

z/OS V1R11: Program Object Signature Verification

IBM Systems and Technology Group

- Allows the signing of program objects and the verification of the signature of program objects when the objects are loaded into storage
 - BINDER: Creates signatures by calling RACF when the SIGN option has been specified
 - RACF: Stores the information (certificates, keys, and options) necessary for the signature generation and validation, calculates the signatures, performs the validations, and logs the results.
 - LOADER: Calls RACF when program objects are loaded
- You can sign your own code and vendors can sign theirs

5

2009 IBM Corporation

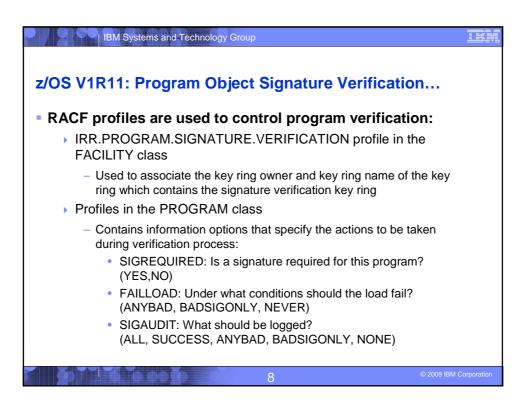
3

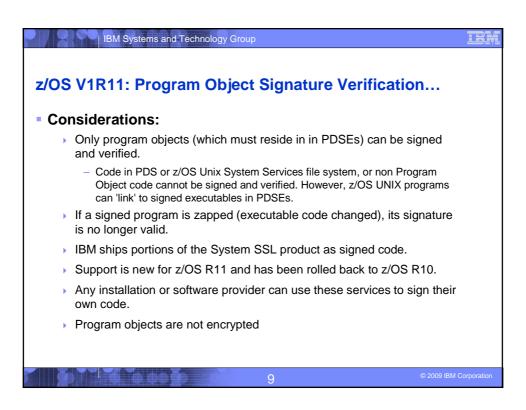
z/OS V1R11: Program Object Signature Verification... Why sign code? "Belts and suspenders" or "defense in depth": This support is intended to be used in conjunction with existing security mechanisms. Digitally signing code can help increase the reliability and security of the system by adding an additional layer of controls on executable programs running on the system. Digitally signing code makes it possible to detect changes to programs due to tampering or corruption. Requiring that certain code be signed makes it easier to enforce

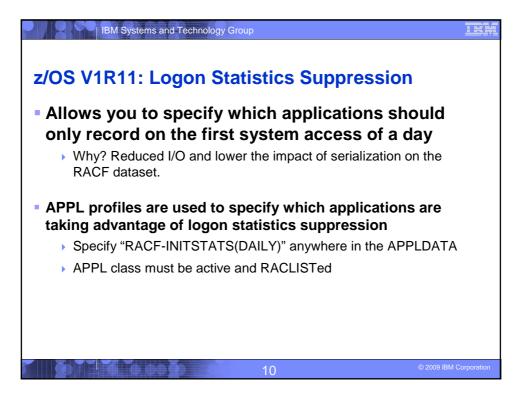
change control procedures and protect against accidental changes to program code libraries. This helps avoid errors such as accidently

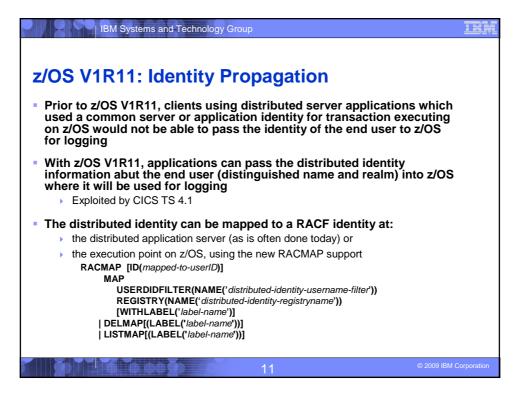
placing 'test' code on a 'production' system.

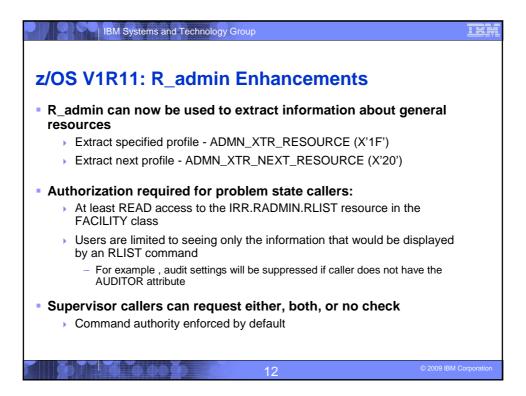
z/OS V1R11: Program Object Signature Verification... RACF profiles are used to control program signing: Key ring associated with the user performing the signing Contains the information appropriate for program signing (private key, X.509 certificates (signing, CertAuth) which themselves must be appropriately signed IRR.PROGRAM.SIGNING profile(s) in the FACILITY class Used to associate the key ring owner, key ring name, and message digest algorithm used in the signature generation and validation process.











