TIBCO WebFOCUS®

Reporting Server Installation

Release 9.0.0
August 2022
DN4501641.0822

Contents

Chapter 1

Introduction to Installation

This chapter describes the different software packages that can be installed and configured from the TIBCO WebFOCUS® Reporting Server software you have downloaded.

While this guide is primarily for WebFOCUS® Reporting Server installations (and the text often cites "server"), the TIBCO® Data Migrator desktop interface as well as non-Windows clients are also installed using the same instructions.

This guide is for all platforms and also suggests where to go for more information once you have installed your package, regardless of its type.

In this chapter:

Versions

The software enables applications to access data without concern for the complexities and incompatibilities of different operating systems, DBMSs, file systems, and networks. The software provides access to both local and remote data on over 35 platforms from more than 65 database formats, including Db2, FOCUS, Informix, Oracle, MS/SQL, Sybase, Teradata, several JDBC based data sources, and SAP BW.

The server includes the Reporting Server browser interface, with which you can administer the server once it has been installed.

What to Read After You Install

After you have completed the installation, for more information about:

- Managing the server, see the *TIBCO WebFOCUS® Reporting Server Administration* manual.
- Using adapters for accessing data, see the *TIBCO WebFOCUS® Adapter Administration* manual.
- Data Migrator Client. This is a Windows application (and associated server client) for developing and running Data Migrator requests.
- Clients Toolkit. This is a client software toolkit for developing and using third-party application access.

To find out more about administering a particular version of the software, for:

- WebFOCUS Reporting Server or Shared Application Server, see the *TIBCO WebFOCUS® Security and Administration* manual.
- Data Migrator desktop interface, see the *TIBCO® Data Migrator User's Guide*.

Chapter 2

Installation for Windows

This chapter describes how to install, or to configure an additional instance on a system running Microsoft® Windows.

In this chapter:

Information You Need Prior to Installation on Windows

The WebFOCUS Reporting Server is installed by going to the TIBCO™ eDelivery site and downloading the software to be used in the actual installation. By selecting your product, version, and operating system, and accepting the EULA agreement, you may then either select to download the full product or individual files.

If you choose individual files, you must open the *TIBCO WebFOCUS Reporting Server Software* folder, select the *TIB_wf-rs_*_win-x86_64.zip* file, where * indicates the release number, and start the download. Once downloaded, unzip the file and proceed with the instructions in the following topics.

The process for a full download is similar. A main directory is created on the desktop with multiple directories and subdirectories. Simply find the applicable TIB_wf-rs_*_win-x86_64.zip file from the download and unzip it.

Note: An actual unzip should be done on the .zip file, and not just a *browse* into the zip file. Installation problems have been reported when executed in this manner.

The server has an email notification feature that requires SMTP mail server information. You can enter these parameters either during installation, or later using the Reporting Server browser interface Administration tool.

You need a server administrator user ID. Server administrators use this ID to install, start, and stop the server. This ID is also used to configure the server if the server is configured to run with an OPSYS (operating system) Security Provider.

- Do not install on primary or backup domain controllers.
- The Installation ID must have administrator privileges on the machine.

Although Administrative privileges are required only during installation, the Server Administrator ID only needs to have at least Power User privileges in order to run the server as a service, once installed.

Note that the name *iadmin* is used to refer to the Server Administrator ID throughout this manual, but you may use any name for this ID.

Windows Installation Requirements

Before you install, review the following requirements.

Type	Description
Operating System	Windows 10 or Windows Server 2012 or higher. The server is a 64-bit product, which must be installed on a 64-bit operating system. The *TIBCO WebFOCUS® Release Notes* maintains a current list of supported operating systems and levels.
Disk Space	Approximately 5.5G (plus additional space during installation). Integrated Hyperstage releases use approximately 7G of disk space.
IP Ports	Up to six consecutive IP ports (two in reserve for typical extra features). Additional Java Listeners (post-installation option) require additional ports (beyond basic reserve).

Type	Description
Java	Java JRE or Java SDK (also known as JDK) 8 or higher Used for Java-based adapters, server-side graphics, XBRL, or user-written CALLJAVA applications. For additional information, see *JVM Requirements for Java Services (Server Installations Only)* on page 16. **Note:** Java 8 and Java 11 are explicitly tested and certified to be compatible with the WebFOCUS Reporting Server. Other Java releases may be compatible with the WebFOCUS Reporting Server. If you use an untested Java release, you must self-certify its compatibility with the WebFOCUS Reporting Server and accept responsibility for using an untested release.
Memory	The memory requirements for installation and operation of the server are: ❑ General memory: 30Mb. (This includes memory used by the primary one-per-server-instance processes such as Workspace Manager, the print log, Deferred Listener, HTTP Listener, and TCP Listener.) ❑ Memory per active agent: 3.5Mb. These numbers apply when the server is in an idle state, so they may fluctuate slightly.
Web Browser	Needed for using the Reporting Server browser interface. Microsoft Edge Mozilla Firefox® 59 or higher. Google Chrome® 65 or higher.

Type	Description
Node.js Caching	The Node.js Caching feature enables Reporting Server independent caching, which allows external access to Reporting Server In-Document Analytics outputs. This feature is normally configured automatically at server installation time, if Node Package Manager (npm) and Node.js are detected during the installation. This may be configured post-installation if not detected, failed during installation, or for older configurations that had software upgraded to Release 8207.28 or higher. For information on npm and Node.js installation requirements and post-configuration instructions for adding the Node.js Caching feature to a qualifying existing configuration, or correcting the configuration, see *Caching Support for Node.js* on page 285.

JVM Requirements for Java Services (Server Installations Only)

Many modern data adapters, server-side graphics, and other services use a Java JVM to implement execution. These require a Java JVM to be installed (separate from the server) and that the server be configured to use it.

The minimum Java JVM release level is 8 or higher, due to required internal components of the server. The Java Listener will not start properly (and will show errors in edaprint) if 8 (or higher) is not in use.

The following URL has Java EOL and EOSL information:

http://www.oracle.com/technetwork/java/eol-135779.html

You may install a commercial Oracle Java JRE, Oracle Java SDK (also known as JDK), or an open-source OpenJDK (from such sites as adoptopenjdk.net or azul.com). The JRE or SDK build version must be 64-bit. When you install a Java SDK, the JRE component (where the JVM is installed) is also included, so either is allowed. However, if you are using the servlet feature, a Java SDK (JDK) is required for access to the jar command, so an SDK (JDK) installation is generally preferred over a JRE installation.

New to 7707 and higher server release levels is an automatic Windows Registry look-up feature for the latest highest commercial Oracle Java available on the system. This feature only requires that an appropriate 8 or higher commercial Oracle Java JRE or SDK of the correct bit size has been installed on the system, using the standard commercial Oracle Java Installer, which registers the installation to the Windows Registry. In addition, it requires that no explicit variables be set on the system that would cause an override. If a commercial Oracle JRE and SDK are both installed (and no override variables are set), the SDK will be used.

The automatic look-up feature also applies to Adopt OpenJDK *https://adoptopenjdk.net/* versions, if the "JavaSoft (Oracle) Registry Keys" option is selected on the installer (it is off by default). Selecting this option will set up registry keys like commercial Oracle Java, so the JDK will be automatically found, as it is with a real commercial Oracle Java installation.

The automatic look-up feature does not apply to a commercial Oracle Java JRE or SDK that has simply been copied to disk using an archive tool such as WinZip or 7zip, as this method does not register the installation. If this has been done, use explicit variables to configure the server.

The automatic look-up feature also does not apply to Oracle OpenJDK *https://openjdk.java.net/*, as its standard installation method is to unzip (copy) to disk, and the installation is not registered.

This automatic look-up feature also does not apply to any other Java download site providing a Java installer that does not register its location, or registers it differently from a commercial Oracle Java install (such as Azul OpenJDK *https://www.azul.com/*).

Explicit JAVA_HOME or JDK_HOME variables, described below, may be used to manually configure Java access (to override locations found by the automatic Java look-up feature or because an unregistered Java is in use). While OpenJDK uses a different directory organization from the Oracle JDK and JRE, the Azul OpenJDK directory structure is more like the Oracle JDK and JRE. The server is aware of both implementations when it attempts to locate and setup use of the actual Java JVM DLL (so you should use JAVA_HOME= or JDK_HOME= to point at the desired implementation).

Some third-party Java JDK/JRE providers, such as Adpotopenjdk.com, provide not only classic JDK and JRE implementations (also known as Hotspot), but also Eclipse OpenJ9 Java virtual machine (JVM) implementations. While the server Java Listener will start with either implementation, it has been found that some third-party JDBC DBMS drivers do not work with some Adpotopenjdk.com Open9J implementations (Vertica and Snowflake JDBC Drivers, in particular, on Windows). If your site chooses to use an Open9J implementation or other third-party JVM provider and experiences JDBC DBMS problems, a classic Java (Hotspot) implementation from Oracle or Adpotopenjdk.com should be installed and tested to confirm that the server software and DBMS setup are not at issue (and to correct, if needed). If the Open9J implementation is still desired, the site should follow up with the Open9J JVM or DBMS provider as to why this combination fails.

Installation of any third-party Java JVM that follows the same directory structure as any of the known implementations should work, but use of such alternate packages should be self-certified.

At server start-up time, if none of the above is true, the server Java Listener may still start if applicable JVM directories happen to be on the system PATH, but this is not a recommended method, as it is not explicit.

If an appropriate JVM is not found at server start-up time, various *failed to find* JVM messages displays in EDAPRINT. Reviewing and following the instructions in this section will usually correct the problem.

JSCOM3 is the actual process name for the Java Services Listener and those terms, as well as the term Java Listener, are often used interchangeably.

To use explicit variables to specify the Java JVM location, do the following:

- For Java SDK, set JDK_HOME (to the Java SDK install home location) in the environment or server environment start-up file (edaenv.cfg).
- For Java JRE, set JAVA_HOME (to the Java JRE install home location) in the environment or server environment configuration file (edaenv.cfg).

To change or add a variable in the server environment start-up file (EDACONF bin\edaenv.cfg), either edit the file in a text editor before starting the server (a start menu icon is also available under the configure folder) or:

1. Start the server (services like Java Listener may fail until configured and the server is restarted).
2. Open the Reporting Server browser interface and sign in using an administrator ID.
3. Select *Workspace* from the main menu.

4. In the navigation pane, open the *Configuration Files* and *Miscellaneous* folders.
5. Right-click *Environment - edaenv.cfg* and select *Edit*.
6. Make the desired edit.
7. Save the file.
8. Restart the server (changes are not effective until the server is restarted).

The format of edaenv.cfg variables are one per line in name=value pairs. Spaces before and after the equal sign are optional. Values with embedded spaces do not have to be enclosed in quotation marks.

To add classes to the JVM class path for customer-written CALLJAVA applications, set the CLASSPATH variable at the operating system level before server start-up or use the Reporting Server browser interface to set the Java Listener IBI_CLASSPATH property.

If Java JVM-based adapters or features are not required, and no Java is installed (or is below the minimum level), various EDAPRINT Java Listener fail messages are *normal*, acceptable, and can be ignored. However, this is not a recommended situation. If you make a support call, please make the representative aware of this, as it may take them unnecessary time to analyze the situation and realize that these messages are normal for your configuration and not part of the problem being called in.

Installation and Configuration Directories on Windows

The installation process creates these high-level directories. The locations documented here often use a release number, such as 90, within location names or, when discussing the release level. However, this number may vary for your particular installation and use an alternate level.

Note: Installation and Configuration directory names are changeable at installation time, but no spaces are allowed in directory names.

Name	Environment Variable	Description	Default Path
Home directory	EDAHOME	Stores the server software programs and other files	`c:\ibi\srv90\home` Must conform to the following pattern *`disk`*`:*\ibi\srv90*\home*`

Name	Environment Variable	Description	Default Path
Configuration directory	EDACONF	Stores the configuration files. If you are configuring multiple instances of the server, create separate configuration directories for each by adding a suffix (for example, a number) to the end of the directory name.	*disk*:\ibi\srv90*product_type* Must conform to the following pattern *disk*:*\ibi\srv90**product_type** Product type can be: ❑ **WFS** for a WebFOCUS Reporting Server
Application directory	APPROOT	Contains your application files.	c:\ibi\apps
Profiles directory	EDAPRFU	Stores the user and group profiles and the admin.cfg file (which specifies the server administrator).	c:\ibi\profiles

Multiple WebFOCUS Reporting Servers. If you plan to install multiple copies of WebFOCUS on the same computer, and you want to provide each copy with its own WebFOCUS Reporting Server, you may wish to maintain a separate root directory for each copy, so that you can keep copies of each set of components, including the server, together in the same path.

You can specify a separate apps directory for each copy of WebFOCUS, or specify a single apps directory to be shared by all copies of WebFOCUS.

Installation Methods

Before you install, review the requirements in the following topics. Exact requirements vary according to your configuration and the number of users and deployed applications.

Choosing Between Interactive and Silent Installation

You can run the installation procedure in:

- **Interactive mode.** This is the default installation mode. It displays windows that prompt you for installation parameters. We recommend that you use this mode the first time you install, so that you become familiar with the procedure. To install interactively, see *Installing a TIBCO WebFOCUS Reporting Server* on page 22.
- **Silent mode.** In this mode you launch the installation and specify a text file that contains the installation parameters. The installation procedure does not prompt for any information. Installing silently can be helpful if, for example, you want to install many instances at once throughout your enterprise. To install silently, see *Installing and Configuring Silently* on page 35.

Choosing Between Private and Shared Access to the Data Migrator Desktop Interface

There are several tools available for administering the server:

- **Reporting Server browser interface,** which is installed with the server on all platforms, and is available to all authorized users with a TCP/IP connection.

  For more information about the Reporting Server browser interface, see the *TIBCO WebFOCUS® Reporting Server Administration* manual.

- **Data Migrator desktop interface,** which is installed with the server on Windows, and is used primarily with Data Migrator.

  For more information about the Data Migrator desktop interface, see the *TIBCO® Data Migrator User's Guide*.

You can install in a way that makes the Data Migrator desktop interface available to remote users as a shared tool. You can choose between:

- **Private access.** You install in a standard Windows folder. The Data Migrator desktop interface is available locally to users on that computer.
- **Shared access.** You install in a shared network folder specified using the Universal Naming Convention (UNC). The Data Migrator desktop interface is available to remote users who access that shared folder.

  Before installing, you need to create a shared folder on the computer on which you will install the software.

Access to the server by means of the Data Migrator desktop interface is limited by system security. To use the Data Migrator desktop interface, you can open it in several ways, such as:

- Mapping a drive to the location of dmcstart.bat.
- Creating a shortcut to dmcstart.bat on the user machine.

The location of dmcstart.bat defaults to ibi\srv90\wfs\bin.

The Data Migrator desktop interface is maintained locally on each client machine in Documents and Settings*UserID*\Application Data\Information Builders. This requires 2M of disk space.

To use the loopback node, reconfigure it to connect to the share server host name, replacing the host name, localhost.

Installing a TIBCO WebFOCUS Reporting Server

When you install, several server properties are configured automatically. After installation, you can configure additional properties using the Reporting Server browser interface. The Data Migrator Client also has properties that can be adjusted post installation.

Procedure: How to Install and Configure a WebFOCUS Reporting Server

Using the location to which you unzipped the software:

1. Preferably, exit all programs before continuing.
2. Execute the following file from the location in which you unarchived the software.

   For a server installation:

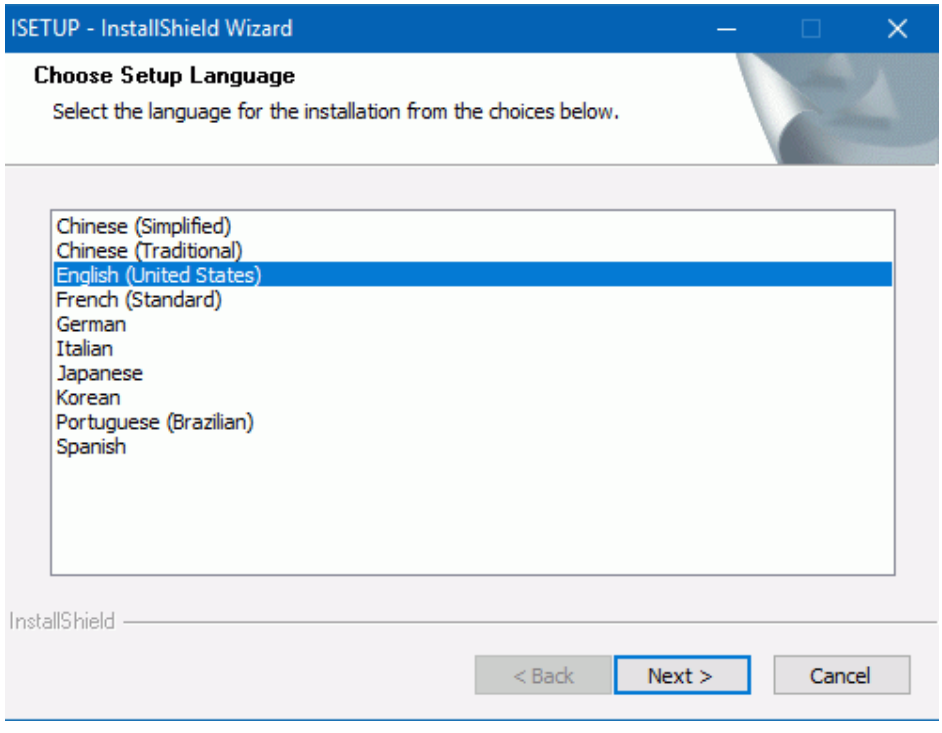
   `setup.exe`

   For a Data Migrator Client installation:

   `setup_dm_client.exe`

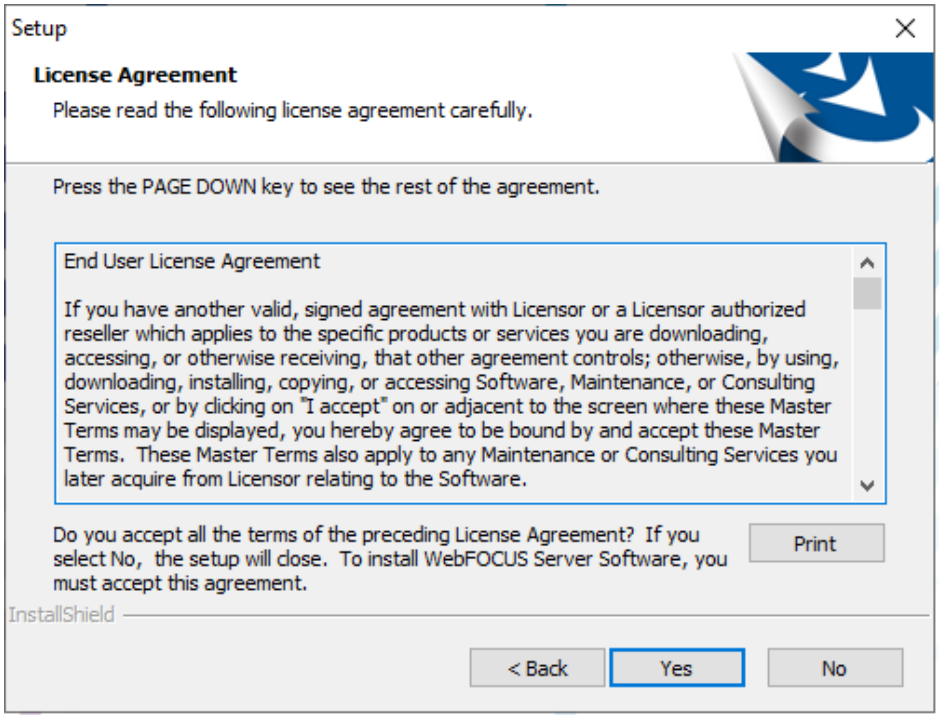
   A User Access Control (UAC) security prompt may appear. Respond *yes*.

The Choose Setup Language window opens.

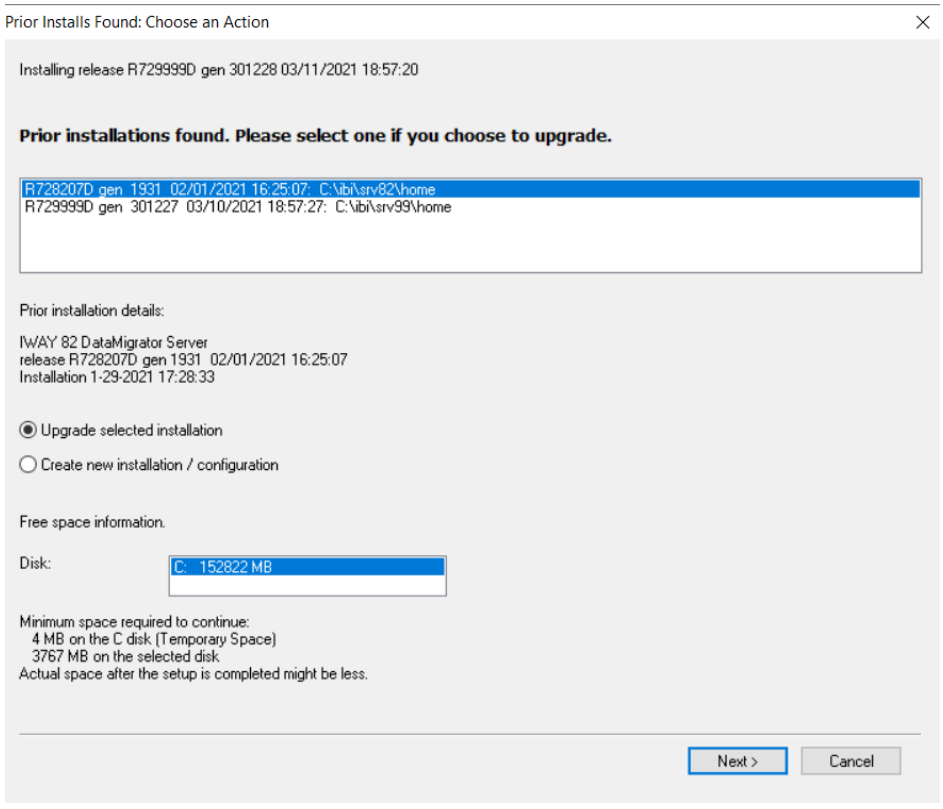


3. Select the language to be used during installation and click *Next*.

   ❑ If you have no prior installation, the License Agreement window opens:



- If a prior installation was found, the Prior Installs Found: Choose an Action window opens.



You can choose to upgrade the selected installation or to create a new installation.

- If you choose to upgrade, the upgrade starts immediately, with no further information needed from you.

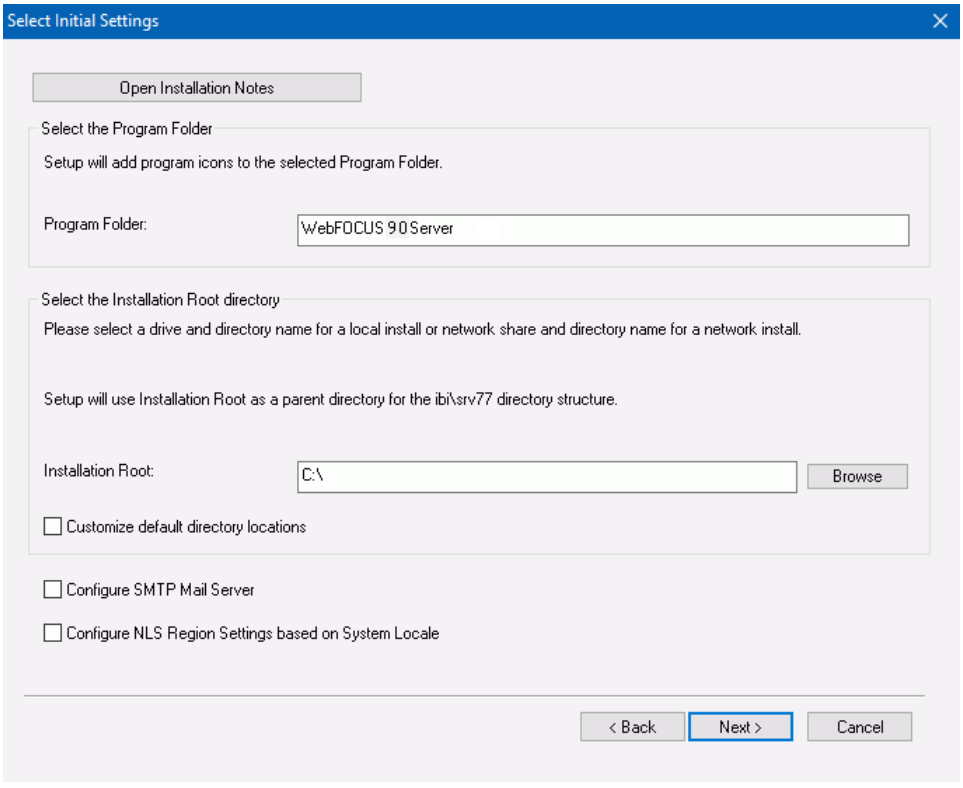
- If you choose to create a new installation/configuration, you will need to choose between a new installation or adding a configuration. If *add configuration* is chosen, the software is not installed, but the highlighted entry from the prior screen is used as a base for adding an additional configuration. Choosing a new installation gives a separate complete new installation and initial configuration, but in this instance, and when adding a new configuration, it is appropriate to not use the default installation paths and server name to avoid overwriting a prior installation or configuration location.

You get a message that the installation is starting.

Click *OK*.

4. Click *Yes* to accept the terms of the license agreement.

   The Select Initial Settings window opens.



5. You can accept the defaults or edit the following settings.

   - **Program Folder.** By default, this is named *WebFOCUS 90 Server*. If you are installing a Data Migrator Client, the name can be changed, but it must include one of the following keywords:

     - WebFOCUS
     - iWay
     - TIBCO
     - IBI

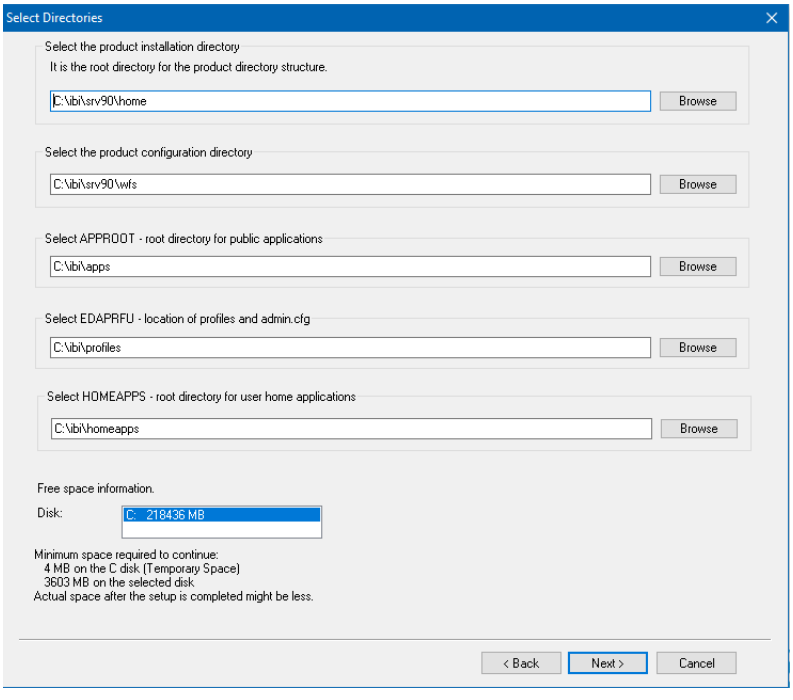
And one of the following additional phrases:

- DM Client
- DataMigrator Client
- Data Migrator Client

- **Installation Root.** By default, this is C:\. You can browse to or enter another location.
- **Customize default directory locations.** Check this box if you want to customize the directory locations. For example, if you are configuring an additional instance of the server, some of the locations, such as EDAHOME and EDACONF must be customized. One way to customize the directories is to just use a different installation root and keep the default location names under that root.
- **Configure SMTP Mail Server.** If you will use any of the server email features, check this box.
- **Configure NLS Region Settings based on System Locale.** By default, this box is checked, so that you inherit the regional settings for your system at installation time instead of having to configure them later on the Reporting Server browser interface.

6. Click *Next*.

If you checked the box to customize the default directories, the Select Directories window opens.



7. Specify the following locations, or accept the default values:

   a. **Product installation directory.** This contains the executable files. We refer to this location as EDAHOME. It must conform to the pattern:

      `*\ibi\srv90*\home*`

      If you are installing new, accept the default directory, or specify a different directory. The new software will be placed in this directory.

      If you are configuring an additional instance, using your existing software, accept the default EDAHOME directory. If several 90 installation directories exist, select the one that corresponds to the software home directory for which you are configuring a new instance.

   b. **Product configuration directory.** This contains configuration information for the instance. We refer to this location as EDACONF.

      If you changed the EDAHOME value, the default EDACONF value changes to conform to EDAHOME.

EDACONF must be in the same srv90 path as EDAHOME. The lowest-level EDAHOME directory (home) becomes the product type directory in EDACONF. For example, if EDAHOME is

```
ibi\srv90\home
```

then EDACONF for a WebFOCUS Reporting Server defaults to:

```
ibi\srv90\wfs
```

Each instance must have its own configuration directory. If you are configuring an additional instance, be sure to append characters to the default name of the directory. (Otherwise, the installation will overwrite the existing configuration directory.) For example:

```
ibi\srv90\wfs2
```

Accept the default value, or click *Browse*, or type a name to specify a different directory.

c. **Application directory.** This contains the server application directories. The application directories are folders under the internal location known as APPROOT.

   Accept the default value, or click *Browse* to select a different directory.

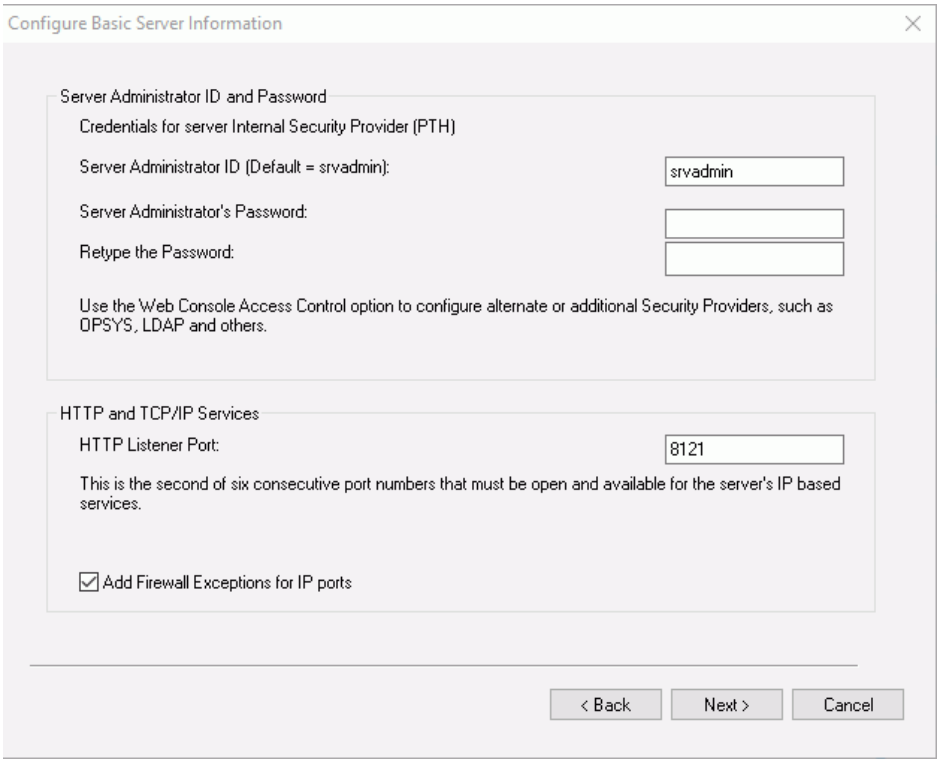
d. **Profiles directory.** This contains the server user and group profiles and the admin.cfg file, which specifies the server administrator. We refer to this location as EDAPRFU.

   Accept the default value, or click *Browse* to select a different directory.

e. **Disk.** If there is more than one disk or shared folder to which the software can be installed, select the one on which you want to install.

f. Click *Next*.

The Configure Basic Information window opens.



8. Enter the following information.

- **Server Administrator user ID.** The default value is srvadmin. You can change it or accept the default. When the server first starts, it is configured for the server internal security provider, called PTH. You must enter the server administrator user ID and password in order to access the server.
- **Server Administrator's Password.** You must configure a password, there is no default.
- **Retype the Password.** Enter the password again for verification that you typed it correctly.
- **HTTP Listener Port.** Accept the default (8121) or enter a new port number. If you are configuring an additional instance of the server, you need a different port number from any other instances that may be running at the same time. The server requires three consecutive ports for the HTTP Listener and other IP-based services. The TCP Listener port will be the one immediately preceding the HTTP Listener port.

If you are configuring multiple instances, be sure to specify a different range of ports for each instance.

The default port automatically varies by product to support multiple instances on a particular computer:

- **SMTP Host Name.** If you will use any of the server email features, enter the host name or TCP/IP number for your SMTP server.
- **SMTP Port Number.** Accept the default (25) or enter a different port number.
- **Sender Email.** Enter an email address for the default sender for users receiving email from the server, or accept the default.
- **Server Administrator Email.** Enter an email address to receive administrative warnings (such as an agent crash) from the server, or accept the default.

The Review Selected Product Parameters window opens showing all of the selections you have made.

9. Click *Next*.

You can now verify your installation, as described in *Verifying Installation* on page 31.

Verifying Installation

After you have installed, verify that the software is functioning properly.

Procedure: How to Verify Server Installation

1. If the server is not already running, start it using whichever security mode you prefer using the Windows menu icon. The server start icons are located on the Windows Start menu in the program group assigned during the installation (for example, Information Builders/ WebFOCUS 90 Server/Start Security ON). The options are:

   - **Start Security ON.** For a new installation, the default security provider is PTH. For a refresh of an existing installation, the server starts with the security provider defined in the security_provider keyword in the edaserve.cfg configuration file.
   - **Start Security OFF.** Security on the server will be OFF regardless of what is configured.

   For information about security providers, see *Security Providers on Windows* on page 33 and the *Server Security* chapter of the *TIBCO WebFOCUS® Reporting Server Administration* manual.

2. Open the Reporting Server browser interface and sign in (if prompted) using the server administrator ID and password entered during configuration, if it is not already running.

The Reporting Server browser interface start icon is located on the Windows Start menu in the program group assigned during the installation (for example, Information Builders/ WebFOCUS 90 Server/Reporting Server browser interface).

The Reporting Server browser interface opens. Online Reporting Server browser interface help, version information, new feature information, release notes, and licensing information are available by clicking *Help* (far right in menu bar).

3. If the Reporting Server browser interface opens and displays application tree folders in the left pane, the server is working because it uses its own underlying data access and reporting technologies to visualize the application tree. The server may be further data tested (if desired).

Now that you have successfully verified your server installation, you can:

- **Configure server security,** as described in *Security Providers on Windows* on page 33.
- **Configure additional server properties,** such as outbound communication nodes and adapter support, using the Reporting Server browser interface.

  For more information about using the Reporting Server browser interface and configuring outbound nodes, see the *TIBCO WebFOCUS® Reporting Server Administration* manual.

  For more information about configuring adapter support, see the *TIBCO WebFOCUS® Adapter Administration* manual.

Procedure: How to Verify Installation

To verify that you have successfully installed, use the base configuration that is created by the installation and start the Data Migrator desktop interface.

The first step is to add a server node (right-click the server icon in the object tree to add one), and then connect. If the portion of the object tree for the newly added server opens to display application directories, the software is properly installed. See the *TIBCO® Data Migrator User's Guide* for further use of the Data Migrator desktop interface.

Using a TIBCO WebFOCUS Reporting Server or Data Migrator Desktop Interface

Commonly used start, stop, and monitor features are available from the Windows Start menu under the folder in which the software was installed.

On Windows, a single start-panel icon is created for tablet or desktop menu mode. Clicking the icon or menu item switches the screen into desktop mode (if it is in tablet mode) and opens a Windows Explorer session displaying the installed icons and folders (as normally seen after an installation). Once the explorer session is open when in tablet mode, it is recommended that you simply use the standard Window Desktop icon to flip from the tablet start panel to desktop mode, otherwise additional Explorer sessions will open.

Under the Diagnostics Functions folder, there is a Command Windows for Manual Operations icon that allows you to issue direct edastart commands and options as documented for other platforms (such as -show, -status, -traceon, -traceoff, -?, or -?s). The *Reporting Server Administration* guide has a list of commonly used options, or you can use the edastart -? or -?s options for the additional options.

Note: Since the server is normally started as a service on Windows, you cannot simply add a parameter to the startup properties of the server Start icon to control a feature, such as blocking Hyperstage on server startup. In these instances, there is usually an equivalent environment variable that may be set at either the system level or in the EDACONF bin \edaenv.cfg file. The Diagnostics Functions folder also has an edit icon to allow editing of the edaenv.cfg file and adding settings, such as WFRS_NOHS=TRUE, as an alternative to edastart -nohs. The *TIBCO WebFOCUS® Reporting Server Administration* guide also documents the full list of environment variables that may be set.

Security Providers on Windows

The default security provider for a new installation is the internal security provider, PTH. The PTH provider implements security using user IDs, passwords, and group memberships stored in the admin.cfg configuration file.

After the initial installation, the Server Administrator that was configured during the installation can start the server and use the Reporting Server browser interface to further customize security settings, for example, to configure alternate or additional security providers, create additional PTH IDs, and register groups and users in a security role. For more information about security providers, see the *Server Security* chapter in the *TIBCO WebFOCUS® Reporting Server Administration* manual.

Additional Installation Options

This section explains how to run the Data Migrator desktop interface in zero footprint mode and uninstall servers or configurations.

Procedure: How to Run the Data Migrator Desktop Interface in Zero Footprint Mode

A full Data Migrator Client must first be installed using UNC Network paths on a machine in the user's network, as a prerequisite. This machine will then be used as a remote software share.

The UNC installation and configuration paths used for the remote machine also must be available to the local machines that will be set up to run in zero footprint mode and must continue to be available after the zero footprint Data Migrator desktop interface is set up.

A Data Migrator Client installation using UNC paths creates an additional command file script in the EDACONF\bin directory called zerofootprint.bat, which is used by local machines to set up a zero footprint Data Migrator desktop interface.

No other installation paths, modes, or products create the zerofootprint.bat file, so if the file is not present, it is likely that an improper non-UNC path was used during installation.

Install the prerequisite Data Migrator Client (as described above) as a first step, if it has not already been done. Be sure to remember to use a UNC path, and note the resulting full UNC path for the EDACONF bin\zerofootprint.bat file so you can use it in the later local machine step.

Once the Data Migrator Client is installed on the share machine, there are several choices for running the zerofootprint.bat script, depending on requirements of a site:

- The end user opens a Command Prompt window and runs the zerofootprint.bat file using the full path UNC name.
- The end user opens the Windows *Run* option, enters the full path UNC name of the zerofootprint.bat file, and clicks OK.
- The end user uses Windows Explorer to navigate to the shared UNC directory where the zerofootprint.bat file is located and double–clicks it.
- An administrator puts the full path UNC name of the zerofootprint.bat file in a batch script that the user is directed to run.
- An administrator puts the full path UNC name of the zerofootprint.bat file in a batch script that is run automatically (such as a system update script).

After the zerofootprint.bat file is run, a Command Prompt window opens and a desktop icon shortcut to the Data Migrator desktop interface is created. On English-speaking locales, a *Shortcut Created/OK* pop-up message will also display. This message times out after a short while, so it is compatible for use with unattended batch files.

Once the shortcut icon is created, the end user can start the Data Migrator desktop interface from the shortcut icon, and the zerofootprint.bat file is no longer needed by that user.

The Data Migrator desktop interface configured using zerofootprint.bat behaves like a locally installed instance. Any software updates to the original software installation location will be reflected to end users upon Data Migrator desktop interface restart, with no need to reinstall on each individual machine.

Procedure: How to Uninstall

To uninstall:

1. For server installations, ensure that the server is stopped first.
2. Using the Windows Start menu, select *Programs*, the program group (for example, *WebFOCUS 90 Server*), and *Uninstall*. This program removes the EDAHOME and EDACONF directories of this instance.

If more than one configuration uses the same EDAHOME directory, the additional configurations contain *unconfigure* icons instead of uninstall icons. If you want to uninstall your initial configuration, you must unconfigure the additional configurations first. If you do not unconfigure these instances before uninstalling the EDAHOME directory, you will disable the additional configurations, including their *unconfigure* icons. A manual cleanup is required.

Installing and Configuring Silently

An installation performed without invoking an installation wizard is also known as a silent install. The most common form of a silent installation is an initial install which also results in an initial configuration. An initial installation and configuration should only be done once per EDAHOME (and program folder) and an additional product configuration used thereafter.

A silent installation is triggered by providing an options flag and file containing the installation options needed for the installation procedure.

Installing silently can be helpful if you want to install multiple instances at once throughout an enterprise. To install an instance silently, you must first create a text file that specifies your installation parameters, and then call isetup with the option and the file name. The silent method may also be used to perform a software refresh.

Note: We recommend that the first time you install, you use the default interactive mode, not the silent mode, so that you become familiar with the procedure. Installing interactively is described in *Installing a TIBCO WebFOCUS Reporting Server* on page 22.

Procedure: How to Create the Installation Parameters File

Use a text editor to create an installation options file with the following syntax to specify your product installation parameters:

```
-inst
-edahome drive:\ibi\srv90\home
-edaprfu drive:\ibi\srv90\profiles
-edaconf drive:\ibi\srv90\wfs
-homeapps drive:\ibi\srv90\homeapps
-approot drive:\ibi\apps
-programfolder "folder-title"
-pth_user  user
-pth_password password
-http_port portnum
-nostart
```

where:

drive:*ibi*\

Is the drive and directory to which you want to install the software.

wfs

Is WebFOCUS Reporting Server. In releases prior to 8207.27, there were wfs, ffs, and dm configurations. However, 8207.27 and above have a merged configuration designated as wfs.

portnum

Is the base TCP/HTTP port for the server. You can use either -http_port (which is the second port number in the range of six port numbers for the server) or -port (which is the first port number in the range of six).

folder-title

Is the name you want to assign to the Windows program folder and service. For example:

```
-programfolder "WebFOCUS 90 Server"
```

When installing the Data Migrator Client, the program folder must contain one of the following keywords:

- WebFOCUS
- iWay
- TIBCO
- IBI

And one of the following additional phrases:

- DM Client
- DataMigrator Client
- Data Migrator Client

These keywords and phrases are not case-sensitive, and can be separated by a version number.

user

Is the PTH administrator/security ID.

password

Is the PTH administrator/security password in clear text.

For pre-encrypted passwords use the -epth_password option.

-nostart

Prevents the server from being started automatically on completion of the configuration.

-firewall

Adds Windows firewall exceptions for IP ports.

To see a list of additional installation, configuration, and refresh options:

1. Open a command prompt window and navigate to the directory containing the installation setup.exe file for the software.
2. Enter one of the following:

   ```
   setup ?
   ```

   ```
   setup -?
   ```

   ```
   setup /?
   ```

   On some machines, there may be a delay in displaying the help information, as the re-distributables must be checked and installed prior to displaying the help.
3. Accept a display language and click *Next*.

   A Help screen with further parameter file options will display.

The user may continue with the installation (interactive) or quit at this point to attempt a silent installation/configuration.

Note: InstallShield has limited display capabilities for help information, but you can copy it into a text editor such as Notepad in order to view it more easily.

Procedure: How to Launch a Silent Installation

1. Open a Command Prompt window and navigate to the directory containing the software and the setup.exe file for the installation.

   Alternatively, you can supply a path in the command in Step 2.

2. Type the following:

   `setup -L`*`code`* `-opt` *`drive:\path\srvoptions.txt`*

   where:

   `code`

   Is the code specifying the language of the Reporting Server browser interface user interface. This language will also be used in the status windows displayed by the installation procedure.

   The language code is preceded by -L (a hyphen followed by the letter "L").

   The language codes are:

Chinese (Simplified)	`0x0804`
Chinese (Traditional)	`0x0404`
English	`0x409`
French	`0x040c`
German	`0x407`
Italian	`0x0410`
Japanese	`0x411`
Korean	`0x0412`
Portuguese (Brazilian)	`0x0416`
Spanish	`0x040a`

drive:\path\srvoptions.txt

Is the full path and file name of the file specifying your installation options.

For example, to specify English and an options file named srvoptions.txt, type:

```
setup -L0x409 -opt C:\temp\srvoptions.txt
```

3. After the installation has completed, you should verify that it was successful, as described in *How to Verify Server Installation* on page 31.

Generating a Trace on Windows

If you encounter a server problem, you can run a set of traces that will help you assess the problem, and, if necessary, communicate it to Customer Support for further assistance. This topic describes trace options and provides instructions for creating the traces.

There are two types of traces you can run to troubleshoot a problem:

- **A server trace,** in which you trace an agent that is running in a server context.
- **A non-server trace,** in which you trace an agent that is running outside a server context, that is, an agent that is running standalone.

Under normal conditions, applications are run in a server context. However, if you run your trace in a non-server context (that is, if you run a non-server trace) and produce the necessary diagnostic information, you can significantly reduce the amount of material that needs to be reviewed. Running a non-server trace also rules out server communications as a cause of a problem.

You can start traces, turn traces off, and perform the edastart -savediag function by selecting options from the Windows Start menu, under the Diagnostics folder. You can also open a DOS session to execute these commands.

Tip: The Diagnostics folder in the Windows Start menu has a Command Window for Manual Operations icon, which will directly open the DOS session in the EDACONF bin.

Procedure: How to Generate a Server Trace

To generate a server trace:

1. Turn tracing on by doing one of the following:
   - Go to the Reporting Server browser interface menu bar, select the Main Reporting Server browser interface *Other Options* control icon and then *Enable Traces*.
   - Start the server by issuing the following command:

     ```
     edastart -traceon
     ```

You must preface edastart with the appropriate path, or place the directory in your system PATH variable.

2. Reproduce the problem.
3. Stop the server.
4. Issue the following command:

   ```
   edastart -savediag
   ```

5. Respond to the prompts to capture, and optionally archive and ship diagnostic information.

   Diagnostic information will commonly contain user data. If the release of that data is considered a security concern when shipping to Customer Support, the -savediag feature also allows a diagnostic to be saved and shipped later to allow the site the opportunity to review and cleanse the traces of data of this nature before shipping.

Procedure: How to Generate a Non-Server Trace

To generate a non-server trace:

1. Create a directory under APPROOT to reproduce the problem.
2. Copy any files required for the reproduction to the directory.
3. Switch to the directory.
4. Reproduce the problem using edastart -traceon and one of these switches -t, -x, or -f.
5. Switch to a directory other than the problem reproduction directory.
6. Issue the following command:

   ```
   edastart –savediag
   ```

7. Respond to the prompts to capture, and optionally archive, diagnostic information.

   Diagnostic information will commonly contain user data. If the release of that data is considered a security concern when shipping to Customer Support, the -savediag feature also allows a diagnostic to be saved and shipped later to allow the site the opportunity to review and cleanse the traces of data of this nature before shipping.

Third-Party Software and Licenses

All third-party and TIBCO Software, Inc. license information is available on the Reporting Server browser interface by clicking the Help (?) menu, then either *TIBCO Software, Inc.* or *3rd Party Licenses*.

General Information for a Windows Installation

This section covers general information for a Windows Installation.

Sample Metadata, Data, and Other Tutorial Samples

The Reporting Server browser interface has a feature on the ribbon and on the application tree (under *new*), *Tutorials* (the Create Tutorial Framework page), which has a pull-down for various samples. The Data Migrator desktop interface also has this feature on the application tree.

There are currently about 10 different tutorial/sample selections available on the pull-down select list to match various customer needs. The bulk of the prior IBISAMP sample objects can be generated by selecting the *Create Legacy Sample Tables and Files* tutorial. Other prior IBISAMP Data Migrator sample objects (usually starting with the characters dm*) are now loaded by choosing their respective Data Migrator tutorials. Under the new method, the tutorials/samples may be loaded to any application, not just IBISAMP.

If you are doing just a software refresh, the prior IBISAMP objects will be unchanged (because a refresh does not touch app directories).

Troubleshooting for Windows

As of Release 7702, separately installable debuggable versions are no longer required to get a full stack trace of information for a savediag. The *Debuggable Version - Install* and *Debuggable Version - Remove* options have been removed from the Windows menu.

If you have an earlier 77x release that contains the debug menu options, and have installed service pack upgrades of 7702 (or higher), these menu options should be deleted, since they no longer function or are needed.

To troubleshoot an installation problem, identify your problem in the following list, and follow the link to a description of the solution.

If you cannot find your problem described in the list, and cannot resolve it yourself, contact Customer Support.

Problems:

- The server starts in safe mode (as indicated by a message in the Reporting Server browser interface at start-up).

  For details, see *Problem: The Reporting Server Starts in Safe Mode* on page 42.

- A server start request partly fails with *JVM not found* messages written to edaprint.log.

  For details, see *Problem: Java Listener Fails to Start With JVM not found Messages Written to the Log* on page 42.

- ❑ The Windows service will not stop.

  For details, see *Problem: Cannot Stop the Windows Service of the Server* on page 43.

Reference: Problem: The Reporting Server Starts in Safe Mode

Problem: The server starts in safe mode. The Reporting Server browser interface home page displays a message stating that the server is in safe mode and describing what triggered it.

Cause: A common cause for the server starting in safe mode is a problem with the server administrator ID password. For example, the password may have been updated on the operating system but not on the server, so the encrypted copy of the password stored by the server is out of synchronization with the password on the operating system.

Solution: The server administrator can click the *fix* hyperlink, which is displayed under the problem description, to display the relevant pane and resolve the problem.

For example, if the problem is that the server administrator password is out of synchronization:

1. Click the *fix* hyperlink displayed under the problem description.
2. In the left pane, open the *Users* folder, then the *Server Administrator* folder.
3. Click your user ID and select *Properties* from the pop-up menu.

   The Access Control pane is displayed on the right.
4. Type the correct operating system password in the *Password* field, and type it again in the *Confirm Password* field.
5. Click *Save and Restart*.

   The Security Mode pane opens on the right.
6. Click the Home icon in the menu bar to return to the Reporting Server browser interface home page.

Reference: Problem: Java Listener Fails to Start With *JVM not found* Messages Written to the Log

Problem: The listener start request fails with *JVM not found* messages written to the edaprint.log file.

Cause: If the server cannot find the Java Virtual Machine (JVM), the JSCOM Listener will not be able to start, and messages will be written to the server log stating that the JVM cannot be found.

Solution: Set up the JVM as described *JVM Requirements for Java Services (Server Installations Only)* on page 16. A known exception to general JVM setup is the use of the Azul Client (JRE) 8 Windows Installer, where JAVA_HOME= must be set as JAVA_HOME={Azul Client path}/jre due to a differing directory structure. As JDK is preferred over JRE, and the directory structure on Azul Client (JRE) 11 is acceptable, this is considered an Azul bug that you can address by adding the suffix to the path, as described.

Reference: Problem: Cannot Stop the Windows Service of the Server

Problem: When you try to stop the server, the associated Windows service does not stop.

Cause: Any server administrator can stop the server. The ID that installed the server is automatically defined as a server administrator. You can specify additional IDs as server administrators using the Reporting Server browser interface.

If an ID is not a server administrator it will not be able to stop the server, even if that same ID had started the Windows service that started the server.

Solution: Specify the ID that was not able to stop the service as a server administrator:

1. In the Reporting Server browser interface menu bar, select *Access Control* from the Workspace menu.

   The Manage Providers page opens.

2. Click the *Users* label (to the right of the folder) in the navigation pane.

   The New User option appears.

3. Click *New User*.

   The Access Control pane opens.

4. Identify the new administrator by filling in the fields in the Access Control pane.

   For more information about these fields and about specifying an additional server administrator, see the *TIBCO WebFOCUS® Reporting Server Administration* manual.

5. Click *Create*, and then click *Save and Restart*.

Reference: Problem: ODBC Test Tool Does Not Show Expected Sources/Connections

Problem: The ODBC Test Tool starts, but either no configured sources (server connections) are shown, or they are not shown as expected.

Cause: The ODBC Test Tool accesses the ODBC Sources configured in the Data Sources (ODBC) section of the Control Panel Administrative Tools. It does not directly use configured connections. To be visible by ODBC, the connections (after creation and configuration) must be registered to ODBC, which is a separate post-installation and post-connection configuration step. Additionally, the connection configuration and registration steps must be done under the Windows icons for a client installation even though some server releases contain the Windows menu icons for these actions. That is why registering from a server installation is ineffective, leaving the connection list either empty or not as expected.

Solution: If a client installation has not been done, complete the client installation as a pre-requisite. Either start the Data Migrator desktop interface or (if you are familiar with the appropriate communication node syntax) use the *Edit Communication Configuration File - ODIN.CFG* icon to add connections and save. When finished adding, use the *Register TIBCO Software, Inc. ODBC Driver* icon to make them visible to ODBC. The *Remove TIBCO Software, Inc. ODBC Driver* icon may be used to remove the connection's ODBC visibility. If you have more than one client installation on the machine, the *Reset Shared* icon may be used to switch the machine's current ODBC configuration to see the client connection configuration within that icon group.

