FUJITSU

FUJITSU Software
Interstage Application Server

Operator's Guide

Windows/Solaris/Linux

B1WS-1086-03ENZ0(00)
April 2014

Preface

Purpose of this Document

This manual documents management of the Interstage Application Server using the Interstage Management Console (hereafter abbreviated as IMC). Where the necessary functionality is unavailable through the IMC, command line operation is described.

Intended Readers

This manual is intended for users who manage and operate Interstage Application Server and users who develop distributed applications with Interstage.

It is assumed that readers of this manual have a basic knowledge of:

- The Internet
- Object-oriented technology
- Distributed object technology (CORBA)
- Relational databases
- AIM on a global server
- Basic knowledge of the OS used

Structure of This Manual

The structure of this manual is as follows:

Chapter 1 Operator's Guide Overview

This chapter provides and overview to concepts and operations of the Interstage Application Server as used through the Interstage Management Console.

Chapter 2 Configuring the Interstage Management Console

This chapter provides details of configuring and starting the Interstage Management Console.

Chapter 3 Using the Interstage Management Console

This chapter describes how to use the Interstage Management Console and how that usage is presented in this manual.

Chapter 4 System

This chapter describes the Interstage System concept and related operations.

Chapter 5 Site Windows32/64 Solaris32 Linux32/64

This chapter describes the multi-server Site concept and related operations.

Chapter 6 Server Groups Windows32/64 Solaris32 Linux32/64

This chapter describes the multi-server Server Groups concept and related operations.

Chapter 7 Resources

This chapter provides information on Resources configurable from the Interstage Management Console.

Chapter 8 Services

This chapter provides information on Services configurable from the Interstage Management Console.

Chapter 9 WorkUnits General and IJServer

This chapter describes the WorkUnits General and IJServer specific concepts and operations.

Chapter 10 CORBA WorkUnits

This chapter describes the CORBA WorkUnits concept and related operations.

Chapter 11 Security

This chapter provides details on Security of the Interstage Application Server and in particular operations performed through the Interstage Management Console.

Chapter 12 Maintenance (Resource Backup)

This chapter provides details of Maintenance operations for the Interstage Application Server.

Chapter 13 Performance Monitoring

This chapter provides details of Performance Monitoring tools available for the Interstage Application Server.

Conventions

Abbreviations

Read occurrences of the following Components as their corresponding Service.

Service	Component
CORBA Service	ObjectDirector
Component Transaction Service	TransactionDirector

Notations

Convention	Description	Example
	Indicates that this product (32-bit) is running on Windows.	Windows32/64 Repository server definition files are all files under: C:\Interstage\F3FMsso\ssoatcsv\conf Solaris32/64 Linux32/64 Repository server definition files are all files under: /etc/opt/FJSVssosv/conf
Windows32	Indicates that this product (64-bit) is running on Windows.	
Windows64	Indicates that this product (32/64-bit) is running on Windows.	
Windows32/64	Indicates that this product (32-bit) is running on Solaris.	
Solaris32	Indicates that this product (64-bit) is running on Solaris.	
Solaris64	Indicates that this product (32/64-bit) is running on Solaris.	
Solaris32/64	Indicates that this product (32-bit) is running on Linux.	
Linux32	Indicates that this product (64-bit) is running on Linux.	
Linux64	Indicates that this product (32/64-bit) is running on Linux.	
Linux32/64	Indicates that this product (32-bit) is running on Windows.	
On screen controls	In procedures, onscreen controls including buttons, radio button options, list options, labels associated with these controls are bolded.	Click the **Create** button to...
Commands	Commands are formatted in italics.	The file is generated by the *otssetup* command.
`Code`	Code is on a beige colored background. Typically this is used to present text such as command line strings, or file content.	`kill `cat PID_FILE``
root node > child node level 1> child node level 2	Tree path to the active folder is given as folders separated by angle brackets.	Interstage Management Console > Site > Resource > Connection Factory
[user defined item name]	Square brackets are used to represent user defined items represented by folders on the Interstage Management Console navigation tree.	Interstage Management Console > Site > Resource > Connection Factory > [data source name]
item1 | item2	The vertical bar character '|', is used to denote that the operation being described is valid for item1 or item 2. Folders in the	Interstage Management Console > Site > Resource > JMS > ConnectionFactory > QueueCF | TopicCF >

Convention	Description	Example
	Interstage Management Console navigation tree representing items 1 and 2 are given.	
[Link name]	Descriptions for link names are bolded and enclosed in square braces.	Click the **[Show]** link to access detailed settings.
Note Note 1 Note 2	Notes are used to highlight important information relating to the task being performed or the concept being described, and to clarify or expand on the information given.	Note MIB is a management information area that has been defined for managing the system and TCP/IP information.

Export Controls

Exportation/release of this document may require necessary procedures in accordance with the regulations of the Foreign Exchange and Foreign Trade Control Law of Japan and/or US export control laws.

Trademarks

Trademarks of other companies are used in this documentation only to identify particular products or systems.

Product Trademarks/Registered Trademarks
Microsoft, Active Directory, ActiveX, Excel, Internet Explorer, MS-DOS, MSDN, Visual Basic, Visual C++, Visual Studio, Windows, Windows NT, Windows Server, Win32 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
Oracle and Java are registered trademarks of Oracle and/or its affiliates.

Other company and product names in this documentation are trademarks or registered trademarks of their respective owners.

Copyrights

April 2014 Third Edition
November 2012 First Edition

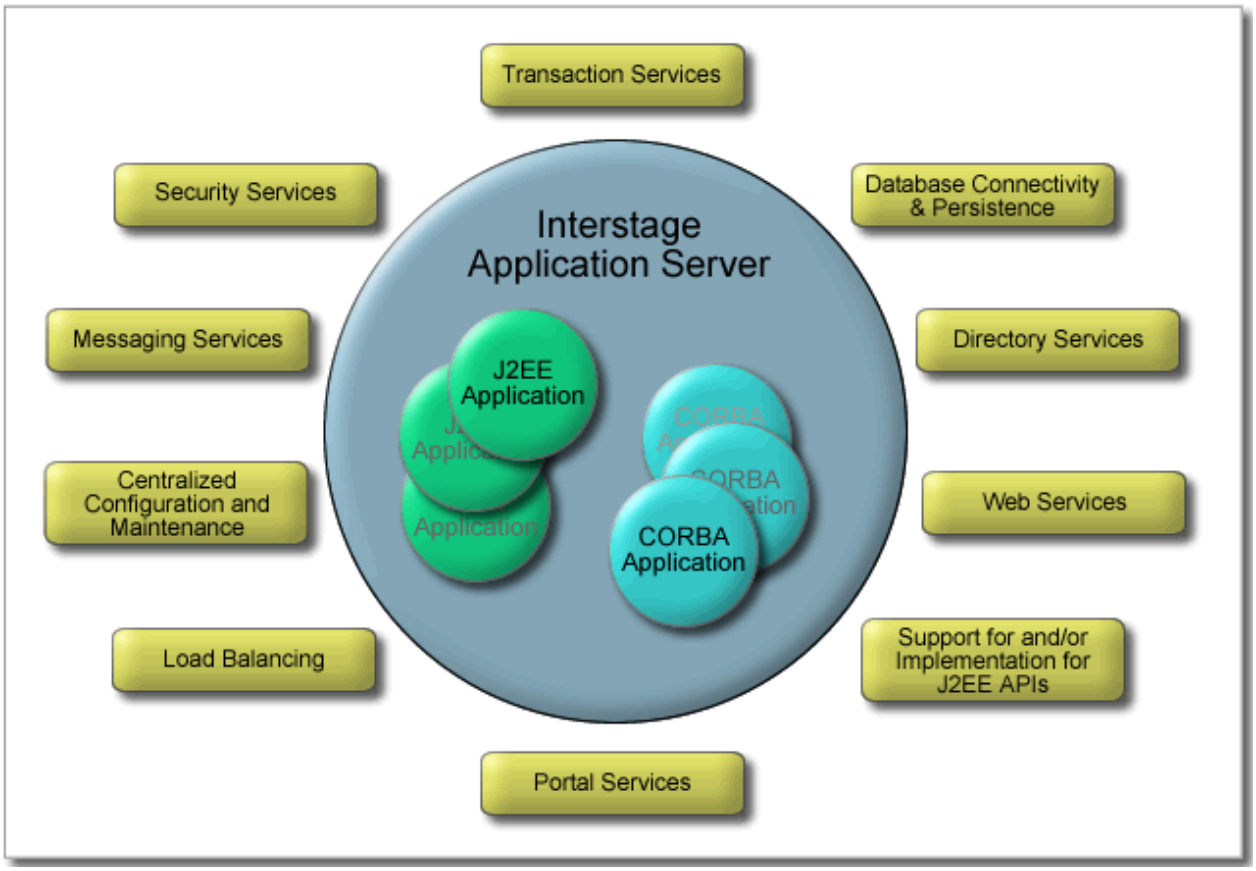
Contents

Chapter 1 Operator's Guide Overview

1.1 Introduction

The Interstage Application Server is a high performance and scalable J2EE and CORBA compliant Application Server. Interstage Application Server provides the infrastructure required for hosting and managing J2EE and CORBA Server-side applications including as shown in the diagram.

Figure 1.1 Interstage Application Server and services provided



Included with the Interstage Application Server is a web based graphical tool for management of the Interstage Application Server and deployed applications. This is called the Interstage Management Console.

Interstage Management Console (IMC)

The Interstage Management Console is a web-based application providing a GUI to configure and manage Interstage Application Servers in both standalone and multi-server environments. By logging into the Interstage Management Console using a web browser, an operator can configure and manage services, resources and applications deployed on any server in the organization.

This Operator's Guide focuses on management of the Interstage Application Server through the Interstage Management Console (IMC) for both standalone and multi-server environments. Where operations are not available through the IMC, command line procedures are described.

This Overview section outlines:

- 1.2 What can be Configured and Managed in Interstage Application Server
- 1.3 Setting up Interstage Application Server

- 1.4 Operating the Interstage Application Server
- 1.5 Overview of Deploying Applications
- 1.6 Configuring a Multi-server Environment
- 1.7 Monitoring Interstage Application Server
- 1.8 Maintenance
- 1.9 Sample J2EE Applications

Note

- Two editions of the Interstage Application Server are available:
  - Interstage Application Server Standard-J Edition
  - Interstage Application Server Enterprise Edition

  Differences in operations are noted in the appropriate sections.

1.2 What can be Configured and Managed in Interstage Application Server

The following items can be configured for Interstage Application Server:

- 1.2.1 Interstage Application Server Type
- 1.2.2 System
- In a Multi-server Environment:
  - 1.2.3 Site
  - 1.2.4 Server Groups
- 1.2.5 Resources
- 1.2.6 Services
- 1.2.7 WorkUnits
- 1.2.8 Security

In addition, applications such as J2EE and CORBA applications can be deployed as well as configured.

1.2.1 Interstage Application Server Type

The Interstage Application Server can be configured to perform one of four roles:

Standalone Server

A Standalone Server is an instance of the Interstage Application Server that does not share its resources, services or WorkUnits with other Application Servers.

Admin Server Windows32/64 Solaris32 Linux32/64

An Admin Server is an instance of Interstage Application Server that is used to manage a Site including all Managed Servers and Server Groups.

Reserved Managed Server Windows32/64 Solaris32 Linux32/64

A Reserved Managed Server is an instance of Interstage Application Server that will only be used as part of a Server Group. All Managed Servers in a Server Group share the same configuration.

Independent Managed Server Windows32/64 Solaris32 Linux32/64

An Independent Managed Server is an instance of Interstage Application Server whose primary purpose is to be managed individually as part of a Site or form the basis of a Server Group. It can be managed as part of the site, but is configured and managed similar to a Standalone Server. If it is then to be used to form the basis of a Server Group, it MUST be the first Server added to that group, it cannot be added as a supplementary member of the group. Only Reserved Managed Servers can be added as supplementary members to a group.

1.2.2 System

System refers to Interstage specific system features (non application specific features). This includes common controls like starting and stopping of IJServers / Server Groups, defining / updating high level settings like CORBA service parameters, Naming service parameters etc, enabling / disabling event services, transaction services, and configuring repository path and size,

On a Standalone Server, System provides overall control and common definitions of the server itself. On an Admin Server, System provides the same level of facilities for each server group. The three major System areas of interest are:

1. System Status
   - On a Standalone Server this shows the current status of Interstage Application Server and its services, and on an Admin Server it provides the same level of support for each Server Group.
   - Provides controls to start, stop and refresh Interstage and all associated services.
2. Environment Settings

   This facilitates definition of common (system wide) and service specific settings for the following services for the server (in the case of Standalone Servers) or for Server Groups (in the case of Admin Servers):
   - Detailed System settings
   - CORBA Service settings
   - Naming Service settings
   - Interface Repository settings
   - Event Service settings
   - Transaction Service Settings
   - Servlet Service settings (Standalone Server only)
   - EJB Service settings (Admin Server only)
3. Repository

   The Repository path and size can be configured for the server (in the case of Standalone Servers) or the Server Group (in the case of Admin Servers).

For details on system management in Interstage, refer to the 'System' chapter.

1.2.3 Site Windows32/64 Solaris32 Linux32/64

A Site is the logical grouping of everything managed by an Admin Server. This includes all Interstage Application Servers, WorkUnits, Applications, Resources and Services managed by the Admin Server. WorkUnits, Resources and Services can be created on the Admin Server, and deployed to site participants.

For details on site creation and management in Interstage, refer to the 'Site' chapter.

1.2.4 Server Groups Windows32/64 Solaris32 Linux32/64

When applications have to scale, more Application Servers may be used to provide the scalability. The Admin Server can be used to prepare the common configurations in a logical entity called the Server Group. When an Application Server is added to a Server Group, the Admin Server copies all the necessary configuration information including the applications to the appropriate locations on the target Server.

For details on server group creation and management in Interstage, refer to the 'Server Groups' chapter.

1.2.5 Resources

A Resource is a component that enables interaction with a Service. Multiple instances of a Resource can be created, configured and/or managed by Interstage.

The following Resources are managed by Interstage:

- JDBC
- JMS
  - ConnectionFactory
  - Destination
- JavaMail
- Connector.

For details on resource creation and management in Interstage, refer to the 'Resources' chapter.

1.2.6 Services

Services provide infrastructure for WorkUnits and applications deployed on them.

Some Services are common to a Site while others are specific to a Server Group, Independent Managed Server or Standalone Server.

Services that can be configured from the Interstage Management Console include:

- Interstage System Services
  - Component Transaction Service (TD)
  - CORBA Service
  - Naming Service
  - Interface Repository Service
  - Interface Repository Service (ValueIF)
- Web Server
- Event Service
  - Stores
  - Event channels.
- Transaction Service (OTS) Windows32/64 Solaris32 Linux32/64
- Transaction Service (JTSRMP)

For details on services management in Interstage, refer to the 'Chapter 4 System' and 'Chapter 8 Services chapters.

1.2.7 WorkUnits

An application requires resources and services to operate. Usually, a set of applications together provide specific business functionality. A WorkUnit is a logical grouping of one or more deployed applications, resources and services that can be started, stopped and monitored independently.

WorkUnits can be deployed to any type of Application Server as follows:

Standalone Server:	WorkUnit is local to the Standalone Server it is deployed to.
Admin Server:	WorkUnit can be deployed from an Admin Server to: - An Independent Managed Server The WorkUnit is local to this Managed Server. - A Server Group The WorkUnit is deployed to all Managed Servers in the Server Group.

In a multi-server environment, a WorkUnit can be split across multiple Interstage instances, e.g. Web Application on one, EJB on another etc. This configuration can be achieved and maintained from an Admin Server. This is referred to as a multi-level WorkUnit.

For details on Interstage WorkUnit creation and management, refer to the 'WorkUnits General and IJServer' chapter.

1.2.8 Security

Interstage security items that can be accessed through the IMC include:

- Deployed application security
- Interstage Directory Service
- Single Sign-on
- IMC User Authentication

For details on configuring Security through the IMC, refer to the 'Security' chapter.

For details on security configuration and management in Interstage Application Server, refer to the Interstage Security Manual.

1.3 Setting up Interstage Application Server

Interstage setup involves:

- Configuring the Interstage Management Console

  For details, refer to the chapter 'Configuring the Interstage Management Console'.

- Configuring Interstage Application Security

  For details, refer to the 'Security' chapter.

- Customizing the System

  For details, refer to the chapter 'Configuring the Interstage Management Console'.

1.4 Operating the Interstage Application Server

The basic operations for Interstage usage are:

- Starting the Server

  The Interstage Application Server is started automatically following installation. To restart Interstage after a stop:

- Standalone

  In the Navigation frame, click Interstage > Interstage Application Server > System. In the Operations frame, click the **Start Interstage** button.

- Multi-server

  From the Application Management tab, click Interstage > Interstage Application Server > System. In the Operations frame, check the checkbox corresponding to the systems to be started, and click the **Start** button.

  For further details, refer to 'Starting Interstage' in the 'System' chapter.

- Stopping the Server

  To stop Interstage:

  - Standalone

    In the Navigation frame, click Interstage > Interstage Application Server > System. In the Operations frame, click the **Stop Interstage** button.

  - Multi-server

    From the Application Management tab, click Interstage > Interstage Application Server > System. In the Operations frame, check the checkbox corresponding to the systems to be stopped, and click the **Stop** button.

    For further details, refer to '4.2.4 Stopping Interstage' in the 'System' chapter.

- Configuring Server Settings

  To configure the Interstage Application Server settings:

  - Standalone

    In the Navigation frame, click Interstage > Interstage Application Server > System. In the Operations frame, click the **Update System Settings** tab and update the System settings as required. For further details, refer to 'Configuring System Services' in the 'Services' chapter.

  - Multi-server

    From the Application Management tab, click Interstage > Interstage Application Server > System > [server group | independent managed server]. Click the Environment Settings tab and update the System settings as required.

    For further details, refer to 'Configuring System Services' in the 'Services' chapter.

- Monitoring Operation

  The Interstage SystemWalker tool is used for extensive monitoring of Interstage Application Server operation. For details on monitoring using this, refer to the 'Performance Monitoring' chapter.

  In addition to status information, limited monitoring information is available at the individual server level from the Site Management tab of the Interstage Management Console. Details are given in the relevant sections of the Operator's Guide. It is however, recommended to use the Systemwalker tool for comprehensive monitoring.

1.5 Overview of Deploying Applications

One or more applications can be deployed to a WorkUnit that provides the applications runtime environment. This may include resources, services, and security configuration. In a multi-server environment, WorkUnits may be deployed across several servers. Interstage supports J2EE and CORBA applications. This section outlines the main steps involved in deploying applications and directs you to more detailed instructions.

The following are the main steps involved in deploying an application:

1. 1.5.1 Configure and Start the Required Services
2. 1.5.2 Configure the Required Resources
3. 1.5.3 Create a WorkUnit

4. 1.5.4 Deploy the Application
5. 1.5.5 Configure Security for Deployed Applications
6. 1.5.6 Start the WorkUnit

1.5.1 Configure and Start the Required Services

Depending on the type of application being deployed, configure the services required.

Services are located under the Services node of the navigation tree.

Start all services to be used by the applications being deployed.

For details on configuring the Interstage System Service, the Event Service, the Web Server and the Repository, refer to the 'System' and 'Services' chapters. For complete details on the Repository, refer to the Directory Service Operator's Guide.

1.5.2 Configure the Required Resources

From the IMC, configure the resources required by the application from JDBC, JMS, Connectors and JavaMail.

Resources are located under the Resources node of the navigation tree.

For details on resources, refer to 'Resources' chapter.

1.5.3 Create a WorkUnit

Create and configure the WorkUnit into which the applications will be deployed, selecting the type as IJServer for J2EE applications or CORBA to deploy CORBA applications.

WorkUnits are located under the WorkUnits node of the navigation tree in the navigation frame.

For details on creating an IJServer, refer to the 'WorkUnits General and IJServer' chapter.

For details on creating a CORBA WorkUnit, refer to the chapter 'CORBA WorkUnits'.

1.5.4 Deploy the Application

Application deployment is done from within the WorkUnit. Additionally for IJServers, Startup and Shutdown classes can be specified to run on WorkUnit startup and shutdown respectively.

For details on deploying an IJServer, refer to the 'WorkUnits General and IJServer' chapter.

For details on deploying a CORBA WorkUnit, refer to the 'CORBA WorkUnits' chapter.

1.5.5 Configure Security for Deployed Applications

For details on configuring security for deployed applications, refer to the 'Security' chapter.

1.5.6 Start the WorkUnit

Starting the WorkUnit starts all applications deployed to that WorkUnit. WorkUnits startup is done from the WorkUnit node of the navigation tree.

For details on starting the WorkUnit, refer to the 'WorkUnits General and IJServer' chapter.

1.6 Configuring a Multi-server Environment Windows32/64 Solaris32 Linux32/64

Configuration of a multi-server environment involves:

1. Installing an Admin Server

   For details, refer to the 'Site' chapter.

2. Installing one or more Standalone Servers

   For details, refer the 'Site' chapter.

3. Adding Standalone Servers to the site using the Admin Server.

   For details, refer to the 'Site' chapter.

   Standalone Servers once added to the site are referred to as Managed Servers.

4. Defining Server Groups

   For details, refer to the 'Server Groups' chapter.

5. Adding Managed Servers to Server Groups.

   For details, refer to the 'Server Groups' chapter.

Once the Site has been constructed, multi-server WorkUnits can be created and deployed across site participants. For details, refer to the 'WorkUnits General and IJServer' section.

1.6.1 Configuring Combined Servers

When the multiserver management function is used, the Admin Server function and the Interstage application server function (Managed Server) can both be run on the same physical server. Such a server is called a Combined Server. The following Combined Server combinations are possible:

- Admin Server and Reserved Managed Server
- Admin Server and Independent Managed Server
- Admin Server and Managed Server that is a Server Group Member.

Under Interstage, the following restrictions apply when a Combined Server is used:

- A Combined Server cannot be changed into a lone Admin Server, Managed Server, or Standalone Server.
- Combined Server resources cannot be migrated to a lone Admin Server, Managed Server, or Standalone Server.
- The Managed Server must be a site participant of the site controlled by the Admin Server
- A site created at a Combined Server cannot be migrated to other Admin Servers.
- Since Admin Server functions and application server functions both run on the same server machine, the operation load of each may affect the other.
- Since Admin Server functions and application server functions both run on the same server machine, an error in one group of functions may affect the other group of functions.
- Operations are possible only from the Interstage Management Console in the Admin Server functions. Since Managed Server and Standalone Server Interstage Management Consoles cannot be used, the range of use may be restricted.
- A Combined Server cannot be used with provisioning functions.

Due to the above restrictions, use of Combined Servers is not recommended. If multiple servers are used with the multiserver management function, use a separate server for the Admin Server.

1.6.1.1 Creating a Combined Server

To create a Combined Server, add the Admin Server function to a Standalone Server running the Interstage application server, and then add the Standalone Server to the Site. Use the following steps to construct a Combined Server.

1.6.1.1.1 Installing Standalone Servers

1. Use the installer to install the application server function from the Interstage package.

1.6.1.1.2 Adding the Admin Server Function

Use the following procedure to add the Admin Server function:

1. Forcibly stop Interstage using the *isstop* command .

```
isstop -f
```

1. Stop the service that enables use of the Interstage Management Console as follows:

   - Windows32/64

     Stop the Interstage Operation Tool service.

   - Solaris32 Linux32/64

     Use the *ismngconsolestop* command to stop the service that enables use of the Interstage Management Console.

2. Execute the *isaddadminfunc* command on the Standalone Server to add the Admin Server function.

   Refer to the Reference Manual (Commands Edition) for details of the *isaddadminfunc* command.

3. Restart the services that enable use of the Interstage Management Console as follows:

   - Windows32/64

     Start the Interstage Operation Tool service.

   - Solaris32 Linux32/64

     Use the *ismngconsolestart* command to start the service that enables use of the Interstage Management Console.

4. Start Interstage.

```
isstart
```

5. From the Interstage Management Console (of the Admin Server) on that server, add the local Standalone Server to the Site.

When construction of the Combined Server is completed as above, the server can operate as a Combined server that has both the Admin Server and the application server functions.

Do not operate an Admin Server and a Standalone Server in a combined state. If these are combined, operations are not guaranteed for either the Admin Server or the Interstage application server. Always add the Standalone Server to a site and operate it as a Managed Server on that Site.

1.6.1.2 Operating a Combined Server

A Combined Server is operated via the Interstage Management Console. When logging in to the Interstage Management Console of a Combined Server, the Admin Server screen is displayed. When the server is operating as an Admin Server, there is no difference between its operation and that of an ordinary Admin Server. Operations in relation to the Managed Server of the Combined Server are performed from the Admin Server Interstage Management Console.

When a Combined Server is used, the business configuration management environment setup information is shared by the Admin Server and the Managed Server. When setting the business configuration management environment, perform operations for the Managed Server from the Application Management tab. If the business configuration management environment settings for the Admin Server are updated from the Site Management tab, the business configuration management environment settings for the combined Managed Server are also updated.

At this time, if the business configuration management environment settings for the relevant Managed Server are referenced from the Application Management tab, the pre-update settings values are displayed. This may lead to accidental modification of the business

configuration management environment settings for the Managed Server. To avoid this, it is recommended that the business configuration management environment settings not be updated from the Site Management tab.

1.7 Monitoring Interstage Application Server

Basic monitoring is available from the IMC, allowing the user to view the status and related information on items managed. This is described throughout the document where available. For more comprehensive monitoring, a tool such as Fujitsu's SystemWalker should be used. For details, refer to the SystemWalker documentation.

1.8 Maintenance

Interstage provides a means of backing up and restoring resources for maintenance purposes.

Configuration data and applications can be backed up all together or separately.

For information on maintenance operations, refer to the 'Maintenance (Resource Backup)' chapter.

1.9 Sample J2EE Applications

Sample applications are provided and installed with Interstage. These demonstrate simple applications being setup and deployed on Interstage Standalone Server.

To access the sample applications, in Windows, click the **Start** button, from Programs menu, click Interstage Application Server > Deploy and run Sample Applications.

Chapter 2 Configuring the Interstage Management Console

2.1 Starting the Interstage Management Console

To use the Interstage Management Console:

1. Start the Interstage Management Console services.

   The Interstage Management Console Services are started by default. For details, refer to "2.1.1 Starting the Interstage Management Console Services".

2. Start the Web browser.

   For details, refer to "2.1.2 Starting the Web Browser".

3. Login to the Interstage Management Console.

   For details, refer to "2.1.3 Logging in to the Interstage Management Console".

4. Configure the display.

   For details, refer to "2.1.6 Configuring the Display".

Note

- The use of SSL encrypted communications to access the Interstage Management Console can be selected during Interstage installation. If the method selected during installation is to be changed, the environment must be customized. For details, refer to "Customizing SSL Encrypted Communication for the Interstage Management Console" in the "Security" chapter.
- For details of environment definition files used by the Interstage Management Console, refer to "2.4 Environment Files used by the Interstage Management Console".
- For details on stopping the Interstage Management Console, refer to "2.2 Stopping the Interstage Management Console".
- Web browsers supported by the Interstage Management Console are shown in the table below.

Web browser type	Version/level
32-bit edition Microsoft(R) Internet Explorer	7, 8, 9, 10

2.1.1 Starting the Interstage Management Console Services

Services for the Interstage Management Console are started automatically at server startup.

These services must be running for the console to operate. If the services need to be started manually later, refer below.

Windows32/64

- Interstage Operation Tool

From Windows click Start, then Settings, and then click Control Panel. In the Control Panel dialog, double-click Administrative Tools. In the Administrative Tools dialog, double-click Services. Select the services listed above, right-click, and then click Start.

The following services are started automatically when Interstage Operation Tool is started:

- Interstage JServlet (OperationManagement).
- Interstage Operation Tool (FJapache)

Solaris32/64 Linux32/64

1. A batch start can be used for all services required for the Interstage management console

```
/opt/FJSVisgui/bin/ismngconsolestart
```

Services started with the batch start above can also be started individually as follows:

- The Interstage JMX service:

```
/opt/FJSVisjmx/bin/isjmxstart
```

- Servlet service for the Interstage Management Console:

```
/opt/FJSVjs2su/bin/jssvstart
```

- Interstage FJapache HTTP Server (dedicated to the Interstage Management Console):

```
/opt/FJSVihs/bin/httpd -f /etc/opt/FJSVisgui/httpd.conf -s "#ISCONSOLE" -K
```

This service allows the Interstage Management Console to communicate with and modify the environment of the Interstage Application Server. The Interstage JMX Service runs under the control of the 'Interstage Operation Tool (*1)' service.

Refer to "2.4 Environment Files used by the Interstage Management Console" for details on configuration of the JMX Service.

Note

- /opt is the default Interstage installation directory under Solaris and Linux.

Checking the Status of the Interstage Management Console

Windows32/64

In Windows(R), click [Control Panel] > [Services] and check that the status of the following services is "Started".

- Interstage JServlet (OperationManagement)
- Interstage Operation Tool
- Interstage Operation Tool (FJapache)

Solaris32/64 Linux32/64

Execute the following commands to check that each service has started.

- jscontdisp
- isjmxstat

2.1.2 Starting the Web Browser

The following browsers are supported:

- Internet Explorer 7 and later

JavaScript must be enabled on the browser.

After starting the IMC services listed in '2.1.1 Starting the Interstage Management Console Services', start the Web browser in the PC used for operating the Interstage Management Console, and specify the URL of the Interstage Management Console for the connection.

The URL specified varies depending on whether SSL encrypted communication is used for communication between the Web browser and the Interstage Management Console.

Select whether or not to use SSL encrypted communication on installation. For details about changing this setting, refer to "Customizing SSL Encrypted Communication for the Interstage Management Console" in the "Security" chapter.

SSL Encrypted Communication is not Used

Specify the following URL:

```
http://host-name:port-number/IsAdmin
```

host-name

Specify the host name or IP address of the server on which the Interstage Application Server is installed. In a multi-server site this will typically be the address of the Admin Server. This value is set in httpd.conf. Refer to "2.4 Environment Files used by the Interstage Management Console".

port-number

Specify the port number used by the Interstage Management Console.

Default: 12000

SSL Encrypted Communication is Used

Specify the following URL:

```
https://host-name:port-number/IsAdmin
```

The host name and port number specified are the same as when SSL encrypted communication is not used.

If 'Use SSL encryption' was selected for access to the Interstage Management Console during Interstage installation, a certificate generated for the Interstage Management Console is used for authentication purposes. This certificate is generated automatically by this product. The purpose of this certificate is simply so that SSL encrypted communication can be used between the Interstage Management Console and the Web browser immediately after installation. Since the certificate is not registered in the Web browser as a reliable certification authority certificate, a dialog informing you that there may be a problem with the reliability of the certificate may be output when the connection is made and the above URL is specified.

Since the Interstage Management Console host name is not contained in this certificate, a dialog informing you that there may be a problem with the reliability of the certificate may be output because it is not possible to check whether the host name matches the host name specified in the URL. Check the information about the certificate used for SSL encrypted communication according to the procedure shown below, and then check the validity of the certificate before using the Interstage Management Console. Also, do not register the certificate in the Web browser.

1. Check the certificate fingerprint

   Compare the fingerprint confirmed during installation of this product with the information output in the dialog in the Web browser.

   The fingerprint is a hash value calculated from a part of the certificate. This value varies depending on the algorithm used. Use the same algorithm when comparing the calculated fingerprint with the information in the dialog.

   If you forgot to confirm the fingerprint when this product was installed, refer to "Post-installation" in the Installation Guide and confirm it.

2. Check the certificate contents

   The contents of the automatically generated certificate are shown in the table below. Compare this with the information in the dialog output in the Web browser.

Information in the certificate	Information that is set
issuer name and subject name	CN=Interstage Application Server

Information in the certificate	Information that is set
validity period	Until 23:59:59 on 31/12/2049

The certificate generated when this product was installed and certificates generated using the *cmcrtsslenv* command are not issued by trusted CAs. They are considered certificates of low authenticity for the following reasons:

- The authenticity of a CA for the private key used in the certificate signature is not guaranteed.
- The authenticity of the certificate owner is not guaranteed.

For this reason, obtain a certificate from a trusted CA before the application starts and then set the application to use the certificate for SSL encrypted communication.

For details on certificate authenticity, refer to the "Security Trends" appendix in the Security System Guide.

If you are running applications when the system is configured not to use SSL encryption, it is recommended to encrypt communications by some other means.

Note

- For details about changing the SSL encrypted communication settings, refer to "Customizing SSL Encrypted Communication for the Interstage Management Console" in the Security chapter.
- For details about changing to an application that performs SSL encrypted communication using a certificate obtained from a certification authority, refer to "Changing the Certificate" in the "Customizing SSL Encrypted Communication for the Interstage Management Console" section in the "Security" chapter.

2.1.3 Logging in to the Interstage Management Console

The default login Authentication method is Operating System Authentication. This means that the first time a user logs into Interstage through the IMC, a valid Operating System User Name (User ID) and Password must be specified for the machine that Interstage is running on. To change the Login Authentication method, refer to "2.1.4 Login Authentication for the Interstage Management Console".

Specify a valid User Name and Password and click the Login button.

2.1.4 Login Authentication for the Interstage Management Console

When the Interstage Management Console starts, a login screen is displayed (please note that auto-completion is disabled). Two forms of user authentication are possible:

1. 2.1.4.1 Authentication Using Operating System Accounts on the IMC Server
2. 2.1.4.2 Authentication using an LDAP Directory Service on the IMC Server

If login was successful, a welcome window is displayed. If login failed, failure cause and a window requiring you to log in again are displayed.

Users are considered to belong to one of these two types of 'User repository'. The default repository is for those with operating system accounts on the Interstage Server.

Note

Set a password that contains alphanumerics and symbols. Specify a minimum of eight characters. Do not use passwords that contain IDs, or personal information such as date of birth.

Windows64 Linux64

Interstage Directory Service is not included with Standard-J Edition. To use directory service authentication, use Interstage Directory Service on Enterprise Edition or another operating system.

2.1.4.1 Authentication Using Operating System Accounts on the IMC Server

In this scenario, users of the Interstage Management Console are also users of, and managed by, the Operating System. A user may have one of two possible roles:

- Those with machine administrator rights.
- Those without machine administrator rights.

Windows32/64

Membership of the administrator group is required to login to the Interstage Management Console as an Administrator. Users belonging to this group have full access to all functions provided by the IMC. The IMC allows restricted functionality for all other users.

Solaris32/64 Linux32/64

A user must login as **root** to the Interstage Management Console to be an Administrator. The root user has full access to all functions provided by the IMC. The IMC allows restricted functionality for all other users.

Table 2.1 Operating System Account Based Roles and Available Operations

Role	Available operations
Non-administrator	- Can view application/service/system settings and their current status. Can also view logs and monitoring information. - Can perform user application operations (such as start/stop/unblock queue). Can also perform service/resource operations (such as Event Channel) that are used by user applications. - Can create new and change configurations for applications as well as deploy applications. Can also create or update resource configurations (such as JDBC, JavaMail, JMS, Connector) that are used by applications.
Administrator	- Can do all operations. In addition to the operations that non-administrators can do, can also update service/system configurations and perform operations on them. In a multiserver environment, can also add/delete servers, add/delete Server Groups, and change the settings for the user repository.

2.1.4.2 Authentication using an LDAP Directory Service on the IMC Server

The Interstage Directory Service LDAP Directory Service can be used as a user repository. Users may have one of four different roles:

Table 2.2 Interstage Directory Service Based Roles and Available Operations

Role	Available operations	Users registered in
Monitors	Can view application/service/system settings and their current status. Can also view logs and monitoring information.	Monitors group.
Operators	Can perform user application operations (such as start/stop/unblock queue). Can also perform service/resource operations (such as Event Channel) that are used by user applications.	Operators group
Configurators	Can create new/change configurations for/deploy applications. Can also create or update resource configurations (such as JDBC, JavaMail, JMS, Connector) that are used by applications.	Configurators group
Administrator	Can do all operations. In addition to the operations that non-administrators can do, can also update service/system configurations and perform operations on them. Windows32/64 Solaris32 Linux32/64 In a multi server environment, can also add/delete servers, add/delete Server Groups, and change the settings for the user repository.	Administrators group

Note

- If multiple users have been registered in the same role, it is not possible to restrict the operations that are available to each user.

2.1.4.2.1 Registering User Information

To set up the user information in Interstage Directory Service, follow the procedure below. For further details, refer to the Interstage Directory Service Operator's Guide and the "Managing the Repository" section in the "Chapter 8 Services" chapter.

Use the user information registered in the server on which Interstage Directory Service is installed. For further details on registering user information, refer to the details for the platform of the server used to set up the Interstage Directory Service in the Interstage Application Server manual.

1. Use the Interstage Management Console to create a repository. Choose a DN for the Public Directory. The following base DN is used by default:

   ou=interstage,o=fujitsu,dc=com

2. Set the operation mode of the repository to 'Stand-alone' or 'Master'. Note that the operation mode can only be set after the repository has been created. Click **[Show]** to display the Detailed Settings and change the mode in the Replication Settings table.

3. Start the Interstage Directory Service Entry Administration Tool and log in to the repository generated using the Interstage Management Console.

4. If there is no User group under the root node (interstage) then select the node and from the menu navigate to Entry > Add. Select organizationalUnit from the List of object classes to set the objectClass attribute and specify 'User' for the ou attribute. Click OK to create a group called 'User' with the DN:

   ou=User,ou=interstage,o=fujitsu,dc=com

   To add users, select the User node and from the menu choose Entry > Add.

   Register entries bearing in mind the following points:

   - Set the objectClass attribute to inetOrgPerson by selecting it from the List of object classes.
   - Set the cn attribute to the user name that the user will login to the Interstage Management Console with.
   - The sn attribute (surname) MUST be specified.
   - The userPassword attribute is the password that the user will login with.
   - Click the OK button to add the user to the group.

   For example, if the user name (cn) is 'Smith' so the DN will be:

   cn=Smith,ou=User,ou=interstage,o=fujitsu,dc=com

5. Create the Role group. The Interstage login roles can be added under this group. Select the root node (interstage) and from the menu choose Entry > Add. Select organizationalUnit from the List of object classes to set the objectClass attribute and specify 'Role' for the ou attribute. Click OK to create a group called 'Root' with the DN:

   ou=Role,ou=interstage,o=fujitsu,dc=com

   To add roles, select the root node and from the menu choose Entry > Add.

   Register entries bearing in mind the following points:

   - Set the objectClass attribute to groupOfNames by selecting it from the List of object classes.
   - The cn attribute indicates the role name. The role names that Interstage uses are: Monitors, Operators, Configurators and Administrators.
   - The member attribute lists the members of this role and at least one user must be specified here for the role to be created. As an example using the user 'Smith' from above, set the member attribute as:

     cn=Smith,ou=User,ou=interstage,o=fujitsu,dc=com

   - Click the OK button to add the role to the group.

Adding Subsequent Users

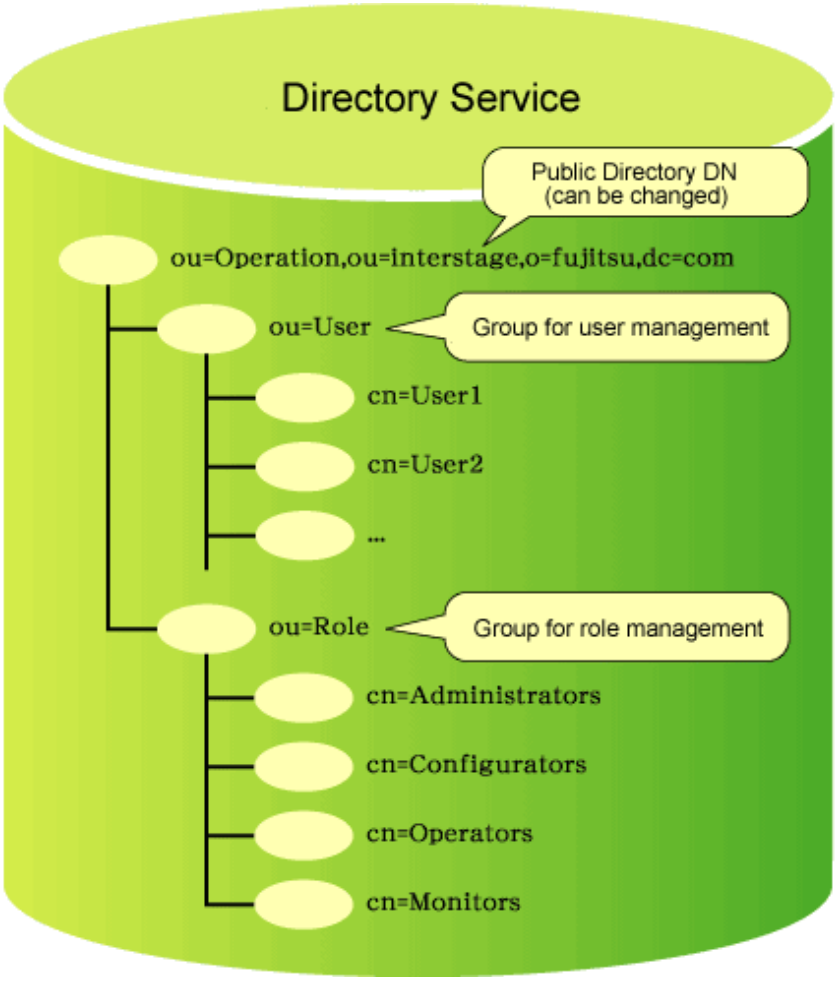
1. To add subsequent users to the various roles:
   - Select the required role (such as 'Administrator') and from the menu choose Entry > Modify.
   - Click the Add attribute button.
   - In the dialog that is displayed set the Attribute name to 'member'.
   - In the Attribute value field specify the user in the format shown above. E.g.

     cn=ken,ou=User,ou=interstage,o=fujitsu,dc=com

     In this example, the user 'ken' is specified as a member of the group.
   - Click the OK button to add the attribute to the role.
   - Repeat the Add attribute operation for other users.
   - Click the OK button to save the changes and add the users to the role..

An image of the directory service configuration is shown below.

Figure 2.1 Directory Service Configuration



Note

- Use the user information registered in the server on which Interstage Directory Service is installed.

  For details of how to register user information, refer to the Interstage Application Server manual for the server used to set up the repository for Interstage Directory Service.

2.1.4.2.2 Changing Authentication Method

Application Management

Interstage > Interstage Application Server > Security > Login User Authentication	Environment Settings

To set up the authentication (LDAP) server settings:

1. In **User Repository** choose LDAP server.
2. In **Import Repository Information**, select the repository to be used.
3. Specify the LDAP Servers **Host** name and **Port** number.
4. Specify the search **Base DN** used when the repository was created.

   This corresponds to the **Public Directory** field during Repository creation.
5. Specify the **Administrator DN** and **Administrator DN Password** used when the repository was created.
6. Select Yes to **Enable SSL Encryption** communications with the LDAP Server, and specify the **SSL Port Number** and **SSL Configuration Information**.
7. Click the **Update** button to update the settings.

   Click the **Refresh** button to refresh the form with the most recently updated values.

2.1.4.2.3 Mapping Directory Service Users with Operating System Users

Solaris32/64 Linux32/64

WorkUnits are started using the permissions assigned to the operating system user of the same name as the ID used to log in to the IMC. Map registered directory service users with operating system users as follows:

- Create the users on each machine specifying a user name (cn) that is registered in the directory service (this maps the directory service user with the operating system user).
- Windows32/64 Solaris32 Linux32/64
  For multi server operation, create an operating system user on each machine to be used in a given Server Group (this maps users on multi servers).

The user logged in to the IMC will then have permission to start the WorkUnit.

The maximum length of the directory service user names and operating system user names is different as shown below.

Directory Service	512 bytes (this includes the base DN)
Operating System	This depends on the operating system limit. The maximum name length for users that can start WorkUnits is eight bytes. Use no more than eight bytes when registering users in the directory service for Solaris/Linux Managed Servers.

2.1.4.2.4 Handling Faults in the Directory Service

If the Interstage Management Console cannot be operated because of a fault in the directory service, use the *isresetuserrep* command to switch the operating system authentication temporarily.

Refer to "Interstage JMX Service Operation Commands" in the Reference Manual (Command Edition) for details of the *isresetuserrep* command.

2.1.5 Logout from the Interstage Management Console

Perform the logout to end Interstage Management Console operations or to stop the Interstage Management Console.

The procedure for logging out is described below.

1. In the Interstage Management Console currently logged in to, click [Logout].

   A confirmation dialog box is displayed.

2. Click [OK].

   The web browser window is closed.

2.1.6 Configuring the Display

Application Management

Interstage	Console Preferences

Standalone

Interstage	Console Preferences

To configure the display:

1. In **Automatic Refresh**, select Enable to enable automatic periodic refresh of the display.

   Interstage Management Console will automatically refresh pages that display monitoring information. This is useful when WorkUnits or deployed applications are being monitored on individual servers in a site.

2. If Automatic Refresh is enabled, in **Automatic Refresh Interval**, specify the refresh interval in seconds.

   Range: 10 to 1799.

3. In **On-Screen Item Descriptions**, select Enable to have short descriptions for input fields displayed on the Console.

   This is enabled by default.

4. Click the **Update** button to save and apply changes.

Note

- When the following conditions are satisfied, a session timeout does not occur in the Monitoring page:
  - **Automatic Refresh** is set to Enable, and
  - **Automatic Refresh Interval** is set to a value equal to or less than the session timeout.

    [30] minutes is set for the session timeout time by default.
- Pages affected by these settings
  - [IJServer] > [Monitoring]
  - [IJServer] > [EJB Application] > [Monitoring]
  - [IJServer] > [Web Application] > [Monitoring]
  - [CORBA] > [Implementation Repository] > [Monitoring]

2.2 Stopping the Interstage Management Console

If parameters in the environment files used by the Interstage Management Console require changing, the Interstage Management Console services must first be stopped. These services and details on how to stop them are given below.

Windows32/64

Stop the following services from [Administrative Tools] - [Services] in Windows(R):

- Interstage JServlet(OperationManagement).
- Interstage Operation Tool
- Interstage Operation Tool (FJapache)

Solaris32/64 Linux32/64

Batch stop all services required for the Interstage Management Console as follows

```
/opt/FJSVisgui/bin/ismngconsolestop
```

Services stopped with the batch process above can also be stopped individually as follows:

- The Interstage JMX service:

  ```
  /opt/FJSVisjmx/bin/isjmxstop
  ```

- Servlet service for the Interstage Management Console:

  ```
  /opt/FJSVjs2su/bin/jssvstop
  ```

- Interstage HTTP Server (dedicated to the Interstage Management Console):

  ```
  kill 'cat /var/opt/FJSVisgui/tmp/httpd.pid'
  ```

Note

- /opt is the default Interstage installation directory under Solaris and Linux.
- Replace PID_FILE in the command above with the path specified as the value of the *PidFile* property in the Interstage HTTP Server's httpd.conf configuration file. Refer to "2.4 Environment Files used by the Interstage Management Console" for the location of this file.
- The Interstage JMX service thread dump is collected when Interstage JMX service stop processing is performed. To prevent the process being stopped before collection of the thread dump is complete, the Interstage JMX service does not stop for at least 20 seconds.

2.3 Interstage Management Console Operations

Interstage Application Server provides the following two Management Consoles:

Interstage Java EE Admin Console

This console is used to perform Java EE feature operations.

This console can be used if "Java EE" was selected at installation time.

Interstage Management Console

This console is used to perform non-Java EE feature operations.

This console can be used if "Interstage Management Console" was selected at installation time.

If both "Java EE" and "Interstage Management Console" are selected at installation time, both Management Consoles can be used.

In this case, select either of the following methods for operating the Management Consoles:

- Integrated GUI operation
- GUI stand-alone operation

Integrated GUI Operation

With the integrated GUI operation, both the Interstage Java EE Admin Console and the Interstage Management Console are operated from a single Web browser page. When the login operation is performed from the Interstage Java EE Admin Console login window, the integrated GUI operation will be used.

The procedure for using the integrated GUI operation is explained below.

Procedure

1. Start the Web browser in a new session, then log into the Interstage Java EE Admin Console to operate the Java EE feature.
2. To operate the Interstage Management Console, click the [Switch to Console] button to switch to the Interstage Management Console. The [Interstage Java EE Admin Console] tree node will not be displayed in the Interstage Management Console.

- Use the following method to start the Web browser in a new session:

  - For Internet Explorer 8/9/10

  If the Web browser is running already, select [New Session] from the [File] menu of the Web browser to start the new Web browser. If a Web browser is not running already, the Web browser will always start in a new session.

  - For Internet Explorer 7

  The Web browser will always start in a new session.

- For the integrated GUI operation, operations must be performed using the same user account. Operations cannot be performed using different user accounts.
- To change the authentication method for the Management Console from the default (operating system authentication), create a user account (user name and password) that can log in to both Management Consoles before they are used. However, even if a user account that can log in to both consoles is used, the integrated GUI operation cannot be used when the user has logged in using the Interstage Management Console login window.
- The integrated GUI operation cannot be used if the user has logged in to the Interstage Java EE Admin Console that was started using the GUI stand-alone operation.
- In Internet Explorer 8/9/10, an error may occur in the window display or transition when the integrated GUI operation and the GUI stand-alone operation are used together.
- Do not click the [Switch to Console] button until the browser window has loaded completely. If the [Switch to Console] button is clicked before the browser window has loaded, an error may occur in the window display or transition.

GUI Stand-alone Operation

With the GUI stand-alone operation, the Interstage Java EE Admin Console and the Interstage Management Console are operated from separate Web browser pages. When the login operation is performed from the Interstage Management Console login window, the GUI stand-alone operation will be used.

The procedure for using the GUI stand-alone operation is explained below.

Procedure

1. Start the new Web browser window and then log in to the Interstage Management Console to operate the Interstage features.

2. To operate the Interstage Java EE Admin Console, click the [Interstage Java EE Admin Console] tree node and then log in from the Interstage Java EE Admin Console login window that opens. The [Switch to Console] button is not displayed in either Management Console.

2.4 Environment Files used by the Interstage Management Console

The following environment files are required to run the Interstage Management Console. These files are automatically configured by the installation process and will not normally require modification.

Windows32/64	Linux32/64 Solaris32/64
%IS_HOME%\gui\etc**httpd.conf**	/etc/opt/FJSVisgui/**httpd.conf**
%IS_HOME%\gui\IsAdmin\WEB-INF**web.xml**	/opt/FJSVisgui/isadmin/WEB-INF/**web.xml**
%IS_HOME%\jmx\etc\isjmx.xml	/etc/opt/FJSVisjmx/isjmx.xml
%IS_HOME%\F3FMjs2su\conf**jsgw_apapi.conf**	/opt/FJSVjs2su/conf/**jsgw_apapi.conf**
%IS_HOME%\F3FMjs2su\conf**jswatch.conf**	/opt/FJSVjs2su/conf/**jswatch.conf**
%IS_HOME%\F3FMjs2su\conf**jscontainer.xml**	/opt/FJSVjs2su/conf/**jscontainer.xml**

In the above table:

- IS_HOME is a Windows environment variable containing the Interstage installation path.
- /opt is the default Interstage installation directory under Solaris and Linux. If this is changed, replace occurrences of opt in the paths above with the new installation directory.

If any parameters in the environment files do need to be changed, the Interstage Management Console services must first be stopped, the files edited, and the services then restarted.

For details on stopping services, refer to "2.2 Stopping the Interstage Management Console". For details on restarting these services after environment file modification, refer to "2.1.1 Starting the Interstage Management Console Services".

A description of each environment file is given below outlining those parameters that may be modified.

httpd.conf

Configuration file for the instance of FJapache dedicated to the Interstage Management Console.

The Interstage Management Console uses its own port. Modify the number assigned to the *Port* property to that used by the Interstage Management Console.

Default: 12000

Port number 12000 is also set when SSL encrypted communication is enabled.

web.xml

Contains application settings for the Interstage Management Console.

Edit the session timeout (in minutes) between the <session-timeout> tags if required. Timeout is shown in bold in the following example.

```
<session-config>
   <session-timeout>
      30
   </session-timeout>
</session-config>
```

Note

- There is also a session timeout setting in the global web.xml file that applies to all applications deployed under the JServlet Engine. The session timeout setting that will be used by the Interstage Management Console is the lower of the two. This file is located at:
  - Windows: %IS_HOME%\F3FMjs2su\conf\web.xml
  - Solaris | Linux: /opt/FJSVjs2su/conf/web.xml
- If a large value is set for session timeout, security risks such as illegal operations by a third party or information leaks, is increased. Configure the session timeout to the minimum value required to operate the Interstage Management Console.

isjmx.xml

Environment definitions for the JMX service.

Table 2.3 Interstage JMX Environment Definition File Format

Tag	Description	Attributes
isjmx	Contains all JMX related information. Elements (all required) - port tag - server tag - registry tag - timeout tag - host tag - loginlog tag - operationlog tag	None
port	Ports used by the JMX service.	rmi - Port number through which the Interstage JMX service will accept requests of RMI registry from the Interstage Management Console. Default : 12200. internal - Port number used internally by Interstage. This must not be changed. rmiinvoke - Port number through which the Interstage JMX service will accept requests for the RMI registry from the Interstage Management Console. If this is omitted, an unused port is used automatically. Default : 12230.
server	Java VM related settings.	java.home - Installation path of the JDK/JRE used by the Interstage JMX service. Does not require changing unless the JDK/JRE is moved from its installed location. Specify a version of JDK/JRE that is 6.0. options

Tag	Description	Attributes
		- Java VM options, comma delimited, for the Interstage JMX service. Refer to the Java VM documentation for details.
registry	JMX registry related information.	max - Maximum number of MBeans that can be registered for Interstage JMX service. MBeans contain resource information managed by the Interstage JMX service. An integer from 1 to 2147483647 can be specified. Default : 100000 It is recommended that this setting is not changed. If required, refer to the Tuning Guide.
timeout	JMX communication information.	rmi - Duration in minutes after which a time-out occurs for communications via the Interstage JMX service. If a time-out is reached, the requested processing continues on Interstage. An integer from 0 to 10,080 can be specified. Specifying a value of 0 means there is no communication time-out. Default: 20. https - Duration in minutes after which a time-out occurs for SSL communications via the Interstage JMX service. If a time-out is reached, the requested processing continues on Interstage. An integer from 0 to 10,080 can be specified. Specifying a value of 0 means there is no SSL communication time-out. Default: 20.
Host	Information about when the Interstage JMX service communicates with other servers.	Localhost IP address used when the Interstage JMX service communicates with other servers. In a server that has more than one IP address, (for example a server in which the LAN used for system operation management, and the LAN used for business are separate), specify the IP address used by the Interstage JMX service. If there is one IP address, there is no need to specify it. If "IP address used for communication with another server" is set, the application runs in the same manner as when "-Djava.rmi.server.hostname=(IP address)" is set for the "server tab 'options' attribute" value specified in the isjmx.xml file.
Login	Information about the login log that records login requests for the Interstage JMX service.	Max Upper limit for the file size of the login log that records login requests for the Interstage JMX service. The unit is MB. Set an integer from 1 to 100. If this definition is omitted, the application runs as though [1] has been set.

Tag	Description	Attributes
		Default: 1.
Operation	Information about the Interstage JMX service internal log.	Max Upper limit for the file size of the Interstage JMX service internal log. The unit is MB. Set [1] for this.

Sample Interstage JMX Service Environment Definition File

```
<?xml version="1.0" encoding="MS932"?>
<isjmx>
  <port rmi="12200" internal="12210" https="12220" rmiinvoke="12230"/>
  <server java.home="c:\interstage\jdk6" options="-Xmx256m -XX: MaxPermSize=128m "/>
  <registry max="100000" />
  <timeout rmi="20" https="20"/>
  <loginlog max="1"/>
  <operationlog max="1"/>
</isjmx>
```

jsgw_apapi.conf

Servlet Gateway environment definition file. This connects the HTTP Server (FJ Apache) with the servlet engine.

This should not be changed.

jswatch.conf

JServlet Engine definition file. This sets up the environment in which the Interstage Management Console and related tools run (CLASSPATH, VM options, etc).

This should not be changed.

jscontainer.xml

Contains application settings (application locations, etc.) for the Interstage Management Console and related tools.

Edit the log file names and destinations if required.

2.5 Product Information Display

The **About Interstage** button is displayed in the top part of the window after the Interstage Management Console login window. Click this button to display the following information:

- Product name
- Edition information
- Version information

2.6 Notes on Operating the Interstage Management Console

Supported Browsers

The Interstage Management Console runs on 32-bit edition Microsoft(R) Internet Explorer 7, 8, 9 and 10.

Using Web Browser Cookies

In the Interstage Management Console, configure the settings so that cookies are enabled in the Web browser.

Using SSL Encrypted Communication

When SSL encrypted communication is used, the "crypt32" error may be output to the event log. This occurs when attempting to connect to Windows(R) Update on the internet fails when the root certificate update component is enabled.

To avoid this problem:

- Connect to the Internet and then update the root certificate.
- Disable the root certificate update component.

Session Timeout Occurrences

If a session timeout occurs, then a confirmation dialog box is displayed, warning that the Web browser will be closed.

Follow the procedure below.

1. In the confirmation dialog box, click [OK] to close the Web browser used in the Interstage Management Console.
2. To continue Interstage Management Console operations, restart the Interstage Management Console and then log in from the Login window.

Using the 'Reuse Windows for Launching Shortcuts' Option

If the "Reuse windows for launching shortcuts" setting is disabled without using the tabbed browsing function, the Interstage Management Console transition screen, or its operations, may behave abnormally.

Take the steps detailed below to enable 'Reuse windows for launching shortcuts'.

1. In the Microsoft(R) Internet Explorer [Tools] menu, select [Internet Options], then click the [Advanced] tab.
2. Check the box next to the relevant item below:
    - "Reuse windows for launching shortcuts (when tabbed browsing is off)"

Web Browser HTTP/1.1 Settings

If the Web browser HTTP/1.1 settings are invalid, the Interstage Management Console might not run normally.

In the Microsoft(R) Internet Explorer [Tools] menu, select [Internet Options], then click the [Advanced] tab. In the [HTTP 1.1 settings] section, select the [Use HTTP 1.1] check box to enable the HTTP/1.1 settings.

Chapter 3 Using the Interstage Management Console

3.1 Overview to Interstage Management Console GUI

The Interstage Management Console (IMC) provides an intuitive user interface for the management of Interstage Application Server(s). Management of the Application Server includes operations such as configuration, creation, update and deletion of resources, services, WorkUnits and security configurations on servers or server groups; application deployment across one or several servers; and status and performance monitoring. These operations include high level operations involved in server, server group or site management, and also operations on new and existing items in or used by the system such as resource adapter configuration.

The Interstage Management Console capabilities are different on the Admin Server from the Standalone Server.

From an Admin Server it can be used for operations across multiple servers in a site, such as WorkUnit start and stop. From the Admin Server it is also possible to manage and monitor the site and all servers on it.

From a Standalone Server, the Interstage Application Server on that server only can be managed.

From a Managed server, it is generally not possible to create new items or update settings. It is however possible to start, stop or monitor WorkUnits and to perform several other operations.

Allowed operations will also vary depending on the user login level. For details, refer to the "Chapter 2 Configuring the Interstage Management Console" chapter.

This section describes the Interstage Management Console, how it is organized and used. It also describes how navigation to Interstage Management Console locations is described.

The Interstage Java EE Admin Console can be accessed via the navigation frame.

3.1.1 Browsers Supported by the IMC

The following web browsers are supported for correct operation of the IMC:

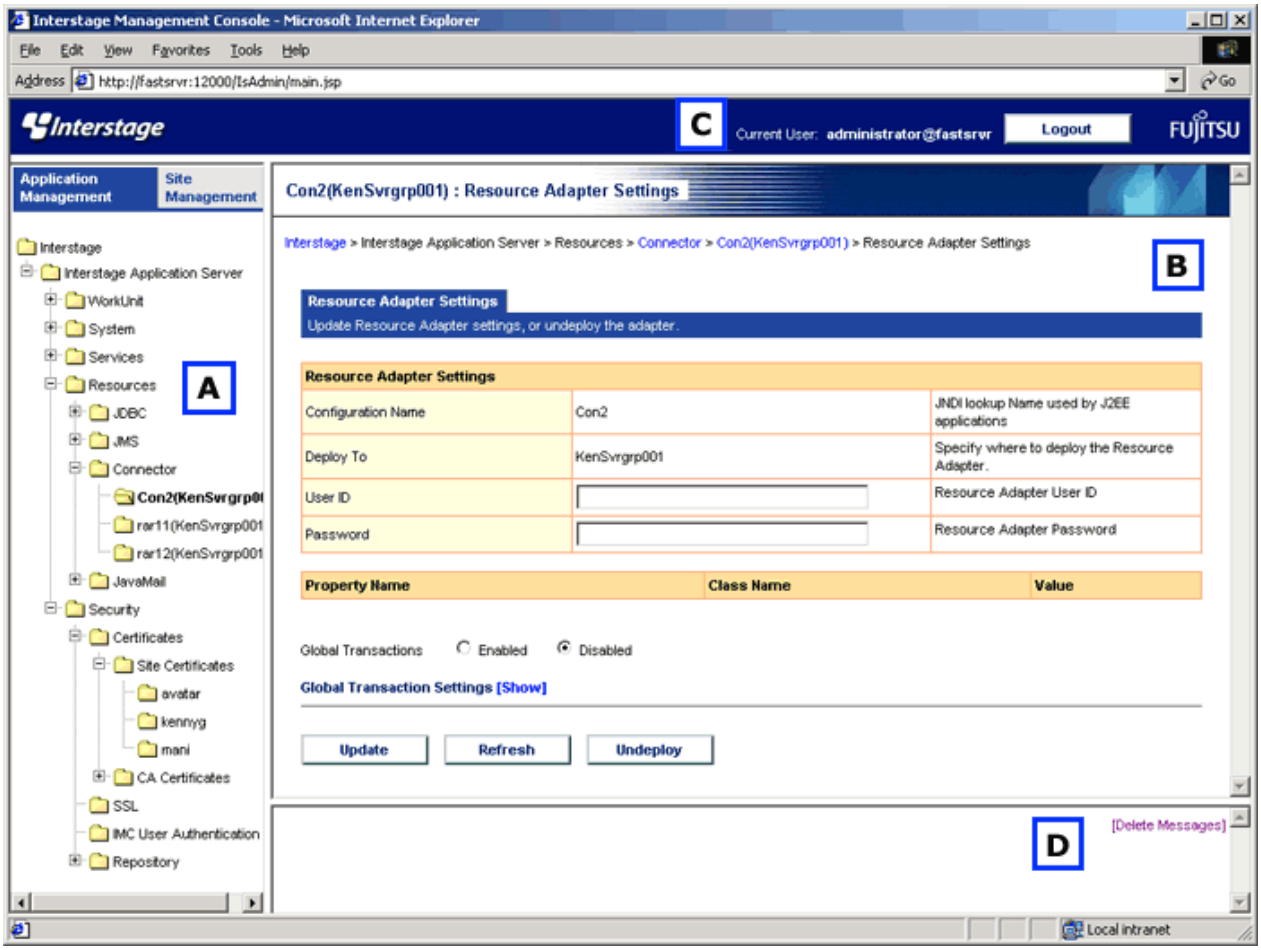
- 32-bit edition Microsoft(R) Internet Explorer 7, 8, 9, and 10

The browser's navigation buttons (Back, Forward, Stop, Refresh and Go To) should not be used during Interstage Management Console Usage, as this may result in display inconsistencies.

