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:

Server	Search Filter		Manning			
Server	Jean Inter		Mapping			
Enable LDAP	User Search Filter	(objectClass=user)	Uid			
Hostname	Group Search Filter	(objectClass=group)	UidNumber			
Protocol Idap -	User Base DN		GidNumber			
Base DN	Group Base DN			Map Uid to the field you want to use as		
Bind DN	Recursive Search			mapped to unique digit	fields!	03 10 08
Bind PW		NOTE: Recursive Search may not work on all LDAP-Servers		Example AD: Uid: sAMAccountName	9	
Test				UidNumber: objectSid: GidNumber: objectSid:	S-x-x-xx-xx S-x-x-xx-xx	
	IN INSTALLING	-				
Group Name	admins	* *				
Group Name File Transfer	admins	v v				
Group Name File Transfer HTTP	admins no	▼ ▼ ▼				
Group Name Group Name HTTP Console	nanuan admins no	*				
rorup Name File Transfer HTTP Console (ID Group Name LDAP Alias	no	v v		File Transfer	нттр с	Console
Sroup Name File Transfer HTTP Console 10 Group Name LDAP Alias 1 admins	natitual admins no	v v		File Transfer no	нттр с	console
File Transfer File Transfer HTTP Console 1 admins 2 users LDAP Alias	naliuai admins no	v v		File Transfer no no	HTTP C	console
File Transfer File Transfer UD Group Name LDAP Alias 1 admins 2 users 3	ndmins admins no	v v		File Transfer no no no		Sonsole
Orgun Name LDAP Alias 1 admins 2 users 3	namina admins no	v v		File Transfer no no no		console
File Transfer File Transfer HTTP Console U Group Name LDAP Alias admins users 3 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	nalitual admins no	* *		File Transfer no no no no no		console
File Transfer File Transfer ITTP Console Ito Group Name LDAP Alias I admins UAP Alias I users I users I users I admins I	ndmins no	• •		File Transfer no no no no no no no no		console
Image: Source Name LDAP Alias File Transfer LDAP Alias HTTP LDAP Alias 1 admins 2 users 3	namua admins no	•		File Trensfer no no no no no no no no		onsole
Image: Second Name LDAP Allas 1 admins LDAP Allas 2 users	Maliual admins no	•		File Transfer no no no no no no no no no		onsole
Image: Source Series	Maliua admins no	•		Filo Transfer no no no no no no no no no no no no no		Console
Image: Concept Name LOAP Alias File Transfer LOAP Alias I admins LOAP Alias 1 admins LOAP Alias 3 admins LOAP Alias 4 admins LOAP Alias 5 admins LOAP Alias 4 admins LOAP Alias 5 admins LOAP Alias 6 admins LOAP Alias 9 admins LOAP Alias 10 admins LOAP Alias	Maliua admins no	• •		File Transfer no no no no no no no no no no no no no		console

Save Reset Cancel

Standardmäßig ist LDAP ausgeschaltet.

Im Block "Server" muss folgendes eingetragen werden:

Hostname: Die IP oder der Hostname des Servers

Protokol:	Das zu verwendende Protokoll, Idap und verschlüsselt oder Idaps 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.