Vanguard Enterprise Security Expo

RACF and Security Update

Walt Farrell
z/OS Security Server Design
wfarrell@us.ibm.com

© 2004 IBM Corporation

Trademarks

- The following are trademarks or registered trademarks of the International Business Machines Corporation in the United States, other countries, or both:
  - IBM
  - CICS
  - AIX
  - DB2
  - RACF
  - z/OS, OS/390, MVS/ESA
  - OS/400
  - zSeries, pSeries, xSeries
  - eServer
- The following are trademarks or registered trademarks of other companies
  - UNIX
  - Microsoft, Windows, Windows NT
  - PKCS
  - RSA
- Other company, product or service names may be trademarks or service marks of others.

© 2004 IBM Corporation

z/OS v1R5 Updates

Heterogeneous Password Synchronization
RACF Dynamic Templates
Multilevel Security (MLS)
PKI Services
EIM Enhancements
What's Our Name Today?

© 2004 IBM Corporation

z/OS v1R6 Preview

RACF SECLABELAUDIT

RACF Dynamic Class Descriptor Table (CDT)

© 2004 IBM Corporation

Heterogeneous Password Synchronization

© 2004 IBM Corporation

What is it?

- **Challenge**
  - **Currently, RACF can receive password updates, but can not send local changes outbound (requires exits)**
- **Solution**
  - **z/OS Support for heterogeneous password synchronization solution provided by IBM Directory Integrator (IDI) 5.1.2**
  - Available 9/03 on z/OS Releases 3 and 4 via
    - OA03853 – RACF updates
    - OA03854 – SAF updates
    - OA03857 – LDAP updates
  - Same APARs available for R5 at R5 GA

© 2004 IBM Corporation

LDAP provides:

- Change log support for SDBM (RACF) backend
  - Enabled by activating new RACFEVNT class and defining NOTIFY.LDAP.USER profile
  - Change log entries created for changes to
    - a user's password, by any method
    - A user's revoke status (FLAG4 field), by any method
    - Other user fields (*) by the ADDUSER, ALTUSER, PASSWORD, and DELUSER commands
      - *exception: changes to group connection info not logged
  - Application changes made using RACROUTE or ICHEINTY not logged
  - Application can call R_Proxyserv to create log entry
- LDAP interface to retrieve RACF password envelope

© 2004 IBM Corporation

LDAP Change log entry contains

- Unique change log entry identifier
- Time and date of change
- Change type (add, modify, delete)
- Change initiator
- Change target

- Does not contain details of actual change (i.e. field names and values)
  - **Except**
    - **racfPassword:*ComeAndGetIt***

© 2004 IBM Corporation

RACF provides

- Creation of LDAP change log entry when a USER profile changes in RACF
- Retrievable user passwords stored in RACF
- R_admin (IRRSEQ00) interface to retrieve encrypted password envelope
- R_Proxyserv (IRRSPY00) interface for applications to create their own change log entries

© 2004 IBM Corporation

Password Enveloping

- New function which allows authorized applications to recover a user's clear-text password
- A key ring owned by the RACF subsystem contains certificates for password recipients
- LDAP change log entry can be created to log the password update and envelope creation
- Retrieval of envelope controlled by a FACILITY profile
  - IRR.RADMIN.EXTRACT.PWENV

© 2004 IBM Corporation

IDI provides

- Session 1793
- Event handler for polling z/OS LDAP change log
- Java method for decrypting the RACF password envelope
- Sample assembly line which detects a RACF password change, retrieves the password envelope, decrypts it, and applies the password to an entry in IBM Directory Server.

© 2004 IBM Corporation

Software Interdependencies

- RACF's LDAP notification is only meaningful if
  - SDBM back-end is configured in LDAP
  - PTF for OA03857 is applied
- Pre-reqs to RACF APAR:
  - UW89972
    - RACF SPE for UID/GID management (z/OS R3 only)
  - UW85562
    - Corrective service to RACDBULD/TB (z/OS R3 only)
  - UA03883/UA03884
    - Corrective service for IRRMPP00 (z/OS R3 and R4, respectively)
  - UW95429/UW95430
    - Corrective service for IRRPCOMP (z/OS R3 and R4, respectively)
  - UW84120 - System SSL (z/OS R3 only)
  - UW84121 - System SSL strong encryption (z/OS R3 only)

© 2004 IBM Corporation

Migration Considerations

- Use of the password enveloping function
  - Will utilize approx. 280 bytes of storage in the USER profile of eligible users
  - Requires the RASP to be a UNIX process
    - RASP initialization may complete later in the IPL sequence – after the OMVS kernel has initialized
    - In the event of an OMVS SHUTDOWN, password enveloping work must wait for OMVS restart
      - Traditional (non-UNIX) RASP work (e.g. RRSF) is not directly affected, but if enveloping uses up available RASP tasks, non-UNIX work will have to wait

