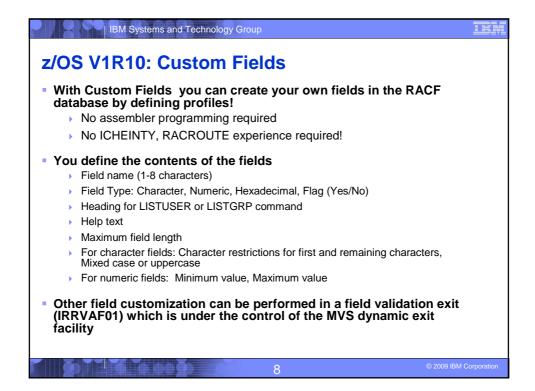


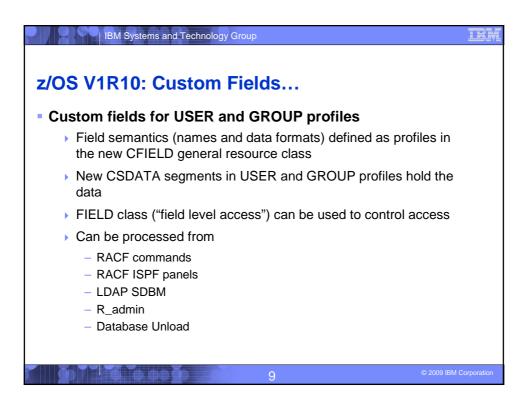
z/OS V1R10: Password Reset Granularity... With V1R10, the authority to issue the LISTUSER command can be granted based on profile ownership or group-tree ownership using FACILITY class profiles: IRR.LU.OWNER.owner-of-user Grants authority based on the user or group that owns the user IRR.LU.TREE.owner-of-group-tree Grants authority based on group tree scope Users can be excluded password reset or LISTUSER with "exclusion" profiles: IRR.PWRESET.EXCLUDE.excluded-user

