24TH ANNUAL
VANGUARD SECURITY 2010
the ONE event you need to attend
Flamingo Las Vegas
April 19-22, 2010

RTT5 - WebSphere Application Server for z/OS V7 Security

Mike Kearney
IBM Corporation

20-Apr-10

Session Abstract:

In this session, we'll cover everything a RACF Administrator needs to know about the WebSphere Application Server for z/OS. Topics include how a cell is built, the RACF classes and profiles involved, how WebSphere performs authentication and authorization, and how it uses SSL. The use of virtual keyrings and other best practices will be discussed.

Instructor's Bio:

Mike Kearney has worked for IBM for 31 years and has specialized in mainframe security for 18 years. He earned his CISSP in 1997. His background includes RACF and Internet security. Mike's current specialty is securing IBM's WebSphere Application Server.

Note: These Materials present the views and opinions of the Author. Vanguard does not necessarily endorse the materials and Vanguard is not responsible for the accuracy of the materials. These materials may not be redistributed or reproduced without the express permission of Vanguard or the Author.

WebSphere software

The leading software platform for on demand business

WebSphere. software

WebSphere Application Server Security

Tuesday, April 20, 2010   4:15pm – 5:30pm
Session RTT5
Mike Kearney, IBM

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.

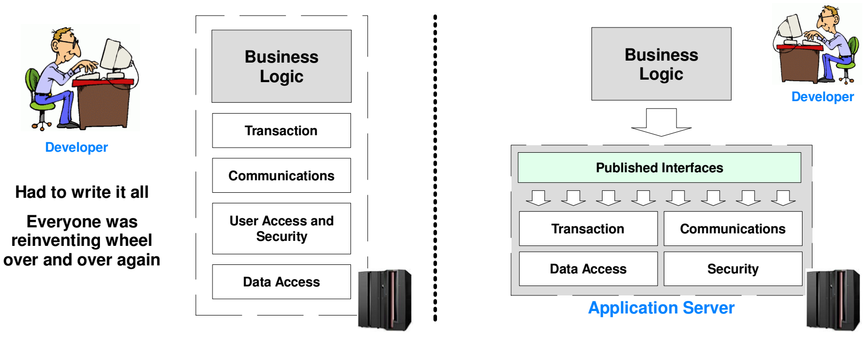
Agenda

- Overview of the WebSphere configuration process.
- Review the RACF definitions.
- Admin users and the virtual keyring.

What An “Application Server” Provides

WebSphere Application Server is an “application server” … but what is that?

In the “Old Days” Nowadays



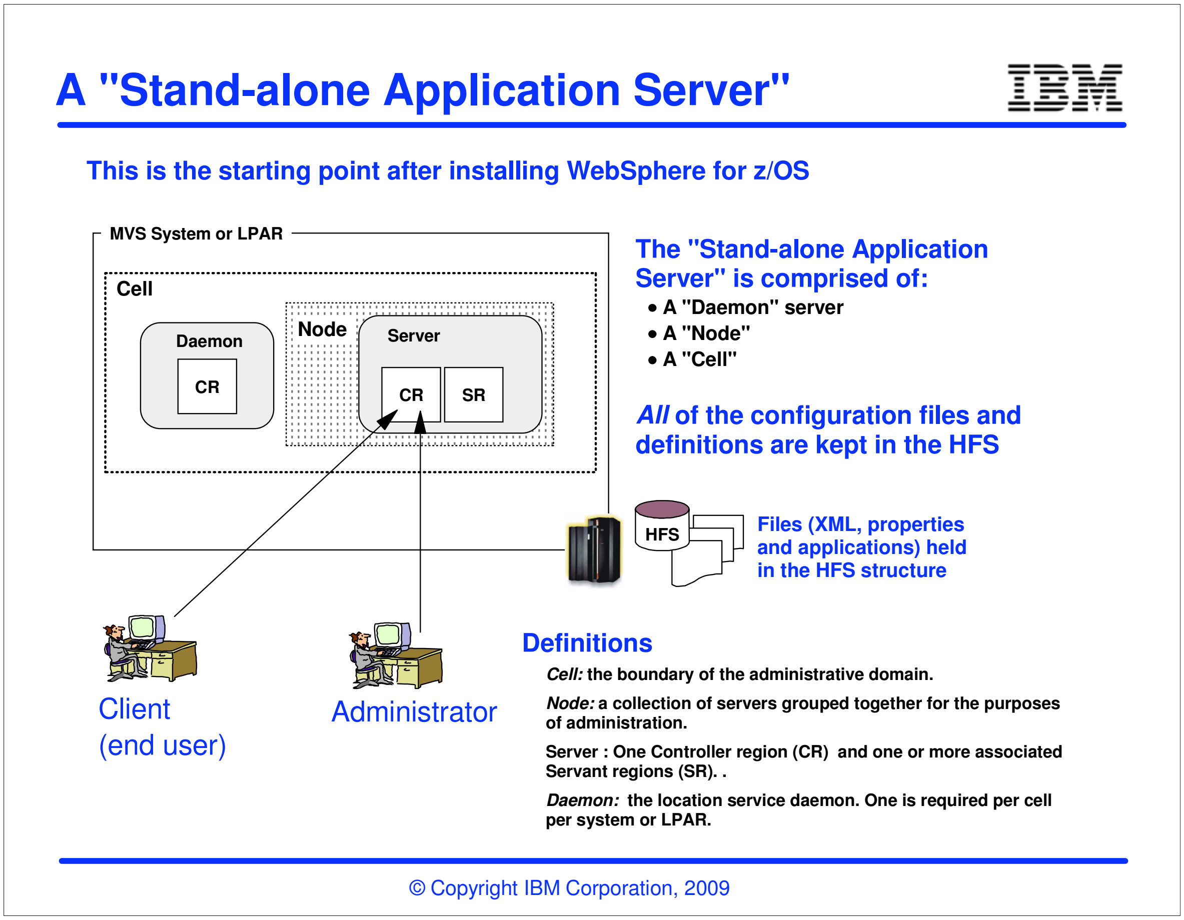
Purpose is to provide pre-packaged application support stuff so developers can focus on the main business task. No more re-inventing the wheel.

This is not new with WebSphere … IBM had an application server back in 1968!*

So what’s the key difference between WebSphere and past application servers?

Backend data…

* CICS is an application server



A "Stand-alone Application Server"

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

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**

Files (XML, properties and applications) held in the HFS structure

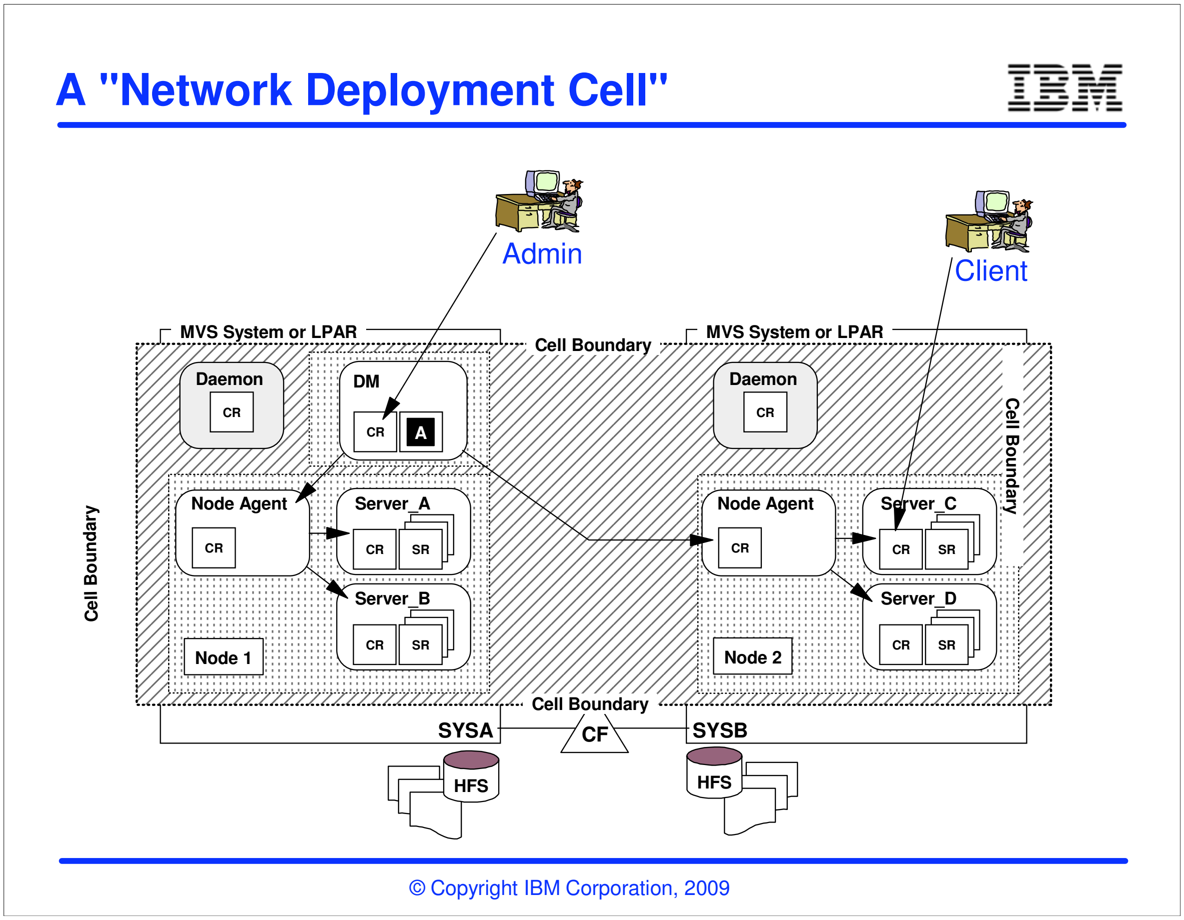
Definitions

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.**



A "Network Deployment Cell"

