z/OS 2.4 IBM Education Assistant (IEA)

Solution (Epic) Name: RACF Pervasive Encryption Phase 2

Element(s)/Component(s): RACF

Agenda

- Trademarks
- Session Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Migration & Coexistence Considerations
- Installation
- Session Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - None

Session Objectives

- Describe the new functions
  - Overview
  - Activation

Overview

- Who (Audience)
  - Security administrators, system programmers
- What (Solution)
  - Specify the ICSF key label to be used for JES spool encryption
  - Ability to encrypt RACF remote sharing VSAM checkpoint files
- Wow (Benefit / Value, Need Addressed)
  - Continuing evolution of Pervasive Encryption extends support to additional types of z/OS data
  - RRSF function can be used for housekeeping and consistent RACF profile protection, even if pervasive encryption is not used

Overview …

- A new JES segment, intended for use with the JESJOBS class, contains a field in which to specify a CKDS key label used to encrypt JES data covered by the profile
- Pervasive encryption works great for new VSAM files, but RACF never deletes its VSAM checkpoint files so that they can be reallocated, and thus encrypted
  - Provide options on TARGET command to “move” the checkpoint files, while in use, on a node by node basis
  - In the process of moving the files, the target file can be covered by a DATASET profile with a DFP segment DATAKEY field, thus initiating encryption
  - The file can be moved back in order to return to the original state

Usage & Invocation … JES

- Specify an ICSF key label for use in encrypting data covered by the JESJOBS profile

```
RALTER JESJOBS JESJOBS ENCRYPT.MYNODE.MYUSER.MYJOB.MYDSN
                       JES(KEYLABEL(JESJOBS.OUTPUT.LABEL))
```

- Support in ISPF panels, IRRDBU00, R_admin, etc, business as usual

- That’s it!
- See JES2 documentation for the beef

Usage & Invocation … RRSF TARGET command

[ALLOWINBOUND | DENYINBOUND | RESETDENYINBOUNDCOUNT]
[DELETE | DORMANT | OPERATIVE]
[DESCRIPTION('*description*')]
[LIST]
[LISTPROTOCOL]
[LOCAL]
[MAIN]
[NEWMAIN | PLEXNEWMAIN]
[NODE(*nodename*|*)]
[**PREFIX**(*qualifier ...*)]
[PROTOCOL(APPC|TCP (…. …)
[PURGE(INMSG | OUTMSG)]
[SYSNAME(*sysname* |*)]
[**WDSQUAL**(*qualifier*)]
[**WORKSPACE**({
[STORCLAS(*class-name*)]
[DATACLAS(*class-name*)]
[MGMTCLAS(*class-name*)]
| [VOLUME(*volume-serial*)] }
[FILESIZE([*nnnnnnnnn* | 500])])]

Existing TARGET command syntax summary. Keywords used in file allocation are in **bold green**.

Usage & Invocation … RRSF

- Say you have a remote node defined using the following TARGET command

```
TARGET NODE(NODE2) SYSNAME(SYS3) MAIN  OPERATIVE                    +
       PROTOCOL(TCP(ADDRESS(ALPS4225.POK.IBM.COM)))                  +
       PREFIX(RRSF.WORK) WORKSPACE(VOLUME(RRSF01) FILESIZE(500))

<target list node(node2) sysname(sys3)

IRRM010I (<) RSWJ SUBSYSTEM PROPERTIES OF REMOTE RRSF NODE NODE2
       SYSNAME SYS3 (MAIN):
   STATE        - OPERATIVE ACTIVE
   …
   WORKSPACE FILE SPECIFICATION
         PREFIX                    - "RRSF.WORK"
         WDSQUAL                   - <NOT SPECIFIED>
         FILESIZE                  - 500
         VOLUME                    - RRSF01
         FILE USAGE
                "RRSF.WORK.SYS1.SYS3.INMSG"
                                   - CONTAINS 0 RECORD(S)
                                   - OCCUPIES 1 EXTENT(S)
                "RRSF.WORK.SYS1.SYS3.OUTMSG"
                                   - CONTAINS 0 RECORD(S)
                                   - OCCUPIES 1 EXTENT(S)
```

these file-related attributes

← derive these

<- file names

Usage & Invocation … RRSF

- The new function introduces the **NEW**PREFIX and **NEW**WORKSPACE keywords of the TARGET command
- When issued against an OPERATIVE ACTIVE connection, it initiates a ‘file conversion’ to the new names (which are allocated automatically)
  - File conversion works only on OPERATIVE ACTIVE nodes
  - NEWPREFIX value must be different than current value
  - NEWWORKSPACE is required when NEWPREFIX is specified
    - Existing values for sub-operands are copied if new values are not specified
  - The only other keywords allowed during a file conversion are NODE (value of “*” not allowed), SYSNAME (“*” not allowed), WDSQUAL, and LIST
  - The node must have only one protocol defined (unless it’s the local node) and not be in the midst of a protocol conversion

