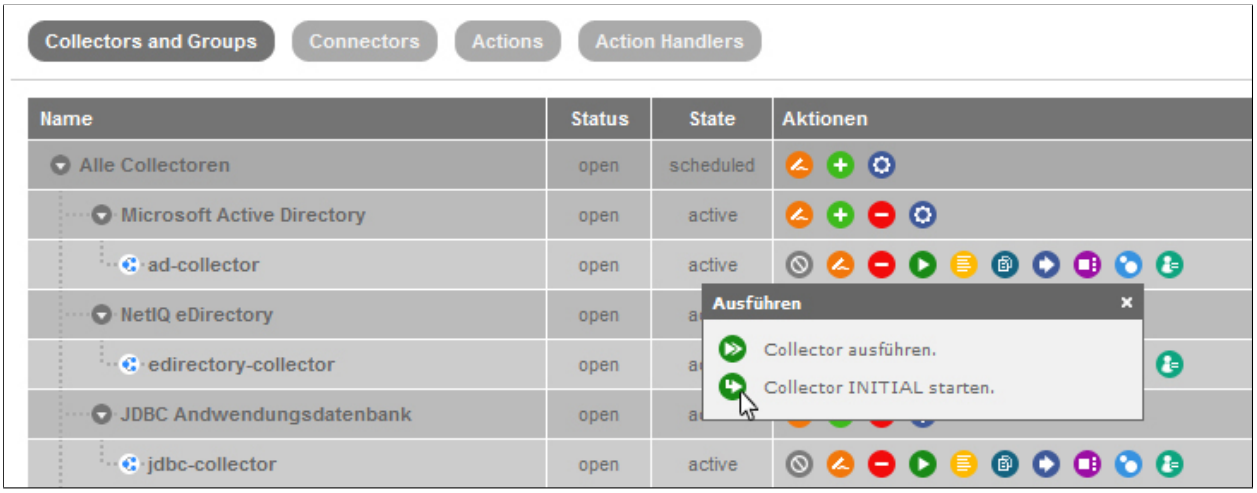

Abbildung 8: Collectorlauf initial ausführen

8 Dauerbetrieb

Über den Scheduler (siehe Punkt 5.4 Einrichten eines neuen Collectors) kann eingestellt werden, zu welchen Zeiten der Collector automatisch laufen soll. Sie können den Abgleich jedoch auch manuell anstoßen:

1. Klicken Sie dazu in der Zeile des Collectors auf den grünen Kreis mit dem Start-Symbol „Collector ausführen".
2. Es öffnet sich ein Dialog. Wählen Sie bitte „Collector ausführen".

