IBM Education Assistance for z/OS V2R1

Item: RACF Remote Sharing:
RRSF TCP/IP Support for ECC
RACF Remote Sharing IPv6 TCP/IP Support
Element/Component: RACF

Material is current as of March 2013

Agenda

- Trademarks
- Presentation Objectives
- Overview
- Usage & Invocation
- Migration & Coexistence Considerations
- Installation
- Presentation Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.

Presentation Objectives

- RRSF TCP/IP Support for ECC
  - Support the use of elliptic curve cryptography (ECC)-based certificates for establishing AT-TLS sessions for an RRSF connection
- RACF Remote Sharing IPv6 TCP/IP Support
  - Support for RRSF connections over TCP/IP using IPv6
  - Support for placing comments and blank lines in RACF parameter library members

Overview of ECC Certificate Support for RRSF

- Problem Statement / Need Addressed
  - RRSF uses Application Transparent Transport Layer Security (AT-TLS) to encrypt data between RRSF nodes, but AT-TLS supports more cryptography suites in z/OS V2R1
- Solution
  - Support the use of additional cryptography suites available in AT-TLS for RRSF connections, including the use of elliptic curve cryptography (ECC)-based certificates for establishing AT-TLS sessions
- Benefit / Value
  - Allows you to use stronger encryption algorithms to protect the RACF profile data transmitted using RRSF

Usage & Invocation

- Certificates are used in AT-TLS to provide secure connections between RRSF systems using TCP/IP
  - In z/OS V2R1, ECC certificates with stronger encryption may be used
  - All cryptography suites in Transport Layer Security (TLS) Protocol Version 1.2 are supported
- When a connection is established between 2 RRSF systems, here is an example of the informational message issued by RACF:

```
IRRI027I (>) RACF COMMUNICATION WITH TCP NODE NODE1 HAS
BEEN SUCCESSFULLY ESTABLISHED USING CIPHER ALGORITHM
C026 TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384.
```

Overview of IPv6 Support in RRSF

- Problem Statement / Need Addressed
  - With the TCP/IP support in RRSF, only the IPv4 protocol is supported
    - Cannot connect to a remote system which has an IPv6 address
  - Cannot have line comments or blank lines in the RACF parameter library members
- Solution
  - Add support in RRSF to allow the use of TCP/IP IPv6 protocol
    - For communications between systems which are enabled for TCP/IP IPv6
    - To specify an IPv6 address on the TARGET statement for the TCP(ADDRESS) operand
  - Allow line comments and blank lines in RACF parameter library members
- Benefit / Value
  - Allow you to choose between IPv4 and IPv6 addressing when setting up RRSF connections over TCP/IP
  - Allow RACF parameter library to be documented more easily

Education - TCP/IP IPv4 vs. IPv6 Addresses

Description	IPv4	IPv6
Address length	32 bits long (4 bytes)	128 bits long (16 bytes). 64 bits for network number, 64 bits for host number
Total addresses	4,294,967,296 (about 4.3 billion)	About 3.4 x 10^{38}
Address format in text	nnn.nnn.nnn.nnn Where 0<=nnn<=255	xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx Where x is hex number. Double colon (::) designates any number of 0 bits
Example	9.127.42.144	`2001:0db8:85a3:0000:` `0000:8a2e:0370:7334`
Equivalent addresses	10.120.78.40	`::ffff:10.120.78.40` IPv4-mapped IPv6 address
Unspecified address	0.0.0.0	`::` (128 0 bits)

Defining a TCP/IP node and activating it using TARGET (Review of R13 Support)

- The only difference from APPC is the PROTOCOL information:
  - Define the local node with a socket listener

```
TARGET NODE(LOCAL1) LOCAL PROTOCOL(TCP)
PREFIX(SYS1.RRSF) WORKSPACE(VOLUME(VOL001))OPERATIVE

IRRC054I (<) RACF REMOTE SHARING TCP LISTENER HAS BEEN SUCCESSFULLY
  ESTABLISHED.
```

