

IBM WebSphere
Software



WebSphere Application Server for z/OS and OS/390

WebSphere Application Server V5 and V6 Security Session F7/F8

Trademarks

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

AIX*
CICS*
e-business logo*
IBM*
IBM eServer
IBM logo*
IMS
OS/390*
RACF*
S/390*
WebSphere*
z/OS*
zSeries*
* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

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.

* 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.

Agenda

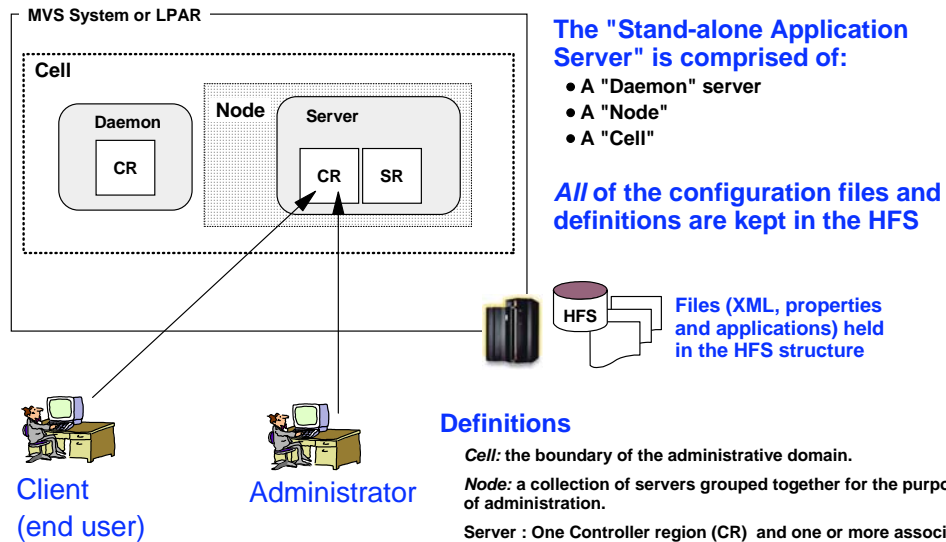


- Overview WebSphere Application Server security.
- Review the RACF definitions needed.
- Describe Global Security and how to activate it.

V5 or V6 "Stand-alone Application Server"



This is the starting point after installing WebSphere for z/OS Version 5



The "Stand-alone Application Server" is comprised of:

- A "Daemon" server
- A "Node"
- A "Cell"

All of the configuration files and definitions are kept in the HFS

Definitions

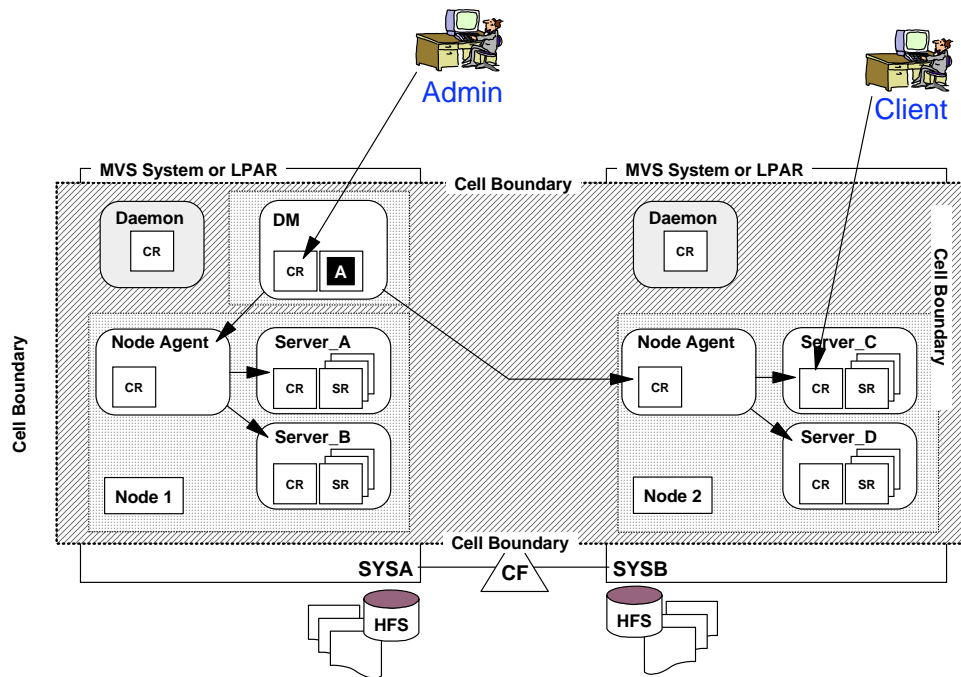
Cell: the boundary of the administrative domain.

