

WebSphere V4.0.1 for z/OS and OS/390: Security Implementation

Session 1727

Glenn Anderson
Consulting Instructor
IBM Learning Services

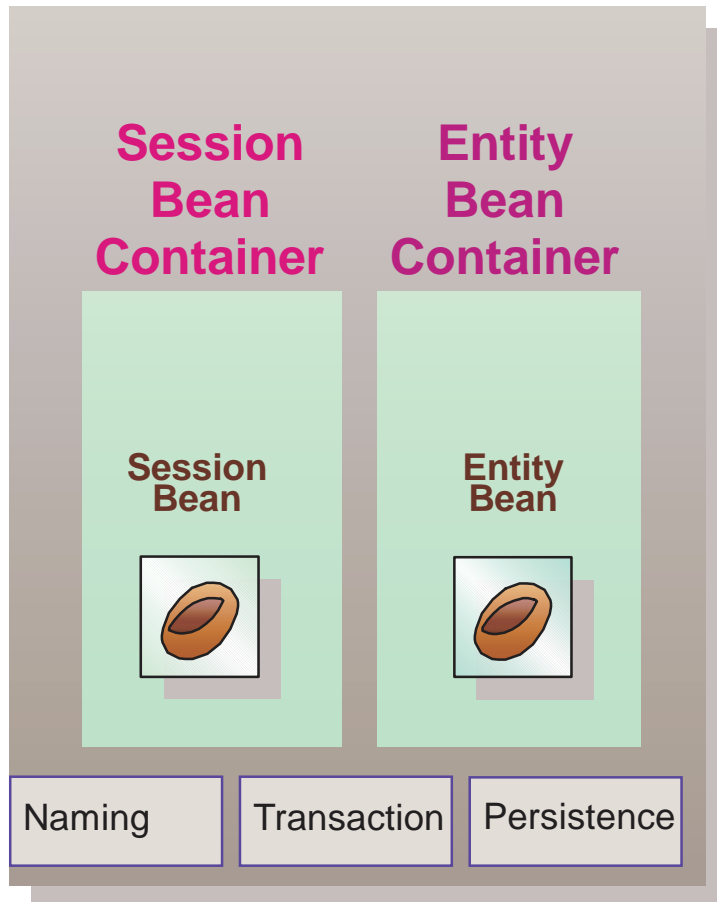


EJB Server

"Server" is a very overloaded term:

- System, Server Application, Server Address Space, Server Instance, Generic Server. . .

EJB Server



Server manages the EJB environment

- Naming
- Transaction
- Persistence
- . . .


Container

- Provides a Home for EJBs
- Required for Transactions
- Manages Session Beans or Entity Beans

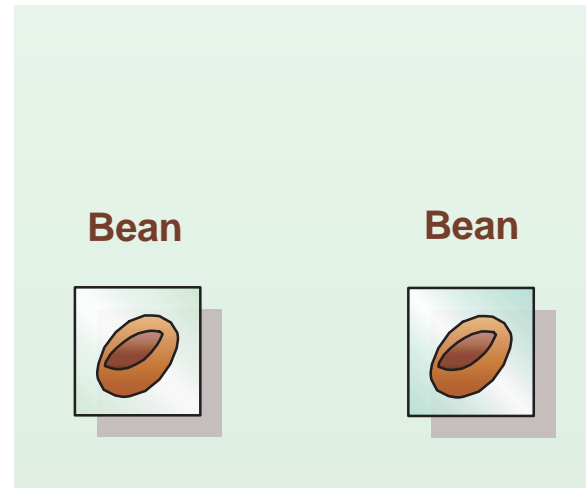
EJB Module / Container

EJB Module



install

deploy

Container



WAS/390 supports:

- EJBs
- Web components

Coordinates transactions

Controls entire bean life cycle

- create
- activate
- deactivate (passivate)
- persist
- destroy

Security

Session Beans & Entity Beans

Session Bean

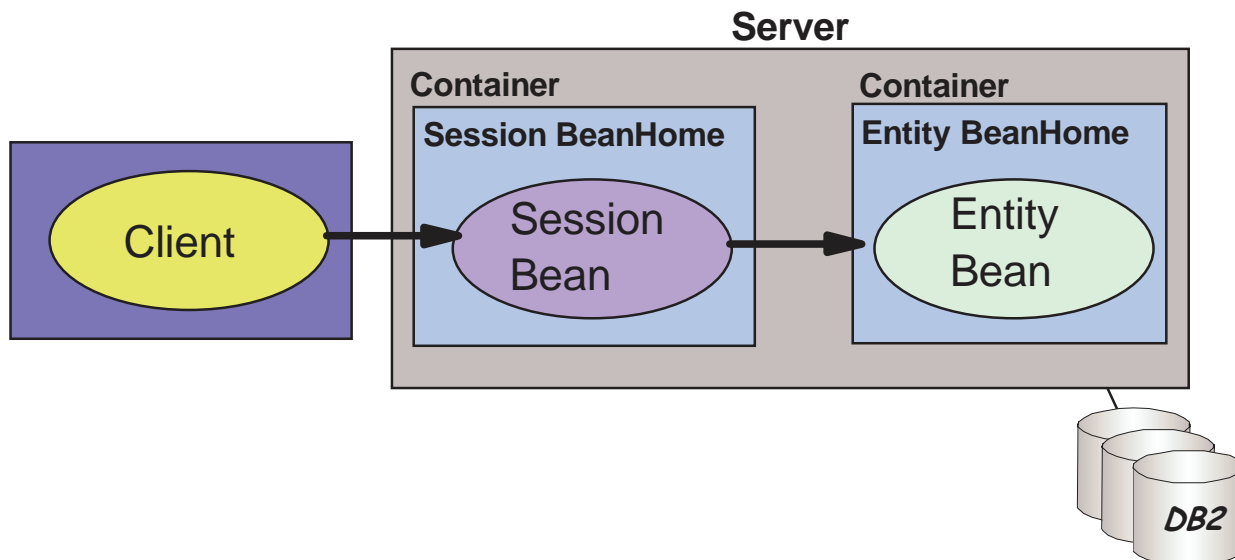


- Most of the business logic in these methods
- Property values are not rolled back following an abort

Entity Bean

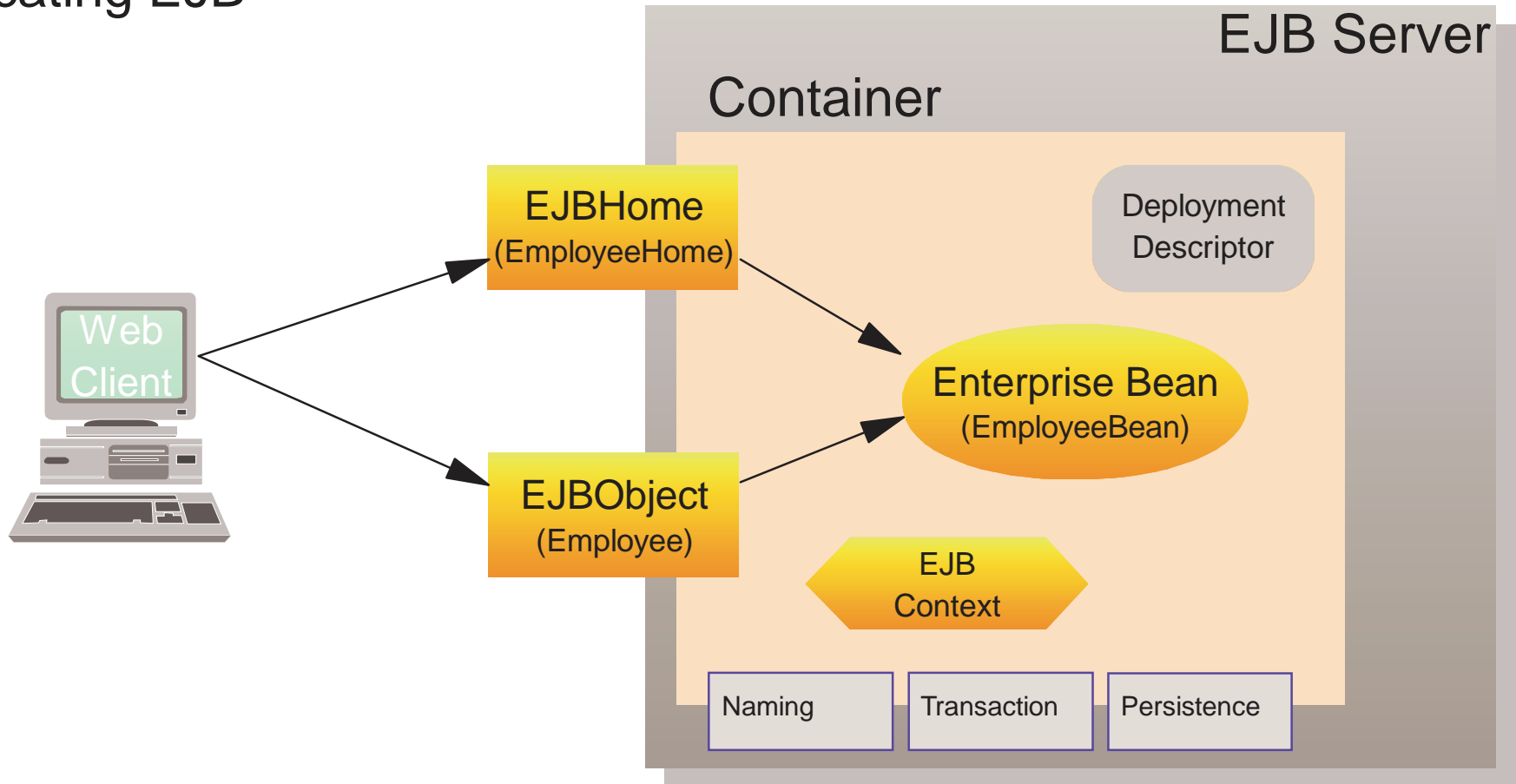


- Represents long-term data
- Container stores properties in database between usage
- Recalls bean when requested.



EJB Architecture

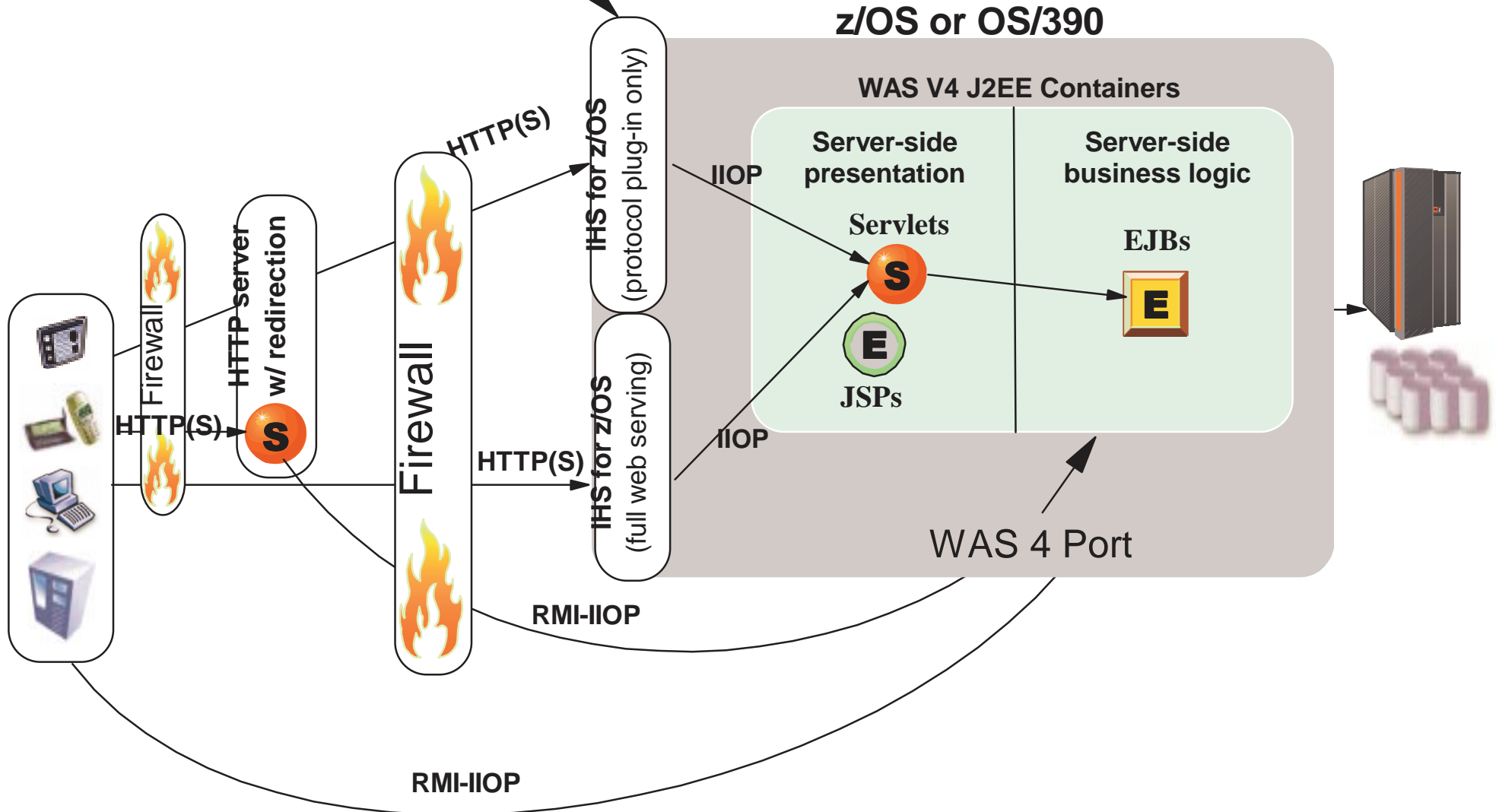
- Home Interface provides methods for creating, destroying and locating EJB



