IBM Explorer for z/OS

Host Configuration Guide

SC27-8437-02

IBM Explorer for z/OS

Host Configuration Guide

SC27-8437-02

Note
Before using this information, be sure to read the general information under "Notices" on page 97.

Third edition (September, 2017)

This edition applies to IBM Explorer for z/OS Version 3.1.1 (program number 5655-EX1) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures

Tables

About this document

This document discusses the configuration of the IBM® Explorer for z/OS® functions. It includes instructions to configure IBM Explorer for z/OS Version 3.0 on your z/OS host system.

From here on, the following names are used in this manual:

- *IBM Explorer for z/OS* is called *z/OS Explorer*.
- *z/OS UNIX System Services* is called *z/OS UNIX*.
- *Remote System Explorer* is called *RSE*.
- *IBM Developer for z Systems*™ (previously known as *Rational® Developer for z Systems*) is called *IDz*.

This document is part of a set of documents that describe z/OS Explorer host system configuration. Each of these documents has a specific target audience. You do not have to read all of these documents to complete the z/OS Explorer configuration.

- *IBM Explorer for z/OS Host Configuration Guide* (SC27-8437) describes in detail all of the planning tasks, configuration tasks, and options and provides alternative scenarios.
- *IBM Explorer for z/OS Host Configuration Reference Guide* (SC27-8438) describes z/OS Explorer design and gives background information for various configuration tasks of z/OS Explorer and z/OS components related to z/OS Explorer.
- *IBM Explorer for z/OS Host Configuration Quick Start Guide* (GI13-4313) describes a minimal setup of z/OS Explorer.
- *IBM Explorer for z/OS Host Configuration Utility Guide* (SC27-8436) describes the Host Configuration Utility, an ISPF panel application that guides you through basic and common optional customization steps for z/OS Explorer.

For the most up-to-date versions of the complete documentation, including installation instructions, white papers, podcasts, and tutorials, see the IBM Explorer for z/OS library page.

Who should use this document

This document is intended for system programmers who are installing and configuring IBM Explorer for z/OS Version 3.0.1.

This document lists in detail the steps that are needed to do a full setup of the product, including some non-default scenarios. Background information that can help you to plan and execute the configuration can be found in the *IBM Explorer for z/OS Host Configuration Reference Guide* (SC27-8438). To use this document, you must be familiar with the z/OS UNIX System Services and MVS™ host systems.

Description of the document content

This section summarizes the information that is given in this document.

Planning

Use the information in this chapter to plan the installation and deployment of z/OS Explorer.

Basic customization

The following customization steps are for a basic z/OS Explorer setup:

- "Customization setup" on page 9
- "PARMLIB changes" on page 10
- "PROCLIB changes" on page 14
- "Security definitions" on page 17
- "FEJJCNFG, the JES Job Monitor configuration file" on page 17
- "rse.env, the RSE configuration file" on page 22
- "ISPF.conf, the Legacy ISPF Gateway configuration file" on page 37

(Optional) Other customization tasks

This section combines a variety of optional customization tasks. To configure the required service, follow the instructions in the appropriate section.

Customizations to z/OS Explorer configuration files:

- pushtoclient.properties, Host-based client control
- ssl.properties, RSE encrypted communication
- rsecomm.properties, RSE tracing

z/OS Explorer related customizations to or for other products:

- Send message
- Interactive ISPF Gateway
- WORKAREA and /tmp cleanup

Installation verification

After completing the product customization, you can verify the successful setup of key product components by using the Installation Verification Programs (IVPs) described in this chapter.

Security definitions

This section describes the required and optional security definitions with sample RACF® commands.

Operator commands

This section provides an overview of the available operator (or console) commands for z/OS Explorer.

Host Configuration Reference

This section summarizes the information in *Host Configuration Reference* (SC27-8438).

Chapter 1. Planning

Use the information in this chapter and the IBM Explorer for z/OS (z/OS Explorer) software requirements to plan the installation and deployment of z/OS Explorer. The following subjects are described:

- "Planning considerations"
- "Preinstallation considerations" on page 2
- "Pre-configuration considerations" on page 5
- "Predeployment considerations" on page 7
- "Client checklist" on page 8

For a complete listing of the z/OS Explorer hardware and software requirements including prerequisites and co-requisites, generate reports from Software Product Compatibility Reports.

Planning considerations

Product overview

z/OS Explorer consists of a client, installed on the user's personal computer, and a server, installed on one or more host systems. This documentation contains information for a z/OS host system.

The client provides developers with an Eclipse-based development environment that facilitates a uniform graphical interface to the host, and that, among other things, can offload work from the host to the client, saving resources on the host.

The host portion consists of several permanently active tasks and tasks that are started ad hoc. These tasks allow the client to work with the various components of your z/OS host system, such as MVS data sets, TSO commands, z/OS UNIX files and commands, job submit, and job output.

Both z/OS Explorer host and client allow other products to be installed on top to extend the capabilities, for example, interacting with Software Configuration Managers (SCMs).

For a basic understanding of the z/OS Explorer design, see "Understanding z/OS Explorer" in the *Host Configuration Reference Guide* (SC27-8438).

To learn more about the functionality that is offered by z/OS Explorer, see Mainframe DEV, or your local IBM representative.

Skill requirements

SMP/E skills are needed for a z/OS Explorer host installation.

The configuration of z/OS Explorer requires more than the typical system programming permissions and expertise, so assistance from others might be needed. Table 3 on page 4 and Table 4 on page 4 list the administrators who are needed for the required and optional customization tasks.

Time requirements

The amount of time that is required to install and configure the z/OS Explorer host system components depends on various factors such as these:

- The current z/OS UNIX and TCP/IP configuration
- The availability of prerequisite software and maintenance
- Whether OMVS segments are defined for z/OS Explorer users
- The availability of a user, who has successfully installed the client, to test the installation and report any problems that might occur

Experience has shown that the installation and configuration process of the z/OS Explorer host system requires from one to four days to complete. This time requirement is for a clean installation performed by an experienced system programmer. If problems are encountered, or if the required skills are not available, the setup will take longer.

Preinstallation considerations

For detailed instructions on the SMP/E installation of the product, see *Program Directory for IBM Explorer for z/OS* (GI13-4314).

The z/OS Explorer servers are single-system minded, and are not SYSPLEX aware. If you are using the servers in a SYSPLEX, you must ensure that the data requested by the users (data sets, job output, z/OS UNIX files) is available on the system z/OS Explorer is installed. See "Predeployment considerations" on page 7 for cloning z/OS Explorer to other systems.

To run multiple instances of z/OS Explorer on a single host system, see "Running multiple instances" in the *Host Configuration Reference Guide* (SC27-8438).

The file system (HFS or zFS) in which z/OS Explorer is installed must be mounted with the `SETUID` permission bit on (this is the system default). Mounting the file system with the `NOSETUID` parameter prevents z/OS Explorer from creating the user's security environment, and rejects the connection requests of the client. The same is true for the file systems hosting Java™ and z/OS UNIX binaries.

Installation user ID

The user ID that is used to install z/OS Explorer, or to install maintenance, must have at least the following attributes:

- TSO access (with a normal region size).

  Note: A large region size is required for the user ID that runs the Installation Verification Programs (IVPs) because functions requiring a lot of memory (such as Java) are executed. You should set the region size to 131072 kilobytes (128 megabytes) or higher.
- An OMVS segment defined to the security system (for example, RACF), both for the user ID and its default group.
  - The `HOME` field must refer to a home directory that is allocated for the user, with READ, WRITE, and EXECUTE access.
  - The `PROGRAM` field in the OMVS segment should be `/bin/sh` or other valid z/OS UNIX shell, such as `/bin/tcsh`.
  - The user ID's default group requires a `GID`.
- `UID=0` or READ authorization to the `BPX.SUPERUSER` profile in the `FACILITY` class.

- If the BPX.FILEATTR.APF or BPX.FILEATTR.PROGCTL profiles are defined in the FACILITY class, READ access to these profiles.
- READ, WRITE, and EXECUTE access to the /tmp directory (or a directory referenced in the TMPDIR environment variable).

Requisite products

z/OS Explorer has a list of prerequisite software that must be installed and operational before the product will work. There is also a list of corequisite software to support specific features of z/OS Explorer. These requisites must be installed and operational at runtime for the corresponding features to work as designed.

For a complete listing of the z/OS Explorer software requirements including prerequisites and co-requisites, generate reports from Software Product Compatibility Reports.

Plan ahead to have these requisite products available, as it might take some time, depending on the policies at your site. The key requisites for a basic setup are:

- z/OS 1.13 or higher
- Latest service release of Java 6.0 or higher (31 or 64 bit)

Required resources

z/OS Explorer requires the allocation of the systems resources listed in Table 1. The resources listed in Table 2 on page 4 are required for optional services. Plan to have these resources available because, depending on the policies at your site, it might take some time to get the software.

Table 1. Required resources

Resource	Default value	Information
LPA data set	FEK.SFEKLPA	"LPA definitions in LPALSTxx" on page 12
APF-authorized data set	FEK.SFEKAUTH	"APF authorizations in PROGxx" on page 12
started task	JMON and RSED	"PROCLIB changes" on page 14
port for host-confined use (JMON)	6715	"FEJJCNFG, the JES Job Monitor configuration file" on page 17
port for client-host communication (RSED)	4035	"rse.env, the RSE configuration file" on page 22
port range for client-host communication (RSED)	Any available port is used	"Defining the PORTRANGE available for RSE server" on page 28
z/OS UNIX server security definition	UPDATE permission to BPX.SERVER for RSED started task	"Define RSE as a secure z/OS UNIX server" on page 62
PassTicket security definitions	No default	"Define the PassTicket support for RSE" on page 64

Table 2. Optional resources

Resource	Default value	Information
TSO logon procedure update	• Add FEK.SFEKAUTH • Remove ISPF panel invocation	• "(Optional) Send message" on page 47 • "(Optional) Interactive ISPF Gateway" on page 49.

The configuration of z/OS Explorer requires more than the typical system programming permissions and expertise; therefore, assistance from others might be needed. Table 3 and Table 4 list the administrators who are needed for the required and optional customization tasks.

Table 3. Administrators needed for required tasks

Administrator	Task	Information
System	Typical system programmer actions are required for all customization tasks	N/A
Security	• Define OMVS segment for z/OS Explorer users • Define data set profiles • Define started tasks • Define operator command security • Define z/OS UNIX server profiles • Define application security • Define PassTicket support • Define program controlled data sets	"Security considerations" in *Host Configuration Reference Guide* (SC27-8438)
TCP/IP	Define new TCP/IP ports	"TCP/IP considerations" in *Host Configuration Reference Guide* (SC27-8438)
WLM	Assign the started task goals to the servers and their child processes	"WLM considerations" in *Host Configuration Reference Guide* (SC27-8438).

Table 4. Administrators needed for optional tasks

Administrator	Task	Information
System	Typical system programmer actions are required for all customization tasks	N/A

Table 4. Administrators needed for optional tasks (continued)

Administrator	Task	Information
Security	• Add certificate for encrypted communication • Define X.509 client certificate support • Define groups and profiles for push-to-client • Define profiles for altering client functions • Define profiles for sending messages	• "Security considerations" in *Host Configuration Reference Guide* (SC27-8438) • "Setting up encrypted communication and X.509 authentication" in the *Host Configuration Reference Guide* (SC27-8438)
LDAP	Define groups for push-to-client	"Push-to-client considerations" in the *Host Configuration Reference Guide* (SC27-8438)

Pre-configuration considerations

For information about z/OS Explorer itself, how it interacts with your system, and with the prerequisite and co-requisite products, see the *Host Configuration Reference Guide* (SC27-8438). This information can assist you in creating a setup that supports your current needs and future growth.

Workload management

Unlike traditional z/OS applications, z/OS Explorer is not a monolithic application that can be identified easily to Workload Manager (WLM). z/OS Explorer consists of several components that interact to give the client access to the host system services and data. To plan your WLM configuration, see "WLM considerations" in the *Host Configuration Reference Guide* (SC27-8438).

Note: z/OS Explorer consists of multiple tasks that communicate with each other and the client. These tasks use various timers to detect communication loss with their partners. Timeout issues can arise (due to lack of CPU time during the timeout window) on systems with a heavy CPU load or incorrect Workload Management (WLM) settings for z/OS Explorer.

Resource usage and system limits

z/OS Explorer uses a variable number of system resources such as address spaces, and z/OS UNIX processes and threads. The availability of these resources is limited by various system definitions. To estimate the usage of key resources so that you can plan your system configuration, see "Tuning considerations" in the *Host Configuration Reference Guide* (SC27-8438). z/OS Explorer can run in either 31-bit or 64-bit mode, changing the storage resource limitations drastically.

Required configuration of requisite products

Consult your MVS system programmer, security administrator, and TCP/IP administrator to verify if the requisite products and software are installed, tested, and working. Some requisite customization tasks that can be overlooked are listed here:

- All z/OS Explorer users must have READ and EXECUTE access to the Java directories.

User ID considerations

The user ID of a z/OS Explorer user must have at least the following attributes:

- TSO access (with a normal region size).

  Note: A large region size is required for the user ID that runs the Installation Verification Programs (IVPs) because functions requiring a lot of memory (such as Java) are executed. You should set the region size to 131072 kilobytes (128 megabytes) or higher.

- An OMVS segment defined to the security system (for example, RACF), both for the user ID and its default group.
  - The `HOME` field must refer to a home directory allocated for the user (with READ, WRITE and EXECUTE access).
  - The `PROGRAM` field in the OMVS segment should be `/bin/sh` or other valid z/OS UNIX shell, such as `/bin/tcsh`.
  - The `ASSIZEMAX` field should not be set, so that system defaults are used.
  - The user ID does not require UID 0.

    Example (command **`LISTUSER userid NORACF OMVS`**):

    ```
    USER=userid

    OMVS INFORMATION
    ----------------
    UID= 0000003200
    HOME= /u/userid
    PROGRAM= /bin/sh
    CPUTIMEMAX= NONE
    ASSIZEMAX= NONE
    FILEPROCMAX= NONE
    PROCUSERMAX= NONE
    THREADSMAX= NONE
    MMAPAREAMAX= NONE
    ```

  - The user ID's default group requires a `GID`.

    Example (command **`LISTGRP group NORACF OMVS`**):

    ```
    GROUP group

    OMVS INFORMATION
    ----------------
    GID= 0000003243
    ```

- READ and EXECUTE access to the z/OS Explorer installation and configuration directories and files, default `/usr/lpp/IBM/zexpl/*`, `/etc/zexpl/*`, and `/var/zexpl/*`.
- READ, WRITE, and EXECUTE access to the z/OS Explorer WORKAREA directory, default `/var/zexpl/WORKAREA`, and user log directory, default `/var/zexpl/logs`.
- READ access to the z/OS Explorer installation data sets, default `FEK.SFEK*`.
- READ, WRITE, and EXECUTE access to the `/tmp` directory or a directory referenced in the `TMPDIR` environment variable.

Server considerations

z/OS Explorer consists of multiple permanently active servers, which can be started tasks or user jobs. These servers provide the requested services themselves or start other servers (as z/OS UNIX threads or user jobs) to provide the service. There is no specific start order. The only requirement is that the servers are up and running before the first user tries to connect. The security mechanisms used by z/OS Explorer servers and services rely on the data sets and file systems they

reside in being secure. This implies that only trusted system administrators should be able to update the program libraries and configuration files.

- JES Job Monitor (JMON) provides all JES-related services.
- Remote Systems Explorer (RSE) provides core services such as connecting the client to the host system and starting other servers for specific services. RSE consists of two logical entities:
  - RSE daemon (RSED), which manages connection setup.
  - RSE server, which handles individual client requests.

As documented in "TCP/IP ports" in *Host Configuration Reference Guide* (SC27-8438), certain host system services, and thus their ports, must be available for the client to connect to, and must be defined to your firewall protecting the host system. All other ports used by z/OS Explorer have host-only traffic. Listed below are the ports that are needed for external communication in a basic z/OS Explorer setup.

- RSE daemon for client-host communication setup (using TCP), default port 4035.
- RSE server for client-host communication (using TCP). By default, any available port is used, but the available ports can be limited to a specified range.

Configuration method

z/OS Explorer provides alternative methods to configure the host system side of the product. These are the methods:

- Using the Host Configuration Utility. This ISPF panel application guides you through the required customization steps and selected optional customization steps. For more information, see the *Host Configuration Utility Guide* (SC27-8436).
- Using the *Host Configuration Quick Start Guide* (GI13-4313). This document guides you through the required customization steps. The scope of this guide is limited to a basic setup.
- Using the *Host Configuration Guide* (SC27-8437). This document guides you through the required customization steps and all of the optional customization steps. All configurable options are covered in this guide, including some non-default scenarios.

Predeployment considerations

z/OS Explorer supports the cloning of an installation to a different system, thus avoiding the need for a SMP/E installation on each system.

The following data sets, directories, and files are mandatory for deployment to other systems. If you copied a file to a different location, this file must replace its counterpart in the following lists.

Note: The following list does not cover the deployment needs of the prerequisite and co-requisite software.

- FEK.SFEKAUTH(*)
- FEK.SFEKLPA(*)
- FEK.SFEKPROC(*)
- FEK.#CUST.PARMLIB(*)
- FEK.#CUST.PROCLIB(*)
- /usr/lpp/IBM/zexpl/*
- /etc/zexpl/*
- /var/zexpl/* (directory structure only)

- optional parts:
  - FEK.#CUST.CNTL(*)
  - definitions, data sets, files, and directories resulting from customization jobs in FEK.#CUST.JCL

Note:

- `FEK` and `/usr/lpp/IBM/zexpl` are the high-level qualifier and path used during the installation of z/OS Explorer. `FEK.#CUST`, `/etc/zexpl` and `/var/zexpl` are the default locations used during the customization of the product (see "Customization setup" on page 9 for more information).
- z/OS Explorer supports distributed Dynamic VIPA, where identical servers on different systems in a SYSPLEX can be presented to the client as a single server. See "Distributed Dynamic VIPA" in the *Host Configuration Reference Guide* (SC27-8438) for more details.
- You should install z/OS Explorer in a private file system (HFS or zFS) to ease the deploying of the z/OS UNIX parts of the product. If you cannot use a private file system, use an archiving tool such as the z/OS UNIX `tar` command to transport the z/OS UNIX directories from one system to another. This method is for preserving the attributes (such as program control) for the z/OS Explorer files and directories.

  For more information about the following sample commands to archive and restore the z/OS Explorer installation directory, see *UNIX System Services Command Reference* (SA22-7802).
  - Archive: `cd /SYS1/usr/lpp/IBM/zexpl; tar -cSf /u/userid/zexpl.tar`
  - Restore: `cd /SYS2/usr/lpp/IBM/zexpl; tar -xSpf /u/userid/zexpl.tar`

Client checklist

Users of the z/OS Explorer client must know the result of certain host system customizations, such as TCP/IP port numbers, for the client to work properly. Use these checklists to gather the information needed.

The checklist in Table 5 lists the required results of mandatory customization steps. Table 6 lists the required results of optional customization steps.

Table 5. Client checklist: Mandatory parts

Customization	Value
RSE daemon TCP/IP port number. The default is `4035`. See "RSED, RSE daemon started task" on page 15.	

Table 6. Client checklist: Optional parts

Customization	Value
(co-requisite) TN3270 port number for Host Connect Emulator. The default is `23`. See "TCP/IP ports" in *Host Configuration Reference Guide* (SC27-8438).	

Chapter 2. Basic customization

The following customization steps are for a basic z/OS Explorer setup. See the chapters about the optional components for their customization requirements.

Requirements and checklist

You need the assistance of a security administrator and a TCP/IP administrator to complete this customization task, which requires the following resources and special customization tasks:

- LPA data set
- APF-authorized data set
- Various PARMLIB updates
- Various security software updates
- Various TCP/IP ports for internal and client-host communication

To verify the installation and to start using z/OS Explorer at your site, do the following tasks. Unless otherwise indicated, all tasks are mandatory.

1. Create customizable copies of samples and create the work environment for z/OS Explorer. For details, see "Customization setup."
2. Update z/OS UNIX system limits, update product registration, start started tasks, and define APF-authorized and LPA data sets. For details, see "PARMLIB changes" on page 10.
3. Create started task procedures. For details, see "PROCLIB changes" on page 14.
4. Update security definitions. For details, see "Security definitions" on page 17. To establish thread security, you must understand how PassTickets are used. See "Using PassTickets" in *Host Configuration Reference Guide* (SC27-8438).
5. Customize Developer for z/OS Explorer configuration files. For details, see:
   - "FEJJCNFG, the JES Job Monitor configuration file" on page 17
   - "rse.env, the RSE configuration file" on page 22
   - "ISPF.conf, the Legacy ISPF Gateway configuration file" on page 37

Customization setup

z/OS Explorer contains several sample configuration files and sample JCL. To avoid overwriting your customizations when applying maintenance, copy all of these members and z/OS UNIX files to a different location, and customize the copy.

Some functions of z/OS Explorer require the existence of certain directories in z/OS UNIX, which must be created during the customization of the product. To ease the installation effort, a sample job, `FEKSETUP`, is provided to create the copies and the required directories.

Note: The *Host Configuration Utility Guide* (SC27-8436) describes the host system configuration when using the Host Configuration utility. The `FEKSETUP` job and the utility do some of the same tasks, with no way of checking if those tasks have already been performed. Therefore, it is possible to undo changes that have already been made. For this reason, do not use both methods for a single installation.

To create customizable copies of configuration files and configuration JCL, and to create required z/OS UNIX directories, customize and submit the sample FEKSETUP member in the FEK.SFEKSAMP data set. The required customization steps are described within the member.

This job performs the following tasks:

- Create FEK.#CUST.PARMLIB and populate it with sample configuration files.
- Create FEK.#CUST.PROCLIB and populate it with sample SYS1.PROCLIB members.
- Create FEK.#CUST.JCL and populate it with sample configuration JCL.
- Create FEK.#CUST.CNTL and populate it with sample server startup scripts.
- Create /etc/zexpl/* and populate it with sample configuration files.
- Create /var/zexpl/* as work directories for various z/OS Explorer functions, and populate it with sample files.

Note:

- The configuration steps in this publication use the member and file locations created by the FEKSETUP job, unless noted otherwise. The original samples, which should not be updated, are in FEK.SFEKSAMP and /usr/lpp/IBM/zexpl/samples/.
- For more details on which sample members are copied to which data set, and for more details on which directories are created, their permission bitmask, and where the various sample files are copied to, see the comments in FEK.SFEKSAMP(FEKSETUP).
- To aid in migrating an existing setup, the comments in FEK.SFEKSAMP(FEKSETUP) also document the changes between different versions of z/OS Explorer.
- If you want to keep all of the z/OS Explorer z/OS UNIX files in the same file system (HFS or zFS), but also want the configuration files placed in /etc/zexpl, you can use symbolic links to solve this problem. The following sample z/OS UNIX commands create a new directory in the existing file system (/usr/lpp/IBM/zexpl/cust) and define a symbolic link (/etc/zexpl) to it:

```
mkdir /usr/lpp/IBM/zexpl/cust
ln -s /usr/lpp/IBM/zexpl/cust /etc/zexpl
```

PARMLIB changes

The following PARMLIB changes are documented in this section:

For more information about the PARMLIB definitions listed in the next sections, see *MVS Initialization and Tuning Reference* (SA22-7592). For more information about the sample console commands, see *MVS System Commands* (SA22-7627).

Set the z/OS UNIX limits in BPXPRMxx

Remote Systems Explorer (RSE), which provides core services such as connecting the client to the host system, is a z/OS UNIX based process. Therefore, it is important to set correct values for the z/OS UNIX system limits in BPXPRMxx, based on the number of concurrently active z/OS Explorer users and their average workload. Define OMVS=xx in the IEASYSxx parmlib member to specify which BPXPRMxx parmlib member should be used during IPL.

See "Tuning considerations" in the *Host Configuration Reference Guide* (SC27-8438) for more information about different BPXPRMxx defined limits and their impact on z/OS Explorer.

MAXASSIZE specifies the maximum address space (process) region size. Set MAXASSIZE in SYS1.PARMLIB(BPXPRMxx) to 2G. This is the maximum value allowed. This is a system-wide limit, and thus active for all z/OS UNIX address spaces. If this is not what you want, you can set the limit only for z/OS Explorer in your security software, as described in "Define the z/OS Explorer started tasks" on page 61.

MAXTHREADS specifies the maximum number of active threads for a single process. Set MAXTHREADS in SYS1.PARMLIB(BPXPRMxx) to 1500 or higher. This is a system-wide limit, and thus active for all z/OS UNIX address spaces. If this is not what you want, you can set the limit only for z/OS Explorer in your security software, as described in "Define the z/OS Explorer started tasks" on page 61.

MAXTHREADTASKS specifies the maximum number of active MVS tasks for a single process. Set MAXTHREADTASKS in SYS1.PARMLIB(BPXPRMxx) to 1500 or higher. This is a system-wide limit, and thus active for all z/OS UNIX address spaces. If this is not what you want, you can set the limit only for z/OS Explorer in your security software, as described in "Define the z/OS Explorer started tasks" on page 61.

MAXPROCUSER specifies the maximum number of processes that a single z/OS UNIX user ID can have concurrently active. Set MAXPROCUSER in SYS1.PARMLIB(BPXPRMxx) to 50 or higher. This setting is intended to be a system-wide limit, because it should be active for each client that uses z/OS Explorer.

