

Kerberos AES support

| IBM Systems and Technology Group

IBM

Rerberos AES support

- z/OS's Kerberos has been extended to support the AES encryption algorithm.
 - This increases compatibility between z/OS Kerberos and implementations of Kerberos on other systems for improved interoperability in support of RFC3962.
- In addition, functionality has been incorporated to implement SPKM/LIPKEY RFCs:
 - > RFC2025 The Simple Public-Key GSS-API Mechanism (SPKM)
 - ▶ RFC2253 UTF-8 String Representation of Distinguished Names
 - RFC2459 X.509 Public Key Infrastructure
 - RFC2847 LIPKEY A Low Infrastructure Public Key Mechanism Using SPKM

9

2009 IBM Corporation

IBM Systems and Technology Group



Java RACF User and Group administration interface

- New Java interfaces
 - Allow administration and querying of users, groups and user-group connection information via JAVA API calls.
 - These APIs internally call the z/OS LDAP (ISS or ITDS) server to perform the functions.
 - This makes these APIs callable from applications running on or off the z/OS platform.

10

IBM Systems and Technology Group



Writeable SAF Keyring and Certificate support

- R_datalib SAF callable services updated to allow programs to perform additional certificate functions.
 - Keyrings may now be created and deleted
 - Certificates can be added and deleted to RACF
 - Certificates can be added and deleted from keyrings
- Prior to this support, the only way to perform these functions was via the RACF RACDCERT TSO command.

11

2009 IBM Corporation

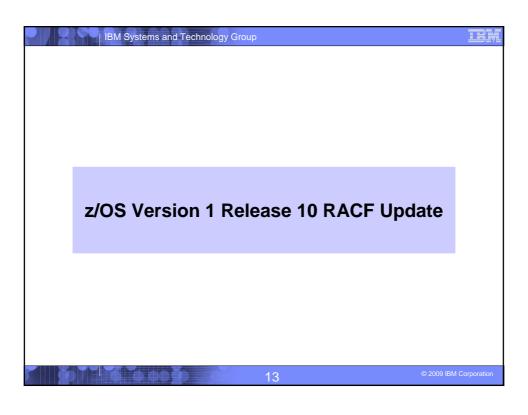
IBM Systems and Technology Group



PKI Services Updates

- Certificates containing 2-byte UTF-8 characters which can be mapped to code page 1047 characters are supported.
- The use of SDBM credential for the LDAP administrator in PKI Services is allowed.
- The maximum limit of the certificate validity period will be changed from 3650 days (10 years) to 9999 days (approx. 27 years).
- Automated certificate renewal can send renewal certificates via e-mail when the expiration dates for older certificates are approaching.
- New e-mail notification for the PKI administrator is provided for pending certificate requests.

12





z/OS V1R10: Password Reset Granularity • More granularity for Password Reset and LISTUSER • Refere V1R10: The EACH LTV resource IRR PASSWORD RESE

| IBM Systems and Technology Group

- Before V1R10: The FACILITY resource IRR.PASSWORD.RESET allowed password resets for users without the SPECIAL, OPERATIONS, AUDITOR, or PROTECTED attribute. Access to the IRR.LISTUSER resource allowed the listing of a USER profile base segment.
- With V1R10, the authority to reset a password can be granted based on profile ownership or group-tree ownership using FACILITY class profiles:
 - IRR.PWRESET.OWNER.owner-of-user
 - Grants authority based on the user or group that owns the user
 - ▶ IRR.PWRESET.TREE.owner-of-group-tree
 - Grants authority based on group tree scope
 - That is, if "owner of group tree" owns the user being reset, or owns a group that owns the user, or owns a group that owns a group that ...

15

© 2009 IBM Corporation

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 • IRR.LU.EXCLUDE.excluded-user

IBM Systems and Technology Group



z/OS V1R10: Group Authorization Check added to EIM Remote Authorization service.

- z/OS V1R8 introduced the remote authorization service which allows a remote application to use IBM Tivoli Directory Server (z/OS LDAP) to check a user id's authorization to RACF resources.
- In z/OS v1R10 this service is enhanced to check the authority of a group id to RACF resources. (The existing user id check is still there and unchanged)
- This gives applications which need to map distributed ids to RACF the ability to reduce the amount of required mapping because there are generally fewer group ids than user IDs.
- This support is available back to z/OS V1R8 via APAR OA23078.

