SD10 – Integration von z/VSE in ein Identity Management System

Ingo Franzki, IBM

Trademarks

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

CICS*
DB2*
DB2 Connect
DB2 Universal Database
e-business logo*
Enterprise Storage Server
HiperSockets
IBM*
IBM logo*
IMS
Intelligent Miner
Multiprise*
MQSeries*
OS/390*
S/390*
SNAP/SHOT*
Virtual Image Facility
VM/ESA*
VSE/ESA
VisualAge*
VTAM*
WebSphere*
xSeries
z/Architecture
z/VM
z/VSE
zSeries

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

LINUX is a registered trademark of Linus Torvalds

Tivoli is a trademark of Tivoli Systems Inc.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries

UNIX is a registered trademark of The Open Group in the United States and other countries.

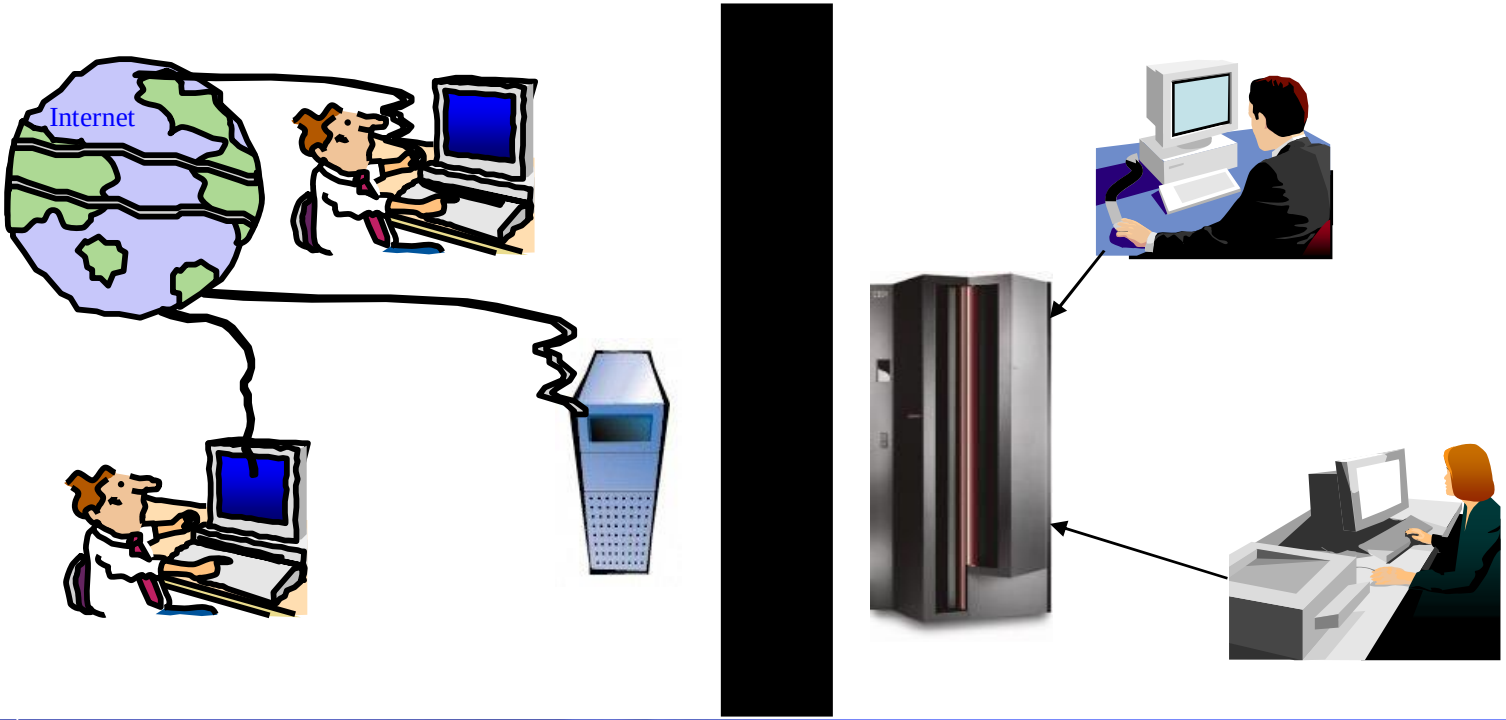
Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

Intel is a registered trademark of Intel Corporation.

Situation heute

- **Unterschiedliche User-ID Management Systeme für z/VSE und die anderen Systeme (Unix, Linux, Windows)**
  - Doppelte User IDs
  - Keine automatische Synchronisation