Chapter 3

Installation for UNIX/Linux

This document describes the requirements and procedures for installing on UNIX/Linux.

In this chapter:

Information You Need Prior to Installation on UNIX/Linux

The WebFOCUS Reporting Server is installed by going to the TIBCO™ eDelivery site and downloading the software to be used in the actual installation. By selecting your product, version, and operating system, and accepting the EULA agreement, you may then either select to download the full product or individual files.

If you choose individual files, you must open the *TIBCO WebFOCUS Reporting Server Software* folder, select a *TIB_wf-rs_*.run* or *TIB_wf-rs_*.tar* file, where * indicates the release number and platform, and start the download. Some platforms, such as Linux, use a compressed self-extracting .run archive format, while others use a traditional .tar format.

Once the desired file is downloaded, and if necessary, transferred to the actual machine where the installation will occur and into a temporary working directory, either run the .run file or untar the .tar file, as appropriate.

More specifically, change directory (cd) to the temporary directory and issue one of the following commands, depending on what you downloaded, where the actual .run or .tar file name is the full file name that was downloaded.

```
sh TIB_wf-rs_*.run
```

or

```
tar -xvf TIB_wf-rs_*.tar
```

Note:

- If the file format is a .run file, the extracted files will be in a temp subdirectory of the current directory.
- If the file format is a .tar file, extraction will result in the files being in the current directory.

After extraction, proceed with the instructions in the following topics.

The process for a full download is similar. A main directory is created on the desktop with multiple directories and subdirectories. Simply find the applicable TIB_wf-rs_*.* file, where *.* indicates the release number, transfer to the desired UNIX machine, and either .run or .tar from the download, and extract, as previously noted.

The server has an email notification feature that requires SMTP mail server information. You can enter these parameters either during installation, or later using the Reporting Server browser interface Administration tool.

You need a server administrator user ID, referred to as *iadmin* in the remainder of this chapter.

- The operating system ID you use when installing the server owns the server files and is the default server administrator for OPSYS mode. You can create a new operating system ID to run and own the server files, or use any ordinary (non-superuser) ID. However, you should not install the server as root. The server administrator ID should have a Korn, Bourne, or Bash shell as the default logon shell.

UNIX/Linux Installation Requirements

Before you install, review the following requirements.

Type	Description	
Operating System	Product version must be compatible with the operating system bit size (64-bit servers on 64-bit operating systems is the only supported combination). AIX Linux for x86_64 Linux for pSeries Kernel-2.6.32 Linux for zSeries Solaris SPARC Solaris x86_64 The *TIBCO WebFOCUS® Release Notes* maintains a current list of supported operating systems and levels.	
Disk Space	Space for installation Space after installation	Approximately 6G Approximately 3G
IP Ports	Up to six consecutive IP ports (two in reserve for typical extra features). Additional Java Listeners (post-installation option) require additional ports (beyond basic reserve).	

Type	Description	
Java	Java JRE or Java SDK (also known as JDK) 8 or higher Used for Java-based adapters, server-side graphics, XBRL, or user-written CALLJAVA applications. For additional information, see *JVM Requirements for Java Services (Server Installations Only)* on page 49. **Note:** Java 8 and Java 11 are explicitly tested and certified to be compatible with the WebFOCUS Reporting Server. Other Java releases may be compatible with the WebFOCUS Reporting Server. If you use an untested Java release, you must self-certify its compatibility with the WebFOCUS Reporting Server and accept responsibility for using an untested release.	
Memory Common framework plus per agent memory.	**O/S**	**Per Agent/Common**
	AIX	5 MB/50 MB
	Solaris (SPARC)	19 MB/125 MB
	Solaris (Intel)	10 MB/72 MB
	Linux for x86_64	9 MB/87 MB
	Linux for pSeries 64b	27 MB/165 MB
	Linux for zSeries 64b	10 MB/93 MB
Web Browser	Needed for using the Reporting Server browser interface. Microsoft Edge Mozilla Firefox® 59 or higher. Google Chrome® 65 or higher.	

Type	Description
Node.js Caching	The Node.js Caching feature enables Reporting Server independent caching, which allows external access to Reporting Server In-Document Analytics outputs. This feature is normally configured automatically at server installation time, if Node Package Manager (npm) and Node.js are detected during the installation. This may be configured post-installation if not detected, failed during installation, or for older configurations that had software upgraded to Release 8207.28 or higher. For information on npm and Node.js installation requirements and post-configuration instructions for adding the Node.js Caching feature to a qualifying existing configuration, or correcting the configuration, see *Caching Support for Node.js* on page 285.

A minimally configured (bare-bones) Linux distribution (such as Alpine and Amazon EC2 t2.micro) may not be a viable run-time platform for the server because of missing utility tools (commands) and libraries. The sheer number of Linux distributions and sub-configurations makes it hard to be exact about the specific issues that might be encountered when trying to use a minimally configured (bare-bones) Linux distribution. However, the issues are typically missing dll errors and tput (missing ncurses) errors at server start-up. Adding the specific missing packages or tools to a distribution will generally allow minimal Linux distributions to be viable for the server and keep a somewhat minimal footprint, but it is the responsibility of the customer to research and resolve such issues.

JVM Requirements for Java Services (Server Installations Only)

Many modern data adapters, server-side graphics, and other services use a Java JVM to implement execution. These require a Java JVM to be installed (separate from the server) and that the server be configured to use it. You may install a commercial Oracle Java JRE, Oracle Java SDK (also known as JDK) or an open-source OpenJDK (from such sites as adoptopenjdk.net or azul.com).

The minimum Java JVM release level is 8 or higher, due to required internal components of the server. The Java Listener will not start unless the applicable minimal level for the platform is used by setting JAVA_HOME/JDK_HOME values.

The following URL has Java EOL and EOSL information:

http://www.oracle.com/technetwork/java/eol-135779.html

You may install a commercial Oracle Java JRE (if available), Oracle Java SDK (also known as JDK, if available), an open-source OpenJDK (from such sites as adoptopenjdk.net or azul.com), or the Java that may have come with the operating system (or available separately from the operating system vendor). The JRE or SDK build version must also match the bit type of the server, which is 64-bit. When you install a Java SDK, the JRE component (where the JVM is installed) is also included, so either is allowed. However, if using the servlet feature, the Java SDK is required for access to the jar command, so an SDK installation is generally preferred over a JRE installation.

While OpenJDK uses a different directory organization from the Oracle JDK and JRE, the Azul OpenJDK directory structure is more like the Oracle JDK and JRE, plus the directory structure may also vary from implementations delivered by the operating system vendor. The server is aware of all of these implementations when it attempts to locate and set up the use of the actual Java JVM DLL (so you can use JAVA_HOME= or JDK_HOME= to point at the desired implementation).

Some third-party Java JDK/JRE providers, such as Adpotopenjdk.com, provide not only classic JDK and JRE implementations (also known as Hotspot), but also Eclipse OpenJ9 Java virtual machine (JVM) implementations. While the server Java Listener will start with either implementation, it has been found that some third-party JDBC DBMS drivers do not work with some Adpotopenjdk.com Open9J implementations (Vertica and Snowflake JDBC Drivers, in particular, on Windows). If your site chooses to use an Open9J implementation or other third-party JVM provider and experiences JDBC DBMS problems, a classic Java (Hotspot) implementation from Oracle or Adpotopenjdk.com should be installed and tested to confirm that the server software and DBMS setup are not at issue (and to correct, if needed). If the Open9J implementation is still desired, the site should follow up with the Open9J or DBMS provider as to why this combination fails.

Installation of any third-party Java JVM that follows the same directory structure as any of the known implementations should work, but use of such alternate packages should be self-certified.

Use explicit variables to specify the Java JVM location:

- For Java JDK, set JDK_HOME (to the install home location) in the environment or server environment start-up file (edaenv.cfg).
- For Java JRE, set JAVA_HOME (to the install home location) in the environment or server environment configuration file (edaenv.cfg).

If JDK_HOME and JAVA_HOME variables are both declared, the JDK_HOME value will be used.

To change or add a variable in the server environment start-up file (EDACONF bin/edaenv.cfg), either edit the file in a text editor before starting the server or:

1. Start the server (services like Java Listener may fail until configured and the server is restarted).
2. Open the Reporting Server browser interface and sign in using an administrator ID.
3. Select *Workspace* from the main menu.
4. In the navigation pane, open the *Configuration Files* and *Miscellaneous* folders.
5. Right-click *Environment - edaenv.cfg*, and click *Edit*.
6. Make the desired edit.
7. Save the file.
8. Restart the server (changes are not effective until the server is restarted).

The format of edaenv.cfg variables are one per line in name=value pairs. Spaces before and after the equal sign are optional. Values with embedded spaces do not have to be enclosed in quotation marks.

To add classes to the JVM class path for customer-written CALLJAVA applications, set and export the CLASSPATH variable to the operating system level before server start-up or use the Reporting Server browser interface to set the Java Listener IBI_CLASSPATH property.

If JVM-based adapters or features are not required, and the JVM environment is not configured, the message *Failed to find JVM* is normal and can be ignored.

Installation and Configuration Directories on UNIX/Linux

The installation process creates these high-level directories. The locations documented here often use 90 within location names or when discussing the release level. However, this number may vary for your particular installation and use an alternate level.

Name	Environment Variable	Description	Default Path

Home directory	EDAHOME	Stores the server software programs and other files	`ibi/srv90/home`
			Must conform to the following pattern
			`*/ibi/srv90*/home*`

Name	Environment Variable	Description	Default Path
Configuration directory	EDACONF	Stores the configuration files. If you are configuring multiple instances of the server, create separate configuration directories for each by adding a suffix (for example, a number) to the end of the directory name.	`ibi/srv90/`*`product_type`* Must conform to the following pattern `*/ibi/srv90*/`*`product_type`* Product type can be: ❑ **WFS** for a WebFOCUS Reporting Server
Application directory	APPROOT	Contains your application files.	`ibi/apps`
Profiles directory	EDAPRFU	Stores the user and group profiles and the admin.cfg file (which specifies the server administrator).	`ibi/profiles`

Multiple WebFOCUS Reporting Servers. If you plan to install multiple copies of WebFOCUS on the same computer, and you want to provide each copy with its own WebFOCUS Reporting Server, you may wish to maintain a separate root directory for each copy, so that you can keep copies of each set of components, including the server, together in the same path.

You can specify a separate apps directory for each copy of WebFOCUS, or specify a single apps directory to be shared by all copies of WebFOCUS.

Running isetup to Install the TIBCO WebFOCUS Reporting Server Software

You can install the server software by running isetup interactively and responding to prompts or by creating a file containing the answers to the prompts and running isetup against that file. The method using a file is called a *silent install*.

Both use a .tar-formatted archive file. The isetup program is also used to later do software refreshes and to add configurations (interactively or silently).

Procedure: How to Run isetup Interactively Using the .tar File

For performance reasons, it is always preferable to install on a local disk, however, it is possible to use NFS if the EDAIPC environment variable is used during Reporting Server run time to point at a local disk location for pipe and fifo creation. For more information on setting EDAIPC, see *EDATEMP and NFS-Mounted Disks* on page 64.

To install the software:

1. Sign in using the iadmin user ID.
2. Set the default protection mask to, at a minimum, read/execute (if it is not already set to that). For example:

   ```
   umask 022
   ```

   Ensure that you have write privileges to the directory from which you are running the isetup command. To test this, enter:

   ```
   touch xxxx
   ```

3. Run the installation procedure, isetup, specifying its full path. You can run the installation procedure from any location. Do not switch the current directory to the location of isetup.

   For example, if you downloaded the installation software to a directory named download under the iadmin home directory:

   ```
   /u/iadmin/download/isetup
   ```

   The following isetup screen displays.

   ```
   ----------------------------------------------------------------------
                    Welcome to the Product Set Up Facility
        Please respond to the prompts or enter Q to quit at any prompt.
   ----------------------------------------------------------------------

     ISETUP: Now Installing TIBCO WebFOCUS  Server

   ----------------------------------------------------------------------

   Select an option:
         1. Install and Configure
         2. Add Additional Configuration Instance
         3. Refresh Installation (Reinstall, Keep Configurations)
         4. Install Debuggables to the Installation Directory
         5. View Installation Notes
   Enter a selection (Default=1) :
   ```

4. Enter *1* for the Install and Configure option.

   You are prompted for the location of the installation file iserver.tar (it defaults to the same directory from which isetup was run).

   ```
   Please enter the full path name of the media for the product
   ```

5. Type the full path name of iserver.tar, or press Enter to accept the default.

   You are prompted for the ID of the server administrator for the internal server security provider.

   ```
   Enter credentials for the server's internal security
   provider (PTH), the server's default start up mode.
   Enter the Server Administrator ID
   (Default=srvadmin) :
   ```

   The server automatically starts with this security provider. You can add other security providers using the server Reporting Server browser interface after installation. For information, see the *TIBCO WebFOCUS® Reporting Server Administration* manual.

6. Enter the server administrator ID or accept the default.

   You are prompted for the server administrator password. There is no default.

   ```
   Enter the Administrator Password :
   ```

7. Type the password of the account you are using to install the software.

   The password, which does not display, is stored in encrypted form.

   You are now shown the default values of the server environment variables and port number, and given an opportunity to change them. For example:

   ```
   Please review the default settings.
   EDAHOME = /prog3/iadmin/ibi/srv/home
   EDACONF = /prog3/iadmin/ibi/srv/wfs  (*EXISTS, owner iadmin *)
   EDAPRFU = /prog3/iadmin/profiles
   APPROOT = /prog3/iadmin/ibi/apps
   HOMEAPPS = /prog3/iadmin/ibi/homeapps
   HTTP_BASE_PORT = 8121
   WARNING: Directories marked as existing will be deleted and recreated!
   If you are satisfied with the default settings you may proceed to
   final confirmation else you will be prompted for individual values.
   Proceed with defaults? (Y/N Default=Y)  :  y
   ```

8. If you want to accept the default values, type *Y* and skip to Step 10. Otherwise, select *N* and change any properties that you wish.

   For information about the EDAHOME, EDACONF, EDAPRFU, and APPROOT environment variables you can set, see *Installation and Configuration Directories on UNIX/Linux* on page 51.

The other properties you can set are described in the following table.

Parameter	Description
HTTP_BASE_PORT	First of three consecutive port numbers for the HTTP Listener and other IP-based services. The default port for a WebFOCUS Reporting Server is 8121, which reserves ports 8121-8123.
TCP_BASE_PORT	Port number on which the server TCP Listener listens. It must be outside the range of the three consecutive HTTP Listener ports. It defaults to the port immediately preceding the first HTTP Listener port. For example, if you accept the default HTTP Listener Port value of 8101, the TCP Listener port defaults to 8100.
SMTP_HOST	SMTP Server node (host) name or TCP/IP number for outbound email features. (Optional, only prompted for if changing directories and ports.)
SMTP_PORT	SMTP Server port number for SMTP Server. The default value is 25. (Optional, only prompted for if changing directories and ports, and the SMTP Server host is supplied.)
SENDER_EMAIL	Default *from* address for users reading an email from the server if none was specified in the originating application. (Optional, only prompted for if changing directories and ports, and the SMTP Server host is supplied.)
SERVER_ADMIN_EMAIL	Server administrator email address to send administrative warnings to, such as an agent crash. (Optional, only prompted for if changing directories and ports, and the SMTP Server host is supplied.)

If you decide to change a default, you are prompted for a replacement value for each of the above variables, and given another chance to accept the default. If the SMTP Server node is not supplied, the remaining SMTP and EMAIL prompts do not occur.

9. Review the configuration options displayed on the screen, and type *Y* if you accept them. Alternatively, to start over, enter *N*; to quit the installation procedure, enter *Q*.

   Several progress messages display while the server is being installed. You are then asked if you want to start the server.

10. If a server installation, type *Y* to start the server or *N* to exit.

    If you start the server, startup messages and the Reporting Server browser interface URL are now displayed.

You should now verify your installation, as described in *How to Verify Installation* on page 59.

Configuring an Additional Instance of the TIBCO WebFOCUS Reporting Server

The prompts for adding a configuration are similar to those for an original installation.

Procedure: How to Configure an Additional Reporting Server Instance

If you need to configure additional instances:

1. Sign in using the iadmin ID.
2. Run *EDAHOME*/bin/isetup, where *EDAHOME* is the directory in which the software was installed.
3. At the main menu, select option 2, *Add Additional Configuration Instance*.

   Each instance must have its own configuration directory. When prompted for the configuration directory, append characters to the default name of the product type directory. Otherwise, the installation will overwrite the existing configuration directory. In the following example, the number 2 has been added to the default name of the WebFOCUS Reporting Server configuration directory:

   ```
   /home/iadmin/ibi/srv90/wfs2
   ```

   If the EDACONF directory you specify already exists, the installation process copies selected files from files in the current configuration to a directory named BACKUP that is a sibling directory to EDACONF, and then deletes the contents of the original directory. For example, if EDACONF is:

   ```
   /home/iadmin/ibi/srv90/wfs
   ```

   then the selected configuration files are backed up to:

   ```
   /home/iadmin/ibi/srv90/BACKUP
   ```

Refreshing or Upgrading an Installation

Refreshing reinstalls the files in the installation directory, without changing any configuration information in the configuration directory.

Procedure: How to Refresh or Upgrade an Installation

If it becomes necessary to refresh, or if you want to upgrade to a new release:

1. Sign in using the iadmin user ID.

   Logging on with the iadmin ID is recommended (rather than with the su command).

2. Set the default protection mask to, at a minimum, read/execute (if it is not already set to that). For example:

   ```
   umask 022
   ```

   Ensure that you have write privileges to the directory from which you are running the command. To test this, type:

   ```
   touch xxxx
   ```

3. Run the installation procedure, isetup, specifying its full path. You can run the installation procedure from any location. Do not switch the current directory to the location of isetup. For example:

   ```
   /u/iadmin/download/isetup
   ```

4. At the main menu, type option 3, *Refresh Installation (Reinstall, Keep Configuration)*, and respond to the prompts.

Installing and Configuring Silently

This is also known as a silent install. The most common form is an initial install, which also results in an initial configuration. An initial installation and configuration should only be done once per EDAHOME. An *add product configuration* should be used thereafter.

Installing silently can be helpful if you want to install multiple servers at once throughout an enterprise. To install a server silently, you must first create a text file that specifies your server installation parameters and then call isetup with the option and the file name. The silent method may also be used to do a software refresh.

We recommend that the first time you install, you use the default interactive mode, not the silent mode, so that you become familiar with the procedure. Installing a server interactively is described in *Running isetup to Install the TIBCO WebFOCUS Reporting Server Software* on page 52.

Run isetup -? to see full information on the setup and specific use of a parameters file for silent installation, configuration, or refresh.

Procedure: How to Create the Installation Parameters File

Use a text editor to create a file with the following syntax to specify your product installation parameters:

```
-inst
-m /yy/iserver.tar
-http_port portnum
-approot /ibi/apps
-edahome /ibi/srv90/home
-edaconf /ibi/srv90/wfs
-edaprfu /ibi/srv90/profiles
-pth_user user
-pth_password password
-nostart
```

where:

portnum

Is the base TCP/HTTP port for the server. You can use either -http_port (which is the second port number in the range of six port numbers for the server) or -port (which is the first port number in the range of six).

/ibi/

Is the suggested top-level directory for the directory path in which you want to install the software. The default top-level directory for an interactive installation is the resolved value of $HOME/ibi/ and can be used in this context.

wfs

Is WebFOCUS Reporting Server. In releases prior to 8207.27, there were wfs, ffs, and dm configurations. However, 8207.27 and above have a merged configuration designated as wfs.

user

Is the server administrator/security ID.

password

Is the server administrator/security password in clear text.

For pre-encrypted passwords use the -epth_password option.

-nostart

Prevents the Workspace Manager from being started automatically on completion of the configuration.

To see a list of additional installation, configuration, and refresh options, on the command line, enter the following:

```
/path/isetup -?
```

where:

path

Is the directory path to the location of the isetup program.

Procedure: How to Launch a Silent Installation

1. On the command line, enter the following:

   ```
   /path/isetup -opt /path/srvoptions.txt
   ```

   where:

   /path/srvoptions.txt

   Is the full path and file name of the file specifying your installation options.

   For example, to specify English and an options file named srvoptions.txt, type:

   ```
   /tmp/isetup -opt /tmp/srvoptions.txt
   ```

2. After the installation has completed, you should verify that it was successful, as described in *Verifying the UNIX/Linux Installation* on page 59.

Verifying the UNIX/Linux Installation

After installing, verify that the software is functioning properly.

Procedure: How to Verify Installation

To verify that you have successfully installed, use the configuration that is created by the base installation. You can verify the installation by bringing up, checking, connecting to, testing, disconnecting from, and shutting down the server. (If you started the server as the last step of the installation procedure, skip ahead to Step 4.)

1. Log on to your UNIX or Linux operating system using the iadmin ID.
2. Start the server with the appropriate path to edastart and the -start option. For example, for a WebFOCUS Reporting Server, you would type:

```
/home/iadmin/ibi/srv90/wfs/bin/edastart -start
```

3. Check to ensure that the processes are up by specifying the -show option:

   ```
   /home/iadmin/ibi/srv90/wfs/bin/edastart -show
   ```

4. Start the Reporting Server browser interface by starting a browser pointed at the server HTTP Listener port, which was specified during installation. The URL format is http://*host:port*. (The URL is also displayed at the end of the installation procedure.)

   For example, if default ports were used during installation, for a WebFOCUS Reporting Server, use http://host:8121.

5. If the server is running in a secure mode, you will first see a logon screen. Log on using the iadmin ID used during server configuration. For information about server security, see *Security Providers on UNIX/Linux* on page 61.

   The Reporting Server browser interface home page opens. The Home Page is arranged in a menu-like context for the various features it supports. Detailed use of the Reporting Server browser interface for configuration or general operation of the server is available by clicking *Help* in the left navigation menu and in the *TIBCO WebFOCUS® Reporting Server Administration* manual.

6. If the Reporting Server browser interface opens and displays application tree folders in the left pane, the server is working because it uses its own underlying data access and reporting technologies to visualize the application tree. The server may be further data tested (if desired).

7. When you are done using the server, you can stop it using the Reporting Server browser interface by clicking the *Stop* option on the Reporting Server browser interface toolbar.

8. If you experience any problems, examine the /home/iadmin/ibi/srv90/*product_type*/edaprint.log file.

Now that you have successfully verified your installation, you can:

- ❑ Configure server security, as described in *Security Providers on UNIX/Linux* on page 61.
- ❑ Configure additional server properties, such as outbound communication nodes and adapter support, using the Reporting Server browser interface.

  For more information about using the Reporting Server browser interface and configuring outbound nodes, see the *TIBCO WebFOCUS® Reporting Server Administration* manual.

  For more information about configuring adapter support, see the *TIBCO WebFOCUS® Adapter Administration* manual.

Security Providers on UNIX/Linux

The default security provider for a new installation is the internal security provider, PTH. The PTH provider implements security using user IDs, passwords, and group memberships stored in the admin.cfg configuration file.

After the initial installation, the Server Administrator that was configured during the installation can start the server and use the Reporting Server browser interface to further customize security settings, for example, to configure alternate or additional security providers, create additional PTH IDs, and register groups and users in a security role. For more information about security providers, see the *Server Security* chapter in the *TIBCO WebFOCUS® Reporting Server Administration* manual.

Procedure: How to Satisfy Security Provider OPSYS Requirements

To run a server in security provider OPSYS mode in UNIX/Linux, you must perform the following steps. You must do this once after installing and after each refresh of the server with fixes.

Set up tscom300.out as a root-owned SUID program:

1. If the server is running, bring it down.
2. Log on to the system as root, or issue the su root command.
3. Change your current directory to the bin directory of the home directory created during the installation procedure.

   For example, type the following command:

   ```
   cd /home/iadmin/ibi/srv90/home/bin
   ```

4. Change file ownership and permissions by typing the following commands:

   ```
   chown root tscom300.out
   chmod 4555 tscom300.out
   ```

5. Verify your changes by issuing the following command:

   ```
   ls -l tscom300.out
   ```

   The output should be similar to the following:

   ```
   -r-sr-xr-x 1 root iadmin 123503 Aug 23 04:45 tscom300.out
   ```

   Note the permissions and ownerships.

When you start the server, it will now run with security provider OPSYS.

The chmod and chown steps will need to be repeated after any server upgrade since the tscom300.out file is replaced during an upgrade and the attributes are lost.

Note: If this Security Provider OPSYS step has been done and the site later decides to switch to Security OFF, special steps must be taken to ensure the mode remains after a full server shutdown (where edastart -start is used to restart the server). The steps are:

1. After the server recycles from the change to OFF, use the Reporting Server browser interface to open the environment configuration file of the server by clicking *Workspace* and expanding the *Configuration Files* folder, followed by the *Miscellaneous* folder.
2. Double-click *Environment - edaenv.cfg* to edit the file and add the *EDAEXTSEC=OFF* variable.
3. Save your work.

After the next full server shutdown, be sure to do an edastart -cleardir before restarting the server. This will clear any root-owned files that would prevent a security OFF server from starting.

Preventing Unsecured Server Starts After Upgrades

If the explicit environment variable EDAEXTSEC is set to OPSYS (or ON) and the server cannot impersonate users because it lacks platform-specific authorization steps, the server start aborts and error messages are written to the edaprint log.

This feature prevents an unsecured server start after a software upgrade if any of the required post-upgrade, reauthorization steps are missed on a UNIX/Linux, IBM i, or z/OS HFS deployment. This is not applicable to other platforms. The setting may be placed in any normal server start-up shell or profile that a site is using or in the server edaenv.cfg environment configuration file. The messages vary slightly by platform.

The edaprint messages are:

```
Configured security is 'ON' as set by EDAEXTSEC variable.

Server has no root privilege.

Workspace initialization aborted.

(EDA13171) UNABLE TO START SERVER
```

Starting and Using a TIBCO WebFOCUS Reporting Server

For information about:

- Starting a server, see *How to Verify Installation* on page 59.
- Using and managing a server, and additional edastart options and environment variables that control server behavior, such as blocking Hyperstage from starting at server startup, see the *TIBCO WebFOCUS® Reporting Server Administration* manual.

- The Node.js Caching feature, which enables Reporting Server independent caching to allow external access to Reporting Server In-Document Analytics outputs, see *Caching Support for Node.js* on page 285.

Reference: Commonly Used Reporting Server Start Options and Functions

Command and Option	Function
`edastart`	Starts the server with the line mode console, which enables you to view the server log and to dynamically issue edastart options, such as show, traceon, and stop. To display the console command prompt, press Ctrl + C.
`edastart -start`	Starts the server without the line mode console.
`edastart -sstart` *n*	Starts the server, but waits *n* seconds for actual start-up.
`edastart -show`	Shows general status of server and agents.
`edastart -stop`	Stops the server.
`edastart -cleardir`	Removes all temporary directories (and their contents), as well as logs and other files created by the server (including the rmlda*.log files, if active) in EDACONF. If Resource Manager is in use and you want to maintain the rmlda*.log data, backup the rmlda*.log files before using this feature and restore them afterward.
`edastart -traceon`	Turns on tracing. May be used at startup or afterward. It is preferable to run traces at startup, unless instructed otherwise. Turn tracing on *only* when there is a problem that needs to be traced, to avoid incurring the associated overhead.
`edastart -traceoff`	Turns off tracing.
`edastart -?`	Displays full set of edastart server control options.

Command and Option	Function
`edastart -?s`	Displays support information and support-related options.

EDATEMP and NFS-Mounted Disks

Part of the Reporting Server process creates pipe and fifo objects in EDATEMP for Interprocess Communication (IPC). However, pipe and fifo object types for IPC use do not work well on NFS-mounted disks, so the prior recommendation was not to use NFS-mounted disks for EDATEMP. To alleviate this problem and allow NFS-mounted disk use, the EDAIPC system variable may be set to a local non-NFS directory location, so pipe and fifo object creation may be redirected to this separate non-NFS location. EDATEMP can be pointed to an NFS-mounted disk, but the pipe and fifo objects go to a local disk.

Normally, the EDATEMP directory defaults to a subdirectory of EDACONF. The EDATEMP variable allows EDACONF file objects, such as edaprint.log and rmdta.log and the EDATEMP directory to be redirected to the location specified by EDATEMP. EDAIPC is usually used in conjunction with EDATEMP, when EDATEMP is pointed to an NFS-mounted disk. It is also possible that EDACONF itself could be on an NFS-mounted disk (the EDATEMP directory is also on an NFS-mounted disk by parentage) and EDAIPC should also be used in this instance.

For example:

```
export EDATEMP=/nfs/wfs
export EDAIPC=/tmp/wfs
.../edastart -start
```

The /tmp directory is always local, but should organizationally be identified by a subdirectory name, such as wfs. If multiple Reporting Servers are run on the same box, there should also be a subdirectory such as wfs/accounting to prevent process collisions.

Note: The pipes and fifos for tscom300 are the only exceptions to the redirection that EDAIPC invokes. Additionally, while the Reporting Server can detect if NFS is in use, EDAIPC has no default and must be explicitly set to redirect the pipes and fifos.

The EDATEMP and EDAIPC variables may also be set in the EDACONF bin/edaenv.cfg file, using the normal edaenv.cfg rule, which is one variable per line in x=y format (no "export" keyword).

Generating a Trace on UNIX/Linux

If you encounter a server problem, you can run a set of traces that will help you assess the problem, and, if necessary, communicate it to Customer Support for further assistance. This topic describes trace options and provides instructions for creating the traces.

There are two types of traces you can run to troubleshoot a problem:

- A server trace, in which you trace an agent that is running in a server context.
- A non-server trace, in which you trace an agent that is running outside a server context, that is, an agent that is running in standalone mode.

Under normal conditions, applications are run in a server context. However, if you run your trace in a non-server context (that is, you run a non-server trace), and produce the necessary diagnostic information while significantly reducing the amount of material that needs to be reviewed. Running a non-server trace also rules out server communications as a cause of a problem.

Procedure: How to Generate a Server Trace

To generate a server trace:

1. Turn tracing on by doing one of the following:
   - Go to the Reporting Server browser interface menu bar, select the Main Reporting Server browser interface *Other Options* control icon and then *Enable Traces*.
   - Start the server by issuing the following command:

     ```
     edastart -traceon
     ```

     You must preface edastart with the appropriate path, or place the directory in your system PATH variable.
2. Reproduce the problem.
3. Stop the server.
4. Issue the following command:

   ```
   edastart -savediag
   ```

5. Respond to the prompts to capture, and optionally archive and ship diagnostic information.

Diagnostic information will commonly contain user data. If the release of that data is considered a security concern when shipping to Customer Support, the -savediag feature also allows a diagnostic to be saved and shipped later to allow the site the opportunity to review and cleanse the traces of data of this nature before shipping.

Procedure: How to Generate a Non-Server Trace

To generate a non-server trace:

1. Create a directory under APPROOT to reproduce the problem.
2. Copy any files required for the reproduction to the directory.
3. Switch to the directory.
4. Reproduce the problem using edastart -traceon and one of these switches -t, -x, or -f.
5. Switch to a directory other than the problem reproduction directory.
6. Issue the following command:

   ```
   edastart –savediag
   ```

   You must preface edastart with the appropriate path, or place the directory in your system PATH variable.
7. Respond to the prompts to capture, and optionally archive, diagnostic information.

Diagnostic information will commonly contain user data. If the release of that data is considered a security concern when shipping to Customer Support, the -savediag feature also allows a diagnostic to be saved and shipped later to allow the site the opportunity to review and cleanse the traces of data of this nature before shipping.

Third-Party Software and Licenses

All third-party and TIBCO Software, Inc. license information is available on the Reporting Server browser interface by clicking the Help (?) menu, then either *TIBCO Software, Inc.* or *3rd Party Licenses*.

General Information for a UNIX/Linux Installation

This section covers general information for a UNIX/Linux Installation.

Sample Metadata, Data, and Other Tutorial Samples

The Reporting Server browser interface has a feature on the ribbon and on the application tree (under *new*), *Tutorials* (the Create Tutorial Framework page), which has a pull-down for various samples. The Data Migrator desktop interface also has this feature on the application tree.

There are currently about 10 different tutorial/sample selections available on the pull-down select list to match various customer needs. The bulk of the prior IBISAMP sample objects can be generated by selecting the *Create Legacy Sample Tables and Files* tutorial. Other prior IBISAMP Data Migrator sample objects (usually starting with the characters dm*) are now loaded by choosing their respective Data Migrator tutorials. Under the new method, the tutorials/samples may be loaded to any application, not just IBISAMP.

If you are doing just a software refresh, the prior IBISAMP objects will be unchanged (because a refresh does not touch app directories).

Java Listener JVM Defaults

The Java Listener on AIX has a pre-set value for Maximum Java Heap Size (JVM_MAX_HEAP) because the internal default for Java for this heap size is insufficient, which causes server features to fail. The pre-set value does not reflect any specific tuning, but is simply a known working value. Specific tuning should be done based on application needs.

Other UNIX/Linux operating systems have not shown issues with internal defaults, and are not pre-set. However, applications may benefit from tuning, and it should be done based on application needs.

Procedure: How to Tune the Java Listener From the Reporting Server Browser Interface

To tune the Java Listener from the Reporting Server browser interface:

1. Select *Workspace* from the menu bar.
2. Open the *Java Services* folder.
3. Right-click *DEFAULT* and select *Properties*.

   The Java Services Configuration pane opens.
4. Expand the *JVM Settings* section.
5. Under *Non-standard JVM options*, enter values in the *Initial Java Heap Size* and *Maximum Java Heap Size* fields.
6. Click *Save and Restart Java Services*.

Troubleshooting for UNIX/Linux

To troubleshoot an installation problem, identify your problem in the following list, and follow the link to a description of the solution.

If you cannot find your problem described in the list, and cannot resolve it yourself, contact Customer Support.

Problems:

- ❑ The server starts in safe mode (as indicated by a message in the Reporting Server browser interface at start-up).

  For details, see *Problem: The Reporting Server Starts in Safe Mode* on page 68.
- ❑ A server start request partly fails with *JVM not found* messages written to the edaprint.log.

For details, see *Problem: Java Listener Fails to Start With JVM not found Messages Written to the Log* on page 69.

- In Linux releases only, isetup gives an immediate error about a GLIBC version not found.

  This means that the underlying glibc libraries are not high enough for isetup (nor the server) to run. Examine the error message to determine which version is missing, and then install that GLIBC RPM version (or higher), and any GLIBC dependencies, before proceeding.

- Server with Non OPSYS Security where tscom300.out is also not configured as setuid does not write core dump information to the edaprint log, so there is no snap (core dump) in the diagnostic.

  For details, see *Problem: Setting ulimit to Allow Core Dumps* on page 69.

- Server with OPSYS Security (where tscom300.out is configured as setuid) does not write core dump information to the edaprint log, so there is no snap (core dump) in the diagnostic.

  Many UNIX/Linux environments intentionally limit the ability to read core files in setuid applications (the mode in which Security Provider OPSYS runs) for security reasons. On some platforms, the feature is configurable, but the commands to activate it vary by platform or may not be implemented in earlier OS releases. If the crash can be reproduced in an unsecured server, the core information will be produced. This is the best route to producing a complete save diagnostic. If the server cannot be run unsecured to produce the crash, see the following for details:

  Problem: Forcing Core Dump Information on Solaris on page 70.

  Problem: Forcing Core Dump Information on AIX on page 70.

  Problem: Forcing Core Dump Information on Linux on page 70.

Reference: Problem: The Reporting Server Starts in Safe Mode

Problem: The server starts in safe mode. The Reporting Server browser interface home page displays a message stating that the server is in safe mode and describing what triggered it.

Cause: A common cause for the server starting in safe mode is a problem with the server administrator ID password. For example, the password may have been updated on the operating system but not on the server, so the encrypted copy of the password stored by the server is out of synchronization with the password on the operating system.

Solution: The server administrator can click the *fix* hyperlink, which is displayed under the problem description, to display the relevant pane and resolve the problem.

For example, if the problem is that the server administrator password is out of synchronization:

1. Click the *fix* hyperlink displayed under the problem description.
2. In the left pane, open the *Users* folder, then the *Server Administrator* folder.
3. Click your user ID and select *Properties* from the pop-up menu.

   The Access Control pane is displayed on the right.
4. Type the correct operating system password in the *Password* field, and type it again in the *Confirm Password* field.
5. Click *Save and Restart*.

   The Security Mode pane opens on the right.
6. Click the Home icon in the menu bar to return to the Reporting Server browser interface home page.

Reference: Problem: Java Listener Fails to Start With *JVM not found* Messages Written to the Log

Problem: The listener start request fails with *JVM not found* messages written to the edaprint.log file.

Cause: If the server cannot find the Java Virtual Machine (JVM), the JSCOM Listener will not be able to start, and messages will be written to the server log stating that the JVM cannot be found.

Solution: Set up the JVM as described in *JVM Requirements for Java Services (Server Installations Only)* on page 49.

Reference: Problem: Setting ulimit to Allow Core Dumps

The ulimit value of a process controls how large (in blocks) a core can grow. If the value is set to zero, no dump is produced, and the dump information is not read, therefore, a proper save diagnostic stack trace (snap) cannot be produced.

To check the current value, issue:

```
ulimit -c
```

To set a ulimit so that dump information can be produced, stop the server, set a value, and restart:

```
bin/edastart -stop
ulimit -c 99999
bin/edastart -start
```

The actual size value is in blocks and will vary by need. Since the need is unpredictable, select a number and then check the dump information. If the information is incomplete, increase the value.

Reference: Problem: Forcing Core Dump Information on Solaris

Solaris uses the coreadm command to control the ability to produce core files.

To see the current value, issue:

```
coreadm
```

For secured servers, before the server starts, issue:

```
coreadm -e proc-setid
```

No reboot of OS or service daemons is required, but core files must have a non-zero ulimit –c value.

Reference: Problem: Forcing Core Dump Information on AIX

AIX uses the chdev command to control the ability to produce core files. This command is on by default, so it only needs to be adjusted if it has been turned off.

To see the current value, issue:

```
lsattr -El sys0 -a fullcore
```

For secured server purposes, before the server starts, issue:

```
chdev -l sys0 -a fullcore=true
```

Reference: Problem: Forcing Core Dump Information on Linux

While Linux has options to activate core dumps, none currently work in the context of the server. Linux sites can only use the unsecured server method to produce a complete save diagnostic for a crash.

On some newer Linux releases, even in unsecured mode, the creation of core files is blocked. This is generally caused by not having an /etc/sysctl.d/50-coredump.conf file, or having one without a "kernel.core_pattern=core" setting.

Reference: Problem: Process Core Dumps, Core Produced, No Snap, and Debugger Missing Error

When a process crashes, the operating system generally produces a core dump. The server software is designed to detect this event and use the system debugger to extract the state of the crashed process from the core and produce what is known as a snap. While the specific debugger command may vary by vendor, the standard debugger for the vendor must be installed or a Not Found condition on running the debugger can occur (effectively a core, but no snap information). Some vendors install the debugger in /bin or /usr/bin, which are normally on $PATH, but some vendors use locations not normally on $PATH. This can result in a secondary reason for a debugger Not Found condition. Once the debugger is installed and/or on the $PATH, reproducing the crash condition will then produce the snap information.

Reference: Problem: Server Fails to Start With *Cannot Create Shared Memory* Message Written to edaprint

The full message indicates the need to review edapth traces for r1shmop* entries with errors. If the server was not started with traces, start it with traces, and then view the edapth trace.

One of the r1shmop* entries in the edapth trace will show a specific error, but a common error is size is greater than the system shared memory limit. This particular message indicates that the system kernel value for shared memory needs to be increased. The actual required value is generally a multiple of machine page size (typically 4K, but it can vary). The number of agents a server runs, and other installed software can also be a factor, and the required value may vary (slightly) from release to release.

There are tools, such as *size* and *ps* that will allow an experienced administrator to narrow down the precise shared memory size requirements, considering all of the software in use. However, a good rule of thumb is to increase memory in 10% increments until a working value is found.

Error messages other than shared memory size can occur, in which case, the system message is displayed. These other messages may provide an administrator with enough information to determine the appropriate action. If not, call Customer Support for a review. Actual kernel change commands or steps vary by vendor, so they are not explicitly outlined here.

Procedure: How to Install and Activate the Debuggable Version of the Server

In core dump (crash) situations, the stack information may or may not provide enough information for a problem to be resolved. Debuggable versions of the software will generally provide that information, but would not normally be installed nor used due to the disk overhead they take and they are not optimized for performance.

If a diagnostic is determined to not have enough information and use of debuggables is warranted, Customer Support will inform you to install and activate the debuggable version of the server and re-run the reproduction to capture a new diagnostic with the detailed stack to help troubleshoot the problem.

Caution: *Do not* activate the debuggable version unless explicitly requested to by Customer Support.

To activate the debuggable version of the server:

1. Log on with the server administrator ID (often referred to as iadmin).
2. Download the iserverd archive file (for example, .tar, .zip, or .bck) from the download site to a local directory. Debuggables for UNIX/Linux environments are not normally shipped on the original CD media, but can be made available on CD by special request to Customer Support and requires a lead time of approximately one week. If CD media is being used, mount the media.
3. Run the isetup installation program located in the EDAHOME bin (if download was used) or in the root directory of the CD media.
4. At the main menu, select option 4, *Install Debuggables to the Installation Directory* and follow its steps supplying information similar to when the original install was performed.
5. After completion of isetup, the server may be run in debug mode with the following steps.

   ```
   edastart -stop
   edastart -dbgon
   edastart -start (run until repro is completed)
   edastart -stop
   edastart -dbgoff
   edastart -start
   ```

6. If the debug version is no longer needed, the debuggables may be removed. If a service pack is being installed, the debuggables *must* be removed to prevent mismatches with the new release. To remove the debuggables, change the directory to the home directory of EDAHOME and issue rm -f dbg.

Customer Support will provide you with additional instructions as your situation requires.

Chapter 4

Installation for z/OS

The unified software for z/OS provides a choice of deployment environments, either:

- z/OS Distributed File Service zSeries File System (ZFS) files on UNIX System Services.
- Partitioned data set (PDS) libraries.

To compare their benefits, see *Choosing How to Deploy* on page 76.

In this chapter:

Information You Need Prior to Installation on z/OS

The WebFOCUS Reporting Server is installed by going to the TIBCO™ eDelivery site and downloading the software to be used in the actual installation. By selecting your product, version, and operating system, and accepting the EULA agreement, you may then either select to download the full product or individual files.

If you choose individual files, you must then open the *TIBCO WebFOCUS Reporting Server Software* folder, select a *TIB_wf-rs_*_mvs_zseries.tar* or *TIB_wf-rs_*_zos_zseries.tar* file, where * indicates the release number, *mvs* is a PDS type install, and *zos* is a ZFS type install for your platform, and start the download.

Once the desired file is downloaded, and if necessary, transferred to the actual machine where the installation will occur and into a temporary working directory, untar the .tar file.

More specifically, change directory (cd) to the temporary directory and issue the following command, where the actual .tar file name is the full file name that was downloaded.

```
tar -xvf TIB_wf-rs_*.tar
```

After extraction, proceed with the instructions in the following topics.

The process for a full download is similar. A main directory is created on the desktop with multiple directories and subdirectories. Simply find the applicable TIB_wf-rs_*.* file from the download, transfer, and extract, as previously noted.

You need a server administrator user ID, referred to as *iadmin* in the remainder of this chapter.

- The operating system ID you use when installing the server owns the server files and is the default server administrator for OPSYS mode. You can create a new operating system ID to run and own the server files, or use any ordinary (non-superuser) ID. However, you should not install the server as root.

The server has an email notification feature that requires SMTP mail server information. You can enter these parameters either during installation, or later using the Reporting Server browser interface Administration tool.

z/OS Installation Requirements

Before you install, review the following requirements.

Type	Description
Operating System	z/OS 2.1 or higher The *TIBCO WebFOCUS® Release Notes* maintains a current list of supported operating systems and levels.
Disk Space	For USS Deployment, approximately 6 GB, however, about double the space is needed during installation. For PDS Deployment, approximately 1555 cylinders of 3390 disk for HOME data sets.
IP Ports	Up to six consecutive IP ports (two in reserve for typical extra features). Additional Java Listeners (post-installation option) require additional ports (beyond basic reserve).

Type	Description
Java	Java JRE or Java SDK (also known as JDK) 8 or higher. Used for Java-based adapters, server-side graphics, XBRL, or user-written CALLJAVA applications. For additional information, see *JVM Requirements for Java Services (Server Installations Only)* on page 75. **Note:** Java 8 and Java 11 are explicitly tested and certified to be compatible with the WebFOCUS Reporting Server. Other Java releases may be compatible with the WebFOCUS Reporting Server. If you use an untested Java release, you must self-certify its compatibility with the WebFOCUS Reporting Server and accept responsibility for using an untested release.
Memory Common framework plus per agent memory.	**Per Agent** 20 MB **Common Framework** 500 MB
Web Browser	Needed for using the Reporting Server browser interface. Microsoft Edge Mozilla Firefox® 59 or higher. Google Chrome® 65 or higher.

JVM Requirements for Java Services (Server Installations Only)

The minimum Java JVM release level is 8 or higher, due to required internal components of the server. The Java Listener will not start properly (and will show errors in the edaprint.log file) if 8 (or higher) is not in use.

When a server starts, it adds search directories based on JDK_HOME or JAVA_HOME variables. If JVM is found with the correct bit size and level (8+), the Java Listener will start, send a *start* message to the edaprint.log file, and no further configuration is needed.

If JVM loading fails, the server will start, but should be corrected by setting JDK_HOME or JAVA_HOME to a respective home directory for a Java that matches the required bit size and release level. If both values are declared, JDK_HOME will be used. Set the environment variable in the server EDAENV environment file.

For example:

```
JDK_HOME=/usr/java/64/jdk1.8.0_20
```

Installation for ZFS and PDS

Before installing, read the topics in this section for:

- Guidance on choosing how to deploy on ZFS in UNIX System Services or PDS.
- Configuration information common to both deployments, such as the location of different types of server files.
- An overview of which steps you will need to perform to install your server.

Choosing How to Deploy

z/OS provides you with a choice of deployment environments. You can deploy using either:

- **The z/OS File System (ZFS)** on UNIX System Services (USS). The ZFS-deployed software stores executable code and user data on the ZFS. Security is provided by UNIX file security and by your z/OS security package, such as RACF, *e*Trust CA-Top Secret®, or *e*Trust CA-ACF2®. You install from ISPF and start it using JCL. All other processes occur under USS.
- **Partitioned data sets (PDS)** which deploys software in partitioned data sets. The PDS-deployed software provides most features of the ZFS-deployed software, but removes the requirement for interaction with Unix System Services at installation time and run time. Administration of the software, from a systems perspective, has been streamlined to match that of the classic MVS version of the server (also known as the SSCTL server).

  The PDS deployment environment is designed to support legacy applications and features. New server features that require some ZFS footprint, such as .xlsx support, file uploads, and the stress tool on the Reporting Server browser interface, will not be available.

  To take advantage of these features, you can either deploy the ZFS version or, alternatively, have a mixed environment, where you create a PDS instance for your legacy applications, and have a small ZFS instance just for the administrator to access the Reporting Server browser interface features missing in PDS. Both server instances can have a shared mapped application to exchange data seamlessly.

The following table compares the benefits of each way of deploying on z/OS.

Feature	ZFS / USS	PDS
File Management: **Server** run-time and configuration files	In the UNIX ZFS file system.	In partitioned data sets (PDSs).
File Management: **User** data, metadata, and procedures	In the UNIX ZFS and, optionally, in a PDS.	In a PDS and, optionally, in the UNIX ZFS.
Security	Standard security packages are supported (RACF, *e*Trust, CA-ACF2®, and *e*Trust CA-Top Secret). All directories and files must have their user/group/world attributes correctly set. A user ID with a UID of 0 (that is, a superuser) is required when running the server with security set to OPSYS or a special UNIXPRIV user ID can be used.	Standard security packages are supported (RACF, *e*Trust CA-ACF2, and *e*Trust CA-Top Secret). No additional security is required.
User IDs	A UID of 0 (that is, a superuser) can install, but not administer or connect to, the server. Each user ID that will install, administer, or connect to the server requires a ZFS segment with sufficient space and appropriate file permissions for the tasks that the ID will perform.	Any user ID can install, administer, and connect to the server.

Feature	ZFS / USS	PDS
Adapters	Use a mixture of USS-based and MVS-based libraries/APIs.	Use MVS-based libraries/APIs. The exception is DBMSs that support only USS-based libraries/APIs, such as Db2 CLI and Java-based adapters, such as MS SQL Server, which use vendor libraries/APIs residing in the hierarchical file system.
Traces and Server Log	Accessible from Reporting Server browser interface	These are available on the JES output of the server job.
Reporting Server browser interface Stress Tool	Available from Reporting Server browser interface	Feature not available.
Format XLSX and PPTX	Supported	Not Supported **Note:** As a workaround, you can SET EXCELSERVURL to point to a WebFOCUS ibi_apps context root.
Adobe Flex	Supported	Not Supported
RACF TEMPDSN class	Supported	Supported except for FOCCACHE app
DFM reports stored in approot app	Supported	Not Supported Use standard DFM data sets instead.
Native ! (bang) USS Operating System commands in applications	Supported	Not Supported
Adapter Flat File via FTP Server	Supported	Not Supported

Feature	ZFS / USS	PDS
Reporting Server browser interface Upload file tool	Supported	Not Supported

PDS deployment also requires each user of the server to be identified to USS by means of a default segment definition. For more information, see *USS Segment Requirements* on page 184.

File Locations

The software includes several groups of files used for installation, configuration, and administration. These groups are implemented differently in USS and PDS deployments:

- **Supplied files (EDAHOME),** which contains programs and related files. For more information, see *Supplied Files Location (EDAHOME)* on page 79.
- **Configuration (EDACONF),** which contains the files that control the behavior of each configured instance. For more information, see *Configuration Files Location (EDACONF)* on page 80.
- **Applications (APPROOT),** which is the default location for storing applications. For more information, see *Application Files Location (APPROOT)* on page 82.
- **Profiles,** which contains user and group profiles. For more information, see *Profile Files Location* on page 81.
- **Administration,** which includes a file that specifies server administrators. For more information, see *Administration Files Location* on page 81.

Supplied Files Location (EDAHOME)

The programs and related files are stored in a location referred to as EDAHOME. The installation process copies the software into EDAHOME.

- **In USS** deployment, EDAHOME defaults to the following directory and several subdirectories:

  `ibi/srv90/home`

- **In PDS** deployment, EDAHOME defaults to the following partitioned data sets:

  `high_level_qualifier``.P.HOME.WFS`

where:

high_level_qualifier

Is the high-level qualifier for HOME.DATA and for all other data sets that the installation procedure allocates. We recommend that the high-level qualifier reflect the release of the software (for example, IADMIN.SRV90). However, you can use any site-specific value.

component_type

Designates the type of server component. The values are:

ETC	for script and text files.
BIN	for binary-based object files.
ACX	for the server Access Files.
MAS	for the server Master Files.
FEX	for the server procedure (FOCEXEC) files.
ERR	for error files.
LOAD	for the load library.

Configuration Files Location (EDACONF)

The configuration files are stored in a location referred to as EDACONF. Each configured instance has its own EDACONF, which controls the behavior of that instance.

- **In USS** deployment, EDACONF defaults to the following directory and several subdirectories:

  ibi/srv90/wfs

- **In PDS** deployment, EDACONF defaults to the following partitioned data sets:

  high_level_qualifier.WFS.CONF.*config_type*

where:

high_level_qualifier

Is the high-level qualifier for HOME.DATA and for all other data sets that the installation procedure allocates. We recommend that the high-level qualifier reflect the release of the software (for example, IADMIN.SRV90). However, you can use any site-specific value.

config_type

Designates the type of configuration file.

The primary configuration file is CFG.

The Reporting Server deferred execution configuration files are DEL, RPE, RPF, RPO, RQD, RQF, RQO, and RQP.

Profile Files Location

Server profiles are stored in the following location:

- **In USS** deployment, the location is specified in the environment variable EDAPRFU, and defaults to the following directory:

  `ibi\profiles`

- **In PDS** deployment, the location is the following partitioned data set

  high_level_qualifier`.WFS.CONF.PRF`

  where:

  high_level_qualifier

  Is the high-level qualifier for HOME.DATA and for all other data sets that the installation procedure allocates. We recommend that the high-level qualifier reflect the release of the software (for example, IADMIN.SRV90). However, you can use any site-specific value.

  This PDS is allocated in ddname EDAPROF in the servers JCL.

Administration Files Location

The file that specifies server administrators is located in:

- **In USS** deployment, the location is specified in the environment variable EDAPRFU, and defaults to the following directory:

`ibi\profiles`

- **In PDS** deployment, the location is member ADMIN of the following partitioned data set

  high_level_qualifier`.WFS.CONF.CFG`

  where:

  high_level_qualifier

  Is the high-level qualifier for HOME.DATA and for all other data sets that the installation procedure allocates. We recommend that the high-level qualifier reflect the release of the software (for example, IADMIN90.). However, you can use any site-specific value.

  This PDS is allocated to ddname EDACFG in the servers JCL.

Application Files Location (APPROOT)

The server application files are stored in a location referred to as APPROOT. APPROOT may be shared by multiple applications.

- **In USS** deployment, APROOT defaults to the following directory:

  `ibi/apps`

- **In PDS** deployment, APPROOT defaults to the following partitioned data sets:

  approot`.`*appname*`.`*type*`.DATA`

  where:

  approot

  Designates the root qualifier for the server applications.

  appname

  Designates the name of the application. There will be one *appname* qualifier for each application.

  type

  Designates the type of application component. The values are:

  `ACCESS` for Access Files.