These values can be checked and set dynamically (until the next IPL) with the following console commands:

- DISPLAY OMVS,O
- SETOMVS MAXASSIZE=2G
- SETOMVS MAXTHREADS=1500
- SETOMVS MAXTHREADTASKS=1500
- SETOMVS MAXPROCUSER=50

Note:

- For more information about other locations where address space sizes can be set or limited, see "Address space size" in the *Host Configuration Reference Guide* (SC27-8438).
- The MAXPROCUSER value suggested here is based upon users having a unique z/OS UNIX user ID (UID). Increase this value if your users share the same UID.
- Ensure that other BPXPRMxx values, such as those for MAXPROCSYS and MAXUIDS, are sufficient to handle the expected amount of concurrently active z/OS Explorer users. See "Tuning considerations" in the *Host Configuration Reference Guide* (SC27-8438) for more details.
- During the SMP/E install of z/OS Explorer, you were advised to place the code in a separate file system (zFS of HFS) and update BPXPRMxx to mount this file system during system IPL. Included is a repeat of the sample mount command in case this update still must be done:

```
MOUNT FILESYSTEM('#dsn')
   MOUNTPOINT('-PathPrefix-usr/lpp/ibm/zexpl')
   MODE(RDWR)                 /* can be MODE(READ) */
   TYPE(ZFS) PARM('AGGRGROW') /* zFS, with extents */
/* TYPE(HFS) */               /* HFS, auto. extent */
```

Add the started tasks to COMMNDxx

Add start commands for the z/OS Explorer RSED and JMON servers to SYS1.PARMLIB(COMMANDxx) to start them automatically at next system IPL. Define CMD=xx in the IEASYSxx parmlib member to specify which COMMNDxx parmlib member should be used during IPL.

After the servers are defined and configured, they can be started dynamically (until the next IPL) with the following console commands:

- S RSED
- S JMON

Note: There is no specific startup order for the servers. The only requirement is that the servers are up and running before the first user tries to connect.

LPA definitions in LPALSTxx

z/OS Explorer requires that the modules in the FEK.SFEKLPA load library are in the Link Pack Area (LPA) for RSE daemon to work with data sets.

LPA data sets are defined in SYS1.PARMLIB(LPALSTxx). Define LPA=xx in the IEASYSxx parmlib member to specify which LPALSTxx parmlib member should be used during IPL.

LPA definitions can be set dynamically (until the next IPL) with the following console command:

- SETPROG LPA,ADD,DSN=FEK.SFEKLPA,MASK=*

Note:

- Data sets listed in LPALSTxx must be cataloged in the master catalog or a user catalog identified in the LPALSTxx member.
- Adding a new data set to LPALSTxx requires an IPL with CLPA (create LPA) to be activated.
- All libraries that are loaded into LPA are automatically considered to be APF-authorized and program controlled. Ensure you have proper security controls in place for these libraries.
- If you choose to not place a library designed for LPA placement in LPA and you use LINKLIST or STEPLIB instead, ensure that you define the APF authorization and program control status.

APF authorizations in PROGxx

For JES Job Monitor to access JES spool files, the modules in the FEK.SFEKAUTH load library and the CEE.SCEERUN* Language Environment® (LE) runtime libraries must be APF-authorized.

For ISPF to create the ISPF Gateway, the ISP* modules in SYS1.LINKLIB must be APF-authorized. The ISPF Gateway is used by z/OS Explorer's TSO Commands service.

APF authorizations are defined in SYS1.PARMLIB(PROGxx) by default. Define PROG=xx in the IEASYSxx parmlib member to specify which PROGxx parmlib member should be used during IPL.

APF authorizations can be set dynamically (until the next IPL) with the following console commands, where volser is the volume on which the data set resides if it is not SMS-managed:

- SETPROG APF,ADD,DSN=FEK.SFEKAUTH,SMS
- SETPROG APF,ADD,DSN=FEK.SFEKLPA,SMS
- SETPROG APF,ADD,DSN=CEE.SCEERUN,VOL=volser
- SETPROG APF,ADD,DSN=CEE.SCEERUN2,VOL=volser
- SETPROG APF,ADD,DSN=REXX.V1R4M0.SEAGLPA,VOL=volser
- SETPROG APF,ADD,DSN=SYS1.LINKLIB,VOL=volser

Note:

- When you use the Alternate Library for REXX product package, the default REXX runtime library name is REXX.*.SEAGALT, instead of REXX.*.SEAGLPA as used in the preceding sample.
- LPA libraries, such as REXX.*.SEAGLPA, are automatically APF-authorized when located in LPA, and thus do not require explicit definitions.

Requisite LINKLIST and LPA definitions

Remote Systems Explorer (RSE) is a z/OS UNIX process that requires access to MVS load libraries. The JES Job Monitor server also needs access to the system, Language Environment (LE) and C libraries. The following prerequisite libraries must be made available, either through STEPLIB or LINKLIST/LPALIB:

- System load library
  - SYS1.LINKLIB
- Language Environment runtime
  - CEE.SCEERUN
  - CEE.SCEERUN2
- C++'s DLL class library
  - CBC.SCLBDLL
- ISPF Gateway
  - ISP.SISPLOAD
  - ISP.SISPLPA
- REXX runtime library
  - REXX.*.SEAGLPA

The following additional libraries must be made available, either through STEPLIB or LINKLIST/LPALIB, to support the use of optional services:

- System load library (for encrypted communication)
  - SYS1.SIEALNKE

Note:

- When you use the Alternate Library for REXX product package, the default REXX runtime library name is REXX.*.SEAGALT, instead of REXX.*.SEAGLPA as used in the preceding sample.

- All libraries that are loaded into LPA are automatically considered to be APF-authorized and program controlled. Ensure you have proper security controls in place for these libraries.
- Libraries that are designed for LPA placement, such as `REXX.*.SEAGLPA`, might require additional program control or APF authorizations if they are accessed through LINKLIST or STEPLIB.

LINKLIST data sets are defined in `SYS1.PARMLIB(PROGxx)` by default. LPA data sets are defined in `SYS1.PARMLIB(LPALSTxx)`.

If you opt to use STEPLIB, you must define the libraries not available through LINKLIST/LPALIB in the STEPLIB directive of `rse.env`, the RSE configuration file. Be aware, however, of these things:

- Using STEPLIB in z/OS UNIX has a negative performance impact.
- If one STEPLIB library is APF-authorized, then all the other STEPLIB libraries must be authorized. Libraries lose their APF authorization when they are mixed with non-authorized libraries in STEPLIB.
- Libraries added to the STEPLIB DD in a JCL are not propagated to the z/OS UNIX processes started by the JCL.

PROCLIB changes

The following PROCLIB changes are documented in this section:

- "JMON, JES Job Monitor started task"
- "RSED, RSE daemon started task" on page 15

Additional information is available in the following sub-sections:

- "JCL limitations for the PARM variable" on page 16
- "TMPDIR processing" on page 16
-

The started task and remote build procedures listed in the following sections must reside in a system procedure library defined to your JES subsystem. In the instructions in the following sections, the IBM default procedure library, `SYS1.PROCLIB`, is used.

JMON, JES Job Monitor started task

Customize the `FEK.#CUST.PROCLIB(JMON)` sample started task member, as described within the member, and copy it to `SYS1.PROCLIB`. As shown in the following code sample, provide this information:

- The high-level qualifier of the (authorized) load library, default `FEK`
- The JES Job Monitor configuration file, default `FEK.#CUST.PARMLIB(FEJJCNFG)`

```
//*
//* JES JOB MONITOR
//*
//JMON     PROC PRM=,             * PRM='-TV' TO START TRACING
//            LEPRM='RPTOPTS(ON)',
//            HLQ=FEK,
//            CFG=FEK.#CUST.PARMLIB(FEJJCNFG)
//*
//JMON     EXEC PGM=FEJJMON,REGION=0M,TIME=NOLIMIT,
//            PARM=('&LEPRM,ENVAR("_CEE_ENVFILE_S=DD:ENVIRON")/&PRM')
//STEPLIB  DD DISP=SHR,DSN=&HLQ..SFEKAUTH
//ENVIRON  DD DISP=SHR,DSN=&CFG
//SYSPRINT DD SYSOUT=*
//SYSOUT   DD SYSOUT=*
//         PEND
//*
```

Figure 1. JMON: JES Job Monitor started task

Note:

- For more information about the startup parameters, see Chapter 7, “Operator commands,” on page 73.
- The sample JCL is initially named `FEK.SFEKSAMP(FEJJJCL)` and is renamed to `FEK.#CUST.PROCLIB(JMON)` in “Customization setup” on page 9.
- Tracing can also be controlled by console commands, as described in Chapter 7, “Operator commands,” on page 73.
- For the recommended Workload Manager (WLM) goals for this task, see "WLM considerations" in the *Host Configuration Reference Guide* (SC27-8438).

RSED, RSE daemon started task

Customize the `FEK.#CUST.PROCLIB(RSED)` sample started task member, as described within the member, and copy it to `SYS1.PROCLIB`. As shown in the following code sample, provide this information:

- The home directory where z/OS Explorer is installed, default `/usr/lpp/IBM/zexpl`.
- The location of the configuration files, default `/etc/zexpl`

```
//*
//* RSE DAEMON
//*
//RSED     PROC IVP=,                  * 'IVP' to do an IVP test
//            PORT=,
//            CNFG='/etc/zexpl',
//            HOME='/usr/lpp/IBM/zexpl'
//*
//RSED     EXEC PGM=BPXBATSL,REGION=0M,TIME=NOLIMIT,
// PARM='PGM &HOME./bin/rsed.sh &IVP -C&CNFG -P&PORT'
//STDOUT   DD SYSOUT=*
//STDERR   DD SYSOUT=*
//         PEND
//*
```

Figure 2. RSED: RSE daemon started task

Note:

- For more information about the startup parameters, see Chapter 7, “Operator commands,” on page 73.
- The sample JCL is initially named `FEK.SFEKSAMP(FEKRSED)` and is renamed to `FEK.#CUST.PROCLIB(RSED)` in “Customization setup” on page 9.

- Limit the length of the job name to 7 characters or fewer. If an 8-character name is used, the **modify** and **stop** operator commands fail with message "IEE342I MODIFY REJECTED-TASK BUSY". This behavior is caused by the z/OS UNIX design for child processes.
- For the recommended Workload Manager goals for this task and the child processes it creates, see "WLM considerations" in the *Host Configuration Reference Guide* (SC27-8438). The child processes have the same name as the parent task, RSED, appended with a random 1-digit number, for example RSED8.

JCL limitations for the PARM variable

The maximum length for the PARM variable is 100 characters, which might cause problems if you use custom directory names. To bypass this problem, use one of these options:

- Use default values.

  The rsed.sh startup script can be started without arguments, in which case the default argument values are used.
- Use symbolic links.

  Symbolic links can be used as shorthand for a long directory name. The following sample z/OS UNIX command defines a symbolic link (/usr/lpp/IBM/zexpl) to another directory (/long/directory/name/usr/lpp/IBM/zexpl).

  ```
  ln -s /long/directory/name/usr/lpp/IBM/zexpl /usr/lpp/IBM/zexpl
  ```

TMPDIR processing

z/OS UNIX needs write access to /tmp, or another directory that is referenced by the TMPDIR variable, to be able to process certain commands during started task startup. z/OS Explorer uses the following logic to set TMPDIR during started task startup.

During started task startup, z/OS Explorer checks whether TMPDIR is already set (DD STDENV). If so, the started task uses that value. If TMPDIR is not set, the started task will test whether it can use /tmp. If not, the started task will test whether it can use the home directory that is assigned to the started task user ID. If this directory cannot be used either, startup fails.

If you cannot use the home directory, which is the default backup for /tmp, then you have to predefine TMPDIR using DD STDENV, as in the following sample:

```
//*
//* RSE DAEMON
//*
//RSED     PROC IVP=,                   * 'IVP' to do an IVP test
//            PORT=,
//            CNFG='/etc/zexpl',
//            HOME='/usr/lpp/IBM/zexpl'
//*
//RSED     EXEC PGM=BPXBATSL,REGION=0M,TIME=NOLIMIT,
// PARM='PGM &HOME./bin/rsed.sh &IVP -C&CNFG -P&PORT'
//STDOUT   DD SYSOUT=*
//STDERR   DD SYSOUT=*
//STDENV   DD PATHOPTS=(ORDONLY),PATH='&CNFG./rsed.stdenv'
//         PEND
//*
```

Figure 3. RSED: alternate TMPDIR processing

Then create the file (/etc/zexpl/rsed.stdenv in this example) that will hold the TMPDIR definition. You can edit the file with the TSO **OEDIT** command. The content of this file looks like the following sample:

```
TMPDIR=/tmp
```

Figure 4. rsed.stdenv: alternate TMPDIR processing

Security definitions

To create the security definitions for z/OS Explorer, customize and submit the sample FEKRACF member. The user submitting this job must have security administrator privileges, such as being RACF SPECIAL.

FEKRACF is located in FEK.#CUST.JCL, unless you specified a different location when you customized and submitted the FEK.SFEKSAMP(FEKSETUP) job. For more details, see "Customization setup" on page 9.

Note: [1]

- For those sites that use CA ACF2™ for z/OS, see the product page on the CA support site (https://support.ca.com) and check for the related z/OS Explorer Knowledge Document, TEC492389. This Knowledge Document has details on the security commands that are necessary to properly configure z/OS Explorer.
- For those sites that use CA Top Secret® for z/OS, see the product page on the CA support site (https://support.ca.com) and check for the related z/OS Explorer Knowledge Document, TEC492091. This Knowledge Document has details on the security commands necessary to properly configure z/OS Explorer.

The following list of security-related definitions for z/OS Explorer are discussed in detail in Chapter 5, "Security definitions," on page 59.

- Activate security settings and classes
- Define an OMVS segment for z/OS Explorer users
- Define the z/OS Explorer started tasks
- Define RSE as a secure z/OS UNIX server
- Define MVS program controlled libraries for RSE
- Define PassTicket support for RSE
- Define application security for RSE
- Define z/OS UNIX file access permission for RSE
- Define JES command security
- Define data set profiles

Attention: The client connection request will fail if PassTickets are not set up correctly.

FEJJCNFG, the JES Job Monitor configuration file

JES Job Monitor (JMON) provides all JES-related services. The behavior of JES Job Monitor can be controlled with the definitions in FEJJCNFG.

1. z/OS Explorer security definitions are based on IDz's.

FEJJCNFG is located in FEK.#CUST.PARMLIB, unless you specified a different location when you customized and submitted the FEK.SFEKSAMP(FEKSETUP) job. For more details, see "Customization setup" on page 9.

Customize the sample JES Job Monitor configuration member FEJJCNFG, as shown in the following sample. Comment lines start with a number sign (#) when using a US code page. Data lines can have only a directive and its assigned value. Comments are not allowed on the same line.

Note: For your changes to take effect, the JMON started task must be restarted.

```
SERV_PORT=6715
TZ=EST5EDT
#APPLID=FEKAPPL
#AUTHMETHOD=SAF
#CODEPAGE=UTF-8
#CONCHAR=$
#CONSOLE_NAME=JMON
#DISPLAY_SYSIN=OFF
#GEN_CONSOLE_NAME=OFF
#HOST_CODEPAGE=IBM-1047
#LIMIT_COMMANDS=NOLIMIT
#LIMIT_CONSOLE=LIMITED
#LIMIT_VIEW=USERID
#LISTEN_QUEUE_LENGTH=5
#LOOPBACK_ONLY=ON
#MAX_DATASETS=32
#MAX_THREADS=200
#TIMEOUT=3600
#TIMEOUT_INTERVAL=1200
#TRACE_STORAGE=OFF
#SEARCHALL=OFF
#SUBMIT_TIMEOUT=30
#SUBMITMETHOD=TSO
#TSO_TEMPLATE=FEK.#CUST.CNTL(FEJTSO)
```

Figure 5. FEJJCNFG, JES Job Monitor configuration file

SERV_PORT

The port number for JES Job Monitor. The default port is 6715. The port can be changed if needed.

Note:

- This value must match the port number set for JES Job Monitor in the rse.env configuration file. If these values differ, RSE cannot connect the client to JES Job Monitor. To learn how to define the variable for RSE, see "rse.env, the RSE configuration file" on page 22.
- Before selecting a port, verify that the port is available on your system by using the **NETSTAT** and **NETSTAT PORTL** TSO commands.

TZ Time zone selector. The default is EST5EDT. The default time zone is UTC -5 hours (Eastern Standard Time (EST) Eastern Daylight Savings Time (EDT)). Change this value to represent your time zone. Additional information can be found in the *UNIX System Services Command Reference* (SA22-7802).

The following definitions are optional. If omitted, default values are used as specified below:

APPLID

Specifies the application identifier used for identifying JES Job Monitor to your security software. The default is FEKAPPL. Uncomment and change to the required application ID.

Note: This value must match the application ID set for RSE in the rse.env configuration file. If these values differ, RSE cannot connect the client to JES Job Monitor. To learn how to define the variable for RSE, see "rse.env, the RSE configuration file" on page 22.

AUTHMETHOD

The default is SAF, which means that the System Authorization Facility (SAF) security interface is used. Do not change unless directed to do so by the IBM support center.

CODEPAGE

The workstation code page. The default is UTF-8. The workstation code page is set to UTF-8 and generally should not be changed. If you have difficulty with multilingual characters, such as the currency symbol, you might need to uncomment the directive and change UTF-8 to match the workstation's code page.

CONCHAR

Specifies the JES console command character. CONCHAR defaults to CONCHAR=$ for JES2, or CONCHAR=* for JES3. Uncomment and change to the requested command character.

CONSOLE_NAME

Specifies the name of the EMCS console used for issuing commands against jobs (Hold, Release, Cancel, and Purge). The default is JMON. Uncomment and change to the required console name, using the following guidelines.

- CONSOLE_NAME must be either a console name consisting of 2 to 8 alphanumeric characters, or '&SYSUID' (without quotes).
- If a console name is specified, a single console by that name is used for all users. If the console by that name is already in use, the command issued by the client will fail.
- If &SYSUID is specified, the client user ID is used as the console name. Thus, a different console is used for each user. If the console by that name is already in use (for example, the user is using the SDSF ULOG), the command issued by the client might fail, depending on the GEN_CONSOLE_NAME setting.

No matter which console name is used, the user ID of the client that is requesting the command is used as the LU of the console, leaving a trace in syslog messages IEA630I and IEA631.

```
IEA630I OPERATOR console NOW ACTIVE,   SYSTEM=sysid, LU=id
IEA631I OPERATOR console NOW INACTIVE, SYSTEM=sysid, LU=id
```

DISPLAY_SYSIN

Enables or disables the display of SYSIN data. The default is OFF. To display SYSIN data, uncomment and change to ON.

GEN_CONSOLE_NAME

Enables or disables automatic generating of alternative console names. The default is OFF. To enable alternative console names, uncomment and change to ON.

This directive is used only when CONSOLE_NAME equals &SYSUID and the user ID is not available as console name.

If GEN_CONSOLE_NAME=ON, an alternative console name is generated by appending a single numeric digit to the user ID. The digits 0 through 9 are attempted. If no available console is found, the command issued by the client fails.

If GEN_CONSOLE_NAME=OFF, the command issued by the client fails.

Note: The only valid settings are ON and OFF.

HOST_CODEPAGE
The host system code page. The default is IBM-1047. Uncomment and change to match your host system code page.

Note that this code page is not used for data interpretation, only for server operations and client connection setup. The z/OS Explorer client provides the code page to be used for data interpretation (which is retrieved from the properties of the "MVS Files" subsystem).

LIMIT_COMMANDS
Defines against which jobs the user can issue selected JES commands (Show JCL, Hold, Release, Cancel, and Purge). The default (LIMIT_COMMANDS=USERID) limits the commands to the jobs owned by the user. To allow the user to issue commands against all spool files, if permitted by your security product, uncomment this directive and specify LIMITED or NOLIMIT.

Table 7. LIMIT_COMMANDS command permission matrix

	Job owner	
LIMIT_COMMANDS	**User**	**Other**
USERID (default)	Allowed	Not allowed
LIMITED	Allowed	Allowed only if explicitly permitted by security profiles
NOLIMIT	Allowed	Allowed if permitted by security profiles or when the JESSPOOL class is not active

Note: The only valid settings are USERID, LIMITED, and NOLIMIT.

LIMIT_CONSOLE
Defines how much authority is granted to the console that is used to execute supported JES commands (Hold, Release, Cancel, and Purge). The default (LIMIT_CONSOLE=LIMITED) limits the authority to commands protected by a security profile in the OPERCMDS class. To allow execution of supported JES commands that are not protected by a security profile, uncomment this directive and specify NOLIMIT.

When a security profile exists for a command, the user must have sufficient permission to execute the command, regardless of the LIMIT_CONSOLE setting. The only valid settings are LIMITED and NOLIMIT.

LIMIT_VIEW
Defines what output the user can view. The default (LIMIT_VIEW=NOLIMIT)

allows the user to view all JES output, if permitted by your security product. To limit the view to output owned by the user, uncomment this directive and specify USERID.

Note: The only valid settings are USERID and NOLIMIT.

LISTEN_QUEUE_LENGTH
The TCP/IP listen queue length. The default is 5. Do not change unless directed to do so by the IBM support center.

LOOPBACK_ONLY
Defines whether JES Job Monitor binds to the loopback address only, or to every available TCP/IP stack. Binding to loopback is more secure, because only tasks local to this z/OS system will be able to contact JES Job Monitor. The default is ON. Uncomment this directive and specify OFF if you want JES Job Monitor to bind to all TCP/IP stacks.

MAX_DATASETS
The maximum number of spooled output data sets that JES Job Monitor will return to the client (for example, SYSOUT, SYSPRINT, SYS00001, and so on). The default is 32. The maximum value is 2147483647.

MAX_THREADS
Maximum number of users that can be using one JES Job Monitor at a time. The default is 200. The maximum value is 7200. Increasing this number might require you to increase the size of the JES Job Monitor address space.

TIMEOUT
The length of time, in seconds, before a thread is killed due to lack of interaction with the client. The default is 3600 (1 hour). The maximum value is 2147483647. TIMEOUT=0 disables the function.

TIMEOUT_INTERVAL
The number of seconds between timeout checks. The default is 1200. The maximum value is 2147483647.

TRACE_STORAGE
Enable storage tracing. The default is OFF. The only valid values are ON and OFF. Use only when directed by the IBM support center. To write a storage report to DD SYSOUT after each command, uncomment this directive and specify ON.

SEARCHALL
Collect APPC and z/OS UNIX output that matches the JES Job Monitor filter. The default is OFF. The only valid values are ON and OFF. To collect the additional spool files, uncomment this directive and specify ON.

SUBMIT_TIMEOUT
The number of seconds that z/OS Explorer will wait for the completion of the TSO_TEMPLATE job. The default is 30. The maximum value is 2147483647. Note: SUBMIT_TIMEOUT has no effect unless SUBMITMETHOD=TSO is also specified.

SUBMITMETHOD=TSO
Submit jobs through TSO. The default (SUBMITMETHOD=JES) submits jobs directly into JES. To submit the job through TSO **SUBMIT** command, uncomment this directive and specify TSO. This method allows TSO exits to be called; however, this method has a performance drawback.

Note:

- The only valid settings are TSO and JES.
- If SUBMITMETHOD=TSO is specified, TSO_TEMPLATE must also be defined.

TSO_TEMPLATE
Wrapper JCL for submitting the job through TSO. The default value is FEK.#CUST.CNTL(FEJTSO). This statement refers to the fully qualified member name of the JCL to be used as a wrapper for the TSO **SUBMIT** command. For more information, see the SUBMITMETHOD statement.

Note:

- A sample wrapper job is provided in FEK.#CUST.CNTL(FEJTSO). See this member for more information about the customization needed.
- TSO_TEMPLATE has no effect unless SUBMITMETHOD=TSO is also specified.

rse.env, the RSE configuration file

The RSE server processes (RSE daemon, RSE thread pool, and RSE server) use the definitions in rse.env.

Remote Systems Explorer (RSE) provides core services such as connecting the client to the host system and starting other servers for specific services.

rse.env is located in /etc/zexpl/, unless you specified a different location when you customized and submitted the FEK.SFEKSAMP(FEKSETUP) job. For more details, see "Customization setup" on page 9. You can edit the file with the TSO **OEDIT** command.

See the following sample rse.env file, which can be customized to match your system environment. Default values are provided for all variables that are not explicitly specified. The syntax of the file follows standard z/OS UNIX shell syntax rules. For example, comments start with a number sign (#) when using a US code page, and spaces around the equal sign (=) are not supported.

