

LDAP v3 szolgáltatások

LDAP

- Az LDAP a Lightweight Directory Access Protocol rövidítése, amely egy szabványos címtár elérési protokoll.
- Katalógus szolgáltatás csak olvasni, lekérdezni képes, addig az LDAP írni is, módosíthatja az NDS adatokat.
- Integrálható a „Katalógus szolgáltatásokkal”
- Az LDAP implementáció az NDS-ben lévő LDAP objektumokon keresztül működik. A NwAdmin segítségével meghatározhatjuk az összes tulajdonságot, amelyet az NDS-ből az LDAP-on keresztül el lehet érni.
- SSL alapú kommunikáció is használható

LDAP

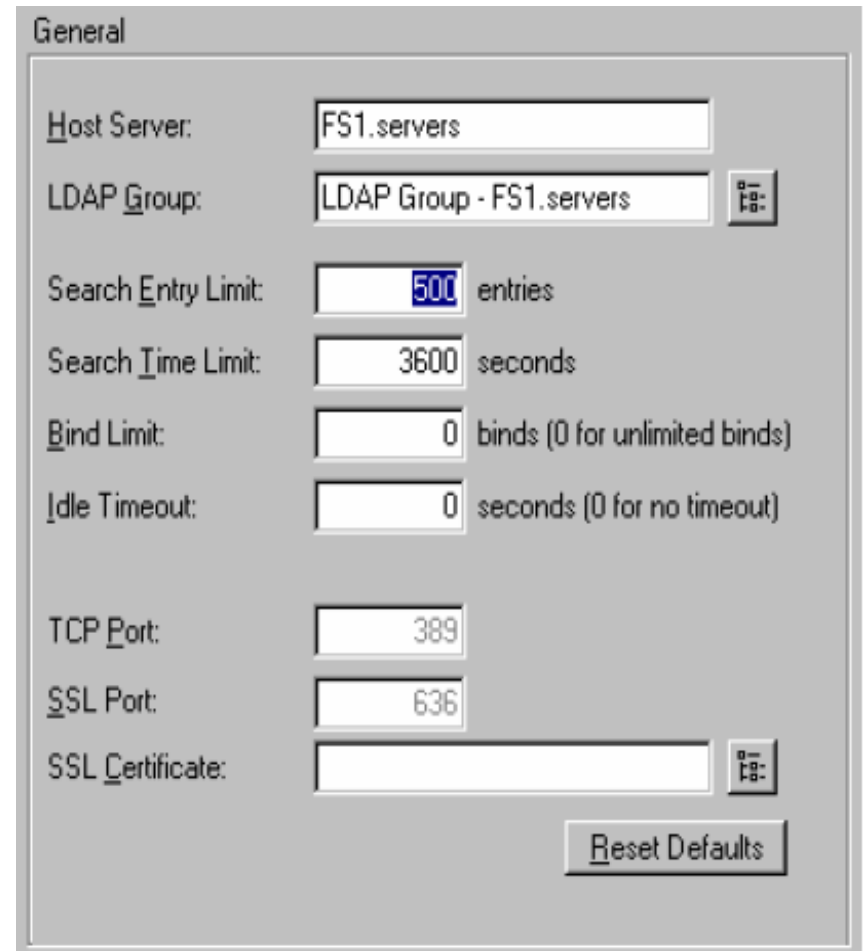
- A szerver oldalon el kell indítani az LDAP.NLM-et.
- Az LDAP kliens információkat akar megszerezni az NDS-ből, amihez jogosultságokkal kell rendelkeznie, az NDS hitelesített kapcsolatot tud csak elfogadni.

LDAP Felhasználói hitelesítés

- Felhasználói hitelesítés típusai:
 - **[Public] user (Anonymous)**
 - Név és jelszó nélküli bejelentkezés
 - [Public] objektum jogaival rendelkezik
 - Objektum tulajdonságokhoz nem fér hozzá
 - **Proxy user**
 - LDAP szolgáltatásokhoz használatos NDS user
 - Név és jelszó nélkül használható
 - Teljes lekérdezés lehetősége az NDS egészére ill. egy részére
 - LDAP groupobjektumon keresztül szűkíthetők a jogok
 - Egy LDAP group→egy NDS Proxy user
 - **NDS user**
 - LDAP kliens hitelesítése NDS beállításai alapján
 - Jelszó és a kommunikáció titkosításához SSL protokoll alkalmazása javasolt

LDAP telepítés, beállítás

- Az általános beállítások
- legfontosabbak, a kiszolgáló objektum neve, az LDAP Group objektum neve.