`ETG`	for Data Migrator flow information.
`FOCEXEC`	for procedure files.
`FTM`	for temporary files.
`GIF`	for image files (both GIF and JPG).
`HTML`	for HTML files.
`MAINTAIN`	for Maintain files.
`MASTER`	for Master Files.
`WINFORMS`	for forms.
`DTD`	for XML DTD files.
`FOCCOMP`	for foccomp files.
`FOCSTYLE`	for stylesheet files.
`SQL`	for SQL files.
`XML`	for XML files.
`XSD`	for XML XSD files.
`FOCUS`	for FOCUS data files.

Two applications are generated automatically during installation: IBISAMP and BASEAPP, a default application space.

Step-By-Step Installation Overview

The installation process differs somewhat, depending on how you are deploying the software for z/OS. To deploy using:

❑ **ZFS/USS:**

1. *Installation Requirements for ZFS* on page 85
2. *Installing New on ZFS* on page 87
3. *Starting and Stopping a TIBCO WebFOCUS Reporting Server for ZFS* on page 123
4. *Db2 Security Exit Configuration for ZFS* on page 128
5. *MSODDX for DD Translation for User Subroutines* on page 133
6. *Overriding the Time Zone Setting* on page 133
7. *Adding a Configuration Instance for ZFS* on page 133
8. *Upgrading Your TIBCO WebFOCUS Reporting Server Release for ZFS* on page 143
9. *Performance Considerations for ZFS* on page 165
10. *General Information for a z/OS ZFS Installation* on page 167
11. *Troubleshooting for ZFS* on page 169

❑ **PDS:**

1. *Installation Requirements for PDS* on page 178
2. *Installing New on PDS* on page 185
3. *Starting and Stopping a TIBCO WebFOCUS Reporting Server for PDS* on page 204
4. *Db2 Security Exit Configuration for PDS* on page 209
5. *MSODDX: DDNAME Translation for User Subroutines* on page 214
6. *Overriding the Time Zone Setting* on page 214
7. *Adding a Configuration Instance for PDS* on page 214
8. *Upgrading Your TIBCO WebFOCUS Reporting Server Release for PDS* on page 221
9. *Performance Considerations for PDS* on page 236
10. *General Information for a z/OS PDS Installation* on page 241
11. *Troubleshooting for PDS* on page 243

USS Deployment

The topics in this section describe how to install your software in a ZFS environment on UNIX System Services.

Installation Requirements for ZFS

Before beginning the installation, review all requirements.

Operating System Requirements

The software runs on any supported release of z/OS. For current information about supported releases, see the *TIBCO WebFOCUS® Release Notes*.

In general, the operating system should have the latest cumulative patch levels applied.

Confirm that your server installation software is labeled for your operating system level.

IP Port Number Requirements

The install process prompts for two IP port numbers: the TCP Listener and HTTP Listener. It also uses the next two consecutive ports after the supplied HTTP Listener port for FDS use. This results in a total of four IP ports.

The supplied IP port numbers must be above the IANA registered well-known reserve range (numbers under 1024) and not over the maximum legal number (65535). Additionally, do not use IP port numbers already being used by other applications or products. Netstat, or netstat like commands, should reveal what actual ports are in use.

Browser Requirements

The Reporting Server browser interface requires one of the following web browsers:

- Microsoft Edge.
- Mozilla Firefox® 59 or higher.
- Google Chrome® 65 or higher.

Disk Space Requirements

The server disk space requirement for:

- Installation is 6 GB. Double that size is required during the installation process.

- Run time is a combination of the server software (2 GB) plus the space required for applications, databases, sorts, output preparation, and logs. The actual space required will depend on the number and size of the applications and databases that you deploy to the server.

  You can divide your space requirements in different ways. For example, you may choose to employ one mount point for the working directory for users and trace files (edatemp), and one mount point for the application directory (apps). Another option is to employ one mount point for edatemp, and one for each individual application.

  For more information about using mount points, see the IBM USS documentation.

Memory Requirements

Memory usage of a configured environment consists of the following elements:

- Workspace Manager
- Listeners
- Concurrently running application agents

Actual memory usage depends on application features, and varies depending on the application. The SHRLIBRGNSIZE parameter (defined on SYS1.PARMLIB, member BPXPRMxx) can affect the amount of memory that the server address space will allocate. For SHRLIBRGNSIZE, we recommend the default MVS installation value of 64Mb:

```
SHRLIBRGNSIZE(67108864)
```

Server memory usage:

- The workspace (including Listeners) uses 200 megabytes.
- Each pre-started agent requires 20 megabytes.

The minimum amount of memory for a newly installed server with no workload is 250Mb. However, depending on usage, workload, and configuration options, 500Mb is recommended to start, to be adjusted as needed.

Communications Requirements

You need four TCP/IP ports for each server instance that you configure. Three of these ports must be consecutive. You specify these port numbers during installation. You may require additional ports depending on which options you configure later.

The server supports only IBM TCP/IP. It does not support Interlink or any other third-party TCP/IP.

Installing New on ZFS

To install on z/OS deployed using the ZFS File System and UNIX System Services (USS), perform the following steps.

Step 1. Establish the ZFS Directory for the Software

The installation requires a set of ZFS directories where the product executable files, configuration files and sample applications are loaded. The software also uses ZFS directories for temporary files during the software operation, by default. Application files can be kept in the ZFS directories or in PDS.

To better control the space allocated to the software, we recommend defining a separate ZFS data set, OMVS.IADMIN, and mounting it as /u/iadmin for the exclusive use of the software. Note that both names can be changed and existing ZFS data sets used as an alternative.

The sample JCL in step 1 is for 1 gigabyte of space. The total space that can be allocated to a ZFS data set is dependent on the operating system release and the physical device type. Refer to IBM documentation for more information about ZFS allocation. For an SMS-managed data set, add the appropriate parameters.

Procedure: How to Establish the ZFS Directory for the Software

To establish the ZFS directory for the server:

1. Create the following JCL to define the ZFS data set:

```
//********* JOB CARD GOES HERE ************//
//
//*************DEFINE ZFS ******************//
//DEFIADR EXEC PGM=IEFBR14
//ROOTIAD DD DSNAME=OMVS.IADMIN,
//  SPACE=(CYL,(1200,5),CONTIG,ROUND),DCB=(DSORG=PO),
//  DSNTYPE=ZFS,
//  DISP=(NEW,CATLG,DELETE),
//  STORCLAS=STANDARD
```

2. Add a job card and submit the JCL.
3. Mount the file system by issuing the following commands at the command line in Option 6 of ISPF:

```
MOUNT FILESYSTEM('OMVS.IADMIN')
MOUNTPOINT ('/u/iadmin') TYPE (ZFS) MODE (RDWR)
```

where:

OMVS.IADMIN

Is the name associated with the file system defined in Step 1.

/u/iadmin

Is the mount entry point for the file system. Specify a directory appropriate for your site.

The specified directory must exist before you issue the MOUNT command. Once the directory is created, the minimum permissions for all directory levels leading to iadmin must be 755.

4. Update your BPXPRM*xx* member of SYS1.PARMLIB to permanently mount the file system.

Step 2. Set Up User IDs

To install and run the software, the following types of user IDs are required:

- ❑ Server installation ID (iinstal).
- ❑ OPSYS Server administrator ID (iadmin).
- ❑ PTH Administrator ID (srvadmin).
- ❑ Server system ID (iserver).
- ❑ General IDs (for connecting users).

The number of IDs and their names depend on the needs and configuration of your site.

Software Installation ID (iinstal)

An ID is required to unload the software installation from tape and to create PDSs and ZFS directories. Many sites already have a suitable ID that they use for installing vendor software.

The sample ID name *iinstal* is used throughout the installation procedure to refer to this ID, but you can choose any name. (We have omitted the second "I" from "install" due to a seven-character length restriction in some RACF and *e*Trust CA-Top Secret® environments.) To define iinstal, see *Step 2A. Define the Software Installation ID* on page 90.

OPSYS Server Administrator ID (iadmin)

An ID is required to administer the server. It will own and have full access to server files installed in the ZFS directory that you specify during installation. This ID should be available only to users who require administrative server privileges, such as starting and stopping the server, adding adapters, and changing run-time parameters.

The sample ID name *iadmin* and group *isrvgrp* are used throughout the installation procedure to refer to this ID, but you can choose any names. To define iadmin, if you are using:

- **RACF,** see *Step 2B/RACF. Define the OPSYS Administrator ID With RACF* on page 91.
- **CA-ACF2,** see *Step 2B/ACF2. Define the OPSYS Administrator ID With CA-ACF2* on page 92.
- **CA-Top Secret,** see *Step 2B/Top Secret. Define the OPSYS Administrator ID With CA-Top Secret* on page 92.

PTH Administrator ID

An ID is required to administer the server immediately after initial installation. This ID is defined and maintained solely in the realm of the server.

For more information about running the server in secure mode, see *Step 7. Configure Security* on page 116.

TIBCO WebFOCUS Reporting Server System ID (iserver)

If you plan to run the server with security provider OPSYS, you must create a user ID for internal use by the server. The server will use this server system ID when it needs superuser privileges. For example, it will use it to impersonate a connected user when the server agent is created.

This ID does not need TSO logon privileges. All IDs require an OMVS segment. Be sure never to delete this ID. Doing so would cause server administration problems.

The sample ID name *iserver* is used throughout the installation procedure to refer to this ID, but you can choose any name.

You can define this server system ID as either:

- **A superuser ID.** This is an ID whose security definition specifies UID(0), authorizing it to perform all z/OS UNIX functions without restriction.

  To define iserver using a superuser ID, if you are using:

  RACF, see *Step 2C/RACF. Define the System User ID With RACF* on page 95.

  CA-ACF2, see *Step 2C/ACF2. Define the System User ID With CA-ACF2* on page 96.

  CA-Top Secret, see *Step 2C/Top Secret. Define the System User ID With CA-Top Secret* on page 96.

- **An ID employing profiles with UNIXPRIV for authorization,** which is necessary for certain superuser privileges.

By granting limited superuser privileges with a high degree of granularity to an ID that does not have superuser authority, you minimize the number of assignments of superuser authority at your installation and reduce your security risk.

This is supported for sites using RACF, *e*Trust CA-ACF2®, and *e*Trust CA-Top Secret. Note that global access checking is not used for authorization checking to UNIXPRIV resources.

To define iserver using UNIXPRIV profiles, see *Step 2D. Define the System User ID With UNIXPRIV Profiles* on page 97.

General IDs (for Connecting Users)

Any user requiring access to the server must have a non-superuser ID (that is, it must have a unique UID other than 0) and have an OMVS segment. For information about this, see *Step 2E. Add the OMVS Segment to General User IDs* on page 99.

User ID Installation Scenarios

There are two user ID installation scenarios:

- **Installation and administrator IDs are the same.**

  The user ID must have a unique non-zero UID. It cannot be a superuser. For this scenario, logon to TSO with this ID and do not change the default administrator ID that is presented on the first full panel of the ISETUP installation process.

- **Installation and administrator IDs are different.**

  The *installation ID* can be a superuser or non-superuser, and must have authority over the administrator ID so that it can change ownership of the server directory structure from the installation ID to the administrator ID. The command issued during the installation process to change ownership is shown.

  The *administrator ID* must have a unique non-0 UID. It cannot be a superuser.

Step 2A. Define the Software Installation ID

When defining the software installation ID:

- The installation ID requires read access to the BPX.FILEATTR.APF facility class.
- The installation ID requires an OMVS segment.

- The installation ID can be any existing user ID. If it is the same as the administrator ID (iadmin), see one of the following topics for a sample definition. If you are using:
  - **RACF,** see *Step 2B/RACF. Define the OPSYS Administrator ID With RACF* on page 91.
  - **CA-ACF2,** see *Step 2B/ACF2. Define the OPSYS Administrator ID With CA-ACF2* on page 92.
  - **CA-Top Secret,** see *Step 2B/Top Secret. Define the OPSYS Administrator ID With CA-Top Secret* on page 92.

Step 2B/RACF. Define the OPSYS Administrator ID With RACF

The server administrator ID requires an OMVS segment.

To define the server administrator ID with RACF:

1. Have the Security Administrator issue the following RACF commands:

```
ADDUSER iadmin PASSW(xxxx)
DFLTGRP(ISRVGRP)
OMVS(UID(8) HOME('/u/iadmin') PROGRAM('/bin/sh)')
TSO(ACCTNUM(12345) PROC(PROC01))
```

2. Verify that the ADDUSER command completed successfully by issuing the following command, and be sure that the command is available to the iadmin ID:

```
[TSO] LISTUSER iadmin OMVS NORACF
```

   You should receive the following response:

```
USER=iadmin
OMVS INFORMATION
------------------------------
UID=0000000008
HOME=/u/iadmin
PROGRAM=/bin/sh
```

3. A Security Administrator must update the Facility classes of RACF, using the following commands issued with ISPF Option 6:

```
RDEFINE FACILITY BPX.FILEATTR.APF  UACC(NONE)
PERMIT BPX.FILEATTR.APF CL(FACILITY) ID(iadmin) ACCESS(READ)
```

4. Refresh the RACF Facility class so that these commands will take effect.

```
SETROPTS RACLIST(FACILITY) REFRESH
```

5. Continue by verifying the server administrator ID, as described in *How to Verify the OPSYS Administrator ID* on page 94.

Step 2B/ACF2. Define the OPSYS Administrator ID With CA-ACF2

The server administrator ID requires an OMVS segment.

To define the server administrator ID with eTrust CA-ACF2:

1. To define the ID that will administer the server, issue the following commands:

   ```
   SET LID
   INSERT iadmin GROUP(admin) PASSWORD(pass) STC
   SET PROFILE(USER) DIV(OMVS)
   INSERT iadmin UID(n) HOME(/) OMVSPGM(/bin/sh)
   ```

   where:

   iadmin

   Is the ID you are creating to administer the server.

   admin

   Is the group in which iadmin will reside.

   pass

   Is the password for iadmin.

   n

   Is the UID.

2. Continue by verifying the server administrator ID, as described in *How to Verify the OPSYS Administrator ID* on page 94.

Step 2B/Top Secret. Define the OPSYS Administrator ID With CA-Top Secret

The server administrator ID requires an OMVS segment.

To define the server administrator ID with eTrust CA-Top Secret:

1. Create a department ID for everyone defined to eTrust CA-Top Secret who will be using the server, by issuing the command

   ```
   TSS CRE(dept) TYPE(DEPT) NAME('formal department name')
   ```

   where:

   dept

   Is the name of the department you are creating.

   formal department name

   Is the label you want to associate with the new department.

2. For users within the department you just created for the server, you can define resource access within a group. To define an ID for that group, issue the command

   ```
   TSS CRE(deptgrp) NAME('dept group') DEPT(dept) TYPE(GROUP) GID(n)
   ```

   where:

   deptgrp

   Is the name of the group you are creating.

   dept group

   Is the label you want to associate with the new group.

   dept

   Is the name of the department you created.

   n

   Is the number you want to assign to the new group.

3. Create the iadmin ID and attach it to the new department by issuing the following commands

   ```
   TSS CRE(iadmin) NAME('iadmin id')
   TYPE(USER) DEPT(dept) PASSWORD(pass)
   GROUP(deptgrp) DFLTGRP(deptgrp)
   ```

   where:

   iadmin

   Is the ID you are creating to administer the server.

   iadmin id

   Is the label you want to associate with the new ID.

   dept

   Is the name of the department that you created.

   pass

   Is the password for the ID you are creating.

   deptgrp

   Is the group you created.

4. Issue the following command to define the user's USS shell program (using OMVSPGM), facility access (using FAC), and, optionally, the initial directory (using HOME).

The OMVS segment of the ACID defines the ACID's UID, the user's home directory, and the initial program that the user will run. The initial program is generally the shell program that the user invokes.

```
TSS ADD(iadmin) UID(n) [HOME(/u/dir)] OMVSPGM(/bin/sh) FAC(BATCH,TSO)
```

where:

iadmin

Is the ID you created to administer the server.

n

Is the UID. It cannot be 0 (zero).

HOME

Defines the initial directory path name. If it is omitted, USS sets the user's initial directory to the root directory.

dir

Is the ID home directory.

5. Issue the following command

```
TSS PER(iadmin) IBMFAC(BPX.FILEATTR.APF) ACC(READ)
```

where:

iadmin

Is the ID you created to administer the server.

6. Continue by verifying the server administrator ID, as described in *How to Verify the OPSYS Administrator ID* on page 94.

Procedure: How to Verify the OPSYS Administrator ID

To verify the server administrator ID:

1. Verify that the home directory of the server administrator ID is correct by logging on to the server administrator ID (if not already logged on) and issuing the following command from ISPF option 6:

```
OSHELL pwd
```

You should receive the following response:

```
/u/iadmin
```

This directory should be the home directory specified in the UID definition for iadmin.

2. For a second confirmation, issue the following command:

   ```
   OSHELL echo $HOME
   ```

   You should receive the following response:

   ```
   /u/iadmin
   ```

3. Verify that the server administrator ID has a unique UID and the correct GID defined by issuing the following command and press Enter:

   ```
   OSHELL id
   ```

   You should receive the following response:

   ```
   uid=8(IADMIN) gid=50(ISRVGRP)
   ```

   This UID and GID should match what is defined in the OMVS segment.

Step 2C/RACF. Define the System User ID With RACF

The RACF commands in this procedure must be issued by the Security Administrator. The server system user ID does not require logon authority.

To define the server system user ID with RACF:

1. Issue the following RACF command

   ```
   ADDUSER iserver DFLTGRP(OMVSGRP) OMVS(UID(0)) NOPASSWORD
   ```

   where:

   iserver

   Is the account you use for the system server ID.

2. Verify that the above ADDUSER command completed successfully by issuing the following command:

   ```
   [TSO] LISTUSER iserver OMVS NORACF
   ```

   You should receive the following output:

   ```
   USER=iserver
   OMVS INFORMATION
   ------------------------------
   UID=0000000000
   HOME=/u/iserver
   PROGRAM=/bin/sh
   ```

Step 2C/ACF2. Define the System User ID With CA-ACF2

To define the server system user ID with *e*Trust CA-ACF2, issue the following commands:

```
SET LID
INSERT iserver NAME(iserverID) GROUP(pgm)
SET PROFILE(USER) DIV(omvs)
INSERT iserver UID(0) HOME(/) PROGRAM(/bin/sh)
SET PROFILE(GROUP) DIV(omvs)
INSERT pgm GID(n)
```

where:

iserver

Is the ID you are defining for the server system ID.

iserverID

Is the description you want to associate with the system server ID.

pgm

Is the ID group.

omvs

Is the name of your OMVS division.

n

Is the group ID.

Step 2C/Top Secret. Define the System User ID With CA-Top Secret

To define the server system user ID with *e*Trust CA-Top Secret:

1. Issue the following commands

   ```
   TSS CRE(iserver) TYPE(USER) NAME('server system ID')
   DEPT(dept) PASS(pass,0) SOURCE(INTRDR)
   ```

   where:

   iserver

   Is the name you wish to assign to the server system ID you are defining.

   dept

   Is the name of the department you created in step 2b.

   server system ID

   Is the label you want to associate with the new ID.

pass

Is the ID password.

This password never expires.

Note that the SOURCE(INTRDR) setting prevents this ACID from logging on.

2. Define the required access for the server system ID by issuing the following command

```
TSS ADD(iserver) UID(0) HOME(/) OMVSPGM(/bin/sh) GROUP(deptgrp) DFLTGRP(deptgrp)
```

where:

iserver

Is the server system ID.

deptgrp

Is the name of the group you created in step 2b.

3. You can choose to audit the server system ID. Each time the ACID is used, an audit record will be written to the eTrust CA-Top Secret audit tracking file. To set this option, issue the following command

```
TSS ADD(iserver) AUDIT
```

where:

iserver

Is the server system ID.

Step 2D. Define the System User ID With UNIXPRIV Profiles

Resource names in the UNIXPRIV class are associated with z/OS UNIX privileges. In order to use authorization to grant z/OS UNIX privileges, you must define profiles in the UNIXPRIV class protecting these resources. The UNIXPRIV class must be active. If you are using RACF, SETROPTS RACLIST must be in effect for the UNIXPRIV class.

To use profiles in the UNIXPRIV class to grant authorization for superuser privileges to a server system ID that does not have superuser authority (UID=0), you must assign:

READ access for `SUPERUSER.FILESYS.CHOWN`

CONTROL access for `SUPERUSER.FILESYS`

Note:

- It is strongly recommended that you do not assign TSO privileges to the UNIXPRIV user ID. This can be done by adding the keyword NOPASSWORD to the RACF command ADDUSER.

- The installation routine ISETUP will ask for the server system ID (default ISERVER). It will check if the supplied userid has a UID of 0. If it does not, UNIXPRIV authorization is assumed. This will result in an entry in the ibi/srv90/WFS/bin/edaserve.cfg file as follows:

  ```
  server_system_id = ISERVR3/PRIV
  ```

  rather than

  ```
  server_system_id = ISERVER
  ```

If you installed the software with the server system ID pointing to a superuser ID (UID=0), and then decide to use UNIXPRIV user ID, the value in the edaserve.cfg file must reflect the /PRIV syntax. Edit the file manually or using the Reporting Server browser interface, click *Workspace*, *Configuration/Monitor*. Open the *Configuration Files* folder, double-click *Workspace*, and change the server_system_id value before starting the server.

For more information about UNIXPRIV authorization, for:

- **RACF**, see the *IBM Security Server RACF Security Administrator's Guide.*
- **ACF2**, see the *eTrust CA-ACF2 Security Cookbook.*
- **Top Secret**, see the *eTrust CA-Top Secret Security Cookbook.*

Example: System User ID With UNIXPRIV

The server system ID requires different authorities in order to be used with UNIXPRIV. The following RACF example lists the authorities for a system server ID with UNIXPRIV authorization, named ISERVR3. Authorizations for your site may differ.

```
Occurrences of ISERVR3
In standard access list of general resource profile UNIXMAP U100122
In standard access list of general resource profile TSOAUTH RECOVER
In standard access list of general resource profile TSOAUTH JCL
In standard access list of general resource profile ACCTNUM EDA
In standard access list of general resource profile UNIXPRIV
   SUPERUSER.FILESYS.CHOWN
In standard access list of general resource profile UNIXPRIV
   SUPERUSER.FILESYS
Owner of profile ISERVR3.* (G)
First qualifier of profile ISERVR3.* (G)
In access list of group EDA
User entry exists
```

Step 2E. Add the OMVS Segment to General User IDs

To add the OMVS segment to general user IDs:

1. For all users connecting to servers, ensure that each user ID has an OMVS segment (or is set up to use a default user ID as documented in the IBM manual *UNIX System Services Planning*).

   For example, to modify an existing RACF TSO user ID profile, from ISPF Option 6, issue the following command

   ```
   ALTUSER user_ID OMVS(UID(nnn) HOME('/u/user_ID') PROGRAM('/bin/sh'))
   ```

   where:

   user_ID

   Is the user ID you are modifying.

Step 3. Collect Required Information for Adapters

For current information about which adapters are supported, see the *TIBCO WebFOCUS® Adapter Administration* manual.

You must provide information to configure the adapters that you want to install. The installation procedure automatically prompts you for this information. When you are prompted for an optional steplib, ddname, or environment variable, the installation procedure will indicate this with an OPT> prompt.

If you are using non-APF-authorized DBMS libraries, you must allocate the libraries to the ddname TASKLIB in IRUNJCL. The installation routine collects the information and allocates the required libraries in STEPLIB.

After you have installed and configured the server, you will be able to further configure your adapters using a web-based server configuration tool called the Reporting Server browser interface.

The following table describes what information you need to provide for each adapter that you have. (If an adapter is not listed, no information needs to be provided for it.) Note that the table refers to:

- **EDAENV.** This parameter file is a member of

  high_level_qualifier.WFS.DATA

- **IRUNJCL.** This procedure starts the server, and is a member of the configuration library

  high_level_qualifier.WFS.DATA

where:

high_level_qualifier

Is the high-level qualifier for HOME.DATA and for all other data sets that the installation procedure allocates. We recommend that the high-level qualifier reflect the release of the software (for example, IADMIN.SRV90). However, you can use any site-specific value.

Adapter	Information you must provide
Adabas	Provide the data set name for the following STEPLIB allocation: ❑ load library This is required only for the synonym creation process. For example, in a production environment in which all synonyms already exist, you can omit this. When you configure the adapter, you will need to provide the name of the Adabas source library and the associated data set name.
CA- DATACOM	Provide the data set names for the following STEPLIB allocations: ❑ CUSLIB load library ❑ CAILIB load library ❑ utility library ❑ URT library
CA- IDMS (both DB and SQL)	Provide the data set names for the following STEPLIB allocations: ❑ load library ❑ DBA load library Provide the data set names to which the following ddnames are allocated: ❑ SYSIDMS. Check with your CA-IDMS DBA regarding this ddname. ❑ SYSCTL. Is the library corresponding to the central version you want to use.

Adapter	Information you must provide
Call Java	You must have the JDK installed. Provide a value for the following environment variables: ❑ CLASSPATH. Provide the paths of the .jar files that you want to access. These paths will be appended to CLASSPATH. ❑ This adapter requires configuration of the JSCOM3 listener. The path to JVM must be provided using either JDK_HOME or JAVA_HOME. The installation will prompt for it.
CICS Transaction	Provide the data set name for the following STEPLIB allocation: ❑ CICS EXCI load library
Db2 CAF	Provide the data set names for the following STEPLIB allocations: ❑ SDSNLOAD load library For security information, see *Db2 Security Exit Configuration for ZFS* on page 128. ❑ SDSNEXIT load library (optional)
Db2 CLI	Provide the data set names for the following STEPLIB allocations: ❑ SDSNLOAD load library For security information, see *Db2 Security Exit Configuration for ZFS* on page 128. ❑ SDSNLOD2 load library ❑ SDSNEXIT load library (optional; this is needed only for an explicit connection). Provide a value for the following environment variable: ❑ DSNAOINI, which contains the full path and file name of the Db2 CLI .ini file.

Adapter	Information you must provide

EJB	You must have the JDK installed.
	
	Provide a value for the following environment variables:
	
	❑ CLASSPATH. Provide the paths of the .jar files that you want to access. These paths will be appended to CLASSPATH.
	
	If you are deploying the adapter to access an EJB on a:
	
	❑ WebLogic server, specify the following path:
	
	`/pathspec/weblogic.jar`
	
	❑ WebSphere server, specify the following paths:
	
	`/pathspec/websphere.jar`
	`/pathspec/ejbcontainer.jar`
	
	(one for each EJB container)
	
	❑ This adapter requires configuration of the JSCOM3 listener. The path to JVM must be provided using either JDK_HOME or JAVA_HOME. The installation will prompt for it.

IMS	Provide the data set names for the following STEPLIB allocations: ❑ DFSPZP load library (optional; not needed if PZP modules are stored in the DFSRESLB library) ❑ DFSRESLB load library
JDBC	You must have the JDK installed. Provide a value for the following environment variables: ❑ CLASSPATH. Provide the paths of the .jar files that you want to access. These paths will be appended to CLASSPATH. ❑ This adapter requires configuration of the JSCOM3 listener. The path to JVM must be provided using either JDK_HOME or JAVA_HOME. The installation will prompt for it.

Adapter	Information you must provide
Microsoft SQL Server	Select the Call Java adapter, in addition to the Microsoft SQL Server adapter. Provide a value for the following environment variables: ❑ CLASSPATH. Provide the paths to the following files. These paths will be appended to CLASSPATH. ❑ msbase.jar ❑ mssqlserver.jar ❑ msutil.jar ❑ This adapter requires configuration of the JSCOM3 listener. The path to JVM must be provided using either JDK_HOME or JAVA_HOME. The installation will prompt for it.
Millennium	Provide the data set name for the following STEPLIB allocation: ❑ load library
Model 204	Provide the data set name for the following STEPLIB allocation: ❑ load library
MQSeries	Provide the data set names for the following STEPLIB allocations: ❑ SCSQLOAD load library ❑ SCSQAUTH load library
NATURAL Batch	Provide the data set name for the following STEPLIB allocation: ❑ NATURAL load library
SAP (SQL)	Provide values for the following environment variables: ❑ LIBPATH, which contains the path to SAP RFC SDK. ❑ SAP_CODEPAGE=0126, or the correct SAP code page for your language environment.

Adapter	Information you must provide
SAP BW	Provide values for the following environment variables: ❑ LIBPATH, which contains the path to SAP RFC SDK.SAP_CODEPAGE=0126, or the correct SAP code page for your language environment.
Supra	Provide the dataset name for the following STEPLIB allocations: ❑ LINKLIB load library. ❑ INTERFLM load library. ❑ ENVLIB load library.

Step 4. Optional Low-Level Qualifier Changes

We recommend retaining the default low-level qualifiers that are supplied for the installation libraries. However, if you need to change any of them (for example, to conform to site-specific naming conventions), you can do so by editing them in member USSSNAME of *high_level_qualifier*.HOME.DATA. You can see a list of the qualifiers in *Default Low-Level Qualifiers* on page 104.

Caution: If you change any low-level qualifiers and do not reflect those changes exactly in USSSNAME, you will experience problems with the server installation and operation.

Once you have finished changing any names, continue with *Step 5. Run ISETUP* on page 105.

Reference: **Default Low-Level Qualifiers**

The following low-level qualifiers are set in *high_level_qualifier*.HOME.DATA(USSSNAME):

```
//          SET  EDAUSSD='HOME.DATA'        Server installation library
//          SET  EDAUSSL='HOME.LOAD'        Server base load library
//          SET  WFSUSSD='WFS.DATA'         WebFocus Reporting server
//          SET  CGWUSSD='CGW.DATA'         Communications Gateway
//          SET  CLNUSSD='CLN.DATA'         Client
//          SET  EDACICS='HOME.CICS.LOAD'   CICS load library
```

Step 5. Run ISETUP

Server installation consists of a series of ISPF panels, which gather the required information. After the panel dialog is complete, JCL is created and submitted to install the server on z/OS. This JCL job retrieves the remainder of the MVS libraries and ZFS files from the media and configures a basic working server.

1. Execute the ISETUP member of your *high_level_qualifier*.HOME.DATA using ISPF option 6.

   The first Installation and Configuration panel opens.

```
TIBCO                    Installation and Configuration   Unified Server Install
Command ===>                                                                   P0

Unified Server Installation
Please select one of the following options:

         1. USS/ZFS Deployment

            . Installation files and temporary files in ZFS
            . Application files, like synonyms and procedures, in ZFS (or
              optionally in both ZFS and PDS)

         2. PDS Deployment

            . Installation files and temporary files in PDS
            . Application files, like synonyms and procedures, in PDS (or
              optionally in both PDS and ZFS)


Enter selection (Default=1) ===> 1

Press Enter to continue, PF3 to END                            Version: 9999
```

2. Type *1* and press Enter to continue to the next panel.

   The following panel opens.

```
TIBCO                    Installation and Configuration        z/OS USS Deploy
Command ===>                                                              P1

Please select one of the following options:

         1. Install and Configure
         2. Add Additional Configuration Instance
         3. Refresh Installation (Reinstall, Keep Configurations)

Enter selection (Default=1) ===> 1
Input source (Option 1 or 3)===> D                      (T)ape or (D)isk
Installation Userid         ===> IADMIN                 Logged on Userid
OPSYS Administrator Userid  ===> IADMIN                 Server install only
PTH Administrator Userid    ===> srvadmin               Server install only
PTH Administrator Password  ===>                        Retype  ===>
Umask setting to use        ===> 0022                   Server install only


Enter Job Card information                 Override JOB name checking ===> N
===> // JOB (ACCT INFO),____________________________________________________
===> //*___________________________________________________________________
===> //*___________________________________________________________________
Press Enter to continue, PF3 to END
```

3. Complete the panel as follows.

Field	Instructions
Enter selection	Accept the default value 1, *Install and Configure*, for a new installation. For option 2, *Add Additional Configuration Instance*, see *Adding a Configuration Instance for ZFS* on page 133. For option 3, *Refresh Installation*, see *Upgrading Your TIBCO WebFOCUS Reporting Server Release for ZFS* on page 143.
Input source	Enter the input source *D*.
Installation Userid	Shows the current logon ID. It cannot be changed.
OPSYS Administrator Userid	Initially, this field shows the same ID as the installation user ID. If the installation user ID is a superuser (UID=0), you must specify a non-superuser ID to administer the server. Specify this ID here.

Field	Instructions
PTH Administrator Userid	An ID is required to administer the server immediately after initial installation. This is defined and maintained solely in the realm of the server. Defaults to *srvadmin* and it can be changed here. For more information about running the server in secure mode, see *Step 7. Configure Security* on page 116.
PTH Administrator Password	Password for the PTH Administrator ID. It cannot be left blank and must be matched at Retype field.
Umask setting to use	Shows the current umask setting for the iadmin ID. The JCL passes this setting to the server for use at run time. Every time the server creates a file in the .../ibi/profiles or .../ibi/apps directory structures (usually in response to Reporting Server browser interface activity), the server assigns to the file the default permissions 666 filtered by the umask value. You specify whichever umask value is necessary to mask out the permissions you do not want to grant. For example, if you specify a umask value of 0022, the server creates files with the permissions 644: umask 0022 is subtracted from the default 666, disallowing the group and world write permissions.
Enter Job Card information	To provide JOB card information for submitting jobs to the JES queue, provide a valid job name (a maximum of seven characters following the // on the first JCL line), which defaults to the user ID that you are currently using. This job name is used for multiple submissions (for example, *jobname*A, *jobname*B, *jobname*C, and so on) in the JCL generated by the installation procedure.
Override JOB name checking	To provide your own JOB card information, including JOB name, enter *Y* and provide valid JOB card information in the *Enter Job Card information* field. The JOB card information that you enter will be used for each job that is submitted.

If you used the same user ID for both installation and administration, skip to Step 6. Otherwise, continue with Step 4.

4. Press Enter to continue to the next panel.

   The following panel opens.

```
TIBCO                    Installation and Configuration        z/OS USS Deploy
Command ===>                                                              P5

                 Please read the following information carefully.

The installation userid and the administrator userid provided are different.
Therefore at the end of the installation process, which will run under the
installation userid, the ownership of the server files in the ZFS file system
will be changed from userid IINSTAL  to userid IADMIN

(If IINSTAL  is not a super user or does not have the authority to perform
this change, the installation will fail.)

An installation PDS will also be created with install and runtime JCL members.
The install JCL will use the JCL previously provided. The runtime JCL (to be
submitted by IADMIN   userid) may require different JOB card information. If
so, please provide it below otherwise the previously entered JCL will be used.

Enter Job Card information (runtime JCL)   Override JOB name checking ===> N
===> // JOB (ACCT INFO),____________________________________________________
===> //*___________________________________________________________________
===> //*___________________________________________________________________
Press Enter to continue, PF3 to return to previous menu
```

   This panel appears only if you provided two different user IDs in the previous panel.

   The installation process will change ownership of ZFS files from the installation ID (iinstal) to the administrator ID (iadmin). The installation ID must have authority to issue the chown command to make this change of ownership. This action is taken at the end of the installation process.

5. Complete the panel as follows.

Field	Instructions
Enter Job Card information	To provide JOB card information for submitting the run-time jobs to the JES queue, provide a valid job name (a maximum of seven characters following the // on the first JCL line), which defaults to the user ID that you are currently using. This job name is used for multiple submissions (for example, *jobname*A, *jobname*B, *jobname*C, and so on) in the JCL generated by the installation procedure.

Field	Instructions
Override JOB name checking	To provide your own JOB card information, including JOB name, enter *Y* and provide valid JOB card information in the *Enter Job Card information* field. The JOB card information that you enter will be used for each run-time job that is created.

6. Press Enter to continue to the next panel.

   Note that in the current panel (and some later panels), if you are running ISETUP from:

   - *high_level_qualifier*.HOME.DATA, the panel will display default values for some fields.
   - Any other library, the panel will not display any default values.

   In this and some later panels, you can see a field default value (if one exists) by blanking out the field and pressing Enter.

```
TIBCO                    Installation and Configuration        z/OS USS Deploy
Command ===>                                                              PN
                                New Installation

Please enter the following information for WebFocus Reporting Server

 Input Media Location
  Directory name of input    ===> /u/iadmin/download

 Product Installation parameters (blank any field for default)
  ZFS Base Directory         ===> /u/iadmin
  Application Directory      ===> /u/iadmin/ibi/apps
  Profile & admin Directory  ===> /u/iadmin/ibi/profiles
  Server System Userid       ===> ISERVER
  HTTP Listener Port         ===> 8121        TCP Listener Port  ===> 8120

 MVS Installation Libraries
  EDACONF Library            ===> IADMIN.SRV77.WFS.DATA
  EDACONF Library Unit       ===> SYSDA    Type ===> VOL=SER  ===>
  EDAHOME Library            ===> IADMIN.SRV77.HOME.LOAD
  EDAHOME Library Unit       ===> SYSDA    Type ===> VOL=SER  ===>

Press Enter to continue, PF3 to return to previous menu
```

   Complete the panel as follows.

Field	Instructions
Input Media	
Directory name of input	Provide the name of the directory in which the installation files reside.
General Installation Parameters	

Field	Instructions
Base Directory	This indicates where to install the software. The default value is the home directory of the user ID you are using to install the product. Change this value, if necessary, to a valid directory that has space for the installation. The installation procedure checks whether this directory exists and has enough space. If either test fails, you will receive a message indicating the failure and available options.
Application Directory	This indicates where application components will reside. The default value is based on the value specified for *Base Directory*. To specify another location for application components, change the value for this field.
Profile & Admin Directory	This indicates where user profiles and administration files will reside. The default value is based on the value specified for *Base Directory*. To specify a different location for application components, change the value for this field.
Server System Userid	This shows the default value, ISERVER. To change this value, see the requirements in *Step 2. Set Up User IDs* on page 88.
HTTP Listener Port	This indicates the port number that the server will use for HTTP. It is the first of three connection ports that must be available to the server. For example, if you choose port 8101, then ports 8101, 8102, and 8103 are used by the server. Ensure that you choose ports that are not currently being used.
TCP Listener Port	This is the port number of the TCP Listener. The default is one less than the port specified for the HTTP Listener, but it can be any port number other than the three reserved for HTTP.
MVS Installation Libraries	

Field	Instructions
EDACONF Library	This is the full data set name the installation procedure will use to allocate the EDACONF configuration library on MVS. If you are running from *high_level_qualifier*.HOME.DATA, this field will have the default value *high_level_qual*.WFS.DATA. If you used another name to unload the first data set, this field will be blank. On subsequent running of ISETUP, the previous value used will be displayed. Change the value as necessary.
EDACONF Library Unit/ Type	These show the values that the installation process will use to allocate the EDACONF library on MVS. If necessary, you can change these to site-specific values. Type can be **VOL=SER** (default), **DATACLAS**, **MGMTCLAS**, or **STORCLAS**.
EDAHOME Library	This is the full data set name the installation procedure will use to allocate the EDAHOME load library on MVS. If you are running from *high_level_qualifier*.HOME.DATA, this field will have the default value *high_level_qualifier*.HOME.LOAD. If you used another name to unload the first data set, this field will be blank. On subsequent running of ISETUP, the previous value used will be displayed. Change the value as necessary.
EDAHOME Library Unit/Type	These show the values that the installation process will use to allocate the EDAHOME load library on MVS. If necessary, you can change these to site-specific values. Type can be **VOL=SER** (default), **DATACLAS**, **MGMTCLAS**, or **STORCLAS**.

7. Press Enter to continue to the next panel.

   The Data Adapter panel may open before the Demonstration Files panel. If the Data Adapter panel opens, continue with Step 10. Otherwise, skip to Step 11.

8. The Data Adapter panel lists adapters that require the allocation of MVS libraries in IRUNJCL or environment variables in the EDAENV member.

   To select specific adapters:

   a. Type *Y* next to the required adapters and press Enter.

   b. Supply the requested information, which is described in *Step 3. Collect Required Information for Adapters* on page 99.

After you have finished installing and configuring, you can use the Reporting Server browser interface to finish configuring these adapters, and to configure adapters that do not have MVS JCL requirements.

c. Press Enter to continue to the next panel.

The JSCOM3 Listener configuration panel opens.

9. Configuration of the JSCOM3 Listener is either optional or mandatory depending on which adapters were selected. If any Java-based adapters were selected (EJB, Call Java, JDBC, Microsoft SQL Server), the configuration is mandatory.

   a. The panel will prompt for the path to the Java environment to be passed to either JDK_HOME or JAVA_HOME, as described in *JVM Requirements for Java Services (Server Installations Only)* on page 75.

   b. If no Java-based adapters were selected, this configuration might still be desirable to enable server-side graphics and Adobe® Flex® features. To skip the configuration, leave the path blank.

10. Press Enter to continue to the next panel.

The confirmation panel opens.

```
TIBCO                    Installation and Configuration        z/OS USS Deploy
Command ===>                                                              PS
                                New Installation

Please confirm the following information for WebFocus Reporting Server

 Input Media Location
  Directory name of input   ===> /pgm/edaporte2/R729999D/tape
 Product Installation parameters
  Installation userid       ===> IADMIN     OPSYS Admin userid ===> IADMIN
  Installation Directory    ===> /u/iadmin/ibi/srv99/home
  Configuration Directory   ===> /u/iadmin/ibi/srv99/wfs
  Application Directory     ===> /u/iadmin/ibi/apps
  Profile & admin Directory ===> /u/iadmin/ibi/profiles
  Server System Userid      ===> ISERVER      PTH Admin userid ===> srvadmin
  HTTP Listener Port        ===> 8121        TCP Listener Port ===> 8120
  EDACONF Library           ===> IADMIN.SRV82.WFS.DATA
  EDACONF Library Unit      ===> SYSDA    Type ===> VOL=SER  ===>
  EDAHOME Library           ===> IADMIN.SRV82.HOME.LOAD
  EDAHOME Library Unit      ===> SYSDA    Type ===> VOL=SER  ===>

Continue ? (N)o, (C)reate JCL only, (S)ubmit JCL  ===> N   (Enter N, C or S)
Press Enter to process, PF3 to return to previous menu
```

11. Ensure that all values on the Confirmation panel are correct, then select one of the following options:

- **N** to return to the initial panel so that you can change installation values.
- **C** to create JCL which you can submit at a later time. The JCL is placed in your *high_level_qualifier*.WFS.DATA configuration library.

- **S** to create JCL and submit the job immediately.

12.As the job is processed, in SDSF, check JESLOG for errors and return codes.

The following is a table of the jobs created. All members are created in the configuration library (EDACONF).

Job	Description
ISETUPJ1	Main JCL Job stream that is used to install the software.
ISOPTS1	Options used to install the server.

The following members all call procedure IRUNJCL, which is the main server JCL. If you need to change the server JCL, change member IRUNJCL.

Member	Description
ISTART	Starts the server.
ISTOP	Stops the server.
ICLEAR	Clears server resources after an abnormal end.
ICLRDIR	Clears superuser-owned directories from a previously run secure server.
ISAVEDIA	Creates a directory called sd*nnnnnn* and populates it with full diagnostic information.
ISHOW	Shows current workspace status.
ITRCON	Turns on dynamic tracing (server will be started if not already running).
ITRCOFF	Turns off dynamic tracing (server will be started if not already running).

The following members contain batch JCL for auxiliary functions, and are created in the configuration library.

Member	Description
CMRUN	JCL to run Data Migrator batch jobs.

Member	Description
DB2V*ver*PR	Db2 DBRM, where *ver* is your supported version of Db2 referenced in GENDB2 JCL.
GENDB2	JCL to bind the Db2/CAF plan.
IRDAAPPC	Example CLIST to run RDAAPP Client test tool.
IRDAAPPJ	Example JCL to run RDAAPP Client test tool.

The following members contain sample started task JCL, and are created in the configuration library.

Member	Description
IWAYS	A started task that starts the server.
IWAYP	A started task that stops the server.
EDAPRMP	A parameter file used by IWAYP.
EDAENV	A parameter file used by IWAYS, IWAYP, ISTART, and ISTOP.

The following table shows the ZFS directory structures created during the installation process.

Directory Structure	Description
`/u/iadmin/ibi/srv90/tape`	Contains ZFS files from the input media.
`/u/iadmin/ibi/srv90/install`	Working directory for the installation process. Log and error files reside here.
`/u/iadmin/ibi/apps`	The installation creates *baseapp* and one or more sample application directories under this directory.

Directory Structure	Description
`/u/iadmin/ibi/profiles`	This is where user profiles are created, as well as admin.cfg.
`/u/iadmin/ibi/srv90/home`	Software system directories are created under this directory.
`/u/iadmin/ibi/srv90/wfs`	Configuration directories are created under this directory.

Step 6. Test the Installation

This section describes how to verify server installation.

Procedure: How to Test the Installation

1. Log on to TSO as iadmin.
2. Submit the ISTART JCL to start the server. This executes the IRUNJCL proc.
3. Check the job output for errors. Look for the EDAPRINT message:

   ```
   (EDA13023) ALL INITIAL SERVERS STARTED
   ```

4. Start the Reporting Server browser interface by opening a browser pointed at the listener port of the server. The URL format is

   `http://host:port`

   where:

   host

   Is the name of the machine on which the server is installed.

   port

   Is one port higher than the port specified when installing the server. For example, if you specified port 8100 during installation, then use port 8101 to access the Reporting Server browser interface.

   The Reporting Server browser interface opens.

5. If the Reporting Server browser interface opens and displays application tree folders in the left pane, the server is working because it uses its own underlying data access and reporting technologies to visualize the application tree. The server may be further data tested (if desired).

6. Continue with adapter configuration, as described in the *TIBCO WebFOCUS® Adapter Administration* manual.

When you are finished using the server, you can use the Reporting Server browser interface to stop the server by going to the Reporting Server browser interface menu bar, selecting *Workspace*, and then *Stop*.

If you experience problems at start-up, examine the job output for more information.

Step 7. Configure Security

If you will be configuring your server with an OPSYS security provider, you must perform the instructions in the following topics. (For PTH, DBMS, and LDAP security providers, skip these topics.)

- *How to Configure Security With All Security Products* on page 118, regardless of which security product you use.
- *How to Configure Security With eTrust CA-ACF2* on page 119 if you use eTrust CA-ACF2.
- *How to Configure Security With eTrust CA-Top Secret* on page 120 if you use eTrust CA-Top Secret.

You can see a full description of all server security providers in the Reporting Server browser interface help, and also in the *TIBCO WebFOCUS® Reporting Server Administration* manual. To see it in the Reporting Server browser interface:

1. From the Reporting Server browser interface menu bar, select *Help*, then *Contents and Search*.

   The Reporting Server browser interface Help window opens.

2. In the left pane, expand *Server Administration*.

Security Providers

The default security provider for a new installation is the internal security provider, PTH. The PTH provider implements security using user IDs, passwords, and group memberships stored in the admin.cfg configuration file.

After the initial installation, the Server Administrator that was configured during the installation can start the server and use the Reporting Server browser interface to further customize security settings, for example, to configure alternate or additional security providers, create additional PTH IDs, and register groups and users in a security role. For more information about security providers, see the *Server Security* chapter in the *TIBCO WebFOCUS® Reporting Server Administration* manual.

Procedure: How to Satisfy Security Provider OPSYS Requirements

To run a server with security provider OPSYS, you must perform the following steps. You must do this once after installing and after each refresh of the server with fixes.

Set up tscom300.out as a root-owned SUID program:

1. If the server is running, bring it down.
2. Log on to the system as root, or issue the su root command.
3. Change your current directory to the bin directory of the home directory created during the installation procedure.

   For example, type the following command:

   ```
   cd /home/iadmin/ibi/srv90/home/bin
   ```

4. Change file ownership and permissions by typing the following commands:

   ```
   chown root tscom300.out
   chmod 4555 tscom300.out
   ```

5. Verify your changes by issuing the following command:

   ```
   ls -l tscom300.out
   ```

   The output should be similar to the following:

   ```
   -r-sr-xr-x 1 root iadmin 123503 Aug 23 04:45 tscom300.out
   ```

   Note the permissions and ownerships.

When you start the server, it will now run with security provider OPSYS.

The chmod and chown steps will need to be repeated after any server upgrade since the tscom300.out file is replaced during an upgrade and the attributes are lost.

Note: The server will issue RACROUTE REQUEST=VERIFY calls to authenticate users, so all users must have access to APPL MSO, which identifies our server.

Note: If this Security Provider OPSYS step has been configured and the site later decides to switch to Security OFF, special steps must be taken to ensure the mode remains after a full server shutdown (where edastart -start is used to restart the server). The steps are:

1. After the server recycles from the change to OFF, use the Reporting Server browser interface to open the environment configuration file of the server by clicking *Workspace* and expanding the *Configuration Files* folder, followed by the *Miscellaneous* folder.
2. Double-click *Environment - edaenv.cfg* to edit the file and add the *EDAEXTSEC=OFF* variable.
3. Save your work.

After the next full server shutdown, be sure to do an edastart -cleardir before restarting the server. This will clear any root-owned files that would prevent a security OFF server from starting.

Preventing Unsecured Starts After Upgrades

If the server cannot impersonate users because it lacks platform-specific authorization steps, the server start aborts and error messages are written to the edaprint log.

This feature prevents an unsecured server start after a software upgrade if any of the required post-upgrade reauthorization steps are missed on a UNIX, IBM i, or z/OS ZFS deployment. This is not applicable to other platforms. The setting may be placed in any normal server start-up shell or profile that a site is using or in the server edaenv.cfg environment configuration file. The messages vary slightly by platform.

The edaprint messages are:

```
Configured security is 'ON' as set by EDAEXTSEC variable.

Server has no root privilege.

Workspace initialization aborted.

(EDA13171) UNABLE TO START SERVER
```

Procedure: How to Configure Security With All Security Products

To configure server security with RACF, eTrust CA-ACF2, or eTrust CA-Top Secret:

1. Log on to TSO using an ID with read access to the BPX.FILEATTR.APF facility class.
2. Using the name of the actual EDAHOME directory, change file attributes by entering the following TSO commands in ISPF Command Shell (option 6):

   ```
   OSHELL extattr +a /u/iadmin/ibi/srv90/home/bin/tscom300.out
   OSHELL extattr +a /u/iadmin/ibi/srv90/home/bin/tsqprx.out
   ```

3. Verify your changes by issuing the following command:

   ```
   OSHELL ls -E /u/iadmin/ibi/srv90/home/bin/tscom300.out
   OSHELL ls -E /u/iadmin/ibi/srv90/home/bin/tsqprx.out
   ```

   The extended attributes portion of the output should be a-s-.

4. The libraries allocated to STEPLIB in IRUNJCL must be APF-authorized. Any non-APF-authorized libraries must be allocated to the TASKLIB DDNAME.

5. Test server security by repeating the process described in *Step 6. Test the Installation* on page 115.

Procedure: How to Configure Security With *e*Trust CA-ACF2

If you are installing the server to run with *e*Trust CA-ACF2 security package, you may have to apply fix number QO71149 for *e*Trust CA-ACF2 6.4 or QO51462 for *e*Trust CA-ACF2 6.5. If you are installing the server under z/OS 2.1 or higher to run with *e*Trust CA-ACF2 14.0, PTF RO24848 may have to be applied if server USS user IDs are to be defined using the USS default segment. For more information about these fixes, contact Computer Associates.

The MVS address space must have access to those system resources that are required by each user. *e*Trust CA-ACF2 will check for job-level access as well as user-level access. Therefore, the job-level user ID must have access to all data sets. For example, this can be done by setting the MAINT attribute on the *e*Trust CA-ACF2 record for the job-level user ID. Refer to *e*Trust CA-ACF2 technical reference guides for further information.

The job-level user ID of the server should have the Multiple User, Single Address Space (MUSSAS) attribute set to on. If the server is run as a started task, you must enable the started task attribute for the job-level user ID. You must also use the Reporting Server browser interface to define this user ID with OPER authority. For more information, see the *TIBCO WebFOCUS® Reporting Server Administration* manual.

Each user ID must be defined to *e*Trust CA-ACF2.

To create the necessary logon IDs and profile records, issue the following commands:

```
ACF
SET LID
INSERT OMVS GROUP(OMVSGRP) STC UID(0)
INSERT INETD GROUP(OMVSGRP) STC UID(0) HOME(/) OMVSPGM(/bin/sh)
INSERT TCPIP GROUP(OMVSGRP) STC UID(0)
```

For more information, see the following sections in the Computer Associates *eTrust CA-ACF2 Security for z/OS and OS/390 Cookbook*:

- *Defining USS Users*
- *Superusers*
- *HTTP Server*
- *Installation Steps*

Procedure: How to Configure Security With *e*Trust CA-Top Secret

If you use Computer Associates *e*Trust CA-Top Secret, follow these guidelines and refer to the security vendor manual for implementing user-level security.

The TSS PERMIT command for BPX.FILEATTR.APF facility class access is:

```
TSS PER(user_acid) IBMFAC(BPX.FILEATTR.APF) ACC(READ)
```

This allows users to turn on the APF-authorized attribute for a ZFS file. Refer to *z/OS UNIX System Services Support* in the *eTrust CA-Top Secret Security Cookbook* for more information.