To use the Interstage Management Console, configure the settings so that cookies are used in the Web browser.

3.1.2 Layout of the Interstage Management Console

Figure 3.1 Interstage Management Console



The Interstage Management Console consists of four areas:

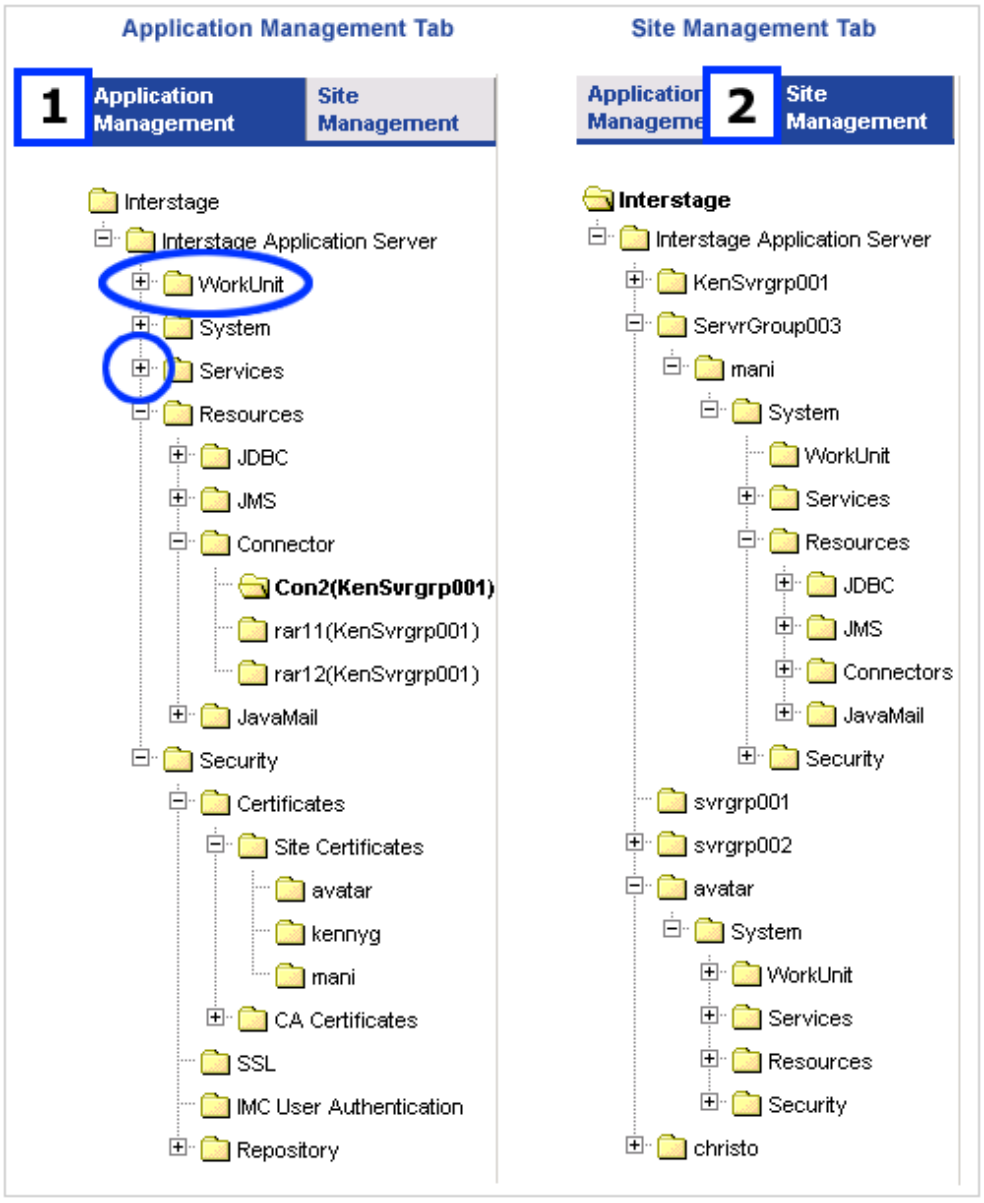
- A.The **navigation frame** is the left frame of the browser. It contains the navigation tree for movement through the Interstage Management Console which provides access to the system and its components. For more details, refer to "3.1.2.1 Navigation Frame".
- B.The **operations frame** is the large center-right frame of the browser. All Application Server operations performed through the Interstage Management Console (with the exception of login and logout) are performed from the Action tabs in this frame. For more details, refer to "3.1.2.2 Operations Frame".
- C.The **ID frame** is the top frame of the browser. It identifies the currently logged-in user and contains a button for logout. The Fujitsu and Interstage logos are also in this frame and link to the international Fujitsu and Interstage web sites.
- D.The **status frame** is located under the operation's frame, in the bottom-right of the browser. This is used to display messages to the user, including reporting operation status.

  Each message has an identification number. Clicking the message ID number, displays a more detailed explanation of the message.

  Clicking the **[Delete Messages]** link deletes all messages from the status frame.

3.1.2.1 Navigation Frame

Figure 3.2 Navigation Frame



The content of the navigation frame varies depending on the point of access as follows:

- Windows32/64 Solaris32 Linux32/64
  The Admin Server navigation frame contains two tabs each containing a navigation tree:

  1. The **Application Management** tab navigation tree provides the ability to configure and operate Independent Managed Servers and Server Groups. This includes the creation and deployment of resources and WorkUnits required by applications. Other typical Application Management tab operations include starting and stopping the Interstage Service itself, Transaction Service, Web Server and WorkUnits of Independent Managed Servers and Server Groups.

     For Servers added to a Site (Managed Servers), the creation, update and deletion of System settings, WorkUnits, Services, Resources and Security configurations can ONLY be done from the Application Management tab.

  2. The **Site Management** tab navigation tree is used for site, server groups and servers specific operations including the addition and deletion of servers to the site; and creation and deletion of server groups. Other typical Site Management tab operations

include viewing and monitoring the Services, Resources and WorkUnits of individual Servers (whether they are Independent Managed Servers or Managed Servers in a Server Group).

Operation from the individual server node in the Site Management tab is the same as operation when directly logged in to the management console on that server.

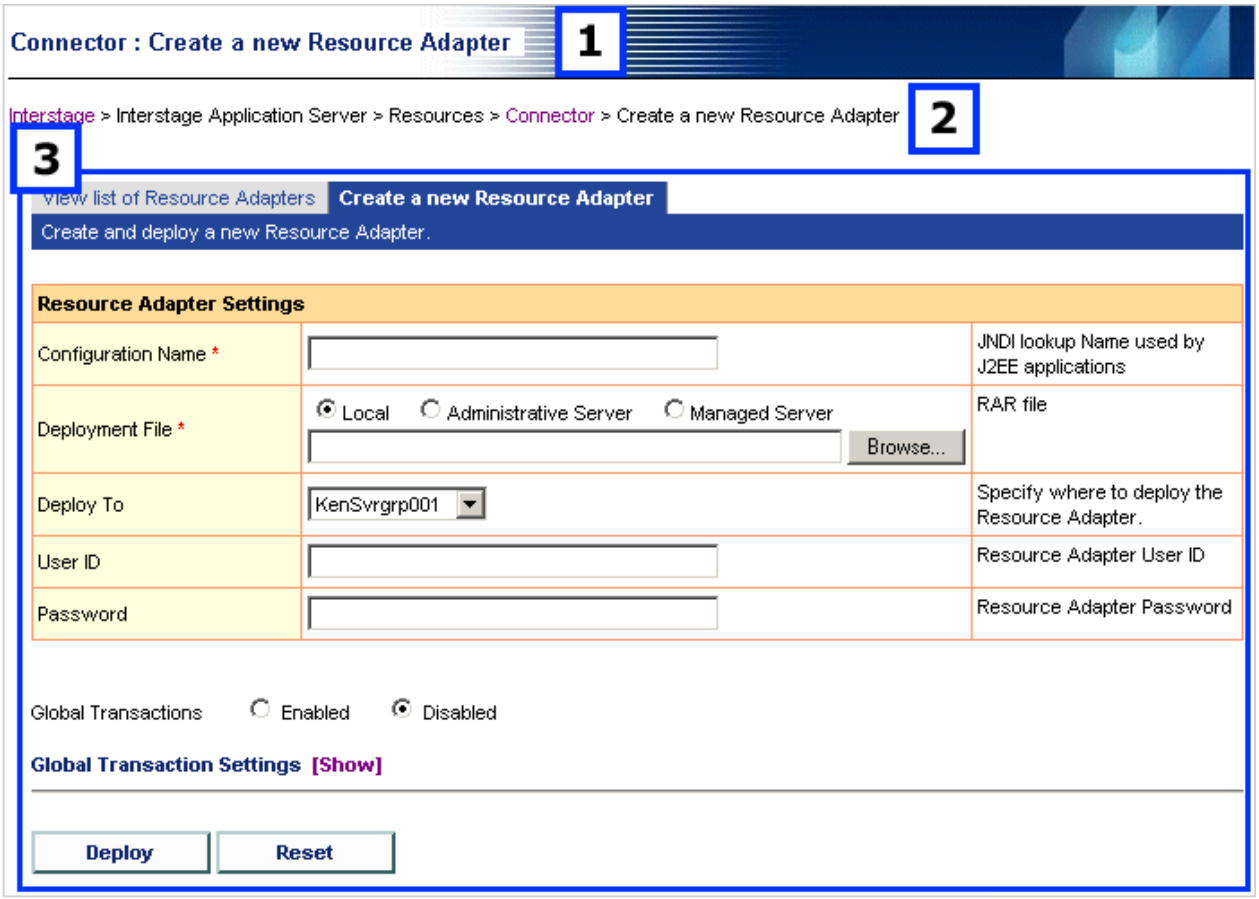
- When logging in directly to a Managed Server, the navigation frame contains a tree that is the same as the tree shown when logging on to a Standalone Server. Operations available are the same except that no updates can be performed.
- Standalone Server contains one tree used for navigation and management of that server. Operations available are the same as those described for the Application Management tab of the Admin Server below except that they apply to the standalone server only.

Clicking a node in the navigation tree provides access to information and operations available for the item represented by the node in the operation's frame. For example, clicking System in the Application Management tab displays a tab containing this system's status information in the operation's frame. The active tree node remains highlighted until another node is selected.

Expandable nodes are expanded by clicking the '+' symbol to the left of the node. This opens the child nodes. Some nodes can only be expanded. These nodes have sub nodes but do not access any specific information.

3.1.2.2 Operations Frame

Figure 3.3 Operations Frame



The Operations frame is located to the right of the navigation frame. It displays information corresponding to the item represented by the highlighted node on the navigation tree. It generally contains the following:

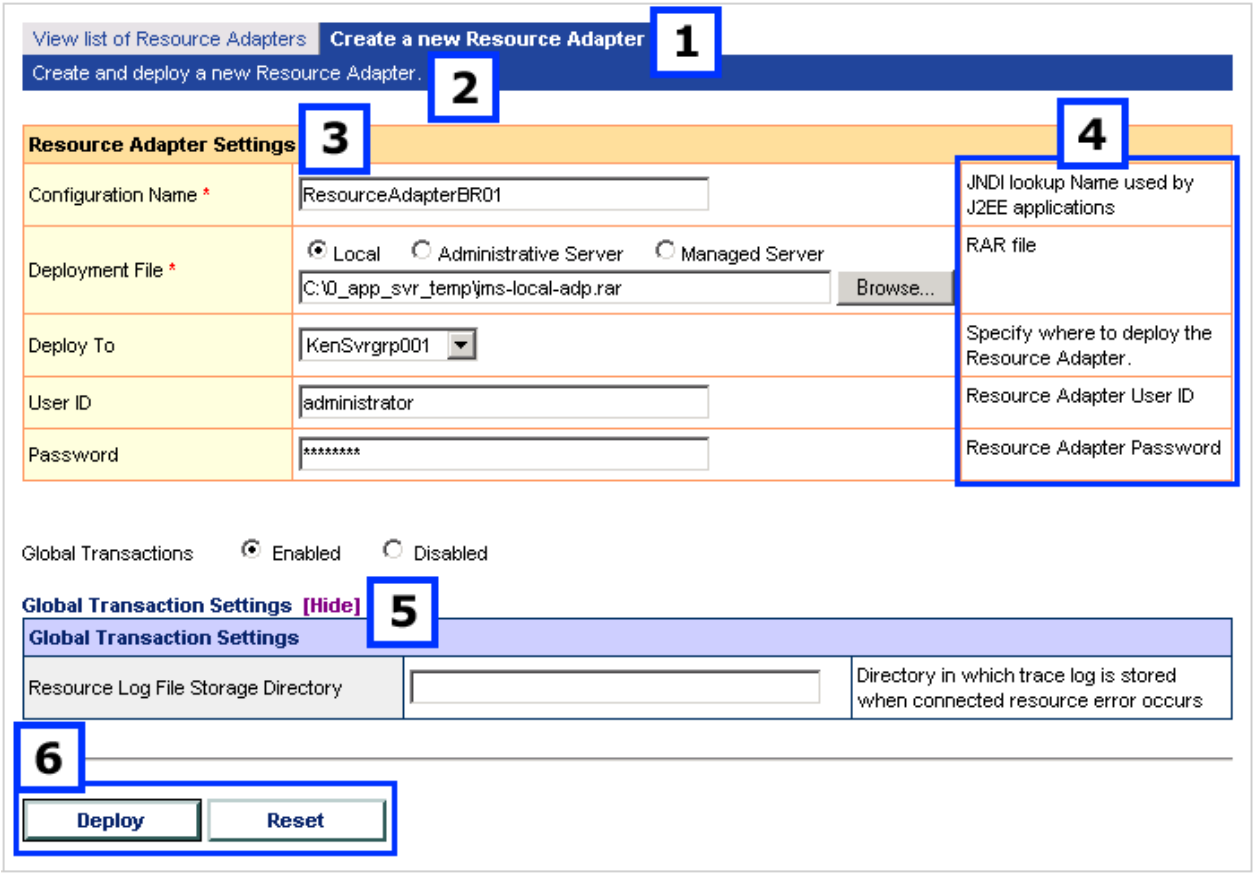
1. **Current operation** shows the item being manipulated (gives the selected tree node) and identifies the operation is being performed.
2. **Navigation path** shows the path from the top node of navigation tree to the highlighted node. The active operation's frame tab is appended to the navigation path. This can be used as a reference when the navigation frame is minimized.

3. **Action tabs** are used to access information and settings for the item represented by the highlighted navigation tree node. The number and type of Action tabs is dependent on the item being manipulated.

   Most operations with the exception of login and logout are performed through the Action tabs.

3.1.2.3 Action Tabs

Figure 3.4 Action Tab



Action tabs contain one or more tables of information and buttons relating to the item. The information may be for view only or it may be editable. The number of tables and buttons and the content on a tab varies depending on context.

1. The **tab caption** identifies the tab, generally providing the name of the item being manipulated and the type of information contained on the tab for that item. An example of this is 'Resource Adapter Settings'.
2. The **tab description** outlines what functions can be performed from the selected operation's frame tab.
3. The **orange tables** contain information about the item represented by the highlighted tree node. This may be a list of instances of the item, for example when the JavaMail resource node is selected, the table in the View JavaMail Configurations tab is a list of all JavaMail configurations, or it can be general status information.

   In editable tables, such as in a new item creation tab, the oranges tables allow such information as item name and basic settings to be defined. For example, in the Create New WorkUnit tab, the WorkUnit name and type are defined in the base table.

   Fields that must be completed contain a red star.
4. The **help column** provides an explanation of the control it corresponds to.

   Help is visible only if it has been switched on. To switch help on, click the Interstage navigation tree node, and in the Console Preferences tab, in On-Screen Item Description, click Enable.

5. Where more information than that contained in the base tables is available, a Detailed Settings **[Show]** link is provided. Clicking the **[Show]** link expands the page to display all available tables. The text on the link changes to [Hide] and is used to hide the detailed settings.

   We refer to additional tables (generally purple) as Detail Tables. Generally Detail Tables allow customization, or in the case of information only tabs, they display more specific information on the items in the base tables.

   The number of tables and their content varies and is context dependent, often varying according to the user's selections. Continuing the WorkUnit example, in the Create New WorkUnit tab, several Detail Tables allow all aspects of the WorkUnit to be configured, but the tables provided differ according to WorkUnit type.

6. **Action Buttons** are located at the base of the Action tab. Buttons vary depending on context, and operate on the content in the tab.

   Further Action buttons may be located within a section of the tab. In this case clicking the buttons affect only information contained within that section.

   Most of the buttons are self explanatory. Some common action buttons are described below. Other buttons are explained where encountered throughout the document.

   - Update - updates the item in the tab with the changed settings.
   - Refresh - refreshes the action tab with the most recent information. This may be information changed by another user.
   - Reset - resets the form to the default values.
   - Delete - deletes the selected list items, or deletes the item in the active tab.
   - Start - starts the selected list items, or starts the item in the active tab.
   - Stop - stops the selected list items, or stops the item in the active tab.
   - Select All - selects all list items.
   - Browse - used to search and select a file for upload to the server.

3.2 Using this Manual to Find your Way Round the GUI

This section describes conventions used in this document to represent on-screen:

3.2.1 Location in GUI

The location of items in the GUI is represented using the following table.

navigation tab

navigation tree path > separated by angle brackets	tab in operation's frame

where:

- 'navigation tab' gives the active tab in the navigation frame. This is displayed as **Application Management**, **Site Management** or **Standalone** in the case of Standalone servers, where there are no tabs in the navigation frame. Managed server operations are the same as that shown from a server node in the Site Management tab.

  Where an operation is available for both standalone and in multi-server, both navigation paths are given.

- 'navigation tree path' provides the path in the navigation tree to the highlighted node representing the item currently being operated on.

- 'operation's frame' gives the tab selected in the operation's frame.

Example

Application Management

Interstage > Interstage Application Server > Security > Certificates > Site Certificates	Certificates

Standalone

Interstage > Interstage Application Server > System > Security > Certificates > Site Certificate	Certificates

3.2.2 Detail Tables

Detail tables allow customization of items. The location of detail tables in the GUI is represented using the following table style.

active tab in operation's frame	name of link for detailed settings	name of detail table

where:

- 'active tab in operation's frame' is the active tab in the operation's frame.
- 'name of link for detailed settings' gives the name of the link in the operation's frame used to access this detailed table.
- 'detail table' is the name of the table itself.

Example

Settings	Detailed Settings	WorkUnit Settings

Note

- Detail tables are generally described as a subsection of the operation performed from an action tab. The navigation tree node and path are identical to those given in the parent description.

3.2.3 Navigation Tree Path

The tree nodes from the top navigation tree node to the highlighted node are listed, separated by the forward angle-bracket character '>'.

User Defined Items

Square braces [] are used to denote user defined items as shown for [configuration name] in the following example:

Interstage > Interstage Application Server > Resources > JavaMail > [configuration name]	View JavaMail Configurations

Here [configuration name] is used to direct you to the tree node representing a user defined JavaMail configuration.

Multi-path Nodes

Where an operation being described is the same for more than one item (represented by different tree nodes), all nodes are given separated by the '|' character, as shown in the following example.

Interstage > Interstage Application Server > Resources > JMS > ConnectionFactory > QueueCF | TopicCF	View Configurations

In this example, this indicates that the operation is the same for both QueueCF and TopicCF type ConnectionFactories.

Chapter 4 System

4.1 System Overview

From the System node of the Interstage Management Console it is possible to start and stop the main Interstage service, view the system status and modify several basic system settings and background system service definitions.

These include:

- System settings:
  - J2EE classpath
  - Enabling Web Server service start/stop synchronization with the Interstage service
  - Enabling automatic performance enhancement
  - Component Operation mode
- System services:
  - CORBA Service
  - Naming Service (NS)
  - Interface Repository (IR)
  - Event Service
  - Transaction Service (OTS) Windows32/64 Solaris32 Linux32/64
  - Servlet Service (standalone servers only)
  - EJB Service.

Windows32/64 Solaris32 Linux32/64

In a multi-server environment, members of Server Groups share common system settings and must be configured from under the System node of Application Management tab for the group as a whole. Independent Managed Servers are configured in the same way. It is only possible to view system settings for individual Server Group members via the Site Management tab.

The main Interstage service must be started and stopped on each Server Group and Independent Managed Server in the site. This will automatically start or stop Interstage on all members of a Server Group. If necessary, for maintenance purposes it is also possible to start and stop Interstage on individual Managed Servers in a group via the Site Management tab.

The system setup for a Standalone server is virtually the same, the exception being that it is possible to configure the servlet service so that the Web Server and WorkUnits can run on separate machines (this is assumed in a multi-server environment).

When a Server Group containing Managed Servers is created (or an Independent Managed Server is added to the site), they automatically appear under the System node of the Application Management tab with default settings and the main Interstage service running.

4.2 Viewing a System Summary in a Multi-server Environment

Windows32/64 Solaris32 Linux32/64

Application Management

Interstage > Interstage Application Server > System	View Server Groups/Servers

Servers and Server Groups are listed and the Interstage service status is given for each.

System status can be:

- Not set up

- Setup in progress (*1)
- Stopped

  For Server Groups, the status will only be 'Stopped' if all servers in the group are stopped.
- Startup in progress (*1)
- Running

  For Server Groups, if some servers did not start successfully, 'Running (partially)' will be displayed.
- Stopping in progress (*1)
- Pre-start startup in progress (*1)

  Server Groups, that are clustered, have a stand-by server which provides failover support. 'Pre-start startup in progress' refers to the state when the stand-by server starts up to provide failover support while the regular server is down.
- Unknown

  This is displayed when the Admin Server cannot get information about the Managed Server(s) for an unknown reason.

*1Server Groups only.

Click an item from the list to display details for that Server Group/Independent Managed Server.

Click the **Refresh** button to refresh the list.

4.2.1 Viewing the System Status

Application Management

Interstage > Interstage Application Server > System > [server group name] | [independent managed server name]	Status

Standalone

Interstage > Interstage Application Server > System	View System Status

The status of the Interstage System for this Standalone Server/Server Group or Independent Managed Server is displayed. The status column indicates if the Interstage Service is 'running' or 'stopped'.

Click the **[Show]** link to view the status of other services.

4.2.2 Starting Interstage

Application Management

Interstage > Interstage Application Server > System	View Server Groups/Servers

In a multi-server environment, check the checkbox corresponding to Server Groups/Independent Managed Servers to start.

Click the **Start** button. This starts all services set up on the selected Server Group(s)/Server(s).

Standalone

Interstage > Interstage Application Server > System	View System Status

Click the **Start Interstage** button. This starts all services set up on the Standalone Server.

In both multi-server and Standalone, the System Status updates to reflect the new status of system(s).

Note

- Starting the Interstage service starts all services provided by Interstage.
- In a multi-server environment, if one or more servers in a Server Group fail to start, the service is still started on those without problems. Rectify the problem, and then click the **Start** button again to retry starting the service for the remaining servers.
- If they are required, the Event Service and Transaction Service must be activated by selecting **Yes** for these under the **Detailed Settings** of the **Environment Settings** tab. For further details, refer to 4.2.3 Activating the Event Service and the Transaction Service.

4.2.3 Activating the Event Service and the Transaction Service

Application Management

Interstage > Interstage Application Server > System > [server group | independent managed server]	Environment Settings

Standalone

Interstage > Interstage Application Server > System	Update System Settings

Click the **[Show]** link, and then select **Yes** in the Event Service Settings table, and select **Yes** in the Transaction Service (OTS) Settings table, and click the **Update** button.

Note

- OTS is linked to Interstage and starts/stops when Interstage is started/stopped.

4.2.4 Stopping Interstage

Application Management

Interstage > Interstage Application Server > System	View Server Groups/Servers

Standalone

Interstage > Interstage Application Server > System	View System Status

To stop Interstage:

1. In a multi-server environment, check the checkbox corresponding to the Server Groups/Independent Managed Servers on which the Interstage is to be stopped.

   Click the **Select All** button to select all systems (Servers and Server Groups) in the list.

2. Click the **Stop Interstage** button.

3. Select:

   - **Normal stop** to have the user application services stop (Component Transaction Service (TD), JTSRMP and OTS transactions). This can only happen if no WorkUnits are currently running on the Servers/Server Groups being stopped (only the JTSRMP service will stop in this case). Other system services are not stopped.

     If WorkUnits are running, a message is displayed in the status frame and Interstage continues running. Either stop running all relevant WorkUnits and then perform the stop Interstage operation again, or use one of the following force stop options.

   - **Forced stop of all user application services only** to shutdown the user application services (Component Transaction Service (TD), JTSRMP and OTS transactions) plus any running WorkUnits, regardless of whether they have been stopped or not. Other system services are not stopped.

   - **Forced system stop** to stop all Interstage services, including system services.

4. Click the **Execute** button to stop the service(s).

5. Click the **OK** button to confirm the stopping of Interstage

   The Status field will display Stopped for systems that have been stopped as well as those not already running.

   In a multi-server environment, click the **[Show]** link to view the result of the operation on each server in a Server Group.

Note

- If one or more servers in a Server Group fail to stop, the services are stopped on those servers that are without problems. Address the problem, and then retry stopping the service on the remaining servers.

4.3 Managing the System

This section describes:

4.3.1 Viewing the System Services

Application Management

Interstage > Interstage Application Server > System > [server group | independent managed server]	Status

Standalone

Interstage > Interstage Application Server > System	View System Status

Click the **[Show]** link to view the status of services that are setup on this system.

Interstage Services currently setup on this system are displayed.

4.3.2 Configuring System Services

Application Management

Interstage > Interstage Application Server > System > [server group | independent managed server]	Environment Settings

Standalone

Interstage > Interstage Application Server > System	Update System Settings

Be default, the following configuration can be viewed/updated:

- Server Group/Server information (*1)
- J2EE Settings
- Synchronized Services

Under Detailed Settings, expandable tables allow the configuration of:

- System
- CORBA service
- Naming service
- Interface repository
- Event service
- Transaction service (OTS)
- Servlet service (*2) and
- EJB service.

*1 View only

*2 Standalone only

1. Under J2EE Settings, specify the **Classpath** for J2EE applications, separating multiple classpaths with carriage returns, and specify the **J2EE Common Directory** if the default is not to be used. If the default is not used and a new value is specified, the J2EE common directory is initialized. Also specify the **Path** for J2EE applications, and the **Java VM Options** specified in the Java command.
2. Under Synchronized Services, select:
   - **Synchronized** to have the Web Server start/stop when Interstage starts/stops.
   - **Not Synchronized** to have Interstage and Web Server start and stop independently.

Click the Detailed Settings **[Show]** link to access settings for individual services.

To update the service configuration:

1. Click the System Settings **[Show]** link, and in **Component Services Operation Mode** select:
   - **mode1** to have Interstage stop when any component service is stopped.
   - **mode2** to have Interstage continue running when any component service is stopped.

2. In **Automatic Performance Enhancement**, select **Enable Automatic Enhancement** to have Interstage automatically increase default system parameters in response to high server loads.

   Note that system settings once increased must be restored manually.

3. Click the CORBA Service Settings **[Show]** link to access these settings for update. For details on configuring CORBA Service Settings, refer to 4.3.3 Configuring the CORBA Service.

4. Click the Naming Service Settings **[Show]** link to access these settings for update. For details on configuring Naming Service Settings, refer to 4.3.4 Configuring the Naming Service.

5. Click the Interface Repository Settings **[Show]** link to access these settings for update. For details on configuring Interface Repository Settings, refer to 4.3.5 Configuring the Interface Repository.

6. Click the Event Service Settings **[Show]** link to access these settings for update. For details on configuring Event Service Settings, refer to 4.3.6 Configuring the Event Service.

7. Click the Transaction Service (OTS) Settings **[Show]** link to access these settings for update. For details on configuring OTS Settings, refer to 4.3.7 Configuring the Transaction Service (OTS) .

8. If configuring a Standalone Server, click the Servlet Service Settings **[Show]** link, and in **Run Web server and WorkUnit on the same machine**, select **Yes** if to set these to operate on the same machine.

9. Click the EJB Service Settings **[Show]** link.

   - In **Use EJB QL Extension of CMP2.0**, select **Yes** to enable use of the extension for the CMP2.0 Entity Bean.
   - In **Judge CMP1.1 byte array update**, specify the method to judge whether the byte array CMF is updated when judging whether to UPDATE CMP instance data in the database. Select between a method to judge whether data is updated for each array element or to judge whether byte array reference is updated.
   - In **Speed up CMP2.0 item search**, specify whether to speed up the search for all CMP2.0 Entity Bean items. Select whether to set each Bean/relationship or to update all Beans/relationships.

10. Click the **Update** button to apply the new configuration to the Server Group or Server.

4.3.3 Configuring the CORBA Service

Update System Settings	Detailed Settings	CORBA Service Settings

1. Specify the **Port Number** for the CORBA Service. Default is 8002.

2. Specify the **Maximum number of client connections** for CORBA clients.

3. Specify the **Maximum number of client requests** from CORBA clients.

   These values should be as low as possible to reduce the memory used by these connections.

4. Specify the **Client connection timeout** in seconds for CORBA clients as a non-zero value. If set to zero, the client will wait for a response indefinitely without relinquishing the connection.

5. Select an **IP Version**.

   'IPv4-dual' supports both IPv4 and IPv6 connections. IPv4 is recommended for client operation.

6. Specify **Server Idle Timeout** in seconds between server response to a client and a subsequent request from that client. The time is specified in 5-second increments. Any other number is rounded down to the nearest multiple of 5.

   If no further request is received during this period, the client connection is closed and associated memory resources freed. This parameter is ignored if a value of zero is specified.

7. Specify **Client Idle Timeout** in seconds during which the server will wait for communication from the client. The time is specified in 5-second increments. Any other number is rounded down to the nearest multiple of 5. This parameter is ignored if a value of zero is specified.

8. In **Use proxy for HTTP tunneling?**, specify if HTTP tunneling for RMI should be enabled.
9. Specify the **Proxy Server Hostname** for HTTP tunneling.
10. Specify the **Proxy Server Port Number** for HTTP tunneling.
11. In **Enable SSL encryption**, determine whether should use SSL for the CORBA service.
12. Specify the **SSL listen port** for the CORBA service (only if **Enable SSL encryption** is **Yes**).
13. In **Select an SSL configuration**, select one of the previously defined SSL configurations to use for SSL setup (only if **Enable SSL** encryption is **Yes**).

4.3.4 Configuring the Naming Service

The Naming Service can be configured on the local (default) server or on a remote server.

If a remote host is selected during naming service detailed setup, selection of a reference source Server Group automatically sets the host name in accordance with the server rank within the Server Group. However, if multiple business IP addresses are set, the host name can be selected. If IPCOM is selected as the reference source, specify the host name.

Update System Settings	Detailed Settings	Naming Service settings

1. Click the **[Show]** link to access the Naming Service Detailed Settings.
2. Windows32/64 Solaris32 Linux32/64
   In a multi-server environment, click the **Copy** button to copy the Interface Repository settings.
3. In **Use Remote Host for Naming Service?**, select **Remote Host** to enable use of a remote host for the Naming Service. Local Host is the default.
4. On a Standalone system, if **Remote Host** is selected specify a **Server Hostname** and **Port Number**.
5. Windows32/64 Solaris32 Linux32/64
   In a multi-server environment, if **Remote Host** is selected, in **Relation** select:
   - **Line**

     Select a participant from **Specify where to refer to** drop down list.

     Specify the **Port** Number.

     Select a **Business IP Address**.
   - **Use IPCOM load balancing**

     Specify the **Representative Hostname**.

     Specify the **Port Number**.

Note

- If the Naming Service is local, no setup is required.

4.3.5 Configuring the Interface Repository

Update System Settings	Detailed Settings	Interface Repository Settings

1. Click the **[Show]** link to access the Interface Repository Detailed Settings.

2. Windows32/64 Solaris32 Linux32/64
   In a multi-server environment, click the **Copy** button to copy the Naming Service settings.
3. In **Use Remote Host for Interface Repository?**, select **Remote Host** to enable use of a remote host for the Interface Repository. Local Host is the default.
4. On a Standalone system, if **Remote Host** is selected specify a **Server Hostname** and **Port Number**.
5. Windows32/64 Solaris32 Linux32/64
   In a multi-server environment, if **Remote Host** is selected, in **Relation** select:

   - **Line**

     Select a participant from **Specify where to refer to** drop down list.

     Specify the **Port Number**.

     Select a **Business IP Address**.

   - **Use IPCOM load balancing**

     Specify the **Representative Hostname**.

     Specify the **Port Number**.

Note

- If the Interface Repository is local, no setup is required.

4.3.6 Configuring the Event Service

Update System Settings	Detailed Settings	Event Service Settings

To configure the Event Service:

1. Select **Yes** in the Event Service title bar to enable the Event Service and then click the **[Show]** link to access the settings.
2. In **Maximum number of connections per dynamic EventChannel**, specify the maximum number of simultaneous Supplier and Consumer connections to dynamic EventChannel.
3. In **Maximum number of processes per dynamic EventChannel**, specify the maximum process concurrency for dynamic EventChannels.
4. In **Enable SSL encryption for dynamic EventChannels**, select **Yes** to enable SSL encryption for dynamic EventChannels.
5. In **Automatic recovery for dynamic EventChannel connections**, select **Yes** to have connection information automatically saved if either the Supplier or Consumer disconnects abruptly.

4.3.7 Configuring the Transaction Service (OTS) Windows32/64 Solaris32 Linux32/64

If a global transaction function is to be used in a multi-server environment, the OTS system (created with 'sys' as the OTS system mode) is set up on a cluster node group or a Standalone server. An OTS system cannot be created on an ordinary Server Group. Instead, a resource management program (which is an OTS system with a mode of 'rmp') can be created.

The procedure below can be used for setup of the OTS server and resource management servers. Differences are specified where necessary.

Update System Settings	Detailed Settings	Transaction Service (OTS) Settings - Detailed Setup

To configure OTS:

1. Select **Yes** in the title bar of the Transaction Service Settings to enable OTS, and then click the **[Show]** link to access the settings.
2. In **System Mode**, select:

   - **sys** to create an OTS system

     Sys should be selected if both a transaction service and a resource management program, or OTS only run on the target cluster node.

   - **rmp** to create a resource management program

     Select rmp if only a resource management tool will run on the target Server Group/Server.

   This value must be set to 'rmp' if setting up on a Server Group.

   Multiple transaction services cannot be created in the same domain, except in the case of building a cluster system.
3. If System Mode is set to 'sys', in **Transaction Log File**, specify the storage location and file name for the transactions log file.
4. In **Maximum Number of Transactions**, specify the maximum number of global transactions that can be handled in a domain.
5. Specify **OTS System Concurrency** (Maximum is 31).
6. In **JTS RMP Process Concurrency** and **JTS RMP Thread Concurrency**, specify the process and thread concurrency respectively for the JTSRMP process that handles transactions between a J2EE application and a resource.
7. In **Maximum Number of resources per global transaction**, specify the number of resources that can be used for a global transaction.
8. If the System Mode is set to 'rmp', specify the **Naming Service Hostname** and the **Naming Service Port Number**

   The values specified here must be those of the server on which the Resource Management Program is setup.
9. Specify the **Node Type**. Normally, select **Active** for this configuration. In case of using cluster system, select **Active** or **Standby** depending on the node settings.
10. Define the required settings in the **Transactions Service Detailed Settings** form found below the OTS Detailed Setup form.

- In a multi-server environment, participants with System Mode set to 'sys' in step 2 above can be selected for creation of the OTS transaction service from the Transaction Service (OTS) child node of the Services node in the Application Management navigation tree node. Those set to 'rmp' are available for creation of the JTSRMP transaction service from the Transaction Service (JTSRMP) child node.

4.3.7.1 Specifying Transaction Service Detailed Settings

The following procedure describes how to set the Transaction Service settings when distributed transactions are used.

Update System Settings	Detailed Settings	Transaction Service (OTS) Settings - Transaction Service Detailed Settings

To configure the Transaction Service settings for distributed transactions:

1. Specify the **Transaction Timeout** in seconds to define the maximum length of any transaction.
2. Specify the **Two-phase Commitment Timeout** time in seconds for the maximum wait time for a 2-phase commit.

3. In **Maximum number of transaction per resource**, specify the maximum number of global transactions that can be handled to a resource at the same time.

   For best performance, this setting should be greater than OTS system concurrency. The value should be doubled if used with J2EE model.

4. In **Path for JDK/JRE for JTS RMP**, specify the absolute path to the Java command used to start JTSRMP.

5. A trace file logging transactions can be output. In **Trace Mode**, select 1, 2 or 3 as follows:

   1) Trace output only for errors

   2) Trace file is always output

   3) Trace file is not output. To generate a trace file if needed, use the 'otsgetdump' command.

   The trace file is located in 'installation directory\ots\var'.

6. In **Trace Level**, specify level of logging for the JTS environment information as an integer between 0 and 5. A value of zero corresponds to no trace output. Higher values result in increasing trace detail.

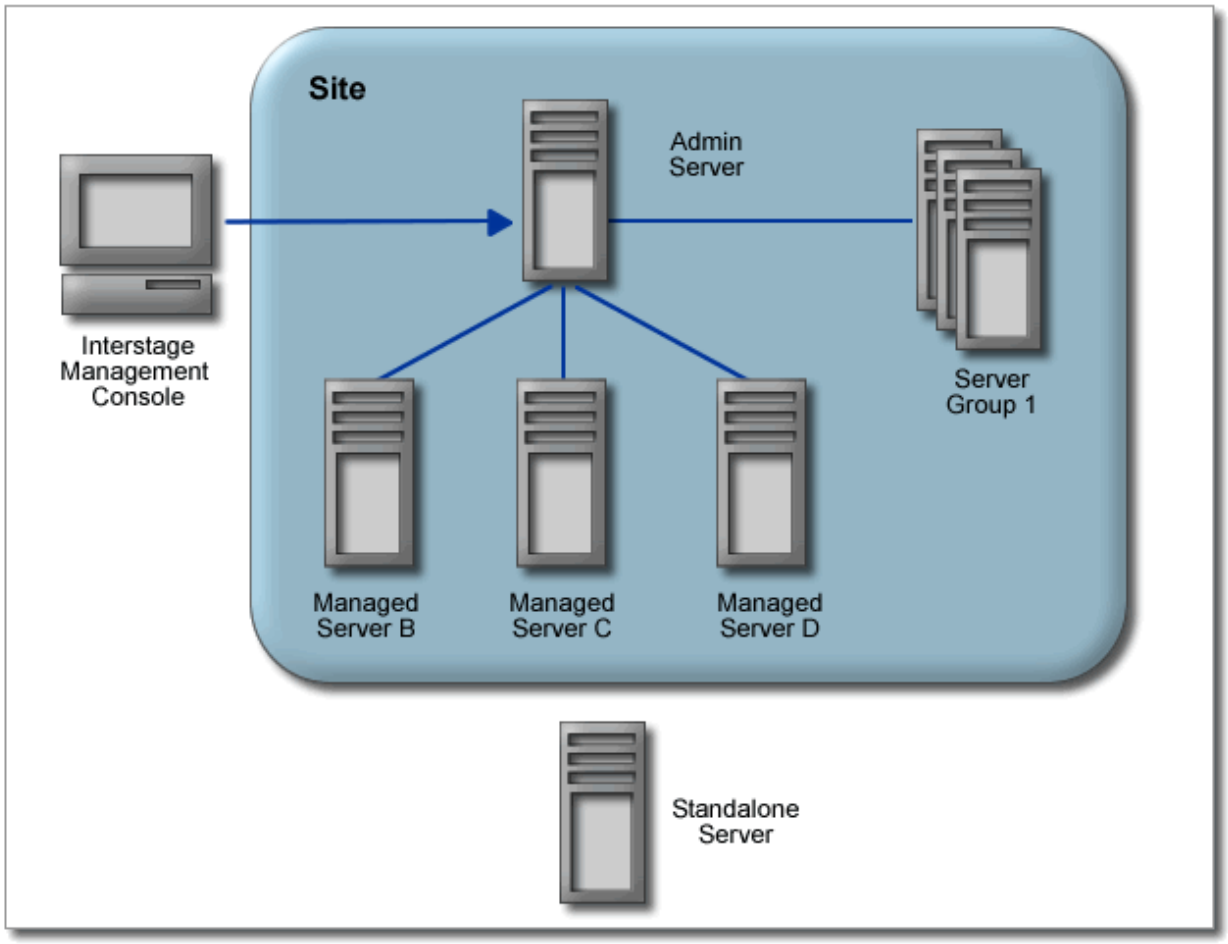
   Note that as the trace level is increased, performance is reduced.

Chapter 5 Site Windows32/64 Solaris32 Linux32/64

5.1 Site Overview Windows32/64 Solaris32 Linux32/64

The site setup is available only when a user logs in to a server in a multi-server environment.

Figure 5.1 Site



A Site consists of multiple servers on a LAN controlled from a single server. Business operations can be distributed across servers in the site.

Admin Servers

The Admin Server manages Managed Servers that participate in the site. All the servers in a site can be managed from within the Interstage Management Console (IMC) of the Admin Server. An Admin Server can control up to 100 servers.

Managed Servers

Servers managed by the Admin Server are called Managed Servers.

A Managed Server cannot participate in more than one site. During addition of a server to a site, the Admin Server checks that the server being added does not already belong to a site. It will not add the server if it does.

A Managed Server can be added to a Site in one of two modes:

- Independent

  When a Managed Server is not intended to be managed as part of a Server Group, the Managed Server must be added to the Site with the 'Independent' mode.

Such servers are referred to as Independent Managed Servers.

- Reserved

  When a Managed Server is intended to be added to a specific Server Group, the Managed Server must be added to the Site with the 'Reserved' mode.

  Such servers are referred to as Reserved Managed Servers.

Server Groups

A Server Group is a logical grouping of Managed Servers. The Admin Server can be used to manage a common configuration for all the Managed Servers in a Server Group. The Admin Server can also be used to operate and manage all the Managed Servers in a Server Group with single operation(s).

A Site can manage one or more Server Groups. A Managed Server can be a member of only one server group.

For details on server groups, refer to the 'Server Groups' chapter.

Standalone Server

A Server that is not managed by an Admin Server is called a Standalone Server. The Standalone Server is managed with the IMC running on that server. Standalone servers can be added to a site, after which they become Managed servers.

During installation, the server type can be set as an Admin Server or Standalone server. The default Interstage installation creates a standalone server.

- Once added to a site, a Managed Server should only be configured via the Application Management tab of the Admin Server. Although the Operator can still log onto the IMC of the Managed Server directly, all configuration and management should be done from the Admin Server.

5.2 Managing a Site Windows32/64 Solaris32 Linux32/64

The Site Management tab of the IMC on the Admin Server can be used to create and manage server groups; add and remove servers from the site and server groups; and for start and stop operations.

5.2.1 Adding a Server to a Site

This procedure describes how to add a server to a Site

Site Management

Interstage > Interstage Application Server	Add Server

To add a standalone server to the site:

1. In **Server Name**, specify a name for the Managed Server being created.

   This name must be unique within the site.

2. In **IP Address**, specify the IP address of the standalone server. This address is used by the Admin Server to communicate with and control the server when it joins the site. In **Business IP Address**, optionally specify the IP address used by IJServer and CORBA applications deployed to this server (other than the Interstage Management Console). This need not be specified if the server has only one IP address.

3. Specify the **User Name** and **Password** of a user with administrative privilege for the Standalone Server being added.

4. In **Managed Server Type**, select the Site Participation Mode as:

   - **Reserved** if the Managed Server is being added to the Site only to be added to an existing Server Group with one or more Managed Servers

     Once a Managed Server has been added to a Site in this mode, no configuration or operation can be performed on this Managed Server until it has been added to a Server Group.

   - **Independent** if the Managed Server is being added to the Site to be managed as a separate Server.

     An Independent Managed Server can be added to a Server Group only if it is the first Managed Server added to that Server Group.

5. Click the **[Show]** link to access the Detailed Settings.
6. In **Connection Protocol**, select the protocol to be used for communication between the Admin Server and the Managed Server:

   - **RMI** (Remote Method Invocation)
   - **HTTPS**

     This is the default protocol.

7. Specify the **Port Number**, for the communication protocol.

   Default: 12200.

8. Click the **Add** button to complete the add operation.

- The IP Address must be IPv4 conformant. The business IP address can be IPv4 or IPv6 conformant. Use IPv4 conformant address to use the business LAN in IJServer.
- In Interstage > Interstage Application Server > System > Update System Settings > Detailed Settings > Transaction Service (OTS) settings, select **No** before adding an Interstage Application server to a site. If Yes is selected, it will not be possible to create an OTS through the Interstage Management Console.
- Only servers of Interstage Enterprise Edition can be added to a Site.
- Managed Servers running a higher version than the Admin Server cannot be added to the Site.

5.2.2 Listing Site Participants

Site Management

Interstage > Interstage Application Server	View Server Groups/Servers

A list of all the participants in the site is displayed. This includes Server Groups, Reserved Managed Servers and Independent Managed Servers.

For each listed participant, the **Type**, operating system **Platform**, Interstage **Version Level** and **Edition** are given.

Click a list item to display details for that server group or server.

- For a Server Group with no Managed Servers the columns for Name, operating system Platform, Interstage Version Level and Edition display the dash ("-") character.

5.2.3 Removing a Participant from the Site (from the Admin Server)

Site Management

Interstage > Interstage Application Server	View Server Groups/Servers

To remove a participant from the site:

1. Click the checkbox corresponding to participants to be deleted.
2. Click the **Delete** button to remove the selected Server(s)/Server Group(s).
   - If the server is a member of a server group, it must be removed from the group before it can be deleted from the site.
   - If the Admin Server cannot communicate with the Managed Server (Managed Server is not running or LAN is down), the Forced Deletion dialog is displayed. Click the **OK** button to confirm forced deletion.

     This deletes the Managed Server configuration information registered at the Admin Server. This is referred to as forced deletion.
3. Click the **OK** button to confirm deletion.
4. Click the **Refresh** button to refresh the list.

Note

- If forced deletion is used (see Step 2 above), this Managed Server must perform a Leave Site operation to become a stand alone server. For details, refer to 5.2.4 Leaving the Site (from Managed Server).

5.2.4 Leaving the Site (from Managed Server)

A Managed Server must leave a site after forced deletion by the Admin Server. This operation is carried out from the command line of the Managed Server using the *isleavesite* command.

The leave mode must always be specified as forced, as follows:

```
isleavesite -f
```

The Managed Server becomes a standalone server on successful execution of the *isleavesite* command.

For details of the *isleavesite* command, refer to Reference Manual (Command Edition).

Note

- Administrator login privileges are required to execute the *isleavesite* command.
- The following conditions must be satisfied before the leave site operation is performed (unless it is being used to change a forcibly deleted Managed Server into a standalone server):
  - The Admin Server and the Managed Server must be running.
  - The Managed Server must be a participant in the Site.
  - The Managed Server must not be part of a Server Group. If it is part of a Server Group, the Managed Server must be deleted from the Server Group before it leaves the Site.

5.2.5 Defining the Configuration Settings

The storage location and the maximum file size for configuration data can be set.

Site Management

Interstage > Interstage Application Server	Configuration Settings

To define the configuration data settings:

1. In **Repository Directory**, specify the directory where repository data is to be stored.
2. In **Maximum Repository Size**, specify the maximum size in bytes to be used for configuration data storage. Set this value to zero to have no size limit.

   When this value is reached or changed the **Maximum Repository Size** less than the size which Interstage is using, an error similar to the following will be output:

   - is20912: The maximum size for the repository has been exceeded. (SIZE=%s)
3. Click the **Update** button to apply the changes.
4. Click the **Refresh** button to refresh the settings

5.2.6 Environment Settings

The Site administrator can enable control of J2EE application deployment and configuration of J2EE application settings from Managed Servers. If this option is switched on, then J2EE applications can be deployed from the IMC of a Managed Server to that server only (or to the Server Group of which the Managed Server is a member). This feature cannot be used for CORBA applications.

The same operations can be done using commands.

Site Management

Interstage > Interstage Application Server	Environment Settings

To switch control of J2EE application deployment and application settings:

1. In **Application Operation Mode** select:

   - **Management Operation Mode** to restrict J2EE application deployment control and application settings configuration to IMCs running on the Admin Server.
   - **Stand-alone Operation Mode** to enable J2EE application deployment control and application settings configuration from an IMC running on a Managed Server or on the Admin Server. Control from the Managed Server includes control of any applications deployed to the server (or Server Group of which it is a member).
2. Click the **Update** button to apply the change.

Note

- Application Operation Mode can only be switched from 'Stand-alone Operation Mode' to 'Management Operation Mode' if all servers in a Server Group have the same application(s) deployed to them.
- On a Combined Server, only the Admin Server IMC can be used. In 'Stand-alone Operation Mode', use commands to deploy J2EE applications and configure their settings.

Chapter 6 Server Groups Windows32/64 Solaris32 Linux32/64

6.1 Server Groups Overview Windows32/64 Solaris32 Linux32/64

A Server Group is a logical grouping of Managed Servers that are part of a Site and sharing common configurations and deployments such as Business Applications, Resources and Services. This enables application scalability. Load Sharing can then be managed by the use of a product such as IPCOM. Server Groups can be created, managed and deleted only from an Admin Server.

Specifying a Server Group for deployment during Service setup, and WorkUnit or Resource creation, allows deployment to multiple servers in a single operation. This reduces the management cost and the possibility of human error during multiple server setups.

Server Groups are managed from the Admin Server for that site.

Note

- There can be a maximum of:
  - 100 Servers per site
  - 100 Server Groups per Site
  - 100 Servers in a Server Group.

  As an example, there can be 50 Managed Servers in ServerGroupA, 40 Managed Servers in ServerGroupB and 10 Independent Managed Servers, reaching the site maximum of 100 servers.
- All Servers in any single Server Group must be all of the same operating system platform, edition and version. To support two different platforms, use separate Server Groups.

6.1.1 Managing Server Groups

6.1.1.1 Listing Server Groups in the Site

Site Management

Interstage>Interstage Application Server	View Server Groups/Servers

The Server Group/Managed Server Type column indicates if the list item is a Server Group, Independent Server or Reserved Server.

The operating system Platform, Interstage Version Level, the Edition, and the Number of Servers (in the case of Server Groups) are also given.

6.1.1.2 Creating a Server Group

Site Management

Interstage>Interstage Application Server	Create Server Group

1. In **Server Group Name**, specify a unique name for the Server Group.

   The Server Group name must be unique among all Server Group names and Server names on the site.
2. Click the **Create** button to create the Server Group.

   The Server Group is then displayed on the navigation tree.

Note

- To add servers to the Server Group, use the Add Server tab displayed when the Server Group is highlighted on the navigation tree. For details, refer to 6.1.1.4 Adding a Server to a Server Group.
- Server Groups must have at least one member Managed Server before anything can be deployed to them.

6.1.1.3 Display Server Group Information

Site Management

Interstage>Interstage Application Server > [server group name]	List

If the Server Group contains at least one member Managed Server, information displayed for the Server Group includes Server Group Name, operating system Platform, Interstage Version Level, Edition and the Number of Servers in the group.

Managed Servers that are members of the Server Group are listed along with their IP address.

Clicking the Server Name displays information for that server.

6.1.1.4 Adding a Server to a Server Group

All members of a Server Group must meet the conditions below, where subsequently added Managed Servers must match the setup of first Managed Server added to the Server Group:

- All Servers of a Server Group must be running on the same OS platform (Windows/Solaris/Linux).
- All Servers of a Server Group must have the same Interstage edition (Standard-J Edition, Enterprise Edition etc)
- All Servers of a Server Group must be of the same Interstage version level.

  Typically, the same business applications will use the same Interstage edition and version level. The major and minor version level must be the same (for example, servers running Interstage 8.0.1 and Interstage 8.1.1 cannot be in the same group). Micro version levels may be mixed in version 8 (for example, servers may run Interstage 8.0.1 and 8.0.5).
- The Interstage installation parameters must be the same (package, installation path, home directory etc.).
- The JDK versions of Interstage on the server being added to the Server Group must be the same as that of the JDK version of other servers in the group.

Site Management

Interstage>Interstage Application Server > [server group name]	Add Server

If the Server Group already contains members, the Platform, Interstage Version Level and Edition are displayed. Reserved Managed Servers (servers added to the Site in Reserved mode that are not yet in a Server Group) are listed (for the allowed version level). Information for each list item includes Server Name, Management IP Address, Platform, Interstage Version Level, Edition, and Managed Server Type.

To add a Managed Server to the Server Group:

1. If the Server Group already has Managed Servers:
   - Select a reference member Managed Server
   - Backup the reference member Managed Server and transfer it to the new Managed Server. Refer to 6.1.1.8 Transferring Configuration from One to Other Servers in a Group.
   - Add the Managed Server to the Site in 'Reserved' mode.

2. Click the checkbox to the left of any Managed Server to be added.

   If this is the first Server to be added to the group, Reserved Managed Servers and Independent Managed Servers on this site can be added. If it is not the first Server to be added, then only Reserved Managed Servers can be added.

   Only Managed Servers that meet the conditions in the notes below can be added.

   Click the **Select All** button to select all servers in the list.

3. Click the **Add** button to add the selected server(s).

   Click the **Refresh** button to refresh the list.

Note

- Servers must first be added to the Site before they are available for addition to a Server Group.
- A Managed Server can only belong to one Server Group.
- An Independent Managed Server can only be added as the first member of the group. Several Reserved Managed Servers can be added to a group.
- For further details on participation modes of Managed Servers, refer to the 'Site' chapter.
- The specified server must be active.

6.1.1.5 Removing a Server from a Server Group

Site Management

Interstage>Interstage Application Server > [server group name]	List

To remove a server from the server group:

1. Click the corresponding checkbox for any server to be deleted.

   Click the **Select All** button to select all servers in the list.

2. Click the **Delete** button to remove the selected server(s).
3. Click the **OK** button to confirm deletion.
4. Click the **Refresh** button to refresh the list.

Note

- A Server becomes a Reserved Managed Server and cannot be operated from the Admin Server once removed from the group.

6.1.1.6 Deleting a Server Group

Site Management

Interstage>Interstage Application Server	View Server Groups/Servers

To delete the server group:

1. Click the checkbox corresponding to server groups to be deleted.
2. Click the **Delete** button.

3. Click the **OK** button to confirm deletion.

Note

- Members must be removed from a server group before it can be deleted.

6.1.1.7 Viewing Information of Server Members of a Server Group

Site Management

Interstage>Interstage Application Server > [server group name] > [server name]	Information

Information on the server is displayed including the Server Group Name of which it is a member, the Platform, Interstage Version Level and Edition. The General Settings table displays the Server Name, IP Address, Business IP Address and Managed Server Type.

Click the **Refresh** button to refresh the information.

Note

- Setup on Managed Servers in the Server Group, and Start and Stop operations can be performed from the tree node representing a Server on the Site Management tab.

6.1.1.8 Transferring Configuration from One to Other Servers in a Group

For Servers to operate successfully as a Server Group, they require the same configuration (WorkUnits, Resources, Services etc). This process transfers a single Interstage configuration to multiple servers on the same Server Group.

To transfer the configuration from one server to one or several other servers:

1. Stop all Interstage services on both servers.
2. Backup the configuration of the server to be copied.
3. Restore the backed up files to the server(s) to be added to the server group.
4. Re-start Interstage Services on all servers.

For details on these steps, refer to the 'Maintenance' chapter.

Note

- New configuration defined after servers have been added to the group can be deployed to all group members simultaneously by selecting the group as the 'Deploy To' during configuration definition.

Chapter 7 Resources

7.1 Configuring Resources

Interstage Resources are configurable components that allow J2EE applications to be customized for a particular operational environment. Multiple instances of a resource can be created, configured and managed by Interstage.

The following resources are managed by Interstage:

- JDBC drivers for database connectivity
- JMS (ConnectionFactory and Destination definitions)
- JMS (Event Channels and Stores - Standalone only)
- JavaMail
- Connectors (Resource Adapters) for connecting to Enterprise Information Systems (EIS).

Resources can be created on Standalone Servers, or deployed from the Admin Server to Independent Managed Servers and Server Groups.

Resources for a Site are created and managed from the Application Management tab of the Admin Server. Resource names must be unique within a site.

Resources on a Standalone Server can be created and managed by logging in to the server directly.

Once a resource has been created and deployed to a Server or Server Group of a Site, the deployed location cannot be changed. The resource must be deleted and created again with the new Deploy To location.

7.2 Creating, Updating and Deleting Resources on Server Groups

When creating, updating or deleting a resource on a Server Group and an error occurs on some (but not all) servers in the group, the create/update/delete action is still considered successful. In this case, an error message is posted for servers for which the action failed.

The Resource will be displayed and the operation (Create, Update or Delete) re-executed until it is successful on all Servers. For example, if JDBC Resource JDBC_01 is deleted, and delete fails on one of the Servers in the Server Group, JDBC_01 remains on the Application Management navigation tree (Interstage > Interstage Application Server > Resources > JDBC > JDBC_01), allowing re-execution of the Delete operation. Once the resource is deleted from all Servers of the Server Group, it will be removed from the Resource list.

In the case of a Create failure, select the Resource and click the **Update** button to create the Resource on any Servers on which the create operation failed.

7.3 Configuring JDBC Data Sources

Interstage supports JDBC drivers that implement the JDBC 2.0 API specifications (including the Optional Package).

The Interstage Management Console can be used to configure JDBC data sources.

For a reference of settings related to JDBC in Interstage, refer to "7.3.5 JDBC Data Source Settings Reference".

7.3.1 Creating a New JDBC Data Source

Application Management

Interstage > Interstage Application Server > Resources > JDBC	Create a new JDBC Data Source

Standalone

Interstage > Interstage Application Server > System > Resources > JDBC	Create a new JDBC Data Source

To create a new JDBC Data Source:

1. In **Configuration Name**, specify the name for J2EE applications looking up this data source.

   This name must be unique within a site.

2. In **Database Type** click the type of database to which this Resource will connect J2EE applications to.

3. If accessing from the Application Management tab, in the **Deploy To** list, click the Server Group/Independent Managed Server to which the data source is to be deployed.

4. Specify the values in the Database Definition and Essential Properties tables. Database Definition is displayed as [Name of Database type selected] Definition. If Generic Definition is selected, this table is not displayed. The entries to be made will vary according to the Database Type selected as follows:

   - For Symfoware databases, complete the steps in 7.3.1.1 Database Settings for Symfoware.
   - For Oracle databases, complete the steps in 7.3.1.2 Database Settings for Oracle.
   - For SQL Server databases, complete the steps in 7.3.1.3 Database Settings for SQL Server.
   - For Generic Definition, complete the steps in 7.3.1.4 Database Settings for Generic Definition.

5. Select the checkbox Test for getConnection before create to test the connection.

6. Click the **Create** button to create and deploy the JDBC data source.

7. Click the **Reset** button to reset this form to the default values.

Note

- For a reference list of settings relating to JDBC in Interstage, refer to "7.3.5 JDBC Data Source Settings Reference".

7.3.1.1 Database Settings for Symfoware

7.3.1.1.1 Symfoware Definition

Set **Data Source Type** to one of the following:

- **Use Interstage Connection Pooling**
- **Use Symfoware Connection Pooling**

7.3.1.1.2 Essential Properties

If **Use Interstage Connection Pooling** is selected:

- Specify **User Name** for use by applications when connecting to the database.
- Specify **Password**.
- Set **Protocol** to **Local** or **Remote (RDB2_TCP)**.

  If **Remote** is selected:

  - Specify **Hostname** of the database server
  - Specify **Port number** used to connect to the database.

- Set **Data resource name** to the database name used to connect to the database.
- In **Detailed settings**, click **[Show]**.