Note: For your changes to take effect, the RSED started task must be restarted.

```
#_RSE_RSED_PORT=4035   # override by port specified as startup argument
#_RSE_JMON_PORT=6715
#RSE_LOGS=/var/zexpl/logs
#RSE_HOME=/usr/lpp/IBM/zexpl
#JAVA_HOME=/usr/lpp/java/J6.0
#CGI_ISPHOME=/usr/lpp/ispf
#RSE_HLQ=FEK

## load balancing
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Xms128m -Xmx512m"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dmaximum.clients=10"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dmaximum.threads=250"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dminimum.threadpool.process=1"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dmaximum.threadpool.process=100"
## logs
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Ddaemon.log=$RSE_LOGS"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Duser.log=$RSE_LOGS"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -DDSTORE_LOG_DIRECTORY="
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dlog.file.mode=RW.N.N"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dlog.retention.period=5"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dkeep.all.logs=false"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dkeep.last.log=true"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dlog.secure.mode=false"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Denable.standard.log=true"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -DDSTORE_TRACING_ON=true"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -DDSTORE_MEMLOGGING_ON=true"
## audit
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Denable.audit.log=true"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Daudit.cycle=30"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Daudit.retention.period=0"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Daudit.log.mode=RW.R.N"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Daudit.action=<user exit>"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Daudit.action.id=<userid>"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Daudit.display.attributes=true"
## security
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -DAPPLID=FEKAPPL"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Denable.port.of.entry=true"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Denable.certificate.mapping=false"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -DDENY_PASSWORD_SAVE=true"
## connect
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dipv6=true"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Denable.dDVIPA=true"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Ddeny.nonzero.port=true"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dsingle.logon=false"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dlogon.action=<user exit>"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dlogon.action.id=<userid>
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dreject.logon.threshold=1000000"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -DDSTORE_TCP_NO_DELAY=true"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -DDSTORE_IDLE_SHUTDOWN_TIMEOUT=3600000"
## system
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dbackupfiles=false"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -DDISABLE_MIGRATE_HRECALL_HDELETE=true"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -DHIDE_ZOS_UNIX=true"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Denable.automount=true"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Ddisplay.users=true"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dprocess.cleanup.interval=0"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dkeep.stats.copy.local=true"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -DDSTORE_USE_THREADED_MINERS=false"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dmaximum.ispf.sessions=0"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Duse.fastpath.getattributes=true"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dallow.retry.on.failed.saf.check=false"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dmaxthreadtasks.threshold=60"
## search
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dsearch.server.limit.hits=0"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dsearch.server.limit.scanned_objects=0"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dsearch.server.limit.lines=0"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dsearch.server.limit.timeout=0"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dsearch.server.limit.errcount=true"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dsearch.server.limit.MaxFilterResults=0"
#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -DDISABLE_TEXT_SEARCH=true"

## ispf
#CGI_ISPCONF=$RSE_CFG
#CGI_ISPWORK=$RSE_LOGS/..
#_RSE_ISPF_OPTS=""
#_RSE_ISPF_OPTS="$_RSE_ISPF_OPTS&ISPPROF=&SYSUID..ISPPROF"
#CGI_ISPPREF="&SYSPREF..ISPF.VCMISPF"
#CGI_CEATSO=TRUE
#CGI_CEATSO_KEEPALIVE=FALSE

## system
#TZ=EST5EDT
#LANG=C
#PATH=$PATH:/bin
#TMPDIR=/tmp
#_CEE_DMPTARG=/tmp
#_RSE_UMASK=RWX.N.N


## connect
#_BPXK_SETIBMOPT_TRANSPORT=TCPIP
#_RSE_PORTRANGE=8108-8118

## security
#_RSE_FEK_SAF_CLASS=FACILITY
#GSK_PROTOCOL_SSLV3=OFF
#GSK_V3_CIPHERS=GSK_V3_CIPHERS_CHAR2
#GSK_V3_CIPHER_SPECS=3538392F3233
#GSK_V3_CIPHER_SPECS_EXPANDED=003500380039002F00320033
#GSK_FIPS_STATE=OFF
#GSK_CRL_SECURITY_LEVEL=HIGH
#GSK_LDAP_SERVER=ldap_server_url
#GSK_LDAP_PORT=ldap_server_port
#GSK_LDAP_USER=ldap_userid
#GSK_LDAP_PASSWORD=ldap_server_password

## push-to-client
#_RSE_LDAP_SERVER=ldap_server_url
#_RSE_LDAP_PORT=389
#_RSE_LDAP_PTC_GROUP_SUFFIX="O=PTC,C=zOSexplorer"

#STEPLIB=$STEPLIB:CEE.SCEERUN:CEE.SCEERUN2:CBC.SCLBDLL
#STEPLIB=$STEPLIB:ISP.SISPLOAD:ISP.SISPLPA:SYS1.LINKLIB
```

Figure 6. rse.env: RSE configuration file

The following definitions are optional. If omitted, default values are used.

_RSE_RSED_PORT

RSE daemon port number. The default is 4035. Uncomment and change to match your needs.

Note:

- Before selecting a port, verify that the port is available on your system by using the TSO commands NETSTAT and NETSTAT PORTL.
- This port is used for client-host communication.
- The RSED started task can override the port number specified here.

_RSE_JMON_PORT
JES Job Monitor port number. The default is `6715`. Uncomment and change to match your needs.

Note:

- This value must match the port number set for JES Job Monitor in the `FEJJCNFG` configuration file. If these values differ, RSE cannot connect the client to JES Job Monitor. To learn how to define the variable for JES Job Monitor, see "FEJJCNFG, the JES Job Monitor configuration file" on page 17.
- Before selecting a port, verify that the port is available on your system by using the TSO commands **`NETSTAT`** and **`NETSTAT PORTL`**.
- All communication on this port is confined to your z/OS host system.

RSE_LOGS
RSE log directory. The default is `/var/zexpl/logs`. Uncomment and change to match your needs.

Note: If you did not use the `SFEKSAMP(FEKSETUP)` sample job to build the customizable environment, verify that the last directory in the path specified in RSE_LOGS has read, write, and execute permission for owner, group, and other (permission bitmask 777).

RSE_HOME
RSE home directory. The default is the directory specified in the HOME variable of the RSED started task (default `/usr/lpp/IBM/zexpl`). Uncomment and change to match your z/OS Explorer installation.

Note: RSE daemon startup will fail if RSE_HOME is not equal to the HOME variable of the RSED started task.

JAVA_HOME
Java home directory. The default is `/usr/lpp/java/J6.0`. Uncomment and change to match your Java installation.

CGI_ISPHOME
Home directory for the ISPF code that provides the ISPF Gateway service. The default is `/usr/lpp/ispf`. Uncomment and change to match your ISPF installation.

RSE_HLQ
The high-level qualifier used to install z/OS Explorer. The default is `FEK`. Uncomment and change to match the location of your z/OS Explorer data sets.

_RSE_JAVAOPTS
Additional RSE-specific Java options. For more information about this definition, see "Defining extra Java startup parameters with _RSE_JAVAOPTS" on page 29.

CGI_ISPCONF
ISPF base configuration directory. The default is `$RSE_CFG`, which holds the z/OS Explorer configuration directory name. When using defaults,

CGI_ISPCONF is set to /etc/zexpl. Uncomment and change to match the location of ISPF.conf, the Legacy ISPF Gateway customization file.

CGI_ISPWORK
ISPF base work directory. The default is $RSE_LOGS/.., which holds the z/OS Explorer log directory name. When using defaults, CGI_ISPWORK is set to /var/zexpl. Uncomment and change to match the location of the WORKAREA directory used by the Legacy ISPF Gateway.

Note:

- The Legacy ISPF Gateway adds /WORKAREA to the path specified in CGI_ISPWORK. Do not add it yourself.
- If you did not use the SFEKSAMP(FEKSETUP) sample job to build the customizable environment, verify that the WORKAREA directory exists in the path specified in CGI_ISPWORK. The directory permission bits must allow read, write, and execute for owner, group, and other (permission bitmask 777).

_RSE_ISPF_OPTS
Additional Legacy ISPF Gateway-specific Java options. The default is "". For more information about this definition, see "Defining extra Java startup parameters with _RSE_ISPF_OPTS" on page 37.

CGI_ISPPREF
High-level qualifier for the temporary data set created by the Legacy ISPF Gateway. The default is "&SYSPREF..ISPF.VCMISPF". Uncomment and change to match your data set naming conventions.

The following variables can be used in the data set name:

- &SYSUID. to substitute the developer's user ID
- &SYSPREF. to substitute the developer's TSO prefix or, if the TSO prefix cannot be determined, the user ID
- &SYSNAME. to substitute the system name as specified in the IEASYMxx parmlib member

Note: This directive requires ISPF APAR OA38740.

CGI_CEATSO
Activate Interactive ISPF Gateway. The default is FALSE. Uncomment and specify TRUE to use the Interactive ISPF Gateway when possible. For more information, see "(Optional) Interactive ISPF Gateway" on page 49.

Note:

- As of z/OS 2.2, Legacy ISPF Gateway, previously named TSO/ISPF Client Gateway, is deprecated and is no longer being enhanced. The functionality is now provided by the Interactive ISPF Gateway.
- Interactive ISPF Gateway requires z/OS 2.2, and the Common Event Adapter (CEA) TSO/E address space manager service.

CGI_CEATSO_KEEPALIVE
Prevent an idle Interactive ISPF Gateway session from timing out after 15 minutes. The default is TRUE. Uncomment and specify FALSE to allow the session to time out when not used.

TZ Time zone selector. The default is EST5EDT. The default time zone is UTC -5 hours (Eastern Standard Time (EST) Eastern Daylight Savings Time (EDT)). Uncomment and change to match your time zone.

Additional information can be found in the *UNIX System Services Command Reference* (SA22-7802).

LANG
Specifies the name of the default locale. The default is `C`. `C` specifies the POSIX locale and (for example) `Ja_JP` specifies the Japanese locale. Uncomment and change to match your locale.

PATH Additional command path entries. The default is `/bin` plus z/OS Explorer specific directories. Uncomment and add your own directories as needed.

TMPDIR
Specifies the path used to store temporary files. The default is `/tmp`. Uncomment and change to use the requested path.

_CEE_DMPTARG
Language Environment (LE) z/OS UNIX dump location used by the Java Virtual Machine (JVM). The default is `/tmp`. Uncomment and change to match your needs.

_RSE_UMASK
Specifies the access permission mask for z/OS UNIX files and directories that are created by users. The default is `RWX.N.N`, which grants the owner read, write, and execute/search access. The owner's default group and everyone else have no access. To set the required access permissions, uncomment and customize this variable.

UNIX standards dictate that permissions can be set for three types of users: owner, group, and other. The fields in this variable match this order, and the fields are separated by a period (**.**). Each field can be empty (which equals **N**), or have **N**, or any combination of **R**, **W**, and **X** as values, where **N** = none, **R** = read, **W** = write, and **X** = execute/search.

_BPXK_SETIBMOPT_TRANSPORT
Specifies the name of the TCP/IP stack to be used. The default is `TCPIP`. Uncomment and change to the requested TCP/IP stack name, as defined in the `TCPIPJOBNAME` statement in the related TCPIP.DATA.

Note:

- Coding a SYSTCPD DD statement in the server JCL does not set the requested stack affinity.
- When this directive is not active, RSE binds to every available stack on the system (BIND INADDRANY).

_RSE_PORTRANGE
Specifies the port range that the RSE server can open for communication with a client. Any port can be used by default. For more information about this definition, see "Defining the PORTRANGE available for RSE server" on page 28.

GSK_PROTOCOL_SSLV3
Specifies whether the specified encryption protocol, SSLV3 in this sample, is enabled. A protocol that is supported by but not enabled in System SSL can be enabled here by specifying `GSK_PROTOCOL_<protocol>=ON`. You can disable a protocol by specifying `OFF` as value. For a list of supported protocols and the matching variable names, see *Cryptographic Services System SSL Programming (SC24-5901)*.

Note: Due to a vulnerability in the SSLv3 (Secure Socket Layer) protocol, support for this protocol is deprecated in z/OS Explorer.

GSK_V3_CIPHERS
Specifies the size of the ID used by System SSL to reference ciphers. Valid values are `GSK_V3_CIPHERS_CHAR2` (default) and `GSK_V3_CIPHERS_CHAR4`. Uncomment and specify `GSK_V3_CIPHERS_CHAR4` if you also want to use ciphers that only have a 4-character ID. For a list of supported ciphers and their ID, see *Cryptographic Services System SSL Programming (SC24-5901)*.

Note: Java 8.0 or higher is required for using 4-character cipher IDs.

GSK_V3_CIPHER_SPECS
Specifies the encryption cipher selection specifications in order of preference as a string consisting of one or more 2-character values. Uncomment and specify the desired string if you want to influence cipher selection when 2-character cipher IDs are used (default). Use `GSK_V3_CIPHERS` to set the desired cipher ID size. For a list of supported ciphers and their 2-character ID, see *Cryptographic Services System SSL Programming (SC24-5901).*

Note: z/OS Explorer disables ciphers that are known to be insecure.

GSK_V3_CIPHER_SPECS_EXPANDED
Specifies the encryption cipher selection specifications in order of preference as a string consisting of one or more 4-character values. Uncomment and specify the desired string if you want to influence cipher selection when 4-character cipher IDs are used. Use `GSK_V3_CIPHERS` to set the desired cipher ID size. For a list of supported ciphers and their 4-character ID, see *Cryptographic Services System SSL Programming (SC24-5901)*.

Note: z/OS Explorer disables ciphers that are known to be insecure.

GSK_FIPS_STATE
Specifies whether the FIPS 140-2 standard for encrypted communication is used. The default is **OFF**. Uncomment and specify **ON** to use encrypted communication that conforms to the FIPS 140-2 standard.

GSK_CRL_SECURITY_LEVEL
Specifies the level of security applications use when contacting LDAP servers to check CRLs for revoked certificates during certificate validation. The default is `MEDIUM`. To enforce the usage of the specified value, uncomment and change. The following values are valid:

- `LOW`: Certificate validation does not fail if the LDAP server cannot be contacted.
- `MEDIUM`: Certificate validation requires the LDAP server to be contactable, but does not require a CRL to be defined. This value is the default.
- `HIGH`: Certificate validation requires the LDAP server to be contactable and a CRL to be defined.

GSK_LDAP_SERVER
Specifies one or more blank-separated LDAP server host names used for certificate validation. To enforce the usage of the specified LDAP servers to obtain their CRL, uncomment and change.

The host name can either be a TCP/IP address or a URL. Each host name can contain an optional port number separated from the host name by a colon sign (:).

GSK_LDAP_PORT
Specifies the LDAP server port used for certificate validation. The default is `389`. To enforce the usage of the specified value, uncomment and change.

GSK_LDAP_USER
Specifies the distinguished name to use when connecting to the LDAP server for certificate validation. To enforce the usage of the specified value, uncomment and change.

GSK_LDAP_PASSWORD
Specifies the password to use when connecting to the LDAP server for certificate validation. To enforce the usage of the specified value, uncomment and change.

_RSE_LDAP_SERVER
Specifies the LDAP server host name used by the push-to-client function. The default is the current z/OS host name. To enforce the usage of the specified value, uncomment and change.

_RSE_LDAP_PORT
Specifies the LDAP server port used by the push-to-client function. The default is `389`. To enforce the usage of the specified value, uncomment and change.

_RSE_LDAP_PTC_GROUP_SUFFIX
Specifies the "O=<organization>, C=<country>" suffix needed to find the push-to-client groups within the LDAP server. The default is `"O=PTC,C=zOSexplorer"`. To enforce the usage of the specified value, uncomment and change.

STEPLIB
Access MVS data sets not in LINKLIST/LPALIB. The default is `"NONE"`.

You can bypass the need of having prerequisite libraries in LINKLIST/LPALIB by uncommenting and customizing one or more of the following STEPLIB directives. For more information about the usage of the libraries in the following list, see "PARMLIB changes" on page 10:

```
# RSE
STEPLIB=$STEPLIB:CEE.SCEERUN:CEE.SCEERUN2:CBC.SCLBDLL
# ISPF
STEPLIB=$STEPLIB:ISP.SISPLOAD:ISP.SISPLPA:SYS1.LINKLIB
```

Note:

- Using STEPLIB in z/OS UNIX has a negative performance impact.
- If one STEPLIB library is APF-authorized, then all the other STEPLIB libraries must be authorized. Libraries lose their APF authorization when they are mixed with non-authorized libraries in STEPLIB.
- Libraries that are designed for LPA placement might require additional program control and APF authorizations if they are accessed through LINKLIST or STEPLIB.
- Coding a STEPLIB DD statement in the server JCL does not set the requested STEPLIB concatenation.

Defining the PORTRANGE available for RSE server

This is a part of `rse.env` customization that specifies the ports on which the RSE server can communicate with the client. This range of ports has no connection with the RSE daemon port.

To help understand the port usage, a brief description of RSE's connection process follows:

1. The client connects to host system port 4035, RSE daemon.
2. The RSE daemon creates an RSE server thread.
3. The RSE server opens a host system port for the client to connect. The selection of this port can be configured by using the `_RSE_PORTRANGE` definition in `rse.env`.
4. The RSE daemon returns the port number to the client.
5. The client connects to the host system port.

Note:

- For more information, see "Understanding z/OS Explorer" in the *Host Configuration Reference Guide* (SC27-8438).

To specify the port range, for the client to communicate with z/OS, uncomment and customize the following line in `rse.env`:

```
#_RSE_PORTRANGE=8108-8118
```

Note: Before selecting a port range, verify that the range is available on your system by using the **NETSTAT** and **NETSTAT PORTL** commands.

The format of PORTRANGE is: `_RSE_PORTRANGE=min-max`. The value for `max` is non-inclusive; for example, the expression `_RSE_PORTRANGE=8108-8118` means port numbers from `8108` up to `8117` are usable.

The port number used by the RSE server is determined in the following order:

1. If a nonzero port number is specified in the subsystem properties on the client, the specified port number is used. If the port is not available, the connection fails. This setup is not recommended.

   Note: The host system can deny this type of connection request by specifying the `deny.nonzero.port=true` directive in `rse.env`. For more information about this directive, see “Defining extra Java startup parameters with _RSE_JAVAOPTS.”
2. If the port number in the subsystem properties is 0 and if `_RSE_PORTRANGE` is specified in `rse.env`, the port range specified by `_RSE_PORTRANGE` is used. If no port in the range is available, the connection fails.

   RSE server does not need the port exclusively for the duration of the client connection. It is only in the time span between the server bind and the client connect that no other RSE server can bind to the port. This means that most connections use the first port in the range, with the rest of the range being a buffer in case of multiple simultaneous logons.
3. If the port number in the subsystem properties is 0 and `_RSE_PORTRANGE` is not specified in `rse.env`, any available port is used.

Defining extra Java startup parameters with _RSE_JAVAOPTS

With the different `_RSE_*OPTS` directives, `rse.env` provides the facility to give extra parameters to Java when it starts the RSE processes. The sample options included in `rse.env` can be activated by uncommenting them.

_RSE_JAVAOPTS defines standard and RSE-specific Java options.

_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Xms128m -Xmx512m"
Set initial (`Xms`) and maximum (`Xmx`) heap size. The defaults are `128M` and `512M` respectively. Uncomment and change to enforce the required heap size values.

Note: To determine the optimal values for this directive, see "Key resource definitions" in the *Host Configuration Reference Guide* (SC27-8438).

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dmaximum.clients=10"
Maximum amount of clients serviced by one thread pool. The default is `10`. To limit the number of clients per thread pool, uncomment and customize. Other limits might prevent RSE from reaching this limit.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dmaximum.threads=250"
Maximum amount of active threads in one thread pool to allow new clients. The default is `250`. To limit the number of clients in each thread pool, based on the number of threads in use, uncomment and customize. Each client connection uses multiple threads and other limits might prevent RSE from reaching this limit.

Note: This value must be lower than the setting for `MAXTHREADS` and `MAXTHREADTASKS` in `SYS1.PARMLIB(BPXPRMxx)`.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dminimum.threadpool.process=1"
The minimum number of active thread pools. The default is 1. To start at least the listed number of thread pool processes, uncomment and customize. Thread pool processes are used for load balancing the RSE server threads. More new processes are started when they are needed. Starting the new processes upfront helps prevent connection delays but uses more resources during idle times.

Note: If the `single.logon` directive is active, at least 2 thread pools are started, even if `minimum.threadpool.process` is set to 1. The default setting for `single.logon` in `rse.env` is active.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dmaximum.threadpool.process=100"
The maximum number of active thread pools. The default is `100`. To limit the number of thread pool processes, uncomment and customize. Thread pool processes are used for load balancing the RSE server threads, so limiting them will limit the amount of active client connections.

_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Ddaemon.log=$RSE_LOGS"
The directory leading to the RSE daemon and server log files, and RSE audit data. The default is `$RSE_LOGS`, which holds the z/OS Explorer log directory name. When using defaults, RSE_LOGS is set to `/var/zexpl/logs`. Uncomment and change to enforce the required location.

Note:

- If this directive does not specify an absolute path (where the path does not start with a forward slash (/)), the actual log location is relative to the configuration directory, which, by default is `/etc/zexpl`.
- The complete path to the server logs is `daemonlog/server`, where `daemonlog` is the value of the `daemon.log` directive.

_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Duser.log=$RSE_LOGS"
Directory leading to the user-specific logs. The default is `$RSE_LOGS`, which holds the z/OS Explorer log directory name. When using defaults, RSE_LOGS is set to `/var/zexpl/logs`. Uncomment and change to enforce

the required location. If this directive value is a null string, the home directory of the client user ID is used. The home directory is defined in the OMVS security segment of the user ID.

Note:

- If this directive or its counterpart, the home directory, does not specify an absolute path (the path does not start with a forward slash (/)), the actual log location is relative to the configuration directory, which, by default is `/etc/zexpl`.
- The complete path to the user logs is `userlog/dstorelog/$LOGNAME/`, where `userlog` is the value of the `user.log` directive, `dstorelog` is the value of the `DSTORE_LOG_DIRECTORY` directive and `$LOGNAME` is the clients user ID in uppercase.
- Ensure that the permission bits for `userlog/dstorelog` are set so that each client can create `$LOGNAME`.

_RSE_JAVAOPTS="$_RSE_JAVAOPTS -DDSTORE_LOG_DIRECTORY="
This directory is appended to the path specified in the `user.log` directive. Together they create the path leading to the user-specific logs. The default is a null-string. Uncomment and change to enforce the usage of the specified directory.

Note:

- The complete path to the user logs is `userlog/dstorelog/$LOGNAME/`, where `userlog` is the value of the `user.log` directive, `dstorelog` is the value of the `DSTORE_LOG_DIRECTORY` directive, and `$LOGNAME` is the clients user ID in uppercase.
- The directory specified here is relative to the directory specified in `user.log` and may, therefore, not start with a forward slash (/).
- Ensure that the permission bits for `userlog/dstorelog` are set so that each client can create `$LOGNAME`.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dlog.file.mode=RW.N.N"
Access permission mask for log files and log directories. The default is `RW.N.N`, which allows the owner read and write access. The owner's default group and everyone else have no access. To set the required access permissions, uncomment and customize.

UNIX standards dictate that permissions can be set for three types of users: owner, group, and other. The fields in this variable match this order, and the fields are separated by a period (.). Each field can be empty (which equals `N`), or have `N`, `R`, `W`, or `RW` as values, where N = none, R = read and W = write.

_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dlog.retention.period=5"
Number of days daemon and user logs are kept. The default is `5`. Uncomment and customize this directive to delete the logs after a given number of days. Specify `0` to set no limit. The maximum value is `365`. Note that daemon log cleanup happens at the next action that requires daemon activity. User logs are cleaned up the next time the user connects.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dkeep.all.logs=false"
Use file names with an embedded time-stamp for daemon and user logs. The default is `true`, which implies that the logs are kept until removed by the `log.retention.period` setting. Uncomment and specify false to use fixed log file names, which are replaced each time the daemon is started or the user connects.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS –Dkeep.last.log=true"
Keep a copy of the host log files belonging to the previous session. The default is `false`. To rename the previous log files to `*.last` during server startup and client connect, uncomment and specify `true`. Note that the `.dstore*` user trace files are not removed automatically upon client reconnect, nor are they part of the `keep.last.log` processing. Removing these files is a manual action. The `keep.all.logs` directive must be set to `false` for `keep.last.log` to take effect.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dlog.secure.mode=false"
Validate log-directory ownership. The default is `true`, which makes RSE validate that a user (RSE daemon itself or a client user ID) is the owner of the directory in which the logs will be written. Uncomment and specify `false` to skip this check and write the log files without checking directory ownership. Console message `FEK301E` is issued when the test is not successful.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS –Denable.standard.log=true"
Write the stdout and stderr streams of the thread pools to a log file. The default is `false`. To save the stdout and stderr streams, uncomment and specify `true`. The resulting log files are located in the directory referenced by the `daemon.log` directive.

Note: The **`MODIFY RSESTANDARDLOG`** operator command can be used to dynamically stop or start the update of the stream log files.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -DDSTORE_TRACING_ON=true"
Start dstore tracing. Use only when directed by the IBM support center. The resulting `.dstoreTrace` log file is created in Unicode (ASCII), not EBCDIC.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -DDSTORE_MEMLOGGING_ON=true"
Start dstore memory tracing. Use only when directed by the IBM support center. The resulting `.dstoreMemLogging` log file is created in Unicode (ASCII), not EBCDIC.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Denable.audit.log=true"
Audit option. The default is `false`. To enforce audit logging of actions done by clients, uncomment and specify `true`. Audit logs are written to the RSE daemon log location. To know the location, see the `daemon.log` option of the `_RSE_JAVAOPTS` variable.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Daudit.cycle=30"
Number of days stored in 1 audit log file. The default is `30`. To control how much audit data is written to 1 audit log file, uncomment and customize. The maximum value is `365`.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Daudit.retention.period=0"
Number of days audit logs are kept. The default is `0`, which means no limit is specified. To delete audit logs after a given number of days, uncomment and customize. The maximum value is `365`.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Daudit.log.mode=RW.R.N"
Access permission mask for audit logs. The default is `RW.R.N`, which allows the owner read and write access. The owner's default group has read access and everyone else has no access. To set the required access permissions, uncomment and customize.