Node: a collection of servers grouped together for the purposes of administration.

Server : One Controller region (CR) and one or more associated Servant regions (SR) . .

Daemon: the location service daemon. One is required per cell per system or LPAR.

V5 or V6 Network Deployment Cell



Building a WebSphere Cell



- ▶ A WebSphere cell is too complex to build by hand. The WebSphere developers provided ISPF scripts to generate the commands and jobs needed to build a cell.
- ▶ The WebSphere Customization ISPF scripts also generate most/all of the RACF commands necessary.
- ▶ You may be asked to run these commands.
- ▶ We'll discuss the Customization Scripts and the RACF commands they produce.
- ▶ Start the Scripts with the TSO command:
 - `exec 'WAS602.WAS.SBBOCLIB(BBOWSTRY)'`
 - You might use a different HLQ than this example.

Customization Panel Main Menu



- WebSphere V6 ISPF scripts are better organized than V5, but have the same info.
- When building a cell, start with step 1, Configure a security domain.

```
----- WebSphere Application Server for z/OS Customization -----
Option ==>                               Appl: VG

Use this dialog to create WebSphere Application Server for z/OS
cells and nodes. Specify an option and press Enter.

1  Configure a security domain.
2  Create stand-alone Application Server nodes. You must complete
   Option 1 before starting this option.
3  Create Network Deployment cells and nodes. You must complete
   Option 1 before starting this option.
4  Migrate V5.x Nodes to V6 Nodes.
```

Configure Security Domain



- We'll pick option 2, Define variables.

```
----- WebSphere Application Server for z/OS Customization -----
Option ==>                               Appl: VG

Configure Security Domain

Use this dialog to define variables and generate customization
jobs for your installation. Specify an option and press Enter.

High level qualifier for product data sets: WAS602.WAS

1  Allocate target data sets. The data sets will contain the
   customization jobs and data generated by the dialog.
2  Define variables. Define your installation-specific information for
   customization.
3  Save security domain variables. Save your security domain configuration
   variables in a data set for later use.
4  Generate customization jobs. Validate your customization variables
   and generate jobs and instructions.
5  View instructions. View the generated customization instructions.

Options for WebSphere Application Server for z/OS Customization Variables
L  Load security domain variables. Load your security domain configuration
   variables from a data set.
```

Step 1: Configure Security domain (1 of 2)



- Here we specify the security domain identifier, as well as other security related info.

```
----- WebSphere Application Server for z/OS Customization -----
Option ==>
Security Domain Configuration (1 of 2)

Specify the following to customize the security domain to be selected
when configuring one or more servers or cells, then press Enter
to continue.

Use security domain identifier in RACF definitions: N
Security domain identifier.....:

WebSphere Application Server Configuration Group Information
Group....: WSCFG1          GID...: 2500

WebSphere Application Server Administrator Information
User ID...: WSADMIN       UID...: 2403
Password.: WSADMIN

WebSphere Application Server Unauthenticated User
User ID...: WSGUEST       UID...: 2402
Group....: WSCLGP        GID...: 2502

WebSphere Application Server Asynchronous Administration Task
User ID...: WSADMSH       UID...: 2504

WebSphere Application Server Servant Group Information
Group....: WSSR1         GID...: 2501

Configure for local OS security registry.....: Y
```

What's a Security Domain?



- **A security domain provides cell-level granularity of security permissions.**
 - Similar in concept to SECPRFX used in CICS RACF security.
 - A prefix unique to this cell.
 - Provides cell-level granularity of roles.
 - Different administrators can be assigned to test and production.
 - Roles are managed using profiles in the EJBROLE class.
 - More detail on this in a few foils....
- **Other notes:**
 - 'Configure for local OS security registry'
 - 'Y' means you want to use RACF, 'N' means LDAP or something else.
 - Defaults aren't always helpful.
 - 'N' is the default for choice of security domain.

Step 1: Configure Security domain (2 of 2)



- More security-related values that affect the operation of the cell.

```
----- WebSphere Application Server for z/OS Customization -----
Option ==>
Security Domain Configuration (2 of 2)

Specify the following to customize the security domain to be selected
when configuring one or more servers or cells, then press Enter
to continue.

SSL Customization

Certificate authority keylabel.....: WebSphereCA
Generate certificate authority (CA) certificate: Y
Expiration date for CA authority: 2010/12/31
Default RACF keyring name.....: WASKeyring
Enable SSL on location service daemon: N

Additional z/OS Security Customization Options
Generate default RACF realm name: N
Default RACF realm name ....: WSCPLEX

Use SAF EJBROLE profiles to enforce J2EE roles: N

Enable SAF authentication using LTPA or ICSF login tokens: Y

WebSphere Application Server user ID home directory:
/var/WebSphere/home
```

