IBM STG Technical Sales System z

LDAP-Anbindung des VSE an Linux oder VM

Jörg Härtel
Senior IT Spezialist
haertel@de.ibm.com

30.04.2009

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

AS/400, DBE, e-business logo, ESCON, eServer, FICON, IBM, IBM Logo, iSeries, MVS, OS/390, pSeries, RS/6000, S/390, VM/ESA, VSE/ESA, Websphere, xSeries, z/OS, zSeries, z/VM, z/VSE

For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml:

The following are trademarks or registered trademarks of other companies

Lotus, Notes, and Domino are trademarks or registered trademarks of Lotus Development Corporation
Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries
LINUX is a registered trademark of Linux Torvalds
UNIX is a registered trademark of The Open Group in the United States and other countries.
Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.
SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.
Intel is a registered trademark of Intel Corporation
*** All other products may be trademarks or registered trademarks of their respective companies.**

Agenda

- **LDAP Nutzen**
- **LDAP**
- **LDAP Client VSE**
- **LDAP z/VM**
- **openLDAp Linux (zSeries)**
- **Verbindung VSE LDAP zu z/VM LDAP**
- **Verbindung VSE LDAP zu open LDAP**
- **Debugging Tipps**

LDAD Nutzen

- **zentrales Benutzer Management**
- **ein möglicher Weg zum ‚Single Sign On‘**
- **Offener Standard**
  - X.500
  - TCP/IP, SSL/TLS Support
- **LPAP Server sind verfügbar für viele Betriebsysteme**
  - z/OS, z/VM, Linux für z Server
  - Unix (allgemein), AIX, Microsoft
- **grosse Anzahl an LDAP Client**
  - jetzt auch mit z/VSE 4.2

LDAP (Lightweight Directory Access Protocol)

- **X.500 Spezifikation**
  - (Verzeichnisdienst nach OSI)
- **Hierarchisches Datenmodel**
- **Standardisierte Objekte**
  - standardisierte Attribute
- **Index gestützter Zugriff**
- **Backends (Datenbanken)**
  - LDBM
  - SDBM
  - RDBM
- **Protokoll Unterstützung**
  - TCP/IP
  - SSL/TLS

LDAP Objekte

- **LDAP Einträge bestehen aus**
  - einem Distinguished Name (DN) Statement ‘dn‘
  - mindestens einem ObjectClass: Eintrag

    z.B.
    - Top, Person, OrganizationalPerson
    - Organization, OrganizationalUnit,,
  - mindesten einen Attribute Eintrag

    z.B.
    - cn= für Commen Name, sn= für Nachname
    - o= für Organization, ou=OrganizationName
  - eine ObjectClass kann das definieren bestimmter Attribute erfordern
    - Z.B.
    - Person erfordert einen cn= Eintrag
    - Organization einen o= , OrganzationUnit einen ou= Eintrag

LDAP Attribute

- **Object Attribute**
  - ergänzen einen ‘dn‘ Eintrag mit zusätzliche Information
    - hierfür können nur spezielle Attribute verwendet werden
    - o, ou, dc
  - Attribute werden in einer ObjetctClass definiert
  - Attribute dienen als
    - Suchargument
    - Filterargument
    - Abfrage eines Passwortes
    - etc.
  - Suchabfragen nutzen Attribut basierende Index
  - Attributwerte können individuell geändert werden

LDAP

- **LDIF (Ldap Data Interchange Format)**
- **Standardisiertes Format zum**
  - Anlegen
  - Ändern
  - Löschen
  - Verschieben von Benutzern
- **Tools und Kommandos**

Linux	**z/VM**
ldapadd	LDAPADD
ldapdelete	LDAPDLET
ldapmodify	LDAPMDFY
ldapmodrdn	LDAPMRDN
ldapsearch	LDAPSRCH
ldapcompare	LDAPCMPR