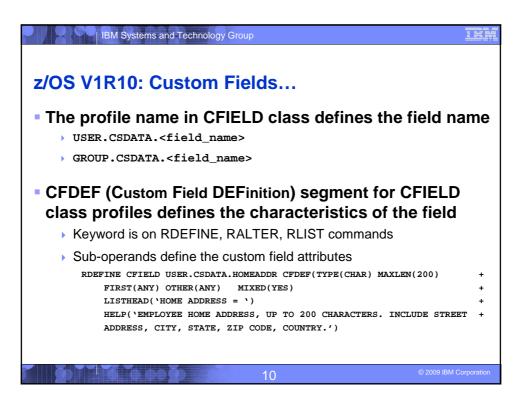
7

IRR.LU.EXCLUDE.excluded-user

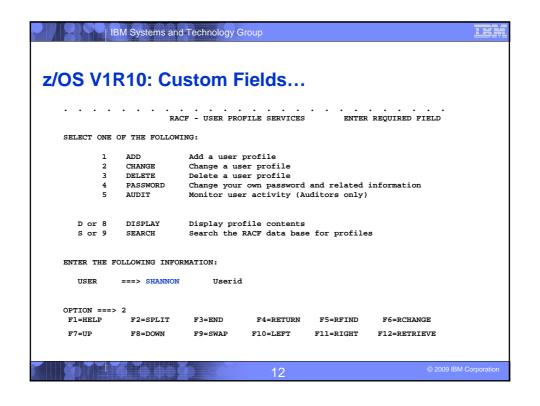
2009 IBM Corporation



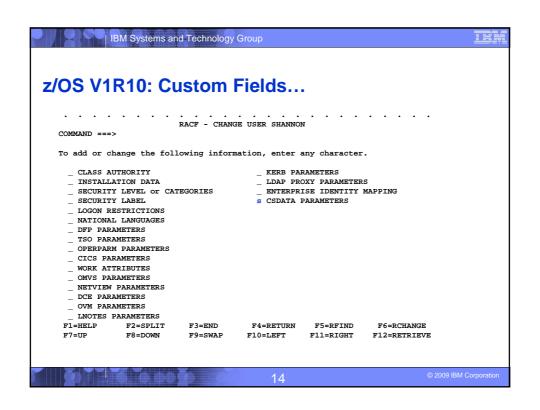




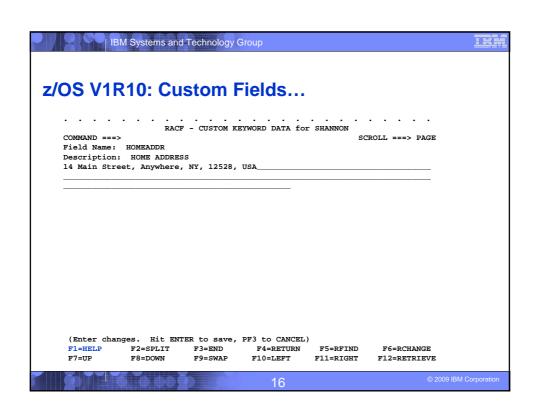


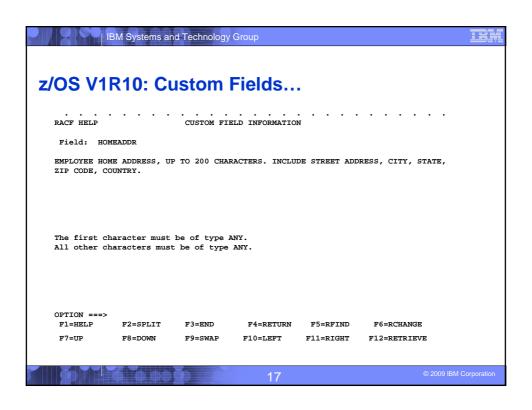


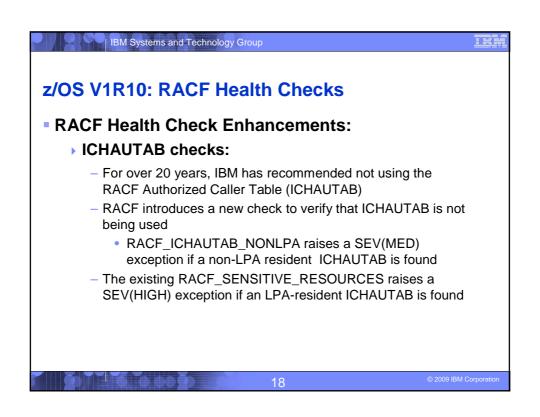
	M Systems an	d Technology	Group			<u>ibm</u>			
z/OS V1F	R10։ Cւ	ıstom	Fields						
RACF - CHANGE USER SHANNON									
OWNER USER NAME		_ Userid or	group name						
DEFAULT GE	ROUP	_ Group nam	ne						
_ Change PASSWORD related information s Add or Change OPTIONAL information									
TO ASSIGN A U	SER ATTRIBUT	E, ENTER YES	, TO CANCEL,	ENTER NO					
GROUP	ACCESS		CIAL ERATIONS						
OIDCA	ARD ASSWORD		DITOR STRICTED						
CHANGE OR DEL	ETE THE MODE	L PROFILE US	SED FOR USER DA	ATA SETS (OPT	'IONAL):				
NEW MODEL DELETE	vec if	no model is	to be used						
COMMAND ===>	1E5 11	. No model is	s to be used						
	F2=SPLIT F8=DOWN	F3=END F9=SWAP	F4=RETURN F10=LEFT	F5=RFIND F11=RIGHT	F6=RCHANGE F12=RETRIEVE				
			40		© 2009 II	BM Corporation			
			13		© 2000 ii	Sin Corporation			



B	M Systems and	Technology (Group			<u>IBM</u>				
z/OS V1R10: Custom Fields										
COMMAND INPUT		 ields for T	 USER SHANNON	so	ROW 1 TO 1 OF 1					
Delete ALL CSDATA information (NOCSDATA) YES or blanks.										
Select one or more custom fields. Use d to delete, h for help, u to undo changes made during this session, or x to set/edit a field. Hit ENTER to continue.										
IIIC ENTER CO	concinue.			Value						
SEL FieldName	SEL FieldName Description+									
						Street, Anywh				
		***** Bottor	m of data ****		*******					
F1=HELP	F2=SPLIT	F3=END	F4=RETURN	F5=RFIND	F6=RCHANGE					
F7=UP	F8=DOWN	F9=SWAP	F10=LEFT	F11=RIGHT	F12=RETRIEVE					
			15		© 2009 IE	BM Corporation				