To use *e*Trust CA-Top Secret, perform the following steps:

1. Create a *e*Trust CA-Top Secret facility entry for the server security module, *PATHNAM.

   This is an example of a facility entry defining the server to *e*Trust CA-Top Secret:

   ```
   FACILITY DISPLAY
   PGM=*PATHNAM ID=9 TYPE=26
   ATTRIBUTES=IN-USE,ACTIVE,SHRPRF,ASUBM,TENV,NOABEND,MULTIUSER,NOXDEF
   ATTRIBUTES=LUMSG,STMSG,SIGN(M),NOPSEUDO,INSTDATA,NORNDPW,AUTHINIT
   ATTRIBUTES=NOPROMPT,MENU,NOAUDIT,RES,NOMRO,WARNPW,NOTSOC
   ATTRIBUTES=NOTRACE,NOLAB,NODORMPW,NONPWR,NOIMSXTND
   MODE=IMPL
   LOGGING=ACCESS,INIT,SMF,MSG,SEC9
   UIDACID=8 LOCKTIME=000 DEFACID=*NONE* KEY=8
   ```

   For more information, see *How to Define z/OS UNIX System Services Users* in the Computer Associates *eTrust CA-Top Secret Security for OS/390 and z/OS Cookbook*.
2. Within this entry, include *e*Trust CA-Top Secret parameters to establish the proper operating characteristics.

   The ISERVER and IADMIN ACIDs must have authority to the facility you have defined for the server and to the resources within the facility:

   `TSS ADD(region_acid) MASTFAC(facility)` <- defines the facility to CA-Top Secret

   `TSS ADD(user_acid) FAC(facility)` <- adds it to users requiring server access
3. Each user of the server must be defined to *e*Trust CA-Top Secret and given access to the appropriate system resources, including the facility you have defined for the server.

   Each user requires an OMVS segment and ZFS directories.
4. If you are operating with *e*Trust CA-Top Secret HFSSEC=ON, continue with Step 5. Otherwise, skip to Step 7.
5. In the definitions for IADMIN and ISERVER ACIDs (shown in the previous examples), set up the following security authorization:

   ```
   XA HFSSEC = /U.IADMIN
   ACCESS = ALL
   ```

6. *e*Trust CA-Top Secret provides superuser granularity with separate definitions for the following resource names:

```
SUPERUSER.FILESYS.FILE (CONTROL access)
SUPERUSER.FILESYS.CHOWN
SUPERUSER.FILESYS.MOUNT
SUPERUSER.FILESYS.PFSCTL
SUPERUSER.FILESYS.VREGISTER
SUPERUSER.IPC.RMID
SUPERUSER.PROCESS.GETPSENT
SUPERUSER.PROCESS.KILL
SUPERUSER.PROCESS.PTRACE
SUPERUSER.SETPRIORITY
```

   Ensure that the server system ID, ISERVER, which has UID=0, is granted full access to all these resources. Grant access to the superuser-listed resources by means of the UNIXPRIV resource class. For example:

```
TSS ADD(owning_acid) UNIXPRIV(SUPERUSE)
TSS PER(acid) UNIXPRIV(SUPERUSER.FILESYS.FILE) ACC(CONTROL)
```

   For details see the *Superuser Granularity* topic in the Computer Associates *eTrust CA-Top Secret Security for OS/390 and z/OS Cookbook*.

7. After you create a new user ID or change a user UID or GID, you must issue the following command to reflect the updates in Top Secret's in-storage tables:

```
TSS MOD(OMVSTABS)
```

   The following commands can also be used to list all UIDs, GIDs and their owners:

```
TSS WHOOWNS UID(*)
TSS WHOOWNS GID(*)
```

   This information can be used for diagnostic purposes.

   For more information, see the Computer Associates *eTrust CA-Top Secret Security for OS/390 and z/OS Cookbook*.

Example: Facility Entry Defining the Server to CA-Top Secret

The following is an example of a facility entry that defines the server to *e*Trust CA-Top Secret:

```
FACILITY DISPLAY
PGM=*PATHNAM ID=9 TYPE=26
ATTRIBUTES=IN-USE,ACTIVE,SHRPRF,ASUBM,TENV,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),NOPSEUDO,INSTDATA,NORNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,MENU,NOAUDIT,RES,NOMRO,WARNPW,NOTSOC
ATTRIBUTES=NOTRACE,NOLAB,NODORMPW,NONPWR,NOIMSXTND
MODE=IMPL
LOGGING=ACCESS,INIT,SMF,MSG,SEC9
UIDACID=8 LOCKTIME=000 DEFACID=*NONE* KEY=8
```

Example: ISERVER ACID Definition for CA-Top Secret

Following is an example of an ISERVER ACID definition for *e*Trust CA-Top Secret. Note that:

- UID is zero.
- The facility of the server is set to IWAY as an example; it can differ at your site.
- The SOURCE = INTRDR setting prevents this ACID from logging on.

```
TSS LIST(ISERVER) DATA(ALL,PROFILE)
ACCESSORID = ISERVER             NAME = IWAY ID
TYPE       = USER                SIZE = 512 BYTES
SOURCE     = INTRDR
DEPT ACID  = IWAY                DEPARTMENT = IWAY DEPT
DIV ACID   = IWAYDIV             DIVISION = IWAYDIV
GROUPS     = IWAYGRP
DFLTGRP    = IWAYGRP
----------- SEGMENT OMVS
HOME       = /
OMVSPGM    = /bin/sh
UID        = 0000000000
```

Example: IADMIN ACID Definition for CA-Top Secret

Following is an example of an IADMIN ACID definition for *e*Trust CA-Top Secret. Note that UID is *not* zero.

```
TSS LIST(IADMIN) DATA(ALL,PROFILE)
ACCESSORID = IADMIN              NAME = IWAY ADMIN ID
TYPE       = USER                SIZE = 512 BYTES
FACILITY   = TSO
FACILITY   = BATCH
DEPT ACID  = IWAY                DEPARTMENT = IWAY DEPT
DIV ACID   = IWAYDIV             DIVISION = IWAY DIVISION
GROUPS     = IWAYGRP
DFLTGRP    = IWAYGRP
----------- SEGMENT OMVS
HOME       = /u/iadmin
OMVSPGM    = /bin/sh
UID        = 0000000008
```

Starting and Stopping a TIBCO WebFOCUS Reporting Server for ZFS

This section provides information on operation and use of the server. Additional information on the server and how to configure adapters is available in the Reporting Server browser interface help. The Reporting Server browser interface help is also available as the *TIBCO WebFOCUS® Reporting Server Administration* manual.

Starting and Stopping the TIBCO WebFOCUS Reporting Server Using a Batch Job

To start the server, submit the ISTART member of the MVS configuration library (*high_level_qualifier*.WFS.DATA).

To stop a server, submit the ISTOP member of the MVS configuration library or use the Reporting Server browser interface. For information about using the Reporting Server browser interface, see the *TIBCO WebFOCUS® Reporting Server Administration* manual.

Starting and Stopping the TIBCO WebFOCUS Reporting Server Using a Started Task

ISETUP creates started task JCL to start and stop the server. These started task members of the MVS configuration library are:

- **IWAYS,** which starts the server.
- **IWAYP,** which stops the server.

In order to execute the started tasks, you must:

- **Copy them** into SYS1.PROCLIB or any other JES2 Proclib data set.
- **Satisfy security requirements.** All external security-related permissions must exist for both the data sets and the started tasks. In order to issue the started tasks, the user must satisfy both of the following requirements:
  - Have at least OPERATOR authority defined within the Reporting Server browser interface.

- Be in the same security group, or associated with the same security group, as the owner of the server directory structure (for example, as iadmin).

To submit the started tasks from the MVS console, issue the following command:

```
S IWAYS
S IWAYP
```

You can add the started tasks to any automation product that you run.

Example: Sample IWAYS Started Task

This is an example of iWAYS, the started task that starts the server:

```
//IWAYS        PROC
//TSCOM300     EXEC PGM=TSCOM300,
//        PARM='ENVAR("_EDC_UMASK_DFLT=0022")/'
//STEPLIB      DD   DSN=IADMIN.SRV90.HOME.LOAD,DISP=SHR
//EDAPRINT     DD   SYSOUT=A
//SYSPRINT     DD   SYSOUT=A
//SYSOUT       DD   SYSOUT=A
//EDAPARM      DD   DUMMY
//EDAENV       DD   DSN=IADMIN.SRV90.WFS.DATA(EDAENV),DISP=SHR
```

Example: Sample IWAYP Started Task

This is an example of iWAYP, the started task that stops the server:

```
//IWAYP        PROC
//TSCOM300     EXEC PGM=TSCOM300
//STEPLIB      DD   DSN=IADMIN.SRV90.HOME.LOAD,DISP=SHR
//EDAPRINT     DD   SYSOUT=A
//SYSPRINT     DD   SYSOUT=A
//SYSOUT       DD   SYSOUT=A
//EDAPARM      DD   DSN=IADMIN.SRV90.WFS.DATA(EDAPRMP),DISP=SHR
//EDAENV       DD   DSN=IADMIN.SRV90.WFS.DATA(EDAENV),DISP=SHR
```

TIBCO WebFOCUS Reporting Server Operations Using MVS Operator Commands

On MVS, you can issue operator MODIFY commands against the server job from either from the MVS Console or SDSF. You can use MODIFY commands to pass options to an already running job:

Use MVS Operator MODIFY commands in the following format:

```
F jobname, parameters
```

For instance:

```
F IWAY90,-SHOW
```

Note: If the server job is cancelled or it abends, submit the ICLEAR job in the configuration data set before restarting the server.

Enabling HTTPS Security on the HTTP Listener for ZFS

If you are using RACF, a private key *must be* generated together with the certificate. The generated key must be type RSA. The supported private key size is up to 4096 bits.

Generating the Certificate and Key

- **Generating the Certificate.** You can generate the certificate using the TSO RACDCERT command with options GENCERT (generate certificate) or GENREQ (generate certificate request). For example:

```
RACDCERT GENCERT SUBJECTSDN(CN('Workspace Manager') -
OU('IOD') -
O('IBI') -
C('US')) -
SIZE(2048) -
NOTAFTER(DATE(2026-12-01)) -
ID(ISERVER) -
RSA -
WITHLABEL('IBIcert')

SETROPTS RACLIST(DIGTCERT) REFRESH
```

- **Creating the Key Ring.** You can create the key ring using the RACDCERT ADDRING command. For example:

```
RACDCERT ADDRING(IBIring1) ID(ISERVER)
```

- **Connecting the Certificate to the Key Ring.** You can connect the certificate to a ring using the RACDCERT CONNECT command. For example:

```
RACDCERT CONNECT(LABEL('IBIcert') DEFAULT RING(IBIring1)) -
ID(ISERVER)
```

The ID owner of all objects is the same. It must be ISERVER.

The following JCL shows how to run the RACDCERT command in batch:

```
//*** JOB CARD *************
//*******************************************************
//STEP1 EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
RACDCERT LIST ID(ISERVER)
```

For detailed information and options of the RACDCERT command, see the IBM document *z/OS Security Server RACF Command Language Reference*.

TLS 1.3 SSL Protocol Requirements

The TLS 1.3 protocol requires additional RACF permissions be given to users and/or groups connecting to the Reporting Server. READ permission must be given to CSFOWH CL(CSFSERV).

If you do not plan to use the default of TLS 1.3, you can force the Reporting Server to use TLS 1.2 by adding the following parameter to the edaserve.cfg file:

```
ssl_protocol = tls_1_2
```

Enabling HTTPS

Once the key ring and label are created, to enable HTTPS:

1. Go to the Reporting Server browser interface Workspace page.
2. Expand *Special Services and LIsteners*.
3. Right-click TCP/HTTP and click *Properties of HTTP*.

   The Listener Configuration page opens.
4. Expand the Security section.
5. In the Enable HTTPS drop-down list, select Yes.

   Additional fields open in which you can enter the certificate label and keyring values you defined using the RACDCERT commands.

   ```
   SSL_CERTIFICATE = keyring
   SSL_LABEL = certificate
   ```
6. Click *Save and Restart Server*.

Defining the ICSF Dataset Key Label for ZFS to Use Pervasive Encryption

In the following sample JCL, values are shown for clarity. These are the current IBM defaults.

```
SYMEXPORTABLE(BYANY) and ASYMUSAGE(HANDSHAKE SECUREEXPORT)
```

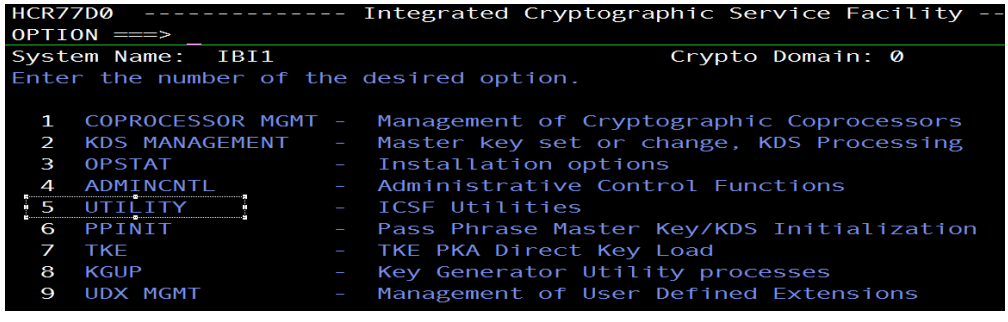
In the following sample PERMIT statement, ID contains only group names, not user ID names. During installation, you can choose which name to use or to use a combination of both.

Note: PGMYMG, PGM, QCS, EDA, and CSD in the sample code are arbitrary users and groups.

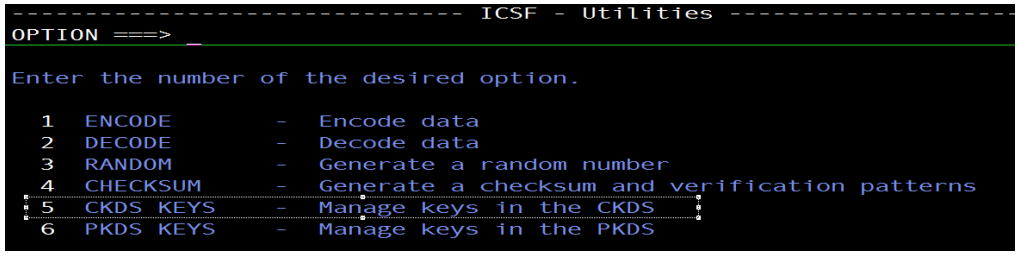
```
//TSOBATCH EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
RDEF CSFKEYS DATASET.PGMYMG.ENCRYPTKEY.001 OWNER(SYS1) UACC(NONE) -
ICSF(SYMCPACFWRAP(YES) SYMCPACFRET(YES)-
SYMEXPORTABLE(BYANY) ASYMUSAGE(HANDSHAKE SECUREEXPORT))
PERMIT DATASET.PGMYMG.ENCRYPTKEY.001 CLASS(CSFKEYS) ACCESS(READ) -
ID(PGM QCS EDA CSD)
SETROPTS RACLIST(CSFKEYS) REFRESH
/*
//
```

ICSF Panels

1. Select option 5, *UTILITY*, as shown in the following image, and press Enter.



2. Select option 5, *CKDS KEYS*, as shown in the following image, and press Enter.



3. Select option 7, *Generate AES DATA keys*, as shown in the following image, and press Enter.

```
------------------------------- ICSF - CKDS KEYS -----------------------------
OPTION ===> 7_

Active CKDS: IBI1.CSF.SCSFCKDS                                   Keys: 4

Enter the number of the desired option.
  1  List and manage all records
  2  List and manage records with label key type __________   leave blank for
                                                              list, see help
  3  List and manage records that are __________  (ACTIVE, INACTIVE, ARCHIVED)
  4  List and manage records that contain unsupported CCA keys
  5  Display the key attributes and record metadata for a record
  6  Delete a record
  7  Generate AES DATA keys

Full or partial record label
  ==>
  The label may contain up to seven wild cards (*)

Number of labels to display ==> 100  (Maximum 100)

Press ENTER to go to the selected option.
Press END   to exit to the previous menu.
```

4. Type the CKDS record label for the new key and select the AES key bit length, as shown in the following image, and press Enter.

```
---------------------------- ICSF - CKDS Generate Key ------
COMMAND ===>

Active CKDS: IBI1.CSF.SCSFCKDS

Enter the CKDS record label for the new AES DATA key
==> DATASET.PGMYMG.ENCRYPTKEY.001

AES key bit length:   _ 128   _ 192   s 256
```

If the operation was successful, Key Generated is returned at the upper-right corner of the screen, as shown in the following image.

```
- ICSF - CKDS Generate Key -----------  KEY GENERATED
```

Db2 Security Exit Configuration for ZFS

Customize the Db2 security exit to allow the Adapter for Db2 to run with user-level security enabled. If you do so, users will connect to Db2 with the authorization of the user ID with which they logged on to the server. The server must also be running with security turned on.

If you do not customize the Db2 security exit, all users will be assigned the connection ID to Db2 that is associated with the region, job submitter, or started task.

For the Adapter for Db2 CLI, the connection to Db2 must be configured as *trusted* for the exit to be invoked.

The changes that must be made to the IBM Db2 sign-on exit, DSN3SATH, differ for RACF and *e*Trust CA-Top Secret sites and *e*Trust CA-ACF2 sites.

The following sections show an example for each security package.

The highlighted text and comments shown in the examples indicate the lines containing the recommended modification of DSN3SATH, which calls the module FOCDSN3 the supplied exit.

After you finish the edits, assemble the exit into an object file. This object file is input to the link JCL found in one of the examples that follow.

Note:

- The positioning of these lines is approximate, assuming that no other changes or additions have already been made to DSN3SATH. If any changes have been made, you should decide on the most appropriate location for this call to FOCDSN3.
- FOCDSN3 is used to set the proper primary (individual user ID) authorization.
- Another program, FOCDSN4, is used to set the proper secondary (group ID) authorization for RACF and *e*Trust CA-Top Secret. FOCDSN4 is not needed with *e*Trust CA-ACF2; the secondary authorization ID(s) will be set correctly without it.

Example: Changing DSN3SATH for RACF and *e*Trust CA-Top Secret Sites

1. Search for the SATH001 label - add two lines (FOCDSN3):

```
SATH001  DS    0H
         USING WORKAREA,R11        ESTABLISH DATA AREA ADDRESSABILITY
         ST    R2,FREMFLAG                SAVE FREEMAIN INDICATOR
         XC    SAVEAREA(72),SAVEAREA CLEAR REGISTER SAVE AREA
         .
         .
         .
*********SECTION 1:  DETERMINE THE PRIMARY AUTHORIZATION ID  ************
*                                                                       *
*  IF THE INPUT AUTHID IS NULL OR BLANKS, CHANGE IT TO THE AUTHID       *
*  IN EITHER THE JCT OR THE FIELD POINTED TO BY ASCBJBNS.               *
*  THE CODE IN THIS SECTION IS AN ASSEMBLER LANGUAGE VERSION OF         *
*  THE DEFAULT IDENTIFY AUTHORIZATION EXIT.  IT IS EXECUTED ONLY        *
*  IF THE FIELD ASXBUSER IS NULL UPON RETURN FROM THE RACROUTE          *
*  SERVICE.  FOR EXAMPLE, IT DETERMINES THE PRIMARY AUTH ID FOR         *
*  ENVIRONMENTS WITH NO SECURITY SYSTEM INSTALLED AND ACTIVE.           *
*                                                                       *
*************************************************************************
SPACE
    LA    R1,AIDLPRIM         LOAD PARM REG1             <--ADD
    CALL  FOCDSN3             GO GET THE IBI EXIT        <--ADD
    CLI   AIDLPRIM,BLANK      IS THE INPUT PRIMARY AUTHID NULL
    BH    SATH020             SKIP IF A PRIMARY AUTH ID EXISTS
```

2. Search for the SATH020 label - add a comment box, add one line, and comment out four lines:

```
SATH020  DS    0H                  BRANCH TO HERE IF PRIMARY EXISTS
*****OPTIONAL CHANGE @CHAR7:  FALLBACK TO SEVEN CHAR PRIMARY AUTHID***
*                                                                    *
*  IF YOUR INSTALLATION REQUIRES ONLY SEVEN CHARACTER PRIMARY        *
*  AUTHORIZATION IDS (POSSIBLY TRUNCATED) DUE TO DB2 PRIVILEGES      *
*  GRANTED TO TRUNCATED AUTHORIZATION IDS, THEN YOU MUST BLANK OUT   *
*  COLUMN 1 OF THE ASSEMBLER STATEMENT IMMEDIATELY FOLLOWING THIS    *
*  BLOCK COMMENT. THEN ASSEMBLE THIS PROGRAM AND LINK-EDIT IT INTO   *
*  THE APPROPRIATE DB2 LOAD LIBRARY AS EXPLAINED IN AN APPENDIX      *
*  OF "THE DB2 ADMINISTRATION GUIDE".                                *
*                                                                    *
*  OTHERWISE, YOU NEED DO NOTHING.                                   *
*                                                          @KYD0271*
**********************************************************************
*      MVI   AIDLPRIM+7,BLANK    BLANK OUT EIGHTH CHARACTER
       SPACE
       .
       .
       .
*   RACF IS ACTIVE ON THIS MVS
********************************************************************* <--ADD
*                                                                   * <--ADD
* The logic was modified because in DB2 V8 AIDLACEE is always not* <--ADD
* NULL. We used to honor AIDLACEE first, FOCDSN4 second and then * <--ADD
* AS ACEE. Now we honor FOCDSN4 first, AIDLACEE second and then  * <--ADD
* AS ACEE.                                                          * <--ADD
*                                                                   * <--ADD
* 03/11/05   ASK0                                                   * <--ADD
********************************************************************* <--ADD
  USING ACEE,R6             ESTABLISH BASE FOR ACEE        @KYL0108
  L     R6,AIDLACEE         Get => caller ACEE if any              <--ADD
* ICM   R6,B'1111',AIDLACEE CALLER PASSED ACEE ADDRESS? @KYL0108  <-COMMENT
* BZ    SATH024             NO, USE ADDRESS SPACE ACEE  @KYL0108 <-COMMENT
* CLC   ACEEACEE,EYEACEE    IS IT REALLY AN ACEE?       @KYL0108  <-COMMENT
* BE    SATH027             YES, PROCEED NORMALLY       @KYL0108  <-COMMENT
      SPACE 1
SATH024  DS    0H                  USE ADDRESS SPACE ACEE      @KYL0108
    .
    .
    .
```

3. Search for the SATH025 label - replace sath025 and add sath026 (FOCDSN4):

```
SATH025  DS    0H

    CALL  FOCDSN4              GO GET THE IBI EXIT (4=GROUP AUTH) <--ADD
    LTR   R6,R6                DOES AN ACEE EXIST?  IF NOT,       <--ADD
    BZ    SATH026              CHECK ACEE IN ADDRESS SPACE        <--ADD
    CLC   ACEEACEE,EYEACEE     DOES IT LOOK LIKE AN ACEE?         <--ADD
    BE    SATH027              YES, GO DO GROUPS                  <--ADD
SATH026  DS    0H                                                 <--ADD
     .
     .
     .

SATH027  DS    0H             CHECK LIST OF GROUPS OPTION
   TM     RCVTOPTX,RCVTLGRP   IS LIST OF GROUPS CHECKING ACTIVE
   BZ     SATH040             SKIP TO SINGLE GROUP COPY IF NOT
   DROP   R7                  DROP RCVT BASE REG
   SPACE 1
* RACF LIST OF GROUPS OPTION IS ACTIVE
   EJECT
    .
    .
    .
```

Example: Changing DSN3SATH for *e*Trust CA-ACF2 Sites

*DSN3SATH source is provided by ACF2.

1. Search for PRIMARY AUTHORIZATION ID - add two lines (FOCDSN3):

```
*****************************************************************
*                                                               *
*           PRIMARY AUTHORIZATION ID                            *
*                                                               *
*****************************************************************
*                                                               *
*      IF THE PRIMARY AUTHORIZATION ID IS NULL OR BLANKS        *
*      IF CA-ACF2 IS AVAILABLE                                  *
*      SET PRIMARY ID FROM ACFASVT (ASVLID)                     *
*      ELSE                                                     *
*      IF TSO FOREGROUND USER                                   *
*      SET PRIMARY ID FROM TSO LOGON ID (ASCBJBNS)              *
*      ELSE                                                     *
*      SET PRIMARY ID FROM JOB USER (JCTUSER)                   *
*                                                               *
*****************************************************************
      SPACE 2                                                   04260000
      LA R1,AIDLPRIM LOAD PARM REG1                <--ADD
      CALL FOCDSN3 GO GET THE IBI EXIT             <--ADD
       CLI   AIDLPRIM,C' '      PRIMARY AUTHID THERE ?          04270000
       BH    PRIMWTO            ..YES, EVERYTHINGS OK HERE      04280000
       L     R3,PSAAOLD-PSA(0)  CURRENT ASCB ADDRESS            04290000
       USING ASCB,R3            ASCB ADDRESSABILITY             04300000
       SPACE 2                                                  04310000
```

Example: Modifying the Link JCL for DSN3SATH

This is a sample link JCL for the IBM exit DSN3SATH. Modify the JCL to link the modules into the Db2 security exit as follows.

```
//LKED  EXEC PGM=IEWL,PARM='LIST,XREF,LET,RENT,AMODE=31'
//OBJECT    DD DSN=db2pref.SDSNSAMP.OBJ,DISP=SHR <--OUTPUT OF ASSEMBLE
STEP
//EDAMOD    DD DSN=high_level_qualifier.HOME.LOAD,DISP=SHR
//SYSLMOD   DD DSN=db2pref.DSNEXIT,DISP=SHR
//SYSPRINT  DD SYSOUT=*
//SYSUT1    DD UNIT=SYSDA,SPACE=(100,(50,50))
//SYSLIN    DD *
  INCLUDE EDAMOD(FOCDSN3)
*********************************************************************
*** Omit the following line for eTrust CA-ACF2
*********************************************************************
  INCLUDE EDAMOD(FOCDSN4)
          ENTRY DSN3@ATH
  NAME DSN3@ATH(R)
/*
```

where:

db2pref

Is the prefix for the Db2 data sets.

high_level_qualifier

Is the high-level qualifier for the data sets.

Once this job finishes successfully, you must recycle the Db2 subsystem in order for the changes to take effect.

MSODDX for DD Translation for User Subroutines

On z/OS, you can incorporate an additional routine called MSODDX into a user-written subroutine that needs to access ddnames allocated to a Reporting Server. MSODDX provides ddname translation services that enable external programs to access files under the ddname used by the Server.

For details, see the *Stored Procedures* chapter in the *TIBCO WebFOCUS® Reporting Server Administration* manual.

Overriding the Time Zone Setting

By default, the server will use the system set value for Time Zone. This can be overridden by setting the TZ in the EDAENV member of the server configuration library.

```
TZ = valid tz string
```

For more information about time zone values, see the *IBM UNIX System Services Command Reference* and search for TZ.

Adding a Configuration Instance for ZFS

Adding a configuration instance allows you to run additional or different configuration instances using the same software binaries. You can add up to nine additional instances.

Step 1. Run ISETUP

To add a configuration instance, perform the following steps.

1. Execute ISETUP again. You should have a *high_level_qualifier*.HOME.DATA PDS. Use option 6 in ISPF to execute the ISETUP member of this PDS.

   Note: If this PDS is not available, run an IEBCOPY job to allocate and unload it from the installation tape.

   The first Installation and Configuration panel opens.

2. Enter *1* and press Enter to continue to the next panel.

   The first Installation and Configuration panel for ZFS opens.

3. Complete the first Installation and Configuration panel as follows.

Field	**Instructions**
Enter selection	Choose option 2, *Add Additional Configuration Instance*.
Input source	This is ignored for option 2.
Installation Userid	Shows the current logon ID. It cannot be changed.
OPSYS Administration Userid	Initially, this field shows the same ID as the installation user ID. If the installation user ID is a superuser (UID=0), you must specify a non-superuser ID to administer the server. Specify this ID here.
PTH Administrator Userid	An ID is required to administer the server immediately after initial installation. This ID is defined and maintained solely in the realm of the server. It defaults to *srvadmin* and it can be changed here. For more information about running the server in secure mode, see *Step 7. Configure Security* on page 116.
PTH Administrator Password	Password for the PTH Administrator ID. It cannot be left blank and must be matched at Retype field.
Enter Job Card information	To provide JOB card information for submitting jobs to the JES queue, provide a valid job name (a maximum of seven characters following the // on the first JCL line), which defaults to the user ID that you are currently using. This job name is used for multiple submissions (for example, *jobname*A, *jobname*B, *jobname*C, and so on) in the JCL generated by the installation procedure.

Field	Instructions
Override JOB name checking	To provide your own JOB card information, including JOB name, enter *Y* and provide valid JOB card information in the *Enter Job Card information* field. The JOB card information that you enter will be used for each job that is submitted.

4. If you used the same user ID for both installation and administration, skip to Step 7. Otherwise, continue with Step 5.
5. Press Enter to continue to the next panel.

   This panel appears only if you provided two different user IDs in the previous panel.

   The installation process will change ownership of ZFS server files from the installation ID (iinstal) to the administrator ID (iadmin). The installation ID must have authority to issue the chown command to make this change of ownership. This action is taken at the end of the installation process.
6. Complete the panel as follows.

Field	Instructions
Enter Job Card information	To provide JOB card information for submitting the run-time jobs to the JES queue, provide a valid job name (a maximum of seven characters following the // on the first JCL line), which defaults to the user ID that you are currently using. This job name is used for multiple submissions (for example, *jobname*A, *jobname*B, *jobname*C, and so on) in the JCL generated by the installation procedure.
Override JOB name checking	To provide your own JOB card information, including JOB name, enter *Y* and provide valid JOB card information in the *Enter Job Card information* field. The JOB card information that you enter will be used for each run-time job that is created.

7. Press Enter to continue to the next panel.

The Add Configuration panel opens.

```
TIBCO                    Installation and Configuration        z/OS USS Deploy
Command ===>                                                              PG
                                Add Configuration

Please enter the following information for WebFocus Reporting Server

 Product Configuration Parameters

  ZFS base Directory                ===> /u/iadmin

Press Enter to continue, PF3 to return to previous menu
```

8. Enter the current base high-level qualifier used for EDAHOME.

   This indicates where to install the configuration (EDACONF) and where the binaries (EDAHOME) are installed. The installation procedure checks whether this directory exists and if an instance is already installed. If either test fails, you receive a message indicating the failure and available options.

9. Press Enter to continue to the next panel.

   The Add Additional Configuration panel opens.

```
TIBCO                    Installation and Configuration        z/OS USS Deploy
Command ===>                                                              PI
                       Add additional Configurations

Please enter the following information for WebFocus Reporting Server

 Using the following existing information
  ZFS base Directory          ===> /u/iadmin
  EDAHOME Library             ===> IADMIN.SRV82.HOME.LOAD
  Base EDACONF Library        ===> IADMIN.SRV82.WFS.DATA
  Current configurations      ===> wfs
 Product Configuration Parameters
  Application Directory       ===> /u/iadmin/ibi/apps
  Profile & admin Directory   ===> /u/iadmin/ibi/profiles
  EDACONF suffix ( wfs plus)  ===> 1          or string suffix   ===>
  Server System Userid        ===> ISERVER
  HTTP Listener Port          ===> 8127      TCP Listener Port  ===> 8126

 MVS Installation Library
  EDACONF Library             ===> IADMIN.SRV82.WFS1.DATA
  EDACONF Library Unit        ===> SYSDA    Type ===> VOL=SER  ===>

Press Enter to continue, PF3 to return to previous menu
```

10. Complete the panel as follows.

Configuration Parameters	
Application Directory	This indicates where application components will reside for the configuration. The default value is based on the value specified for *Base Directory* on the previous panel. To specify another location for application components, change the value for this field.
Profile & Admin Directory	This indicates where user profiles and administration files will reside. The default value is based on the value specified for *Base Directory*. To specify another location for application components, change the value for this field.

Configuration Parameters	
EDACONF suffix	You are prompted for this information *only* if you are configuring an *additional* instance. Each software instance must have its own set of configuration libraries. To guarantee this, and to prevent a new set of configuration libraries from overwriting an existing set, the suffix that you specify here will be appended to the name of the software type qualifier. For example, if you are configuring the second instance of a WebFOCUS Reporting Server, you could specify that the suffix "1" be added, so that the EDACONF high-level qualifier would be: `IADMIN.SRV.WFS1` You can add a new configuration as a numeric or string suffix to the base software type. If you supply a string, the installation procedure ignores any numeric suffix. For a: ❑ Numeric suffix, Enter a digit between 1 and 9. This will be added to the software type in the directory name and library name to distinguish it from other configuration instances. ❑ String suffix, enter a string of between 1 and 5 characters (for example, TEST, PROD, or DEV). The string cannot contain embedded spaces. You can also use the string suffix to extend the numeric numbering past 9. Just supply a number greater than 9. If you change the suffix value, when you press Enter, the panel refreshes with a new value for EDACONF Library.
Server System Userid	This shows the default value, ISERVER. To change this value, see the requirements in *Step 2. Set Up User IDs* on page 88.
HTTP Listener Port	This indicates the port number that the server will use for HTTP. It is the first of three connection ports that must be available to the server. For example, if you choose port 8101, then ports 8101, 8102, and 8103 are used by the server. Ensure that you choose ports that are not currently being used.

Configuration Parameters	
TCP Base Port	This is the port number of the TCP Listener. The default is one less than the port specified for the HTTP Listener, but it can be any port number other than the three reserved for HTTP.
EDACONF Library	This is the full data set name the installation procedure will use to allocate the EDACONF configuration library on MVS. If you are running from *high_level_qualifier*.HOME.DATA, this field will have the default value *high_level_qualifier*.WFS.DATA. If you are adding an additional configuration, the default value will reflect the EDACONF suffix value. If you used another name to unload the first data set, this field will be blank. On subsequent running of ISETUP, the previous value used will be displayed. Change the value as necessary.
Unit/Type	You are prompted for this information *only* if you are configuring the *first* instance. These show the values that the installation process will use to allocate the output libraries. If necessary, you can change these to site-specific values. Type can be **VOL=SER** (default), **DATACLAS**, **MGMTCLAS**, or **STORCLAS**.

11. Press Enter to continue to the next panel.

    The Data Adapter panel may open before the Demonstration Files panel. If the Data Adapter panel opens, continue with Step 12. Otherwise, skip to Step 13.

12. The Data Adapter panel lists adapters that require the allocation of MVS libraries in IRUNJCL or environment variables in the EDAENV member. To select specific adapters:

    a. Type *Y* next to the required adapters and press Enter.

    b. Supply the requested information, which is described in *Step 3. Collect Required Information for Adapters* on page 99.

After you have finished installing and configuring the server, you can use the Reporting Server browser interface to finish configuring these adapters, and to configure adapters that do not have MVS JCL requirements.

c. Press Enter.

The JSCOM3 Listener configuration panel opens.

13. Configuration of the JSCOM3 Listener is either optional or mandatory depending on which adapters were selected. If any Java-based adapters were selected (EJB, Call Java, JDBC, MS SQL Server), the configuration is mandatory.

a. The panel will prompt for the path to the Java environment to be passed to either JDK_HOME or JAVA_HOME, as described in *JVM Requirements for Java Services (Server Installations Only)* on page 75.

b. If no Java-based adapters were selected, this configuration might still be desirable to enable server-side graphics and Adobe® Flex® features. To skip the configuration, leave the path blank.

c. Press Enter to continue to the next panel.

14. Ensure that all values on the Confirmation panel are correct, then select one of the following options:

- **N** to return to the initial panel so that you can change installation values.
- **C** to create JCL which you can submit at a later time. The JCL is placed in your configuration library.
- **S** to create JCL and submit the job immediately.

15. As the job is processed, in SDSF, check JESLOG for errors and return codes.

Following is a table of the jobs created. All members are created in the configuration library (EDACONF).

Job	Description
ISETUPJ2	Main JCL Job stream that is used to install an additional server configuration.
ISOPTS2	Options used to install an additional server configuration.

The following members all call procedure IRUNJCL, which is the main server JCL. If you need to change the server JCL, change member IRUNJCL.

Member	Description
ISTART	Starts the server.
ISTOP	Stops the server.
ICLEAR	Clears server resources after an abnormal end.
ICLRDIR	Clears superuser-owned directories from a previously run secure server.
ISAVEDIA	Creates a directory called sd*nnnnnn* and populates it with full diagnostic information.
ISHOW	Shows current workspace status.
ITRCON	Turns on dynamic tracing (server will be started if not already running).
ITRCOFF	Turns off dynamic tracing (server will be started if not already running).

The following members contain batch JCL for auxiliary functions, and are created in the configuration library.

Member	Description
CMRUN	JCL to run Data Migrator batch jobs.
DB2V*ver*PR	Db2 DBRM, where *ver* is your supported version of Db2 referenced in GENDB2 JCL.
GENDB2	JCL to bind the Db2/CAF plan.
IRDAAPPC	Example CLIST to run RDAAPP Client test tool.
IRDAAPPJ	Example JCL to run RDAAPP Client test tool.

The following members contain sample started task JCL, and are created in the configuration library.

Member	Description
IWAYS	A started task that starts the server.

Member	Description
IWAYP	A started task that stops the server.
EDAPRMP	A parameter file used by IWAYP.
EDAENV	A parameter file used by IWAYS, IWAYP, ISTART, and ISTOP.

The following table shows the ZFS directory structures created during the installation process.

Directory Structure	Description
`/u/iadmin/ibi/srv90/tape`	Contains ZFS files from the input media.
`/u/iadmin/ibi/srv90/install`	Working directory for the installation process. Log and error files reside here.
`/u/iadmin/ibi/apps`	The installation creates *baseapp* and one or more sample application directories under this directory.
`/u/iadmin/ibi/profiles`	This is where user profiles are created, as well as admin.cfg.
`/u/iadmin/ibi/srv90/home`	Server system directories are created under this directory.
`/u/iadmin/ibi/srv90/wfs`	Configuration directories are created under this directory.

Step 2. Test the Installation

This section describes how to verify server installation.

Procedure: How to Test the Installation

1. Log on to TSO as iadmin.
2. Submit the ISTART JCL to start the server. This executes the IRUNJCL proc.

3. Check the job output for errors. Look for the EDAPRINT message:

   `(EDA13023) ALL INITIAL SERVERS STARTED`

4. Start the Reporting Server browser interface by opening a browser pointed at the listener port of the server. The URL format is

   `http://host:port`

   where:

   host

   Is the name of the machine on which the server is installed.

   port

   Is one port higher than the port specified when installing the server. For example, if you specified port 8100 during installation, then use port 8101 to access the Reporting Server browser interface.

   The Reporting Server browser interface opens.

5. If the Reporting Server browser interface opens and displays application tree folders in the left pane, the server is working because it uses its own underlying data access and reporting technologies to visualize the application tree. The server may be further data tested (if desired).
6. Continue with adapter configuration, as described in the *TIBCO WebFOCUS® Adapter Administration* manual.

When you are finished using the server, you can use the Reporting Server browser interface to stop the server by going to the Reporting Server browser interface tools menu, selecting *Workspace*, and then *Stop* for *Server Actions*.

If you experience problems at start-up, examine the job output for more information.

Upgrading Your TIBCO WebFOCUS Reporting Server Release for ZFS

Use this option to upgrade a server to a new maintenance level within the same major release. A major release is indicated by the first two digits of the release number.

Prerequisite Step When Upgrading From a Release Prior to 8207.27 to Release 8207.27 or Higher

If you are upgrading from a release that did not support the Golden Key (in which you needed to supply a license key in order to install the server) to a release that supports the Golden Key (in which you do not need a license key in order to install the server), you may need to perform a one-time prerequisite step.

In Release 8207.27 and higher, the only type of server that can be installed is a WebFOCUS Reporting Server. This server provides all of the functionality that was available in prior releases for a Full Function Server or a TIBCO® Data Migrator Server. A WebFOCUS Reporting Server requires a configuration directory named wfs directly under the server installation root directory.

If you installed a Data Migrator Server, you have a directory named dm instead of wfs. If you installed a Full Function Server, you have a directory named ffs instead of wfs.

1. In TSO, edit member EDAENV that is in your current configuration directory (either ffs or dm), for example:

   ```
   srvhlq.FFS.DATA(EDAENV)
   ```

   or

   ```
   srvhlq.DM.DATA(EDAENV)
   ```

   where:

   srvhlq
   Is the high-level qualifier for your server installation directory, for example IBI.SERVER.SRV90.

   Change the configuration directory path. For example, assume your EDAENV member has the following entry

   ```
   EDACONF=/ibi/server/srv90/ffs
   ```

   or

   ```
   EDACONF=/ibi/server/srv90/dm
   ```

   Change ffs or dm to wfs and save the file.

   ```
   EDACONF=/ibi/server/srv90/wfs
   ```

2. Exit TSO, and go to your server installation directory under USS. You can issue the OMVS command to enter the USS environment.

   For example, if your server installation directory is /ibi/server/srv90, issue the following command:

   ```
   cd /ibi/server/srv90
   ```

3. Copy your existing configuration directory to a new configuration directory named wfs, using the following command.

   For a Full Function Server:

   ```
   cp -R ffs wfs
   ```

For a Data Migrator Server:

```
cp -R dm wfs
```

After you have completed and tested the upgrade, you can delete the original ffs or dm directory.

Run ISETUP

Caution: Ensure that all server processes are stopped before upgrading.

Server upgrade consists of a series of ISPF panels, which gather information for the upgrade. After the panel dialog is complete, JCL is created and submitted (if required) to upgrade the server on z/OS. This JCL job retrieves the remainder of the MVS libraries and ZFS files from the media.

1. Execute the ISETUP member of your *high_level_qualifier*.HOME.DATA using ISPF option 6.

   The Installation and Configuration panel opens.

2. Select *1* for USS deployment and press Enter to continue to the next panel.
3. Complete the panel as follows.

Field	Instructions
Enter selection	Choose option *3*, *Refresh Installation*.
Input source	Choose the Input source, D for disk. **Note:** On the next panel, provide the directory name where the transferred files reside.
Installation Userid	Shows the current logon ID. It cannot be changed.
OPSYS Administration Userid	Initially, this field shows the same ID as the installation user ID. If the installation user ID is a superuser (UID=0), you must specify a non-superuser ID to administer the server. Specify this ID here.

Field	Instructions
PTH Administrator Userid	An ID is required to administer the server immediately after initial installation. This ID is defined and maintained solely in the realm of the server. It defaults to *srvadmin*. **Note:** For a Refresh Installation, this parameter is ignored, as no configuration files are updated. ISETUP must be run by the OPSYS Administration userid.
PTH Administrator Password	Password for the PTH Administrator ID. **Note:** For a Refresh Installation, this parameter is ignored, as no configuration files are updated. ISETUP must be run by the OPSYS Administration userid.
Umask setting to use	Shows the current umask setting for the iadmin ID. The JCL passes this setting to the server for use at run time. Every time the server creates a file in the .../ibi/profiles or .../ibi/apps directory structures (usually in response to Reporting Server browser interface activity), the server assigns to the file the default permissions 666 filtered by the umask value. You specify whichever umask value is necessary to mask out the permissions you do not want to grant. For example, if you specify a umask value of 0022, the server creates files with the permissions 644: umask 0022 is subtracted from the default 666, disallowing the group and world write permissions.
Enter Job Card information	To provide JOB card information for submitting jobs to the JES queue, provide a valid job name (a maximum of seven characters following the // on the first JCL line), which defaults to the user ID that you are currently using. This job name is used for multiple submissions (for example, *jobname*A, *jobname*B, *jobname*C, and so on) in the JCL generated by the installation procedure.

Field	Instructions
Override JOB name checking	To provide your own JOB card information, including JOB name, enter *Y* and provide valid JOB card information in the *Enter Job Card information* field. The JOB card information that you enter will be used for each job that is submitted.

If you used the same user ID for both installation and administration, skip to Step 7. Otherwise, continue with the following step.

4. Press Enter to continue to the next panel.

   This panel appears only if you provided two different user IDs in the previous panel.

   The installation process will change ownership of ZFS server files from the installation ID (iinstal) to the administrator ID (iadmin). The installation ID must have authority to issue the chown command to make this change of ownership. This action is taken at the end of the installation process.

5. Complete the panel as follows.

Field	Instructions
Enter Job Card information	To provide JOB card information for submitting the run-time jobs to the JES queue, provide a valid job name (a maximum of seven characters following the // on the first JCL line), which defaults to the user ID that you are currently using. This job name is used for multiple submissions (for example, *jobname*A, *jobname*B, *jobname*C, and so on) in the JCL generated by the installation procedure.

Field	Instructions
Override JOB name checking	To provide your own JOB card information, including JOB name, enter *Y* and provide valid JOB card information in the *Enter Job Card information* field. The JOB card information that you enter will be used for each run-time job that is created.

Field	Instructions
ZFS Base Directory	Base directory of the current server that is to be refreshed. The value will be checked to see if it contains a valid server directory structure. (It should contain .../ibi/srv*xx*/home/bin where *xx* is the major release level.) From this value, the current installation library name is obtained and this will be the location used to create the refresh JCL.

6. Press Enter to continue to the next panel, and complete the panel as follows.

Field	Instructions
Input Media (installing from tape)	
Volume serial number	Provide the volume serial number of the server media. The number is located on the tape supplied in your server package.
Volume unit type	Review the default value and change it, if necessary.
Work unit type	Review the default value and change, if necessary. You can specify a UNIT= *type* value (for example, SYSDA), or you can direct work files to a specific volume serial number by specifying, in single quotation marks (''), 'SYSDA,VOL=SER=*volume*'.
Input Media (installing from disk)	
Directory name of input	Provide the name of the directory in which the installation files reside.

Field	Instructions
MVS Installation Libraries	
EDAHOME Library	This is the full data set name the installation procedure will use to allocate the EDAHOME load library on MVS and where the refresh load modules will be stored. If you are running from *high_level_qualifier*.HOME.DATA, this field will have the default value *high_level_qualifier*.HOME.LOAD. If you used another name to unload the first data set, this field will be blank. On subsequent running of ISETUP, the previous value used will be displayed. Change the value as necessary.
EDAHOME Library Unit/Type	These show the values that the installation process will use to allocate the EDAHOME load library on MVS. If necessary, you can change these to site-specific values. Type can be **VOL=SER** (default), **DATACLAS**, **MGMTCLAS**, or **STORCLAS**.

Note: The EDACONF Library name is where the refresh JCL will be created. This library is the current server installation library. The value cannot be changed.

7. Ensure that all values on the panel are correct, then select one of the following options:
   - **N** to return to the initial panel so that you can change installation values.
   - **C** to create JCL which you can submit at a later time. The JCL is placed in your configuration library.
   - **S** to create JCL and submit the job immediately.
8. As the job is processed, in SDSF, check JESLOG for errors and return codes.

The following jobs are added to the current configuration library of the server:

Job	Description
`ISETUPJ3` `ISOPTS3`	Main JCL Job stream that is used to refresh the server installation.

The following directories are added to the ZFS directory structure of the existing server:

Directory	Description
`/u/iadmin/ibi/srv90/tape`	Contains ZFS files from the input media.
`/u/iadmin/ibi/srv90/install`	Working directory for the installation process. Log and error files reside here.

Test the Installation

This section describes how to test the server installation.

Procedure: How to Test the Installation

1. Log on to TSO as iadmin.
2. Submit the ISTART JCL to start the server.
3. Check the job output for errors. Look for the EDAPRINT message:

   ```
   (EDA13023) ALL INITIAL SERVERS STARTED
   ```

4. Start the Reporting Server browser interface by opening a browser pointed at the listener port of the server. The URL format is

   `http://host:port`

   where:

   host

   Is the name of the machine on which the server is installed.

   port

   Is one port higher than the port specified when installing the server. For example, if you specified port 8100 during installation, then use port 8101 to access the Reporting Server browser interface.

   The Reporting Server browser interface opens.

5. If the Reporting Server browser interface opens and displays application tree folders in the left pane, the server is working because it uses its own underlying data access and reporting technologies to visualize the application tree. The server may be further data tested (if desired).

When you are finished using the server, you can use the Reporting Server browser interface to stop the server by going to the Reporting Server browser interface menu bar, selecting *Workspace*, and then *Stop*.

If you experience problems at start-up, examine the job output for more information.

Reconfigure Security

For information about configuring server security, see *Step 7. Configure Security* on page 116.

To reconfigure server security to OPSYS provider only:

1. Log on to TSO using an ID with read access to the BPX.FILEATTR.APF facility class.
2. Using the name of the actual EDAHOME directory, change file attributes by entering the following TSO commands in ISPF Command Shell (option 6):

   ```
   OSHELL extattr +a /u/iadmin/ibi/srv90/home/bin/tscom300.out
   OSHELL extattr +a /u/iadmin/ibi/srv90/home/bin/tsqprx.out
   ```

3. Verify your changes by issuing the following command:

   ```
   OSHELL ls -E /u/iadmin/ibi/srv90/home/bin/tscom300.out
   OSHELL ls -E /u/iadmin/ibi/srv90/home/bin/tsqprx.out
   ```

   The extended attributes portion of the output should be a-s-.

4. The libraries allocated to STEPLIB in IRUNJCL must be APF-authorized. Any non-APF-authorized libraries must be allocated the TASKLIB DDNAME.
5. Test server security by repeating the process described in *Test the Installation* on page 150.

This step will need to be repeated after any server upgrade since these files are replaced during an upgrade.

Preventing Unsecured Starts After Upgrades

If the security provider is set to OPSYS in the configuration file and, additionally, explicit environment variable EDAEXTSEC is set to OPSYS (or ON), and the server cannot impersonate users because it lacks platform-specific authorization steps, the server start aborts and error messages are written to the edaprint log.

This feature prevents an unsecured server start after a software upgrade if any of the required post-upgrade reauthorization steps are missed on a UNIX, IBM i, or z/OS USS deployment. This is not applicable to other platforms. The setting may be placed in any normal server start-up shell or profile that a site is using or in the server edaenv.cfg configuration file. The messages vary slightly by platform.

The edaprint messages are:

```
I Configured primary security is 'OPSYS' as set in configuration file

E Server security explicitly set to OPSYS, but lacks authority!

Workspace initialization aborted.

(EDA13171) UNABLE TO START SERVER
```

Reconfigure Adapters

While most adapters do not require additional steps after updating binary files, the following table notes the adapters that do require some consideration.

Adapter	Steps After Updating Binaries
Adabas	❑ Re-enable the module containing SVC using the Reporting Server browser interface adapter configuration page. ❑ Test the adapter from the adapter page before running your applications.
Db2 CAF	❑ Rebind the Db2 plan using the Reporting Server browser interface adapter configuration page. ❑ Test the adapter from the adapter page before running your applications.

Accounting for ZFS - SMF Records

The server provides an optional facility to use for accounting purposes that enables you to log resource utilization on a per-user basis. This facility enables the server to generate SMF records for query-level and user-level accounting.

Server accounting requires that the server STEPLIB data sets be APF-authorized. When SMF records are generated, they contain:

- ❑ The logon ID and security ID of the user.
- ❑ The CPU time and EXCPs consumed.
- ❑ Data based on the type of record written.

You can process the SMF records using the accounting programs that exist at your site. Examples of SMF records are provided in *SMF Record Format for RECTYPES 1 and 4* on page 155.

In order to write SMF records, the server must be running APF authorized.

Two sample Master Files (SMFVSAM and SMFFIX) are provided for accessing accounting statistics. They reside under the catalog subdirectory in the EDAHOME location. Their difference is that SMFVSAM can be used to report directly from the system-live SYS1.MANx records, while SMFFIX can be used to report from a sequential file produced from running the SMFDUMP utility. These Master Files enable you to interpret the SMF records generated by the accounting facility using reporting requests or store procedures. Both Master Files are for logoff records only, as indicated by ALIAS=2 on the RECTYPE field entry.

A sample procedure report to query the SMF data is also provided under the same location. It is called smfman1.fex.

Syntax:

How to Enable Accounting

To enable accounting, insert the following statement into the server configuration file (edaserve.cfg):

```
smf_recno=smfnumber
```

where:

smfnumber

Is an integer in a range from 128 to 255, inclusive. This number represents the SMF number used by the accounting facility when it sends records to the SMF system.

By default, both RECTYPE pairs will be created when accounting is enabled. You can override the default by coding the following parameter on edaserve.cfg:

```
smf_subtype = {all|logon|query}
```

where:

all

Cuts all records. This is the default.

logon

Cuts logon records only (RECTYPE pair 1 and 2).

query

Cuts query records only (RECTYPE pair 4 and 5).

Syntax: How to Set the Accounting Field

Up to 40 characters can be supplied that appear in the SMF records field SMFOFA40. The SET BILLCODE command can be used in any support server profile to provide the account field information. The syntax is

```
SET BILLCODE=value
```

where:

value

Is the 1–40 characters to be used on each SMF record produced.

This information can also be set dynamically from a client application by coding an RPC with the SET command and executing it with the value as a parameter. WebFOCUS users can send the SET command to the server.

Procedure: How to Report From SMF Data

To report from SMF data, execute the sample procedure *smfman1.fex*, provided under home/catalog (DDNAME EDAHFEX for a PDS Deployment server).

You will be prompted for the DSN of the SMF VSAM data set from which you want to report, and the *smf_recno* value used to produce the SMF records.

