Einleitung

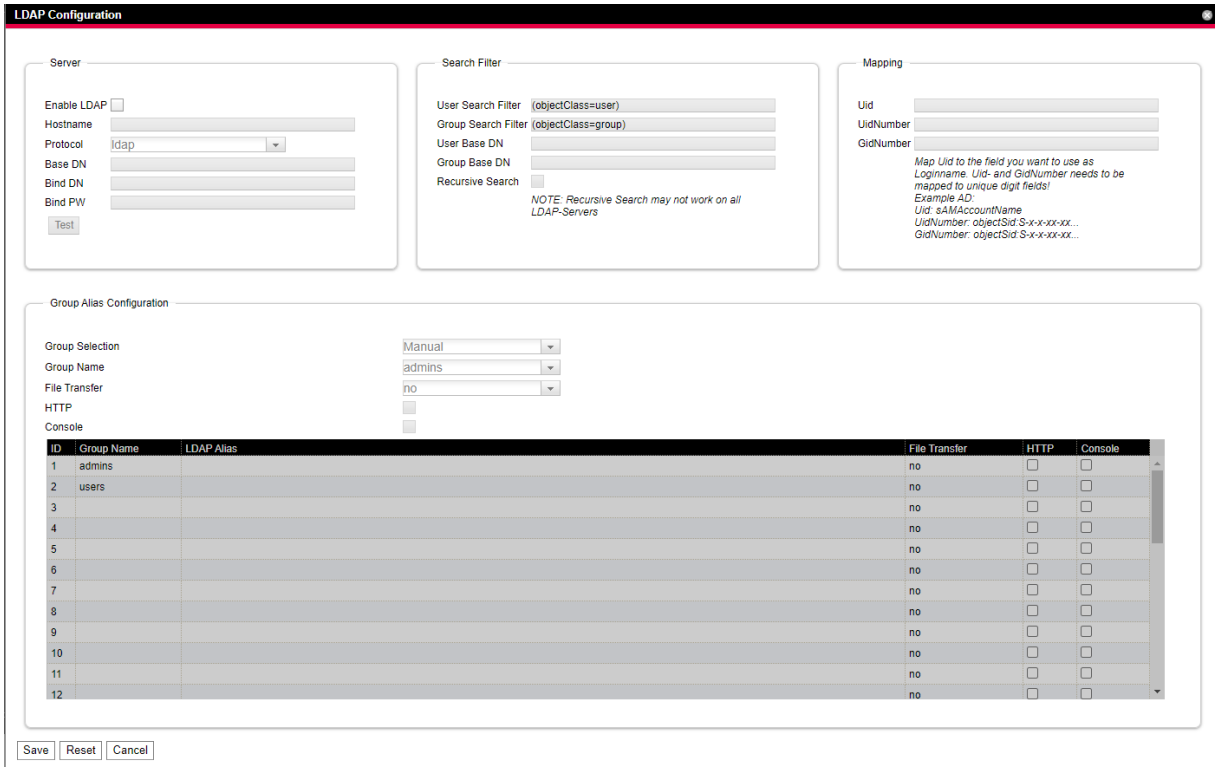
Das CMC III unterstützt das Protokoll LDAP (Lightweight Directory Access Protokoll). Mit Hilfe dieses Protokolls wird die Benutzerverwaltung des CMC III zentralisiert und mit einem Active Directory-Server verknüpft. Sind viele CMC III-Systeme im Netzwerk in Betrieb, geschieht das Hinzufügen oder Löschen eines Benutzers nicht mehr auf jedem System einzeln, sondern nur noch auf dem Server. Dies vereinfacht den Verwaltungsaufwand erheblich, da nicht mehr auf jedes CMC III System per Browser zugegriffen werden muss, sondern der jeweilige Benutzer nur einmalig auf dem Server gelöscht/hinzugefügt wird. Dieses Howto beschreibt, wie Sie das CMC III mittels LDAP an einen Active Directory-Server anbinden.