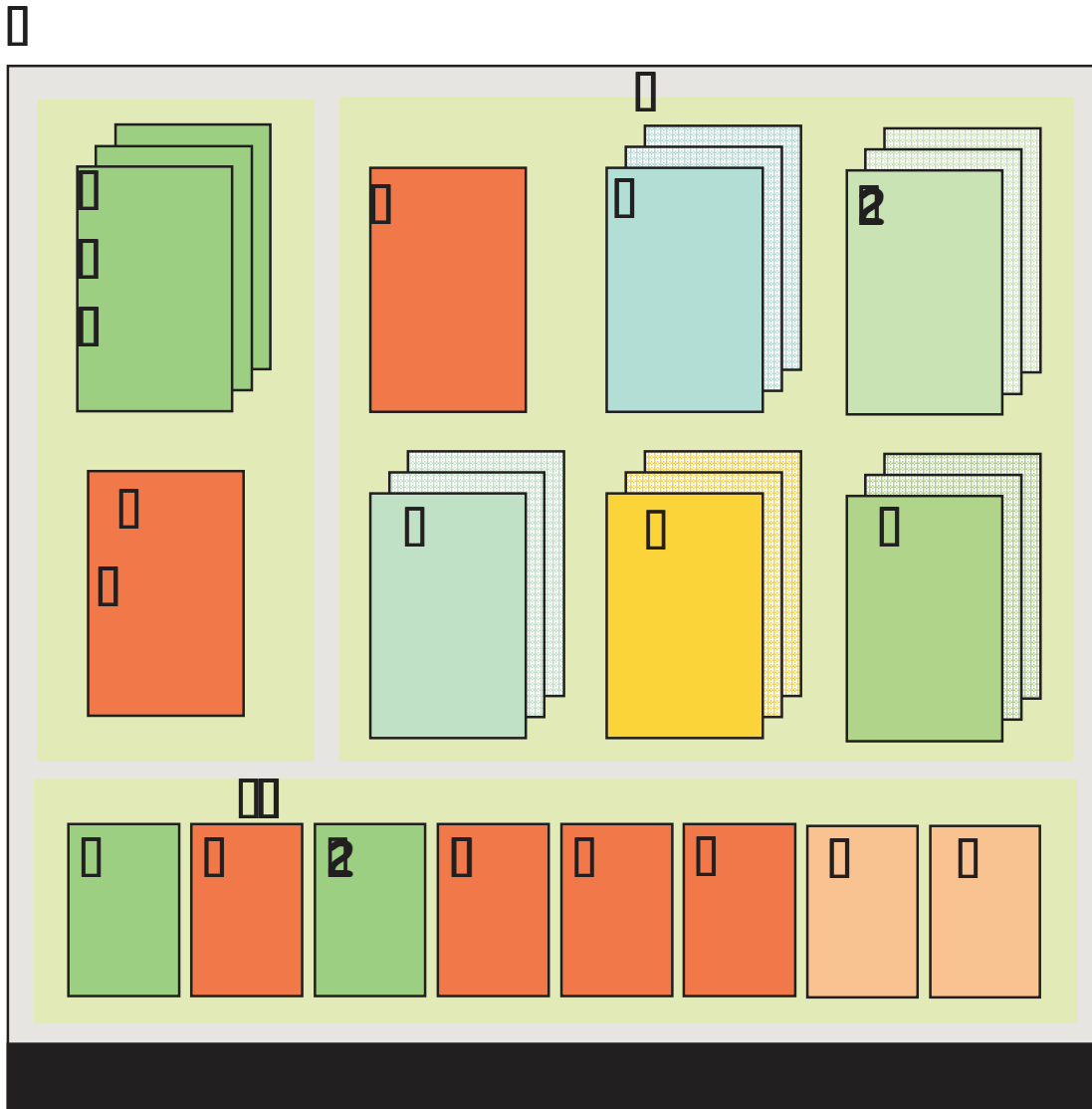
- Remote Interface defines the business methods offered by an EJB

WAS V4.0 for z/OS topologies

In V4.01, the HTTP "catcher" can be the IHS, or the HTTP catcher that is part of WAS.

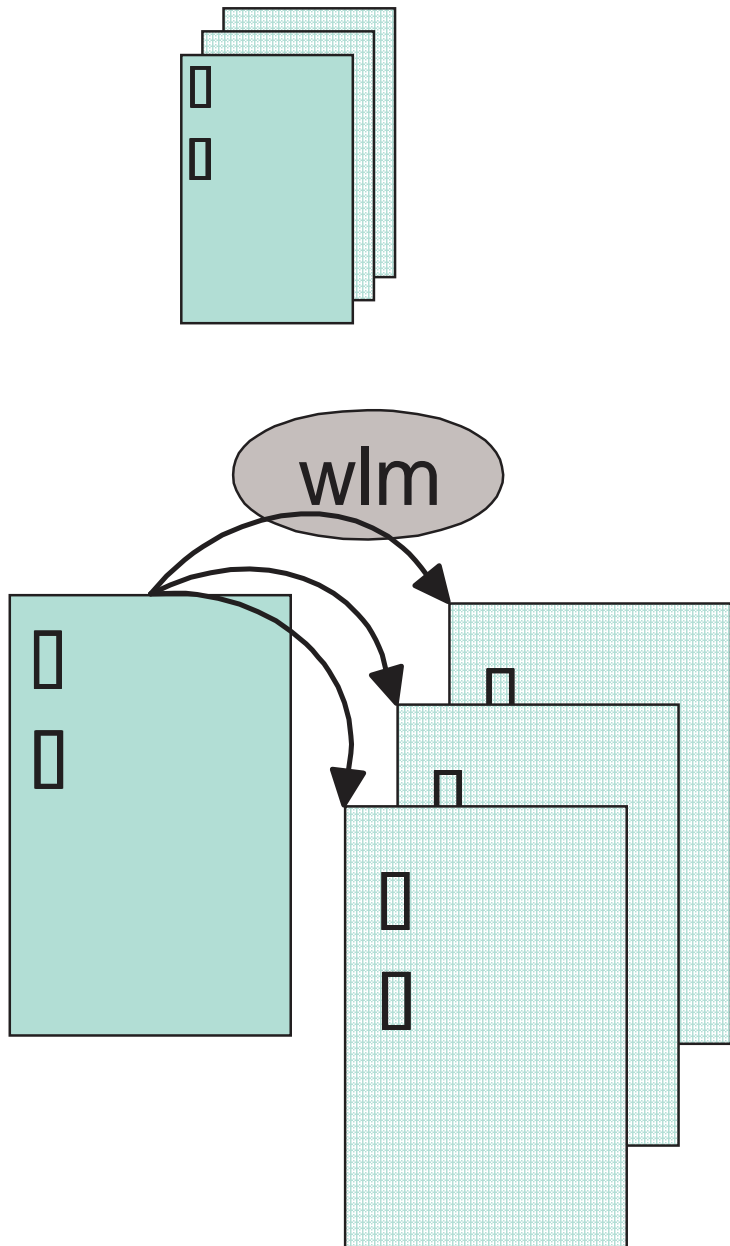


WAS/390 System Structure



- Infrastructure
 - ▶ LDAP
 - ▶ DB2
 - ▶ WLM goal mode
 - ▶ RRS (LOGR)
 - ▶ TCPIP
- WAS 390
 - ▶ System 'servers'
 - ▶ Application 'servers'
- Supporting Transaction Mgrs
 - ▶ CICS TS 1.3
 - Must be local to WAS
 - ▶ IMS 6.1
 - Local or Remote
- Users - local
 - ▶ fat C++ clients
 - ▶ Servlets / JAVA clients
- Users - remote (not shown)
- Security
 - ▶ RACF
 - ▶ DCE - remote client authentication.

WAS/390 Server Instance Structure



- **Server Instance**
 - ▶ Control Region
 - ▶ zero, one, or many Server Regions
- **Control Region**
 - ▶ Trusted/Authorized/Integrity
 - ▶ No Application Code
 - ▶ Communications Endpoint
 - ▶ Recoverable Resources
 - ▶ Workload Classification and Routing
 - ▶ Scalable Transaction Recovery/Restart
 - ▶ Choice of Scheduling Policies
- **Server Region**
 - ▶ Transaction/User Isolation
 - ▶ Application Code
 - ▶ Backend Data Attachments
 - ▶ Started and Managed by WLM
 - ▶ No Recoverable Resources

WAS Customization Assistant

- **ISPF Application**
- **Use for your first WAS/390 Installation**

- -----+ **Websphere for z/OS Customization** +-----
- **Option ==>__**
- **Use this dialog to customize the installation Jobs for WAS/390.**
- **1 Allocate Target Datasets for customization for jobs and other data.**
- **2 Customize variables for installation specific information.**
- **3 Generate Installation Jobs (after you have done the above options.)**
- **4 View the customized installation instructions.**
- **Utility functions to save and restore customization variables.**
- **S Save current customization values as a file.**
- **L Load customization values from a file (or the IBM default values.)**

Enter your installation data . . .

- **12 - 15 Panels to fill in Installation-specific names and values**
 - ▶ You will need to consult with specialists in your installation.
- **Variables validity-checked, and tracked for completeness.**

- -----+ **Websphere for z/OS Customization**

- +-----

- **Option ==>_**

- **Welcome to the customization section of the installation dialog. In the following panels, you will be asked about all the variable data needed to install WebSphere. These values can be primed to the IBM supplied defaults, or you can load a previously saved set of variables....**

■	Changed?
■ 1 - System Locations (directories, HLQs, etc)	Y
■ 2 - WAS related customization	Y
■ 3 - Server related customization	N
■ 4 - IVP related customization	Y
■ 5 - LDAP related customization	N
■ 6 - Security related customization	N

Generate Installation Jobs, etc.