LDAP Client VSE

- **Aktivierung**
  - Copy Skeleton SKLDCFG Lib.59 -> prim. Lib
    - Anpassen und katalogisieren
    - Mit CEMT SET PROG(IESLDCFG) NEWCOPY aktivieren
  - im Minimum erforderliche Anpassungen
    - LDAP_SERVERS (Host name| IP_Addr:PORT)
    - KEYRING_LIBRARY (SSL/TLS)
    - KEYNAME (SSL/TLS)
    - DN_BIND_PATTERN (cn=%u, +DN Attribute)
      - dn: cn=Joerg Haertel, ou=vse, o=ibm
      - dn: cn=Dagmar Kruse, dc=ibm, dc=com
    - BASE_DN

LDAP Client VSE

- **Aktivierung**
  - Benutzer in der Mapping File definieren
  - Batch Mapping Tool (IESLDUMA)
    - Commands
      - ID, ADD, CHANGE, DELETE, LIST, EXPORT
    - ‘cn‘ einen existierenden VSE-Benutzer zuweisen
  - LDAPUSER TYPE=LDAP mit GENPWD=
    - nur LDAP Logon für standard Benutzer (empfohlen)
  - LDAPUSER TYPE=LDAP mit VSEPWD
    - Logon nur mit BMS User-ID und Passwort
      - für SYSA, OPER, PROG im Falle eines LDAP Ausfalls
      - nicht empfohlen für standard Benutzer

LDAP z/VM

- **Supports / Provides (Auszug)**
  - Version 2 und 3 LDAP Clients
  - besitzt internen SSL Support
    - z/VM SSLSERV Server wird nicht benötigt
  - SSL V3 TLS V1
    - Client and Server Autorisierung
  - Passwort Verschlüsselung
  - RACF Zugriff (Backend Support)

LDAP z/VM

- **Konfiguration**
  - TCPMAINT
    - DS CONF auf TCPMAINT 198
      - Beispiel Datei LDAP-DS SCONFIG auf TCPMAINT 591
    - DS ENVVARS
      - Beispiel Datei LDAP-DS SAMPENVT auf TCPMAINT 591
  - LDAPSRV nutzt z/VM BFS
    - LDBM Standard Verzeichnis
      - /var/ldap
      - /var/ldap/ldbm ist das Standard LDAP Verzeichnis
      - neue LDBM Verzeichnisse werden automatisch mit neuem Sufix angelegt
      - /var/ldap/ldbm1, /var/ldbm2 etc.
  - LDBMSRV mit Schema initialisieren
    - Schema basieren auf Industrie und Produkt Regeln
    - USERSCHM LDIF und IBMSCHM LDIF von TCPMAINT 591
    - sollten nicht geändert werden

LDAP SSL/TLS

- **Aktivierung**
  - GSKKYMAN (CMS TOOL)
    - Zertifikat Management Tool
      - Beschreibung TCP/IP LDAP Administration Guide
    - USER LDAPSRC hat /var/ldap im Schreib Zugriff
    - /var/ldap hält die Datenbank für die Zertifikate und Schlüssel
    - CA oder Self-Signed Zertifikate anlegen (z.B. ldap)
    - OPENVM get/put zum Im/Export der BFS Dateien verwenden
  - DS CONFIG
    - listen ldaps://:636
    - # sslAuth serverAuth
    - sslAuth serverClientAuth
    - sslKeyRingFile /var/ldap/mykey.kdb
    - sslKeyRingFilePW password
    - sslCertificate ldap

openLDAP Linux (zSeries)

- **Installation**
  - OpenLDAP ist Teil jeder Linux Distribution
  - LDAP Server ist ein eigenes RPM
  - slapd.conf ist die Standard Konfigurations- Datei
    - meist /etc/openldap/slapd.conf
    - enthält die komplette Konfiguration
  - ./ssl Verzeichnis für
    - Server Zertifikate, private Schlüssel
    - /etc/init.d/ldap start

openSSL

- **Installation**
  - Basis um LDAP SSL/TLS zu ermöglichen
    - enthält Funktionen zur Verschlüsselung von Daten
  - openSSL ist Teil jeder Linux Distribution
  - openssl hat Funktionen zum erzeugen von
    - privaten Schlüsseln
    - von Zertifikats Anforderungen
    - erstellen selbst signierter Zertifikaten
    - kann als ‘CA‘ agieren

