IBM Education Assistance for z/OS V2R2

Item: RRSF Unidirectional Connections
Element/Component: RACF/RRSF

Material current as of May 2015

Agenda

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

Trademarks

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

Presentation Objectives

Discuss the new ability to establish one-way RRSF connections

Overview

- Problem Statement / Need Addressed
  - It is impossible to prevent a privileged user on a test system from escalating his privilege on a production system when they are connected using RRSF. The honor system applies.
- Solution
  - Any RRSF node can define another RRSF node such that inbound requests from that node are to be denied
- Benefit / Value
  - Protect against accidental or malicious damage to your production system
  - Demonstrate to an auditor your compliance with your security policy, regardless of the configuration established on the remote node

Usage & Invocation

- Use a new TARGET command keyword when defining a remote node
  - TARGET NODE(THATNODE) DENYINBOUND
- When the remote node is a multisystem node:
  - TARGET NODE(THATNODE) SYSNAME(*) DENYINBOUND
  - SYSNAME(*) is not required; RACF will ensure that the setting is consistent across all systems when a single SYSNAME is changed.
- To change your mind, use ALLOWINBOUND
  - This is the default, so you don't need to code it in the parameter library
- DENYINBOUND is ignored if specified for the LOCAL node

Usage & Invocation … Parameter library examples

```
// A REMOTE SSN
TARGET NODE(SSNNODE) DENYINBOUND                                      -
       PREFIX(RSFJ.WORK) PROTOCOL(TCP(ADDRESS(ALPS4060.POK.IBM.COM))) -
       WORKSPACE(VOLUME(TEMP01) FILESIZE(500))       OPERATIVE

// A REMOTE MSN
TARGET NODE(MSNNODE) SYSNAME(*) DENYINBOUND                              ← Bad: Node not yet defined
TARGET NODE(MSNNODE) SYSNAME(SYS1) MAIN DENYINBOUND                   -
       PREFIX(RSFJ.WORK) PROTOCOL(TCP(ADDRESS(ALPS4092.POK.IBM.COM))) -
       WORKSPACE(VOLUME(TEMP01) FILESIZE(500)) OPERATIVE
TARGET NODE(MSNNODE) SYSNAME(*) DENYINBOUND                                ← Good: Node has been defined
TARGET NODE(MSNNODE) SYSNAME(SYS2) DENYINBOUND                                     -
       PREFIX(RSFJ.WORK) PROTOCOL(TCP(ADDRESS(ALPS4196.POK.IBM.COM))) -
       WORKSPACE(VOLUME(TEMP01) FILESIZE(500)) OPERATIVE
TARGET NODE(MSNNODE) SYSNAME(*) DENYINBOUND                                ← Good: Node has been defined
```

Only one of the DENYINBOUND keywords for the entire MSN is necessary, and any green one will suffice. It may be preferable for the sake of clarity to specify it for each of the systems, and not use the SYSNAME(*) notation.

Usage & Invocation ...

- DENYINBOUND setting is exchanged during handshaking as a connection is established
- A new message indicates that work is not being accepted from your system

```
IRRI082I (<) ATTENTION: PARTNER NODE IS NOT ACCEPTING INBOUND WORK
        FROM THIS NODE.
IRRI027I (<) RACF COMMUNICATION WITH TCP NODE NODE1 SYSNAME SYS1 HAS
        BEEN SUCCESSFULLY ESTABLISHED USING CIPHER ALGORITHM 35
        TLS_RSA_WITH_AES_256_CBC_SHA.
```

- It is possible for both sides to deny each other. This might still have some value in that OUTPUT/NOTIFY requests can be sent across the connection

Usage & Invocation ...

- The setting can be changed on the fly, and will take effect, but TARGET LIST on the denied system won't be aware of this unless the connection is restarted
-

```
IRRM105I (<) SYSTEMS WERE FOUND IN THE OPERATIVE STATE WHEN THE
        DENYINBOUND SETTING WAS CHANGED. THE CHANGE IS EFFECTIVE
        IMMEDIATELY, HOWEVER THE TARGET LIST COMMAND MAY NOT
        PROPERLY REFLECT THIS UNTIL COMMUNICATIONS ARE RESTARTED.
```

Usage & Invocation ...