Step 1: Configure Security domain (2 of 2)



- **Notes on Configure Security domain (2 of 2)**
 - WebSphere generates certs for the servers in the cell. Here you specify the details of the CERTAUTH certificate to use.
 - Keyrings will be created for the servers. Specify the keyring name.
 - The RACF Realm name is your sysplex name by default.
 - 'Use SAF EJBROLE profiles to enforce J2EE roles'
 - 'Y' means WebSphere will use RACF for authorization decisions.
 - 'N' means that it will use WebSphere bindings, not RACF.
 - So no EJBROLE profiles will be generated by the customization jobs.
 - Note that the default value is 'N'.
 - 'Enable SAF authentication using LTPA or ICSF login tokens'
 - 'Y' enables single signon in WebSphere after SAF authentication.
 - 'N' means single signon is not enabled.

Output of Customization Scripts



- **The jobs produced by the Customization scripts do various things:**
 - ▶ Build the file system used by WebSphere.
 - ▶ Build many control files used by WebSphere
 - Control statements for WebSphere are usually XML.
 - ▶ Build JCL for starting the various WebSphere regions.
 - ▶ **Build RACF commands for defining the cell.**
 - The book recommends you look them over before you run them.
 - As if you'd trust RACF commands generated by someone else....
 - **The jobs produced by the Customization steps go into the .CNTL library.**
 - **These jobs execute commands which are stored in members in the .DATA library.**
-

Output of Customization Scripts (V6.0.2)



- **These Customization Steps produce RACF commands:**
 - ▶ **Step 1: Configure security domain**
 - Creates the BBOSBRAJ job in the .CNTL library, which when run creates RACF commands in the BBOSBRAK member in the .DATA library. These are executed by the BBOSBRAK job in the .CNTL library.
 - ▶ **Step 2: Create stand-alone Application Server nodes**
 - Creates the BBOCBRAJ job in the .CNTL library, which when run creates RACF commands in the BBOWBRAK member in the .DATA library. These are executed by the BBOCBRAK job in the .CNTL library.
 - ▶ **Step 3: Create Network Deployment cells and nodes.**
 - Creates the BBODBRAJ job in the .CNTL library, which when run creates RACF commands in the BBODBRAK member in the .DATA library. These are executed by the BBODBRAK job in the .CNTL library.
 - ▶ These are commonly known as the BRAK jobs
-

Output of Customization Scripts



- **The BRAK jobs contain RACF commands to create:**
 - ▶ Userids and groups used by the cell.
 - ▶ STARTED class profiles
 - ▶ CBIND class profiles
 - ▶ SERVER class profiles
 - ▶ EJBROLE class profiles
 - ▶ APPL class profile (optional)
 - ▶ PKTDATA class profile (optional)
 - ▶ Keyrings and Digital Certificates
 - ▶ FACILITY class profiles

 - **We'll review these in the following charts.**
-

Users and Groups



- **For a Stand-alone app server configuration:**
 - ▶ Userids are created for the:
 - Daemon region
 - Application Server Controller region
 - Application Server Controller Adjunct region
 - Application Server Servant region
 - Administrative userid
 - Owns the files used by the server, has initial administrative authority over the cell.
 - Asynchronous Admin Task userid
 - A 'protected' userid under which some administration tasks run.
 - Unauthenticated guest userid
 - A 'restricted' userid used for access to applications that do not require authentication.
-

- **For a ND configuration:**
 - ▶ Users are created for the:
 - Daemon region
 - Application Server Controller region
 - Application Server Controller Adjunct region
 - Application Server Servant region
 - Deployment Manager Controller region
 - Deployment Manager Servant region
 - Node Agent
 - Administrative userid
 - Asynchronous Admin Task userid
 - Unauthenticated guest userid
-

- **For a Stand-alone app server or ND configuration:**
 - ▶ Groups are created:
 - The 'config' group
 - The Daemon, Application Server Controller region, Application Server Servant region, Administrative userid and Asynchronous Admin Task userid belong to this group.
 - In an ND configuration, the DM controller region, DM servant region and Node Agent regions also belong to the 'config' group.
 - The 'server' group
 - The Application Server Servant region, the DM servant region and Control Region Adjunct belong to this group.
 - The 'guest' group
 - The unauthenticated guest userid belongs to this group.
-

Users and Groups



■ My Recommendation:

- ▶ All the Servant Regions run under one RACF userid.
 - Application Server servant regions, DM servant region.
 - Applications run in these regions.
 - ▶ All the 'WebSphere Plumbing' regions run under another RACF userid.
 - The Daemon, Application Server Controller regions, DM Controller region, NA regions, Application Server Controller Adjunct regions.
 - Application code doesn't run in these regions.
 - Some run authorized code.
 - They all need access to keyrings and (except the Adjunct) certificates for SSL.
 - ◆ They can share a keyring and cert. More on this later...
 - ▶ If you use a different userid for each started task, things will get very complicated, very fast.
-

