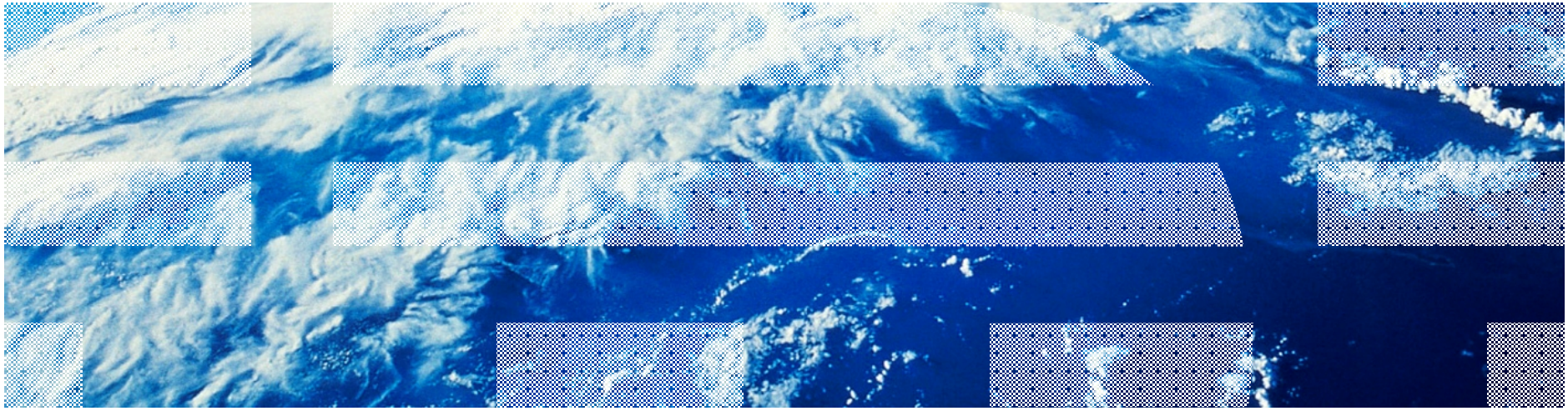
Integrating z/VSE into an Identity Management System

Ingo Franzki, IBM



Trademarks

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

Not all common law marks used by IBM are listed on this page. Failure of a mark to appear does not mean that IBM does not use the mark nor does it mean that the product is not actively marketed or is not significant within its relevant market.

Those trademarks followed by ® are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.

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

*, AS/400®, e business(logo)®, DBE, ESCO, eServer, FICON, IBM®, IBM (logo)®, iSeries®, MVS, OS/390®, pSeries®, RS/6000®, S/30, VM/ESA®, VSE/ESA, WebSphere®, xSeries®, z/OS®, zSeries®, z/VM®, System i, System i5, System p, System p5, System x, System z, System z9®, BladeCenter®

The following are trademarks or registered trademarks of other companies.

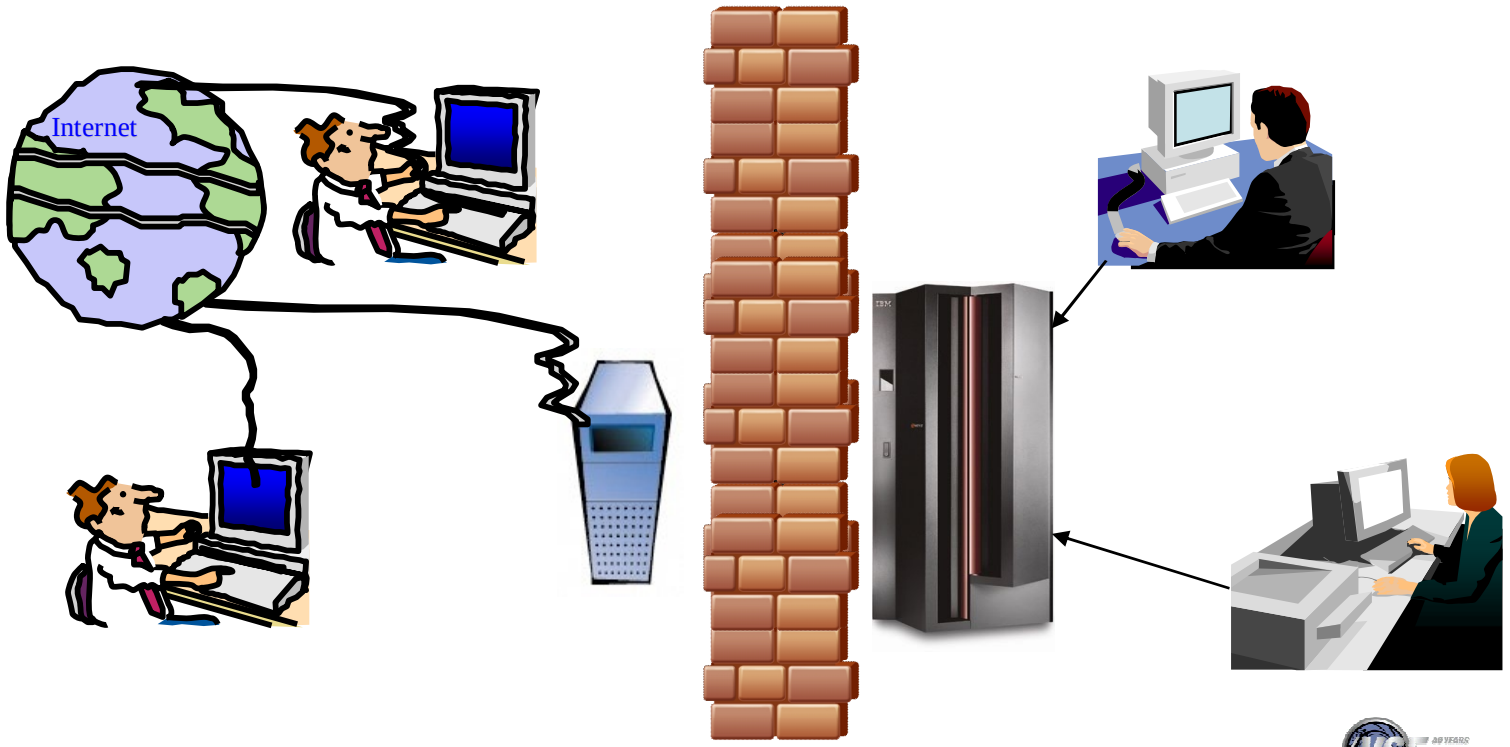
Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:
Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.
IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.
All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.
Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Situation today