Situation Heute - Risiken

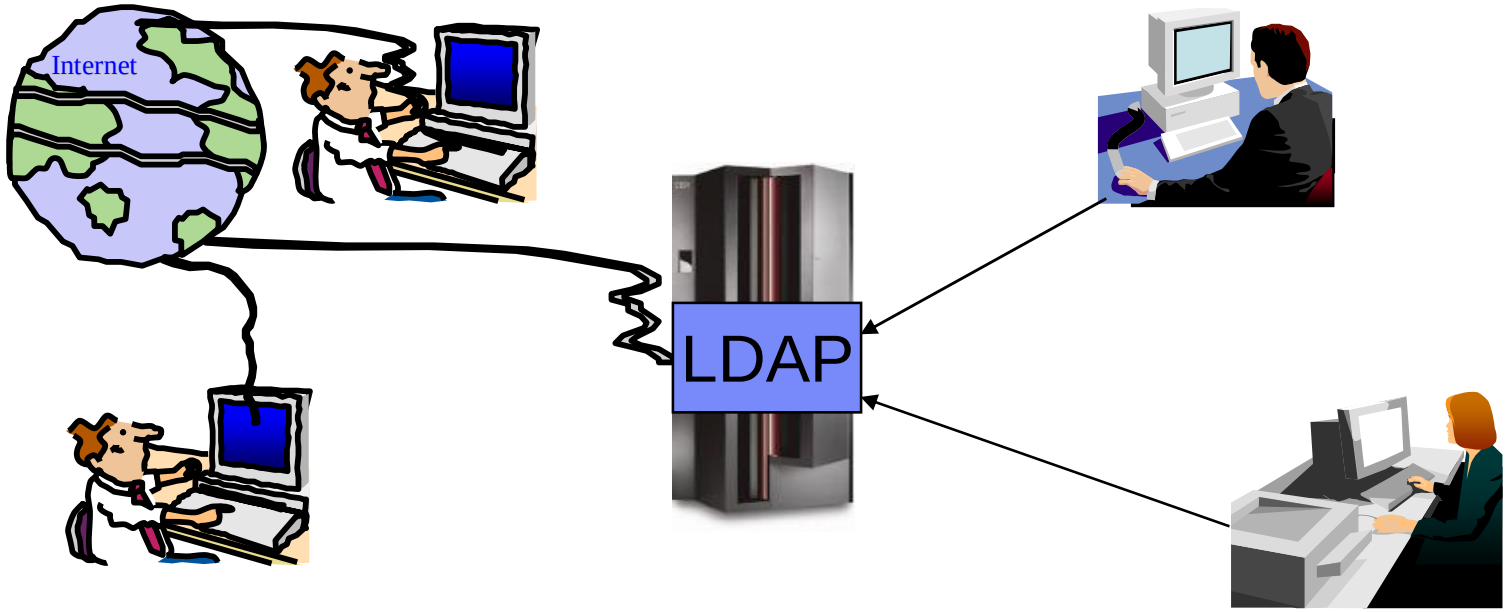
- **Das User-ID Management ist sehr komplex wenn viele unterschiedliche Systeme verwaltet werden müssen**
- **Einige User-IDs sieht man nicht direkt an wer der Besitzer ist**
  - z.B. z/VSE 4 Character User-IDs
- **Es ist schwierig bis unmöglich unternehmensweite Policies/Regeln durchzusetzen, wie z.B. regelmäßige Passwort Änderungen, Auditing, ...**
- **Beispiele:**
  - Ein Mitarbeiter verlässt die Firma
    - **Alle** seine User-IDs müssen auf **allen** Systemen deaktiviert werden.
  - Ein Mitarbeiter wechselt in eine andere Abteilung
    - Zugriffsrechte auf Dateien und Programme müssen in **allen** Systeme an seinen neuen Job angepasst werden
- **Wenn ein System vergessen wird, hat der Mitarbeiter (oder andere) möglicherweise immer noch Zugriff auf vertrauliche Daten**

Die Lösung: Zentralisiertes Identity Management

- **Ziel:**
  - Nur **EINE** Stelle, wo alle Identitäten und dazugehörige Informationen gespeichert sind
    - User-IDs
    - Zugriffsrechte
    - Gruppenzugehörigkeit, Rollen
  - Alle umgebenden Systeme greifen auf dieses eine Identity Management System zu
  - Änderungen an User-IDs (Deaktivierung, Zugriffsrechte, ...) sind automatisch für alle Systeme gültig, ohne weitere Einstellungen an den anderen Systemen machen zu müssen
  - Unternehmensweite Policies/Regeln können einfacher durchgesetzt werden
  - Selbsthilfe Help-Desks können einfacher verwirklicht werden
    - Z.B. Passwort-reset, User-ID-unlock, ...

Die Lösung: Zentralisiertes Identity Management

- **Identity Management Systeme verwenden typischerweise ein Directory um Identitäten und die dazugehörigen Informationen zu speichern**
  - Protokoll um auf das Directory zuzugreifen: **LDAP**



Was ist LDAP ?

- **The Lightweight Directory Access Protocol (LDAP) is an application protocol for querying and modifying directory services running over TCP/IP**
  - A directory is a set of objects with similar attributes organized in a logical and hierarchical manner.
    - The most common example is the telephone directory, which consists of a series of names (either of persons or organizations) organized alphabetically, with each name having an address and phone number attached.
- **Due to this basic design (among other factors) LDAP is often used by other services for authentication**
- **An LDAP directory tree often reflects various political, geographic, and/or organizational boundaries, depending on the model chosen.**
- **LDAP deployments today tend to use Domain name system (DNS) names for structuring the topmost levels of the hierarchy.**
- **Deeper inside the directory might appear entries representing people, organizational units, printers, documents, groups of people or anything else that represents a given tree entry (or multiple entries).**

- **See: Wikipedia: http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol**

Was ist LDAP ?

§ LDAP Begriffe:

– Directory

- Ein Baum aus Directory Entries.

– Entry

- Ein Entry enthält ein oder mehrere Attribute.
- Jeder Entry hat einen eindeutigen Identifier: Distinguished Name (DN).