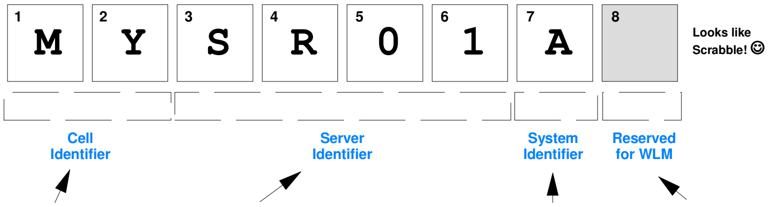
Building a WebSphere Cell

- A WebSphere cell is too complex to build by hand. A tool called the PMT is provided to generate the commands and jobs needed to build a cell.
  - Previous to V6.1, ISPF scripts were used.
  - The ISPF scripts were retired in V7.
- The PMT generates RACF commands, which you may be asked to run.
- We'll discuss the PMT and the RACF commands produced.

A Best Practice Cell Naming Convention

The focus is on the short names, since that's what imposes the length limitations. Here are the bare-bones basics of it:

Plan out the server short names and make the z/OS JOBNAME for the controller equal to the server short name



This is the key … start all names for a cell with the same starting characters

Example shows two characters. You may expand to three or four, but realize you'll have to take it from elsewhere in the limit of 7 characters

Spreadsheet based on a two character cell identifier

Suggestions:
- SRnn for application servers
- AGNT for Node Agents
- DMGR for Deployment Managers
- DEMN for Daemons

Just characters … you can use whatever works best for you

Use this to identify which LPAR this component resides on

WLM will automatically start servants and adjunct regions (used for default messaging)

S = servant

A = adjunct

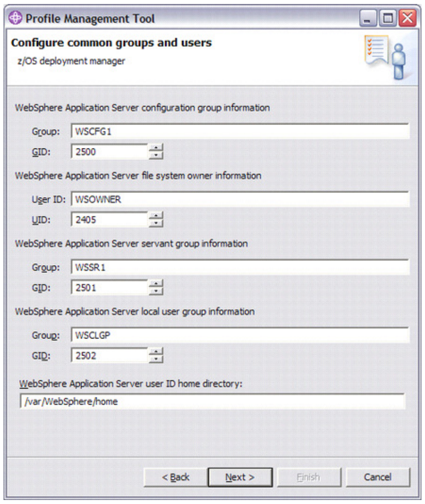
Other things -- JCL start procedures, RACF userids -- are also limited in length, but the naming is a bit more flexible.

But start all names with same cell identifier

http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101030

The PMT Configuration Tool

Is a workstation graphical tool that captures key names, values and input from the WebSphere Admin (sysprog) and imbeds those values in customized batch jobs.



Configure common groups and users

z/OS deployment manager

WebSphere Application Server configuration group information

Group: WSCFG1

GID: 2500

WebSphere Application Server file system owner information

User ID: WSOWNER

UID: 2405

WebSphere Application Server servant group information

Group: WSSR1

GID: 2501

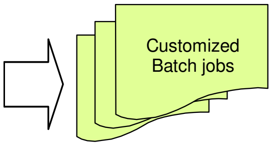
WebSphere Application Server local user group information

Group: WSCLGP

GID: 2502

WebSphere Application Server user ID home directory:

/var/WebSphere/home



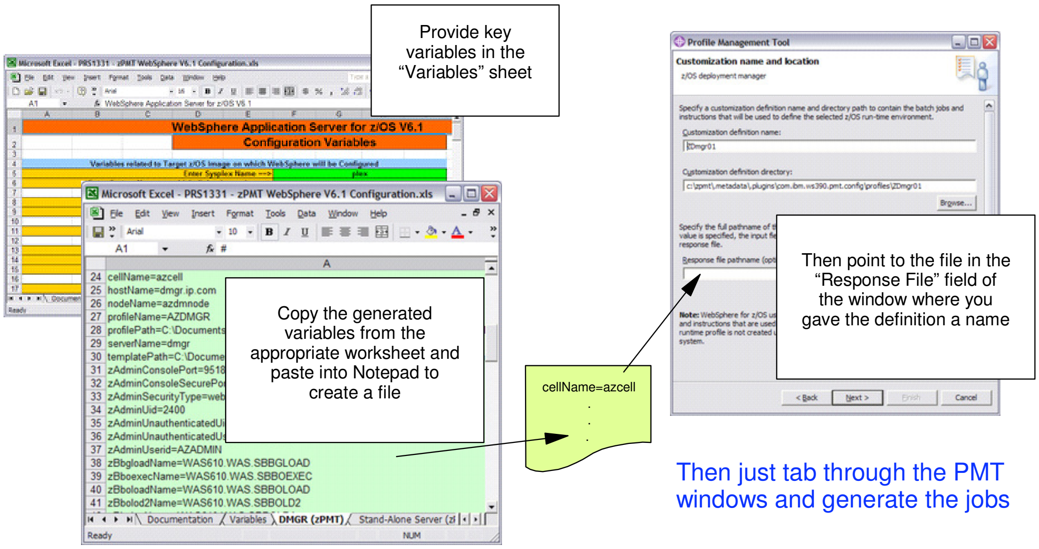
These get uploaded to z/OS where they're submitted, one after another, to create the configuration runtime.

Uploading and running the jobs is the easy part.

The real challenge is coming up with all the names and values and ports the PMT is going to ask for. Without a plan for those names you'll very quickly get confused.

Best Practice: PRS3341 Planning Spreadsheet

An Excel spreadsheet that makes planning values and using the PMT much easier, enforcing a disciplined "top down" design:


Microsoft Excel - PRS1331 - zPMT WebSphere V6.1 Configuration.xls
File Edit View Insert Format Tools Data Window Help
Arial 10
A1
WebSphere Application Server for z/OS V6.1
Configuration Variables
Variables related to Target z/OS image on which WebSphere will be Configured
Enter Sysplex Name -->
plex
Documentation
Variables
DMGR (zPMT)
Stand-Alone Server (z
Ready
NUM
Profile Management Tool
Browse...
< Back
Next >
Finish
Cancel

Provide key variables in the "Variables" sheet

```
24 cellName=azcell
25 hostName=dmgr.ip.com
26 nodeName=azdmnode
27 profileName=AZDMGR
28 profilePath=C:\Documents
29 serverName=dmgr
30 templatePath=C:\Docume
31 zAdminConsolePort=9518
32 zAdminConsoleSecurePo
33 zAdminSecurityType=web
34 zAdminUid=2400
35 zAdminUnauthenticatedUi
36 zAdminUnauthenticatedU
37 zAdminUserid=AZADMIN
38 zBbgloadName=WAS610.WAS.SBBGLOAD
39 zBboexecName=WAS610.WAS.SBBOEXEC
40 zBboloadName=WAS610.WAS.SBBOLOAD
41 zBbolod2Name=WAS610.WAS.SBBOLD2
```

Copy the generated variables from the appropriate worksheet and paste into Notepad to create a file

cellName=azcell
.
.
.

Customization name and location

z/OS deployment manager

Specify a customization definition name and directory path to contain the batch jobs and instructions that will be used to define the selected z/OS run-time environment.

Customization definition name: ZDmgr01

Customization definition directory: c:\zpmt\.metadata\.plugins\com.ibm.ws390.pmt.config\profiles\ZDmgr01

Specify the full pathname of t value is specified, the input fi response file.

