z/OS 3.1 IBM Education Assistant

Solution Name: FTP Server JES access control

Solution Element: z/OS Communications Server

July 2023

Agenda

- Trademarks
- Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Upgrade & Coexistence Considerations
- Installation & Configuration
- Summary
- Appendix

Trademarks

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

Objectives

- This initiative provides an easy-to-use and comprehensive control over which z/OS user IDs are permitted to submit jobs through the z/OS FTP server's JES operational mode. (FTP's JES mode has been noted by z/OS penetration testers as a way to introduce malware to an unprotected z/OS system)

- This new control is NOT intended to be a replacement for the JESJOBS or JESSPOOL classes. Those classes (and FTP JESINTERFACELEVEL 2) should still be implemented as they control JES access well beyond FTP

Overview

- Who (Audience)
  - z/OS system programmers with responsibility for FTP server security

- What (Solution)
  - New SAF resource for controlling access to the z/OS FTP server's JES operational mode

- Wow (Benefit / Value, Need Addressed)
  - By defining a SAF profile for the EZB.FTP.*sysname*.*ftpdaemonname*.ACCESS.JES resource, you can easily control which z/OS user IDs or groups are permitted to enter FILETYPE=JES operating mode to submit jobs for execution. Before this control was introduced, the only way to achieve such control was through custom-written user exits.
  - This function is also available on z/OS V2R4 and V2R5 with APAR PH42618 .

Usage & Invocation

- Define a profile for the following resource in your SAF security product:

```
EZB.FTP.sysname.ftpdaemonname.ACCESS.JES
```

- z/OS user IDs and groups with READ permission to this profile are permitted to enter FTP JES mode (for example, by using the SITE FILETYPE=JES FTP subcommand*)
- For users without permission to this profile, any attempt to enter JES mode is rejected with:

```
200 – User username is not allowed to use FILETYPE=JES
```

* For details on z/OS FTP subcommands, check the [z/OS Communications Server IP User's Guide and Commands FTP subcommands topic]

Interactions & Dependencies

- Software Dependencies: None

- Hardware Dependencies: None

- Exploiters: n/a

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Plex must be at the new z/OS level: No

- There are no toleration/coexistence APARs/PTFs. However, this function is available on z/OS V2R4 and V2R5 with APAR PH42618

- With z/OS 3.1 (and once APAR PH42618 is applied to a V2R4 or V2R5 system), the FTP server will **always** check the logged-in FTP user's z/OS user ID against the new SAF resource when it attempts to enter FTP mode using the **`site filetype=jes`** command

- If the SAF check results in a "no decision" return code (no profile found), access is permitted. However…

- When you upgrade to 3.1 (or after you apply the PTF with APAR PH42618 to a V2R4 or V2R5 system), existing FTP users may lose FTP JES access IF…

  …you use an external security manager that denies access by default

  …you have a generic profile defined that encompasses the **`EZB.FTP.`*`systemname`*`.`*`ftpdaemonname`*`.ACCESS.FTP`** resource (for example, **`EZB.FTP.PRODZOS1.FTPD1.ACCESS.*`**)

For cases like this, the upgrade action is to set up the appropriate SAF profile(s) before starting your z/OS FTP server

Installation & Configuration

- For a smooth deployment using RACF, we suggest initially defining a profile for the **EZB.FTP.*systemname.ftpdaemonname*.ACCESS.FTP** resource in **WARNING** mode and with **UACC(NONE)** to determine which z/OS user IDs are using FTP JES mode.

  Once JES mode usage is thoroughly understood, define access control lists that only permit users with a legitimate need to enter JES mode, and then remove **WARNING** from the profile.

- An easy way to "turn off" the new control is to define a profile for the **EZB.FTP.*systemname.ftpdaemonname*.ACCESS.FTP** resource with **UACC(READD)** (or equivalent for your security product).

  However, we recommend limiting FTP JES access only to those z/OS user IDs with a legitimate need to use JES mode.

Summary

- This initiative provides an easy-to-use and comprehensive control over which z/OS user IDs are permitted to submit jobs through the z/OS FTP server's JES operational mode.
- This new control is NOT intended to be a replacement for the JESJOBS or JESSPOOL classes. Those classes (and FTP JESINTERFACELEVEL 2) should still be implemented as they control JES access well beyond FTP
- In many cases, no migration action is required since access is permitted when the new SAF check results in a "no decision" return code. As noted, however, there are some cases where an upgrade action (defining the new profile) will be required.
- Regardless of upgrade considerations, we recommend using the new access control to limit FTP JES access only to those z/OS user IDs with a legitimate need to use JES mode.

Appendix

- z/OS Communications Server: IP Configuration Guide
  - Local user access control to TCP/IP resources using SAF
  - (Optional) Steps for controlling user access to FTP JES mode

- z/OS Communications Server: IP User's Guide and Commands
  - Restricting access to FTP JES mode with SAF profiles