– Attribute

- Ein Attribute hat einen Namen (Attribute-Tpe oder Attribute-Description) und einen oder mehrere Werte. Die Attribute werden in einem Schema definiert.

– Schema

- Das Schema definiert welche Attribute ein Directory Entry enthalten kann.

– Distinguished Name

- Voll qualifizierter Name in einem LDAP Directory Baum.
- Besteht aus Relative Distinguished Namen (RDN), die aus einigen Attributen des Entries gebildet werden, gefolgt von dem DN des übergeordneten Entries (Parent).
- Analog zu: DN ist der komplette Dateiname und RDN ist der relative Dateiname in einem Ordner.
- Mittels der DN kann ein Entry eindeutig identifiziert werden
- Beispiel: `uid=104903724,c=de,ou=bluepages,o=ibm.com`

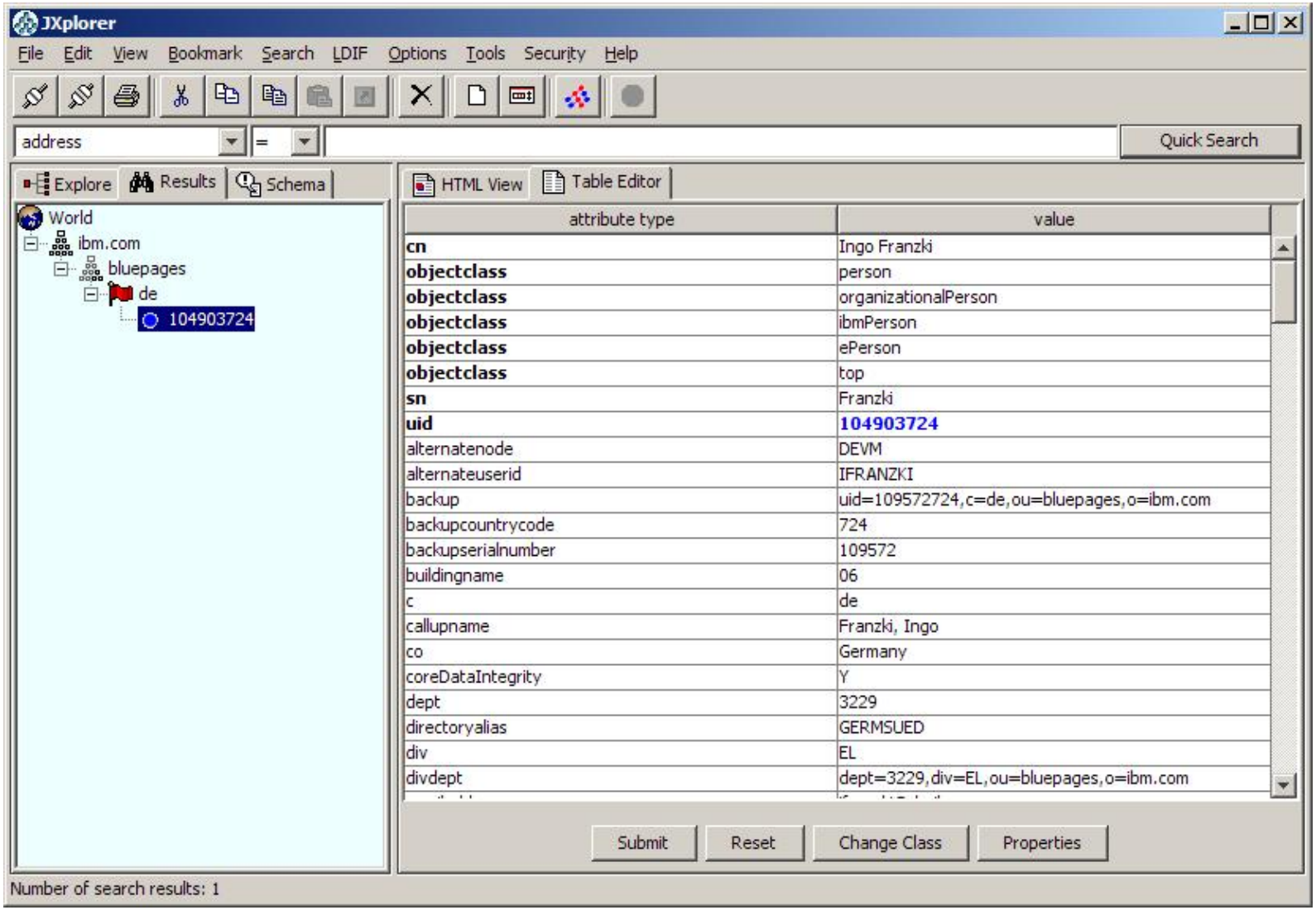
LDAP Operationen

- **Bind (Authentifizieren)**
  - Die Bind Operation authentifiziert den Client beim Server.
  - Simple Bind schickt die DN des Benutzers und sein Passwort in Klartext, man sollte also Transport Layer Security (TLS/SSL) verwenden.
  - Der Server vergleicht das Passwort typischerweise typically mit dem Attribut *userPassword* des Entries den die DN identifiziert.
  - Anonymous Bind (ohne DN und Passwort) setzt die Verbindung in den Anonymous-State zurück.
  - Bind überträgt auch die LDAP Protokoll Version. Normalerweise verwenden Clients heute LDAPv3. Das ist der Default für das Protokoll, aber nicht immer in den LDAP Libraries.