UNIX standards dictate that permissions can be set for three types of users: owner, group, and other. The fields in this variable mask match this order,

and the fields are separated by a period (.). Each field can be empty (which equals N), or have N, R, W, or RW as values, where N=none, R = read and W = write.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Daudit.action=<user exit>"
Name of a user exit which is called when an audit log file is closed. There is no default value, but a sample exit is provided in `/usr/lpp/IBM/zexpl/samples/process_audit.rex`. To enable post-processing of audit logs, uncomment and specify the full pathname of the user exit program.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Daudit.action.id=<userid>"
User ID to be used for running the exit specified in the `audit.action` variable. The default is the user ID assigned to RSE daemon. To use the specified ID for executing the audit post-processing exit, uncomment and specify a user ID.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Daudit.display.attributes=true"
Enables or disables the display of data set attributes on the audit log. The default is `true`. Uncomment and specify `false` to prevent data set attributes to be displayed.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -DAPPLID=FEKAPPL"
RSE server application ID. The default is `FEKAPPL`. To enforce the use of the required application ID, uncomment and customize.

Note:

- For the security implications when changing this value, see "Using PassTickets" in *Host Configuration Reference Guide* (SC27-8438).
- This value must match the application ID set for JES Job Monitor in the `FEJJCNFG` configuration file. If these values differ, RSE cannot connect the client to JES Job Monitor. To learn how to define the variable for JES Job Monitor, see “FEJJCNFG, the JES Job Monitor configuration file” on page 17.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Denable.port.of.entry=true"
Port Of Entry (POE) check option. The default is `false`. To enforce POE checking for client connections, uncomment and specify `true`. During POE checking, the IP address of the client is mapped into a network access security zone by your security software. The client user ID must have permission to use the profile that defines the security zone.

Note:

- POE checking must also be enabled in your security product.
- Enabling POE checking enables the product for other z/OS UNIX services also, such as INETD.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Denable.certificate.mapping=false"
Use your security software to authenticate a logon with a X.509 certificate. The default is `true`. To have RSE daemon do the authentication without relying on the X.509 support of your security software, uncomment and specify `false`.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -DDENY_PASSWORD_SAVE=true"
Password save option. The default is `false`. To prevent users from saving their host password on the client, uncomment and specify `true`. Previously saved passwords are removed.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dipv6=true"
TCP/IP version. The default is `false`, which means that an IPv4 interface is used. To use an IPv6 interface, uncomment and specify `true`.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS –Denable.dDVIPA=true"
Distributed Dynamic VIPA support. The default is `false`. To use TCP/IP's distributed Dynamic VIPA, which allows servers on multiple systems to present themselves as a single server, uncomment and specify `true`.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Ddeny.nonzero.port=true"
Disallow the client to choose the communication port number. The default is `false`. To refuse connections where the client specifies which host system port must be used by RSE server for the connection, uncomment and specify `true`. For more information, see "Defining the PORTRANGE available for RSE server" on page 28.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dsingle.logon=false"
Disallow a user ID to log on multiple times. The default is `true`. To allow a user ID to log on multiple times to a single RSE daemon, uncomment and specify `false`.

Note:

- A second logon attempt causes the first one to be canceled by the host system if this directive is not active or set to `true`. This cancellation action is accompanied by console message FEK210I.
- If the `single.logon` directive is active, at least 2 thread pools are started, even if `minimum.threadpool.process` is set to 1. The default setting for `minimum.threadpool.process` in `rse.env` is 1.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dlogon.action=<user_exit>"
Name of a user exit which is called when a user logs on. There is no default value, but a sample exit is provided in `/usr/lpp/IBM/zexpl/samples/process_logon.sh`. To enable post-processing of a logon, uncomment and specify the full pathname of the user exit program.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dlogon.action.id=<userid>"
User ID to be used for running the exit specified in the `logon.action` variable. The default is the user ID assigned to RSE daemon. To use the specified ID for executing the logon post-processing exit, uncomment and specify a user ID.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dreject.logon.threshold=1000000"
A thread pool opening a file larger than the specified size will not accept new logon requests until the file is loaded. The default file size is `1000000` bytes. To specify the file size at which a thread pool is to ignore logon requests when such a file is opened, uncomment and customize. Other thread pools can still accept new logon requests.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -DDSTORE_TCP_NO_DELAY=true"
Disable the TCP/IP DELAY ACK function. The default is `false`. To stop TCP/IP from doing DELAY ACK for z/OS Explorer client-host communication, uncomment and specify `true`.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -DDSTORE_IDLE_SHUTDOWN_TIMEOUT=3600000"
Disconnect idle clients. By default, idle clients are not disconnected. To disconnect clients who are idle for the listed number of milliseconds, uncomment and customize. 3600000 milliseconds equal 1 hour.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dbackupfiles=false"
Create a temporary backup before updating a z/OS UNIX file. The default is `true`. The temporary backup file is a copy of the original file, and it is placed in the same directory and prefixed with the tilde character (~). Uncomment and specify `false` to prevent the creation of the temporary backup file.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -DDISABLE_MIGRATE_HRECALL_HDELETE=true"
Hide migrated data set actions on the client. The default is `false`. Uncomment and specify `true` to ensure that z/OS Explorer V3.0.1.6 and later clients do not show the migrate, hrecall, and hdelete menu actions. Although you still see these menu actions in the clients of previous versions, these menu actions do not work when this option is set.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS –DHIDE_ZOS_UNIX=true"
Hide z/OS UNIX option. The default is `false`. To prevent users from seeing z/OS UNIX elements, that is the directory structure and command line, on the client, uncomment and specify `true`.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Denable.automount=true"
Support home directories created by z/OS UNIX automount. The default is `false`. To ensure that z/OS UNIX automount uses the client user ID as owner of the directory, uncomment and specify `true`.

Note: z/OS UNIX automount uses the user ID of the process that called the service when creating a file system. If this option is disabled, this process is the RSE thread pool server, with the STCRSE user ID. If this option is enabled, a new, temporary process is created by using the client user ID before invoking the service.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Ddisplay.users=true"
Automated display of active users. The default is `false`. Uncomment and specify `true` to enable an automated display of active users in `rseserver.log` on each user logon and logoff.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dprocess.cleanup.interval=0"
Automatically remove RSE thread pools that are in an unrecoverable error state. By default, erroneous RSE thread pools are not automatically removed. To automatically remove erroneous RSE thread pool servers at every interval, where the interval unit is seconds, uncomment and customize. Specifying `0` does not start an interval timer, but erroneous RSE thread pool servers are removed when the RSE daemon checks the RSE thread pools during a new client logon or the DISPLAY PROCESS command.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dkeep.stats.copy.local=true"
Keep ISPF statistics during a local copy. The default is `false`, which implies that ISPF statistics like `create-date` and `changed-by` are updated for the target data set or member. Uncomment and specify `true` to keep the original ISPF statistics during a copy where source and target are on the same host system.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -DDSTORE_USE_THREADED_MINERS=false"
Run each miner on a separate thread. The default is `true`. Uncomment and specify `false` to run all user-specific miners from a single thread. Grouping

all miners for a user on a single thread reduces thread usage within the thread pool, but might cause some delays in command processing when a user is multitasking.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dmaximum.ispf.sessions=0"
Limit the number of concurrent invocations of TSO/ISPF commands in one user session. The default is 0 (no limit). Uncomment and customize this directive to limit the number of concurrent ISPF Gateway sessions per user.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Duse.fastpath.getattributes=true"
Use ISPF file statistics when obtaining attribute information including line counts for members of partitioned data sets. The default is `true`. Uncomment and specify `false` to use an implementation that reports byte counts instead of line counts.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dallow.retry.on.failed.saf.check=false"
Allow re-querying the host security product multiple times in a single login session when access to an MVS file resource is denied. The default is `false`. Uncomment and specify `true` to allow re-querying the host security product.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dmaxthreadtasks.threshold=60"
Allow specifying how close to the MAXTHREADTASKS limit can be reached before displaying a pop-up alert. The default is `60`. Uncomment and adjust the number to specify a new MAXTHREADTASKS threshold.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dsearch.server.limit.hits=0"
Limit the resource usage of non-indexed file and text searches. The default is `0` (no limit). Uncomment and customize this directive to stop a search after the specified number of results have been found.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dsearch.server.limit.scanned_objects=0"
Limit the resource usage of non-indexed file and text searches. The default is `0` (no limit). Uncomment and customize this directive to stop a search after the specified number of objects (data set or PDS(E) member) has been scanned.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dsearch.server.limit.lines=0"
Limit the resource usage of non-indexed file and text searches. The default is `0` (no limit). Uncomment and customize this directive to stop a search after the specified number of lines has been scanned.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dsearch.server.limit.timeout=0"
Limit the resource usage of non-indexed file and text searches. The default is `0` (no limit). Uncomment and customize this directive to stop a search after the specified number of seconds have passed.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -Dsearch.server.limit.errcount=true"
Limit the resource usage of non-indexed file and text searches. The default is `false` (no limit). Uncomment and specify `true` to stop a search before it exceeds a nonzero Language Environment (LE) `ERRCOUNT` value.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS
-Dsearch.server.limit.MaxFilterResults=0"
Limit the number of data sets that are returned for an MVS Files filter. The default is 0 (no limit). Uncomment and specify a positive number (maximum 2,147,483,647) to set a limit. Setting this limit can avoid high CPU consumption for filters that return large number of data sets.

Note: This directive applies to v3.0.1 and later clients only. If the limit is reached, a warning message is displayed in the client, and functions such as Locate do not work.

#_RSE_JAVAOPTS="$_RSE_JAVAOPTS -DDISABLE_TEXT_SEARCH=true"
Disable non-indexed text searches. The default is `false`. To prevent users from starting a full text search on the host, uncomment and specify `true`.

Defining extra Java startup parameters with _RSE_ISPF_OPTS

With the different `_RSE_*OPTS` directives, `rse.env` provides the facility to give extra parameters to Java when it starts the RSE processes. The sample options included in `rse.env` can be activated by uncommenting them.

The `_RSE_ISPF_OPTS` directives are RSE-specific Java options for Legacy ISPF Gateway.

_RSE_ISPF_OPTS=""
Disable reusable Legacy ISPF Gateway sessions. Uncomment to use non-reusable Legacy ISPF Gateway sessions, where each command requires a new session.

_RSE_ISPF_OPTS="$_RSE_ISPF_OPTS&ISPPROF=&SYSUID..ISPPROF"
Use an existing ISPF profile for the ISPF initialization. To use the specified ISPF profile, uncomment and change the data set name.

The following variables can be used in the data set name:

- `&SYSUID.` to substitute the developer's user ID
- `&SYSPREF.` to substitute the developer's TSO prefix, or user ID if the TSO prefix cannot be determined
- `&SYSNAME.` to substitute the system name as specified in the `IEASYMxx` parmlib member

ISPF.conf, the Legacy ISPF Gateway configuration file

Legacy ISPF Gateway uses the definitions in `ISPF.conf` to create a valid environment to execute batch TSO and ISPF commands. z/OS Explorer uses this environment to run the TSO Commands service.

Note: As of z/OS 2.2, Legacy ISPF Gateway, previously named TSO/ISPF Client Gateway, is deprecated and will no longer be enhanced. The functionality is now provided by the Interactive ISPF Gateway. For more information, see "(Optional) Interactive ISPF Gateway" on page 49.

`ISPF.conf` is located in `/etc/zexpl/`, unless you specified a different location when you customized and submitted job `FEK.SFEKSAMP(FEKSETUP)`. For more details, see "Customization setup" on page 9. You can edit the file with the TSO **`OEDIT`** command.

Definitions must start in column 1. Comment lines start with an asterisk (*) when using a US code page. Data lines can have only a directive and its assigned value. Comments are not allowed on the same line. Line continuations are not supported. When concatenating data set names, add them on the same line and separate the names with a comma (,).

In addition to providing the correct names for the ISPF data sets, also add the TSO Commands service data set name, `FEK.SFEKPROC`, to the `SYSPROC` or `SYSEXEC`

statement, as shown in the following example.

```
* REQUIRED:
sysproc=ISP.SISPCLIB,FEK.SFEKPROC
ispmlib=ISP.SISPMENU
isptlib=ISP.SISPTENU
ispplib=ISP.SISPPENU
ispslib=ISP.SISPSLIB
isplLib=ISP.SISPLOAD

* OPTIONAL:
*allocjob = ISP.SISPSAMP(ISPZISP2)
*ISPF_timeout = 900
```

Figure 7. ISPF.conf: ISPF configuration file

Note:

- You can add your own DD-like statements and data set concatenations to customize the TSO environment, thus mimicking a TSO logon procedure. For more details, see "Customizing the TSO environment" in the *Host Configuration Reference Guide* (SC27-8438).
- You cannot define a `STEPLIB` directive. Use the `STEPLIB` directive in `rse.env` instead.
- The Legacy ISPF Gateway might not function properly if you use a third-party product that intercepts ISPF commands, such as **`ISPSTART`**. To see how it can be disabled for z/OS Explorer, check the documentation for that product . If the product requires the allocation of a specific DD statement to DUMMY, you can simulate this behavior in `ISPF.conf` by allocating that DD statement to `nullfile`.

  For example:

  ```
  ISPTRACE=nullfile
  ```
- When using the `allocjob` directive, be careful not to undo the DD definitions done earlier in `ISPF.conf`.
- System abend 522 for module `ISPZTSO` is to be expected if the `JWT` parameter in the `SMFPRMxx` parmlib member is set lower than the `ISPF_timeout` value in `ISPF.conf`. This does not impact z/OS Explorer operations because the Legacy ISPF Gateway is restarted automatically when needed.
- Changes are active for all new invocations. No server restart is needed.

Optional components

This section combines a variety of optional customization tasks. Follow the instructions in the appropriate section to configure the required service.

Customizations to z/OS Explorer configuration files:

- “(Optional) pushtoclient.properties, the host-based client control” on page 41
- “(Optional) ssl.properties, the RSE encrypted communication” on page 44
- “(Optional) rsecomm.properties, the RSE tracing” on page 46

z/OS Explorer related customizations to or for other products:

- “(Optional) Send message” on page 47
- “(Optional) Interactive ISPF Gateway” on page 49
- “(Optional) WORKAREA and /tmp cleanup” on page 50

Installation verification

The detailed description of the various installation verification programs (IVPs) is located in Chapter 4, "Installation verification," on page 53 because some of the IVPs are for the optional components.

You can test the basic functions with the following scenario:

1. Start the JMON started task or user job. The startup information in DD STDOUT should end with the following message:

   ```
   FEJ211I Server ready to accept connections.
   ```

   If the job ends with return code 66, `FEK.SFEKAUTH` is not APF-authorized.
2. Start the RSED started task or user job with the `IVP=IVP` parameter. With this parameter, the server will end after doing some installation verification tests. Check DD STDOUT for messages indicating that the following IVPs were successful:
   - Java startup
   - JES Job Monitor connection
   - TCP/IP setup
3. Start the RSED started task or user job without the IVP parameter. RSE daemon issues the following console message upon successful startup:

   ```
   FEK002I RseDaemon started. (port=4035)
   ```
4. Issue the following operator commands and verify in the resulting console messages that the tests ran successfully:

   ```
   F RSED,APPL=IVP PASSTICKET,userid
   F RSED,APPL=IVP DAEMON,userid
   F RSED,APPL=IVP ISPF,userid
   ```

   Replace `userid` with a valid TSO user ID that has a unique z/OS UNIX UID. If this UID is not unique, all users sharing it must be valid TSO users.

Chapter 3. (Optional) Other customization tasks

This section combines various optional customization tasks. To configure the required service, follow the instructions in the appropriate section.

Customizations to z/OS Explorer configuration files:

- "(Optional) pushtoclient.properties, the host-based client control"
- "(Optional) ssl.properties, the RSE encrypted communication" on page 44
- "(Optional) rsecomm.properties, the RSE tracing" on page 46

z/OS Explorer related customizations to or for other products:

- "(Optional) Send message" on page 47
- "(Optional) Interactive ISPF Gateway" on page 49
- "(Optional) WORKAREA and /tmp cleanup" on page 50

(Optional) pushtoclient.properties, the host-based client control

This customization task does not require assistance, special resources, or special customization tasks for a basic setup.

If you enable group support, you need the assistance of a security administrator or an LDAP administrator to complete this customization task, which requires the following resources or special customization tasks:

- Security rule to allow users access to `FEK.PTC.*` profiles
- Or define user membership of `FEK.PTC.*` LDAP groups

z/OS Explorer clients can pull client configuration files and product update information from the host system when they connect, ensuring that all clients have common settings and that they are up-to-date.

`pushtoclient.properties` tells the client if these functions are enabled, and where the related data is stored. The data is maintained by a z/OS Explorer client administrator.

`pushtoclient.properties` is located in `/etc/zexpl/`, unless you specified a different location when you customized and submitted the `FEK.SFEKSAMP(FEKSETUP)` job. For more details, see "Customization setup" on page 9. You can edit the file with the TSO **OEDIT** command. Changes are active for all new invocations. No server restart is needed.

The client administrator can create multiple client configuration sets and multiple client update scenarios to fit the needs of different developer groups. These multiple sets and scenarios can be used to provide users with a customized setup, based on criteria such as membership of an LDAP group or permit to a security profile. For more information about supporting multiple groups, see "Push-to-client considerations" in *Host Configuration Reference* (SC27-8438).

Table 8. Push-to-client group support

Key value	Is the related push-to-client function enabled?
False	No, disabled
True	Yes, enabled for all
LDAP	Yes, but availability is controlled by membership of LDAP groups
SAF	Yes, but availability is controlled by permit to security profiles

The following code sample shows the `pushtoclient.properties` file, which must be customized to match your system environment. Comment lines start with a number sign (#) when using a US code page. Data lines can have only a directive and its assigned value. Comments are not allowed on the same line. Line continuations are not supported.

```
#
# host-based client control
#
config.enabled=false
product.enabled=false
reject.config.updates=false
reject.product.updates=false
accept.product.license=false
primary.system=false
pushtoclient.folder=/var/zexpl/pushtoclient
default.store=com.ibm.ftt.configurations.USS
file.permission=RWX.RWX.RX
```

Figure 8. pushtoclient.properties: Host-based client control configuration file

config.enabled
Indicates whether host-based client control is used for configuration files. The default is `false`. The valid values are `true`, `false`, `LDAP`, or `SAF`. For the meaning of these values, see Table 8.

product.enabled
Indicates whether host-based client control is used for product updates. The default is `false`. The valid values are `true`, `false`, `LDAP`, or `SAF`. For the meaning of these values, see Table 8.

reject.config.updates
Indicates whether a user can reject configuration updates that are pushed to the client. The default is `false`. The valid values are `true`, `false`, `LDAP`, or `SAF`. For the meaning of these values, see Table 8.

reject.product.updates
Indicates whether a user can reject product updates that are pushed to the client. The default is `false`. The valid values are `true`, `false`, `LDAP`, or `SAF`. For the meaning of these values, see Table 8.

accept.product.license
Indicates whether the product license is automatically accepted during updates that are initiated by push-to-client. If enabled, IBM Installation Manager does not ask to accept the license during client update. The default is `false`. The only valid values are `true` and `false`.

primary.system
Host-based client control supports storing system-specific data for each system, while maintaining common data on a single system to reduce management effort. This directive indicates whether this is the system that

stores global, non-system specific, client definitions. The default is `false`. The only valid values are `true` and `false`.

Note: Ensure that you have one, and only one, system that is defined as primary system. z/OS Explorer client administrators cannot export global configuration data unless the target system is a primary system. z/OS Explorer clients might show erratic behavior when connecting to multiple primary systems with out-of-sync configurations.

pushtoclient.folder
The base directory for the host-based client control definitions. The default is `/var/zexpl/pushtoclient`.

default.store
Host-based client control supports different methods for storing the data that is pushed to the client. This directive identifies the driver, or store, that is used to access the data. The default is `com.ibm.ftt.configurations.USS`, which supports the data being stored in z/OS UNIX flat files.

z/OS Explorer only provides the `com.ibm.ftt.configurations.USS` store. A third-party store is needed when the data is located somewhere else.

file.permission
The `com.ibm.ftt.configurations.USS` store uses `file.permission` to determine the required access permissions for files that are created by the store. The default is `RWX.RWX.RX`, which allows the owner and the owner's default group read and write access to the directory structure and the files within. Everyone else has only read access to the directory structure and the files within.

According to the UNIX standards, permissions can be set for three types of users: owner, group, and other. The fields in the `file.permission` mask match this order, and the fields are separated by a period (.). Each field can either be empty, or have `R`, `W`, `RW`, `X`, `RX`, `WX`, or `RWX` as value (where R = read, W = write, X = execute or list directory content).

Note:

- To activate host-based client control, a `keymapping.xml` file must exist in `/var/zexpl/pushtoclient`. This file is created and maintained by a z/OS Explorer client administrator.
- For more information about host-based projects, host-based client configuration, and upgrade control, see "Push-to-client considerations" in the *Host Configuration Reference* (SC27-8438).
- When a file is created, z/OS UNIX uses by default the effective UID (user ID) of the creating thread and the GID (group ID) of the owning directory, not the effective GID of the creating thread. For more information on how to change this behavior or how to adjust your host-based client control setup to get the required GID assignment, see "z/OS UNIX directory structure" in *Host Configuration Reference* (SC27-8438).

(Optional) ssl.properties, the RSE encrypted communication

You need assistance of a security administrator to complete this customization task, which requires the following resources or special customization tasks:

- LINKLIST update
- Security rule to add program controlled data sets
- (Optional) Security rule to add a certificate for host authentication

Note: Due to a vulnerability in the SSLv3 (Secure Socket Layer) protocol, support for this protocol is deprecated in z/OS Explorer.

External, client-host communication can be encrypted using TLS (Transport Layer Security). This feature is disabled by default and is controlled by the settings in `ssl.properties`.

Note: Client authentication with an X.509 certificate requires the use of encrypted communication.

`ssl.properties` is located in `/etc/zexpl/`, unless you specified a different location when you customized and submitted the `FEK.SFEKSAMP(FEKSETUP)` job. For more details, see "Customization setup" on page 9. You can edit the file with the TSO **`OEDIT`** command. RSE must be restarted for the changes to take effect.

The client communicates with RSE daemon during connection setup and with RSE server during the actual session. Both data streams are encrypted when encryption is enabled.

Note:

- SAF-compliant key rings are the supported method for managing certificates.
- SAF-compliant key rings can store the certificate's private key either in the security database or by using ICSF, the interface to z Systems cryptographic hardware. Access to ICSF is protected by profiles in the `CSFSERV` security class.

RSE daemon uses System SSL functions to manage encrypted communications. This implies that `SYS1.SIEALNKE` must be program controlled by the security software and be available to RSE when using LINKLIST or the STEPLIB directive in `rse.env`.

The following code sample shows the sample `ssl.properties` file, which must be customized to match your system environment. Comment lines start with a number sign (#) when using a US code page. Data lines can have only a directive and its assigned value; comments are not allowed on the same line. Line continuations are not supported.

```
# ssl.properties – encrypted communication configuration file
enable_ssl=false

# Daemon Properties

daemon_keydb_file=
daemon_key_label=

# Server Properties

server_keystore_file=
server_keystore_label=
server_keystore_type=JCERACFKS
```

Figure 9. ssl.properties – encrypted communication configuration file

The daemon and server properties must be set only if you enable communication encryption. For more information about encrypted communication setup, see "Setting up encrypted communication and X.509 authentication" in the *Host Configuration Reference Guide* (SC27-8438).

enable_ssl
Enable or disable encrypted communication. The default is `false`. The only valid options are `true` and `false`.

daemon_keydb_file
RACF or similar security product key ring name. If encrypted communication is enabled, customize this directive.

daemon_key_label
The certificate label used in the key ring. If encrypted communication is enabled, customize this directive. Key labels are case-sensitive.

server_keystore_file
Name of the RACF or similar security product key ring name. If encrypted communication is enabled, customize this directive.

server_keystore_label
The certificate label used in the key ring. If encrypted communication is enabled, customize this directive. Key labels are case-sensitive.

server_keystore_type
Keystore type. The default is `JCERACFKS`. Valid values are these:

Table 9. Valid keystore types

Keyword	Keystore type
JCERACFKS	SAF-compliant key ring, where the certificate's private key is stored in the security database.
JCECCARACFKS	SAF-compliant key ring, where the certificate's private key is stored using ICSF, the interface to z Systems cryptographic hardware.

Note:

- You can use the `rse.env` configuration file that is located in the same directory as `ssl.properties` to specify additional options (`GSK_*`) to adjust your encrypted communication.

- As documented in *Cryptographic Services ICSF Administrator's Guide (SA22-7521)*, ICSF uses profiles in the CSFKEYS and CSFSERV security classes to control who can use cryptographic keys and services.
- At the time of publication, IBM z/OS Java requires an update of the /usr/lpp/java/J6.0/lib/security/java.security file to support JCECCARACFKS. The following line must be added:

  ```
  security.provider.1=com.ibm.crypto.hdwrCCA.provider.IBMJCECCA
  ```

  The resulting file looks like this:

  ```
  security.provider.1=com.ibm.crypto.hdwrCCA.provider.IBMJCECCA
  security.provider.2=com.ibm.jsse2.IBMJSSEProvider2
  security.provider.3=com.ibm.crypto.provider.IBMJCE
  security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
  security.provider.5=com.ibm.security.cert.IBMCertPath
  ...
  ```
- Chapter "Setting up encrypted communication and X.509 authentication" in the *Host Configuration Reference (SC27-8438)* provides step-by-step guidance for setting up encrypted communication.