Usage & Invocation … RRSF

- Now issue the following command:

```
<TARGET NODE(NODE2) SYSNAME(SYS3) NEWPREFIX(RRSF.TEMP)
                                  NEWWORKSPACE(VOL(TEMP01) SIZE(1400))
```

- On the console:

```
IRRM002I (<) RSWJ SUBSYSTEM TARGET COMMAND HAS COMPLETED SUCCESSFULLY.
IRRI027I (<) RACF COMMUNICATION WITH TCP NODE NODE2 SYSNAME SYS3 HAS
             BEEN SUCCESSFULLY ESTABLISHED USING CIPHER ALGORITHM 35
             TLS_RSA_WITH_AES_256_CBC_SHA.
IRRC082I (<) REALLOCATION OF RRSF WORKSPACE DATASETS IS COMPLETE FOR
             NODE NODE2 SYSNAME SYS3.
```

- Note the conversion requires a re-establishment of the connection, which TARGET performs automatically (indicated by IRRI027I)

Usage & Invocation … RRSF

```
<target list node(node2) sysname(sys3)

IRRM010I (<) RSWJ SUBSYSTEM PROPERTIES OF REMOTE RRSF NODE NODE2
       SYSNAME SYS3 (MAIN):
   STATE        - OPERATIVE ACTIVE
   …
   WORKSPACE FILE SPECIFICATION
         PREFIX                      - "RSFJ.TEMP"
         WDSQUAL                     - <NOT SPECIFIED>
         FILESIZE                    - 500
         VOLUME                      - TEMP01
         FILE USAGE
                 "RRSF.TEMP.SYS1.SYS3.INMSG"
                                     - CONTAINS 0 RECORD(S)
                                     - OCCUPIES 1 EXTENT(S)
                 "RRSF.TEMP.SYS1.SYS3.OUTMSG"
                                     - CONTAINS 0 RECORD(S)
                                     - OCCUPIES 1 EXTENT(S)
         CONVERSION FILE
                 "RRSF.WORK.SYS1.SYS3.INMSG"
                                     - CONTAINS 0 RECORD(S)
                                     - OCCUPIES 1 EXTENT(S)
                 "RRSF.WORK.SYS1.SYS3.OUTMSG"
                                     - CONTAINS 0 RECORD(S)
                                     - OCCUPIES 1 EXTENT(S)
```

- When old files are drained, they are automatically deleted, and no longer appear in TARGET LIST output
- This can happen in an eyeblink. **Hint:** specify LIST on the conversion command to see it

Usage & Invocation … RRSF

- Let's encrypt some files. Assume:
  - The current PREFIX value is RRSF.WORK. The goal is to keep using these names.
  - All of the RRSF VSAM files are protected by RRSF.* in the DATASET class

1. Assign encryption key to covering DATASET profile

```
ALTDSD 'RRSF.*' DFP(DATAKEY(MY.ENCRYPTION.KEY))
```

2. Relocate files to temporary values

```
<TARGET NODE(NODE2) NEWPREFIX(RRSF.TEMP) NEWWORKSPACE(VOL(TEMP01))
<TARGET NODE(NODE3) NEWPREFIX(RRSF.TEMP) NEWWORKSPACE(VOL(TEMP01))
<TARGET NODE(NODEn …) …
```

3. Move the files back

```
<TARGET NODE(NODE2) NEWPREFIX(RRSF.WORK) NEWWORKSPACE(STORCLAS(VSAMEXT) DATACLAS(VSAMEXT))
<TARGET NODE(NODE3) NEWPREFIX(RRSF.WORK) NEWWORKSPACE(STORCLAS(VSAMEXT) DATACLAS(VSAMEXT))
<TARGET NODE(NODEn …) …
```

- If current naming conventions aren't so friendly, you may need to define temporary DATASET profiles to maintain RACF protection (and even encryption) of the temporary names

Interactions & Dependencies

- To exploit this item, all systems in the Plex must be at the new z/OS level: No
- Software Dependencies
  - None
- Hardware Dependencies
  - None
- Exploiters
  - None

Migration & Coexistence Considerations

- None

Installation

- No considerations

Session Summary

- Pervasive encryption capability is extended to JES spool files and RACF remote sharing checkpoint files
- For JES spool encryption, RACF simply provides a key label field in a new JES segment, which JES will extract and use.
- For RRSF, RACF provides a useful file relocate function that just happens to be able to facilitate pervasive encryption

Appendix

- Bruce Wells (brwells@us.ibm.com)

- **Security Server RACF Security Administrator's Guide**
- **Security Server RACF System Programmer's Guide**
- **Security Server RACF Command Language Reference**