STARTED Class Profiles



- **STARTED class profiles are generated to assign userids to the various WebSphere regions.**
 - **Regions include:**
 - ▶ Daemon
 - ▶ Deployment Manager (controller and servant)
 - ▶ Node Agent
 - ▶ Application Server(s) (controller, servant, adjunct)
-

CBIND Class Profiles



- **CBIND profiles control access to WebSphere servers and to objects in the servers, from Java application clients and other WebSphere servers.**
 - **Access to Servers**
 - ▶ CB.CBIND.<cluster>
 - ▶ CB.CBIND.<security domain>.<cluster>
 - **Access to objects within servers**
 - ▶ CB.<cluster>
 - ▶ CB.<security domain>.<cluster>
-

SERVER Class Profiles



- **SERVER class profiles control whether a servant region can call authorized routines in the associated controller region.**
 - **Access to Controller using Static Application Env.**
 - ▶ CB.<server>.<cluster>
 - ▶ CB.<security domain>.<server>.<cluster>
 - **Access to Controller using Dynamic Application Env.**
 - ▶ CB.<server>.<cluster>.<cell>
-

APPL Class Profile



- An APPL class profile controls whether an authenticated user can use any applications in the cell.
 - If a Security Domain is specified, the APPL class profile name will be the Security Domain name.
 - If Security Domain is not specified, the APPL class profile name will be CBS390.
-

PKTDATA Class Profile



- A PKTDATA class profile indicates the PassTicket key value used by servers in the cell when handling PassTickets.
 - If a Security Domain is specified, the PKTDATA profile name will be the Security Domain name.
 - If no Security Domain is specified, the PKTDATA profile name will be CBS390.
-

EJBROLE Class Profiles



- **Used for J2EE Role-Based Authorization, EJBROLE class profiles control access to applications in a cell.**
 - Access to Servlets or EJB methods is based upon the 'role' (job title, function, etc.) of the user or caller.
 - Roles are associated with Servlets or EJBs at assembly time.
 - The Role needed to use a Servlet or EJB method is named in the application's .ear file.
 - Which users and groups have which Roles is determined by RACF, using profiles in the EJBROLE class.
 - If a user is in the access list of an EJBROLE profile, he has that role.
 - If a group is in the access list of an EJBROLE profile, users in that group have that role.
 - If the EJBROLE profile has UACC of READ, all users have that role.
 - Roles are managed through RACF.
 - Works the same way in WebSphere V4, V5 and V6 for z/OS.
-

How Does the Security Domain Affect EJBROLE profile names?



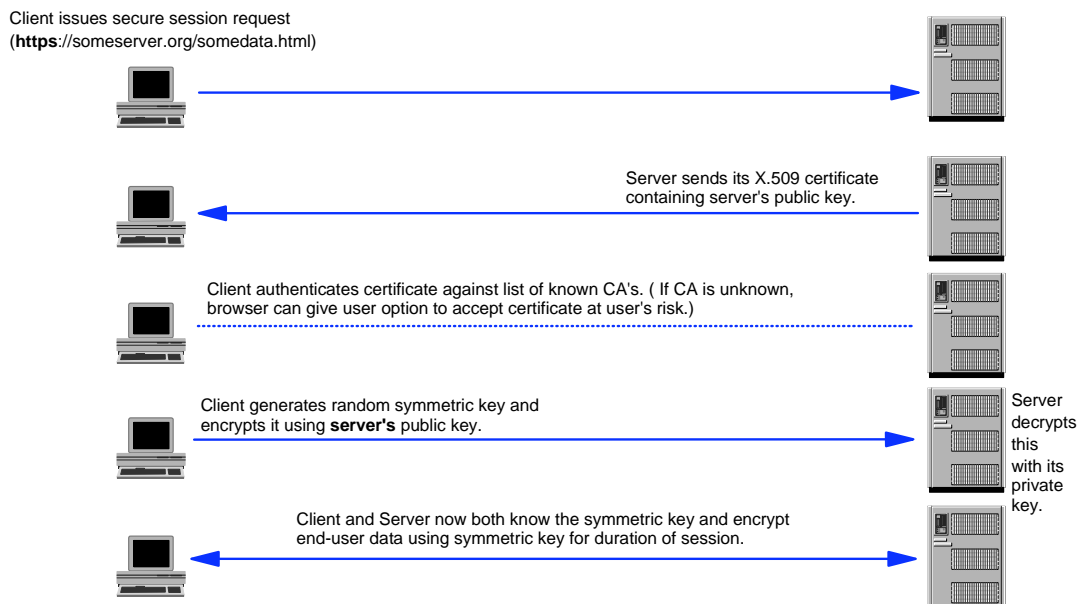
- The Security Domain, if specified, becomes a prefix used by WebSphere and RACF when checking EJBROLE profiles.
 - This provides cell-level granularity of roles.
 - No need to modify roles in the applications to achieve this.
 - Example:
 - Test Cell has Security Domain=TEST
 - Production Cell has Security Domain=PROD
 - An application using role Clerk is deployed on both Cells.
 - On the Test Cell, users need READ access in EJBROLE profile TEST.Clerk
 - On the Production Cell, users need READ access in EJBROLE profile PROD.Clerk
-