Response file pathname (opt

Note: WebSphere for z/OS us and instructions that are used runtime profile is not created u system.

Then point to the file in the "Response File" field of the window where you gave the definition a name

Then just tab through the PMT windows and generate the jobs

http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS3341

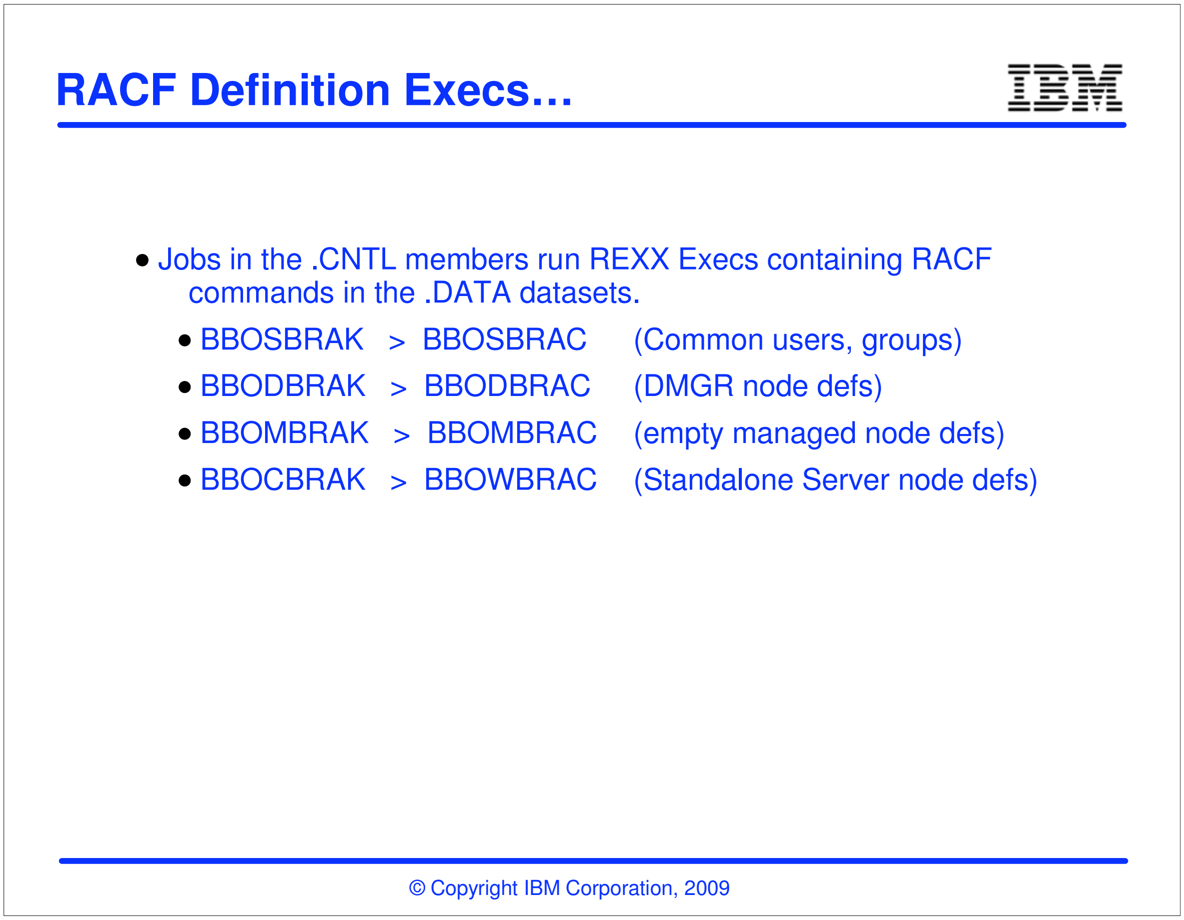
Best Practice for WebSphere Userids

- **All the Servant Regions run under one RACF userid.**
  - Application Server servant regions, DM servant region.
    - Applications run in these regions.
    - Additional userids as circumstances warrant.
- **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.
- **Also known as the 'two userid' approach.**

- http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100653

Output of PMT

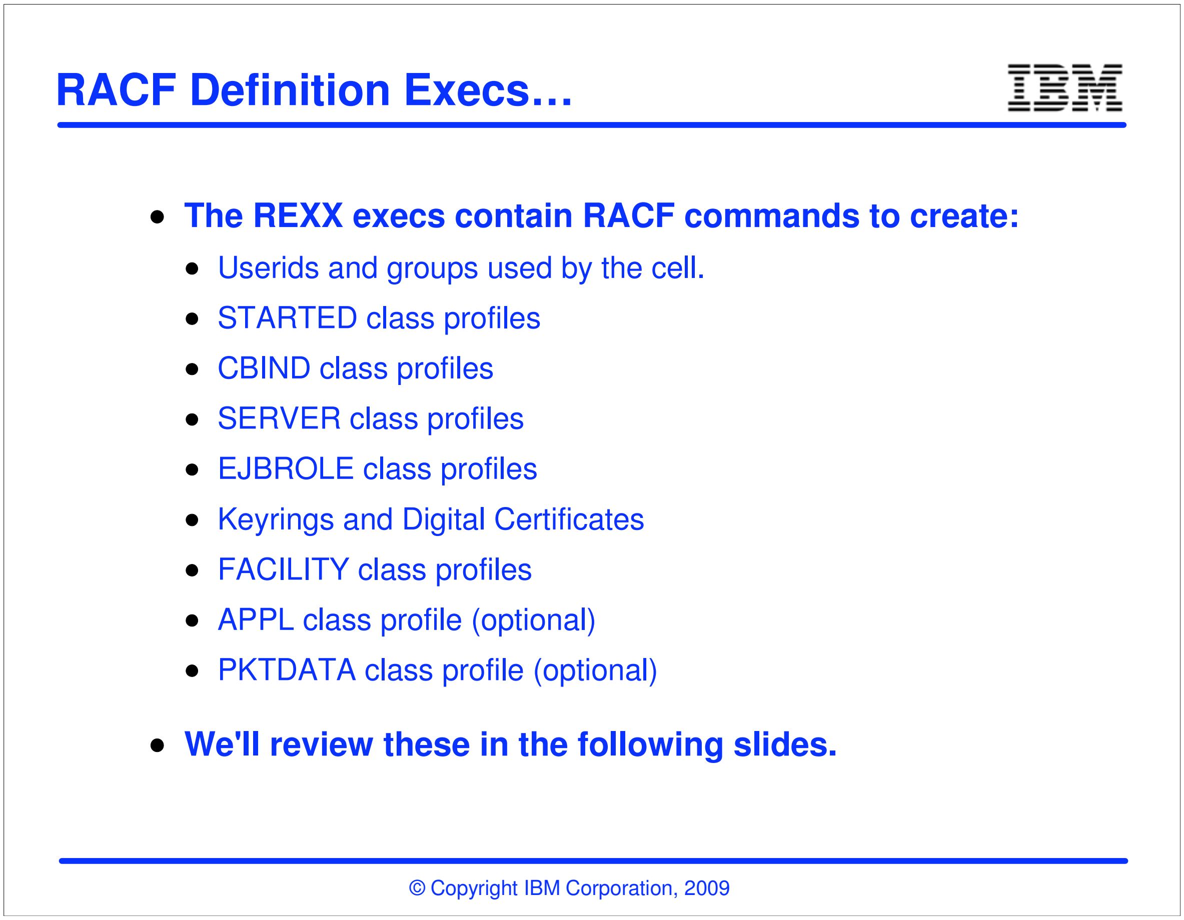
- **The jobs produced by the PMT build the cell:**
  - Build the file system used by WebSphere.
  - Build the many .xml control files used by WebSphere
  - Build procs for starting the various WebSphere regions.
  - **Build RACF commands for defining the cell.**
- **The jobs produced by the Customization steps go into the .CNTL pds.**
- **These jobs execute commands which are stored in members in the .DATA pds.**



