LDAP Konfiguration

Definition

Menüaufruf: (Administration) - (LDAP Konfiguration)

Bei einem LDAP handelt es sich um einen Verzeichnisdienst, d.h. eine spezielle Art einer hierarchischen Datenbank. Blätter sind einzelne Resourcen, die verwaltet werden sollen, wie z.B. Benutzer. Andere Knoten gruppieren diese Resourcen in verschiedene Kategorien (ähnlich wie Ordner in einem Dateisystem, allerdings können im LDAP auch diese Knoten weitergehende Informationen (z.B. Attribute) beinhalten). Es gibt Knoten (also auch Blätter), die einen 'Link' auf andere Knoten ermöglichen. Die LDAP Bezeichnung hierfür ist '*Referrals*'. Mittels *Referrals* ist es möglich, innerhalb eines LDAP mehrere unabhängige Resourcenhierarchien zu verwalten (obwohl die Knoten im LDAP logisch nur einen Baum bilden). So ist es z.B. möglich, die User nach Standorten zu strukturieren *und gleichzeitig* nach Funktion im Unternehmen.

Ein LDAP stellte eine *standardisierte API* für die *zentrale* Verwaltung von IT Resourcen bereit. Diese Verwaltung um fasst (auch) Autorisierung, Authentifizierung und Synchronisation. Microsofts *Active Directory* (oft AD abgekürzt) umfasst einen LDAP. Sollten Sie daher bereits AD zum Verwalten ihrer Benutzer verwenden, dann haben Sie bereits einen LDAP im Einsatz!

Über sogenannte LDAP Schemata sind die Attributsname der Resourcen (und die Art deren Werte und die Knotennamen und ...) ebenfalls standardisiert. Durch diese Standarisierung ist es oft einfach, weitere Softwaresysteme so zu konfigurieren, dass diese die Informationen aus dem LDAP verwenden.

Auch wenn innerhalb eines LDAPs vieles standardisiert ist, ist die *Verzeichnisstruktur* als ganzes frei wählbar. Dies ermöglicht einen sehr flexiblen Einsatz des LDAPs für ganz unterschiedliche Resourcen.

LDAP Abfragen

Als Verzeichnisdienst ermöglicht ein LDAP Abfragen nach Resourcen mittels einer speziellen Abfragesprache. Beispielsweise liefert folgende Abfrage alle User:

```
(|(objectClass=inetOrgPerson)(objectClass=user))
```

Die Abfragesprache ist ebenfalls standardisiert. Weitere Informationen zur Abfragesprache finden sich u.a. unter folgenden Links:

- LDAP Filter Syntax
- Famous Filters
- Search Filter Syntax
- LDAP Search Filter

LDAP Explorer

Da die Verzeichnisstruktur frei wählbar ist, ist es für die Anbindung an einen LDAP oft sehr hilfreich, sich einen Überblick für die Baumstruktur des *kon kreten* LDAPs zu verschaffen. Hierzu stehen diverse GUI Tools zu Verfügung. Diese Tools ermöglichen meist auch das Arbeiten mit LDAP Abfragen (s.o.).

- JXplorer (Java)
- Apache Directory Studio (Java, Eclipse RCP basiert)
- Microsoft Active Directory Explorer (Windows, AD)
- LDAP Admin (Windows)

Nuclos und LDAP

Nuclos kann einen LDAP z.Z. für eine (einfache) Synchronisation (LDAP -> Nuclos) und die Authentifizierung verwenden. Eine Verwendung des LDAP zur Autorisierung ist z.Z. nicht implementiert.

Nuclos und LDAP Synchronisation

Ist ein LDAP in Nuclos konfiguriert (s.u.), so enthält die *Benutzer Detail Ansicht* oben ein zusätzliches Icon 'Synchronisation'. Wird dieses Icon angeklickt, dann werden die LDAP Attribute gemäß der Konfiguration in den in Nuclos hinterlegten Benutzer übernommen.

> Die Synchronisation umfasst z.Z. (höchstens) die Felder *Vorname*, *Nachname* und *E-Mail-Adresse*. Diese Felder können aus beliebigen LDAP Attributen übernommen werden.
>
> Eine Synchronisation aller im LDAP hinterlegten Benutzer ist z.Z. *nicht* implementiert. Die einzelnen Benutzer müssen zunächst in Nuclos manuell angelegt werden!

Anlegen der Benutzer

Die Synchronisation legt z.Z. keine Nutzer an (und löscht auch keine Nutzer)! Die Nutzer müssen *manuell* angelegt werden - sie müssen den gleichen (Benutzer-)Namen bekommen wie die entsprechenden Nutzer im LDAP. Das Passwort kann beliebig gewählt werden. Wenn eine LDAP Konfiguration aktiv ist, werden die in Nuclos hinterlegten Passwörter (für 'normale' User) nicht verwendet, sondern es wird gegen den LDAP authentifiziert.