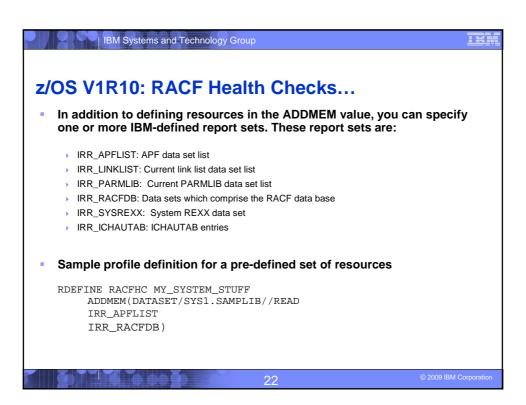


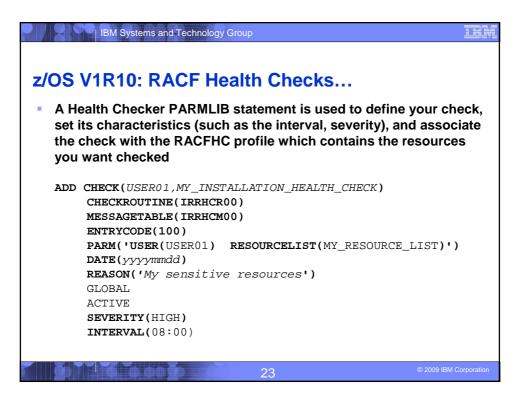
z/OS V1R10: RACF Health Checks... The current RACF checks examine key elements of the z/OS infrastructure, but: The checks look at the resources IBM thinks are important Unless you wrote your own check you can't examine the protection of your data resources With z/OS V1R10, you can check the protection of the resources you want simply by defining profiles and registering your check with the IBM Health Checker for z/OS

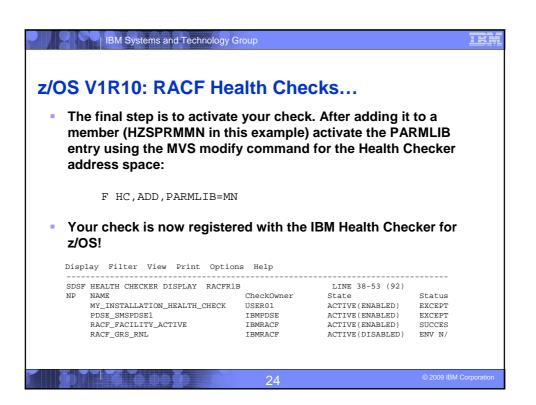
z/OS V1R10: RACF Health Checks...
Defining your own resource check takes these three steps:
1. Defining a RACF profile in the new RACFHC general resource class. This profile contains the list of resources that you want to check
2. Define a PARMLIB entry that defines your check using the IBM Health Checker for z/OS Dynamic Registration
3. Activate your PARMLIB entry

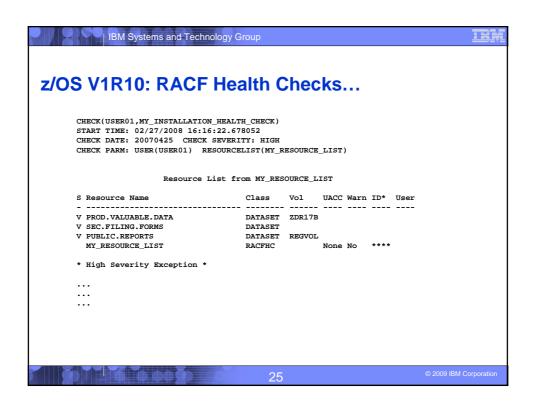
IBM Systems and Technology Group z/OS V1R10: RACF Health Checks... The RACFHC class contains profiles which have the resources you want to check. The RDEFINE command to add a profile is: RDEFINE RACFHC MY_RESOURCE_LIST ADDMEM(DATASET/PROD. VALUABLE. DATA/ZDR17B/NONE DATASET/SEC.FILING.FORMS//NONE RACFHC/MY_RESOURCE_LIST//NONE) The ADDMEM field defines the resources that you want checked. The format is: className/resourceName/volume/maximumPublicAccess className is any valid RACF class resourceName is a resources name within the class Volume is the volume serial for a DATASET resource, otherwise no value should be specified maximumPublicAccess is the access level which if exceeded results in an exception. Valid values are NONE, READ, UPDATE, and CONTROL.