- Separate User-ID Management Systems for z/VSE and the others (Unix, Linux, Windows)
  - Duplicate User IDs
  - No automatic syncronisation



Situation today - Risks

§ User-ID management is very complex if different systems need to be updated

§ Some User-IDs do not explicitely show who is the owner
  – e.g. z/VSE 4 character User-IDs

§ Difficult to enforce corporate policies, like password renewal, auditing, ...

§ Examples:
  – If an employee leaves the company
    • Deactive **all** of his User-IDs on **all** systems
  – If an emloyee moves to another department
    • Permissions to access files/programs needs to be adjusted according to his new job on **all** systems

§ If you miss to update one system, the employee (or others) may still have access to confidential data

Solution: Centralized Identity management

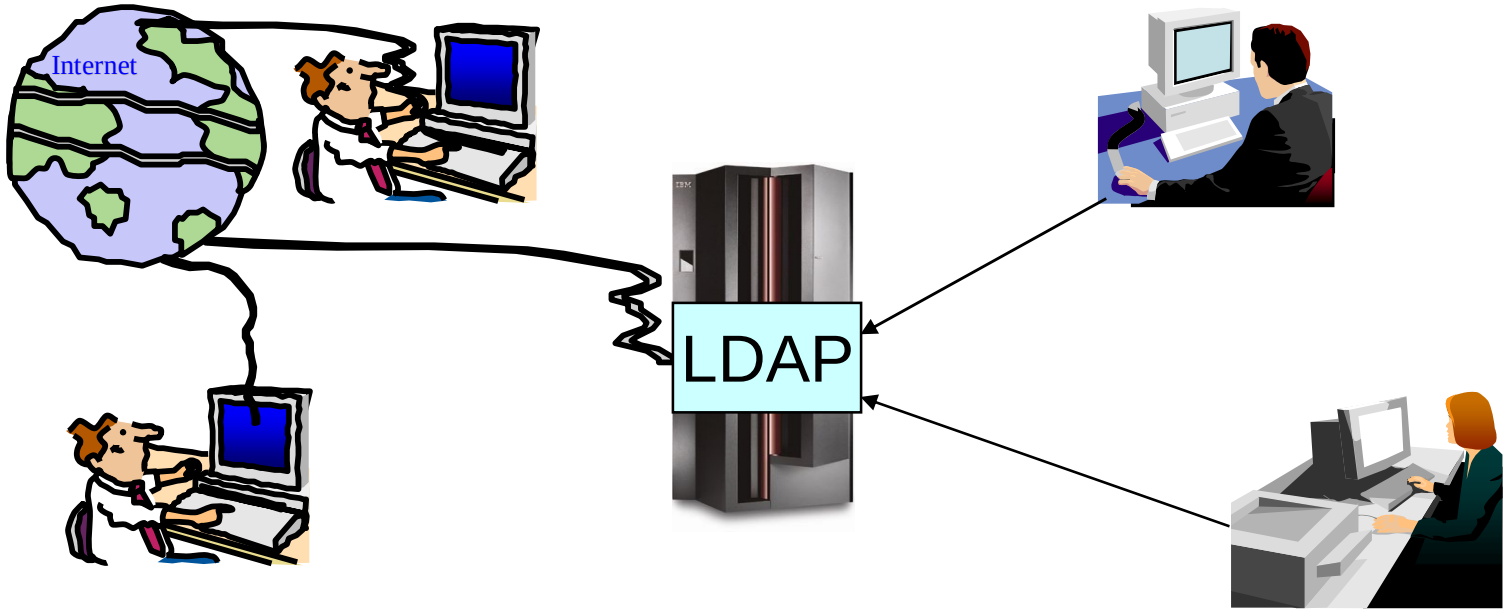
§ Goal:

- –Only **ONE** place where all Identity related information is stored
  - User-IDs
  - Permissions
  - Groups, Roles
- –All suronding systems access that single Identity Management System
- –Changes to a User-ID (deactivation, modification) automatically affect all systems, without any additional actions
- –Corporate policies can easily be enforced
- –Self servcie Help-Desk can easier be accomplished
  - e.g. Password reset, User-ID unlock, ...