© 2004 IBM Corporation

RACF Dynamic Templates

© 2004 IBM Corporation

Template Overview

RACF Templates:

- Map how profiles are written on the RACF database.
- Are updated to add new segments or fields for line items, either at a release boundary or in a PTF.
- Exist in three places:
  - The latest version shipped with RACF
  - The version on the database, written there by utility IRRMIN00
    - PARM=NEW initialize new database
    - PARM=UPDATE update the templates on existing database
  - The in-storage version
    - Built by RACF Initialization and used when accessing profiles
    - Can only be updated via IPL

© 2004 IBM Corporation

Issues

- Install a new release or PTF with template changes. If IRRMIN00 not run
  - **RE-IPL required**.

- IRRMIN00 requires correct IRRTEMP1 source. Latest level not obvious.
  - $/VERSION HRF7707
  - $/VERSION OA01234
  - **If wrong level used RE-IPL required**

- Apply a PTF with template changes
  - **RE-IPL required even if no mods in PTF require IPL**

- Could mistakenly run IRRMIN00 to initialize the database rather than update it, **wiping out database.**

Many consider these issues to be system outages and want IBM to prevent them.

© 2004 IBM Corporation

Dynamic Template Objectives Overview

Address the Issues:

- Have RACF Initialization build the in-storage templates automatically from the latest level whether or not IRRMIN00 PARM=UPDATE was run
- Have IRRMIN00 PARM=NEW and PARM=UPDATE automatically write the latest level of templates to the database.
- Do not allow IRRMIN00 PARM=UPDATE to down-level the templates on the database.
- Provide a means of dynamically ‘activating’ new templates by replacing the in-storage templates with the new templates.
- Do not allow an existing, active database to be newly initialized (from the system on which the database is active).

© 2004 IBM Corporation

New Template Support

The templates shipped with RACF:

- Are no longer shipped in source format as IRRTEMP1
- Are shipped as a module in compiled format as IRRTEMP2.
- Contain the release and apar level so RACF can determine the latest level of the templates:

  $/VERSION FMID/APAR# rrrrrrr.aaaaaaaa

  - `$/VERSION HRF7708 00000010.00000000`
  - `$/VERSION OA01234 00000010.00000010`
  - `$/VERSION OA01567 00000010.00000020`
  - `$/VERSION HRFxxxx 00000023.00000020`

- SET LIST operator command displays the in-storage template level and the dynamic parse level in effect on the system.

```
RACF STATUS INFORMATION:
    TEMPLATE VERSION          - HRF7708 00000010.00000000
    DYNAMIC PARSE VERSION     - HRF7708
```

© 2004 IBM Corporation

RACF Initialization

During IPL, RACF Initialization puts the templates in storage

- If the Master Primary database level is higher or the same as IRRTEMP2, it builds them from the database
- Otherwise, it builds the in-storage templates from IRRTEMP2 and issues message

```
ICH579E RACF TEMPLATES ON DATABASE ARE DOWNLEVEL:
    HRF7708 00000000.00000000; USING TEMPLATES AT LEVEL
    HRF7708 00000010.00000000 FROM IRRTEMP2.
    RUN IRRMIN00 PARM=UPDATE
```

© 2004 IBM Corporation

IRRMIN00

This database initialization utility now:

- Will no longer make use of the SYSTEMP data set, which customers typically pointed to SYS1.MODGEN(IRRTEMP1). Now it gets the templates from IRRTEMP2.
- Will fail PARM=NEW if the output database is active on the system where IRRMIN00 is invoked.
- Will not apply downlevel templates to a database.
- Will make templates active dynamically for the new PARM=ACTIVATE invocation when the templates on the active master primary database are a higher level than the in-storage templates.

© 2004 IBM Corporation

IRRMIN00

- PARM=NEW
  - formats a non-VSAM DASD data set as a RACF database. It divides the database into 4K blocks, or records, and initializes them
    - will now fail if invoked against an active database on the system where IRRMIN00 is invoked.
- PARM=UPDATE
  - Writes new templates to the database
    - Will fail if new templates are not at higher level than ones in database
- PARM=ACTIVATE
  - If the active master primary database has higher level templates than those in storage, they are copied to storage

© 2004 IBM Corporation

Multilevel Security (MLS)

More info in Session 1733

© 2004 IBM Corporation

What is Multilevel Security?

- A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories (Security Labels).
- Characteristics
  - Access controls
    - Mandatory Access Control (MAC)
    - Discretionary Access Control (DAC)
  - Accountability
    - Auditing
    - Identification and Authentication
  - Trusted Computing Base
    - Hardware
    - Software

Extends B1 support shipped with RACF 1.9

© 2004 IBM Corporation

Why Multilevel Security?