17

2009 IBM Corporation

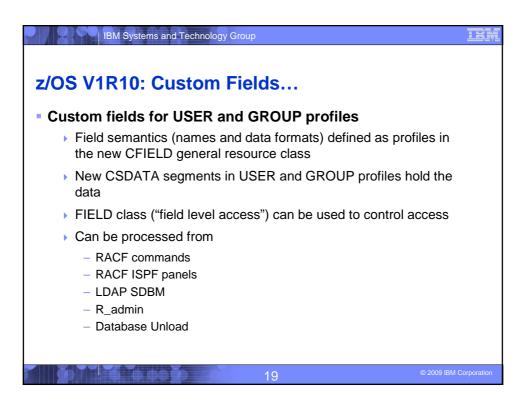
| IBM Systems and Technology Group

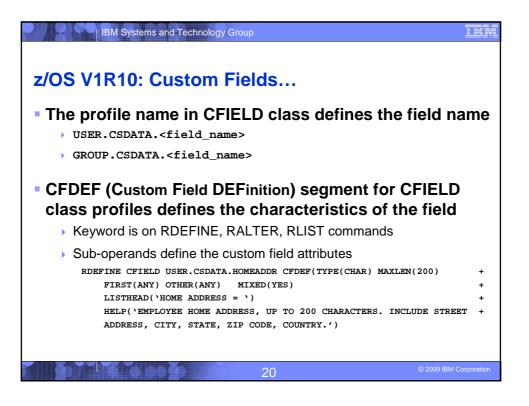


z/OS V1R10: Custom Fields

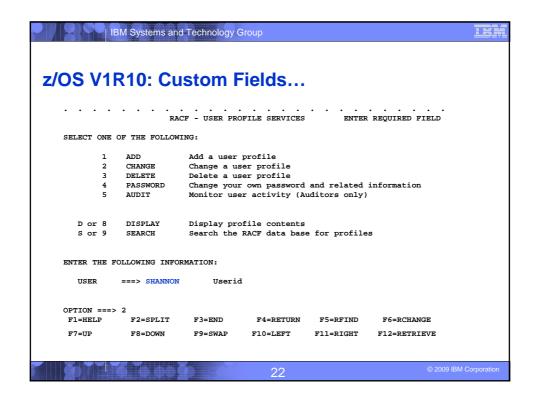
- With Custom Fields you can create your own fields in the RACF database by defining profiles!
 - No assembler programming required
 - No ICHEINTY, RACROUTE experience required!
- You define the contents of the fields
 - Field name (1-8 characters)
 - Field Type: Character, Numeric, Hexadecimal, Flag (Yes/No)
 - ▶ Heading for LISTUSER or LISTGRP command
 - Help text
 - Maximum field length
 - For character fields: Character restrictions for first and remaining characters, Mixed case or uppercase
 - For numeric fields: Minimum value, Maximum value
- Other field customization can be performed in a field validation exit (IRRVAF01) which is under the control of the MVS dynamic exit facility