Solution: Centralized Identity management

§ Identity Management Systems typically use a Directory to store ID related information

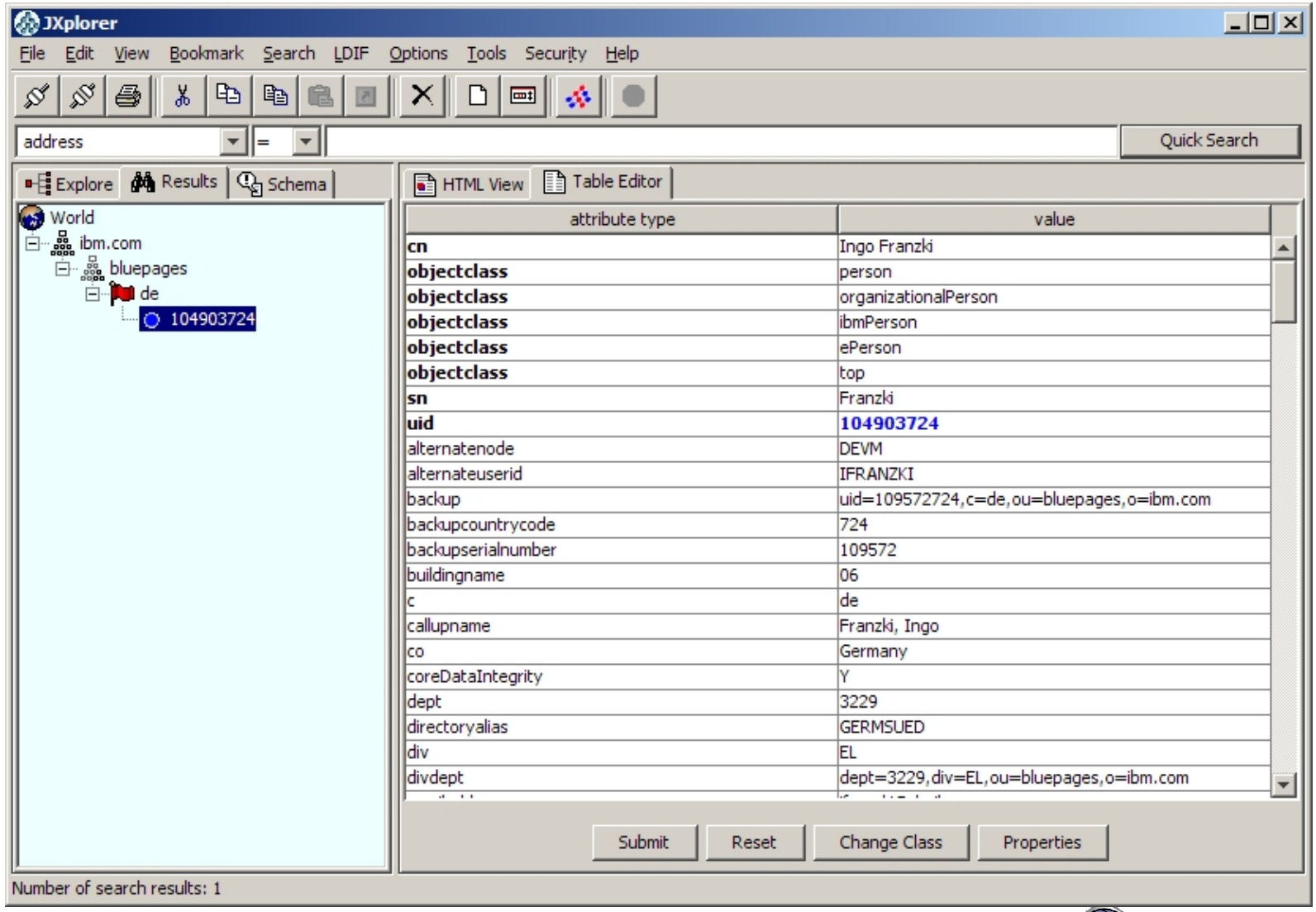
  –Protocol to access the directory: **LDAP**



What is LDAP ?

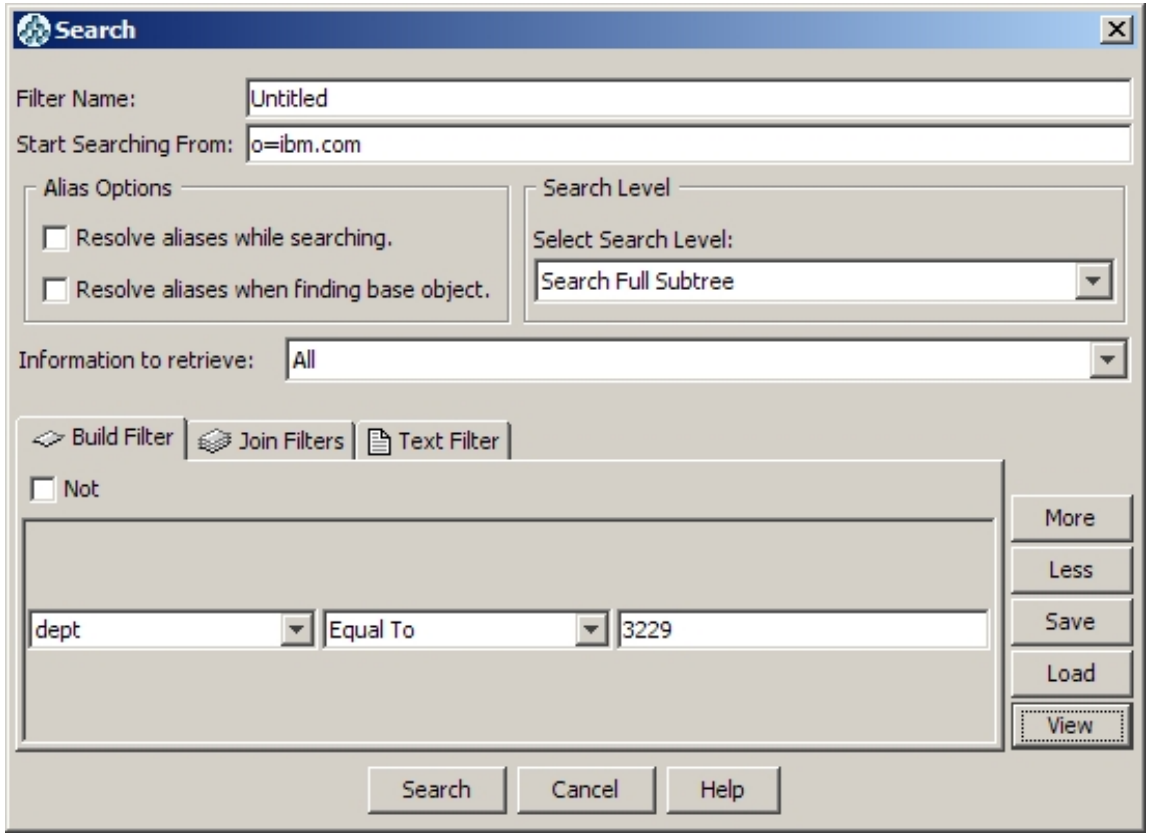
- The Lightweight Directory Access Protocol (LDAP) is an application protocol for querying and modifying directory services running over TCP/IP
  - A directory is a set of objects with similar attributes organized in a logical and hierarchical manner.
    - The most common example is the telephone directory, 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

