HINWEISE
KONFIGURATION OPEN LDAP

VORBEMERKUNG

Im Rahmen der Einführung eines neuen Identity Management Systems (IDM) wurden auch die LDAP-Server erneuert. Dabei wurden folgende Ziele verfolgt:

- Weitestgehende Kompatibilität zu den bisher verwendeten Systemen
- Vollständige Einhaltung der Standards und damit größtmögliche Kompatibilität zu Client-Systemen
- Erweiterbarkeit, um den zukünftigen Bedürfnissen der RUB genügen zu können

VERBESSERUNG VON SICHERHEIT, PERFORMANZ & STABILITÄT

Die neuen LDAP-Server basieren auf OpenLDAP, einer bewährten und performanten Software, die seit vielen Jahren bei Universitäten und Unternehmen zum Einsatz kommt.

Trotz aller Bemühungen war es nicht möglich, die aktuelle Datenstruktur unverändert auf die neuen Systeme zu übernehmen, so dass es bedauerlicherweise zu nicht rückwärtskompatiblen Änderungen gekommen ist, um den aktuellen LDAP-Standard einzuhalten. Die Änderungen sind in diesem Dokument zusammengefasst.

WICHTIGSTE ÄNDERUNGEN AUF EINEN BLICK

Hier werden nur die wichtigsten Änderungen beschrieben. Diese Änderungen sollten müssen in jedem Fall überprüft und ggfs. angepasst werden.

- Der Hostname hat sich geändert
- Es sind ausschließlich verschlüsselte Verbindungen erlaubt
- Das auszulesende Attribut für Gruppenmitgliedschaften hat sich geändert.

Besondere Aufmerksamkeit sollte der Prüfung von Gruppenmitgliedschaften gelten, da hier in jedem Fall Änderungen erforderlich sind.

Die vollständigen Änderungen zu den einzelnen LDAP-Zweigen befinden sich in den nachfolgenden Kapiteln.

Verbindungsinformationen

Das neue LDAP ist aus Sicherheitsgründen nur noch verschlüsselt zu erreichen! Bitte beachten Sie, dass sich der Hostname geändert hat.

	ALT	NEU
Hostname:	ldap.ruhr-uni-bochum.de	openldap.ruhr-uni-bochum.de
Port:	636 LDAPS, verschlüsselt mit TLS 389 LDAP unverschlüsselt	636 LDAPS, verschlüsselt mit TLS 389 LDAP+STARTTLS verschlüsselt
Verschlüsselungsmethode:	SSL (ldaps://) oder keine Verschlüsselung (ldap://)	SSL (ldaps://)

Attribute

Vergleiche und Suchen beachten jetzt die Groß- / Kleinschreibung (case-sensitive)

WO	ALT	NEU
groups (mitglieder)	uniqeMember	member
Userobjekte	memberOf (normales Attribut)	memberOf (operationales Attribut) (sollte in den meisten Fällen keine Auswirkung haben)

Objektklassen

Objektklassen haben sich grundsätzlich geändert. Verweise oder Suchen auf Objektklassen sollten geändert werden (ausgenommen auf Objektklasse Top). Hier die wichtigsten:

Objekte	ALT	NEU
groups	groupOfUniqueNames	groupOfNames posixGroup rubAccessControl
users	rubBadPwd rubRole rubTmpAccount	eduPerson posixAccount rubAccessControl rubOrgPerson rubPerson schacPersonalCharacteristics homeInfo

ÄNDERUNGEN ZWEIGE ALLGEMEIN

Hier werden die Änderungen zu den einzelnen Zweigen beschrieben. Die vollständige Beschreibung aller Attribute befindet sich in der LDAP Dokumentation.

Weggefallener Zweig

Zweig	Ehemaliger DN
Mailaccounts fh-gelsenkirchen	ou=mailaccounts,dc=fh-gelsenkirchen,dc=de

ÄNDERUNGEN USERS-ZWEIG

Geänderte Attribute

Nur Änderungen, keine vollständige Liste der Attribute

	Attribute
Weggefallene Attribute	dfnEduPersonPkiIntegrity dfnEduPersonVerifiedMobile facsimileTelephoneNumber freischaltDatum rubBadPwdLockoutDuration rubBadPwdLockoutThreshold Vdejoindn RubcardId
Neu hinzugekommene Attribute	gidNumber homeDirectory homeEmailAddress l loginShell personalMobile rubAccountStatus uidNumber

Objektklassen

	Objektklassen
Alt	rubBadPwd rubRole rubTmpAccount
Neu	eduPerson posixAccount rubAccessControl rubOrgPerson rubPerson schacPersonalCharacteristics

ÄNDERUNGEN GROUPS-ZWEIG

Geänderte Attribute

Nur Änderungen, keine vollständige Liste der Attribute.