SSL Certificates and Keyrings



- WebSphere uses SSL for inter-server communication when global security is enabled, and (sometimes) for communication with clients.
- WebSphere uses only RACF (or CA-TS or CA-ACF2) certs and keyrings. No gskkyman keyfiles, etc.
- The BRAK jobs will create RACF keyrings and certs for you.
 - ▶ If you use an outside Certification Authority, you may have to create some yourself.
 - ▶ RACDCERT commands are OK, but the RACF panels are easier.
 - Option 7, DIGITAL CERTIFICATES AND KEY RINGS.

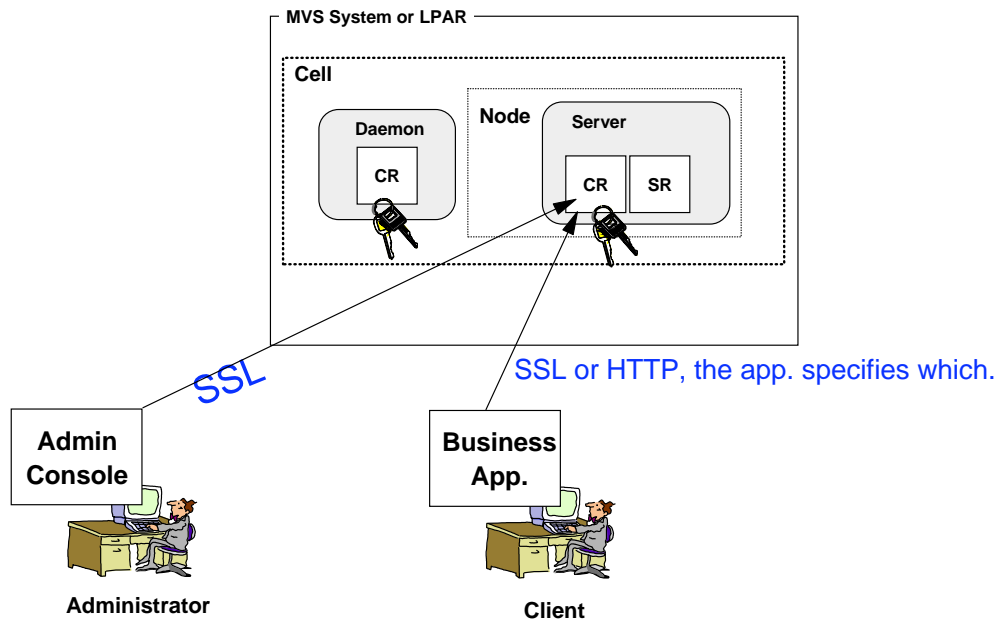
SSL Overview



SSL in a Stand-alone Application Server



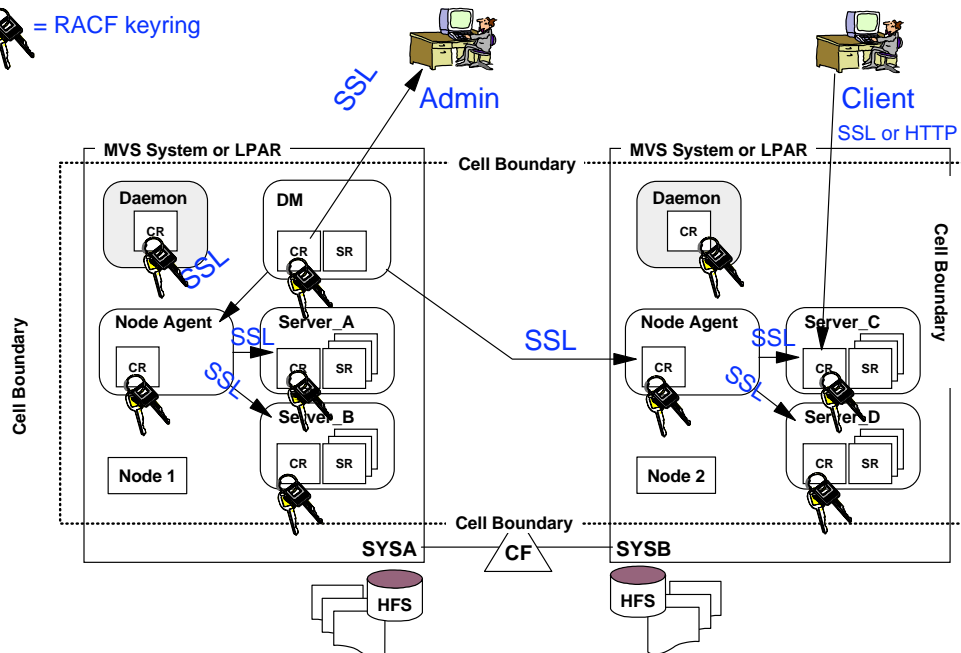
= RACF keyring



SSL in an ND Configuration



= RACF keyring



SSL Certificates and Keyrings



- **The cell needs a Certification Authority (CA).**
 - ▶ The CA signs the certs used by all the servers in the cell.
 - ▶ You can use Verisign, Entrust or another 'outside' CA.
 - ▶ Or the ISPF dialogs can create a CA in RACF for you.

 - **The BRAK jobs create a keyring and certificate for:**
 - ▶ The Daemon, DM Controller region, Node Agent, App Server Controller region.
 - They use SSL for administrative conversations (JMX).
 - Different userids for each region means a cert and keyring for each.
 - Another advantage of a single userid for WebSphere 'plumbing'.

 - **The BRAK jobs create just a keyring for:**
 - ▶ The DM Servant, the App Server Servant, the Default Admin user, the Asynch Admin user.
-

SSL Server Keyring



- **A Working SSL Keyring Should Contain**
 - ▶ The Server's Certificate, signed by a Certificate Authority
 - ▶ The Server's Private Key (you can't display this)
 - ▶ Root certificate of Certificate Authority that signed the Server's Cert.

 - **Questions or Problems with Keyrings/Certs?**
 - ▶ Contact Mike Kearney
 - kearney@us.ibm.com
 - (301) 240-3760
-

FACILITY Class Profiles



- FACILITY class profiles are generated to permit servers access to their keyrings and certificates.
 - Access by a server to its cert:
 - ▶ IRR.DIGTCERT.LIST