LDAP Example: IBM Bluepages

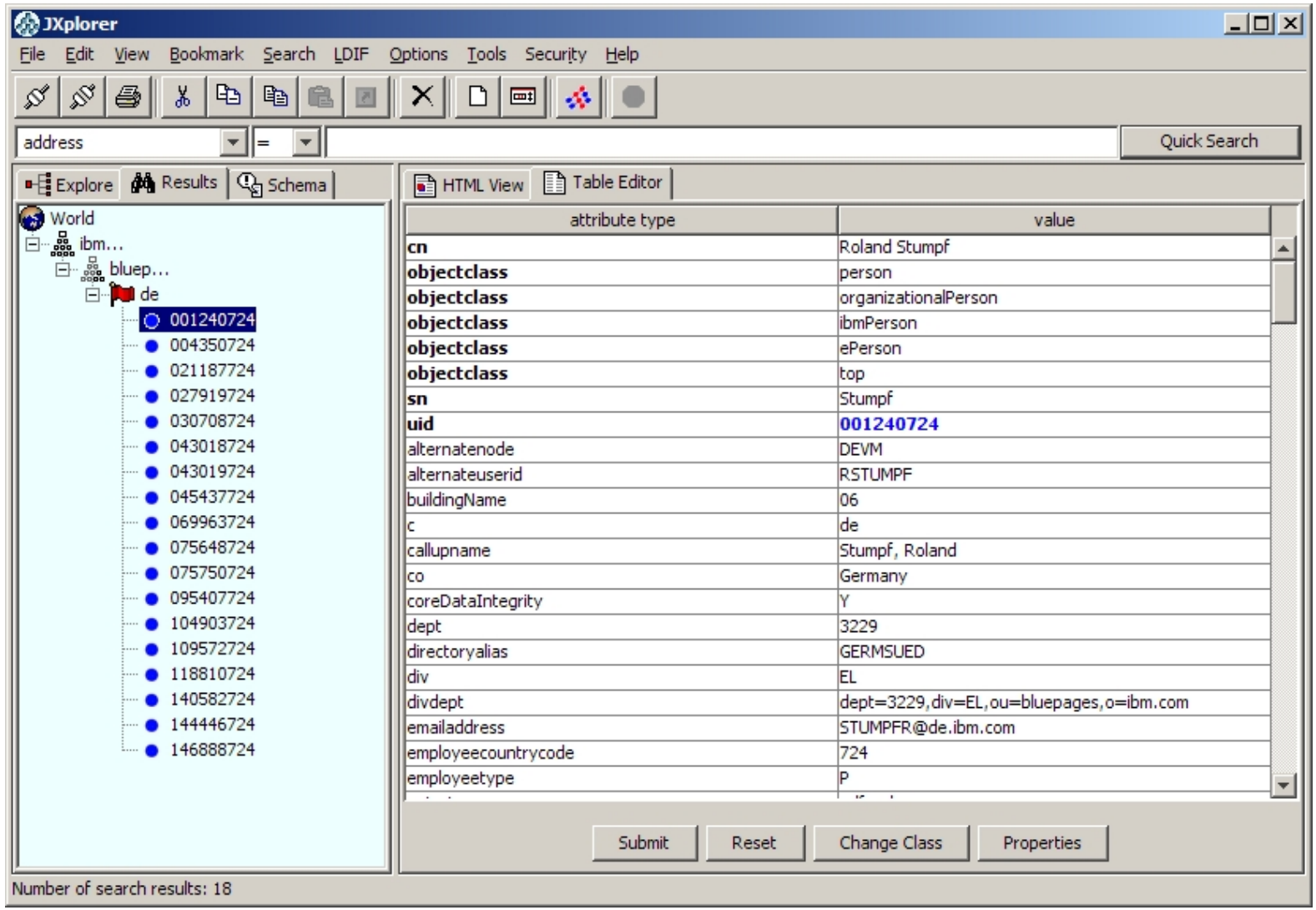


LDAP Example: IBM Bluepages

§ Search for all Entries with „dept=3229“



LDAP Example: IBM Bluepages



LDAP Servers (incomplete list)

- 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
- ....