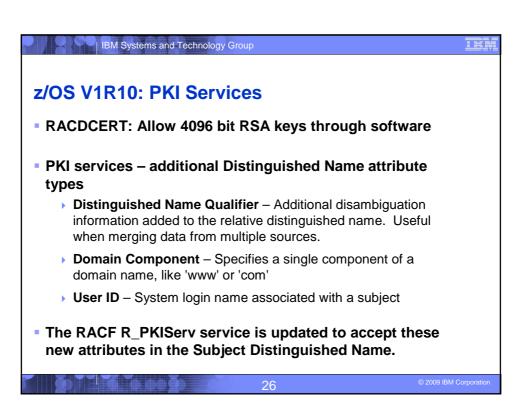
21

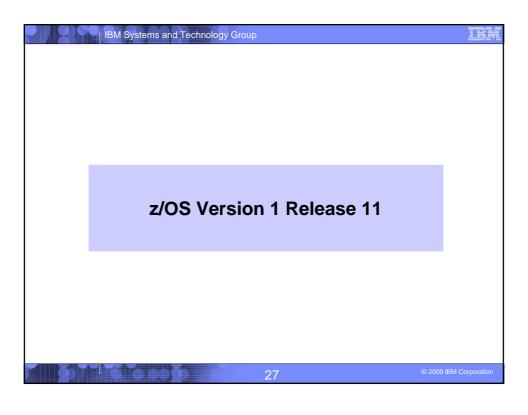


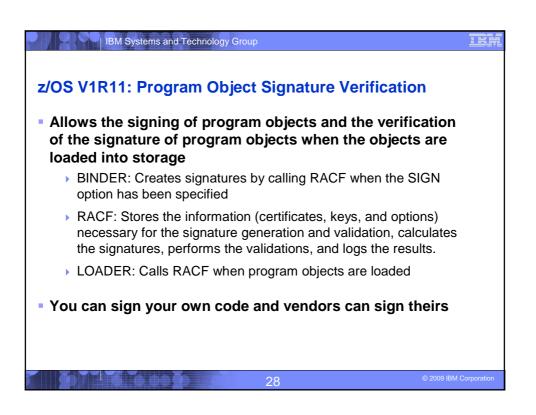


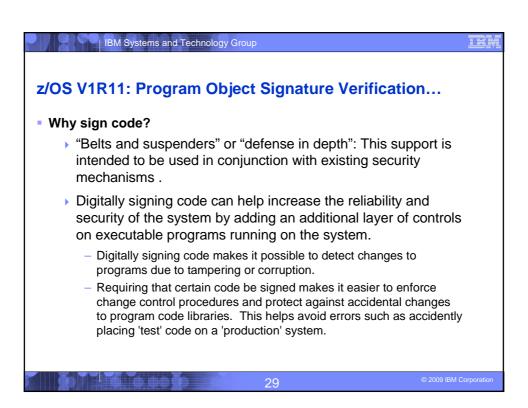


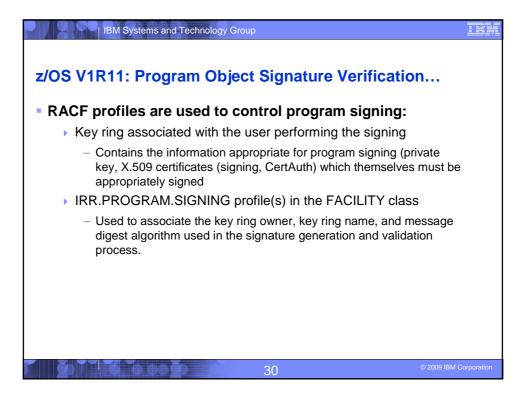




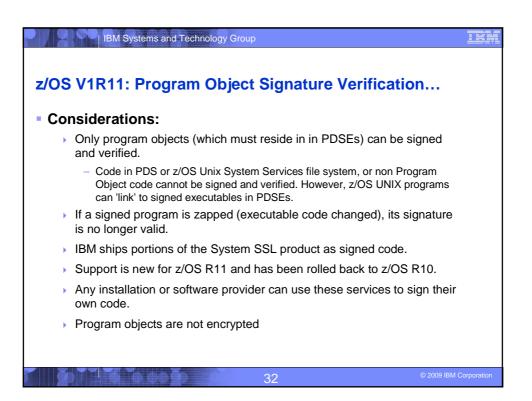








IBM Systems and Technology Group z/OS V1R11: Program Object Signature Verification... RACF profiles are used to control program verification: ▶ IRR.PROGRAM.SIGNATURE.VERIFICATION profile in the **FACILITY class** Used to associate the key ring owner and key ring name of the key ring which contains the signature verification key ring Profiles in the PROGRAM class Contains information options that specify the actions to be taken during verification process: SIGREQUIRED: Is a signature required for this program? (YES,NO) FAILLOAD: Under what conditions should the load fail? (ANYBAD, BADSIGONLY, NEVER) SIGAUDIT: What should be logged? (ALL, SUCCESS, ANYBAD, BADSIGONLY, NONE)



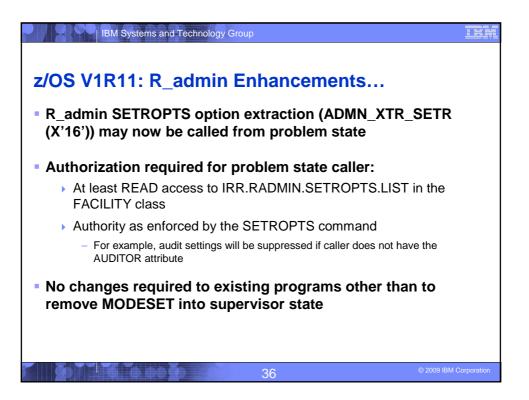
z/OS V1R11: Logon Statistics Suppression Allows you to specify which applications should only record on the first system access of a day Why? Reduced I/O and lower the impact of serialization on the RACF dataset. APPL profiles are used to specify which applications are taking advantage of logon statistics suppression Specify "RACF-INITSTATS(DAILY)" anywhere in the APPLDATA APPL class must be active and RACLISTEd

33