- Multilevel Security provides a way to isolate data from users.
- Aside from the obvious value to government agencies, it can be valuable to commercial customers.
  - Example
    - A service bureau can isolate what data certain customer can access

© 2004 IBM Corporation

Existing B1 support (before z/OS V1R5)

- RACF and other evaluated system components support Security Labels (a.k.a. SECLABELs)
  - Hierarchical definitions used to compartmentalize resources
- Special system-defined SECLABELs
  - **SYSNONE**
    - Combines the lowest Security Level and has NO Categories
  - **SYSLOW**
    - Combines the lowest Security Level and has NO Categories
  - **SYSHIGH**
    - Combines the highest Security Level and ALL Categories

© 2004 IBM Corporation

Existing B1 support

- Various options to control such functions as
  - Whether users and resources must have SECLABELs or not
  - Whether write-down is allowed or not (system wide option)
  - How auditing should be performed
- Authorization checking:
  - RACF compares resource SECLABEL with user's SECLABEL (MAC)
  - If that passes, RACF checks access list and universal access (DAC)
  - If that passes, RACF grants access

© 2004 IBM Corporation

z/OS V1R5 Multilevel Security enhancements

- New special system-defined SECLABEL
  - **SYSMULTI**
    - Used in cases where any classification of data could be "processed".
    - Compares as "equivalent" to any other defined SECLABEL for MAC decisions.
    - Intended for
      - Daemons and servers that can accept connections from users running at different classification levels (SECLABELs) and properly mediate data access
      - UNIX directories (often, not always, root in a file system) that can have subdirectories of different SECLABELs.
    - Generally should not be assigned to real users, nor to a server that is not designed to handle multiple SECLABELs.

© 2004 IBM Corporation

SECLABELs and MAC checking

- Three types of MAC checking
  - MAC
    - User's current SECLABEL dominates Resource's SECLABEL
  - RVRSMAC (Reverse MAC)
    - Resource's SECLABEL dominates User's current SECLABEL
  - EQUALMAC (Equal MAC)
    - User's current SECLABEL is equivalent to the Resource's SECLABEL.
- New operand EQUALMAC= added on the ICHERCDE macro
  - EQUALMAC=YES
    - The class requires SECLABEL equivalence

© 2004 IBM Corporation

SECLABELs for z/OS UNIX Processes and Sockets

- Currently TSO/E users:
  - Have the ability to select their current SECLABEL by specifying it on the logon panel, or they can use their default.
  - The value they enter is saved in the TSO segment and used as the default the next time they log on.
- This function has been modified to:
  - Handle workstations (allowing for both reading and writing)
  - Support the z/OS UNIX environment where a user may enter the system from a remote IP address using an application such as rlogin
  - Associate SECLABELs to IP addresses
    - IP V6 supported

© 2004 IBM Corporation

SECLABELs for z/OS UNIX Processes and Sockets

- Program access to SERVAUTH (enhancements to WHEN(PROGRAM) Conditional Access to the SERVAUTH class)
  - Allow appropriate use of PING and TRACEROUTE by a network administrator when multilevel security is enabled
    - Communications Server (TCP/IP) has the ability to restrict access to SERVAUTH resources to users running certain programs
- Allowed **ONLY** in a "**clean environment**" (like PADS – Program Access to Data Set)
  - All programs previously loaded must be program-controlled
  - Uncontrolled programs cannot be loaded into the environment after access has been granted to the SERVAUTH based on the program name

© 2004 IBM Corporation

SECLABELs for z/OS UNIX Files and Directories

- MAC protection for files and directories.
- RACF assigns user's SECLABEL to new file or directory when it is created.
- New SETROPTS option **MLFSOBJ/NOMLFSOBJ**
  - Requires that UNIX Files and Directories have SECLABELs. It is similar to the existing option MLACTIVE.

© 2004 IBM Corporation

SECLABELs for z/OS UNIX Interprocess Communications

- MAC protection for
  - Pipes
  - UNIX Sockets
- Communication can only occur between processes with equivalent SECLABELs (a.k.a. EQUALMAC).
  - With limited exceptions:
    - The resource or the accessor SECLABEL is SYSMULTI.
- SECLABEL cannot be changed later.
- Enabled via the new SETROPTS option **MLIPCOBJ/NOMLIPCOBJ**
  - Requires that UNIX Interprocess Communications functions (shared memory, message queues, semaphores) have SECLABELs. It is similar to the existing option MLACTIVE.