	Attribute
Weggefallene Attribute	uniqueMember
Neu hinzugekommene Attribute	gidNumber member rubReadAllow

Objektklassen

	Objektklassen
Alt	groupOfUniqueNames
Neu	groupOfNames posixGroup rubAccessControl

ÄNDERUNGEN USERSX-ZWEIG

Geänderte Attribute

Nur Änderungen, keine vollständige Liste der Attribute.

	Attribute
Weggefallene Attribute	facsimileTelephoneNumber freischaltDatum rubBadPwdLockoutDuration rubBadPwdLockoutThreshold rubBadPwdRealmNr rubCardID specialPassword vdejoindn
Neu hinzugekommene Attribute	rubAccountStatus

Objektklassen

	Objektklassen
Alt	rubBadPwd rubOrgPerson rubSpecBadPwd rubTmpAccount
Neu	eduPerson rubAccessControl rubOrgPerson rubPerson schacPersonalCharacteristics

ÄNDERUNGEN HOSTS-ZWEIG

Host-Gruppen

Geänderte Attribute

Nur Änderungen, keine vollständige Liste der Attribute.

	Attribute
Weggefallene Attribute	//keine
Neu hinzugekommene Attribute	rubReadAllow

Objektklassen

	Objektklassen
Alt	organizationalUnit
Neu	organizationalUnit rubAccessControl

Host-Gruppen-Mitglieder

Geänderte Attribute

Nur Änderungen, keine vollständige Liste der Attribute.

	Attribute
Weggefallene Attribute	authLevel description eduPersonAffiliation facsimileTelephoneNumber gecos mailDirectory memberOf rubBadPwdCount rubBadPwdHash rubBadPwdLockoutDuration rubBadPwdLockoutThreshold rubBadPwdLockoutTime rubBadPwdTime rubCardID rubPrivateIPv4 userClass userPassword vdejoindn
Neu hinzugekommene Attribute	rubAccountStatus

Objektklassen

	Objektklassen
Alt	posixAccount rubBadPwd rubRole
Neu	eduPerson posixAccount rubAccessControl rubOrgPerson rubPerson schacPersonalCharacteristics

ÄNDERUNGEN MAILACCOUNTS-ZWEIG

Geänderte Attribute

Nur Änderungen, keine vollständige Liste der Attribute.

	Attribute
Weggefallene Attribute	authLevel eduPersonAffiliation loginShell mailQuotaHardBlocks mailQuotaHardFiles mailQuotaSoftBlocks mailQuotaSoftFiles rubBadPwdCount rubBadPwdHash rubBadPwdLockoutDuration rubBadPwdLockoutThreshold rubBadPwdLockoutTime rubBadPwdTime rubCardID specialPassword userPassword vdejoindn
Neu hinzugekommene Attribute	givenName l ou postalAddress postalCode rubAccountStatus schacDateOfBirth sn telephoneNumber

Objektklassen

	Objektklassen
Alt	posixAccount rubBadPwd
Neu	eduPerson posixAccount rubAccessControl rubOrgPerson rubPerson schacPersonalCharacteristics

ÄNDERUNGEN SICHERHEITS-ZWEIG

Sicherheitsgruppen

Wurden vorher nicht im LDAP repräsentiert und waren nur im IDM vorhanden. Jetzt sind Sicherheitsgruppen als Gruppen im openLDAP abgebildet und die Binduser sind Mitglieder dieser Gruppen.

Geänderte Attribute

Nur Änderungen, keine vollständige Liste der Attribute.

	Attribute
Weggefallene Attribute	//es gab keine Sicherheitsgruppen im ldap
Neu hinzugekommene Attribute	cn member objectClass

Objektklassen

	Objektklassen
Alt	//es gab keine Sicherheitsgruppen im ldap
Neu	groupOfNames

Binduser

Binduser sind jetzt in der Lage, ihren eigenen Eintrag nach erfolgreicher Authentifizierung abzurufen.

Geänderte Attribute

Nur Änderungen, keine vollständige Liste der Attribute.

	Attribute
Weggefallene Attribute	givenName l mail rubBadPwdLockoutDuration rubBadPwdLockoutThreshold vdejoindn
Neu hinzugekommene Attribute	memberOf rubAccountStatus sn

Objektklassen

	Objektklassen
Alt	rubAdmin rubBadPwd
Neu	person rubAccessControl

ÄNDERUNGEN UNIXACCOUNTS-ZWEIG

Geänderte Attribute

Nur Änderungen, keine vollständige Liste der Attribute.

	Attribute
Weggefallene Attribute	gecos gidNumber homeDirectory loginShell uidNumber userPassword
Neu hinzugekommene Attribute	ou postalAddress postalCode schacDateOfBirth rubAccountStatus sn telephoneNumber

Objektklassen

	Objektklassen
Alt	posixAccount
Neu	eduPerson rubAccessControl rubOrgPerson rubPerson schacPersonalCharacteristics

KONTAKT & HILFE:

Bei Fragen und Problemen wenden Sie sich an unseren Helpdesk unter: **its-helpdesk@ruhr-uni-bochum.de**