- **Input parameters checked for validity and consistency**
- **Jobstreams and data written to user-specified PDS**
- **Customized instruction document created to guide the installation**

- **Manual Configuration Instructions**

- ▶ WLM Application Environments
- ▶ Parmlib Updates (SHED, PROG, SMFPRM, BPXPRM, TCPIP, CFRM)
- ▶ Automation Updates

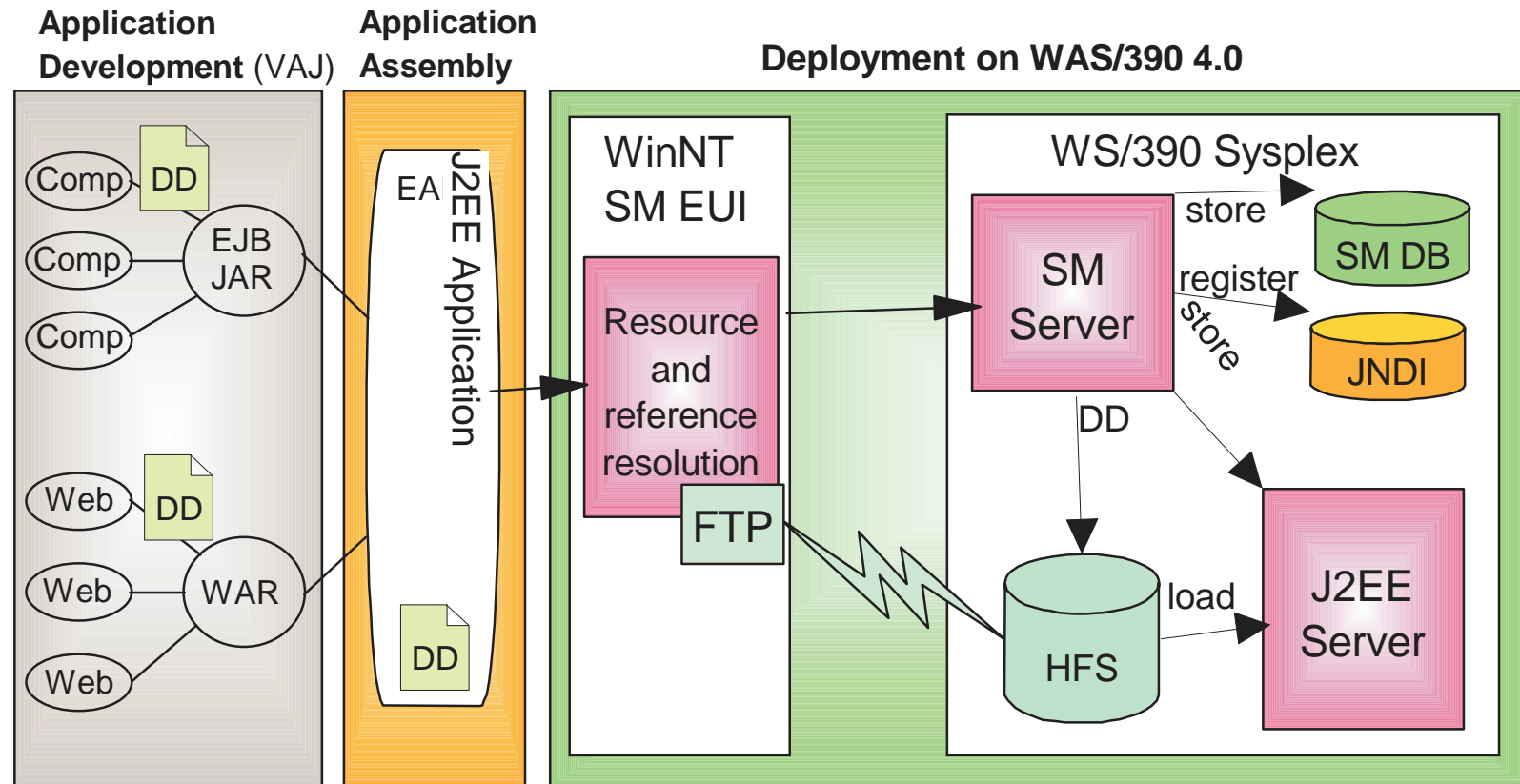
- **Configuration Jobs, Description, Userid Required for Submission, and Check-off**



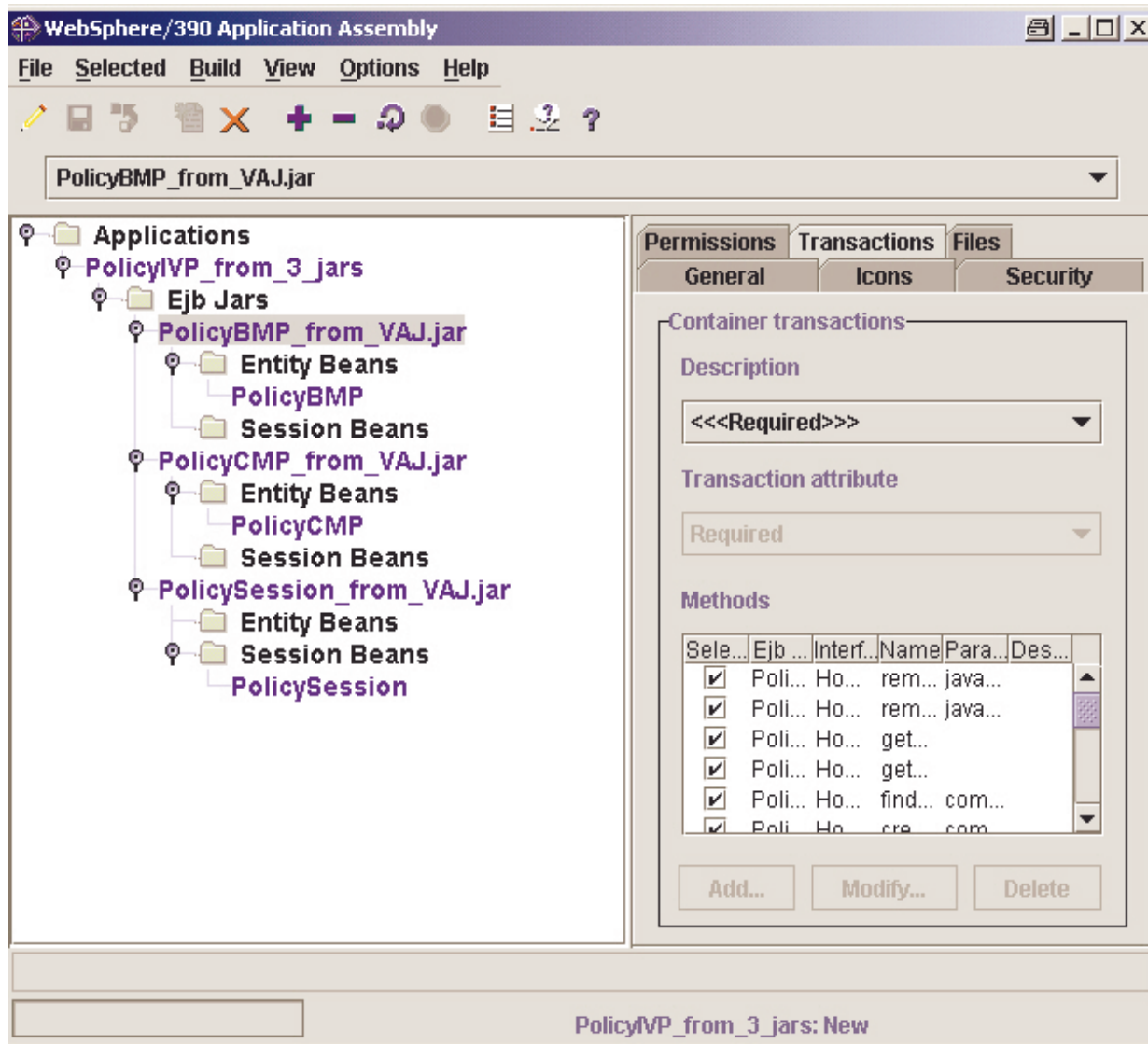
	Jobname	Description & Instructions
	BBOMSGC	Userid req'd: SYSxxx Authority
	BBOERRLG	This job creates the error logstream
	BBORRSL	Note: Check xxx
	BBOCBRAC	Verify the output with your Security Administrator
	...	
	<bootstrap>	Enter these commands . . .
	IVP	

- ▶ Misc other jobstreams and data produced (utilities, back-out jobs, etc.)

J2EE Application Development, Assembly & Deployment:



Application Assembly Tool



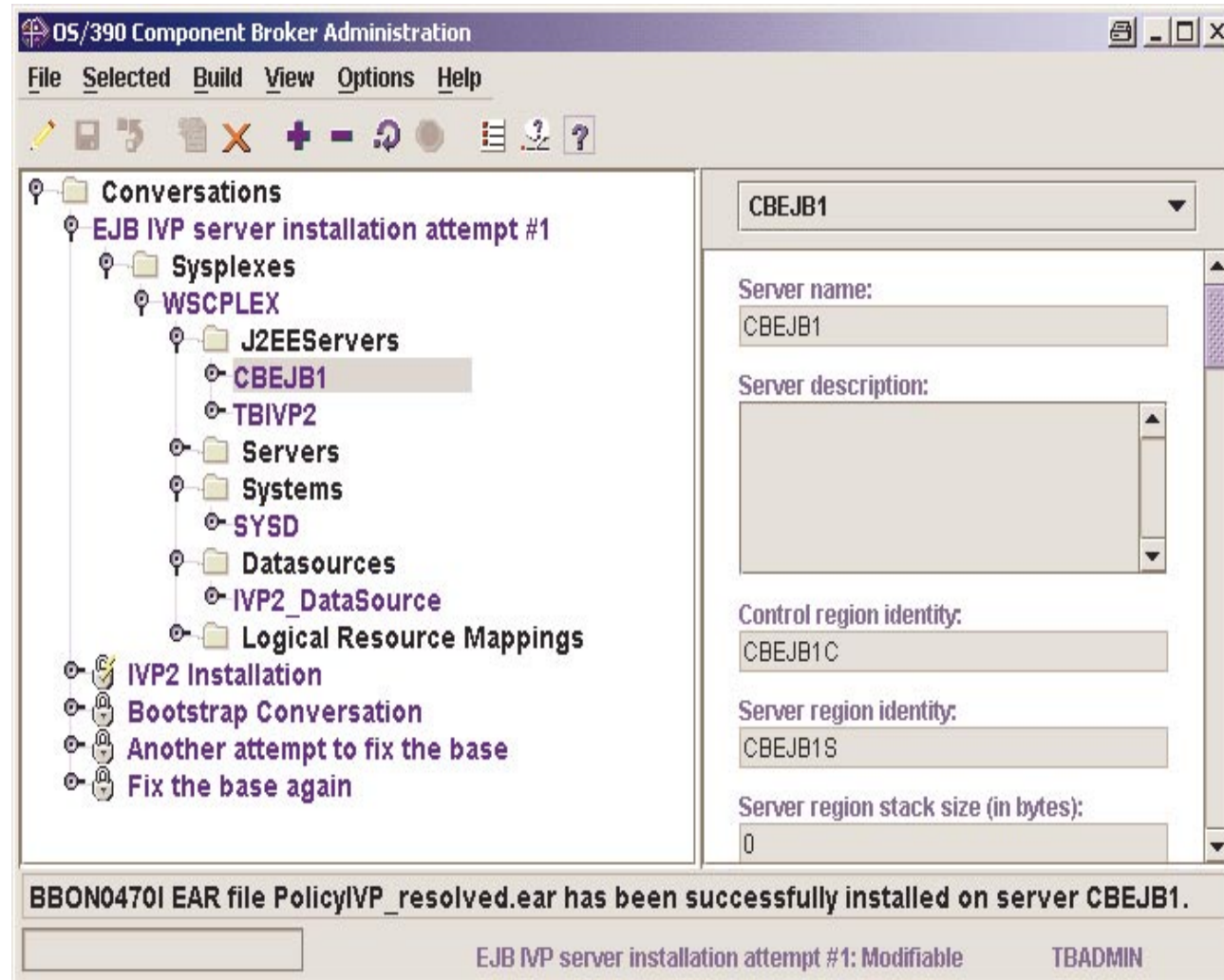
- Converts 1.0 EJBs to 1.1 EJBs
 - ▶ Export deployed jar from VAJ
 - ▶ Import jar files into AAT
 - import other stuff
 - ▶ Inspect, modify deployment descriptors
 - Assign JNDI names
 - Resolve references, Links to other beans, and Resources
 - ▶ Export deployed .ear file
- SM Admin. EUI will:
 - ▶ Transfer to host
 - ▶ Deploy J2EE application on server
- Complete tasks . . .