  - Define the remote node and make it operative

```
TARGET NODE(REMOTE1) PROTOCOL(TCP(ADDRESS(remote.pok.ibm.com)))
PREFIX(SYS1.RRSF) WORKSPACE(VOLUME(VOL001)) OPERATIVE

IRRI027I (<) RACF COMMUNICATION WITH TCP NODE REMOTE1 HAS BEEN
  SUCCESSFULLY ESTABLISHED USING CIPHER ALGORITHM 35
  TLS_RSA_WITH_AES_256_CBC_SHA.
```

Syntax of the TARGET command (R13)

```
subsystem-prefixTARGET
        [ DELETE | DORMANT | OPERATIVE ]
        [ DESCRIPTION('description') ]
        [ LIST ]
        [ LISTPROTOCOL ]
        [ LOCAL ]
        [ MAIN ]
        [ NODE(nodename |*) ]
        [ PREFIX(qualifier ...) ]
        [ PROTOCOL(
          [ APPC(
            [ LUNAME(luname) ]
            [ TPNAME(profile-name) ]
            [ MODENAME(mode-name) ]
            ) ]
          [ TCP(
            [ ADDRESS(host-name) ]
            [ PORTNUM(number) ]
            ) ]
          ) ]
        [ PURGE(INMSG | OUTMSG) ]
        [ SYSNAME(sysname |*) ]
        [ WDSQUAL(qualifier) ]
        [ WORKSPACE( {
          [ STORCLAS(class-name) ]
          [ DATACLAS(class-name) ]
          [ MGMTCLAS(class-name) ]
            | [ VOLUME(volume-serial) ] }
          [ FILESIZE([ nnnnnnnnnn | 500 ]
            ) ]
          ) ]
```

No syntax checking or validation of ADDRESS, so just update documentation

Description of the ADDRESS operand on TARGET command (New updates in blue)

ADDRESS(*address*)
Defines or changes the host name or IP address of the remote node. You need not define ADDRESS for the local node.

address

Specifies a 1 - 255-character address expressed as a host name or a static IP address. Lowercase characters in the host name are translated to uppercase characters. An IP address may be specified as an IPv4 address or an IPv6 address (if TCP IPv6 is enabled on the system).

- If omitted, the default value for the local node is 0.0.0.0, or :: if TCP IPv6 is enabled on the system. If omitted for a remote node, the address is listed as <NOT SPECIFIED> in the TARGET LIST output.
- You must define ADDRESS for a remote node before activating it using the OPERATIVE operand.
- RACF performs no validity checking on the specified ADDRESS value. You must ensure that the specified address is correct.
- If IPv6 is enabled on the system, TARGET LIST detailed output will display resolved IPv6 addresses, where possible.

TARGET LIST: detailed version (R13)

```
NODE1  <target list node(node1)
NODE1  IRRM010I (<) RSWJ SUBSYSTEM PROPERTIES OF LOCAL RRSF NODE NODE1:
   STATE       - OPERATIVE ACTIVE
   DESCRIPTION - <NOT SPECIFIED>
   PROTOCOL    - APPC
                 LU NAME           - MF1AP001
                 TP PROFILE NAME   - IRRRACF
                 MODENAME          - <NOT SPECIFIED>
                 LISTENER STATUS   - ACTIVE
   PROTOCOL    - TCP
                 HOST ADDRESS      - 0.0.0.0
                 IP ADDRESS        - 9.57.1.243
                 LISTENER PORT     - 18136
                 LISTENER STATUS   - ACTIVE
   TIME OF LAST TRANSMISSION TO   - <NONE>
   TIME OF LAST TRANSMISSION FROM - <NONE>
   WORKSPACE FILE SPECIFICATION
         PREFIX                   - "NODE1.WORK"
         WDSQUAL                  - <NOT SPECIFIED>
         FILESIZE                 - 500
         VOLUME                   - TEMP01
         FILE USAGE
                 "NODE1.WORK.NODE1.INMSG"
                                  - CONTAINS 0 RECORD(S)
                                  - OCCUPIES 1 EXTENT(S)
                 "NODE1.WORK.NODE1.OUTMSG"
                                  - CONTAINS 0 RECORD(S)
                                  - OCCUPIES 1 EXTENT(S)
```

For the local node, shows protocol information
For all defined protocols

1st line indicates 'default' – not specified on TARGET.
2nd line is resolved address, if different than specified.
Note that TARGET LIST will display what RRSF thinks is the LAST resolved IP address.