LDAP-Verzeichnis des Servers

Der Aufbau des LDAP-Verzeichnisses auf dem zentralen Server unterscheidet sich von Unternehmen zu Unternehmen. Die Struktur des Servers muss deshalb vor der Einrichtung des CMC III speziell geklärt werden. Diese Informationen müssen in der Konfiguration des CMC III hinterlegt werden. Detailinformationen zum Aufbau eines LDAP-Verzeichnisses und zu den Begriffen finden Sie auch bei Wikipedia: http://de.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol#LDAP-Verzeichnis

LDAP Konfiguration des CMC III

Wird der Button „LDAP“ gedrückt, öffnet sich das folgende Konfigurationsfenster:



Standardmäßig ist LDAP ausgeschaltet.

Im Block „Server“ muss folgendes eingetragen werden:

Hostname: Die IP oder der Hostname des Servers

Protokol: Das zu verwendende Protokoll, ldap und verschlüsselt oder ldaps Verschlüsselt!
Base DN: Der Distinguished Name (DN) des Knotens, ab dem der „Verwaltunguser“ gesucht werden soll.
Bind DN: Der DN des „Verwaltungsusers“
Bind PW: Das Passwort des „Verwaltungsusers“

Es wird empfohlen statische Anmeldeinformationen (Bind DN und PW) zu verwenden, die sich nicht regelmäßig ändern. Andernfalls muss das Passwort in jedem CMC III bei einer Änderung erneuert werden.

Im Block „Search Filter“ muss folgendes eingetragen werden

User Search Filter: Der für den Usernamen zu nutzende Filter. Standard ist „(objectClass=user)“!
Group Search Filter: Der für die Gruppen zu nutzende Filter. Standard ist „(objectClass=group)“!
User Base DN: Der (DN) des Knotens, ab dem nach dem Nutzer der sich einloggen will, gesucht werden soll.
Group Base DN: Der (DN) des Knotens, ab dem nach der Gruppe gesucht werden soll, in der der sich einloggende Nutzer, Mitglied ist.
Recursive Search: Sollten Nested Groups existieren, sollte diese Option gewählt werden.

Im Block „Mapping“ sollte folgendes eingetragen werden.

Uid: Das Attribute, mit dem sich der Benutzer anmelden möchte. Z.B. „sAMAccountName“

UidNumber: Hier muss eine eindeutige Zahl angegeben werden. Für einen AD Server wäre das die objectSid der Domain. Z.B. „S-1-5-21-1793229399-2355805357-1971770083“ muss wie folgt im Feld UidNumber eingetragen werden „objectSid:S-1-5-21-1793229399-2355805357-1971770083“.

GidNumber: Hier muss eine eindeutige Zahl angegeben werden. Für einen AD Server wäre das die objectSid der Domain. Z.B. „S-1-5-21-1793229399-2355805357-1971770083“ muss wie folgt im Feld GidNumber eingetragen werden „objectSid:S-1-5-21-1793229399-2355805357-1971770083“.

Jedes Element im AD hat noch einen weiteren Zahlen Block, z.B. S-1-5-21-1793229399-2355805357-1971770083-**2345** dieser darf nicht mit angegeben werden.

Im Feld „Group Alias Configuration” kann dann festgelegt werden, welcher lokalen Gruppe die Benutzer zugeordnet werden sollen. So kann jeder Nutzer:

„Manuel“: eine Gruppe zugeordnet werden, sowie Zugriffsrechte auf FTP, http und die Console eingeschränkt werden.

„LDAP“: Das Mapping und die Zugriffsrechte werden entsprechend der Tabelle vorgenommen. Dabei muss im Feld „LDAP Alias“ der DN der Gruppe eingetragen werden dessen Mitglieder auf die Gruppe „Group Name“ gemapped werden sollen.

„LDAP, manual if no match“: Hier wird zunächst versucht die Konfiguration aus der Tabelle anzuwenden, ist dies nicht möglich werden dem Nutzer die „manuel“ eingestellten Werte zugeordnet.

Der „Test“ Button Prüft nur ob mit den angegebenen Bind User eine Verbindung zum Server aufgebaut werden kann und ob Ergebnisse für die Anfragen mit dem User bzw. Group-Filter geliefert werden.