LDAP Operationen

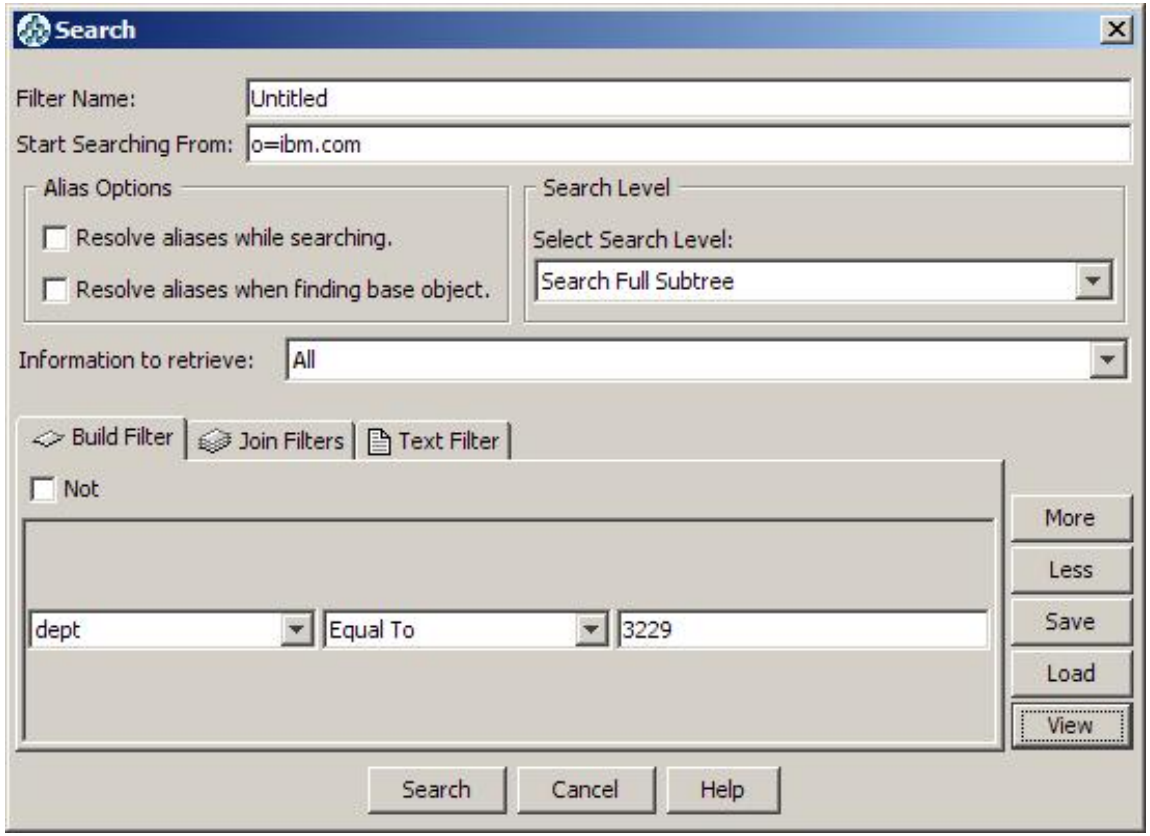
- **Search**
  - Die Search Operation wird benutzt um nach Entries zu suchen und sie anzuzeigen. Search Parameter:
    - **baseObject**
      - Der DN (Distinguished Name) des Entries wo die Suche beginnen soll,
    - **scope**
      - BaseObject (Suche nur innerhalb des spezifizierten Entries), singleLevel (Entries die dem spezifizierten DN folgen), oder wholeSubtree (der komplette Teilbaum ab dem spezifizierten DN).
    - **filter**
      - Suchfilter. z.B. (&(objectClass=person)(|(givenName=John)(mail=john*))) – Suche nach Personen, die entweder als Vorname John heißen, oder deren e-Mail Adresse mit john anfängt.
    - **derefAliases**
      - Legt fest ob Alias Entries (Referenzen auf andere Entries) gefolgt werden soll oder nicht.
    - **attributes**
      - Welche Attribute im Suchergebnis zurückgegeben werden sollen.
    - **sizeLimit, timeLimit**
      - Maximale Anzahl der Entries im Resultat, maximale Zeit.
    - **typesOnly**
      - Legt fest ob die Attribut-Werte zurückgegeben werden sollen oder nur die Attribut-Namen.
  - Der Server gibt die Entries zurück, die dem Filter entsprechen und einen Return Code.