18

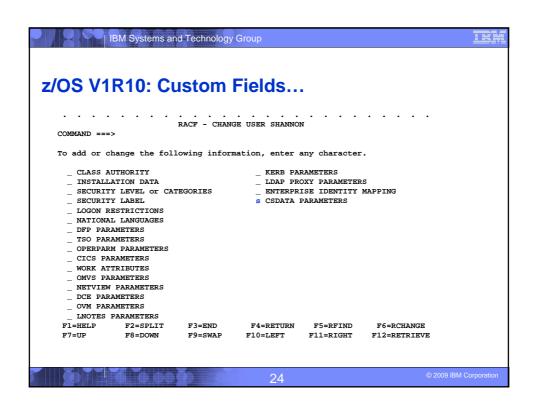




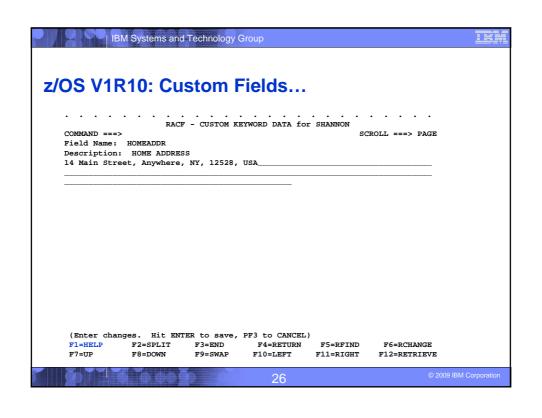


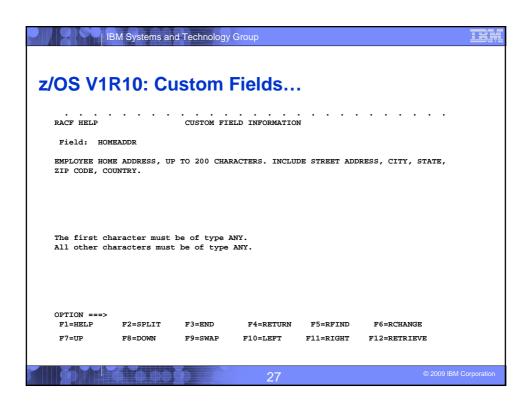


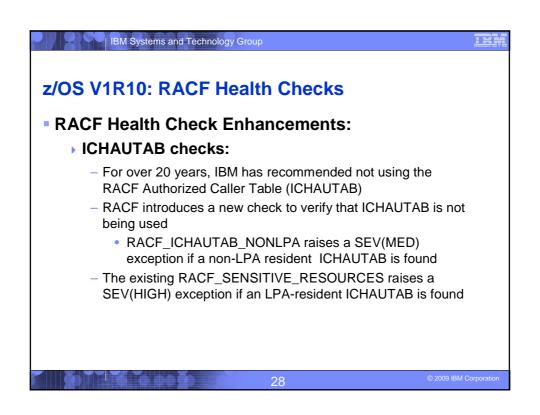
	M Systems ar	d Technology	Group			<u>IBM</u>			
-/OO \/4E	40- 0-		Etalala						
z/OS V1R	(10: Cl	Istom	Fields	•					
RACF - CHANGE USER SHANNON									
OWNER USER NAME		Userid or	group name						
DEFAULT GR	OUP	Group nam	ne						
		lated information							
TO ASSIGN A U	SER ATTRIBU	TE, ENTER YES	, TO CANCEL,	ENTER NO					
	ACCESS		ECIAL						
	ADSP OPERATIONS OIDCARD AUDITOR								
NO-PA	SSWORD	RES	STRICTED						
CHANGE OR DEL	ETE THE MODI	L PROFILE US	SED FOR USER DA	ATA SETS (OPT	CIONAL):				
NEW MODEL									
DELETE COMMAND ===>	YES if	no model is	s to be used						
	F2=SPLIT	F3=END	F4=RETURN	F5=RFIND	F6=RCHANGE				
F7=UP	F8=DOWN	F9=SWAP	F10=LEFT	F11=RIGHT	F12=RETRIEVE				
	1 0 00	Ď Ž	23		© 2009	IBM Corporation			



	M Systems and	Technology (Group			<u> TRM</u>					
z/OS V1R10: Custom Fields											
		 Tields for N	 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+					12-					
	HOME ADDRESS		14 Main Street, Anywh								
		***** Botto	m or 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						
			25		© 2009 IE	BM Corporation					