- If the remote system tries sending me requests anyway, they will be denied with a message indicating that inbound work is not accepted
  - For RACLINK DEFINE (Note RACLINK APPROVE is OK)

```
IRRP023I RACLINK could not be completed for user IBMUSER because node NODE1 is not
accepting inbound work. IBMUSER
```

  - For directed command (AT/ONLYAT) or automatically directed work

```
IRRT035I Node NODE1 is not accepting work from NODE2.
```

- A counter of rejected work from that system will be maintained, and displayed by TARGET LIST
  - So you can identify and correct “misconfigured” systems
- The counter can be reset with:
  - TARGET NODE(x) SYSNAME(Y) RESETDENYINBOUNDCOUNT

Usage & Invocation … TARGET LIST

- On the **denied** system

```
IRRM010I (<) RSWL SUBSYSTEM PROPERTIES OF REMOTE RRSF NODE NODE1
             SYSNAME SYS1 (MAIN):
   STATE       - OPERATIVE ACTIVE
   DESCRIPTION - <NOT SPECIFIED>
   PROTOCOL    - TCP
                 HOST ADDRESS     - ALPS4092.POK.IBM.COM
                 IP ADDRESS       - 9.57.1.93
                 LISTENER PORT    - 18136
                 AT-TLS POLICY:
                   RULE_NAME      - RRSF-CLIENT
                   CIPHER ALG     - 35 TLS_RSA_WITH_AES_256_CBC_SHA
                   CLIENT AUTH    - REQUIRED
   THIS NODE IS NOT ACCEPTING INBOUND WORK
   TIME OF LAST TRANSMISSION TO   - 16:56:50 JAN 23, 2014
...
```

Usage & Invocation … TARGET LIST

- On the **denying** system

```
IRRM010I (<) RSWJ SUBSYSTEM PROPERTIES OF REMOTE RRSF NODE NODE2
             SYSNAME SYS3 (MAIN):
   STATE       - OPERATIVE ACTIVE
   DESCRIPTION - <NOT SPECIFIED>
   PROTOCOL    - TCP
                 HOST ADDRESS     - ALPS4220.POK.IBM.COM
                 IP ADDRESS       - 9.57.1.221
                 LISTENER PORT    - 18136
                 AT-TLS POLICY:
                   RULE_NAME      - RRSF-CLIENT
                   CIPHER ALG     - 35 TLS_RSA_WITH_AES_256_CBC_SHA
                   CLIENT AUTH    - REQUIRED
   INBOUND WORK IS NOT ACCEPTED FROM THIS NODE
         NUMBER OF REQUESTS DENIED FROM THIS SYSTEM: 4
   TIME OF LAST TRANSMISSION TO   - 17:22:07 JAN 23, 2014
...
```

Behavior on a denied downlevel system

- For a directed command (AT/ONLYAT) or automatically directed work

```
IRRT035I Node remote-node is not accepting work from local-node.
```

This message is returned just fine through the returned output infrastructure

- For RACLINK DEFINE (Note RACLINK APPROVE is OK)

```
IRRP096I Peer association with target-userID at node node-name by issuer-userID failed.
RACROUTE VERIFY RACF rc is 7.
```

Return code 7 means “denied” and is not understood on downlevel systems

–

- RACLINK UNDEFINE of an established association only removes the association locally and results in

```
IRRP020I RACF ICHEINTY rc 7 received while deleting association (node.user)
for user user.
```

Usage & Invocation...OPERCMDS protection of TARGET command

- All TARGET keywords are protected at the keyword level. E.G.:
  - Subsys-name.TARGET.keyword   E.G.:
    - RACF.TARGET.MAIN
- The DENYINBOUND, ALLOWINBOUND, and RESETDENYINBOUNDCOUNT keywords will all be protected under the DENYINBOUND keyword. E.G.:
  - RACF.TARGET.DENYINBOUND

Usage & Invocation...obtaining RRSF information using APIs

- The R_admin callable service (IRRSEQ00) and IRRXUTIL will report on
  - The denyinbound setting
    - Our notion of the remote partner
    - And its notion of us, as of the last time a connection was established between us
  - The number of denied requests from each remote partner

Migration & Coexistence Considerations

- A downlevel system may be denied. It will just not be as obvious to them, especially in the case of RACLINK commands (see slide 13).

Presentation Summary

- True one-way RRSF connections can now be enforced without relying on the configuration settings of the remote node
- This can be used to prevent privilege escalation on a production system from a privileged user on a test system
- You can prove this to auditors
- R_admin and IRRXUTIL report the relevant settings/fields

Appendix

- *RACF: System Programmer's Guide* (SA23-2287)
- *RACF: Command Language Reference* (SA23-2292)
- *RACF: Security Administrator's Guide* (SA23-2289)
- *RACF: Callable Services* (SA23-2293)
- *RACF: Macros and Interfaces* (SA23-2288)
- *RACF: Messages and Codes* (SA23-2291)