 - Access by a server to its keyring:
 - ▶ IRR.DIGTCERT.LISTRING
-

Troubleshooting SSL Problems



- If your Administrative Console doesn't answer...
 - See if your server(s) came up.
 - Check for SSL problems. (find 'gsk')
 - gsk return codes indicate problems with RACF keyrings or certs.
 - See 'System SSL Programming', Chapter 12, SC24-5901-04 for return code meaning.
 - Look in z/OS 1.7 library for SC24-5901-04.
 - Double check BBOXBRAK jobs.
 - ICH408I messages may indicate the server doesn't have access to ICSF CSFSERV class profiles.



Troubleshooting SSL Problems: Example



- Couldn't connect to admin console.
 - Issued 'find gsk' in controller region sysout from SDSF.
 - Found BBOO0036E FUNCTION gsk_environment_init FAILED WITH RC=202.
 - Checked SC24-5901-04 for gsk return code meaning.
 - "Error detected while opening the key database"
 - RC=202 has several possible causes:
 - The keyring the server is using doesn't exist, or the keyring name has a typo.
 - The server's userid doesn't own the keyring (or the cert).
 - The server's userid (or group) doesn't have READ access to FACILITY class profile IRR.DIGTCERT.LIST or LISTRING.
-

Troubleshooting SSL Problems



1. Who is the client and who is the server?
 - The client starts the conversation, the server responds.
 2. Does the client have a keyring? Does the server have a keyring?
 - Client keyrings can be in a browser, a PC, in RACF, or a .kdb or .jks file.
 - Server keyrings can be in RACF, or a .kdb or .jks file.
 - With System SSL, keyring not found results in gsk rc=202.
 - Keyring names are case sensitive, a typo will result in a gsk rc=202.
 3. Do the client and server have the authority to use their own keyrings?
 - RACF keyrings require ownership and READ access in FACILITY class profile IRR.DIGTCERT.LISTRING
 - Insufficient authority to System SSL keyring results in gsk rc=202.
 - hfs files require at least file read permission and usually a password or stash file.
 4. Any certificates in the server keyring?
 - Empty keyring, no handshake. Results in gsk rc=7.
-