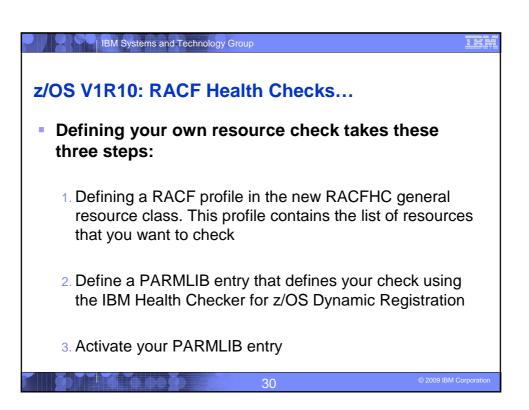


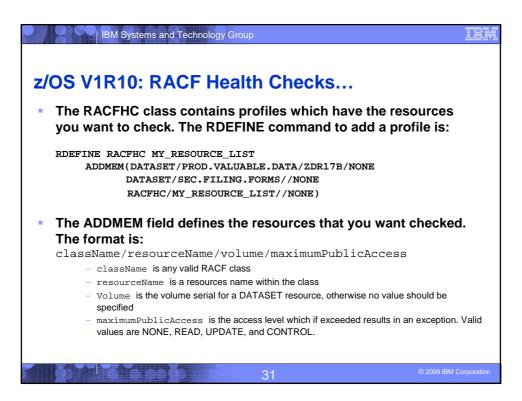


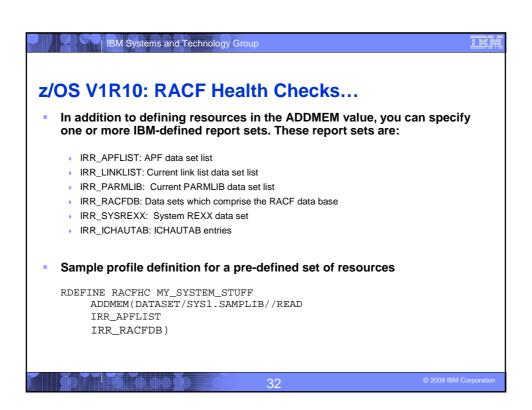


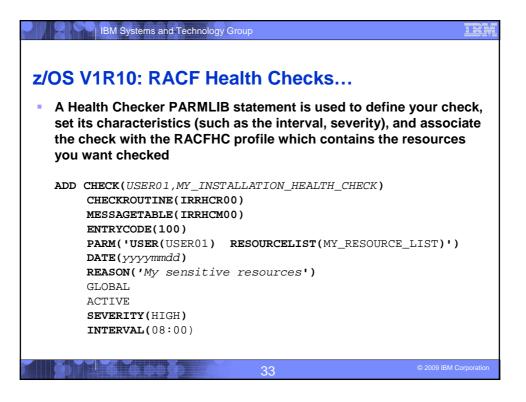
z/OS V1R10: RACF Health Checks... The current RACF checks examine key elements of the z/OS infrastructure, but: The checks look at the resources IBM thinks are important Unless you wrote your own check you can't examine the protection of your data resources With z/OS V1R10, you can check the protection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