  - Set **Output Web server connection information to the Audit Log** to **Yes**.
  - Specify the **Default Schema Name** for the SQL statement used in the application.
  - Set **Other Parameter** to the 'ctuneparam' option.

If **Use Symfoware connection pooling** is selected:

- Specify **User name** for use by applications when connecting to the database.
- Specify **Password**.
- Specify a **Data Source Name** registered with the File System Service Provider's Naming Service.
- Specify the **Naming Service's Hostname**.
- Specify the **Naming Service's Port Number**.
- In **Detailed Settings**, click **[Show]**.
  - Set **Output Web server connection information to the Audit Log** to **Yes**.

7.3.1.2 Database Settings for Oracle

7.3.1.2.1 Oracle Definition

1. Set **Data Source Type** to one of the following:
   - **Use Interstage connection pooling (oracle.jdbc.pool.OracleConnectionPoolDataSource)**
   - **Use Oracle connection pooling (oracle.jdbc.pool.OracleDataSource)**
   - **Use global transaction (oracle.jdbc.xa.OracleXADataSource)**

     This option is only available when 'Interstage > Interstage Application Server > System > Update System Settings > **Transaction Service (OTS) Settings**' is set to '**Yes**'.
2. Select **Use RAC** to use the RAC function.

7.3.1.2.2 Essential Properties

1. If **Use RAC** is selected:
   - Specify **User ID** used for access to the database.
   - Specify **Password**.
   - Specify the **Server URL** used for access to the database.

     Click **Template (thin)** or **Template (oci)** to select the type of template required.
2. If Use RAC is not selected:
   - Specify **User ID** for use by applications when connecting to the database.
   - Specify **Password**.
   - Set **Driver Type/Network Protocol** to the JDBC driver type and network protocol, where:
     - The thin driver is a 100% Java driver for use where the client server(s) hosting the JDBC client (i.e., application) do not have Oracle Client Software installed.
     - The OCI driver uses Oracle Client Software (based on JNI) installed on the client server(s) to communicate with the Oracle installation.
     - TCP means use standard TCP/IP network connections to communicate with the Oracle installation.
     - If the JDBC client (i.e., application) and Oracle installation are running on the same machine, the OCI driver can use IPC (InterProcess Communication) to connect to the database instead of a network connection. An IPC connection is typically faster than a network connection.
   - Set **Hostname** to the database server.
   - Set **Port Number** to the port used to connect to the database.
   - Specify the **SID/Net Service Name** used to identify the Oracle database.

- In **Detailed Settings**, click **[Show]**.
  - If necessary, in Connection Properties and Other Data Source Properties, click Add.
  - If Data Source Type is set to Use Oracle Connection Pooling, then Connection Cache Properties can also be added if needed.
  - If necessary, in Use File System Service Provider, select Yes (this field is only enabled when Data Source Type is set to Use Interstage Connection Pooling and Use RAC is not selected).

  If **Yes** is selected:
  - Set **Provider URL** to the URL of the File System Service Provider's Naming Service.
  - Set **Data Source Name** to the name that will be registered with the Naming Service to identify the database.
  - In **Register data source**, selected **Register** to register the data source in File System Service Provider.

7.3.1.3 Database Settings for SQL Server

7.3.1.3.1 SQL Server Definition

Set **Data Source Type** to:

- **Use SQL Server 2005 (com.microsoft.sqlserver.jdbc.SQLServerXADataSource)**

7.3.1.3.2 Essential Properties

1. Specify **User ID** for use by applications when connecting to the database.
2. Specify **Password**.
3. Specify **Hostname** of the database server.
4. Specify **Port Number** used to connect to the database.
5. Specify **Database Name** for which the data source is being created.
6. In **Detailed Settings**, click **[Show]**.
   - If necessary, in **Other Data Source Properties**, click **Add**.
   - If necessary, in **Use File System Service Provider**, select **Yes**.

   If **Yes** is selected:
   - Set **Provider URL** to the URL of the File System Service Provider's Naming Service.
   - Set **Data Source Name** to the name that will be registered with the Naming Service to identify the database.
   - In **Register data source**, selected **Register** to register the data source in File System Service Provider.

7.3.1.4 Database Settings for Generic Definition

7.3.1.4.1 Essential Properties

1. Specify **Data source class name** used to connect to the database.
2. Set **Log writer** to the file used for log output (the file name must be prefixed by the full path).

   Leave this field empty if no log is to be generated.
3. If necessary, in **Other data source properties**, click **Add**.

7.3.2 Viewing Deployed JDBC Data Sources

Application Management

Interstage > Interstage Application Server > Resources > JDBC	View list of JDBC Data Sources

Standalone

Interstage > Interstage Application Server > System > Resources > JDBC	View list of JDBC Data Sources

A list of JDBC Data Sources is displayed. The **JDBC Configuration Name** and database **Type** is given for each.

When viewing from the Application Management tab of the Admin Server, the Server Group/Independent Managed Server to which the data source was **Deployed To** is also displayed, along with the **Version**.

Click the **Refresh** button to refresh the list.

Click a list item to display details and the status for that data source.

7.3.3 Updating a JDBC Data Source

Application Management

Interstage > Interstage Application Server > Resources > JDBC > [data source name]	Environment Settings

Standalone

Interstage > Interstage Application Server > System > Resources > JDBC > [data source name]	Environment Settings

1. Edit the required settings on the form as described in the tables in section 7.3.5 JDBC Data Source Settings Reference or in 7.3.1 Creating a New JDBC Data Source.
2. Select the **Test for getConnection before update** checkbox to test the JDBC connection before updating. Click the **Update** button to update the JDBC data source settings.
3. Click the **Refresh** button to refresh the form with the most recently updated values.
4. Click the **Test** button to test the connection to the specified Database.

7.3.4 Deleting a JDBC Data Source

Application Management

Interstage > Interstage Application Server > Resources > JDBC	View list of JDBC Data Sources

Standalone

Interstage > Interstage Application Server > System > Resources > JDBC	View list of JDBC Data Sources

To delete a JDBC data source:

1. Click the checkbox to the left of any data source to be deleted.

   Click the **Select All** button to select all JDBC data source in the list.
2. Click the **Delete** button to remove the selected JDBC data source(s).
3. Click the **OK** button to confirm deletion.

7.3.5 JDBC Data Source Settings Reference

The following tables are reference tables for information displayed or configurable from the IMC relating to JDBC data sources.

Note

- An asterisk (*) character inside a field denotes that a value must be specified for that item.

Table 7.1 JDBC Data Source Settings

Field	Value	Description
Configuration Name*	Max 32 chars.	The lookup name seen by J2EE applications for this data source.
Database Type	Symfoware Oracle SQL Server Generic Definition	Four database types and a generic type are supported.
Deploy To	Defaults to the first server on the list. The list is populated from all Server Groups/ Independent Managed Servers on the site.	Click the Server Group/Independent Managed Server from the drop down list to which the data source will be deployed. Application Management View only. This value cannot be updated once the Resource has been created.

Table 7.2 Symfoware Settings

Field	Description
Data Source Type	Select the JDBC driver data source type for Symfoware. - Use Interstage Connection Pooling - Use Symfoware Connection Pooling
User Name*	User ID for use by applications when connecting to the database.
Password*	Password for the User Name above.
Protocol	Symfoware Network Protocol. - Local - Remote (RDB2_TCP)
Hostname	Specify the hostname or IP address of the database.
Port Number	Specify the port number of the database on the hostname specified above. Default: 2050
Data Resource Name	Specify the database resource name (database name) used to connect to the database.
Default Schema Name	Specify the default schema name for the SQL statement used in the application.
Other Parameter	Specify the ctuneparam option for the other parameters.
Data Source Name*	Data source name that will be registered with the File System Service provider's Naming Service.
Naming Service's Host Name*	Host name under which the database is registered with the File System Service provider's Naming Service.
Naming Service's Port Number	Port number of the above host. Default: 10326

Table 7.3 Oracle Settings

Field	Description
Data Source Type	Select the JDBC driver data source type for Oracle. - Use Interstage Connection Pooling (oracle.jdbc.pool.OracleConnectionPoolDataSource) - Use Oracle Connection Pooling

Field	Description
	(oracle.jdbc.pool.OracleDataSource) Use Global Transaction (oracle.jdbc.xa.OracleXADataSource)
Use RAC	Select this to use the RAC function
User ID (user)*	User ID for use by applications when connecting to the database.
Password (password)*	Password for the user ID above.
Server URL (url)*	Specify the server url used for access to the database (when 'Use RAC' is selected).
Driver Type/Network Protocol (driverType / networkProtocol)	The JDBC driver type and network protocol. Can be one of: - thin/tcp - oci/tcp - oci/ipc.
Hostname (serverName)*	Host name under which the database is registered with the File System Service provider's Naming Service.
Port Number (portNumber)	Port number for connection to the above host. Default: 1521
SID / Net Service Name	SID used to identify the Oracle database.
Provider URL	Specify the URL of the File System Service provider's Naming Service. Auto completed.
Data Source Name*	Data source name registered with the File System Service provider's Naming Service.
Register data source (in the .bindings file)	Select this to register the data source in File System Service Provider.

Table 7.4 SQL Server Settings

Field	Description
Data Source Type	Select the JDBC driver data source type for SQL Server. - Use SQL Server 2005 (com.microsoft.sqlserver.jdbc.SQLServerXADataSource) - Use SQL Server 2000 (com.microsoft.jdbcx.sqlserver.SQLServerDataSource)
User ID (user)*	User ID for use by applications when connecting to the database.
Password (password)*	Password for the user ID above.
Hostname (serverName)*	Host name on which the SQL Server DBMS is running.
Port Number (portNumber)	Port number for the above host. Default: 1433
Database Name (databaseName)*	Database name of the SQL Server database on the host specified below.
Provider URL	Specify the URL of the File System Service provider's Naming Service. Auto completed.
Data Source Name*	Data source name registered with the File System Service provider's Naming Service.
Register data source (in the .bindings file)	Select this to register the data source in File System Service Provider

Table 7.5 Generic Definition

Field	Description
Data Source Class Name	Specify the data source class name used to connect to the database.
Log Writer (logWriter)	Specify whether to output data source log information.

7.4 Configuring JMS

The JMS (Java Message Service) API is a Java API that allows applications to create, send, receive, and read messages. The JMS API defines a common set of interfaces and associated semantics that allow programs written in the Java programming language to communicate with other messaging implementations.

Some aspects of JMS setup are the same as for the Event Service and involve configuring:

- Stores (Message Store) - these are the storage used by persistent channels to hold retained messages.

  For details on creating/viewing from the Application Management tab of the Admin Server, refer to the "Chapter 8 Services" chapter.

- Event Channels - these control the delivery of messages. They exist between the producer and the consumer (subscriber or receiver) during asynchronous communication.

  For details on creating/viewing from the Application Management tab of the Admin Server, refer to the "Chapter 8 Services" chapter.

JMS Resource setup includes the configuration of:

- ConnectionFactories - these provide interfaces that a JMS client uses to create a connection with a JMS provider. Two interface types are available:

  - QueueCF

    An application uses a QueueCF (QueueConnectionFactory) to create queue connections with a JMS PTP provider.

  - TopicCF

    A client uses a TopicCF (TopicConnectionFactory) to create topic connections with a JMS Pub/Sub provider.

  Default TopicCF and QueueCFs are created by the system.

- Destinations - these hold the event channel group name and channel name information and are the JNDI address definition information used by JMS applications when sending and receiving messages.

In a multi-server environment the Event Service must be enabled on each Managed Server *before* it is added to the site. Navigate to Interstage > Interstage Application Server > System > Update System Settings and click the **[Show]** link to view the Detailed Settings. In the header of the Event Service Settings table select **Yes** to enable the Event Service. Event Channels and Stores are created from the Application Management tab under the Interstage > Interstage Application Server > Services > Event Service node on a per server group basis.

Event Channels specified for use with JMS during are automatically assigned a destination (JNDI name). From the Application Management tab, JNDI Destinations can be viewed from Interstage > Interstage Application Server > Resources > JMS > Destination > View Configurations. On a standalone server navigate to Interstage > Interstage Application Server > System > Resources > JMS > EventChannels > Destination.

For details on creation of Event Channels and Stores for Managed Servers, refer to the "Chapter 8 Services" chapter.

For details on enabling and setting up the Event Service, refer to the "Chapter 4 System" and "Chapter 8 Services" chapters.

For a reference of settings related to JMS in Interstage, refer to "7.4.3 JMS Configuration Settings Reference".

7.4.1 Viewing / Updating the JMS Configuration (Standalone Server)

Standalone

Interstage > Interstage Application Server > System > Resources > JMS	JMS Configuration

To view or update the JMS Configuration:

1. Edit the required settings on the form as described in the tables in 7.4.3 JMS Configuration Settings Reference.

   Interstage must be restarted for these settings to be applied.

2. Click the **Update** button to update the JMS configuration settings.
3. Click the **Refresh** button to refresh the form with the most recently updated values.

7.4.2 Viewing / Updating the JMS Configuration (Multi Server)

Application Management

Interstage > Interstage Application Server > Services > Event Service > [server group | independent managed server]	Event Service

For Managed Servers, these settings are found under Services > EventService. For details, refer to the "Chapter 8 Services" chapter.

7.4.3 JMS Configuration Settings Reference

The following tables are reference tables for information displayed or configurable from the IMC relating to JMS.

Note

- An asterisk (*) character inside a field denotes that a value must be specified for that item.

Table 7.6 JMS Configuration Settings

Field	Description
Dynamic EventChannels Max No. of Starts *	The maximum number of dynamic Event Channels that can be simultaneously active. Dynamic channels are used by a temporary topic or queue. (Max: 10000).
Static EventChannels Max No. of Starts *	The maximum number of static Event Channels that can be simultaneously active. All channels created using the IMC are static. (Max: 10000).
Error Log File Size *	The size of the error log file in K bytes used by the Event Service. (Max: 512000 KB).
Event Channels Auto Start	Indicates if Event Channels will start automatically when Interstage starts.
Max Concurrent Global Transactions *	Defines the maximum number of global transactions that can be executed simultaneously. (Max: 1024).
2-Phase Commit Transaction Timeout *	This is the timeout value (seconds) for 2-phase commit transactions. (Max: 20000).
Automatic Recovery Retry Interval *	The interval between successive automatic recovery attempts in Seconds. (Max: 1000).
Automatic Recovery Retry Count *	The maximum number of times to attempt recovery after failure (max: 100).
Event Data Waiting Time *	The wait time for event data. The value should be less than the client timeout interval of the CORBA Service. Seconds.
Volatile Event Data Persistence Time *	Not available on Standalone Server. The lifetime of event data recorded in EventChannels (in seconds). Use a value from 1 to 1,000,000. Specifying 0 sets no limit. Default value is 0.
Local Transaction Timeout *	The timeout interval for local transactions in Seconds. (Max: 1000000)
Error return when consumer is disconnected	Interstage returns a BAD_OPERATION exception with the error code 0x464a09e9 to the Send or Publish method this is enabled.

Field	Description
Notification of EventChannel Termination 1	Indicates whether to notify suppliers and consumers of the termination of the associated EventChannel by invoking the disconnect method.
Block Operation Mode	The EventChannel block function, to disable blocking, enable blocking, or enable both blocking and automatic blocking.
Repository Monitoring Level	A percentage of the [Maximum Number of EventChannel Messages]. When the repository size reaches this level, an alarm will be triggered.
Repository Monitoring Restart Level	A percentage of the [Maximum Number of EventChannel Messages]. When the repository size reaches this level, repository monitoring will be restarted.
Event Data Automatic Unblock Level	A percentage of the [Maximum Number of EventChannel Messages]. When the repository size drops below this level, then the EventChannel will be automatically unblocked.
Maximum Number of EventChannel Messages *	Defines the maximum number of messages that can be stored in an Event Channel. (Max: 10000000) Note: Updates to this setting will only affect Event Channels created after the updates are applied.
Involatile Event Data Persistence Time *	Not available on Standalone Server. The lifetime of event data recorded in non-volatile EventChannel for event data and connection information. Use a value from 1 to 2000000000. Specifying 0 sets no limit. The default value is 0.

Note

- Configuration settings on this page are the same as those on the Event Service Configuration page. If using the Event Service, be careful when updating these settings.

7.4.4 Managing JMS Connection Factories

A default connection factory is provided for both the Queue and Topic connection factory types (QueueCF001 and Topic001). These default configurations are editable but cannot be removed.

7.4.4.1 Viewing Connection Factory Configurations

Application Management

Interstage > Interstage Application Server > Resources > JMS > ConnectionFactory	View Configurations

Standalone

Interstage > Interstage Application Server > System > Resources > JMS > ConnectionFactory	View Configurations

A list of all connection factories used to connect to the Interstage JMS provider is displayed. The following information is given for each:

- **Deploy To** (Application Management view only), the Server Group/Independent Managed Servers to which the connection factory is deployed
- The **JNDI Name**, which is a hyperlink to a page from where the connection factory settings can be viewed, or updated.
- The connection factory **Type** (queue or topic), **Client ID**, if **Global Transactions** are being used.
- **Last Action Status** (Application Management view only) giving the status of the connection factory creation/update operation as:
  - Normal where connection factory definition setup completed normally for all servers in the case of the Server Group, or for the Independent Managed Server.
  - Normal (Part) in the case of Server Groups where an error occurred at some servers during connection factory definition setup.

- Abnormal where an error occurred during connection factory definition setup.

Click the **[Show]** link to view Details for each connection factory and the servers to which it is deployed. For each server, the **Last Action Status** is given. An error message is given for servers for which definition setup failed. Corrective action can be taken on the relevant servers based on this information.

Click the **Refresh** button to refresh the list.

Click the **JNDI Name** to access the JNDI definition for view or edit.

Viewing Queue Connection Factories

Application Management

Interstage > Interstage Application Server > Resources > JMS > ConnectionFactory > QueueCF	View Configurations

Standalone

Interstage > Interstage Application Server > System > Resources > JMS > ConnectionFactory > QueueCF	View Configurations

A list of all Queue type connection factory configurations is displayed giving the **JNDI Name**, **Client ID**, and if **Global Transactions** are enabled. In a multi-server environment **Deploy To**, **Type** and **Last Action Status** giving the status of the connection factory creation/ update operation are also given.

Viewing Topic Connection Factories

Application Management

Interstage > Interstage Application Server > Resources > JMS > ConnectionFactory > TopicCF	View Configurations

Standalone

Interstage > Interstage Application Server > System > Resources > JMS > ConnectionFactory > TopicCF	View Configurations

A list of all Topic type connection factory configurations is displayed giving the **JNDI Name**, **Client ID**, and if **Global Transactions** are enabled. In a multi-server environment **Deploy To**, **Type** and **Last Action Status** giving the status of the connection factory creation/ update operation are also given.

7.4.4.2 Creating a Connection Factory

Application Management

Interstage > Interstage Application Server > Resources > JMS > ConnectionFactory > QueueCF | TopicCF	Create a New QueueCF | TopicCF

Standalone

Interstage > Interstage Application Server > System > Resources > JMS > ConnectionFactory > QueueCF | TopicCF	Create a New QueueCF | TopicCF

To create a connection factory:

1. If accessing from the Application Management tab, in the Server Name or Server Group Name list, click the Server Group(s)/ Independent Managed Server(s) to which the configuration is to be deployed.
2. In **JNDI Name**, specify a unique name for the connection factory.

   By default the lowest available unused ID will be specified.
3. Specify a value in **Client ID**, for use by the JMS provider to identify a durable subscriber.

4. Select **Enable** to enable Global Transactions.
5. Click the **Create** button to create the connection factory.
6. Click the **Reset** button on this form to the default values.

Note

- 'java:comp/env/jms/' is automatically prefixed to the JNDI name.
- For a reference of settings related to JMS Connection Factories in Interstage, refer to "7.4.4.5 JMS Connection Factory Settings Reference".

7.4.4.3 Updating a Connection Factory

Application Management

Interstage > Interstage Application Server > Resources > JMS > ConnectionFactory > QueueCF | TopicCF	Unit Configuration

In the Operations frame, click the **JNDI Name** of the connection factory name that is to be modified.

Standalone

Interstage > Interstage Application Server > System > Resources > JMS > ConnectionFactory > QueueCF | TopicCF > [connection factory name]	Unit Configuration

To update a connection factory:

1. Edit the required settings on the form as described in the tables in the 7.4.4.2 Creating a Connection Factory section or in Table 7.7 Connection Factory Settings.
2. Click the **Update** button to update the resource adapter settings.
3. Click the **Refresh** button to refresh the form with the most recently updated values.

Note

- The method used to update all connection factories (default queue and topic types and user defined connection factories) is the same. Only the Client ID used by the JMS provider to identify durable subscribers, and enabling of global transactions for this connection factory can be modified.

7.4.4.4 Deleting a Connection Factory

Application Management

Interstage > Interstage Application Server > Resources > JMS > ConnectionFactory	View Configurations

Standalone

Interstage > Interstage Application Server > System > Resources > JMS > ConnectionFactory	View Configurations

To delete a connection factory:

1. Click the checkbox to the left of all connection factories to be deleted.

   Click the **Select All** button to select all connection factories in the list.
2. Click the **Delete** button to remove the selected connection factory(ies).
3. Click the **OK** button to confirm deletion.

Note

- The default connection factories (QueueCF001 and TopicCF001) cannot be removed.
- Applications using the deleted connection factory will be disabled.
- If the connection factory being deleted was deployed to a Server Group, it will be removed from all servers in the group. If an error occurs at some servers in the group, an error message is posted for each.

7.4.4.5 JMS Connection Factory Settings Reference

Following is a reference table for information displayed or configurable from the IMC relating to JMS connection factories.

Note

- An asterisk (*) character inside a field denotes that a value must be specified for that item.

Table 7.7 Connection Factory Settings

Field	Description
Server Name or Server Group Name	Not available on Standalone Server. Select Server Groups/Independent Managed Servers to which the connection factory is to be deployed (Multi Server only).
JNDI Name*	Specify the name used for JNDI lookup. ('java:comp/env/jms/' will automatically be prepended to the JNDI name.)
Type	The type of connection factory Auto completes reflecting tree node selected: - QueueConnectionFactory - TopicConnectionFactory
Client ID*	Client ID used by the JMS provider to identify durable subscribers.
Global Transactions	Enable or disable the use of global transactions.

7.4.5 Managing JMS Destination

7.4.5.1 Viewing JMS Destination

Application Management

Interstage > Interstage Application Server > Resources > JMS > Destination	View Configurations

Standalone

Interstage > Interstage Application Server > System > Resources > JMS > Destination	View Configurations

A list of all destinations associated with JMS Event Channels created is displayed. The following information is given for each:

- The JNDI Name,
- The **Type** (Queue or Topic)
- The EventChannel Server or Server Group (Multi Server only), Group Name and Channel Name
- The Naming Service Host name or IP address and Port number.

- The **Last Action Status** which can have the following values (Multi Server only):

    1. Normal where destination environment setup completed normally for all servers in the case of the Server Group or for the server not a member of a group.
    2. Normal (Part) in the case of Server Groups where an error occurred at some servers during destination environment setup.
    3. Abnormal where an error occurred during destination environment setup.

  Select the **Modify Definition** tab to modify the JNDI Name of each Destination configuration.

Click the Details **[Show]** link to view the Last Action Status for each Destination item on each Server it was deployed to (Multi Server only). Error details will be displayed for Managed Servers for which environment setup failed. Corrective action can be taken on the relevant servers based on this information.

Click the **Refresh** button to refresh the list.

7.4.5.2 Creating New JMS Destination (Standalone)

Standalone

Interstage > Interstage Application Server > System > Resources > JMS > Destination	Create a New Destination

Enter the following settings to create a new destination:

- The Destination **JNDI Name**.
- The Destination **Type** (topic or queue)
- The associated EventChannel Group Name
- The associated **EventChannel** Channel **Name**
- The Naming Service **Host name or IP address** and **Port Number** if required (In Details [Show]).

7.4.6 Managing JMS Storage Destinations (Standalone)

7.4.6.1 Viewing Storage Destinations

Standalone

Interstage > Interstage Application Server > System > Resources > JMS > Stores	View Unit

A list of storage destinations used for the JMS Event Channels is displayed. The **Unit ID**, **Unit Mode**, **System Usage**, **Event Data Usage**, **System Data Storage Areas** and **Event Data Storage Areas** are displayed for each.

Click a **Unit ID** to access the configuration information of that Storage Destination.

7.4.6.2 Creating Storage Destinations for JMS Event Channels

Standalone

Interstage > Interstage Application Server > System > Resources > JMS > Stores	Create a New Unit

To create a Storage Destination:

1. In **Unit ID**, type a unique name for the storage destination.

   This is used by the persistent channel.
2. Click the Detailed Settings **[Show]** link to access the Detailed Setup.
3. In **Unit Mode**, select Extended Mode if global transactions are to be used.

4. In **Storage Directory**, specify where this unit should be stored.
5. In **Transaction Concurrency**, specify it from 1 to 1024. Initial value is 1024 for Windows, 100 for Solaris and Linux.
6. In **Size of System File**, specify it from 1 to 2047 MB. Initial value is 10 MB.
7. In **Number of System Data Storage Areas**, specify it from 4 to 32768. Initial value is 1000.
8. In **Size of Event Data File** specify it from 1 to 2047 MB. Initial value is 30MB.
9. In **Number of Event Data Storage Areas**, specify it from 1 to 32768. Initial value is 50.
10. In **Size of Shared Memory**, specify it from 1 to 1024 MB to share memory between messages stores. Initial value is 80 MB.
11. Click the **Create** button to create the new Storage Destination.
12. Click the **Reset** button to return this form to the default values.

7.4.6.3 Deleting Storage Destinations

Standalone

Interstage > Interstage Application Server > System > Resources > JMS > Stores	View Unit

To delete a Store:

1. Click the checkbox to the left of any Store to be deleted.

   Click the **Select All** button to select all Stores in the list.
2. Click the **Delete** button to remove the selected Store(s).
3. Click the **OK** button to confirm deletion.

7.4.7 Managing JMS Event Channels (Standalone)

Interstage supports two types of Event Channels:

- Event Channels used by the Event Service
- Event Channels used by JMS.

Manipulations on JMS Event Channels are detailed below.

7.4.7.1 View JMS Event Channels

Standalone

Interstage > Interstage Application Server > System > Resources > JMS > EventChannels	View Status

A list of the event channels created for JMS is displayed. The channel **Group Name**, **Channel Name**, **Type**, **Destination**, **Unit**, **Start Status**, **Number of Messages (Current/Monitoring/Maximum)**, **No. of Consumer Connections**, **No. of Producer Connections** and the **Control** are given for each. For each queue type event channel created, the Control field displays **Block** and **Unblock** buttons for the EventChannel block function.

Click a Channel Name to view settings of that event channel.

7.4.7.2 Creating a JMS Event Channel

Standalone

Interstage > Interstage Application Server > System > Resources > JMS > EventChannels	Create a New EventChannel

To create a JMS Event Channel:

1. Specify the **EventChannel Group Name**. If the Naming Service is shared, the same group name cannot be created.
2. Specify the **EventChannel Name**.
3. In Event Channel **Type**, select **Topic** or **Queue**.
4. Click the Detailed Settings **[Show]** link to access the Detailed Setup.
5. Enable or Disable **Persistent Channel.** If enabled,
   - Specify a **Unit ID (Required only when using Persistent Channels)** from the list, which identifies the Storage Destination (previously created for use by this Event Channel.
   - Select **Enabled** if **Global Transactions (Required only when using Persistent Channels)** are to be used.
6. Specify the **Maximum Number of Connections** between producers and consumers
7. Select **Enable** if **SSL Communication** for the Event Channel is to be used.
8. Select **Enable** if **Automatic connection recovery** is to be used.

   This will cause remaining connection information in the EventChannel to be automatically collected when the consumer and producer disconnect, without issuing the connection 'close' method.
9. Click the **Create** button to create the Event Channel.
10. Click the **Reset** button to return this form to the default values.

7.4.7.3 Starting JMS Event Channels

Standalone

Interstage > Interstage Application Server > System > Resources > JMS > EventChannels	View Status

To start an Event Channel:

1. Click the checkbox to the left of any Event Channels to be started.

   Click the **Select All** button to start all Event Channels in the list.
2. Click the **Start** button to start the selected Event Channels.
3. If any of the selected Event Channels use Global Transactions, select:
   - **Normal start** to start the event channel normally
   - **Rollback Incomplete Transactions** to roll back an incomplete transaction forcibly and start the event channel. Select this option if error message es11017 is posted to the status frame
   - **Commit Incomplete Transactions** to commit an incomplete transaction forcibly and start the event channel. Select this option if error message es11017 is posted to the status frame.
4. Click the **Execute** button to complete the start process.

7.4.7.4 Stopping JMS Event Channels

Standalone

Interstage > Interstage Application Server > System > Resources > JMS > EventChannels	View Status

To stop a JMS Event Channel:

1. Click the checkbox to the left of any Event Channels to be stopped.

   Click the **Select All** button to stop all Event Channels in the list.

2. Click the **Stop** button to stop the selected Event Channels.
3. If any of the selected Event Channels use Global Transactions, select:
   - **Normal Stop** to block new requests and to wait for completion of existing requests. Then stop the Event Channel.
   - **Forced Stop** to stop the event channel in compulsion mode.
4. Click the **Execute** button to complete the stop process.

7.4.7.5 Setting JMS Event Channels to Start Automatically

Standalone

Interstage > Interstage Application Server > System > Resources > JMS > EventChannels	Auto Start Settings

To set an event channel to start automatically:

1. Select **On** in the **Auto Start** column for each Event Channel that is required to start at Interstage startup.
2. Click the **Update** button to save the changes.

7.4.7.6 Updating JMS Event Channel Settings

Standalone

Interstage > Interstage Application Server > System > Resources > JMS > EventChannels > [EventChannel name]	Settings

To update event channel Settings:

1. Specify the **Event Data Waiting Time** in seconds.
2. Specify the **Local Transaction Timeout** in seconds.
3. Select **Enable** to use **Error return when consumer is disconnected**.
4. Select the **Block Operation Mode,** which is the EventChannel block function, to disable blocking, enable blocking, or enable both blocking and automatic blocking.
5. Specify the **Repository Monitoring Level**, which is a percentage of the [Maximum Number of EventChannel Messages]. When the repository size reaches this level, an alarm will be triggered.
6. Specify the **Repository Monitoring Restart Level**, which is a percentage of the [Maximum Number of EventChannel Messages]. When the repository size reaches this level, repository monitoring will be restarted.
7. Specify the **Event Data Automatic Unlock Level**, which is a percentage of the [Maximum Number of EventChannel Messages]. When the repository size drops below this level, then the EventChannel will be automatically unblocked.
8. Specify the **Maximum Number of EventChannel Messages**. Maximum value is 10,000,000.
9. Click the **Update** button to update the event channel details.

7.4.7.7 Deleting JMS Event Channels

Standalone

Interstage > Interstage Application Server > Settings > Resources > JMS > EventChannels	View Status

To delete Event Channels:

1. Click the checkbox to the left of Event Channels to be deleted.

   Click the **Select All** button to select all Event Channels in the list.

2. Click the **Delete** button to delete the selected Event Channels.
3. Click the **OK** button to confirm deletion.

7.5 Configuring JavaMail

JavaMail provides a platform-independent and protocol-independent framework for building mail and messaging applications. The JavaMail API provides facilities for reading and sending email.

The JavaMail API provides access from Java applications to IMAP, POP3 and SMTP capable mail servers on a network or the Internet. As it does not provide mail server functionality; access to a mail server is required to use JavaMail.

A JavaMail configuration created with the Interstage Management Console provides a common JavaMail Session object for use by any application that requires it.

For a reference of settings related to JavaMail in Interstage, refer to "7.5.5 JavaMail Configuration Settings Reference".

7.5.1 Creating a JavaMail Configuration

Application Management

Interstage > Interstage Application Server > Resources > JavaMail	Create a new JavaMail Configuration

Standalone

Interstage > Interstage Application Server > System > Resources > JavaMail	Create a new JavaMail Configuration

To create a JavaMail configuration:

1. In **Configuration Name**, specify a unique name for the JavaMail configuration.

   This name becomes the name for JNDI lookup, and it is used by J2EE applications to lookup the javax.mail.Session object.
2. If accessing from the Application Management tab, in the **Deploy To** list, click the Server Group to which the configuration is to be deployed.
3. In **Mail Sender** specify the ID that will be used by default for mail sent from the application.
4. In **Login ID**, specify the login user name of the mail server.
5. In **Mail Server Settings**, select:

   - POP3 if the mail server from which mail will be read is POP3.
   - IMAP if the mail server from which mail will be read is IMAP.

   For the mail server selected:

   - In **Server**, specify the IP address or the host name of the mail server.
   - In **Port Number**, specify the port number for that server.
6. In **SMTP Server**, specify the IP address or the host name of the SMTP mail server mail will be sent through, and in **SMTP Server Port Number**, specify the port number for that server.
7. Click the **Create** button to create and deploy the JavaMail configuration.
8. Click the **Reset** button this form to the default values.

Note

- For a reference of settings related to JavaMail in Interstage, refer to "7.5.5 JavaMail Configuration Settings Reference".

7.5.2 Viewing Deployed JavaMail Configurations

Application Management

Interstage > Interstage Application Server > Resources > JavaMail	View JavaMail Configurations

A list of JavaMail configurations deployed on the site is displayed. For each item in the list, the **Configuration Name**, participant to which it is **Deployed To** and **Version** are given.

Standalone

Interstage > Interstage Application Server > System > Resources > JavaMail	View JavaMail Configurations

A list of all JavaMail configurations deployed on the Standalone server is displayed. For each item in the list only the **Configuration Name** is displayed.

Each name is a hyperlink to the JavaMail Configuration page from where it can be updated or deleted.

7.5.3 Updating a JavaMail Configuration

Application Management

Interstage > Interstage Application Server > Resources > JavaMail > [configuration name]	JavaMail Configuration

Standalone

Interstage > Interstage Application Server > System > Resources > JavaMail > [configuration name]	JavaMail Configuration

To update a JavaMail configuration:

1. Edit the required settings on the form as described in the tables in section 7.5.5 JavaMail Configuration Settings Reference or in 7.5.1 Creating a JavaMail Configuration.
2. Click the **Update** button update and configuration with the modified settings.
3. Click the **Refresh** button to refresh the form with the most recently updated values.

7.5.4 Deleting a JavaMail Configuration

Application Management

Interstage > Interstage Application Server > Resources > JavaMail	View JavaMail Configurations

Standalone

Interstage > Interstage Application Server > System > Resources > JavaMail	View JavaMail Configurations

To delete a JavaMail configuration:

1. Click the checkbox to the left of the configurations to be deleted.

   Click the **Select All** button to select all resource adapters in the list.
2. Click the **Delete** button to remove the selected JavaMail configuration(s).
3. Click the **OK** button to confirm deletion.

- Deleting a JavaMail configuration may cause failure of any deployed applications using it.

7.5.5 JavaMail Configuration Settings Reference

The following tables are reference tables for information displayed or configurable from the IMC relating to JavaMail.

Note

- An asterisk (*) character inside a field denotes that a value must be specified for that item.

Table 7.8 JavaMail Configuration Settings

Field	Description
Configuration Name*	Name used for JNDI lookup, and seen by J2EE applications looking up the javax.mail.Session object. This is the configuration name displayed in the IMC. Max 32 chars.
Deploy To	Only present if accessing from the Application Management tab. This is used to define the Server Group to which the data source is to be deployed. This value cannot be updated once the Resource has been created.
Mail Server*	Name used by default for mail sent from an application using the configuration. Max 255 chars.
Login ID*	Login user name of the Mail Server. The Mail Sender ID will be a default value that can be overridden by an application (e.g. via the api "msg.setFrom(new InternetAddress("otherMailId@company.com "));") Max 255 chars.
Mail Server Settings*	Refer to Table Table 7.9 Mail Server Settings.
SMTP Server*	IP address or host name of the SMTP mail server that mail will be sent through.
SMTP Server Port Number*	Port number on which to connect to the SMTP server. Default : 25

Table 7.9 Mail Server Settings

Field	Description
POP3*	If selected, specifies POP3 as the type of mail server from which mail will be read.
IMAP*	If selected, specifies IMAP as the type of mail server from which mail will be read.
Server*	IP address or host name of mail server.
Port Number*	Port number on which to connect to the mail server. Default for POP3: 110 Default for IMAP: 143

7.6 Configuring Connectors (Resource Adapters)

Connectors are J2EE components that implement the J2EE Connector Architecture. Interstage supports connectors that conform to Oracle J2EE Connector Architecture (JCA) Specification versions 1.0 and 1.5.

A Resource Adapter (RA) is a J2EE connector that allows a J2EE application to communicate with an external EIS (Enterprise Information System) via a standard API. Resource adapters are usually supplied with the EIS or by third party vendors and can be deployed on any J2EE server. RAs are packaged in a Resource Adapter aRchive (RAR) file.

Interstage JCA1.5 compliant RAs offer the additional functionality of Inbound (as well as Outbound) RAs; a selection of JCA1.5 RAs as the target type for receipt of messages by EJB2.1 compliant Message-driven Beans; the definition of Managed Objects; and the addition of start/stop processing and endpoint activation/deactivation.

RAs can be deployed on Interstage as part of an Enterprise ARchive (EAR file) or individually. Interstage allows RARs to be deployed to either a Server Group or an Independent Managed Server. Applications that need to refer to the adapter instance should use the configuration name defined for it during creation. The instance user name and password for connection to the EIS can also be configured.

The deployment descriptor of an RAR file may contain properties specific to the resource adapter and underlying EIS, such as an IP address or URL. Because it is likely that the same RAR file may be deployed several times but with different settings, Interstage only allows properties to be edited after deployment has been completed. This ensures that any modifications are unique to that adapter instance.

Interstage allows Connectors to execute using Global Transactions.

For a reference of settings related to Connectors in Interstage, refer to "7.6.5 Resource Adapter Settings Reference (JCA1.0 RAs)".

Only JCA1.0 RAs can be deployed by uploading them to Site Participants from the Connectors node of the navigation tree. From this node, deployed 1.0 RAs can also be accessed for view and modification. Details for these operations are described below.

All RA versions can be deployed directly to an IJServer WorkUnit. Operations on RAs deployed in this manner are described in "Managing J2EE Applications" in the "WorkUnits General and IJServer" chapter.

7.6.1 Deploying a Resource Adapter (JCA1.0 RAs)

Application Management

Interstage > Interstage Application Server > Resources > Connector	Create a new Resource Adapter

Standalone

Interstage > Interstage Application Server > System > Resources > Connectors	Create a new Resource Adapter

To deploy a resource adapter:

1. In **Configuration Name**, specify a unique name for the resource adapter.

   This is used by applications to refer to the adapter.

2. In **Deployment File**, select:

   - **Upload a local file for deployment** and use the **Browse** button to select an EAR/RAR file to be uploaded from the machine on which the web browser is running to the Admin Server. This is the default option.
   - **Deploy a file stored on the Admin Server** and specify the path and file name of an EAR/RAR file located on the Admin Server.
   - **Deploy a file stored on the Managed Server** and specify the path and file name of an EAR/RAR file located on the Managed Servers. Note that the file must already exist in the same location on all Managed Servers that the file is to be deployed to.

   Properties defined in the RAR file's deployment descriptor may need to be updated. This can be done manually before uploading to the server or else after deployment by updating the Resource Adapter settings.

3. If accessing from the Application Management tab, in the **Deploy To** list, click the Server Groups/Independent Managed Server to which the resource adapter is to be deployed.

4. Specify the **User ID** and **Password** for the EIS that the resource adapter will connect to, if the EIS requires these.

5. Select **Enabled** to enable **Global Transactions**, click the Global Transaction Settings **[Show]** link to access the Global Transaction Settings, and in Resource Log File Storage Directory specify the storage location for the trace log.

6. Click the **Deploy** button to deploy the resource adapter.

   Click the **Reset** button this form to the default values.

Note

- EAR files containing RAR files can also be selected for upload and deployment. The rest of the EAR contents are ignored.
- RAR files (and EAR files containing RAR files) can also be deployed when deploying applications in an IJServer Work Unit. In this instance, the Configuration Name is automatically chosen to be the same as the RAR file name (without the .RAR extension). For details, refer to the "WorkUnits General and IJServer" chapter.
- For a reference of settings related to Connectors in Interstage, refer to "7.6.5 Resource Adapter Settings Reference (JCA1.0 RAs)".

7.6.2 Viewing Deployed Resource Adapters (JCA1.0 RAs)

Application Management

Interstage > Interstage Application Server > Resources > Connectors	View list of Resource Adapters

Standalone

Interstage > Interstage Application Server > System > Resources > Connectors	View list of Resource Adapters

A list of all deployed Resource Adapters is displayed. For each item in the list, the **Configuration Name** is given and from the Application Management tab of the Admin Server the participant to which it is **Deployed To** and **Version** are given.

Click the **Configuration Name** link to access the settings for that adapter.

7.6.3 Updating a Resource Adapter (JCA1.0 RAs)

Application Management

Interstage > Interstage Application Server > Resources > Connectors > [adapter name]	Resource Adapter Settings

Standalone

Interstage > Interstage Application Server > System > Resources > Connectors > [adapter name]	Resource Adapter Settings

To update a resource adapter:

1. Edit the required settings described in the tables in section 7.6.5 Resource Adapter Settings Reference (JCA1.0 RAs) or in 7.6.1 Deploying a Resource Adapter (JCA1.0 RAs).

   If the deployed RAR file contains properties, these are listed in a table under the Resource Adapter Settings table.

   Edit the value of any property as required.
2. Click the **Update** button to update the resource adapter settings.
3. Click the **Refresh** button to refresh the form with the most recently updated values.

7.6.4 Undeploying a Resource Adapter (JCA1.0 RAs)

Application Management

Interstage > Interstage Application Server > Resources > Connectors	View list of Resource Adapters

Standalone

Interstage > Interstage Application Server > System > Resources > Connectors	View list of Resource Adapters

To undeploy a resource adapter:

1. Click the checkbox corresponding to resource adapters to be undeployed.

   Click the **Select All** button to select all resource adapters in the list.

2. Click the **Undeploy** button to remove the selected resource adapter(s).

3. Click the **OK** button to confirm deletion.

7.6.5 Resource Adapter Settings Reference (JCA1.0 RAs)

The following tables are reference tables for information displayed or configurable from the IMC relating to Resource Adapters.

Note

- An asterisk (*) character inside a field denotes that a value must be specified for that item.

Table 7.10 Resource Adapter Settings

Field	Description
Configuration Name *	Name by which the adapter will displayed on the system and for J2EE lookup. The name must be unique amongst resource adapters on the site. Max 32 characters.
Deployment File *	Path on the local machine of the RAR file to be uploaded to the Admin Server and then deployed. Max 255 characters.
Deploy To	Only present if accessing from the Application Management tab. This is used to define the Server Group to which the resource adapter is to be deployed. This value cannot be updated once the Resource has been created.
User ID	User ID used by the Resource Adapter to connect to the EIS. Max 255 characters.
Password	Password used by the Resource Adapter to connect to the EIS. Max 255 characters.

Table 7.11 Second Table in Resource Adapter Settings pg (Property Name|Class Name| Value)

Field	Description
Property Name	Name of the resource Property
Class Name	Java type of the property
Value	Property value

Table 7.12 Global Transaction Settings

Field	Description
Resource Log File Storage Directory	Storage location for the trace log.

Chapter 8 Services

8.1 Services Overview

Services provide infrastructure for WorkUnits and applications deployed in them.

Services that can be configured from the Interstage Management Console include the Interstage system services, the Web server and Event Service (stores and event channels). Interstage system services include the CORBA Service, Naming Service (NS), Interface Repository (IR), Object Transaction Service (OTS), Servlet Service.

For services configured at the site level, including all Interstage system services, refer to the Chapter 4 System chapter.

The Services that can be setup for individual site participants and Standalone servers varies as follows:

Services available for Standalone Servers

- Event Service

  For details, refer to 8.2 Managing the Event Service.

- Web Server

  For details, refer to 8.3 Managing the Web Server.

- Repository (*1)

  For details, refer to 8.4 Managing the Repository.

*1 This is not valid for Linux (64 bit).

Services available for Multi-server (Server Group or Independent managed server)

- Event Service

  For details, refer to 8.2 Managing the Event Service.

- Web Server

  For details, refer to 8.3 Managing the Web Server.

- Transaction Service (OTS) Windows32/64 Solaris32 Linux32/64

  For details, refer to 8.5 Managing the Transaction Service (OTS) Multi-server Only .

- Transaction Service (JTSRMP)

  For details, refer to 8.6 Managing the Transaction Service (JTSRMP) Multi-server Only .

Services are accessed from the Services node of the navigation tree node. In a multi-server environment, services are configured for each Server Group/Independent Managed Server.

Server Groups have their own set of services, configured to suit the requirements of the group. The set of services used by an Independent Managed Server or a Standalone server can be configured in the same way as for a group. The service setup is the same when a user logs in to a Standalone server or to a server in a multi-server environment to set up a service with the exception that the setup destination may be the server where the user logs in, or it may be a server or Server Group within a site.

Services are accessible from the Services node of the Application Management tab of the Admin Server and Standalone servers. Under the Services node, the Event Service, Web Server, OTS Transaction Service and JTSRPM Transaction Service are located. From the Application Management tab of the Admin Server, Server Groups/Independent Managed Servers having that service setup is located under the corresponding node. Service settings can be modified from here and reapplied to that Server Group/Independent Managed Server.

When a non-empty Server Group is created (or an Independent Managed Server added to the site), it automatically appears under the Services node with default settings. The Reserved Managed Server or an empty Server Group does not appear under the Services node.

8.1.1 Viewing Services Summary

To view a summary of the services setup on a site participant or Standalone server, refer to the Chapter 4 System chapter.

8.2 Managing the Event Service

Using the Interstage Management Console, it is possible to manage the Interstage Event Service. Typical operations a user may need to perform include:

- 8.2.1 Viewing the Event Service Status
- 8.2.2 Configuring the Event Service
- 8.2.3 Managing Storage Destinations for the Event Service and JMS
- 8.2.4 Managing Event Channels

Details of these operations are given in the following sections.

8.2.1 Viewing the Event Service Status

Application Management

Interstage > Interstage Application Server > Services > Event Service	Settings Information

The status of the event service configuration of a Server Group or server is displayed as:

- **Normal** where configuration completed normally for all servers in the case of the Server Group or for the server not a member of a group.
- **Normal (Part)** in the case of Server Groups where an error occurred at some servers during event service configuration setup.
- **Abnormal** for an Independent Managed Server where an error occurred during event service configuration setup.

Click the **[Show]** link to view the status of each server in a Server Group. An error message is given for servers for which definition setup failed.

8.2.2 Configuring the Event Service

Application Management

Interstage > Interstage Application Server > Services > Event Service > [server group | independent managed server]	Event Service

Standalone

Interstage > Interstage Application Server > System > Services > Event Service	Event Service

To configure the event service for a Server Group or server:

1. In **Dynamic EventChannels Max No. of Starts** specify a value between 1 and 10000, (default is 50), and in **Static EventChannels Max No. of Starts**, specify a value between 1 and 10000, (default is 50).
2. In **Error Log File Size**, specify a value from 1 KB to 512000 KB (default is 1024 KB).
3. In **EventChannel Auto Start**, select **On** to have event channels start automatically at Interstage startup.
4. In **Max Concurrent Global Transactions**, specify a value between 1 and 1024 (default is 256).
5. In **2-Phase Commit Transaction Timeout**, specify a value between 1 and 20000 seconds (default is 60 seconds).

6. In **Automatic Recovery Retry Interval**, specify a value between 1 and 1000 seconds (default is 30 seconds), and in **Automatic Recovery Retry Count**, specify a value between 1 and 100 (default is 60).
7. Specify the **Event Channel Common Settings**.

   For details, refer to 8.2.2.1 Setting the Event Channel Common Settings.
8. Click the **Update** button to apply the new configuration to the Server Group or Independent Managed Server highlighted on the navigation tree.

   An execution results message is output to the event log of all servers in the Server Group when processing is complete.

- During deployment to a group, even if configuration fails for any server(s) in the group, deployment to the group is considered successful. In this case, error messages are posted for servers for which deployment failed. Rectify the problem and then click the **Update** button to redeploy to these servers.

8.2.2.1 Setting the Event Channel Common Settings

To set the event channel shared operating environment:

1. In **Event Data Waiting Time (Mixed Model)**, specify a value between 1 and 1,000,000 seconds (default is 40 seconds).
2. In **Volatile Event Data Persistent Time**, specify a value between 0 and 1,000,000 seconds. A value of 0 sets this to unlimited (default is 0). This is the lifetime of event data accumulated in volatile EventChannels
3. In **Local Transaction Timeout**, specify a value between 1 and 1,000,000 seconds (default is 300 seconds).
4. In **Error return when consumer is disconnected,** select **Enable** to return an error to the calling Send or Publish method.
5. In **Notification of EventChannel Termination**, select **Enable** to call the disconnect method when the event channel ends, to notify suppliers and consumers of the termination of the associated EventChannel.
6. Select the **Block Operation Mode,** which is the EventChannel block function, to disable blocking, enable blocking, or enable both blocking and automatic blocking.
7. Specify the **Repository Monitoring Level**, which is a percentage of the [Maximum Number of EventChannel Messages]. When the repository size reaches this level, an alarm will be triggered.
8. Specify the **Repository Monitoring Restart Level**, which is a percentage of the [Maximum Number of EventChannel Messages]. When the repository size reaches this level, repository monitoring will be restarted.
9. Specify the **Event Data Automatic Unlock Level**, which is a percentage of the [Maximum Number of EventChannel Messages]. When the repository size drops below this level, then the EventChannel will be automatically unblocked.
10. In **Maximum Number of EventChannel Messages**, specify a value between 1 and 10,000,000 (default is 3000).
11. In **Involatile Event Data Persistence Time**, specify a value between 1 and 2,000,000 or 0 for unlimited (default is 0), which is the lifetime of event data stored in a EventChannel when it is a non-volatile channel for event data and connection information in seconds.

- If the fields in steps 4, 5 and 6 are changed during non volatile operation, the event channel must be created again.

8.2.3 Managing Storage Destinations

8.2.3.1 Viewing Storage Destinations

Application Management

Interstage > Interstage Application Server > Services > Event Service > [server group | independent managed server] > Stores	View Unit

A list of storage destinations used for the event channels created for the selected Server Group/Server is displayed. The destination type (standard or extended) and Last Action Status is given for each.

Click the Details **[Show]** link to view the storage destination information for each server in a Server Group. For each server in a Server Group, System Usage (%), Event Data Usage (%), System Data Storage Areas, Event Data Storage Areas and Last Action Status are given. Last Action Error are listed for servers where there was a problem creating the storage destination.

The Last Action Status is displayed as:

- **Normal** where storage creation completed normally for all servers in the case of the Server Group or for the server not a member of a group.
- **Normal (Part)** in the case of Server Groups where an error occurred at some servers during storage creation.
- **Abnormal** for member server where an error occurred during storage creation.

Click a Unit ID to view the configuration information of that Storage Destination as defined in 8.2.3.2 Creating Storage Destinations for Event Channels.

Standalone

Interstage > Interstage Application Server > System > Services > Event Service > Stores	View Unit

A list of storage destinations used for the event channels created for the server is displayed. The destination type (standard or extended) and environment setup status is given for each. The System Usage (%), Event Data Usage (%), System Data Storage Areas and Event Data Storage Areas are given for each.

8.2.3.2 Creating Storage Destinations for Event Channels

Application Management

Interstage > Interstage Application Server > Services > Event Service > [server group | independent managed server] > Stores	Create a New Unit

Standalone

Interstage > Interstage Application Server > System > Services > Event Service > Stores	Create a New Unit

To create a Storage Destination:

1. In **Unit ID**, type a unique name for the storage destination.

   This is used by the persistent channel.

2. Click the **[Show]** link to access the Detailed Settings
3. In **Unit Mode**, select **Extended Mode** if global transactions are to be used.
4. In **Storage Directory**, specify where this unit should be stored.
5. In **Transaction Concurrency**, specify a value between 1 and 1024 (default is 1024 for Windows, 100 for Solaris and Linux).

6. In **Size of System File**, specify a value between 1 and 2047 MB (default is 10 MB). In **Number of System Data Storage Areas**, specify a value between 4 and 32768 (default is 1000).
7. In **Size of Event Data File**, specify a value between 1 and 2047 MB (default is 30MB). In Number of **Event Data Storage Areas**, specify a value between 1 and 32768 (default is 50).
8. In **Size of Shared Memory**, specify a value between 1 and 1024 MB to share memory between messages stores (default is 80 MB).
9. Click the **Create** button to create the new Event Service Storage Destination on the server/all servers in the Server Group.

   An execution results message is posted when processing is complete at all servers in a Server Group.

   Click the **Reset** button to return this form to the default values.

- If a storage destination with the name specified already exists on a server that is a member of a Server Group, storage destination creation fails for that server, but is successful for other servers in the group and for the Server Group.
- During deployment to a group, even if storage destination creation fails for any server(s) in the group, deployment to the group is considered successful. In this case, error messages are posted for servers for which deployment failed. Rectify the problem and then click the **Update** button to redeploy to these servers.

8.2.3.3 Deleting Storage Destinations

Application Management

Interstage > Interstage Application Server > Services > Event Service > [server group | independent managed server] > Stores	View Unit

Standalone

Interstage > Interstage Application Server > System > Services > Event Service > Stores	View Unit

To delete a Store:

1. Click the checkbox to the left of any Store to be deleted.

   Click the **Select All** button to select all Store in the list.
2. Click the **Delete** button to remove and undeploy the selected Store(s).
3. Click the **OK** button to confirm deletion.

- If the Store being deleted was deployed to a Server Group, it will be removed from all servers in the group. If an error occurs at some servers in the group, an error message is posted for those servers.

8.2.4 Managing Event Channels

Interstage supports two types of Event Channels:

- Event Channels used by the Event Service
- Event Channels used by JMS.

Manipulations on event channels are detailed below.

8.2.4.1 Viewing Event Channels

Application Management

Interstage > Interstage Application Server > Services > Event Service > [server group | independent managed server] > EventChannels	View Status

A list of the event channels created for the Server Group or Independent Managed Server is displayed. The following information is displayed for the respective channel types:

Event Service channels

The channel Group Name, Channel Name, Model, Unit, Status and Last Action Status

JMS channels

The channel Group Name, Channel Name, Type, the JMS Destination, Unit, Status and Last Action Status.

Click the Details **[Show]** link to view the event channel status for each server in a Server Group. Additional information given for each server includes the Current number of accumulated messages, and the number of consumers and publishers connected.

The Status is given for each item. The table below details the possible status values for Server Groups/servers.

Table 8.1 Event channel status for Server Groups/Independent Managed Servers

Last Action Status	Explanation	
	Server Group	Server
Not yet connected	Cannot connect to server	Cannot connect to server
Running	Event channel is started on all servers in the Server Group.	Event channel is started.
Running (part)	Event channel is started, but some event channels in the Server Group are stopped.	-
Stopped	Event channel is stopped on all servers in the Server Group.	Event channel is stopped.
Stop processing in progress	Event channel stop processing is in progress on all servers in the Server Group.	Event channel stop processing is in progress.
Partial stop processing in progress	Stop processing is in progress for some event channels in the Server Group.	-

The Last Action Status for an event channel is displayed as:

- **Normal** where event service configuration setup completed normally for all servers in the case of the Server Group, or for the server not a member of a group.
- **Normal (Part)** in the case of Server Groups where an error occurred at some servers during event service configuration setup.
- **Abnormal** for a Independent Managed Server where an error occurred during event service configuration setup.

Error information is given on servers where there was a problem creating the event channel.

Standalone

Interstage > Interstage Application Server > System > Services > Event Service > EventChannels	View Status

A list of the event channels created for the server is displayed. The channel Group name, Channel Name, the Model (for JMS channels shows the type), Unit (shows the destination), Status (shows the operating status), the Number of Messages (shows current number of accumulated messages), the number of Consumer Connections and that of Producer Connections.

Click a unit ID to view to access the configuration information of that event channel.

8.2.4.2 Creating an Event Service Event Channel

Application Management

Interstage > Interstage Application Server > Services > Event Service > [server group | independent managed server] > EventChannels	Create a New EventChannel

Standalone

Interstage > Interstage Application Server > System > Services > Event Service > EventChannels	Create a New EventChannel

To create an Event Service Event Channel:

1. If in the Application Management tab, in **EventChannel Type**, select Event Service.
2. Specify the **EventChannel Group Name**. If the Naming Service is shared, the same group name cannot be created in some patterns.

   This name must be unique within the site.
3. Specify the **EventChannel Name**.
4. Click the **[Show]** link to access the Detailed Setup, and in **Notification Service**, select **Enable** to use notification service function.
   - Select the **Model** from the dropdown list:

Model	Description
Point-To-Point	For use when a message is addressed to a specific recipient. It is communication between one sender and one receiver. The IP and port of the recipient is needed to uniquely identify the recipient.
Multicast	For use to send the same message to a large number of recipients. It involves sending data from one sender to multiple receivers. In multicasting, a multicast group is given a class D IP address to which an interested recipient may join and listen to the data that's published on that multicast group.

   - In **Persistent Channel**, select one of the following options if message persistence is required:
     - **On (Event Data, Involatile Connection Information)**
   - Make event data and connection information persistent
     - **On (Involatile Connection Information)**
   - Make only connection information persistent

     Select Unit ID from the dropdown list

     In **Global Transactions,** select Enable if Global Transactions are to be supported.
   - In **Local Transactions** , select Enable if **Local Transactions** are to be used.
5. In **Maximum Number of Connections,** specify a value between 1 and 9999 (default is 16).
6. Select Enable if **SSL Communication** for the Event Channel is to be used.

7. Select Enable if **Automatic connection recovery** is to be used.

   This will cause remaining connection information in the EventChannel to be automatically collected when the consumer and producer disconnect, without issuing the connection 'close' method.

8. Click the **Create** button to create the Event Channel.

   An execution results message is posted when processing is complete at all servers in a Server Group.

Note

- If a event channel with the name specified already exists on a server that is a member of a Server Group, event channel creation fails for that server, but is successful for other servers in the group and for the Server Group.
- During event channel creation for a Server Group, even if creation fails for any server(s) in the group, creation to the group is considered successful. In this case, error messages are posted for servers for which creation failed. Rectify the problem and then click the **Update** button to retry on these servers.

8.2.4.3 Creating a JMS Event Channel (Admin Server Only)

For details on creating a JMS Event Channel on a Standalone Server, refer to Creating a JMS Event Channel, under Managing JMS Event Channels (Standalone) of the Resources chapter.

Application Management

Interstage > Interstage Application Server > Services > Event Service > [server group | independent managed server] > EventChannels	Create a New EventChannel

To create a JMS Event Channel:

1. In **EventChannel Type**, select JMS.
2. Specify the **EventChannel Group Name**. If the Naming Service is shared, the same group name cannot be created in some patterns.

   This name must be unique within the site.

3. Specify the **EventChannel Name**.
4. Select **Type** (Topic or Queue) from the dropdown list.
5. Click the **[Show]** link to access the Detailed Setup, and in Persistent Channel, select Enable to use persistent channel.
   - Select Unit ID from the dropdown list
   - Select Enable if Global Transactions are to be supported.
6. In **Maximum Number of Connections,** specify a value between 1 and 9999 (default is 16).
7. Select Enable if **SSL Communication** for the Event Channel is to be used.
8. Select Enable if **Automatic connection recovery** is to be used.

   This will cause remaining connection information in the EventChannel to be automatically collected when the consumer and producer disconnect, without issuing the connection 'close' method.

9. Click the **Create** button to create the Event Channel.

   An execution results message is posted when processing is complete at all servers in a Server Group.

Note

- If an event channel with the name specified already exists on a server that is a member of a Server Group, event channel creation fails for that server, but is successful for other servers in the group and for the Server Group.

- During event channel creation for a Server Group, even if creation fails for any server(s) in the group, creation to the group is considered successful. In this case, error messages are posted for servers for which creation failed. Rectify the problem and then click the **Update** button to retry on these servers.

8.2.4.4 Starting Event Channels

Application Management

Interstage > Interstage Application Server > Services > Event Service > [server group | independent managed server] > EventChannels	View Status

Standalone

Interstage > Interstage Application Server > System > Services > Event Service > EventChannels	View Status

To start an Event Channel:

1. Click the checkbox to the left of any Event Channels to be started.

   Click the **Select All** button to start all Event Channels in the list.

2. Click the **Start** button to start the selected Event Channels.

   An execution results message is posted when service startup is completed at all servers in a Server Group.

3. If any of the selected Event Channels use Global Transactions, select:

   - **Normal start** to start the event channel normally
   - **Rollback Incomplete Transactions** to roll back an incomplete transaction forcibly and start the event channel. Select this option if error message es11017 is posted to the status frame.
   - **Commit Incomplete Transactions** to commit an incomplete transaction forcibly and start the event channel. Select this option if error message es11017 is posted to the status frame.

4. Click the **Execute** button to start the selected event channels in the manner selected.

   An execution results message is posted when service startup is completed at all servers in a Server Group.

Note

- In a multi-server environment, if start processing fails for any server(s) in the group, the service continues running and start processing continues for other servers. Click the **Start** button again to retry the start process on servers that did not start successfully.

8.2.4.5 Stopping Event Channels

Application Management

Interstage > Interstage Application Server > Services > Event Service > [server group | independent managed server] > EventChannels	View Status

Standalone

Interstage > Interstage Application Server > System > Services > Event Service > EventChannels	View Status

To stop an Event Channel on a Server Group/Server:

1. Click the checkbox to the right of any Event Channels to be started.

   Click the **Select All** button to start all Event Channels in the list.