(Optional) rsecomm.properties, the RSE tracing

This customization task does not require assistance, special resources, or special customization tasks.

z/OS Explorer supports different levels of tracing the internal program flow for problem-solving purposes. RSE, and some of the services called by RSE, use the settings in rsecomm.properties to know the required initial detail level in the output logs.

Attention: Changing these settings can cause performance degradations and should be done only under the direction of the IBM support center.

rsecomm.properties is located in /etc/zexpl/, unless you specified a different location when you customized and submitted FEK.SFEKSAMP(FEKSETUP) job. For more details, see "Customization setup" on page 9. You can edit the file with the TSO **OEDIT** command. RSE must be restarted for the changes to take effect.

The following code sample shows the rsecomm.properties file, which can be customized to match your tracing needs. Comment lines start with a number sign (#) when using a US code page. Data lines can have only a directive and its assigned value; comments are not allowed on the same line. Line continuations are not supported.

```
# Logging level
# 0 - Log error messages
# 1 - Log error and warning messages
# 2 - Log error, warning and info messages
debug_level=1
#USER=userid
#USER=(userid,userid,...)
```

Figure 10. rsecomm.properties - Logging configuration file

debug_level

Detail level for output logs. The default is 1, which logs error and warning messages. The debug_level detail controls the detail level of multiple services and, thus, multiple output files. Increasing the detail level will cause performance degradations and should be done under only the

direction of the IBM support center. For more information about which logs are controlled by this directive, see "RSE tracing" in the *Host Configuration Reference Guide* (SC27-8438).

Table 10. Detail level for output logs

Value	Detail level
0	Log error messages only
1	Log error and warning messages
2	Log error, warning, and informational messages

Note: `debug_level` can be changed dynamically for specific log files with the **modify rsecommlog**, **modify rseserverlog**, and **modify rsedaemonlog** operator commands, as described in Chapter 7, "Operator commands," on page 73.

USER Set debug level 2 (log error, warning, and informational messages) for the specified user IDs during server startup. The debug level for all other users is the default as specified in the `debug_level` directive. The `USER` directive alters the trace detail level for RSE server (`rsecomm.log`) and the MVS data set services (`lock.log` and `ffs*.log`), and is equivalent to issuing the **modify trace user** operator command.

(Optional) Send message

You need the assistance of a security administrator to complete this customization task, which requires the following resources or special customization tasks:
• Define FEK.CMD.SEND.** security profiles
• Update TSO logon procedure to add FEK.SFEKAUTH to STEPLIB

z/OS Explorer allows sending messages to clients, similar to the TSO `SEND` command. Messages can be sent via an operator command (`MODIFY SEND`), a z/OS UNIX command (`send`) or the TSO `SEND` command. Messages are delivered immediately to connected users, and are also stored for users that log on later. This message buffer can be cleared using the operator command and the z/OS UNIX command.

z/OS Explorer will query your security product for access permits to `FEK.CMD.SEND.**` profiles to determine if the requestor is allowed to send a message or clear the buffer. The RSED started task user ID is verified when using the operator command interface.

MODIFY SEND Operator command

The operator command interface has one of the following formats, where `userid` is a target userid, and `pid` is the process ID of a target thread pool.

```
MODIFY rsed,APPL=SEND 'message'[,User={userid | (userid,userid,...)}]
MODIFY rsed,APPL=SEND 'message'[,Pid={pid | (pid,pid,...)}]
MODIFY rsed,APPL=SEND CLEAR
```

- By default, a message is delivered to all users of this RSE daemon.
- A message sent using the PID filter is not stored, only users active in the referenced thread pools receive it.
- The single quotation mark (') character is not allowed in the message text as the message must be enclosed in single quotation marks.

z/OS UNIX send command

The z/OS UNIX interface has one of the following formats, where `userid` is a target userid, `pid` is the process ID of a target thread pool and `jobname` is the job name of a target RSE daemon. The `-c` option clears the message buffer.

```
send [-u userid[,userid,...]] [-d jobname] message
send [-p pid[,pid,...]] [-d jobname] message
send -c [-d jobname]
```

- The send command is located in `/usr/lpp/IBM/zexpl/bin/send`, unless you used a different path during the SMP/E install of z/OS Explorer.
- By default, a message is delivered to all users of all active RSE daemons.
- A message sent using the `-p` filter is not stored, only users active in the referenced thread pools will receive it.
- The message text is interpreted by the z/OS UNIX shell before it is passed to the send command. Use standard techniques to avoid interpretation by the shell if this is not desired.
- The maximum length of the send command including the options and message text is limited to 320 bytes.

Note: The `/usr/lpp/IBM/zexpl/bin/` path is part of the `PATH` variable when a user opens a z/OS UNIX command line in the z/OS Explorer client.

TSO SEND command

The TSO `SEND` command can be enhanced with the `IKJEESX0` user exit so it can send messages to z/OS Explorer users. The `IKJEESX0` user exit that is provided by z/OS Explorer supports a subset of the normal TSO `SEND` options.

```
{SEND | SE} 'message' USER({* | userid [userid ...]}) [{NOW | LOGON | SAVE}]
```

- The `IKJEESX0` user exit is in `FEK.SFEKAUTH`, unless you used a different high-level qualifier during the SMP/E install of z/OS Explorer.
- The only required configuration is making the exit available to TSO using STEPLIB, LINKLIST, or LPA.
- The message is delivered to the specified users at all active RSE daemons.
- The single quotation mark (') character is not allowed in the message text as the message must be enclosed in single quotation marks.
- The maximum length of the `SEND` command including the options and message text is limited to 320 bytes.
- Keyword `NOW` is used to send a message to active users only. This is the default.
- Keyword `LOGON` is used to send a message to active users, and to store the message for disconnected users, who will receive the message upon next logon.
- Keyword `SAVE` is used to send a message to disconnected users only, who will receive the message upon next logon.

Note: When you are using a Legacy ISPF Gateway to provide the TSO command line in the z/OS Explorer client, you can add `FEK.SFEKAUTH` to STEPLIB in `rse.env` to provide the `IKJEESX0` user exit to TSO. You must use LINKLIST or update the user's TSO logon procedure when you are using an Interactive ISPF Gateway for the TSO command line. For a description of these system services, see "(Optional) Interactive ISPF Gateway" on page 49.

(Optional) Interactive ISPF Gateway

You need the assistance of a security administrator to complete this customization task, which requires the following resources or special customization tasks:

- Define Common Event Adapter (CEA) security profiles
- SYS1.PARMLIB update

As of z/OS 2.2, Legacy ISPF Gateway, previously named TSO/ISPF Client Gateway, is deprecated and will no longer be enhanced. The functionality is now provided by Interactive ISPF Gateway. As the name implies, Interactive ISPF Gateway supports the usage of interactive commands (for example `TSO RECEIVE`). ISPF services are also supported, but ISPF panel applications are not supported.

z/OS Explorer uses the ISPF Gateway for the TSO Commands service.

Legacy ISPF Gateway relies on various `CGI_ISP*` variables in `rse.env` and the definitions in `ISPF.conf`. Except for `CGI_ISPHOME` and possible LINKLIST definitions, Interactive ISPF Gateway does not share any configuration definition with Legacy ISPF Gateway.

Interactive ISPF Gateway, which is activated with the `CGI_CEATSO` variable in `rse.env`, requires z/OS 2.2, and the Common Event Adapter (CEA) TSO/E address space manager service.

Common Event Adapter (CEA) TSO/E address space manager is a subcomponent of the z/OS CEA services. Refer to *MVS Callable Services for HLL (SA22-7613)* for details on prerequisites and setup instructions for the CEA TSO/E address space manager service. Refer to *z/OS Common Information Model User's Guide (SC34-2671)* for a description of error reason codes.

- CEA started task must be active.
- The CEA started task configuration file is `SYS1.PARMLIB(CEAPRMxx)`.
- CEA must be started in full function mode, which implies that security setup is required. See `SYS1.SAMPLIB(CEASEC)` for sample commands.
- CEA started task must have the TRUSTED attribute.

```
RALTER STARTED (CEA.*) STDATA(TRUSTED(YES))
SETROPTS  RACLIST(STARTED)REFRESH
```

- All z/OS Explorer users must have READ access to the `CEA.CEATSO.TSOREQUEST` profile in the `SERVAUTH` security class.

```
RDEFINE SERVAUTH (CEA.CEATSO.TSOREQUEST) UACC(NONE)
PERMIT CEA.CEATSO.TSOREQUEST CLASS(SERVAUTH) ID(*) ACCESS(READ)
SETROPTS  RACLIST(SERVAUTH) REFRESH
```

Unlike Legacy ISPF Gateway, Interactive ISPF Gateway creates traditional TSO address spaces, which result in different behavior on the host and client.

- TSO address spaces that are created using CEA are regular `TSUxxxxx` user jobs in your JES system (whereas Legacy ISPF Gateway sessions are `STCxxxxx` started tasks).
- CEA requires that a logon procedure, account number, group ID, and region size is provided by the caller (whereas Legacy ISPF Gateway required no TSO logon information).
- z/OS Explorer clients allow the user to provide (and alter) this TSO logon information.

- The TSO logon procedure that is used for Interactive ISPF Gateway may not invoke ISPF panel applications.
- As with regular TSO logon through a 3270 session, TSO stores the logon data in the user's security TSO segment, replacing what was already there. This can result in unexpected logon values if the user uses different values for a TSO session that uses 3270.
- If users use multiple Interactive ISPF Gateways simultaneously, or use TSO via 3270 simultaneously with the Interactive ISPF Gateway, TSO and ISPF must be set up to allow for multiple simultaneous logons.
- Interactive ISPF Gateway requires you to upper-case TSO commands and prefix them with the TSO keyword.

(Optional) WORKAREA and /tmp cleanup

This customization task does not require assistance, special resources, or special customization tasks.

Legacy ISPF Gateway uses the `WORKAREA` and `/tmp` directories to store temporary work files, which are removed before the session is closed. However, temporary output is sometimes left behind, for example, if there is a communication error while processing. Therefore, clear the `WORKAREA` and `/tmp` directories from time to time.

z/OS UNIX provides a shell script, `skulker`, that deletes files according to the directory they are in and their age. Combined with the z/OS UNIX `cron` daemon, which runs commands at specified dates and times, you can set up an automated tool that periodically cleans targeted directories. For more information about the `skulker` script and the `cron` daemon, see *UNIX System Services Command Reference* (SA22-7802).

Note: `WORKAREA` is located in `/var/zexpl/`, unless you specified a different location when you customized and submitted the `FEK.SFEKSAMP(FEKSETUP)` job. For more details, see "Customization setup" on page 9.

(Optional) z/OS Explorer consumers configuration

The products that utilize z/OS Explorer might require additional host configuration before they are operational. For more details, see the documentation of those products or their common components.

- IBM Developer for z Systems and IBM z/OS Debugger
- IBM File Manager for z/OS and IBM Fault Analyzer for z/OS
- IBM Application Performance Analyzer for z/OS
- Rational Team Concert™
- IBM CICS Explorer® SDK
- CICS® Transaction Gateway for z/OS
- CICS Configuration Manager for z/OS
- CICS Deployment Assistant for z/OS
- CICS Interdependency Analyzer for z/OS
- CICS Performance Analyzer for z/OS
- IBM Data Studio

- IBM MQ Explorer
- IBM IMS™ Explorer for Development
- IBM z/OS Connect Enterprise Edition

Chapter 4. Installation verification

After completing the product customization, you can use the Installation Verification Programs (IVPs) described in this chapter to verify the successful setup of key product components.

Verify the started tasks

JMON, the JES Job Monitor

Start the JMON started task or user job. The server should issue the following console message:

```
FEJ211I Server ready to accept connections on port <portnumber>
```

If the job ends with return code 66, then FEK.SFEKAUTH is not APF-authorized.

Note: Start JES Job Monitor before continuing with the other IVP tests.

RSED, the RSE daemon

Start the RSED started task or user job with the IVP=IVP parameter. With this parameter, the server ends after doing some installation verification tests. The output of these tests is available in DD STDOUT. In case of certain errors, data is also available in DD STDERR. Check DD STDOUT for messages that indicate that the following IVPs were successful:

- Java startup
- JES Job Monitor connection
- TCP/IP setup

Note: Start RSE daemon before continuing with the other IVP tests.

IVP operator commands

An active RSE daemon supports the **IVP** modify command, which you can use to do selected IVPs from the console.

PassTicket reusability

z/OS Explorer requires that the PassTickets it generates are reusable because PassTicket generation is limited to one for a user every second. Verify the PassTicket reusability by executing the following operator command. Replace userid with a valid TSO user ID that has a unique z/OS UNIX UID. If this UID is not unique, all users sharing it must be valid TSO users.

```
MODIFY RSED,APPL=IVP PASSTICKET,userid
```

The command should return a success message.

RSE daemon connection

Verify the RSE daemon connection by executing the following command. Replace userid with a valid TSO user ID that has a unique z/OS UNIX UID. If this UID is not unique, all users sharing it must be valid TSO users.

```
MODIFY RSED,APPL=IVP DAEMON,userid
```

This command is functionally identical to the `fekfivpd` IVP described in "Verify the services" but with the benefit that no password is required. RSE generates a PassTicket and uses this as password. The command should return a success message.

ISPF Client Gateway

Verify the ISPF Gateway connection by executing one of the following commands, with these replacements:

- Replace `userid` with a valid TSO user ID that has a unique z/OS UNIX UID. If this UID is not unique, all users sharing it must be valid TSO users.
- Replace `proc` with a valid TSO logon procedure for this user ID that does not invoke ISPF panels.
- Replace `acct` with a valid account number for this user ID.
- Replace `group` with a valid security group ID for this user ID.
- Replace `size` with a valid region size for this user ID.

For Legacy ISPF Gateway, issue:

```
MODIFY RSED,APPL=IVP ISPF,userid
```

For Interactive ISPF Gateway, issue:

```
MODIFY RSED,APPL=IVP ISPF,userid,P=proc,A=acct,G=group,S=size
```

These commands are functionally identical to the `fekfivpi` IVP described "Verify the services." The commands should return a success message.

Verify the services

The z/OS Explorer installation provides several Installation Verification Programs (IVP) for the basic and optional services. The IVP scripts are located in the installation directory which, by default, is `/usr/lpp/IBM/zexpl/bin/`.

Table 11. IVPs for services. This table lists IVPs for services.

IVP	Description
fekfivpd	"RSE daemon connection" on page 56
fekfivpi	"ISPF Gateway connection" on page 57
fekfivpj	"JES Job Monitor connection" on page 56
fekfivpt	"TCP/IP setup" on page 56

The tasks described in the following sections require you to be active in z/OS UNIX. This can be done by issuing the **OMVS** TSO command. To return to TSO, use the **exit** command.

A large region size is required for the user ID that executes the IVPs because functions such as Java, which require a lot of memory, are executed. You should set the region size to 131072 kilobytes (128 megabytes) or more.

The following sample error is a clear indication of an insufficient region size, but other errors can occur, too. For example, Java might fail to start.

```
CEE5213S The signal SIGPIPE was received.
%z/OS UNIX command%: command was killed by signal number 13
    %line-number% *-*   %REXX command%
       +++ RC(137) +++
```

Note: The z/OS Explorer started tasks must be active before starting the IVP test.

IVP initialization

All sample commands in this section require certain environment variables to be set. This way, the IVP scripts are available through the PATH statement and the location of the customized configuration files is known. Use the **pwd** and **cd** commands to verify and change your current directory to the directory with the customized configuration files. The `ivpinit` shell script can then be used to set the RSE environment variables, such as in the following sample, where $ is the z/OS UNIX prompt:

```
$ pwd
/u/userid
$ cd /etc/zexpl
$ . ./ivpinit
-- RSE_CFG set to /etc/zexpl -- based on current location
-- RSE_HOME set to /usr/lpp/IBM/zexpl -- defined in $RSE_CFG/rse.env
-- added $RSE_HOME/bin to PATH
```

The first period (.) in `. ./ivpinit` is a z/OS UNIX command to run the shell in the current environment, so that the environment variables set in the shell are effective even after exiting the shell. The second period (.) is referring to the current directory.

Note:

- If `. ./ivpinit` is not executed before the `fekfivp*` scripts, the path to these scripts must be specified when calling them, as in the following sample:

  ```
  /usr/lpp/IBM/zexpl/bin/fekfivpt
  ```

  Also, if `. ./ivpinit` is not executed first, all `fekfivp*` scripts ask for the location of the customized `rse.env`, which in turn must specify RSE_HOME.
- Some IVP tests use the TCP/IP REXX socket API, which requires that the TCP/IP load library, which, by default, is`TCPIP.SEZALOAD`, is in LINKLIST or STEPLIB. The following command might be necessary to be able to execute these IVP tests :

  ```
  $ EXPORT STEPLIB=$STEPLIB:TCPIP.SEZALOAD
  ```

  Adding a non-APF authorized library to an existing STEPLIB removes the APF authorization for existing STEPLIB data sets.

  If `CEE.SCEELKED` is in LINKLIST or STEPLIB, `TCPIP.SEZALOAD` must be placed before `CEE.SCEELKED`. Failure to do so will result in a 0C1 system abend for the TCP/IP REXX socket calls.

For information about diagnosing host system connection problems, see "Troubleshooting configuration problems" in the *Host Configuration Reference Guide* (SC27-8438).

Port availability

The JES Job Monitor and RSE daemon port availability can be verified by issuing the **netstat** command. The result should show the ports used by these services, as in the following samples:

IPv4

```
$ netstat
MVS TCP/IP NETSTAT CS VxRy    TCPIP Name: TCPIP       13:57:36
User Id  Conn     Local Socket      Foreign Socket    State
```

```
-------  ----     ------------      --------------    -----
RSED     0000004B 0.0.0.0..4035     0.0.0.0..0        Listen
JMON     00000037 0.0.0.0..6715     0.0.0.0..0        Listen
```

IPv6

```
$ netstat
MVS TCP/IP NETSTAT CS VxRy    TCPIP Name: TCPIP       14:03:35
User Id  Conn     State
-------  ----     -----
RSED     0000004B Listen
  Local Socket:   0.0.0.0..4035
  Foreign Socket: 0.0.0.0..0
JMON     00000037 Listen
  Local Socket:   0.0.0.0..6715
  Foreign Socket: 0.0.0.0..0
```

TCP/IP setup

z/OS Explorer is dependent upon TCP/IP having the correct host name when it is initialized. This implies that the different TCP/IP and Resolver configuration files must be set up correctly. For more information about TCP/IP and Resolver setup, see "Setting up TCP/IP" in the *Host Configuration Reference Guide* (SC27-8438). Verify the current settings by executing the following command:

```
fekfivpt
```

Note: This IVP issues the TCPIP **`netstat -u`** command, which might be protected against execution by your security software. See the `EZB.NETSTAT.mvsname.tcpprocname.UP` profile in the `SERVAUTH` class.

The command should return a success message.

RSE daemon connection

Verify the RSE daemon connection by executing the following command.

```
fekfivpd
```

After prompting for a password, the command should return a success message.

When testing an encrypted connection, ensure that the user ID executing the IVP has access to all of the required certificates, including the CA certificates that are used to sign the z/OS Explorer certificate. The operator command version of this IVP, `F RSED,APPL=IVP DAEMON,userid`, uses the setup that is done for RSE host system, and is therefore less error prone. Some common encryption-related errors are given in the following list:

- Verify that the user ID executing the IVP has access to all of the required certificates if you get this error message: `gsk_environment_init() failed: Error detected while opening the certificate data base`
- Verify that the signing CA certificates are also on the key ring if you get this error message: `gsk_secure_socket_init() failed: Certificate validation error`

JES Job Monitor connection

Verify the JES Job Monitor connection by executing the following command.

```
fekfivpj
```

The command should return a success message.

ISPF Gateway connection

Verify the ISPF Gateway connection by executing one of the following commands, with these replacements:

- Replace `proc` with a valid TSO logon procedure for this user ID that does not invoke ISPF panels.
- Replace `acct` with a valid account number for this user ID.
- Replace `group` with a valid security group ID for this user ID.
- Replace `size` with a valid region size for this user ID.

For Legacy ISPF Gateway, issue:

```
fekfivpi
```

For Interactive ISPF Gateway, issue:

```
fekfivpi –P proc –A acct –G group –S size
```

The commands should return a success message.

`fekfivpi` has the following optional, non-positional, parameters:

-file `fekfivpi` can produce large amounts of output, running into hundreds of lines. The `-file` parameter sends this output to a file, `$TMPDIR/fekfivpi.log`, where `$TMPDIR` is the value of the `TMPDIR` directive in `rse.env` which, by default, is `/tmp`.

-debug
The `-debug` parameter creates detailed test output. Do not use this option unless directed by the IBM support center.

Chapter 5. Security definitions

Customize and submit the sample FEKRACF member, which has sample RACF and z/OS UNIX commands to create the basic security definitions for z/OS Explorer.

FEKRACF is located in FEK.#CUST.JCL, unless you specified a different location when you customized and submitted the FEK.SFEKSAMP(FEKSETUP) job. For more details, see "Customization setup" on page 9.

See the *RACF Command Language Reference* (SA22–7687), for more information about RACF commands.

Note: [2]

- For those sites that use CA ACF2™ for z/OS, see the product page on the CA support site (https://support.ca.com) and check for the related z/OS Explorer Knowledge Document, TEC492389. This Knowledge Document has details on the security commands that are necessary to properly configure z/OS Explorer.
- For those sites that use CA Top Secret® for z/OS, see the product page on the CA support site (https://support.ca.com) and check for the related z/OS Explorer Knowledge Document, TEC492091. This Knowledge Document has details on the security commands that are necessary to properly configure z/OS Explorer.

The following sections describe the required steps, optional configuration, and possible alternatives.

Requirements and checklist

To complete the security setup, the security administrator must know the values that are listed in Table 12. These values were defined during previous steps of the installation and customization of z/OS Explorer.

Table 12. Security setup variables

Description	• **Default value** • **Where to find the answer**	Value
z/OS Explorer product high-level qualifier	• FEK • SMP/E installation	
z/OS Explorer customization high-level qualifier	• FEK.#CUST • FEK.SFEKSAMP(FEKSETUP), as described in "Customization setup" on page 9.	
JES Job Monitor started task name	• JMON • FEK.#CUST.PROCLIB(JMON), as described in "PROCLIB changes" on page 14.	

2. z/OS Explorer security definitions are based on IDz's.

Table 12. Security setup variables (continued)

Description	• **Default value** • **Where to find the answer**	Value
RSE daemon started task name	• `RSED` • `FEK.#CUST.PROCLIB(RSED)`, as described in "PROCLIB changes" on page 14.	
Application ID	• `FEKAPPL` • `/etc/zexpl/rse.env`, as described in "Defining extra Java startup parameters with _RSE_JAVAOPTS" on page 29	

The following list is an overview of the actions that are required to complete the basic security setup of z/OS Explorer. As documented in the following sections, different methods can be used to fulfill these requirements, depending on the required security level. For information about the security setup of optional z/OS Explorer services, see the previous sections.

Activate the security settings and classes

z/OS Explorer uses a variety of security mechanisms to ensure a secure and controlled host system environment for the client. To do so, several classes and security settings must be active, as shown with the following sample RACF commands:

- Display current settings
  - `SETROPTS LIST`
- Activate facility class for z/OS UNIX, and digital certificate profiles
  - `SETROPTS GENERIC(FACILITY)`
  - `SETROPTS CLASSACT(FACILITY) RACLIST(FACILITY)`
- Activate started task definitions
  - `SETROPTS GENERIC(STARTED)`
  - `RDEFINE STARTED ** STDATA(USER(=MEMBER) GROUP(STCGROUP) TRACE(YES))`
  - `SETROPTS CLASSACT(STARTED) RACLIST(STARTED)`
- Activate console security for JES Job Monitor

  - SETROPTS GENERIC(CONSOLE)
  - SETROPTS CLASSACT(CONSOLE) RACLIST(CONSOLE)
- Activate operator command protection for JES Job Monitor
  - SETROPTS GENERIC(OPERCMDS)
  - SETROPTS CLASSACT(OPERCMDS) RACLIST(OPERCMDS)
- Activate z/OS UNIX file access permission for RSE
  - o SETROPTS GENERIC(UNIXPRIV)
  - o SETROPTS CLASSACT(UNIXPRIV) RACLIST(UNIXPRIV)
- Activate application protection for RSE
  - SETROPTS GENERIC(APPL)
  - SETROPTS CLASSACT(APPL) RACLIST(APPL)
- Activate secured signon using PassTickets for RSE
  - SETROPTS GENERIC(PTKTDATA)
  - SETROPTS CLASSACT(PTKTDATA) RACLIST(PTKTDATA)
- Activate program control to ensure that only trusted code can be loaded by RSE
  - RDEFINE PROGRAM ** ADDMEM('SYS1.CMDLIB'//NOPADCHK) UACC(READ)
  - SETROPTS WHEN(PROGRAM)

    Note: Do not create the ** profile if you already have a * profile in the PROGRAM class. It obscures and complicates the search path used by the security software. In this case, you must merge the existing * and the new ** definitions. Use the ** profile, as documented in *Security Server RACF Security Administrator's Guide* (SA22-7683).