RACF Definition Execs…

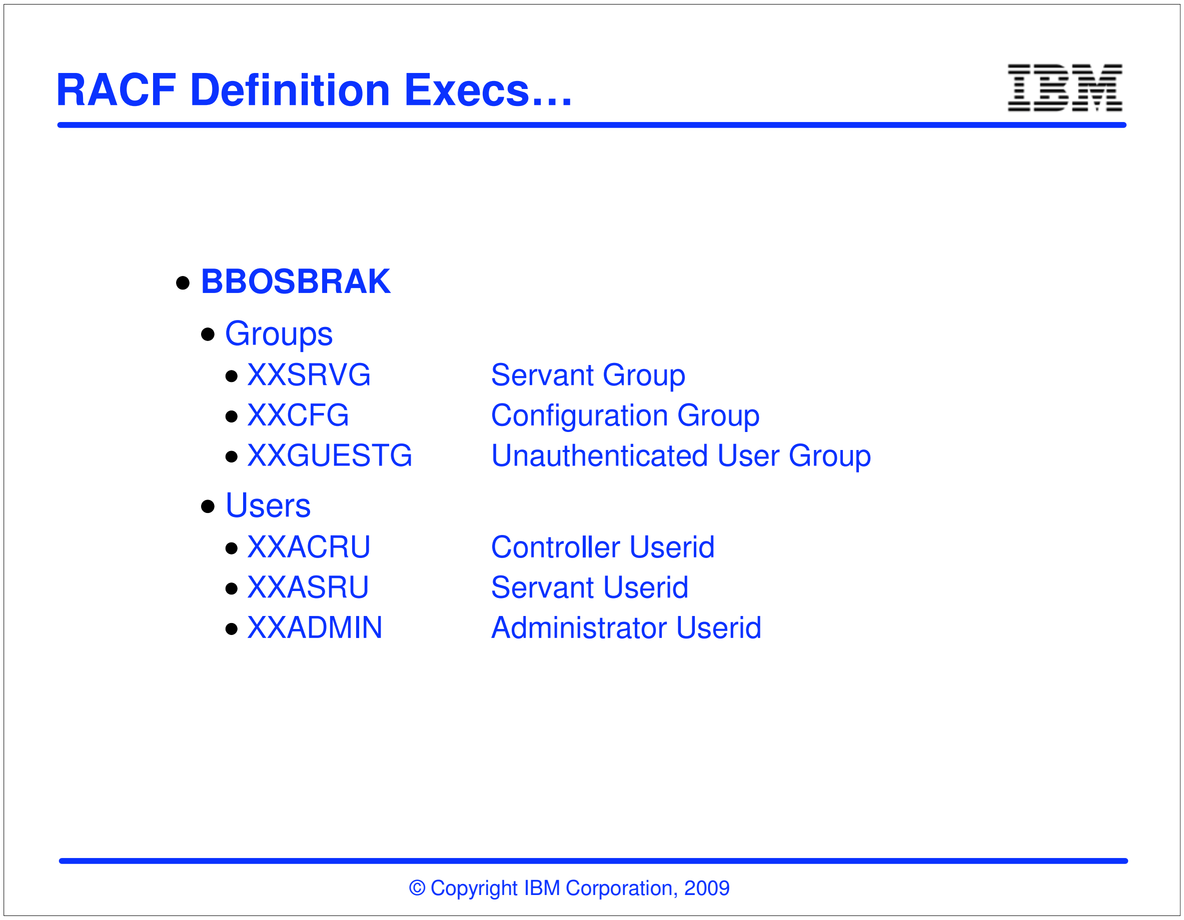
- Jobs in the .CNTL members run REXX Execs containing RACF commands in the .DATA datasets.

• BBOSBRAK	>	BBOSBRAC	(Common users, groups)
• BBODBRAK	>	BBODBRAC	(DMGR node defs)
• BBOMBRAK	>	BBOMBRAC	(empty managed node defs)
• BBOCBRAK	>	BBOWBRAC	(Standalone Server node defs)



RACF Definition Execs…

- **The REXX execs contain RACF commands to create:**
  - Userids and groups used by the cell.
  - STARTED class profiles
  - CBIND class profiles
  - SERVER class profiles
  - EJBROLE class profiles
  - Keyrings and Digital Certificates
  - FACILITY class profiles
  - APPL class profile (optional)
  - PKTDATA class profile (optional)
- **We'll review these in the following slides.**



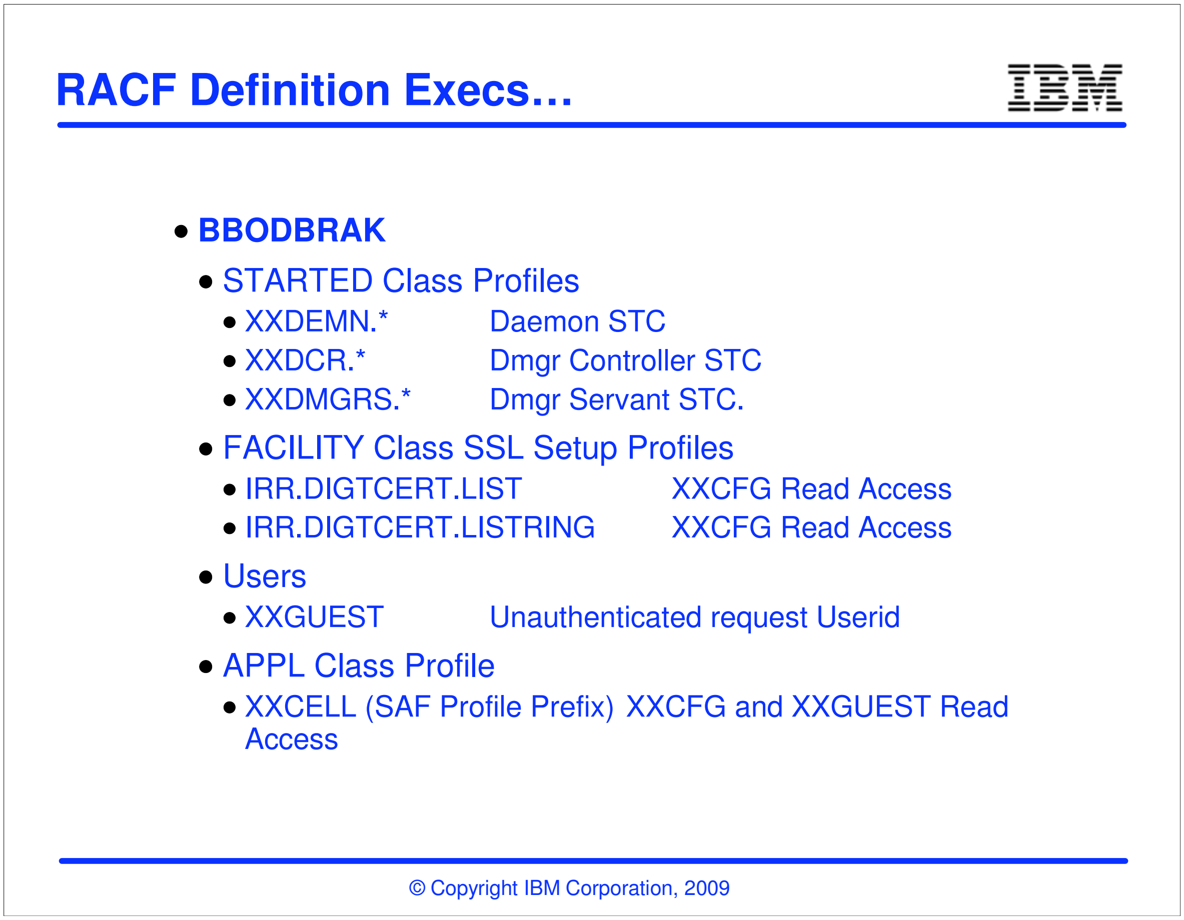
RACF Definition Execs…

- **BBOSBRAK**
  - Groups

XXSRVG	Servant Group
XXCFG	Configuration Group
XXGUESTG	Unauthenticated User Group

  - Users

XXACRU	Controller Userid
XXASRU	Servant Userid
XXADMIN	Administrator Userid



RACF Definition Execs…

- **BBODBRAK**
  - STARTED Class Profiles

XXDEMN.*	Daemon STC
XXDCR.*	Dmgr Controller STC
XXDMGRS.*	Dmgr Servant STC.

