z/OS Communications Server

Documentation changes for APAR PH42618

FTP server JES access control

Version 2 Release 3

Version 2 Release 4

Version 2 Release 5

z/OS Communications Server

z/OS Communications Server

CONTENTS

New Function Summary 2

FTP server JES access control 2

RACF interfaces 2

Samples provided in MVS data set SEZAINST 3

IP Configuration Guide 4

Local user access control to TCP/IP resources using SAF 4

Security for the FTP server 4

(Optional) Steps for controlling user access to FTP JES mode 5

Customizing the FTP-to-JES interface for JESINTERFACELevel 2 (optional) 6

IP Configuration Reference 8

FILETYPE (FTP client and server) statement 8

IP User's guide and commands 10

Restricting access to FTP JES mode with SAF profiles 10

JES security using JESINTERFACELEVEL 2 10

Changing JESSTATUS, JESOWNER, and JESJOBNAME 10

IP and SNA Codes 12

200-: User *user_name* is not allowed to use FILETYPE=JES 12

Trademarks 13

NEW FUNCTION SUMMARY

FTP server JES access control

z/OS V2R3, V2R4, and V2R5 Communications Server, with APAR PH42618, support a new SAF resource in the SERVAUTH class to control which users are allowed to access FTP JES mode. When the SERVAUTH class is active and a profile is defined for the EZB.FTP.*sysname.ftpdaemonname.*ACCESS.JES SAF resource, only users with permission to the profile are allowed to access FTP JES mode.

Dependency:

The SERVAUTH class must be active for the EZB.FTP.*sysname.ftpdaemonname.*ACCESS.JES SAF resource to provide access controls.

Using FTP server JES access control

To use FTP server JES access control, perform the tasks in Table 1. FTP server JES access control.

Table 1. FTP server JES access control

Task/Procedure	**Reference**
Implement FTP JES access controls using the SERVAUTH class • Activate the SERVAUTH class, if it is not already active • Define an EZB.FTP.*sysname.ftpdaemonname.*ACCESS.JES SAF resource profile with UACC(NONE) • For each user that should be allowed to use FTP FILETYPE=JES, give the user READ permission to the defined profile	See (Optional) Steps for controlling user access to FTP JES mode in IP Configuration Guide

RACF interfaces

Table 2. New and changed Communications Server RACF interfaces lists the functions for which new or changed RACF support is available.

Table 2. New and changed Communications Server RACP interfaces

z/OS Communications Server

New and changed Communications Server RACF interfaces		
Function name	**Description**	**Reason for change**
EZB.FTP.*sysname.ftpdaemonname*.ACCESS.JES	New SAF resource defined in the SERVAUTH class	FTP server JES access control

Samples provided in MVS data set SEZAINST

Table 3. IP samples provided in MVS data set SEZAINST for z/OS lists the changes to the samples that are provided in MVS data set SEZAINST..

Table 3. IP samples provided in MVS data set SEZAINST for z/OS

Member	Description	Reason for change
EZARACF	A new resource profile in the SERVAUTH class is provided for the EZB.FTP.*sysname.ftpdaemonname*.ACCESS.JES resource	FTP server JES access control

Local user access control to TCP/IP resources using SAF

Table 4. SERVAUTH resource names used by TCP/IP

Function	Description	No SAF decision	SERVAUTH resource name LOGSTR in any SAF logging (SMF type 80 records for RACF®)
FTP server JES access control	Controls ability to use FILETYPE JES mode based on SAF user ID used to log in	Permit	EZB.FTP.*sysname.ftpdaemonname*.ACCESS.JES
			(none)

Security for the FTP server

To provide security for the FTP server, you must perform the following tasks:

1. (Optional) Activate and define the SERVAUTH class (see (Optional) Steps for activating and defining the SERVAUTH class).
2. Set up security for the FTP server (see Steps for setting up security for your FTP server).
3. Provide and control user access to the FTP server (see Steps for controlling user access to the FTP server).
4. Set up a port of entry for users of the FTP server (see Steps for setting up a port of entry for users of the FTP server).
5. Provide and control user access to the z/OS® UNIX file system (see (Optional) Steps for controlling user access to the z/OS UNIX file system).
6. Provide and control user access to FTP JES mode (see (Optional) Steps for controlling user access to FTP JES mode)
7. Prevent exploitation of your FTP server (see Preventing exploitation of your FTP server).
8. (Optional) Assign password phrases to user IDs that are used to log in to the FTP server (see (Optional) Assigning password phrases to user IDs that are used to log in to the FTP server).

FTP uses resource profiles in the System Authorization Facility (SAF) SERVAUTH class to control access to certain facilities and servers. When access to a resource is controlled by a profile in the SERVAUTH class, you must activate and RACLIST the SERVAUTH class. You do not have to use the SERVAUTH class, but when a profile is defined in that class, all FTP users who require access to it must be permitted to it.