Attention: Some products, such as FTP, require being program controlled if "WHEN PROGRAM" is active. Test this program control before activating it on a production system.

- (Optional) Activate X.509 HostIdMappings and extended Port Of Entry (POE) support
  - SETROPTS GENERIC(SERVAUTH)
  - SETROPTS CLASSACT(SERVAUTH) RACLIST(SERVAUTH)

Define an OMVS segment for z/OS Explorer users

A RACF OMVS segment or equivalent that specifies a valid nonzero z/OS UNIX user ID (UID), home directory, and shell command must be defined for each user of z/OS Explorer. Their default group also requires an OMVS segment with a group ID.

In the following sample RACF commands, replace the #userid, #user-identifier, #group-name, and #group-identifier placeholders with actual values:

- ALTUSER #userid
  OMVS(UID(#user-identifier) HOME(/u/#userid) PROGRAM(/bin/sh) NOASSIZEMAX)
- ALTGROUP #group-name OMVS(GID(#group-identifier))

Define the z/OS Explorer started tasks

The following sample RACF commands create the JMON, and RSED started tasks, with protected user IDs (STCJMON, and STCRSE) and the STCGROUP group assigned to them.

- ADDGROUP STCGROUP OMVS(AUTOGID)
  DATA('GROUP WITH OMVS SEGMENT FOR STARTED TASKS')

- `ADDUSER STCJMON DFLTGRP(STCGROUP) NOPASSWORD NAME('JES JOBMONITOR') OMVS(AUTOUID HOME(/tmp) PROGRAM(/bin/sh) ) DATA('IBM Explorer for z/OS')`
- `ADDUSER STCRSE DFLTGRP(STCGROUP) NOPASSWORD NAME('RSE DAEMON') OMVS(AUTOUID HOME(/tmp) PROGRAM(/bin/sh) ASSIZEMAX(2147483647) ) DATA('IBM Explorer for z/OS')`
- `RDEFINE STARTED JMON.* DATA('JES JOBMONITOR') STDATA(USER(STCJMON) GROUP(STCGROUP) TRUSTED(NO))`
- `RDEFINE STARTED RSED.* DATA('RSE DAEMON') STDATA(USER(STCRSE) GROUP(STCGROUP) TRUSTED(NO))`
- `SETROPTS RACLIST(STARTED) REFRESH`

Note:

- Ensure that the started tasks user IDs are protected by specifying the `NOPASSWORD` keyword.
- Ensure that RSE daemon has a unique OMVS `uid` due to the z/OS UNIX related privileges granted to this `uid`.
- RSE daemon requires a large address space size (2GB) for proper operation. Set this value in the `ASSIZEMAX` variable of the OMVS segment for user ID `STCRSE`. Setting this value ensures that RSE daemon gets the required region size, regardless of changes to `MAXASSIZE` in `SYS1.PARMLIB(BPXPRMxx)`.
- RSE also requires a large number of threads for proper operation. You can set the limit in the `THREADSMAX` variable of the OMVS segment for user ID `STCRSE`. Setting the limit ensures that RSE gets the required thread limit, regardless of changes to `MAXTHREADS` or `MAXTHREADTASKS` in `SYS1.PARMLIB(BPXPRMxx)`. To determine the correct value for the thread limit, see "Tuning considerations" in the *Host Configuration Reference Guide* (SC27-8438).
- User ID `STCJMON` is another good candidate for setting `THREADSMAX` in the OMVS segment, because JES Job Monitor uses a thread per client connection.

Consider making the `STCRSE` user ID restricted. Users with the `RESTRICTED` attribute cannot access protected (MVS) resources that they are not specifically authorized to access.

```
ALTUSER STCRSE RESTRICTED
```

To ensure that restricted users do not gain access to z/OS UNIX file system resources through the “other” permission bits, define the `RESTRICTED.FILESYS.ACCESS` profile in the `UNIXPRIV` class with `UACC(NONE)`. For more information about restricting user IDs, see *Security Server RACF Security Administrator’s Guide* (SA22-7683).

Attention: If you use restricted user IDs, explicitly add the permission to access a resource by using the TSO **`PERMIT`** or the z/OS UNIX **`setfacl`** commands. The resources include those resources where the z/OS Explorer documentation uses UACC, such as the `**` profile in the `PROGRAM` class, or where it relies on common z/OS UNIX conventions, such as everyone having read and execute permission for Java libraries. Test the access before activating it on a production system.

Define RSE as a secure z/OS UNIX server

RSE requires UPDATE access to the `BPX.SERVER` profile to create or delete the security environment for the client's thread. Note that using `UID(0)` to bypass this requirement is not supported. This step is required for clients to be able to connect.

- `RDEFINE FACILITY BPX.SERVER UACC(NONE)`

- PERMIT BPX.SERVER CLASS(FACILITY) ACCESS(UPDATE) ID(STCRSE)
- SETROPTS RACLIST(FACILITY) REFRESH

Attention: Defining the BPX.SERVER (or BPX.DAEMON) profile makes z/OS UNIX as a whole switch from UNIX level security to z/OS UNIX level security, which is more secure. This switch might impact other z/OS UNIX applications and operations. Test the security before activating it on a production system. For more information about the different security levels, see *UNIX System Services Planning* (GA22-7800).

Define the MVS program controlled libraries for RSE

Servers with authority to BPX.SERVER must run in a clean, program-controlled environment. This requirement implies that all programs called by RSE must also be program controlled. For MVS load libraries, program control is managed by your security software. This step is required for clients to be able to connect.

RSE uses system (SYS1.LINKLIB), Language Environment's runtime (CEE.SCEERUN*) and ISPF Gateway (ISP.SISPLOAD) load libraries.

- RALTER PROGRAM ** UACC(READ) ADDMEM('SYS1.LINKLIB'//NOPADCHK)
- RALTER PROGRAM ** UACC(READ) ADDMEM('SYS1.CSSLIB'//NOPADCHK)
- RALTER PROGRAM ** UACC(READ) ADDMEM('CEE.SCEERUN'//NOPADCHK)
- RALTER PROGRAM ** UACC(READ) ADDMEM('CEE.SCEERUN2'//NOPADCHK)
- RALTER PROGRAM ** UACC(READ) ADDMEM('ISP.SISPLOAD'//NOPADCHK)
- SETROPTS WHEN(PROGRAM) REFRESH

Note: Do not use the ** profile if you already have a * profile in the PROGRAM class. The profile obscures and complicates the search path used by your security software. In this case, you must merge the existing * and the new ** definitions. Use the ** profile, as documented in *Security Server RACF Security Administrator's Guide* (SA22-7683).

The following additional prerequisite libraries must be made program controlled to support the use of optional services. This list does not include data sets that are specific to a product that z/OS Explorer interacts with.

- System load library, for encrypted communication
  - SYS1.SIEALNKE

Note: Libraries that are designed for LPA placement also require program control authorizations if they are accessed through LINKLIST or STEPLIB. This publication documents the usage of the following LPA libraries:

- ISPF, for ISPF Gateway
  - ISP.SISPLPA
- REXX runtime library
  - REXX.*.SEAGLPA
- z/OS Explorer
  - FEK.SFEKLPA

Define the PassTicket support for RSE

The client's password or other means of identification, such as an X.509 certificate is used only to verify the identity upon connection. Afterward, PassTickets are used to maintain thread security. This step is required for clients to be able to connect.

PassTickets are system-generated passwords with a lifespan of about 10 minutes. The generated PassTickets are based on a secret key. This key is a 64-bit number (16 hexadecimal characters). In the following sample RACF commands, replace the `key16` placeholder with a user-supplied 16-character hexadecimal string that has characters 0-9 and A-F.

- `RDEFINE PTKTDATA FEKAPPL UACC(NONE) SSIGNON(KEYMASKED(key16))`
  `APPLDATA('NO REPLAY PROTECTION - DO NOT CHANGE')`
  `DATA('IBM Explorer for z/OS')`
- `RDEFINE PTKTDATA IRRPTAUTH.FEKAPPL.* UACC(NONE)`
  `DATA('IBM Explorer for z/OS')`
- `PERMIT IRRPTAUTH.FEKAPPL.* CLASS(PTKTDATA) ACCESS(UPDATE) ID(STCRSE)`
- `SETROPTS RACLIST(PTKTDATA) REFRESH`

RSE supports using an application ID other than `FEKAPPL`. Uncomment and customize the "`APPLID=FEKAPPL`" option in `rse.env` to activate this, as documented in "Defining extra Java startup parameters with _RSE_JAVAOPTS" on page 29. The `PTKTDATA` class definitions must match the actual application ID used by RSE.

You should not use `OMVSAPPL` as application ID, because it will open the secret key to most z/OS UNIX applications. You should also not use the default MVS application ID, which is `MVS` followed by the system's SMF ID, because this will open the secret key to most MVS applications, including user batch jobs.

Note:

- If the `PTKTDATA` class is already defined, verify that it is defined as a generic class before creating the profiles listed above. The support for generic characters in the `PTKTDATA` class is new since z/OS release 1.7, with the introduction of a Java interface to PassTickets.
- Substitute the wildcard (*) in the `IRRPTAUTH.FEKAPPL.*` definition with a valid user ID mask to limit the user IDs for which RSE can generate a PassTicket.
- Depending on your RACF settings, the user defining a profile might also be on the access list of the profile. Remove this permission for the `PTKTDATA` profiles.
- JES Job Monitor and RSE must have the same application ID to allow JES Job Monitor to evaluate the PassTickets presented by RSE. For JES Job Monitor, the application ID is set in the `FEJJCNFG` configuration file with the `APPLID` directive.
- If the system has a cryptographic product installed and available, you can encrypt the secured signon application key for added protection. To do so, use the `KEYENCRYPTED` keyword instead of `KEYMASKED`. For more information, see *Security Server RACF Security Administrator's Guide* (SA22-7683).

Attention: The client connection request fails if PassTickets are not set up correctly.

Define z/OS UNIX file access permission for RSE

The **MODIFY LOGS** operator command uses the RSED started task user ID to collect host logs and setup information. And by default, user log files are created with secure file access permissions (only owner has access). To be able to collect secure user log files, the RSED started task user ID must be permitted to read them.

The `OWNER` argument of the **MODIFY LOGS** operator command results in the specified user ID becoming the owner of the collected data. In order to change ownership, the RSED started task user ID must be permitted to use the CHOWN z/OS UNIX service.

- `RDEFINE UNIXPRIV SUPERUSER.FILESYS UACC(NONE) DATA('OVERRIDE UNIX FILE ACCESS RESTRICTIONS')`
- `RDEFINE UNIXPRIV SUPERUSER.FILESYS.CHOWN UACC(NONE) DATA('OVERRIDE UNIX CHANGE OWNER RESTRICTIONS')`
- `PERMIT SUPERUSER.FILESYS CLASS(UNIXPRIV) ACCESS(READ) ID(STCRSE)`
- `PERMIT SUPERUSER.FILESYS.CHOWN CLASS(UNIXPRIV) ACCESS(READ) ID(STCRSE)`
- `SETROPTS RACLIST(UNIXPRIV) REFRESH`

Note that when the `SUPERUSER.FILESYS.ACLOVERRIDE` profile is defined, access permissions defined in ACL (access Control List) take precedence over the permissions granted through `SUPERUSER.FILESYS`. The RSED started task user ID will need READ access permit to the `SUPERUSER.FILESYS.ACLOVERRIDE` profile to bypass ACL definitions.

Define the application protection for RSE

During client logon, RSE daemon verifies that a user is allowed to use the application.

- `RDEFINE APPL FEKAPPL UACC(READ) DATA('IBM Explorer for z/OS')`
- `SETROPTS RACLIST(APPL) REFRESH`

Note:

- As described in more detail in "Define the PassTicket support for RSE" on page 64, RSE supports the using of an application ID other than `FEKAPPL`. The `APPL` class definition must match the actual application ID used by RSE.
- The client connection request succeeds if the application ID is not defined in the `APPL` class.
- The client connection request will fail only if the application ID is defined and the user lacks READ access to the profile.

Define the JES command security

JES Job Monitor issues all JES operator commands requested by a user through an extended MCS (EMCS) console, whose name is controlled with the `CONSOLE_NAME` directive, as documented in "FEJJCNFG, the JES Job Monitor configuration file" on page 17.

The following sample RACF commands give z/OS Explorer users conditional access to a limited set of JES commands, which are Hold, Release, Cancel, and Purge. Users have only execution permission if they issue the commands through JES Job monitor. Replace the `#console` placeholder with the actual console name.

- `RDEFINE OPERCMDS MVS.MCSOPER.#console UACC(READ) DATA('IBM Explorer for z/OS')`
- `RDEFINE OPERCMDS JES%.** UACC(NONE)`
- `PERMIT JES%.** CLASS(OPERCMDS) ACCESS(UPDATE) WHEN(CONSOLE(JMON)) ID(*)`
- `SETROPTS RACLIST(OPERCMDS) REFRESH`

Note:

- Usage of the console is permitted if no `MVS.MCSOPER.#console` profile is defined.
- The `CONSOLE` class must be active for `WHEN(CONSOLE(JMON))` to work, but there is no actual profile check in the `CONSOLE` class for EMCS consoles.
- Do not replace `JMON` with the actual console name in the `WHEN(CONSOLE(JMON))` clause. The `JMON` keyword represents the point-of-entry application, not the console name.

Attention: Defining JES commands with universal access `NONE` in your security software might impact other applications and operations. Test the security before activating it on a production system.

Table 13 and Table 14 show the operator commands issued for JES2 and JES3, and the discrete security profiles that can be used to protect them.

Table 13. JES2 Job Monitor operator commands

Action	Command	OPERCMDS profile	Required access

Hold	`$Hx(jobid)`
	
	with x = {J, S or T}
		`jesname.MODIFYHOLD.BAT`
		`jesname.MODIFYHOLD.STC`
		`jesname.MODIFYHOLD.TSU`
			`UPDATE`

Release	`$Ax(jobid)`
	
	with x = {J, S or T}
		`jesname.MODIFYRELEASE.BAT`
		`jesname.MODIFYRELEASE.STC`
		`jesname.MODIFYRELEASE.TSU`
			`UPDATE`

Cancel	`$Cx(jobid)`
	
	with x = {J, S or T}
		`jesname.CANCEL.BAT`
		`jesname.CANCEL.STC`
		`jesname.CANCEL.TSU`
			`UPDATE`

Purge	`$Cx(jobid),P`
	
	with x = {J, S or T}
		`jesname.CANCEL.BAT`
		`jesname.CANCEL.STC`
		`jesname.CANCEL.TSU`
			`UPDATE`

Table 14. JES3 Job Monitor operator commands

Action	Command	OPERCMDS profile	Required access
Hold	`*F,J=jobid,H`	`jesname.MODIFY.JOB`	`UPDATE`
Release	`*F,J=jobid,R`	`jesname.MODIFY.JOB`	`UPDATE`
Cancel	`*F,J=jobid,C`	`jesname.MODIFY.JOB`	`UPDATE`
Purge	`*F,J=jobid,C`	`jesname.MODIFY.JOB`	`UPDATE`

Note:

- The Hold, Release, Cancel, and Purge JES operator commands, and the Show JCL command, can be executed only against spool files owned by the client user ID, unless `LIMIT_COMMANDS=` with value `LIMITED` or `NOLIMIT` is specified in the JES Job Monitor configuration file. For more information, see "Actions against jobs - target limitations" in the *Host Configuration Reference Guide* (SC27-8438).

- Users can browse any spool file, unless LIMIT_VIEW=USERID is defined in the JES Job Monitor configuration file. For more information, see "Access to spool files" in *Host Configuration Reference Guide* (SC27-8438).
- Even if users are not authorized for these operator commands, they will still be able to submit jobs and read job output through JES Job Monitor if they have sufficient authority to possible profiles that protect these resources, such as those in the JESINPUT, JESJOBS and JESSPOOL classes.

Assuming the identity of the JES Job Monitor server by creating a JMON console from a TSO session is prevented by your security software. Even though the console can be created, the point of entry is different; for example, JES Job Monitor versus TSO. JES commands issued from this console will fail the security check if your security is set up as documented in this publication and the user does not have authority to the JES commands through other means.

Define the data set profiles

READ access for users and ALTER for system programmers is sufficient for most z/OS Explorer data sets. Replace the #sysprog placeholder with valid user IDs or RACF group names. Also, ask the system programmer who installed and configured the product for the correct data set names. FEK is the default high-level qualifier used during installation and FEK.#CUST is the default high-level qualifier for data sets created during the customization process.

```
• ADDGROUP (FEK) OWNER(IBMUSER) SUPGROUP(SYS1)
  DATA('IBM Explorer for z/OS - HLQ STUB')
• ADDSD  'FEK.*.**' UACC(READ)
  DATA('IBM Explorer for z/OS')
• PERMIT 'FEK.*.**' CLASS(DATASET) ACCESS(ALTER) ID(#sysprog)
• SETROPTS GENERIC(DATASET) REFRESH
```

Note:

- Protect FEK.SFEKAUTH against updates because this data set is APF-authorized. The same is true for FEK.SFEKLPA, but here because this data sets is program controlled.
- The sample commands in this publication and in the FEKRACF job assume that Enhanced Generic Naming (EGN) is active. When EGN is active, the ** qualifier can be used to represent any number of qualifiers in the DATASET class. Substitute ** with * if EGN is not active on your system. For more information about EGN, see *Security Server RACF Security Administrator's Guide* (SA22-7683).

Verify the security settings

Use the following sample commands to display the results of your security-related customizations.

- Security settings and classes
  - SETROPTS LIST
- OMVS segment for users
  - LISTUSER #userid NORACF OMVS
  - LISTGRP #group-name NORACF OMVS
- Started tasks
  - LISTGRP STCGROUP OMVS
  - LISTUSER STCJMON OMVS
  - LISTUSER STCRSE   OMVS

  - `RLIST STARTED JMON.*  ALL STDATA`
  - `RLIST STARTED RSED.*  ALL STDATA`
- RSE as a secure z/OS UNIX server
  - `RLIST FACILITY BPX.SERVER ALL`
- MVS program controlled libraries for RSE
  - `RLIST PROGRAM ** ALL`
- PassTicket support for RSE
  - `RLIST PTKTDATA FEKAPPL ALL SSIGNON`
  - `RLIST PTKTDATA IRRPTAUTH.FEKAPPL.* ALL`
- Application protection for RSE
  - `RLIST APPL FEKAPPL ALL`
- z/OS UNIX file access permission for RSE
  - `RLIST   UNIXPRIV SUPERUSER.FILESYS ALL`
  - `RLIST   UNIXPRIV SUPERUSER.FILESYS.CHOWN ALL`
- JES command security
  - `RLIST CONSOLE JMON ALL`
  - `RLIST OPERCMDS MVS.MCSOPER.JMON ALL`
  - `RLIST OPERCMDS JES%.** ALL`
- Data set profiles
  - `LISTGRP FEK`
  - `LISTDSD PREFIX(FEK) ALL`

Optionally, profiles can exist that direct the z/OS Explorer behavior for a specific user. These profiles match the `FEK.**` filter and are by default located in the `FACILITY` class. See the `_RSE_FEK_SAF_CLASS` directive in `rse.env`. You can use the **SEARCH** command to list the profile names. Use the **RLIST** command to show the details for a profile.

- `SEARCH CLASS(FACILITY) FILTER(FEK.**)`
- `RLIST FACILITY #profile-name ALL`

Chapter 6. Migration guide

Migration considerations

This section highlights installation and configuration changes compared to previous releases of the product. It also gives some general guidelines to migrate to this release. For more information, see the related sections in this manual.

- If you are a previous user of IBM Explorer for z/OS, save the related customized files before upgrading to this version of IBM Explorer for z/OS .
- If you plan on running multiple instances of z/OS Explorer, read "Running multiple instances" in the *Host Configuration Reference Guide* (SC27-8438).
- If your migration scenario spans more than two releases, you should do the customizations again, as if there is no older release present.

Backing up the previously configured files

If you are a previous user of z/OS Explorer, save the related customized files before installing this version of IBM Explorer for z/OS.

Customizable z/OS Explorer files can be found at the following locations:

- `FEK.#CUST.FEK*.**`, Configuration Utility work files
- `FEK.SFEKSAMP`, some members are copied to `FEK.#CUST.*` by the `FEKSETUP` sample job, where `*` equals `PARMLIB`, `PROCLIB`, `JCL`, and `CNTL`.
- `/usr/lpp/IBM/zexpl/samples/`, some files are copied to `/etc/zexpl/` by the `FEKSETUP` sample job

Migrate from version 3.0 to version 3.1

These notes are for a migration from a base version 3.0 to version 3.1. It includes changes that are already documented as part of version 3.0 maintenance. The changes that are part of the maintenance stream, and thus possibly already implemented, are marked with the release where they were introduced.

- The default SMP/E install location for MVS and z/OS UNIX components did not change and remain `FEK.*` and `/usr/lpp/IBM/zexpl/*`.
- Since version 3.0.1.7
  - RSE: New operator commands have been added:
    - F rsed,APPL=LOGS {RANGE | R}=hh
- Since version 3.0.1.6
  - RSE: Optional directives have been added to rse.env:
    - _RSE_JAVAOPTS -DDISABLE_MIGRATE_HRECALL_HDELETE
- Since version 3.0.1.5
  - RSE: Optional directives have been added to rse.env:
    - _RSE_UMASK
- Since version 3.0.1.0
  - RSE: Optional directives have been added to rse.env:
    - GSK_FIPS_STATE
    - _RSE_JAVAOPTS -Dsearch.server.limit.MaxFilterResults

In order to increase the Java heap available to users, the default value of `maximum.clients` has changed from 30 to 10 and the default value of `maximum.threads` has changed from 600 to 250.

Configurable files

Table 15 shows an overview of files that are customized in version 3.1. The z/OS Explorer sample libraries, `FEK.SFEKSAMP`, `FEK.SFEKSAMV` and `/usr/lpp/IBM/zexpl/samples/`, contain more customizable members than listed here, such as sample user exits.

Note: Sample job `FEKSETUP` copies all listed members to different data sets and directories, default `FEK.#CUST.*` and `/etc/zexpl/*`.

Table 15. Version 3.1 customizations

Member/File	Default location	Purpose	Migration notes
FEKSETUP	FEK.SFEKSAMP [FEK.#CUST.JCL]	JCL to create data sets and directories, and populate them with customizable files	None
JMON	FEK.SFEKSAMP(FEJJJCL) [FEK.#CUST.PROCLIB]	JCL for JES Job Monitor	None
FEJJJCL	FEK.SFEKSAMP [FEK.#CUST.PROCLIB(JMON)]	Name for JMON member	See JMON member
RSED	FEK.SFEKSAMP(FEKRSED) [FEK.#CUST.PROCLIB]	JCL for RSE daemon	None
FEKRSED	FEK.SFEKSAMP [FEK.#CUST.PROCLIB(RSED)]	Name for RSED member	See RSED member
FEKRACF	FEK.SFEKSAMP [FEK.#CUST.JCL]	JCL for security definitions	None
FEJJCNFG	FEK.SFEKSAMP [FEK.#CUST.PARMLIB]	JES Job Monitor configuration file	None
FEJTSO	FEK.SFEKSAMP [FEK.#CUST.CNTL]	JCL for TSO submits	None
rse.env	/usr/lpp/IBM/zexpl/samples/ [/etc/zexpl/]	RSE environment variables	Optional variables added
ISPF.conf	/usr/lpp/IBM/zexpl/samples/ [/etc/zexpl/]	ISPF Legacy Gateway configuration file	None
ssl.properties	/usr/lpp/IBM/zexpl/samples/ [/etc/zexpl/]	RSE encrypted communication configuration file	None

Table 15. Version 3.1 customizations (continued)

Member/File	Default location	Purpose	Migration notes
`rsecomm.properties`	`/usr/lpp/IBM/zexpl/samples/ [/etc/zexpl/]`	RSE trace configuration file	None
`pushtoclient.properties`	`/usr/lpp/IBM/zexpl/samples/ [/etc/zexpl/]`	Push information to the client configuration file	None

Chapter 7. Operator commands

This chapter provides an overview of the available operator (or console) commands for z/OS Explorer. If you are unfamiliar with the syntax diagrams used to explain the command format, see How to read a syntax diagram.

Start (S)

Use the **START** command to dynamically start a started task (STC). The abbreviated version of the command is the letter S.

JES Job Monitor

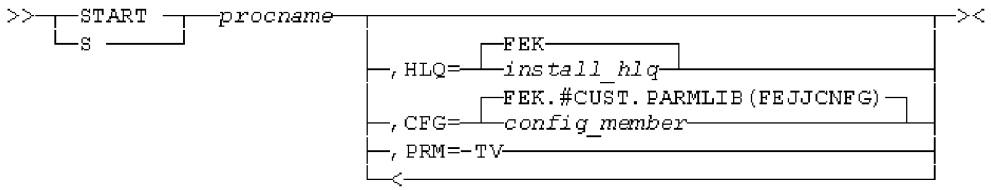


Figure 11. START JMON operator command

procname
The name of the member in a procedure library that is used to start the server. The default name used during the host system configuration is `JMON`.

HLQ=install_hlq
High-level qualifier used to install z/OS Explorer. The default is `FEK`.

CFG=config_member
Absolute data set and member name of the JES Job Monitor configuration file. The default is `FEK.#CUST.PARMLIB(FEJJCNFG)`. If this variable is set to `NULLFILE`, JES Job Monitor will use default configuration values.