Following is a listing of smfman1.fex

```
DYNAM ALLOC FI SMFVSAM DSN &SMFDSN.Please provide SMF VSAM DSN. SHR REU
DEFINE FILE SMFVSAM
CPU/D8.2 = SMFOFCPU / 100 ;
USER/A20 = SMFOFUID ;
EXCPS/I6 = SMFOFEXC ;
TIME/D9.2 = SMFOFLTM / 100 ;
HR/I2 = SMFOFTME / 360000 ;
MIN/I2 = (SMFOFTME  - (HR*360000)) / 6000 ;
TOD/A5 = EDIT(HR) | ':' | EDIT(MIN) ;
END
TABLE FILE SMFVSAM
PRINT USER CPU EXCPS TIME TOD
WHERE SMFOFRTY EQ &SMFNUM.Please provide SMF number(type) for report.
END
```

Reference: SMF RECTYPES

There are four RECTYPE values defined to produce SMF records:

RECTYPE	Description
1	Indicates a start of task record. When included in a report, these statistics tell when a task initiation occurred, and are of no particular use in chargeback. By pairing start and end of task records for all tasks within a time period, statistics, such as average active time, peak task count, and average task count, can be determined. These values can be used for future capacity planning activities for the server.
2	Indicates the start of a task record. When included in a report, these statistics tell when a task termination occurred. These records are cut for both publicly and privately deployed services and contain statistics for the subtask as a whole. For privately deployed services, RECTYPE (2) records contain statistics associated with a single user connection.
4	Begin query. Record layout is the same as RECTYPE (1).
5	End query. Record layout is the same as RECTYPE (2).

Reference: SMF Record Format for RECTYPES 1 and 4

The record format for RECTYPES 1 and 4 of the SMF records written by the server is defined below. The format is provided in the system 390 assembler DSECT form.

```
SMFON    DSECT
         SPACE
*-----------------------------------------------------*
*  USAGE ACCOUNTING SMF RECORD LAYOUT FOR LOGON RECORDS.                *
*                                                                       *
*  THIS IS THE DSECT DESCRIBING THE SMF RECORD WHICH IS PASSED TO       *
*  YOUR EXIT ON AT USER LOGON TIME.  IT IS COMPLETELY READY TO BE       *
*  WRITTEN WHEN YOUR EXIT RECEIVES CONTROL.                             *
*-----------------------------------------------------*
         SPACE

*-----------------------------------------------------*
*  THE FIRST TWENTY FOUR BYTES OF THE RECORD ARE THE SMF HEADER.        *
*  THESE FIELDS ARE REQUIRED IN ALL SMF RECORDS (18 BYTES FOR RECORDS *
*  WITHOUT SUBTYPES; WE USE SUBTYPES, THE HEADER IS 24 BYTES).          *
         SPACE
```

```
SMFONLEN DS    H'116'            RECORD LENGTH
SMFONSEG DS    XL2'0000'         SEGMENT DESCRIPTOR (0 UNLESS SPANNED)
SMFONFLG DS    XL1               SYSTEM INDICATOR
SMFONRTY DS    XL1               RECORD TYPE
SMFONTME DS    XL4               TIME, IN HUNDREDTHS OF A SECOND
SMFONDTE DS    PL4               DATE, 00CYYDDDF, WHERE F IS THE SIGN
SMFONSID DS    CL4               SYSTEM IDENTIFICATION
SMFONSBS DS    CL4               SUBSYSTEM IDENTIFICATION
SMFONSBT DS    XL2'0001'         SUBTYPE OF RECORD - X'0001' INDICATES X
                                 THIS IS A LOGON RECORD
         SPACE

*-----------------------------------------------------*
*  THE NEXT FIELDS ARE THOSE PRESENT IN THE LOGON                    *
*  RECORD FOR THE START OF A USER SESSION.                            *
*-----------------------------------------------------*
         SPACE
SMFONMSO DS    CL8               JOBNAME
SMFONJID DS    CL8               JOBID (FROM SSIBJBID)
SMFONASI DS    Y                 ASID
SMFONRV1 DS    XL2               RESERVED
SMFONUID DS    CL20              SECURITY USERID
SMFONLID DS    CL20              USERID PRESENTED AT LOGON (SAME AS    X
                                 SMFONSID UNLESS CHANGED VIA MSIDTR    X
                                 SECURITY EXIT)
SMFONRSV DS    XL8               RESERVED FOR FUTURE EXPANSION
SMFONCTI DS    XL4               RESERVED FOR FUTURE EXPANSION
SMFONSRV DS    CL8               SERVICE NAME FROM SERVICE BLOCK
SMFONRS0 DS    XL4               RESERVED FOR FUTURE EXPANSION
SMFONCNT DS    XL1               CONNECTION TYPE
         SPACE

SMFONTSO EQU   1                 CONNECTION VIA TSO
SMFONCIC EQU   2                 CONNECTION VIA CICS
SMFONVTM EQU   4                 CONNECTION VIA VTAM
SMFONPSR EQU   8
         SPACE
SMFONRS1 DS    XL3               RESERVED
SMFONID1 DS    F                 SYSPLEX ID 1
SMFONID2 DS    F                 SYSPLEX ID 2
SMFOFPID DS        XL20              POOLED USER ID
SMFONRS2 DS    XL12              RESERVED
SMFONL   EQU   *-SMFON           LENGTH OF THE SMF LOGON RECORD
```

Reference: SMF Record Format for RECTYPES 2 and 5

The record format for RECTYPES 2 and 5 of the SMF records written by the server is defined below. The format is provided in the system 390 assembler DSECT form.

```
SMFOF    DSECT
         SPACE
*-----------------------------------------------------*
*  USAGE ACCOUNTING SMF RECORD LAYOUT FOR LOGOFF RECORDS.            *
*                                                                    *
*  THIS IS THE DSECT DESCRIBING THE SMF RECORD WHICH IS PASSED TO    *
*  YOUR EXIT ON AT USER LOGOFF TIME.  IT IS COMPLETELY READY TO BE   *
*  WRITTEN WHEN YOUR EXIT RECEIVES CONTROL.                          *
*-----------------------------------------------------*
         SPACE

*-----------------------------------------------------*
*  THE FIRST TWENTY FOUR BYTES OF THE RECORD ARE THE SMF HEADER.     *
*  THESE FIELDS ARE REQUIRED IN ALL SMF RECORDS (18 BYTES FOR RECORDS *
*  WITHOUT SUBTYPES; WE USE SUBTYPES, THE HEADER IS 24 BYTES).       *
*-----------------------------------------------------*
         SPACE
SMFOFLEN DS    H'168'            RECORD LENGTH
SMFOFSEG DS    XL2'0000'         SEGMENT DESCRIPTOR (0 UNLESS SPANNED)
SMFOFFLG DS    XL1               SYSTEM INDICATOR
SMFOFRTY DS    XL1               RECORD TYPE
SMFOFTME DS    XL4               TIME, IN HUNDREDTHS OF A SECOND
SMFOFDTE DS    PL4               DATE, 00CYDDDF, WHERE F IS THE SIGN
SMFOFSID DS    CL4               SYSTEM IDENTIFICATION
SMFOFSBS DS    CL4               SUBSYSTEM IDENTIFICATION
SMFOFSBT DS    XL2'0002'         SUBTYPE OF RECORD - X'0002' INDICATES X
                                 THIS IS A LOGOFF RECORD
         SPACE

*-----------------------------------------------------*
*  THE NEXT FIELDS ARE THOSE PRESENT IN THE LOGOFF                   *
*  RECORD FOR THE END OF A USER SESSION.                             *
*-----------------------------------------------------*
         SPACE
SMFOFMSO DS    CL8             JOBNAME
SMFOFJID DS    CL8             JOBID (FROM SSIBJBID)
SMFOFASI DS    Y               ASID
SMFOFRV1 DS    XL2             RESERVED
SMFOFUID DS    CL20            SECURITY USERID
SMFOFLID DS    CL20            USERID PRESENTED AT LOGON (SAME AS    X
                               SMFOFSID UNLESS CHANGED VIA MSIDTR    X
                               SECURITY EXIT)
SMFMEMA  DS    XL4             MEMORY ABOVE THE LINE (IN KILOBYTES)
SMFMEMB  DS    XL4             MEMORY BELOW THE LINE (IN KILOBYTES)
SMFZIIP  DS    XL4             ZIIP CPU NORMALIZED (HUNDREDTHS OF A SEC)
SMFOFSRV DS    CL8             SERVICE NAME FROM THE SERVICE BLOCK
SMFZPOCP DS    XL4             ZIIP ON CP (HUNDREDTHS OF A SEC)
SMFOFCNT DS    XL1             CONNECTION TYPE
         SPACE
```

```
SMFOFTSO EQU   1                 CONNECTION VIA TSO
SMFOFCIC EQU   2                 CONNECTION VIA CICS
SMFOFVTM EQU   4                 CONNECTION VIA VTAM
SMFOFPSR EQU   8
SMFOFCC  DS    XL3               COMPLETION CODE FOR THE TASK
SMFOFACT DS    CL8               USER ACCOUNTING INFORMATION; THIS     X
                                 FIELD CURRENTLY PASSED AS LOW VALUE
SMFOFCPU DS    XL4               CPU TIME IN HUNDREDTHS OF A SECOND
SMFOFEXC DS    XL4               COUNT OF EXCP'S
SMFOFLTM DS    FL4               LOGON DURATION IN HUNDREDTHS OF A     X
                                 SECOND
SMFPRTY  DS    XL1               PRIORITY
SMFCOMPL DS    XL1               COMPLETION TYPE
         DS    XL2               RESERVED
SMFOFID1 DS    F                 SYSPLEX ID 1
SMFOFID2 DS    F                 SYSPLEX ID 2
SMFOPID  DS    XL20              POOLED USERID
SMFOFA40 DS    CL40              FULL 40-BYTE ACCOUNTING FIELD
         SPACE
SMFOFL   EQU   *-SMFOF           LENGTH OF THE SMF LOGOFF RECORD
```

Reference: **Accounting for Db2 in a Reporting Server Task**

When using a server to access Db2 data, certain processing takes place within the Db2 address space and is governed by the Db2 chargeback system. If a user requests data from Db2, the server passes the request to the Db2 subsystem. The Db2 subsystem then processes the request, performing such tasks as retrieving rows and aggregating the data. It generates the answer set, and passes the output back to the server. The server then performs any joins and formatting which have not been performed by Db2 to satisfy the original request.

Charges incurred while the request was being processed by the Db2 subsystem are added to the charges accumulated in the server task that originated the request for processing. If the server accounting is enabled, these charges are associated with the user logon and security IDs in the SMF records described earlier.

Enabling Use of the zIIP Specialty Engine

If your site has a zIIP (System **z** **I**ntegrated **I**nformation **P**rocessor) specialty engine from IBM, you can offload specific categories of workload from the Central Processors to the zIIP.

The zIIP engine is a restricted version of a Central Processor (CP), also referred to as a General Processor (GP). The capacity of the zIIP engine does not count toward the overall MIPS rating of the mainframe image, so the CPU usage incurred on the zIIP is effectively free. Central Processors are often configured to run at speeds below their maximum rating for cost saving and capacity planning purposes. For Central Processors, *100% capacity* typically refers to the maximum MIPS that the processor is allowed to generate at that installation, in accordance with your contract with IBM. In contrast, the zIIP engine always runs at true 100 percent of capacity.

As much as 80 percent of server processing is enabled to run on the zIIP engine. Typical workloads are expected to offload 30 to 80 percent of CPU processing to the zIIP engine.

To make use of the zIIP enablement feature, the server must run in an authorized state.

What Is a zIIP Specialty Engine?

Though physically identical to a Central Processor, the zIIP engine is microcoded at installation time to run specific types of workloads. The Central Processor continues to handle the operating system, I/O interrupts and timer interrupts, job initiations, and user interactions with the operating system. The zIIP concentrates on CPU intensive workloads, leaving the Central Processor more time to absorb otherwise queued workloads, thereby achieving some overall performance improvement across all mainframe activity.

Steps to zIIP Enablement

This section describes steps and requirements for the server use of the zIIP processor.

The steps to server zIIP enablement are:

1. Obtain APF authorization for the server load library.
2. Activate the zIIP feature using the SET ZIIP=ON or SET ZIIP=ON/SIMMAXZIIP command. For instructions, see *Activating a zIIP Environment or Projecting zIIP Usage* on page 160.

Reference: Usage Notes for Use of the zIIP Processor

- Maximize the blocksizes of data sources that are read or written by the server to reduce the number of I/Os required to access the file. This will reduce the number of switches to non-zIIP mode that the server agents have to make, thus permitting a greater percentage of zIIP contribution to the request.

- Move or rewrite functions developed at your site since the server must switch to non-zIIP mode for each call to such routines. You may be able to use one of the following possible solutions:
  - Move the routines from DEFINEs to COMPUTEs to reduce the number of times they are referenced. This tactic must be applied carefully, and only when report results would not change.
  - Rewrite the routines using DEFINE FUNCTION, which executes on the zIIP processor.
  - Confine the routine to a pre-step run with ZIIP=OFF which collects its calculated results, then use those calculations in the next step with ZIIP=ON.

Activating a zIIP Environment or Projecting zIIP Usage

The last step in zIIP enablement is to activate the use of the zIIP processor in the server. zIIP enablement is activated by the SET ZIIP command.

The SET ZIIP command has three options:

- **OFF.** This setting prevents the server from offloading its processing to a zIIP.
- **ON.** This setting causes the server to offload processing to a zIIP engine if you have a zIIP processor and the environment is properly APF-authorized.
- **ON/SIMMAXZIIP.** This setting enables you to project zIIP processing in two different environments:
  - **You do not have a zIIP processor.** Using this setting along with the PROJECTCPU parameter, you can project how much server workload would have been offloaded to a zIIP.
  - **You do have a zIIP processor.** Using this setting you can project how much advantage you would achieve by offloading 100% of eligible server processing to the zIIP.

Syntax:

How to Activate the zIIP Enablement Feature

You can issue the SET ZIIP command in a server profile or in a particular FOCEXEC.

```
SET ZIIP={ON[/SIMMAXZIIP]|OFF}
```

where:

`ON`

Configures the server to offload processing to the zIIP engine.

This setting:

- Determines if the zIIP processor is accessible to the LPAR in which a job is running.
- Determines if the server environment has been properly authorized to run a zIIP workload.

Note: If the server determines that the zIIP processor is not accessible or that the environment has not been authorized correctly, it issues a message describing the reason and continues in ZIIP=OFF mode, which forwards all subsequent work to the Central Processor.

`ON/SIMMAXZIIP`

Configures the server to either:

- Project what the zIIP usage would be if the server could offload processing to a zIIP, when the server is operating in an LPAR without a zIIP. This requires that the PROJECTCPU parameter be set to YES.

  The SYS1.PARMLIB member IEAOPT*xx* contains the PROJECTCPU statement. Activating the PROJECTCPU parameter projects zIIP consumption when a zIIP processor is not yet defined to the LPAR. SMF type 30 records will show the potential calculated zIIP time, so that you can accurately project zIIP usage. This enables you to evaluate the effect of configuring a zIIP processor to be available for server usage. The Systems Programmer for your site will have access to this data. Use this option for simulation purposes only.

  Since the zIIP engine actually is not present, all zIIP-eligible workload will be diverted to the Central Processor. Thus, all of that CPU utilization will be recorded in a server variable called &FOCZIIPONCP. This is the amount of workload that would have run on the zIIP engine, and would have appeared in &FOCZIIPCPU, had the zIIP been present and accessible to server work. This information is also recorded in the server job statistics as well as in IBM SMF type 30 records.

  To use this option, insert the following parameter in SYS1.PARMLIB for your LPAR, and also issue the SET ZIIP=ON/SIMMAXZIIP command:

  ```
  PROJECTCPU=YES
  ```

  This setting:

  - Determines if the PROJECTCPU=YES command has been set in the LPAR.
  - Determines if the server environment has been properly authorized to run a zIIP workload.

- Projects zIIP utilization if 100% of eligible server processing could be offloaded to the zIIP, when the server is running in an LPAR with a zIIP. This lets you determine what you would gain by configuring Workload Manager to give the server a bigger share of zIIP processing.

  IBM Workload Manager (WLM) prioritizes workloads among the Central Processors and zIIP processors at your site based on a complex set of goals and rules established by the system administrator. These rules apply to all workloads from all sources, not just the server. These goals combine to influence the decision to direct server requests to the zIIP engine at any particular moment.

  Utilizing this setting with a zIIP present can help you determine how much advantage you would get if the server had more of a share of the zIIP processor. To see the difference in actual and projected zIIP usage, run the same job with SET ZIIP=ON and then with SET ZIIP=ON/SIMMAXZIIP and compare the results. For more information about evaluating zIIP usage, see *Evaluating zIIP Usage* on page 164.

  This setting:

  - Determines if the zIIP processor is accessible to the LPAR in which a job is running.
  - Determines if the server environment has been properly authorized to run a zIIP workload.

  Note: If the server determines that the environment has not been authorized correctly, it issues a message describing the reason and continues in ZIIP=OFF mode, which forwards all subsequent work to the Central Processor.

OFF

Configures the server not to offload processing to the zIIP engine. OFF is the default value.

Note: Turn off zIIP enablement only when you know for sure that a job will not gain any advantage from using the zIIP processor or if the system operator or administrator requires that you turn it off.

Example: **Setting the PROJECTCPU Parameter in SYS1.PARMLIB Member IEAOPTxx**

Use the following sample as a guide for setting the PROJECTCPU parameter in SYS1.PARMLIB(IEAOPTxx):

```
/* ************************************************************ */
/*                    SYS1.PARMLIB(IEAOPTxx)                    */
/* ************************************************************ */
PROJECTCPU=YES
```

How the TIBCO WebFOCUS Reporting Server Takes Advantage of the zIIP Processor

The server diverts eligible workload to the zIIP engine by switching from TCB (Task Control Block) mode for workloads that can run only on a Central Processor to SRB (Service Request Block) mode for execution of enabled workloads on the zIIP engine.

Types of server processing that are offloaded to the zIIP engine include:

- Computations.
- Aggregation.
- Screening.
- Sorting.
- Report formatting and styling.
- Transaction Processing.

The server zIIP Monitor detects situations in which the overhead cost of zIIP usage is exceeding the CPU benefits gained. When this threshold is reached, the server may decide to suspend use of the zIIP for the duration of a logical phase of the server request. When it does so, it places a message to that effect in the JES log. It then resets to make the zIIP processor accessible to the next logical phase of the server request.

TABLE, MATCH, MODIFY, and MORE requests may suspend and resume more than once as they progress through logical phases of execution.

In every case, the server attempts to optimize the use of the zIIP and minimize chargeable CPU costs.

Applications that perform significant database I/O, high-volume sorting, or the use of third-party tools or user functions during processing require switching out of SRB (zIIP) mode into TCB (non-zIIP) mode to communicate, and then back again to continue processing. Although each switch is minuscule, the cumulative effect can absorb measurable amounts of CPU time on both the zIIP engine and the Central Processor.

In order to diminish this effect, the server buffers the collection of records passed to the system sort utility and some adapters rather than passing one record at a time, thus reducing the number of switches between TCB and SRB modes.

These third-party products may themselves be zIIP enabled and may offload some or all of their processing to the zIIP engine independent of the server. The server always calls these products from the Central Processor because it cannot know whether they will perform any processing that is prohibited on the zIIP.

Even though zIIP usage occurs more frequently on non-optimized requests to a relational data source, optimized requests are still inherently more efficient and, therefore, may incur less CPU time. Being zIIP enabled, Db2 may also take advantage of the zIIP processor for server requests based on the local configuration of Db2 relative to the server.

Requests against some types of data sources whose I/O can be buffered gain a lot of advantage from zIIP enablement. Data sources that gain the most benefit from zIIP processing due to buffered I/O include:

- Blocked flat files.
- FOCUS.
- XFOCUS.
- VSAM.
- Db2.

Evaluating zIIP Usage

In order to evaluate server zIIP processing in a session, you can query three Dialogue Manager variables that accumulate statistics about CPU processing:

- &FOCCPU accumulates the time spent on a Central Processor. This is an existing variable that precedes zIIP enablement.
- &FOCZIIPCPU accumulates the time actually spent on the zIIP processor (in SRB mode). This is the normalized CPU value using the same scale as &FOCCPU.
- &FOCZIIPONCP accumulates the time that processing could have been offloaded to the zIIP processor but was diverted to the Central Processor by the system.

  Note:

  - &FOCCPU includes the value of &FOCZIIPONCP.
  - The sum of &FOCZIIPCPU and &FOCCPU represents the total CPU utilized by the server agent.
  - If you set ZIIP=OFF, the zIIP variables do not accumulate further but are not reset to zero. If you later set ZIIP=ON, they resume accumulating statistics.

The RM (Resource Manager) that monitors server usage also captures zIIP statistics.

Performance Considerations for ZFS

There are several ways in which you can improve the server performance:

- **Non-swappable address space.** We recommend that you run the server in a non-swappable address space. For more information, see *Running the TIBCO WebFOCUS Reporting Server in a Non-Swappable Address Space* on page 165.
- **Workload Manager (WLM).** You can balance server workload by using Workload Manager. For more information, see *Workload Manager* on page 165.

Running the TIBCO WebFOCUS Reporting Server in a Non-Swappable Address Space

We recommend that you run the server in a non-swappable address space. In order to make the server address space permanently non-swappable, add the following entry to SYS1.PARMLIB(SCHEDxx):

```
PPT PGMNAME(TSCOM300)          /* PROGRAM NAME */
NOSWAP                         /* NON-SWAPPABLE */
CANCEL                         /* CAN BE CANCELLED */
```

Do not use the KEY 0 parameter, or any other parameter (such as NOPASS), unless the system programmer completely understands the consequences of adding the parameter.

All local spawn transactions will perform in the mode of the server. For example, if the server address space is non-swappable, all local spawn transactions execute as non-swappable.

The server executes limited non-local spawn, such as when the user executes a UNIX system command. Non-local spawn execute as swappable.

The server never executes a fork subroutine. (A fork subroutine creates a new process. The new process, called the child process, is an almost exact copy of the calling process, which is called the parent process.)

Workload Manager

Although the server may run in a specific performance group, transactions submitted by server agents may perform differently than the server by adding the following keyword to edaserve.cfg:

`wlm_enclave_trname = WLM_transaction_name`

where:

WLM_transaction_name

Can be up to 8 characters.

This is a service-level keyword.

Using this setting, the task will join a Workload Manager (WLM) enclave when a request starts, and leave the enclave when the request finishes. This gives WLM control of the dispatching priority of the task. The transaction rules defined on WLM will determine the default service class assigned to this transaction, and that service class will determine how the request runs.

This feature helps to balance a workload so that a long request will not affect a short request. This can be achieved through WLM rules designed to lower the priority of a long request after a certain period of time. Without this feature, all requests share the region priority.

The transaction name passed in this keyword must match one defined in the WLM Classification Rules for the Job Entry Subsystem (JES). A corresponding WLM Service Class pointed to by this rule will then be associated with this service.

The classification rules for JES must be used even if the server is started as a started task. The subtasks are always run under JES.

For example, you would include the following in edaserve.cfg:

```
SERVICE = DEFAULT

BEGIN
wlm_enclave_trname = IWAYFAST
.
.
.
END
```

The WLM definition is:

```
Subsystem Type JES - Batch Jobs
Classification:

Default service class is PRDBATLO
There is no default report class.

  Qualifier  Qualifier      Starting       Service   Report
# type       name           position       Class     Class
- ---------- -------------- ---------      --------- --------
1 TN         IWAYFAST                      EDAQRYHI
```

WLM subrules (levels 2 and above) are supported. For a server request to join an enclave in a particular service class, the names of all rule qualifiers below our transaction name are checked. For example, consider the following WLM definition:

```
Subsystem Type JES - Batch Jobs
Classification:

Default service class is PRDBATLO
There is no default report class.

  Qualifier Qualifier     Starting Service  Report
# type      name          position Class    Class
- --------- ------------- -------- -------- --------
1 SSC       PRDMVS                 PRDDFLT
2 . TN      . IWAYFAST             EDAQRYHI
```

In this particular case, the qualifier 1 type is SSC (Subsystem Collection), and a server request will only join the enclave IWAYFAST if it is running on a particular LPAR in the SYSPLEX. This qualifier (PRDMVS) must match the XCF group definition: issue $DMASDEF (for JES2) and check the value of XCFGRPNM field.

You can handle WLM scheduling environments by defining them to WLM and then adding the JOB statement parameter SCHENV=xxxxx to the ISTART JCL.

General Information for a z/OS ZFS Installation

This section covers general information for a z/OS installation.

Sample Metadata, Data, and Other Tutorial Samples

The Reporting Server browser interface has a feature on the ribbon and on the application tree (under *new*), *Tutorials* (the Create Tutorial Framework page), which has a pull-down for various samples. The Data Migrator desktop interface also has this feature on the application tree.

There are currently about 10 different tutorial/sample selections available on the pull-down select list to match various customer needs. The bulk of the prior IBISAMP sample objects can be generated by selecting the *Create Legacy Sample Tables and Files* tutorial. Other prior IBISAMP Data Migrator sample objects (usually starting with the characters dm*) are now loaded by choosing their respective Data Migrator tutorials. Under the new method, the tutorials/samples may be loaded to any application, not just IBISAMP.

If you are doing just a software refresh, the prior IBISAMP objects will be unchanged (because a refresh does not touch app directories).

Frequently Asked Questions for ZFS

Q: How do I execute server user profiles from a PDS?

A: We recommended that you copy the server user profiles from the PDS to the ZFS directory /ibi/profiles, and rename them to add the extension .prf (for example, *user_id*.prf). Alternatively, you can use the following technique to execute user profiles from a PDS:

1. In the IRUNJCL member, allocate DDNAME //MVSPROF to the PDS containing user profiles. For example:

```
//MVSPROF DD DISP=SHR,DSN=high_level_qualifier.EDAPROF.DATA
```

2. Add the highlighted lines to the global server profile, edasprof.prf:

```
APP MAP MVSPROF fex=//dd:mvsprof
APP MAP MVSAPP mas=//dd:master;fex=//dd:focexec;acx=//dd:access;
...
APP PATH IBISAMP MVSAPP
-SET &USERID='12345678';
-SET &USERID=GETUSER(&USERID);
EX MVSPROF/&USERID
```

Q: What permissions are specified for application component files?

A: Application component files, such as FOCEXEC procedures (.FEX), Master Files (.MAS), and Access Files (.ACX), reside in the /ibi/apps/*applicationname* directory, where they are created with a permission of 666 minus the UMASK setting.

For example, if the UMASK value is 022, each application component is created with a permission of 644.

Caution: When using the above UMASK values, if one user ID creates application components, all other users will be able to read them, but not to write, update, or refresh.

You can provide write access by changing the value of UMASK at installation time, or manually in IRUNJCL. For example:

```
//TSCOM300  EXEC PGM=TSCOM300,
//          PARM='ENVAR("_EDC_UMASK_DFLT=0022")/'
//STEPLIB   DD DISP=SHR,DSN=EDABXV.SRV90.HOME.LOAD
```

Q: Can I monitor server startup by checking the MVS SYSLOG?

A: Yes.

The following messages are written to the SYSLOG when

- The Server starts successfully:

```
(EDA13023) ALL INITIAL SERVERS STARTED
```

- The Server does not start:

```
(EDA13171) UNABLE TO START IWAY SERVER
```

Troubleshooting for ZFS

To troubleshoot an installation problem, identify your problem in the following list, and follow the link to a description of the solution.

If you cannot find your problem described in the list, and cannot resolve it yourself, contact Customer Support. In addition, supply the following information to Customer Support:

- Server trace (see *How to Generate a Trace* on page 171).
- JCL for IRUNJCL.
- Job output.
- System dump, if needed (see *How to Generate a System Dump* on page 171).
- Any additional information regarding how the problem occurred.

Problems:

- The server abends with a U4039 code.

  For details, see *Problem: The Reporting Server Abends With a U4039 Code* on page 169.

- INSUFFICIENT AUTHORITY TO GETSPENT messages appear in JESLOG.

  For details, see *Problem: INSUFFICIENT AUTHORITY TO GETPSENT messages in JESLOG* on page 169.

- The request fails, and *JVM not found* messages are written to edaprint.log.

  For details, see *Problem: Request fails, and JVM not found messages written to edaprint.log* on page 170.

Reference: Problem: The Reporting Server Abends With a U4039 Code

Problem: The server abends with a U4039 code.

Cause: This is a generic abend.

Solution: Find out what caused the abend by checking the edaprint.log file, SYSOUT *ddname*, and the MVS system log.

Reference: Problem: INSUFFICIENT AUTHORITY TO GETPSENT messages in JESLOG

Problem: INSUFFICIENT AUTHORITY TO GETPSENT messages appearing in JESLOG.

Cause: See IBM APAR II11813.

Solution: The APAR recommends issuing one of the following RACF commands:

```
SETROPTS LOGOPTIONS (NEVER(PROCACT))
SETOPTS LOGOPTIONS (DEFAULT(PROCACT))
```

However, when a non-superuser in the OMVS shell issues the command ps -ef, the following security message is repeated in SYSLOG:

```
ICH408I USER(default) GROUP(dgltgrp) NAME(bpxdefaultuser) 060
CL(PROCACT) INSUFFICIENT AUTHORITY TO GETPSENT
```

This does not indicate an error. It is an informational message issued because of RACF LOGOPTIONS settings. The ps -ef command is a request to show all processes that the requester is authorized to see, but a non-superuser is allowed to see only his or her own processes.

Reference: Problem: Request fails, and *JVM not found* messages written to edaprint.log

Problem: The request fails, and *JVM not found* messages are written to edaprint.log.

Cause: If the server cannot find the Java Virtual Machine (JVM), the JSCOM Listener will not be able to start, and messages will be written to the server log stating that the JVM cannot be found.

Solution: Specify the location of the JVM in JDK_HOME or JAVA_HOME. (For information, see *JVM Requirements for Java Services (Server Installations Only)* on page 75.)

Reference: Secured Reporting Server Starts Unsecured or Does not Start After Upgrade

A server will implicitly attempt to start unsecured if proper authorization steps have not been completed. Starting the server normally clears edatemp. If prior edatemp files exist (and authorization has not been done), start-up will fail due to an inability to clear the directory. However, if an edastart -cleardir command was issued just before the upgrade, there is nothing to clear, no error occurs, and the server starts. If the server starts and is not inspected after the initial start-up, the server being in the wrong mode may go unnoticed.

The proper solution is to add proper authorizations after an upgrade, as described in *Reconfigure Security* on page 151, and restart the server. A new safety measure has also been added. If the environment variable EDAEXTSEC is set to OPSYS explicitly, and a server lacks authorization, it will not start (see *Preventing Unsecured Starts After Upgrades* on page 151 for details).

Procedure: How to Generate a Trace

To generate a server trace:

1. Turn tracing by going to the Reporting Server browser interface menu bar, selecting *Workspace*, and then *Diagnostics*; or else by running the ITRCON JCL member.
2. Reproduce the problem.
3. Submit the ISAVEDIA member to produce the diagnostic information.

   A directory called sd*nnnnnn* is created under your configuration directory (for example, /ibi/srv/ffs/sd123456). Diagnostic information is placed in this directory. Make sure you have access to this directory.

Do not change anything in the EDAENV member: changes could prevent the correct information from being copied to your directory.

Procedure: How to Generate a System Dump

To generate a system dump:

1. Allocate DDNAME SYSMDUMP pointing to the data set with the following DCB parameters:

   ```
   RECFM=FB,LRECL=4160,BLKSIZE=4160
   ```

2. To get the first dump, add the parameter FREE=CLOSE to your DD statement. The DD statement should appear as follows:

   ```
   //SYSMDUMP DD DISP=SHR,DSN=MYID.EDAPTH.SYSMDUMP,FREE=CLOSE
   ```

3. To get the last dump, the statement should appear as follows:

   ```
   //SYSMDUMP DD DISP=SHR,DSN=MYID.EDAPTH.SYSMDUMP
   ```

   Only two IDs must have privileges to write into this data set: ISERVER and IADMIN. General server users DO NOT need read or write access to the SYSMDUMP data set.

4. To prevent Abend-AID from intercepting the dump, add:

   ```
   //ABNLIGNR DD DUMMY
   ```

5. To prevent Language Environment from intercepting the dump, specify:

   ```
   EDADUMPOPT=UAIMM in EDAENV DD
   ```

   This enables you to get more accurate information reflecting the moment the abend actually occurs.

6. Save the entire job output for the server (including JES logs), and send it to Customer Support.

Instead of using JCL allocations to add SYSMDUMP, the procedure described below can be used alternatively.

Procedure: How to Add JCL Allocations to a Running Reporting Server

A z/OS operator can issue modify commands from the z/OS system console to allocate DDNAMES to the server without restarting it. This procedure is useful if you need to reallocate a file that was freed to allow a batch overnight utility to run, or perhaps to add SYSMDUMP allocation to a running server.

Syntax: How to Allocate a Data set From the z/OS System Console

```
F <iway_server_jobname/started task>,DYNAM ALLOC FI <ddname> DA <dsname>
<optional dynam parameters>
```

Example: Allocating a VSAM Data set

```
F IWAY2,DYNAM ALLOC F VSAMFILE DA VSAM.FILEA.CLUSTER SHR
```

Example: Allocating a SYSMDUMP Data set With FREE=CLOSE Option

```
F IWAY2,DYNAM ALLOC FILE SYSMDUMP DA PROD2.SYSMDUMP.DATA SHR CLOSE
```

Note: The examples above assume IWAY2 is the jobname/started task ID for the server.

All valid DYNAM ALLOC syntaxes are supported. For more information on the DYNAM command, refer to the *TIBCO WebFOCUS® Stored Procedure and Subroutine Reference for 3GL Languages* manual.

The following message will be issued in the server JESMSGLG indicating if the command was processed successfully or not.

Success:

```
+DYNAM COMMAND SUCCESSFULLY PROCESSED Rc=0
```

Failure:

```
+DYNAM ERROR: IKJ56225I DATA SET IWAY.TEST ALREADY IN USE, TRY LATER
```

Procedure: **How to Free Data sets Allocated to the Reporting Server**

A z/OS operator can issue modify commands from the z/OS system console to free DDNAMEs or DSNAMEs allocated to the server. Both global allocations (made at the server ISTART JCL) and local ones (DYNAM ALLOC commands issued by user tasks) can be freed. This procedure is useful if you need to free an allocation to run a batch utility overnight, without restarting the server.

Syntax: **How to Free a Data set From the MVS System Console**

To free a single DDNAME:

```
F <iway_server_jobname/started task>,DYNAM FREE FI <ddname>
```

To free a single DSNAME (all occurrences in the server):

```
F <iway_server_jobname/started task>,DYNAM FREE DS <dsname>
```

To free multiple DDNAMEs, passing a pattern (free all DDNAMEs starting with AB):

```
F <iway_server_jobname/started task>,DYNAM FREE FI AB*
```

To free multiple DSNAMEs (all occurrences in the server), passing a pattern (free all allocations of data sets starting with IWAY.VSAM):

```
F <iway_server_jobname/started task>,DYNAM FREE DA IWAY.VSAM*
```

A message will be issued in the iway_server JESMSGLG indicating if the command was processed successfully or not, as follows.

Success:

```
+DYNAM COMMAND SUCCESSFULLY PROCESSED Rc=0
```

Failure:

```
+DYNAM ERROR: IKJ56225I DATA SET IWAY.TEST ALREADY IN USE, TRY LATER
```

Example: **Freeing an Allocated Data Set**

Suppose ISTART JCL (jobname IWAY2) has the following allocation:

```
//VSAMFILE DD DISP=SHR,DSN=VSAM.FILEA.CLUSTER
```

The operator can free this file using the command (from MVS console):

```
F IWAY2,DYNAM FREE FI VSAMFILE
```

Procedure: How to Initialize the RDAAPP Application

RDAAPP is an interactive client test application that facilitates the execution of SQL statements and stored procedures on the Unified server. During the installation process, JCL and REXX routines are created in the installation data set as members IRDAAPPJ and IRDAAPPC respectively.

The following installation data set is used for USS deployment.

qualify.WFS.DATA

The following installation data set is used for PDS deployment.

qualify.PDS.WFS.DATA

Note: The RDAAPP application is not intended for use as a production tool.

1. To use the IRDAAPPJ JCL, you must first edit the member IRDAAPPJ and add your request details.

   a. To edit the member IRDAAPPJ, change the following field,

   ```
   //SYSIN DD *
   Put your request here
   //
   ```

   to

   ```
   //SYSIN DD *
   1
   <userid>
   <password>
   S SELECT COUNTRY   FROM CAR
   S SELECT CAR,SEATS FROM CAR
   Q
   //
   ```

b. Complete the panel as follows.

Field	Instructions	
`<enter userid>`	Enter a valid user ID or blank line if the userid of the user who submitted the job is to be used for a trusted connection.	
`<enter password>`	Enter the password for the above userid or a blank line if the userid/password of the user who submitted the job is to be used for a trusted connection.	
`1`	Match a node name in the EDACS3 allocation in the IRDAAPPJ JCL. Default (1) means LOOPBACK.	
`<enter request>`	Enter one of the following values:	
	`S`	To enter an SQL SELECT statement. Type the statement after you enter the value S (see the following example).
	`Q`	To quit.
	`?`	For this list of commands.
`Q`	Quit RDAAPP (It is needed twice).	

c. Once you have made the above edits, submit the JCL for execution.

2. Type the following command at the TSO ready prompt to use the IRDAAPPC REXX routine:

```
EX 'qualif.WFS.DATA(IRDAAPPC)'
```

or

```
EX 'qualif.PDS.WFS.DATA(IRDAAPPC)'
```

3. After the prompts, enter the same information as specified in the above table.

Example: **IRDAAPPC REXX Execution**

The following is the screen output from a sample execution of the IRDAAPPC REXX routine:

```
*********************************************************************
**                   RDAAPP Client test tool                       **
*********************************************************************
```

```
Allocating environment handle...
List of available servers:
 1 - LOOPBACK
Enter corresponding server entry number or name (default=1):


1
Enter User Name:
Enter Password:
Allocating connection handle...
Attempting connect to the datasource: LOOPBACK ...
Connect status = 0


New ODBC Connector Test.
Enter Command:
S SELECT COUNTRY   FROM CAR
Alloc stmt ...
Return code from alloc stmt is 0
Issuing SQLPrepare call for  SELECT COUNTRY   FROM CAR
Return code from SQLPrepare call is 0
Executing  SELECT COUNTRY   FROM CAR stmt...
Issuing SQLNumResultCols call for  SELECT COUNTRY   FROM CAR
Number of resultset columns is 1
Printing select item descriptions:


Issuing SQLDescribeCol call for colNum=1
item #1
colname = COUNTRY
coltype = 1
precision = 10
scale = 0
nullable = 0


Binding columns...
Fetching report data...
ENGLAND
FRANCE
ITALY
JAPAN
W GERMANY
<<< 5 record(s) processed. >>>


New ODBC Connector Test.
Enter Command:
S SELECT CAR,SEATS FROM CAR
Alloc stmt ...
Return code from alloc stmt is 0
Issuing SQLPrepare call for  SELECT CAR,SEATS FROM CAR
Return code from SQLPrepare call is 0
Executing  SELECT CAR,SEATS FROM CAR stmt...
Issuing SQLNumResultCols call for  SELECT CAR,SEATS FROM CAR
Number of resultset columns is 2
Printing select item descriptions:
```

```
Issuing SQLDescribeCol call for colNum=1
item #1
colname = CAR
coltype = 1
precision = 16
scale = 0
nullable = 0
 Issuing SQLDescribeCol call for colNum=2
item #2
colname = SEATS
coltype = 4
precision = 22
scale = 0
nullable = 0

Binding columns...
Fetching report data...
JAGUAR
2
JAGUAR
5
JENSEN
4
TRIUMPH
2
PEUGEOT
5
ALFA ROMEO
2
ALFA ROMEO
2
ALFA ROMEO
4
```

```
MASERATI
2
DATSUN
4
TOYOTA
4
AUDI
5
BMW
5
BMW
4
BMW
5
BMW
5
BMW
5
BMW
5
<<< 18 record(s) processed. >>>


New ODBC Connector Test.
Enter Command:
Q

Committing...
Return code from commit is 0
Disconnecting DBC ...
Freeing DBC handle...
Freeing ENV handle...
<<< RDAAPP : Exiting... >>>
```

PDS Deployment

The topics in this section describe how to install your server in a partitioned data set (PDS) environment.

Installation Requirements for PDS

Before beginning server installation, review all requirements.

Operating System Requirements

The server runs on any supported release of z/OS. For current information about supported releases, see the *TIBCO WebFOCUS® Release Notes*.

In general, the operating system should have the latest cumulative patch levels applied.

Confirm that your server installation software is labeled for your operating system level.

JVM Requirements for Java Services

If JVM-based adapters, server-side graphics, XBRL, or user-written CALLJAVA applications are to be used, a Java Runtime Environment (JRE) JVM must be installed on the machine, and the server must be configured to use it

The minimum JVM release level is 8 or higher, due to required internal components of the server. The Java Listener will not start unless 8 (or higher) is in use. Prior 7.x releases would allow the listener to start with any release, and sub-components would fail if they required a higher Java Level. The primary reason for this change is that Java 1.5 (and prior releases) are past their End of Service Life (EOSL) dates, and, as such, are unsupportable, in addition to lacking newer functionality. The following URL has Java EOL and EOSL information:

http://www.oracle.com/technetwork/java/eol-135779.html

Installing maintenance updates to the EDAHOME of an existing server running releases prior to production 7.7.05 will also have the requirement of moving up all dependent configurations to use Java 8 (as instructed in this section).

You may install a Java JRE or a Java SDK. When you install a Java SDK, the JRE component (where the JVM is installed) is included, so either is allowed. If using servlet, the Java SDK is required for the jar command, so it is generally preferred over the Java JRE. The SDK or JRE build type must also match the bit size of the server, which is 64-bit. If an appropriate JVM from a JRE or SDK is not found on the library path or using variables as described below, or is not the appropriate bit type, a *Failed to find JVM* message will be displayed. Further Java Services debugging information about loading the JVM will be written to the server start log indicating *JSCOM3 start failed* as well as additional information that may be useful in resolving the problem. JSCOM3 is the actual process name for the Java Services Listener and the terms are often used interchangeably.

The JDK JRE bin and server (or client) subdirectories must be specified in the load library path environment variable. A server restart is required, plus the appropriate JVM must be on the path if switching JRE levels. The load library path will be prompted at install time if JVM-based adapters or features are required. Otherwise, it can be manually set by editing the EDAENV file using any of the following methods.

- For Java JDK, set JDK_HOME (to the install home location) in the server environment configuration file (EDAENV).
- For Java JRE, set JAVA_HOME (to the install home location) in the server environment configuration file (EDAENV).
- Use library path (LIBPATH) to set explicit pathing. Use of JDK_HOME or JAVA_HOME is preferred as they are less prone to error. The JRE bin and server (or client) subdirectories must be specified in a path-based environment variable and a server restart is required.

To change or add operating system environment variables, set and export the variable in a .profile or script that always gets called during a server start. It is very common to place variables in the server edastart script, but it is recommended that they be placed in a script that in turn calls edastart (so that the edastart script remains vanilla).

To change or add a variable in a server environment start-up file (EDACONF bin\edaenv.cfg), either edit the file in a text editor before starting the server or:

1. Start the server (services like Java Listener may fail until configured and the server is restarted).
2. Open the Reporting Server browser interface and log on using an administrator ID.
3. Select *Workspace* from the main menu.
4. In the navigation pane, open the *Configuration Files* and *Miscellaneous* folders.
5. Right-click *Environment - edaenv.cfg* and select *Edit*.
6. Make the desired edit.
7. Save the file.
8. Restart the server (changes are not effective until the server is restarted).

The format of the edaenv.cfg variables is one per line in name=value pairs. Spaces before and after the equal sign are optional. Values with embedded spaces do not require quoting. Variables are always uppercase.

If JVM-based adapters or features are not required, and the JVM environment is not configured, the message *Failed to find JVM* is normal and can be ignored.

To add classes to the JVM class path for customer-written CALLJAVA applications, set and export the CLASSPATH variable to the operating system level before server start-up or use the Reporting Server browser interface to set the Java Listener IBI_CLASSPATH property.

IP Port Number Requirements

The installation process prompts for two IP port numbers: the TCP Listener and HTTP Listener. It also uses the next two consecutive ports after the supplied HTTP Listener port for FDS use. This results in a total of four IP ports.

The supplied IP port numbers must be above the IANA registered well-known reserve range (numbers under 1024) and not over the maximum legal number (65535). Do not use IP port numbers already used by other applications or products. Netstat, or netstat like commands, should reveal what actual ports are in use.

Browser Requirements

The Reporting Server browser interface requires one of the following web browsers:

- Microsoft Edge.
- Mozilla Firefox® 59 or higher.
- Google Chrome® 65 or higher.

Disk Space Requirements

The server disk space requirements are:

Supplied (EDAHOME) Data Sets	3390 Cylinders
high_level_qualifier.P.HOME.ACX	2
high_level_qualifier.P.HOME.BIN	1100
high_level_qualifier.P.HOME.CICS.LOAD	10
high_level_qualifier.P.HOME.ERR	500
high_level_qualifier.P.HOME.ETC	100
high_level_qualifier.P.HOME.FEX	25
high_level_qualifier.P.HOME.LOAD	750
high_level_qualifier.P.HOME.MAS	4

Configuration (EDACONF) Data Sets	3390 Cylinders
high_level_qualifier.WFS.CONF.ACX	2
high_level_qualifier.WFS.CONF.CFG	2
high_level_qualifier.WFS.CONF.MAS	2
high_level_qualifier.WFS.CONF.PRF	2

Installation Data Sets	3390 Cylinders
high_level_qualifier.HOME.DATA	10
high_level_qualifier..DATA	2

Application Data Sets	3390 Cylinders
approot.IBISAMP.type.DATA	38 (across 14 data sets)
approot.BASEAPP.type.DATA	56 (14 data sets using 4 cylinders per file)

Deferred Execution Data Sets (Optional)	3390 Cylinders
high_level_qualifier.WFS.CONF.DFM.DEL	5
high_level_qualifier.WFS.CONF.DFM.RPE	5
high_level_qualifier.WFS.CONF.DFM.RPF	5
high_level_qualifier.WFS.CONF.DFM.RPO	100
high_level_qualifier.WFS.CONF.DFM.RQD	5
high_level_qualifier.WFS.CONF.DFM.RQF	5
high_level_qualifier.WFS.CONF.DFM.RQO	5
high_level_qualifier.WFS.CONF.DFM.RQP	5

Note: Deferred Execution Datasets are not created by the installation procedure. They are created when the Scheduler/Deferred service starts. By default, the Scheduler/Deferred service auto starts at server startup. To disable the feature, enter dfm_autostart = n in the EDASERVE administration control file.

Supplementary Data Sets	3390 Cylinders
high_level_qualifier.WFS.SYSRPC.FOCUS	1
high_level_qualifier.WFS.ETLLOG.FOCUS	1

Supplementary Data Sets	3390 Cylinders
high_level_qualifier.WFS.ETLSTATS.FOCUS	1
high_level_qualifier.WFS.CONF.SMARTLIB.DATA	1

high_level_qualifier

Is the high-level qualifier to be used for all output libraries. You specify the high-level qualifier during server installation, as described in *Step 4. Run ISETUP* on page 193, in Step 4.

approot

Is the default location for storing applications. You specify approot during server installation, as described in *Step 4. Run ISETUP* on page 193,

Memory Requirements

Memory usage of a configured environment consists of the following elements:

- Workspace Manager
- Listeners
- Concurrently running application agents

Actual memory usage depends on application features, and varies depending on the application. The SHRLIBRGNSIZE parameter (defined on SYS1.PARMLIB, member BPXPRMxx) can affect the amount of memory that the server address space will allocate. For SHRLIBRGNSIZE, we recommend the default MVS installation value of 64Mb:

```
SHRLIBRGNSIZE(67108864)
```

Server memory usage:

- The workspace (including Listeners) uses 200 megabytes.
- Each pre-started agent requires 4 megabytes.

The minimum amount of memory for a newly installed server with no workload is 250Mb. However, depending on usage, workload, and configuration options, 500Mb is recommended to start, to be adjusted as needed.

Communication Requirements

You need four TCP/IP ports for each server instance that you configure. Three of these ports must be consecutive. You specify these port numbers during installation. You may require additional ports depending on which options you configure later.

The server supports only IBM TCP/IP. It does not support Interlink or any other third-party TCP/IP.

USS Segment Requirements

PDS deployment requires each user of the server to be identified to USS by means of a default segment definition. This default OMVS segment is defined when USS is installed as a part of z/OS. Refer to your IBM UNIX System Services documentation for more information about this subject.

ZFS Home and Configuration Directory Requirements

Libraries and the APIs supporting them must reside in the ZFS file system to enable the following features:

- Server-side graphics.

They are also required for the following Java-based and SAP-based adapters:

- Call Java.
- EJB.
- JDBC.
- Microsoft SQL Server.
- SQL SAP.
- SAP BWB.

At installation time, a panel with a list of adapters to be configured will be displayed. If any of the above adapters are selected, the installation will require the path for two ZFS locations as follows:

- **edahome_dir**. Provide the edahome path for the dll modules that interface with Java/SAP and must reside in ZFS. The directory will be created with 755 permissions, if it does not exist.

- **edaconf_dir**. Provide the edaconf path to be used for both configuration files (such as codepage files), as well as the root location for temporary files (such as traces and logs), that must reside in ZFS. If it does not exist, the directory will be created with 755 permissions.

If no data adapters were selected, the next panel will allow an optional configuration for the JSCOM3 listener. If server-side graphics support is desired, the listener must be configured and all three paths are required (edahome_dir, edaconf_dir, plus the path to Java passed to either JDK_HOME or JAVA_HOME).

If edahome_dir is not defined at installation time, it will not be possible to configure it later using the Reporting Server browser interface. The server will have to be re-installed, configuring the JSCOM3 listener.

Installing New on PDS

To install a new Server for z/OS deployed using partitioned data set (PDS) libraries, perform the following steps.

Step 1. Set Up User IDs

You can use any user ID to install and run the server. Whichever ID you use becomes the first server administrator ID (sometimes referred to as iadmin).

Step 2. Collect Required Information for Adapters

For current information about which adapters are supported, see the *TIBCO WebFOCUS® Adapter Administration* manual.

You must provide information to configure the adapters that you want to install. The installation procedure automatically prompts you for this information. When you are prompted for an optional steplib, ddname, or environment variable, the installation procedure will indicate this with an OPT> prompt.

After you have installed and configured the server, you will be able to further configure your adapters using a web-based server configuration tool called the Reporting Server browser interface.

The following table describes what information you need to provide for each adapter that you have. (If an adapter is not listed, no information needs to be provided for it.) Note that the table refers to:

- **IRUNJCL.** This procedure contains the JCL procedure for the server, and is a member of the configuration library

high_level_qualifier.PDS.WFS.DATA

where:

high_level_qualifier

Is the high-level qualifier to be used for all output libraries. You specify the high-level qualifier during server installation, as described in *Step 4. Run ISETUP* on page 193, in Step 6.

Adapter	Information you must provide
Adabas	Provide the data set name for the following STEPLIB allocation: ❑ load library This is required only for the synonym creation process. For example, in a production environment in which all synonyms already exist, you can omit this. When you configure the adapter, you will need to provide the name of the Adabas source library and the associated data set name.
CA- DATACOM	Provide the data set names for the following STEPLIB allocations: ❑ CUSLIB load library ❑ CAILIB load library ❑ utility library ❑ URT library

Adapter	Information you must provide
CA- IDMS (both DB and SQL)	Provide the data set names for the following STEPLIB allocations: ❑ load library ❑ DBA load library Provide the data set names to which the following ddnames are allocated: ❑ SYSIDMS. Check with your CA-IDMS DBA regarding this ddname. ❑ SYSCTL. Is the library corresponding to the central version you want to use.
CICS Transaction	Provide the data set name for the following STEPLIB allocation: ❑ CICS EXCI load library
Call Java	You must have the JDK installed. Provide a value for the following environment variables: ❑ CLASSPATH. Provide the paths of the .jar files that you want to access. These paths will be appended to CLASSPATH. This adapter requires configuration of the JSCOM3 listener. Provide three required paths: ❑ The path to JVM using either JDK_HOME or JAVA_HOME, as described in *JVM Requirements for Java Services* on page 179. ❑ The paths to edahome_dir and edaconf_dir, as described in *ZFS Home and Configuration Directory Requirements* on page 184.

Adapter	Information you must provide

EJB	You must have the JDK installed.
	
	Provide a value for the following environment variables:
	
	❑ CLASSPATH. Provide the paths of the .jar files that you want to access. These paths will be appended to CLASSPATH.
	
	If you are deploying the adapter to access an EJB on a:
	
	❑ WebLogic server, specify the following path:
	`/pathspec/weblogic.jar`
	
	❑ WebSphere server, specify the following paths:
	`/pathspec/websphere.jar`
	
	`/pathspec/ejbcontainer.jar` (one for each EJB container)
	
	This adapter requires configuration of the JSCOM3 listener. Provide three required paths:
	
	❑ The path to JVM using either JDK_HOME or JAVA_HOME, as described in *JVM Requirements for Java Services* on page 179.
	
	❑ The paths to edahome_dir and edaconf_dir, as described in *ZFS Home and Configuration Directory Requirements* on page 184.