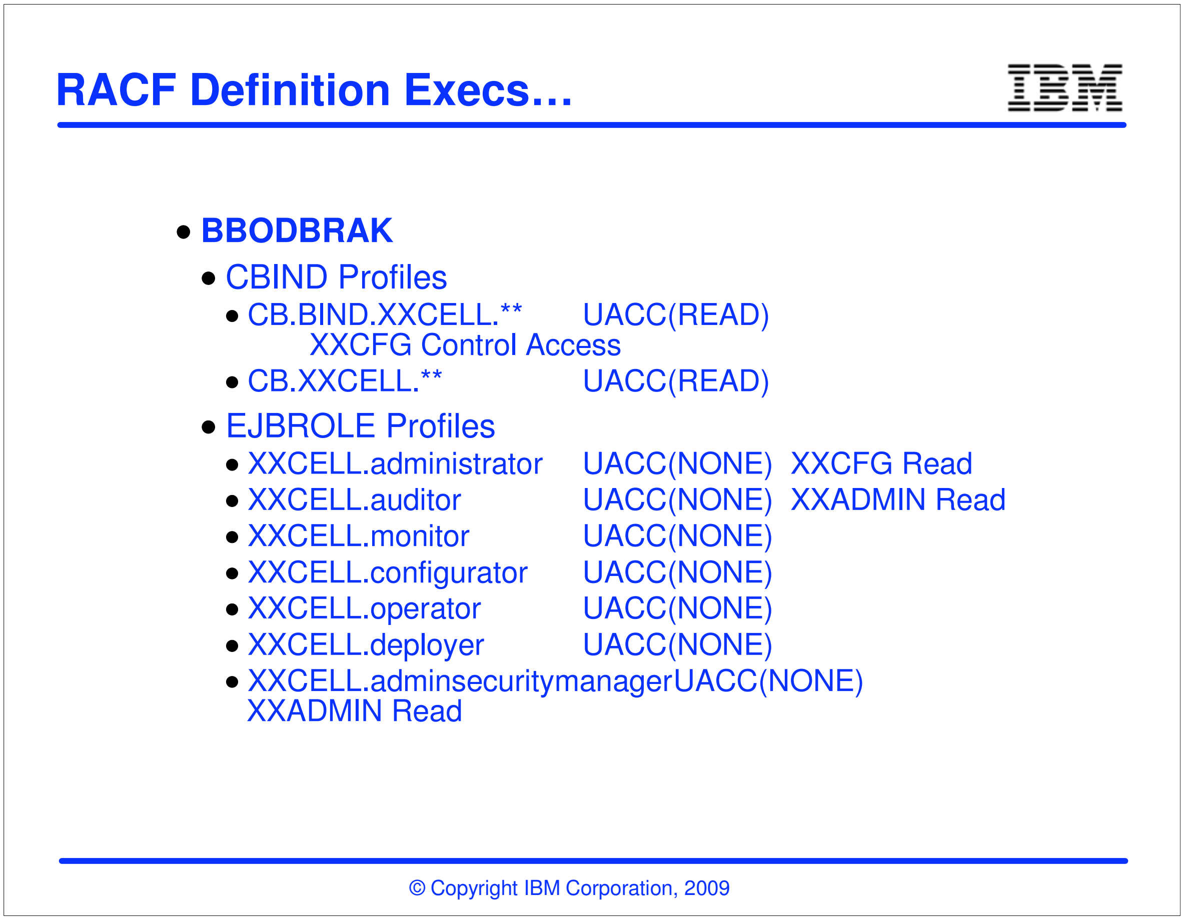
  - FACILITY Class SSL Setup Profiles

IRR.DIGTCERT.LIST	XXCFG Read Access
IRR.DIGTCERT.LISTRING	XXCFG Read Access

  - Users

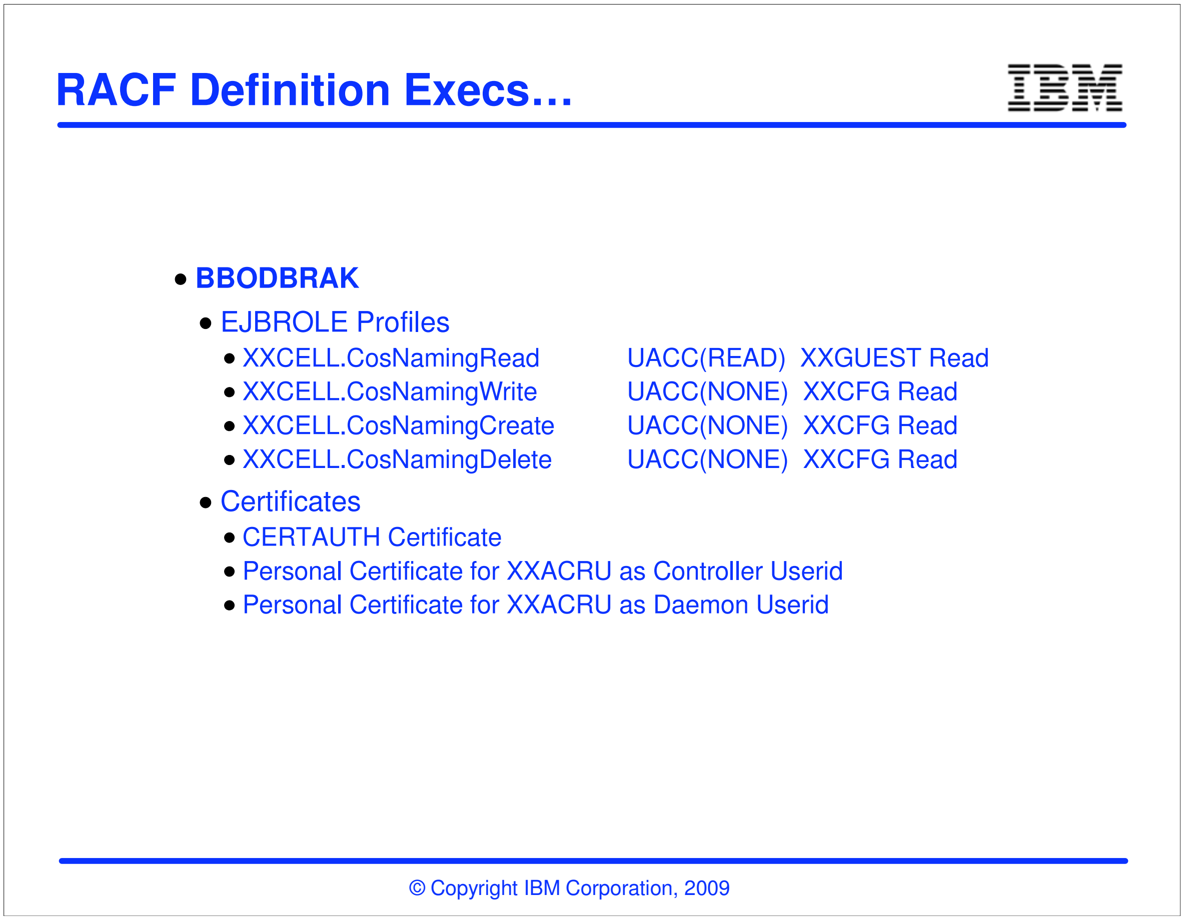
XXGUEST	Unauthenticated request Userid

  - APPL Class Profile
    - XXCELL (SAF Profile Prefix) XXCFG and XXGUEST Read Access



RACF Definition Execs…

- **BBODBRAK**
  - CBIND Profiles
    - CB.BIND.XXCELL.**   UACC(READD)
      XXCFG Control Access
    - CB.XXCELL.**   UACC(READ)
  - EJBROLE Profiles
    - XXCELL.administrator   UACC(NONE) XXCFG Read
    - XXCELL.auditor   UACC(NONE) XXADMIN Read
    - XXCELL.monitor   UACC(NONE)
    - XXCELL.configurator   UACC(NONE)
    - XXCELL.operator   UACC(NONE)
    - XXCELL.deployer   UACC(NONE)
    - XXCELL.adminsecuritymanagerUACC(NONE)
      XXADMIN Read



RACF Definition Execs…

- **BBODBRAK**
  - EJBROLE Profiles
    - XXCELL.CosNamingRead   UACC(READ) XXGUEST Read
    - XXCELL.CosNamingWrite   UACC(NONE) XXCFG Read
    - XXCELL.CosNamingCreate   UACC(NONE) XXCFG Read
    - XXCELL.CosNamingDelete   UACC(NONE) XXCFG Read
  - Certificates
    - CERTAUTH Certificate
    - Personal Certificate for XXACRU as Controller Userid
    - Personal Certificate for XXACRU as Daemon Userid

RACF Definition Execs…

- **BBODBRAK**
  - Keyrings

XXACRU Personal	Personal (Controller and Daemon), CERTAUTH, and Commercial
XXACRU Root Keyrings (2)	CERTAUTH
XXASRU	CERTAUTH and Commercial
XXADMIN	CERTAUTH and Commercial

  - FACILITY CLASS Miscellaneous Profiles.