The screenshot shows the 'General' configuration window for LDAP. It contains the following fields and values:

Field	Value	Unit/Description
Host Server:	FS1.servers	
LDAP Group:	LDAP Group - FS1.servers	
Search Entry Limit:	500	entries
Search Time Limit:	3600	seconds
Bind Limit:	0	binds (0 for unlimited binds)
Idle Timeout:	0	seconds (0 for no timeout)
TCP Port:	389	
SSL Port:	636	
SSL Certificate:		

Buttons: 'Reset Defaults' is located at the bottom right of the window.

- A Log File Options és a Screen Options azokat a beállításokat szabályozza, amelyek a napló fájlba és amelyek az LDAP szerver képernyőjére kerüljenek.
- A napló fájl helye a SYS:ETC
- Katalógusok is használhatók az LDAP lekérdezések gyorsítására. A konfiguráció a Catalog Usage és a Catalog Schedule paramétereivel állítható be.
- Az LDAP Katalógus frissítési paramétere megegyeznek a Katalógus frissítési paramétereivel.
- A Katalógusban meghatározott szűrési, és jog korlátozási feltételek természetesen érvényesek az LDAP lekérdezés számára is.

- **LDAP Group objektum konfigurálása**
- Az LDAP Group (csoport) objektum tartalmazza az osztály és attribútum összerendeléseket, valamint a védelmi konfigurációt.
- Az általános beállítások a General lapon állíthatók be.

- A Suffix mező kiválaszthatóan azt a fa részt adja meg, ahova a keresést engedélyezzük.
- A Referral mezőbe egy másik LDAP szerver URL nevét adhatjuk meg

The image shows a 'General' configuration dialog box. It contains the following elements:

- Suffix:** A text input field with a small button to its right.
- Referral:** A text input field.
- Allow Clear Text Passwords:** A checkbox that is currently unchecked.
- Proxy Username:** A text input field with a small button to its right.

- Egy Acces By listában foglaljuk össze a jogosultsági korlátozásokat, amelyek életbe lépnek a megadott objektumok vagy tulajdonságlistájuk elérése közben.
 - **Everyone**: azaz bárki, beleértve az anonymous hozzáférést is.
 - **Self**: a saját objektuma számára képes az attribútumok között lekérdezni.
 - **LDAP Distinguished Name**: az NDS fában kijelölt objektum számára, melyet LDAP formátumban kell megadnunk, a keresési paraméterek figyelembe vételével. N D S
 - **IP address**: kiválasztott cím, vagy címtartomány kijelölésére is van mód, mely segítségével fizikailag korlátozhatjuk a hozzáférést. (pl. 135.12.*.*)

- **Keresési karakterek az LDAP rendszerben**
- Az Access By listában megadhatunk speciális karaktereket, melyeket az LDAP lekérdezés kereső karakterekként értelmez.

\	Másképpen, mint esc karakter volt már szó róla, ha a speciális karaktereket mint karakter akarjuk használni és nem mint vezérlő vagy kereső karakter, a visszafelé-perjelet kell használnunk a karakter előtt.
.	A pont használható bármely karakter jelölésére, kivéve az új sor karaktert (NEWLINE).
^	A hiányjel a sor elejének egyezőségét jelenti.
\$	A dollár jel a sor végi egyezőséget jelenti.
[string]	A kapcsos zárójelek közötti karakter, vagy karakterek bármely karakter egyezőségét jelenti.
[^string]	A kapcsos zárójelek közötti karakter, vagy karakterek, amelyeket a hiányjellel kezd bármely karakter kizárását jelenti.
[a-d]	A kötőjel két ASCII karakter között az összes kódtáblában foglalt karaktert jelenti a két karakter között.
r*	Egy csillag egy karakter után a karakter nulla vagy több egymás utáni előfordulását igényli.
r+	Egy plusz jel egy karakter után a karakter egy vagy több egymás után következő előfordulását igényli.
char	A speciális karaktereket leszámítva a karaktert jelenti. (A speciális karakterek az előbb említettek.)