2. Click the **Stop** button to stop the selected Event Channels.
3. Select:
   - **Normal Stop** to block new requests and to wait for completion of existing requests. Then stop the Event Channel.
   - **Forced Stop** to stop the event channel in compulsion mode.
4. Click the **Execute** button to stop the selected event channels in the manner selected.

   An execution results message is posted when the service stop processing is completed on all servers.

Note

- In a multi-server environment, if stop processing fails for any server(s) in the group, stop processing continues for other servers. Click the Stop button again to retry the service stop process on servers that where it failed.
- If **Volatile Event Data Persistence Time** is set to 0, use **Forced Stop** to terminate the Event Channel.

8.2.4.6 Setting Event Channels to Start Automatically

Application Management

Interstage > Interstage Application Server > Services > Event Service > [server group | independent managed server] > EventChannels	Auto Start Settings

Standalone

Interstage > Interstage Application Server > System > Services > Event Service > EventChannels	Auto Start Settings

To set an event channel to start automatically:

1. Select **On** for each Event Channel that is required to start at Interstage startup.
2. Click the **Update** button to save the changes.

Note

- An execution results message is posted when processing is complete at all servers in the Server Group. If an error occurs at some servers in the Server Group, error messages indicating the servers where errors occurred are posted.

8.2.4.7 Updating Event Channel Configuration Information

Application Management

Interstage > Interstage Application Server > Services > Event service > [server group name] | [server name] > EventChannels > [Event Channel name]	Settings

Standalone

Interstage > Interstage Application Server > System > Services > Event Service > EventChannels> [Event Channel name]	Settings

To update event channel configuration information:

1. If the Event Channel Type is 'Event Service', specify the **Event Data Waiting Time (Mixed Model)** in seconds, and specify the **Volatile Event Data Persistence Time** in seconds.
2. If in the Application Management tab, if the Event Channel Type is 'JMS', specify the **Event Data Waiting Time** in seconds.
3. Specify the **Local Transaction Timeout** in seconds.
4. In **Error return when consumer is disconnected**, select Enable to use this feature.
5. If the Event Channel Type is 'Event Service', in **Notification of EventChannel Termination** select Enable to use this feature.
6. Select the **Block Operation Mode,** which is the EventChannel block function, to disable blocking, enable blocking, or enable both blocking and automatic blocking.
7. Specify the **Repository Monitoring Level**, which is a percentage of the [Maximum Number of EventChannel Messages]. When the repository size reaches this level, an alarm will be triggered.
8. Specify the **Repository Monitoring Restart Level**, which is a percentage of the [Maximum Number of EventChannel Messages]. When the repository size reaches this level, repository monitoring will be restarted.
9. Specify the **Event Data Automatic Unlock Level**, which is a percentage of the [Maximum Number of EventChannel Messages]. When the repository size drops below this level, then the EventChannel will be automatically unblocked.
10. In **Maximum Number of EventChannel Messages**, specify a value between 1 and 10,000,000 (default is 3000).
11. If the Event Channel Type is 'Event Service', specify the **Involatile Event Data Persistence Time** in seconds.
12. Click the **Update** button to update the event channel details.

    An execution results message is posted when processing is complete at all servers in the Server Group.

- For a definition applied to a Server Group, even if update fails for any server(s) in the group, update for the group is considered successful. In this case, error messages are posted for servers for which deployment failed. Rectify the problem and then click the **Update** button to redeploy to these servers.

8.2.4.8 Deleting Event Channels

Application Management

Interstage > Interstage Application Server > Services > Event Service > [server group name] | [independent managed server] > EventChannels	View Status

Standalone

Interstage > Interstage Application Server > System > Services > Event Service > EventChannels	View Status

To delete Event Channels:

1. Check the Event Channels to be deleted.

   Click the **Select All** button to select all Event Channels in the list.
2. Click the **Delete** button to delete the selected Event Channels.
3. Click the **OK** button to confirm deletion.

Note

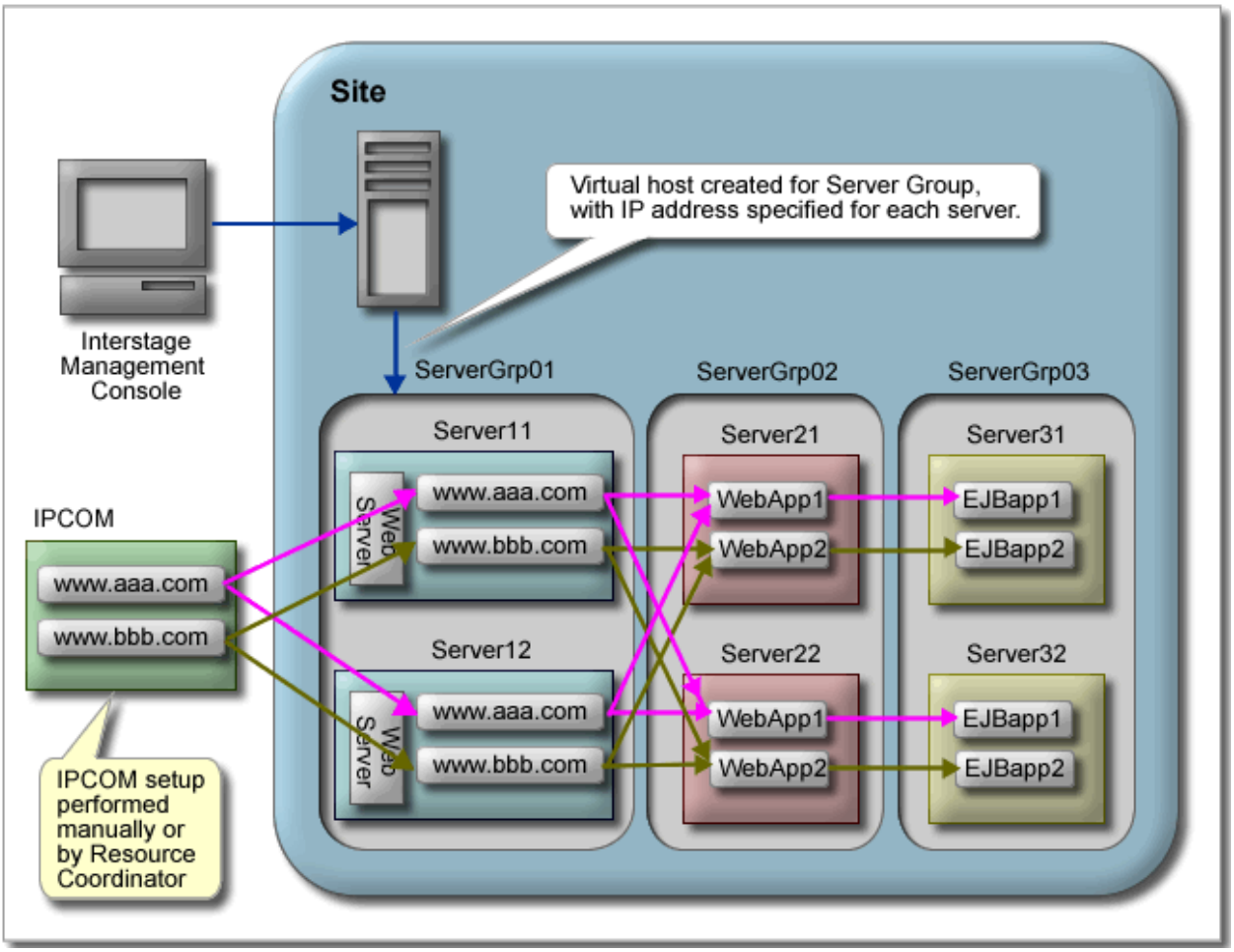
- If the event channel being deleted was deployed to a Server Group, it will be removed from all servers in the group. If an error occurs at some servers in the group, an error message is posted for each.

8.3 Managing the Web Server

To set the Web Server Synchronization mode, refer to the Chapter 4 System chapter.

In a multi-server environment, Web Server settings are the same for all servers in a Server Group and Virtual Hosts operate on all servers in the group. The Systemwalker Resource Coordinator can be used to set up Fujitsu's IPCOM or similar load distribution products to distribute client requests.

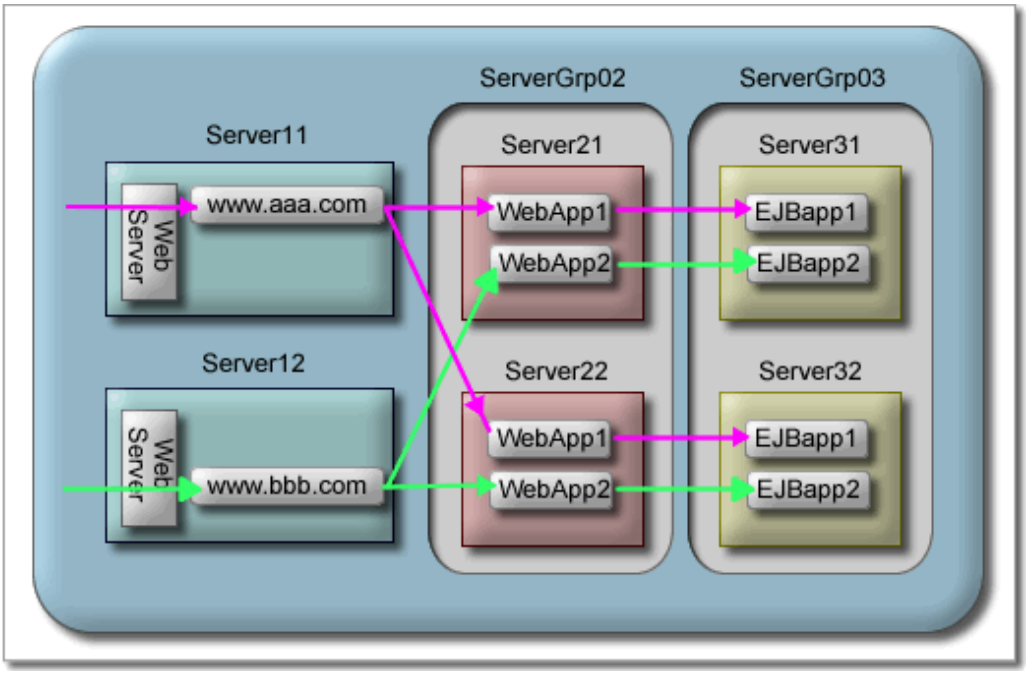
Figure 8.1 SystemWalker Resource Coordinator for IPCOM or similar load distribution set up



Note

- Although the Web Server can be configured at the Server Group level, it is not possible to specify a load distribution pattern where the individual servers in the group handle requests for different web applications (as shown in the following diagram). Every server in the group can handle any requests that the Web Server may receive.

Figure 8.2 Load distribution pattern that splits entry from the Web server



8.3.1 Viewing/Starting/Stopping the Web Server

8.3.1.1 Viewing the Web Server List / Web Server Status

Application Management

Interstage > Interstage Application Server > Services > Web Server	List

Standalone

Interstage > Interstage Application Server > System > Services > Web Server	List

A list of all Web Servers created is displayed. By default one Web Server is always created. The status of the Web Server is one of the following values:

- Running
- Running (partially)

  This is displayed where the item is a Server Group, and the Web server is running on some but not all servers in the group.
- Stopped.

Click on a Web Server name to view details of that Web Server - the Web Server Status.

Application Management

Interstage > Interstage Application Server > Services > Web Server > [Web Server name (server group | independent managed server)]	Web Server Status

Standalone

Interstage > Interstage Application Server > System > Services > Web Server > [Web Server name]	Web Server Status

The Web Server Status displays the status of the Web Server selected. For multi-servers a list of all Server Group(s), Independent Managed Server(s) or Standalone server(s) is displayed. The status of the Web Server is one of the following values:

- Running
- Running (partially)

  This is displayed where the item is a Server Group, and the Web server is running on some but not all servers in the group.
- Stopped.

For a Server Group, click the Details **[Show]** link to view the Web Server status for each server in the group. The status is given for each as Running or Stopped.

Click the **Refresh** button to refresh the list.

8.3.1.2 Starting/Stopping the Web Server from List / from Status

Application Management

Interstage > Interstage Application Server > Services > Web Server	List

Standalone

Interstage > Interstage Application Server > System > Services > Web Server	List

From the List, select the check box corresponding to the Web Server to start/stop. Click the **Start** or **Stop** button to start or stop the Web Server.

Alternatively, a Web Server can be started/stopped from its detailed view by clicking on the Web Server name from the List.

Application Management

Interstage > Interstage Application Server > Services > Web Server > [Web Server name (server group | independent managed server)]	Web Server Status

Standalone

Interstage > Interstage Application Server > System > Services > Web Server > [Web Server name]	Web Server Status

Click on the Start or Stop button to start or stop the Web Server respectively.

In a multi-server environment, the Status field will display Running, Stopped or Running (partially) where the Web Server did not start on all servers in a Server Group. Click the **[Show]** link at **Application Management** to view the status for each server in the group.

Note

- In a multi-server environment, if one or more servers in a Server Group fail to start/stop, the Web Server service is started/stopped on those without problems. Address the problem, and then click the **Start/Stop** button again to retry starting/stopping the service on the remaining servers.

8.3.2 Creating a New Web Server (Standalone)

Standalone

Interstage > Interstage Application Server > System > Services > Web Server	Create a new Web Server

To create a new Web Server, enter the following settings:

1. Specify the **Web Server Name**.
2. Specify the **Port Number**, or IP address:port number used for receiving connections requests from the client.
3. Specify the **Server Hostname or IP Address** used for the Web Server.

8.3.3 Configuring the Web Server

Configuring the Web Server involves configuring the General Settings, the Error Log, the Access Log, and SSL encryption if required.

Application Management

Interstage > Interstage Application Server > Services > Web Server > [Web Server name (server group | independent managed server)]	Web Server Settings

Standalone

Interstage > Interstage Application Server > System > Services > Web Server > [Web Server name]	Web Server Settings

To configure the Web Server environment general settings:

1. In **DocumentRoot Folder**, specify the top level directory for server resources available to clients (e.g. C:/Interstage/F3FMihs/[Web Server Name]/htdocs).
2. Specify the **Port Number**, click the **[Show]** link to access Detailed Settings, and specify the **Server Host Name or IP Address**, of the Web Server.

   For Server Groups, the 'Host name or IP address' can be specified for each server in the group.
3. In **Timeout with client connection**, specify the timeout in seconds for client connections. A value of 0 means there is no timeout.
4. In **Enable HTTP Keep-Alive**, select **Yes** to have the connection remain open between browser requests, and in **Timeout between requests when Keep-Alive is used**, specify for how long the connection should remain open between requests before it is closed. A value of 0 means the connection will not be closed.
5. Specify the **Maximum number of simultaneous client connections** and the **Maximum size of request messages** in bytes. A value of 0 for the request size means there is no maximum size.
6. Refer to 8.3.3.1 Defining Error and Access Log Settings for details on setting up **Error Log** and **Access log**.
7. Under **SSL Settings**, in **Enable SSL Encryption?,** select **Yes** to enable encryption for communications with the Web Server(s) and select the required **SSL Configuration** from the dropdown list.

   For details on SSL Configuration, refer to the Chapter 11 Security chapter.
8. Click the **Update** button to apply these settings.

8.3.3.1 Defining Error and Access Log Settings

The procedure to define the error and access logs is the same, with access logs allowing the additional selection of the log file format. The Access Log Settings table is located below the Error Log Settings table.

Web Server Settings	Detailed Settings	Error Log Settings | Access Log Settings

To define the log settings for the Web Server:

1. In **Log file**, specify the path and filename for the log file.

2. In **Format**, select one of the following:
   - **ihs-analysis**
   - **combined** to record all information on common, referer and agent in the log
   - **common** to record the log with Common Log Format
   - **referer** to record the trace information on the client to the log
   - **agent** to record information on Web browser that the client uses to the log
3. In **Rotation type and rotation interval**, select one of the following:
   - **Log file size (MB)** and specify the maximum log file size (a new log file is created when this limit is reached).
   - **Time interval (no. of days)** and specify the number of days after which a new log file should be created.
   - **Time (Hours and Minutes)** and specify the number of hours and minutes after which a new log file should be created.
   - **Date** and specify when a new log file should be created.
   - **Day of Week** and specify the days of the week in which a new log file should be created.
   - **Not required** if multiple log files are not required. No further fields need be specified for this option.
4. If setting up the Error Log, specify the **Number of log files to maintain**. New log file will be created based on the rotation settings in step 2 until the specified number of log files is reached. Log files will then be overwritten starting from the oldest file.

8.3.4 Viewing the Web Server Logs

Site Management

Interstage > Interstage Application Server > [server group > managed server | independent managed server] > [server] > System > Services > Web Server > [Web Server name]	View Log

Standalone

Interstage > Interstage Application Server> System > Services > Web Server > [Web Server name]	View Log

Click the Error Log or Access Log tab to view the required log.

8.3.5 Managing Virtual Hosts

A virtual host with the same name can be created on all servers in a Server Group. All the virtual hosts have the same settings except that different IP addresses and port numbers can be specified for each server.

Since each server has a different real IP address, only the host name of the virtual host is displayed in the tree.

8.3.5.1 Viewing Virtual Hosts

Application Management

Interstage > Interstage Application Server > Services > Web Server > [Web Server name (server group | independent managed server)] > Virtual Hosts	View list of the Virtual Hosts

Standalone

Interstage > Interstage Application Server > System > Services > Web Server > [Web Server name] > Virtual Hosts	View list of the Virtual Hosts

A list of virtual host names is displayed.

Each Virtual Host Name is a hyperlink to the page from where the virtual host can be configured.

Click the **Refresh** button to refresh the list.

8.3.5.2 Creating a New Virtual Host

Application Management

Interstage > Interstage Application Server > Services > Web Server > [Web Server name (server group | independent managed server)] > Virtual Hosts	Create a new Virtual Host

Standalone

Interstage > Interstage Application Server > System > Services > Web Server > [Web Server name] > Virtual Hosts	Create a new Virtual Host

To create a virtual host:

1. Specify the **IP Address**, **Port Number**, **Server Hostname** and **DocumentRoot Folder** for the virtual host.

   If working on a Server Group, a different IP Address and Port Number can be defined for each server in the group.

2. Click the **[Show]** link to access Detailed Settings.

   Refer to 8.3.3.1 Defining Error and Access Log Settings for details on setting up these logs.

3. Under **Enable SSL Encryption?**, select **Yes** to enable encryption for communications with the Web Server(s) and select the required **SSL Configuration** from the dropdown list.

4. Click the **Create** button to create the virtual host.

   Click the **Reset** button to return this form to the default values.

8.3.5.3 Updating a Virtual Host

Application Management

Interstage > Interstage Application Server > Services > Web Server > [Web Server name (server group | independent managed server)] > Virtual Hosts > [Virtual Host name]	Configuration

Standalone

Interstage > Interstage Application Server > System > Services > Web Server > [Web Server name] > Virtual Hosts > [Virtual Host name]	Configuration

To update a virtual host:

1. Edit the required modifiable settings on the form as described in the tables in section 8.3.5.2 Creating a New Virtual Host.

2. Click the **Update** button to update the virtual host settings.

3. Click the **Refresh** button to refresh the form with the most recently updated values.

8.3.5.4 Deleting a Virtual Host

Application Management

Interstage > Interstage Application Server > Services > Web Server > [Web Server name (server group | independent managed server)] > Virtual Hosts	View list of the Virtual Hosts

Standalone

Interstage > Interstage Application Server > System > Services > Web Server > [Web Server name] > Virtual Hosts	View list of the Virtual Hosts

To delete a virtual host:

1. Click the checkbox to the right of virtual hosts to be deleted.

   Click the **Select All** button to select all virtual hosts in the list.

2. Click the **Delete** button to remove the selected virtual host(s).
3. Click the **OK** button to confirm deletion.

8.3.6 Managing Web Server Connectors

Web Server Connectors are created automatically by the system if the 'Run Web server and WorkUnit on the same machine?' option (under Interstage>Interstage Application Server > System > Update System Settings tab > Servlet Service Settings table) is set to 'Yes'.

If that option is set to 'No', then a Web connector must be manually created as described in '8.3.6.1 Creating a Web Server Connector.

The log definitions for the Web Server Connectors for a Server Group can be set from the Application Management tab. Users can also select a specific server in the Server Group and browse or download the server's logs from the Site Management tab.

8.3.6.1 Creating a Web Server Connector

Standalone

Interstage > Interstage Application Server > System > Services > Web Server > [Web Server name] > Web Server Connectors	Create a new Web Server Connector

To create a Web Server Connector:

1. In **WorkUnit Name,** specify the WorkUnit name (IJServer name) at the connection destination
2. In **Servlet Container IP Address : Port Number**, specify IP address and port number of the machine that runs WorkUnit at the connection destination.
3. In the **Web Application Name**, specify Web application name deployed to the WorkUnit at the connection destination.
4. Click the **[Show]** link to access Detailed Settings.

   To define Web Server Connector Settings,

5. In **Web Server Virtual Host**, specify the virtual host that accepts the demand for the Web application deployed to the WorkUnit at the connection destination.
6. Select **On** in **Use SSL between Servlet Container and Connector?** to use SSL communication between the Web server connector and the Servlet container, and select SSL configuration from the dropdown list

To define **Servlet Container Settings**,

1. In **Send/Receive Timeout**, specify the timeout of the request transmission and the response reception to the Servlet container (*1).
2. In **Maximum number of connections to the Servlet container**, specify the maximum connections that the Servlet container processes (*2).
3. Click the **Reset** button to return this form to the default values.

Note

*1Set the same value as the **Timeout** of the Servlet container set by the environmental setting of the WorkUnit of the machine at the connection destination.

*2Please set the same value as the **Maximum number of connections** of Servlet containers set by the environmental setting of the WorkUnit of the machine at the connection destination.

8.3.6.2 Updating a Web Server Connector

Standalone

Interstage > Interstage Application Server > System > Services > Web Server > [Web Server name] > Web Server Connectors	View list of Web Server Connectors

To update a Web Server Connector:

1. Edit the required modifiable settings on the form as described in the tables in section 8.3.6.1 Creating a Web Server Connector
2. Click the **Update** button to update the Web Server Connector settings.
3. Click the **Refresh** button to refresh the form with the most recently updated values.

8.3.6.3 Deleting a Web Server Connector

Standalone

Interstage > Interstage Application Server > System > Services > Web Server > [Web Server name] > Web Server Connectors	View list of the Virtual Hosts

To delete a Web Server Connector:

1. Click the checkbox to the right of Web Server Connectors to be deleted.

   Click the **Select All** button to select all Web Server Connectors in the list.
2. Click the **Delete** button to remove the selected Web Server Connector(s).
3. Click the **OK** button to confirm deletion.

8.3.6.4 Viewing Web Server Connector Log

Site Management

Interstage > Interstage Application Server > [server group > managed server | independent managed server] > System > Services > Web Server > [Web Server name] > Web Server Connectors	View Log

Standalone

Interstage > Interstage Application Server > System > Services > Web Server > [Web Server name] > Web Server Connectors	View Log

1. Select a log from **Select log file to view** dropdown list to view
2. Click the **Refresh** button to retrieve the latest log data
3. Click the navigation buttons (**First Line, Previous, Next, Last Line)** button to navigation the log data
4. Click the **Download** button to save the log data

8.3.6.5 Configuring the Web Server Connector Log

Application Management

Interstage > Interstage Application Server > Services > Web Server > [Web Server name (server group | independent managed server)] > Web Server Connectors	Log Settings

Standalone

Interstage > Interstage Application Server > System > Services > Web Server > [Web Server name] > Web Server Connectors	Log Settings

1. In **Log File Directory,** specify the folder for log file output.
2. In **Rotate log file based on:** select:
   - **Log Size**, and specify the size of log file (MB).
   - **Backup start time** and specify the start time and interval.
3. In **Number of log files to maintain**, specify the number of generations of the rotated log file to be stored.
4. In **Write debugging info to log?**, select **Yes** to output debugging information.
5. Click the **Update** button to update the log settings.

   Click the **Refresh** button to refresh the form with the most recently updated values.

8.3.6.6 Configuring the Web Server Connector Fault Monitoring

Application Management

Interstage > Interstage Application Server > Services > Web Server > [Web Server name (server group | independent managed server)] > Web Server Connectors	Fault Monitoring Settings

Standalone

Interstage > Interstage Application Server > System > Services > Web Server > [Web Server name] > Web Server Connectors	Fault Monitoring Settings

1. In **Fault Monitoring Method:**, select:
   - **Do not use** to disable the fault monitoring.
   - **Ping Monitoring** to use the Ping method for fault monitoring.
   - **Port Monitoring** to use the Port method for fault monitoring.
2. In **Fault Monitoring Interval**, specify the fault monitoring interval from 1 to 99999 seconds.
3. In **Response Wait Time**, specify the response wait time from the Servlet container.
4. In **Fault Retry Count**, specify the retry count for determining fault status when there is no reply from the Servlet container.
5. Click the **[Show]** link to access **Fault Monitoring Settings**, and in **Startup Wait Time** specify the startup wait time for fault monitoring linkage after the Web server connector is started.
6. Click the **Update** button to update the fault monitoring settings.

   Click the **Refresh** button to refresh the form with the most recently updated values.

8.3.7 Importing Existing Web Server Definitions

In a multi-server environment it is possible to import existing Web Server definitions from one server in a Server Group and then automatically copy them to all other servers in the group.

Application Management

Interstage > Interstage Application Server > Services > Web Server > [Web Server name (server group | independent managed server)]	Import Definition

To import Web Server definitions from a specific server:

1. In **Source of Importing,** select a server name from the **Server** drop down list.
2. Click the **Select** button to view the definition file.

3. Click the **Update** button to import the definition.

   Click the **Back** button to cancel the importing.

8.4 Managing the Repository

For details of global repository settings, refer to the Chapter 4 System chapter.

8.4.1 Viewing/Starting/Stopping the Repository

Application Management

Interstage > Interstage Application Server > Security > Repository	View Status

Standalone

Interstage > Interstage Application Server > System > Services > Repository	View Status

A list of repository set up is displayed. The status of the Repository is one of the following values:

- Running
- Stopped.

Click the **Refresh** button to refresh the list.

8.4.1.1 Starting/Stopping the Repository

Check the check box corresponding to repositories to start/stop.

Click the **Start** or **Stop** button to start or stop the Repository.

8.4.2 Creating a New Repository

Application Management

Interstage > Interstage Application Server > Security > Repository	Create a New Repository

Standalone

Interstage > Interstage Application Server > System > Services > Repository	Create a New Repository

To create a repository:

1. In **Repository Name**, specify the name for the repository.
2. In **Administrator DN**, specify the administrator for management of the created repository. Specify the DN (Distinguished Name) format. The initial value is "cn=manager". (*1)
3. In **Administrator DN password**, specify the Administrator DN password and repeat the password in **Administrator DN password (re-renter)**.
4. In **Public Directory**, specify the top entry for the public repository. Use the DN (Distinguished Name) format. The initial value is "ou=interstage,o=fujitsu,dc=com". (*1)
5. In **Repository Database**, select the database to be used as the repository database. This option can only be specified when creating a new repository. (*1)

   There are three options to select from:

   - Standard DB (default)

- Symfoware
- Oracle

6. In **Database Storage Directory**, specify an existing directory for the database storage destination. (*1)
7. In **Cache Size**, specify cache size used by search processing. Specify a number from 100 to 65535.

If Symfoware is selected as the Repository Database, enter the following settings:

1. In **Database Hostname**, specify the database Hostname.
2. **In Database Port Number**, specify the database port number.
3. In **Database Name**, specify the name of the database.
4. In **Database User ID**, specify the user account password used for connection to the database.
5. In **Database Password**, specify the user account password used for connection to the database.

If Oracle is selected as the Repository Database, enter the following settings:

1. In **Net Service Name**, specify the Net Service name specified when the Oracle database was set up.
2. In **Oracle Home directory**, specify the Oracle home directory set when the Oracle database was installed.
3. In **Database User ID**, specify the user account password used for connection to the database.
4. In **Database Password**, specify the user account password used for connection to the database.
5. Click the **[Show]** link to access Detailed Settings

   Refer to 8.4.2.1 Connection Settings, 8.4.2.2 Search Settings and 8.4.2.3 Access Log Settings for details on the detailed settings.
6. Click the **Create** button to create the Repository.

   Click the **Reset** button to return this form to the default values.

*****1 These settings can be specified only during creation of a new repository.

8.4.2.1 Connection Settings

The procedure to define the Connection settings is shown below.

Create a New Repository	Detailed Settings	Connection Settings

To define the Connection settings for the Repository:

1. In **Port number**, specify the port number used for non-SSL communication. Specify a number from 1 to 65535. (*1)
2. In **Enable SSL encryption?**, select Yes to use SSL communication. (*1)
3. In **SSL Port number**, specify a port number used for SSL communication. (*1)
4. In **SSL configuration**, select an SSL configuration from the drop down list for SSL communication.
5. In **Connection Idle Timeout**, specify the waiting time until the connection with the client is closed. Specify a number from 0 to 3600. 0 means the waiting time is unlimited.

*****1 These settings can be specified only during creation of a new repository.

8.4.2.2 Search Settings

The procedure to define the Search settings is shown below.

Create a New Repository	Detailed Settings	Search Settings

To define the Search settings for the Repository:

1. In **Maximum number of entries that can be searched for**, specify the maximum number of entries returned by search processing. Specify a number from 0 to 10000.
2. In **Search Timeout**, specify search timeout in search processing. Specify a number from 0 to 3600.

8.4.2.3 Access Log Settings

The procedure to define the Access Log settings is shown below:

Create a New Repository	Detailed Settings	Access Log Settings

To define the access log settings for the Repository:

1. In **Maintain Access Log?**, specify **Yes** to output access log.
2. In **Output types**, select the checkbox next to the contents for outputting access log. One or more contents can be selected if it is necessary.
3. In **Access log storage directory**, specify an existing directory for access log storage destination.
4. In **Rotation Type**, select the rotation method used to decide when to create a new access log file. Note that new log file is started whenever the maximum log file size is reached, even if rotate daily or monthly is selected. Select between Size, Daily and Monthly.
5. In **Size**, specify the maximum size of an access log file. When the maximum size is reached, a new log file is started.
6. In **Number of access log files to maintain**, specify the number of access log files to maintain. If the number is exceeded, delete access log files from the oldest one.

8.4.2.4 Defining Replication Settings

Application Management

Interstage > Interstage Application Server > Security > Repository > [repository]	Settings

Standalone

Interstage > Interstage Application Server > System > Services > Repository > [repository]	Settings

The following procedure describes how to define the repository replication settings. The replication settings are available during repository update only.

Settings	Detailed Settings	Replication Settings

To define the replication settings for the Repository:

1. In **Operation mode**, select:
   - **Stand-alone** to operate in standalone mode. Repository replication is not performed.
   - **Slave**, and in **Master host name** specify the hostname of the machine to be specified as the master. The replication is performed automatically by the slave.
   - **Master**, and click the **Add** button to add one or more replication hosts. For details, refer to 8.4.2.5 Defining Replication Connection Settings.
2. Click the **Update** button to update the replication settings.

   Click the **Refresh** button to refresh the form with the most recently updated values.

Note

- The repository must be stopped before performing this operation.
- In a large scale system where the load is to be distributed, the directory is replicated on a master repository server and one or more slave servers. Repositories are always created to operate in standalone mode on a single server and replication settings cannot be modified during creation.

  After creation (and only when it is not running) the repository can be modified to operate in either a master or a slave mode. Once the operation mode has been modified it cannot be changed (except by deleting the repository, and recreating it. In this case, all environmental definitions and data bases are deleted.).
- Replication settings are not available during repository creation. Hence, new repositories are set to standalone by default and can be changed to Slave or Master after creation.

8.4.2.5 Defining Replication Connection Settings

The following procedure describes how to define replication connection settings when adding replication hosts. This is accessible from a Master repository only.

Application Management

Interstage > Interstage Application Server > Security > Repository > [repository]	Settings

Standalone

Interstage > Interstage Application Server > System > Services > Repository > [repository]	Settings

Click the **Add** button to access the Replication Connection Settings table.

To define the replication connection settings for the Repository:

Settings	Detailed Settings	Replication Connection Settings

1. In **Host name**, specify the host name of the slave. (*1)
2. In **Port number**, specify the port number defined for replication on slave. (*1)
3. In **Enable SSL encryption?**, select **Yes** to use SSL encryption during connection to the slave. (*1)
4. In **Present client certificate?**, select **Yes** to have the presentation of client certificate in SSL connection. Specify this according to the selected status of the slave's client authentication.
5. In **SSL Configuration**, select the SSL configuration from the drop down list for presentation of the client certificate.
6. In **DN for connection**, specify the Administrator DN for connection to the slave. (*1)
7. In **Password for connection**, specify the Administrator DN password for connection to the slave. (*1)
8. Click the **Update** button to update the replication connection settings.

   If update succeeds, the added host will appear on the **Replication destination host list**.

   Click the **Cancel** button to cancel the setting.

*1 These settings can only be specified during addition of a new replication host.

Note

- The Master repository must be stopped to perform this operation.
- The Slave must be already created for this operation to succeed.

8.4.2.6 Updating Replication Connection Settings

This operation is only possible for configurations in which there is at least one slave and one master, and is accessible from the Master repository only.

Settings	Detailed Settings	Replication connection Settings

To modify an existing replication connection setting for the Repository:

1. Click the checkbox to the left of the host to be modified from the '**Replication destination host list**', and click the **Edit** button.
2. Modify the settings as required. For details, refer to 8.4.2.5 Defining Replication Connection Settings.
3. Click the **Update** button.

8.4.2.7 Deleting Replication Connection Settings

Settings	Detailed Settings	Replication connection Settings

To delete an existing replication connection setting for the Repository:

1. Click the checkbox to the left of the host to be modified from the '**Replication destination host list**'.
2. Click the **Delete** button.
3. Click the **OK** button to confirm deletion.

8.4.3 Updating a Repository

Application Management

Interstage > Interstage Application Server > Security > Repository	View Status

Standalone

Interstage > Interstage Application Server > System > Services > Repository	View Status

To update a repository:

1. If the repository is running, click the **Stop** button to stop the service.
2. Click the Repository Name corresponding to the repository to be modified to access its Environment Settings.
3. Edit the required modifiable settings. For details, refer to 8.4.2 Creating a New Repository.
4. Click the **Update** button to update the repository settings.

   Click the **Refresh** button to refresh the form with the most recently updated values.

8.4.4 Deleting a Repository

Application Management

Interstage > Interstage Application Server > Security > Repository	View Status

Standalone

Interstage > Interstage Application Server > System > Services > Repository	View Status

To delete a Repository:

1. Click the checkbox to the left of the repository to be deleted.
2. Click the **Delete** button to remove the selected repository.
3. Click the **OK** button to confirm deletion.

8.5 Managing the Transaction Service (OTS) Multi-server Only

Windows32/64 Solaris32 Linux32/64

This section describes the procedure and environment setup required to use distributed transactions for CORBA services. These are referred to as Object Transaction Service (OTS). OTS is required only if a CORBA application uses global transactions. OTS Transaction Service can be created on an Independent Managed Server only, (not a Server Groups).

This section describes to the following:

- 8.5.1 Creating an OTS
- 8.5.2 Viewing/Starting/Stopping OTS
- 8.5.3 Updating OTS
- 8.5.4 Deleting an OTS

OTS System

The OTS System consists of multiple objects. It manages transaction information, controls recovery and so on.

8.5.1 Creating an OTS

The procedure below can be used to create a Distributed Transaction Service for CORBA and C/C++ applications.

Application Management

Interstage > Interstage Application Server > Services > Transaction Service(OTS) > [independent managed server]	Create New

To create an OTS:

1. In **Server Information table**, select the name of an **Independent Managed Server** from the dropdown list as the OTS destination.
2. In the **J2EE Settings** table, in **Classpath**, specify the CLASSPATH. Delimit each Classpath entry with a carriage-return.
3. Specify the **Detailed Setup**. Refer to 8.6.1.1 Specifying the Transaction Service Detailed Setup.
4. Specify values for the **Transaction Service Detailed Settings**. Refer to 8.6.1.2 Specifying Transaction Service Detailed Settings.
5. Click the **Create** button.

Note

- In Interstage > Interstage Application Server > System > [Independent Managed Server] > Environment Settings > Detailed Settings > Transaction Service (OTS) settings, select **No** before adding an Interstage Application server to a site. If Yes is selected, it will not be possible to create an OTS using the above procedure.

- An OTS can be created for an Independent Managed Server only (not for a Server Group).

8.5.2 Viewing/Starting/Stopping OTS

Application Management

Interstage > Interstage Application Server > Services > Transaction Service(OTS)	Status

The Server Groups/Independent Managed Servers with OTS transaction enabled are listed along with their status.

Check the checkbox corresponding to Server Groups/Independent Managed Servers on which this service is to be started.

Click the **Start (IS)**/**Stop (IS)** button as appropriate.

The Status field will display Running or Stopped for each Server Group/Independent Managed Server.

Click the **[Show]** link to view the result of the operation on each server in a Server Group.

Note

- The Transaction Service must be activated. To activate the Transaction Service, go to System > Update System Settings tab > Detailed Settings > Transaction Service (OTS) Settings table, and select Yes.
- OTS is linked to Interstage and starts/stops when Interstage is started/stopped.

8.5.3 Updating OTS

Application Management

Interstage > Interstage Application Server > Services > Transaction Service(OTS) > [OTS service name]	Environment Settings

The Server Group Name/Independent Managed Server Name is displayed and cannot be edited.

To update OTS settings:

1. In the **J2EE settings,** modify the **Classpath** if required. Delimit each Classpath entry with a carriage-return.
2. Update the Detailed Setup values as required.

   For details, refer to 8.6.1.1 Specifying the Transaction Service Detailed Setup.
3. Update Transaction Service Detailed Settings values as required.

   For details, refer to 8.6.1.2 Specifying Transaction Service Detailed Settings.
4. Click the **Update** button.

8.5.4 Deleting an OTS

Application Management

Interstage > Interstage Application Server > Services > Transaction Service(OTS) > [OTS service name]	Status

To delete an OTS Transaction Service:

1. If the OTS Transaction Service is running, click the **Stop** button to stop the service.
2. Click the **Delete** button.

   A confirmation dialog is displayed.

3. Click the **OK** button to continue the delete operation.

8.6 Managing the Transaction Service (JTSRMP) Multi-server Only

Windows32/64 Solaris32 Linux32/64

JTSRMP is required for Distributed Transaction support for EJB applications.

This section describes:

- 8.6.1 Creating a JTSRMP
- 8.6.2 Starting/Stopping JTSRMP
- 8.6.3 Updating a JTSRMP
- 8.6.4 Deleting a JTSRMP

8.6.1 Creating a JTSRMP

The procedure below can be used for creating a JTS resource management program.

Application Management

Interstage > Interstage Application Server > Services > Transaction Service (JTSRMP)	Create New

To create JTSRMP:

1. In **Server Group/Server information** table, select the name of a Server Group / Independent Managed Server from the dropdown list.
2. In the **J2EE Settings** table, specify the **Classpath**. Delimit each Classpath entry with a carriage-return.
3. Specify the **Detailed Setup** values as required.

   For details, refer to 8.6.1.1 Specifying the Transaction Service Detailed Setup.
4. Specify the **Transaction Service Detailed Settings**.

   For details, refer to 8.6.1.2 Specifying Transaction Service Detailed Settings.
5. Click the **Create** button.

Note

- In Interstage > Interstage Application Server > System > [Independent Managed Server] > Environment Settings > Detailed Settings > Transaction Service (OTS) settings, select **No** before adding an Interstage Application server to a site. If Yes is selected, it will not be possible to create an OTS using the above procedure.
- A JTSRMP can be created for a Server Group or an independent Managed Server.

8.6.1.1 Specifying the Transaction Service Detailed Setup

To specify the transaction service detailed setup, in the Detailed Setup table:

1. If **System Mode** is set to 'sys', in **Transaction Log Path**, specify the storage location and file name for the transactions log file.
2. In **Maximum Number of Transactions**, specify the maximum number of global transactions that can be handled in a domain.
3. Specify the **OTS System Concurrency** (Maximum is 31).
4. In **JTS RMP Process Concurrency** and **JTS RMP thread Concurrency**, specify the process and thread concurrency respectively for the JTSRMP process that handles transactions between a J2EE application and a resource.

5. In **Maximum Number of resources per global transaction**, specify the number of resources that can be used for a global transaction.
6. If the **System Mode** is set to 'rmp', specify the **Naming Service Hostname** and **Naming Service Port Number**, and the OTS system locale.

   The values specified here must be those of the server on which the Resource Management Program is setup.
7. In **Node Type**, select:

   Active

   This is generally used for this configuration.

   Standby

   When using a cluster system, select **Active** or **Standby** depending on the node settings.
8. Define the required settings in the **Transactions Service Detailed Settings** table below this table. For details, refer to 8.6.1.2 Specifying Transaction Service Detailed Settings.

8.6.1.2 Specifying Transaction Service Detailed Settings

The following procedure describes how to set the Transaction Service settings when distributed transactions are created / used.

To configure the Transaction Service settings for distributed transactions, in the **Transaction Service Detailed Setup** table:

1. Specify the **Transaction Timeout** in seconds to define the maximum length of any transaction
2. Specify the **Two-phase Commitment Timeout** time in seconds for the maximum wait time for a 2-phase commit.
3. In **Maximum number of transactions per resource**, specify the maximum number of global transactions that can be handled to a resource at the same time.

   For best performance, this setting should be greater than OTS system concurrency. The value should be doubled if used with J2EE model.
4. In **Path for JDK/JRE for JTS RMP**, specify the absolute path to the Java command used to start JTSRMP.
5. A trace file logging transactions can be output. Select the **Trace Mode** as 1, 2 or 3 as follows:

   1) Trace output only for errors

   2) Trace file is always output

   3) Trace file is not output. To generate a trace file if needed, use the 'otsgetdump' command.

   The trace file is located in 'installation directory\ots\var'.
6. In **Trace Level**, specify level of logging for the JTS environment information as an integer between 0 and 5. A value of zero corresponds to no trace output. Higher values result in increasing trace detail.

   Note that as the trace level is increased, performance is reduced.

8.6.2 Starting/Stopping JTSRMP

Application Management

Interstage > Interstage Application Server > Services > Transaction Service (JTSRMP)	Status

The Server Groups/Independent Managed Servers with JTSRMP transaction enabled are listed along with their status.

Check the checkbox corresponding to Server Groups/Independent Managed Servers on which this service is to be started.

Click the **Start/Stop** button as appropriate.

The Status field will display Running or Stopped for each Server Group/Independent Managed Server.

Click the **[Show]** link to view the result of the operation on each server in a Server Group.

Note

- If one or more servers in a Server Group fail to start, the service is still started on those without problems. Address the problem, and then click the **Start** button again to retry starting the service for the remaining servers.
- The Transaction Service (OTS) must be activated. This can be done from by selecting **Yes** for this under the Detailed Settings of the Update System Settings tab on the System node.

8.6.3 Updating a JTSRMP

Application Management

Interstage > Interstage Application Server > Services > Transaction Service (JTSRMP) > [JTSRMP name]	Environment Settings

To update JTSRMP settings:

1. Server Group Name / Independent Managed Server Name is displayed and cannot be edited.
2. In the J2EE Settings table, modify the **Classpath** if required. Delimit each Classpath entry with a carriage-return.
3. Update the Detailed Setup values as required. For details, refer to 8.6.1.1 Specifying the Transaction Service Detailed Setup.
4. Update Transaction Service Detailed Settings values as required. For details, refer to 8.6.1.2 Specifying Transaction Service Detailed Settings.
5. Click the **Update** button and check for a successful task completion message.

8.6.4 Deleting a JTSRMP

Application Management

Interstage > Interstage Application Server > Services > Transaction Service (JTSRMP) > [JTSRMP name]	Status

To delete a JTSRMP Transaction Service:

1. If the JTSRMP Transaction Service if it is running, click the **Stop** button to stop the service.
2. Click the **Delete** button.

   A confirmation dialog is displayed.
3. Click the **OK** button to continue the delete operation.

   Check the status frame for a successful task completion message.

Chapter 9 WorkUnits General and IJServer

9.1 Managing WorkUnits

Interstage WorkUnits are business application runtime environments that provide applications with infrastructure for services and resources.

A WorkUnit can be used to deploy one or more related business applications. Interstage Application Server can host multiple WorkUnits. Each WorkUnit has its own configuration and can be started and stopped independently of other WorkUnits. Modifying the settings and configuration of a WorkUnit affects all applications hosted by the WorkUnit.

Interstage Enterprise Edition supports two types of WorkUnit for enterprise systems construction using the J2EE and the CORBA models.

Note

- J2EE WorkUnits are called IJServers and encapsulate J2EE Servlet and EJB containers.

9.1.1 WorkUnit Scenarios

9.1.1.1 Single WorkUnit

All applications in the Site are deployed in a single WorkUnit.

Advantage

Single WorkUnits are simple to configure. Consider single WorkUnit configuration if all resources are shared by the WorkUnit applications and this rarely changes.

Disadvantages

Changing the configuration to suit one application will also affect the other applications and reduce flexibility.

If one application fails causing the WorkUnit to stop, all other applications of the WorkUnit are also stopped.

9.1.1.2 Business Application

Several applications that together serve a business purpose or carry out a business process are deployed to one WorkUnit.

Other applications that serve other business purposes are deployed to separate WorkUnits.

Advantages

Each WorkUnit can be individually configured and maintained by the responsible Business Unit without impacting other applications.

If one application fails causing the WorkUnit to stop, other WorkUnits are not affected.

Disadvantage

More complex to configure.

9.1.2 WorkUnits in a Multi-server Environment

Interstage Application Server can be set up in one of two ways:

1. Standalone

   Interstage is installed on a Server as a Standalone Server installation. This Server is not a Site participant. This configuration is recommended for development, testing and simple scenarios.

2. Multi-server

   Interstage is installed on multiple servers to form a scalable Site. Servers in the Site can be configured as a:

   - Admin Server (one per Site)
   - Managed Servers in Independent or Reserved modes
   - Managed Servers as Server Group Members.

   For details of Site construction, refer to the "Site" chapter.

The operational differences between a Standalone and scalable multi-server environment result in differences in WorkUnit creation and management.

9.1.2.1 WorkUnits Created on Standalone Servers

WorkUnits created on a Standalone Server are confined to that Server, are non-scalable and any changes made are limited to that Server only.

9.1.2.2 WorkUnits Created on an Admin Server

WorkUnits created on the Admin Server are scalable across servers in a Site. Operations performed on the WorkUnit are automatically duplicated across all members of the Server Groups/Independent Managed Servers it is allocated to. This avoids the inefficiencies and inherent risks of manually duplicating and managing WorkUnit settings across servers.

WorkUnits created on the Admin Server and allocated to Independent Managed Servers can subsequently be changed to apply to one or more scalable Server Groups.

Management operations for WorkUnits created and managed on the Admin Server are processed in parallel on all servers to which it is allocated.

9.1.2.3 Operations on WorkUnits

For Managed Servers of all types, the WorkUnit configurations can be maintained from the Admin Server only. However, by directly accessing the IMC of the Managed Server, the Operator can start or stop the WorkUnit. Direct access to the Managed Server is only recommended in cases when access through the Admin Server is not available.

9.1.2.4 IJServer WorkUnits

In IJServer WorkUnits, the Web Connector, EJB Container or Servlet Container components can be allocated to separate Server Groups or Independent Managed Servers. IJServers, whose components are allocated in this manner, are referred to as multi-level IJServers. When an individual WorkUnit item is allocated to a Server Group, the deployed application is scalable to user demand. Such scalability is achievable by simply adding extra servers to this Server Group.

When a single WorkUnit is allocated to one or more Independent Managed Servers, it is not scalable.

It is recommended to always use Server Groups for deployment of any production grade WorkUnits.

9.1.2.5 CORBA WorkUnits

When CORBA WorkUnits with the same deployed applications are created and operated on several Standalone servers, to the outside world, they appear to be logically just one WorkUnit. However the individual WorkUnits have to be configured, started, and stopped independently of each other.

In a multi-server environment, the WorkUnit configuration on each Server is centrally managed and distributed to each Server, providing scalability. Central management of the WorkUnit also supports operations such as simultaneous start and stop.

For more information on CORBA WorkUnits, refer to the "Chapter 10 CORBA WorkUnits" chapter.

9.1.2.6 Update of WorkUnit Settings in a Multi-server Environment

When the settings of a WorkUnit or its applications are managed from the Admin Server, and WorkUnit definitions are updated, the Admin Server ensures that all Managed Servers to which the WorkUnit is deployed receive the updates and that any out of date WorkUnit Settings are updated.

9.1.2.7 Error Recovery in a Multi-server Environment

Any operations on a multi-server WorkUnit may result in operations on multiple Managed Servers. The results may differ for each Managed Server.

Due to the distributed nature of the operation, it might result in failures on a partial set of the applicable Managed Servers. In such cases, refer to the logs of the Managed Server(s) where the operation failed. Address the problem on each failed Managed Server, then, repeat the operation. The Admin Server ensures that the operations are repeated only on the Managed Servers where failure occurred.

Generally, 'repeat the operation' means clicking the same action button. Exceptions are errors that occur when performing a Create type operation. Whenever a create operation is failed, then, to continue the create operation, go to the Settings page for the created item, and without modifying the settings, click the **Update** button.

Whenever application deployment fails, that application cannot be redeployed until error recovery is performed. However, servers where deployment was completed normally can still be started.

9.1.3 Viewing WorkUnits in the Site

Application Management

Interstage > Interstage Application Server > WorkUnit	View WorkUnit Status

Standalone

Interstage > Interstage Application Server > System > WorkUnit	View WorkUnit Status

A list of all WorkUnits in the Site is displayed. The **WorkUnit Name** gives the name of the WorkUnit. The **Type** column indicates if the WorkUnit is CORBA or IJServer (the type of IJServer is also given). The **Status** column indicates if the WorkUnit is running, and for running WorkUnits, the **Start Time** is given. The **Deploy To** column (Application Management tab only) shows to which Site Participants the WorkUnit is deployed (multi-level IJServers are deployed over up to three Site Participants). The **Version** column (Application Management tab only) gives the Interstage version running on the machine from which the WorkUnit was created.

Click a WorkUnit Name in the list to access it for view or update.

Note

- 8.0(*) denotes a WorkUnit created from a later version but compatible to version 8.0.

9.1.4 Creating a WorkUnit

Application Management

Interstage > Interstage Application Server > WorkUnit	Create a new WorkUnit

Standalone

Interstage > Interstage Application Server > System > WorkUnit	Create a new WorkUnit

To create an IJServer, refer to "9.2.2 Creating an IJServer".

To create a CORBA WorkUnit, refer to "Creating a CORBA WorkUnit".

9.1.5 Starting and Stopping WorkUnits

WorkUnits can be started or stopped from the IMC. This may be required for maintenance or application update purposes. For a WorkUnit allocated to a Server Group, the WorkUnit can be stopped on one Server, then restarted. The WorkUnit continues operation on the other servers. This might be used for example, where there is a failure on one Server when starting/stopping a multi-server WorkUnit. The WorkUnit can be stopped on that Server, the problem addressed and rectified, and the WorkUnit restarted on the individual Server without affecting WorkUnit operation on the other servers.

9.1.5.1 Starting a WorkUnit

Application Management

Interstage > Interstage Application Server > WorkUnit	View WorkUnit Status

Standalone

Interstage > Interstage Application Server > System > WorkUnit	View WorkUnit Status

To start a WorkUnit:

1. Click the checkbox to the left of the **WorkUnit Name** to be started.

   Click the **Select All** button to select all WorkUnits in the list.

2. Click the **Start** button to start the WorkUnit.

   The **Status** field for the WorkUnit changes to 'Running' and the current date and time are added to the Start Time field.

Note

- Interstage must be running for a WorkUnit to be started.
- Services assigned to the Server Groups to which the WorkUnit is allocated must be started before the WorkUnit can be started.
- The WorkUnit must have at least one application deployed within it before it will start.
- If the WorkUnit is already running the start operation will be ignored.
- Multi-server WorkUnits can be started on the individual Managed Servers to which they are allocated.

9.1.5.2 Stopping a WorkUnit

Application Management

Interstage > Interstage Application Server > WorkUnit	View WorkUnit Status

Standalone

Interstage > Interstage Application Server > System > WorkUnit	View WorkUnit Status

To stop a WorkUnit:

1. Click the checkbox to the left of the **WorkUnit Name** to be stopped.

   Click the **Select All** button to select all WorkUnits in the list.

2. Click the **Stop** button to stop the WorkUnit.
3. On the WorkUnit Stop Selection page select:

   - **Normal Stop** to bring down the applications of this WorkUnit independently in an orderly fashion (e.g., after completing all ongoing transactions, etc.)
   - **Forced Stop** to bring down all applications of this WorkUnit abruptly (e. g. aborting the current transaction for all applications of the WorkUnit).

4. Click the **Stop** button to stop the WorkUnit.

   Click **Cancel** to return to the WorkUnit list without stopping the WorkUnit.

   The **Status** field for the WorkUnit changes to 'Stopped' when the WorkUnit stop operation is complete.

Note

- Multi-server WorkUnits can be stopped on the individual Managed Servers to which they are allocated.

9.1.5.3 Inhibiting and Permitting Queues

This is available for IJServer WorkUnits of type 'EJB only' and CORBA WorkUnits. Each queue can be inhibited from, or permitted to, temporarily reject requests from the client, or restart accepting requests. The queue inhibit/permit function is used to:

- Restrict the use of a job according to the time zone.
- Temporary reject requests because the load is too high.
- Suppress requests before stopping a job so that the job stops after processing is completely finished.

If the client issues a request while the queue is inhibited, an error is posted to the client.

9.1.5.3.1 Inhibit Queue of an EJB only type WorkUnit

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit Name]	Status

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit Name]	Status

To inhibit queue of a WorkUnit:

1. Click the **Inhibit Queue** button to close the client request queue of the WorkUnit.

   The **Status** field for the WorkUnit changes to 'Running(Queue Inhibited)' when the WorkUnit Inhibit Queue operation is completed.

   A message like "Succeeded in blocking message queue (IJServer name=[WU name])" will be displayed on the Status Frame of the IMC when the inhibit operation is completed successfully.

9.1.5.3.2 Permit Queue of an EJB only type WorkUnit

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit Name]	Status

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit Name]	Status

To permit messages of an inhibited queue of a WorkUnit:

1. Click the **Permit Queue** button to open the client request queue of the WorkUnit.

   The **Status** field for the WorkUnit changes to 'Running' when the WorkUnit Permit Queue operation is completed.

   A message like 'Released message queue block for IJServer (WorkUnit name)' will be displayed on the Status Frame of the IMC when the permit operation is completed successfully.

9.1.6 Updating a WorkUnit

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name]	Settings

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name]	Settings

To update a WorkUnit:

1. Click the **WorkUnit Settings [Show] link**:

   The settings that can be updated depend on the type of the WorkUnit.

   - To update CORBA WorkUnit settings, refer to the "CORBA WorkUnits" chapter.
   - To update settings of an IJServer WorkUnit with Web and EJB applications on the same VM, refer to "9.2.2.1 Creating an IJServer with Web and EJB Applications Running in the Same VM".
   - To update settings of an IJServer WorkUnit with Web and EJB application on different VMs, refer to "9.2.2.2 Creating an IJServer with Web and EJB Applications Running in Separate VMs".
   - To update settings of an IJServer WorkUnit with Web applications on the same VM, refer to "9.2.2.3 Creating an IJServer for Web Applications Only".
   - To update settings of an IJServer WorkUnit with EJB applications on the same VM, refer to "9.2.2.4 Creating an IJServer for EJB Applications Only".

2. Click the **Update** button to update the WorkUnit settings.
3. Click the **Refresh** button to return this form to the most recently saved values.

- A WorkUnit must be stopped before its settings can be updated.
- The WorkUnit's name and type cannot be updated.
- When the settings of a multi-server WorkUnit or its applications are updated from the Application Management tab, the modified information is compared internally against the most recent WorkUnit definitions and only updated on those Managed Servers where the definitions differ to the new settings.
- The WorkUnit's name and type, component allocation settings and the connection between WorkUnit components across multi-servers cannot be updated after WorkUnit creation.

9.1.7 Combining IJServers (Admin Server Only)

A 'Web Applications Only' IJServer can be combined with an 'EJB Applications Only' IJServer to to create a multi-level IJServer. This can only be done from the Admin Server.

Application Management

Interstage > Interstage Application Server > WorkUnit	Combine

To create a multi-level IJServer by combining two IJServers:

1. In **Servlet Container**, select a an IJServer from the Web Only IJServers listed.
2. In **EJB Container**, select an IJServer from the EJB Only IJServers listed.
3. Click the **Combine** button to create the multi-level IJServer.

- The same Interstage version must be running on both Site Participants to which the source IJServers are currently deployed .This includes V8 compatible IJServers (identified by 8.0 (*)).

9.2 IJServers

IJServer WorkUnits are capable of deploying all kinds of J2EE applications including servlet/JSP based web applications, web plus EJB based applications, non web J2EE (EJB, JMS, J2EE connector based) applications and J2EE based Web Services.

9.2.1 Viewing the Status of an IJServer

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name]	Status

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name]	Status

The IJServer Status is displayed. The **WorkUnit Name**, **WorkUnit Type**, **Status** and **Start Time** are given. Multi-server IJServers also show the aggregate Environment Setup Status of all servers to which the WorkUnit is allocated. Tables below detail possible values for this and the Status field.

For multi-server IJServers viewed from the Application Management tab the following additional information is given:

- A table summarizing the status of the WorkUnit Components (Web Server Connector/Servlet Container/EJB Container). This consists of the **Component**, **Server Group/Server**, **Status**, **Last Action Status** and **Start Time**. For details of possible status values, refer to "9.2.1.3 Component Allocation Status".
- If the IJServer has a Servlet Container, a table showing the container status on each Server allocated to the servlet container is shown. For details of possible status values, refer to "9.2.1.5 Servlet Container Status".
- If the IJServer has an EJB Container, a table showing the container status on each Server allocated to the EJB container is shown. For details of possible status values, refer to "9.2.1.6 EJB Container Status".
- If the IJServer has a Web Server Connector, the connector status can be seen from "9.2.1.4 Web Server Connector Status".
- If an error has occurred during an update operation (i.e., when modifying the detailed settings or deploying an application) at a Managed Server hosting the WorkUnit, it will be shown in the Last Action Errors table. The Server on which the error occurred, the operation that was being processed, and the error message generated are displayed.

When viewed on a Managed Server to which the WorkUnit is deployed, the display is the same as for a conventional WorkUnit and the detailed status information listed above will not be provided.

9.2.1.1 Status

The table below details the possible operating status values for Server Groups or Independent Managed Servers.

Table 9.1 IJServer Status for Site Participants

Value	Explanation	
	Server Group	Server
Running	WorkUnit is running on the Server or on all servers in Server Group	WorkUnit is running on the Server
Started (part stopped)	WorkUnit is running. Some WorkUnit instances on servers in the Server Group are stopped	
Stopped	WorkUnit is stopped on the Server or all servers in the Server Group	WorkUnit is stopped on the Server
Starting	WorkUnit start processing is in progress on the Server or all servers in the Server Group	WorkUnit start processing is in progress on the Server
Stopping	WorkUnit stop processing is in progress on the Server or all servers in the Server Group	WorkUnit stop processing is in progress on the Server

Value	Explanation	
	Server Group	Server
Started (EJB closed)	WorkUnit is running on the Server or all servers in the Server Group, but EJB applications are closed.	WorkUnit is running on the Server, but EJB applications are closed.
Started (EJB part closed)	Some WorkUnit instances are running in the Server Group, but EJB applications are closed.	
Error	An error occurred during an IJServer operation	

Standalone Servers can be in the following state:

- Running
- Stopped

9.2.1.2 Last Action Status

For a multi-server IJServer the Last Action Status is the aggregate status of the WorkUnit or component on all servers that it is allocated to. The Last Action Status of the IJServer can be:

- **Normal** where all WorkUnit operations were processed normally for all servers allocated to the WorkUnit or component.
- **Error** where an error occurred during a WorkUnit update operation (i.e., when updating environment settings or deploying an application), that failed for the WorkUnit or component as a whole.
- **Normal (Part)** where an error occurred at some servers during a WorkUnit update operation.

9.2.1.3 Component Allocation Status

The table below details the component allocation status information of a multi-server IJServer WorkUnit.

Table 9.2 Component Allocation Status

Field	Description
Component	Displays the IJServer component (Web Server connector, Servlet container, or EJB container). Displayed components depend on the IJServer type specified when the IJServer is created.
Server Group/ Server	Displays the Server or Server Group to which the component is allocated.
Status	The aggregate status of all servers that the component it is allocated to. Refer to "9.2.1.1 Status".
Last Action status	The aggregate status of update operations for all servers that the component is allocated to. Error information for individual servers is shown in the Environment Setup Error table.
Start Time	The time the component was started from the Admin Server.

9.2.1.4 Web Server Connector Status

The table below details the web connector status information.

Table 9.3 Web Connector Status

Field	Description
Server Group/ Server	Displays the Server (and Server Group to which it belongs, if applicable) that the component is allocated to.
Status	Displays the Server operating status. Refer to "9.2.1.1 Status".
Last Action status	The status of update operations on the Server. Valid values for an individual Server are **Normal** or **Error**. Refer to "9.2.1.2 Last Action Status".
Start Time	The time the component was started from the Admin Server.