LDAP Beispiel: IBM Bluepages

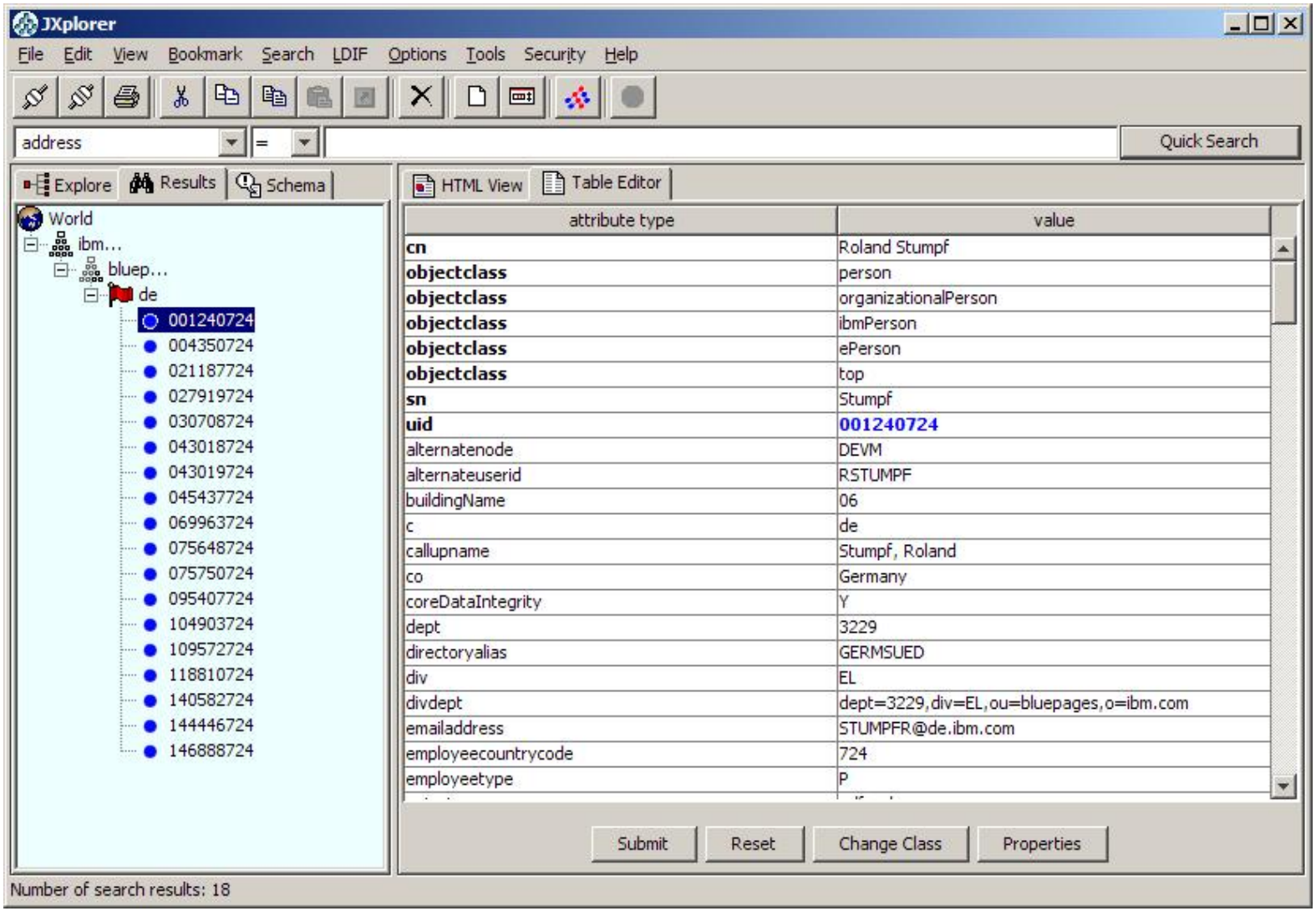


LDAP Beispiel: IBM Bluepages

- **Suche nach allen Entries mit „dept=3229“**



LDAP Beispiel: IBM Bluepages



LDAP Server (unvollständige Liste)

- **IBM Tivoli Directory Server**
- **z/VM LDAP Server**
- **Microsoft Active Directory**
- **OpenLDAP**
- **Apache Directory Server**
- **Apple Open Directory**
- **CA Directory from CA, Inc. (formerly eTrust Directory)**
- **Fedora Directory Server (Red Hat Directory Server)**
- **MXMS, from Atos Origin**
- **M-Vault, from Isode Limited**
- **Novell eDirectory**
- **OneLDAP**
- **OpenDS**
- **Oracle Internet Directory**
- **Penrose - a Java-based Virtual Directory Server.**
- **Siemens DirX**
- **SIDVault**
- **Sun Java System Directory Server**
- **....**
- **(Und viele weitere)**

z/VSE V4.2 LDAP Signon Support

- **Der LDAP Signon Support sitzt oberhalb des aktiven z/VSE Security Managers**
  - Kann mit dem Basic Security Manager (BSM) verwendet werden
  - Als auch mit einem External Security Manager (ESM)