Adapter	Information you must provide
JDBC	You must have the JDK installed. Provide a value for the following environment variables: ❑ CLASSPATH. Provide the paths of the .jar files that you want to access. These paths will be appended to CLASSPATH. This adapter requires configuration of the JSCOM3 listener. Provide three required paths: ❑ The path to JVM using either JDK_HOME or JAVA_HOME, as described in *JVM Requirements for Java Services* on page 179. ❑ The paths to edahome_dir and edaconf_dir, as described in *ZFS Home and Configuration Directory Requirements* on page 184.
Microsoft SQL Server	You must select Call Java adapter in addition to the Microsoft SQL Server adapter. Provide a value for the following environment variables: ❑ CLASSPATH. Provide the paths to the following files; these paths will be appended to CLASSPATH. ❑ msbase.jar ❑ mssqlserver.jar ❑ msutil.jar This adapter requires configuration of the JSCOM3 listener. Provide three required paths: ❑ The path to JVM using either JDK_HOME or JAVA_HOME, as described in *JVM Requirements for Java Services* on page 179. ❑ The paths to edahome_dir and edaconf_dir, as described in *ZFS Home and Configuration Directory Requirements* on page 184.

Adapter	Information you must provide
Db2 CAF	Provide the data set names for the following STEPLIB allocations: ❑ SDSNLOAD load library For security information, see *Db2 Security Exit Configuration for PDS* on page 209. ❑ SDSNEXIT load library (optional)
Db2 CLI	Provide the data set names for the following STEPLIB allocations: ❑ SDSNLOAD load library For security information, see *Db2 Security Exit Configuration for PDS* on page 209. ❑ SDSNLOD2 load library ❑ SDSNEXIT load library (optional; this is needed only for an explicit connection). Provide the data set name (including member name if applicable) for the following DDname: ❑ DSNAOINI, which contains the Db2 CLI ini file.
IMS	Provide the data set names for the following STEPLIB allocations: ❑ DFSPZP load library (optional; not needed if PZP modules are stored in the DFSRESLB library) ❑ DFSRESLB load library
Millennium	Provide the data set name for the following STEPLIB allocation: ❑ load library

Adapter	Information you must provide
Model 204	Provide the data set name for the following STEPLIB allocation: ❑ load library
MQSeries	Provide the data set names for the following STEPLIB allocations: ❑ SCSQLOAD load library ❑ SCSQAUTH load library
NATURAL Batch	Provide the data set name for the following STEPLIB allocation: ❑ NATURAL load library
SAP (SQL)	Provide values for the following environment variables: ❑ LIBPATH, which contains the path to SAP RFC SDK. ❑ SAP_CODEPAGE=0126, or the correct SAP code page for your language environment. This adapter requires configuration of two required paths: ❑ The paths to edahome_dir and edaconf_dir, as described in *ZFS Home and Configuration Directory Requirements* on page 184 It is recommended that the code page conversion tables be created under the edaconf_dir directory.

Adapter	Information you must provide
SAP BW	Provide values for the following environment variables: ❑ LIBPATH, which contains the path to SAP RFC SDK.SAP_CODEPAGE=0126, or the correct SAP code page for your language environment. This adapter requires configuration of two required paths: ❑ The paths to edahome_dir and edaconf_dir, as described in *ZFS Home and Configuration Directory Requirements* on page 184. Is recommended that the code page conversion tables be created under the edaconf_dir directory.
Supra	Provide the dataset name for the following STEPLIB allocations: ❑ LINKLIB load library. ❑ INTERFLM load library. ❑ ENVLIB load library.

Step 3. Optional Low-Level Qualifier Changes

We recommend retaining the default low-level qualifiers that are supplied for the installation libraries. However, if you need to change any of them (for example, to conform to site-specific naming conventions), you can do so by editing them in member PDSSNAME of *high_level_qualifier*.HOME.DATA. You can see a list of the qualifiers in *Default Low-Level Qualifiers* on page 192.

Caution: If you change any low-level qualifiers and do not reflect those changes exactly in PDSSNAME, you will experience problems with the server installation and operation.

Do not change the value of &CONFTYPE.

Once you have finished changing any names, continue with *Step 4. Run ISETUP* on page 193.

Reference: **Default Low-Level Qualifiers**

The following low-level qualifiers are set in *high_level_qualifier*.HOME.DATA(PDSSNAME):

```
//          SET  EDALOAD='P.HOME.LOAD'       Load Library
//          SET  EDAHETC='P.HOME.ETC'        Server html and text files
//          SET  EDAHACX='P.HOME.ACX'        Access files
//          SET  EDAHFEX='P.HOME.FEX'        RPCs
//          SET  EDAHMAS='P.HOME.MAS'        Master files
//          SET  EDAHBIN='P.HOME.BIN'        Server binary files
//          SET  EDAERR='P.HOME.ERR'         Server NLS and error files
//          SET  EDACICS='P.HOME.CICS.LOAD' CICS Load Library
//          SET  PDSWFSD='PDS.WFS.DATA'      WebFocus Reporting server
```

Step 4. Run ISETUP

Server installation consists of a series of ISPF panels, which gather the required information. After the panel dialog is complete, JCL is created and submitted to install the server on z/OS. This JCL job retrieves the remainder of the data sets from the media and configures a basic working server.

1. Execute the ISETUP member of your *high_level_qualifier*.HOME.DATA using ISPF option 6.

   The first Installation and Configuration panel opens.

```
TIBCO                    Installation and Configuration   Unified Server Install
Command ===>                                                                   P0

Unified Server Installation
Please select one of the following options:

         1. USS/ZFS Deployment

            . Installation files and temporary files in ZFS
            . Application files, like synonyms and procedures, in ZFS (or
              optionally in both ZFS and PDS)

         2. PDS Deployment

            . Installation files and temporary files in PDS
            . Application files, like synonyms and procedures, in PDS (or
              optionally in both PDS and ZFS)


Enter selection (Default=1) ===> 1

Press Enter to continue, PF3 to END                              Version: 9999
```

2. Type *2* and press Enter to continue to the next panel.

The following panel opens.

```
TIBCO                    Installation and Configuration        z/OS PDS Deploy
Command ===>                                                              D1

Please select one of the following options:


         1. Install and Configure
         2. Add Additional Configuration Instance
         3. Refresh Installation (Reinstall, Keep Configurations)


Enter selection (Default=1) ===> 1
Input source                ===> D                    (T)ape or (D)isk
Installation Userid         ===> IADMIN               Logged on Userid
PTH Administrator Userid    ===> srvadmin             Server install only
PTH Administrator Password  ===> _                    Retype  ===>


Enter Job Card information                Override JOB name checking ===> N
===> // JOB (ACCT INFO),_____________________________________________________
===> //*____________________________________________________________________
===> //*____________________________________________________________________
Press Enter to continue, PF3 to END
```

3. Complete the panel as directed in the following table.

Field	Instructions
Enter selection	Accept the default value 1, *Install and Configure*, for a new installation. For option 2, *Add Additional Configuration Instance*, see *Adding a Configuration Instance for PDS* on page 214. For option 3, *Refresh Installation*, see *Upgrading Your TIBCO WebFOCUS Reporting Server Release for PDS* on page 221.
Input source	Enter the input source: ❑ *D* for Disk - If you selected manual download from the download instructions.
Installation Userid	Shows the current logon ID. It cannot be changed.

Field	Instructions
PTH Administrator Userid	An ID is required to administer the server immediately after initial installation. This ID is defined and maintained solely in the realm of the server. It defaults to *srvadmin*, and it can be changed here. For more information about running the server in secure mode, see *Step 6. Configure Security* on page 201.
PTH Administrator Password	Password for the PTH Administrator ID. It cannot be left blank and must be matched at Retype field.
Enter Job Card information	To provide JOB card information for submitting jobs to the JES queue, provide a valid job name (a maximum of seven characters following the // on the first JCL line), which defaults to the user ID that you are currently using. This job name is used for multiple submissions (for example, *jobname*A, *jobname*B, *jobname*C, and so on) in the JCL generated by the installation procedure.
Override JOB name checking	To provide your own JOB card information, including JOB name, enter *Y* and provide valid JOB card information in the *Enter Job Card information* field. The JOB card information that you enter will be used for each job that is submitted.

4. Press Enter to continue to the next panel.

   Note that in the current panel (and some later panels), if you are running ISETUP from:

   - *high_level_qualifier*.HOME.DATA, the panel will display default values for some fields.
   - Any other library, the panel will not display any default values.

In this and some later panels, you can see a field's default value (if one exists) by blanking out the field and pressing Enter.

```
TIBCO                    Installation and Configuration        z/OS PDS Deploy
Command ===>                                                              D8
                                 New Installation

Please enter the following information for WebFocus Reporting Server

  Input Libraries HLQ       ===> IADMIN.SRV82 _
  (EDAHOME)
  Copy to runtime libraries ===> N           (Y or N)

 Output Libraries (blank any field for default)

  Output Libraries HLQ      ===> IADMIN.SRV82
  (EDACONF)            Unit ===> SYSDA    Type ===> VOL=SER  ===>

 Configuration options
  Approot value             ===> PLEASE SUPPLY VALUE     (21 Characters max)
  HTTP Listener Port        ===> 8121         TCP Listener Port  ===> 8120

  Installation JCL Library  ===> IADMIN.SRV82.PDS.WFS.DATA


Press Enter to continue, PF3 to return to previous menu
```

Complete the panel as follows.

Field	Instructions
Input Media	
Input Libraries HLQ (EDAHOME)	This is the high-level qualifier that you had specified when you manually downloaded the installation software from the download site. This is an input field if Disk input source was previously selected. Otherwise, it is a protected field.
Copy to runtime libraries	If you want to use the downloaded installation software as a backup, and create a new copy from which to run, enter *Y*. If the Input Libraries HLQ and the Output Libraries HLQ are the same, this value will be ignored and no copy will take place. Otherwise, accept the default *N* to run from the downloaded software.
General Installation Parameters	
Output Libraries HLQ	This is the high-level qualifier that the installation procedure will use to allocate output libraries.

Field	Instructions
Unit/Type	These show the values that the installation process will use to allocate the output libraries. If necessary, you can change these to site-specific values. Type can be **VOL=SER** (default), **DATACLAS**, **MGMTCLAS**, or **STORCLAS**.
Approot value	This is where application components will reside. Note that this high-level qualifier *must* differ from the output libraries high-level qualifier (EDACONF) that you entered at the top of the panel. To specify a different qualifier for application components, change the value for this field. It can be up to 21 characters.
HTTP Listener Port	This is the port number that the server will use for HTTP. It is the first of three connection ports that must be available to the server. For example, if you choose port 8101, then ports 8101, 8102, and 8103 are used by the server. Ensure that you choose ports that are not currently being used.
TCP Listener Port	This is the port number of the TCP Listener. The default is one less than the port specified for the HTTP Listener, but it can be any port number other than the three reserved for HTTP.

5. Press Enter to continue to the next panel.

   The Data Adapter panel may open. If the Data Adapter panel opens, continue with Step 8; otherwise, skip to Step 9.

6. The Data Adapter panel lists adapters that require the allocation of MVS libraries in IRUNJCL or environment variables in the EDAENV member. To select specific adapters:
   a. Type *Y* next to the required adapters and press Enter.
   b. Supply the requested information, which is described in *Step 2. Collect Required Information for Adapters* on page 185.

      After you have finished installing and configuring the server, you can use the Reporting Server browser interface to finish configuring these adapters, and to configure adapters that do not have MVS JCL requirements.

7. Press Enter to continue to the next panel.

   The JSCOM3 Listener configuration panel opens.

   a. The panel will prompt for the path to the Java environment to be passed to either JDK_HOME or JAVA_HOME, as described in *JVM Requirements for Java Services* on page 179, and it will also prompt for edahome_dir and edaconf_dir, as described in *ZFS Home and Configuration Directory Requirements* on page 184.

   b. Configuration of the JSCOM3 Listener is either optional or mandatory depending on which adapters were selected. If any Java-based adapters were selected (EJB, Call Java, JDBC, Microsoft SQL Server), the configuration of all three paths listed above is mandatory. If SAP-based adapters were selected (SAP or SAP BW), only edahome_dir and edaconf_dir are required.

   c. If no Java-based or SAP-based adapters were selected, this configuration might still be desirable to enable the server-side graphics feature. To skip the configuration, leave the path blank.

8. Press Enter to continue to the next panel.

   The confirmation panel opens.

```
TIBCO                      Installation and Configuration        z/OS PDS Deploy
Command ===>                                                                  D9
                                 New Installation

Please confirm the following information for WebFocus Reporting Server
 Input Media
  Input Libraries HLQ       ===> IADMIN.SRV82
  (EDAHOME)

 Product Configuration parameters
  Output Libraries HLQ      ===> IADMIN.SRV82
  (EDACONF)             Unit===> SYSDA    Type ===> VOL=SER  ===>
 (Above will be used for all output libraries)

  Approot  value            ===> IADMIN.APPS
  HTTP Listener Port        ===> 8121      TCP Listener Port  ===> 8120
  PTH Administrator userid  ===> srvadmin

  Installation JCL Library  ===> IADMIN.SRV82.PDS.WFS.DATA
  Review output allocations ===> N           (Y or N)

Continue ? (N)o, (C)reate JCL only, (S)ubmit JCL  ===> N   (Enter N, C or S)
Press Enter to process, PF3 to return to previous menu
```

9. If you wish to review a list of the data sets to be allocated, type *Y* in the Review output allocations field and press Enter.

   A panel opens listing the data sets. You may need to page down to see the entire list. Press Enter when you are done to return to the confirmation panel.

10. Ensure that all values on the Confirmation panel are correct, then select one of the following options

- **N** to return to the initial panel so that you can change installation values.
- **C** to create JCL which you can submit at a later time. The JCL is placed in your *high_level_qualifier*.PDS.WFS.DATA configuration library.
- **S** to create JCL in *high_level_qualifier*.PDS.WFS.DATA, and submit the job immediately.

where:

high_level_qualifier

Is the high-level qualifier to be used for all output libraries. You specified the high-level qualifier during installation, as described in *Step 4. Run ISETUP* on page 193, in Step 4.

11. As the job is processed, in SDSF, check JESLOG for errors and return codes.

The following is a table of the jobs created. All members are created in the configuration library (as described in Step 11).

Job	Description
ISETUPJ1	Main JCL Job stream that is used to install the server.
ISOPTS1	Options used to install.

The following members all call procedure IRUNJCL, which is the main server JCL. If you need to change the server JCL, change member IRUNJCL.

Member	Description
ISTART	Starts the server.
ISAVEDIA	JCL to print a copy of configuration files for diagnostic purposes.
ITRCON	Starts the server with traces on.

The following members contain batch JCL for auxiliary functions, and are created in the configuration library.

Member	Description
CMRUN	JCL to run Data Migrator batch jobs.
DB2V*ver*PR	Db2 DBRM, where *ver* is your supported version of Db2 referenced in GENDB2 JCL.
GENDB2	JCL to bind the Db2/CAF plan.
IRDAAPPC	Example CLIST to run RDAAPP Client test tool.
IRDAAPPJ	Example JCL to run RDAAPP Client test tool.

The following members contain sample started task JCL, and are created in the configuration library.

Member	Description
IWAYS	A started task that starts the server.
EDAENV	A parameter file used by the server. It contains all required environment variables.

Step 5. Test the Installation

To test the server installation:

1. Log on to TSO as iadmin.
2. Submit the ISTART JCL from the configuration library to start the server. This executes the IRUNJCL proc. The configuration library is

   high_level_qualifier.PDS.WFS.DATA

   where:

   high_level_qualifier

   Is the high-level qualifier to be used for all output libraries. You specified the high-level qualifier during server installation, as described in *Step 4. Run ISETUP* on page 193, in Step 6.

3. Check the job output for errors. Look for the EDAPRINT message:

   ```
   (EDA13023) ALL INITIAL SERVERS STARTED
   ```

4. Start the Reporting Server browser interface by opening a browser pointed at the listener port of the server. The URL format is

   `http://host:port`

   where:

   host

   Is the name of the machine on which the product is installed.

   port

   Is one port higher than the port specified when installing the server. For example, if you specified port 8100 during installation, then use port 8101 to access the Reporting Server browser interface.

   The Reporting Server browser interface opens.

5. If the Reporting Server browser interface opens and displays application tree folders in the left pane, the server is working because it uses its own underlying data access and reporting technologies to visualize the application tree.
6. Continue with adapter configuration, as described in the *TIBCO WebFOCUS® Adapter Administration* manual.

When you are finished using the server, you can use the Reporting Server browser interface to stop the server by going to the Reporting Server browser interface menu bar, selecting *Workspace*, and then *Stop*.

If you experience problems at start-up, examine the job output for more information.

Step 6. Configure Security

If you will be configuring security provider OPSYS, you must perform the instructions in *How to Configure Security With All Security Products* on page 204, regardless of which security product you use. (For security providers PTH, DBMS, and LDAP, skip these topics.)

For a full description of all security providers:

1. From the Reporting Server browser interface menu bar, select *Help*, then *Contents and Search*.

   The Reporting Server browser interface Help window opens.

2. In the left pane, expand *Server Administration*.

Alternatively, see the *TIBCO WebFOCUS® Reporting Server Administration* manual.

Security Providers

The default security provider for a new installation is the internal security provider, PTH. The PTH provider implements security using user IDs, passwords, and group memberships stored in the admin.cfg configuration file.

After the initial installation, the Server Administrator that was configured during the installation can start the server and use the Reporting Server browser interface to further customize security settings, for example, to configure alternate or additional security providers, create additional PTH IDs, and register groups and users in a security role. For more information about security providers, see the *Server Security* chapter in the *TIBCO WebFOCUS® Reporting Server Administration* manual.

Procedure: How to Satisfy Security Provider OPSYS Requirements

To run a server with security provider OPSYS, you must perform the following steps. You must do this once after installing and after each refresh of the server with fixes.

Set up tscom300.out as a root-owned SUID program:

1. If the server is running, bring it down.
2. Log on to the system as root, or issue the su root command.
3. Change your current directory to the bin directory of the home directory created during the installation procedure.

   For example, type the following command:

   ```
   cd /home/iadmin/ibi/srv90/home/bin
   ```

4. Change file ownership and permissions by typing the following commands:

   ```
   chown root tscom300.out
   chmod 4555 tscom300.out
   ```

5. Verify your changes by issuing the following command:

   ```
   ls -l tscom300.out
   ```

   The output should be similar to the following:

   ```
   -r-sr-xr-x 1 root iadmin 123503 Aug 23 04:45 tscom300.out
   ```

   Note the permissions and ownerships.

When you start the server, it will now run with security provider OPSYS.

The chmod and chown steps will need to be repeated after any server upgrade since the tscom300.out file is replaced during an upgrade and the attributes are lost.

Note: The server will issue RACROUTE REQUEST=VERIFY calls to authenticate users, so all users must have access to APPL MSO, which identifies our server.

Note: If this Security Provider OPSYS step has been configured and the site later decides to switch to Security OFF, special steps must be taken to ensure the mode remains after a full server shutdown (where edastart -start is used to restart the server). The steps are:

1. After the server recycles from the change to OFF, use the Reporting Server browser interface to open the environment configuration file of the server by clicking *Workspace* and expanding the *Configuration Files* folder, followed by the *Miscellaneous* folder.
2. Double-click *Environment - edaenv.cfg* to edit the file and add the *EDAEXTSEC=OFF* variable.
3. Save your work.

After the next full server shutdown, be sure to do an edastart -cleardir before restarting the server. This will clear any root-owned files that would prevent a security OFF server from starting.

Preventing Unsecured TIBCO WebFOCUS Reporting Server Starts After Upgrades

If the server cannot impersonate users because it lacks platform-specific authorization steps, the server start aborts and error messages are written to the edaprint log.

This feature prevents an unsecured server start after a software upgrade if any of the required post-upgrade reauthorization steps are missed on a UNIX, IBM i, or z/OS USS deployment. This is not applicable to other platforms. The setting may be placed in any normal server start-up shell or profile that a site is using or in the server edaenv.cfg environment configuration file. The messages vary slightly by platform.

The edaprint messages are:

```
Configured security is 'ON' as set by EDAEXTSEC variable.

Server has no root privilege.

Workspace initialization aborted.

(EDA13171) UNABLE TO START SERVER
```

Procedure: How to Configure Security With All Security Products

To configure security with RACF, *e*Trust CA-ACF2, or *e*Trust CA-Top Secret:

1. Log on to TSO using the ID used to install the server.
2. The libraries allocated to STEPLIB in IRUNJCL must be APF-authorized. Any non-APF-authorized libraries must be allocated to the TASKLIB DDNAME.
3. Restart the server.

Note: If you want to use *e*Trust CA-ACF2 or *e*Trust CA-Top Secret, contact Customer Support.

Procedure: How to Configure Security With *e*Trust CA-Top Secret

To use *e*Trust CA-Top Secret security, perform the following step:

1. Create an *e*Trust CA-Top Secret facility entry for the server security module, R1SEC. The only need for permissions is for the RACROUTE call from the R1SEC program.

Example: Facility Entry Defining the Server to CA-Top Secret

The following is an example of a facility entry that defines the server to *e*Trust CA-Top Secret:

```
PGM=R1SEC ID=1 TYPE=099
ATTRIBUTES=IN-USE,ACTIVE,SHRPRF,ASUBM,NOABEND,MULTIUSER,NOXDEF
ATTRIBUTES=LUMSG,STMSG,SIGN(M),INSTDATA,RNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,WARNPW,NOTSOC,LCFTRANS
ATTRIBUTES=NOMSGLC,NOTRACE,NOEODINIT,IJU,NODORMPW,NONPWR
ATTRIBUTES=LUUPD MODE=FAIL DOWN=GLOBAL LOGGING=ACCESS,INIT
UIDACID=8 LOCKTIME=000 DEFACID=*NONE* KEY=8
MAXUSER=03000 PRFT=003
```

Starting and Stopping a TIBCO WebFOCUS Reporting Server for PDS

This section provides information on operation and use of the server. Additional information on the server and how to configure adapters is available in the Reporting Server browser interface help. The Reporting Server browser interface help is also available as the *TIBCO WebFOCUS® Reporting Server Administration* manual.

Starting the TIBCO WebFOCUS Reporting Server Using a Batch Job

To start the server, submit the ISTART member of the MVS configuration library (*high_level_qualifier*.WFS.DATA) for your server.

Starting the TIBCO WebFOCUS Reporting Server Using a Started Task

ISETUP creates started task JCL to start the server. This started task in a member of the MVS configuration library is IWAYS.

In order to execute the started task, you must:

- **Copy it** into SYS1.PROCLIB or any other JES2 Proclib data set.
- **Satisfy security requirements.** All external security-related permissions must exist for both the data sets and the started tasks. In order to issue the started tasks, the user must satisfy both of the following requirements:
  - Have at least OPERATOR authority defined within the Reporting Server browser interface.
  - Be in the same security group, or associated with the same security group, as the owner of the server directory structure (for example, as iadmin).

To submit the started task from the MVS console, issue the following command:

```
S IWAYS
```

You can add the started task to any automation product that you run.

Stopping the TIBCO WebFOCUS Reporting Server

You can stop the server using any of the following methods:

- **Reporting Server browser interface.** From the Reporting Server browser interface menu, bar select *Workspace* and then *Stop*.
- **MVS operator command.** On the MVS Console or SDSF, issue the following operator MODIFY command:

  ```
  F jobname, -stop
  ```

  where:

  jobname

  Is the job under which the server is running.
- **Cancel the server job.** In SDSF, cancel the job.

Enabling HTTPS Security on the HTTP Listener for PDS

If you are using RACF, a private key *must be* generated together with the certificate. The generated key must be type RSA. The supported private key size is up to 4096 bits.

Generating the Certificate and Key

- **Generating the Certificate.** You can generate the certificate using the TSO RACDCERT command with options GENCERT (generate certificate) or GENREQ (generate certificate request). For example:

```
RACDCERT GENCERT SUBJECTSDN(CN('Workspace Manager') -
OU('IOD') -
O('IBI') -
C('US')) -
SIZE(2048) -
NOTAFTER(DATE(2026-12-01)) -
ID(JOBOWNID) -
RSA -
WITHLABEL('IBIcert')

SETROPTS RACLIST(DIGTCERT) REFRESH
```

- **Creating the Key Ring.** You can create the key ring using the RACDCERT ADDRING command. For example:

```
RACDCERT ADDRING(IBIring1) ID(JOBOWNID)
```

- **Connecting the Certificate to the Key Ring.** You can connect the certificate to a ring using the RACDCERT CONNECT command. For example:

```
RACDCERT CONNECT(LABEL('IBIcert') DEFAULT RING(IBIring1)) -
ID(JOBOWNID)
```

The ID owner of all objects is the same. It must be the owner ID of the server job. In these examples, the value JOBOWNID is used arbitrarily.

The following JCL shows how to run the RACDCERT command in batch:

```
//*** JOB CARD *************
//*******************************************************
//STEP1 EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
RACDCERT LIST ID(JOBOWNID)
```

For detailed information and options of the RACDCERT command, see the IBM document *z/OS Security Server RACF Command Language Reference*.

TLS 1.3 SSL Protocol Requirements

The TLS 1.3 protocol requires additional RACF permissions be given to users and/or groups connecting to the Reporting Server. READ permission must be given to CSFOWH CL(CSFSERV).

If you do not plan to use the default of TLS 1.3, you can force the Reporting Server to use TLS 1.2 by adding the following parameter to the edaserve.cfg file:

```
ssl_protocol = tls_1_2
```

Enabling HTTPS

Once the key ring and label are created, to enable HTTPS:

1. Go to the Reporting Server browser interface Workspace page.
2. Expand *Special Services and LIsteners*.
3. Right-click TCP/HTTP and click *Properties of HTTP*.

   The Listener Configuration page opens.
4. Expand the Security section.
5. In the Enable HTTPS drop-down list, select Yes.

   Additional fields open in which you can enter the certificate label and keyring values you defined using the RACDCERT commands.

   ```
   SSL_CERTIFICATE = keyring
   SSL_LABEL = certificate
   ```

6. Click *Save and Restart Server*.

Defining the ICSF Dataset Key Label for PDS to Use Pervasive Encryption

In the following sample JCL, values are shown for clarity. These are the current IBM defaults.

```
SYMEXPORTABLE(BYANY) and ASYMUSAGE(HANDSHAKE SECUREEXPORT)
```

In the following sample PERMIT statement, ID contains only group names, not user ID names. During installation, you can choose which name to use or to use a combination of both.

Note: PGMYMG, PGM, QCS, EDA, and CSD in the sample code are arbitrary users and groups.

```
//TSOBATCH EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
RDEF CSFKEYS DATASET.PGMYMG.ENCRYPTKEY.001 OWNER(SYS1) UACC(NONE) -
ICSF(SYMCPACFWRAP(YES) SYMCPACFRET(YES)-
SYMEXPORTABLE(BYANY) ASYMUSAGE(HANDSHAKE SECUREEXPORT))
PERMIT DATASET.PGMYMG.ENCRYPTKEY.001 CLASS(CSFKEYS) ACCESS(READ) -
ID(PGM QCS EDA CSD)
SETROPTS RACLIST(CSFKEYS) REFRESH
/*
//
```

ICSF Panels

1. Select option 5, *UTILITY*, as shown in the following image, and press Enter.

```
HCR77D0  -------------- Integrated Cryptographic Service Facility --
OPTION ===> _
System Name:  IBI1                                Crypto Domain: 0
Enter the number of the desired option.

  1  COPROCESSOR MGMT -  Management of Cryptographic Coprocessors
  2  KDS MANAGEMENT   -  Master key set or change, KDS Processing
  3  OPSTAT           -  Installation options
  4  ADMINCNTL        -  Administrative Control Functions
  5  UTILITY          -  ICSF Utilities
  6  PPINIT           -  Pass Phrase Master Key/KDS Initialization
  7  TKE              -  TKE PKA Direct Key Load
  8  KGUP             -  Key Generator Utility processes
  9  UDX MGMT         -  Management of User Defined Extensions
```

2. Select option 5, *CKDS KEYS*, as shown in the following image, and press Enter.

```
------------------------------- ICSF - Utilities --------------------
OPTION ===> _

Enter the number of the desired option.

  1  ENCODE        -  Encode data
  2  DECODE        -  Decode data
  3  RANDOM        -  Generate a random number
  4  CHECKSUM      -  Generate a checksum and verification patterns
  5  CKDS KEYS     -  Manage keys in the CKDS
  6  PKDS KEYS     -  Manage keys in the PKDS
```

3. Select option 7, *Generate AES DATA keys*, as shown in the following image, and press Enter.

```
------------------------------- ICSF - CKDS KEYS ----------------------------
OPTION ===> 7_

Active CKDS: IBI1.CSF.SCSFCKDS                                  Keys: 4

Enter the number of the desired option.
  1  List and manage all records
  2  List and manage records with label key type __________   leave blank for
                                                              list, see help
  3  List and manage records that are __________  (ACTIVE, INACTIVE, ARCHIVED)
  4  List and manage records that contain unsupported CCA keys
  5  Display the key attributes and record metadata for a record
  6  Delete a record
  7  Generate AES DATA keys

Full or partial record label
  ==> ____________________________________________________________________
  The label may contain up to seven wild cards (*)

Number of labels to display ==> 100  (Maximum 100)

Press ENTER to go to the selected option.
Press END   to exit to the previous menu.
```

4. Type the CKDS record label for the new key and select the AES key bit length, as shown in the following image, and press Enter.

```
---------------------------- ICSF - CKDS Generate Key ------
COMMAND ===>

Active CKDS: IBI1.CSF.SCSFCKDS

Enter the CKDS record label for the new AES DATA key
==> DATASET.PGMYMG.ENCRYPTKEY.001

AES key bit length:   _ 128   _ 192   s 256
```

If the operation was successful, Key Generated is returned at the upper-right corner of the screen, as shown in the following image.

```
- ICSF - CKDS Generate Key ----------- KEY GENERATED
```

Db2 Security Exit Configuration for PDS

Customize the Db2 security exit to allow the Adapter for Db2 to run with user-level security enabled. If you do so, users will connect to Db2 with the authorization of the user ID with which they logged on to the server. The server must also be running with security turned on.

If you do not customize the Db2 security exit, all users will be assigned the connection ID to Db2 that is associated with the region, job submitter, or started task.

For the Adapter for Db2 CLI, the connection to Db2 must be configured as *trusted* for the exit to be invoked.

The changes that must be made to the IBM Db2 sign-on exit, DSN3SATH, differ for RACF and *e*Trust CA-Top Secret sites and *e*Trust CA-ACF2 sites.

An example of each is shown in the following sections.

The highlighted text and comments shown in the examples indicate the lines containing the recommended modification of DSN3SATH, which calls the module FOCDSN3, the supplied exit.

After you finish the edits, assemble the exit into an object file. This object file is input to the link JCL found in one of the examples that follow.

Note:

- The positioning of these lines is approximate, assuming that no other changes or additions have already been made to DSN3SATH. If any changes have been made, you should decide on the most appropriate location for this call to FOCDSN3.

- FOCDSN3 is used to set the proper primary (individual user ID) authorization.
- Another program, FOCDSN4, is used to set the proper secondary (group ID) authorization for RACF and *e*Trust CA-Top Secret. FOCDSN4 is not needed with *e*Trust CA-ACF2. The secondary authorization ID(s) will be set correctly without it.

Example: Changing DSN3SATH for RACF and *e*Trust CA-Top Secret Sites

1. Search for the SATH001 label - add two lines (FOCDSN3):

```
SATH001  DS    0H
         USING WORKAREA,R11        ESTABLISH DATA AREA ADDRESSABILITY
         ST    R2,FREMFLAG                SAVE FREEMAIN INDICATOR
         XC    SAVEAREA(72),SAVEAREA CLEAR REGISTER SAVE AREA
         .
         .
         .
*********SECTION 1:  DETERMINE THE PRIMARY AUTHORIZATION ID  ************
*                                                                       *
*  IF THE INPUT AUTHID IS NULL OR BLANKS, CHANGE IT TO THE AUTHID       *
*  IN EITHER THE JCT OR THE FIELD POINTED TO BY ASCBJBNS.               *
*  THE CODE IN THIS SECTION IS AN ASSEMBLER LANGUAGE VERSION OF         *
*  THE DEFAULT IDENTIFY AUTHORIZATION EXIT.  IT IS EXECUTED ONLY        *
*  IF THE FIELD ASXBUSER IS NULL UPON RETURN FROM THE RACROUTE          *
*  SERVICE.  FOR EXAMPLE, IT DETERMINES THE PRIMARY AUTH ID FOR         *
*  ENVIRONMENTS WITH NO SECURITY SYSTEM INSTALLED AND ACTIVE.           *
*                                                                       *
************************************************************************
SPACE
    LA    R1,AIDLPRIM         LOAD PARM REG1            <--ADD
    CALL  FOCDSN3             GO GET THE IBI EXIT       <--ADD
    CLI   AIDLPRIM,BLANK      IS THE INPUT PRIMARY AUTHID NULL
    BH    SATH020             SKIP IF A PRIMARY AUTH ID EXISTS
```

2. Search for the SATH020 label - add a comment box, add one line, and comment out four lines:

```
SATH020  DS    0H                  BRANCH TO HERE IF PRIMARY EXISTS
*****OPTIONAL CHANGE @CHAR7:  FALLBACK TO SEVEN CHAR PRIMARY AUTHID***
*                                                                    *
*  IF YOUR INSTALLATION REQUIRES ONLY SEVEN CHARACTER PRIMARY        *
*  AUTHORIZATION IDS (POSSIBLY TRUNCATED) DUE TO DB2 PRIVILEGES      *
*  GRANTED TO TRUNCATED AUTHORIZATION IDS, THEN YOU MUST BLANK OUT   *
*  COLUMN 1 OF THE ASSEMBLER STATEMENT IMMEDIATELY FOLLOWING THIS    *
*  BLOCK COMMENT. THEN ASSEMBLE THIS PROGRAM AND LINK-EDIT IT INTO   *
*  THE APPROPRIATE DB2 LOAD LIBRARY AS EXPLAINED IN AN APPENDIX      *
*  OF "THE DB2 ADMINISTRATION GUIDE".                                *
*                                                                    *
*  OTHERWISE, YOU NEED DO NOTHING.                                   *
*                                                            @KYD0271*
**********************************************************************
*      MVI   AIDLPRIM+7,BLANK    BLANK OUT EIGHTH CHARACTER
       SPACE
       .
       .
       .
*   RACF IS ACTIVE ON THIS MVS
********************************************************************* <--ADD
*                                                                   * <--ADD
* The logic was modified because in DB2 V8 AIDLACEE is always not* <--ADD
* NULL. We used to honor AIDLACEE first, FOCDSN4 second and then * <--ADD
* AS ACEE. Now we honor FOCDSN4 first, AIDLACEE second and then  * <--ADD
* AS ACEE.                                                          * <--ADD
*                                                                   * <--ADD
* 03/11/05   ASK0                                                   * <--ADD
********************************************************************* <--ADD
  USING ACEE,R6             ESTABLISH BASE FOR ACEE        @KYL0108
  L     R6,AIDLACEE         Get => caller ACEE if any              <--ADD
* ICM   R6,B'1111',AIDLACEE CALLER PASSED ACEE ADDRESS? @KYL0108  <-COMMENT
* BZ    SATH024             NO, USE ADDRESS SPACE ACEE  @KYL0108 <-COMMENT
* CLC   ACEEACEE,EYEACEE    IS IT REALLY AN ACEE?       @KYL0108  <-COMMENT
* BE    SATH027             YES, PROCEED NORMALLY       @KYL0108  <-COMMENT
      SPACE 1
SATH024  DS    0H                  USE ADDRESS SPACE ACEE      @KYL0108
    .
    .
    .
```

3. Search for the SATH025 label - replace sath025 and add sath026 (FOCDSN4):

```
SATH025  DS    0H

    CALL  FOCDSN4              GO GET THE IBI EXIT (4=GROUP AUTH) <--ADD
    LTR   R6,R6                DOES AN ACEE EXIST?  IF NOT,       <--ADD
    BZ    SATH026              CHECK ACEE IN ADDRESS SPACE        <--ADD
    CLC   ACEEACEE,EYEACEE     DOES IT LOOK LIKE AN ACEE?         <--ADD
    BE    SATH027              YES, GO DO GROUPS                  <--ADD
SATH026  DS    0H                                                 <--ADD
     .
     .
     .

SATH027  DS    0H             CHECK LIST OF GROUPS OPTION
   TM     RCVTOPTX,RCVTLGRP   IS LIST OF GROUPS CHECKING ACTIVE
   BZ     SATH040             SKIP TO SINGLE GROUP COPY IF NOT
   DROP   R7                  DROP RCVT BASE REG
   SPACE 1
* RACF LIST OF GROUPS OPTION IS ACTIVE
   EJECT
    .
    .
    .
```

Example: Changing DSN3SATH for *e*Trust CA-ACF2 Sites

*DSN3SATH source is provided by ACF2.

1. Search for PRIMARY AUTHORIZATION ID - add two lines (FOCDSN3):

```
*****************************************************************
*                                                               *
*           PRIMARY AUTHORIZATION ID                            *
*                                                               *
*****************************************************************
*                                                               *
*      IF THE PRIMARY AUTHORIZATION ID IS NULL OR BLANKS        *
*      IF CA-ACF2 IS AVAILABLE                                  *
*      SET PRIMARY ID FROM ACFASVT (ASVLID)                     *
*      ELSE                                                     *
*      IF TSO FOREGROUND USER                                   *
*      SET PRIMARY ID FROM TSO LOGON ID (ASCBJBNS)              *
*      ELSE                                                     *
*      SET PRIMARY ID FROM JOB USER (JCTUSER)                   *
*                                                               *
*****************************************************************
      SPACE 2                                                   04260000
      LA R1,AIDLPRIM LOAD PARM REG1                <--ADD
      CALL FOCDSN3 GO GET THE IBI EXIT             <--ADD
       CLI   AIDLPRIM,C' '      PRIMARY AUTHID THERE ?         04270000
       BH    PRIMWTO            ..YES, EVERYTHINGS OK HERE     04280000
       L     R3,PSAAOLD-PSA(0)  CURRENT ASCB ADDRESS           04290000
       USING ASCB,R3            ASCB ADDRESSABILITY            04300000
       SPACE 2                                                  04310000
```

Example: Modifying the Link JCL for DSN3SATH

This is a sample link JCL for the IBM exit DSN3SATH. Modify the JCL to link the modules into the Db2 security exit as follows.

```
//LKED  EXEC PGM=IEWL,PARM='LIST,XREF,LET,RENT,AMODE=31'
//OBJECT    DD DSN=db2pref.SDSNSAMP.OBJ,DISP=SHR <--OUTPUT OF ASSEMBLE
STEP
//EDAMOD    DD DSN=high_level_qualifier.HOME.LOAD,DISP=SHR
//SYSLMOD   DD DSN=db2pref.DSNEXIT,DISP=SHR
//SYSPRINT  DD SYSOUT=*
//SYSUT1    DD UNIT=SYSDA,SPACE=(100,(50,50))
//SYSLIN    DD *
  INCLUDE EDAMOD(FOCDSN3)
*********************************************************************
*** Omit the following line for eTrust CA-ACF2
*********************************************************************
  INCLUDE EDAMOD(FOCDSN4)
          ENTRY DSN3@ATH
  NAME DSN3@ATH(R)
/*
```

where:

db2pref

Is the prefix for the Db2 data sets.

high_level_qualifier

Is the high-level qualifier for the data sets.

Once this job finishes successfully, you must recycle the Db2 subsystem in order for the changes to take effect.

MSODDX: DDNAME Translation for User Subroutines

On z/OS, you can incorporate an additional routine called MSODDX into a user-written subroutine that needs to access ddnames allocated to a Reporting Server. MSODDX provides ddname translation services that enable external programs to access files under the ddname used by the Reporting Server.

For details, see the *Stored Procedures* chapter in the *TIBCO WebFOCUS® Reporting Server Administration* manual.

Overriding the Time Zone Setting

By default, the server will use the system set value for Time Zone. This can be overridden by setting the TZ in the EDAENV member of the server configuration library.

```
TZ = valid tz string
```

For more information about time zone values, see the *IBM UNIX System Services Command Reference* and search for TZ.

Adding a Configuration Instance for PDS

Adding a configuration instance allows you to run different server configuration instances using the same server binaries. You can add up to nine additional servers.

Step 1. Run ISETUP

To add a configuration instance, perform the following steps.

1. Execute ISETUP again. You should have a *high_level_qualifier*.HOME.DATA PDS. Use option 6 in ISPF to execute the ISETUP member of this PDS.

   Note: If this PDS is not available, run an IEBCOPY job to allocate and unload it from the installation tape.

The first Installation and Configuration panel opens.

```
TIBCO                    Installation and Configuration   Unified Server Install
Command ===>                                                                   P0

Unified Server Installation
Please select one of the following options:

         1. USS/ZFS Deployment

            . Installation files and temporary files in ZFS
            . Application files, like synonyms and procedures, in ZFS (or
              optionally in both ZFS and PDS)

         2. PDS Deployment

            . Installation files and temporary files in PDS
            . Application files, like synonyms and procedures, in PDS (or
              optionally in both PDS and ZFS)



Enter selection (Default=1) ===> 1

Press Enter to continue, PF3 to END                            Version: 9999
```

2. Type *2* and press Enter to continue to the next panel.

   The following panel opens.

```
TIBCO                      Installation and Configuration        z/OS PDS Deploy
Command ===>                                                                  D1

Please select one of the following options:


         1. Install and Configure
         2. Add Additional Configuration Instance
         3. Refresh Installation (Reinstall, Keep Configurations)


Enter selection (Default=1) ===> 1
Input source                ===> D                      (T)ape or (D)isk
Installation Userid         ===> IADMIN                 Logged on Userid
PTH Administrator Userid    ===> srvadmin               Server install only
PTH Administrator Password  ===> _                      Retype  ===>


Enter Job Card information                Override JOB name checking ===> N
===> // JOB (ACCT INFO),
===> //*
===> //*
Press Enter to continue, PF3 to END
```

3. Complete the first Installation and Configuration panel, as follows.

Field	Instructions
Enter selection	Choose option 2, *Add Additional Configuration Instance*.

Field	Instructions
Input source	This is ignored for option 2, adding a configuration instance.
Installation Userid	Shows the current logon ID. It cannot be changed.
PTH Administrator Userid	An ID is required to administer the server immediately after initial installation. This ID is defined and maintained solely in the realm of the server. It defaults to *srvadmin*, and it can be changed here. For more information about running the server in secure mode, see *Step 6. Configure Security* on page 201.
PTH Administrator Password	Password for the PTH Administrator ID. It cannot be left blank and must be matched at Retype field.
Enter Job Card information	To provide JOB card information for submitting jobs to the JES queue, provide a valid job name (a maximum of seven characters following the // on the first JCL line), which defaults to the user ID that you are currently using. This job name is used for multiple submissions (for example, *jobname*A, *jobname*B, *jobname*C, and so on) in the JCL generated by the installation procedure.
Override JOB name checking	To provide your own JOB card information, including JOB name, enter *Y* and provide valid JOB card information in the *Enter Job Card information* field. The JOB card information that you enter will be used for each job that is submitted.

4. Press Enter to continue to the next panel.

   The following panel opens.

```
TIBCO                    Installation and Configuration        z/OS PDS Deploy
Command ===>                                                              DG
                                Add Configuration

Please enter the following information for WebFocus Reporting Server

 Product Configuration Parameters

  Current base HLQ (EDAHOME)       ===> IADMIN.SRV82_



Press Enter to continue, PF3 to return to previous menu
```

5. Enter the current base high-level qualifier used for EDAHOME.

   This indicates where to install the configuration (EDACONF) and where the binaries (EDAHOME) are installed. The installation procedure checks whether the required set of EDAHOME data sets exist. If the test fails, you receive a message indicating the failure and available options.

6. Press Enter to continue to the next panel.

```
TIBCO                    Installation and Configuration        z/OS PDS Deploy
Command ===>                                                              DI
                       Add additional Configurations

Please enter the following information for WebFocus Reporting Server

 Using the following existing information
  Current base HLQ            ===> IADMIN.SRV82
  Base Install Library        ===> IADMIN.SRV82.PDS.WFS.DATA

  Current configurations      ===> WFS


 Configuration Options (blank any field for default)

  Approot value               ===> PLEASE SUPPLY VALUE                    _
  EDACONF suffix ( WFS plus)  ===> 1          or string suffix   ===>
 (EDACONF)                 Unit===> SYSDA     Type ===>          ===>
  HTTP Listener Port          ===> 8121      TCP Listener Port  ===> 8120

  Installation JCL Library    ===> IADMIN.SRV82.PDS.WFS1.DATA

Press Enter to continue, PF3 to return to previous menu
```

7. Complete the configuration parameters on the panel as follows.

Field	Instructions
Approot value	Indicates where application components reside for this configuration. The default value is based on the value specified for *Current Base HLQ (EDAHOME)* on the previous panel. To specify a different location for application components, change the value of this field. Different configurations which use the same base HLQ (high-level qualifier) libraries (EDAHOME) can share the same approot value (that is, the same application files). They can also use different approot values to have different sets of application files. If you specify the approot value of an existing server configuration, the installation process recreates the server supplementary data sets and sample files (see *Disk Space Requirements* on page 181). If you do not want them to be recreated, provide a different value for approot.

Field	Instructions
EDACONF suffix	Each instance must have its own set of configuration libraries. To guarantee this, and to prevent a new set of configuration libraries from overwriting an existing set, the specified suffix is appended to the name of the WFS qualifier. For example, if you configure the second instance of a WebFOCUS Reporting Server, you can specify a suffix of "1", to make the EDACONF high-level qualifier: `IADMIN.SRV.PDS.WFS1.DATA` You can add the new configuration as a numeric or string suffix to the base product type. If you supply a string, the installation procedure ignores any numeric suffix. For a: ❑ **Numeric suffix.** Enter a digit between 1 and 9. This suffix is added to the product type in the directory name and library name to distinguish it from other configuration instances. ❑ **String suffix.** Enter a one to five-character string (for example, TEST, PROD, or DEV) that does not contain embedded spaces. You can also use the string suffix to extend the numeric numbering past 9 by supplying a number greater than 9. If you change the suffix value and press Enter, the panel refreshes with a new value for the EDACONF Library.

Field	Instructions
HTTP Listener Port	This indicates the port number that the server will use for HTTP. It is the first of three connection ports that must be available to the server. For example, if you choose port 8101, then ports 8101, 8102, and 8103 are used by the server. Ensure that you choose ports that are not currently being used.
TCP Listener Port	This is the port number of the TCP Listener. The default is one less than the port specified for the HTTP Listener, but it can be any port number other than the three reserved for HTTP.

8. Press Enter to continue to the next panel.

   The Data Adapter panel may open before the confirmation panel. If the Data Adapter panel opens, continue with Step 9; otherwise, skip to Step 10.

9. The Data Adapter panel lists adapters that require the allocation of libraries in IRUNJCL or environment variables in the EDAENV member. To select specific adapters:

   a. Type *Y* next to the required adapters and press Enter.

   b. Supply the requested information, which is described in *Step 2. Collect Required Information for Adapters* on page 185.

      After you have finished installing and configuring the server, you can use the Reporting Server browser interface to finish configuring these adapters, and to configure adapters that do not have JCL requirements.

10. Press Enter to continue to the next panel.

    The JSCOM3 Listener configuration panel opens.

    a. The panel will prompt for the path to the Java environment to be passed to either JDK_HOME or JAVA_HOME, as described in *JVM Requirements for Java Services* on page 179, and it will also prompt for edahome_dir and edaconf_dir, as described in *ZFS Home and Configuration Directory Requirements* on page 184.

    b. Configuration of the JSCOM3 Listener is either optional or mandatory depending on which adapters were selected. If any Java-based adapters were selected (EJB, Call Java, JDBC, Microsoft SQL Server), the configuration of all three paths listed above is mandatory. If SAP-based adapters were selected (SAP or SAP BW), only edahome_dir and edaconf_dir are required.

    c. If no Java-based or SAP-based adapters were selected, this configuration might still be desirable to enable the server-side graphics feature. To skip the configuration, leave the path blank.

11. Press Enter to continue to the next panel.

    The confirmation panel opens.

12. Ensure that all values on the Confirmation panel are correct, then select one of the following options:

    - **N** to return to the initial panel so that you can change installation values.
    - **C** to create JCL which you can submit at a later time. The JCL is placed in your configuration library.
    - **S** to create JCL and submit the job immediately.

13. As the job is processed, validate the installation as described in *Step 2. Test the New Configuration Instance* on page 220.

Step 2. Test the New Configuration Instance

To test the configuration instance that you just added:

1. Log on to TSO as iadmin.
2. Submit the ISTART JCL from the configuration library to start the server. This executes the IRUNJCL proc. The configuration library is

   `high_level_qualifier.PDS.WFS[suffix].DATA`

   where:

   high_level_qualifier

   Is the high-level qualifier to be used for all output libraries. You specified the high-level qualifier during server installation, as described in *Step 4. Run ISETUP* on page 193, in Step 6.

   suffix

   If you are testing an additional instance, the new configuration library product type qualifier will have a suffix (for example, WFS*1* or WFS*DEV*). The suffix distinguishes the new configuration library from the original one.

3. Check the job output for errors. Look for the EDAPRINT message:

   ```
   (EDA13023) ALL INITIAL SERVERS STARTED
   ```

4. Start the Reporting Server browser interface by opening a browser pointed at the listener port of the server. The URL format is

   `http://host:port`

where:

host

Is the name of the machine on which the server is installed.

port

Is one port higher than the port specified when installing the server. For example, if you specified port 8100 during installation, then use port 8101 to access the Reporting Server browser interface.

The Reporting Server browser interface opens.

5. If the Reporting Server browser interface opens and displays application tree folders in the left pane, the server is working because it uses its own underlying data access and reporting technologies to visualize the application tree.
6. Continue with adapter configuration, as described in the *TIBCO WebFOCUS® Adapter Administration* manual.

Upgrading Your TIBCO WebFOCUS Reporting Server Release for PDS

Use this option to upgrade to a new maintenance level within the same major release or, starting with major release 77, upgrade to a higher major release level. A major release is indicated by the first two digits of the release number.

You can replace the libraries with the new set of downloaded files, after making a backup copy of the existing installation.

The purpose of the PDS refresh option is to create a new set of EDAHOME libraries. It is recommended that you test the new libraries in a test environment before manually changing your production JCL (IRUNJCL) to point to the new software. The upgrade process can overwrite an existing set of EDAHOME libraries (not recommended) if both "Current Base HLQ" and "HLQ for downloaded files" or "Output Libraries HLQ" are the same value.

Step 3. Test the Installation

To test the installation:

1. Log on to TSO as iadmin.
2. Using a test server, replace all the EDAHOME libraries referenced in IRUNJCL with the new set.
3. Submit the ISTART JCL to start the server.
4. Check the job output for errors. Look for the EDAPRINT message:

   ```
   (EDA13023) ALL INITIAL SERVERS STARTED
   ```

5. Start the Reporting Server browser interface by opening a browser pointed at the listener port of the server. The URL format is

   `http://host:port`

   where:

   host

   Is the name of the machine on which the server is installed.

   port

   Is one port higher than the port specified when installing the server. For example, if you specified port 8100 during installation, then use port 8101 to access the Reporting Server browser interface.

   The Reporting Server browser interface opens.

6. If the Reporting Server browser interface opens and displays application tree folders in the left pane, the server is working because it uses its own underlying data access and reporting technologies to visualize the application tree.

When you are finished using the server, you can use the Reporting Server browser interface to stop the server by going to the Reporting Server browser interface menu bar, selecting *Workspace*, and then *Stop*.

If you experience problems at start-up, examine the job output for more information.

Step 4. Reconfigure Security

For information about configuring server security, see *Step 6. Configure Security* on page 201.

To reconfigure server security to OPSYS provider only:

1. Log on to TSO.
2. The libraries allocated to STEPLIB in IRUNJCL must be APF-authorized. Any non APF-authorized libraries must be allocated the TASKLIB DDNAME.
3. Test server security by repeating the process described in *Step 3. Test the Installation* on page 221.

Preventing Unsecured Starts After Upgrades

If the security provider is set to OPSYS in the configuration file and, additionally, explicit environment variable EDAEXTSEC is set to OPSYS (or ON), and the server cannot impersonate users because it lacks platform-specific authorization steps, the server start aborts and error messages are written to the edaprint log.

This feature prevents an unsecured server start after a software upgrade if any of the required post-upgrade reauthorization steps are missed on a UNIX, IBM i, or z/OS USS deployment. This is not applicable to other platforms. The setting may be placed in any normal server start-up shell or profile that a site is using or in the server edaenv.cfg configuration file. The messages vary slightly by platform.

The edaprint messages are:

```
I Configured primary security is 'OPSYS' as set in configuration file

E Server security explicitly set to OPSYS, but lacks authority!

Workspace initialization aborted.

(EDA13171) UNABLE TO START SERVER
```

Step 5. Reconfigure Adapters

While most adapters do not require additional steps after updating binary files, the following table notes the adapters that do require some consideration.

Adapter	Steps After Updating Binaries
Adabas	❑ Change the value for EDALOAD in member EDAENV of your current server configuration library (*qualif*.PDS.WFS.DATA) to point to the new P.HOME.LOAD. ❑ Re-enable the module containing SVC using the Reporting Server browser interface adapter configuration page. ❑ Test the adapter from the adapter page before running your applications.
Db2 CAF	❑ Rerun the IDB2BIND JCL found in your current server configuration library WFS.PDS.WFS.DATA. This needs to be done for each subsystem that is used. ❑ Test the adapter from the adapter page before running your applications.

Accounting for PDS - SMF Records

The server provides an optional facility to use for accounting purposes that enables you to log resource utilization on a per-user basis. This facility enables the server to generate SMF records for query-level and user-level accounting.