- (And many more)

z/VSE V4.2 LDAP Signon Support

- LDAP Signon Support sits on top of any existing Security Manager
  - It can be used with the Basic Security Manager (BSM)
  - As well as with an External Security Manager (ESM)

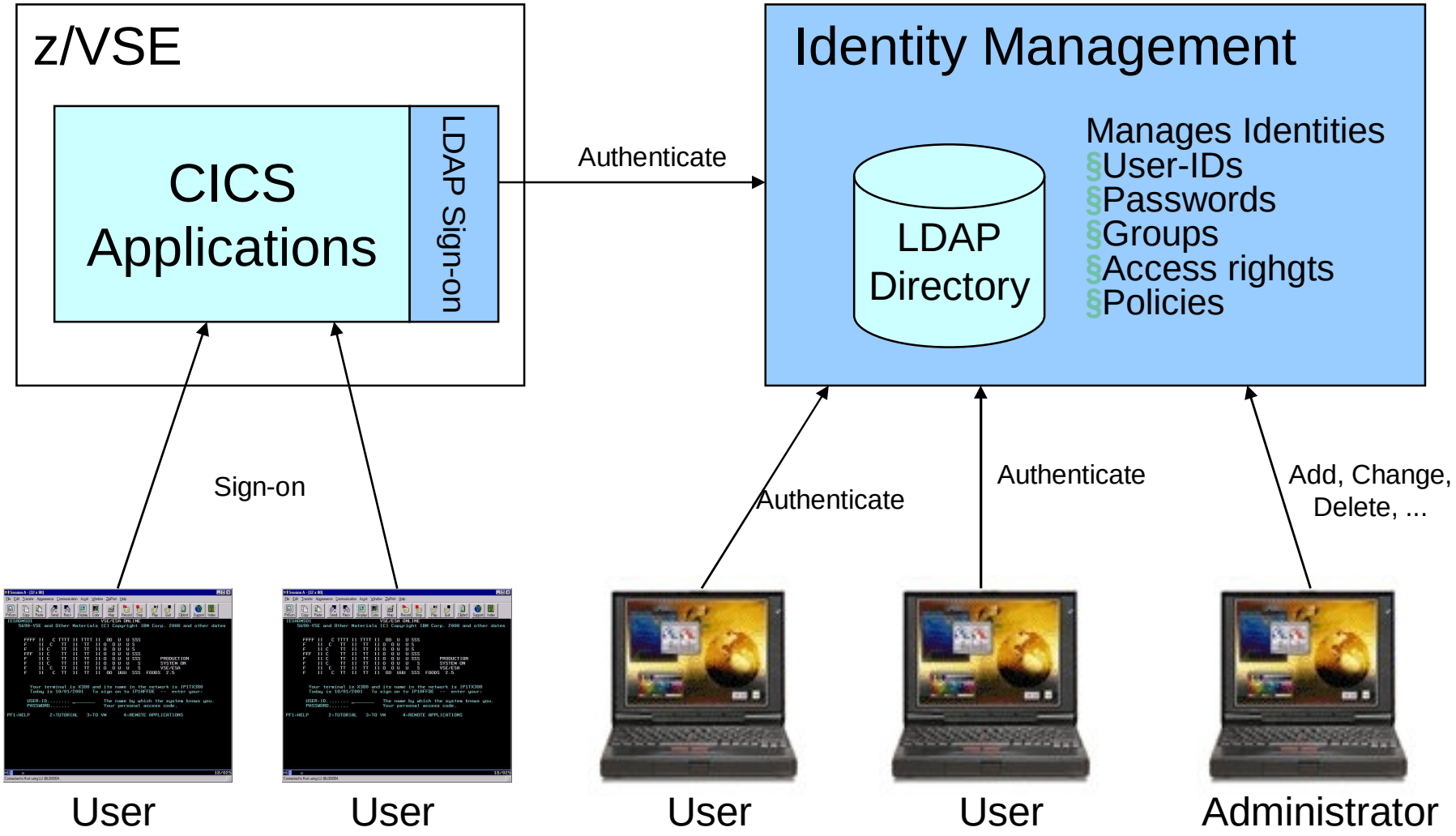
- Signon process (simplified):
  1. It first authenticates an user against a remote LDAP server
     - Via LDAP Bind and Search operations
  2. Then it maps the LDAP user to a short VSE user
     - Using a LDAP User Mapping File
  3. Finally passes the short VSE user and password to the existing signon process (BSM or ESM)

- Available for CICS signon (z/VSE V4.2) and Batch (z/VSE V4.3)