IBM Systems and Technology Group z/OS V1R11: Identity Propagation Prior to z/OS V1R11, clients using distributed server applications which used a common server or application identity for transaction executing on z/OS would not be able to pass the identity of the end user to z/OS for logging With z/OS V1R11, applications can pass the distributed identity information abut the end user (distinguished name and realm) into z/OS where it will be used for logging Exploited by CICS TS 4.1 The distributed identity can be mapped to a RACF identity at: the distributed application server (as is often done today) or the execution point on z/OS, using the new RACMAP support RACMAP [ID(mapped-to-userID)] MAP **USERDIDFILTER(NAME(**'distributed-identity-username-filter')) REGISTRY(NAME('distributed-identity-registryname')) [WITHLABEL('label-name')] | DELMAP[(LABEL('label-name'))] | LISTMAP[(LABEL('label-name'))]

34

z/OS V1R11: R_admin Enhancements R_admin can now be used to extract information about general resources Extract specified profile - ADMN_XTR_RESOURCE (X'1F') Extract next profile - ADMN_XTR_NEXT_RESOURCE (X'20') Authorization required for problem state callers: At least READ access to the IRR.RADMIN.RLIST resource in the FACILITY class Users are limited to seeing only the information that would be displayed by an RLIST command For example, audit settings will be suppressed if caller does not have the AUDITOR attribute Supervisor callers can request either, both, or no check Command authority enforced by default



z/OS V1R11: LDAP Change Logging of General Resources

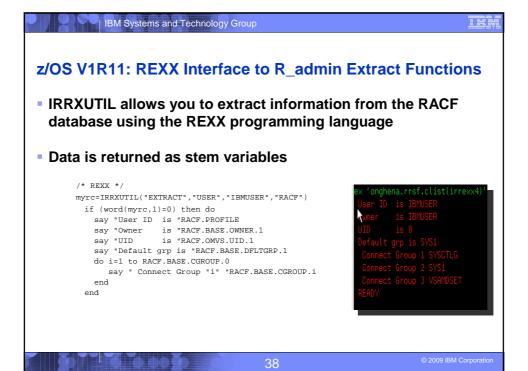
 You can now tell RACF to create change log entries for changes to general resources by defining the profile NOTIFY.LDAP.class-name in the RACFEVNT class and activate the class