Deploy a J2EE Application

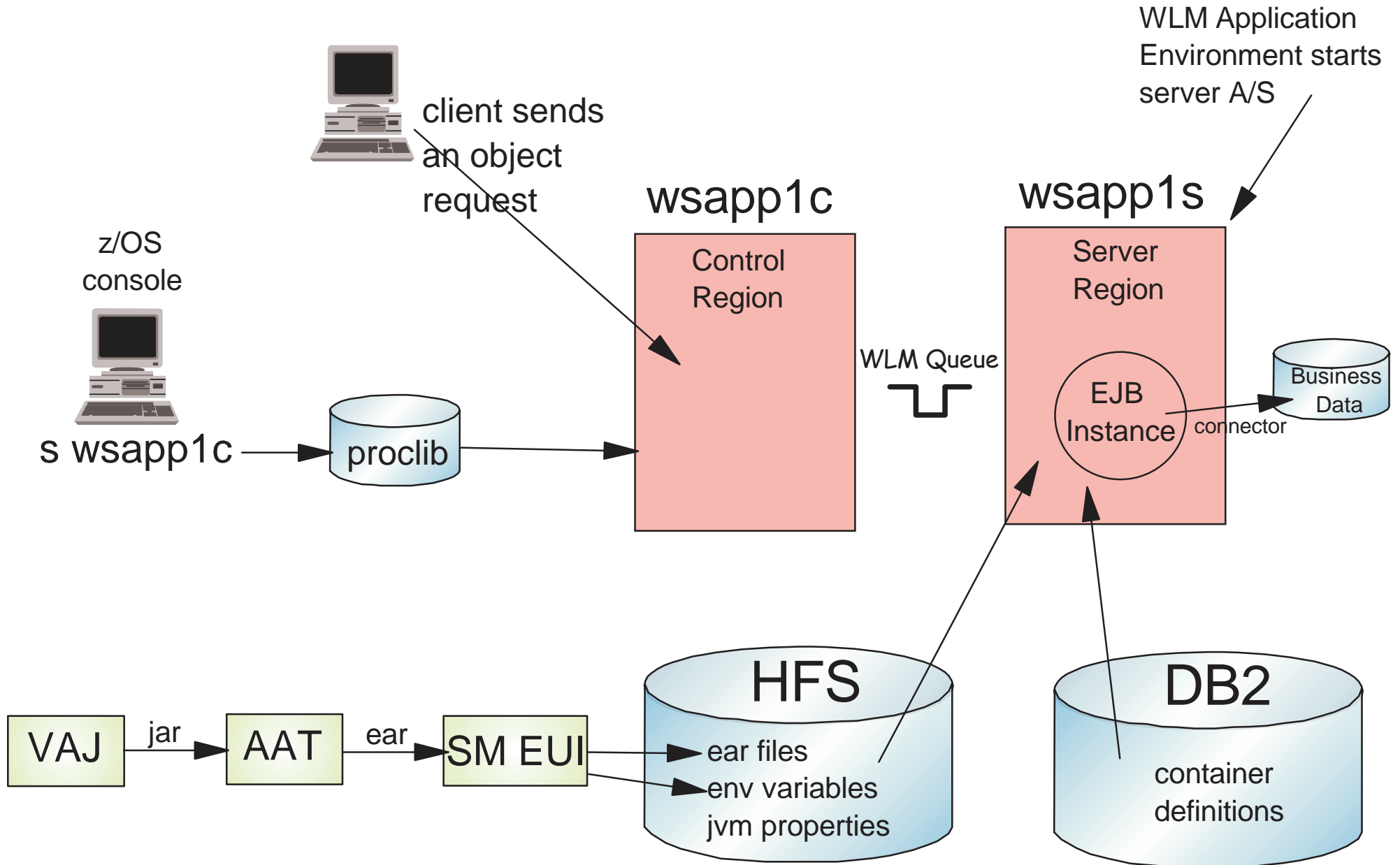
- **Graphical Systems Management administrative application**
 - ▶ Shipped with WAS/390 -- Runs on Windows NT (or 2000)
 - ▶ Primary interface for deploying J2EE Applications

Steps to install a new application server:

- ▶ Start a new "Conversation"
- ▶ Add a new Server
- ▶ Add Server Instance
- ▶ Add Datasource ("J2EE Resource")
- ▶ Add Resource Instance
- ▶ Install application (FTP ear file to HFS)
- ▶ Validate, Commit, and Activate Conversation



Starting an EJB Application



WebSphere 4.0 Security Mechanisms

■ Security in WAS/390 runtime

- ▶ RACF profiles & permissions
- ▶ HFS file/directory permission & ownership
- ▶ LDAP ACLs
- ▶ DB2 GRANTS
- ▶ SSL
- ▶ Kerberos
- ▶ EJB Roles & Runas support

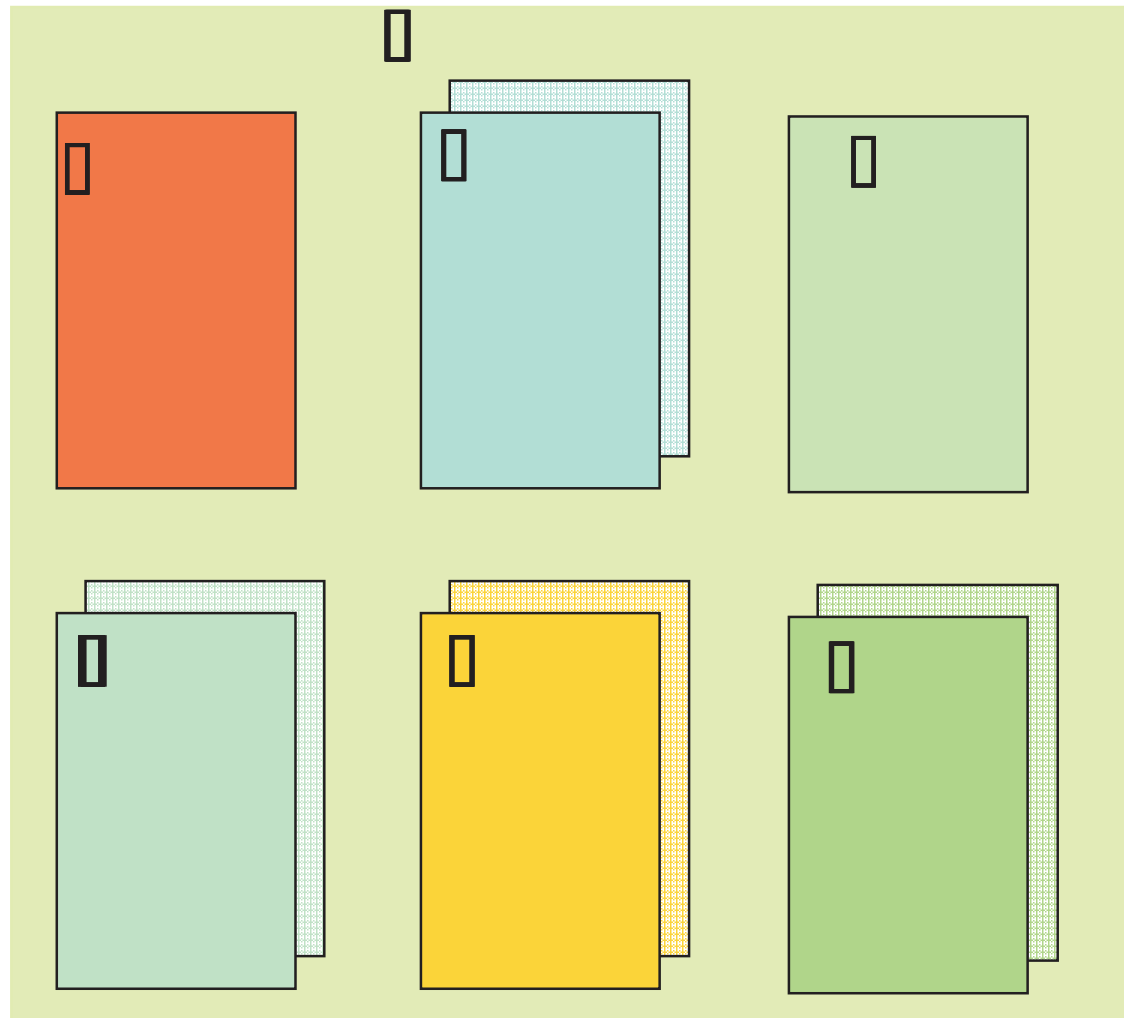


The Security Challenge

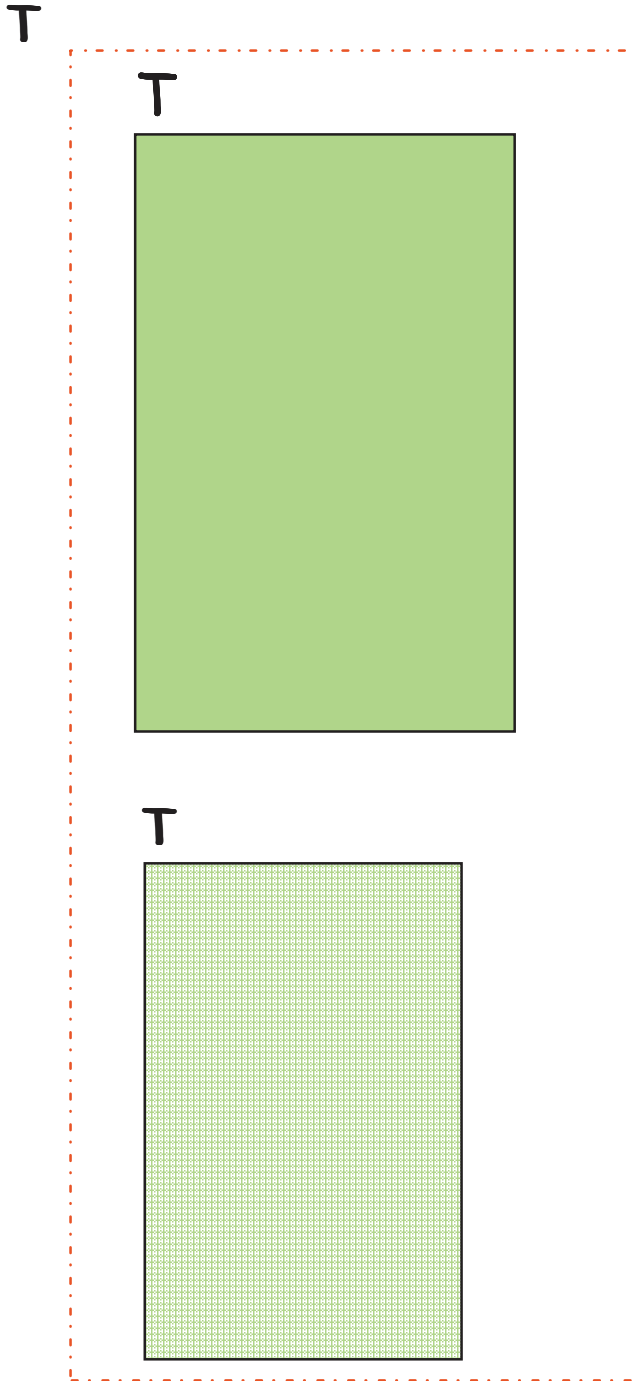
- **Need to authorize servers to infrastructure services**
 - ▶ MVS constructs, Data base managers, Transaction Managers
 - ▶ Distinguish between Control Regions vs. Server Regions
 - ▶ Establish 'trust' among servers
- **Need to authenticate users and map other credentials into SAF entities (i.e. native operating system constructs).**
 - ▶ SSL
 - ▶ Kerberos
- **Need to authorize users to servers and objects within servers**
 - ▶ local users vs. remote users
 - ▶ Authenticated users vs. un-Authenticated users
 - ▶ CORBA objects vs. EJBs
 - ▶ Other transaction managers

WAS Server Definitions:

- For each Server (Control Region, Server Region):
 - ▶ Procedure Name
 - ▶ Generic Name
 - ▶ Instance Name
 - ▶ User ID, UID
 - ▶ Group ID, GID
 - ▶ Unath. Local Client
User ID, UID,
Group ID, GID
 - ▶ Unath. Remote Client
User ID, UID,
Group ID, GID



Basic CR/SR Profiles



► Control Region

- STARTED Class
 - profile: <proc_name>.*
 - assigns userid/group
 - ◆ unique userid/uid
- All control regions belong to the same GROUP (i.e. CBCTL1)
 - All belong to a common configuration group (i.e.CBCFG1)
 - RACF List of Groups option must be enabled
- LOGSTRM
 - profile: <logstream_name>
 - update access to write
- DSNR class access to DB2
 - profile: <DB2_ssn>.RRSAF
- Access to appropriate DB2 packages and data bases.