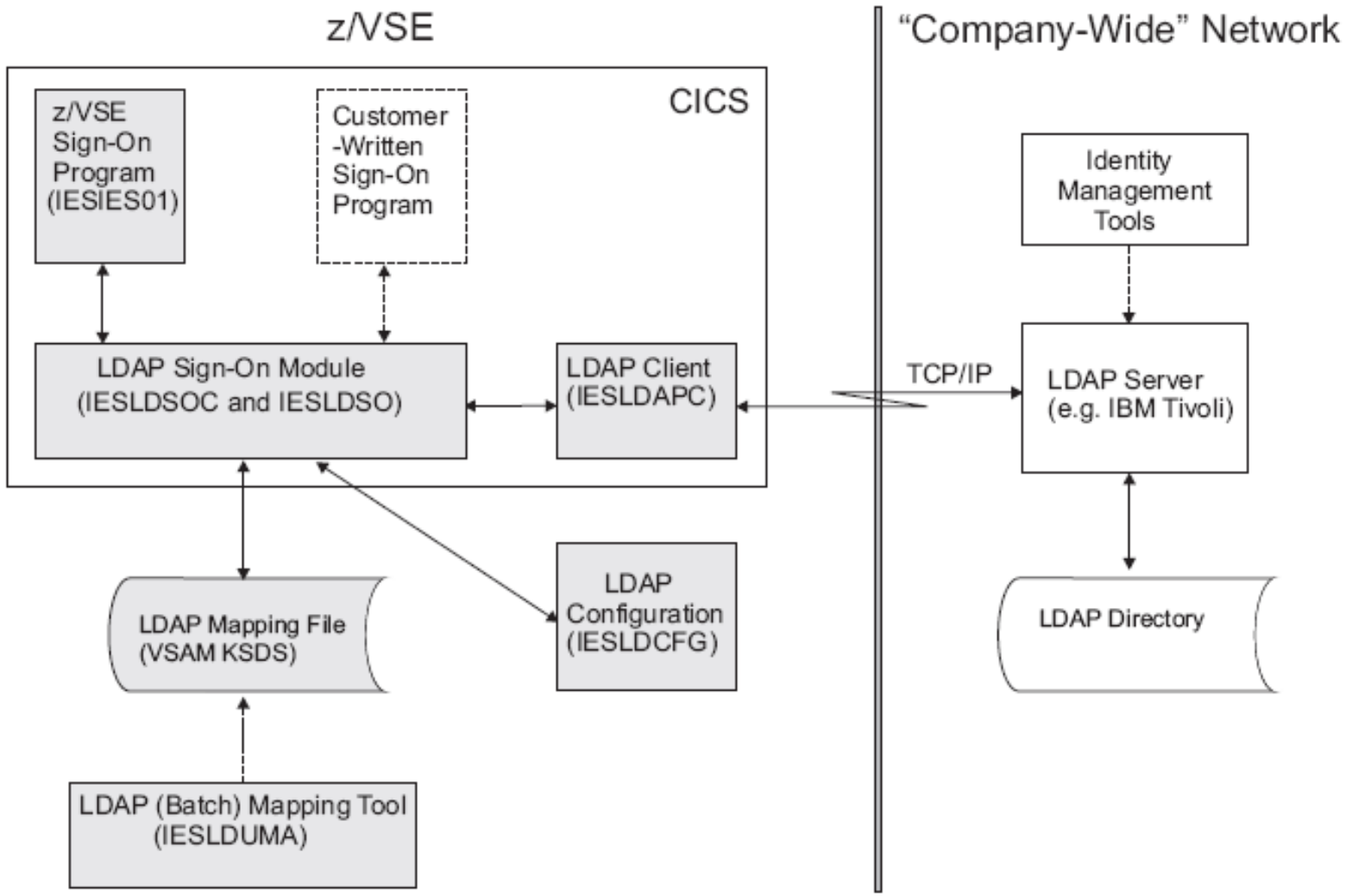
z/VSE V4.2 LDAP Signon Support

- Enables users to sign on z/VSE using a single, comprehensive, corporate-wide 'Identity Management' systems (i.e. IBM Tivoli Identity Manager, etc.)
- LDAP user-IDs and passwords can be up to 64 characters. Helps overcome VSE internal limits:
  - 4 character VSE/ICCF user-IDs
  - 4 and 8 character CICS user-IDs
  - up to 8 character Passwords
- LDAP sign on sits on top of existing z/VSE security manager (i.e. BSM, ESM, etc.)
- z/VSE LDAP client can work with common LDAP servers
  - IBM Tivoli Directory server
  - z/VM LDAP server (with optional RACF repository)
  - Microsoft Active Directory, OpenLDAP, Apache Directory server, Novell eDirectory, and many others.
- Potential benefits include improved protection, consistent access rules, ease of use for end-users

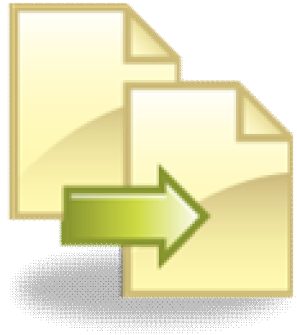
The big picture



z/VSE V4.2 LDAP Signon Support



LDAP User Mapping File



- VSAM KSDS file used to store the user-ID mappings
  - LDAP Users & Passwords: up to 64 characters
  - VSE Users & Passwords: up to 8 characters
- The LDAP mapping file contains:
  - Records containing user-IDs that are to be used for LDAP-authentication
    - Contain a mapping of a long-user-ID (used in the LDAP environment) to a short-user-ID (used in z/VSE)
    - These user-IDs are referred to as being LDAP-enabled.
  - Records containing user-IDs that are not used for LDAP-authentication (for example, the SYSA user-ID)
    - These user-IDs are referred to as being not LDAP-enabled, and these users can sign on to z/VSE even if the LDAP server is not operational.
- Maintained using batch tool IESLDUMA

LDAP Password cache

- Authentication against a remote LDAP server can be time consuming (requires network communication)
- When a user signs on multiple times within a short period of time, it is very unlikely that the LDAP password has changed
- If caching is enabled, a shortpath is used to authenticate a user
  - A password hash (SHA-256) of the last sucessfull signon attempt (LDAP bind) is stored in the User Mapping File
    - There is no way to recover the password from a hash
  - A subsequent signon request builds the password hash, and compares the hash against the stored hash
    - If it is the same, the user has entered the same password
  - A stored password hash has an expiration period. When it is over, a full LDAP signon (LDAP bind) is enforced

LDAP Configuration

- Per default, LDAP signon is not enabled.
- You need to create a configuration to enable LDAP signon support
  - Use Skeleton SKLDCFG in ICCF library 59
- Specifies (summary)
  - DLBL Name of LDAP User Mapping File (default: IESLDUM)
  - IPs or hostnames of one or multiple LDAP Servers
  - Settings for Authentication method (see next foils)
  - Settings for Cache usage and expiration
  - Settings for Secure Socket Layer (SSL)

LDAP Authentication Methods

- LDAP Authentication relies on the LDAP bind operation with distinguished name (DN) and password

- **Direct Authentication:**
  - The specified user-ID is used directly for the LDAP bind operation.
  - A pattern is used to build the distinguished name for the bind, e.g. „`cn=%u,dc=ibm,dc=com`“

- **Search Authentication:**
  - In case the specified user-ID cannot be used directly for bind.
  - Instead, a LDAP search operation is performed first using the attribute that is specified in the configuration (e.g. „email“).
  - An additional search filter can be specified to further limit the search result, e.g. „`dept=3229`“
  - The search result’s distinguished name is then used for the LDAP bind operation.