For more information, see z/OS UNIX System Services Planning and z/OS Security Server RACF Security Administrator's Guide. For more information about network access security zones, see Network access control. If you are planning to implement a multilevel security environment on your z/OS system, see Preparing for IP networking in a multilevel secure environment.

(Optional) Steps for controlling user access to FTP JES mode

FTP uses the SAF resource EZB.FTP.*sysname.ftpdaemonname*.ACCESS.JES in the SERVAUTH class to control access to FTP JES mode. If you do not control access to this resource, then all users can use FTP JES mode. While in JES mode a user can submit a job, display job output, and delete job output. You are strongly encouraged to define a profile to control access to the EZB.FTP.*sysname.ftpdaemonname.*ACCESS.JES resource and grant read access only to users with a legitimate need to use JES mode.

Before you begin

You must have the authority to issue the necessary RACF® commands.

The following procedure assumes that you are using RACF as your security product. You can, however, use any SAF-compliant security product.

Procedure

Perform the following steps to control access to FTP JES mode.

1. Define the profile for the FTP user access to FTP JES mode.

   The profile has the following form:

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

   For example, the profile name for FTP daemon FTPD running on system MVSA is the following name:

   ```
   EZB.FTP.MVSA.FTPD1.ACCESS.JES
   ```

   Tip: The profile name can contain wildcard values as allowed by the security product. All security-product rules (for example wildcards, PROTECTALL, and so on) apply. For example, if all systems will use the same access list and RACF generic profile checking is active for the SERVAUTH class, you could use the following profile name:

   EZB.FTP.*.FTPD1.ACCESS.JES

2. Permit the user IDs that require access to JES mode to the profile:

   ```
   PERMIT EZB.FTP.sysname.ftpdaemonname.ACCESS.JES CLASS(SERVAUTH)
          ID(ftpuser) ACCESS(READ)
   ```

Tip: If you allow anonymous users to login by configuring the ANONYMOUS statement in FTP.DATA, consider whether those users require access to JES mode (such a requirement would be very unusual). If anonymous users do require access to JES mode, the anonymous user ID must be permitted to the profile. The anonymous user ID is configured on the ANONYMOUS statement or defaults to ANONYMO. See ANONYMOUS (FTP server) statement in z/OS Communications Server: IP Configuration Reference for more information.

3. Take one of the following actions:
   - If the RACF SERVAUTH class is not already activated issue the following commands:

```
SETROPTS CLASSACT(SERVAUTH)
SETROPTS RACLIST(SERVAUTH)
```

   - Otherwise (the SERVAUTH class is active), refresh the SERVAUTH class if a new profile has been added or an existing profile has changed:

```
SETROPTS RACLIST (SERVAUTH) REFRESH
```

Results

- When you are finished, only certain users will be able to access FTP JES mode.
- When a user issues SITE FILETYPE=JES, the user's access to FTP JES mode is checked. If the user is not allowed to access FTP JES mode, the FILETYPE for the connection remains unchanged.
- When a user logs into an FTP server that is configured with FILETYPE JES, the user's access to FTP JES mode is checked. If the user is not allowed to access FTP JES mode, the FILETYPE for the connection is set to the default value of sequential (SEQ) mode.

Customizing the FTP-to-JES interface for JESINTERFACELevel 2 (optional)

If JESINTERFACELEVEL is set or defaulted to 1, the FTP user is allowed to submit jobs to JES, retrieve held output matching their logged-in user ID plus one character, and delete held jobs matching their logged-in user ID plus one character.

If JESINTERFACELevel is set to 2, FTP users have the ability to retrieve and delete any job in the system permitted by the System Authorization Facility (SAF) resource class JESSPOOL. For that reason, JESINTERFACELevel=2 should be specified only if the appropriate JES and SDSF security measures are in place to protect access to JES output. The SAF controls used for JESINTERFACELevel=2 are essentially a subset of those used by SDSF. Therefore, if an installation has customized SAF facilities for SDSF, they are configured for FTP JES level 2.

Note: You are not required to have SDSF to use JESINTERFACELEVEL 2. If you do not use SDSF, you still need to create SAF profiles. Both SDSF and JESINTERACELEVEL 2 use the same SAF profile names.

z/OS Communications Server

Before customizing the FTP-to-JES interface, complete JES customization. For example, JESJOBS is an SAF class that controls which users can submit jobs to JES. JESSPOOL is the SAF class that controls which users can access output jobs. Customize these SAF classes before beginning customization of the FTP-to-JES interface.