9.2.1.5 Servlet Container Status

The table below details the servlet container status information.

Table 9.4 Servlet Container Status

Field	Description
Server Group/ Server	Displays the Server (and Server Group to which it belongs, if applicable) that the component is allocated to.
Status	Displays the Server operating status. Refer to "9.2.1.1 Status".
Last Action status	The status of update operations on the Server. Valid values for an individual Server are Normal or Error. Refer to "9.2.1.2 Last Action Status".
Start Time	The time the component was started from the Admin Server.

9.2.1.6 EJB Container Status

The table below details the EJB container status information.

Table 9.5 EJB Container Status

Field	Description
Server Group/ Server	Displays the Server (and Server Group to which it belongs, if applicable) that the component is allocated to.
Status	Displays the Server operating status. Refer to "9.2.1.1 Status".
Last Action status	The status of update operations on the Server. Valid values for an individual Server are **Normal** or **Error**. Refer to "9.2.1.2 Last Action Status".
Start Time	The time the component was started from the Admin Server.

9.2.2 Creating an IJServer

Four types of J2EE WorkUnit can be created. The settings that can be configured for each type vary and are detailed in the following sections:

- 9.2.2.1 Creating an IJServer with Web and EJB Applications Running in the Same VM
- 9.2.2.2 Creating an IJServer with Web and EJB Applications Running in Separate VMs
- 9.2.2.3 Creating an IJServer for Web Applications Only
- 9.2.2.4 Creating an IJServer for EJB Applications Only

Note

- For multi-level IJServers, the Interstage version must be the same on all Site Participants to which the IJServer components are allocated. Once a Site Participant has been selected for one component, selection lists for other components display only Site Participants of the same version.

9.2.2.1 Creating an IJServer with Web and EJB Applications Running in the Same VM

The following procedure describes how to create an IJServer where Web and EJB applications run in the same JVM. In a multi-server environment this means that the Servlet and EJB Containers must be allocated to the same Server Group. In this scenario, the Web and EJB applications still run in a single JVM, but on each Server in the group.

This configuration is recommended for use under normal operating conditions, or where memory or Server resources available to the WorkUnit may be limited. In this configuration the concurrency level of both the servlets and EJBs is the same.

Application Management

Interstage > Interstage Application Server > WorkUnit	Create a new WorkUnit

Standalone

Interstage > Interstage Application Server > System > WorkUnit	Create a new WorkUnit

To create an IJServer WorkUnit where Web and EJB applications run in the same JVM:

1. In **WorkUnit Name**, specify a unique name for the WorkUnit.
2. In **WorkUnit Type**, select **IJServer**.
3. In **IJServer Type** select **Web and EJB Applications run in same Java VM**.
4. In **Create V8.0 compatible version IJServer**, click **Enabled** to create the IJServer in V8.0 compatible version format.
5. If creating a multi-server WorkUnit from the Application Management tab of the Admin Server:
   - in **Deploy To - Web Server Connector**, select the Independent Managed Server / Server Group to be allocated to this component.
   - in **Deploy To - Servlet and EJB Containers**, select the Independent Managed Server / Server Group to be allocated to these components.
6. If creating a WorkUnit across multiple Site participants (different participants selected for the components in step 4 above), select the **Relation between servers** between the WorkUnit components as:
   - **Line type** for one-to-one HTTP communication between the Web Server Connector and Servlet Container components; and IIOP is used between Servlet and EJB Containers.
   - **Mesh type** for n-to-m http communication between the Web Server Connector and Servlet Container components; and IIOP is used between Servlet and EJB Containers.
   - **IPCOM** to use the IPCOM for load balancing.
7. Click the Detailed Settings **[Show]** link, then click the WorkUnit Settings **[Show]** link and specify the general settings for the WorkUnit.

   For details, refer to "9.2.2.5 Specifying WorkUnit Settings (Web and EJB Same VM, EJB or Web Only)".
8. Click the Common Application Settings **[Show]** link and specify the settings of this WorkUnit component.

   For details, refer to "9.2.2.7 Specifying Common Application Settings".
9. Click the Web Server Connector Settings **[Show]** link and specify the settings of this WorkUnit component.

   For details, refer to "9.2.2.8 Specifying Web Server Connector Settings".
10. Click the Servlet Container Settings **[Show]** link and specify the settings of this WorkUnit component.

    For details, refer to "9.2.2.9 Specifying Servlet Container Settings".
11. Click the EJB Container Settings **[Show]** link and specify the settings of this WorkUnit component.

    For details, refer to "9.2.2.10 Specifying EJB Container Settings".
12. Click the DB Connection Settings **[Show]** link and specify the settings for this WorkUnit.

    For details, refer to "9.2.2.11 Specifying DB Connection Settings".
13. Click the Session Recovery Settings **[Show]** link and specify the settings for this WorkUnit.

    For details, refer to "9.2.2.12 Specifying Session Recovery Settings".
14. Click the **Create** button to create the WorkUnit.

    Click the **Reset** button to return this form to the default values.

Note

- WorkUnit names must be unique among multi-server WorkUnits created on the Admin Server. The name cannot be the same as a Conventional WorkUnit name on any Managed Server to which the new WorkUnit is to be allocated.
- The WorkUnit name and type cannot be changed after creation.
- WorkUnits can be created only when Interstage is running or has been stopped normally. They cannot be created if Interstage has been forcefully shut down.

9.2.2.2 Creating an IJServer with Web and EJB Applications Running in Separate VMs

The following procedure describes how to create an IJServer where Web and EJB applications run in separate JVMs. In a multi-server environment this means that the Servlet and EJB Containers can be deployed to different Server Groups. Interprocess communications are handled by IIOP.

This configuration is recommended for use where flexible resource configuration is required. For example, the concurrency level of the servlets and EJBs can be specified as different values, depending on the relative weight of presentation to business logic. In this configuration Intranet systems can use IIOP for direct client-server invocation of business logic to reduce the communication and processing overhead of accessing the business logic via a servlet.

Application Management

Interstage > Interstage Application Server > WorkUnit	Create a new WorkUnit

Standalone

Interstage > Interstage Application Server > System > WorkUnit	Create a new WorkUnit

To create an IJServer WorkUnit where Web and EJB applications run in separate JVMs:

1. In **WorkUnit Name**, specify a name for the WorkUnit.
2. In **WorkUnit Type**, select **IJServer**.
3. In **IJServer Type** select **Web and EJB Applications run in separate Java VMs**.
4. In **Create V8.0 compatible version IJServer**, select **Enabled** to create the IJServer in V8.0 compatible version format.
5. If creating a multi-server WorkUnit from the Application Management tab of the Admin Server:
   - In **Deploy To - Web Server Connector**, select the Independent Managed Server / Server Group to be allocated to this component.
   - In **Deploy To - Servlet Container**, select the Independent Managed Server / Server Group to be allocated to this component.
   - In **Deploy To - EJB Container**, select the Independent Managed Server / Server Group to be allocated to this component.
6. If creating a WorkUnit across multiple Site participants (different participants selected for the components in step 4 above), select the **Relation between servers** between the WorkUnit components as:
   - **Line type** for one-to-one HTTP communication between the Web Server Connector and Servlet Container components; and IIOP is used between Servlet and EJB Containers.
   - **Mesh type** for n-to-m http communication between the Web Server Connector and Servlet Container components; and IIOP is used between Servlet and EJB Containers.
   - **IPCOM** to use the IPCOM for load balancing.
7. Click the Detailed Settings **[Show]** link, then click the WorkUnit Settings **[Show]** link and specify the general settings for the WorkUnit.

   For details, refer to "9.2.2.6 Specifying WorkUnit Settings (Web and EJB Separate VM)".

8. Click the Common Application Settings **[Show]** link and specify the settings of this WorkUnit component.

   For details, refer to "9.2.2.7 Specifying Common Application Settings".

9. Click the Web Server Connector Settings **[Show]** link and specify the settings of this WorkUnit component.

   For details, refer to "9.2.2.8 Specifying Web Server Connector Settings".

10. Click the Servlet Container Settings **[Show]** link and specify the settings of this WorkUnit component.

    For details, refer to "9.2.2.9 Specifying Servlet Container Settings".

11. Click the EJB Container Settings **[Show]** link and specify the settings of this WorkUnit component.

    For details, refer to "9.2.2.10 Specifying EJB Container Settings".

12. Click the DB Connection Settings **[Show]** link and specify the settings for this WorkUnit.

    For details, refer to "9.2.2.11 Specifying DB Connection Settings".

13. Click the Session Recovery Settings **[Show]** link and specify the settings for this WorkUnit.

    For details, refer to "9.2.2.12 Specifying Session Recovery Settings".

14. Click the **Create** button to create the WorkUnit.

    Click the Reset button to return this form to the default values.

- WorkUnit names must be unique among multi-server WorkUnits created on the Admin Server. The name must also not already be in use by a Conventional WorkUnit on any Managed Server to which the new WorkUnit is to be allocated.
- The WorkUnit name and type cannot be changed after creation.
- WorkUnits can be created only when Interstage is running or has been stopped normally. They cannot be created if Interstage has been forcefully shut down.

9.2.2.3 Creating an IJServer for Web Applications Only

The following procedure describes how to create an IJServer for web applications with no EJB component. Servlets/JSPs can be used to implement basic business logic.

Application Management

Interstage > Interstage Application Server > WorkUnit	Create a new WorkUnit

Standalone

Interstage > Interstage Application Server > System > WorkUnit	Create a new WorkUnit

To create an IJServer WorkUnit suitable for Web Applications only:

1. In **WorkUnit Name**, specify a name for the WorkUnit
2. In **WorkUnit Type**, select **IJServer**.
3. In **IJServer Type** select **Web Applications Only**.
4. In **Create V8.0 compatible version IJServer**, select **Enabled** to create the IJServer in V8.0 compatible version format.
5. If creating a multi-server WorkUnit from the Application Management tab of the Admin Server:
   - in **Deploy To - Web Server Connector**, select the Independent Managed Server / Server Group to be allocated to this component.
   - in **Deploy To - Servlet Container**, select the Independent Managed Server / Server Group to be allocated to this component.

6. If creating a WorkUnit across multiple Site participants (different participants selected for the components in step 4 above), select the **Relation between servers** between the WorkUnit components as:

   - **Line type** for one-to-one HTTP communication between the Web Server Connector and Servlet Container components.
   - **Mesh type** for n-to-m http communication between the Web Server Connector and Servlet Container components.
   - **IPCOM** to use the IPCOM for load balancing.

7. Click the Detailed Settings **[Show]** link, then click the WorkUnit Settings **[Show]** link and specify the general settings for the WorkUnit.

   For details, refer to "9.2.2.5 Specifying WorkUnit Settings (Web and EJB Same VM, EJB or Web Only)".

8. Click the Common Application Settings **[Show]** link and specify the settings of this WorkUnit component.

   For details, refer to "9.2.2.7 Specifying Common Application Settings".

9. Click the Web Server Connector Settings **[Show]** link and specify the settings of this WorkUnit component.

   For details, refer to "9.2.2.8 Specifying Web Server Connector Settings".

10. Click the Servlet Container Settings **[Show]** link and specify the settings of this WorkUnit component.

    For details, refer to "9.2.2.9 Specifying Servlet Container Settings".

11. Click the DB Connection Settings **[Show]** link and specify the settings for this WorkUnit.

    For details, refer to "9.2.2.11 Specifying DB Connection Settings".

12. Click the Session Recovery Settings **[Show]** link and specify the settings for this WorkUnit.

    For details, refer to "9.2.2.12 Specifying Session Recovery Settings".

13. Click the **Create** button to create the WorkUnit.

    Click the **Reset** button to return this form to the default values.

- WorkUnit names must be unique among multi-server WorkUnits created on the Admin Server. The name must also not already be in use by a Conventional WorkUnit on any Managed Server to which the new WorkUnit is to be allocated.
- The WorkUnit name and type cannot be changed after creation.
- WorkUnits can be created only when Interstage is running or has been stopped normally. They cannot be created if Interstage has been forcefully shut down.

9.2.2.4 Creating an IJServer for EJB Applications Only

The following procedure describes how to create an IJServer with no Web Server Connector or Servlet Container components. EJBs can be used to provide direct client-server invocation of business logic by way of RMI-IIOP communications.

Application Management

Interstage > Interstage Application Server > WorkUnit	Create a new WorkUnit

Standalone

Interstage > Interstage Application Server > System > WorkUnit	Create a new WorkUnit

To create an IJServer WorkUnit where for EJB applications only:

1. In **WorkUnit Name**, specify a unique name for the WorkUnit.
2. In **WorkUnit Type**, select **IJServer**.
3. In **IJServer Type** select **EJB Applications Only**.

4. In **Create V8.0 compatible version IJServer**, select **Enabled** to create the IJServer in V8.0 compatible version format.
5. If creating a multi-server WorkUnit from the Application Management tab of the Admin Server:
   - In **Deploy To - EJB Container**, select the Independent Managed Server / Server Group to be allocated to this component.
6. Click the Detailed Settings **[Show]** link, then click the WorkUnit Settings **[Show]** link and specify the general settings for the WorkUnit.

   For details, refer to "9.2.2.5 Specifying WorkUnit Settings (Web and EJB Same VM, EJB or Web Only)".
7. Click the Common Application Settings **[Show]** link and specify the settings of this WorkUnit component.

   For details, refer to "9.2.2.7 Specifying Common Application Settings".
8. Click the EJB Container Settings **[Show]** link and specify the settings of this WorkUnit component.

   For details, refer to "9.2.2.10 Specifying EJB Container Settings".
9. Click the DB Connection Settings **[Show]** link and specify the settings for this WorkUnit.

   For details, refer to "9.2.2.11 Specifying DB Connection Settings".
10. Click the **Create** button to create the WorkUnit.

    Click the **Reset** button to return this form to the default values.

- WorkUnit names must be unique among multi-server WorkUnits created on the Admin Server. The name must also not already be in use by a Conventional WorkUnit on any Managed Server to which the new WorkUnit is to be allocated.
- The WorkUnit name and type cannot be changed after creation.
- WorkUnits can be created only when Interstage is running or has been stopped normally. They cannot be created if Interstage has been forcefully shut down.

9.2.2.5 Specifying WorkUnit Settings (Web and EJB Same VM, EJB or Web Only)

The settings below apply to IJServers of types Web and EJB on the Same VM, Web Only and EJB Only.

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name]	Settings

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name]	Settings

To specify WorkUnit Settings:

1. Specify the WorkUnit **Process Concurrency** up to a maximum value of 255. Concurrency refers to the number of instances of applications within a WorkUnit that could be spawned simultaneously.
2. Specify the **Classpath** for applications deployed in the WorkUnit. In **Application Library Path**, specify the path for using an application library. The application library is executed using the same class loader as the application. In **Path**, specify the paths for external programs called by these applications. And in **Environment Variables**, specify any environment variables used by applications in the following format: 'env_var=value'.

   PATH cannot be used as an environment variable name.

   For all fields, place each path/variable on a new line.
3. Select the **Java SDK Version** for the applications deployed to this WorkUnit.
4. In **Java VM Options**, specify any Java VM options required by the applications deployed in this WorkUnit. Multiple options should be enclosed in double-quotes.

5. In **Control for insufficient Java heap/Java Permanent area**, specify the control for insufficient Java heap/Java Permanent area. The two options are:
   - Returns java.lang.OutOfMemoryError to the application
   - Restarts the process
6. Select **Auto Start** to have the WorkUnit started when Interstage is started.
7. In **Maximum application processing time**, specify the timeout in seconds for a business transaction involving applications of this WorkUnit (specify 0 for unlimited processing time). In **Forcefully end application on timeout?**, select the action to take when any application exceeds the specified maximum time:
   - **Displays alert message** to have a message posted.
   - **Forcefully stop all the running processes** to stop all other applications in the WorkUnit.
8. Specify the **WorkUnit maximum startup time** in seconds. If the WorkUnit startup time exceeds this value, active processes will be shutdown and startup aborted.
9. Specify the **Process maximum stop time** in seconds. If normal process stop is not completed within specified time, the process will be forcefully shut down.
10. In **Retry Count**, specify the number of times to retry WorkUnit startup after abnormal termination.

    In **Retry Count Reset Interval**, specify the time in seconds after which the retry count will be reset. Whenever WorkUnits failed to start properly, it will be retried. For each retry, the counter is getting decremented. After the reset interval, the counter will be reset to its original value.
11. Select the **WorkUnit Start Mode** as:
    - **Normal mode**
    - **Debug Mode**
12. In **Working Directory** for the java VM process select:
    - **Default directory** - the directory defaults to (Interstage displays the default directory).
    - **User defined** - specify a user path as working directory, if the default directory is not appropriate.

      Check the **Make this a unique current directory in IJServer** checkbox have all processes share the specified working directory.
13. In **Number of generations of the current directory to avoid**, select a number that corresponds to the number of generations of current directories to be saved. Interstage normally creates separate working directories for each WorkUnit process. This parameter specifies the number of instances of these working directories that will be saved and recycled.
14. In **Log File Directory** select:
    - **Default directory**.
    - **User defined** and specify a user defined path.
15. If the IJServer type is 'EJB Only', in **Maximum Size of Queue**, specify the maximum number of messages the client request queue can contain. An alarm notification is sent to the status frame of the IMC, when the number of messages in the queue reaches the value specified in **Queue alarm level**. The alarm is reset when the number of messages drops back below the value in **Queue alarm reset level**.

    Specify a maximum queue size of 0 to allow an unlimited queue size.
16. If the IJServer is 'EJB Only', in **Communication Buffer Count**, specify the communication buffer count used in the WorkUnit.
17. If the IJServer is 'EJB Only', in **Communication Buffer Length**, specify the communication buffer length used in the WorkUnit.
18. In **Stop the WorkUnit if the application failed to restart automatically?** select:
    - **Stop WorkUnit** to stop the WorkUnit and all deployed applications if any application fails to restart.
    - **Continue to operate WorkUnit** to keep the rest of the WorkUnit's applications running when any application fails to restart.

Note

- If '**Make this a unique current directory in IJServer**' option is not selected, Interstage creates a sub directory for each process started. The directory name is the Process ID.

9.2.2.6 Specifying WorkUnit Settings (Web and EJB Separate VM)

The settings below apply to IJServers of type 'Web and EJB on the Separate VMs'. Settings are divided into settings Common to all components, Servlet Container Settings and EJB Container Settings.

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name]	Settings

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name]	Settings

9.2.2.6.1 Specifying WorkUnit Settings

To specify WorkUnit Settings common to all components:

1. Select **Auto Start** to have the WorkUnit start automatically when Interstage is started.
2. Specify the **WorkUnit maximum startup time** in seconds. If the WorkUnit startup time exceeds this value, active processes will be shutdown and startup aborted.
3. Specify the **Process maximum stop time** in seconds. If normal process stop is not completed within specified time, the process will be forcefully shut down.
4. In **Retry Count**, specify the number of times to retry WorkUnit startup after abnormal termination.
5. Select the **WorkUnit Start Mode** as:
   - **Normal mode**
   - **Debug Mode** to get debug / trace information while the WorkUnit is running
6. In **Working Directory** for the java VM process select:
   - **Default directory** - the directory defaults to a sub directory of the Interstage home directory (Interstage displays the default directory)
   - **User defined** - specify a user path as working directory, if the default directory is not appropriate.

     Check the **Make this a unique current directory in IJServer** checkbox have all processes share the specified working directory.
7. In **Number of generations of the current directory to avoid**, click the number required.
8. In **Log File Directory** select:
   - **Default directory**.
   - **User defined** and specify a user defined path.

   If the Servlet container and EJB container are allocated to different Site participants, select a log file directory for each.
9. In S**top the WorkUnit if the application failed to restart automatically?**, select:
   - **Stop WorkUnit** to stop the WorkUnit and all deployed applications if an application fails to restart.
   - **Continue to operate WorkUnit** to keep the rest of the WorkUnit's applications running when an application fails to restart.

Note

- If '**Make this a unique current directory in IJServer**' option is not selected, Interstage creates a sub directory for each process started. The directory name is the Process ID.

9.2.2.6.2 Specifying Servlet Container VM settings

To specify Servlet Container settings:

1. Specify the WorkUnit **Process Concurrency** up to a maximum value of 255. Concurrency refers to the number of instances of servlet based web applications within a WorkUnit that could be spawned simultaneously.
2. Specify the **Classpath** for applications deployed in the WorkUnit. In **Application Library Path**, specify the path for using an application library. The application library is executed using the same class loader as for the application. In **Path**, specify the paths for external programs called by these applications. And in **Environment Variables**, specify any environment variables used by applications in the following format: 'env_var=value'.

   PATH cannot be used as an environment variable name.

   For all fields, place each path/variable on a new line.
3. In **Retry Count Reset Interval**, specify the time in seconds before retrying WorkUnit startup after abnormal termination.
4. Select the **Java SDK Version** for the applications deployed to this WorkUnit.
5. In **Java VM Options**, specify any Java VM options required by the applications deployed in this WorkUnit. Multiple options should be enclosed in double-quotes.
6. In **Control for insufficient Java heap/Java Permanent area**, specify the control for insufficient Java heap/Java Permanent area. The two options are:
   - Returns java.lang.OutOfMemoryError to the application
   - Restarts the process
7. In **Maximum application processing time**, specify the timeout in seconds for a business transaction involving applications of this WorkUnit (specify 0 for unlimited processing time). In **Forcefully end application on timeout?**, select the action to take when any application exceeds the specified maximum time:
   - **Display alert message** to have a message posted to status frame of IMC whenever Maximum application processing time is exceeded
   - **Forcefully stop all running processes** to abruptly stop all the remaining applications of the WorkUnit. This option is recommended if running of the remaining applications of a WorkUnit do not serve any real purpose (e.g., a business transaction may need all the applications of a WorkUnit)

9.2.2.6.3 Specifying EJB Container VM settings

To specify the EJB Container VM settings:

1. Specify the WorkUnit **Process Concurrency** up to a maximum value of 255. Concurrency refers to the number of instances of EJB applications within a WorkUnit that could be spawned simultaneously.
2. Specify the **Classpath** for applications deployed in the WorkUnit. In **Application Library Path**, specify the path for using an application library. The application library is executed using the same class loader as for the application. In **Path**, specify the paths for external programs called by these applications. And in **Environment Variables**, specify any environment variables used by applications in the following format: 'env_var=value'.

   PATH cannot be used as an environment variable name.

   For all fields, place each path/variable on a new line.
3. In **Retry Count Reset Interval**, specify the time in seconds before retrying WorkUnit startup after abnormal termination.
4. Select the **Java SDK Version** for the applications deployed to this WorkUnit.

5. In **Java VM Options**, specify any Java VM options required by the applications deployed in this WorkUnit. Multiple options should be enclosed in double-quotes.
6. In **Control for insufficient Java heap/Java Permanent area**, specify the control for insufficient Java heap/Java Permanent area. The two options are:
   - Returns java.lang.OutOfMemoryError to the application
   - Restarts the process
7. In **Maximum application processing time**, specify the timeout in seconds for a business transaction involving applications of this WorkUnit (specify 0 for unlimited processing time). In **Forcefully end application on timeout?**, select the action to take when any application exceeds the specified maximum time:
   - **Display alert message** to have a message posted to the status frame of IMC.
   - **Forcefully stop all running processes** to stop all remaining applications abruptly.
8. In **Maximum Size of Queue**, specify the maximum number of messages the queue can contain. An alarm notification is sent when the number of messages in the queue reaches the value specified in **Queue alarm level**, and the alarm is reset when the number of messages drops back below the value in **Queue alarm reset level**.

   Specify a maximum queue size of 0 to allow an unlimited queue size.
9. In **Communication Buffer Count**, specify the communication buffer count used in the WorkUnit.
10. In **Communication Buffer Length**, specify the communication buffer length used in the WorkUnit.

9.2.2.7 Specifying Common Application Settings

Create a new WorkUnit	Detailed Settings	Common Application Settings

To specify WorkUnit Common Application Settings, click the Common Application Settings **[Show]** link:

1. In **Use HotDeploy**, select **Enabled** to enable allow deploy / re-deploy of WorkUnit applications without stopping and re-starting the Interstage Application Server.
2. In **Type of XML parser to use**, select **Xerces2**, or **Fujitsu XML Processor** to use one of these built-in parsers, or select **User defined parser path** and specify the install directory of the required third party XML processor. Crimson is not available for IJServers of type Web and EJB running in the same VM.
3. In **Container Web Service**, specify whether to disable the container Web Service.
4. In **Class Loaders**, select the class loader configuration as:
   - **One for each EAR** to load each EAR through a different class loader.
   - **One for each application** to load each JAR and WAR through their own class loader.
   - **Use a single class loader** to load all JARs, WARs and EARs using the same class loader.
5. In **Search order of class loaders**, select the class loader search order as:
   - **Parent is Last** to have the child level class loaders searched first, then the parent class loader.
   - **Parent is First** to have the parent class loader searched first, then the children level class loaders.
6. In **Auto Reload s**pecify whether to reload if the application class file is modified, and specify the reload time.
7. In **Transaction Type Analysis**, specify whether to use the transaction type analysis. This item is only applicable to Standalone servers and not applicable to IJServers of type EJB Only.
8. Solaris32/64 Linux32/64

   In **Application File Protection Level**, specify the application file protection level.

9.2.2.8 Specifying Web Server Connector Settings

Create a new WorkUnit	Detailed Settings	Web Server Connector Settings

To specify the Web Server Connector Settings, click the Web Server Connector Settings **[Show]** link:

1. If the Web Server is running on a separate host, specify the **IP address of the Web server to receive requests** (applicable to standalone servers only).
2. On a Server Group or Independent Managed Server, in **Web Server/Web server Virtual Host**, select the Web Server and/or Virtual hosts that accept requests for applications deployed on this IJServer.
3. In **Send/Receive Timeout**, specify the maximum wait time after the connector sends/receives a data packet to/from the Servlet container.
4. In **Maximum number of Servlet container connections**, specify the maximum number of Servlet container connections allowed.
5. If the Servlet Container and Web Server are on the separate machines, it is recommended to select **Yes** to **Use SSL between Servlet Container and Connector?** and in **SSL configuration to be used for the Servlet Container and Connector**, select an SSL configuration used by the Web Server connector and by the Servlet Container. In Admin servers, a different SSL configuration can be used for each.

   SSL Configurations are set up under the Security node.
6. In **KeepAlive between the connector and the Servlet container**, specify this if KeepAlive is not used for communication between the connector and the Servlet container.

9.2.2.9 Specifying Servlet Container Settings

Create a new WorkUnit	Detailed Settings	Servlet Container Settings

To specify the Servlet Container Settings, click the Servlet Container Settings **[Show]** link:

1. On a standalone server, if the Servlet Container and Web Server are on two different machines, specify the **Servlet Container IP address**. This is applicable to the standalone server only.
2. Specify the **Timeout** for client requests in seconds.
3. Specify the **Port Number** that the Servlet container uses for connection with the web server. If multiple port numbers are used, delimit port numbers with a semicolon (;).

   For a multi-server WorkUnit where the Servlet Container is allocated to a Server Group, use a **Port Number** that is free on all servers in the group.
4. In **Number of connections**, specify the maximum number of requests that can connect to the Servlet container.
5. In **Simultaneous processes**, specify the minimum and maximum number of simultaneous processes that can be handled by the Servlet container. In **Minimum**, specify the minimum number of Servlet container processing threads. If there are insufficient processing threads, the maximum number is used. In **Maximum**, specify the maximum number of Servlet container processing threads. In **Maximum during standby**, specify the maximum number of processing threads that are retained after processing is complete or during standby. Monitoring occurs at one minute intervals. Processing threads that exceed this value are destroyed.

   In a multi-server environment, if the connection mode (**Relation between servers** field) is set to **Mesh** between WorkUnit components spread across multiple Site participants, set this value as:

Operating system	Setup formulae
Windows32/64 Solaris32/64 Linux32/64	'Maximum number of simultaneous client connections' for Web server connector x number of Web servers - 'Maximum number of simultaneous connections' is set in the Web Server Detailed Settings, found under the Services > Web Server tree node. For details, refer to the "Chapter 8 Services" chapter.

Operating system	Setup formulae
	In multi-server WorkUnits, the number of Web servers is the number of servers in the group the Web server component is allocated to.
Solaris32/64 Linux32/64	Web Server's 'Maximum number of simultaneous client connections' x number of Web servers. - 'Maximum number of simultaneous client connections' is set in the Web Server Detailed Settings under the Services > Web Server tree node. For details, refer to the "Chapter 8 Services" chapter.

If the connection mode is set to 'line type' between WorkUnit components spread across multiple Site participants, or the Web Server connector and Servlet container are deployed to the same Site participant, or this is a conventional WorkUnit, then the value specified here is also used for the Web Server Connector.

6. In **Show file list**, select **On** if a directory listing should be displayed when a URL maps to a directory that does not contain an index HTML file.
7. In **Run servlet even if mapping is not present?**, select **On** to run the servlet even when URL mapping is not present.
8. In **Use custom tag pooling**, select **Enabled** to use custom tag pooling in JSP pages.
9. In **Request URI encoding**, specify the encoding used for request URI parsing.
10. In **Use request body processing encoding for query parameters**, select **Enabled** to use the encoding used for request body processing for query parameters.
11. In **Encoding for dispatch to static resources**, specify the encoding used for static resource processing when dispatching static resources from JSP and Servlet.
12. In **JSP reload**, specify the mechanism for enabling/disabling JSP reload - whenever there is a request or at fixed intervals.
13. In **Control Port**, for **Port Number**, specify the port for receiving Servlet container control information, and for **Access permission IP address**, specify the access permission IP address (Session Registry Server IP address). Connections are only received from the specified IP address.

- The **Relation between servers** is set during WorkUnit creation.

9.2.2.10 Specifying EJB Container Settings

Create a new WorkUnit	Detailed Settings	EJB Container Settings

To specify the EJB Container Settings select the EJB Container settings **[Show]** link (for IJServers of type Web and EJB running in the same VM, only item 3 below is applicable). These settings are not available to IJServers of type Web Only.

1. In **Use SSL for IIOP?**, select **Yes** to use SSL when an EJB application is called using IIOP.
2. In **IIOP CallSimultaneous processes**, specify the minimum and maximum number of simultaneous processes allowed for handling of client connections by the EJB container. If more simultaneous client connections are received, the excess requests will be queued.
3. In **Simultaneous Message-driven Bean processes**, specify the maximum and minimum values for the number of processes that can be processed simultaneously in a message-driven bean on the process for running EJB (Thread Count), and the timeout until pooled threads are released without being used.
4. In **Use Distributed Transactions for EJB applications?**, select Yes to enable Global Transactions for EJB applications.
5. In **Use IPCOM load balancing?**, select whether to use IPCOM load balancing. When **Enabled**, specify the **Virtual Host Name** and **Representative Port** number. This item is not applicable to IJServers of type Web and EJB running on separate VMs.
6. In **Monitor operating status of the WorkUnit by IPCOM**, select **Enabled** to monitor the operating status of the WorkUnit by IPCOM. This item is not applicable to Admin server IJServers of type Web and EJB running on separate VMs.

9.2.2.11 Specifying DB Connection Settings

Create a new WorkUnit	Detailed Settings	DB Connection Settings

To specify the DB Connection Settings, click the DB Connection settings **[Show]** link:

1. Select the data sources to be used by this WorkUnit by selecting the checkbox corresponding to the **Data Source Name**, and specify the following for each data source selected.
2. **Transaction Isolation Level**, indicates how sensitive this application is to changes other users' transactions make, and consequently, how long the transaction must hold locks to protect against these changes. Refer to the DB product documentation to find out more about these options. Select one of the following options:
   - **default**
   - **Transaction-read-committed**
   - **Transaction-read-uncommitted**
   - **Transaction-repeatable-read**
   - **Transaction-serializable**
3. In **Pre-existing Connections**, specify the initial number of connections in the connection pool, and in **Maximum Connections**, specify the maximum number of connections in the pool.
4. In **Connection Timeout (s)**, specify the duration a J2EE application waits for a connection to be returned to the empty connection pool, before an error occurs.
5. In **Idle Timeout (sec)**, specify the maximum idle time for pooled connections held by an application before the connection is returned to the pool.
6. In **Connection Monitoring Time (Minutes)**, specify the duration for which usage of an open connection is monitored before a warning message is output to either the container log or the system log. This connection monitoring time starts when the connection is acquired.
7. In **Statement Cache Size**, specify the area of the data source to reserve for caching statements executed by applications.
8. In **Statement Automatic Close**, select **Close** to have the JDBC driver automatically close statements when the statement cache function is used.
9. In **Communication Wait Time (Seconds)**, specify the execution time limit for the following SQL statements. A warning message is output to the container or system log if execution exceeds the specified time.
   - java.sql.Statement

     execute(String)

     execute(String, int)

     execute(String, int[])

     execute(String, String[])

     executeBatch()

     executeQuery(String)

     executeUpdate(String)

     executeUpdate(String, int)

     executeUpdate(String, int[])

     executeUpdate(String, String[])
   - java.sql.PreparedStatement

     execute()

     executeQuery()

executeUpdate()

10. In **Reconnect on Failure?**, select **Enable** to reconnection to the database following failure, and in **Interval(s)**, specify the time in seconds before a reconnection attempt is mad. In **Retry Count**, specify the number of reconnection attempts that should be made.

9.2.2.12 Specifying Session Recovery Settings

Create a new WorkUnit	Detailed Settings	Session Recovery Settings

To specify the Session Recovery Settings, click the Session Recovery settings **[Show]** link:

1. In **Session Recovery**, specify whether to use Session Registry Server in IJServer.
2. In **Session backup destination Session Registry Server address:Port**, specify the session backup destination Session Registry Server. If Session Recovery is used, this option cannot be omitted.
3. In **Backup Mode**, specify the session backup mode.
4. In **Response waiting time from the Repository server**, specify the response waiting time from the Repository server.
5. In **End of the non-session URL**, specify the non-session contents. Specify the extension at the end of the URL.
6. In **Outputs the access log**, specify whether to output the access log.

9.2.3 Monitoring an IJServer

Site Management

Interstage > Interstage Application Server > [server group > member server] | [independent managed server] > System > WorkUnit > [WorkUnit name]	Monitoring

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name]	Monitoring

Performance monitoring information is displayed for the WorkUnit. The information available is context dependent.

Information provided is detailed below.

- Monitoring information is only available for individual servers. Overall monitoring of multi-server WorkUnits is not possible.
- The screen will be periodically refreshed based on the interval set in the IMC Console Preferences. For details refer to "Configuring the Display" in the "Chapter 2 Configuring the Interstage Management Console" chapter.

  Click the **Refresh** button to update the display.

Table 9.6 General Monitoring Information Provided for all IJServers

Field	Description
Process Serial Number	Serial number of the process
Process ID	Process ID of the running application.
Container Type	Servlet or EJB
Java VM Running Time	How long the VM is running? In HH MM SSS
Java VM Heap Size (Kbytes)	Heap (memory) size. Present, Lowest, Highest and Maximum are given.
Java VM Perm Size (Kbytes)	Present, Lowest, Highest and Maximum are given.
Garbage Collection	Count, Total Running Time, Average GC interval are given.

Field	Description
Port Number	Port number on which the WorkUnit is listening
Debugging Port Number	Port number used for debugging.

Monitoring Information Provided on Data Sources for IJServers

A wide variety of Data Source (DB Connection) related information like the number of connections in use, the status of the connections, etc., is provided.

Monitoring Information Provided on Transactions for IJServers

A wide variety of JTS and OTS (transactions) related information like Total number of application transactions executed, Number of Concurrent Transactions, min, max and average transaction times, number of concurrent transactions performed are provided.

Monitoring Information Provided on Message Queues for IJServers

When message JMS queues are used, message queue related information are provided for monitoring.

9.2.4 Logging IJServer Activity

9.2.4.1 Configuring IJServer Log Files

Site Management

Interstage > Interstage Application Server > [server group > member server] | [independent managed server] > System > WorkUnit > [WorkUnit name]	Log Settings

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit Name]	Log Settings

To define an IJServer's log file settings:

1. In **Rotate log file based on**, select:
   - **Log size**, and specify the maximum log file size in MBytes. When this is reached a new log file will be created.
   - **Backup start time**, and specify the hour on which backup should start, and in **Backup every**, specify the number of hours after which a new log file should be created.
2. Specify the **Number of log files to maintain**.
3. Click the **Update** button.

New log file will be created based on the rotation settings in step 1 until the specified Number of log files to maintain is reached. Log files will then be overwritten starting from the oldest file.

Note

- It is not possible to specify log settings individually for Managed Servers to which a WorkUnit is deployed.
- The WorkUnit must be stopped before log settings can be updated.

9.2.4.2 Viewing IJServer Log Files

Site Management

Interstage > Interstage Application Server > [server group > member server] | [independent managed server] > System > WorkUnit > [WorkUnit name]	View Log

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit Name]	View Log

Click and open the Container Log tab.

To view log files for an IJServer WorkUnit:

1. In **Select log file to view**, click the process serial number of the required log.
2. Click:
   - the Container Log tab to view the container log.
   - the Startup Info tab to view the Startup information.
3. On the **Container Log or Startup Info** tab, click:
   - the **First Line** button to go to the first line of the log.
   - the **Previous** button to view the previous page of the log.
   - the **Next** button to view the next page of the log.
   - the **Last Line** button to view the last line of the log..
   - the **Download** button to download the log file to the local machine.
   - The **Refresh** button to refresh the page.

Note

- IJServer log files are only available for individual servers. Overall logging of multi-server WorkUnits is not possible.

9.2.5 Managing J2EE Applications

Applications that conform to J2EE standards are supported by Interstage Application Server. These applications typically use Java Enterprise Edition features like Servlets, JSP, EJB, JMS, Java Connector, etc.

J2EE Applications are deployed through one of the following four file archives:

- A web archive (.WAR) file that contains a single web application
- A Java archive (.JAR) file that contains one or more EJBs
- A resource archive (.RAR) file that contains a single Resource Adapter (Connector).
- An enterprise archive (.EAR) file that contains at least one of the above archives. Can be any number or combination of the above.

Applications can be deployed simply by specifying a deployment file and the WorkUnit restart option. Alternately, application and connector settings can be specified.

9.2.5.1 Viewing Deployed J2EE Applications

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name]	Application Status

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit Name]	Application Status

The WorkUnit Name is displayed along with its WorkUnit Type, Use HotDeploy mode and Class Loaders setting. Select:

- **Module List** to display top level archive files deployed to this WorkUnit.

  For details on items displayed, refer to "9.2.5.1.1 Module List" below.

- **Application List** to display all deployed J2EE applications and connectors deployed to this WorkUnit.

  For details on items displayed, refer to "9.2.5.1.2 Application List" below.

Click a Module Name to view the module's content and their status', configure its environment settings and define its name in the Java Naming and Directory Service.

9.2.5.1.1 Module List

For each deployed module, the Module Name, Type, Status and the Deployment Status are given. The type can be any of:

- EAR: J2EE module
- WAR: Web module
- ejb-jar: EJB module
- RAR: RAR module

The following table details the possible Status values.

Table 9.7 Possible Status Values for Deployed Archive Files

Status	Explanation
Running	The deployed module can receive requests.
Starting	Deployed module classes and definition files are being loaded and modules are starting to begin receiving requests.
Stopped	The deployed module cannot receive requests.
Stopping	The deployed module status is initialized, receipt of requests has stopped, and the module is being stopped. Stopping corrupts Servlet sessions and STATEFUL Session Bean instances, and these must be created again after the module is started. Application monitor information is cleared during stop.
Abnormal	Some IJServer processes were restarted during deployment, undeployment, or restart. This caused an error in the deployed module. Normal processing cannot be executed.
Running (partially)	The deployed module can receive requests. But the status of some processes run by the module is 'Stopped'.
Running (inconsistently)	The deployed module can receive requests, but the state of that module started in each process is inconsistent (some of the IJServer processes that were deployed have restarted, and so the module was loaded before some processes were redeployed). This status also occurs in a mixed Running (partially) and Running (inconsistently) status.

The following table details the possible Deployment Status values. This is visible only from the Admin Server.

Table 9.8 Possible Deployment Status Values for Deployed Archive Files (Admin Server Only)

Deployment Status	Explanation
Normal	The Deployment Status of all Managed Servers is "Normal".
Partial Error	The Deployment Status of some Managed Servers in a Server Group, or some of the Site Participants to which a multi-tiered IJServer is deployed is "Error".
Error	The Deployment Status of all Managed Servers in the Server Group is "Error" because deployment to one or more servers failed. Fix the problem on the server(s) with the error, and try to deploy again.

9.2.5.1.2 Application List

Items are grouped as follows:

- Web Applications lists deployed web modules
- EJB Applications lists deployed EJB modules

  The Bean Type column gives the EJB application type. This can be one of:

  - STATEFUL Session Bean
  - STATELESS Session Bean
  - CMP1.x Entity Bean
  - CMP2.x Entity Bean
  - BMP Entity Bean
  - Message-driven Bean
- Connectors/Resource Adapter lists deployed definition names or resource adapter names.

Click on an Application Name to view monitoring information for the application, and access the deployment descriptor file for edit. For details, refer to "9.2.5.7 Monitoring an Application" and "9.2.5.10 Updating the Deployment Descriptor File for a Deployed EJB Application".

Click on a Connector Definition Name to view the environment settings for the Resource Adapter.

Note

- Archive files deployed to this WorkUnit are accessible as nodes under the node for this WorkUnit. If the archive file contains other archives (for example, an .ear file may contain a .war and two .jar files), each of these are accessible as sub-nodes to the parent archive node.

9.2.5.2 Viewing Application Status Information

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name] > [module name]	Status

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name] > [module name]	Status

The Status of each component in the deployed module and it's type is shown.

9.2.5.3 Working with Deployed Resource Adapters

Deployed Resource Adapters can be accessed from the IMC navigation tree, their status can be viewed, and the Configuration Name, User ID and Password changed. When a deployed JCA1.0 compliant RA is selected on the navigation tree, it's Environment Settings can be viewed or modified in the same way as described in "Configuring Connectors (Resource Adapters)" of the "Resources" chapter. Refer to this section for details.

For JCA1.5 RAs their deployment descriptor can be viewed, and settings for their ConnectionFactorys and Managed Objects, if used, can be modified. Details are given below. These JCA1.5 RAs can be selected as the target type for receipt of messages in EJB2.1 compliant applications.

9.2.5.3.1 Viewing the Resource Adapter (JCA 1.5)

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name] > [rar file] | [module name > rar file]	Status

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name] > [rar file] | [module name > rar file]	Status

The **Resource Adapter Definition**, and the **Interface Name** and **Definition Name** for **ConnectionFactorys** and **Managed Objects**, are displayed.

Click an **Interface Name** to access environment settings for a ConnectionFactory or a Managed Object.

9.2.5.3.2 Viewing the Resource Adapter's Deployment Descriptor (JCA 1.5)

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name] > [rar file] | [module name > rar file]	Deployment Descriptor

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name] > [rar file] | [module name > rar file]	Deployment Descriptor

The content of the deployment descriptor file (ra.xml) is displayed.

The deployment descriptor must be modified externally (by editing ra.xml directly), and then redeployed.

9.2.5.3.3 Updating the Definition of a Resource Adapter's ConnectionFactory (JCA 1.5)

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name] > [rar file] | [module name > rar file]	Status

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name] > [rar file] | [module name > rar file]	Status

To update a ConnectionFactory definition for a registered Resource Adapter:

1. Click the ConnectionFactory's Interface Name.
2. In **Definition Name**, specify the JNDI name to be used for the ConnectionFactory for lookup by J2EE applications.
3. Type the **User ID**, and **Password** to use when connecting to the Resource Adapter.
4. Click the **Update** button.

9.2.5.3.4 Updating the Definition of a Resource Adapter's Managed Object (JCA 1.5)

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name] > [rar file] | [module name > rar file]	Status

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name] > [rar file] | [module name > rar file]	Status

To update a Managed Object definition for a registered Resource Adapter:

1. Click the Managed Object's Interface Name.
2. In **Definition Name**, specify the JNDI name to be used for the Management Object for lookup by J2EE applications.
3. Click the **Update** button.

9.2.5.4 J2EE Application Deployment

To deploy an application to a WorkUnit:

1. Specify the deployment file containing the application(s).

   For details, refer to "9.2.5.5 Deploying a J2EE Application".

2. Define the Web and/or EJB application(s) deployment settings.

   For details, refer to "9.2.5.5.2 Defining Web Application Deployment Settings" and "9.2.5.5.3 Defining EJB Application Deployment Settings".

3. Click the **Deploy** button.

   The deployment file is uploaded to the server on which this operation is being performed, and then deployed. In the case of multi-server WorkUnits, it is deployed to the Managed Servers.

For details, refer to "9.2.5.5 Deploying a J2EE Application".

Note

- If the deployment file is an EAR file, it may contain .WAR and .JAR files (containing Web applications and EJB Applications respectively). In this case, the EAR node under the WorkUnit node will contain sub nodes for each file type it contains.
- For details on updating the deployment descriptor settings for an application, refer to "9.2.5.10 Updating the Deployment Descriptor File for a Deployed EJB Application".

9.2.5.5 Deploying a J2EE Application

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name]	Deploy

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit Name]	Deploy

To deploy a J2EE application:

1. In **Deployment File**, specify the EAR, WAR, EJB-JAR or RAR file to be deployed.
2. Click the **WorkUnit Restart** checkbox to automatically restart the WorkUnit after the application has been deployed.

   To deploy accepting default values, skip to step 7.

3. Click the Detailed Settings **[Show]** link to specify the application settings for applications to be deployed.

   Settings are displayed for applications valid for the IJServer type and only if the specified deployment file contains applications of that type. For example, if the IJServer type is 'EJB Only', and an EAR containing both Web application and EJBs is selected, only an 'EJB Application Settings' table is displayed and will be deployed.

4. To specify basic settings for the deployment file, click the Common Settings **[Show]** link.

   For details, refer to "9.2.5.5.1 Defining Common Deployment Settings".

5. To specify a Web application's deployment settings, click the Web Application Settings **[Show]** link.

   For details, refer to "9.2.5.5.2 Defining Web Application Deployment Settings".

6. To specify a EJB applications deployment settings, click the EJB Application Settings **[Show]** link.

   For details, refer to "9.2.5.5.3 Defining EJB Application Deployment Settings".

7. Click an application name to access its constituents (JARs, WARs, RARs, etc.)

8. Click the **Deploy** button to deploy the application into the WorkUnit.

   The deployment file is uploaded to the Server on which this operation is being performed, and then deployed. If the WorkUnit is a multi-server WorkUnit, it is then deployed to the managed servers deployed for the respective WorkUnit components.

   Click the **Select Again** button to return this form to the default values.

Note

- It is possible to select any EAR, WAR, EJB-JAR or RAR file for deployment, but only those components within the file that are compatible with the IJServer type will be deployed. For instance if an EAR contains both a Web and EJB Application, only the Web Application will be deployed to a Web only IJServer.
- The detailed Web Application and EJB Application settings that can be edited are dependent on the contents of the file being deployed.
- When the Detailed Settings **[Show]** link is clicked, the deployment file is uploaded to the Server but not deployed. Click the **Select Again** button to reset the page, hide the details and chose and upload another file.
- Neither Interstage nor the WorkUnit have to be running for a deployment to take place. A running WorkUnit must be restarted for the deployment to take effect.
- If Separate VMs is set such that the Servlet container and EJB container are allocated to separate servers, client distribution data is automatically allocated to the Servlet container.
- A Web application cannot be deployed with the same name twice unless into another WU that has a different virtual host.

9.2.5.5.1 Defining Common Deployment Settings

Deploy	Detailed Settings	Common Settings

To specify the common settings of the deployment file, in the Weblogic Messaging Bridge Adapter (No TX)(jms-notran-adp.rar) table:

1. In **Module Name**, specify the name by which the deployment unit can be identified.

9.2.5.5.2 Defining Web Application Deployment Settings

Deploy	Detailed Settings	Web Application Settings

The Web application contained in the .war of the deployment file is displayed.

To define settings for the Web application:

1. In **Web Application Name**, specify the path and file name of the application to be deployed.
2. In **Shared Context**, select **On** to allow dispatch of this WAR to other web applications operating in the same WorkUnit.
3. In **Store session information in cookies?**, select **Yes** to save the session information in the browser. This item is changed to the default value, if the value is not specified at the time of overwrite deployment. Select **Store session information in web browser** to allow reconnection when the Web browser is closed and then restarted within a valid session. Select **Always add the Secure attribute to cookies** to add the Secure attribute to cookies, if using SSL Accelerator.
4. Specify the **Encoding** used to parse the parameters for requests from the Web client and for body processing as:
5. In **Certification method**, select 'Use Web server authentication information' to use the authentication details that were specified in the Web server.

9.2.5.5.3 Defining EJB Application Deployment Settings

Deploy	Detailed Settings	EJB Application Settings

Typically each EJB application consists of many Enterprise Java Beans (hereinafter referred as bean). Beans are named by the developers and hence may not have a meaningful name for the administrator / user. A meaningful application name can be provided for each bean. Each bean contained in the .jar of the deployment file is displayed. The bean name is given along with it's current EJB Application Name.

For each bean:

1. In **EJB Application Name**, specify a meaningful name by which the bean can be accessed. The default name is the bean name.

9.2.5.5.4 Defining Connector Settings for a Deployment Archive that contains a Connector

Deploy	Detailed Settings	Connector Settings

The connector contained in the .rar of the deployment file is displayed. The bean name is given along with its current EJB Application Name.

To configure the Connector Settings:

1. If the .rar is JCA 1.0, in **Definition Name** specify the JNDI name to be used for the resource adapter for look up by J2EE applications.

   If the .rar is JCA 1.5, in **Resource Adaptor Name**, specify the name used to identify the resource adapter.

2. If the .rar is J2EE Connector Architecture 1.0, specify a **User ID** and **Password** for the resource adapter.

- The Definition Name of the JCA1.5 Resource Adapter's ConnectionFactory and Managed Objects, and a Resource Adapter's User ID and Password can be updated after deployment. For details, refer to "9.2.5.3.3 Updating the Definition of a Resource Adapter's ConnectionFactory (JCA 1.5)".

9.2.5.6 Updating the JNDI Name of an Application

The JNDI name is the name by which other programs, machines, etc. can access applications across a network.

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name] > [module name]	Name Conversion

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name] > [module name]	Name Conversion

The **Application Name**, **Reference Type** and **Reference Name** are displayed for each application.

To update the **JNDI Name** of a J2EE, web or EJB application in the Interstage Naming Service:

1. In **JNDI Name**, specify the name by which this application can be referenced by any client or other distributed applications.
2. Click the **Update** button to save the new JNDI name.

- If the application was deployed inside an EAR deployment file, then the JNDI is changed from the Name Conversion tab for the EAR node on the tree.

9.2.5.7 Monitoring an Application

Web Application

To monitor a Web application, go to the following location:

Site Management

Interstage > Interstage Application Server > [server group > member server] | [independent managed server] > System > WorkUnit > [WorkUnit name] > [war file name] | [parent Archive>war file name]	Monitoring

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name] > [war file name] | [parent archive > war file name]	Monitoring

The application name is displayed, along with the Session Count, Servlet Name, Invocation Count for that servlet and the Method Execution Times in milliseconds (Average, Lowest, Highest).

Note

- Monitoring information is only available for the Web Application on the individual servers it has been deployed to. Overall monitoring of a Web Application deployed in a multi-server WorkUnit is not possible.
- The screen is refreshed based on the interval set in the IMC Console Preferences. For further details, refer to the "Chapter 2 Configuring the Interstage Management Console" chapter.

EJB Application

To monitor an EJB application, go to the following location:

Site Management

Interstage > Interstage Application Server > [server group > member server] | [independent managed server] > System > WorkUnit > [WorkUnit name] > [jar file name] | [parent Archive>jar file name]	Monitoring

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name] > [jar file name] | [parent Archive > jar file name]	Monitoring

A list of EJB applications contained in the selected archive is displayed.

In the Status tab, click the EJB Application Name of the application to be monitored.

The application name is displayed. Other information displayed is dependent on the application and the type of bean.

Note

- Monitoring information is only available for the EJB Application on the individual servers it has been deployed to. Overall monitoring of an EJB Application deployed in a multi-server WorkUnit is not possible.
- The screen will be periodically refreshed based on the interval set in the IMC Console Preferences. For details, refer to "Configuring the Display" in the "Chapter 2 Configuring the Interstage Management Console" chapter.

9.2.5.8 Viewing the Status of an EAR File

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name] > [ear file name]	Status

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name] > [ear file name]	Status

A list of archive files contained in this .ear file is displayed. The archive type is given for each, and the status. The status can have the following values:

- Running
- Stopped
- Error

9.2.5.9 Viewing the Deployment Descriptor of a Deployed Module

The deployment descriptor of deployed web archives (.WAR), EJB2.1 Java archives (.JAR), and JCA1.5 resource archives (.RAR), can be viewed from the IMC.

To view these deployment descriptors, select the required module from the navigation tree, and click the Deployment Descriptor tab in the Operation Frame.

9.2.5.10 Updating the Deployment Descriptor File for a Deployed EJB Application

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name] > [EJB Module] > [jar module]	Status

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name] > [EJB Module]>[jar module]	Status

For archives that contain a Web service implemented as a STATELESS Session Bean, the EJB SOAP router information is displayed.

A list of EJB applications contained in the selected archive is displayed.

To update the deployment descriptor file for an EJB application:

1. Click the EJB Application Name to access the EJB application.
2. Click the Deployment Descriptor tab to access the applications basic settings.
3. Click the Detailed Settings **[Show]** link to access further application settings.
4. Click the **Update** button to apply changes.

Note

- The EJB Application Name and Bean Type are displayed for all applications. Other information displayed varies depending on the type of application, the compliancy version of the EJB, and configuration settings made on this page.
- The applications **EJB Version** and the **JDK Version Used for Deployment** are displayed under Detailed Settings > Interstage Additional Settings,
- Some of the information can be updated, some is for information only. It is recommended that only user's familiar with the application or the EJB standards edit these settings.
- To modify settings of the deployment descriptor that cannot be edited from this page, edit ejb-jar.xml in the development environment and redeploy the JAR.

9.2.5.11 Viewing "webservice.xml" and Downloading a WSDL

Site Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name] > [war file name] | [parent archive > war file name]	Web Service environment configuration

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name] > [war file name] | [parent archive > war file name]	Web Service environment configuration

To view the Web Services environment configuration file:

1. Click the **deployment descriptor [Show]** link.

   The Web Services environment configuration file is displayed.

To download a WSDL for publication of the Web service (not available from Application Management):

1. In **URL Prefix** select:

   - **Enter Directly** and specify the connection URL (URL excluding the path) used to call the deployed Web Service from the client (http:// and https:// are valid)
   - **Select those shown below** and from the drop-down list, select the required option (Standalone only)

   An appropriate path for the deployed environment will be added and set as the connection URL for WSDL publication.

2. Click the **Download WSDL** button.
3. Follow options to Open or Save

- To modify the Web Services environment configuration file, modify it externally and then redeploy it.
- If "/" is specified in the URL path part, it is ignored. Other paths cannot be specified.
- For details on WSDL for publication, refer to "How to Operate Web Services (the Server Function)" in the "Interstage Web Service Operation" chapter of the J2EE User's Guide.

9.2.5.12 Viewing the Application Environment Definition (Web Application Only)

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name] > [war file name] | [parent archive > war file name]	Application Settings

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name] > [war file name] | [parent archive > war file name]	Application Settings

The **Web Application Name** is displayed, along with the **Context Settings**: **Shared Context**, **Store session information in cookies?**, **Encoding** and **Certification method**.

9.2.5.13 Updating Web Application Settings

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name] > [war file name] | [parent archive > war file name]	Application Settings

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name] > [war file name] | [parent archive > war file name]	Application Settings

To update the Web application environment settings:

1. In the Context Settings table, update the settings as required.

   For details, refer to "9.2.5.5.2 Defining Web Application Deployment Settings".

2. Click the **Update** button to save the new environment settings. The Web application must be redeployed with the updated settings. Otherwise the changes will not be effective.

Note

- If the web application was deployed inside an EAR deployment file, then the Auto reload options are changed from the Environment Settings tab for the EAR node on the tree.

9.2.5.14 Undeploy a Deployed Application

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name]	Application Status

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name]	Application Status

To undeploy a deployed J2EE application.

1. Select **Module List** to view a list of application archives deployed to the WorkUnit.
2. Click the checkbox to the left of Module Names of archives to be removed.
3. Click the **Restart WorkUnit automatically after undeployment** to have the WorkUnit restart when the undeploy operation is complete.
4. Click the **Undeploy** button.

9.2.5.15 Reloading a Deployed Application

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name]	Application Status

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name]	Application Status

This option loads the specified application while the server is running, and re-reads the class files and definition files.

To reload a deployed J2EE application:

1. Select **Module List** to view a list of application archives deployed to the WorkUnit.
2. Click the checkbox to the left of Module Names of archives to be reloaded.
3. Click the **Restart WorkUnit automatically after undeployment** to have the WorkUnit restart when the reactivate operation is complete.
4. Click the **Reactivate** button.

Note

- Applications cannot be reloaded on individual Managed Servers because this would involve an update to the definition/settings for the entire WorkUnit.
- The Hot Deploy option in the WorkUnit settings must be enabled for the Reload option to work successfully.

9.2.5.16 Redeploy an Application which fail to be deployed

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name]	Application Status

This option is not applicable for a standalone server

An application failed to be deployed on a Managed Server in a Server Group can be redeployed. To redeploy such an application:

1. Select **Module List** to view a list of application archives deployed to the WorkUnit.
2. Click the checkbox to the left of Module Names of archives to be redeployed.
3. Click the **Restart WorkUnit automatically after undeployment** to have the WorkUnit restart when the redeploy operation is complete.
4. Click the **Redeploy** button.

9.2.6 Managing Startup / Shutdown Classes

From the Interstage Management Console, it is possible to specify one or more user defined Java classes to be executed during startup or shutdown of a WorkUnit. Startup classes are executed before applications deployed to the WorkUnit are started, while shutdown classes are executed after applications in the WorkUnit have stopped.

The order in which the startup or shutdown classes are executed can be specified.

In a multi-server WorkUnit, classes specified by the Admin Server are copied to each Server allocated to the WorkUnit and executed on all servers in parallel. The classes are deployed/copied to each server and executed (as with all operations from the Application Management tab, if one fails, fix the problem and re-execute).

9.2.6.1 Viewing IJServer Startup / Shutdown Classes

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name]	Startup/Shutdown

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name]	Startup/Shutdown

Click and open the 'View Classes' tab.

The list of Startup and of Shutdown Execution classes is displayed.

Classes are listed in the order they are executed on IJServer startup/shutdown. This order can be set when creating or updating a class. The **Class** value is the fully qualified java classname of this execution class.

Click a list item access that class settings for view/update.

Note

- For a multi-server WorkUnit when accessed from the Server tab or directly via the Managed Server, the classes that are listed are those created from the Application Management tab.

9.2.6.2 Specifying a Class to Execute at IJServer Startup

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name]	Startup/Shutdown

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name]	Startup/Shutdown

Click and open the 'Create a new Class' tab.

To specify an IJServer Startup Execution class:

1. Select **Startup Class** to create a class that will run at startup of the WorkUnit, before applications deployed to the WorkUnit have started.
2. In **Name**, specify the class ID, and in **Class Name**, specify the fully qualified name of the java class.
3. If one or more Startup classes have already been specified for this WorkUnit, in **Start Order**, click **Call after** or **Call before**, and click a Startup class from the list to define when this class will be called relative to that selected.
4. In **Arguments**, specify arguments passed to the method.
5. In **Abort startup if error occurs in startup class?**, select:
   - **Abort startup** to abort WorkUnit startup if an error occurs.
   - **Continue startup** to have WorkUnit start up continue even if an error occurs during execution of this startup class.
6. Select **Call in all VMs**, to have the class executed in all VMs on which this WorkUnit is running. Otherwise, the class is executed only in this VM.
7. Click the **Create** button to create a startup class.

Note

- Classes must be at the location specified in the java class path defined for the WorkUnit.
- The WorkUnit must be stopped in order to create execution classes.

9.2.6.3 Specifying a Class to Execute at IJServer Shutdown

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name]	Startup/Shutdown

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name]	Startup/Shutdown

Click and open the 'Create a new Class' tab.

To specify an IJServer Shutdown Execution class:

1. Select **Shutdown Class** to create a class that will run at shutdown of the WorkUnit, after the WorkUnit has stopped.
2. In **Name**, specify the class ID, and in **Class Name**, specify the fully qualified name of the java class.
3. If one or more Startup classes have already been specified for this WorkUnit, in **Start Order**, click **Call after** or **Call before**, and click a Startup class from the list to define when this class will be called relative to that selected.
4. In **Arguments**, specify arguments passed to the class method called.

5. Select **Call in all VMs**, to have the class executed in all VMs on which this WorkUnit is running. Otherwise, the class is executed only in this VM.
6. Click the **Create** button.

Note

- Classes must be at the location specified in the java class path defined for the WorkUnit.
- The WorkUnit must be stopped in order to create execution classes.
- If the IJServer type is specified as having 2 VMs, the servers or Server Groups allocated for the Servlet and EJB Containers may have different operating systems. In this case the Argument field is split into two - one for each Container

9.2.6.4 Updating an IJServer Startup / Shutdown Class

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name]	Startup/Shutdown

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name]	Startup/Shutdown

Click and open the 'View Classes' tab.

To update an IJServer Execution class:

1. Click the **Name** of the class that is to be updated.
2. Modify the settings as required.

   For details refer to "9.2.6.2 Specifying a Class to Execute at IJServer Startup" and "9.2.6.3 Specifying a Class to Execute at IJServer Shutdown" for details on Startup and Shutdown class settings respectively.
3. Click the **Update** button to update settings for the execution class.