BBO.SYNC.XXCELL.**	UACC(NONE)
BBO.TRUSTEDAPPS.XXCELL.**	UACC(NONE) XXCFG Read

RACF Definition Execs…

- **BBOMBRAK**
  - Users

XXADMSH	Asynchronous Admin Task Userid

  - SERVER Class Profiles

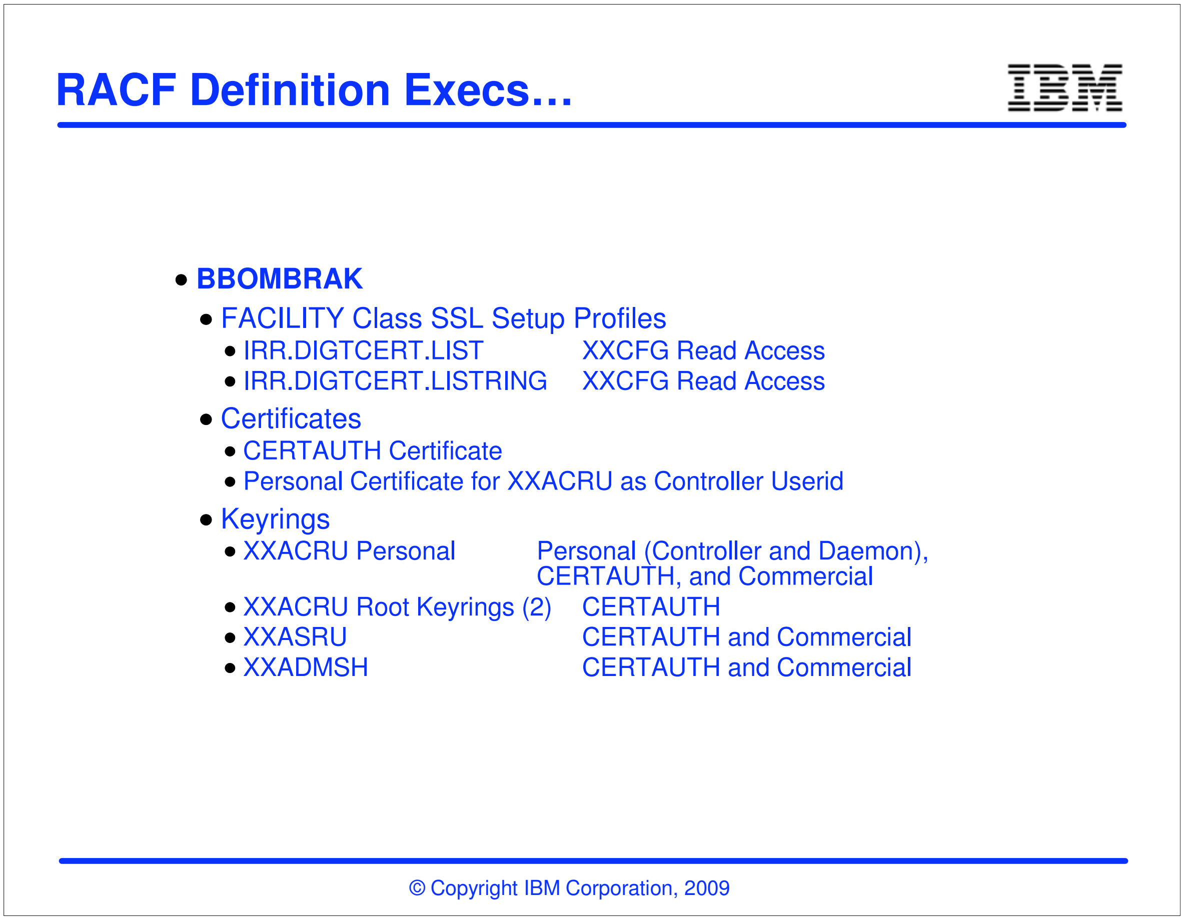
CB.*	UACC(NONE)

  - FACILITY Class Profile for WLM Services

BPX.WLMSERVER	UACC(NONE) XXSRVG Read

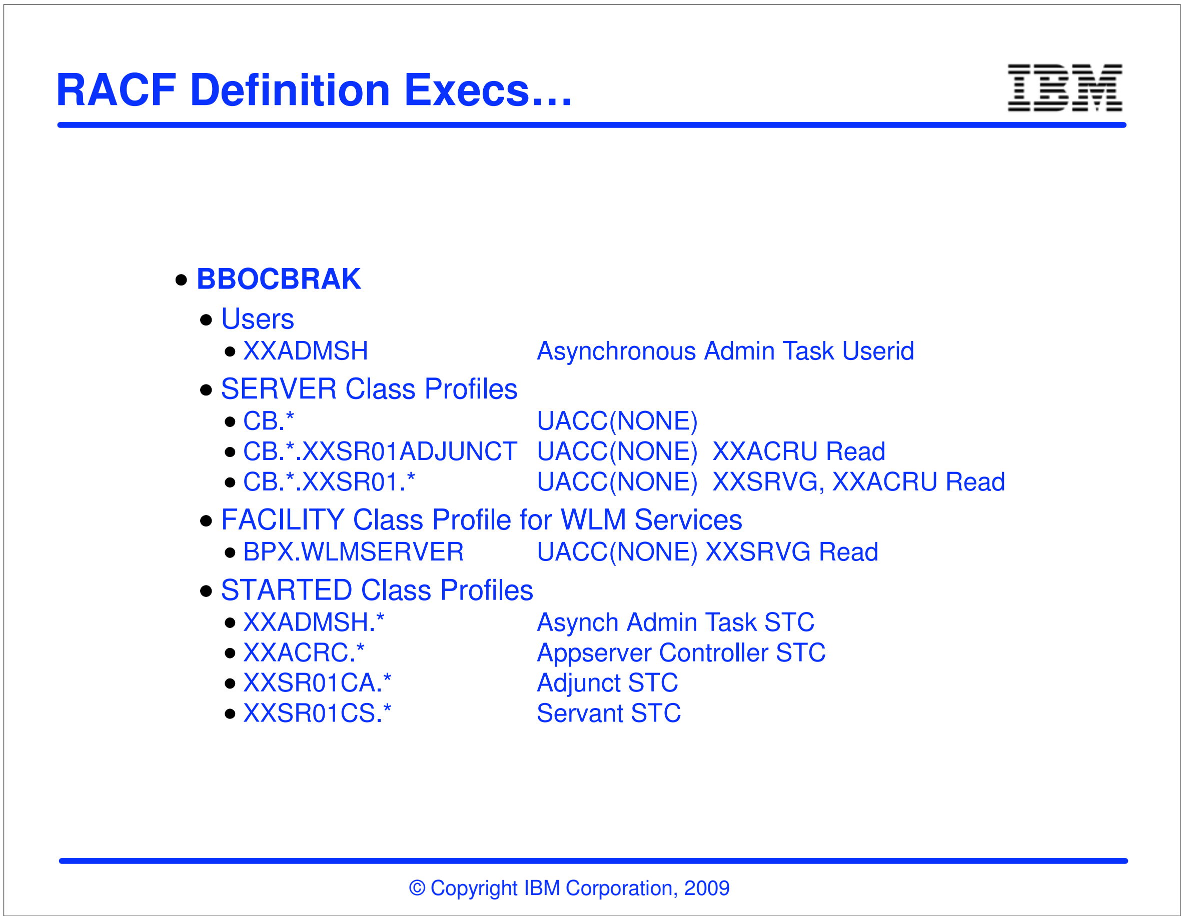
  - STARTED Class Profiles

XXADMSH.*	Asynch Admin Task STC
XXDEMNC.*	Node Specific Daemon STC
XXACRC.*	Appserver Controller STC