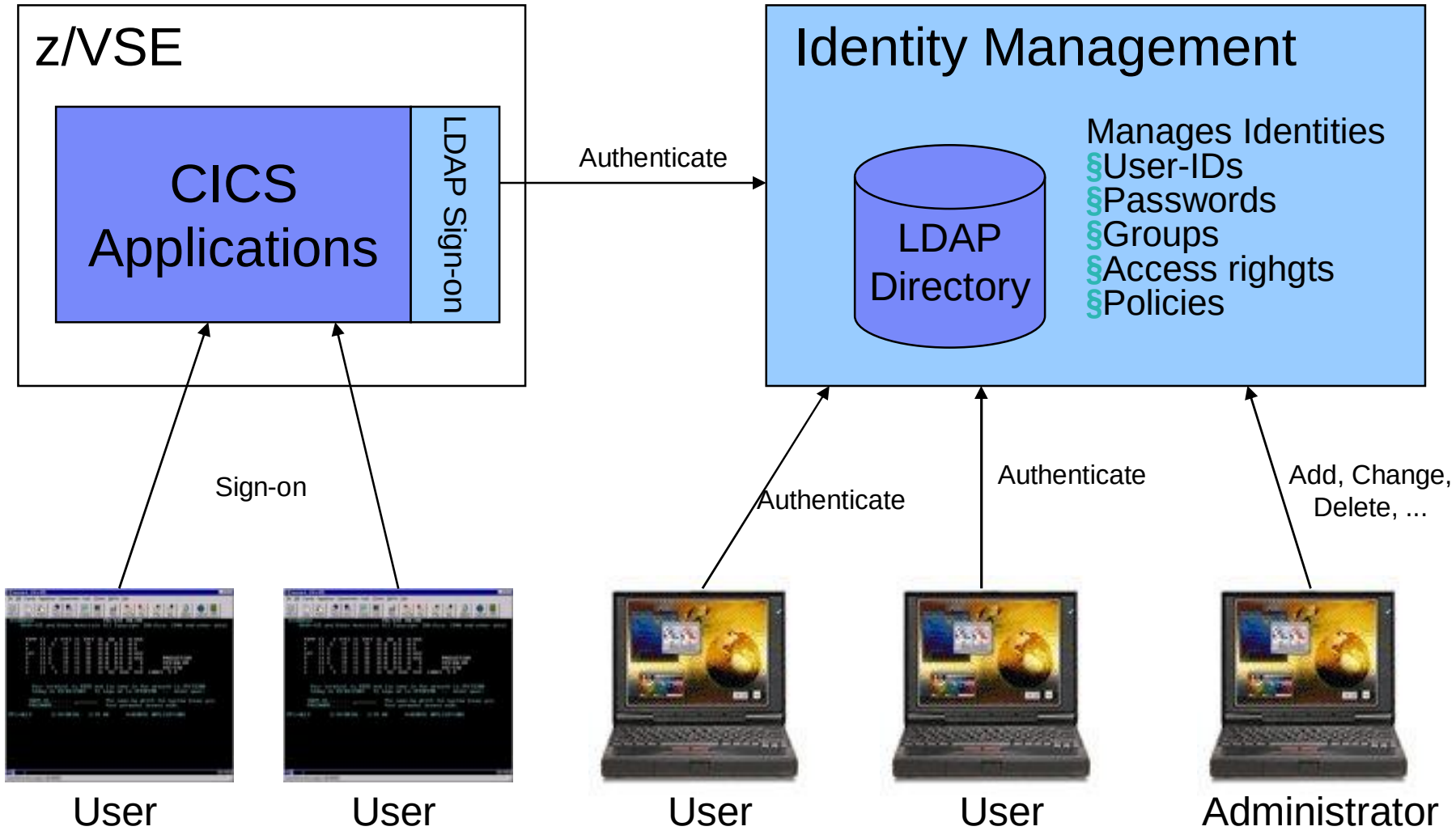
- **Der Signon Ablauf (vereinfacht)**
  1. Zuerst wird die eingegebene User-ID und Passwort gegen den LDAP Server authentifiziert
     - Mittels LDAP Bind und Search Operationen
  2. Wenn erfolgreich, wird die LDAP User-ID auf eine kurze VSE USer-ID gemapped
     - Mittels einem LDAP User Mapping File
  3. Letztlich wird die kurze VSE User-ID zusammen mit dem VSE Passwort zu dem bisherigen Signon Programm weitergegeben (BSM or ESM)