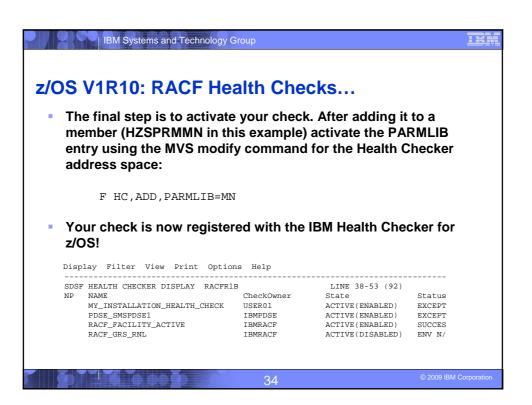
29

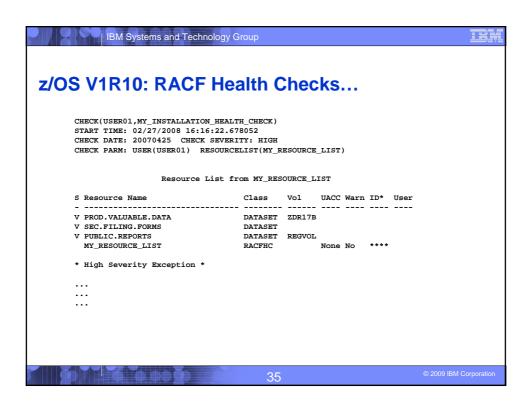


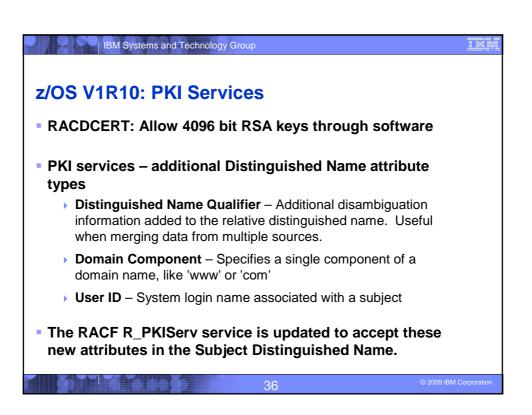


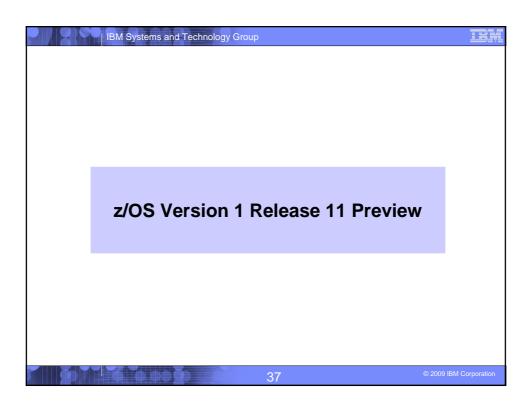


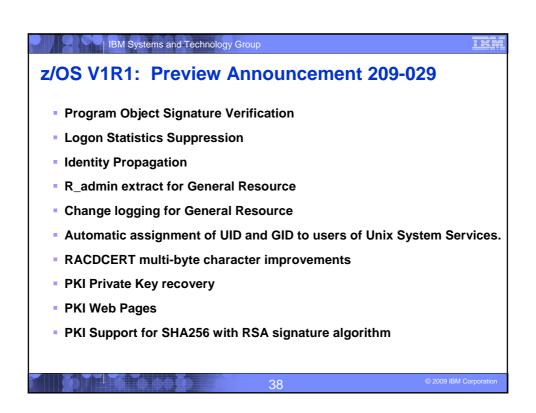


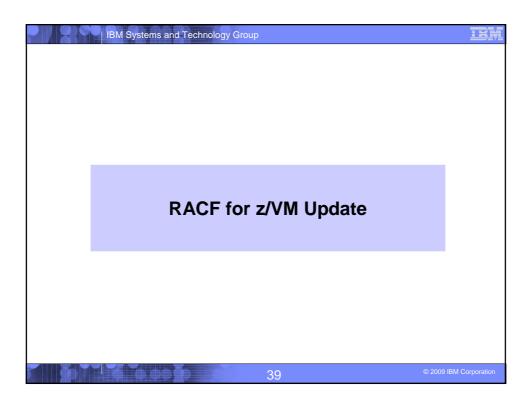


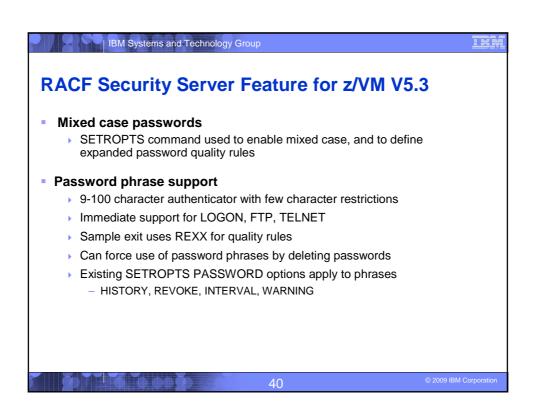




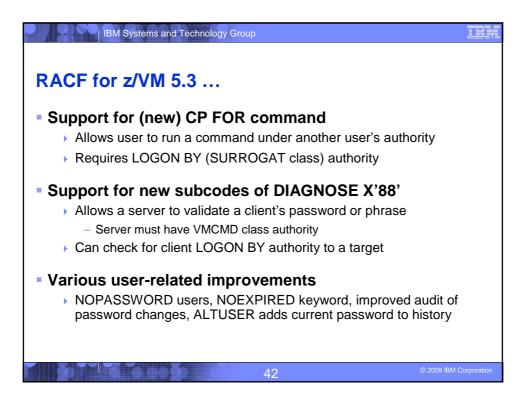








RACF for z/VM 5.3 ... Support for (new) z/VM LDAP Query, update RACF user and group profiles via SDBM backend Clients (e.g.Linux) can authenticate to LDAP using RACF password Remote authorization and auditing services Logging of LDAP server events in SMF DATA file SMF Unload utility (RACFADU) updated Support for LDAP server and client auditing Output available in XML format



RACF Security Server Feature for z/VM V5.4

- LDAP change log support for RACF user and group updates
- Password/phrase enveloping

| IBM Systems and Technology Group

- Allows secure retrieval of clear-text password/phrase values from RACF
- Provides underpinning for bidirectional registry and password synchronization, for example, using IBM Tivoli Directory Integrator

43