© 2004 IBM Corporation

SECLABEL By System

- Allows sharing of a RACF database between systems and isolate use of specified SECLABELs to specified systems
  - Not applicable to RACF defined SECLABELs
  - new SETROPTS option **SECLBYSYS/NOSECLBYSYS**

© 2004 IBM Corporation

SECLABEL By System

- Example:

  SECLABELs A, B, and C

  Systems SYS1 and SYS2

  - Administrator could define them as follows:
    - RDEF SECLABEL (A,B) … ADDMEM(SYS1)
    - RDEF SECLABEL C … ADDMEM(SYS2)
  - Then
    - Any attempt to access system SYS2 using SECLABEL A or B, or any attempt from SYS2 to access resources with SECLABEL A or B, would fail.

© 2004 IBM Corporation

Other enhancements

- Write-Down privilege
  - Allows the Security Administrator to authorize specific users to Write-Down (de-classify) when SETR MLS is in effect
    - R_writepriv callable service
    - RACPRIV command
- Name Hiding
  - Allows installations to prevent users from discovering data set names, file names, and directory names that they didn't already know
    - Enabled via the new SETROPTS option **MLNAMES/NOMLNAMES**
    - Needed only if the dataset or file names contain sensitive data

© 2004 IBM Corporation

PKI Services

More info in Session 1744

© 2004 IBM Corporation

PKI Services Overview

- Complete Certificate Authority (CA) package
  - Full certificate life cycle management
    - User request driven via customizable web pages
      - Browser or server certificates
    - Automatic or administrator approval process
      - Administered using same web interface
    - End user / administrator revocation process
  - Certificate validation service for z/OS applications

© 2004 IBM Corporation

Certificate Suspension

Temporarily revoke a certificate

- End user may suspend own browser certificate via web page
  - Requires SSL w/client auth
- PKI Administrator may suspend end user's certificate
- Only PKI Administer may resume end user's certificate

Some possible reasons to suspend a certificate

- On vacation
- Fear private key may have been compromised

Optional suspension "Grace Period"

- Time period after which suspended certificates are permanently revoked
- Configuration file directive

© 2004 IBM Corporation

Performance Updates

VSAM usage

- Each VSAM data set (ObjectStore and ICL) now has:
  - Status Alternate Index – For background tasks, e.g., creating CRLs
  - Requestor Alternate Index – For user queries based on requestor's name
    - Ensure requestor names are meaningful. Should be unique (e.g., e-mail address)
- VSAM Buffering
  - Use AMP= on DD cards

CRL Distribution Points

- Subdivision based on serial number

Replaced OCSF Crypto with System SSL

- In PKI Services daemon only
  - Certificate validation API (pkitp) still uses OCSF crypto
- No directives to control this. Should be an invisible change

ICL cleanup

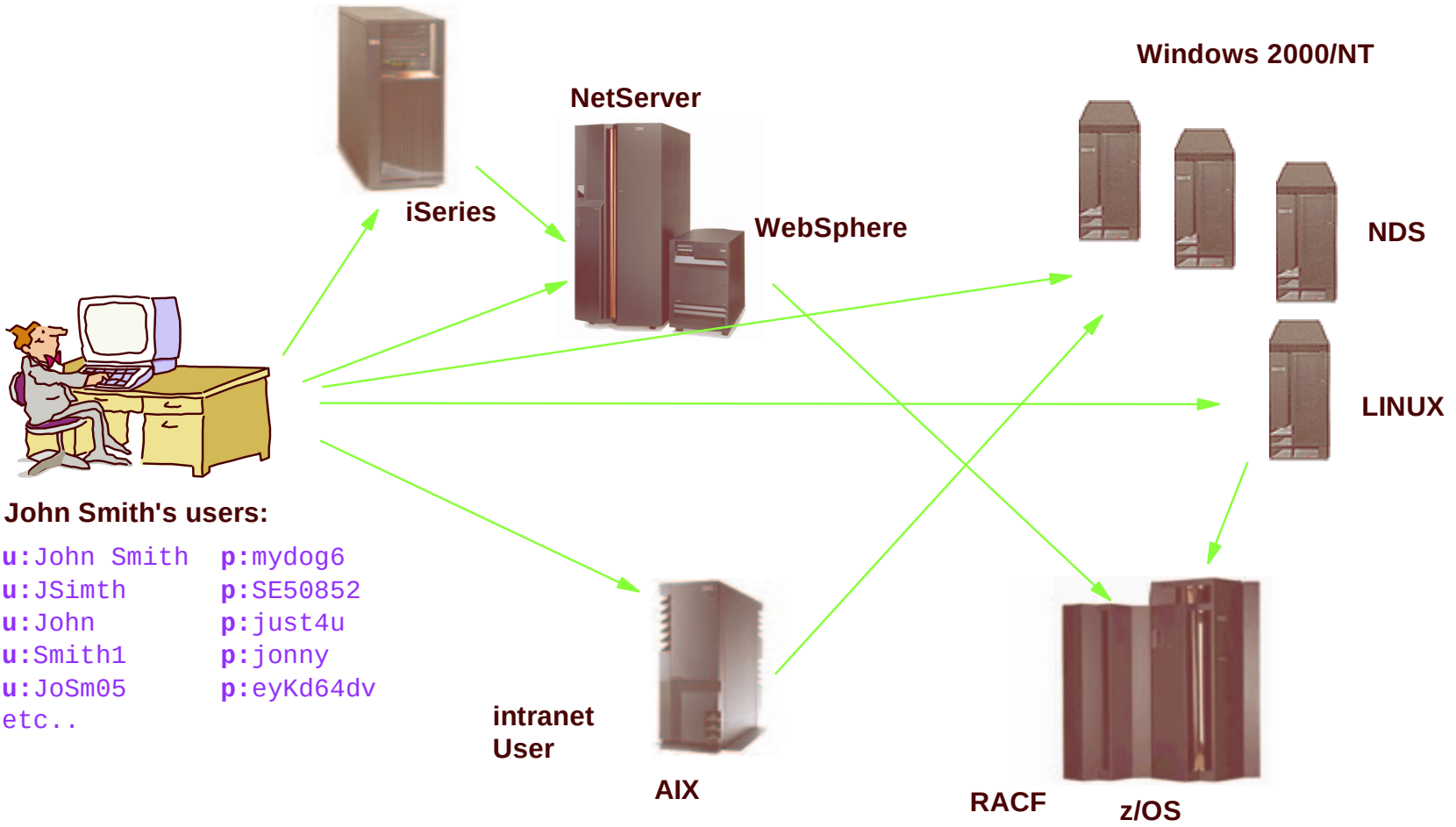
- Option to remove expired certificate from the ICL after a given time period