- **Zur Zeit nur für CICS Signon verfügbar**

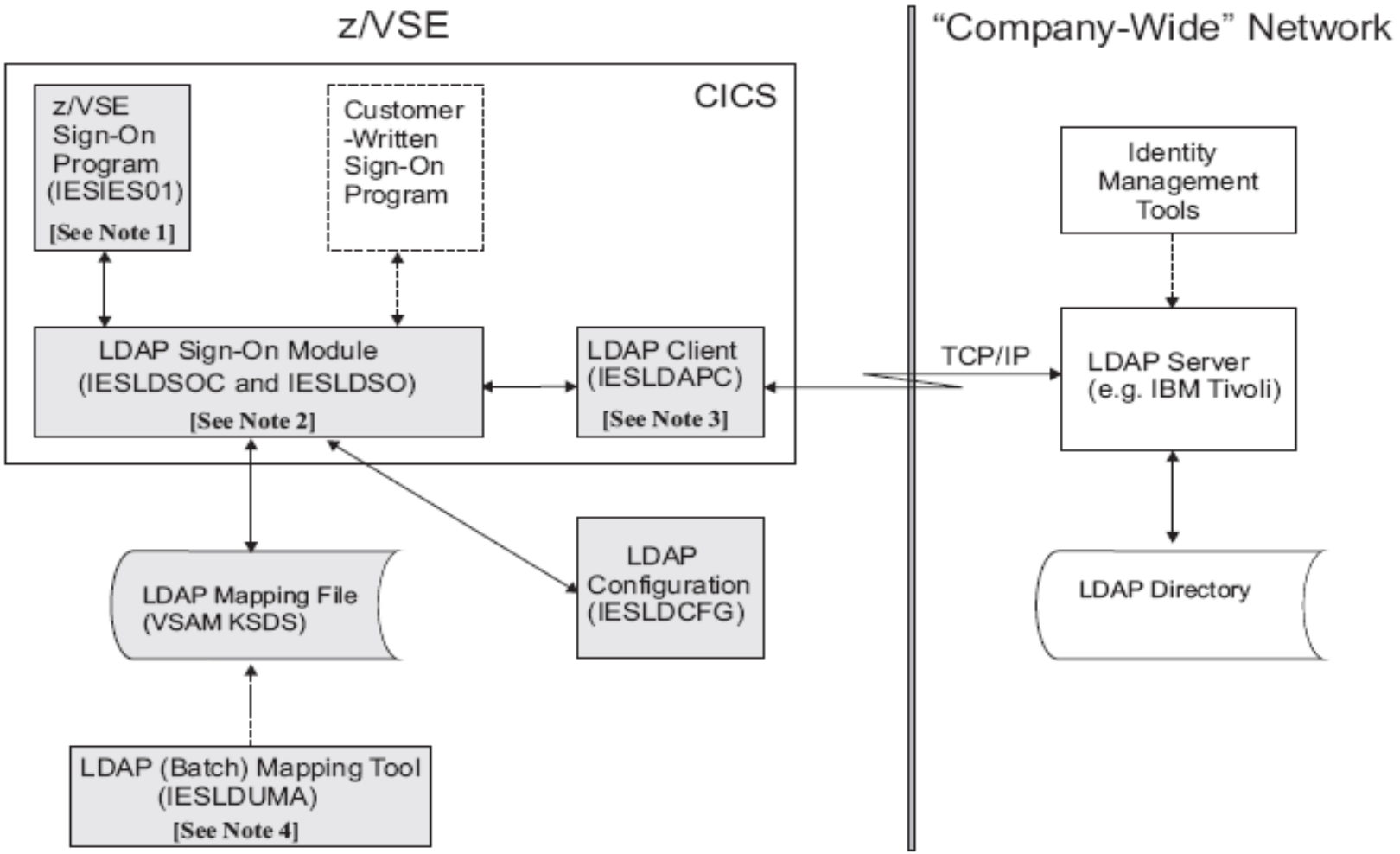
z/VSE V4.2 LDAP Signon Support

- **Ermöglicht die Integration von z/VSE in unternehmensweite Identity Management Systeme (z.B. IBM Tivoli Identity Manager, etc.)**
- **LDAP User-IDs und Passwörter können bis zu 64 Zeichen haben. Umgeht also die folgenden bisherigen Limitationen:**
  - 4 Zeichen lange VSE/ICCF User-IDs
  - 4 bis 8 Zeichen lange CICS User-IDs
  - Bis zu 8 Zeichen lange Passwörter
- **Der LDAP Signon Support sitzt oberhalb des aktiven z/VSE Security Managers (z.B. BSM, ESM, etc.)**
- **Der z/VSE LDAP Client kann mit üblichen LDAP Servern kommunizieren**
  - IBM Tivoli Directory Server
  - z/VM LDAP Server (optional mit RACF Repository)
  - OpenLDAP, Apache Directory server, Novell eDirectory, und viele andere.
- **Mögliche Vorteile sind: Verbesserter Schutz, konsistente Zugriffsregeln, Einfachere Anmeldung für Endbenutzer**

Das Gesamtbild



z/VSE V4.2 LDAP Signon Support



LDAP User Mapping File

- **Ein VSAM KSDS welches die User-ID Mappings speichert**
  - LDAP User & Passwörter: bis zu 64 Zeichen
  - VSE User & Passwörter : bis zu 8 Zeichen
- **Das LDAP Mapping File enthält:**
  - Records mit User-IDs die LDAP-enabled sind
    - Enthält ein Mapping von einer langen User-ID (für die LDAP Umgebung) zu einer kurzen User-ID (für z/VSE)
  - Records mit User-IDs die nicht LDAP-enabled sind (z.B. SYSA)
    - Diese User können sich auch anmelden, wenn der LDAP Server nicht verfügbar ist
- **Wird verwaltet mit dem Batch Tool IESLDUMA**

LDAP Password Cache

- **Authentifizierung mit einem remote LDAP Server kann sehr zeitaufwändig sein (Netzwerk-Kommunikation)**
- **Wenn sich der selbe Benutzer mehrere Male innerhalb kürzerer Zeit anmeldet, dann ist es sehr unwahrscheinlich, dass sich sein LDAP Passwort dazwischen geändert hat**
- **Wenn Caching aktiviert ist, wird eine Abkürzung verwendet um den Benutzer zu authentifizieren**
  - Das LDAP User Mapping File enthält einen Password-Hash (SHA-256) der letzten erfolgreichen Anmeldung (LDAP bind)
    - Der Hash kann **nicht** wieder in das Klartext-Passwort zurückgeführt werden
  - Bei nachfolgenden Anmeldungen wird der Passwort-Hash erzeugt, und mit dem gespeicherten Hash verglichen
    - Wenn das Hash exakt gleich ist, dann hat der Benutzer das selbe Passwort eingegeben, wie beim letzten mal
  - Der gespeicherte Passwort-Hash hat einen Gültigkeits-Zeitraum. Anmeldungen, die zu einem Zeitpunkt der nach dem Ablauf liegt erfolgen, verwenden wieder das komplette LDAP Signon (LDAP bind)