TARGET LIST: detailed version - New

```
NODE1  <target list node(node1)
NODE1  IRRM010I (<) RSWJ SUBSYSTEM PROPERTIES OF LOCAL RRSF NODE NODE1:
   STATE       - OPERATIVE ACTIVE
   DESCRIPTION - <NOT SPECIFIED>
   PROTOCOL    - APPC
                 LU NAME           - MF1AP001
                 TP PROFILE NAME   - IRRRACF
                 MODENAME          - <NOT SPECIFIED>
                 LISTENER STATUS   - ACTIVE
   PROTOCOL    - TCP
                 HOST ADDRESS      - ::                      <<< IPv6 default
                 IP ADDRESS        - ::FFFF:9.57.1.243       <<< IPv6 address
                 LISTENER PORT     - 18136
                 LISTENER STATUS   - ACTIVE
   TIME OF LAST TRANSMISSION TO    - <NONE>
   TIME OF LAST TRANSMISSION FROM  - <NONE>
   WORKSPACE FILE SPECIFICATION
         PREFIX                    - "NODE1.WORK"
         WDSQUAL                   - <NOT SPECIFIED>
         FILESIZE                  - 500
         VOLUME                    - TEMP01
         FILE USAGE
                 "NODE1.WORK.NODE1.INMSG"
                                   - CONTAINS 0 RECORD(S)
                                   - OCCUPIES 1 EXTENT(S)
                 "NODE1.WORK.NODE1.OUTMSG"
                                   - CONTAINS 0 RECORD(S)
                                   - OCCUPIES 1 EXTENT(S)
```

If IPv6 is enabled, addresses Are displayed in IPv6 format

TARGET LIST: detailed version

- For a **connected** IPv4 remote node (R13)

```
NODE1  <target list node(node2)
NODE1  IRRM010I (<) RSWJ SUBSYSTEM PROPERTIES OF REMOTE RRSF NODE NODE2:
   STATE       - OPERATIVE ACTIVE
   DESCRIPTION - <NOT SPECIFIED>
   PROTOCOL    - TCP
                 HOST ADDRESS     - ALPS4012.POK.IBM.COM       <<< entered on TARGET
                 IP ADDRESS       - 9.57.1.13                  <<< resolved IP address
                 LISTENER PORT    - 18136
                 AT-TLS POLICY:
                   RULE_NAME      - RRSF-CLIENT
                   CIPHER ALG     - 35 TLS_RSA_WITH_AES_256_CBC_SHA
                   CLIENT AUTH    - REQUIRED
   TIME OF LAST TRANSMISSION TO   - <NONE>
   TIME OF LAST TRANSMISSION FROM - <NONE>
   WORKSPACE FILE SPECIFICATION
         PREFIX                   - "RSFJ.BRUCE"
         WDSQUAL                  - <NOT SPECIFIED>
         FILESIZE                 - 500
         VOLUME                   - TEMP01
         FILE USAGE
                 "RSFJ.BRUCE.NODE1.NODE2.INMSG"
                                  - CONTAINS 0 RECORD(S)
                                  - OCCUPIES 1 EXTENT(S)
                 "RSFJ.BRUCE.NODE1.NODE2.OUTMSG"
                                  - CONTAINS 0 RECORD(S)
                                  - OCCUPIES 1 EXTENT(S)
```

"IP Address" line is only displayed if the address is different than line above.