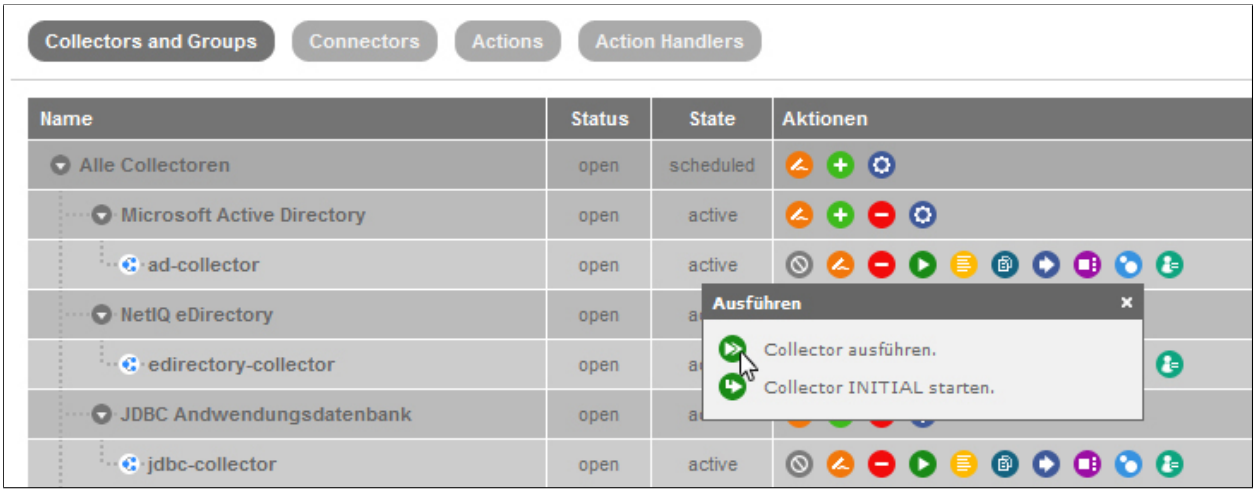

Abbildung 9: Collectorlauf manuell anstoßen

9 Glossar

Termini	Beschreibung
Microsoft Active Directory	Ein System zur zentralen Ablage von Benutzerinformationen. Das Microsoft Active Directory Schema bestimmt die Informationen, die in dem Microsoft Active Directory abgelegt werden können.
Lightweight Directory Access Protocol (LDAP)	Ein standardisiertes Zugriffsprotokoll um auf einen Verzeichnisdienst zuzugreifen und Informationen auszulesen oder zu verändern.
daccord	daccord ist eine Software, die Zugriffsberechtigungen sämtlicher Systeme (herstellerunabhängig) aus einer IT-Landschaft jederzeit transparent darstellen kann.
Rights Manager	Ein Collector kann in der Art konfiguriert werden, so dass er Zuordnungen zwischen Personen und Rechten importieren kann. Der so genannte Rights Manager kann im User Frontend die Rechteinhaber des ihm zugeordneten Rechtes einsehen und kontrollieren. Im Falle einer Abweichung vom Soll-Zustand kann der Rights Manager entsprechend des vorher festgelegten Workflows reagieren.
Person Manager	Ein Collector kann in der Art konfiguriert werden, so dass er Zuordnungen zwischen verschiedenen Personen importieren kann. Der so genannte Person Manager kann im User Frontend die User und Rechte der zugeordneteten Personen einsehen und kontrollieren. Im Falle einer Abweichung vom Soll-Zustand kann der Person Manager entsprechend des vorher festgelegten Workflows reagieren.
Connector	Ein Connector ist die daccord Komponente, welche die Daten innerhalb einer Datenbeschaffung über einen daccord Collector systemspezifisch aus dem jeweiligen System ausliest und dem daccord Collector aufbereitet zur Verfügung stellt.
Collector	Ein Collector (to collect = dt. sammeln) ist die daccord Komponente, die manuell oder zeitgesteuert über einen daccord Connector Daten aus Zielsystemen ausliest und in das daccord System importiert.
Mapping	Um die ausgelesenen Daten aus dem Verzeichnisdienst in die richtigen Datenbankfelder der daccord Datenbank zu übertragen, müssen die Felder miteinander verknüpft, also das so genannte Mapping Verfahrung durchgeführt werden.
Converting	Um die aus dem Verzeichnisdienst gelieferten Daten in ein für daccord geeignetes, auswertbares Format zu bringen, müssen sie zunächst konvertiert, also das so genannte Converting Verfahren durchgeführt werden.
Scripts	Die Scripts dienen dazu Daten in ein geeignetes Format zum Import in die daccord Datenbank zu konvertieren.

Termini	Beschreibung
Usermatching	Um die User aus einem angeschlossen Zielsystem mit einer natürlichen Person zu verknüpfen, müssen die User anhand einer individuellen Eigenschaft, wie Name, Geburtsdatum und/oder Personalnummer zugeordnet werden.
Collector Engine	Die Collector Engine ist die Umgebung in der Collectoren ausgeführt werden. Ein daccord System kann mehrere Collector Engines beinhalten. Ein Collector ist jeweils einer Collector Engine zugeordnet.
Collector Group	Die Anzahl an Collectoren ist individuell festlegbar und kann unter Umständen sehr hoch werden. Um eine höhere Anzahl an Collectoren im Admin Frontend sinnvoll und übersichtlich darzustellen, werden sie in den so genannten Collector Groups angelegt. Die Collectoren werden somit in logische Einheiten eingeteilt.
Scheduler	Der Scheduler (dt. Planer oder Steuerer) legt fest, wann der nächste Ist-/Soll-Abgleich bezüglich der Rechtestrukturen in den Systemen durchgeführt werden soll. Er kann entweder in einem beliebigen Zeitintervall konfiguriert werden (z.B. monatlich, wöchentlich, täglich) oder auch manuell angestoßen werden, um jederzeit eine Überprüfung der Systeme zu ermöglichen.
CRON	daccord verwendet intern eine Komponente zur zeitbasierten Ausführung von Prozessen. Die Konfiguration der Zeitsteuerung erfolgt über das allgemein bekannte CRON-Format.
Polling-Verfahren	Für Connectoren, bei denen eine längere Laufzeit zu erwarten ist, sollte der Collector im so genannten indirect Mode betrieben werden. Bei diesem Verfahren wird der Connector im ersten Schritt aufgefordert, die Daten beim jeweiligen System zu beschaffen. Anschließend wird zyklisch beim Connector angefragt, ob die Daten mittlerweile zur weiteren Verarbeitung zur Verfügung stehen. Über Parameter kann die Anzahl der Versuche, die Daten im indirect Mode zu holen, und die Wartezeit zwischen den Versuchen in Millisekunden, bestimmt werden.

Tabelle 3: Glossar

Abbildungsverzeichnis

Tabellenverzeichnis

G+H Systems GmbH

Ludwigstraße 8
63067 Offenbach am Main

Tel.: +49 (0) 69 85 00 02-0
Fax: +49 (0) 69 85 00 02-51

Email: info@guh-systems.de
Web: www.guh-systems.de