Troubleshooting SSL Problems



5. Does the server have a personal certificate in its keyring?
 - The server's personal certificate should be marked as the default cert.
 - No personal cert or no default cert results in gsk rc=6.
 6. Does the server have the authority to use its own personal cert?
 - RACF personal certs require ownership and READ access in FACILITY class profile IRR.DIGTCERT.LIST
 - A personal cert not owned by the server will result in gsk rc=6 or 428.
 - For certs in .kdb or .jks keyfiles, just need access to the keyfile.
 7. Is the CA cert that signed the server's cert in the server's keyring?
 - RACF CERTAUTH certs must be connected with usage CERTAUTH, and not be the default cert.
 - In RACF, the CA cert must have the TRUST attribute.
 - If it's an intermediate CA cert, you must have the chain to the root CA cert.
 - Otherwise, gsk rc=8 or message 'unknown certificate'.
-

Troubleshooting SSL Problems



8. Is the CA cert that signed the server's cert in the client's keyring?
 - On a browser, you get a popup warning that you don't trust the signer.
 - On anything else, the client refuses to talk, resulting in gsk rc=8 or message 'unknown certificate'.
 - RACF CERTAUTH certs must be connected with usage CERTAUTH, and must have the TRUST attribute.
 - If it's an intermediate CA cert, client must have the chain to the root CA cert.
 - If the server's personal cert is self signed, you must connect it to the client's keyring as usage CERTAUTH, i.e. as a CA cert.
 9. Is the server's personal cert valid?
 - Not expired? Date range of the cert within the valid date range of the CA cert?
 - Personal certs must have the TRUST attribute in RACF.
 - Otherwise gsk rc=8 or 401.
 10. Is the CA's cert valid?
 - Not expired? Date range of the cert within the valid date range of the CA cert?
 - Have the TRUST attribute in RACF?
 - Connected to the keyring with as a CERTAUTH cert?
-

Troubleshooting SSL Problems



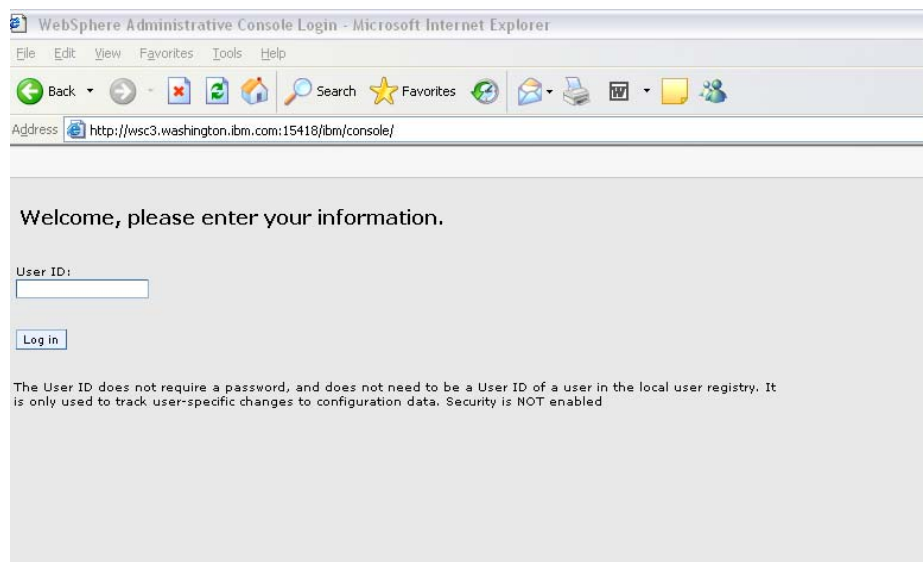
11. Is ICSF and hardware crypto involved?

- ICH408I messages may indicate the server doesn't have access to ICSF CSFSERV class profiles.
- If ICSF/crypto hardware is active/available, but the server doesn't have permission to use it, System SSL stops.

12. Does the server's certificate have an associated private key?

- In RACF, you can store private keys in the RACF database or in ICSF.
- Private keys in the RACF database have private key type: Non-ICSF
- RACF private keys in the ICSF PKDS have private key type: ICSF.
- RRSF doesn't copy private keys in either case.
- ICH408I messages may indicate the server doesn't have access to ICSF CSFKEYS class profiles protecting the server's private key.
- If ICSF is not active, private keys in ICSF will not be available.
- A RACF private key in ICSF will only be available to systems sharing the same RACF database and PKDS dataset
- Private key not found gets gsk rc=428.

With Global Security Off



What's Global Security?