TARGET LIST: detailed version

- For a **connected** IPv6 remote node - NEW

```
NODE1  <target list node(node2)
NODE1  IRRM010I (<) RSWJ SUBSYSTEM PROPERTIES OF REMOTE RRSF NODE NODE2:
   STATE       - OPERATIVE ACTIVE
   DESCRIPTION - <NOT SPECIFIED>
   PROTOCOL    - TCP
                 HOST ADDRESS     - ALPS4012.POK.IBM.COM       <<< entered on TARGET
                 IP ADDRESS       - 2001:0db8:85a3:0000:0000:8a2e:0370:7334 <<< IPv6 address
                 LISTENER PORT    - 18136
                 AT-TLS POLICY:
                   RULE_NAME      - RRSF-CLIENT
                   CIPHER ALG     - 35 TLS_RSA_WITH_AES_256_CBC_SHA
                   CLIENT AUTH    - REQUIRED
   TIME OF LAST TRANSMISSION TO   - <NONE>
   TIME OF LAST TRANSMISSION FROM - <NONE>
   WORKSPACE FILE SPECIFICATION
         PREFIX                   - "RSFJ.BRUCE"
         WDSQUAL                  - <NOT SPECIFIED>
         FILESIZE                 - 500
         VOLUME                   - TEMP01
         FILE USAGE
                 "RSFJ.BRUCE.NODE1.NODE2.INMSG"
                                  - CONTAINS 0 RECORD(S)
                                  - OCCUPIES 1 EXTENT(S)
                 "RSFJ.BRUCE.NODE1.NODE2.OUTMSG"
                                  - CONTAINS 0 RECORD(S)
                                  - OCCUPIES 1 EXTENT(S)
```

Displayed in IPv6 format
if system is enabled for IPv6.

TARGET LIST: detailed version

- For a **connected** IPv6 remote node - NEW

```
NODE1  <target list node(node2)
NODE1  IRRM010I (<) RSWJ SUBSYSTEM PROPERTIES OF REMOTE RRSF NODE NODE2:
   STATE       - OPERATIVE ACTIVE
   DESCRIPTION - <NOT SPECIFIED>
   PROTOCOL    - TCP
                 HOST ADDRESS     - 10.120.78.40       <<< entered on TARGET
                 IP ADDRESS       - ::FFFF:10.120.78.40 <<< IPv6 address
                 LISTENER PORT    - 18136
                 AT-TLS POLICY:
                   RULE_NAME      - RRSF-CLIENT
                   CIPHER ALG     - 35 TLS_RSA_WITH_AES_256_CBC_SHA
                   CLIENT AUTH    - REQUIRED
   TIME OF LAST TRANSMISSION TO   - <NONE>
   TIME OF LAST TRANSMISSION FROM - <NONE>
   WORKSPACE FILE SPECIFICATION
         PREFIX                   - "RSFJ.BRUCE"
         WDSQUAL                  - <NOT SPECIFIED>
         FILESIZE                 - 500
         VOLUME                   - TEMP01
         FILE USAGE
                 "RSFJ.BRUCE.NODE1.NODE2.INMSG"
                                  - CONTAINS 0 RECORD(S)
                                  - OCCUPIES 1 EXTENT(S)
                 "RSFJ.BRUCE.NODE1.NODE2.OUTMSG"
                                  - CONTAINS 0 RECORD(S)
                                  - OCCUPIES 1 EXTENT(S)
```

Displayed in IPv6 format if system is enabled for IPv6. (whatever format is returned by BPX1GNI - getnameinfo.)

Usage – Comments and Blank Lines in RACF Parameter Library

- RACF parameter library members contain SET and TARGET statements which define your RRSF systems
- Prior to z/OS V2R1, a blank line or a whole-line comment in the RACF parameter library caused an error message when the commands were issued
  - A blank line would cause something like this

```
IRRC003I (@) COMMAND ???????? IS NOT VALID.
```

  - For a whole-line comment, you will see something like:

```
IRRC003I (@) COMMAND // THIS IS MY COMMENT IS NOT VALID.
```

Usage – Comments and Blank Lines in RACF Parameter Library...