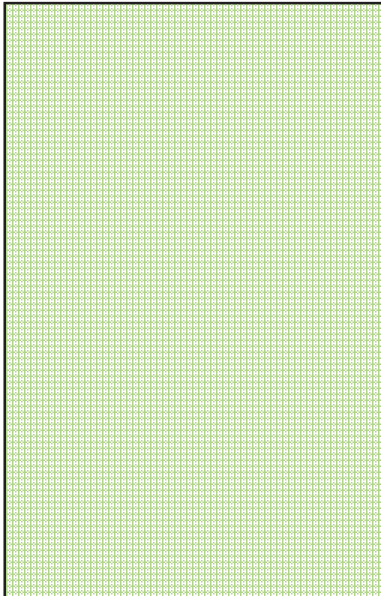
Basic CR/SR Profiles

T

T



T



► Server Region

- STARTED Class
 - profile: <proc_name>.*
 - assigns userid/group
 - ◆ unique userid/uid
- ApplicationServer regions generally have belong to unique GROUPs but connected to a common group (CBCFG1)
 - Runtime servers all belong to same group (CBSR1)
- SERVER Class
 - profile: CB.*.server_name
- LOGSTRM
 - profile: logstream_name
 - update access to write
- DSNR class access to DB2
 - profile: <DB2_ssn>.RRSAF
- Facility Class access to IMS
 - profile: <ims_xcf_group>.OTMA
- Surrogat Class access to CICS
 - profile: *.DFHEXCI
- Access to appropriate DB2 packages and data bases

Associate Servers & Users/Groups

Server	User ID	UID	Group ID	GID
daemon	CBDMNCR1	2111	CBCTL1	2211
SM Ctl Reg	CBSYMCR1	2112	CBCTL1	2211
SM Svr Reg	CBSYMSR1	2104	CBSR1	2201
Naming CR	CBNAMCR1	2113	CBCTL1	2211
Naming SR	CBNAMSR1	2105	CBSR1	2201
IR CR	CBINTCR1	2114	CBCTL1	2211
IR SR	CBINTSR1	2106	CBSR1	2201
J2EE IVP CR	CBACRU2	2115	CBCTL1	2211
J2EE IVP SR	CBASRU2	2116	CBASR2	2216

π

```
ADDUSER CBDMNCR1 DFLTGRP(CBCTL1) OMVS(UID(2111))
RDEFINE STARTED BBODMN.* STDATA(USER(CBDMNCR1) GROUP(CBCTL1))
```

RACF Definitions

- WAS provides sample definitions and jobstreams to install the tailored definitions
 - ▶ Two step process for the WAS and LDAP security definition setup
 - Jobs BBOCBRAJ/BBOLDRAJ runs the tailored REXX exec to generate 'real' RACF commands that can be tailored/alterd for your installation.
 - Jobs BBOCBRAK/BBOLDRAK execute the commands generated by the previous the previous jobs
 - ▶ By default, the REXX exec defines basic RACF entities for 'sample' WAS/390 installation.
 - Defines profiles for servers, logstream access, DB2 access, etc.
 - Defines userids/groups for servers, administrators, IVP file system owners.
 - ▶ Optionally, the REXX exec will generate profiles for advanced features
 - SSL, EJBROLES, DSNR, etc.
 - Requires basic RACF infrastructure prior to implementing advanced features

More UserIDs...



- **The built-in administrator**

- ▶ Userid/Group: CBADMIN/CBADMGPP
- ▶ uid/gid: 2103/2203



- **The built-in un-authenticated user**

- ▶ Userid/Group: CBGUEST/CBCLGP
- ▶ uid/gid: 2102/2202



- **The built-in IVP userid**

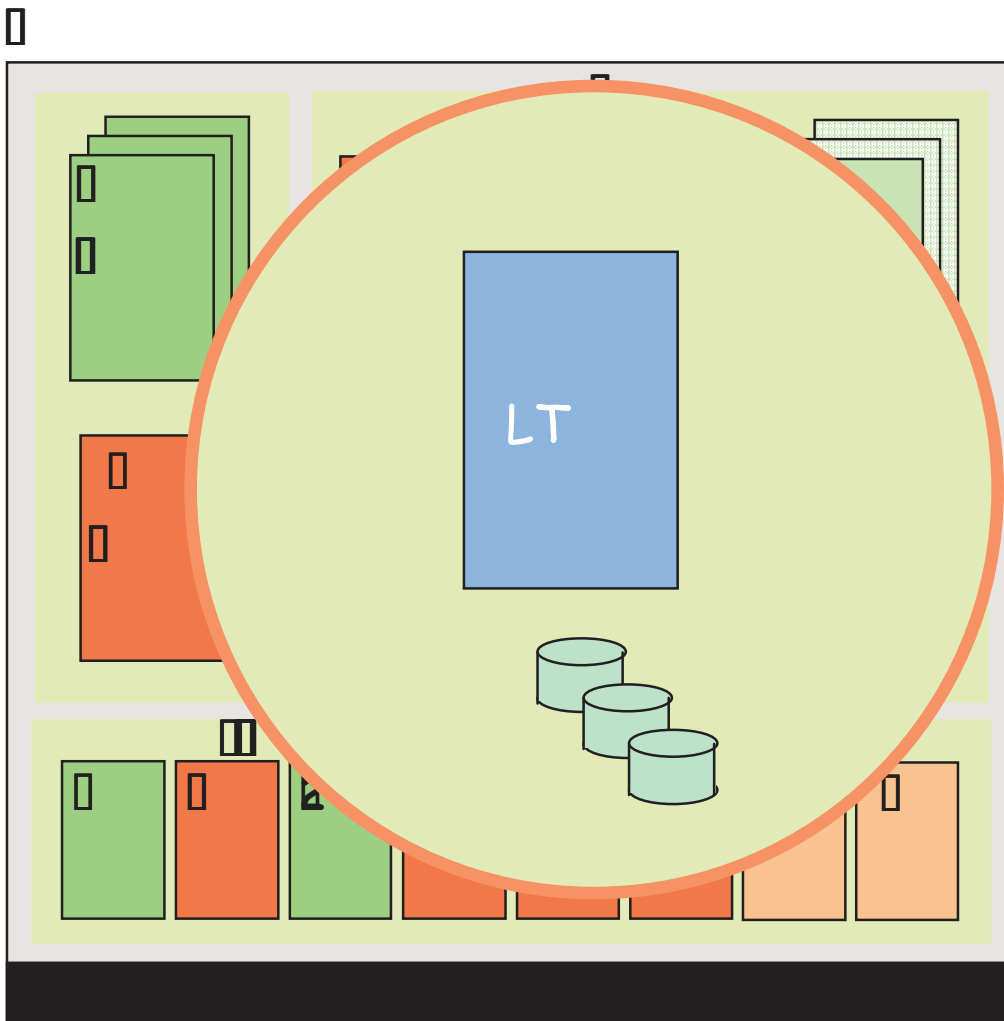
- ▶ Userid/Group: CBIVP/CBIVPGP
- ▶ uid/gid: 2109/2209



- **The built-in group owning WAS/390's HFS**

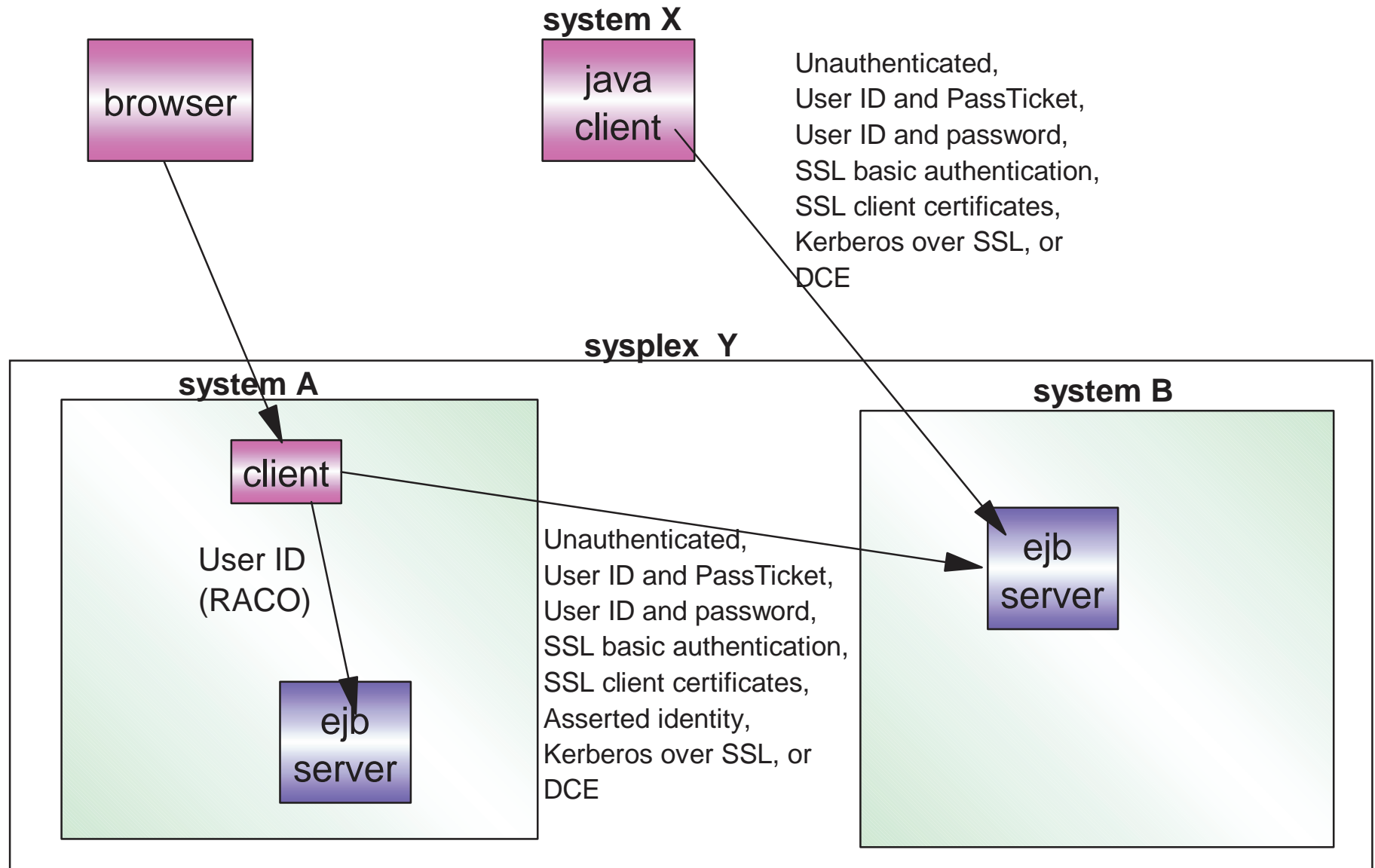
- ▶ Group: CBCFG1
- ▶ gid: 2300

Why WAS Needs LDAP ?

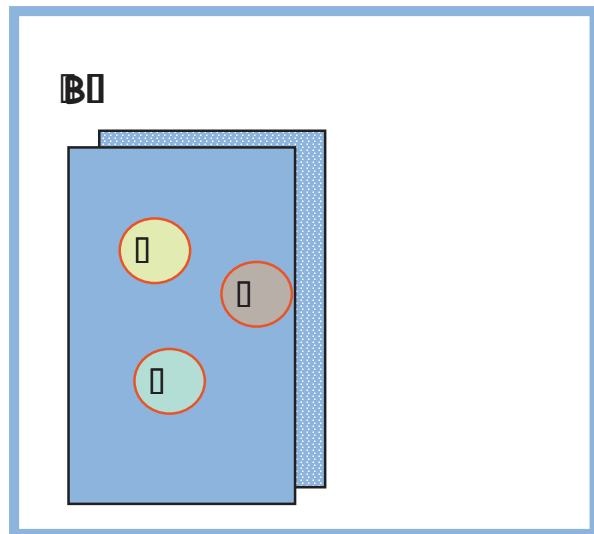
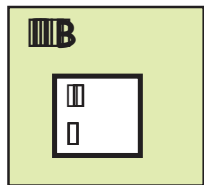
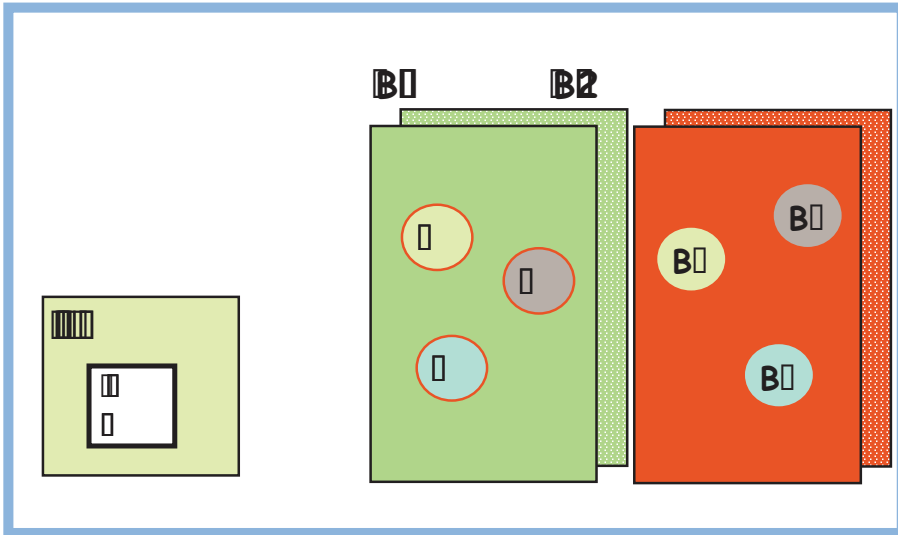


- WAS uses LDAP to store information in the name space and interface repository
- J2EE servers need JNDI access to an LDAP server
 - ▶ Systems Management and Naming servers also require JNDI access.
- An administrative LDAP server is needed to maintain the ACLs

User identification, authentication, & network security issues



Client Access to Servers...