IBM Systems and Technology Group



z/OS V1R11: R_admin Enhancements...

- R_admin SETROPTS option extraction (ADMN_XTR_SETR (X'16')) may now be called from problem state
- Authorization required for problem state caller:
 - At least READ access to IRR.RADMIN.SETROPTS.LIST in the FACILITY class
 - Authority as enforced by the SETROPTS command
 - For example, audit settings will be suppressed if caller does not have the AUDITOR attribute
- No changes required to existing programs other than to remove MODESET into supervisor state

13

© 2009 IBM Corporation

| IBM Systems and Technology Group

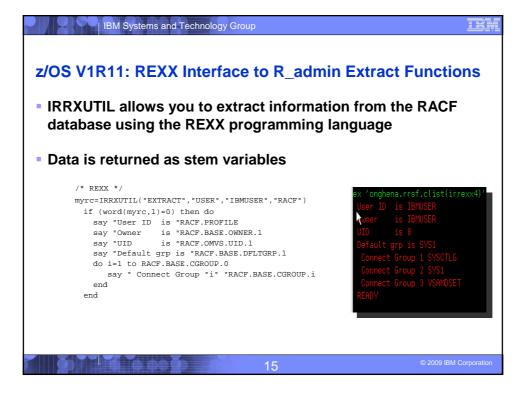


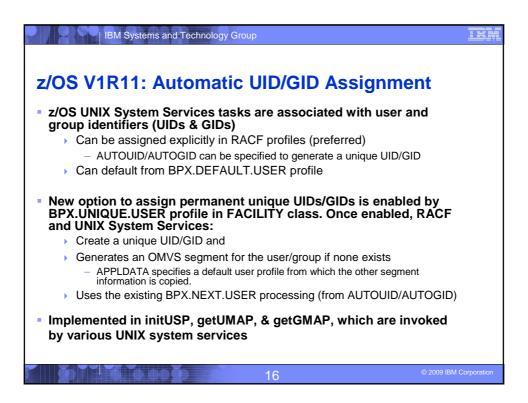
z/OS V1R11: LDAP Change Logging of General Resources

- 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
- 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)

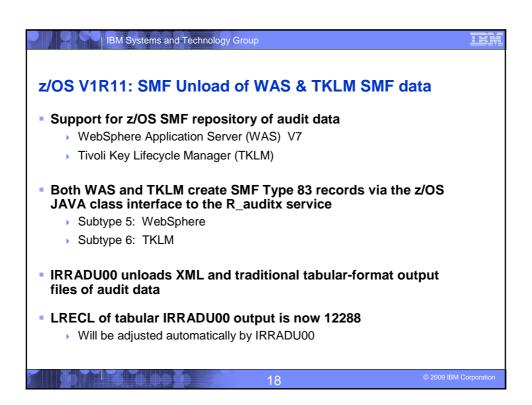
14

2009 IBM Corporation





z/OS V1R11: Profile Name in Authorization Exits The RACROUTE REQUEST=AUTH (ICHRCX02) and REQUEST=FASTAUTH(ICHRFX02,ICHRFX04) exits have always received a pointer to the profile which was used in the access control decision Profile is one which allowed or denied the request Can differ from the resource name (if a generic profile was matched) With z/OS V1R11, the exits receive the name of the profile as well For REQUEST=FASTAUTH, if the profile name is generic, then the internal format of the profile name is returned RACROUTE REQUEST=AUTH, the profile name is always in external format A new service is provided to map the internal format of the profile name to the external format



z/OS V1R11: Digital Certificate Support

RACDCERT multi-byte character improvements

IBM Systems and Technology Group

- Support (installation, retrieval and authentication) for certificates which contain characters which are outside the 1047 code page.
- If a character does not map to code page 1047, the character will be represented by 6 characters in the format of U+nnnn, where nnnn is the Unicode code point of that character in hexadecimal format
- When the certificate profile is created, the 6-character format will contribute to the profile name.
 - There is a risk of exceeding the profile name limit, which will prevent the creation of the certificate in RACF.
- PKI Private Key recovery
 - Prior to z/OS V1R11, PKI services did not generate private/public key pairs. In R11, key generation and key archival capabilities are being introduced. The certificate requestor will have the option to generate the public/private key pair themselves as in previous releases or have PKI Services generate the key pair.

1 a

2009 IBM Corporation

IBM Systems and Technology Group

TRA

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

20

2009 IBM Corporation