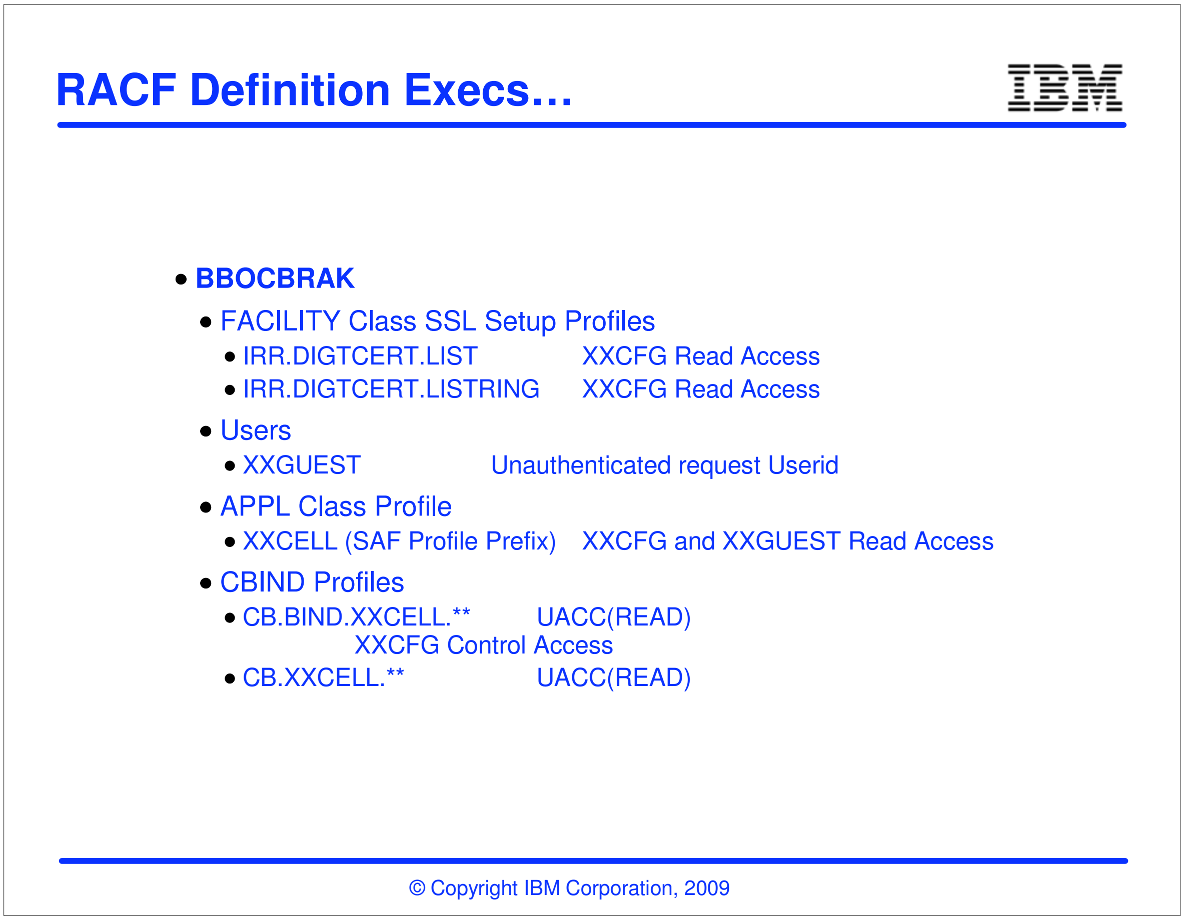
RACF Definition Execs…

- **BBOMBRAK**
  - FACILITY Class SSL Setup Profiles
    - IRR.DIGTCERT.LIST XXCFG Read Access
    - IRR.DIGTCERT.LISTRING XXCFG Read Access
  - Certificates
    - CERTAUTH Certificate
    - Personal Certificate for XXACRU as Controller Userid
  - Keyrings
    - XXACRU Personal Personal (Controller and Daemon), CERTAUTH, and Commercial
    - XXACRU Root Keyrings (2) CERTAUTH
    - XXASRU CERTAUTH and Commercial
    - XXADMSH CERTAUTH and Commercial



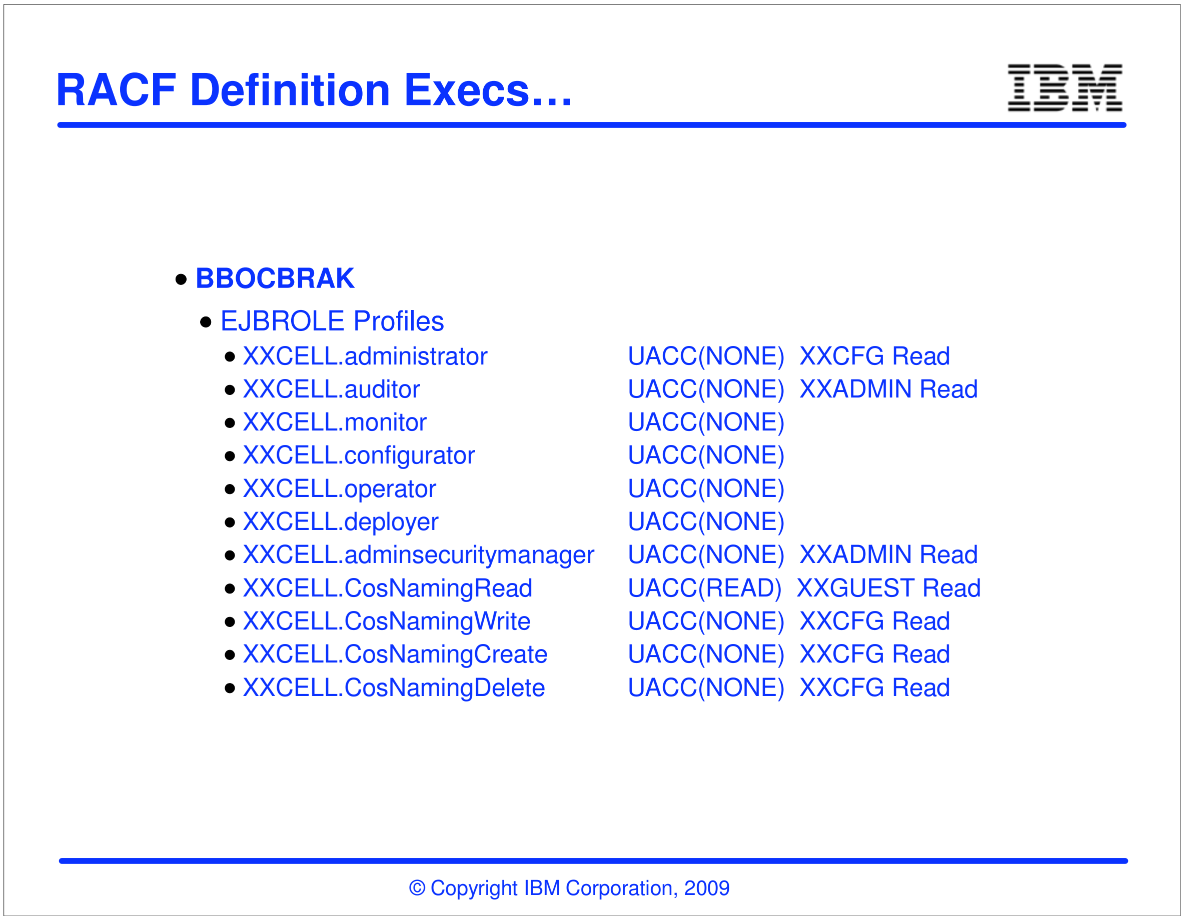
RACF Definition Execs…

- **BBOCBRAK**
  - Users
    - XXADMSH Asynchronous Admin Task Userid
  - SERVER Class Profiles
    - CB.* UACC(NONE)
    - CB.*.XXSR01ADJUNCT UACC(NONE) XXACRU Read
    - CB.*.XXSR01.* UACC(NONE) XXSRVG, XXACRU Read
  - FACILITY Class Profile for WLM Services
    - BPX.WLMSERVER UACC(NONE) XXSRVG Read
  - STARTED Class Profiles
    - XXADMSH.* Asynch Admin Task STC
    - XXACRC.* Appserver Controller STC
    - XXSR01CA.* Adjunct STC
    - XXSR01CS.* Servant STC



RACF Definition Execs…

- **BBOCBRAK**
  - FACILITY Class SSL Setup Profiles
    - IRR.DIGTCERT.LIST XXCFG Read Access
    - IRR.DIGTCERT.LISTRING XXCFG Read Access
  - Users
    - XXGUEST Unauthenticated request Userid
  - APPL Class Profile
    - XXCELL (SAF Profile Prefix) XXCFG and XXGUEST Read Access
  - CBIND Profiles
    - CB.BIND.XXCELL.** UACC(READ)
      XXCFG Control Access
    - CB.XXCELL.** UACC(READ)



RACF Definition Execs…

- **BBOCBRAK**
  - EJBROLE Profiles
    - XXCELL.administrator UACC(NONE) XXCFG Read
    - XXCELL.auditor UACC(NONE) XXADMIN Read
    - XXCELL.monitor UACC(NONE)
    - XXCELL.configurator UACC(NONE)
    - XXCELL.operator UACC(NONE)
    - XXCELL.deployer UACC(NONE)
    - XXCELL.adminsecuritymanager UACC(NONE) XXADMIN Read
    - XXCELL.CosNamingRead UACC(READ) XXGUEST Read
    - XXCELL.CosNamingWrite UACC(NONE) XXCFG Read
    - XXCELL.CosNamingCreate UACC(NONE) XXCFG Read
    - XXCELL.CosNamingDelete UACC(NONE) XXCFG Read

RACF Definition Execs…

- **BBOCBRAK**
  - Certificates
    - CERTAUTH Certificate
    - Personal Certificate for XXACRU as Controller Userid
    - Personal Certificate for XXACRU as Daemon Userid
  - Keyrings

• XXACRU Personal	Personal (Controller and Daemon), CERTAUTH, and Commercial
• XXACRU Root Keyrings (2)	CERTAUTH
• XXASRU	CERTAUTH and Commercial
• XXADMIN	CERTAUTH and Commercial
• XXADMSH	CERTAUTH and Commercial

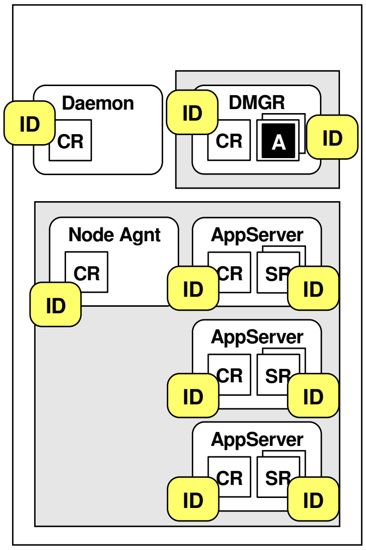
RACF Definition Execs…

- **BBOCBRAK**
  - FACILITY CLASS Miscellaneous Profiles.