© 2004 IBM Corporation

EIM Updates

© 2004 IBM Corporation

Typical Environment Today



© 2004 IBM Corporation

Enterprise Identity Mapping Goals

- Accept the fact that multiple registries (IBM and non-IBM) will exist in the enterprise
- Make it easy to associate a user's multiple identities in the enterprise and to manage those associations
- Use IBM's platform breadth of software offerings to differentiate eServer platforms while providing a complete solution for heterogeneous environments
- Develop this in such a way that it can be extended to other facets of cross-platform management

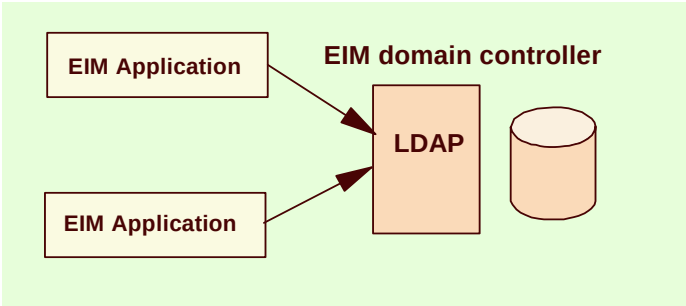
© 2004 IBM Corporation

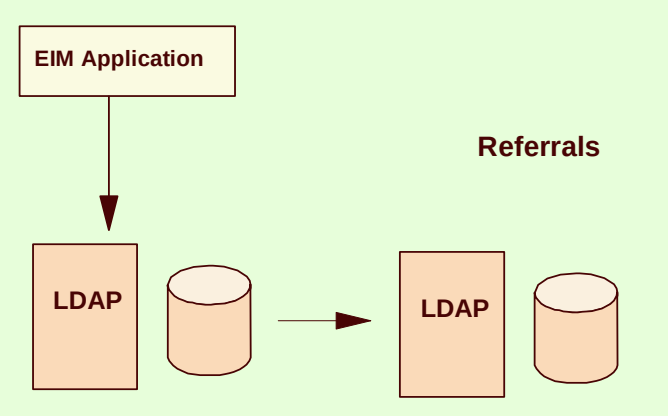
eServer EIM Support

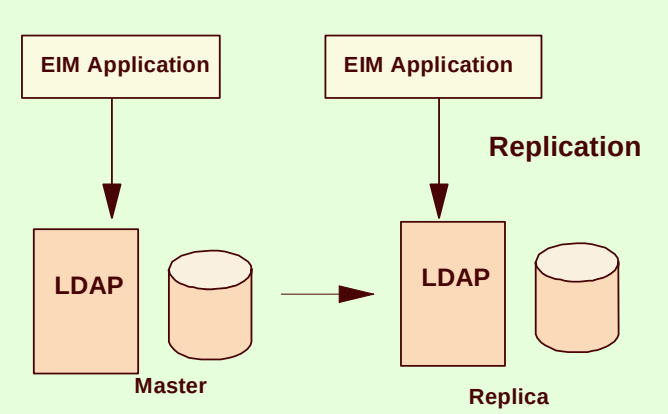
- EIM domain controllers
  - z/OS V1R4 LDAP + PTF UW92346
  - OS/400 V5R2
- EIM client APIs
  - z/OS V1R4 Security Server EIM SPE OW57137 or z/OS V1R5 Integrated Security Services EIM
  - OS/400 V5R2
  - AIX V5.2
  - Linux (x86 architecture, download from IBM website)
- EIM administration tools
  - z/OS V1R4 Security Server EIM eimadmin utility
  - OS/400 V5R2 Operations Navigator