- **Hozzáférési jogok**
- Az Access By listában megadhatjuk a jogokat is
- A megadott jogok természetesen csak az Access To listában megadott objektumokra érvényes.

None	A hozzáférési jogok megvonása.
Compare	Összehasonlítás, az objektum tulajdonságok értékeinek egy megadott értékkel való összehasonlítása, de nem jelenti az objektumok keresését.
Search	Keresés, az objektumok és tulajdonságaik keresését jelenti, de nem jelenti az olvasást.
Read	Olvasás, az objektumok és tulajdonságok értékeinek olvasása, keresése, összehasonlítása.
Write	Írás, az objektumok és tulajdonságaik írásához jog.

- **Access To beállítása**
- Az Access To lista beállítása megadja azok körét, akik hozzáférhetnek az itt beállított tulajdonságokhoz.

- Az első az ACL lista névadás.
- A hozzáférést beállíthatjuk, hogy mindenre (Everything) vagy az LDAP névvel megadott konténerobjektumra
- Az „All Attributes and Object Rights” egy fontos beállítás.

The screenshot shows the 'LDAP ACL Name' dialog box. The 'LDAP ACL Name' field contains 'fejlesztés'. Under 'Access To:', the radio button for 'LDAP Distinguished Name' is selected, and the text box below it contains 'OU=fejlesztés, O=NeTeN'. The checkbox for 'All Attributes and Object Rights' is unchecked. In the 'Add Object Rights to LDAP ACL' section, the checkboxes for 'Search and Delete Object' and 'Add Children to Container Object' are checked. The 'Selected LDAP Attributes' list contains the following items: administratorContactInfo, adminURL, aliasedObjectName, attributeCertificate, authorityRevocationList, authorityRevocationList;binary, c, cACertificate, cACertificate;binary, certificateRevocationList, and certificateRevocationList;binary.

- **Search and Delete Object:** Ha nem választjuk ki, az ACL-ben nem lesz objektum jog korlátozás. Ha kiválasztjuk, az alábbiak szerint módosul az objektum hozzáférés:
 - None Nincs keresés, vagy törlési jog
 - Compare Nincs keresés, vagy törlési jog
 - Search Keresési jog van, nincs törlési jog
 - Read Keresési jog van, nincs törlési jog
 - Write Keresési és törlési jog

- **Add Children to Container Object:** Az Access To listában megadott objektumokra vonatkoztatva lehet korlátozásokat eszközölni, az objektum tulajdonságokra nincs hatással. Ha kijelöljük, a megadott jogokat az alábbiakat jelenti:
 - None Nincs Add objektum jog.
 - Compare Nincs Add objektum jog.
 - Search Nincs Add objektum jog.
 - Read Nincs Add objektum jog.
 - Write Add objektum jog.

- **Selected LDAP Attributes:** Ha az LDAP Distinguished Name-ben megadott objektum tulajdonságai közül szeretne kiválasztani egyet vagy néhányat, azt itt teheti meg.

- **Access By beállítása**
- Ha beállítottuk az objektumokat, amelyekre definiáljuk a jogokat, meg kell adnunk azokat az **Access By** listában

Access By:

Everyone

Self

LDAP Distinguished Name:

IP Address:

Access Level:

None

Compare

Search

Read

Write

- **Felhasználói objektum sémaváltozása**
- Az LDAP szolgáltatások használata esetén a user objektum séma kiegészül egy E-mail addresses oldallal. Itt megadhatja a felhasználó e-mail címeit, hogy az LDAP kérések, amelyek ezt tudakolják, sikeresek legyenek.

- **Kontextus nélküli bejelentkezés**
- A munkaállomás konfigurálásának része a kontextus nélküli bejelentkezés beállítása. Ekkor a felhasználó kontextusát nem kell beállítania a bejelentkezéshez. A beállításoknál megadhatunk címtárfa nevet és a hozzátartozó katalógus nevét is, engedélyezhetünk kereső karaktereket a névben.