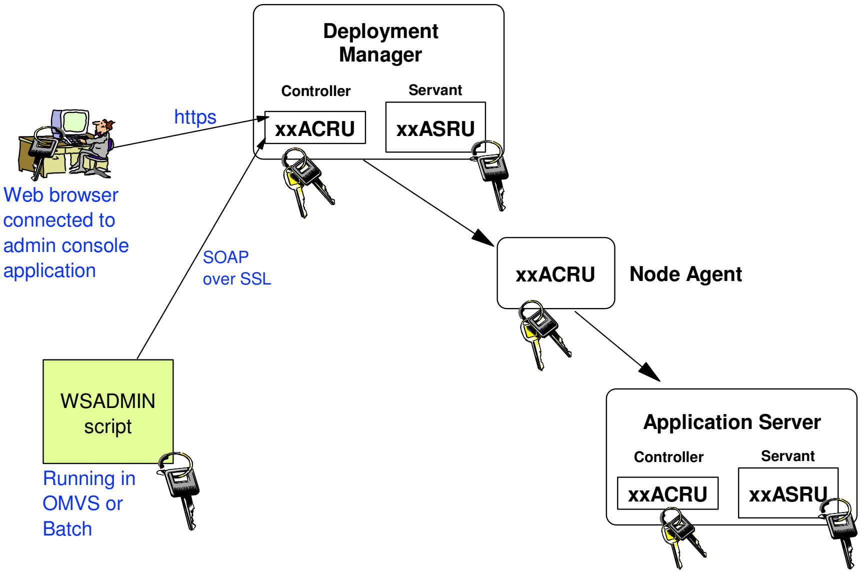
• BBO.SYNC.XXCELL.**	UACC(NONE)
• BBO.TRUSTEDAPPS.XXCELL.**	UACC(NONE) XXCFG Read

RACF profiles

- Daemon Userid gets created twice.
- Guest Userid gets created twice.
- Async Admin Task Userid gets created twice.
- More certificates than necessary are created.
- More STARTED profiles than necessary are created.
- EJBROLE profiles get created twice.
- FACILITY class profiles get created multiple times.
- This is due to the 'two userid' approach.



SSL and WebSphere Administration



Web browser connected to admin console application

Running in OMVS or Batch

WSADMIN scripting keyring

- A file named ssl.client.props names the client keyring.
- Located in the Deployment Manager's
  - /profiles/default/properties/ssl.client.props
- Sample Contents:

```
.
.
# TrustStore information
com.ibm.ssl.trustStoreName=ClientDefaultTrustStore
com.ibm.ssl.trustStore=safkeyring:///D1CellKeyring
com.ibm.ssl.trustStorePassword={xor}Lz4sLCgwLTs=
com.ibm.ssl.trustStoreType=JCERACFKS
com.ibm.ssl.trustStoreProvider=IBMJCE
com.ibm.ssl.trustStoreFileBased=false
```

Virtual Keyring

An imaginary keyring that everyone shares, that contains all of the CERTAUTH certs.

- Eliminates the need for all those client keyrings.
  - Especially useful for FTP and WebSphere clients.
- If you have authority to read your own keyring, you
  - can use the virtual keyring.
- The virtual keyring is owned by virtual user *AUTH*
- The virtual keyring has name *
- Example:
  - com.ibm.ssl.trustStore=safkeyring://*AUTH*/*

Configuring for a Virtual Keyring

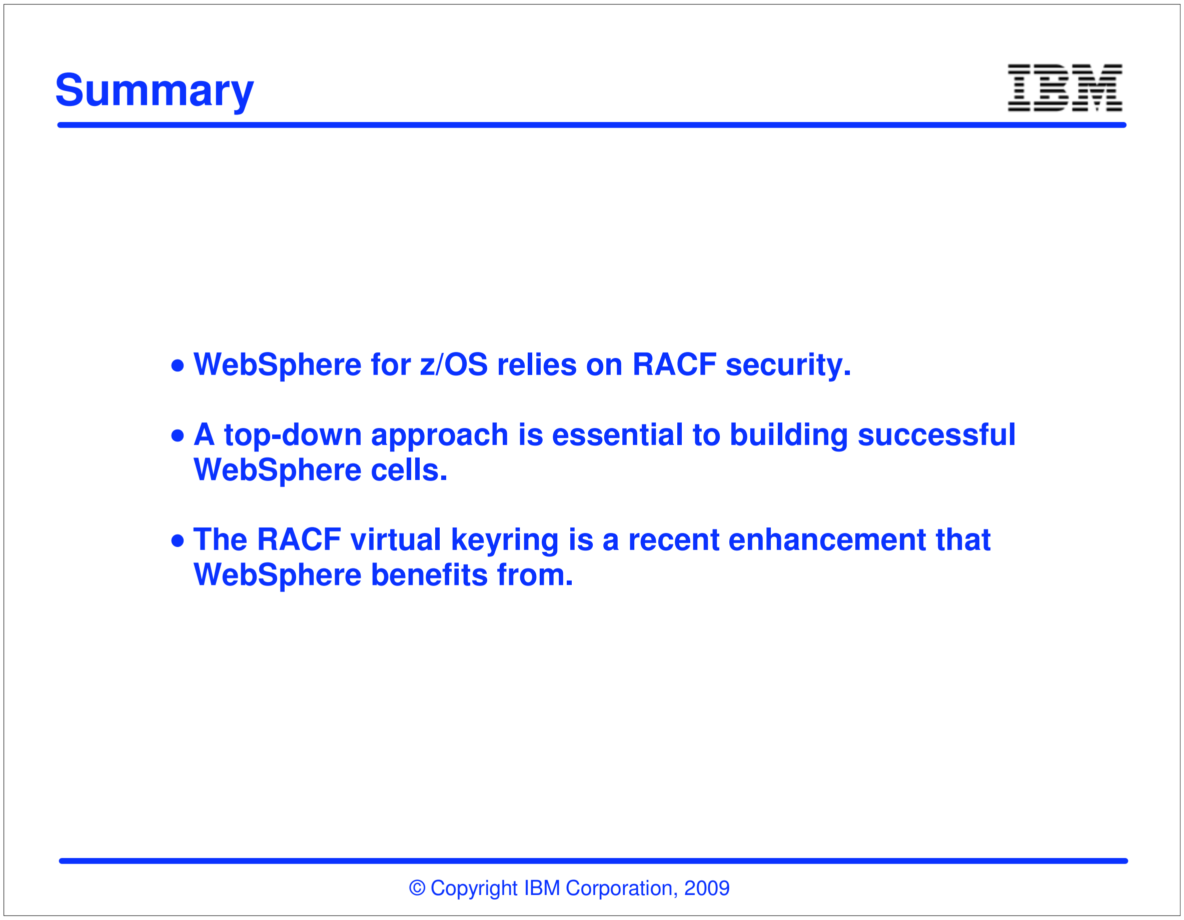
Instructions for WebSphere. FTP is similar.

1. Ensure all users have authority to use a keyring.
   READ access in FACILITY class profile:
   IRR.DIGTCERT.LISTRING
2. Edit the DM's ssl.client.props file from this:
   - com.ibm.ssl.trustStore=safkeyring:///xxWASKeyring
   - com.ibm.ssl.keyStore=safkeyring:///xxWASKeyring
   - to this:
     - com.ibm.ssl.trustStore=safkeyring://*AUTH*/*
     - com.ibm.ssl.keyStore=safkeyring://*AUTH*/*

Configuring for a Virtual Keyring (cont.)

3. No need to recycle anything.

4. Test using WSADMIN.



Summary

- WebSphere for z/OS relies on RACF security.
- A top-down approach is essential to building successful WebSphere cells.
- The RACF virtual keyring is a recent enhancement that WebSphere benefits from.