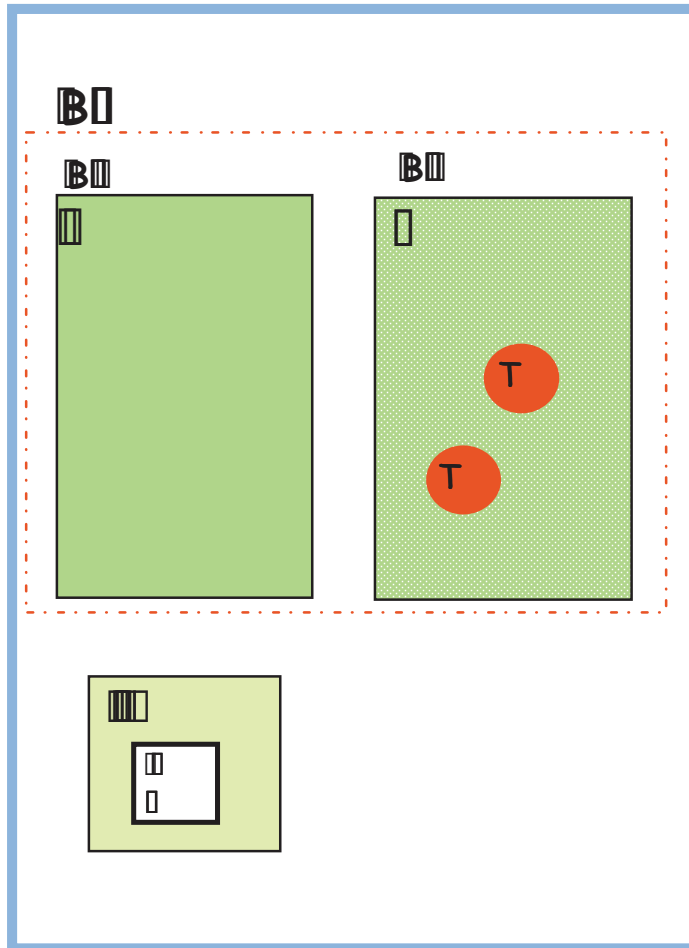


Rules:

- ▶ Certificates are kept in RACF
- ▶ Holders of certificates must map to a RACF identity
- ▶ SSL ports must be specified
- ▶ Asserted identities allow installation to specify trust among servers
 - Allows propagation of MVS identity (i.e., RACO) with less setup/overhead
 - SSL secure connection between servers required and CBIND class definitions
- ▶ Unauthenticated user ids do not flow,
 - enter unauthenticated, leave unauthenticated
- ▶ Security mechanisms are established through the SMS EUI when defining/altering a server.

Access to J2EE Servers

MT

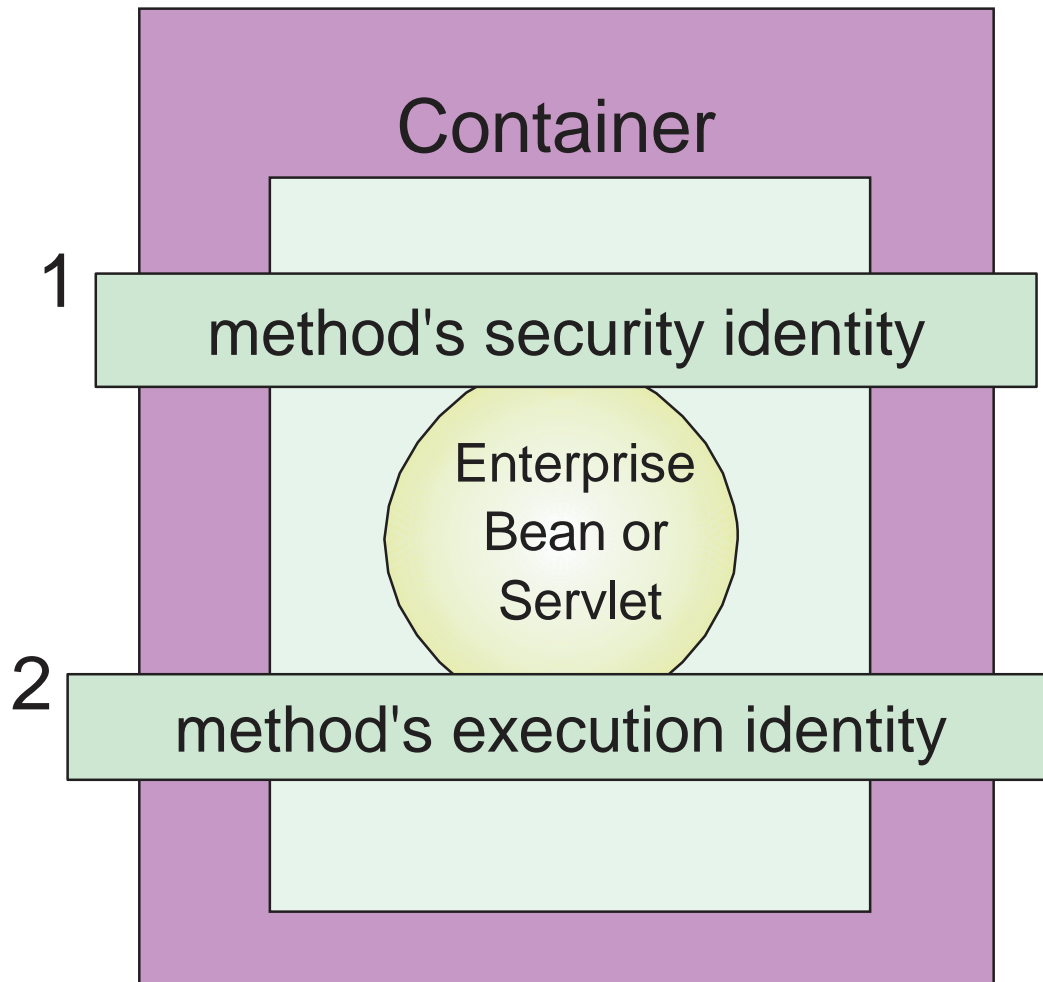


► Client

- Access to server
 - CBIND class
 - profile; CB.BIND.<server_name>
 - READ access (*)
- Access to objects in server
 - CBIND class
 - profile: CB.<server_name>
 - READ access
- Access to methods on objects
 - EJBROLES class / GEJBROLES
 - profile: <any valid string>
 - Read Access
- Access to DB2
 - User packages and tables
- Access to IMS/CICS transactions

WebSphere Authorization Overview

J2EE Server Region

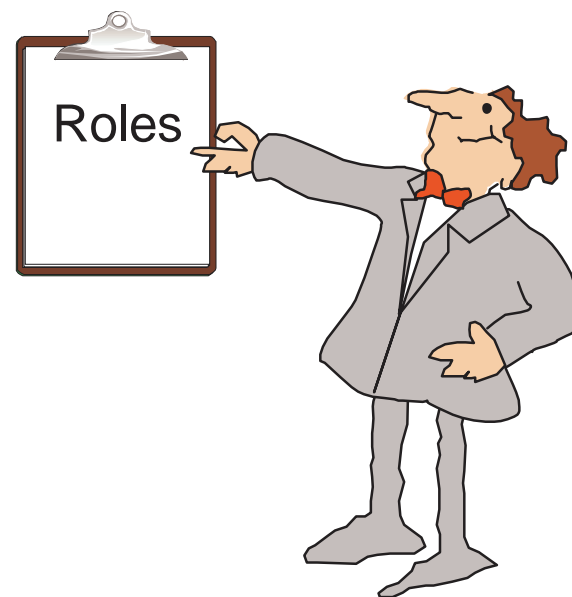


An enterprise bean or servlet has two identities associated with it:

1. A security identity, used to control access to J2EE resources or for downstream processing.
2. An execution identity, associated with the operating system thread.

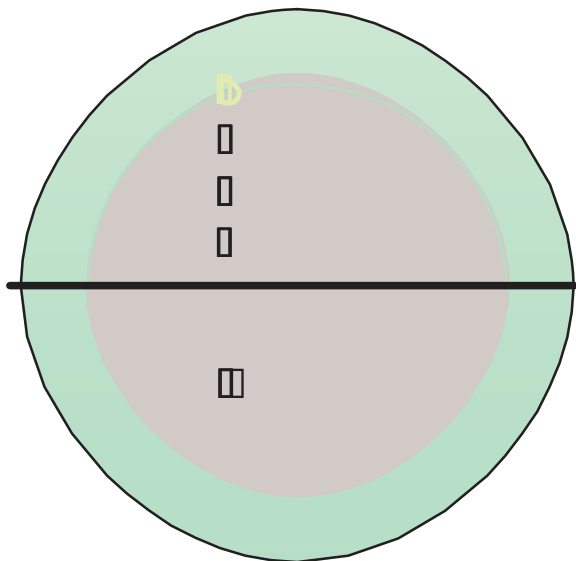
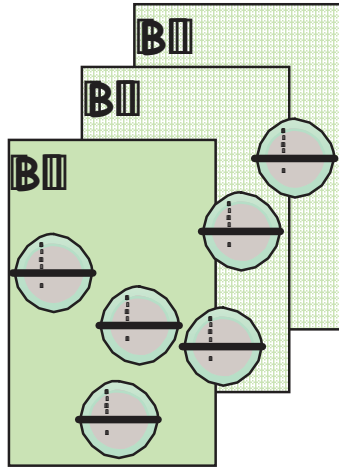
EJB "Roles"

- J2EE Authorization Model based on security Roles
- RACF Introduces a new **EJBROLE** class
 - ▶ Bean provider declares security-role-ref elements:
`isCallerInRole(String role-Name)`
 - ▶ Deployment descriptor contains rolename
 - ▶ RACF profile=rolename to check access to method.
- Container tests user's credentials against each role
 - ▶ Evaluation stops with an "is authorized" outcome on the first role that the container is able to map the user to. . .
 - ▶ Otherwise, the user is "not authorized".