© 2004 IBM Corporation

Basic EIM Configurations







© 2004 IBM Corporation

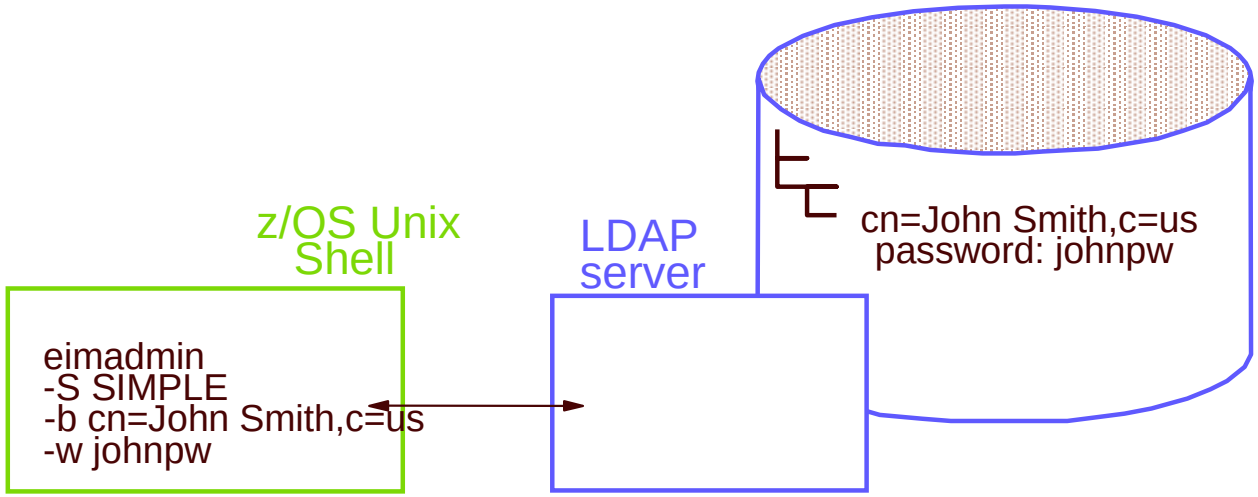
z/OS V1R5 EIM Authentication

- Supported binds to EIM domain controller
  - Simple
  - Simple with CRAM-MD5 password protection
  - External (digital certificates)
  - GSSAPI (Kerberos)

- Secure sessions to LDAP server supported by both APIs and eimadmin
  - Previously only APIs