Verbindung VSE LDAP zu z/VM LDAP

- **Non SSL**
  - VSE Seite
    - leicht und schell zu realisieren
  - VM Seite
    - erfordert leicht höheren Aufwand
      - erstellen der Konfigurations- Dateien
      - initialisieren der LDAP Directory
      - erstellen der LDIF Dateien
- **SSL/TLS mit Server Autorisierung**
  - VSE Seite
    - leicht und schell zu realisieren
    - es werden keine Zertifikate benötigt
  - VM Seite
    - erfordert das Erzeugen oder Anfordern von Zertifikaten
    - GSKKYMAN Kenntnisse sind erforderlich

Verbindung VSE LDAP zu z/VM LDAP

- **SSL/TLS mit ClientServer Autorisierung**
  - VSE Seite
    - leider kein Ergebnis
    - eventuell ein TLS Protokoll Problem
    - wird mit dem VSE Labor geklärt
  - VM Seite
    - erfordert das Erzeugen oder Anfordern von Zertifikaten
    - GSKKYMAN Kenntnisse sind erforderlich
    - mit einem openLDAP Client erfolgreich nachgewiesen

Verbindung VSE LDAP zu openLDAP

- **Non SSL**
  - VSE Seite
    - leicht und schell zu realisieren
  - openLDAP Seite
    - erfordert leicht höheren Aufwand
      - Erstellen der slapd.conf Datei
      - Erstellen der LDIF Dateien
- **SSL/TLS mit Server Autorisierung**
  - VSE Seite
    - leicht und schell zu realisieren
    - es werden keine Zertifikate benötigt
  - openLDAP Seite
    - erfordert das Erzeugen oder Anfordern von Zertifikaten
    - openSSL Kenntnisse sind erforderlich

Verbindung VSE LDAP zu openLDAP

- **SSL/TLS mit ClientServer Autorisierung**
  - VSE Seite
    - leider kein Ergebnis
    - eventuell ein TLS Protokoll Problem
    - wird mit dem VSE Labor geklärt
  - openLDAP Seite
    - erfordert das Erzeugen oder Anfordern von Zertifikaten
    - openSSL Kenntnisse sind erforderlich
    - mit einem openLDAP Client erfolgreich nachgewiesen

Debugging Tipps

- **z/VSE**
  - IESLDCFG
    - FLAGS DC XL4‘8000000x‘
    - Ausgabe ist im SYSLOG vom CICS
  - IP TRACE
    - TRACE,ID=xxxx,IPADDR=ipaddr
    - Formatierung mit VSE IP Trace Tool von der VSE Homepage
    - Auswertung über Ethereal/Wireshark

Debugging Tipps

- **z/VM LDAP Server**
  - SMSG LDAPSRV
    - Option DEBUG
      - ANY sehr viel Information
      - weiter Level vorhanden
    - Ausgabe
      - Konsol Log
      - Konsole wenn LDAPSRV ist LOGON

Debugging Tipps

- **openLDAP Client**
  - ldapsearch
    - Option –d1 , -d2 ,-d3 viel Information
      - SSL/TLS
      - welchen Inhalt haben die Zertifikate
- **openLDAP Server**
  - slapd.conf
    - Option logging any
      - Messages in /var/log/messages

Links zu weiteren Informationen

- **Security on IBM z/VSE**
  - http://www.redbooks.ibm.com/redpieces/abstracts/sg247691.html
- **z/VM V5R4.0 TCP/IP LDAP Administration Guide**
  - http://publibz.boulder.ibm.com/epubs/pdf/hcsk8b30.pdf
- **z/VM V5R4.0 TCP/IP Planinng and Customization**
  - http://publibz.boulder.ibm.com/epubs/pdf/hcsk5b31.pdf
- **OpenLDAP 2.4 Administration Guide**
  - http://www.openldap.org/doc/admin24/OpenLDAP-Admin-Guide.pdf