Methods on J2EE Objects: EJBROLE

BI

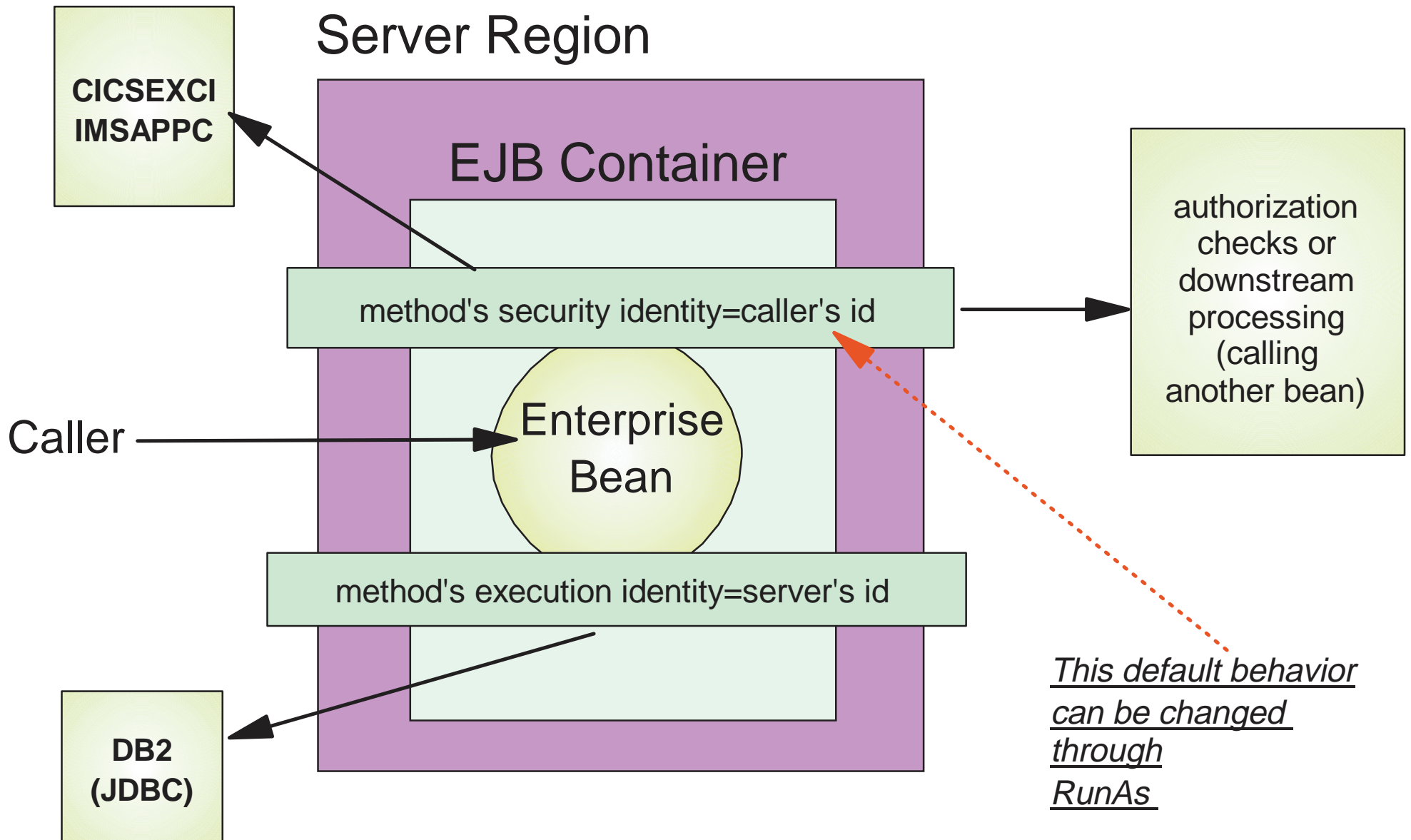


■ EJBROLE class

- ▶ profile: <role_name>
- ▶ No blanks allowed
- ▶ Case sensitive search
- ▶ Profile limited to 245 characters
- ▶ User must have read access to profile to be considered in that role
- ▶ Profiles are FRACHECKed
- ▶ EJBROLEscan be grouped into GEJBROLE
- ▶ For caller to be in role must have READ access to RACF profile
- ▶ EJBROLEs and EJBROLE-Refs are assigned to application/jar and method by the Assembling Application Tool.

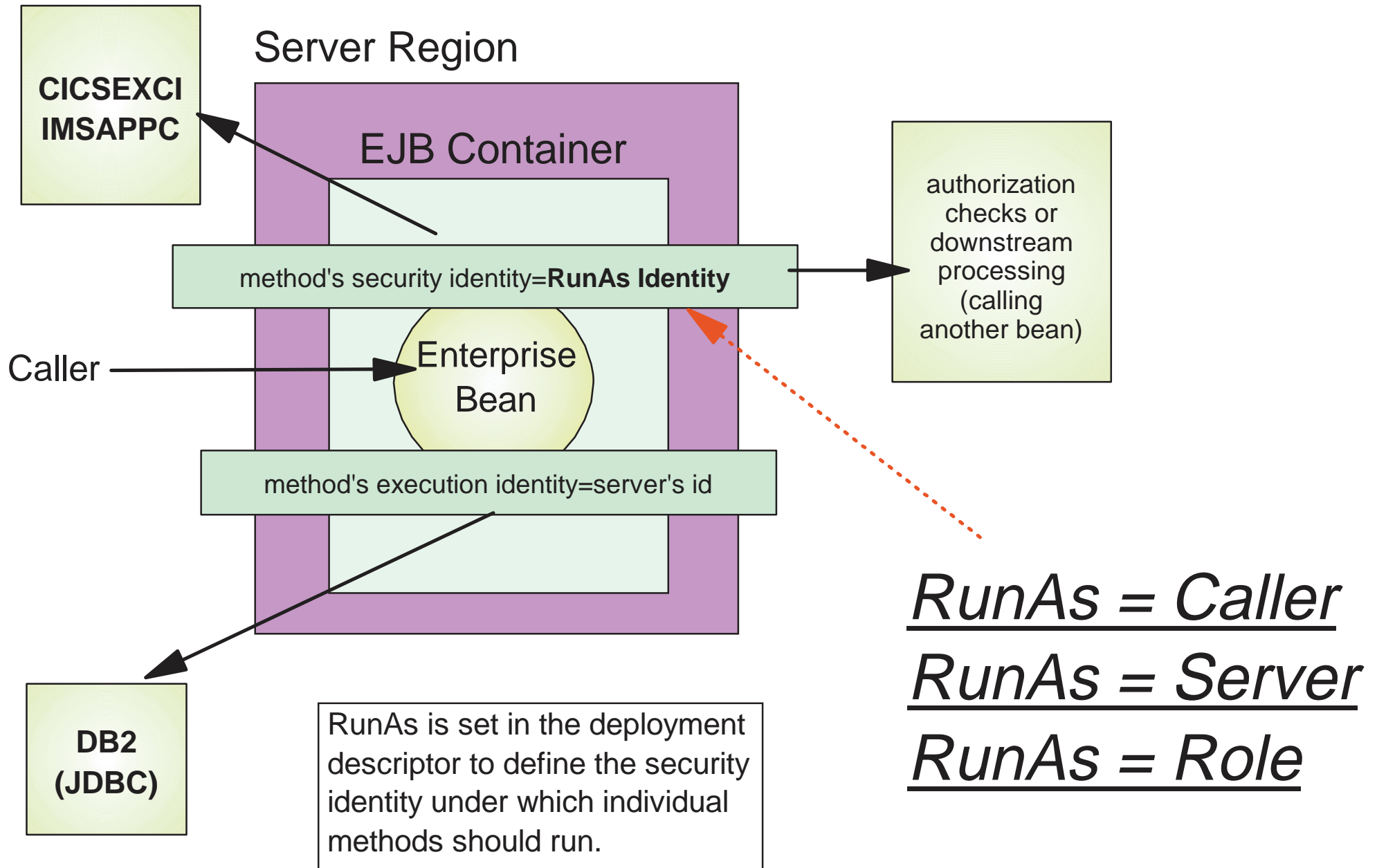
WebSphere Authorization

EJB Container - Default Behaviors



WebSphere Authorization

EJB Container - RunAs

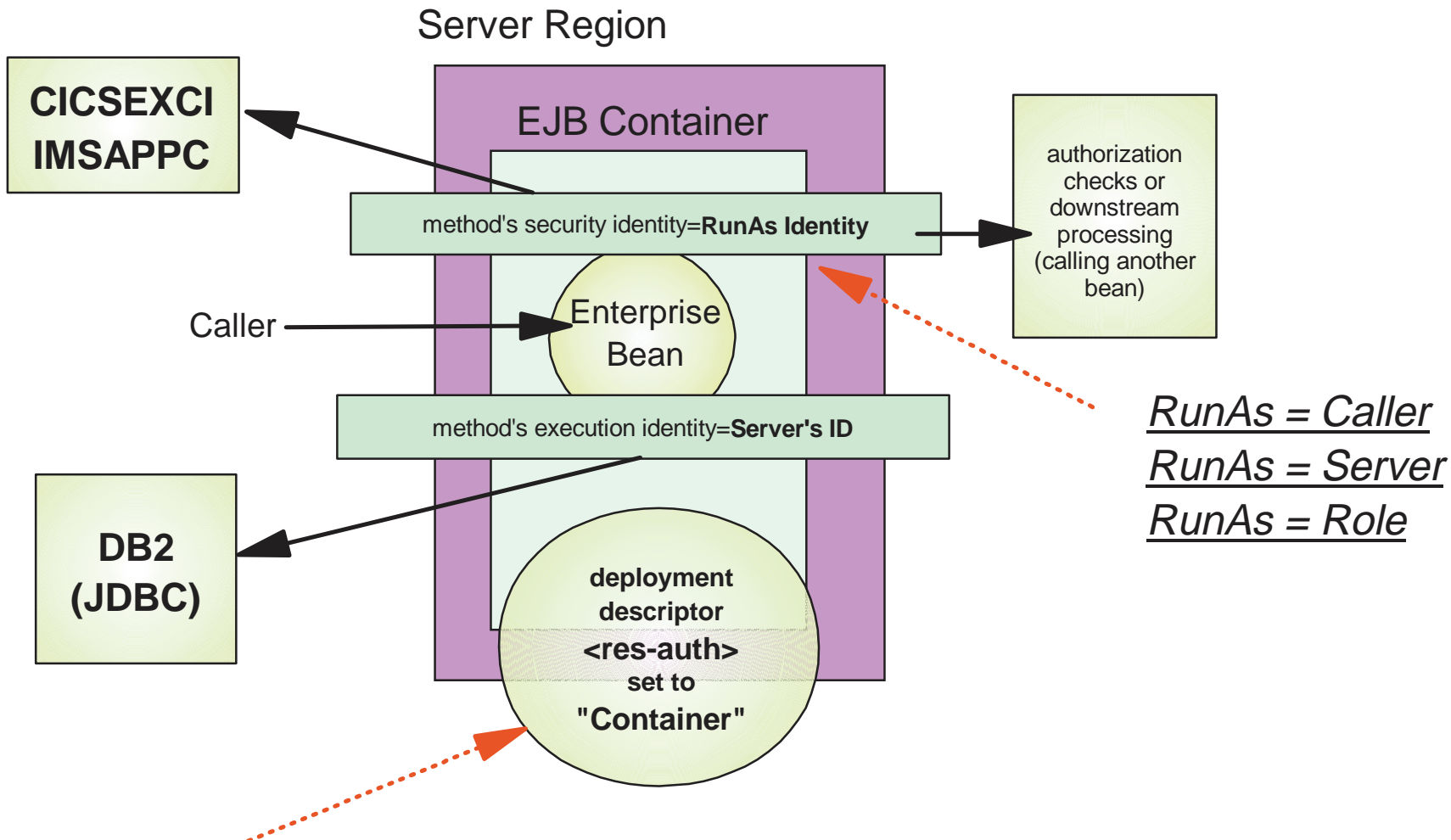


Resource Authorization

- Resource authorization allows deployer to say what identity should be passed to a resource manager:
 - ▶ "Container"
 - ▶ "Application"
- JCA Connections
 - ▶ "Container" - the current identity set by RunAs will be passed
 - ▶ "Application" - userid passed on getConnection method will be used (or if none, then server region's userid)
- JDBC Connections
 - ▶ "Container" - server region's userid will be passed
 - ▶ "Application" - userid passed on getConnection method will be used (or if none, then server region's userid)

WebSphere Authorization

EJB Container - Connectors



Control user identity on getConnection method by setting **<res-auth>** element in deployment descriptor:

- **Container**
- **Application**

WebSphere Authorization

EJB Container - Connectors

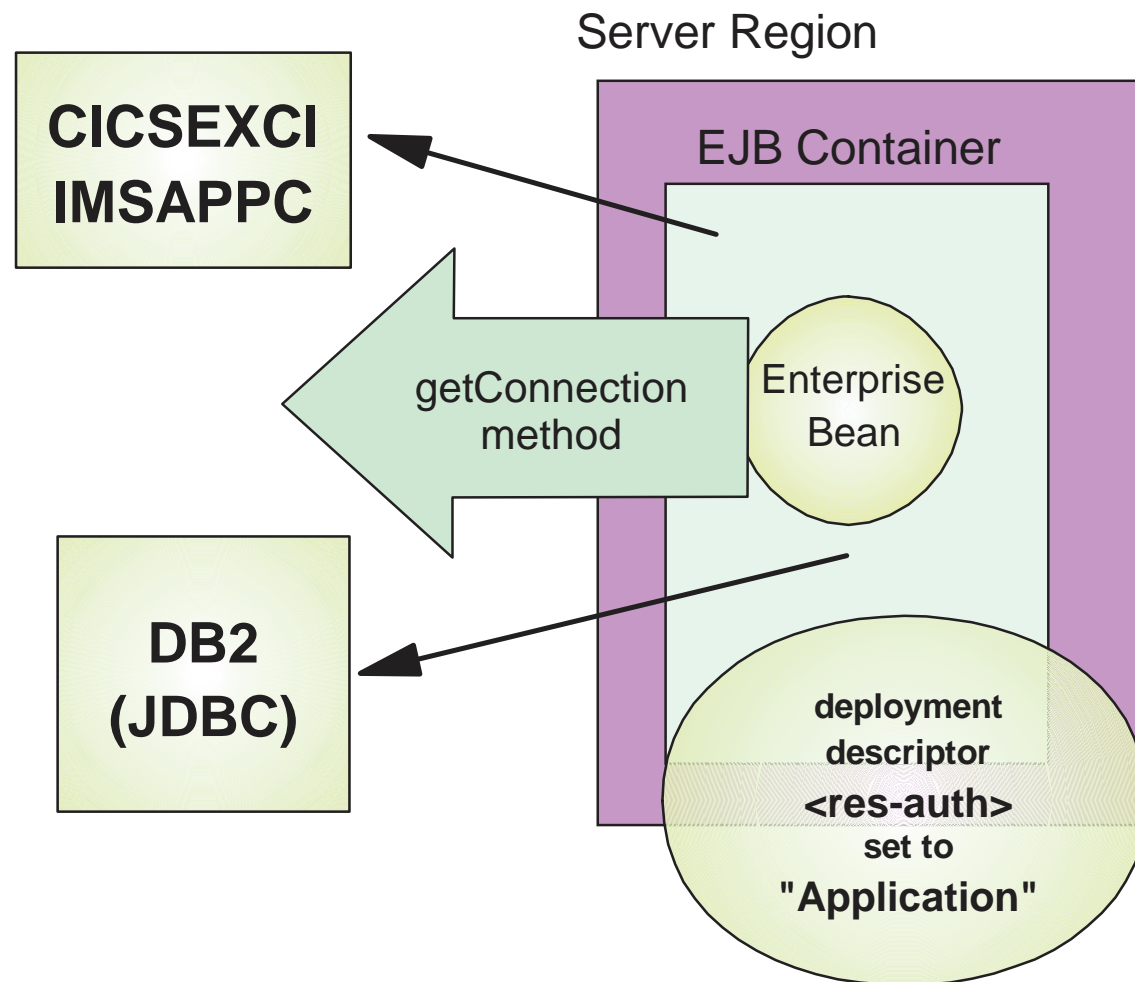
Deployment Descriptor
<res-auth> set to "Application"

getConnection method without user ID and password:

- connectors use server region user ID

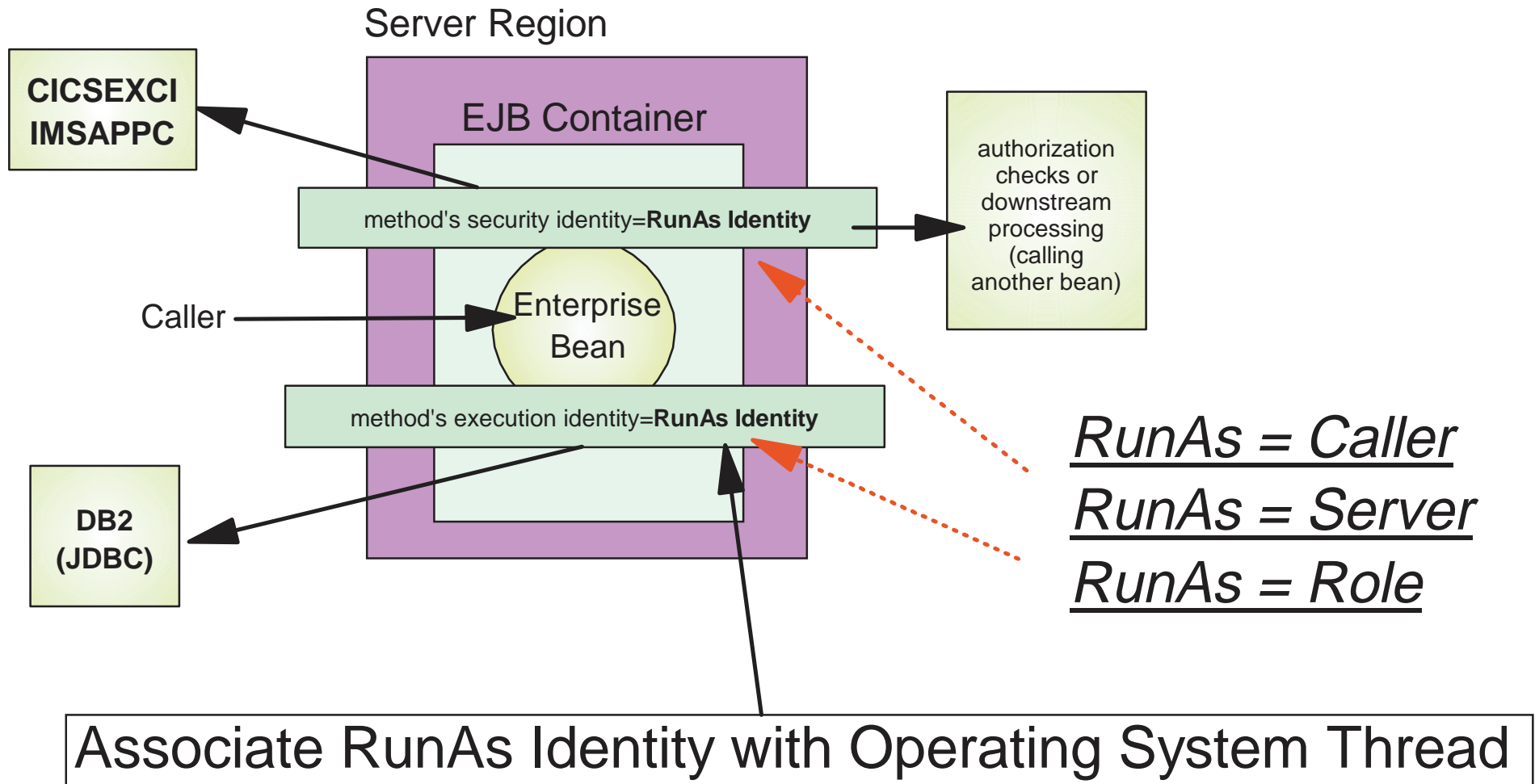
getConnection method with user ID and password:

- connectors use user ID passed on getConnection method



WebSphere Authorization

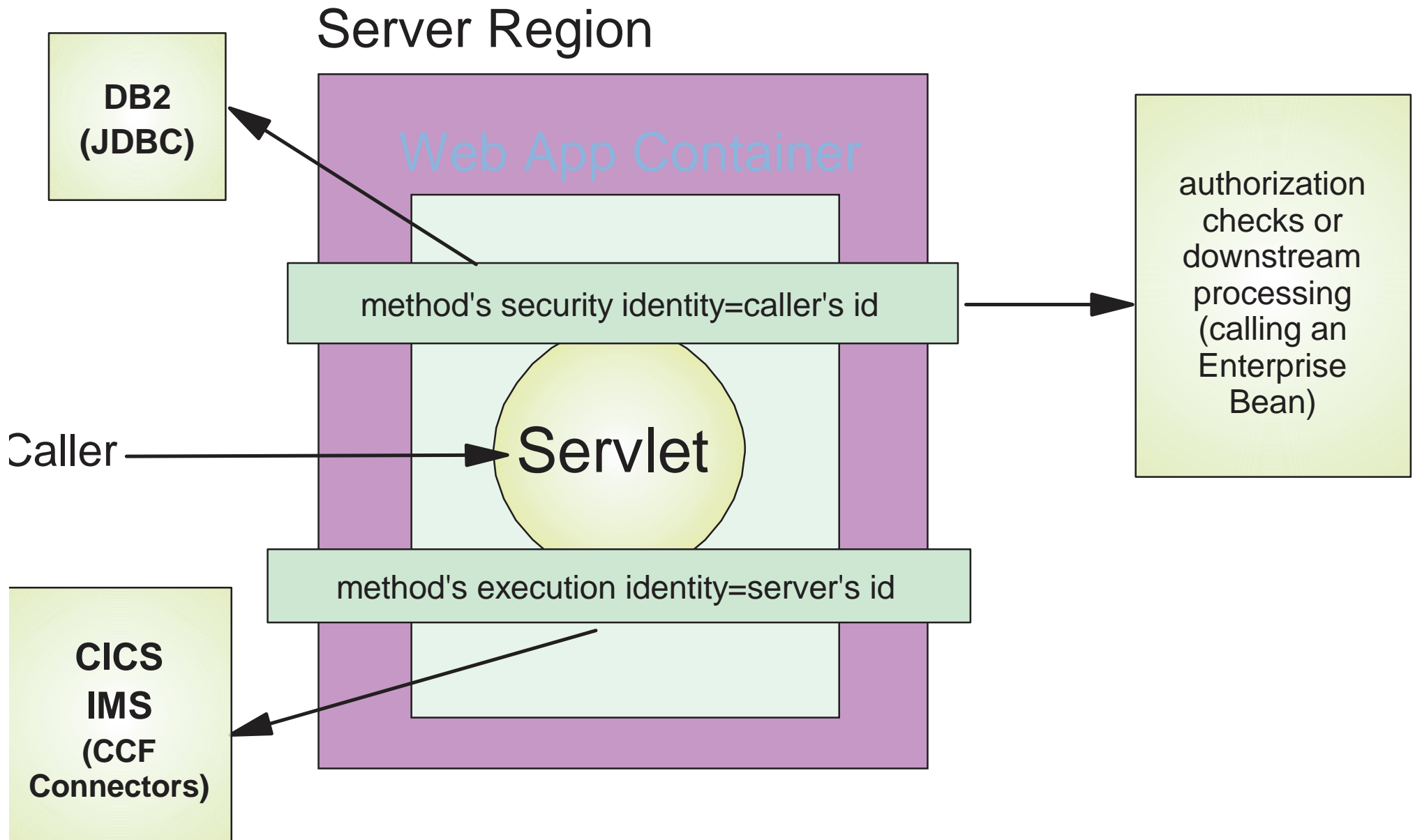
Synchronize OS Thread to RunAs Identity



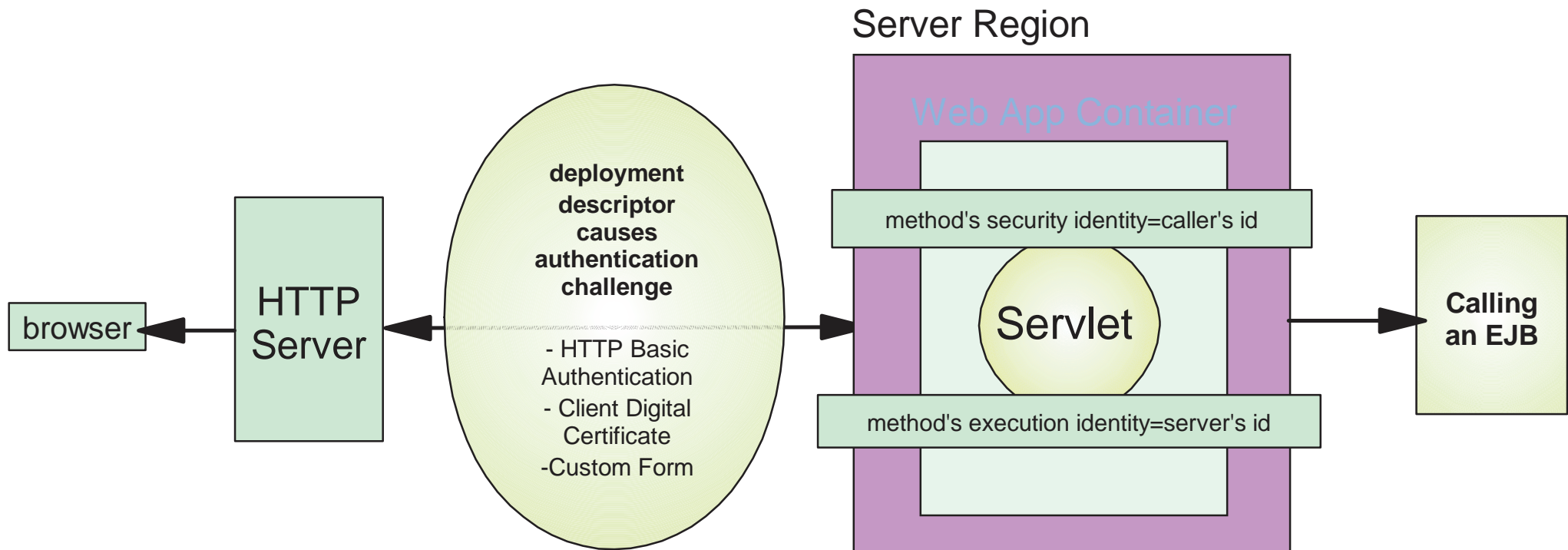
1. Use AAT to set "Synchronize to OS Thread" property for a specific method
2. Use SMUI to configure J2EE server to enable setting OS Thread to RunAs identity

WebSphere Authorization

Web App Container - Default Behaviors



Web Application Container Authentication



WebSphere 4.0 Security Mechanisms

■ Security in WAS/390 runtime

- ▶ RACF profiles & permissions
- ▶ HFS file/directory permission & ownership
- ▶ LDAP ACLs
- ▶ DB2 GRANTS
- ▶ SSL
- ▶ Kerberos
- ▶ EJB Roles & Runas support