   Click **Refresh** to restore the most recently saved settings.
4. Click the **Back** button to return to the list of execution classes.

Note

- The WorkUnit must be stopped in order to update execution classes.

9.2.6.5 Deleting an IJServer Startup / Shutdown Class

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name]	Startup/Shutdown

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name]	Startup/Shutdown

Click and open the 'View Classes' tab.

To delete an IJServer Execution class:

1. Click the checkbox to the left of the **Name** to be deleted.

   Click the **Select All** button to select all classes in the list.

2. Click the **Delete** button to delete the class.

Note

- The WorkUnit must be stopped in order to delete execution classes.

9.2.7 Moving Web Server Connector

It is possible to change the Web server connector from the current server group to another server group.

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name]	Move Web server connector

Under General Settings, specify the server group where the **Web Server Connector** is to be deployed. Under Web Server Connector Settings, specify the Web Server/Web Server Virtual Host. A new WorkUnit can be created only when Interstage is running or has been stopped normally. It cannot be created if Interstage has been forcefully shut down.

Chapter 10 CORBA WorkUnits

10.1 Managing CORBA WorkUnits

For details on Developing CORBA Applications for Interstage, refer to Distributed Application Development Guide (CORBA Service Edition).

10.1.1 Viewing the Status of a CORBA WorkUnit

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name]	Status

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name]	Status

The CORBA WorkUnit Status is displayed. The information displayed depends on if it is a multi-server or standalone WorkUnit.

The WorkUnit Name, Type (CORBA in this case), Status and Start Time are given.

For multi-server CORBA WorkUnits viewed from the Application Management tab the following should be noted:

- The Status is the aggregate status of all servers to which it is allocated. Refer to the Status table below for possible values Status field.
- The aggregate Last Action Status of all servers to which the WorkUnit is allocated is given. This is the status of update operations (environment settings, application deployment etc.) of servers. Refer to Last Action Status table below for possible values.
- If an error has occurred during an update operation (i.e. when modifying the environment settings or deploying an application) at a Managed Server to which the WorkUnit is allocated, the error will be shown in the Last Action Status table. The server on which the error occurred, the operation that was being processed, and the error message generated are displayed.

Status

The table below details the possible operating status values for Server Groups or individual servers.

Table 10.1 CORBA WorkUnit Status for site participants

Value	Method of accessing the WorkUnit status screen	
	Application Management tab	Site Management tab
Started	WorkUnit is running on the server or on all servers in Server Group	WorkUnit is running on the server
Started (part stopped)	WorkUnit is running. Some WorkUnit instances on servers in the Server Group are stopped	
Stopped	WorkUnit is stopped on the server or all servers in the Server Group	WorkUnit is stopped on the server
Starting	WorkUnit start processing is in progress on the server or all servers in the Server Group	WorkUnit start processing is in progress on the server
Stopping	WorkUnit stop processing is in progress on the server or all servers in the Server Group	WorkUnit stop processing is in progress on the server
Error	An error occurred during an IJServer operation	

Last Action Status

For a multi-server CORBA WorkUnit the Last Action Status is the aggregate status of the WorkUnit on Server Groups/Independent Managed Server it is allocated to. The possible Last Action Status values for Server Groups or Independent Managed Servers are:

- **Normal** where all WorkUnit operations were processed normally for all servers to which the WorkUnit is allocated.
- **Error** where an error occurred during a WorkUnit update operation (i.e. when updating environment settings or deploying an application), that failed for the WorkUnit.
- **Normal (Part)** where an error occurred at some servers during a WorkUnit update operation.

10.1.2 Creating a CORBA WorkUnit

Application Management Operation

Interstage > Interstage Application Server > WorkUnit	Create a New WorkUnit

Standalone

Interstage > Interstage Application Server > System > WorkUnit	Create a New WorkUnit

To create a CORBA WorkUnit:

1. In **WorkUnit Name**, specify a name for the CORBA WorkUnit.
2. In **Type**, select CORBA.
3. If creating a WorkUnit across multiple participants in a site, in **Deploy To**, select the Independent Managed Server/Server Group to which the WorkUnit is to be deployed.
4. Click the Detailed Settings **[Show]** link, to access and specify the WorkUnit settings.

   For details, refer to 10.1.2.1 Specifying CORBA WorkUnit Settings.

Note

- WorkUnit names must be unique among multi-server WorkUnits created on the Admin Server. The name cannot be the same as a Conventional WorkUnit name on any Independent Managed Server to which the new WorkUnit is to be allocated.
- WorkUnit names cannot be modified. If the name needs to be changed, the WorkUnit must be deleted and a new WorkUnit created.

10.1.2.1 Specifying CORBA WorkUnit Settings

Create a New WorkUnit {CORBA}	Detailed Settings	WorkUnit Settings

To specify General WorkUnit Settings:

1. In **Application Folder**, specify the absolute path of the CORBA application. For a Java-based CORBA application, this is the directory containing the Java interpreter executable (e.g., 'c:\interstage\JDK6\bin' for Windows, '/usr/bin' for Solaris).
2. In **Application Working Directory**, specify the absolute path of the working directory (current directory) used by the application(s). By default, application standard output and standard error output are written to stdout/stderr files here.
3. In **Number of generations of the current directory to avoid**, click the required number.
4. In **Retry count**, specify the number of times to retry WorkUnit startup after abnormal termination.

5. In **Path**, specify the full path that applications and exit programs use to run (for example, if they use a DLL that is not in the system PATH). Up to 30 line-feed delimited paths can be specified. And in **Environment Variables**, specify any environment variables used by applications in the following format: 'env_var=value'.

   PATH cannot be used as an environment variable name.

6. If using an exit program, in **Exit program name**, specify the name of the exit program that gets called when the WorkUnit starts and also stops. Note that this is not the same functionality as that of pre/post exit programs that can be defined for the underlying CORBA application. In **Exit program maximum processing time**, specify the maximum time in seconds for exit program processing.

   In **Exit program module**, specify the name of the execution file containing the WorkUnit exit program, and process collection exit program. This item is required if a WorkUnit exit program name has been specified.

7. In **Request dispatch type**, select:

   - **LIFO** (LRU algorithm)
   - **FIFO** (Round-robin algorithm)

   as the method of distribution of client request messages to server application processes.

   When there are several of the same CORBA server process instances ready to receive requests, the dispatch type determines how requests are dispatched to them from the request queue.

8. In **Auto Start**, select **Automatic Start** to have the WorkUnit start when Interstage is started, and specify the **WorkUnit maximum startup time** in seconds. If the WorkUnit startup time exceeds this value, active processes will be shutdown and startup aborted.
9. Specify the **Process maximum stop time** in seconds. If normal process stop is not completed within specified time, the process will be forcefully shut down.
10. In **Output process start log of the CORBA WorkUnit**, select **Yes** to output a process start log for the CORBA WorkUnit.
11. In Use **IPCOM for monitoring?**, select **Yes** to monitor the WorkUnit.
12. In **Stop the WorkUnit if the application failed to restart automatically?**, select:

    - **Stop WorkUnit** to stop the WorkUnit and all deployed applications if an application fails to restart.
    - **Continue to operate WorkUnit** if an application fails to restart.

- By default, the application standard output and standard error output are written to stdout/stderr files in a two-level subdirectory under the Application Working Directory. The first-level subdirectory carries the WorkUnit name, the subdirectory under that carries the name of the CORBA application process id. By default, each time the WorkUnit is re-started, the previous lowest-level subdirectory containing the stdout/stderr files is deleted.

  By defining the environment variable setting 'EXTP_CURRENTDIR_HISTORY=YES' in step 5, it is possible to get Interstage to backup up to five generations of the work directory contents.

10.2 Managing CORBA Applications

This section describes how to perform the following CORBA application operations:

- 10.2.1 Viewing Application Status
- 10.2.2 Deploying CORBA Applications and Interfaces
- 10.2.3 Undeploying an Application from a CORBA WorkUnit
- 10.2.4 Blocking/Unblocking Applications
- 10.2.5 Updating Application Settings
- 10.2.6 Monitoring CORBA Applications

10.2.1 Viewing Application Status

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name] > [deployed application]	Status

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name] > [deployed application]	Status

The status of the deployed application is displayed.

The Implementation table shows Implementation Repository ID, Status and Action.

The Object info table shows Interface Repository ID, Status and Settings.

Click the **Refresh** button to display the most recent information.

10.2.2 Deploying CORBA Applications and Interfaces

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name]	Deploy

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name]	Deploy

To deploy an application to a CORBA WorkUnit:

1. In **Implementation Repository ID**, specify the ID that uniquely identifies a CORBA application within this WorkUnit.
2. In **Program EXE file**, specify the name of the application and exit program module.
3. Click the **WorkUnit Restart** checkbox to automatically restart the WorkUnit after the application has been deployed.

   For simple deployment using default values, skip to step 8.
4. Click the Show Details **[Show]** link to access detailed deployment settings.
5. Click the CORBA Application **[Show]** link to specify the CORBA application settings.

   For details, refer to 10.2.2.1 Specifying CORBA Application Deployment Settings.
6. Click the Interface **[Show]** link, and click the **Add Interface** button to specify the Interface settings. For details on Specifying Interface Settings, refer to 10.2.2.2 Registering an Interface.
7. Click the **Add** button to add the Interface to the WorkUnit.
8. Click the **Deploy** button to deploy the application into the WorkUnit.

   Click the **Reset** button to return this form to the default values.

Note

- Interfaces currently added are listed in the Interface section.
- WorkUnit settings defined for the WorkUnit may be overridden at the application level.

10.2.2.1 Specifying CORBA Application Deployment Settings

Deploy	Detailed Settings	CORBA Application

To specify settings of the CORBA application to be deployed:

1. In **Encoding Type**, select the encoding type of the object reference for the CORBA application.

   This must match the value specified in the Implementation Repository definition for the CORBA application.

2. Specify the **Process Concurrency** for the application. This is the maximum number of processes for that CORBA application that may be run concurrently to handle requests. This value corresponds to the 'proc_conc_max' setting in the Implementation Repository settings.

3. In **Threads**, specify the **Initial** and **Maximum** threads in the thread pool of each process instance (dynamically increases/decreases according to load). These values correspond to the 'thr_conc_init' and 'thr_conc_max' settings in the Implementation Repository settings. The number of threads automatically increases and decreases within the specified Initial-Maximum range with variations in load.

4. In **Degenerate Thread**, specify whether to degenerate the thread when thread automatic enhancement is used.

5. In **Application Folder**, specify the top-level directory in which the application programs are located. To use Java applications, specify the absolute path to the directory where the Java executables are stored (example, /opt/FJSVisas/var/system/default/CORBA_WU/WU001).

6. In **Maximum application processing time**, specify the maximum time in seconds to allow the CORBA application to process a client request. Specify a value of 0 for unlimited processing time.

7. In **Forcefully end application on timeout?**, select the action to take when any application exceeds the specified maximum time:

   - **Warning Message** to display warning messages.
   - **Perform application forced stop** to forcefully stop the application on the server(s) to which the WorkUnit is allocated.

8. In **Maximum Size of Queue**, specify the maximum number of messages the queue can contain. An alarm notification is posted when the number of messages in the queue reaches the value specified in **Queue alarm level**, and the alarm is reset when the number of messages drops back below the value in **Queue alarm reset level**.

   Specify a maximum queue size of 0 to allow an unlimited queue size.

9. If the CORBA application is written in Java, specify the **Classpath**s, separated by a line feed character. And in **Environment Variables**, specify any environment variables used by applications in the following format: 'env_var=value'.

   PATH and LD_LIBRARY_PATH cannot be used as an environment variable name.

10. If using an exit program, in **Exit program name**, specify the name of a process collection exit program. This must be a C program. And in **Exit program maximum processing time**, specify the maximum time in seconds for exit program processing.

    In **Exit program module**, specify the name of the execution file containing the process collection exit program.

11. In **Startup parameters**, specify the startup parameters for the application. For a Java application, specify the application class name to be designated for java commands.

12. In **Request dispatch type**, select how request messages from clients are to be distributed to server application processes. When there are multiple instances of the same CORBA server process ready to receive requests, the dispatch type determines how requests are dispatched to them from the queue of requests - either LIFO (LRU algorithm) or FIFO (Round-robin algorithm).

13. In **Buffers**, specify the number of queuing buffers. If no value is specified, Interstage dynamically allocates buffers. In **Buffer Length**, specify the length of one unit of data in the queue. Default is 4096.

14. In **Maintain instance data on client?**, specify the application instance retention function. The parameter is applicable to C++, Java and COBOL applications only. Select **Do not use**, or if to be used, select **Use (connections)** or **Use (objects)**.

15. In **Session Timeout**, specify the session timeout time, if [Use (objects)] has been selected for [**Maintain instance data on client?**].

16. In **Object Reference SSL Settings**, select:

    - **Disabled**
    - **Enabled** to have SSL information added to the server application object reference upon instantiation.

- **Auto**

17. In **Operation Mode**, select the CORBA application operating mode from:

    - **COMPATIBLE**
    - **SYNC_END** (*1)

    This value must correspond to the 'mode' setting in the Implementation Repository definition.

18. In **Use IPCOM load balancing?**, select **Enabled** to enable the Load Balancing. Then specify the **Virtual Host Name** and **Representative Port**.

Note

*1 In Interstage 8.0, the operating mode on the server for C and C++ sample programs is SYNC_END. If deploying the sample server application to CORBA WorkUnits from the Interstage Management Console, set the operating mode to SYNC_END.

10.2.2.2 Registering an Interface

Deploy	Detailed Settings	Interface

To register an Interface for the application being deployed:

1. Click the **Add Interface** button to access the Interface Add table and specify the **Interface Repository ID** of the CORBA object.
2. In **Naming Service Entry**, select **Register** to register the application in step 1 with the Naming Service, and in **Naming Service Name**, specify the name by which the application can be referenced by CORBA clients.
3. In **Priority**, specify the object priority.
4. Specify the **Library Path**.
5. In **COBOL Dynamic Skeleton Interface**, select **Use Cobol Skeleton Interface** to use a dynamic skeleton interface for Cobol applications.
6. Click the **Add** button.

10.2.2.3 Viewing Interfaces

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name] > [deployed application]	Settings

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name] > [deployed application]	Settings

Click the Show Details **[Show]** link, and then click the Interface **[Show]** link to display a list of interfaces deployed for this application. The Interface Repository ID, CORBA Naming Service Entry and Name, Settings, Library Path, and the COBOL Dynamic Skeleton are given for each.

10.2.2.4 Editing an Interface

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name] > [deployed application]	Settings

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name] > [deployed application]	Settings

Click the Show Details **[Show]** link, and then click the Interface **[Show]** link to display a list of interfaces deployed for this application.

To edit settings of an interface:

1. Check the checkbox to the left of interface to be edited.
2. Click the **Edit** button.

   Refer to 10.2.2.2 Registering an Interface for details on Interface settings.
3. Click the **Add** button to update the interface settings and redeploy the interface with the updated settings.

   Click the **Back** button to return to the Interface listing screen.

Note

- The WorkUnit must be stopped to edit settings.

10.2.2.5 Deleting an Interface

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name] > [deployed application]	Settings

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name] > [deployed application]	Settings

Click the Show Details **[Show]** link, and then click the Interface **[Show]** link to display a list of interfaces deployed for this application.

To remove an interface:

1. Check the checkbox to the left of interface(s) to be removed.
2. Click the **Delete** button.

10.2.3 Undeploying an Application from a CORBA WorkUnit

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name]	Undeploy

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name] > [deployed application]	Undeploy

To undeploy an application from a CORBA WorkUnit:

1. Click the checkbox to the left of the **Implementation Repository ID** to be deleted.

   Click the **Select All** button to select all **Implementation Repository ID** in the list.
2. Click the **Restart WorkUnit after undeployment** checkbox to automatically restart the WorkUnit after the application has been undeployed.
3. Click the **Undeploy** button to undeploy the CORBA application.

10.2.4 Blocking/Unblocking Applications

The client request queue for a server or for each server in a Server Group to which the WorkUnit is allocated can be blocked, and unblocked. The queue can be blocked to prevent the server from accepting further requests for this application from clients. When the block is released,

the server can again accept requests for this application. The queue can be blocked at the implementation or the interface level. Queue block and release might be useful under the following circumstances:

- For time zones in which there is business for which restricted use is desirable
- For periods of high load when non-acceptance of requests is desirable
- To stop requests before business stops, so that all processes can be completed before business stops.

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit Name] > [deployed application]	Status

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name] > [deployed application]	Status

A list of implementations and a list of interfaces are displayed.

The Implementation Repository ID, and the Status (Running or Stopped corresponds to blocked/unblocked respectively) is given all listed items. Buttons are provided for the blocking the queue to implementation and interfaces. These are described for implementation units and interfaces below. An error is returned to a client if the client issues a request while the queue is blocked.

Note

- The WorkUnit must be running for block/unblock to succeed.
- Blocking/unblocking can be performed on the individual Independent Managed Servers that a multi-server CORBA WorkUnit is allocated to.
- If a Server Group is specified as the WorkUnit allocation destination, block and unblock processing is executed in parallel on all the servers in the Server Group. When processing is completed at all servers, an execution results message is posted.
- Timeout will occur if processing is not completed within a specific amount of time. Processing results are posted to the Status frame. If an error occurs, refer to the error message and rectify the problem. Then execute the block/unblock operation again.

10.2.4.1 Blocking and Removing Blocks on Implementations

Click the **Block** button in the Action column to block the corresponding queue in the server or Server Group implementation unit.

Click the **Remove Block** button in the Action column to remove the block from the corresponding queue in the server or Server Group implementation unit.

10.2.4.2 Dynamically Changing the Process Concurrency

Click the **Concurrency** button in the Action column corresponding to the implementation to dynamically change the application process concurrency.

In **Number of processes**, specify the new number of concurrent processes.

Click **Reset to the original value** to reset to the original value.

Click the **Update** button to apply the updated process concurrency settings.

Click the **Cancel** button to display the most recent information.

10.2.4.3 Blocking and Removing Blocks on Interfaces

If a queue is blocked in interface units, set the interfaces for which block is desired in the implementation repository definitions before the WorkUnit is started.

Click the **Block** button in the Settings column to block the corresponding queue in the interface unit of the interfaces implemented by the server or Server Group implementation units.

Click the **Remove Block** button in the Settings column to remove the block from the corresponding queue in the interface units of the interfaces implemented by the server or Server Group implementation units.

Click the **Refresh** button to display the most recent information.

10.2.5 Updating Application Settings

Application Management

Interstage > Interstage Application Server > WorkUnit > [WorkUnit name] > [deployed application]	Settings

Standalone

Interstage > Interstage Application Server > System > WorkUnit > [WorkUnit name] > [deployed application]	Settings

To update the detailed settings of the deployed CORBA application:

1. Verify that the WorkUnit is stopped.

   For details, refer to 10.1.1 Viewing the Status of a CORBA WorkUnit.

2. Click the Show Details **[Show]** link to access and update the application settings.

3. Click the CORBA Application **[Show]** link to edit the CORBA application settings.

   For details, refer to 10.2.2.1 Specifying CORBA Application Deployment Settings.

4. Click the Interface **[Show]** link to add, edit or delete an interface:

   - Click the **Add Interface** button, specify the interface settings and then click the **Add** button to add the interface.

     For details, refer to 10.2.2.2 Registering an Interface.

   - Check the checkbox to the left of the **Interface Repository ID** to be updated, click the **Edit** button to update the interface settings, and then click the **Add** button.

     For details, refer to 10.2.2.4 Editing an Interface.

   - Check the checkbox to the left of **Interface Repository ID**s to be deleted, and click the **Delete** button to remove the interface.

     For details, refer to 10.2.2.5 Deleting an Interface.

5. Click the **Update** button to update the CORBA application settings.

   Click the **Refresh** button to refresh the form with the most recently saved values.

Note

- The WorkUnit must be stopped to have write access to settings.

10.2.6 Monitoring CORBA Applications

Site Management

Interstage > Interstage Application Server > [server group name | server group name > server name] > System > WorkUnit > [WorkUnit name] > [deployed application]	Monitoring

From the Admin Server, performance information of CORBA applications is displayed for each server to which the WorkUnit is allocated.

Information displayed for each Implementation repository (application) on each server includes the Process Concurrency, the number of Threads, the number of Queued Messages and the number of Processed messages.

The Admin Server fetches the WorkUnit performance information from each of the Managed Servers at regular intervals.

Click the **Refresh** button to display the most recent information.

Chapter 11 Security

11.1 Security Overview

Interstage includes extensive support for security in all layers of the Application Server. A separate Security System Guide documents all security features provided by Interstage Application Server and associated products including:

- Security Risks and Measures
- Firewall and Proxy Server issues
- Authentication and Encrypted Communication through support for SSL
- Security Systems for Web Services.

11.1.1 Interstage Directory Service (IDS)

This is not valid for Linux (64 bit).

Interstage provides an LDAP capable directory server called Interstage Directory Service. For detailed information on Interstage Directory Service (IDS), refer to the Directory Service Operator's Guide.

11.1.2 Single Sign-on (SSO)

For applications that require a single sign on capability, Interstage provides a 'Single Sign-on (SSO)' facility. For detailed information on SSO refer to the Single Sign-on Operator's Guide.

11.1.3 SSL

When application data security is critical, communications between the client, application server and its deployed applications can be encrypted. For detailed information on how to create SSL certificates, refer to the Security System Guide.

Created certificates can be viewed from the Interstage Management Console, and are available for use by SSL configurations. SSL configurations can be created/modified/viewed from the Interstage Management Console.

11.1.3.1 Viewing Site Certificates

Application Management

Interstage > Interstage Application Server > Security > Certificates > Site Certificates > [managed server name]	Certificates

Standalone

Interstage > Interstage Application Server > System > Security > Certificates > Site Certificates	Certificates

This displays a list of Site Certificates that have been created. The certificate Nickname and content is given for each.

11.1.3.2 Viewing CA Certificates

Application Management

Interstage > Interstage Application Server > Security > Certificates > CA Certificates > [managed server name]	Certificates

Standalone

Interstage > Interstage Application Server > System > Security > Certificates > CA Certificates	Certificates

This displays a list of CA Certificates that have been created. The certificate Nickname and contents (is given for each.

11.1.3.3 Viewing a List of SSL Configurations

Application Management

Interstage > Interstage Application Server > Security > SSL	View SSL Configurations

Standalone

Interstage > Interstage Application Server > System > Security > SSL	View SSL Configurations

This displays a list of the SSL Configurations already created.

11.1.3.4 Creating a SSL Configuration

Application Management

Interstage > Interstage Application Server > Security > SSL	Create a new SSL Configuration

Standalone

Interstage > Interstage Application Server > System > Security > SSL	Create a new SSL Configuration

To create an SSL Configuration:

1. If accessing from the **Application Management** tab, in the **Deploy To** list, click the Server Group/Independent Managed Server to which the SSL configuration is to be deployed.

   Click the **Next** button to configure the SSL settings.

2. Specify the **Configuration Name**.

   This name must be unique within the site.

3. Check the checkbox corresponding to the **Protocol Version** that this configuration will support.

4. In **Verify Client Certificate?**, select the required client certificate verification method.

5. Select the **Site Certificate Nickname** from the list of previously created Site Certificates. If deploying to a Server Group, the certificates must have been created on each Managed Server in the group.

6. Click the Detailed Settings [**Show**] link, and in **Encryption Method**, check the checkboxes corresponding to the encryption methods to be supported by this configuration (check all that apply).

7. In **CA Certificate Nickname**, select:

   - **Select All Digital Certificate Providers** to accept all providers.
   - **Select Digital Certificate Provider from the list**, and then check the Digital Certificate Providers that this configuration should accept.

8. Click the **Create** button to create the SSL Configuration. A result message is displayed in the message frame when processing is complete.

   - Click the **Reset** button to reset this form to the default values.
   - Click **Back** to return to the **Deploy To** page. This button only appears if accessing from the **Application Management** tab.

- For details on creating Site Certificates, refer to the Security System Guide.

11.1.3.5 Updating a SSL Configuration

Application Management

Interstage > Interstage Application Server > Security > SSL > [configuration name]	SSL Settings

Standalone

Interstage > Interstage Application Server > System > Security > SSL > [configuration name]	SSL Settings

To update the selected SSL Configuration:

1. Edit the required settings as described in 11.1.3.4 Creating a SSL Configuration.
2. Click the **Update** button to update the SSL Configuration.

   A result message is displayed in the message frame when processing is complete.

11.1.4 Customizing SSL Encrypted Communication for the Interstage Management Console

SSL encryption of communications with the Interstage Management Console can be enabled during Interstage installation. The procedures below describe how to subsequently enable or disable SSL after installation and customize an installed operating environment.

Note

- If SSL encryption is not used, the ID and password used to access the Interstage Management Console are transferred across the network. For this reason, it is recommended that you either use SSL encryption communication, or implement security to ensure that communicated data is not intercepted.

11.1.4.1 Enabling SSL Encrypted Communication

To enable SSL encryption if it was not selected during Interstage installation:

1. 11.1.4.1.1 Define a Certificate/Key Management Environment using the cmcrtsslenv Command
2. 11.1.4.1.2 Check the Certificate Fingerprint
3. 11.1.4.1.3 Edit the Interstage HTTP Server Definition File to Enable SSL Encryption
4. 11.1.4.1.4 Restart the Interstage HTTP Server for the Interstage Management Console

These steps are explained in the following sections.

11.1.4.1.1 Define a Certificate/Key Management Environment using the cmcrtsslenv Command

Windows32/64

```
"C:\Program Files\Common Files\Fujitsu Shared\F3FSSMEE\cmcrtsslenv.exe" -ed
[The installation folder for this product]\gui\etc\cert
```

Solaris32/64

```
"/opt/FJSVsmee/bin/cmcrtsslenv" -ed /etc/opt/FJSVisgui/cert
```

Linux32/64

When Linux for Intel64 is not used

```
"/opt/FJSVsmee/bin/cmcrtsslenv" -ed /etc/opt/FJSVisgui/cert
```

When Linux for Intel64 is used

```
"/opt/FJSVsmee64/bin/cmcrtsslenv" -ed /etc/opt/FJSVisgui/cert
```

11.1.4.1.2 Check the Certificate Fingerprint

The certificate used for SSL encryption in the Interstage Management Console is generated. To check that connection from the Web browser to the Interstage Management Console is correct, check the generated certificate's fingerprint by executing the following:

For details on the command storage destinations, and other details, refer to "cmdspcert" in the "SSL Environment Setting Commands" chapter of the Reference Manual (Command Edition).

Windows32/64

```
cd [SSL environment settings command storage destination]
cmdspcert.exe -ed [The installation folder for this product]\gui\etc\cert -nn SSLCERT | find
"FINGERPRINT"
```

Solaris32/64 Linux32/64

```
cd [SSL environment settings command storage destination]
cmdspcert -ed /etc/opt/FJSVisgui/cert -nn SSLCERT | grep FINGERPRINT
```

The fingerprint is displayed as follows:

```
FINGERPRINT(MD5):     40 79 98 2F 37 12 31 7C AE E7 B4 AB 78 C8 A2 28
FINGERPRINT(SHA1):    07 28 BE 26 94 89 6D F9 ... <-- (20 bytes of data are displayed in hexadecimal
notation.)
FINGERPRINT(SHA256):  F7 16 00 6E A1 6E A2 14 ... <-- (32 bytes of data are displayed in hexadecimal
notation.)
```

Record the fingerprint that is output.

This certificate is generated automatically by this product so that SSL communication encryption can be easily used between the Interstage Management Console and the Web browser. For enhanced security, certificates issued by the CA can be used. For details on how to switch to using CA certificates, refer to "11.1.4.3 Changing the Certificate".

11.1.4.1.3 Edit the Interstage HTTP Server Definition File to Enable SSL Encryption

Windows32/64

Edit the Interstage HTTP Server definition file for the Interstage Management Console, located at:

Interstage-install-folder\gui\etc\httpd.conf

Edit the file as follows:

```
# ---- Configuration for SSL ---
AddModule mod_ihs_ssl.c
SSLEnvDir "C:\Interstage/gui/etc/cert"
```

```
SSLSlotDir "C:\Interstage/gui/etc/cert/slot"
SSLTokenLabel SSLTOKEN
SSLUserPINFile "C:\Interstage/gui/etc/cert/sslssl"
SSLExec on
SSLVersion 3-3.1
SSLVerifyClient none
SSLCipherSuite RSA-AES-256-SHA:RSA-AES-128-SHA:RSA-3DES-SHA:RSA-RC4-SHA:RSA-RC4-MD5
SSLCertName SSLCERT
#SSLClCACertName cli01
```

Solaris32/64 Linux32/64

Edit the Interstage HTTP Server definition file for the Interstage Management Console, located at:

/etc/opt/FJSVisgui/httpd.conf

Edit the file as follows:

```
# ---- Configuration for SSL ---
AddModule mod_ihs_ssl.c
SSLEnvDir "/etc/opt/FJSVisgui/cert"
SSLSlotDir "/etc/opt/FJSVisgui/cert/Slot"
SSLTokenLabel SSLTOKEN
SSLUserPINFile "/etc/opt/FJSVisgui/cert/sslssl"
SSLExec on
SSLVersion 2-3-3.1
SSLVerifyClient none
SSLCipherSuite RSA-AES-256-SHA:RSA-AES-128-SHA:RSA-3DES-SHA:RSA-RC4-SHA:RSA-RC4-MD5
SSLCertName SSLCERT
#SSLClCACertName cli01
```

11.1.4.1.4 Restart the Interstage HTTP Server for the Interstage Management Console

Windows32/64

Restart the following service:

Interstage Operation Tool(FJapache)

Note

- The 'Interstage Management Console' shortcut registered in the Windows start menu must also be updated. Change the URL registered for this shortcut to https://localhost:12000/IsAdmin

Solaris32/64 Linux32/64

To restart the Interstage HTTP Server for the Interstage Management Console:

1. Use the *kill* command to stop the Interstage HTTP Server process for the Interstage Management Console:

   ```
   # kill 'cat /var/opt/FJSVisgui/tmp/httpd.pid'
   ```

2. Start the Interstage HTTP Server for the Interstage Management Console:

   ```
   # /opt/FJSVihs/bin/httpd -f /etc/opt/FJSVisgui/httpd.conf -s "#ISCONSOLE" -K
   ```

11.1.4.2 Disabling SSL Encrypted Communication

To disable SSL encrypted communication if it was enabled during Interstage installation:

1. 11.1.4.2.1 Edit the Interstage HTTP Server Definition File to Disable SSL Encryption
2. 11.1.4.2.2 Restart the Interstage HTTP Server for the Interstage Management Console

These steps are explained in the following sections.

11.1.4.2.1 Edit the Interstage HTTP Server Definition File to Disable SSL Encryption

Windows32/64

Edit the Interstage HTTP Server definition file for the Interstage Management Console, located at:

Interstage-install-folder\gui\etc\httpd.conf

Comment out the SSL configuration as follows:

```
# ---- Configuration for SSL ---
#AddModule mod_ihs_ssl.c
#SSLEnvDir "C:\Interstage/gui/etc/cert"
#SSLSlotDir "C:\Interstage/gui/etc/cert/slot"
#SSLTokenLabel SSLTOKEN
#SSLUserPINFile "C:\Interstage/gui/etc/cert/sslssl"
#SSLExec on
#SSLVersion 3-3.1
#SSLVerifyClient none
#SSLCipherSuite RSA-AES-256-SHA:RSA-AES-128-SHA:RSA-3DES-SHA:RSA-RC4-SHA:RSA-RC4-MD5
#SSLCertName SSLCERT
#SSLClCACertName cli01
```

Solaris32/64 Linux32/64

Edit the Interstage HTTP Server definition file for the Interstage Management Console, located at:

/etc/opt/FJSVisgui/httpd.conf

Comment out the SSL configuration as follows:

```
# ---- Configuration for SSL ---
#AddModule mod_ihs_ssl.c
#SSLEnvDir "/etc/opt/FJSVisgui/cert"
#SSLSlotDir "/etc/opt/FJSVisgui/cert/Slot"
#SSLTokenLabel SSLTOKEN
#SSLUserPINFile "/etc/opt/FJSVisgui/cert/sslssl"
#SSLExec on
#SSLVersion 3-3.1
#SSLVerifyClient none
#SSLCipherSuite RSA-AES-256-SHA:RSA-AES-128-SHA:RSA-3DES-SHA:RSA-RC4-SHA:RSA-RC4-MD5
#SSLCertName SSLCERT
#SSLClCACertName cli01
```

11.1.4.2.2 Restart the Interstage HTTP Server for the Interstage Management Console

Windows32/64

Restart the following service:

Interstage Operation Tool (FJapache)

Note

- The 'Interstage Management Console' shortcut registered in the Windows start menu must also be updated. Change the URL registered for this shortcut to http://localhost:12000/IsAdmin

Solaris32/64 Linux32/64

To restart the Interstage HTTP Server for the Interstage Management Console:

1. Use the *kill* command to stop the Interstage HTTP Server process for the Interstage Management Console:

```
# kill 'cat /var/opt/FJSVisgui/tmp/httpd.pid'
```

2. Start the Interstage HTTP Server for the Interstage Management Console:

```
# /opt/FJSVihs/bin/httpd -f /etc/opt/FJSVisgui/httpd.conf -s "#ISCONSOLE" -K
```

11.1.4.3 Changing the Certificate

The certificate generated during product installation and by the *cmcrtsslenv* command allows simplifies SSL encryption of communication with the Interstage Management Console.

A certificate issued by a reliable CA can also be used. This is recommended for enhanced security.

The procedure for using a certificate issued by an official CA is described below.

To change the Interstage Certificate Environment:

1. 11.1.4.3.1 Define an Interstage Certificate Environment
2. 11.1.4.3.2 Use the Created CSR to Request that a Certificate be Issued
3. 11.1.4.3.3 Register the CA Certificate (ca-cert.cer) with the Interstage Certificate Environment
4. 11.1.4.3.4 Register the Intermediate CA Certificate (intermediateCA-cert.cer) with the Interstage Certificate Environment
5. 11.1.4.3.5 Register the SSL Server Certificate (site-cert.cer) in the Interstage Certificate Environment
6. 11.1.4.3.6 Create a User PIN file for the Interstage HTTP Server
7. 11.1.4.3.7 Edit the Interstage HTTP Server Definition File
8. 11.1.4.3.8 Restart the Interstage HTTP Server for the Interstage Management Console

These steps are explained in the following sections.

11.1.4.3.1 Define an Interstage Certificate Environment

Use the *scsmakeenv* command to define an Interstage certificate environment and create a certificate signing request (CSR):

Note

- When the scsmakeenv command is executed, the nickname specified in the -n option must also be specified when the site certificate is registered. In the examples below, this nickname is 'IS-Console-SSL-Cert'.

Windows32/64

```
# scsmakeenv -n IS-Console-SSL-Cert -f c:\temp\csr.txt -c
New Password:           <---Set a password for the Interstage certificate
```

```
                        <---environment.  This password becomes USER-PIN.
Retype:
Input X.500 distinguished names.
What is your first and last name?
  [Unknown]:host.domain.com   <--- Enter the Interstage Management Console host name.
What is the name of your organizational unit?
  [Unknown]:xx
What is the name of your organization?
  [Unknown]:xxxx
What is the name of your City or Locality?
  [Unknown]:xxxxxx
What is the name of your State or Province?
  [Unknown]:xxxxxxxx
What is the two-letter country code for this unit?
  [Un]:AU
Is <CN=host.domain.com, OU=xx, O=xxxx, L=xxxxxx, ST=xxxxxxxx, C=AU> correct?
  [no]:yes
SCS: Information: scs0101: A CSR was issued.  <c:\tmp...>
```

Solaris32/64 Linux32/64

```
# scsmakeenv -n IS-Console-SSL-Cert -f /usr/home/my_dir/my_csr.txt -c
New Password:                <---Specify the password for the Interstage
certificate environment.  The password becomes USER-PIN.
Retype:

Input X.500 distinguished names.
What is your first and last name?
  [Unknown]:host.domain.com   <--- Enter the Interstage Management Console host name.
What is the name of your organizational unit?
  [Unknown]:xx
What is the name of your organization?
  [Unknown]:xxxx
What is the name of your City or Locality?
  [Unknown]:xxxxxx
What is the name of your State or Province?
  [Unknown]:xxxxxxxx
What is the two-letter country code for this unit?
  [Un]:AU
Is <CN=host.domain.com, OU=xx, O=xxxx, L=xxxxxx, ST=xxxxxxxx, C=AU> correct?
  [no]:yes
UX: SCS: Information: scs0101: A certificate signing request (CSR) was
created.</usr/home/my_dir/my_csr.txt>
```

For more information, refer to the "Authentication and Access Control for the Interstage HTTP Server" chapter in the Security System Guide.

11.1.4.3.2 Use the Created CSR to Request that a Certificate be Issued

Use the created CSR to request that a certificate be issued.

For processing details, refer to "Requesting Certificate Issuance" in the Security System Guide.

11.1.4.3.3 Register the CA Certificate (ca-cert.cer) with the Interstage Certificate Environment

This processing is not required if a certificate supported by this product has been obtained.

The following assumes that the CA certificate exists in the file 'ca.cert.cer'.

Windows32/64

```
# scsenter -n CA-Cert -f c:\temp\ca-cert.cer
Password:
Certificate was added to keystore
SCS: Information: scs0104: The certificate has been registered.
```

Solaris32/64 Linux32/64

```
# scsenter -n CA-Cert -f /usr/home/my_dir/ca-cert.cer
Password:
Certificate was added to keystore
SCS: Information: scs0104: The certificate was registered.
```

11.1.4.3.4 Register the Intermediate CA Certificate (intermediateCA-cert.cer) with the Interstage Certificate Environment

Depending on the CA, the intermediate CA certificate may be provided in addition to the CA certificate and site certificate. In this case, also register the intermediate CA certificate distributed by the CA.

The following assumes that the intermediate CA certificate exists in the file intermediateCA-cert.cer.

Windows32/64

```
# scsenter -n intermediateCA-Cert -f c:\temp\intermediateCA-cert.cer
Password:
Certificate was added to keystore
SCS: Information: scs0104: The certificate has been registered.
```

Solaris32/64 Linux32/64

```
# scsenter -n intermediateCA-Cert -f /usr/home/my_dir/intermediateCA-cert.cer
Password:
Certificate was added to keystore
SCS: Information: scs0104: The certificate was registered.
```

11.1.4.3.5 Register the SSL Server Certificate (site-cert.cer) in the Interstage Certificate Environment

The following assumes that the issued SSL server certificate exists in the file site-cert.cer.

Windows32/64

```
# scsenter -n IS-Console-SSL-Cert -f c:\temp\site-cert.cer -o
Password:
Certificate reply was installed in keystore
SCS: Information: scs0104: The certificate has been registered.
```

Solaris32/64 Linux32/64

```
# scsenter -n IS-Console-SSL-Cert -f /usr/home/my_dir/site-cert.cer -o
Password:
Certificate reply was installed in keystore
```

```
SCS: Information: scs0104: The certificate was registered.
```

11.1.4.3.6 Create a User PIN file for the Interstage HTTP Server

In the user PIN file, specify the password for the Interstage certificate environment.

Windows32/64

```
# ihsregistupin -f C:\Interstage\gui\etc\cert\upinfile -d
C:\Interstage\etc\security\env\smee\slot
UserPIN:            <-- Specify the password for the Interstage certificate environment.
Re-type UserPIN:    <-- Specify the password for the Interstage certificate environment.
```

Solaris32/64 Linux32/64

```
# ihsregistupin -f /etc/opt/FJSVisgui/cert/upinfile -d
/etc/opt/FJSVisscs/security/env/smee/slot
UserPIN:            <---Specify the password of the Interstage certificate environment.
Re-type UserPIN:    <---Specify the password of the Interstage certificate environment.
```

11.1.4.3.7 Edit the Interstage HTTP Server Definition File

Edit the Interstage HTTP Server definition file for the Interstage Management Console as follows:

Windows32/64

```
# ---- Configuration for SSL ---
AddModule mod_ihs_ssl.c
SSLEnvDir "C:/Interstage/etc/security/env/smee"
                          <-- Fixed(Modify the Interstage installation folder as needed.)
SSLSlotDir "C:/Interstage/etc/security/env/smee/slot"
                          <-- Fixed(Modify the Interstage installation folder as needed.)
SSLTokenLabel Token01           <-- Fixed
SSLUserPINFile "c:/Interstage/gui/etc/cert/upinfile"
                          <-- User PIN file created by ihsregistupin
SSLExec on
SSLVersion 3-3.1
SSLVerifyClient none
SSLCipherSuite RSA-AES-256-SHA:RSA-AES-128-SHA:RSA-3DES-SHA:RSA-RC4- SHA:RSA-RC4-MD5
SSLCertName IS-Console-SSL-Cert
                             <-- Nickname of SSL server certificate
#SSLClCACertName cli01
```

Solaris32/64 Linux32/64

```
# ---- Configuration for SSL ---
AddModule mod_ihs_ssl.c
SSLEnvDir "/etc/opt/FJSVisscs/security/env/smee"       <---Fixed
SSLSlotDir "/etc/opt/FJSVisscs/security/env/smee/slot" <---Fixed
SSLTokenLabel Token01                                  <---Fixed
SSLUserPINFile "/etc/opt/FJSVisgui/cert/upinfile"
                               <---User PIN file having been created by ihsregistupin
SSLExec on
SSLVersion 3-3.1
SSLVerifyClient none
```

```
SSLCipherSuite RSA-AES-256-SHA:RSA-AES-128-SHA:RSA-3DES-SHA:RSA-RC4-SHA:RSA-RC4-MD5
SSLCertName IS-Console-SSL-Cert  <---Nickname of SSL server certificate
#SSLClCACertName cli01
```

11.1.4.3.8 Restart the Interstage HTTP Server for the Interstage Management Console

Windows32/64

Restart the following service:

Interstage Operation Tool (FJapache)

Solaris32/64 Linux32/64

To restart the Interstage HTTP Server for the Interstage Management Console:

1. Use the *kill* command to stop the Interstage HTTP Server process for the Interstage Management Console:

   ```
   # kill 'cat /var/opt/FJSVisgui/tmp/httpd.pid'
   ```

2. Start the Interstage HTTP Server for the Interstage Management Console:

   ```
   # /opt/FJSVihs/bin/httpd -f /etc/opt/FJSVisgui/httpd.conf -s "#ISCONSOLE" -K
   ```

11.1.4.4 Changing the SSL Encrypted Communication Settings

In SSL encryption communication, the SSL protocol version and encryption algorithms that can be used can be changed to improve security.

The procedure for changing the SSL protocol version and encryption algorithms is described below.

Note

Select at least 1 SSL protocol version or encryption algorithm that is implemented by the Web browser so that it can be connected to from the Web browser.

1. 11.1.4.4.1 Edit the Interstage HTTP Server Definition File
2. 11.1.4.4.2 Restart the Interstage HTTP Server for the Interstage Management Console

11.1.4.4.1 Edit the Interstage HTTP Server Definition File

Edit the Interstage HTTP Server definition file for the Interstage Management Console as follows:

Windows32/64

```
# ---- Configuration for SSL ---
AddModule mod_ihs_ssl.c
SSLEnvDir "C:/Interstage/etc/security/env/smee"
SSLSlotDir "C:/Interstage/etc/security/env/smee/slot"
SSLTokenLabel Token01
SSLUserPINFile "c:/Interstage/gui/etc/cert/upinfile"
SSLExec on
SSLVersion 3-3.1     <-- Specify the SSL protocol version (Note)
SSLVerifyClient none
SSLCipherSuite RSA-AES-256-SHA:RSA-AES-128-SHA:RSA-3DES-SHA:RSA-RC4-
SHA:RSA-RC4-MD5     <--Specify the encryption algorithm
```

```
SSLCertName IS-Console-SSL-Cert
#SSLClCACertName cli01
```

Solaris32/64 Linux32/64

```
# ---- Configuration for SSL ---
AddModule mod_ihs_ssl.c
SSLEnvDir "/etc/opt/FJSVisscs/security/env/smee"
SSLSlotDir "/etc/opt/FJSVisscs/security/env/smee/slot"
SSLTokenLabel Token01
SSLUserPINFile "/etc/opt/FJSVisgui/cert/upinfile"
SSLExec on
SSLVersion 3-3.1              <-- Specify the SSL protocol version (Note)
SSLVerifyClient none
SSLCipherSuite RSA-AES-256-SHA:RSA-AES-128-SHA:RSA-3DES-SHA:RSA-RC4-
SHA:RSA-RC4-MD5               <--Specify the encryption algorithm
SSLCertName IS-Console-SSL-Cert
#SSLClCACertName cli01
```

Note: "2", "3","3.1","2-3","2-3.1", or "3-3.1" can be specified for the SSLVersion directive. To prevent connection in SSL2.0, however, specify "3", "3.1", or "3-3.1".

For details on the method to specify and change these, refer to the "How to Use SSL with Interstage HTTP Server" chapter in the Security System Guide.

For details about selecting encryption algorithms, refer to the "Security Trends" appendix in the Security System Guide.

11.1.4.4.2 Restart the Interstage HTTP Server for the Interstage Management Console

Windows32/64

Restart the following service:

Interstage Operation Tool (FJapache)

Solaris32/64 Linux32/64

To restart the Interstage HTTP Server for the Interstage Management Console:

1. Use the *kill* command to stop the Interstage HTTP Server process for the Interstage Management Console:

   ```
   # kill 'cat /var/opt/FJSVisgui/tmp/httpd.pid'
   ```

2. Start the Interstage HTTP Server for the Interstage Management Console:

   ```
   # /opt/FJSVihs/bin/httpd -f /etc/opt/FJSVisgui/httpd.conf -s "#ISCONSOLE" -K
   ```

Chapter 12 Maintenance (Resource Backup)

This chapter explains system maintenance and how to back up resources to protect against resource deterioration or destruction and how to restore resource files from backup copies. This is necessary to protect resources before carrying out system maintenance, moving applications, or performing similar operations.

Maintenance operations can also be executed individually or collectively.

Note

Windows32/64

The descriptions in this chapter are based on the assumption that "C:\Interstage" is the installation directory of Interstage.

12.1 Backing Up and Restoring Resources

This section describes the procedures for backing up resources and for restoring backed up resources in the event of system maintenance and Interstage maintenance, and in an emergency such as when Interstage resources are damaged.

Note

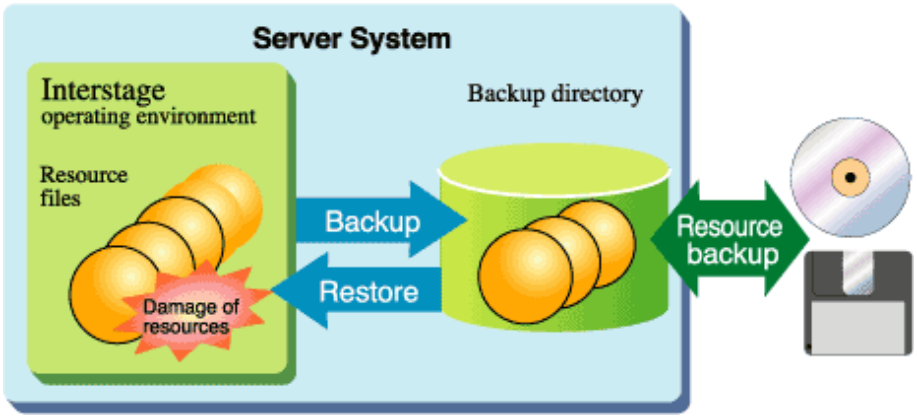
- The backup and restore procedures described in this section can only be executed on the same system. If the resources are moved to another system or if system information (such as hostname, IP address) is modified even within the same machine, resources cannot be restored using the backup/restore procedure described here. For details on moving resources, refer to "12.2 Moving Resources to Another Server".
- The applicable resources for backup/restore are only those files that define the application environment and that are held by Interstage. User applications are not applicable resources, and should be saved as required.

12.1.1 Outline

The backup/restore procedure assists in restoring the application environment when an emergency such as damage to Interstage resources occurs.

The backup/restore procedure for Interstage resources involves backing up (saving) the resource files in the backup directory and restoring the resource files as required (refer to the following figure).

Figure 12.1 Interstage Backup/Restore Procedure



When backing up resources, it is better to save the resources to a removable medium that is not usually accessed rather than to accessible disks on the server system.

To save the latest resource files, execute a backup before the resource file update.

Windows32/64

When upgrading the version or edition of Interstage, backup/restore is not required because the Interstage installer supports the existing resources. However, backing up resources is recommended in case of an emergency.

Note

Solaris32/64 Linux32/64

When saving resources stored in the backup directory on the hard disk to removable storage media in the Solaris/Linux system, save the resources in archive format (using the *tar* or *cpio* command). If the resources are saved with their original file system format (by copying the file), the authority attribute of the file may be changed.

12.1.2 Backup/Restore in a Multiserver Environment Windows32/64 Solaris32 Linux32/64

This section explains Backup/Restore and Import functionality for the Admin Server and the Managed Server in the multiserver environment.

Note

- The recovery of backed up resources that have not been changed on the server is referred to as 'restore', and the recovery of settings (such as IP address and host name) that have been changed is referred to as 'import'.

12.1.2.1 Backup/Restore of the Admin Server

Back up the Admin Server in anticipation of trouble that might occur on the Admin Server. Recovery of the admin server is used for:

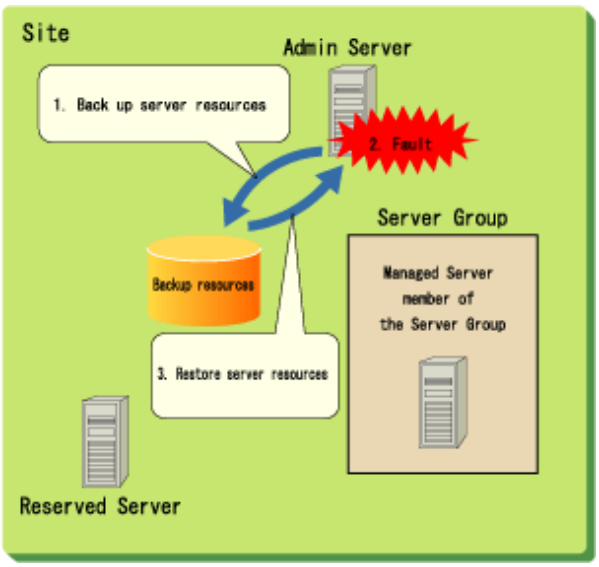
- 12.1.2.1.1 Recovering the Admin Server
- 12.1.2.1.2 Switching the Admin Server Functions to Another Server

12.1.2.1.1 Recovering the Admin Server

Back up the Interstage resources regularly in anticipation of problems that might occur in the Admin Server. If a problem occurs in the Admin Server, recover the server, restore the Interstage resources and then recover the Interstage environment.

The procedure for these tasks is described below.

Figure 12.2 Recovering Admin Server



Preliminary Tasks

1. Use the backup function to back up the Admin Server resources.

   For details of the backup procedure, refer to "12.1.4 Backup Procedure (Admin Server) ".

2. Back up the following resources:

   Interstage Management Console resources

   Interstage JMX Service resources Solaris32 Linux32/64

   Business configuration management resources

   Interstage Directory Service resources

Note

- Interstage Directory Service should only be backed up if the LDAP directory service is used for login authentication.

Recovering the Admin Server

1. Restore the Admin Server resources.
2. Recover the Admin Server on which the trouble occurred, and then restore the Interstage backup resources that were already collected. For details on the restore procedure, refer to "12.1.6 Restore Procedure (for Systems Other than the Admin Server)".

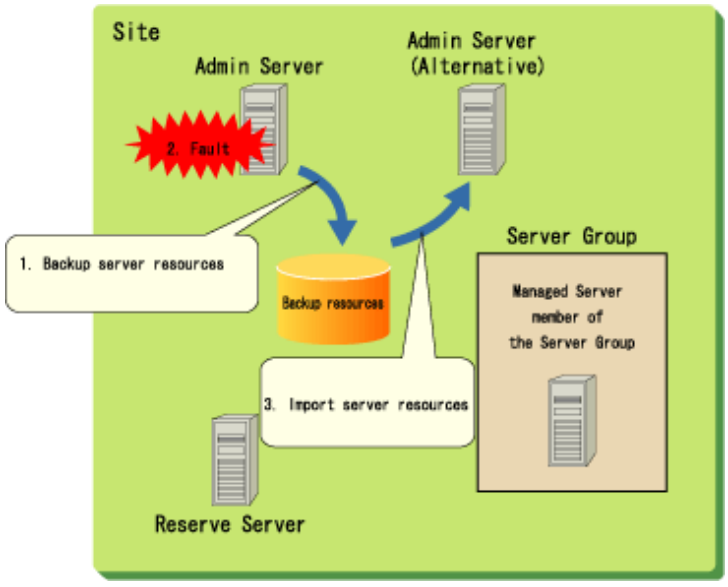
   The target 'restore' and 'backup' functions are the same.

12.1.2.1.2 Switching the Admin Server Functions to Another Server

Back up the Interstage resources regularly in anticipation of trouble that might occur in the Admin Server. If trouble occurs in the Admin Server, and another server is used as an alternative Admin Server, import the Admin Server Interstage resources to the new server.

The procedure for these tasks is described below.

Figure 12.3 Switching Admin Server Functions to Another Server



Preliminary Tasks

1. Use the backup function to back up the Admin Server resources.

   For details of the backup procedure, refer to "12.1.4 Backup Procedure (Admin Server) ".

2. Back up the following resources:

   Interstage Management Console resources

   Interstage JMX Service resources Solaris32 Linux32/64

   Business configuration management resources

   Interstage Directory Service resources

Note

- Interstage Directory Service should only be backed up if the LDAP directory service is used for login authentication.

Setup Tasks for the Admin Server (Alternative Machine)

1. Import the Admin Server resources to the alternative Admin Server.
2. Import the Interstage backup resources that were already collected to the alternative Admin Server. For details on the import procedure, refer to "12.2 Moving Resources to Another Server".

   The target import and backup functions are the same.

12.1.2.2 Backup/Restore of the Managed Server

Backup/Restore and import of the Managed Server are used for the following purposes:

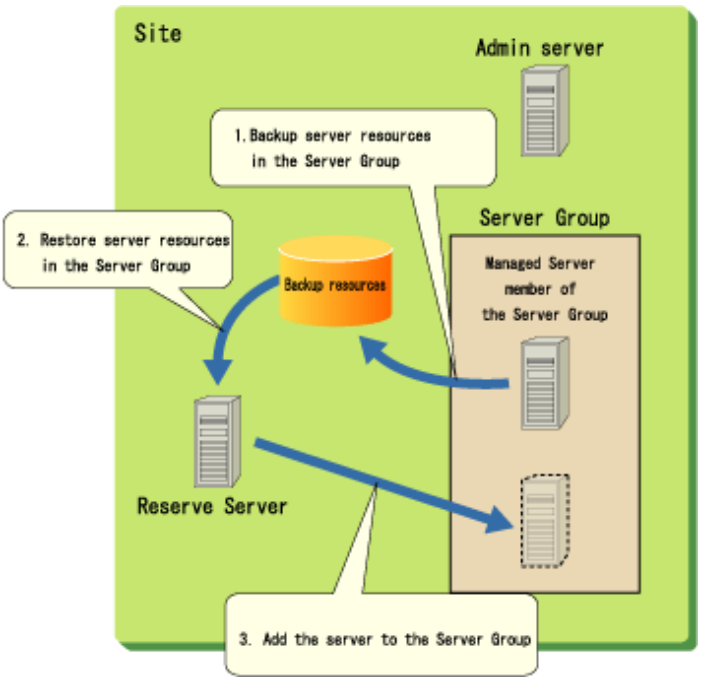
- 12.1.2.2.1 Adding Servers to a Server Group
- 12.1.2.2.2 Recovering a Managed Server

12.1.2.2.1 Adding Servers to a Server Group

To add a Managed Server to the Server Group, the Interstage resources of the Managed Server must match the Interstage resources of any Managed Servers already in the Server Group. For this reason, the backup/import function is used to ensure that the Interstage resources correspond.

The procedure for these tasks is described below.

Figure 12.4 Adding Servers to a Server Group



Preliminary Tasks

1. Use the backup function to back up the resources of Managed Servers that belong to the Server Group.

   For details of the backup procedure, refer to "12.1.5 Backup Procedure (for Systems Other than the Admin Server)".

2. Back up the following resources:

   - Interstage Management Console resources
   - Interstage JMX Service resources Solaris32 Linux32/64
   - Business configuration management resources
   - Interstage Directory Service resources

Adding servers to a Server Group

1. Import the resources of Managed Servers that belong to the Server Group.

   Import the resources that were backed up in Preliminary Tasks to the Reserve Server intended for addition to the Server Group. For details of the import procedure, refer to "12.2 Moving Resources to Another Server".

   The target import and backup functions are the same.

2. Add the Managed Server to the Server Group.

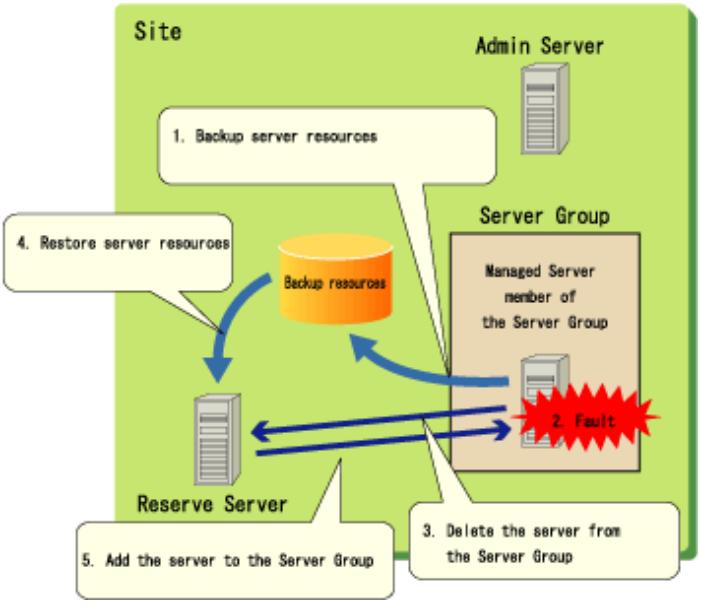
   Add the Managed Server for which the resources were imported to the Server Group.

12.1.2.2.2 Recovering a Managed Server

Back up the Interstage resources regularly in anticipation of trouble that might occur in the Managed Server. If trouble occurs in the Managed Server, recover the server, restore the Interstage resources and then recover the Interstage environment.

The procedure for these tasks is described below.

Figure 12.5 Recovering a Managed Server



Preliminary Tasks

1. Use the backup function to back up the resources of Managed Servers that belong to the Server Group. For details of the backup procedure, refer to "12.1.5 Backup Procedure (for Systems Other than the Admin Server)".

2. Back up the following resources:

   - Interstage Management Console resources

- Interstage JMX Service resources Solaris32 Linux32/64
- Business configuration management resources
- Interstage Directory Service resources

Recovering the Server

1. Delete the Managed Server from the Server Group.

   Delete the Managed Server on which the trouble occurred from the Server Group, and change it to Reserve Server status. For details on deleting Managed Servers from the Server Group, refer to "6.1.1.6 Deleting a Server Group" in the "Server Groups" chapter.

2. Restore the Managed Server resources.

   Recover the server on which the trouble occurred, and then restore the Interstage backup resources that were already collected. For details of the restore procedure, refer to "12.1.6 Restore Procedure (for Systems Other than the Admin Server)".

   The target 'restore' and 'backup' functions are the same.

3. Add the Managed Server to the Server Group.

   Add the Managed Server to the Server Group. For details on adding servers to a Server Group, refer to "6.1.1.4 Adding a Server to a Server Group" in the "Server Groups" chapter.

12.1.2.3 Backup/Restore of a Combined Server

In a Combined Server, the Admin Server function and the Interstage application server function (Managed Server) operate on the same physical machine, and therefore backup involves backing up both. For details concerning backup, restore, and importing, refer to the following:

- 12.1.2.1 Backup/Restore of the Admin Server
- 12.1.2.2 Backup/Restore of the Managed Server

Resources backed up for a Combined Server can be restored and imported only to a Combined Server.

When performing backups, back up the resources for both the Admin Server and the Managed Server at the same time. Also, when restoring and importing, restore the resources for both the Admin Server and the Managed Server.

12.1.3 Resources that can be Backed Up and Restored

Backup and restore can be executed for the resources shown below. For information about backing up or restoring the resources collectively, refer to "12.3 Collective Maintenance".