- In V2R1, blank lines and whole-line-comments are allowed
  - A whole-line comment is any line that starts with “//”, in any column
  - Specifying a continuation character in a whole-line comment will have no effect; it is treated as part of the comment.
  - A whole-line comment or blank line may not be specified within a continued command.
  - If a shared parameter library is shared among downlevel systems, error messages will be issued on the downlevel systems for blank lines and whole-line comments
- The following are examples of valid whole-line comments:

```
//This is a comment line

// This is a comment line //

                    // This is a comment line
```

Usage – Comments and Blank Lines in RACF Parameter Library...

- The following are examples of incorrect whole-line comments

Example 1:

```
// This is a comment, trailing dash ignored  -
This is treated as a new command, not a continuation of above
comment.
```

Example 2:

```
TARGET LIST   // This is not a valid comment and will fail
```

Example 3:

```
TARGET   -
// This will be treated as part of a TSO command and will be
// failed when runs
   LISTPROTOCOL
```

Usage – Comments and Blank Lines in RACF Parameter Library...

```
//*************************************************************/
// THIS MEMBER DEFINES 1 MULTI-SYSTEM NODE AND 1 SINGLE SYSTEM NODE
//
// NODE1/NODE1     LOCAL NODE1 MAIN
// NODE1/NODE2SY1 LOCAL NODE1 NON-MAIN
// NODE2           REMOTE SSN
//*************************************************************/

// THE LOCAL MSN */
TARGET NODE(NODE1) SYSNAME(NODE1) MAIN                          -
       PREFIX(RRSF.FILE) PROTOCOL(APPC(LUNAME(MF1AP001)))       -
       WORKSPACE(VOLUME(TEMP01) FILESIZE(500)) LOCAL OPERATIVE

TARGET NODE(NODE1) SYSNAME(NODE2SY1)                            -
       PREFIX(RRSF.FILE) PROTOCOL(APPC(LUNAME(MF2AP001)))       -
       WORKSPACE(VOLUME(TEMP01) FILESIZE(500)) LOCAL OPERATIVE

// THE REMOTE SSN */
TARGET NODE(NODE2)                                              -
       PREFIX(RRSFRACF) PROTOCOL(APPC(LUNAME(MF3AP001)))        -
       WORKSPACE(VOLUME(TEMP02) FILESIZE(500))       OPERATIVE
```

Migration & Coexistence Considerations

- If a customer is migrating from a previous z/OS release and already had IPv6 enabled, then immediately upon installation of z/OS V2R1, the TARGET LIST output may display IPv6 addresses.
  - Even when IPv4 addresses are specified in the TARGET commands, the TARGET LIST detailed output for an RRSF node will display IPv6 addresses.
- No action necessary

Installation

- To use IPv6 support in RRSF, you must have IPv6 enabled in TCP/IP.
  - See SC31-8885 IPv6 Network and Application Design Guide
    - http://publib.boulder.ibm.com/infocenter/zos/v1r13/topic/com.ibm.zos.r13.hale001/f1a1f190.htm

Presentation Summary

- RRSF TCP/IP Support for ECC
  - Support the use of elliptic curve cryptography (ECC)-based certificates for establishing AT-TLS sessions for an RRSF connection
- RACF Remote Sharing IPv6 TCP/IP Support
  - Support for RRSF connections over TCP/IP using IPv6
  - Support for placing comments in RACF parameter library members

Appendix

- SC31-8885 IPv6 Network and Application Design Guide
  - http://publib.boulder.ibm.com/infocenter/zos/v1r13/topic/com.ibm.zos.r13.hale001/f1a1f190.htm
- RACF Command Language Reference SA22-7687
  - Updated ADDRESS operand of the TARGET command
- RACF System Programmer's Guide SA22-7681
  - Updated sections on using TCP/IP with the IPv6 protocol