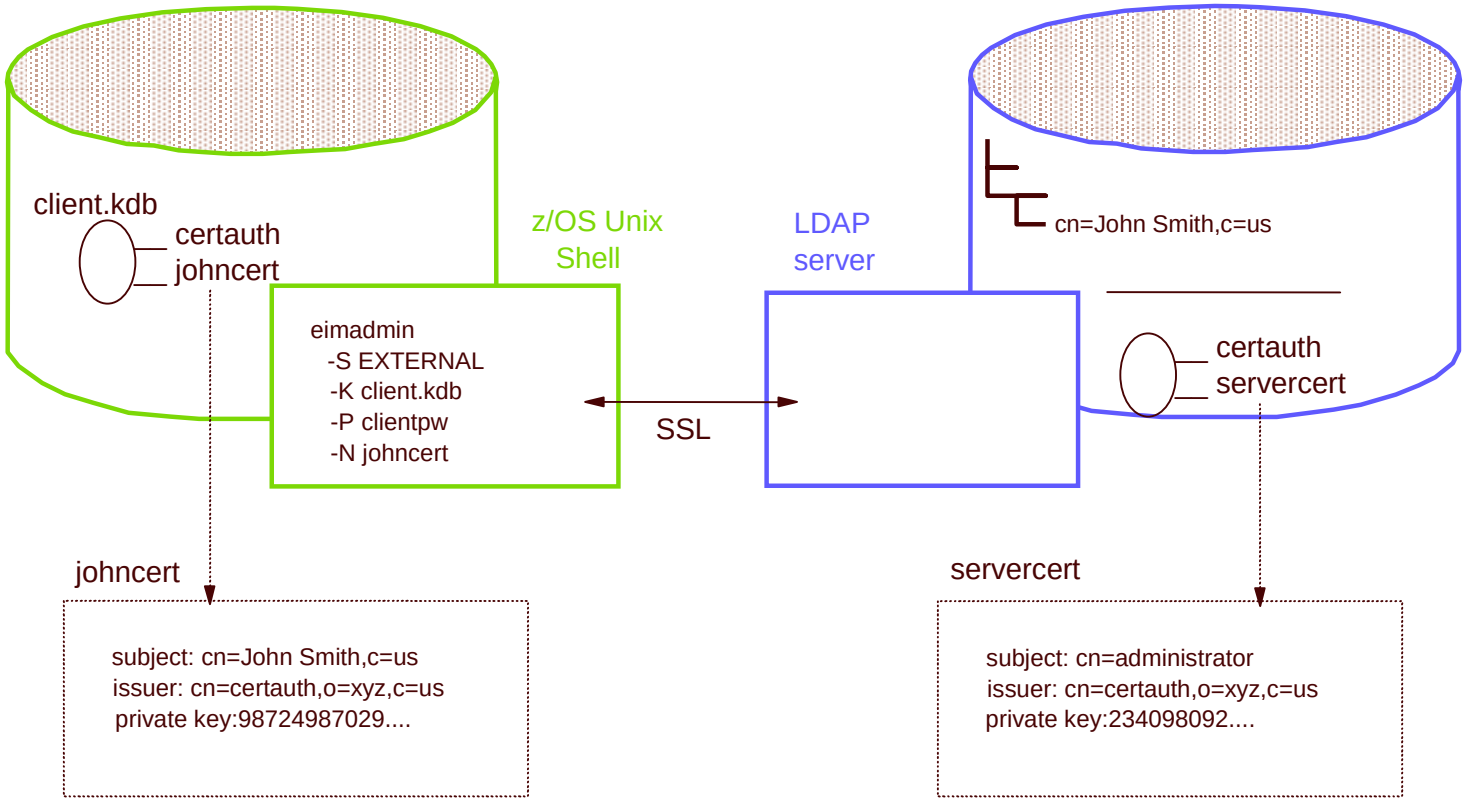
© 2004 IBM Corporation

Simple Authentication



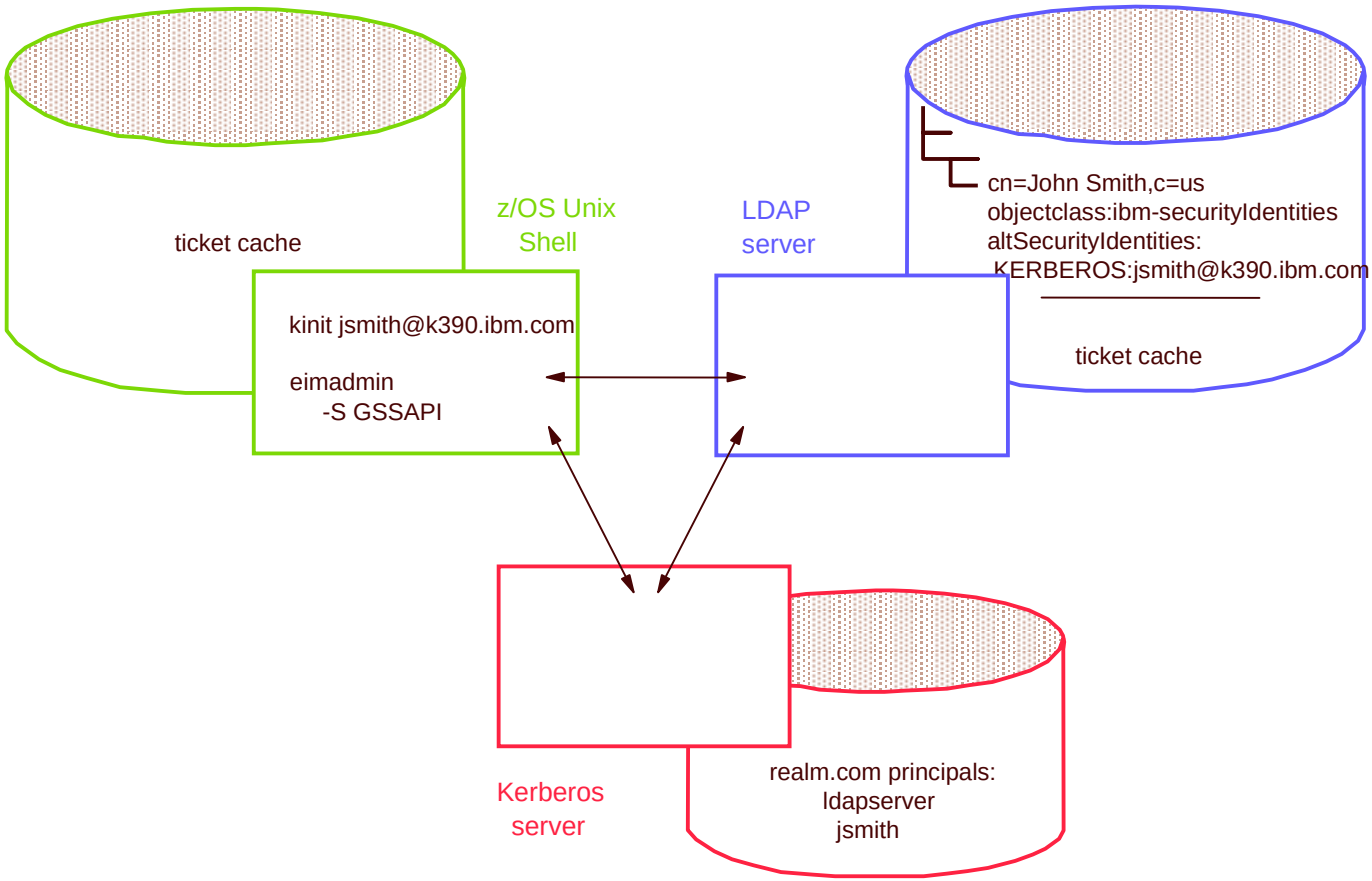
© 2004 IBM Corporation

Digital Certificate Authentication



© 2004 IBM Corporation

Kerberos Authentication



© 2004 IBM Corporation

What's Our Name Today?

- It's a trick question: z/OS Security Server
- However, the z/OS Security Server is ONLY RACF now.
- New Integrated Security Services:
  - DCE
  - Open Cryptographic Enhanced Plug-ins (OCEP)
  - LDAP Server
  - Firewall Technologies
  - Network Authentication Service
- Cryptographic Services:
  - ICSF, PKI, and System SSL

© 2004 IBM Corporation

What we've discussed

- Enhancements made in R5
  - Heterogeneous Password Synchronization
  - Dynamic Templates
  - Multilevel Security
  - PKI Services Updates
  - EIM Updates
- Packaging/Naming Change

© 2004 IBM Corporation

z/OS V1R6 Preview

- RACF SECLABELAUDIT enhancements
  - Function: Enable auditing based on the AUDIT specifications in a SECLABEL profile
  - Pre-V1R6: Applies only to SECLABEL associated with a resource profile
  - V1R6: Also applies to SECLABEL associated with User.
  - Example: JOE reads data set ‘ABC.DATA’. JOE has SECLABEL S1, ABC.DATA has SECLABEL S2. If either S1 or S2 specifies appropriate auditing, RACF will create an audit record.

© 2004 IBM Corporation

z/OS V1R6 Preview

- RACF Dynamic Class Descriptor Table (CDT)