12.1.3.1 Interstage Setup Resource Files

Windows32/64

```
Interstage system definition
  C:\Interstage\td\etc\isdef\isconf.txt (*1)
Interstage operation environment definition
  C:\Interstage\td\etc\isreg\isinitdef.txt (*1)
Interstage setup resource
  C:\Interstage\td\var\iscom\isegintr.dat
  C:\Interstage\td\var\iscom\iseiinfo.dat
  C:\Interstage\td\var\iscom\iseiippinfo.dat
  C:\Interstage\td\var\iscom\iserodcn.dat (*1)
  C:\Interstage\td\var\iscom\isei_odenvfile (*1)
  C:\Interstage\td\var\iscom\iscmd.lock
  C:\Interstage\td\var\iscom\isjmxservice.ser (*1)
  C:\Interstage\td\var\iscom\isjmxapache.ser (*1)
```

Solaris32/64

```
Interstage system definition
  /etc/opt/FSUNtd/isdef/isconf.txt (*1)
Interstage operation environment definition
  /etc/opt/FSUNtd/isreg/isinitdef.txt (*1)
Interstage setup resource
  /var/opt/FJSVisas/system/default/FJSVisas/var/iscom/isegintr.dat
  /var/opt/FJSVisas/system/default/FJSVisas/var/iscom/iseiinfo.dat
  /var/opt/FJSVisas/system/default/FJSVisas/var/iscom/iseiippinfo.dat
  /var/opt/FJSVisas/system/default/FJSVisas/var/iscom/iserodcn.dat (*1)
  /var/opt/FJSVisas/system/default/FJSVisas/var/isei_odenvfile (*1)
  /var/opt/FJSVisas/system/default/FJSVisas/var/iscom/iscmd.lock
  /var/opt/FJSVisas/system/default/FJSVisas/var/iscom/isjmxservice.ser (*1)
  /var/opt/FJSVisas/system/default/FJSVisas/var/iscom/isjmxapache.ser (*1)
Profile file (*1)
  /opt/FJSVisas/etc/profile/default.txt
```

Linux32/64

```
Interstage system definition
  /etc/opt/FJSVtd/isdef/isconf.txt (*1)
Interstage operation environment definition
  /etc/opt/FJSVtd/isreg/isinitdef.txt (*1)
Interstage setup resource
  /var/opt/FJSVisas/system/default/FJSVisas/var/iscom/isegintr.dat
  /var/opt/FJSVisas/system/default/FJSVisas/var/iscom/iseiinfo.dat
  /var/opt/FJSVisas/system/default/FJSVisas/var/iscom/iseiippinfo.dat
  /var/opt/FJSVisas/system/default/FJSVisas/var/iscom/iserodcn.dat (*1)
  /var/opt/FJSVisas/system/default/FJSVisas/var/iscom/isei_odenvfile (*1)
  /var/opt/FJSVisas/system/default/FJSVisas/var/iscom/iscmd.lock
  /var/opt/FJSVisas/system/default/FJSVisas/var/iscom/isjmxservice.ser (*1)
  /var/opt/FJSVisas/system/default/FJSVisas/var/iscom/isjmxapache.ser (*1)
Profile file (*1)
  /opt/FJSVisas/etc/profile/default.txt
```

*1 Backup is done only when a file exists.

12.1.3.2 Interstage Management Console Resource Files

Windows32/64

```
Environment definition file of Interstage Management Console
  C:\Interstage\gui\etc\config
```

Solaris32/64 Linux32/64

```
Environment definition file of Interstage Management Console
  /etc/opt/FJSVisgui/config
```

12.1.3.3 Interstage JMX Service Resource File

Windows32/64

```
Interstage management console environment definition file
  C:\Interstage\gui\etc\config
Interstage management console Interstage HTTP Server environment definition file
  C:\Interstage\gui\etc\httpd.conf
Environment definition file of Interstage JMX Service
  C:\Interstage\jmx\etc\isjmx.xml
User repository information setting file of Interstage JMX Service
  C:\Interstage\jmx\etc\user-repository.xml
Transaction grid-based manager definition file
  C:\Interstage\jmx\etc\manager-mbean-mappings.xml
Server site ID key subject to transaction grid-based management
  C:\Interstage\jmx\etc\.siteAgent.ser*
Transaction grid-based management server site ID key
  C:\Interstage\jmx\etc\.siteManager.ser*
```

Solaris32/64

```
Environment definition file of Interstage JMX Service
  /etc/opt/FJSVisjmx/isjmx.xml
Transaction configuration management environment definition file
  /etc/opt/FJSVisas/repository/repository.system
User repository information setting file of Interstage JMX Service
  /etc/opt/FJSVisjmx/user-repository.xml
Transaction grid-based manager definition file
  /etc/opt/FJSVisjmx/manager-mbean-mappings.xml
Server site ID key subject to transaction grid-based management
  /etc/opt/FJSVisjmx/.siteAgent.ser*
Transaction grid-based management server site ID key
  /etc/opt/FJSVisjmx/.siteManager.ser*
```

Linux32/64

```
Environment definition file of Interstage JMX Service
  /etc/opt/FJSVisjmx/isjmx.xml
Transaction configuration management environment definition file
  /etc/opt/FJSVisas/repository/repository.system
User repository information setting file of Interstage JMX Service
  /etc/opt/FJSVisjmx/user-repository.xml
Transaction grid-based manager definition file
  /etc/opt/FJSVisjmx/manager-mbean-mappings.xml
Server site ID key subject to transaction grid-based management
  /etc/opt/FJSVisjmx/.siteAgent.ser*
Transaction grid-based management server site ID key
  /etc/opt/FJSVisjmx/.siteManager.ser*
```

* Files are backed up only when they exist.

12.1.3.4 CORBA Service Resource Files

12.1.3.4.1 CORBA Service (ORB)

Windows32/64

```
Server default information
```

```
  C:\Interstage\ODWIN\etc\boa.env
CORBA Service environment definition information
  C:\Interstage\ODWIN\etc\config
Implementation repository
  C:\Interstage\ODWIN\etc\impl.db
Host information
  C:\Interstage\ODWIN\etc\inithost
Initial service
  C:\Interstage\ODWIN\etc\init_svc
Queue control information
  C:\Interstage\ODWIN\etc\queue_policy
CORBA Service environment setting information
  C:\Interstage\ODWIN\var\odenvfile
SSL environment definition file (Note)
  C:\Interstage\ODWIN\etc\ssl.env
```

Solaris32/64

```
Server default information
  /etc/opt/FSUNod/boa.env
CORBA Service environment definition information
  /etc/opt/FSUNod/config
Implementation repository
  /etc/opt/FSUNod/impl.db
Host information
  /etc/opt/FSUNod/initial_hosts
Initial service
  /etc/opt/FSUNod/initial_services
Queue control information
  /etc/opt/FSUNod/queue_policy
CORBA Service environment setting information
  /var/opt/FSUNod/odenvfile
SSL environment definition file (Note)
  /etc/opt/FSUNod/ssl.env
```

Linux32/64

```
Server default information
  /etc/opt/FJSVod/boa.env
CORBA Service environment definition information
  /etc/opt/FJSVod/config
Implementation repository
  /etc/opt/FJSVod/impl.db
Host information
  /etc/opt/FJSVod/initial_hosts
Initial service
  /etc/opt/FJSVod/initial_services
Queue control information                              (*1)
  /etc/opt/FJSVod/queue_policy
CORBA Service environment setting information
  /etc/opt/FJSVod/odenvfile
SSL environment definition file (Note)
  /etc/opt/FJSVod/ssl.env
```

*1 Not valid for Linux (64 bit).

Note

- This file can only be the target when the SSL linkage function is used.

  The slot information directory and the certificate operation control directory are not included.

12.1.3.4.2 Naming Service

Windows32/64

```
Naming service registration information
  C:\Interstage\ODWIN\etc\CosNaming\*
Naming service environment definition information
  C:\Interstage\ODWIN\etc\nsconfig
```

Solaris32/64

```
Naming service registration information
  /etc/opt/FSUNod/CosNaming/*
Naming service environment definition information
  /etc/opt/FSUNod/nsconfig
```

Linux32/64

```
Naming service registration information
  /etc/opt/FJSVod/CosNaming/*
Naming service environment definition information
  /etc/opt/FJSVod/nsconfig
```

12.1.3.4.3 Load Balancing Function (Enterprise Edition only)

This is not valid for Linux (64 bit).

Windows32/64

```
Load balancing function registration information
  C:\Interstage\ODWIN\etc\LBO\*
Loading balancing environment definition information
  C:\Interstage\ODWIN\etc\nslbo.conf
```

Solaris32/64

```
Load balancing function registration information
  /etc/opt/FSUNod/LBO/*
Loading balancing environment definition information
  /etc/opt/FSUNod/nslbo.conf
```

Linux32/64

```
Load balancing function registration information
  /etc/opt/FJSVod/LBO/*
Loading balancing environment definition information
  /etc/opt/FJSVod/nslbo.conf
```

12.1.3.4.4 Interface Repository

Windows32/64

```
Interface repository environment information
  C:\Interstage\ODWIN\etc\irconfig
  C:\Interstage\ODWIN\etc\irpth
Interface repository data (*1)
  C:\Interstage\TD\var\IRDB\irobf.qfl
  C:\Interstage\TD\var\IRDB\irobf.qfp
  C:\Interstage\TD\var\IRDB\irobftran
```

Solaris32/64

```
Interface repository environment information
  /etc/opt/FSUNod/irconfig
  /etc/opt/FSUNod/irpth
  /etc/opt/FSUNod/obfconfig
Interface repository data  (*1)
  /opt/FSUNtd/var/IRDB/irobf.qfl
  /opt/FSUNtd/var/IRDB/irobf.qfp
  /opt/FSUNtd/var/IRDB/irobftran
```

Linux32/64

```
Interface repository environment information
  /etc/opt/FJSVod/irconfig
  /etc/opt/FJSVod/irpth
  /etc/opt/FJSVod/obfconfig
Interface repository data  (*1)
  /opt/FJSVtd/var/IRDB/irobf.qfl
  /opt/FJSVtd/var/IRDB/irobf.qfp
  /opt/FJSVtd/var/IRDB/irobftran
```

*1 The Interface Repository data file can be saved in an arbitrary location.

The above pathname represents the *isinit* command and the default path created when the Interface Repository is constructed (defined by "IR path for DB file" in the Interstage operation environment definition file). The default path, when constructed by the *odadmin* command, is as follows:

Solaris32/64

```
/opt/FSUNod/IRDB
```

Linux32/64

```
/opt/FJSVod/IRDB
```

Note

- The file that specifies the cache object (file set by the parameter select cache obj of the irconfig file) is excluded from the backup subject. Back up or restore the file if necessary.

12.1.3.5 Event Service Resource Files

Windows32/64

```
Event Service configuration information
  C:\Interstage\eswin\etc\group\essystem.cfg
Event channel operation environment (*1)
  C:\Interstage\eswin\etc\group\esgrpX.grp
Event channel group control information
  C:\Interstage\eswin etc\group\esmnggrp.db
Unit information file
  C:\Interstage\eswin\etc\mqd\(unitID).bin
```

Solaris32/64 Linux32/64

```
Event Service configuration information
  /etc/opt/FJSVes/group/essystem.cfg
Event channel operation environment (*1)
  /etc/opt/FJSVes/group/esgrpX.grp
Event channel group control information
  /etc/opt/FJSVes/group/esmnggrp.db
Unit information file
  /etc/opt/FJSVes/mqd/(unitID).bin
```

*1 esgrpX.grp exists only during static generation and application of the event channel. (X is a number.)

12.1.3.6 Portable-ORB Resource Files

Windows32/64

```
Portable-ORB environment definition information
  C:\Interstage\PORB\etc\config  (*1)
Host information
  C:\Interstage\PORB\etc\initial_hosts  (*1)
Initial  service
  C:\Interstage\PORB\etc\initial_services  (*1)
Keystore file
  A file under the storage directory specified in
[keystore storage location] of porbeditenv command (arbitrary)
Embedded certificate control information
  - When specifying a storage directory in -rl option in executing porbMngCert command
     (Specified storage directory)\removelist
  - When not specifying a storage directory in -rl option in executing porbMngCert command
     (The current directory in executing porbMngCert
```

```
command) \removelist
```

Solaris32/64 Linux32/64

```
Portable-ORB environment definition information
  /etc/opt/FJSVporb/config  (*1)
Host information
  /etc/opt/FJSVporb/initial_hosts  (*1)
Initial  service
  /etc/opt/FJSVporb/initial_services  (*1)
Keystore file
  A file under the storage directory specified in [keystore storage
location] of porbeditenv command (arbitrary)
Embedded certificate control information
  - When specifying a storage directory in -rl option in executing
porbMngCert command
     (Specified storage directory)/removelist
  - When not specifying a storage directory in -rl option in executing
porbMngCert command
     (The current directory in executing porbMngCert command) /removelist
```

*1 In the situation in which Portable-ORB is downloaded, PORB_HOME is located under the document root folder of the web server.

12.1.3.7 Component Transaction Service Resource Files

Windows32/64

```
Interstage definition file
  C:\Interstage\etc\isconfig.xml
System Environment Definition
  C:\Interstage\td\etc\sysdef
Setup information
  C:\Interstage\td\var\td001\def\cwb\*.cwb (*1)
  C:\Interstage\td\var\td001\def\wu\*.wu (*1)
  C:\Interstage\td\var\td001\def\wu\*.def (*1)
Wrapper attribute information Windows32
  C:\Interstage\td\atrbinf\*.*
User created APM
  C:\Interstage\extp\bin\extp_apm*.*
User authentication / Access control information
  C:\Interstage\td\sys\aso\.manager
```

Solaris32/64

```
Interstage definition file
  /etc/opt/FJSVisas/isconfig.xml
System Environment Definition
  /var/opt/FSUNtd/etc/sysdef
Setup information
  /var/opt/FJSVisas/system/default/FSUNextp/td001/def/cwb/*.cwb (*1)
  /var/opt/FJSVisas/system/default/FSUNextp/td001/def/wu/*.wu (*1)
  /var/opt/FJSVisas/system/default/FSUNextp/td001/def/wu/*.def (*1)
Wrapper attribute information Solaris32
  /var/opt/FSUNtd/atrbinf/*
User created APM
  /opt/FSUNextp/bin/extp_apm*.*
```

```
User authentication / Access control information
  /var/opt/FSUNtd/sys/aso/.manager
```

Linux32/64

```
Interstage definition file
  /etc/opt/FJSVisas/isconfig.xml
System Environment Definition
  /var/opt/FJSVtd/etc/sysdef
Setup information
  /var/opt/FJSVisas/system/default/FJSVextp/td001/def/cwb/*.cwb (*1)
  /var/opt/FJSVisas/system/default/FJSVextp/td001/def/wu/*.wu (*1)
  /var/opt/FJSVisas/system/default/FJSVextp/td001/def/wu/*.def (*1)
User created APM
  /opt/FSUNextp/bin/extp_apm*.*
```

*1 This directory can vary depending on the setup contents of "TD path for system" in the Interstage operation environment definition.

12.1.3.8 Database Linkage Service Resource Files Windows32/64 Solaris32 Linux32/64

Windows32/64

```
System environment setup file
  C:\Interstage\ots\etc\config
Tuning information setup file
  C:\Interstage\ots\etc\ots.ini
sysconfig file
  C:\Interstage\ots\etc\sysconfig (*1)
RMP property
  C:\Interstage\ots\etc\RMP.properties
system information file
  C:\Interstage\ots\systeminfo\system (*2)
Setup information
  All files under C:\Interstage\ots\etc\repository (*3)
```

Solaris32

```
System environment setup file
  /opt/FSUNots/etc/config
sysconfig file
  /opt/FSUNots/etc/sysconfig (*1)
RMP property
  /opt/FSUNots/etc/RMP.properties
system information file
  /opt/FSUNots/systeminfo/system (*2)
Setup information
  All files under /opt/FSUNots/etc/repository (*3)
```

Linux32/64

```
System environment setup file
  /opt/FJSVots/etc/config
sysconfig file
```

```
  /opt/FJSVots/etc/sysconfig (*1)
RMP property
  /opt/FJSVots/etc/RMP.properties
system information file
  /opt/FJSVots/systeminfo/system (*2)
Setup information
  All files under /opt/FJSVots/etc/repository (*3)
```

*1 This file is generated by the *otssetup* command. It contains the information specified in the setup information file.

*2 This file contains information required for the Database Linkage Service to operate.

*3 The resource definition file registered by the *otssetrsc* command and other files are stored.

- To back up the resources of the Database Linkage Service, the CORBA Service resource file must also be backed up at the same time. For details, refer to "12.1.3.4 CORBA Service Resource Files".

12.1.3.9 Interstage Single Sign-on Resource Files

12.1.3.9.1 Repository Server Resource Files

This is not valid for Standard-J Edition on Windows (64 bit).

This is not valid for Standard-J Edition on Linux (64 bit).

Windows32/64

```
Repository server definition files
All files under:
   C:\Interstage\F3FMsso\ssoatcsv\conf
```

Solaris32/64 Linux32/64

```
Repository server definition files
All files under:
   /etc/opt/FJSVssosv/conf
```

12.1.3.9.2 Authentication Server Resource Files

Windows32/64

```
Authentication server definition files.
All files under:
   C:\Interstage\F3FMsso\ssoatcag\conf

Message files displayed in the web browser.
All files under:
   C:\Interstage\F3FMsso\ssoatcag\pub\template
   C:\Interstage\F3FMsso\ssoatcag\webapps\winauth\custom\page

Integrated Windows Authentication application resources
   C:\Interstage\F3FMsso\ssoatcag\webapps\winauth\WEB-INF\web.xml
```

Solaris32/64 Linux32/64

```
Authentication server definition files.
All files under:
   /etc/opt/FJSVssoac/conf

Message files displayed in the web browser.
All files under:
   /etc/opt/FJSVssoac/pub/template
   /etc/opt/FJSVssoac/webapps/winauth/custom/page

Integrated Windows Authentication application resources
   /etc/opt/FJSVssoac/webapps/winauth/WEB-INF/web.xml
```

12.1.3.9.3 Business Server Resource Files

Windows32/64

```
Business server definition files.
All files under:
   C:\Interstage\F3FMsso\ssoatzag\conf

Message files displayed in the web browser.
All files under:
   C:\Interstage\F3FMsso\ssoatzag\pub\template
```

Solaris32/64 Linux32/64

```
Business server definition files.
All files under:
   /etc/opt/FJSVssoaz/conf

Message files displayed in the web browser.
All files under:
   /etc/opt/FJSVssoaz/pub/template
```

12.1.3.10 Interstage HTTP Server Resource File

Windows32/64

```
Environment definition file of the Interstage HTTP Server
  C:\Interstage\F3FMihs\etc\.servers.conf
  All files under [C:\Interstage\F3FMihs\servers\(Web Server name)\conf] directory
Password file (arbitrary)                                          (*1)
  Files specified in the environment definition file (httpd.conf) AuthGroupFile directive and
AuthUserFile directive
Public root directory                                              (*2)
  Directory specified in the environment definition file (httpd.conf)
  DocumentRoot directive
```

Solaris32/64 Linux32/64

```
Environment definition file of the Interstage HTTP Server
```

```
  /etc/opt/FJSVihs/etc/.servers.conf
  /etc/opt/FJSVihs/boot/FJapache
  All files under [/var/opt/FJSVihs/servers/(Web Server name)/conf] directory
Password file (arbitrary)                                    (*1)
  Files specified in the environment definition file (httpd.conf) AuthGroupFile directive and
AuthUserFile directive
Public root directory                                        (*2)
  Directory specified in the environment definition file (httpd.conf) DocumentRoot directive
```

*1 This applies in the following case:

When the *ihsbackup* command is executed, the -t pass|all option is specified, and user authorization is carried out.

*2 This applies in the following case:

When the *ihsbackup* command is executed, the -t all option is specified.

12.1.3.11 J2EE Common Resource Files

Windows32/64

```
Interstage J2EE common resource files

All files in
   C:\Interstage\J2EE\def
All files in
   C:\Interstage\J2EE\etc
All files in
   C:\Interstage\J2EE\var
```

Solaris32/64 Linux32/64

```
Interstage J2EE common resource files

All files in
   /etc/opt/FJSVj2ee/def
All files in
   /etc/opt/FJSVj2ee/etc
All files in
   /var/opt/FJSVj2ee
```

12.1.3.12 IJServer Resource Files

Windows32/64

```
Common resources
  Data under C:\Interstage\F3FMjs5\conf\jk2
IJServer resources V9 and IJServer resources
  Environment definition file under [J2EE common directory]\ijserver\[IJServer name] directory
  Data under [J2EE common directory]\ijserver\[IJServer name]\conf directory
  Data under [J2EE common directory]\ijserver\[IJServer name]\apps directory
  Data under [J2EE common directory]\ijserver\[IJServer name]\distribute directory
  Data under [J2EE common directory]\ijserver\[IJServer name]\Shared directory
  Data under [J2EE common directory]\ijserver\[IJServer name]\ext directory

IJServer resources before V7/V8
  Environment definition file under [J2EE common directory]\ijserver\[IJServer name] directory
```

```
  Data under [J2EE common directory]\ijserver\[IJServer name]\apps directory
  Data under [J2EE common directory]\ijserver\[IJServer name]\distribute directory
  Data under [J2EE common directory]\ijserver\[IJServer name]\Shared directory
  Data under [J2EE common directory]\ijserver\[IJServer name]\ext directory

IJServer resources for V6
  Environment definition file under [J2EE common directory]\ijserver\[IJServer name] directory
  Data under [J2EE common directory]\ijserver\[IJServer name]\webapps directory
  Data under [J2EE common directory]\ijserver\[IJServer name]\ejbapps directory
  Data under [J2EE common directory]\ijserver\[IJServer name]\client directory
  Data under [J2EE common directory]\ijserver\[IJServer name]\common directory
  Data under [J2EE common directory]\ijserver\[IJServer name]\distribute directory
  Data under [J2EE common directory]\ijserver\[IJServer name]\ext directory
```

Solaris32/64 Linux32/64

```
Common resources
  Data under /etc/opt/FJSVjs5/conf/jk2

IJServer resources V9 and IJServerresources
  Environment definition file under [J2EE common directory]/ijserver/[IJServer name] directory
  Data under [J2EE common directory]/ijserver/[IJServername]/conf  directory
  Data under [J2EE common directory]/ijserver/[IJServername]/apps  directory
  Data under [J2EE common directory]/ijserver/[IJServername]/distribute directory
  Data under [J2EE common directory]/ijserver/[IJServername]/Shared directory
  Data under [J2EE common directory]/ijserver/[IJServername]/ext directory

IJServer resources before V7/V8
  Environment definition file under [J2EE common directory]/ijserver/[IJServer name] directory
  Data under [J2EE common directory]/ijserver/[IJServername]/apps  directory
  Data under [J2EE common directory]/ijserver/[IJServername]/distribute directory
  Data under [J2EE common directory]/ijserver/[IJServername]/Shared directory
  Data under [J2EE common directory]/ijserver/[IJServername]/ext directory
IJServer resources for V6
  Environment definition file under [J2EE common directory]/ijserver/[IJServer name] directory
  Data under [J2EE common directory]/ijserver/[IJServername]/webapps  directory
  Data under [J2EE common directory]/ijserver/[IJServername]/ejbapps directory
  Data under [J2EE common directory]/ijserver/[IJServername]/client directory
  Data under [J2EE common directory]/ijserver/[IJServername]/common directory
  Data under [J2EE common directory]/ijserver/[IJServername]/distribute directory
  Data under [J2EE common directory]/ijserver/[IJServername]/ext directory
```

Note

- Web applications anywhere on the server are not backed up using the *ijsbackup* command. These must be backed up separately.

12.1.3.13 Interstage JMS Resource Files

Windows32/64

```
JNDI definition file
  C:\Interstage\JMS\etc\fjmsjndi.ser.*
JMS nonvolatile file (*1)
  C:\Interstage\JMS\etc\fjmsmng.ser.*
  C:\Interstage\JMS\etc\dsub\fjmsdsubXXXX.ser
  C:\Interstage\JMS\etc\dsub\lock\.XXXX
```

```
Cluster environmental definition file (*2)
  C:\Interstage\JMS\etc\fjmscluster.ser
```

Solaris32/64 Linux32/64

```
JNDI definition file
  /etc/opt/FJSVjms/fjmsjndi.ser.*
JMS nonvolatile file (*1)
  /etc/opt/FJSVjms/fjmsmng.ser.*
  /etc/opt/FJSVjms/dsub/fjmsdsubXXXX.ser
  /etc/opt/FJSVjms/dsub/lock/.XXXX
Cluster environmental definition file (*2)
  /etc/opt/FJSVjms/fjmscluster.ser
```

*1 jmsdsubXXXX.ser and .XXXX are existent only when JMS applications run in nonvolatile operation mode (X is a digit).

*2 fjmscluster.ser exists only in a cluster environment.

12.1.3.14 Interstage Directory Service Resource Files

The Interstage Directory Service resource files are different depending on whether a standard database or a relational database (RDB) is used as the repository database.

12.1.3.14.1 Using a Standard Database

```
Repository Environment
   Environment definition information required for the operation of each
repository of Interstage Directory Service.
Repository Data
   Repository directory created with Interstage Directory Service (*1)
```

 Example

Windows32/64

```
C:\Interstage\Enabler\EnablerDStores\IREP\rep001\data
```

Solaris32/64

```
/var/opt/FJSVena/EnablerDStores/FJSVirep/rep001/data
```

Linux32/64

```
/var/opt/FJSVena/DStores/FJSVirep/rep001/data


Access log
   Access log directory created with Interstage Directory Service (*2)
```

Example

Windows32/64

```
C:\Interstage\IREP\var\rep001\log
```

Solaris32/64 Linux32/64

```
/var/opt/FJSVirep/rep001/log
```

*1 Directory specified as [Database Storage Directory] of each repository when the repositories were created from Interstage Management Console.

*2 Directory specified as [Access Log Directory] in the access log settings of each repository when the repositories were created from the Interstage Management Console.

12.1.3.14.2 Using RDB

If RDB is used, repository data in the Interstage Directory Service resources is managed by RDB. In addition to the Interstage Directory Service backup function, the RDB backup function must also be used for backup.

Interstage Directory Service backup function target resources

Windows32/64

```
Repository environment
Environment definition information required for running each Interstage Directory Service repository

Access log
Directory of the access log created in Interstage Directory Service (*1)
Example: C:\Interstage\IREP\var\rep001\log
```

Solaris32/64

```
Repository environment
Environment definition information required for running each Interstage Directory Service repository

Access log
Directory of the access log created in Interstage Directory Service (*1)
Example: /var/opt/FJSVirep/rep001/log
```

Linux32/64

```
Repository environment
Environment definition information required for running each Interstage Directory Service repository

Access log
Directory of the access log created in Interstage Directory Service (*1)
Example: /var/opt/FJSVirep/rep001/log
```

*1 This is the directory specified in [Directory] of the repository access log definition after the repository is created using the Interstage Management Console.

Resources Saved Using the RDB (Symfoware/RDB) Backup Function

Save the resources shown below.

```
Database space information on the disk, and disk (volume) configuration information
The database name specified when the database was created, the database
space information list, and disk configuration information (*1)
Table DSI
All table DSI created using the irepgendb or irepcrttbl command (*2)
RDB dictionaries
Archive logs (*3)
```

Note

- Make a note of the database name specified when the database was created and the database space information list.
- For details on how to obtain table DSI created using the *irepgendb* or *irepcrttbl* command, refer to "12.1.5.16 Backing Up Interstage Directory Service Resources".
- These are saved when the archive log application is used.

Resources Saved Using the RDB (Oracle Database) Backup Function

Save the resources shown below.

```
Data files
Control files
Temporary log files
REDO log files
Password files and important files such as PFILE files
Configuration files required to connect to the Oracle database (listener.ora, tnsnames.ora etc.)
```

Back up database resources not shown above according to the database configuration and operating method.

12.1.3.14.3 The Relationship between the Backup/Restore Command Options Provided in Interstage Directory Service and their Target Resources

The table below lists the Interstage Directory Service backup/restore command (*irepbacksys* / *ireprestsys*) options and the target resource relationship.

Using a Standard Database

Target resource	Command option		
	None specified	-confonly	-dataonly
Repository environment	1	1	2
Repository data	1	2	1
Access log	1	2	2

Using RDB

Target resource	Command option		
	None specified	-confonly	-dataonly
Repository environment	1	1	
Access log	1	2	

1 The target resource can be backed up/restored.

2 The target resource cannot be backed up/restored.

Note

Connection Information Settings of the Entry Administration Tool cannot be backed up.

- Windows32/64

  The relationship settings between the repository and the RDB in the *irepadmin* command are not a target of the backup.

- Solaris32/64 Linux32/64

  The *irepadmin* command automatic start settings are not a target of the backup.

12.1.3.15 Interstage Certificate Environment Resource Files

Interstage Certificate Environment resource files are classified into the following two types:

- Certificate environment files
- SSL configuration files.

Windows32/64

Certificate environment files

All files under:

```
C:\Interstage\etc\security\env
```

SSL configuration files

All files under:

```
C:\Interstage\etc\security\sslconf
```

Solaris32/64 Linux32/64

Certificate environment files

All files under:

```
/etc/opt/FJSVisscs/security/env
```

SSL configuration files

All files under:

```
/etc/opt/FJSVisscs/security/sslconf
```

12.1.4 Backup Procedure (Admin Server) Windows32/64 Solaris32 Linux32/64

This section explains the backup procedure for Interstage resources on the Admin Server.

Back up the following resources:

- Interstage Management Console resources
- Solaris32 Linux32/64

  Interstage JMX Service resources
- Business configuration management resources
- Interstage Directory Service resources

Note

- Interstage Directory Service should only be backed up if the directory service is used for login authentication.

This section explains the directory for storing backup resources as the following directories:

Windows32/64

```
X:\Backup
```

Solaris32 Linux32/64

```
/backup
```

Before starting the backup, check there is enough disk space in the backup directory for storing backup resources.

The disk space required for storing backup resources is the total amount indicated for backup target resources in Overview and Target Files.

Operation Procedure

Back up the resources according to the following procedure.

Stopping Services

Stop the service as follows:

- Interstage Directory Service

  This is not valid for Standard-J Edition on Windows (64 bit).

  This is not valid for Standard-J Edition on Linux (64 bit).

  Windows32/64

  Stop this using one of the following:

  - Using the Interstage Management Console, click [Application Management] > [Interstage Management Console] > [Interstage Application Server] > [Security] > [Repository] > [Repository: Status].
  - Use the Windows(R) service "Interstage Directory Service(%s1)".

    %s1 is the repository name.

Solaris32 Linux32/64

Stop this using one of the following:

- Using the Interstage Management Console, click [Application Management] > [Interstage Management Console] > [Interstage Application Server] > [Security] > [Repository] > [Repository: Status].
- Use the *irepstop* command. Specify the repository name to be stopped in the -R option.

- Interstage Management Console and Interstage JMX Service

Windows32/64

- Use the Windows(R) service 'Interstage Operation Tool'.

Solaris32 Linux32/64

- Use the *ismngconsolestop* command

Creating the Directory for Storing Backup Resources

Create one directory for storing Interstage backup resources. The Interstage backup resources are stored under this directory.

Windows32/64

```
mkdir X:\Backup
```

Solaris32 Linux32/64

```
mkdir /backup
```

Note

- Check that there is sufficient disk space for creating the directory for storing backup resources. The disk space required for storing backup resources is the total amount indicated for backup target resources in Overview and Target Files.

Backing up Resources

The procedure for backing up resources is the same as for that described in 12.1.5 Backup Procedure (for Systems Other than the Admin Server) below. For other backup methods, refer to the following sections:

- 12.1.5.4 Backing Up Interstage Management Console Resources
- 12.1.5.5 Backing Up Interstage JMX Service Resource
- 12.1.5.16 Backing Up Interstage Directory Service Resources

Confirming the 8.3 Format Short Name of the Interstage Installation Directory

Confirm the 8.3 format short name of the Interstage installation directory. Refer to "12.1.5.18 8.3 Format (Short Name) of the Interstage Installation Directory" later in this chapter.

Starting Up the Services

Start services that were stopped before processing.

12.1.5 Backup Procedure (for Systems Other than the Admin Server)

This section explains Interstage resource backup procedures.

Windows32/64

It explains on the assumption that it backs up to a folder for backup resources storing called X:\Backup.

Solaris32/64 Linux32/64

It explains on the assumption that it backs up to a directory for backup resources storing called /backup.

12.1.5.1 Stopping Interstage Services

Windows32/64

Log in with Administrator authority and use the *isstop* command to stop all services and the server application.

```
isstop -f
```

Solaris32/64 Linux32/64

Use the *isstop* command to stop all services and the server application.

```
isstop -f
```

Note

- Services that are not stopped by the *isstop* command must be stopped separately as described below.

12.1.5.1.1 Stopping the Interstage HTTP Server

If the connection with Interstage has not been set, stop the Interstage HTTP Server using to either of the following methods:

Windows32/64

- In the Interstage Management Console, click [System] > [Services] > [Web Server] > [Web Server: View list of the Web Server], and then stop all web servers.
- Stop all web servers using the *ihsstop* command.

```
ihsstop -all
```

- Stop the Windows(R) "FJapache" service and "Interstage HTTP Server(Web Server name)".

Solaris32/64 Linux32/64

- In the Interstage Management Console, click [System] > [Services] > [Web Server] > [Web Server: View list of the Web Server], and then stop all web servers.
- Stop all web servers using the *ihsstop* command.

```
/opt/FJSVihs/bin/ihsstop -all
```

12.1.5.1.2 Stopping the Interstage Management Console and Interstage JMX Service

Windows32/64

- Use the Windows(R) service 'Interstage Operation Tool'.

Solaris32/64 Linux32/64

- Use the *ismngconsolestop* command

12.1.5.1.3 Stopping the Interstage Directory Service

Windows32/64

Application Management

Interstage > Interstage Application Server > Security > Repository	View Status

Standalone

Interstage > Interstage Application Server > System > Services > Repository	View Status

To stop the service:

1. Check the check box to the left of repositories to be stopped.
2. Click the **Stop** button.

Note

- Alternately, stop the service as follows:
  - Windows32/64

    Stop the 'Interstage Directory Service(%s1),' Windows® service,

    where %s1 is the repository name.
  - Solaris32/64 Linux32/64

    Use the *irepstop* command to stop the service. The -R option specifies the repository name to stop.

  Example

```
/opt/FJSVirep/bin/irepstop -R rep001
```

  For details on the *irepstop* command, refer to the Reference Manual (Command Edition).

12.1.5.2 Creating a Backup Resource Directory

Create a directory used to store Interstage backup resources. Interstage backup resources are stored under this directory.

Windows32/64

```
mkdir X:\Backup
```

Solaris32/64 Linux32/64

```
mkdir /backup
```

Note

- Ensure in advance that the disk on which a backup resource directory is to be created has enough free space. The size of disk space required for storing backup resources is the total sum of the amounts of backup resources shown in "12.1.1 Outline".

12.1.5.3 Backing Up Interstage Setup Resource

This section explains the setup resource backup procedure that is created on Interstage initialization using the *isinit* command.

Backup Command

The following command is used for backing up the Interstage setup resource:

Windows32/64

```
C:\Interstage\bin\iscbackupsys.exe
```

Solaris32/64

```
/opt/FSUNtd/bin/iscbackupsys
```

Linux32/64

```
/opt/FJSVtd/bin/iscbackupsys
```

The *iscbackupsys* command must be executed while Interstage is stopped.

Backup Procedure

Windows32/64

An example is shown below when the resource backup destination folder is "X:\Backup ".

Execute the *iscbackupsys* command.

```
iscbackupsys  X:\Backup
```

Solaris32/64 Linux32/64

An example is shown below where the resource backup destination directory is /backup/isc.

Execute the *iscbackupsys* command.

```
iscbackupsys /backup
```

- If the path of the backup directory includes a space, the path must be enclosed in double quotes when it is specified for a command parameter.
- If Interstage is running, enter the *isstop -f* command to stop it in advance. For a cluster system, stop it according to the cluster system stop procedure.
- The *iscbackupsys* command creates an "isc" directory under the backup directory and backs up Interstage setup resources under the "isc" directory. If a directory or file named "isc" already exists, delete it before executing this command.

12.1.5.4 Backing Up Interstage Management Console Resources

This section explains the Interstage Management Console resource backup procedure.

Backup Command

The following command is used for backing up of the Interstage Management Console resource:

Windows32/64

```
C:\Interstage\gui\bin\isguibackup.bat
```

Solaris32/64

```
/opt/FJSVisgui/bin/isguibackup
```

The *isguibackup* command must be executed when Interstage is stopped. For command details, refer to the Reference Manual (Command Edition).

Backup Procedure

Before the *isguibackup* command is executed, a directory must be created in the resource backup directory for the Interstage Management Console storage.

Windows32/64

An example is shown below where the Interstage installation path is 'C:\Interstage' and the resource backup destination folder is 'X:\Backup\isgui'

1. Create the folder for storing the Interstage Management Console resources.

   ```
   mkdir  X:\Backup\isgui
   ```

2. Execute the *isguibackup* command.

   ```
   C:\Interstage\gui\bin\isguibackup  C:\Interstage  X:\Backup\isgui
   ```

Solaris32/64

An example is shown below where the resource backup destination directory is /backup/isgui.

1. Create a backup directory.

   ```
   mkdir  /backup/isgui
   ```

2. Execute the *isguibackup* command.

   ```
   isguibackup  /backup/isgui
   ```

Linux32/64

Use the *cp* or other command to copy the resource files of the Interstage Management Console to the backup directory.

The following shows an example of operation when the resource backup directory is /backup/isgui:

1. Create a backup directory to store the resource files of the Interstage Management Console.

```
mkdir  /backup/isgui
```

2. Use the *cp* or other command to copy the resource files of the Interstage Management Console to the backup directory.

```
cp -p /etc/opt/FJSVisgui/config /backup/isgui
```

Note

- Perform the backup only when the directory under the backup directory is empty
- When Interstage is running, stop Interstage with the *isstop -f* command
- This backup operation need not be executed if the Interstage Management Console has not been customized.
- If any message is output before the command termination message is output, execution of the command has ended with failure. In this case, execute the command again referring to the details in the output message and these 'Notes' during execution.
- If the backup directory name contains a whitespace character, the parameter must be enclosed in " " (double-quotation marks).

12.1.5.5 Backing Up Interstage JMX Service Resource

This section explains the Interstage JMX Service resource backup procedure.

Backup Command

Use the following command for the backup of the Interstage JMX Service resource:

Windows32/64

```
C:\Interstage\bin\isjmxbackup.bat
```

Solaris32/64 Linux32/64

```
/opt/FJSVisjmx/bin/isjmxbackup
```

You must execute the *isjmxbackup* command while Interstage and the Interstage JMX service stop. For details on the command, refer to the Reference Manual (Command Edition).

Backup Procedure

Before executing the *isjmxbackup* command, you need to create a directory for storing the Interstage JMX service resources in the resource backup destination directory.

An operation example when the resource backup destination directory is /backup and the directory storing the resources of the operation tools is "/backup/isjmx" is shown below.

1. Create the directory storing the resources of the operation tools.

```
mkdir  /backup/isjmx
```

2. Execute the *isjmxbackup* command.

```
isjmxbackup  /backup/isjmx
```

Note

- Perform the backup while the directory storing the Interstage JMX service resources is empty.
- When Interstage is operational, stop Interstage by the *isstop -f* command.
- When the Interstage JMX service is operational, stop the Interstage JMX service by the *isjmxstop* command.
- When the environment definition of the Interstage JMX service has not been customized, it is not necessary to perform the backup.
- A message output before the command end message is an indication that the execution of the command failed. In such a case, re-execute the command according to the output message and notes on executing the command.
- When the path of the directory storing the Interstage JMX service resources includes a blank, enclose the blank with double quotation marks (") on specifying the command parameter.

Windows32/64

- Stop the 'Interstage Operation Tool' service and the 'Interstage JServlet(OperationManagement)' service while the Interstage JMX service is operating

Solaris32/64 Linux32/64

- During operation of the Interstage JMX service, use the *isjmxstop* command to stop the Interstage JMX service.

Solaris32

- The Interstage JMX service does not support the multisystem function. Therefore, operations for the extended systems are not required.

12.1.5.6 Backing Up CORBA Service Resource

This section explains the CORBA Service resource backup procedure.

Backup Command

The following command is used for backing up the CORBA Service resource:

Windows32/64

```
C:\Interstage\ODWIN\bin\odbackupsys.exe
```

Solaris32/64

```
/opt/FSUNod/bin/odbackupsys
```

Linux32/64

```
/opt/FJSVod/bin/odbackupsys
```

The *odbackupsys* command must be executed when the CORBA Service is stopped.

Backup Procedure

Windows32/64

An example is shown below where the backup destination path is X:\Backup\OD.

The *odbackupsys* command is executed, and the CORBA Service resource file is backed up.

```
odbackupsys X:\Backup
```

Solaris32/64

An example is shown below where the backup destination path is /backup/FSUNod.

The *odbackupsys* command is executed, and the CORBA Service resource file is backed up.

```
odbackupsys  /backup
```

Linux32/64

An example is shown below where the backup destination path is /backup/FJSVod.

The *odbackupsys* command is executed, and the CORBA Service resource file is backed up.

```
odbackupsys  /backup
```

Note

- The *odbackupsys* command creates a directory under the specified backup destination path and makes a backup copy of the CORBA Service resources under the directory.

  If the following directory already exists, perform the operation after deleting the directory:

  - Windows32/64

    OD

  - Solaris32/64

    FSUNod

  - Linux32/64

    FJSVod

- When using the SSL linkage function, save the following resources in the backup directory:

  - Slot information directory (directory specified in -sd option of *odsetSSL* command)
  - Operation control directory (directory specified in -ed option of *odsetSSL* command)
  - Windows32/64 Solaris32/64

    SSL environment definition file (ssl.env file).

12.1.5.7 Backing Up Event Service Resource

This section explains the backup procedure for the Event Service resource.

Backup Command

The following command is used for backing up the Event Service resource:

Windows32/64

```
C:\Interstage\bin\esbackupsys.exe
```

Solaris32/64 Linux32/64

```
/opt/FJSVes/bin/esbackupsys
```

The *esbackupsys* command must be executed when the Event Service is stopped.

Backup Procedure

Windows32/64

An example is shown below where the backup destination path is X:\Backup\ES.

Execute the *esbackupsys* command to back up the Event Service resource.

```
esbackupsys -d X:\Backup
```

Solaris32/64 Linux32/64

An example is shown below where the backup destination path is /backup/FJSVes.

Execute the *esbackupsys* command to back up the Event Service resource.

```
esbackupsys -d /backup
```

Note

- The *esbackupsys* command creates a directory under the specified backup destination path and makes a backup copy of the Event Service resources under the directory.

  If the following directory already exists, perform the operation after deleting the directory:

  - Windows32/64

    ES

  - Solaris32/64 Linux32/64

    FJSVes

12.1.5.8 Backing Up Portable-ORB Resource

This section explains the Portable-ORB resource backup procedure.

Backup Procedure

Windows32/64

An example is shown below where the backup destination path is X:\Backup\PORB.

1. Create a backup directory.

```
mkdir  X:\Backup\PORB
```

2. Copy the Portable-ORB resource to the backup directory using the *copy* command (or Explorer). (*1)

```
copy  %PORB_HOME%\etc\config  X:\Backup\PORB
copy  %PORB_HOME%\etc\initial_hosts  X:\Backup\PORB
copy  %PORB_HOME%\etc\initial_services  X:\Backup\PORB
```

Solaris32/64 Linux32/64

An example is shown below where the backup destination path is /backup/porb.

1. Create a backup directory.

```
mkdir  /backup/porb
```

2. Copy the Portable-ORB resource to the backup directory using the *cp* command. (*1)

```
cp -p $PORB_HOME/etc/config  /backup/porb
cp -p $PORB_HOME/etc/initial_hosts  /backup/porb
cp -p $PORB_HOME/etc/initial_services  /backup/porb
```

*1 When downloading the Portable-ORB, when multiple PORB_HOME were specified, all must be backed up. When doing so, change the backup destination path so that overwriting will not take place.

Note

When using the SSL linkage function, make copies to the backup directory of the resources below (for details on the files, refer to "12.1.3.6 Portable-ORB Resource Files"):

- Keystore file
- Embedded certificate control information.

12.1.5.9 Backing Up Component Transaction Service Resource

This section explains the backup procedure for the Component Transaction Service resource.

Backup Command

The following command is used for backing up the Component Transaction Service resource:

Windows32/64

```
C:\Interstage\bin\tdbackupsys.exe
```

Solaris32/64

```
/opt/FSUNtd/bin/tdbackupsys
```

Linux32/64

```
/opt/FJSVtd/bin/tdbackupsys
```

The *tdbackupsys* command must be executed while Interstage is stopped.

Backup Procedure

Windows32/64

An example where the resource backup destination folder is X:\Backup\ is shown below.

Execute the *tdbackupsys* command.

```
tdbackupsys  X:\Backup\
```

Solaris32/64 Linux32/64

An example where the resource backup destination directory is /backup/td is shown below.

Execute the *tdbackupsys* command.

```
tdbackupsys  /backup/
```

Note

- If the backup directory contains a space, the parameter must be enclosed in " " (double-quotation marks).
- The Interstage setup resource and CORBA Service resource must be backed up before the Component Transaction Service resource is backed up.
- After creating the following directories under the control of the backup directory, the *tdbackupsys* command backs up the Component Transaction Service resource under the control of each directory. If the following directories already exist, delete them before executing this command.

Platform	Directory
Windows32/64	TD, EXTP
Solaris32/64	FSUNtd, FSUNextp
Linux32/64	FJSVtd, FJSVextp

- If Interstage is running, stop Interstage with the *isstop -f* command. Stop the cluster system using the cluster system stopping method.
- Windows32 Solaris32 Linux32
  The server machine status monitoring mechanism application status is not backed up using this command. If the server machine status monitoring mechanisms "ServiceServerMachineMonitor" and "ServerMachineMonitorAgent" are used, the parameters specified in service registration commands *issetsmm* and *issetsmma* must be recorded.

12.1.5.10 Backing Up Database Linkage Service Resource Windows32/64 Solaris32 Linux32/64

This section explains the Database Linkage Service resource backup procedure.

Backup Command

The following command is used for backing up the Database Linkage Service resource:

Windows32/64

```
C:\Interstage\ots\bin\otsbackupsys
```

Solaris32

```
/opt/FSUNots/bin/otsbackupsys
```

Linux32/64

```
/opt/FJSVots/bin/otsbackupsys
```

The *otsbackupsys* command must be executed only when Interstage is stopped.

Backup Procedure

Windows32/64

An example where the resource backup destination folder is "X:\Backup" is shown below.

Execute the *otsbackupsys* command.

```
otsbackupsys X:\Backup\
```

Solaris32 Linux32/64

An example where the resource backup destination directory is "/backup/ots" is shown below.

Execute the *otsbackupsys* command.

```
otsbackupsys  /backup/
```

Note

- If the path of the backup directory includes a blank, the path must be enclosed in double quotes when it is specified for a command parameter.
- If Interstage is running, stop Interstage using the *isstop -f* command. Stop the cluster system using the cluster system stopping method.
- The Interstage setup resource and CORBA Service resource must be backed up before the Database Linkage Service resource is backed up.
- The *otsbackupsys* command creates a directory under the specified backup destination path and makes a backup copy of the Database Linkage Service resources under that directory.

  If the following directory already exists, perform the operation after deleting the directory:

Platform	Directory
Windows32/64	OTS
Solaris32	FSUNots
Linux32/64	FJSVots

- In a cluster system, back up the resources on both the operational node (node 1) and the standby node (node 2).

12.1.5.11 Backing up Interstage Single Sign-on Resources

This section explains the procedure for backing up Interstage Single Sign-on resources.

Backup Command

The following command is used for backing up Interstage Single Sign-on resources.

Windows32/64

```
C:\Interstage\bin\ssobackup.exe
```

Solaris32/64 Linux32/64

```
/opt/FJSVssocm/bin/ssobackup
```

Backup Procedure (Repository Server Resources)

This is not valid for Standard-J Edition on Windows (64 bit).

This is not valid for Standard-J Edition on Linux (64 bit).

The following explains how to back up the Interstage Single Sign-on Repository server resources.

Windows32/64

The following example shows how to back up the resources in the "X:\Backup\ssoatcsv" directory.

1. Create a backup directory.

   ```
   mkdir X:\Backup\ssoatcsv
   ```

2. Back up the repository server resources to "ssosv_back" using the *ssobackup* command.

   ```
   ssobackup -f X:\Backup\ssoatcsv\ssosv_back -sv (*1)
   ```

3. If using a cluster system and session management, copy the shared disk encryption information (service ID) file stored in "E:\sso" to the backup directory using the *copy* command.

   ```
   copy E:\sso\serviceid X:\Backup\ssoatcsv\serviceid
   ```

Solaris32/64 Linux32/64

The following example shows how to back up the resources in the "/backup/FJSVssosv" directory.

1. Create a backup directory.

```
mkdir /backup/FJSVssosv
```

2. Back up the repository server resources to "ssosv_back" using the *ssobackup* command.

```
ssobackup -f /backup/FJSVssosv/ssosv_back -sv (*1)
```

3. If using a cluster system and session management, copy the shared disk encryption information (service ID) file stored in "/sso" to the backup directory using the *cp* command.

```
cp -p /sso/serviceid /backup/FJSVssosv/serviceid
```

Backup Procedure (Authentication Server Resources)

The following explains how to backup the Interstage Single Sign-on Authentication server resources.

Windows32/64

The following example shows how to back up the resources in the "X:\Backup\ssoatcag\ssoac_back" file.

1. Create a backup directory.

```
mkdir X:\Backup\ssoatcag
```

2. Back up the authentication server resources using the *ssobackup* command.

```
ssobackup -f X:\Backup\ssoatcag\ssoac_back -ac (*1)
```

Solaris32/64 Linux32/64

The following example shows how to back up the resources in the "/backup/FJSVssoac/ssoac_back" file.

1. Create a backup directory.

```
mkdir /backup/FJSVssoac
```

2. Back up the authentication server resources using the *ssobackup* command.

```
ssobackup -f /backup/FJSVssoac/ssoac_back -ac (*1)
```

Backup Procedure (Business Server Resources)

The following explains how to back up Interstage Single Sign-on Business server resources.

Windows32/64

The following example shows how to back up the resources in the "X:\Backup\ssoatzag\ssoaz_back" file.

1. Create a backup directory.

```
mkdir X:\Backup\ssoatzag
```

2. Back up the business server resources using the *ssobackup* command.

```
ssobackup -f X:\Backup\ssoatzag\ssoaz_back -az (*1)
```

Solaris32/64 Linux32/64

The following example shows how to back up the resources in the "/backup/FJSVssoaz/ssoaz_back" file.

1. Create a backup directory.

```
mkdir /backup/FJSVssoaz
```

2. Back up the business server resources using the *ssobackup* command.

```
ssobackup -f /backup/FJSVssoaz/ssoaz_back -az (*1)
```

*1 Do not specify the files and sub-folders in the Interstage installation directory in the resource storage file specified in the -f option. If the contents under the Interstage installation directory are specified, the resource storage file may not be created correctly.

Note

- Restore the following resources at the same time as restoring the Repository server resources.
  - Interstage HTTP Server
  - Interstage Directory Service

  For details about backing up the Interstage HTTP Server resources, refer to "12.1.5.12 Backing Up Interstage HTTP Server Resource".

  For details about backing up the Interstage Directory Service resources, refer to "12.1.5.16 Backing Up Interstage Directory Service Resources".
- When backing up Repository server resources, also back up the following resources:
  - If Repository server is using SSL of the Interstage certificate environment constructed with Interstage Management Console, the Interstage certificate environment resources need to be backed up. For details on backing up the Interstage certificate environment resources, refer to "12.1.5.17 Backing up Interstage Certificate Environment Resources".
- When backing up Authentication server resources, also back up Interstage HTTP Server resources. For details about backing up the Interstage HTTP Server resources, refer to"12.1.5.12 Backing Up Interstage HTTP Server Resource".

  If SSL of the Interstage certificate environment constructed with Interstage Management Console is in use, the Interstage certificate environment resources need to be backed up. For details on backing up the Interstage certificate environment resources, refer to "12.1.5.17 Backing up Interstage Certificate Environment Resources".
- When using Integrated Windows Authentication, also back up the IJServer resources. For details about backing up the IJServer resources, refer to "12.1.5.14 Backing Up IJServer Resource File".
- When backing up Business server resources, also back up the web server resources and Interstage certificate environment resources. For details about backing up the Interstage certificate environment resources, refer to "12.1.5.17 Backing up Interstage Certificate Environment Resources".

- When developing Java applications, also back up IJServer resources or IJServer cluster resources.
  - For details on how to back up IJServer resources, refer to "12.1.5.14 Backing Up IJServer Resource File".
  - For details on how to back up IJServer cluster resources, refer to "Maintenance (Resource Backup/migration of Resources to Another Server)" - "Backing up and Restoring Resources" - "Backup Procedure" in the Java EE Operator's Guide.

12.1.5.12 Backing Up Interstage HTTP Server Resource

The following explains the backup procedure for Interstage HTTP Server resources.

Backup Command

The following command is used for backing up Interstage HTTP Server resources.

Windows32/64

```
C:\Interstage\bin\ihsbackup.exe
```

Solaris32/64 Linux32/64

```
/opt/FJSVihs/bin/ihsbackup
```

Backup Procedure

1. Execute the *ihsbackup* command to back up Interstage HTTP Server resources. (*1)

   Windows32/64

   ```
   ihsbackup -d  X:\Backup -t all
   ```

   Solaris32/64 Linux32/64

   ```
   ihsbackup -d  /backup -t all
   ```

*1 As well as being specified for the environment definition file, the -t all option of the *ihsbackup* command is also specified, when necessary, for the password file and public root directory (the directory specified in the DocumentRoot directive of the environment definition file, httpd.conf).

Note

- To back up the content (except for those in the directory specified in the DocumentRoot directive), and when a file used in setting the environment other than httpd.conf and the password file exists, save the corresponding file to the backup directory.
- When using the SSL of the Interstage certificate environment (configured with the Interstage Management Console), it is necessary to back up the Interstage certificate environment resources. For information on how to back up Interstage certificate environment resources refer to "12.1.5.17 Backing up Interstage Certificate Environment Resources".
- When using SSL of certificate/key management environment (configured with the SMEE command), restore the following backed up resources to the path specified in the corresponding directive of the SSL environment definition file:
  - Slot information directory (directory specified in SSLSlotDir directive of httd.conf file)
  - Operation control directory (directory specified in SSLEnvDir directive of httd.conf file)
  - User PIN control file (directory specified in SSLUserPINFile directive of httd.conf file)

- When performing an operation such as compression or copy for the backup/export resources, make sure that all resources are the target of the operation, including files that start with a dot (.).

Windows32/64 Solaris32 Linux32/64

- To restore/import to the Managed Server, back up/export when there is just one "FJapache" web server.

Solaris32/64 Linux32/64

- The root directory (/) cannot be specified in the -d option as the storage directory for Interstage HTTP Server resources.

12.1.5.13 Backing Up J2EE Common Resource File

A procedure for backing up the J2EE common resource files is explained.

Backup Command

Use the following command to back up the J2EE common resource file:

Windows32/64

```
C:\Interstage\J2EE\bin\j2eebackup.exe
```

Solaris32/64 Linux32/64

```
/opt/FJSVj2ee/bin/j2eebackup
```

The *j2eebackup* command can only be executed while Interstage is stopped.

Backup Procedure

Windows32/64

The following is an example of operation when the backup destination path is X:\Backup.

1. Confirm that the directory in which the *jar* command is stored is contained in the environment variable PATH. (*1)
2. Execute the *j2eebackup* command to back up the J2EE common resource file.

   ```
   C:\Interstage\J2EE\bin\j2eebackup -d X:\backup
   ```

   Solaris32/64 Linux32/64

The following is an example of operation when the backup destination path is /backup.

1. Check that the directory in which the *jar* command is stored is contained in the path set in the environment variable PATH. (*1)
2. Execute the *j2eebackup* command to back up the J2EE common resource file.

   ```
   /opt/FJSVj2ee/bin/j2eebackup -d /backup
   ```

*1 This check is required because the *j2eebackup* command uses the *jar* command for internal processing.

12.1.5.14 Backing Up IJServer Resource File

A procedure for backing up the IJServer resource files is explained.

Backup Command

Use the following command to back up the IJServer resource file:

Windows32/64

```
C:\Interstage\J2EE\bin\ijsbackup.exe
```

Solaris32/64 Linux32/64

```
/opt/FJSVj2ee/bin/ijsbackup
```

Backup Procedure

Windows32/64

The following is an example of operation when the backup destination path is X:\Backup.

Execute the *ijsbackup* command to back up the IJServer resource file:

```
C:\Interstage\J2EE\bin\ijsbackup -d X:\Backup
```

Solaris32/64 Linux32/64

The following is an example of operation when the backup destination path is /backup.

Execute the *ijsbackup* command to back up the IJServer resource file:

```
/opt/FJSVj2ee/bin/ijsbackup -d /backup
```

Note

- Before backing up the IJServer resource file, back up the target service resources displayed with the *isprintbackuprsc* command.
- Web applications deployed to a directory on the server are not backed up using the *ijsbackup* command. These must be backed up separately

12.1.5.15 Backing Up Interstage JMS Resource

A procedure for backing up the Interstage JMS resource is explained.

Backup Command

The following command is used for backing up the Interstage JMS resource:

Windows32/64

```
C:\Interstage\bin\jmsbackup.exe
```

Solaris32/64 Linux32/64

```
/opt/FJSVjms/bin/jmsbackup
```

Note

- The *jmsbackup* command must be executed while JMS applications are stopped.

Backup Procedure

Enter the *jmsbackup* command to back up the Interstage JMS resource.

Windows32/64

An example of an operation when the backup destination path is X:\Backup is shown below.

```
jmsbackup -d  X:\Backup
```

Solaris32/64 Linux32/64

An example of operation when the backup destination path is /backup is shown below.

```
jmsbackup -d  /backup
```

Note

- The *jmsbackup* command creates a directory under the specified backup destination path and makes a backup copy of the Interstage JMS resources under the directory. If the following directory already exists, perform the operation after deleting the directory.

Platform	Directory
Windows32/64	JMS
Solaris32/64 Linux32/64	FJSVjms

12.1.5.16 Backing Up Interstage Directory Service Resources

This section explains the Interstage Directory Service resources backup procedure.

The backup method is different depending on whether a standard database or RDB is used as the repository database.

The standard database is backed up only according to the following "Repository backup method" that uses the backup command:

1. Repository backup

   If RDB is used, repository data in the Interstage Directory Service resources is managed by RDB. In addition to the following" Repository backup method" using the backup command, the RDB backup function must also be used for the repository data backup using the "Repository data backup method":

2. Repository backup
3. Repository data backup

Backup Command

The following commands are used to backup Interstage Directory Service resources.

Windows32/64

```
C:\Interstage\bin\irepbacksys.exe
```

Solaris32/64 Linux32/64

```
/opt/FJSVirep/bin/irepbacksys
```

Repository backup method

Windows32/64

The following example demonstrates the operation to back up the 'rep001' repository resources to a directory named 'X:\Backup\irep \rep001_back'.

1. Create a backup directory

   ```
   mkdir X:\Backup\irep
   ```

2. Execute the *irepbacksys* command.

   ```
   C:\Interstage\bin\irepbacksys -d X:\Backup\irep\rep001_back -R rep001
   ```

Solaris32/64 Linux32/64

The following example demonstrates the operation to back up the 'rep001' repository resources to a file named '/backup/irep/ rep001_back.tar.gz'.

1. Create a backup directory

   ```
   mkdir /backup/irep
   ```

2. Execute the *irepbacksys* command.

   ```
   /opt/FJSVirep/bin/irepbacksys -f /backup/irep/rep001_back -R rep001
   ```

Repository data backup method

Method for Backing up Repository Data Managed by RDB (Symfoware/RDB)

An overview of the method for backing up repository data managed by Symfoware/RDB is described below.

For details about the backup method, refer to the Symfoware Server online manual.

1. Back up database space information on the disk, and disk (volume) configuration information

   Make a note of the database name specified when the database was created and the database space information list, and also back up the disk configuration information.

2. Displaying the status of archive log files

   If archive logs are used, check the utilization status of archive log files and adjust the timing for forced switchover, discard, and backups.

   If archive logs are not used, proceed to Step 4.

3. Forced switchover of archive log files

   Forcibly switch the archive log files before backing up the RDB dictionaries and DSIs.

4. Settings to suppress RDB dictionary and DSI updates

   If archive logs are not used, before collecting RDB dictionary and DSI backup data, use the *rdbrtr* command to set up update suppression in order to prevent inconsistency with the backup data being collected. The method for collecting table DSIs is described later in this section.

   If archive logs are used, this step is unnecessary. Proceed to Step 5.

5. Back up the table DSI (database)

   Use the *rdbdmp* command to back up the entire table DSI that were created using the *irepgendb* or *irepcrttbl* command. The method to obtain the table DSI is described below. There is no need to back up index DSI.

6. Back up the RDB dictionaries

   In the event of a possible abnormality occurring, back up the RDB dictionaries and RDB directory files using the *rdbdmpdic* command.

7. Back up the archive logs

   If the archive log application is used, back up the archive log using the *rdblog* command.

   If archive logs are not used, this step is unnecessary. Proceed to Step 8.

8. Canceling update suppression for the RDB dictionaries and DSIs

   If archive logs are not used, use the *rdbrls* command to cancel the update suppression that was set up in Step 4.

For details about the database backup procedure, refer to "Backup/Recovery" in the Symfoware Server online manual.

Method for obtaining table DSI

The method for obtaining table DSI created using the *irepgendb* or *irepcrttbl* command is described below.

1. Use the *rdbprt* command to obtain the table created using the *irepgendb* or *irepcrttbl* command.

```
# rdbprt -d DSDB(*1) -m DEF -p -
SCHEMA(DSADMIN(*2))
Ctrl+Z(*3)
  :
No. 1         Schema name ...... DSADMIN

  Database name ...... DSDB
  Creator       ...... DSADMIN
  Created date  ...... Tue Mar  7 08:37:06 2006

    :           :                      :

  Table information(*4)
    No. Table name                     Type
    :           :                          :
    10        IREP_TBL                     PROCEDURE
    :           :                          :
```

   *1 The database name specified using the *irepgendb* or *irepcrttbl* command

   *2 The schema name specified using the *irepgendb* or *irepcrttbl* command

   *3 To enter Ctrl+Z, hold down the Ctrl key and press the "Z" key. This represents the EOF character (in Windows(R)). In Solaris/Linux, the EOF character is normally assigned by Ctrl+D.