JESSPOOL defines resource names as <nodeid>.<userid>.<jobname>.<Dsid>.<dsname>. An FTP user can delete an output job if they have UPDATE access to the resource that matches their nodeid, userid, and job name. If the FTP user has READ access to the resource, they can list, retrieve, or GET the job output. For more information on JES security, see z/OS JES2 Initialization and Tuning Guide. For more information on the SAPI interface, see z/OS MVS Using the Subsystem Interface.

There are three filters used by the FTP server to control the display of jobs:

- JESSTATUS
- JESOWNER
- JESJOBNAME

SAF resources in the SDSF class are employed for this.

JESSTATUS can be changed by an FTP user with the SITE command to filter jobs in INPUT, ACTIVE, or OUTPUT state. The SAF resources checked for these states are ISFCMD.DSP.INPUT.jesx, ISFCMD.DSP.ACTIVE.jesx, and ISFCMD.DSP.OUTPUT.jesx, respectively. The default value is set to ALL if READ access is allowed to all three classes. Otherwise it attempts to set the default value to OUTPUT, ACTIVE, and then INPUT if the appropriate READ access is allowed. If no READ access is allowed to any of the classes, JESSTATUS is set to OUTPUT but JESOWNER and JESJOBNAME cannot be changed from the default. In this way, SAF controls can be put in place to limit FTP users to whatever status of jobs an installation requires.

By default, JESOWNER will have the value of the logged-in user ID. Authority to change JESOWNER is obtained through READ access to SAF resource ISFCMD.FILTER.OWNER. An FTP user who has READ access to ISFCMD.FILTER.OWNER will be allowed to change the JESOWNER parameter with the SITE command.

By default, JESJOBNAME will have the value of the logged-in user ID plus an asterisk (*). Authority to change JESJOBNAME is obtained through READ access to SAF resource ISFCMD.FILTER.PREFIX. An FTP user who has READ access to ISFCMD.FILTER.PREFIX will be allowed to change the JESJOBNAME parameter with the SITE command.

For example, to allow all users except USER1 to change JESOWNER enter the following commands:

```
SETROPTS CLASSACT(SDSF) REFRESH
RDEFINE SDSF (ISFCMD.FILTER.OWNER) UACC(READ)
PERMIT ISFCMD.FILTER.OWNER ACCESS(NONE) CLASS(SDSF) ID(USER1)
SETROPTS CLASSACT(SDSF) REFRESH
```

For more information on SDSF security, see z/OS SDSF Operation and Customization.

FILETYPE (FTP client and server) statement

Use the FILETYPE statement to specify the method of operation for FTP.

Syntax

```
   .-FILETYPE SEQ------.
>>-+-------------------+-------------------------------------><
   '-FILETYPE--+-JES-+-'
               +-SEQ-+
               '-SQL-'
```

Parameters

JES

Remote job submission.

Restriction: This parameter applies to the server only.

SEQ

MVS™ data sets or z/OS® UNIX files. SEQ is the method of operation supported by all FTP platforms. This is the default.

SQL

SQL query function. SQL method affects the RETR command at the server and the PUT subcommand at the client.

Examples

Set the operational method to SQL:

```
Filetype SQL
```

Usage notes

- SQL pertains to z/OS platform only. For more information about the effects on command processing when FILETYPE is SQL, see z/OS Communications Server: IP User's Guide and Commands.
- When the SQL method is in specified for the server, it affects the RETR command only. When the SQL method is specified for the client, it affects the STOR command only.

z/OS Communications Server

- JES pertains to the z/OS platform only and is valid only in the FTP.DATA file for a server. For more information about the effects on command processing at the server when the server's FILETYPE is JES, see z/OS Communications Server: IP User's Guide and Commands.
- JES method affects the STOR, LIST, RETR, and NLST commands.
- The SAF resource EZB.FTP.*sysname.daemonname.*ACCESS.JES can be used to control access to FTP JES mode. See (Optional) Steps for controlling user access to FTP JES mode in the z/OS Communications Server: IP Configuration Guide.

Restricting access to FTP JES mode with SAF profiles

The SAF resource EZB.FTP.*sysname.ftpdaemonname.*ACCESS.JES in the SERVAUTH class can be used to control access to FTP JES mode. If a profile for the SAF resource is defined, a user must have READ access to the profile to connect to an FTP server in JES mode or to issue the SITE FILETYPE=JES command. This SAF resource is checked independently of the JESINTERFACELEVEL setting.

If a user is not authorized to use JES mode, an attempt to connect to an FTP server in JES mode is accepted but the file mode is set to SEQ. The stat command can be used to verify the FileType setting.

If a user is not authorized to use JES mode, any SITE FILETYPE=JES command is rejected with a reply:

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

JES security using JESINTERFACELEVEL 2

If JESINTERFACELEVEL is set or defaulted to 1, FTP clients are allowed to submit jobs to JES, retrieve held output that matches their logged in user ID plus one character, and delete held jobs that match their logged in user ID plus one character.