  - Function: Allow customers to add or delete RACF classes without
    - Assembling / Link-editing ICHRRCDE
    - IPL
    - Updating RACF Router Table

© 2004 IBM Corporation

References

- Security Server Manuals:
  - RACF Command Language Reference (SC28-1919)
  - RACF Security Administrator's Guide (SC28-1915)
  - RACF Callable Services Guide (SC28-1921)
  - RACF Messages and Codes ((SA22-7686)
  - RACF System Programmers Guide (SA22-7681)
  - RACF Diagnosis Guide (GA22-7689)
  - RACF Macros and Interfaces (SA22-7682)
  - RACF Migration Guide (GA22-7690)
  - EIM Guide and Reference (SA22-7875)
  - LDAP Administration and Use (SC24-5923)
  - OCEP Application Programming (SC24-5925)
- z/OS manuals
  - Planning for Multilevel security (GA22-7509)
- PKI Services web site and manual
  - http://www-1.ibm.com/servers/eserver/zseries/zos/pki
  - PKI Services Guide and Reference (SA22-7693)
- Cryptographic Services
  - OCSF Service Provider Developer's Guide and Reference (SC24-5900)
  - ICSF Administrator's Guide (SA22-7521)
  - System SSL Programming (SC24-5901)
- IBM HTTP Server Manuals:
  - Planning, Installing, and Using (SC31-8690)
- Other Sources:
  - RACF – http://www.ibm.com/servers/eserver/zseries/zos/racf
  - PKIX - http://www.ietf.org/html.charters/pkix-charter.html
  - Identrus – http://www.identrus.com
  - Globus Project – http://www.globus.org
  - IBM Grid Corner – http://www-1.ibm.com/grid/

© 2004 IBM Corporation

© 2004 IBM Corporation