Server accounting requires that the server STEPLIB data sets be APF-authorized. When SMF records are generated, they contain:

- The logon ID and security ID of the user.
- The CPU time and EXCPs consumed.
- Data based on the type of record written.

You can process the SMF records using the accounting programs that exist at your site. Examples of SMF records are provided in *SMF Record Format for RECTYPES 1 and 4* on page 226.

In order to write SMF records, the server must be running APF authorized.

Two sample Master Files (SMFVSAM and SMFFIX) are provided for accessing accounting statistics. They reside in qualif.P.HOME.MAS.

Their difference is that SMFVSAM can be used to report directly from the system-live SYS1.MANx records, while SMFFIX can be used to report from a sequential file produced from running the SMFDUMP utility. These Master Files enable you to interpret the SMF records generated by the accounting facility using reporting requests or store procedures. Both Master Files are for logoff records only, as indicated by ALIAS=2 on the RECTYPE field entry.

A sample procedure report to query the SMF data is also provided in qualif.P.HOME.FEX(SMFMAN1).

Syntax:

How to Enable Accounting

To enable accounting, insert the following statement into the server configuration file (edaserve.cfg):

`smf_recno=`*`smfnumber`*

where:

`smfnumber`

Is an integer in a range from 128 to 255, inclusive. This number represents the SMF number used by the accounting facility when it sends records to the SMF system.

By default, both RECTYPE pairs will be created when accounting is enabled. You can override the default by coding the following parameter on edaserve.cfg:

```
smf_subtype = {all|logon|query}
```

where:

`all`

Cuts all records. This is the default.

`logon`

Cuts logon records only (RECTYPE pair 1 and 2).

`query`

Cuts query records only (RECTYPE pair 4 and 5).

Syntax: **How to Set the Accounting Field**

Up to 40 characters can be supplied that appear in the SMF records field SMFOFA40. The SET BILLCODE command can be used in any support server profile to provide the account field information. The syntax is

```
SET BILLCODE=value
```

where:

value

Is the 1–40 characters to be used on each SMF record produced.

This information can also be set dynamically from a client application by coding an RPC with the SET command and executing it with the value as a parameter. WebFOCUS users can send the SET command to the server.

Procedure: **How to Report From SMF Data**

To report from SMF data, execute the sample procedure *smfman1.fex*, provided under home/catalog (DDNAME EDAHFEX for a PDS Deployment server).

You will be prompted for the DSN of the SMF VSAM data set from which you want to report, and the *smf_recno* value used to produce the SMF records.

The following is a listing of smfman1.fex:

```
DYNAM ALLOC FI SMFVSAM DSN &SMFDSN.Please provide SMF VSAM DSN. SHR REU
DEFINE FILE SMFVSAM
CPU/D8.2 = SMFOFCPU / 100 ;
USER/A20 = SMFOFUID ;
EXCPS/I6 = SMFOFEXC ;
TIME/D9.2 = SMFOFLTM / 100 ;
HR/I2 = SMFOFTME / 360000 ;
MIN/I2 = (SMFOFTME  - (HR*360000)) / 6000 ;
TOD/A5 = EDIT(HR) | ':' | EDIT(MIN) ;
END
TABLE FILE SMFVSAM
PRINT USER CPU EXCPS TIME TOD
WHERE SMFOFRTY EQ &SMFNUM.Please provide SMF number(type) for report.
END
```

Reference: SMF RECTYPES

There are four RECTYPE values defined to produce SMF records:

RECTYPE	Description
1	Indicates a start of task record. When included in a report, these statistics tell when a task initiation occurred, and are of no particular use in chargeback. By pairing start and end of task records for all tasks within a time period, statistics, such as average active time, peak task count, and average task count, can be determined. These values can be used for future capacity planning activities for the server.
2	Indicates the start of a task record. When included in a report, these statistics tell when a task termination occurred. These records are cut for both publicly and privately deployed services and contain statistics for the subtask as a whole. For privately deployed services, RECTYPE (2) records contain statistics associated with a single user connection.
4	Begin query. Record layout is the same as RECTYPE (1).
5	End query. Record layout is the same as RECTYPE (2).

Reference: SMF Record Format for RECTYPES 1 and 4

The record format for RECTYPES 1 and 4 of the SMF records written by the server is defined below. The format is provided in the system 390 assembler DSECT form.

```
SMFON    DSECT
         SPACE
*-----------------------------------------------------*
*  USAGE ACCOUNTING SMF RECORD LAYOUT FOR LOGON RECORDS.              *
*                                                                     *
*  THIS IS THE DSECT DESCRIBING THE SMF RECORD WHICH IS PASSED TO     *
*  YOUR EXIT ON AT USER LOGON TIME.  IT IS COMPLETELY READY TO BE     *
*  WRITTEN WHEN YOUR EXIT RECEIVES CONTROL.                           *
*-----------------------------------------------------*
         SPACE


*-----------------------------------------------------*
*  THE FIRST TWENTY FOUR BYTES OF THE RECORD ARE THE SMF HEADER.      *
*  THESE FIELDS ARE REQUIRED IN ALL SMF RECORDS (18 BYTES FOR RECORDS *
*  WITHOUT SUBTYPES; WE USE SUBTYPES, THE HEADER IS 24 BYTES).        *
         SPACE
SMFONLEN DS    H'116'            RECORD LENGTH
SMFONSEG DS    XL2'0000'         SEGMENT DESCRIPTOR (0 UNLESS SPANNED)
SMFONFLG DS    XL1               SYSTEM INDICATOR
SMFONRTY DS    XL1               RECORD TYPE
SMFONTME DS    XL4               TIME, IN HUNDREDTHS OF A SECOND
SMFONDTE DS    PL4               DATE, 00CYYDDDF, WHERE F IS THE SIGN
SMFONSID DS    CL4               SYSTEM IDENTIFICATION
SMFONSBS DS    CL4               SUBSYSTEM IDENTIFICATION
SMFONSBT DS    XL2'0001'         SUBTYPE OF RECORD - X'0001' INDICATES X
                                 THIS IS A LOGON RECORD
         SPACE


*-----------------------------------------------------*
*  THE NEXT FIELDS ARE THOSE PRESENT IN THE LOGON                     *
*  RECORD FOR THE START OF A USER SESSION.                            *
*-----------------------------------------------------*
         SPACE
SMFONMSO DS    CL8               JOBNAME
SMFONJID DS    CL8               JOBID (FROM SSIBJBID)
SMFONASI DS    Y                 ASID
SMFONRV1 DS    XL2               RESERVED
SMFONUID DS    CL20              SECURITY USERID
SMFONLID DS    CL20              USERID PRESENTED AT LOGON (SAME AS    X
                                 SMFONSID UNLESS CHANGED VIA MSIDTR    X
                                 SECURITY EXIT)
SMFONRSV DS    XL8               RESERVED FOR FUTURE EXPANSION
SMFONCTI DS    XL4               RESERVED FOR FUTURE EXPANSION
SMFONSRV DS    CL8               SERVICE NAME FROM SERVICE BLOCK
SMFONRS0 DS    XL4               RESERVED FOR FUTURE EXPANSION
SMFONCNT DS    XL1               CONNECTION TYPE
         SPACE


SMFONTSO EQU   1                 CONNECTION VIA TSO
SMFONCIC EQU   2                 CONNECTION VIA CICS
SMFONVTM EQU   4                 CONNECTION VIA VTAM
SMFONPSR EQU   8
         SPACE
```

```
SMFONRS1 DS    XL3               RESERVED
SMFONID1 DS    F                 SYSPLEX ID 1
SMFONID2 DS    F                 SYSPLEX ID 2
SMFOFPID DS    XL20              POOLED USER ID
SMFONRS2 DS    XL12              RESERVED
SMFONL   EQU   *-SMFON           LENGTH OF THE SMF LOGON RECORD
```

Reference: SMF Record Format for RECTYPES 2 and 5

The record format for RECTYPES 2 and 5 of the SMF records written by the server is defined below. The format is provided in the system 390 assembler DSECT form.

```
SMFOF    DSECT
         SPACE
*-----------------------------------------------------*
*  USAGE ACCOUNTING SMF RECORD LAYOUT FOR LOGOFF RECORDS.             *
*                                                                     *
*  THIS IS THE DSECT DESCRIBING THE SMF RECORD WHICH IS PASSED TO     *
*  YOUR EXIT ON AT USER LOGOFF TIME.  IT IS COMPLETELY READY TO BE    *
*  WRITTEN WHEN YOUR EXIT RECEIVES CONTROL.                           *
*-----------------------------------------------------*
         SPACE

*-----------------------------------------------------*
*  THE FIRST TWENTY FOUR BYTES OF THE RECORD ARE THE SMF HEADER.      *
*  THESE FIELDS ARE REQUIRED IN ALL SMF RECORDS (18 BYTES FOR RECORDS *
*  WITHOUT SUBTYPES; WE USE SUBTYPES, THE HEADER IS 24 BYTES).        *
*-----------------------------------------------------*
         SPACE
SMFOFLEN DS    H'168'            RECORD LENGTH
SMFOFSEG DS    XL2'0000'         SEGMENT DESCRIPTOR (0 UNLESS SPANNED)
SMFOFFLG DS    XL1               SYSTEM INDICATOR
SMFOFRTY DS    XL1               RECORD TYPE
SMFOFTME DS    XL4               TIME, IN HUNDREDTHS OF A SECOND
SMFOFDTE DS    PL4               DATE, 00CYDDDF, WHERE F IS THE SIGN
SMFOFSID DS    CL4               SYSTEM IDENTIFICATION
SMFOFSBS DS    CL4               SUBSYSTEM IDENTIFICATION
SMFOFSBT DS    XL2'0002'         SUBTYPE OF RECORD - X'0002' INDICATES X
                                 THIS IS A LOGOFF RECORD
         SPACE
```

```
*-----------------------------------------------------*
*  THE NEXT FIELDS ARE THOSE PRESENT IN THE LOGOFF                    *
*  RECORD FOR THE END OF A USER SESSION.                              *
*-----------------------------------------------------*
         SPACE
SMFOFMSO DS    CL8              JOBNAME
SMFOFJID DS    CL8              JOBID (FROM SSIBJBID)
SMFOFASI DS    Y                ASID
SMFOFRV1 DS    XL2              RESERVED
SMFOFUID DS    CL20             SECURITY USERID
SMFOFLID DS    CL20             USERID PRESENTED AT LOGON (SAME AS    X
                                SMFOFSID UNLESS CHANGED VIA MSIDTR    X
                                SECURITY EXIT)
SMFMEMA  DS    XL4              MEMORY ABOVE THE LINE (IN KILOBYTES)
SMFMEMB  DS    XL4              MEMORY BELOW THE LINE (IN KILOBYTES)
SMFZIIP  DS    XL4              ZIIP CPU NORMALIZED (HUNDREDTHS OF A SEC)
SMFOFSRV DS    CL8              SERVICE NAME FROM THE SERVICE BLOCK
SMFZPOCP DS    XL4              ZIIP ON CP (HUNDREDTHS OF A SEC)
SMFOFCNT DS    XL1              CONNECTION TYPE
         SPACE

SMFOFTSO EQU   1                 CONNECTION VIA TSO
SMFOFCIC EQU   2                 CONNECTION VIA CICS
SMFOFVTM EQU   4                 CONNECTION VIA VTAM
SMFOFPSR EQU   8
SMFOFCC  DS    XL3               COMPLETION CODE FOR THE TASK
SMFOFACT DS    CL8               USER ACCOUNTING INFORMATION; THIS     X
                                 FIELD CURRENTLY PASSED AS LOW VALUE
SMFOFCPU DS    XL4               CPU TIME IN HUNDREDTHS OF A SECOND
SMFOFEXC DS    XL4               COUNT OF EXCP'S
SMFOFLTM DS    FL4               LOGON DURATION IN HUNDREDTHS OF A     X
                                 SECOND
SMFPRTY  DS    XL1               PRIORITY
SMFCOMPL DS    XL1               COMPLETION TYPE
         DS    XL2               RESERVED
SMFOFID1 DS    F                 SYSPLEX ID 1
SMFOFID2 DS    F                 SYSPLEX ID 2
SMFOPID  DS    XL20              POOLED USERID
SMFOFA40 DS    CL40              FULL 40-BYTE ACCOUNTING FIELD
         SPACE
SMFOFL   EQU   *-SMFOF           LENGTH OF THE SMF LOGOFF RECORD
```

Reference: Accounting for Db2 in a Reporting Server Task

When using a server to access Db2 data, certain processing takes place within the Db2 address space and is governed by the Db2 chargeback system. If a user requests data from Db2, the server passes the request to the Db2 subsystem. The Db2 subsystem then processes the request, performing such tasks as retrieving rows and aggregating the data. It generates the answer set, and passes the output back to the server. The server then performs any joins and formatting which have not been performed by Db2 to satisfy the original request.

Charges incurred while the request was being processed by the Db2 subsystem are added to the charges accumulated in the server task that originated the request for processing. If the server accounting is enabled, these charges are associated with the user logon and security IDs in the SMF records described earlier.

Enabling Use of the zIIP Specialty Engine

If your site has a zIIP (System **z I**ntegrated **I**nformation **P**rocessor) specialty engine from IBM, you can offload specific categories of workload from the Central Processors to the zIIP.

The zIIP engine is a restricted version of a Central Processor (CP), also referred to as a General Processor (GP). The capacity of the zIIP engine does not count toward the overall MIPS rating of the mainframe image, so the CPU usage incurred on the zIIP is effectively free. Central Processors are often configured to run at speeds below their maximum rating for cost saving and capacity planning purposes. For Central Processors, *100% capacity* typically refers to the maximum MIPS that the processor is allowed to generate at that installation, in accordance with your contract with IBM. In contrast, the zIIP engine always runs at true 100 percent of capacity.

As much as 80 percent of server processing is enabled to run on the zIIP engine. Typical workloads are expected to offload 30 to 80 percent of CPU processing to the zIIP engine.

To make use of the zIIP enablement feature, the server must run in an authorized state.

What Is a zIIP Specialty Engine?

Though physically identical to a Central Processor, the zIIP engine is microcoded at installation time to run specific types of workloads. The Central Processor continues to handle the operating system, I/O interrupts and timer interrupts, job initiations, and user interactions with the operating system. The zIIP concentrates on CPU intensive workloads, leaving the Central Processor more time to absorb otherwise queued workloads, thereby achieving some overall performance improvement across all mainframe activity.

Steps to zIIP Enablement

This section describes steps and requirements for the server use of the zIIP processor.

The steps to server zIIP enablement are:

1. Obtain APF authorization for the server load library.
2. Activate the zIIP feature using the SET ZIIP=ON or SET ZIIP=ON/SIMMAXZIIP command. For instructions, see *Activating a zIIP Environment or Projecting zIIP Usage* on page 231.

Reference: **Usage Notes for Use of the zIIP Processor**

- Maximize the blocksizes of data sources that are read or written by the server to reduce the number of I/Os required to access the file. This will reduce the number of switches to non-zIIP mode that the server agents have to make, thus permitting a greater percentage of zIIP contribution to the request.
- Move or rewrite functions developed at your site since the server must switch to non-zIIP mode for each call to such routines. You may be able to use one of the following possible solutions:
  - Move the routines from DEFINEs to COMPUTEs to reduce the number of times they are referenced. This tactic must be applied carefully, and only when report results would not change.
  - Rewrite the routines using DEFINE FUNCTION, which executes on the zIIP processor.
  - Confine the routine to a pre-step run with ZIIP=OFF which collects its calculated results, then use those calculations in the next step with ZIIP=ON.

Activating a zIIP Environment or Projecting zIIP Usage

The last step in zIIP enablement is to activate the use of the zIIP processor in the server. zIIP enablement is activated by the SET ZIIP command.

The SET ZIIP command has three options:

- **OFF.** This setting prevents the server from offloading its processing to a zIIP.
- **ON.** This setting causes the server to offload processing to a zIIP engine if you have a zIIP processor and the environment is properly APF-authorized.
- **ON/SIMMAXZIIP.** This setting enables you to project zIIP processing in two different environments:
  - **You do not have a zIIP processor.** Using this setting along with the PROJECTCPU parameter, you can project how much server workload would have been offloaded to a zIIP.
  - **You do have a zIIP processor.** Using this setting you can project how much advantage you would achieve by offloading 100% of eligible server processing to the zIIP.

Syntax: **How to Activate the zIIP Enablement Feature**

You can issue the SET ZIIP command in a server profile or in a particular FOCEXEC.

```
SET ZIIP={ON[/SIMMAXZIIP]|OFF}
```

where:

ON

Configures the server to offload processing to the zIIP engine.

This setting:

- Determines if the zIIP processor is accessible to the LPAR in which a job is running.
- Determines if the server environment has been properly authorized to run a zIIP workload.

Note: If the server determines that the zIIP processor is not accessible or that the environment has not been authorized correctly, it issues a message describing the reason and continues in ZIIP=OFF mode, which forwards all subsequent work to the Central Processor.

ON/SIMMAXZIIP

Configures the server to either:

- Project what the zIIP usage would be if the server could offload processing to a zIIP, when the server is operating in an LPAR without a zIIP. This requires that the PROJECTCPU parameter be set to YES.

  The SYS1.PARMLIB member IEAOPT*xx* contains the PROJECTCPU statement. Activating the PROJECTCPU parameter projects zIIP consumption when a zIIP processor is not yet defined to the LPAR. SMF type 30 records will show the potential calculated zIIP time, so that you can accurately project zIIP usage. This enables you to evaluate the effect of configuring a zIIP processor to be available for server usage. The Systems Programmer for your site will have access to this data. Use this option for simulation purposes only.

  Since the zIIP engine actually is not present, all zIIP-eligible workload will be diverted to the Central Processor. Thus, all of that CPU utilization will be recorded in a server variable called &FOCZIIPONCP. This is the amount of workload that would have run on the zIIP engine, and would have appeared in &FOCZIIPCPU, had the zIIP been present and accessible to server work. This information is also recorded in the server job statistics as well as in IBM SMF type 30 records.

  To use this option, insert the following parameter in SYS1.PARMLIB for your LPAR, and also issue the SET ZIIP=ON/SIMMAXZIIP command:

  ```
  PROJECTCPU=YES
  ```

This setting:

- Determines if the PROJECTCPU=YES command has been set in the LPAR.
- Determines if the server environment has been properly authorized to run a zIIP workload.

- Projects zIIP utilization if 100% of eligible server processing could be offloaded to the zIIP, when the server is running in an LPAR with a zIIP. This lets you determine what you would gain by configuring Workload Manager to give the server a bigger share of zIIP processing.

  IBM Workload Manager (WLM) prioritizes workloads among the Central Processors and zIIP processors at your site based on a complex set of goals and rules established by the system administrator. These rules apply to all workloads from all sources, not just the server. These goals combine to influence the decision to direct server requests to the zIIP engine at any particular moment.

  Utilizing this setting with a zIIP present can help you determine how much advantage you would get if the server had more of a share of the zIIP processor. To see the difference in actual and projected zIIP usage, run the same job with SET ZIIP=ON and then with SET ZIIP=ON/SIMMAXZIIP and compare the results. For more information about evaluating zIIP usage, see *Evaluating zIIP Usage* on page 235.

  This setting:

  - Determines if the zIIP processor is accessible to the LPAR in which a job is running.
  - Determines if the server environment has been properly authorized to run a zIIP workload.

Note: If the server determines that the environment has not been authorized correctly, it issues a message describing the reason and continues in ZIIP=OFF mode, which forwards all subsequent work to the Central Processor.

OFF

Configures the server not to offload processing to the zIIP engine. OFF is the default value.

TIBCO Software, Inc. Note: Turn off zIIP enablement only when you know for sure that a job will not gain any advantage from using the zIIP processor or if the system operator or administrator requires that you turn it off.

Example: **Setting the PROJECTCPU Parameter in SYS1.PARMLIB Member IEAOPTxx**

Use the following sample as a guide for setting the PROJECTCPU parameter in SYS1.PARMLIB(IEAOPTxx):

```
/* ************************************************************ */
/*                    SYS1.PARMLIB(IEAOPTxx)                    */
/* ************************************************************ */
PROJECTCPU=YES
```

How the TIBCO WebFOCUS Reporting Server Takes Advantage of the zIIP Processor

The server diverts eligible workload to the zIIP engine by switching from TCB (Task Control Block) mode for workloads that can run only on a Central Processor to SRB (Service Request Block) mode for execution of enabled workloads on the zIIP engine.

Types of server processing that are offloaded to the zIIP engine include:

- Computations.
- Aggregation.
- Screening.
- Sorting.
- Report formatting and styling.
- Transaction Processing.

The server zIIP Monitor detects situations in which the overhead cost of zIIP usage is exceeding the CPU benefits gained. When this threshold is reached, the server may decide to suspend use of the zIIP for the duration of a logical phase of the server request. When it does so, it places a message to that effect in the JES log. It then resets to make the zIIP processor accessible to the next logical phase of the server request.

TABLE, MATCH, MODIFY, and MORE requests may suspend and resume more than once as they progress through logical phases of execution.

In every case, the server attempts to optimize the use of the zIIP and minimize chargeable CPU costs.

Applications that perform significant database I/O, high-volume sorting, or the use of third-party tools or user functions during processing require switching out of SRB (zIIP) mode into TCB (non-zIIP) mode to communicate, and then back again to continue processing. Although each switch is minuscule, the cumulative effect can absorb measurable amounts of CPU time on both the zIIP engine and the Central Processor.

In order to diminish this effect, the server buffers the collection of records passed to the system sort utility and some adapters rather than passing one record at a time, thus reducing the number of switches between TCB and SRB modes.

These third-party products may themselves be zIIP enabled and may offload some or all of their processing to the zIIP engine independent of the server. The server always calls these products from the Central Processor because it cannot know whether they will perform any processing that is prohibited on the zIIP.

Even though zIIP usage occurs more frequently on non-optimized requests to a relational data source, optimized requests are still inherently more efficient and, therefore, may incur less CPU time. Being zIIP enabled, Db2 may also take advantage of the zIIP processor for server requests based on the local configuration of Db2 relative to the server.

Requests against some types of data sources whose I/O can be buffered gain a lot of advantage from zIIP enablement. Data sources that gain the most benefit from zIIP processing due to buffered I/O include:

- Blocked flat files.
- FOCUS.
- XFOCUS.
- VSAM.
- Db2.

Evaluating zIIP Usage

In order to evaluate server zIIP processing in a session, you can query three Dialogue Manager variables that accumulate statistics about CPU processing:

- &FOCCPU accumulates the time spent on a Central Processor. This is an existing variable that precedes zIIP enablement.
- &FOCZIIPCPU accumulates the time actually spent on the zIIP processor (in SRB mode). This is the normalized CPU value using the same scale as &FOCCPU.
- &FOCZIIPONCP accumulates the time that processing could have been offloaded to the zIIP processor but was diverted to the Central Processor by the system.

  Note:

  - &FOCCPU includes the value of &FOCZIIPONCP.

- The sum of &FOCZIIPCPU and &FOCCPU represents the total CPU utilized by the server agent.
- If you set ZIIP=OFF, the zIIP variables do not accumulate further but are not reset to zero. If you later set ZIIP=ON, they resume accumulating statistics.

The RM (Resource Manager) that monitors server usage also captures zIIP statistics.

Performance Considerations for PDS

There are several ways in which you can improve the server performance:

- **Server initialization commands.** You can specify DYNAM commands in member SRVINIT of the data set referenced by //EDACCFG DD in IRUNJCL. For more information, see *Server Initialization Commands Configured in SRVINIT Member* on page 236.
- **Non-swappable address space.** We recommend that you run the server in a non-swappable address space. For more information, see *Running the TIBCO WebFOCUS Reporting Server in a Non-Swappable Address Space* on page 239.
- **Workload Manager (WLM).** You can balance server workload by using Workload Manager. For more information, see *Workload Manager* on page 239.

Server Initialization Commands Configured in SRVINIT Member

It is possible to specify DYNAM commands in member SRVINIT of the data set referenced by //EDACCFG DD in IRUNJCL. These commands will be executed during server startup and will be in effect until the server is shut down. You can execute the following DYNAM commands from SRVINIT:

- `DYNAM SET APP FOR` *`filetype`* `[SKIP}CREATE] [POSTFIX` *`a.b`*`] [` *`parms`*`]`

  Specify the types of component files that are skipped or created for the application when an APP CREATE command is issued. By default, all component file types are generated.

  where:

  `filetype`

  Are the component types that may be affected by this command: ACCESS, DTD, ETG, FOCCOMP, FOCEXEC, FOCSTYLE, GIF, HTML, MAINTAIN, MASTER, SQL, WINFORMS, XML, XSD. You must issue a separate command for each component type you wish to affect.

`SKIP`

Indicates that the designated file type should not be created when the APP CREATE command is issued.

`CREATE`

Creates the designated file type when the APP CREATE command is issued. This is the default setting.

`POSTFIX`

Specifies the lower-level qualifier of the DSN (data set name) for the component type. The APPROOT value is used to complete the full DSN, which is expressed as

`approotvalue.appname.component_type`

The default value for component_type is

`filetype``.DATA`

`parms`

Are the allocation parameters you can set. The default parameter values are:

Filetype	Parms
ACCESS	`RECFM FB TRKS LRECL 80 BLKSIZE 22000 SPACE 50 50 DIR 50`
DTD	`RECFM VB TRKS LRECL 4096 BLKSIZE 27998 SPACE 50 50 DIR 50`
ETG	`RECFM FB TRKS LRECL 80 BLKSIZE 22000 SPACE 50 50 DIR 50`
FOCCOMP	`RECFM VB TRKS LRECL 32756 BLKSIZE 32760 SPACE 50 50 DIR 50`
FOCEXEC	`RECFM VB TRKS LRECL 4096 BLKSIZE 27998 SPACE 50 50 DIR 50`
FOCSTYLE	`RECFM FB TRKS LRECL 1024 BLKSIZE 27648 SPACE 50 50 DIR 50`

Filetype	Parms
GIF	`RECFM VB TRKS LRECL 1028 BLKSIZE 27998 SPACE 50 50 DIR 50` GIF type creates libraries for GIF and JPG files.
HTML	`RECFM VB TRKS LRECL 4096 BLKSIZE 27998 SPACE 50 50 DIR 50`
MAINTAIN	`RECFM VB TRKS LRECL 4096 BLKSIZE 27998 SPACE 50 50 DIR 50`
MASTER	`RECFM FB TRKS LRECL 80 BLKSIZE 22000 SPACE 50 50 DIR 50`
SQL	`RECFM VB TRKS LRECL 32756 BLKSIZE 32760 SPACE 50 50 DIR 50`
WINFORM	`RECFM VB TRKS LRECL 4096 BLKSIZE 27998 SPACE 50 50 DIR 50`
XML	`RECFM VB TRKS LRECL 4096 BLKSIZE 27998 SPACE 50 50 DIR 50`
XSD	`RECFM VB TRKS LRECL 4096 BLKSIZE 27998 SPACE 50 50 DIR 50`

- `DYNAM APP` *`app1 [app2 ...]`*

  Enable application libraries to be allocated during the server startup, improving performance. This command is not applicable to sequential data sets in the application (for example, FOCUS, FTM) which will only be allocated when they are referenced. For example:

  `DYNAM APP IBISAMP BASEAPP` (default command at installation time)

- `DYNAM ALLOC` commands

  For sequential data sets in the application (for example, FOCUS, FTM) to be allocated at server startup (equivalent to adding a JCL allocation for these files in IRUNJCL).

Running the TIBCO WebFOCUS Reporting Server in a Non-Swappable Address Space

We recommend that you run the server in a non-swappable address space. In order to make the server address space permanently non-swappable, add the following entry to SYS1.PARMLIB(SCHED*xx*):

```
PPT PGMNAME(TSCOM300)          /* PROGRAM NAME */
NOSWAP                         /* NON-SWAPPABLE */
CANCEL                         /* CAN BE CANCELLED */
```

Do not use the KEY 0 parameter, or any other parameter (such as NOPASS), unless the system programmer completely understands the consequences of adding the parameter.

All local spawn transactions will perform in the mode of the server. For example, if the server address space is non-swappable, all local spawn transactions execute as non-swappable.

The server executes limited non-local spawn, such as when the user executes a UNIX system command. Non-local spawn execute as swappable.

The server never executes a fork subroutine. (A fork subroutine creates a new process. The new process, called the child process, is an almost exact copy of the calling process, which is called the parent process.)

Workload Manager

Although the server may run in a specific performance group, transactions submitted by server agents may perform differently than the server by adding the following keyword to edaserve.cfg:

`wlm_enclave_trname = WLM_transaction_name`

where:

WLM_transaction_name

Can be up to 8 characters.

This is a service-level keyword.

Using this setting, the task will join a Workload Manager (WLM) enclave when a request starts, and leave the enclave when the request finishes. This gives WLM control of the dispatching priority of the task. The transaction rules defined on WLM will determine the default service class assigned to this transaction, and that service class will determine how the request runs.

This feature helps to balance a workload so that a long request will not affect a short request. This can be achieved through WLM rules designed to lower the priority of a long request after a certain period of time. Without this feature, all requests share the region priority.

The transaction name passed in this keyword must match one defined in the WLM Classification Rules for the Job Entry Subsystem (JES). A corresponding WLM Service Class pointed to by this rule will then be associated with this service.

The classification rules for JES must be used even if the server is started as a started task. The subtasks are always run under JES.

For example, you would include the following in edaserve.cfg:

```
SERVICE = DEFAULT

BEGIN
wlm_enclave_trname = IWAYFAST
.
.
.
END
```

The WLM definition is:

```
Subsystem Type JES - Batch Jobs
Classification:

Default service class is PRDBATLO
There is no default report class.

  Qualifier  Qualifier      Starting       Service   Report
# type       name           position       Class     Class
- ---------- -------------- ---------      --------- --------
1 TN         IWAYFAST                      EDAQRYHI
```

WLM sub-rules (levels 2 and above) are supported. For a server request to join an enclave in a particular service class, the names of all rule qualifiers below our transaction name are checked. For example, consider the following WLM definition:

```
Subsystem Type JES - Batch Jobs
Classification:

Default service class is PRDBATLO
There is no default report class.

  Qualifier Qualifier     Starting Service  Report
# type      name          position Class    Class
- --------- ------------- -------- -------- --------
1 SSC       PRDMVS                 PRDDFLT
2 TN        IWAYFAST               EDAQRYHI
```

In this particular case, the qualifier 1 type is SSC (Subsystem Collection), and a server request will only join the enclave IWAYFAST if it is running on a particular LPAR in the SYSPLEX. This qualifier (PRDMVS) must match the XCF group definition: issue $DMASDEF (for JES2) and check the value of XCFGRPNM field.

You can handle WLM scheduling environments by defining them to WLM and then adding the JOB statement parameter SCHENV=xxxxx to the ISTART JCL.

General Information for a z/OS PDS Installation

This section covers general information for a z/OS installation.

Sample Metadata, Data, and Other Tutorial Samples

The Reporting Server browser interface has a feature on the ribbon and on the application tree (under *new*), *Tutorials* (the Create Tutorial Framework page), which has a pull-down for various samples. The Data Migrator desktop interface also has this feature on the application tree.

There are currently about 10 different tutorial/sample selections available on the pull-down select list to match various customer needs. The bulk of the prior IBISAMP sample objects can be generated by selecting the *Create Legacy Sample Tables and Files* tutorial. Other prior IBISAMP Data Migrator sample objects (usually starting with the characters dm*) are now loaded by choosing their respective Data Migrator tutorials. Under the new method, the tutorials/samples may be loaded to any application, not just IBISAMP.

If you are doing just a software refresh, the prior IBISAMP objects will be unchanged (because a refresh does not touch app directories).

Frequently Asked Questions for PDS

Q: Why might someone want to use the PDS deployment?

A: PDS deployment provides the same rich level of features as the USS-deployed server, including the Reporting Server browser interface, but removes the requirement for interaction with Unix System Services at installation and run time. It deploys the server software in partitioned data sets. Configuration and user-created source files, such as procedures and metadata, are also stored in PDS libraries.

Administration of the server, from a systems perspective, has been streamlined to match that of the classic MVS version of the server (also known as the SSCTL server). There are fewer user ID requirements for installing and operating the PDS-deployed server than the USS-deployed version, and security management has been simplified.

Q: Does this replace the older MVS server (also known as SSCTL)?

A: The z/OS server with PDS deployment is a migration path from the older MVS server.

Q: Can one refresh a server's installation software that had been deployed one way with software using other type of deployment?

A: No. Each deployment type is independent of the other with regards to installation.

Q: Can both deployments of the server coexist on one z/OS system?

A: Yes.

Q: Can one configure two server instances of the same server, one instance a USS deployment, and the other a PDS deployment?

A: No. Although the media and installation are unified, once the base server software is installed, the two deployment types run separately.

As with the USS deployment, the PDS deployment can have many instances running from the same EDAHOME set of libraries.

Q: Can I monitor server startup by checking the MVS SYSLOG?

A: Yes.

The following messages are written to the SYSLOG when

- The Server starts successfully:

  ```
  (EDA13023) ALL INITIAL SERVERS STARTED
  ```

- The Server does not start:

  ```
  (EDA13171) UNABLE TO START IWAY SERVER
  ```

Q: What, if anything, does the PDS deployment not support? In what installation implementation?

A: The PDS deployment of the server currently does not support the following functions:

- The Reporting Server browser interface Run Stress option.
- Displaying server logs and traces in the Reporting Server browser interface.
- Formats XLSX and PPTX. WebFOCUS Client

  Note: As a workaround, you can issue the SET EXCELSERVURL command to point to a TIBCO WebFOCUS® Client ibi_apps context root.

  To set this parameter, you can issue the following in a procedure:

  ```
  SET EXCELSERVURL = http[s]://servername:port/ibi_apps
  ```

  Alternatively, you can issue the following in the WebFOCUS Administration Console:

  ```
  IBIF_excelservurl = http[s]://servername:port/ibi_apps
  ```

where:

servername
Is the name of the machine where the Application Server is running.

port
Is the port used by WebFOCUS to communicate with the Application Server. The default port is 8080. It should also be noted that the protocol may be http or https based on the customer configuration.

- Adobe Flex.
- RACF TEMPDSN class—Supported except for FOCCACHE application datasets.

Third-Party Software and Licenses

All third-party and TIBCO Software, Inc. license information is available on the Reporting Server browser interface by clicking the Help (?) menu, then either *TIBCO Software, Inc.* or *3rd Party Licenses*.

Troubleshooting for PDS

If you have a problem and cannot resolve it yourself, contact Customer Support. In addition, supply the following information to Customer Support:

- Server trace (see *How to Generate a Trace* on page 244).
- JCL for IRUNJCL.
- Job output.
- System dump, if needed (see *How to Generate a System Dump* on page 244).
- Any additional information regarding how the problem occurred.

Reference: Problem: The Reporting Server Abends With a U4039 Code

Problem: The server abends with a U4039 code.

Cause: This is a generic abend.

Solution: Find out what caused the abend by checking the edaprint.log file, SYSOUT *ddname*, and the MVS system log.

Procedure: How to Generate a Trace

To generate a server trace:

1. Turn tracing on by doing one of the following:
   - ❑ Going to the Reporting Server browser interface menu bar, selecting *Workspace*, and then *Enable Traces.*
   - ❑ Starting the server by running the ITRCON JCL member.
   - ❑ On the MVS Console or SDSF, issue the following operator MODIFY command

     ```
     F jobname , -traceon
     ```

     where *jobname* is the job under which the server is running.
2. Reproduce the problem.
3. Submit the ISAVEDIA member to produce additional diagnostic information.
4. Send the server JES log, and the ISAVEDIA JES log, to Customer Support.

Procedure: How to Generate a System Dump

To generate a system dump:

1. Allocate DDNAME SYSMDUMP pointing to the data set with the following DCB parameters:

   ```
   RECFM=FB,LRECL=4160,BLKSIZE=4160.
   ```

2. To get the first dump, add the parameter FREE=CLOSE to your DD statement. The DD statement should appear as follows:

   ```
   //SYSMDUMP DD DISP=SHR,DSN=MYID.EDAPTH.SYSMDUMP,FREE=CLOSE
   ```

3. To get the last dump, the statement should appear as follows:

   ```
   //SYSMDUMP DD DISP=SHR,DSN=MYID.EDAPTH.SYSMDUMP
   ```

   Only two IDs must have privileges to write into this data set: ISERVER and IADMIN. General server users DO NOT need read or write access to the SYSMDUMP data set.
4. To prevent Abend-AID from intercepting the dump, add:

   ```
   //ABNLIGNR DD DUMMY
   ```

5. To prevent Language Environment from intercepting the dump, specify:

   ```
   EDADUMPOPT=UAIMM in EDAENV DD
   ```

   This enables you to get more accurate information reflecting the moment the abend actually occurs.

6. Save the entire job output for the server (including JES logs), and send it to Customer Support.

Instead of using JCL allocations to add SYSMDUMP, the procedure described below can be used alternatively.

Procedure: How to Add JCL Allocations to a Running Reporting Server

A z/OS operator can issue modify commands from the z/OS system console to allocate DDNAMES to the server without restarting it. This procedure is useful if you need to re-allocate a file that was freed to allow a batch overnight utility to run, or perhaps to add SYSMDUMP allocation to a running server.

Syntax: How to Allocate a Data set From the z/OS System Console

```
F <iway_server_jobname/started task>,DYNAM ALLOC FI <ddname> DA <dsname>
<optional dynam parameters>
```

Example: Allocating a VSAM Data set

```
F IWAY2,DYNAM ALLOC F VSAMFILE DA VSAM.FILEA.CLUSTER SHR
```

Example: Allocating a SYSMDUMP Data set With FREE=CLOSE Option

```
F IWAY2,DYNAM ALLOC FILE SYSMDUMP DA PROD2.SYSMDUMP.DATA SHR CLOSE
```

Note: The examples above assume IWAY2 is the jobname/started task ID for the server.

All valid DYNAM ALLOC syntaxes are supported. For more information on the DYNAM command, refer to the *TIBCO WebFOCUS® Stored Procedure and Subroutine Reference for 3GL Languages* manual.

The following message will be issued in the server JESMSGLG indicating if the command was processed successfully or not.

Success:

```
+DYNAM COMMAND SUCCESSFULLY PROCESSED Rc=0
```

Failure:

```
+DYNAM ERROR: IKJ56225I DATA SET IWAY.TEST ALREADY IN USE, TRY LATER
```

Procedure: How to Free Data sets Allocated to the Reporting Server

A z/OS operator can issue modify commands from the z/OS system console to free DDNAMEs or DSNAMEs allocated to the server. Both global allocations (made at the server ISTART JCL) and local ones (DYNAM ALLOC commands issued by user tasks) can be freed. This procedure is useful if you need to free an allocation to run a batch utility overnight, without restarting the server.

Syntax: How to Free a Data set From the MVS System Console

To free a single DDNAME:

```
F <iway_server_jobname/started task>,DYNAM FREE FI <ddname>
```

To free a single DSNAME (all occurrences in the server):

```
F <iway_server_jobname/started task>,DYNAM FREE DS <dsname>
```

To free multiple DDNAMEs, passing a pattern (free all DDNAMEs starting with AB):

```
F <iway_server_jobname/started task>,DYNAM FREE FI AB*
```

To free multiple DSNAMEs (all occurrences in the server), passing a pattern (free all allocations of data sets starting with IWAY.VSAM):

```
F <iway_server_jobname/started task>,DYNAM FREE DA IWAY.VSAM*
```

A message will be issued in the iway_server JESMSGLG indicating if the command was processed successfully or not, as follows.

Success:

```
+DYNAM COMMAND SUCCESSFULLY PROCESSED Rc=0
```

Failure:

```
+DYNAM ERROR: IKJ56225I DATA SET IWAY.TEST ALREADY IN USE, TRY LATER
```

Example: Freeing an Allocated Data Set

Suppose ISTART JCL (jobname IWAY2) has the following allocation:

```
//VSAMFILE DD DISP=SHR,DSN=VSAM.FILEA.CLUSTER
```

The operator can free this file using the command (from MVS console):

```
F IWAY2,DYNAM FREE FI VSAMFILE
```

Procedure: How to Initialize the RDAAPP Application

RDAAPP is an interactive client test application that facilitates the execution of SQL statements and stored procedures on the Unified server. During the installation process, JCL and REXX routines are created in the installation data set as members IRDAAPPJ and IRDAAPPC respectively.

The following installation data set is used for USS deployment.

qualify.WFS.DATA

The following installation data set is used for PDS deployment.

qualify.PDS.WFS.DATA

Note: The RDAAPP application is not intended for use as a production tool.

1. To use the IRDAAPPJ JCL, you must first edit the member IRDAAPPJ and add your request details.

   a. To edit the member IRDAAPPJ, change the following field,

   ```
   //SYSIN DD *
   Put your request here
   //
   ```

   to

   ```
   //SYSIN DD *
   1
   <userid>
   <password>
   S SELECT COUNTRY   FROM CAR
   S SELECT CAR,SEATS FROM CAR
   Q
   //
   ```

b. Complete the panel as follows.

Field	Instructions	
`<enter userid>`	Enter a valid user ID or blank line if the userid of the user who submitted the job is to be used for a trusted connection.	
`<enter password>`	Enter the password for the above userid or a blank line if the userid/password of the user who submitted the job is to be used for a trusted connection.	
`1`	Match a node name in the EDACS3 allocation in the IRDAAPPJ JCL. Default (1) means LOOPBACK.	
`<enter request>`	Enter one of the following values:	
	`S`	To enter an SQL SELECT statement. Type the statement after you enter the value S (see the following example).
	`Q`	To quit.
	`?`	For this list of commands.
`Q`	Quit RDAAPP (It is needed twice).	

c. Once you have made the above edits, submit the JCL for execution.

2. Type the following command at the TSO ready prompt to use the IRDAAPPC REXX routine:

```
EX 'qualif.WFS.DATA(IRDAAPPC)'
```

or

```
EX 'qualif.PDS.WFS.DATA(IRDAAPPC)'
```

3. After the prompts, enter the same information as specified in the above table.

Example: **IRDAAPPC REXX Execution**

The following is the screen output from a sample execution of the IRDAAPPC REXX routine:

```
*********************************************************************
**                   RDAAPP Client test tool                       **
*********************************************************************
```

```
Allocating environment handle...
List of available servers:
 1 - LOOPBACK
Enter corresponding server entry number or name (default=1):


1
Enter User Name:
Enter Password:
Allocating connection handle...
Attempting connect to the datasource: LOOPBACK ...
Connect status = 0


New ODBC Connector Test.
Enter Command:
S SELECT COUNTRY   FROM CAR
Alloc stmt ...
Return code from alloc stmt is 0
Issuing SQLPrepare call for  SELECT COUNTRY   FROM CAR
Return code from SQLPrepare call is 0
Executing  SELECT COUNTRY   FROM CAR stmt...
Issuing SQLNumResultCols call for  SELECT COUNTRY   FROM CAR
Number of resultset columns is 1
Printing select item descriptions:


Issuing SQLDescribeCol call for colNum=1
item #1
colname = COUNTRY
coltype = 1
precision = 10
scale = 0
nullable = 0


Binding columns...
Fetching report data...
ENGLAND
FRANCE
ITALY
JAPAN
W GERMANY
<<< 5 record(s) processed. >>>


New ODBC Connector Test.
Enter Command:
S SELECT CAR,SEATS FROM CAR
Alloc stmt ...
Return code from alloc stmt is 0
Issuing SQLPrepare call for  SELECT CAR,SEATS FROM CAR
Return code from SQLPrepare call is 0
Executing  SELECT CAR,SEATS FROM CAR stmt...
Issuing SQLNumResultCols call for  SELECT CAR,SEATS FROM CAR
Number of resultset columns is 2
Printing select item descriptions:
```

```
Issuing SQLDescribeCol call for colNum=1
item #1
colname = CAR
coltype = 1
precision = 16
scale = 0
nullable = 0
 Issuing SQLDescribeCol call for colNum=2
item #2
colname = SEATS
coltype = 4
precision = 22
scale = 0
nullable = 0

Binding columns...
Fetching report data...
JAGUAR
2
JAGUAR
5
JENSEN
4
TRIUMPH
2
PEUGEOT
5
ALFA ROMEO
2
ALFA ROMEO
2
ALFA ROMEO
4
```

```
MASERATI
2
DATSUN
4
TOYOTA
4
AUDI
5
BMW
5
BMW
4
BMW
5
BMW
5
BMW
5
BMW
5
<<< 18 record(s) processed. >>>

New ODBC Connector Test.
Enter Command:
Q

Committing...
Return code from commit is 0
Disconnecting DBC ...
Freeing DBC handle...
Freeing ENV handle...
<<< RDAAPP : Exiting... >>>
```

Chapter 5

Installation for IBM i

This chapter describes the requirements and procedures for installing on IBM i.

Note. This manual uses the term IBM i generically to refer to all OS/400, i5/OS, and IBM i releases.

In this chapter:

Information You Need Prior to Installation on IBM i

The WebFOCUS Reporting Server is installed by going to the TIBCO™ eDelivery site and downloading the software to be used in the actual installation. By selecting your product, version, and operating system, and accepting the EULA agreement, you may then either select to download the full product or individual files.

If you choose individual files, you must open the *TIBCO WebFOCUS Reporting Server Software* folder, select the *TIB_wf-rs_*_ibmi_power.zip* file, where * indicates the release number for the platform, and start the download to a machine that supports unzipping.

Once the desired file is downloaded, unzip the file. The zip file contains an IBM i .savf saveset.

To restore the saveset (assuming MYLIB is either the actual value of *CURLIB or the library you want to use for the saveset), either:

- FTP it to an existing saveset, for example, MYLIB/*install_saveset*, where *install_saveset* is the name of the installation saveset on the IBM i machine, using the "(REPLACE" option.

For example:

```
cd MYLIB
get i9000M_359.savf MYSAVESET (REPLACE
```

- FTP it to an IFS file and then use the cp command to copy it to the existing saveset, for example, MYLIB/*install_saveset*, where *install_saveset* is the name of the installation library saveset on the IBM i machine. For example:

```
cp i9000M_359.savf /QSYS.LIB/MYLIB.LIB/MYSAVESET.FILE
```

Once the file exists as a saveset on the IBM i machine, use the DSPSAVF command to determine the actual library name to restore. It will be the object name with *LIB as the type. Then, using the QSECOFR user ID, use the actual library name (as found using the DSPSAVF command) as the SAVELIB name, as shown in the following example RSTLIB command:

```
RSTLIB SAVLIB(M729000DTP) DEV(*SAVF) SAVF(MYLIB/install_saveset)
MBROPT(*ALL) ALWOBJDIF(*ALL) RSTLIB(install_saveset)
```

After restoration, proceed with the instructions below using the restored library name, for example M729000DTP.

The process for full download is similar. A main directory is created on the desktop with multiple directories and subdirectories. Simply find the applicable TIB_wf-rs_*.zip file from the download directory, transfer it, and follow the steps as previously noted.

The server has an email notification feature that requires SMTP mail server information. You can enter these parameters either during installation, or later using the Reporting Server browser interface Administration tool.

You need a server administrator user ID, referred to as *iadmin* in the remainder of this chapter.

- The operating system ID you use when installing the server owns the server files and is the default server administrator for OPSYS mode. You can create a new operating system ID to run and own the server files, or use any ordinary (non-superuser) ID. However, you should not install the server as root. The server administrator ID should have a Korn, Bourne, or Bash shell as the default logon shell.

- In addition to the iadmin ID, you have the option of creating a iserver user ID that is QSECOFR for internal use by the server to proxy the authority of QSECOFR. The ID can be an account never used for logging in. You might wish to create an iserver ID if, for example, you do not want certain server processes to appear as owned by QSECOFR.

For specific information on creating IDs, see *Creating User IDs on IBM i* on page 262.

IBM i Installation Requirements

Before you install, review the following requirements.

Type	Description	
Operating System	IBM i V7R2 or higher The *TIBCO WebFOCUS® Release Notes* maintains a current list of supported operating systems and levels.	
Disk Space (Do not install to iASP based locations)	Space for installation Space after installation	Approximately 3G Approximately 2G
IP Ports	Up to six consecutive IP ports (two in reserve for typical extra features). The supplied IP port numbers must be above the IANA registered well-known reserve range (numbers under 1024) and not over the maximum legal number (65535). Additionally, do not use IP port numbers already being used by other applications or products. Netstat, or netstat like commands, should reveal what actual ports are in use. Additional Java Listeners (post-installation option) require additional ports (beyond basic reserve).	
Memory	Memory and shared memory usage depend on the following elements: ❑ Number of data access agents. ❑ Type of access that is performed, such as joins and large retrieval. ❑ Connection queue. Actual memory usage differs between applications and the server load.	

Type	Description
Java	Java JRE or Java SDK (also known as JDK) 8 or higher Needed if JVM-based adapters, server-side graphics, XBRL, or user-written CALLJAVA applications are to be used. For additional information, see *JVM Requirements for Java Services* on page 256. **Note:** Java 8 and Java 11 are explicitly tested and certified to be compatible with the WebFOCUS Reporting Server. Other Java releases may be compatible with the WebFOCUS Reporting Server. If you use an untested Java release, you must self-certify its compatibility with the WebFOCUS Reporting Server and accept responsibility for using an untested release.
Web Browser	Needed for using the Reporting Server browser interface. Microsoft Edge Mozilla Firefox® 59 or higher. Google Chrome® 65 or higher.
Shell	The IBM i - QShell Interpreter (IBM i Installation Option 30) must be installed to use the product. The QShell Interpreter is a free optional feature of IBM i. The easiest way to check if this feature is installed is to enter QSH on the IBM i command line. If it is installed, a UNIX-like environment starts (F3 to exit). If it is not installed, you receive a *Command QSH in library *LIBL not found* message. If it is not installed, install it before proceeding.

JVM Requirements for Java Services

If Java-based adapters, server-side graphics, XBRL, or user-written CALLJAVA applications are to be used, a Java Runtime Environment (JRE) JVM must be installed on the machine, and the server must be configured to use it.

The minimum Java JVM release level is 8 or higher, due to required internal components of the server. The Java Listener will not start properly (and will show errors in the edaprint.log file) if 8 (or higher) is not in use.

The following URL has Java EOL and EOSL information:

http://www.oracle.com/technetwork/java/eol-135779.html

On IBM i5, Java is a system installed option and there is no differentiation between JRE and SDK, but the build version it uses must also match the bit size of the server, which is 64-bit.

By default, the server uses the system default Java level and directories. If JVM is found with the correct bit size and level (8+), the Java Listener will start and send the *start* message to the edaprint.log file, in which case no further configuration is needed. If 8 is not the default and the site does not want it as the default, then an explicit set up variable must be configured.

If JVM loading fails, the server will start, but not the Java Listener. This should be corrected. The default IBM i Java level may be set at a system level, however, changing this may affect other processes, so control is best done at the server level. For V7R2 (or higher), this is done by setting the following in the server environment file, edaenv.cfg,

```
JAVA_HOME=/QOpenSys/QIBM/ProdData/JavaVM/jdk80/64bit
```

The location of the default JVM on IBM i is controlled by the object QSYS/QJVAJNI. This is normally on the system path, so you do not need to do anything to fulfill basic JVM *find* requirements. However, if the default JVM level of the machine is not 8 or higher, corrective action may be required to access the correct JVM level.

If the default JVM is not found or is set to an appropriate release at server start time, a *Failed to find JVM* message will be displayed. Further Java Services debugging information about loading the JVM will be written to the server start log, indicating *JSCOM3 start failed*, as well as additional information that may be useful in resolving the problem. JSCOM3 is the actual process name for the Java Services Listener, and the terms are often used interchangeably.

The easiest way to determine the current default for the server iadmin ID is to issue the command QSH CMD('java -version'), which will display the default release level for the ID.

There are several choices on how to address using the correct JVM level, but as of V7R2, the steps no longer vary by operating system.

- Change the Java (5761-JV1) install options to point at the desired JVM level as a machine default. This may or may not be desirable based on other applications that may be using Java.
- Set JAVA_HOME to point at a desired JVM release level.

The various Java releases and PTF releases that may be available at any time will be found in the following folder:

```
/QOpenSys/QIBM/ProdData/JavaVM
```

For example:

```
/QOpenSys/QIBM/ProdData/JavaVM/jdk70/64bit
/QOpenSys/QIBM/ProdData/JavaVM/jdk71/64bit
/QOpenSys/QIBM/ProdData/JavaVM/jdk80/64bit
```

To use the JVM from one of these releases, specifically for the server iadmin ID (if it is not already the system default), set the JAVA_HOME variable to point at a 64bit JDK. For example:

```
JAVA_HOME=/QOpenSys/QIBM/ProdData/JavaVM/jdk80/64bit
```

Note that Java 80 is currently the minimum requirement for the server.

The variable may be set in any of the following ways:

- As a system variable set from the profile of the server iadmin ID, using INLPGM exit, a JOBD RQSDTA() CL option, or any number of other methods for setting system variables within the environment of a job.
- As an exported QSH variable in any script that is used to call the edastart script.
- As a system variable in any customized CL that is used to call the QSH IFS edastart script, or as an export variable within the QSH portion of the CL.
- Add to the edaenv.cfg environment configuration file of the server.

Formerly, a -Djava class property could be used to control the Java JVM release level, however, this method is no longer supported as of V7R2. If this method was used previously under V7R1, and the machine is upgraded to V7R2, the parameter should be removed and the server must be configured using V7R2 methods (described above).