If JESINTERFACELevel is set to 2, then FTP clients have the ability to retrieve and delete any job in the system permitted by the Security Access Facility (SAF) resource class JESSPOOL. For that reason, JESINTERFACELevel=2 should be specified only if the proper JES and SDSF security measures are in place to protect access to JES output. The SAF controls used for JESINTERFACELevel=2 are essentially a subset of those used by SDSF. Therefore, if an installation has customized SAF facilities for SDSF, then they are configured for FTP JES level 2.

Before customizing the FTP-to-JES interface, you must complete JES customization. For example, JESJOBS is an SAF class that controls which users can submit jobs to JES. JESSPOOL is the SAF class that controls which users can access output jobs. Customize these SAF classes before beginning customization of the FTP-to-JES interface.

JESSPOOL defines resource names as <nodeid>, <userid>, <jobname>, <Dsid>, <dsname>. An FTP client can delete an output job if it has ALTER access to the resource that matches its nodeid, userid, and job name. If the FTP client has READ access to the resource, it can list, retrieve, or GET the job output. (JESINTERFACELevel 2 uses the SAPI interface to JES, so READ authority is required to list job status or retrieve job output.) See the z/OS JES2 Initialization and Tuning Guide for more information on JES security. See z/OS MVS Using the Subsystem Interface for more information on the SAPI interface.

Changing JESSTATUS, JESOWNER, and JESJOBNAME

There are three filters used by the FTP server to control the display of jobs:

- JESSTATUS

- JESOWNER
- JESJOBNAME

SAF resources in the SDSF class are employed for this.

JESSTATUS can be changed by an FTP client using the SITE command to filter jobs in INPUT, ACTIVE, or OUTPUT state. The SAF resources checked for these states are ISFCMD.DSP.INPUT.*jesx*, ISFCMD.DSP.ACTIVE.jesx, and ISFCMD.DSP.OUTPUT.jesx, respectively. The default value is set to ALL if READ access is allowed to all three classes. Otherwise it attempts to set the default value to OUTPUT, ACTIVE, and then INPUT if the appropriate READ access is allowed. If no READ access is allowed to any of the classes, JESSTATUS is set to OUTPUT but JESOWNER and JESJOBNAME cannot be changed from the default. In this way, SAF controls can be put in place to limit FTP clients to whatever status of jobs an installation requires.

By default, JESOWNER has the value of the logged in user ID. Authority to change JESOWNER is obtained by READ access to SAF resource ISFCMD.FILTER.OWNER. An FTP client with READ access to ISFCMD.FILTER.OWNER is allowed to change the JESOWNER parameter using the SITE command.

By default, JESJOBNAME has the value of the logged in user ID plus an asterisk (*). Authority to change JESJOBNAME is obtained by READ access to SAF resource ISFCMD.FILTER.PREFIX. An FTP client with READ access to ISFCMD.FILTER.PREFIX is allowed to change the JESJOBNAME parameter using the SITE command.

If a user is not authorized to the appropriate `ISFCMD.DSP.<status>.jesx`, any SITE JESSTATUS command is rejected with a reply:

```
200 User xxxxxxx is not authorized to filter on JESSTATUS, JESSTATUS remains
xxxxxxx
```

If a user is not authorized to filter on JESOWNER, any SITE JESOWNER command is rejected with a reply:

```
200 User xxxxxxx is not authorized to filter on JESOWNER, JESOWNER remains
xxxxxxx
```

If a user is not authorized to filter on JESJOBNAME, any SITE JESJOBNAME command is rejected with a reply:

```
200 User xxxxxxx is not authorized to filter on JESJOBNAME, JESJOBNAME
remains
xxxxxxx*
```

IP AND SNA CODES

A new FTPD 200 reply code is added with FTP server JES access control.

200-: User *user_name* is not allowed to use FILETYPE=JES

Explanation

The SITE command was specified with the FILETYPE=JES parameter. *user_name* is not permitted to change the FILETYPE to JES with the SITE command because the user is not allowed access by the server's security product.

In the message text:
user_name
The login name on the host.

System action

The FILETYPE=JES parameter is ignored. FTP continues.

User response

Contact the system programmer. Try again after your user ID is added to the resource class.

System programmer response

If the user should be allowed to change the FILETYPE to JES with the SITE command, grant the user read access to the SAF resource profile defined by the security product for the resource EZB.FTP.*sysname*.*ftpdaemonname*.ACCESS.JES. For more information, see "(Optional) Steps for controlling user access to FTP JES mode in z/OS Communications Server: IP Configuration Guide.

Module

EZAFTPMK

Example

```
200-User USER1 is not allowed to use FILETYPE=JES
```

TRADEMARKS