What‘s coverd by LDAP signon support and what‘s not covered?

As the name impiles, LDAP signon support only covers the signon process, but no ressource security.

Once a user is signed on, its associated VSE user-ID is used by z/VSE to check for permission to access ressources via BSM or ESM

Covered by LDAP signon support:

- Signon processing
- User-ID checking
- Password checking
- Password expiration (by LDAP server)
- Password complexity requirements
- Audit logging for signon (by LDAP server)

Covered by z/VSE‘s security (BSM/ESM)

- Ressource security
- Transaction security
- Batch security
- TCP/IP Security
- User groups
- Audit logging for VSE user-ID
- Audit logging for ressource access

Using your own CICS Sign-on program

- The Interactive Interface signon program (IESIES01) has been adapted to support LDAP authentication
  - If LDAP authentication is configured and enabled, it will automatically show longer fields for userid and password
- If you use your own sign-on program, you need to adapt it to use LDAP sign-on support:
  - Enlarge fields in screen (BMS map) for userid and password
  - Support case sensitive input
  - Call LDAP Sign-on Program IESLDSOC to perform LDAP authentication
    - Using EXEC CICS LINK with COMMAREA (see Admin Guide)
- Sample CICS Sign-on Program supporting LDAP is available for download:
  http://www.ibm.com/systems/z/os/zvse/downloads/samples.html#samplecode

New since z/VSE V4.3: LDAP Sign-on support for batch

§ ID statement or * $$ JOB specifies user id and password for a job

```
* $$ JOB JNM=MYJOB,...,SEC=(user,password)
```

or

```
// ID USER=user,PWD=password
```

§ User id and password are verified against (assumes SYS SEC=YES)

- DTSECTAB
- Security Manager (RACROUTE)

§ Subsystems (LIBR, VSAM, ...) uses this user id to verify access rights against DTSECTAB

§ Batch LDAP Sign-on Support can replace the ID statement for selected jobs:

Instead of

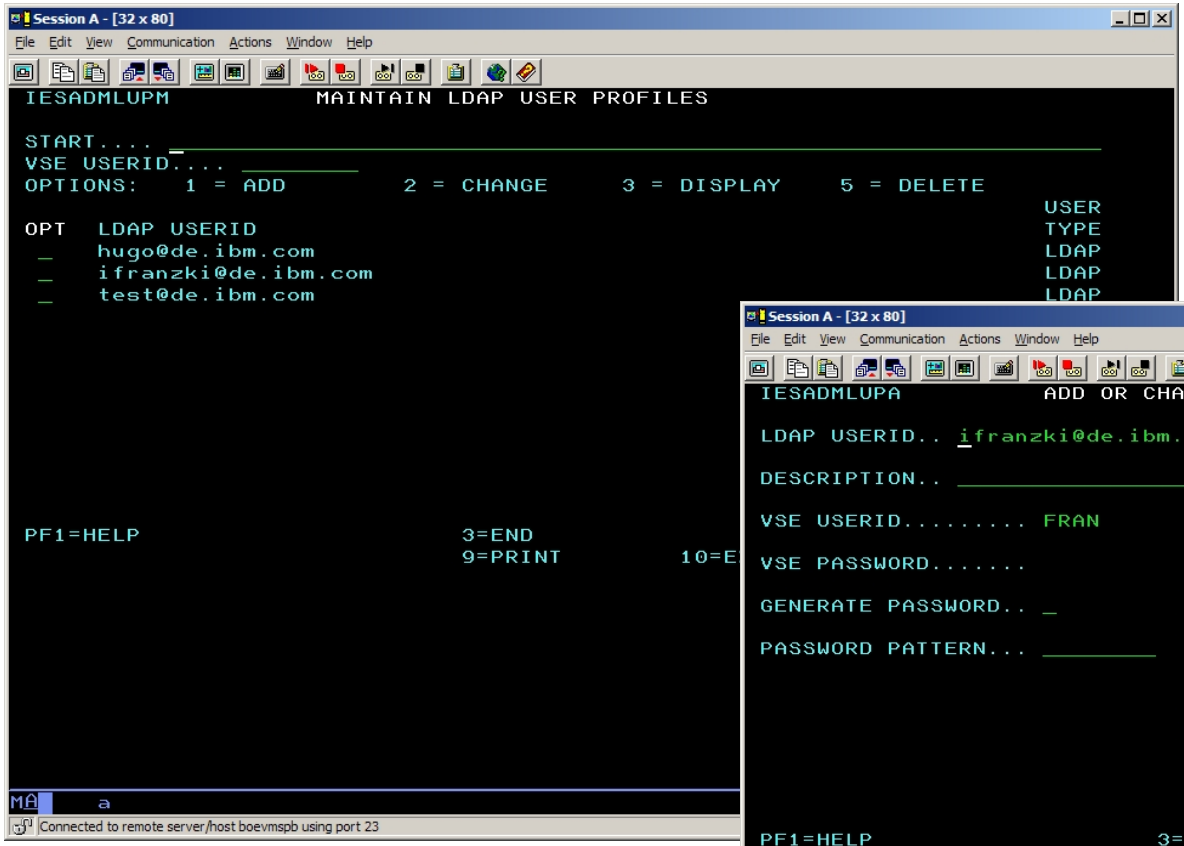
```
// ID USER=user,PWD=password
```

Use:

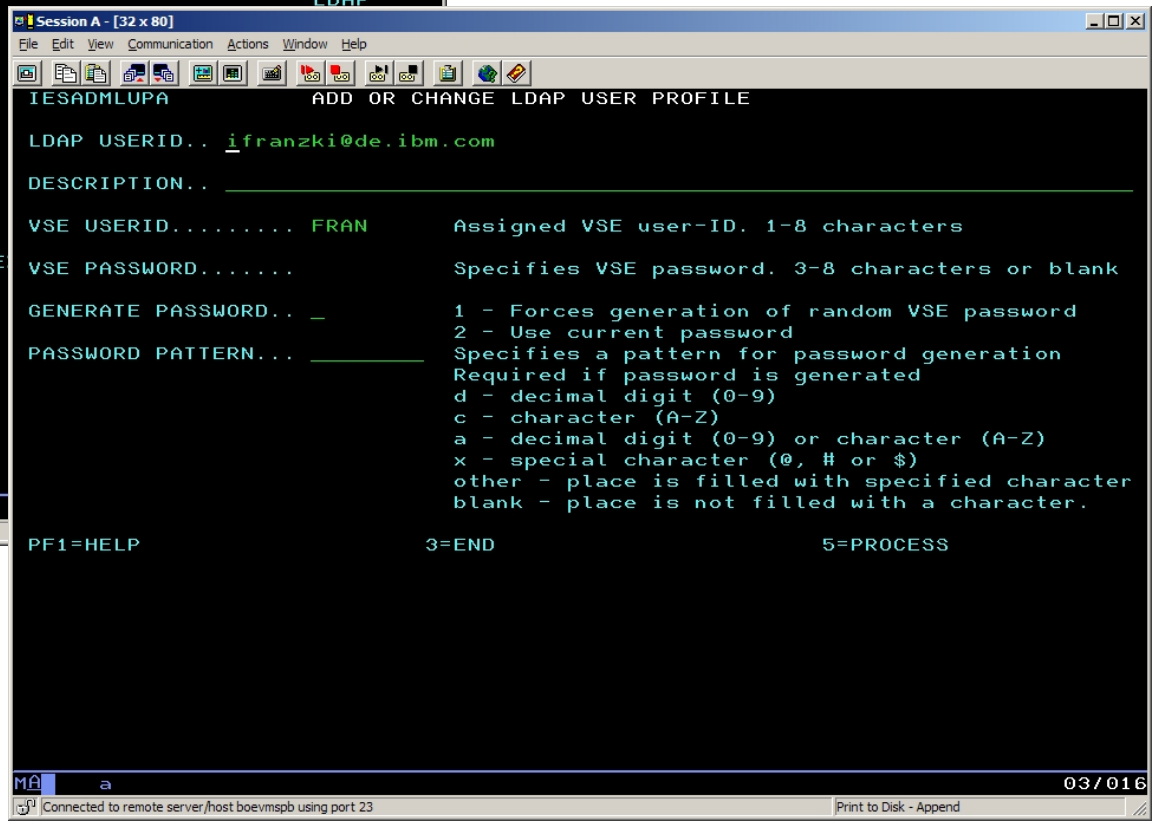
```
// EXEC IESLDSOB
USER=xxx...
PWD=xxx...
/*
```

ß this can be a long LDAP user ID
ß and the user's LDAP password

New since z/VSE V4.3: Interactive Interface Dialogs for LDAP users



ß SYSA fast path 217



Add or change an LDAP user à

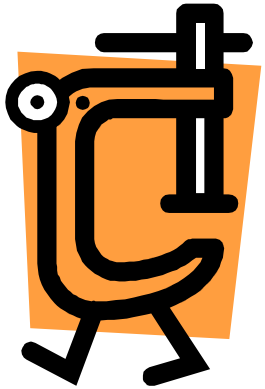
New: LDAP Query Callable Module

- The z/VSE LDAP Query Callable Module allows you to programmatically query an LDAP server from within your programs to retrieve attributes of an LDAP user
- You can either call the z/VSE LDAP Query Callable Module directly (i.e. via an COBOL external call), or via EXEC CICS LINK when running under CICS.
- The z/VSE LDAP Query Callable Module can be used on z/VSE 4.2 or later

```
01 LDGA-AREA.
  03 AREA-LENGTH PIC S9(9) BINARY.      <-- In: Length of the Area in Bytes
  03 USER-ID PIC X(64).                 <-- In: LDAP user ID to get attributes for
  03 SEARCH-FILTER PIC X(128).          <-- In: Additional Search filter or blanks
  03 RET-CODE PIC S9(9) BINARY.         <-- Out: Return code
  03 LDAP-CODE PIC S9(9) BINARY.        <-- Out: LDAP Return code
  03 ATTR-COUNT PIC S9(4) BINARY.       <-- In: Number of attr entries following
  03 ATTR-ENTRY OCCURS x TIMES.
    05 ATTR-NAME PIC X(64).             <-- In: Name of Attribute to get
    05 VALUE-LENGTH PIC S9(4) BINARY.   <-- In: Length of ATTR-VALUE
    05 VALUE-COUNT PIC S9(4) BINARY.    <-- In/out: Number of Values following
    05 VALUE-ENTRY OCCURS y TIMES.
      07 ATTR-VALUE PIC X(n).           <-- Out: Attribute Values(s).
                                             Length (n) must match the VALUE-LENGTH

01 IESLDGAB PIC X(8) VALUE 'IESLDGAB‘
…
Fill the parameter area here
…
CALL IESLDGAB USING BY REFERENCE LDGA-AREA.
```

LDAP Tools and Documentation



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

Questions ?