> Nutzer, die nicht im LDAP zu finden sind, können sich bei aktivierter LDAP Konfiguration nicht in Nuclos einloggen (Ausnahme: Superuser).

> Manuelles Anlegen eines Nutzer reicht allein nicht, damit sich der Nutzer in Nuclos einloggen kann. Der Nutzer muss zudem einer Benutzergruppe zugewiesen werden, die (mindestens) das Systemrecht 'Nuclos starten' hat.

Nuclos und LDAP Authentifizierung

Nutzer, deren Benutzername über den konfigurierten *Authentifizierungsfilter* im LDAP gefunden werden, werden gegen den LDAP authentifiziert, d.h. das in Nuclos hinterlegte Passwort wird *nicht* verwendet. Statt dessen wird geprüft, ob das gegebene Passwort mit dem im LDAP hinterlegten übereinstimmt.

> Nutzer, die *nicht* über den konfigurierten *Authentifizierungsfilter* im LDAP gefunden werden und die kein Superuser sind, können sich *nicht* in Nuclos einloggen, wenn eine LDAP Konfiguration aktiviert ist.

> Für Benutzer, die als *Superuser* in Nuclos hinterlegt sind, wird nach der Authentifizierung gegen den LDAP noch eine Authentifizierung gegen das in Nuclos hinterlegte Passwort versucht.
>
> Dies verhindert, dass sich Superuser nicht einloggen können, falls der LDAP nicht verfügbar bzw. falsch konfiguriert ist.

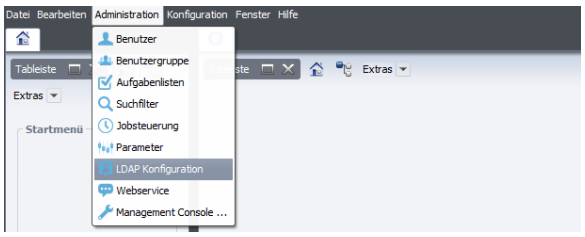
Test Authentifizierung

Die LDAP Konfigurationsseite enthält oben einen Button *Authentisierung testen*. Hier kann dann ein User/Passwort Kombination gegen den LDAP getestet werden.

Nuclos und LDAP Autorisierung

LDAP Autorisierung ist z.Z. nicht implementiert. Die Rechte der einzelnen Benutzer müssen innerhalb von Nuclos (z.B. mittels der Benutzergruppen) gepflegt werden.

Menüpunkt *LDAP Konfiguration*



Füllen Sie die benötigten Felder mit Ihren spezifischen Daten aus.

Beispiel für die Anbindung an ein Active Directory

blocked URL

> Bei der Suche nach der passenden Base DN oder der Manager DN kann das Tool AD Explorer von Microsoft eine gute Hilfestellung leisten.

Name	Beschreibung	Wert
Name	Name der LDAP Anbindung	Beispiel:yourdc
URL	LDAP Verbindungsstring mit IP-Adresse und Port	ldap://192.168.1.1:389
Base DN	Basis DN in der die Benutzerdaten liegen	DC=yourdomain,DC=de
Search Scope	Suchtiefe im LDAP Verzeichnis	SUBTREE
Manager DN	Benutzer der für den Zugriff auf das LDAP Verzeichnis benötigt wird. Legen Sie hierzu am besten einen eigenen Benutzer an. Der Benutzer kann in 2 verschiedenen Formaten angegeben werden. 1. domain\user 2. DN des Users	1. yourdomain\manager 2. CN=manager,OU=Users,DC=yourdomain,DC=de
Manager Passwort	Passwort des Manager Benutzers	Passwort
Filter (Authentifizierung)	Filter für Eingrenzung der Authentifizierung	(sAMAccountName={0})
Alternativer-Filter (Authentifizierung)	Filter für Eingrenzung der Authentifizierung auf eine Gruppe. Bedeutet Nur Benutzer einer bestimmten AD-Gruppen können sich anmelden.	(&(objectClass=user)(sAMAccountName={0})(memberof=CN=Gruppenname,OU=Users,DC=yourdomain,DC=de))
Filter (Synchronisation)	Filter für Eingrenzung der Synchronisierung	(objectClass=user)

> Die Zuordnung der Attribute ist zwingend notwendig

Nuclos Attribut	Beschreibung	LDAP Attribut
name	Benutzername	sAMAcountName
firstname	Vorname	givenName
lastname	Nachname	sn
email	E-Mail Adresse	mail