LDAP/AD - die richtigen Ports

LDAP-Port

Der UCS LDAP-Dienst ist über die Ports 7389 (ungesichert) und 7636 (TLS-gesichert) erreichbar. Der LDAP-Dienst hat unter UCS zwei fest zugewiesene Ports.

Port 7389 (ungesichert) + START TLS

Port 7636 (SSL-gesichert) –> LDAPS

Wenn Samba auf dem Server installiert und als AD kompatibler Domänencontroller konfiguriert ist, sind die Ports 389 (ungesichert) und 636 (TLS-gesichert) für Samba reserviert und können nicht mehr für die OpenLDAP-Kommunikation genutzt werden.Soll Ihr LDAP aber im Austausch mit dem Microsoft Active Directory stehen, so ist die Verwendung von Samba notwendig. Ist Samba auf dem Server installiert und als AD kompatibler Domänencontroller konfiguriert, so werden die Ports:

389 (ungesichert)

636 (TLS-gesichert)

für Samba reserviert und stehen für die OpenLDAP-Kommunikaiton nicht mehr zur Verfügung. Benötigen spezielle Tools Daten aus einem MS AD, müssen sie immer gegen den von Samba bereitgestellten Verzeichnisdienst konfiguriert werden. Kommunizieren Tools rein über OpenLDAP, sollte den Ports eine „7“ vorangestellt werden.

Beispiel: 7389 Übliche Benennungen für dieses Feld sind Port oder LDAP Port.

ACHTUNG

Standardmäßig ist der OpenLDAP-Server so konfiguriert, dass er zusätzlich zu den Standard-Ports 389 und 636 auch auf den Ports 7389 und 7636 Anfragen entgegen nimmt.

Wird Samba/AD eingesetzt, belegt der Dienst Samba/AD-Domänencontroller die Ports 389 und 636. In diesem Fall wird OpenLDAP automatisch umkonfiguriert, so dass nur noch die Ports 7389 und 7636 eingesetzt werden. Dies ist insbesondere bei der Konfiguration von syncrepl zu beachten (siehe Syncrepl zur Anbindung von Nicht-UCS OpenLDAP-Servern). univention-ldapsearch verwendet automatisch den Standard-Port.

LDAP-Suchfilter

Durch die Nutzung des LDAP-Suchfilters kann die Anzahl der Ergebnisse bereits vor der Ausgabe reduziert werden und Suchzeit eingespart werden, indem z.B. nur Benutzerkonten oder Windows-Clients angefragt werden.

Beispiel: `(&(objectClass=person)(mailPrimaryAddress=*)` (es wird nach Objekten gesucht, die für eine Person stehen und eine primäre E-Mail-Adresse haben) Übliche Benennungen für dieses

Feld sind Filter oder LDAP filter.

Benutzer für die LDAP-Suche

Wenn der LDAP-Server keine anonymen Suchabfragen zulässt, muss in der Konfiguration für die LDAP-Suche zusätzlich ein Benutzername in Form dessen DN (Distinguished Name) angegeben werden.

Beispiel: `uid=searchuser,cn=users,dc=example,dc=com` Übliche Benennungen für dieses Feld sind Account, BindDN oder Bind-DN.

Passwort für den Suchbenutzer Damit die LDAP-Abfrage durchgeführt werden kann, muss das Passwort angegeben werden. Um die LDAP-Abfrage durchzuführen, muss der Searchuser nun auch sein Passwort angeben. Hierbei handelt es sich um das unverschlüsselte und ungehashte Passwort im Klartext. Üblicherweise werden solche Felder in einer Weboberfläche korrekt als Passwortfeld konfiguriert, sodass das Passwort nicht eingesehen werden kann.

Übliche Benennungen für dieses Feld sind Password, Bind-PWD oder Bind-DN Password.

Quelle:

- https://www.univention.de/blog-de/2021/03/integrate-with-ldap-redmine/
- https://docs.software-univention.de/manual/5.0/de/domain-ldap/ldap-directory.html