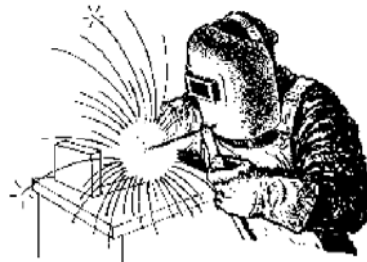
- ▶ **One big WebSphere 'switch' that activates many settings related to WebSphere V5 and V6 security. The settings include:**
 - ▶ User Registry (LocalOS, LDAP, CUR)
 - ▶ Authentication Mechanisms (LTPA or ICSF)
 - ▶ Application and Administrative Console Security
 - ▶ Other Misc. Security Stuff
- ▶ **Global Security is specified at the administrative console or using wsadmin.sh and is indicated in the security.xml file(s).**



When to Enable Global Security



- After WebSphere is up and running, and you are familiar with WebSphere and the Administrative Console, it's time to Enable Global Security.
- Global Security must be active in order to secure the Administrative Console.
- Global Security must be active in order to secure any applications (Basic Authentication, Form Based, etc.).
- Don't wait until it's time to go into production to enable Global Security!



Preparing for Global Security



1. **System SSL for z/OS or OS/390 must be installed**
 - Part of z/OS and OS/390 base.
 - Provides SSL libraries for WebSphere, HTTP Server, etc.
 - Put *hlq.SGSKLOAD* in Linklist. (prior to z/OS 1.6)
 - Put *SYS1.SIEALNKE* in Linklist (z/OS 1.6)
 - You've probably already installed System SSL.
 2. **Crypto hardware and ICSF has benefits, but is not required for SSL.**
 - Crypto hardware reduces CPU utilization from SSL workload.
 - Integrated Cryptographic Services Facility (ICSF) provides crypto APIs for System SSL and other applications.
 - ICSF provides administrative interface for managing crypto hardware.
-

Preparing for Global Security (cont.)



3. **Build your cell using the Customization Scripts.**
 - Be sure to check the BRAK jobs.
 4. **If you plan to use ICSF in support of login tokens, configure that before enabling Global Security.**
 - <http://www-1.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/TD100745>
 - Other choice is LTPA, which does not require the crypto hardware.
 - Not supported in V6.
 5. **If you plan on using Java 2 security, investigate the access requirements of your apps.**
 - If in doubt, leave Java 2 security off until you Global Security is working properly.
 - Or set **com.ibm.websphere.java2secman.norethrow** property to log Java 2 violations without stopping them.
-

Java 2 Security



- **Java 2 security prevents unauthorized applications from:**
 - Opening sockets.
 - Reading/writing to hfs files (even if the server is permitted).
 - Reading/writing JVM system properties.
 - Calling certain WebSphere APIs.
 - **New to WebSphere V5**
 - **Requires planning, preparation to activate.**
 - The server will work with Java 2 security turned on, but your applications probably won't.
 - **Can enable Global Security without enabling Java 2 security.**
-

Preparing for Global Security (cont.)



6. **Give administrative permissions to your administrators.**
 - Role based authority:
 - Specified in Admin Console if you use WebSphere bindings.
 - Specified in RACF EJBROLE profiles if you use RACF roles.
 - Remember that the Security Domain is used as a prefix, if specified.
 - **monitor** - can view, but not change admin settings.
 - **configurator** - can change cell configuration.
 - **operator** - can change cell state (e.g. start, stop).
 - **administrator** - can do anything.
 - Remember the Security Domain is used as a prefix, if specified.
 7. **Now you can enable Global Security....**
-

Enabling Global Security



1. **Logon to the Admin Console web application.**
 2. **Select Authentication Mechanism**
 - ICSF (V5 only) or LTPA (V5 and V6)
 3. **Select User Registry**
 - Local OS, LDAP or Custom
 4. **Select Active Protocol**
 - CSI and SAS, or CSI
 5. **Click Enable Global Security**
 - Unclick Enforce Java 2 Security
 6. **Restart the Server(s).**
-

With Global Security On



WebSphere Administrative Console Login - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Print Mail

Address <https://wsc4.washington.ibm.com:29519/ibm/console/login.jsp>

Welcome, please enter your information.

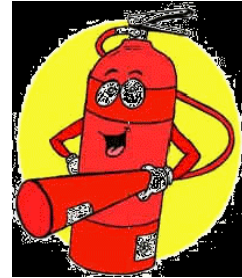
User ID:

Password:

Deactivating Global Security



- If you can log on to the Administrative Console,
 - Click 'Security-->Global Security'. Uncheck 'Enabled'.
 - Restart the server.
- If you can't log on to the Administrative Console,
 - From the bin directory of the Deployment Manager and each Node Agent, issue:
 - `./wsadmin.sh -conntype NONE`
 - At the command-line prompt for wsadmin, issue:
 - `securityoff`
 - Restart the server.



In Summary...



- **RACF provides security services in support of WebSphere Application Server and J2EE.**
 - **The Customization dialogs generate the RACF definitions needed.**
 - **Enabling Global Security enables cell security settings.**
 - **Most production environments will require Global Security.**
 - **SSL is still the most likely thing to go wrong.**
 - **Proper planning ensures success.**
-