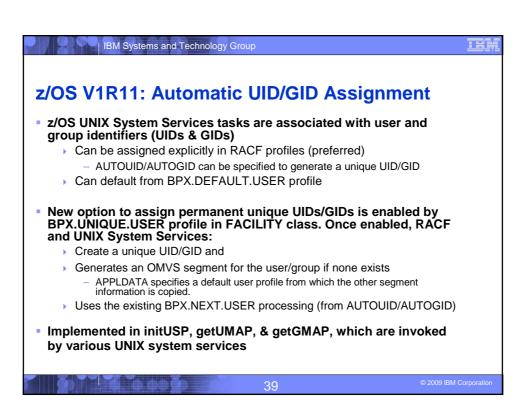
| IBM Systems and Technology Group

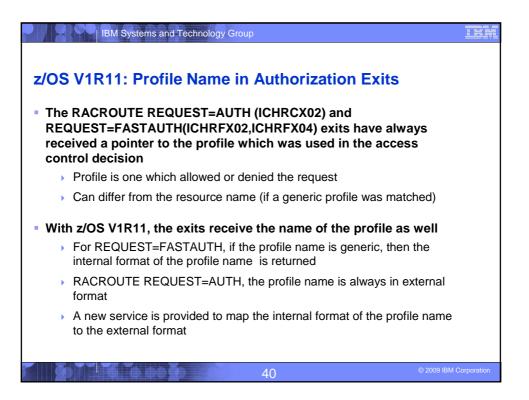
- Events which are logged:
 - Resource additions made using the RDEFINE command
 - Resource modifications made using the RALTER command
 - Changes to the resource's access list using the PERMIT command
 - Resource deletions made using the RDELETE command
- ICHEINTY/RACROUTE applications can create their own change log entries using R_proxyserv (IRRSPY00)

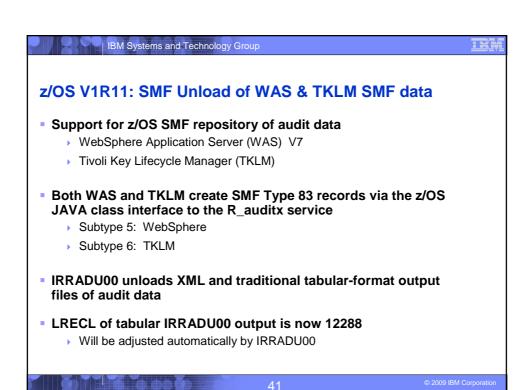
37

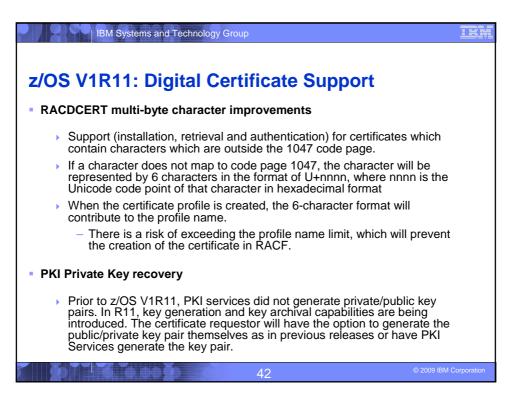
© 2009 IBM Corporation











z/OS V1R11: Digital Certificate Support PKI Web Pages PKI services now provides Java server pages (JSPs) and an XML template file to create and customize the PKI Services Web application as an alternative to the existing REXX CGI support. PKI Support for SHA256 with RSA signature algorithm PKI Services will support the "SHA256 with RSA encryption" signature algorithm for signing certificates, certificate and authority revocation lists (CRL/ARL), and OCSP responses