PRM=-TV
Enable verbose (trace) mode. Tracing will cause performance degradations and should only be done under the direction of the IBM support center.

RSE daemon

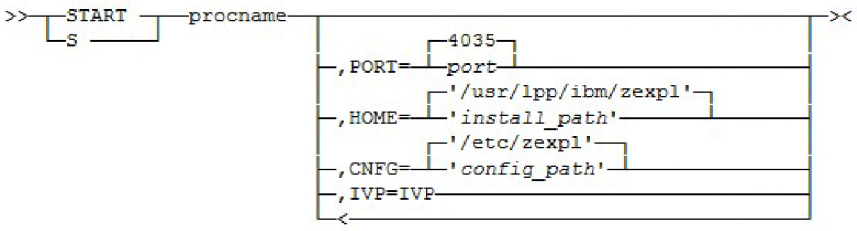


Figure 12. START RSED operator command

procname
The name of the member in a procedure library that is used to start the server. The default name used during the host system configuration is `RSED`.

PORT=port
The port used by the RSE daemon for the clients to connect. If not specified, the port defined in `/etc/zexpl/rse.env` in the variable `_RSE_RSED_PORT` is used. The default is `4035`.

IVP=IVP
Do not start the server but run the RSE daemon installation verification program (IVP).

CNFG='config_path'
Absolute location of the configuration files stored in z/OS UNIX. The default is `'/etc/zexpl'`. The z/OS UNIX path is case-sensitive and must be enclosed in single quotation marks (') to preserve lowercase characters.

HOME='install_path'
Path prefix and the mandatory `/usr/lpp/IBM/zexpl` used to install z/OS Explorer. The default is `'/usr/lpp/IBM/zexpl'`. The z/OS UNIX path is case-sensitive and must be enclosed in single quotation marks (') to preserve lowercase characters.

Modify (F)

The **`MODIFY`** command can be used to dynamically query and change the characteristics of an active task. The abbreviated version of the command is the letter `F`.

JES Job Monitor

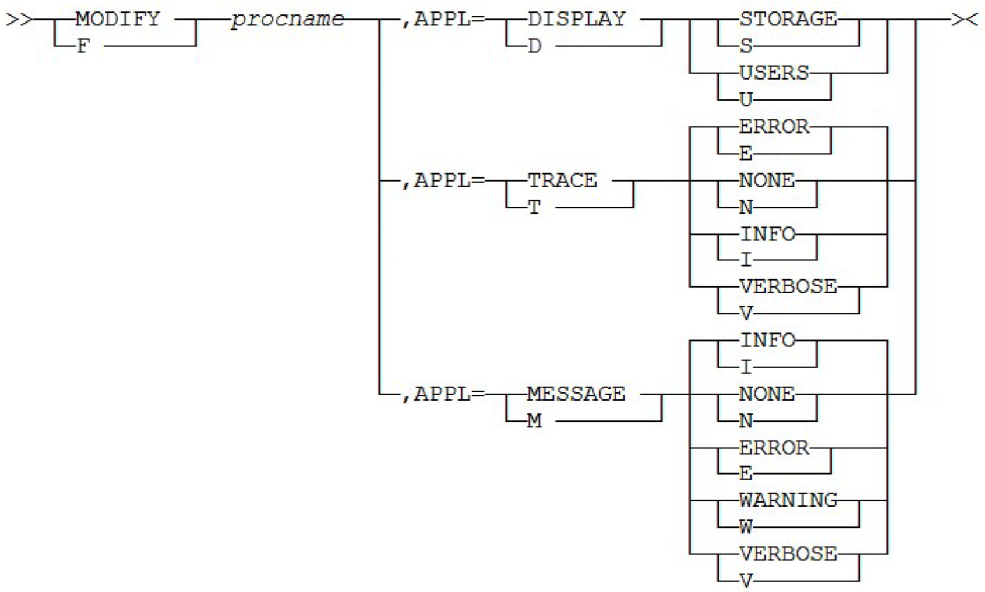


Figure 13. MODIFY JMON operator command

procname
The name of the member in a procedure library that was used to start the server. The default name used during the host system configuration is JMON.

DISPLAY STORAGE
Write a storage usage report to DD SYSOUT. A message "JMON storage information written to SYSOUT" is written to the console with message ID BPXM023I. The storage usage report shows various storage-related fields with sizes in bytes, kilobytes, and megabytes.

```
>>>STORAGE TRACE (console request)<<<
LDAREGRQ    00000000000 00000000K 00000M requested region size
  below 16M line
LDASIZA     00006266880 00006120K 00005M maximum region size
LDALIMIT    00006266880 00006120K 00005M limit
LDAVVRG     00006266880 00006120K 00005M getmain limit
LDALOAL     00000061440 00000060K 00000M in use
LDAHIAL     00000266240 00000260K 00000M LSQA/SWA/private subpools
_GAP        00000000000 00000000K 00000M gaps in allocation
_AVAIL      00005939200 00005800K 00005M available (including gaps)
_MAX        00006000640 00005860K 00005M current limit
  above 16M line
LDAESIZA    01905262592 01860608K 01817M maximum region size
LDAELIM     01905262592 01860608K 01817M limit
LDAEVVRG    01905262592 01860608K 01817M getmain limit
LDAELOAL    00000937984 00000916K 00000M in use
LDAEHIAL    00012754944 00012456K 00012M ELSQA/ESWA/private subpools
_EGAP       00000000000 00000000K 00000M gaps in allocation
_EAVAIL     01891569664 01847236K 01803M available (including gaps)
_EMAX       01892507648 01848152K 01804M current limit
```

DISPLAY USERS
Write a list of active users to DD SYSOUT. A message "JMON user list written to SYSOUT" is written to the console with message ID BPXM023I. The user list shows various user-related data, including CPU usage.

```
S0   userid    USER     4:04(elapsed)     4:04(idle)
Users: 1
```

TRACE {NONE | ERROR | INFO | VERBOSE}
Control the detail level of the JES Job Monitor trace log (DD SYSOUT). The default is E (Error). A message "JMON TRACE LEVEL:{NONE | ERROR | INFO | VERBOSE}" is written to the console with message ID BPXM023I.

Table 16. Detail levels of the JES Job Monitor trace log. This table lists the detail levels of the JES Job Monitor trace log and their descriptions.

Detail level	Description
N or NONE	Startup messages only
E or ERROR	Startup and Error messages only (default)
I or INFO	Startup, Error, and Informational messages
V or VERBOSE	Startup, Error, Informational, and Verbose messages

Detailed tracing will cause performance degradations and should only be done under the direction of the IBM support center.

MESSAGE {NONE | ERROR | WARNING | INFO | VERBOSE}
Control the detail level of the JES Job Monitor message log (DD

SYSPRINT). The default is `I` (Informational). A message `"JMON MESSAGE LEVEL:{NONE | ERROR | WARNING | INFO | VERBOSE}"` is written to the console with message ID BPXM023I.

Table 17. Detail levels of the JES Job Monitor message log. This table lists the detail levels of the JES Job Monitor message log and their descriptions.

Detail level	**Description**
N or NONE	No messages
E or ERROR	Error messages only
W or WARNING	Error and Warning messages
I or INFO	Error, Warning, and Informational messages (default)
V or VERBOSE	Error Warning, Informational, and Verbose messages

Detailed tracing will cause performance degradations and should only be done under the direction of the IBM support center.

RSE daemon

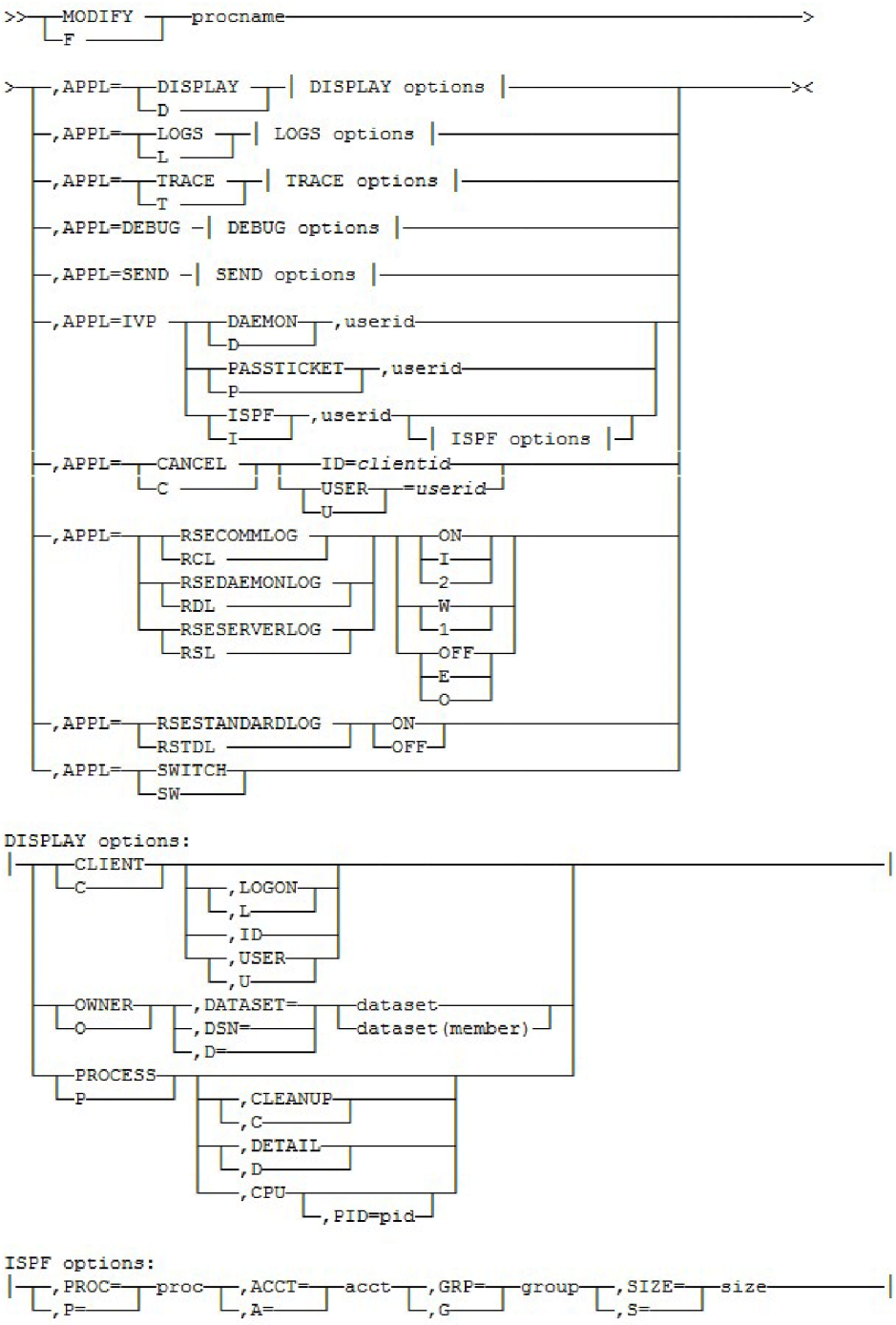


Figure 14. MODIFY RSED operator command

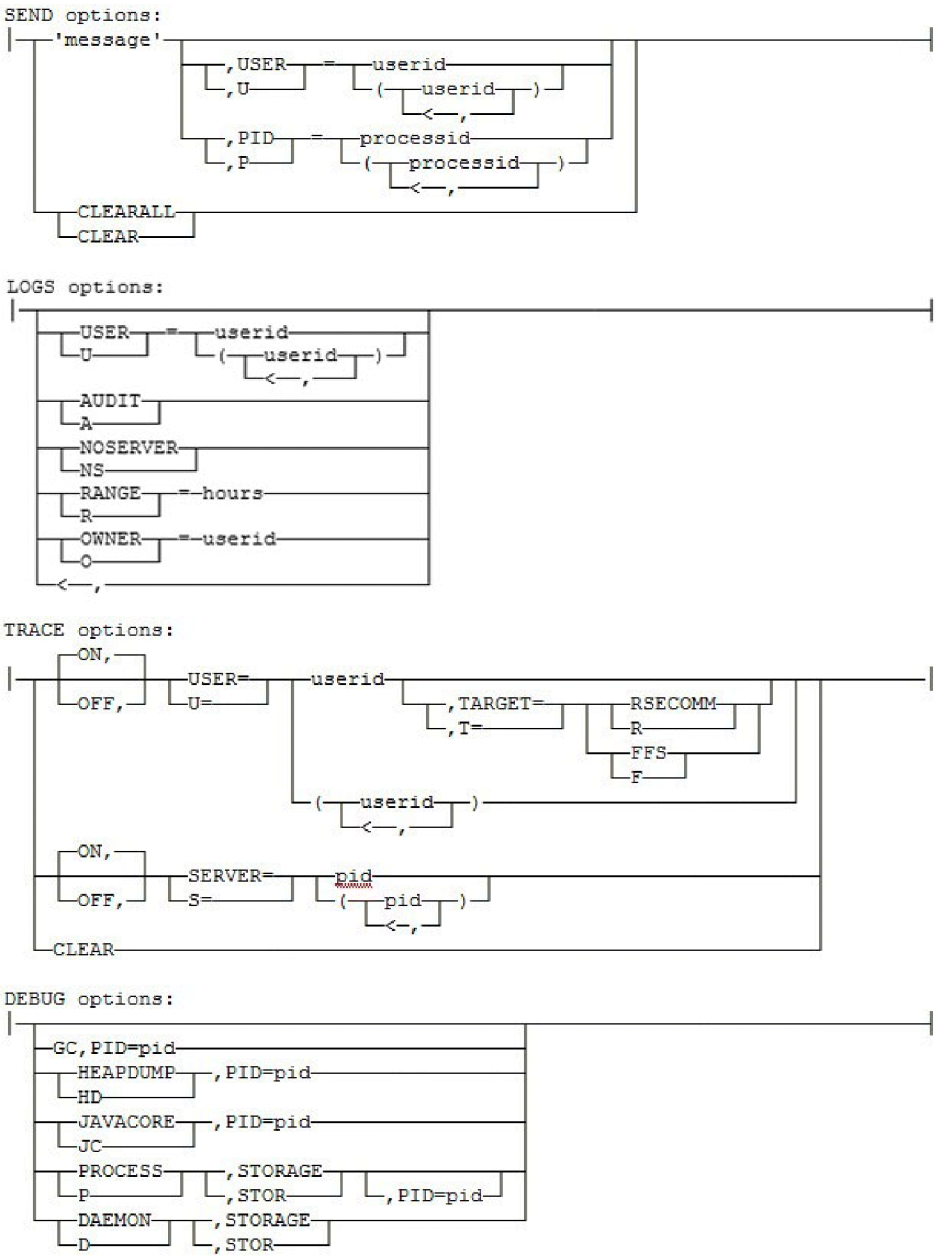


Figure 15. MODIFY RSED operator command (continued)

procname

The name of the member in a procedure library that was used to start the server. The default name used during the host system configuration is `RSED`.

DISPLAY CLIENT[{,LOGON | ,ID | ,USER}]

Display the active clients in a single BPXM023I message. The result layout depends on the command option that was used. You can change the sorting order with the optional command arguments.

- No command option: Clients are grouped by the thread pool process that serves them.

  ```
  ProcessId(<processid>) ASId(<asid>) JobName(<jobname>)
  Clients(<local>/<total>) Order(<startup order>)
  <clientid><userid><connected since>
  ```

- LOGON command option: Clients are ordered by logon time.

```
LOGON TIME------------------ ID----- USERID--
<connected since>         <clientid> <userid>
```

- ID command option: Clients are ordered by client ID. Each session has a unique client ID, even if the related user ID is the same.

```
ID----- USERID-- LOGON TIME------------------
<clientid> <userid> <connected since>
```

- USER command option: Clients are ordered by user ID.

```
USERID-- ID----- LOGON TIME------------------
<userid> <clientid> <connected since>
```

DISPLAY OWNER,DATASET={dataset | dataset(member)}

Display the data set enqueue owner in a single BPXM023I message.

```
FEK217I <dataset[(member)]> is locked by <userid>
FEK218I <dataset[(member)]> is not locked
FEK219E Failed to determine lock owner for <dataset[(member)]>
```

- The server also reports the locks held by other products, such as ISPF.
- The **D GRS,RES=(*,dataset)** operator command is unable to tell which z/OS Explorer user is the actual enqueue holder, all it can tell you is the threadpool in which the user is active.

DISPLAY PROCESS[{,CLEANUP | ,CPU [,PID=pid] | ,DETAIL}]

Display the RSE thread pool processes in one or more BPXM023I messages. There can be multiple processes, which are used for load balancing the connected users.

```
ProcessId(<processid>) Memory Usage(<java heap usage>%)
  Clients(<number of clients>) Order(<startup order>) <error status>
```

Note:

- `<processid>` can be used in process-specific z/OS UNIX operator commands.
- Each process has its own Java heap, whose size can be set in `rse.env`. The reported Java heap usage includes storage that is released by z/OS Explorer, but which is not yet freed by the Java garbage collection process.
- `<startup order>` is a sequential number that indicates the order that the thread pools were started. The number corresponds to the number used in the filename of the `stderr.*.log` and `stdout.*.log` files.

In normal situations, `<error status>` is blank. Table 18 documents the possible non-blank values for `<error status>`.

Table 18. Thread pool error status. This table lists the thread pool error status and their descriptions.

Status	Description
severe error	The thread pool process encountered an unrecoverable error and halted operations. The other status fields show the last known values. To remove this entry from the table, use the CLEANUP option of the **DISPLAY PROCESS** modify command.

Table 18. Thread pool error status (continued). This table lists the thread pool error status and their descriptions.

Status	Description
killed process	The thread pool process was killed by Java, z/OS UNIX or an operator command. The other status fields show the last known values. To remove this entry from the table, use the CLEANUP option of the **DISPLAY PROCESS** modify command.
timeout	The thread pool process did not respond in a timely manner to RSE daemon during a client connect request. The other status fields show the current values. The thread pool is excluded for future client connect requests. The *timeout* status is reset when a client served by this thread pool logs off.
rejectLogon	The thread pool temporarily will not accept logon requests due to a heavy workload. Note that the logon request will be honored by another thread pool. Once the resource intensive task - for example, uploading a large file to a client - has completed, the *rejectLogon* status is reset.

More information is provided when the DETAIL option of the **DISPLAY PROCESS** modify command is used:

```
ProcessId(33555087) ASId(002E) JobName(RSED8) Order(1)
 PROCESS LIMITS:    CURRENT  HIGHWATER      LIMIT
  JAVA HEAP USAGE(%)     10         56        100
  CLIENTS                 0         25         30
  MAXFILEPROC            83        103      64000
  MAXPROCUSER            97         99        200
  MAXTHREADS              9         14       1500
  MAXTHREADTASKS          9         14       1500
 REGION LIMITS:     CURRENT  HIGHWATER      LIMIT
  PRIVATE < 16M       72.0K          -       6.7M (6.9M)
  PRIVATE > 16M      610.8M          -    1731.0M (1811.0M)
  PRIVATE > 2G         2.0M       2.0M    NOLIMIT
```

The ASId field is the address space ID, in hexadecimal notation. The process limits table shows the current resource usage, the high-water mark for the resource usage, and the resource limit. Due to other limiting factors, the defined limit might never be reached. The region limits table shows the current private storage usage below the 16MB line, between the 16 MB line and the 2GB bar, and above the 2GB bar. The limits column shows a calculated limited, with the absolute number mentioned in braces. If storage usage is capped, then this will also be mentioned.

The CPU option of the **DISPLAY PROCESS** modify command shows the accumulated CPU usage, in milliseconds, of each thread in a thread pool. Every thread pool has a BPXM023I message. By default, all thread pools report the CPU usage, but you can limit the scope to a single thread pool by specifying `PID=pid` on the operator command, where `pid` is the process ID of the target thread pool.

```
ProcessId(421     ) ASId(007D) JobName(RSED8) Order(1)
USERID   THREAD-ID        TCB@     ACC_TIME TAG
STCRSE   0EDE540000000000 005E6B60      822 1/ThreadPoolProcess
STCRSE   0EDE870000000001 005E69C8      001
```

```
STCRSE   0EDE980000000002 005E6518     1814
STCRSE   0EDEBA0000000003 005E66B0     2305
STCRSE   0EDECB0000000004 005E62F8      001
STCRSE   0EDEDC0000000005 005E60D8      001
STCRSE   0EDF860000000006 005C2BF8      628 6/ThreadPoolMonitor$Memory
UsageMonitor
STCRSE   0EDF970000000007 005C2D90      003 7/ThreadPoolMonitor
STCRSE   0EDFDB0000000008 005C29D8      001
STCRSE   0EE22E000000000E 005C1BE0      070
IBMUSER  0EE0EB0000000011 005C22B8      276 20/ServerReceiver
IBMUSER  0EE2500000000012 005C19C0      137 16/ServerUpdateHandler
IBMUSER  0EE2610000000013 005C17A0      509 15/ServerCommandHandler
IBMUSER  0EE1840000000014 005C1E00      065 21/ZosSystemMiner
STCRSE   0EE1510000000016 005C2098      078
STCRSE   0EE1950000000017 005C1580      001
IBMUSER  0EE23F0000000018 005C1360      021 26/UniversalFileSystemMine
r
IBMUSER  0EE2A5000000001C 005C0CF0      003 27/EnvironmentMiner
IBMUSER  0EE283000000001D 005C1140      002 31/CommandMiner
IBMUSER  0EE272000000001E 005C0E88      081 32/MVSFileSystemMiner
IBMUSER  0EE294000000001F 005C0AD0      002 33/MVSByteStreamHandler$Op
enCloseThread
STCRSE   0EE2E90000000023 005C0470      001
IBMUSER  0EE2C70000000024 005C08B0      050 38/JESMiner
```

If the output size exceeds the maximum number of lines for a console message, the output is split over multiple BPXM023I messages. These additional messages have the same header as the first message, but with the `CONTINUATION` keyword added to the first line.

```
ProcessId(421     ) ASId(007D) JobName(RSED8) Order(1) CONTINUATION
USERID   THREAD-ID        TCB@     ACC_TIME TAG
```

The output is limited to the first 4000 threads for each thread pool.

SEND 'message'[,USER={userid | (userid,userid,...)}]
Send a message to one, some, or all z/OS Explorer users. By default the message is sent to all users. Users that are currently active receive the message immediately, others receive it on the next logon.

SEND 'message'[,PID={processid | (processid,processid,...)}]
Send a message to all users in one, some, or all thread pools. By default the message is sent to all thread pools. Thread pools are identified by their process ID.

SEND CLEARALL
Clear the buffer holding all messages to be delivered to users logging on.

CANCEL ID=clientid
Cancel a client connection based on the client ID, which is shown in the **`DISPLAY CLIENT`** modify command. Each session has a unique client ID, even if the related user ID is the same.

When a client connection is cancelled, the host system threads go through normal termination processing to clean up resources used by them. This action implies that some threads can take a few minutes before they end; for example, because they are waiting on the keep-alive mechanism to time out.

CANCEL USER=userid
Cancel a client connection based on the client's user ID, which is shown in the **`DISPLAY CLIENT`** modify command.

When a client connection is cancelled, the host system threads go through normal termination processing to clean up resources used by them. This

action implies that some threads can take a few minutes before they end; for example, because they are waiting on the keep-alive mechanism to time out.

LOGS [USER={userid | (userid,userid,...)},]
[AUDIT,][NOSERVER,][RANGE=hours,][OWNER=userid,]

Collect z/OS Explorer host logs and setup information. The collected data is placed in a z/OS UNIX file, `$TMPDIR/feklogs%sysname.%jobname`, where `$TMPDIR` is the value of the TMPDIR directive in `rse.env` (default `/tmp`), `%sysname` is your z/OS system name and `%jobname` is the name of the RSED started task. Results are shown in a single FEK201I console message.

```
FEK220I Host logs are written onto /tmp/feklogs.CDFMVS08.RSED.log
```

By default, only the server logs are collected. The following command options allow you to collect different logs.

Table 19. Command options. This table lists the options of the command that collects host logs and setup information.

Option	Description
USER	Collect log files for the specified user ID's
AUDIT	Collect audit logs
NOSERVER	Do not collect server logs

By default, all available log files are collected. The **RANGE** command option allows you to limit this selection to those log files that were updated in the last given number of hours.

z/OS Explorer will query your security product for access permits to `FEK.CMD.LOGS.**` profiles to determine if the requestor is allowed to collect the specified logs. By default, the requestor is the RSED started task user ID, unless the `OWNER` option is specified. Only the requestor has access to the file holding the collected data.

RSECOMMLOG {ON | OFF | I | W | E | 2 | 1 | 0}

Control the trace detail level for RSE server (`rsecomm.log`) and the MVS data set services (`lock.log` and `ffs*.log`). The startup default is defined in `rsecomm.properties`. The following detail levels are available.

Table 20. Trace detail levels for RSE server (`rsecomm.log`) and the MVS data set services (`lock.log` and `ffs*.log`). This table lists the trace detail levels for RSE server (`rsecomm.log`) and the MVS data set services (`lock.log` and `ffs*.log`).

Detail level	Description
E or 0 or OFF	Error messages only.
W or 1	Error and warning messages. This is the default setting in `rsecomm.properties`.
I or 2 or ON	Error, warning, and informational messages.