To change or add operating system environment variables, set and export the variable in a .profile, script, or CL that always gets called during a server start. It is very common to place variables in the server edastart script, but it is recommended that they be placed in a script that in turn calls edastart (so that the edastart script remains vanilla).

To change or add a variable in a server environment start-up file (EDACONF bin\edaenv.cfg), either edit the file in a text editor before starting the server or:

1. Start the server (services like Java Listener may fail until configured and the server is restarted).
2. Open the Reporting Server browser interface and log on using an administrator ID.
3. Select *Workspace* from the main menu.

4. In the navigation pane, open the *Configuration Files* and *Miscellaneous* folders.
5. Right-click *Environment - edaenv.cfg* and select *Edit*.
6. Make the desired edit.
7. Save the file.
8. Restart (changes are not effective until restart).

The format of the edaenv.cfg variables is one per line in name=value pairs. Spaces before and after the equal sign are optional. Values with embedded spaces do not require quoting. Variables are always uppercase.

To add classes to the JVM class path for customer-written CALLJAVA applications, set and export the CLASSPATH variable to the operating system level before server start-up or use the Reporting Server browser interface to set the Java Listener IBI_CLASSPATH property by using the Reporting Server browser interface to access the Java Listener:

1. Select *Workspace* from menu bar.
2. Open the *Java Services* folder.
3. Right-click *DEFAULT* and select *Properties*.

   The Java Services Configuration pane opens.
4. Expand the *Class Path* section.
5. Add the desired full path jar names (one per line).
6. Click *Save and Restart Java Services*.

If JVM-based adapters or features are not required, and the JVM environment is not configured, the message *Failed to find JVM* is normal and can be ignored.

Installation and Configuration Directories on IBM i

The installation process creates these high-level directories. The locations documented often use 90 in the location names or when discussing the release level, however, this value may vary for your particular installation and reference an alternate level.

Name	Environment Variable	Description	Default Path

Home directory	EDAHOME	Stores the server software programs and other files	`ibi/srv90/home`
			Must conform to the following pattern`90`
			`*/ibi/srv90*/home*`

Home library		This installation library contains the actual server programs that appear in the home directory as symbolic links.	The default library name is SRV90, but you can specify any valid library name.
Configuration directory	EDACONF	Stores the configuration files. If you are configuring multiple instances of the server, create separate configuration directories for each by adding a suffix (for example, a number) to the end of the directory name.	`ibi/srv90/`*`product_type`* Must conform to the following pattern. `*/ibi/srv90*/`*`product_type`* Product type can be: ❑ **WFS** for a WebFOCUS Reporting Server

Name	Environment Variable	Description	Default Path
Application directory	APPROOT	Contains your application files. Security for application directories is handled at the operating system level. To avoid any possibility of these directories being accessed inappropriately by means of APP commands (such as APP DELETE *AppDirName*), use directory security to set the appropriate permissions on these directories.	`ibi/apps`
Profiles directory	EDAPRFU	Stores the user and group profiles and the admin.cfg file (which specifies the server administrator).	`ibi/profiles`

Multiple WebFOCUS Reporting Servers. If you plan to install multiple copies of WebFOCUS on the same computer, and you want to provide each copy with its own WebFOCUS Reporting Server, you may wish to maintain a separate root directory for each copy, so that you can keep copies of each set of components, including the server, together in the same path.

You can specify a separate apps directory for each copy of WebFOCUS, or specify a single apps directory to be shared by all copies of WebFOCUS.

Creating User IDs on IBM i

Server administrator ID (iadmin)

The installation of a server requires an ID to install and own the files as well as to administer the server; this is also known as the iadmin ID. The iadmin ID should:

- Not be QSECOFR, not have a group of QSECOFR, and not have other special authorities.
- Have authority to use RSTLIB for the duration of the installation process.
- Have a message queue delivery of *NOTIFY if this is not the default for the system.
- Have a writable explicit CURLIB (not *CRTDFT QGPL). We recommend a library that is the same name as the user ID (for example, CRTLIB IADMIN). However, if the Db2 interface is being used in SQL mode (vs. CLI) then the library should be created as a Db2 Collection (for example, STRTSQL -> CREATE COLLECTION IADMIN) so Db2 Journaling is active for the server. Alternately, Journaling for Db2 may be redirected (instead of creating a specific collection) by creating a QDFTJRN Data Area entry in the CURLIB with:

  ```
  CRTDTAARA DTAARA(IADMIN/QDFTJRN) TYPE(*CHAR) LEN(25) VALUE('IADMIN
  QSQJRN *FILE')
  ```

  The CRTDTAARA VALUE parm must be padded to the sizing shown (10 10 5). If not, Journal redirection will not work.

  Note: The Reporting Server requires the IADMIN ID to have an explicit CURLIB and that it is not QGPL, as server management CL/CMD files would be placed there, which is not a good practice. The easiest way to check if an ID has a CURLIB, and what it is set to, is to do a DSPLIBL and look for a library entry with a type of CUR. A CURLIB library name matching the software installation library (for example, SRV90) is also not recommended, as this allows the software library to possibly get corrupted with files from daily activities. It also creates a high possibility of accidental overwrites or deletions of important software.
- The server administrator ID should only have basic IBM i libraries and no System/36 compatibility libraries.
- The server administrator ID should have a user profile sort sequence default for SRTSEQ() of *HEX, either explicitly or because *SYSVAL system default resolves to *HEX.
- Have a HOMEDIR other than the IBM i default of "/" and the directory should exist, for example, /home/iadmin.

- The server administrator ID (at the operating system level) must be configured for code page 37 (EBCDIC 8-bit West European) or a code page that is compatible with 37 in order for the server to work properly. Code Page 65535 (raw data mode) is not acceptable. After installation, the server itself (using the Reporting Server browser interface) may be configured for a particular code page configuration (and language).

  To determine if the code page you use is compatible with code page 37, check if the square brackets ([ ]) in your code page are in the same position as on code page 37.

  - If square brackets are in the same position, your code page is compatible with 37. You do not need to do anything else.
  - If square brackets are *not* in the same position, change the code page that is specified in the IBM i iadmin profile to 37 (or to a code page compatible with 37). Then log iadmin off the system, and log it on again to install.

  You can find IBM code page descriptions at:

  http://www.ibm.com/servers/eserver/iseries/software/globalization/codepages.html

This documentation refers to the server administrator ID, which you use to install and administer the server, as the iadmin ID, but you can name it anything you want. If you name it something other than iadmin, you will need to create a second ID, literally named iadmin, for the DVD library to properly unload. If you do not use this literal iadmin ID to install and own the files, you can remove it after installation.

While logged on as QSECOFR, create the server administrator ID and home directory using the following sample code:

```
CRTUSRPRF USRPRF(IADMIN) PASSWORD(MYPASS) HOMEDIR('/home/iadmin')
CCSID(37) TEXT('Server Administrator ID') DLVRY(*NOTIFY)
QSH CMD('mkdir /home/iadmin')
QSH CMD('chmod 755 /home/iadmin')
QSH CMD('chown iadmin /home/iadmin')
```

Running the server in secured mode also requires that particular files have their ownership changed to QSECOFR (this step is done after installation).

User IDs

Users of the server will also require an ID and password created/configured for the Security Provider modes a server is using. For the OPSYS Security Provider mode, no special authorities or setup parameters are needed for the IDs.

To keep the server secure, you should make the iadmin ID available only to users that require server administrative privileges.

Server system ID (iserver)

You have the option of creating a user ID that is QSECOFR for internal use by the server to proxy the authority of QSECOFR. We call this the Server system ID (iserver). The ID can be an account that is never used for logging in. You might wish to create an iserver ID if, for example, you do not want certain server processes to appear as owned by QSECOFR.

To create iserver, issue the following command

```
CRTUSRPRF USRPRF(id) PASSWORD(*NONE) USRCLS(*SECADM)
TEXT('Server System Security ID') SPCAUT(*SECADM *ALLOBJ *JOBCTL)
```

where:

id

Is the name of the actual iserver ID.

Running ISETUP to Install the TIBCO WebFOCUS Reporting Server Software

You can install the server software by running isetup interactively and responding to prompts or by creating a file containing the answers to the prompts and running isetup against that file. The method using a file is called a *silent install*.

Regardless of the installation being an interactive or silent installation, the library name from the *DSPSAVF* and *RSTLIB SAVLIB(M729000DTP)* steps is used in the CALL *library/*ISETUP steps below.

For information about the parameters required for a silent installation, you can display the installation help information by navigating to the library of the downloaded installation software (*library*, as used in the example) and issuing the following command:

```
CALL library/ISETUP '?'
```

Procedure: How to Run ISETUP Interactively

1. Sign in using the iadmin user ID.
2. On the IBM i command line, call the installation procedure using the library from the example restore:

   ```
   CALL library/ISETUP
   ```

   where:

   library

   Is the name of the installation library.

The following isetup screen displays.

```
-----------------------------------------------------------------------
                 Welcome to the Product Set Up Facility
     Please respond to the prompts or enter Q to quit at any prompt.
-----------------------------------------------------------------------

  ISETUP: Now Installing TIBCO WebFOCUS 90 Server

-----------------------------------------------------------------------

Select an option:
      1. Install and Configure
      2. Add Additional Configuration Instance
      3. Refresh Installation (Reinstall, Keep Configurations)
      4. Install Debuggables to the Installation Directory
      5. View Installation Notes
Enter a selection (Default=1) :
```

3. Enter *1* for the Install and Configure option.

   You are prompted for the location of the installation file.

4. Enter the name of the installation library that you restored to or press Enter to accept the default.

   You are prompted for the ID of the server administrator for the internal server security provider.

```
Enter credentials for the server's internal security
provider (PTH), the server's default start up mode.
Enter the Server Administrator ID
(Default=srvadmin) :
```

   The server automatically starts with this security provider. You can add other security providers using the server Reporting Server browser interface after installation. For information, see the *TIBCO WebFOCUS® Reporting Server Administration* manual.

5. Enter the server administrator ID or accept the default.

   You are prompted for the server administrator password. There is no default.

```
Enter the Administrator Password :
```

6. Type the password of the account you are using to install the software.

   The password, which does not display, is stored in encrypted form.

   You are now shown the default values of the server environment variables and port number, and given an opportunity to change them. For example:

```
Please review the default settings.
EDAHOME = /prog3/iadmin/ibi/srv90/home
EDACONF = /prog3/iadmin/ibi/srv90/wfs  (*EXISTS, owner iadmin *)
EDAPRFU = /prog3/iadmin/profiles
APPROOT = /prog3/iadmin/ibi/apps
HOMEAPPS = /prog3/iadmin/ibi/homeapps
HTTP_BASE_PORT = 8121
WARNING: Directories marked as existing will be deleted and recreated!
If you are satisfied with the default settings you may proceed to
final confirmation else you will be prompted for individual values.
Proceed with defaults? (Y/N Default=Y)  :  y
```

If any of the prompted locations (such as EDAHOME) exist, they will be marked with "(*EXISTS*)" on the display line. This gives you the opportunity to change a location if you do not want to overwrite it by changing the default values.

When specifying a location, note these requirements:

- The EDAHOME directory path name directory path name must conform to the pattern *ibi/srv90*/home* and must be an absolute path.
- If you changed the EDAHOME value, the default EDACONF and EDAHOMELIB values change to conform to EDAHOME.

  EDACONF must be in the same srv90 path as EDAHOME. The lowest-level EDAHOME directory (home) becomes the product type directory in EDACONF.

  For example, if EDAHOME is

  ```
  iadmin/ibi/srv90/home
  ```

  then EDACONF for a WebFOCUS Reporting Server defaults to:

  ```
  iadmin/ibi/srv90/wfs
  ```

  If you are configuring an additional server instance, be sure to specify a new configuration directory here; do not use an existing directory. Each instance must have its own configuration directory. You can append characters to the name of the *product_type* directory to avoid overwriting the existing directory. For example:

  ```
  iadmin/ibi/srv90/wfs2
  ```

7. If you want to accept the default values, type *Y* and skip to Step 10. Otherwise, change any properties that you wish.

   For information about the EDAHOME, EDACONF, EDAPRFU, and APPROOT environment variables you can set, see *Installation and Configuration Directories on IBM i* on page 260.

The other properties you can set are described in the following table.

Parameter	Description
HTTP_BASE_PORT	First of three consecutive port numbers for the HTTP Listener and other IP-based services. The default ports are 8121-8123.
TCP_BASE_PORT	Port number on which the server TCP Listener listens. It must be outside the range of the three consecutive HTTP Listener ports. It defaults to the port immediately preceding the first HTTP Listener port. For example, if you accept the default HTTP Listener Port value of 8121, the TCP Listener port defaults to 8120.
SMTP_HOST	SMTP Server node (host) name or TCP/IP number for outbound email features. (Optional, only prompted for if changing directories and ports.)
SMTP_PORT	SMTP Server port number for SMTP Server. The default value is 25. (Optional, only prompted for if changing directories and ports, and the SMTP Server host is supplied.)
SENDER_EMAIL	Default *from* address for users reading an email from the server if none was specified in the originating application. (Optional, only prompted for if changing directories and ports, and the SMTP Server host is supplied.)
SERVER_ADMIN_EMAIL	Server administrator email address to send administrative warnings to, such as an agent crash. (Optional, only prompted for if changing directories and ports, and the SMTP Server host is supplied.)

If you decide to change a default, you are prompted for a replacement value for each of the above variables, and given another chance to accept the default. If the SMTP Server node is not supplied, the remaining SMTP and EMAIL prompts do not occur.

8. Review the configuration options displayed on the screen, and type *Y* if you accept them. Alternatively, to start over, enter *N*; to quit the installation procedure, enter *Q*.

   Several progress messages display while the server is being installed. You are then asked if you want to start the server.

9. If a server installation, type *Y* to start the server or *N* to exit.

   If you start the server, startup messages and the Reporting Server browser interface URL are now displayed.

You should now verify your installation, as described in *Verifying the Installation* on page 268.

Verifying the Installation

To verify that you have successfully installed, use the configuration that is created by the installation. You can verify the installation by bringing up, checking, connecting to, testing, disconnecting from, and shutting down the server.

After verifying the installation, you can create any product tutorials you need and configure adapters.

Procedure: How to Verify Installation

1. Log on to your IBM i operating system with the iadmin user ID.
2. There are several methods to start a server and options that may be used. The following method for starting a server (using the appropriate library name and TSCOM300 options) would be the most familiar to an IBM i Administrator:

   ```
   CALL SRV90/TSCOM300 PARM('-edaconf' '/home/iadmin/ibi/srv90/wfs'
   '-start')
   ```

   Alternate startup methods and batch examples are noted below.

3. Check to ensure that the processes are up with -show:

   ```
   CALL SRV90/TSCOM300 PARM('-edaconf' '/home/iadmin/ibi/srv90/wfs'
   '-show')
   ```

4. Start the Reporting Server browser interface by starting a browser pointed at the server HTTP Listener port specified during installation. The URL format is http://*host*:*port*. (The URL is also displayed at the end of the installation procedure.)

   For example, if default ports were used during installation, use http://*host*:8121 for a WebFOCUS Reporting Server.

5. If the server is running in a secure mode, you will first see a logon screen. Log on using the iadmin ID used during server configuration. For information about configuring the server security, see *Security Providers on IBM i* on page 269.

The Reporting Server browser interface home page opens. The Home Page is arranged in a menu-like context for the various features it supports. Detailed use of the Reporting Server browser interface for configuration or general operation of the server is available by clicking *Help* in the left navigation menu and in the *TIBCO WebFOCUS® Reporting Server Administration* manual.

6. If the Reporting Server browser interface opens and displays application tree folders in the left pane, the server is working because it uses its own underlying data access and reporting technologies to visualize the application tree. The server may be further data tested (if desired).
7. When you are done using the server, you can stop it using the Reporting Server browser interface by clicking the *Stop* option on the Reporting Server browser interface toolbar.
8. If you experience any problems, examine the IFS /home/iadmin/ibi/srv90/wfs/edaprint.log file.

Security Providers on IBM i

The default security provider for a new installation is the internal security provider, PTH. The PTH provider implements security using user IDs, passwords, and group memberships stored in the admin.cfg configuration file.

After the initial installation, the Server Administrator that was configured during the installation can start the server and use the Reporting Server browser interface to further customize security settings, for example, to configure alternate or additional security providers, create additional PTH IDs, and register groups and users in a security role. For more information about security providers, see the *Server Security* chapter in the *TIBCO WebFOCUS® Reporting Server Administration* manual.

Procedure: How to Satisfy Security Provider OPSYS Requirements

To run a server with security provider OPSYS in IBM i, you must satisfy the following requirements. You must do this once after installing and after each refreshing of the server with fixes.

Certain files must be owned and run under the QSECOFR profile or a QSECOFR-authorized ID (such as iserver) that allows impersonation for the OPSYS security mode. Running with security mode OPSYS requires users to send a password to connect to the server, or to use some other form of verification. Although general installation of the server software is done by iadmin (an ordinary user ID), this step requires QSECOFR authority.

To change ownerships, do the following:

1. Log on as QSECOFR.

2. Using the library specified during the installation, change the file ownership by entering the following commands, then restart the server and configure for OPSYS:

   ```
   CHGPGM PGM(SRV/TSCOM300) USRPRF(*OWNER)
   CHGOBJOWN OBJ(SRV/TSCOM300) OBJTYPE(*PGM) NEWOWN(QSECOFR)
   ```

   Review and register IDs and groups for various user roles as well as setup folder access control at the role or user level (right-click role or user).

The CHGPGM and CHGOBJOWN steps will need to be repeated after any server upgrade since the tscom300.out file is replaced during an upgrade and the attributes are lost.

Note: If this Security Provider OPSYS step has been done and the site later decides to switch to Security OFF, then special steps must be done to ensure the mode remains after a full server shutdown, where edastart -start is used to restart the server.

After the server recycles from the change to OFF, use the Reporting Server browser interface to open the environment configuration file of the server. Select *Workspace*, *Configuration Files*, *Miscellaneous,* and then select *Environment -edaenv*. Next, double-click to edit, add the variable EDAEXTSEC=OFF, and then save.

After the next full server shutdown, be sure to do an edastart -cleardir before restarting the server. This will clear any root-owned files that would prevent a security OFF server from starting.

Preventing Unsecured Server Starts After Upgrades

If the explicit environment variable EDAEXTSEC is set to OPSYS (or ON) and the server cannot impersonate users because it lacks platform-specific authorization steps, the server start aborts and error messages are written to the edaprint log.

This feature prevents an unsecured server start after a software upgrade if any of the required post-upgrade reauthorization steps are missed on a UNIX, IBM i, or z/OS HFS deployment. This is not applicable to other platforms. The setting may be placed in any normal server start-up shell or profile that a site is using or in the server edaenv.cfg configuration file. The messages vary slightly by platform.

The edaprint messages are:

```
Configured security is 'ON' as set by EDAEXTSEC variable.

TSCOM300.PGM has no QSECOFR authority.

Workspace initialization aborted.
```

```
(EDA13171) UNABLE TO START SERVER
```

Starting and Using the IBM i TIBCO WebFOCUS Reporting Server

After configuring for secured mode (if desired), the server is started and managed using the same server startup and Reporting Server browser interface startup steps used for validating the server.

If the server has not been configured for adapters, now is an appropriate time to do so, using the Reporting Server browser interface and the *TIBCO WebFOCUS® Reporting Server Administration* manual. For current information about which adapters are supported, see the *TIBCO WebFOCUS ® Adapter Administration* manual.

To ensure that the Reporting Server browser interface is accessible, the ID that starts the server must be iadmin (the ID that installed the server) and have a code page compatible with the one you specified during installation in *Running ISETUP to Install the TIBCO WebFOCUS Reporting Server Software* on page 264. For more information about code pages, see *Creating User IDs on IBM i* on page 262.

IBM i sites have the option of using QSH commands that run edastart or a CALL TSCOM300 to start and manage a server. CALL TSCOM300 is described in *General Information for an IBM i Installation* on page 275.

The following chart lists commonly used edastart options and functions (the parameters are the same for CALL TSCOM300 usage).

Command and Option	Function
`edastart`	(No parameters) Starts the server with the line mode console to actively view the server log (edaprint). Also allows dynamically issuing edastart options, such as show, traceon, traceoff, quit, and stop. Use your 5250 SysReq key and enter *2* to receive the console command prompt to enter commands. If you are using a PC and 5250 emulator software, see your emulator keyboard map for the equivalent key or use the Help instructions of your emulator on how to create mapping for the SysReq key.
`edastart -start`	Starts the server in the background. Only a short message appears.

Command and Option	Function
`edastart -sstart n`	Starts the server, but waits *n* seconds for actual startup.
`edastart -show`	Shows general status of server and agents.
`edastart -stop`	Stops the server.
`edastart -cleardir`	Removes all temporary directories (and their contents), as well as logs and other files created by the server (including the rmlda*.log files, if active) in EDACONF. If Resource Manager is in use and you want to maintain the rmlda*.log data, backup the rmlda*.log files before using this feature and restore them afterward.
`edastart -quit`	Exits the server line mode console log (edaprint) and returns to the operating system command prompt, but leaves the server running.
`edastart -console`	Re-enters the server line mode console log (edaprint).
`edastart -traceon`	Turns on tracing. May be used at initial startup or after. Tracing should not be turned on (due to overhead) unless there is a problem that needs to be traced. It is always preferable to start traces at initial startup time unless instructed otherwise.
`edastart -traceoff`	Turns off tracing.
`edastart -?`	Displays the full set of edastart server control options.
`edastart -?s`	Displays support information and support related options.

Note: The IBM i commands WRKACTJOB and WRKSBMJOB should not be used to shutdown a running server.

Alternate startup methods, which start the server either with command line options or as a submitted job, are detailed in *General Information for an IBM i Installation* on page 275.

You can use the following methods to start and manage the server environment using either native IBM i CALL syntax or QSH syntax. The directory and library names shown are examples; the actual names you use may differ.

- To start the server from the native IBM i menu command line, use:

```
CALL SRV90/TSCOM300 PARM('-edaconf' '/home/iadmin/ibi/srv90/ffs'
'-start')
```

- To start the server from the native IBM i menu command line with traces, use:

```
CALL SRV90/TSCOM300 PARM('-edaconf' '/home/iadmin/ibi/srv90/ffs'
'-start' '-traceon')
```

- To stop the server from the native IBM i menu command line, use:

```
CALL SRV90/TSCOM300 PARM('-edaconf' '/home/iadmin/ibi/srv90/ffs'
'-stop')
```

- To clear all server resources after a malfunction or after server termination using WRKACTJOB or WRKSBMJOB from the native OS400 menu command line, use:

```
CALL SRV90/TSCOM300 PARM('-edaconf' '/home/iadmin/ibi/srv90/ffs'
'-clear')
```

- To start the server from the command line of a QSH session, use:

```
QSH (starts QSH)
/home/iadmin/ibi/srv90/ffs/bin/edastart -start
```

- To stop the server from the command line of a QSH session, use:

```
QSH (starts QSH)
/home/iadmin/ibi/srv90/ffs/bin/edastart -stop
```

- To start the server as a QSH session, but from the IBM i command line, use:

```
QSH CMD('/home/iadmin/ibi/srv90/ffs/bin/edastart -start &')
```

- To stop the server as a QSH session, but from the IBM i command line, use:

```
QSH CMD('/home/iadmin/ibi/srv90/ffs/bin/edastart -stop')
```

- To start the server as a submitted QSH session on the IBM i command line with a code page (Belgium), use:

```
SBMJOB CMD(QSH CMD('/home/iadmin/ibi/srv90/ffs/bin/edastart
-start &'))
JOB(MYJOB) LANGID(NLB) CNTRYID(BE) CCSID(500)
```

- To start the server as a submitted job on the IBM i command line with a code page (Belgium) and specific job queue, use:

```
SBMJOB CMD(CALL SRV90/TSCOM300 PARM('-edaconf'
'/home/iadmin/ibi/srv90/ffs'))
JOB(MYJOB) LANGID(NLB) CNTRYID(BE) CCSID(500) JOBQ(MYQUEUE)
```

If the -start or -sstart option is:

- **Included in a submitted job,** the full edaprint log is written to the edaprint.log file on disk, and standard short server start-up messages are written to the job system spool file.
- **Omitted from a submitted job,** the full edaprint log is written to the edaprint.log file on disk, and the full edaprint log is written to the job system spool file.

You can view the spool file by means of WRKSBMJOB Option 8 (Work with spooled files) of the PGM-QZSHSH task (start using QSH shell scripts) or of the PGM-TSCOM300 task (start using TSCOM300) task.

You can issue other combinations of standard server control parameters by replacing the option in one of the examples above with another edastart option, such as -traceon, -traceoff, -stop, and -show.

CL and CMD Programs

The process of installing will also create and compile CL and CMD sources so that server functions, such as start, stop, show, and tracing may be activated on the IBM i menu command line. The start command starts the server as a batch job issued to a specified job queue, and is particularly useful for automatically starting a server at boot time or with minimal effort.

The CL and CMD sources are created in a configuration bin directory, then copied into QTEMP and compiled into the user CURLIB (for example, the IADMIN library). The core EDASTART program is generic for any installation and is driven by the defaults within the command files. If you want to have more than one configuration, use separate libraries or rename the programs to prevent overwriting.

The basic commands and functions are listed in the following table.

Command	Function
ISTART	edastart
ISTOP	edastart -stop

Command	Function
ISHOW	edastart -show
ISHOWLOG	edastart -showlog
ITRCON	edastart -traceon
ITRCOFF	edastart -traceoff
ICLEAR	edastart -clear
ICLRDIR	edastart -cleardir
ISAVEDIA	edastart -savediag

To use any of the commands, type the command at the IBM i menu command line. You may also point to other EDACONF directories using the IBM i F4 Prompt mode.

The CL and CMD script may be further customized, or the defaults may be changed, by manually copying the desired file to a library and then changing and recompiling it. Detailed instructions for all steps are contained within the EDASTART CL source. Configuration of a particular language on the Reporting Server browser interface does not currently change the defaults with the file sources. These must be changed manually.

General Information for an IBM i Installation

This section covers general information for an IBM i installation.

Sample Metadata, Data, and Other Tutorial Samples

The Reporting Server browser interface has a feature on the ribbon and on the application tree (under *new*), *Tutorials* (the Create Tutorial Framework page), which has a pull-down for various samples. The Data Migrator desktop interface also has this feature on the application tree.

There are currently about 10 different tutorial/sample selections available on the pull-down select list to match various customer needs. The bulk of the prior IBISAMP sample objects can be generated by selecting the *Create Legacy Sample Tables and Files* tutorial. Other prior IBISAMP Data Migrator sample objects (usually starting with the characters dm*) are now loaded by choosing their respective Data Migrator tutorials. Under the new method, the tutorials/samples may be loaded to any application, not just IBISAMP.

If you are doing just a software refresh, the prior IBISAMP objects will be unchanged (because a refresh does not touch app directories).

Accessing IFS Files and QSYS Libraries

The location of procedure (FOCEXEC) files, Master Files (MASTER), Access Files (ACCESS), and FOCUS database files may be QSYS, IFS, or both. IFS is the preferred location, and is the location used for files created by the HTTP Reporting Server browser interface.

Accessing IFS Files

The native mode of the server is to use the QSH Integrated File System (IFS), which follows standard file syntax as found on UNIX platforms to access files.

Syntax: How to Access IFS Files

IFS access follows the standards of a number of other platforms for FILEDEF, USE, and APPS, but is most like UNIX because the file names follow the same rules. The following is a summary of the respective commands and conventions

```
FILEDEF ddname DISK filename [(options]
USE
filename [AS name]
END

APP MAP MYAPP directory
```

where:

ddname

Is the reference name for the file being opened.

filename

Is either the relative path or full path and the file name (for example, myfile.dat, acctng/myfile.dat, or /home/iadmin/acctng/myfile.dat).

options

Are the available access options, such as LRECL or RECFM.

For more information about FILEDEF options, see the *Stored Procedures Reference*.

name

Is the optional alternate name of the Master File.

directory

Is the full path name of the directory (for example, /home/iadmin/acctng).

Use of a relative path name is not recommended, since this varies with any given connection to the server. Use of environment variables or shortcuts (for example, $HOME or ~) is not supported in any context.

Accessing QSYS Libraries

QSYS access works with libraries and has the following APP, FILEDEF, DATASET, and USE support for accessing existing applications.

The option to use IFS references to QSYS libraries is a native feature of IBM i. IFS references to QSYS names, such MYLIB, use IFS-style references, such as /QSYS.LIB/MYLIB.LIB, which are clearly recognizable as QSYS references.

To map a QSYS library to a WebFOCUS application root directory (APPROOT), use the APP MAP command, as described in *How to Map a QSYS Library to APPROOT* on page 277.

To access or create a FOCUS database in a QSYS library, you need to issue a USE command, as described in *How to Use the USE Command to Access a FOCUS Database* on page 279.

To access a member of a physical file (other than a FOCUS database) in a QSYS library, you can use either:

- **The FILEDEF command,** as described in *How to Use FILEDEF to Access a QSYS Library Member* on page 278.
- **The DATASET attribute** in a Master File synonym, as described in *How to Use DATASET to Access a QSYS Library Member* on page 279.

  Using the DATASET attribute has the advantage of automatically specifying the correct member when you refer to the synonym.

If you issue an explicit FILEDEF command, and a DATASET attribute exists, the FILEDEF command takes precedence.

Creating a HOLD file automatically creates the physical file if it does not already exist. Issuing a -WRITE or -READ statement, however, requires that the physical file exist.

Syntax:

How to Map a QSYS Library to APPROOT

To assist with existing applications outside the pre-defined application root directory (APPROOT), the APP MAP command allows an alias to be assigned to a non-APPROOT directory. This alias becomes a virtual directory under APPROOT so it can then be referenced in an APP PATH command. Mapping does *not* automatically add to the path. It simply makes it available to participate in an APP PATH command. For more information about APPROOT, see the *TIBCO WebFOCUS® Developing Reporting Applications* manual.

In APP mode, the APP MAP command supports use of IFS QSYS library references so that the application name can be used for path search purposes in applications through the APP PATH command. However, the contents of a QSYS mapping are not available from the Reporting Server browser interface.

The syntax for mapping an application to a QSYS library is:

```
APP MAP appname /QSYS.LIB/libname.LIB
```

where:

appname

Is the name of the application.

libname

Is the name of the library to which you are mapping the application. The name must be uppercase.

Syntax: **How to Use FILEDEF to Access a QSYS Library Member**

To use the FILEDEF command to access a member of a physical file in a QSYS library, the syntax is

```
FILEDEF ddname DISK QSYS:library/file(member) (LRECL n
```

where:

ddname

Is the logical name you want to assign to the member. It can be up to eight characters in length, and can contain letters, numbers, and underscores. It must begin with a letter.

When used to associate a data source with a Master File, the ddname must match the name of the Master File.

library

Is the QSYS library in which the file is located.

file

Is the name of the file.

member

Is the name of the member to which you are assigning a logical name.

For the member of a single-member physical file, the member name must be identical to the file name. The operating system shorthand of *FIRST is not a valid alternative.

For a member of a multiple-member physical file, you can specify any member name.

`LRECL`

Specifies the logical record length (LRECL) of the member.

n

Is the local record length.

Syntax: How to Use DATASET to Access a QSYS Library Member

To use the DATASET attribute of a Master File synonym to access a member of a physical file in a QSYS library, the syntax is

```
DATASET = QSYS:library/file(member) (LRECL n
```

where:

library

Is the QSYS library in which the physical file is located.

file

Is the name of the physical file.

member

Is the name of the member that you want to access.

`LRECL`

Specifies the logical record length (LRECL) of the member.

n

Is the local record length.

Syntax: How to Use the USE Command to Access a FOCUS Database

To access a FOCUS database, the syntax is

```
USE
library/file[(member)] [AS name] [NEW]
END
```

where:

library

Is the QSYS library in which the physical file is located.

file

Is the name of the physical file.

member

Is the name of the member that you want to access. If you omit the name, it defaults to the name of the physical file.

This is the default name used by WebFOCUS to refer to the member. You can override it by specifying AS *name*.

AS

Defines a logical name that you can use instead of the member name.

name

Is the logical name you want to assign to the member.

NEW

Creates the member, and also creates the physical file if it does not exist. The data source is created as a member of a physical file starting with "F$". The file is created in the specified QSYS library.

This construction allows you to organize multiple FOCUS databases within a single QSYS physical file with a functional name, such as FOCUS, ACCTG, SHIPPING, AR, or AP; or as individual QSYS physical file members, such as SHIP(SHIP), AR(AR), AP(AP), or SHIP(FOCUS).

For more information about the USE command, see the *TIBCO WebFOCUS® Developing Reporting Applications* manual.

Generating a Trace on IBM i

If you encounter a server problem, you can run a set of traces that will help you assess the problem, and, if necessary, communicate it to Customer Support for further troubleshooting. This topic describes trace options and provides instructions for creating the traces.

There are two types of traces you can run to troubleshoot a problem:

- **A server trace,** in which you trace an agent that is running in a server context.
- **A non-server trace,** in which you trace an agent that is running outside a server context, that is, an agent that is running in standalone mode.

Under normal conditions, applications are run in a server context. However, if you run your trace in a non-server context (that is, you run a non-server trace), and produce the necessary diagnostic information, you can significantly reduce the amount of material that needs to be reviewed. Running a non-server trace also rules out server communications as a cause of a problem.

If you prefer to use native IBM i commands, a number of CMD/CL programs are created during installation in the server administrator comment library and can be used to start traces, turn traces off, and perform edastart -savediag functions. The commands are, respectively, ITRCON, ITRCOFF, and ISAVEDIA. To use them (instead of using edastart under QSH), enter the required command and press *F4* for prompted mode, then edit parameters, as needed, and press Enter. For related information, see *CL and CMD Programs* on page 274.

Procedure: How to Generate a Server Trace

To generate a server trace:

1. Turn tracing on by doing one of the following:
   - ❑ Go to the Reporting Server browser interface menu bar, select the Main Reporting Server browser interface *Other Options* control icon and then *Enable Traces*.
   - ❑ Start the server by issuing the following command:

     ```
     edastart -traceon
     ```

     You must preface edastart with the appropriate path, or place the directory in your system PATH variable.
2. Reproduce the problem.
3. Stop the server.
4. Issue the following command:

   ```
   edastart -savediag
   ```

5. Respond to the prompts to capture, and optionally archive and ship diagnostic information.

   Diagnostic information will commonly contain user data. If the release of that data is considered a security concern when shipping to Customer Support, the -savediag feature also allows a diagnostic to be saved and shipped later to allow the site the opportunity to review and cleanse the traces of data of this nature before shipping.

Procedure: How to Generate a Non-Server Trace

To generate a non-server trace:

1. Create a directory under APPROOT to reproduce the problem.
2. Copy any files required for the reproduction to the directory.
3. Switch to the directory.
4. Reproduce the problem using edastart -traceon and one of these switches -t, -x, or -f.
5. Switch to a directory other than the problem reproduction directory.
6. Issue the following command

   ```
   edastart –savediag
   ```

   You must preface edastart with the appropriate path, or place the directory in your system PATH variable.
7. Respond to the prompts to capture, and optionally archive, diagnostic information.

   Diagnostic information will commonly contain user data. If the release of that data is considered a security concern when shipping to Customer Support, the -savediag feature also allows a diagnostic to be saved and shipped later to allow the site the opportunity to review and cleanse the traces of data of this nature before shipping.

Third-Party Software and Licenses

All third-party and TIBCO Software, Inc. license information is available on the Reporting Server browser interface by clicking the Help (?) menu, then either *TIBCO Software, Inc.* or *3rd Party Licenses*.

Troubleshooting for IBM i

To troubleshoot an installation problem, identify your problem in the following list, and follow the link to a description of the solution.

If you cannot find your problem described in the list, and cannot resolve it yourself, contact Customer Support.

Problems:

- ❑ The server starts in safe mode (as indicated by a message in the Reporting Server browser interface at start-up).

  See *Problem: The Reporting Server Starts in Safe Mode* on page 283.

- ❑ A server start request partly fails with *JVM not found* messages are written to edaprint.log.

See *Problem: Java Listener Fails to Start With JVM not found Messages Written to the Log* on page 283.

Reference: Problem: The Reporting Server Starts in Safe Mode

Problem: The server starts in safe mode. The Reporting Server browser interface home page displays a message stating that the server is in safe mode and describing what triggered it.

Cause: A common cause for the server starting in safe mode is a problem with the server administrator ID password. For example, the password may have been updated on the operating system but not on the server, so the encrypted copy of the password stored by the server is out of synchronization with the password on the operating system.

Solution: The server administrator can click the *fix* hyperlink, which is displayed under the problem description, to display the relevant pane and resolve the problem.

For example, if the problem is that the server administrator password is out of synchronization:

1. Click the *fix* hyperlink displayed under the problem description.
2. In the left pane, open the *Users* folder, then the *Server Administrator* folder.
3. Click your user ID and select *Properties* from the pop-up menu.

   The Access Control pane is displayed on the right.
4. Type the correct operating system password in the *Password* field, and type it again in the *Confirm Password* field.
5. Click *Save and Restart*.

   The Security Mode pane opens on the right.
6. Click the Home icon in the menu bar to return to the Reporting Server browser interface home page.

Reference: Problem: Java Listener Fails to Start With *JVM not found* Messages Written to the Log

Problem: The listener start request fails with *JVM not found* messages written to the edaprint.log file.

Cause: If the server cannot find the Java Virtual Machine (JVM), the JSCOM Listener will not be able to start, and messages will be written to the server log stating that the JVM cannot be found.

Solution: Set up the JVM as described in *JVM Requirements for Java Services* on page 256.

Reference: Problem: Secured Reporting Server Starts Unsecured or Does not Start after Upgrade

A server will implicitly attempt to start unsecured if proper authorization steps have not been completed. Starting the server normally clears edatemp. If prior edatemp files exist (and authorization has not been done), start-up will fail due to an inability to clear the directory. However, if an edastart -cleardir command was issued just before the upgrade, there is nothing to clear, no error occurs, and the server starts. If the server starts and is not inspected after the initial start-up, the server being in the wrong mode may go unnoticed.

The proper solution is to add proper authorizations after an upgrade, as described in *How to Satisfy Security Provider OPSYS Requirements* on page 269, and restart the server. A new safety measure has also been added. If the environment variable EDAEXTSEC is set to OPSYS explicitly, and a server lacks authorization, it will not start (see *Preventing Unsecured Server Starts After Upgrades* on page 270 for details).

Reference: Problem: CREATE SYNONYM Fails for Excel 2007 (or Higher) Workbooks

Problem: Using the Adapter for Excel Direct Retrieval, the CREATE SYNONYM process for Excel 2007 (or higher) Workbook .xlsx files fails on i5 V5R4.

Cause: The server uses Apache poi-ooxml-schemas (a light version of Java ooxml-schemas) to interpret Excel files. However, poi-ooxml-schemas fail on i5 V5R1 (but work on higher operating system levels). This has been investigated and determined to be outside the server code. It works if the ooxml-schemas jar file is substituted for the poi-ooxml-schemas jar file, or if the JVM is forced into interpret mode.

Solution: If you need to create synonyms from Excel 2007 .xlsx files on i5 V5R4, the simplest solution is to add a JVM property of -Dos400.run.mode=interpret to the Java Listener properties, rather than substituting jar files.

Appendix A

Caching Support for Node.js

Node Package Manager (npm) is a package manager for the Reporting Server Node.js® caching server run-time environment. Node Package Manager and Node.js are third-party software packages that should, preferably, be installed before you install the Reporting Server so that automatic configuration and usage occurs.

On Windows, npm and Node.js are packaged together. Other platforms typically require npm to be installed first and then for npm to install Node.js second.

Note: Throughout this topic, the npm software and Node.js caching server environment are referred to as Node.js.

In this appendix:

Node.js Installation and Configuration

When Node.js is installed and running, and a Reporting Server is configured to use it, In-Document Analytics reports are cached under Node.js and can be accessed independent of the Reporting Server.

If Node.js is installed on Windows or Linux/UNIX and is detected as available during Reporting Server installation time, the In-Document Analytics Caching feature will automatically be configured in the EDACONF etc/ar_v2 directory and registered in the edaserve.cfg file, using a port in the reserved port range for the Reporting Server (HTTP port number plus 5).

The In-Document Analytics Caching feature can also be configured post-installation, with a few simple steps as outlined below, if:

- Node.js was not detected during installation, due to not being installed or not added to the PATH environment variable.
- Node.js configuration failed during automatic configuration.
- Reporting Server binaries were upgraded to a level that supports Node.js caching and the earlier Reporting Server did not support Node.js caching or was not configured.

Node.js Process

Starting the Reporting Server checks if the configured Node.js port is already available, and therefore Node.js is already running. If the Node.js process is not running, the Reporting Server will start the Node.js caching server process. The Node.js caching server process has the name *node* or *node.exe*, depending on your platform. If the Reporting Server starts the Node.js process, it will also stop the process on server shutdown. In this way, you may control your own Node.js usage or let the Reporting Server be in control.

By default, the Reporting Server process is configured to point to a URL for a local Node.js In-Document Analytics Caching process. As such, the Node.js URL may be reconfigured to run against a remote machine, provided the remote machine is properly configured and running. If a remote URL is used, you are expected to start the remote Node.js server process before the local Reporting Server, as the local server cannot start a remote Node.js process. The simplest form of remote configuration is to point to another Reporting Server Node.js In-Document Analytics Caching URL and let that server's start-up control the Node.js start-up. A more complex variation is to create a *freestanding* Node.js In-Document Analytics Caching environment with no Reporting Server involved and then point any number of Reporting Servers to it. For more information, see *How to Manually Configure a Freestanding Node.js In-Document Analytics Caching Environment on a Separate Machine* on page 291.

Note: On Linux/UNIX, if the installation ID has a non-writable root-owned $HOME/.npm directory tree, the automatic configuration, as well as manual configuration, will fail for both the internal *npm install* step and the Reporting Server's Node.js startup. The solution for this is to delete the $HOME/.npm directory tree or use an installation ID that does not have a $HOME/.npm directory.

Node.js Prerequisites

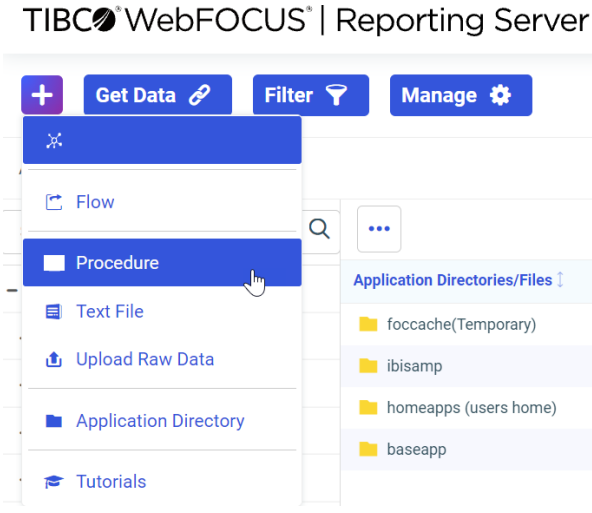
The following are the prerequisites for Node.js:

- **For Windows.** Download and run the Node.js Windows 64-bit installer from *https://nodejs.org/en/download*. You can use any recent release. Take the default installation options. Do not deselect the *Add to PATH* option and do *not* check *Automatically install the necessary tools* option, unless you have need for this option for other software that may also be using this Node.js instance.

- **Linux/UNIX.** Most Linux/UNIX vendors will have their own npm and Node.js installer. Any recent release may be used. The installation steps may be found by performing an internet search on *install nodejs on {distribution name such as RedHat or Ubuntu}*. The npm portion is typically a separate step, but noted within the Node.js package instructions.

Procedure: How to Verify the Node.js In-Document Analytics Caching Environment is Running

1. Start the Reporting Server, if it is not already running.
2. Sign in to the Reporting Server browser interface using any ID that has open (create) procedure authority.
3. Click the plus button + and select *Procedure* from the menu to create a new procedure, as shown in the following image.



4. In the procedure text window, type the following command:

```
EX ADAPTIVP NODEJS
```

An example of the procedure text window is shown in the following image.

5. Click the run button ▶.

Note: There is no need to save the procedure first.

An In-Document Analytics-based report should appear, as shown in the following image.

1 - 57 of 157 records Page: 1 / 3

AR NODEJS Caching Manager Test								
Table of Supported Currencies								
Currency	ISO code	Symbol	Symbol hexadecimal	Symbol Char-length	Symbol Byte-length	Decimals	Position in report	Non-UTF Symbol
USA dollar	USD	$	24	1	1	2	4	
Eurozone euro	EUR	€	80	1	1	2	3	
Japanese yen	JPY	¥	a5	1	1	0	2	
British pound sterling	GBP	£	a3	1	1	2	1	
United Arab Emirates dirham	AED			0	0	2	0	
Afghan afghani	AFN	Afs	41, 66, 73	3	3	2	0	Afs
Albanian lek	ALL	Lek	4c, 65, 6b	3	3	2	0	
Armenian dram	AMD			0	0	2	0	
Netherlands Antillean guilder	ANG	ƒ	83	1	1	2	0	f

If the Node.js process is not working, a *refuse to connect* message containing the URL host name will appear.

If the test fails, check for *nodejs startup failed* in the edaprint file, during initial startup of the Reporting Server. This typically happens if Node.js was not installed, Node.js is not on the PATH, or the initial automatic or manual configuration failed. Follow the steps in *How to Add Node.js Configuration to a Reporting Server Not Originally Configured With Node.js* on page 289 to investigate and correct.

Another possible failure is the Node.js process is no longer running. To check:

- On Linux/UNIX, issue the following command to limit output:

  ```
  ps -edf | grep "node"
  ```

  Look for processes, such as:

  ```
  webfocus 122264 122253 0 10:20 ? 00:00:00 sh -c set DEBUG=http,express:*
  & node --max-old-space-size=16192 server.js "--PORT=8126"
  webfocus 122266 122264 0 10:20 ? 00:00:00 node --max-old-space-
  size=16192 server.js --PORT=8126
  ```

- On Windows Task Manager, find the process icon Node.js JavaScript Runtime and turn on the Task Manager command line column, which will show something similar to the following:

  ```
  node --max-old-space-size=16192 server.js --PORT=8126
  "C:\Program Files\nodejs\node.exe" "C:\Program Files\nodejs\\node_modules
  \npm\bin\npm-cli.js" run mystart --prefix=c:\ibi\srv90\wfs\etc
  \ar_v2\cachemanager -- --PORT=8126
  ```

- Check for issues, such as a wrong port number or the process is not running. If not running, check the EDACONF edatemp/npmrun.trc file for the possible reason.

Procedure: How to Add Node.js Configuration to a Reporting Server Not Originally Configured With Node.js

Note: Be prepared to recycle the Reporting Server as part of this procedure. You may want to do this during scheduled maintenance down time.

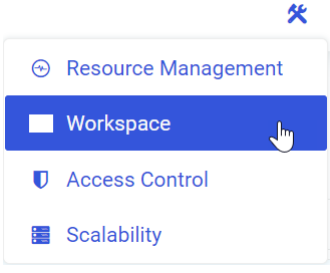
1. Sign in to the Reporting Server browser interface, using the server administrator ID.
2. Click the plus button and select *Procedure* from the menu to create a new procedure.
3. In the procedure text window, type the following command:

   ```
   EX ADAPTIVP NODEJS,REBUILD
   ```

4. Click the run button ▶.

   Note: There is no need to save the procedure first. It is normal to see warnings and npm update failed messages. Any other fail messages should be investigated and reported.

5. Navigate to the Workspace page by clicking the *Tools* icon in the banner and selecting *Workspace*, as shown in the following image.



6. Under Data Services on the tree, open the *Configuration Files* folder, and double-click *Workspace - edaserve.cfg* to edit the file.
7. In the [Workspace] section add, if not already present, or correct the following nodejs_url line:

   ```
   nodejs_url = http://{hostname}:{port}
   ```

where:

hostname

May be localhost or a specific host name, with or without the domain portion. The host name does not need to be the same machine as the Reporting Server, but the automatic Node.js start feature will not work if it is not on the same machine. If a remote Node.js configuration is in use, it is expected to be running before the Reporting Server is started.

port

Is typically the Reporting Server HTTP port number plus 5, if automatic configuration was successful. For example, HTTP port number 8101 would be 8106 for Node.js, but it may be any free port. The Node.js default port number is 8090, if you wish to skip the "–PORT=####" parameter in the manual start instructions.

8. Click the Save button , which will save and restart the Reporting Server. If the nodejs_url line was already present and did not need edits, still click the *Save* button to force a restart of the Reporting Server.

Procedure: How to Manually Start and Stop Node.js In-Document Analytics Caching

To manually start Node.js In-Document Analytics Caching, you will need to know:

- Where the *npm* command is installed on your machine if it is not on $PATH (Linux/UNIX) or %PATH% (Windows) and add that path to the npm commands below (for example, /usr/local/bin/npm).
- Full path directory for the server EDACONF etc/ar_v2/cachemanager directory.
- A writable directory for output. This is normally in the EDACONF edatemp directory when a Reporting Server starts Node.js. This directory is not advisable in a privately started environment. From an organizational perspective, EDACONF would be a reasonable location.

The following are examples of starting Node.js In-Document Analytics Caching. Replace the applicable paths and port number with your paths and port number.

Note: These commands must be typed on a single line.

For Linux/UNIX:

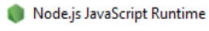
```
npm run mystart --prefix=/webfocus/ibi/srv90/wfs/etc/ar_v2/cachemanager --
--PORT=8126 > /webfocus/ibi/srv90/wfs/npmrun.trc 2>&1 &
```

For Windows:

```
npm run mystart --prefix=c:\ibi\srv90\wfs\etc\ar_v2\cachemanager -- --
PORT=8126 > c:\ibi\srv90\wfs\npmrun.trc 2>&1
```

On Linux/UNIX, a ps -edf command will show something similar to the following:

```
webfocus 122264 122253 0 10:20 ? 00:00:00 sh -c set DEBUG=http,express:* &
node --max-old-space-size=16192 server.js "--PORT=8126"
webfocus 122266 122264 0 10:20 ? 00:00:00 node --max-old-space-size=16192
server.js --PORT=8126
```

On Windows Task Manager, find the 

process icon and turn on the Task Manager command line column, which will show something similar to the following:

```
node --max-old-space-size=16192 server.js --PORT=8126
"C:\Program Files\nodejs\node.exe" "C:\Program Files\nodejs\\node_modules
\npm\bin\npm-cli.js" run mystart --prefix=c:\ibi\srv90\wfs\etc
\ar_v2\cachemanager -- --PORT=8126
```

The following are examples for stopping Node.js In-Document Analytics Caching. Replace the applicable paths and port number with your paths and port number.

Note: These commands must be typed on a single line.

For Linux/UNIX:

```
npm stop mystart --prefix=/webfocus/ibi/srv90/wfs/etc/ar_v2/cachemanager > /
webfocus/ibi/srv90/wfs/npmrun.trc 2>&1 &
```

For Windows:

```
npm stop mystart --prefix=c:\ibi\srv90\wfs\etc\ar_v2\cachemanager > c:\ibi
\srv90\wfs\npmrun.trc 2>&1
```

Procedure: How to Manually Configure a Freestanding Node.js In-Document Analytics Caching Environment on a Separate Machine

Note: This assumes Node.js is already installed and on the PATH of the separate machine.

1. Navigate to the EDAHOME etc/etc/ar_v2 directory on a Reporting Server where Node.js In-Document Analytics Caching is supported.
2. Archive, using zip or tar, the following files for transfer to the target new machine:
   - ar_v2/cachemanager/*.js
   - ar_v2/cachemanager/package.json
   - ar_v2/cachemanager/template/stored.html

3. Restore the files to a writable directory on the new machine, for example, on Linux/UNIX:

   ```
   $HOME/webfocus/ar_v2
   ```

4. Edit the ar_v2/cachemanager/config.json file.

   - On the redirect_host line, change the redirect_host http value, usually localhost, to the actual full DNS machine name, for example:

     ```
     "redirect_host":"http://mymachine.mycompany.com"
     ```

   - On the cache_port line, change the cache_port number to the port number you want to use for the configuration, matching the port used by the Reporting Server nodejs_url value.

5. Change the directory to the cachemanager directory, for example, on Linux/UNIX:

   ```
   cd $HOME/webfocus/ar_v2/cachemanager
   ```

6. Run the following command:

   ```
   npm install
   ```

7. Review the installation for any errors. It is normal to see warnings and npm update failed messages. Any other fail messages should be investigated and reported.

   Note: A root-owned $HOME/.npmrc directory is typically a reason for failure and should be deleted beforehand or, another ID, without a root-owned $HOME/.npmrc directory, should be used.

8. Start and stop the environment, as described in *How to Manually Start and Stop Node.js In-Document Analytics Caching* on page 290, using the applicable paths and ports.

Procedure: How to Block Automatic Node.js Startup By the Reporting Server

If you want to stop the server from attempting automatic Node.js startup, even though it is configured, you can set the BLOCK_NODEJS environment variable to a value of Y.

The best place to do this is in the EDACONF bin/edaenv.cfg file by adding the "BLOCK_NODEJS=Y" line, and saving and restarting the Reporting Server. It may also be set as an environment variable, and exported on Linux/UNIX, before Reporting Server startup, although this is less convenient for Windows Reporting Servers running as a service, as it needs to be set up at a system level.

Note: The edaenv.cfg file may not exist. If this is the case, create the file and add the "BLOCK_NODEJS=Y" line.

Legal and Third-Party Notices

Index

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

Z