LDAP Konfiguration

- **Standardmäßig ist LDAP Signon nicht aktiviert**
- **Sie müssen eine Konfiguration anlegen, um den LDAP Signon Support zu aktivieren**
  - Skeleton SKLDCFG in ICCF Library 59
- **Die Konfiguration enthält Angaben zu (Zusammenfassung)**
  - DLBL Name des LDAP User Mapping Files (default: IESLDUM)
  - IPs oder Hostnamen des/der LDAP Server
  - Einstellungen für die Authentication Method (siehe folgende Folien)
  - Einstellungen für den Cache und Gültigkeits-Zeitraum
  - Einstellungen für Secure Socket Layer (SSL)

LDAP Authentication Methoden

- **LDAP Authentication basiert auf der LDAP Bind Operation mit dem Distinguished Name (DN) und Passwort**

- Direct Authentication:
  - Die eingegebene User-ID wird direkt für die LDAP Bind Operation verwendet.
  - Mittels eines Pattern wird der Distinguished Name gebildet z.B. „cn=%u,dc=ibm,dc=com“

- Search Authentication:
  - In dem Fall kann die eingegebene User-ID nicht direkt fürs Bind verwendet werden.
  - Stattdessen wird zuerst eine LDAP Search Operation durchgeführt, die anhand eines Attributes sucht (z.B. „email“, spezifiziert in der Konfiguration) den dazugehörigen Entry sucht.
  - Es kann ein zusätzlicher Such-Filter angegeben werden, um die Suche weiter einzuschränken, z.B. „dept=3229“
  - Das Suchergebnis ist der Distinguished Name, welcher dann für die LDAP Bind Operation verwendet wird.

LDAP Authentication Beispiele mit IBM Bluepages

- **LDAP Server: bluepages.ibm.com**

- **Direct Authentication:**
  - DN ist also "**uid=104903724,c=de,ou=bluepages,o=ibm.com**"
  - Das Pattern ist dann „**uid=%u,c=de,ou=bluepages,o=ibm.com**"
  - Der LDAP User ID ist dann die IBM Personal-Nummer: „**104903724**"
  - Das LDAP Bind wird dann durchgeführt mit der DN „**uid=104903724,c=de,ou=bluepages,o=ibm.com**" und dem angegebenen Passwort

LDAP Authentication Beispiele mit IBM Bluepages

§ Search Authentication:

- Jeder „Person“ Entry hat ein Attribute names „**email**“ welches die e-Mail Adresse des Benutzers enthält
- BaseDN für die Suche (Start-Entry) ist dann „**ou=bluepages,o=ibm.com**“
- Der zusätzliche Such-Filter kann entweder leer sein (kein Filter) oder „**dept=3229**“ um die Suche auf Personen zu limitieren, die in der Abteilung 3229 sind.
- LDAP User-ID ist also die e-Mail Addresse: „**ifranzki@de.ibm.com**“

- LDAP Search wird wie folgt durchgeführt:
  - Beginne bei „**ou=bluepages,o=ibm.com“** und suche nach Entries wo **email=ifranzki@de.ibm.com & dept=3229**
  - Das Resultat enthält dann nur meinen Entry, z.B. meine DN: **uid=104903724,c=de,ou=bluepages,o=ibm.com**

- LDAP Bind wird dann durchgeführt mit der DN „**uid=104903724,c=de,ou=bluepages,o=ibm.com“** und den eingegebenen Passwort

Selbstgeschriebene CICS Sign-on Programme

- **Das Interactive Interface Signon Programm (IESIES01) wurde mit z/VSE 4.2 angepasst, um LDAP Authentication zu unterstützen**
  - Wenn LDAP Authentication konfiguriert und aktiviert wurde, enthält das Sign-on Panel lange Felder für User-ID und Passwort.

- **Wenn Sie ein selbstgeschriebenes CICS Sign-on Programm verwenden, müssen Sie es gegebenenfalls anpassen, um LDAP Authentication zu unterstützen**
  - Vergrößern der Felder im Screen (BMS Map) für User-ID und Passwort
  - Case-sensitive Eingaben
  - Aufrufen des LDAP Sign-on Programm IESLDSOC um die LDAP Authentication durchzuführen
    - Mittels EXEC CICS LINK und COMMAREA (siehe Admin Guide)
  - Ein Beispiel CICS Sign-on Programm welches LDAP Authentication unterstützt ist auf Anfrage verfügbar (zvse@de.ibm.com).

Restriktionen

- **Im Batch ID Statement können keine langen User-IDs verwendet werden**
  - Mit ID Statements können nach wie vor nur die kurzen VSE User-IDs und Passwörter verwendet werden
- **Das LDAP Sign-on ist im Moment nur über ein CICS Sign-on Programm möglich**
  - Entweder das Interactive Interface LDAP Sign-on Programm
  - Oder ein selbstgeschriebenes Sign-on Programm .
- **Lediglich „LDAP Authentication“ (mittels Bind) wird unterstützt**
  - Kerberous Authentication (oft von MS Active Directory benutzt) wird nicht unterstützt

LDAP Tools und Dokumentation

- **LDAP Browser**
  - JXplorer (http://www.jxplorer.org/)
- **z/VSE Bücher:**
  - **Planning:** Unterkapitel in Kapitel 18. Security and Encryption Support: LDAP Sign-On Support
  - **Administration:** Kapitel 45. Maintaining User Profiles in an LDAP Environment
- **Internet:**
  - Wikipedia: http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol

Fragen ?