Detailed tracing will cause performance degradations and should only be done under the direction of the IBM support center.

RSEDAEMONLOG {ON | OFF | I | W | E | 2 | 1 | 0}

Control the trace detail level for RSE daemon (`rsedaemon.log`). The startup default is defined in `rsecomm.properties`. The following detail levels available.

Table 21. Trace detail levels for RSE daemon (rsedaemon.log). This table lists the trace detail levels for RSE daemon (rsedaemon.log).

Detail level	Description
E or 0 or OFF	Error messages only.
W or 1	Error and warning messages. This is the default setting in rsecomm.properties.
I or 2 or ON	Error, warning, and informational messages.

Detailed tracing will cause performance degradations and should only be done under the direction of the IBM support center.

RSESERVERLOG {ON | OFF | I | W | E | 2 | 1 | 0}
Control the trace detail level for RSE thread pools (rseserver.log). The startup default is defined in rsecomm.properties. The following detail levels are available.

Table 22. Trace detail levels for RSE thread pools (rseserver.log). This table lists the trace detail levels for RSE thread pools (rseserver.log).

Detail level	Description
E or 0 or OFF	Error messages only.
W or 1	Error and warning messages. This is the default setting in rsecomm.properties.
I or 2 or ON	Error, warning, and informational messages.

Detailed tracing will cause performance degradations and should only be done under the direction of the IBM support center.

RSESTANDARDLOG {ON | OFF}
Disable (OFF) or enable (ON) the updating of the log files that hold the stdout and stderr streams of the stdout.*.log and stderr.*.log thread pools. The startup default is defined by the enable.standard.log directive in rse.env.

Detailed tracing will cause performance degradations and should only be done under the direction of the IBM support center.

TRACE [{ON, | OFF,}]USER=userid[,TARGET={FFS | RSECOMM}]
Enable (ON) or disable (OFF) tracing for the specified user IDs. The default is ON. This setting overrules the default setting controlled by the **MODIFY RSECOMMLOG** operator command. The following detail levels are available.

Table 23. Trace detail levels for the specified user IDs. This table lists the trace detail levels for the specified user IDs.

Detail level	Description
OFF	Error messages only
ON (default)	Error, warning, and informational messages.

The command alters the trace detail level for RSE server (rsecomm.log) and the MVS data set services (lock.log and ffs*.log). This can be limited with the TARGET keyword, which accepts the following values.

Table 24. Keyword values. This table lists the values of the TARGET keyword of the command.

Values	Description
FFS	Set the specified log level only for MVS data set services (lock.log and ffs*.log)
RSECOMM	Set the specified log level only for RSE server (rsecomm.log)

The command can be issued for users that are currently not logged on. The setting remains active when a user logs off and will be used again when the user logs on.

Use the USER directive in rsecomm.properties to simulate issuing the **MODIFY TRACE USER** command at server startup. Existing settings from previous **MODIFY TRACE USER** or **MODIFY TRACE SERVER** operator commands or the USER directive in rsecomm.properties will be replaced by the setting of this command.

Detailed tracing will cause performance degradations and should only be done under the direction of the IBM support center.

TRACE [{ON, | OFF,}]USER=(userid,userid,...)

Enable (ON) or disable (OFF) tracing for the specified user IDs. The default is ON. This setting overrules the default setting controlled by the **MODIFY RSECOMMLOG** operator command. The following detail levels are available.

Table 25. Trace detail levels for the specified user IDs. This table lists the trace detail levels for the specified user IDs.

Detail level	Description
OFF	Error messages only.
ON (default)	Error, warning, and informational messages.

The command alters the trace detail level for RSE server (rsecomm.log) and the MVS data set services (lock.log and ffs*.log). The command can be issued for users that are currently not logged on. The setting remains active when a user logs off and will be used again when the user logs on. Use the USER directive in rsecomm.properties to simulate issuing the **MODIFY TRACE USER** command at server startup. Existing settings from previous **MODIFY TRACE USER** or **MODIFY TRACE SERVER** operator commands or the USER directive in rsecomm.properties will be replaced by the setting of this command.

Detailed tracing will cause performance degradations and should only be done under the direction of the IBM support center.

TRACE [{ON, | OFF,}] SERVER={pid | (pid,pid,...)}

Enable (ON) or disable (OFF) tracing for all users in the specified thread pool where pid is the process ID of an RSE thread pool. The default is ON. This setting overrules the default setting controlled by the **MODIFY RSECOMMLOG** operator command. The following detail levels are available.

Table 26. Trace detail levels for all users in the specified thread pool. This table lists the trace detail levels for all users in the specified thread pool.

Detail level	Description
OFF	Error messages only.
ON (default)	Error, warning, and informational messages.

The command alters the trace detail level for RSE server (`rsecomm.log`) and the MVS data set services (`lock.log` and `ffs*.log`). Existing settings from previous **MODIFY TRACE USER** or **MODIFY TRACE SERVER** operator commands or the `USER` directive in `rsecomm.properties` will be replaced by the setting of this command.

Detailed tracing will cause performance degradations and should only be done under the direction of the IBM support center.

TRACE CLEAR

Remove all trace overrides set by the **MODIFY TRACE USER** and **MODIFY TRACE SERVER** operator commands and the `USER` directive in `rsecomm.properties`.

DEBUG HEAPDUMP,PID=pid

Request a Java Heap dump for a specified thread pool, where `pid` is the process ID of an RSE thread pool. The dump is written to the directory specified by `_CEE_DUMPTARG` in `rse.env`, where the default value is `/tmp`. Results are shown in a single BPXM023I console message.

```
JVMDUMP034I User requested Heap dump using '/tmp/heapdump.20120223.211'
430.16777590.0001.phd' through JVMRI
```

DEBUG JAVACORE,PID=pid

Request a Java Core dump for a specified thread pool, where `pid` is the process ID of an RSE thread pool. The dump is written to the directory specified by `_CEE_DUMPTARG` in `rse.env`, where the default value is `/tmp`. Results are shown in a single BPXM023I console message.

```
JVMDUMP034I User requested Java dump using '/tmp/javacore.20120223.214
244.16777590.0002.phd' through JVMRI
```

DEBUG GC,PID=pid

Request a Java Garbage Collection for a specified thread pool, where `pid` is the process ID of an RSE thread pool.

DEBUG DAEMON,STORAGE

Request an overview of current real storage usage for RSE daemon. Results are shown in a BPXM023I message. See the description of DEBUG PROCESS,STORAGE for a sample output.

DEBUG PROCESS,STORAGE [,PID=pid]

Request an overview of current real storage usage for a thread pool. Every thread pool has a BPXM023I message showing the results. By default, all thread pools report the storage usage, but you can limit the scope to a single thread pool by specifying PID=pid on the operator command, where pid is the process ID of the target thread pool. The storage usage report shows various storage-related fields with sizes in bytes, kilobytes, and megabytes. If storage usage is capped, then this will also be mentioned. A summarized version of this data is included in the output of the **DISPLAY PROCESS,DETAIL operator command**.

```
ProcessId(484     ) ASId(00C9) JobName(RSED9   ) Order(2)
  below 16M line
LDASIZA     7315456    7144.0K    6.9M maximum region size
```

```
LDALIMIT    7315456    7144.0K    6.9M limit
LDAVVRG     7315456    7144.0K    6.9M getmain limit
LDALOAL       73728      72.0K    0.0M in use
LDAHIAL      253952     248.0K    0.2M LSQA/SWA/private subpools
_GAP              0       0.0K    0.0M gaps in allocation
_AVAIL      6987776    6824.0K    6.6M available (including gaps)
_MAX        7061504    6896.0K    6.7M current limit
  above 16M line
LDAESIZA 1898971136 1854464.0K 1811.0M maximum region size
LDAELIM  1898971136 1854464.0K 1811.0M limit
LDAEVVRG 1898971136 1854464.0K 1811.0M getmain limit
LDAELOAL  639860736  624864.0K  610.2M in use
LDAEHIAL   83677184   81716.0K   79.8M ELSQA/ESWA/private subpools
_EGAP         12288      12.0K    0.0M gaps in allocation
_EAVAIL  1175433216 1147884.0K 1120.9M available (including gaps)
_EMAX    1815293952 1772748.0K 1731.1M current limit
  above 2G bar
RAXLVMEMLIM  17592186040320.0M NOLIMIT limit (REG=0)
RAXLVABYTES               2.0M    2.0M allocated
RAXLVHBYTES                  0       0 guarded
RAXLVGBYTES               2.0M    2.0M high water mark
RAXLVNMOMB                           2 # of objects
```

IVP DAEMON,userid

Log user ID `userid` on to RSE daemon to do a connection test. Results are shown with one or more FEK900I console messages. The return code is shown with console message FEK901I.

Note:

- When the test is successful, the function displays a success message.
- The function is similar to what the `fekfivpd` IVP (Installation Verification Program) does.
- RSE daemon generates a PassTicket which is used as password for the IVP, so there is no Write To Operator with Reply (WTOR) requesting a password.

IVP ISPF,userid[,PROC=proc,Acct=acct,GRP=group,SIZE=size]

Test Legacy ISPF Gateway or Interactive ISPF Gateway with user ID userid. Interactive ISPF Gateway requires that you specify a TSO logon procdure (proc), TSO account number (acct), security group (group) and TSO region size (size). Results are shown with one or more FEK900I console messages. The return code is shown with console message FEK901I.

Note:

- When the test is successful, the function displays a success message.
- The function is similar to what the `fekfivpi` IVP (Installation Verification Program) does.
- RSE daemon generates a PassTicket which is used as password for the IVP, so there is no Write To Operator with Reply (WTOR) requesting a password.

IVP PASSTICKET,userid

Test the reusability of a PassTicket generated for user ID `userid`. Results are shown with one or more FEK900I console messages. The return code is shown with console message FEK901I.

Note:

- When the test is successful, the function displays a success message.

- When using RACF as security product, reusable PassTickets require the "NO REPLAY PROTECTION" keyword in the security definitions.
- There is no equivalent IVP (Installation Verification Program) for this test.
- RSE daemon generates a PassTicket which is used as password for the IVP, so there is no Write To Operator with Reply (WTOR) requesting a password.

SWITCH
Switch to a new audit log file.

Stop (P)

Use the **STOP** command to stop an active task. The abbreviated version of the command is the letter P.

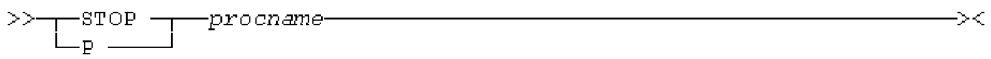


Figure 16. STOP operator command

procname
The name of the member in a procedure library that was used to start the server. The default names used during the host system configuration are and RSED for JES Job Monitor, and the RSE daemon, respectively.

How to read a syntax diagram

The syntax diagram shows you how to specify a command so that the operating system can correctly interpret what you type. Read the syntax diagram from left to right and from top to bottom, following the horizontal line, which is the main path.

Symbols

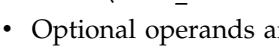
The following symbols are used in syntax diagrams:

Symbol	Description
>>	Marks the beginning of the syntax diagram.
>	Indicates that the syntax diagram is continued.
|	Marks the beginning and end of a fragment or part of the syntax diagram.
><	Marks the end of the syntax diagram.

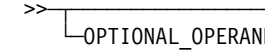
Operands

The following types of operands are used in syntax diagrams:

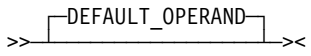
- Required operands are displayed on the main path line:

- Optional operands are displayed below the main path line:

- Default operands are displayed above the main path line:

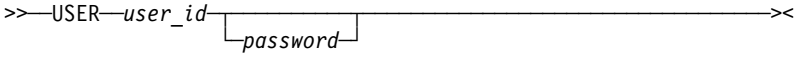


Operands are classified as keywords or variables:

- Keywords are constants that must be provided. If the keyword appears in the syntax diagram in both uppercase and lowercase, the uppercase portion is the abbreviation for the keyword; for example, KEYword. Keywords are not case-sensitive.
- Variables are italicized, appear in lowercase letters, and represent names or values you supply. For example, a data set name is a variable. Variables can be case-sensitive.

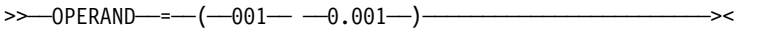
Syntax example

In the following example, the `USER` command is a keyword. The required variable parameter is `user_id`, and the optional variable parameter is `password`. Replace the variable parameters with your own values:



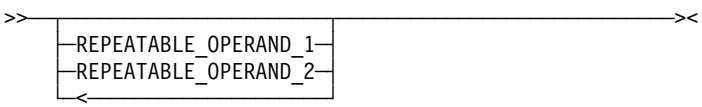
Nonalphanumeric characters and blank spaces

If a diagram shows a character that is not alphanumeric, such as parentheses, periods, commas, equal signs, and blank spaces, you must code the character as part of the syntax. In this example, you must code `OPERAND=(001 0.001)`:



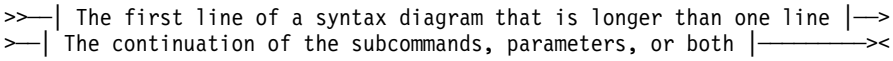
Selecting more than one operand

An arrow returning to the left in a group of operands means that more than one can be selected, or that a single one can be repeated:



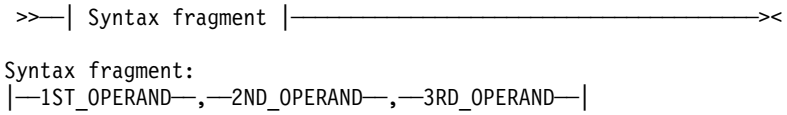
Longer than one line

If a diagram is longer than one line, the first line ends with a single arrowhead and the second line begins with a single arrowhead:



Syntax fragments

Some diagrams might contain syntax fragments, which serve to break up diagrams that are too long, too complex, or too repetitious. Syntax fragment names are in mixed case and are shown in the diagram and in the heading of the fragment. The fragment is placed below the main diagram:



Chapter 8. Host Configuration Reference

This section summarizes the information in *Host Configuration Reference* (SC27-8438). For more details, see that publication.

Understanding z/OS Explorer

The z/OS Explorer host consists of several components that interact to give the client access to the host services and data. Understanding the design of these components can help you make the correct configuration decisions.

Security considerations

z/OS Explorer provides mainframe access to users on a non-mainframe workstation. Validating connection requests, providing secure communication between the host and the workstation, and authorizing and auditing activity are therefore important aspects of the product configuration.

TCP/IP considerations

z/OS Explorer uses TCP/IP to provide mainframe access to users on a non-mainframe workstation. It also uses TCP/IP for communication between various components and other products.

WLM considerations

Unlike traditional z/OS applications, z/OS Explorer is not a monolithic application that can be identified easily to Workload Manager (WLM). z/OS Explorer consists of several components that interact to give the client access to the host services and data. Some of these services are active in different address spaces, resulting in different WLM classifications.

Tuning considerations

RSE (Remote Systems Explorer) is the core of z/OS Explorer. To manage the connections and workloads from the clients, RSE is composed of a daemon address space, which controls thread pooling address spaces. The daemon acts as a focal point for connection and management purposes, while the thread pools process the client workloads.

This makes RSE a prime target for tuning the z/OS Explorer setup. However, maintaining hundreds of users, each using multiple threads, a certain amount of storage, and possibly one or more address spaces requires proper configuration of both z/OS Explorer and z/OS.

Performance considerations

z/OS is a highly customizable operating system, and (sometimes small) system changes can have a huge impact on the overall performance. This chapter highlights some of the changes that can be made to improve the performance of z/OS Explorer.

Push-to-client considerations

Push-to-client, or host-based client control, supports central management of the following:

- Client configuration files
- Client product version

User exit considerations

This chapter assists you with enhancing z/OS Explorer by writing exit routines.

Customizing the TSO environment

This chapter assists you with mimicking a TSO logon procedure by adding DD statements and data sets to the TSO environment in z/OS Explorer.

Troubleshooting configuration problems

This chapter is provided to assist you with some common problems that you may encounter during your configuration of z/OS Explorer, and has the following sections:

- Log and setup analysis using FEKLOGS
- Log files
- Dump files
- Tracing
- z/OS UNIX permission bits
- Reserved TCP/IP ports
- Address Space size
- Miscellaneous information
- Host Connect Emulator

Setting up encrypted communication and X.509 authentication

This section is provided to assist you with some common problems that you may encounter when setting up encrypted communication, or during checking or modifying an existing setup. This section also provides a sample setup to support users authenticating themselves with an X.509 certificate.

Setting up TCP/IP

This section is provided to assist you with some common problems that you may encounter when setting up TCP/IP, or during checking or modifying an existing setup.

Appendix. Accessibility features for z/OS Explorer

Accessibility features assist users who have a disability, such as restricted mobility or limited vision, to use information technology content successfully.

Overview

z/OS Explorer includes the following major accessibility features:

- Keyboard-only operation
- Operations that use a screen reader
- Color and typeface preferences

z/OS Explorer uses IBM Installation Manager to install the product. You can read about the accessibility features for IBM Installation Manager in IBM Installation Manager documentation.

z/OS Explorer uses the latest W3C Standard, WAI-ARIA 1.0, to ensure compliance with US Section 508 and Web Content Accessibility Guidelines (WCAG) 2.0. To take advantage of accessibility features, use the latest release of your screen reader and the latest web browser that is supported by z/OS Explorer.

The z/OS Explorer online product documentation in IBM Knowledge Center is enabled for accessibility. The accessibility features of IBM Knowledge Center are described in the Accessibility section of the IBM Knowledge Center help.

Keyboard navigation

You can use keyboard shortcuts to navigate the help system and the product without using a mouse. For more information, see the *Keyboard shortcuts for the help system in the product* topic in z/OS Explorer documentation.

Interface information

The z/OS Explorer online product documentation is available in IBM Knowledge Center, which is viewable from a standard web browser.

PDF files have limited accessibility support. With PDF documentation, you can use optional font enlargement, high-contrast display settings, and can navigate by keyboard alone.

To enable your screen reader to accurately read syntax diagrams, source code examples, and text that contains period or comma PICTURE symbols, you must set the screen reader to speak all punctuation.

Related accessibility information

In addition to standard IBM help desk and support websites, IBM has a TTY telephone service for use by deaf or hard of hearing customers to access sales and support services:

TTY service 800-IBM-3383 (800-426-3383) (within North America)

For more information about the commitment that IBM has to accessibility, see IBM Accessibility.

Bibliography

Referenced publications

The following publications are referenced in this document:

Table 27. Referenced publications

Publication title	Order number	Reference	Reference Web site
Program Directory for IBM Explorer for z/OS	GI13-4314	z/OS Explorer	http://www-01.ibm.com/support/docview.wss?uid=swg27047234
IBM Explorer for z/OS Host Configuration Quick Start Guide	GI13-4313	z/OS Explorer	http://www-01.ibm.com/support/docview.wss?uid=swg27047234
IBM Explorer for z/OS Host Configuration Guide	SC27-8437	z/OS Explorer	http://www-01.ibm.com/support/docview.wss?uid=swg27047234
IBM Explorer for z/OS Host Configuration Reference	SC27-8438	z/OS Explorer	http://www-01.ibm.com/support/docview.wss?uid=swg27047234
IBM Explorer for z/OS Host Configuration Utility Guide	SC27-8436	z/OS Explorer	http://www-01.ibm.com/support/docview.wss?uid=swg27047234
Communications Server IP Configuration Guide	SC31-8775	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
Communications Server IP Configuration Reference	SC31-8776	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
Communications Server IP Diagnosis Guide	GC31-8782	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
Communications Server IP System Administrator's Commands	SC31-8781	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
Communications Server SNA Network Implementation Guide	SC31-8777	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
Communications Server SNA Operations	SC31-8779	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
Cryptographic Services System SSL Programming	SC24-5901	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
DFSMS Macro Instructions for Data Sets	SC26-7408	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
DFSMS Using data sets	SC26-7410	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
JES2 Initialization and Tuning Guide	SA22-7532	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
JES3 Initialization and Tuning Guide	SA22-7549	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
Language Environment Customization	SA22-7564	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
Language Environment Debugging Guide	GA22-7560	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/

Table 27. Referenced publications (continued)

Publication title	Order number	Reference	Reference Web site
MVS Callable Services for HLL	SA22-7613	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
MVS Diagnosis: Tools and Service Aids	GA22-7589	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
MVS Initialization and Tuning Guide	SA22-7591	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
MVS Initialization and Tuning Reference	SA22-7592	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
MVS JCL Reference	SA22-7597	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
MVS Planning APPC/MVS Management	SA22-7599	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
MVS Planning Workload Management	SA22-7602	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
MVS System Commands	SA22-7627	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
Security Server RACF Command Language Reference	SA22-7687	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
Security Server RACF Security Administrator's Guide	SA22-7683	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
TSO/E Customization	SA22-7783	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
TSO/E REXX Reference	SA22-7790	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
UNIX System Services Command Reference	SA22-7802	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
UNIX System Services Planning	GA22-7800	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
UNIX System Services User's Guide	SA22-7801	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
Using REXX and z/OS UNIX System Services	SA22-7806	z/OS 1.13	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
Java™ Diagnostic Guide	SC34-6650	Java 6.0	http://www.ibm.com/developerworks/java/jdk/diagnosis/
Java SDK and Runtime Environment User Guide	/	Java 6.0	http://www-03.ibm.com/servers/eserver/zseries/software/java/

The following Web sites are referenced in this document:

Table 28. Referenced Web sites

Description	Reference Web site
z/OS Explorer IBM Knowledge Center	http://www-01.ibm.com/support/knowledgecenter/SSBDYH/welcome.html
z/OS Explorer library page	http://www-01.ibm.com/support/docview.wss?uid=swg27047051

Table 28. Referenced Web sites (continued)

Description	Reference Web site
z/OS Explorer product page	http://www-01.ibm.com/software/htp/cics/ibmexplforzos/
z/OS Explorer download page	https://developer.ibm.com/mainframe/
z/OS Explorer Recommended service	http://www-01.ibm.com/support/docview.wss?rs=2294 &context=SS2QJ2&uid=swg27006335
z/OS internet library	http://www-03.ibm.com/servers/eserver/zseries/zos/bkserv/
IBM Tivoli® Directory Server	http://www-01.ibm.com/software/tivoli/products/directory-server/
Java security information	http://www.ibm.com/developerworks/java/jdk/security/
CA support home page	https://support.ca.com/

Informational publications

The following publications can be helpful in understanding setup issues for the requisite host system components:

Table 29. Informational publications

Publication title	Order number	Reference	Reference website
ABCs of z/OS System Programming Volume 9 (z/OS UNIX)	SG24-6989	Redbook	http://www.redbooks.ibm.com/
System Programmer's Guide to: Workload Manager	SG24-6472	Redbook	http://www.redbooks.ibm.com/
TCPIP Implementation Volume 1: Base Functions, Connectivity, and Routing	SG24-7532	Redbook	http://www.redbooks.ibm.com/
TCPIP Implementation Volume 3: High Availability, Scalability, and Performance	SG24-7534	Redbook	http://www.redbooks.ibm.com/
TCP/IP Implementation Volume 4: Security and Policy-Based Networking	SG24-7535	Redbook	http://www.redbooks.ibm.com/
Tivoli Directory Server for z/OS	SG24-7849	Redbook	http://www.redbooks.ibm.com/

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing IBM Corporation North Castle Drive Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing Legal and Intellectual Property Law IBM Japan, Ltd. 19-21, Nihonbashi-Hakozakicho, Chuo-ku Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created

programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

Intellectual Property Dept. for Rational Software IBM Corporation Silicon Valley Lab 555 Bailey Avnue San Jose, CA 95141-1003 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Copyright license

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 1992, 2017.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

Terms and conditions for product documentation

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED “AS-IS” AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Copyright license

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademark acknowledgments

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at `www.ibm.com/legal/copytrade.shtml`.

Adobe and PostScript are trademarks of Adobe Systems Incorporated.

Cell Broadband Engine - Sony Computer Entertainment Inc.

Rational is a trademark of International Business Machines Corporation and Rational Software Corporation, in the United States, other countries, or both.

Intel, Intel Centrino, Intel SpeedStep, Intel Xeon, Celeron, Itanium, and Pentium are trademarks of Intel Corporation in the United States, or other countries, or both.

IT Infrastructure Library is a trademark of Central Computer and Telecommunications Agency

ITIL is a trademark of The Minister for the Cabinet Office

Linear Tape-Open, LTO, and Ultrium are trademarks of HP, IBM Corp., and Quantum

Linux is a trademark of Linus Torvalds

Microsoft, Windows, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States, or other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Index

Special characters

A

B

C

D

E

F

G

H

I

S

T

U

V

W

Z

Readers' Comments — We'd Like to Hear from You

IBM Explorer for z/OS
Host Configuration Guide

Publication No. SC27-8437-02

We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state on this form.

Comments:

Thank you for your support.

Send your comments to the address on the reverse side of this form.

If you would like a response from IBM, please fill in the following information:

Name	Address
Company or Organization	
Phone No.	Email address

Readers' Comments — We'd Like to Hear from You
SC27-8437-02

IBM

Cut or Fold
Along Line

Fold and Tape | **Please do not staple** | Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM
Corporation
Building 501
P.O Box 12195
Research Triangle Park, NC
USA 27709-2195

Fold and Tape | **Please do not staple** | Fold and Tape

SC27-8437-02

Cut or Fold
Along Line

Printed in USA

SC27-8437-02