   *4 "Table information" is an example.

2. "DSI" is always added to the table name for the table that was obtained. The table DSI format is shown below.

```
table name_DSI ("_DSI" is always added)
Example: If the table name is "IREP_TBL", the DSI is "IREP_TBL_DSI".
```

Backing up Repository Data Managed by RDB (Oracle Database)

Back up the repository data managed in the Oracle database using the EXPORT command.

For details about the backup method, refer to the Oracle database manual.

Note

1. Windows32/64

   Stop the repository before executing the *irepbacksys* command.

2. Windows32/64

   The settings for the relationship between the repository and the RDB set in the *irepadmin* command are not a target of the backup.

3. Solaris32/64 Linux32/64

   Stop the repository before executing the *irepbacksys* command. If the backup is executed without stopping the repository, entries updated during backup may not be backed up. For this reason, stop the repository to ensure that all entries are backed up.

   If the repository cannot be stopped due to operational conditions, using the newest file among those that have been backed up, output the backup information with 'ireprestsys -f backup-file -l'.

   Example

   ```
   ireprestsys -f /backup/irep/rep001_back.tar.gz -l
   ```

   Output Information

   ```
   Date 2007-02-06,09:39:16
   irepVL 4.0
   OSname SunOS
   HostName host01
   Option none
   Repository rep001
   Database symfoware (*)
   ```

   (*) This is only output if the database used as the repository is RDB.

   Compare the time in the Date line of the output information with the time of entry update information in the access log of the target repository. Back up again if the access log contains entries for update information later than the backup time. For further details on the access log, refer to "Monitoring Repository Operation" in the "Operating and Maintaining Repositories" chapter of the Directory Service Operator's Guide.

4. Solaris32/64 Linux32/64

   The file to which the resources are backed up has the file name specified by -f with an extension (.tar.gz) appended.

5. Solaris32/64 Linux32/64

   The automatic start method set using the *irepadmin* command is not a target of the backup.

6. When using the SSL of the Interstage certificate environment (configured with the Interstage Management Console), it is necessary to back up the Interstage certificate environment resources. For information on how to back up Interstage certificate environment resources refer to "12.1.5.17 Backing up Interstage Certificate Environment Resources".

7. When using SSL of certificate/key management environment (configured with the SMEE command), save the following resources to the backup directory:

   - Slot information directory (the directory specified in the slot information directory definition item in the SSL environment definition file)
   - Operation management directory (the directory specified in the operation management directory definition item in the SSL environment definition file).

12.1.5.17 Backing up Interstage Certificate Environment Resources

This section explains the procedure for backing up the Interstage Certificate Environment resources.

Backup Procedure

Windows32/64

An example of the operation to be performed when the backup destination path is X:\Backup\scs is shown below:

1. Create a backup directory.

```
mkdir  X:\Backup\scs
```

2. Use the *xcopy* command (or Explorer) to copy the Interstage Certificate Environment resources to the backup directory.

```
xcopy  /E  C:\Interstage\etc\security  X:\Backup\scs
```

Solaris32/64 Linux32/64

An example of the operation to be performed when the backup destination path is /backup/scs is shown below:

1. Create a backup directory.

```
mkdir /backup/scs
```

2. Use the *cp* command (or Explorer) to copy the Interstage Certificate Environment resources to the backup directory.

```
cp -rp /etc/opt/FJSVisscs/security /backup/scs
```

Note

- The Interstage Certificate Environment can be accessed from the group specified during environment configuration. For this reason, back up also system information on the user accounts and groups.

12.1.5.18 8.3 Format (Short Name) of the Interstage Installation Directory

Windows32/64

In Interstage, 8.3 format (short) file and directory names may sometimes be retained for backup resources. To restore/import backup resources, the short name of the restore environment installation directory must match the short name of the backup resources installation directory.

Use the following procedure to obtain the short name of the Interstage installation directory.

Example: When the installation directory of this product is "C:\Interstage"

1. Change to the Interstage installation directory.

```
cd C:\Interstage
cd ..
```

2. Using the *dir* command, confirm the short directory name.

```
dir /x
XXXX/XX/XX  XX:XX    <DIR>     INTERS~1     Interstage
```

   In this example, the short name of the Interstage installation directory is "C:\INTERS~1".

12.1.5.19 Starting Up Services

Windows32/64

Log in with Administrator authority. Start up the services that were stopped in "(1) Stopping Services" with the *isstart* command.

```
isstart
```

Solaris32/64 Linux32/64

Start up the service that was stopped with the *isstart* command.

```
isstart
```

Note

- Services that cannot be started by the *isstart* command must be started by a separate startup operation.

12.1.6 Restore Procedure (for Systems Other than the Admin Server)

This section describes the procedure for restoring Interstage resources (that have been backed up previously) in an emergency situation, such as when resources are damaged.

Note

Before starting the restore procedure, check the following:

- Reinstallation of Interstage, if required, has been completed.
- All services and server applications have been stopped.
- All of the resources (user resources, user applications) used to run Interstage have been allocated in the same directory configuration as the original configuration before backup. This is necessary because the Interstage installation directory cannot be restored.
- That the 8.3 format (short) directory name of the Interstage installation directory is the same as the directory name that was used for the resource backup.

12.1.6.1 Stopping Services

Windows32/64

Log in with Administrator authority. Stop all services of Interstage and the server application using the *isstop* command.

```
isstop -f
```

Solaris32/64 Linux32/64

Log in as a superuser. Stop all services of Interstage and the server application using the *isstop* command.

```
isstop -f
```

Note

- Services that are not stopped by the *isstop* command must be stopped separately. For more information on how to stop Interstage services, refer to "12.1.5.1 Stopping Interstage Services".

12.1.6.1.1 Stopping the Interstage HTTP Server

If the connection with Interstage has not been set, stop the Interstage HTTP Server using either of the following methods:

Windows32/64

- In the Interstage Management Console, click [System] > [Services] > [Web Server] > [Web Server: View list of the Web Server], and then stop all web servers.
- Stop all web servers using the *ihsstop* command.

```
ihsstop -all
```

- Stop the Windows(R) "FJapache" service and "Interstage HTTP Server(Web Server name)".

Solaris32/64 Linux32/64

- In the Interstage Management Console, click [System] > [Services] > [Web Server] > [Web Server: View list of the Web Server], and then stop all web servers.
- Stop all web servers using the *ihsstop* command.

```
/opt/FJSVihs/bin/ihsstop -all
```

12.1.6.2 Restoring Interstage Setup Resource

This section explains the setup resource restore procedure that is created when Interstage initialization is performed using the *isinit* command.

Restore Command

The following command is used for restoring the Interstage setup resource:

Windows32/64

```
C:\Interstage\bin\iscrestoresys.exe
```

Solaris32/64

```
/opt/FSUNtd/bin/iscrestoresys
```

Linux32/64

```
/opt/FJSVtd/bin/iscrestoresys
```

The *iscrestoresys* command must be executed when Interstage is stopped.

Restore Procedure

Windows32/64

An example of operation when the resource backup folder is X:\Backup\ is shown below.

Execute the *iscrestoresys* command.

```
iscrestoresys X:\Backup\
```

Solaris32/64 Linux32/64

An example of operation, where the resource backup destination directory is /backup, is shown below.

Execute the *iscrestoresys* command.

```
iscrestoresys /backup
```

Note

- If the path of the backup folder includes a blank, the path must be enclosed in double quotes when it is specified for a command parameter.
- If Interstage is operating, use the *isstop -f* command to stop Interstage in advance. For a cluster system, stop it according to the cluster system stop procedure.

12.1.6.3 Restoring Interstage Management Console Resource

This section explains the Interstage Management Console resource restore procedure.

Restore Command

The following command is used for restoring the Interstage Management Console resource:

Windows32/64

```
C:\Interstage\gui\bin\isguirestore.bat
```

Solaris32/64

```
/opt/FJSVisgui/bin/isguirestore
```

The *isguirestore* command must be executed while Interstage is stopped. For command details, refer to the Reference Manual (Command Edition).

Restore Procedure

For the *isguirestore* command, specify the path of the folder in which the Interstage Management Console resources were backed up.

Windows32/64

An example is shown below. The example assumes that the Interstage installation path is C:\Interstage, the resource backup folder is X:\Backup, and the Interstage Management Console resource folder is X:\Backup\isgui.

1. Execute the *isguirestore* command.

```
C:\Interstage\gui\bin\isguirestore  C:\Interstage  X:\Backup\isgui
```

Solaris32/64

For the *isguirestore* command, specify the path of the directory in which the Interstage Management Console resources were backed up.

An example is shown below where the resource backup destination directory is /backup/isgui.

Execute the *isguirestore* command.

```
isguirestore  /backup/isgui
```

Linux32/64

Use the *cp* or other command to copy the source file of the Interstage Management Console resource files from the backup directory to the original directory.

The following shows an example of operation when the resource backup directory is /backup/isgui:

```
cp -p /backup/isgui/config /etc/opt/FJSVisgui
```

Note

- This restore operation need not be executed if the Interstage Management Console has not been customized or backup has not been executed.
- Customize the operating environment of the Interstage Management Console again if the Interstage Management Console was customized on the backup Server.

Windows32/64

- If the path of the backup folder or Interstage install folder includes a blank character, the path must be enclosed in double quotes (" ") when it is specified as a command parameter.
- If any message is output before the command termination message is output, command execution has failed. In this case, execute the command again referring to the output message and these 'Notes' during execution.

Solaris32/64

- If the backup directory contains a blank character, the command parameter must be enclosed in " " (double-quotation marks).

12.1.6.4 Restoring Interstage JMX Service Resource

This section explains the procedure for restoring the Interstage JMX Service resource.

Restore Command

Use the following command for restoring the Interstage JMX Service resource:

Windows32/64

```
C:\Interstage\bin\isjmxrestore
```

Solaris32/64 Linux32/64

```
/opt/FJSVisjmx/bin/isjmxrestore
```

You must execute the *isjmxrestore* command while Interstage and the Interstage JMX service stop. For details on the command, refer to the Reference Manual (Command Edition).

Restore Procedure

The *isjmxrestore* command requires the path of the directory having stored the Interstage JMX service resources at the backup.

An operational example of the resource backup destination directory as /backup, and the directory storing the resources of the operation tools as "/backup/isjmx" is shown below.

Execute the *isjmxrestore* command.

```
isjmxrestore  /backup/isjmx
```

Note

- When the path of the backup destination directory includes a blank, enclose the blank with double quotation marks (") when specifying the command parameter.
- Solaris32/64

  The Interstage JMX Service does not support the multisystem function. Therefore, operations for the extended systems are not required.

12.1.6.5 Restoring CORBA Service Resource

This section explains the CORBA Service resource restore procedure.

Restore Command

The following command is used for restoring the CORBA Service resource:

Windows32/64

```
C:\Interstage\ODWIN\bin\odrestoresys.exe
```

Solaris32/64

```
/opt/FSUNod/bin/odrestoresys
```

Linux32/64

```
/opt/FJSVod/bin/odrestoresys
```

The *odrestoresys* command must be executed while the CORBA Service is stopped.

Depending on the option specified, the *odrestoresys* command can be used to restore CORBA Service (ORB) resources, Naming Service resources, and Interface Repository resources.

Restore Procedure

Windows32/64

An example is shown below where the backup destination path is X:\Backup\OD.

The *odrestoresys* command is executed, and the CORBA Service resource file is restored.

```
odrestoresys  -r  X:\Backup
```

Solaris32/64

An example is shown below where the backup destination path is /backup/FSUNod.

The *odrestoresys* command is executed, and the CORBA Service resource file is restored.

```
odrestoresys -r /backup
```

Linux32/64

An example is shown below where the backup destination path is /backup/FJSVod.

The *odrestoresys* command is executed, and the CORBA Service resource file is restored.

```
odrestoresys -r /backup
```

Note

- When using the SSL linkage function, restore the following backed up resources to the directory specified by *odsetSSL* command.
  - Slot information directory (directory specified in -sd option of *odsetSSL* command)
  - Operation control directory (directory specified in -ed option of *odsetSSL* command)
  - SSL environment definition file (ssl.env file) (on Windows® system or Solaris system).

Windows32/64

- After restoring the CORBA service resources, the startup type of the following services may be registered with "automatic" being set as the type.
  - InterfaceRep_Cache Service
  - InterfaceRep_Cache_e Service

- Naming Service
- NS LoadBalancingOption

Change the startup type, if required, using the following procedure when the setting such as the automatic activation of Interstage was set in the backup environment.

1. Log in using the Administrator's authority.
2. Click [Control Panel] > [Management Tools] > [Service] to activate.
3. Check the startup type for each service.
4. If "Automatic" is registered for the startup type, change it to "Manual" in [Property] after selecting a service.

12.1.6.6 Restoring Event Service Resource

This section explains the Event Service resource restore procedure.

Restore Command

The following command is used for restoring the Event Service resource:

Windows32/64

```
C:\Interstage\bin\esrestoresys.exe
```

Solaris32/64 Linux32/64

```
/opt/FJSVes/bin/esrestoresys
```

The *esrestore* command must be executed when the Event Service is stopped.

Restore Procedure

When restoring Event Service resources, the CORBA Service resource must already have been restored.

Windows32/64

An example is shown below where the backup destination path is X:\Backup\ES.

The directory for the backup is specified by the *esrestoresys* command, and the Event Service resource is restored.

```
esrestoresys  -d  X:\Backup
```

Solaris32/64 Linux32/64

An example is shown below where the backup destination path is /backup/FJSVes.

The directory for the backup is specified by the *esrestoresys* command, and the Event Service resource is restored.

```
esrestoresys -d /backup
```

12.1.6.7 Restoring Portable-ORB Resource

This section explains the Portable-ORB resource restore procedure.

Restore Procedure

Windows32/64

An example is shown below where the backup destination path is X:\Backup\PORB.

1. Copy the Portable-ORB resource file of the backup directory to the original PORB_HOME directory using the *copy* command (or Explorer).

```
copy  X:\Backup\PORB\config  %PORB_HOME%\etc
copy  X:\Backup\PORB\initial_hosts  %PORB_HOME%\etc
copy  X:\Backup\PORB\initial_services  %PORB_HOME%\etc
```

Solaris32/64 Linux32/64

An example is shown below where the backup destination path is /backup/porb.

1. Copy the Portable-ORB resource file of the backup directory to the original PORB_HOME directory using the *cp* command.

```
cp -p /backup/porb/config  $PORB_HOME/etc
cp -p /backup/porb/initial_hosts  $PORB_HOME/etc
cp -p /backup/porb/initial_services  $PORB_HOME/etc
```

Note

When using the SSL linkage function, make a copy to the original directory of the following backed up resources (for details on the resources, refer to "12.1.3.6 Portable-ORB Resource Files"):

- Keystore file
- Embedded certificate control information

12.1.6.8 Restoring the Component Transaction Service Resource

This section explains the Component Transaction Service resource restore procedure.

Restore Command

The following command is used for restoring the Component Transaction Service resource:

Windows32/64

```
C:\Interstage\bin\tdrestoresys.exe
```

Solaris32/64

```
/opt/FSUNtd/bin/tdrestoresys
```

Linux32/64

```
/opt/FJSVtd/bin/tdrestoresys
```

The *tdrestoresys* command must be executed while Interstage is stopped.

Restore Procedure

Windows32/64

An example is shown below where the resource backup destination folder is "X:\Backup\".

The *tdrestoresys* command is executed.

```
tdrestoresys  X:\Backup\
```

Note

- If the path of the backup folder includes a blank, the path must be enclosed in double quotes when it is specified for a command parameter.
- Stop Interstage by using the *isstop -f* command when Interstage is operating.
- It is necessary to restore the Interstage setup resource and the CORBA Service resource before the Component Transaction Service resource is restored.

Solaris32/64 Linux32/64

An example is shown below where the resource backup destination directory is /backup/td.

Execute the *tdrestoresys* command.

```
tdrestoresys  /backup
```

Note

- If the backup directory contains a space, " " (double-quotation marks) must be used to enclose the parameter.
- The Interstage setup resource and CORBA Service resource must be restored before the Component Transaction Service resource is restored.
- If Interstage is running, stop Interstage using the *isstop -f* command.

12.1.6.9 Restoring Database Linkage Service Resource Windows32/64 Solaris32 Linux32/64

This section explains the Database Linkage Service resource restore procedure.

Restore Command

The following command is used for restoring the Database Linkage Service resource:

Windows32/64

```
C:\Interstage\ots\bin\otsrestoresys.exe
```

Solaris32

```
/opt/FSUNots/bin/otsrestoresys
```

Linux32/64

```
/opt/FJSVots/bin/otsrestoresys
```

The *otsrestoresys* command must be executed when Interstage is stopped.

Restore Procedure

Windows32/64

An example is shown below where the resource backup destination folder is "X:\Backup\".

The *otsrestoresys* command is executed.

```
otsrestoresys  X:\Backup\
```

Solaris32 Linux32/64

An example is shown below where the resource backup destination directory is /backup/.

Execute the *otsrestoresys* command.

```
otsrestoresys  /backup/
```

Note

- If the backup directory contains a space, the command parameter must be enclosed in double quotes ("").
- It is necessary to restore the Interstage setup resource and the CORBA Service resource before the Database Linkage Service resource is restored.
- If Interstage is running, stop Interstage using the *isstop -f* command. Stop the cluster system using the cluster system stop method.
- In a cluster system, restore the resources on both the operational node (node 1) and the standby node (node 2).

  Additionally, after the resources have been restored, overwrite the following files on node 2 with the files on node 1:

  Windows32/64

  ```
  C:\Interstage\ots\etc\repository\_recoveryinfo
  ```

  Solaris32

  ```
  /opt/FSUNots/etc/repository/_recoveryinfo
  ```

  Linux32/64

  ```
  /opt/FJSVots/etc/repository/_recoveryinfo
  ```

12.1.6.10 Restoring Interstage Single Sign-on Resources

The following explains how to restore Interstage Single Sign-on resources.

Restore Command

The following command is used for restoring Interstage Single Sign-on resources.

Windows32/64

```
C:\Interstage\bin\ssorestore.exe
```

Solaris32/64 Linux32/64

```
/opt/FJSVssocm/bin/ssorestore
```

Restore Procedure (Repository Server Resources)

This is not valid for Standard-J Edition on Windows (64 bit).

This is not valid for Standard-J Edition on Linux (64 bit).

The following explains how to restore Interstage Single Sign-on Repository server resources.

Windows32/64

The following example shows how to restore the resources backed up in the "X:\Backup\ssoatcsv" directory.

1. Restore the repository server resources backed up in "ssosv_back" using the *ssorestore* command.

   ```
   ssorestore -f X:\Backup\ssoatcsv\ssosv_back
   ```

2. From the Interstage Management Console of the Repository server for which the environment is to be restored, expand the navigation tree to Security > Single Sign-on > Authentication infrastructure > Repository server. From the Settings tab click the Update button.

3. If the encryption information (service ID) file was backed up from the shared disk into "E:\sso", restore the backed up file using the *copy* command.

   ```
   copy X:\Backup\ssoatcsv\serviceid E:\sso\serviceid
   ```

Solaris32/64 Linux32/64

The following example shows how to restore the resources backed up in the "/backup/FJSVssosv" directory.

1. Restore the repository server resources backed up in "ssosv_back" using the *ssorestore* command.

   ```
   ssorestore -f /backup/FJSVssosv/ssosv_back
   ```

2. From the Interstage Management Console of the Repository server for which the environment is to be restored, expand the navigation tree to Security > Single Sign-on > Authentication infrastructure > Repository server. From the Settings tab click the Update button.

3. If the encryption information (service ID) file was backed up from the shared disk into "E:\sso", restore the backed up file using the *cp* command.

```
cp -p /backup/FJSVssosv/serviceid /sso/serviceid
```

Restore Procedure (Authentication Server Resources)

The following explains how to restore Interstage Single Sign-on Authentication server resources.

Windows32/64

The following example shows how to restore the resources backed up in the "X:\Backup\ssoatcag\ssoac_back" file.

1. Specify the resource storage file in the *ssorestore* command to restore the authentication server resources.

```
ssorestore -f X:\Backup\ssoatcag\ssoac_back
```

2. From the Interstage Management Console of the Authentication server for which the environment is to be restored, expand the navigation tree to Security > Single Sign-on > Authentication infrastructure > Authentication server. From the Settings tab click the Update button.

Solaris32/64 Linux32/64

The following example shows how to restore the resources backed up in the "/backup/FJSVssoac/ssoac_back" file.

1. Specify the resource storage file in the *ssorestore* command to restore the authentication server resources.

```
ssorestore -f /backup/FJSVssoac/ssoac_back
```

2. From the Interstage Management Console of the Authentication server for which the environment is to be restored, expand the navigation tree to Security > Single Sign-on > Authentication infrastructure > Authentication server. From the Settings tab click the Update button.

Restore Procedure (Business Server Resources)

The following explains how to restore Interstage Single Sign-on Business server resources.

Windows32/64

The following example shows how to restore the resources backed up in the "X:\Backup\ssoatzag\ssoaz_back" file.

1. Specify the resource storage file in the *ssorestore* command to restore the business server resources.

```
ssorestore -f X:\Backup\ssoatzag\ssoaz_back
```

2. From the Interstage Management Console of the Business Server for which the environment is to be restored, expand the navigation tree to Security > Single Sign-on > Business system > Business system Name. From the Settings tab click the Update button.

Solaris32/64 Linux32/64

The following example shows how to restore the resources backed up in the "/backup/FJSVssoaz/ssoaz_back" file.

1. Specify the resource storage file in the *ssorestore* command to restore the business server resources.

```
ssorestore -f /backup/FJSVssoaz/ssoaz_back
```

2. From the Interstage Management Console of the Business Server for which the environment is to be restored, expand the navigation tree to Security > Single Sign-on > Business system > Business system Name. From the Settings tab click the Update button.

Note

- When backing up repository server resources, restore the following resources in advance:
  - Interstage HTTP Server
  - Interstage Directory Service

  For details about restoring the Interstage HTTP Server resources, refer to "12.1.6.11 Restoring Interstage HTTP Server Resources".

  For details about restoring the Interstage Directory Service resources, refer to "12.1.6.15 Restoring Interstage Directory Service".
- If Repository server is using SSL of the Interstage certificate environment constructed with Interstage Management Console, the Interstage certificate environment resources backed up need to be restored. For details on restoring the Interstage certificate environment resources, refer to "12.1.6.16 Restoring Interstage Certificate Environment Resources".
- When restoring Authentication server resources, restore the Interstage HTTP Server resources in advance: For details about restoring the Interstage HTTP Server resources, refer to "12.1.6.11 Restoring Interstage HTTP Server Resources".

  If the Authentication server is using SSL of the Interstage certificate environment constructed with Interstage Management Console, the backed up Interstage certificate environment resources need to be restored. For details on restoring the Interstage certificate environment resources, refer to "12.1.6.16 Restoring Interstage Certificate Environment Resources".
- When using Integrated Windows Authentication, also restore the IJServer resources. For details about restoring the IJServer resources, refer to "12.1.6.13 Restoring IJServer Resource File".
- When restoring Business server resources, also restore the web server resources and Interstage certificate environment resources. For details about restoring the Interstage certificate environment resources, refer to "12.1.6.16 Restoring Interstage Certificate Environment Resources".
- When developing Java applications, also restore IJServer resources or IJServer cluster resources.
  - For details on how to restore IJServer resources, refer to "12.1.6.13 Restoring IJServer Resource File".
  - For details on how to restore IJServer cluster resources, refer to "Maintenance (Resource Backup/migration of Resources to Another Server)" - "Backing up and Restoring Resources" - "Restore Procedure" in the Java EE Operator's Guide.

12.1.6.11 Restoring Interstage HTTP Server Resources

The following explains the restore procedure for Interstage HTTP Server resources.

Restore Command

The following command is used for restoring Interstage HTTP Server resources.

Windows32/64

```
C:\Interstage\bin\ihsrestore.exe
```

Solaris32/64 Linux32/64

```
/opt/FJSVihs/bin/ihsrestore
```

All web servers must be stopped before the *ihsrestore* command can be used.

Restore Procedure

Windows32/64

In the following example the backup destination path is X:\Backup\IHS.

Specify the backup directory with the *ihsrestore* command, and restore the Interstage HTTP Server resources (*1).

```
ihsrestore  -d  X:\Backup  -t all
```

Solaris32/64 Linux32/64

In the following example the backup destination path is /backup/FJSVihs.

Specify the backup directory with the *ihsrestore* command, and restore the Interstage HTTP Server resources (*1).

```
ihsrestore  -d  /backup  -t all
```

*1 As well as being specified for the environment definition file, the -t all option of the *ihsrestore* command is also specified, when necessary, for the password file and public root directory (the directory specified in the DocumentRoot directive of the environment definition file (httpd.conf). If the -t all option of the *ihsrestore* command is specified, the -t all option of the *ihsbackup* command must also be specified

Note

- If the restore destinations contain files, they will be overwritten.
- The system where the files are to be restored needs to have the same disk configuration as the system that was backed up.
- When the content (except for those in the directory specified in the DocumentRoot directive), and the file used in setting the environment (other than httpd.conf) and the password file were backed up, restore the corresponding files.
- When using the SSL of the Interstage certificate environment (configured with the Interstage Management Console), it is necessary to restore the Interstage certificate environment resources backup. Refer to "12.1.6.16 Restoring Interstage Certificate Environment Resources" for more information on restoring the backed up resources.

  When using the SSL of certificate/key management environment (configured with the SMEE command), restore the following backed up resources to the path specified in the corresponding directive of httpd.conf file:

  - Slot information directory (directory specified in SSLSlotDir directive of httd.conf file)
  - Operation control directory (directory specified in SSLEnvDir directive of httd.conf file)
  - User PIN control file (file specified in SSLUserPINFile directive of httd.conf file)
- To restore V9 or later, backup target resources (Apache HTTP Server 2.0-based), execute the command applicable to the destination server type when the conditions are as follows:
  - For Standalone Server
    - The number of web servers and the web server names match those of the environment that was backed up.
    - All web servers have been deleted.
    - There is just one "FJapache" web server, and the Interstage Single Sign-on business server, authentication server, and repository server environment have not been set up in the "FJapache" web server.
  - For Admin Server Windows32/64 Solaris32 Linux32/64
    - The number of web servers and the web server names match those of the environment that was backed up.
    - All web servers have been deleted.
    - There is only one "FJapache" web server.
  - For Managed Server Windows32/64 Solaris32 Linux32/64
    - There is only one "FJapache" web server, and one "FJapache" web server in the operating environment that was backed up.

- If V8/V7 backup target resources (Apache HTTP Server 1.3-based) are restored, the web server name is "FJapache". If the "FJapache" web server does not exist, create it. Settings for existing "FJapache" web servers will be overwritten.
- Backup target resources (Apache HTTP Server 1.3-based) in V6 and before cannot be restored using the *ihsrestore* command.

12.1.6.12 Restoring J2EE Common Resource File

The procedure for restoring the J2EE Common resource file is explained.

Restore Command

Use the following command to restore the J2EE common resource file:

Windows32/64

```
C:\Interstage\J2EE\bin\j2eerestore.exe
```

Solaris32/64 Linux32/64

```
/opt/FJSVj2ee/bin/j2eerestore
```

The *j2eerestore* command can only be executed while Interstage is stopped.

Restore Procedure

Windows32/64

The following is an example of operation when the backup destination path is X:\Backup:

1. Check that the directory in which the *jar* command is stored is contained in the environment variable path. (*1)
2. Execute the *j2eerestore* command to restore the J2EE common resource file.

```
C:\Interstage\j2ee\bin\j2eerestore -d X:\backup
```

Solaris32/64 Linux32/64

The following is an example of operation when the backup destination path is /backup:

1. Confirm that the directory in which the *jar* command is stored is contained in the environment variable path. (*1)
2. Execute the *j2eerestore* command to restore the J2EE common resource file.

```
/opt/FJSVj2ee/bin/j2eerestore -d /backup
```

*1 This check is required because the *j2eerestore* command uses the *jar* command for internal processing.

12.1.6.13 Restoring IJServer Resource File

The procedure for restoring the IJServer resource file is explained.

Restore Command

Use the following command to restore the IJServer resource file:

Windows32/64

```
C:\Interstage\J2EE\bin\ijsrestore.exe
```

Solaris32/64 Linux32/64

```
/opt/FJSVj2ee/bin/ijsrestore
```

Restore Procedure

Windows32/64

The following is an example of operation when the backup destination path is X:\Backup:

Execute the *ijsrestore* command to restore the IJServer resource file.

```
C:\Interstage\j2ee\bin\ijsrestore -d X:\backup
```

Solaris32/64 Linux32/64

The following is an example of operation when the backup destination path is /backup:

Execute the *ijsrestore* command to restore the IJServer resource file.

```
/opt/FJSVj2ee/bin/ijsrestore -d /backup
```

Note

- Before restoring the IJServer resource file, restore the resources that were backed up as displayed in the *isprintbackuprsc* command. To restore IJServer resources of Interstage Application Server 8.0 or earlier version, the Servlet service based on Tomcat 4.1 must be already installed.
- When IJServer resources of Interstage Application Server 8.0 or earlier version are restored, the log output destination of the web server connector will be changed as follows. The log output destination of the web server connector that was set arbitrarily will not be changed.

  Windows32/64

  ```
  C:\Interstage\F3FMjs5\logs\jk2\FJapache
  ```

  Solaris32/64 Linux32/64

  ```
  /opt/FJSVjs5/logs/jk2/FJapache
  ```

- To restore the resources from an environment that was operating with the Interstage HTTP Server, the resources of the Interstage HTTP Server must be restored before executing this command.
- Web applications deployed to a directory on the server are not restored using the *ijsrestore* command. These must be restored separately. The web application deployment directory is configured in the IJServer configuration information. For this reason, restore the web application using the path used for the backup source directory
- To restore the Session Registry Server IJServer and enable session serialization, use the *jssrsadmin* command *clearsession* subcommand to clear the information for the serialized session before starting the restored Session Registry Server.

12.1.6.14 Restoring Interstage JMS Resource

The procedure for restoring the Interstage JMS resource is explained.

Restore Command

Use the following command to restore the Interstage JMS resource:

Windows32/64

```
C:\Interstage\bin\jmsrestore.exe
```

Solaris32/64 Linux32/64

```
/opt/FJSVjms/bin/jmsrestore
```

Note

- The *jmsrestore* command must be executed while the JMS application is stopped.

Restore Procedure

Windows32/64

An example of operation when the backup destination path is X:/Backup is shown below.

Enter the *jmsrestore* command, with the backup folder specified, to restore the Interstage JMS resource.

```
jmsrestore -d X:\Backup
```

Solaris32/64 Linux32/64

An example of operation when the backup destination path is /backup is shown below.

Enter the *jmsrestore* command, with the backup directory specified, to restore the Interstage JMS resource.

```
jmsrestore -d /backup
```

12.1.6.15 Restoring Interstage Directory Service

This is not valid for Standard-J Edition on Windows (64 bit).

This is not valid for Standard-J Edition on Linux (64 bit).

This section explains the restore procedure for Interstage Directory Service resources.

The restore method is different depending on whether a standard database or RDB is used as the repository database.

The standard database is restored only according to the following "Repository restore method" that uses the restore command.

1. Repository restore

   If an RDB is used, repository data in the Interstage Directory Service resources is managed by the RDB. The repository data is restored using the RDBs recovery or restore function using the 'Repository data restore method', and the repository is restored using the restore command using the 'Repository restore method'.

2. Repository data restore

3. Repository restore

   For details about the restore method, refer to the Symfoware Server online manual.

   For details about the method to restore the Oracle database, refer to the Oracle database manual.

Repository data restore method

Method for Restoring Repository Data Managed by RDB (Symfoware/RDB)

Restore repository data managed by Symfoware/RDB before restoring the Interstage Directory Service resources.

Restore the following resources that were backed up in the event of a possible database abnormality occurring.

- RDB dictionaries
- Database

1. Create the database

   Create the database using the Interstage Directory Service table creation command (*irepgendb* or *irepcrttbl*). For details about the method to create the database, refer to "Setting up Symfoware/RDB" in the "Creating Databases" chapter of the Directory Service Operator's Guide.

2. Restore the RDB dictionaries

   Restore the RDB dictionaries and RDB directory files using the *rdbrcvdic* command. The following message may be output from Symfoware Server, but there is no problem if you continue the operation. "qdg13528e Failed to restore [DSI name] because the contents are incomplete."

3. Make the forbidden access settings

   Before restoring the database, make forbidden access settings for all the table and index DSI that were created using the *irepgendb* or *irepcrttbl* command. The DSI name can be checked using the *rdbinf* or *rdbprt* command. The method of acquiring the DSI for the index using the *rdbprt* command is described as follows:

```
#rdbprt -d DSDB(*1) -m DEF -f -
TABLE(DSADMIN.IREP_TBL(*2))
Ctrl+Z(*3)
  :
  :
  Related index DSI information(*4)
    No.         Index DSI name
    1           IDXDSI_IREP_TBL_XXX
    2           IDXDSI_IREP_TBL_YYY
  :
  :
```

   *1 The database name specified using the *irepgendb* or *irepcrttbl* command

   *2 The schema name specified using the *irepgendb* or *irepcrttbl* command. (The table name.)

   *3 To enter Ctrl+Z, hold down the Ctrl key and press the "Z" key. This represents the EOF character (in Windows(R)). In Solaris/Linux, the EOF character is normally assigned by Ctrl+D.

   *4 "DSI information" is an example.

4. Restore the Database

   Use the *rdbrcv* command.

   For details about rdbXXX commands (Symfoware Server commands), refer to "Symfoware Server Command Reference" in the Symfoware Server manual.

Restoring Repository Data Managed by RDB (Oracle Database)

Restore the repository data managed in the Oracle database before restoring the Interstage Directory Service resources.

Restore the resources backed up in case of a database error. Restore the resources using the IMPORT command.

For details about the method to restore the resources, refer to the Oracle database manual.

Restore Command

The following commands are used to restore Interstage Directory Service resource files:

Windows32/64

```
C:\Interstage\bin\ireprestsys.exe
```

Solaris32/64 Linux32/64

```
/opt/FJSVirep/bin/ireprestsys
```

Restore Procedure

Windows32/64

In the following example the backup destination path is X:\Backup\irep\rep001_back and the repository that has been backed up is rep001:

1. Execute the *represtsys* command to confirm that the backup directory contains repository rep001.

   ```
   C:\Interstage\bin\ireprestsys -d X:\Backup\irep\rep001_back -l
   ```

2. Execute the *ireprestsys* command to restore the Interstage Directory Service resource files.

   ```
   C:\Interstage\bin\ireprestsys -d X:\Backup\irep\rep001_back -R rep001
   ```

Solaris32/64 Linux32/64

In the following example the backup destination path is /backup/irep/rep001_back and the repository that has been backed up is rep001:

1. Execute the *ireprestsys* command to confirm that the backup folder contains repository rep001.

   ```
   /opt/FJSVirep/bin/ireprestsys -f /backup/irep/rep001_back.tar.gz -l
   ```

2. Execute the *ireprestsys* command to restore the Interstage Directory Service resource files.

   ```
   /opt/FJSVirep/bin/ireprestsys -f /backup/irep/rep001_back.tar.gz -R rep001
   ```

Note

- Ensure that the repository is stopped before executing this command.
- When the backup data is restored, the same repository name, same database storage directory, and same access log storage directory are used. If the database storage directory path or access log storage directory path is not given, first create the path and then perform the restore.
- If the SSL of the Interstage Certificate Environment established with Interstage Management Console is used, the Interstage Certificate Environment resources that have been backed up need to be restored. For details on how to restore the Interstage Certificate Environment resources, refer to "12.1.6.16 Restoring Interstage Certificate Environment Resources".

- If the SSL of the certificate/key management environment established with the SMEE command is used, restore the following resources, which have been backed up, to the paths specified in the corresponding definition items of the SSL environment definition file:
  - Slot information directory (the directory specified in the slot information directory definition item in the SSL environment definition file)
  - Operation management directory (the directory specified in the operation management directory definition item in the SSL environment definition file).
- Backup/restore can only be performed when the resources are on the same OS and use the same database. Repository resources on a different OS or in an environment that uses a different database cannot be restored.
- Repository resources cannot be restored if the Interstage Directory Service version is older than the backed up environment.

Windows32/64

- The relationship between the repository and the RDB must be set using the *irepadmin* command after the restore.

Solaris32/64 Linux32/64

- The automatic start method must be set using the *irepadmin* command after the restore.

12.1.6.16 Restoring Interstage Certificate Environment Resources

This section explains the procedure for restoring the Interstage Certificate Environment resources.

Restore Procedure

Windows32/64

An example of the operation to be performed when the backup destination path is X:\Backup\scs is shown below:

Use the *xcopy* command (or Explorer) to copy the Interstage Certificate Environment resources from the backup directory back to the original directory.

```
xcopy  /E /I  X:\Backup\scs  C:\Interstage\etc\security
```

Solaris32/64 Linux32/64

An example of the operation to be performed when the backup destination path is /backup/scs is shown below.

Use the *cp* command to copy the Interstage Certificate Environment resources from the backup directory back to the original directory:

```
cp -rp /backup/scs/security /etc/opt/FJSVisscs
```

Note

- Restore the resources back to the original directory, which was used before backup, with the same authority.

  Solaris32/64 Linux32/64

  The Interstage Certificate Environment can be accessed from the group specified during environment configuration. For this reason, restore also system information on the user accounts and groups as needed.

12.1.6.17 Starting Up the Services

Windows32/64

Log in with Administrator authority. Start up the services that were stopped by "(1) Stopping Services" using the *isstart* command:

```
isstart
```

Solaris32/64 Linux32/64

Start up the services that were stopped previously by "(1) Stopping Services" using the *isstart* command:

```
isstart
```

Note

- Services that cannot be started by the *isstart* command must be started using their own startup operation.
- If service startup fails after importing the resource, check whether there is a shortage of the imported resources or an error in the importing procedure before taking the action in the output message.

12.1.7 Restore Procedure (Admin Server) Windows32/64 Solaris32 Linux32/64

This section explains the restore procedure for recovering backed up Interstage resources on the Admin Server. This might be used in the event of the resources being corrupted, for example.

The following can be restored:

- Interstage Management Console resources
- Interstage JMX Service resources Solaris32 Linux32/64
- Business configuration management resources
- Interstage Directory Service resources.

Note

- Interstage Directory Service should only be restored if the directory service is used for login authentication.
- The explanations in this section assume that the following directories are used for storing backup resources:
  - Windows32/64

    ```
    X:\Backup
    ```

  - Solaris32 Linux32/64

    ```
    /backup
    ```

- Before starting the restore operation:
  - If it was necessary to re-install Interstage, verify that installation is complete.
  - Verify that the Interstage installation directory and the installation drive (for Windows®) are under the same directory configuration as prior to backup.
  - Verify that the 8.3 format (short) directory name of the Interstage installation directory is the same as the directory name that was used for the resource backup.

Operation Procedure

Restore the resources as described below.

Stopping Services

Before stopping the service, refer to "12.1.5.1 Stopping Interstage Services".

Restoring Resources

The method for restoring resources is the same as the 12.1.5 Backup Procedure (for Systems Other than the Admin Server) above. For other restore methods, refer to the following sections:

- 12.1.6.3 Restoring Interstage Management Console Resource
- 12.1.6.4 Restoring Interstage JMX Service Resource
- 12.1.6.15 Restoring Interstage Directory Service

Starting Services

Note

- If the service fails to start after the resources are restored, verify that the restored resources are sufficient, and that there was no error in the restore procedure. Use the output message to determine what action to take.

12.1.8 Backup/Restore of Resources (Cluster Environments)

This section explains 1:1 standby type cluster environments.

On single node clusters, perform the following procedures according to the server role:

- 12.1.5 Backup Procedure (for Systems Other than the Admin Server)
- 12.1.4 Backup Procedure (Admin Server)
- 12.1.6 Restore Procedure (for Systems Other than the Admin Server)
- 12.1.7 Restore Procedure (Admin Server)

Additionally, when restoring the resources, immediately after installing Interstage disable the Interstage automatic startup settings according to "High Availability System Guide" - "Installing Interstage".

12.1.8.1 Backup Procedure (Cluster Environments)

Use the procedure below to back up the resources (the node on which the backup data is collected first is called "node 1", and the node on which the backup data is collected after that is called "node 2"). For details on each command and the cluster system operations, refer to "Reference Manual (Command Edition)" and the cluster system manual respectively.

1. Stop the cluster system.

   Interstage will stop on both nodes.

2. Ensure that the shared disk file system can be accessed from node 1 if any of the following resources have been placed on a shared disk:

   - Interstage JMS resources
   - Interstage HTTP Server resources
   - Interstage HTTP Server 2.2 resources
   - Interstage Single Sign-on resources (Repository Server)
   - Interstage Directory Service resources
   - Job configuration manager repository resources

- IJServer cluster resources

  Solaris32/64 Linux32/64

  Start the GDS volume on this node, and mount the file system.

  Windows32/64

  Ensure that the shared disk on this node is online.

3. Back up the resources on node 1.

   The collected resources are identified by the *isprintbackuprsc* command.

   Refer to the following, according to the server role:

   - 12.1.5 Backup Procedure (for Systems Other than the Admin Server)
   - 12.1.4 Backup Procedure (Admin Server)

4. Ensure that the shared disk made accessible in step 2 and the file system on the shared disk cannot be accessed from node 1.

   Solaris32/64 Linux32/64

   Unmount the file system on this node, and stop the GDS volume.

   Windows32/64

   Ensure that the shared disk on this node is offline.

5. Ensure that the shared disk file system can be accessed from node 2 if any of the following resources have been placed on a shared disk:

   - Interstage JMS resources
   - Interstage HTTP Server resources
   - Interstage HTTP Server 2.2 resources

6. Back up the resources on node 2, except for the following:

   - Interstage Single Sign-on resources (Repository Server)
   - Interstage Directory Service resources
   - Job configuration manager repository resources
   - IJServer cluster resources
   - Interstage certificate environment resources (Note)

   Note

   If certificates for each node have been registered in the Interstage certificate environment, also back up the resources on node 2.

   Refer to the following, according to the server role:

   - 12.1.5 Backup Procedure (for Systems Other than the Admin Server)
   - 12.1.4 Backup Procedure (Admin Server)

7. Ensure that the shared disk made accessible in step 5 and the file system on the shared disk cannot be accessed from node 2.
8. Start the cluster system.

12.1.8.2 Restore Procedure (Cluster Environments)

Use the procedure below to restore the resources (the node on which the resources are restored first is called "node 1", and the node on which the resources are restored after that is called "node 2").

Solaris32/64

Recover the PRIMECLUSTER environment and resource definition beforehand, and then stop RMS on both nodes.

Linux32/64

Restore the data that was backed up in the backup system recommended by PRIMECLUSTER, and then stop RMS on both nodes. Additionally, uninstall Interstage from both nodes.

Windows32/64

Change the MSCS environment so that it has the status described in "High Availability System Guide" - "Cluster System Presetting" beforehand.

1. Install Interstage on nodes 1 and 2.
2. Disable the Interstage automatic startup settings.
3. Ensure that the shared disk file system can be accessed from node 1 if any of the following resources have been placed on a shared disk:
   - Interstage JMS resources
   - Interstage HTTP Server resources
   - Interstage HTTP Server 2.2 resources
   - Interstage Single Sign-on resources (Repository Server)
   - Interstage Directory Service resources
   - Job configuration manager repository resources
   - IJServer cluster resources

     Solaris32/64 Linux32/64

     Start the GDS volume on this node, and mount the file system.

     Windows32/64

     Ensure that the shared disk on this node is online.
4. Restore the resources collected on node 1 to node 1.

   Refer to the following, according to the server role:

   - 12.1.6 Restore Procedure (for Systems Other than the Admin Server)
   - 12.1.7 Restore Procedure (Admin Server)
5. Ensure that the shared disk made accessible in step 3 and the file system on the shared disk cannot be accessed from node 1.

   Solaris32/64 Linux32/64

   Mount the file system on this node, and stop the GDS volume.

   Windows32/64

   Ensure that the shared disk on this node is offline.
6. Ensure that the shared disk file system can be accessed from node 2 if any of the following resources have been placed on a shared disk:
   - Interstage JMS resources
   - Interstage HTTP Server resources
   - Interstage HTTP Server 2.2 resources
   - IJServer cluster resources
7. Restore the resources to node 2.

   Restore any resources for which a backup was collected on node 2.

   Restore to node 2 any resources that were only backed up on node 1.

Except for the Interstage Directory Service resources, the method used to restore each resource depends on the server role - refer to the following:

- 12.1.6 Restore Procedure (for Systems Other than the Admin Server)
- 12.1.7 Restore Procedure (Admin Server)

Restore the Interstage Directory Service resources just to the repository environment of node 2 by using the *ireprestsys* command with the *-confonly* option (for details, refer to "Reference Manual (Command Edition)" - "Backup Commands" - "ireprestsys"):

Example

Windows32/64

```
ireprestsys -d X:\Backup\irep\rep001_back -R rep001 -confonly
```

Solaris32/64 Linux32/64

```
ireprestsys -f /backup/irep/rep001_back.tar.gz -R rep001 -confonly
```

8. Ensure that the shared disk made accessible in step 5 and the file system on the shared disk cannot be accessed from node 2.

Windows32/64

1. Register the Interstage resources in MSCS.

   For details, refer to "High Availability System Guide" - "Environment Setup Procedure for Cluster Service" - "For MSCS".

12.2 Moving Resources to Another Server

This section explains copying (moving) the Interstage resources or moving the application environment to another server.

Resources can be exported from the server (original server) in which the Interstage application environment is configured, and imported into the copy destination server (destination server). The copy destination server can configure the equivalent application environment without prior initialization of the Interstage application environment.

Note

- When moving resources, the destination server must have the same system configuration as that of the movement source server.
  - Operating system
  - Interstage version level
  - Interstage installation path
  - Interstage services used
  - Storage path of user application and resource files
- The files that can be moved are the files held by Interstage for defining the application environment. User applications cannot be moved. Move them by other appropriate means.

12.2.1 Overview and Applicable Files

Movement of resources to other servers is performed to copy the Interstage environment that is configured on one server machine to another server machine, setting the same configuration in the destination servers. The destination servers do not need the Interstage initial

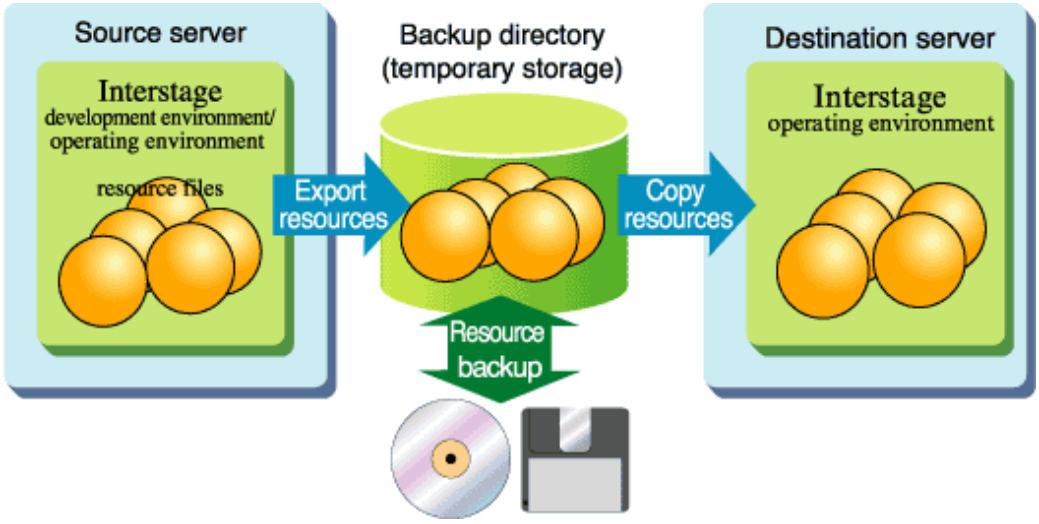
setting or the initial setting of other services, and the environment configuration does not need to be set in each server. Setting of the server application environment in multiple machines can therefore be accomplished in a short period of time.

Use the following procedure to move resources:

1. Export the resources to the backup disk from the source server.
2. Copy the resources that are saved in the backup disk to the destination server.
3. Import the resources that are saved in the backup disk of the destination server.

The following figure provides an overview of moving resources to another server.

Figure 12.6 Moving Resources to Another Server



12.2.1.1 Applicable Resources

The files that can be moved are the same as those that can be restored. For details, refer to "12.1.1 Outline".

To transfer the following resources/files to the other server collectively, refer to "12.3 Collective Maintenance".

12.2.2 Resource Exporting Procedure

The Interstage resource export procedure is the same as the backup procedure on the same machine. Refer to "12.1.5 Backup Procedure (for Systems Other than the Admin Server)".

12.2.3 Resource Importing Procedure

This section explains the importing procedure of the destination server when importing Interstage resources.

Windows32/64

This explanation assumes that the backup resource storage folder of X:\Backup already exists.

Solaris32/64 Linux32/64

This explanation assumes that the backup resource storage directory of /backup already exists.

Note

- Perform the resource importing procedure after confirming the following:
  - Interstage installation has been completed.
  - The Interstage installation directory and any resources (such as user resources and user applications used in the Interstage application) that cannot be restored have already been configured in the same folder configuration as in the resource exporting server.

- All services and all server applications have been stopped.
- That the 8.3 format (short) directory name of the Interstage installation directory is the same as the resource export source server.

12.2.3.1 Stopping Services

Windows32/64

Log in as Administrator. Stop all of the Interstage services and server applications using the *isstop* command.

Solaris32/64 Linux32/64

Stop all of the Interstage services and server applications using the *isstop* command (or other appropriate commands).

```
isstop -f
```

Note

- Services that are not stopped by the *isstop* command must be stopped separately. For more information on how to stop Interstage services, refer to "12.1.5.1 Stopping Interstage Services".

12.2.3.1.1 Stopping the Interstage HTTP Server

If the connection with Interstage has not been set, stop the Interstage HTTP Server using to either of the following methods:

Windows32/64

- In the Interstage Management Console, click [System] > [Services] > [Web Server] > [Web Server: View list of the Web Server], and then stop all web servers.
- Stop all web servers using the *ihsstop* command.

```
ihsstop -all
```

- Stop the Windows(R) "FJapache" service and "Interstage HTTP Server(Web Server name)".

Solaris32/64 Linux32/64

- In the Interstage Management Console, click [System] > [Services] > [Web Server] > [Web Server: View list of the Web Server], and then stop all web servers.
- Stop all web servers using the *ihsstop* command.

```
/opt/FJSVihs/bin/ihsstop -all
```

12.2.3.2 Importing Interstage Setup Resource

This section describes the procedure for importing the setup resources that are created when the *isinit* command is used to initialize Interstage.

Import Command

The following command is used for importing the Interstage setup resource.

Windows32/64

```
C:\Interstage\bin\iscrestoresys.exe
```

Solaris32/64

```
/opt/FSUNtd/bin/iscrestore
```

Linux32/64

```
/opt/FJSVtd/bin/iscrestore
```

The *iscrestoresys* command must be executed while Interstage is stopped.

Import Procedure

Windows32/64

An example is shown below. The example assumes that the resource backup folder is X:\Backup\ and the host name used by the CORBA Service is hostname.

Execute the *iscrestoresys* command.

```
iscrestoresys -h hostname X:\Backup\
```

Solaris32/64 Linux32/64

An example is shown below where the resource backup destination directory is /backup/isc.

Execute the *iscrestoresys* command.

```
iscrestoresys  -h  hostname  /backup
```

Solaris32/64

In the Interstage setup resource import, the following items (that are definition items of the Interstage operating environment definition) can be customized using the restore definition file:

- Corba Host Name (host name that operates the CORBA Service)
- Corba Port Number (port number used for CORBA communication)
- IR Path for DB file (directory in which the database used in the Interface Repository is created)
- TD path for system (directory in which the operating environment of the Component Transaction Service is created)
- SSL Port Number (port number used for SSL linkage).

Create a restore definition file that describes the definition information after any definition content changes for the definition items above, then specify the file in the **-f** option of the *iscrestoresys* command.

Describe the restore definition file in the same way as the Interstage operating environment definition. A restore definition file example and operational example using a restore definition file are shown below.

- Import conditions
  - Change Corba Host Name to host1.

  - Change Corba Port Number to 8003.
  - Change IR Path for DB file to "/IRPATH".
  - Change TD path for system to "/TDPATH".

- Restore definition file (/BKUP/rest.txt)

```
Corba Host Name=host1
Corba Port Number=8003
IR Path for DB file=/IRPATH
TD path for system=/TDPATH
```

- Command execution example

  Execute the *iscrestoresys* command.

```
iscrestoresys -f  /BKUP/rest.txt  /backup
```

Note

- If the backup directory contains a blank, " " (double-quotation marks) must be used to enclose the parameter.
- If Interstage is running, enter the *isstop -f* command to stop it in advance. Stop cluster systems according to the cluster system stop procedure.

12.2.3.3 Importing Interstage Management Console Resources

The Interstage Management Console resource importing procedure is explained.

Import Command

The following command is used for importing the Interstage Management Console resource.

Windows32/64

```
C:\Interstage\gui\bin\isguirestore.bat
```

Solaris32/64

```
/opt/FJSVisgui/bin/isguirestore
```

The *isguirestore* command must be executed while Interstage is stopped. For details of the command, refer to the Reference Manual (Command Edition).

Import Procedure

Windows32/64

For the *isguirestore* command, specify the path of the folder into which the Interstage Management Console resources were exported.

An operation example is shown below. The example assumes that the Interstage installation path is C:\Interstage, the resource backup folder is X:\Backup, and the Interstage Management Console resource folder is X:\Backup\isgui.

1. Execute the *isguirestore* command:

```
C:\Interstage\gui\bin\isguirestore  C:\Interstage  X:\Backup\isgui
```

2. When the following items are specified in the web server environment definition file for the Interstage Management Console, use an editor to modify the setup values to the appropriate values to suit each importing machine.

   - Server name (definition name:ServerName)

Solaris32/64

An example is shown below where the resource backup destination directory is /backup/isgui.

1. Execute the *isguirestore* command:

```
isguirestore  /backup/isgui
```

2. When the following items are specified in the web server environment definition file (/etc/opt/FJSVisgui/FJSVisgui.dat) for the Interstage Management Console, modify the setup values to the appropriate values for each importing machine using a text editor or similar.

```
Server name (definition name:ServerName)
```

Linux32/64

The procedure for importing the Interstage Management Console resources is the same as that for restoring them on the same machine. For details, refer to "12.1.6.3 Restoring Interstage Management Console Resource".

Note

Windows32/64

- If the path of the backup folder or Interstage install folder includes a blank character, the path must be enclosed in double quotes (" ") when it is specified as a command parameter.
- If any message is output before the command termination message is output, command execution has failed. In this case, execute the command again referring to the output message and these 'Notes' during execution.
- If the environment definition of the Interstage Management Console is not customized and no exporting has been performed, this import operation need not be performed.

Solaris32/64

- If the backup directory contains a blank character, " " (double-quotes) must be used to enclose the command parameter.

12.2.3.4 Importing Interstage JMX Service Resource

This subsection explains the procedure for importing the Interstage JMX service resource.

Import Command

Use the following command for importing the Interstage JMX service resource:

Windows32/64

```
C:\Interstage\bin\isjmxrestore
```

Solaris32/64 Linux32/64

```
/opt/FJSVisjmx/bin/isjmxrestore
```

You must execute the *isjmxrestore* command while Interstage and the Interstage JMX service stop. For details on the command, refer to the Reference Manual (Command Edition).

Import Procedure

The *isjmxrestore* command requires the path of the directory in which the operation tool resources have been stored at time of export.

An operational example of the resource backup destination directory as /backup, and the directory having stored the resources of the operation tools as "/backup/isjmx" is shown below.

Execute the *isjmxrestore* command:

```
isjmxrestore  /backup/isjmx
```

Note

- When the path of the backup destination directory includes a blank, enclose the blank with double quotation marks (") when specifying the command parameter.

12.2.3.5 Importing CORBA Service Resource

The section explains importing the CORBA Service resource.

Import Command

The following command is used for importing the CORBA Service resource:

Windows32/64

```
C:\Interstage\ODWIN\bin\odrestoresys.exe
C:\Interstage\ODWIN\bin\OD_or_adm.exe
C:\Interstage\ODWIN\bin\OD_set_env.exe
C:\Interstage\ODWIN\bin\odchgservice.exe
C:\Interstage\ODWIN\bin\odexportns.exe
C:\Interstage\ODWIN\bin\odimportns.exe
C:\Interstage\ODWIN\bin\odlistns.exe
```

Solaris32/64

```
/opt/FSUNod/bin/odrestoresys
/opt/FSUNod/bin/OD_or_adm
/opt/FSUNod/bin/OD_set_env
/opt/FSUNod/bin/odchgservice
/opt/FSUNod/bin/odexportns
/opt/FSUNod/bin/odimportns
```

```
/opt/FSUNod/bin/odlistns
```

Linux32/64

```
/opt/FJSVod/bin/odrestoresys
/opt/FJSVod/bin/OD_or_adm
/opt/FJSVod/bin/OD_set_env
/opt/FJSVod/bin/odchgservice
/opt/FJSVod/bin/odexportns
/opt/FJSVod/bin/odimportns
/opt/FJSVod/bin/odlistns
```

By specifying the option, the *odrestoresys* command can be imported by changing the hostname and the port number set in the CORBA Service resource file (config, inithost/initial_hosts, init_svc/initial_services, impl.db, and the file under the control of the CosNaming directory). Alternatively, change the destination of the storage in the database of the interface repository service resource. The procedure when not changing these settings, it is the same as the restore procedure on the same machine. Refer to "12.1.6.5 Restoring CORBA Service Resource".

Import Procedure (CORBA Service resource)

The import procedure of the CORBA Service resource is shown below.

Change the following information if necessary after importing CORBA Service resource.

- Change the host information embedded in the object reference
- Change Initial Service host information
- Change Naming Service registration information

Windows32/64

An example is shown below where the backup destination path is X:\Backup\OD.

The *odrestoresys* command is executed, and the CORBA Service resource file is imported:

```
odrestoresys  -u h hostname  -p 8002  -irpath X:\Interstage2\TD\var\IRDB  X:\Backup
```

Solaris32/64

An example is shown below where the backup destination path is /backup/FSUNod.

The *odrestoresys* command is executed, and the CORBA Service resource file is imported:

```
odrestoresys -u -h hostname -p 8002 -irpath /opt2/FSUNtd/var/IRDB /backup
```

Linux32/64

An example is shown below where the backup destination path is /backup/FJSVod.

The *odrestoresys* command is executed, and the CORBA Service resource file is imported:

```
odrestoresys -u -h hostname -p 8002 -irpath /opt2/FJSVtd/var/IRDB /backup
```

Change the host information embedded in the object reference

The -h option and -p option specified in the *odrestoresys* command are set in the host information that is embedded in the object reference. To set other host information, change the information in the *OD_set_env* command.

An example of how to set the host information that is embedded in the object reference is shown below:

1. Display the object reference configuration information in the *OD_set_env* command, and check the host name implicit value.

```
OD_set_env -l
```

2. Set the host information that is embedded in the object reference in the *OD_set_env* command. Specify the host name that was checked in 1. for HostName.

```
OD_set_env -n HostName
```

Change Initial Service host information

If the import source host information (host name/port number) remains in the initial service, change the import destination host information (host name/port number) in the *odchgservice* command.

An example of how to set the host information (host name/port number) of the initial service is shown below:

1. Display the list of services registered for the initial service in the *OD_or_adm* command, and check the initial service name.

```
OD_or_adm -l
```

2. Set the initial service host name/port number in the *odchgservice* command.

   For host, specify the host name. For port, specify the port number. For service, specify the initial service name that was checked in 1.

```
odchgservice -h host -p port service
```

Change Naming Service registration information

When the object information that references the other host exists in the naming service registration information and the other host is included in the conversion target, the host name/port number of the object information that references the other host must be updated to that of the conversion destination of the other host.

An example of operation for converting the host name/port number of the object information that references the other host is shown as follows:

1. Check if the host name of the object is different from own host name.

   When the host corresponding to the host name is included in the conversion target, the host name/port number must be changed to that of the conversion destination.

```
odlistns -l
```

2. Export the naming service registration information.

```
odexportns -o filename
```

3. Delete all the naming service registration information.

```
OD_or_adm -d -n object
```

or

```
OD_or_adm -d -z context
```

or

```
OD_or_adm -d -n object group
```

4. Import the naming service registration information.

   As the Hostlistfile, specify the file with the description of the change in the host name/port number of the object information that references the other host.

```
odimportns -i filename -h Hostlistfile
```

Note

- The *odrestoresys* command must be executed in the state that the CORBA Service is stopped.
- When using the SSL of the Interstage certificate environment (configured with the Interstage Management Console), it is necessary to restore the Interstage certificate environment resources backup. Refer to "12.1.6.16 Restoring Interstage Certificate Environment Resources" for more information on restoring the backed up resources.
- If the "Corba Host Name" statement is set in the Interstage operating environment definition file, the host name will be set for the config "IIOP_hostname" parameter through the import of the resources. If there is no need for IIOP_hostname to be set, delete the IIOP_hostname definition. For details on the IIOP_hostname, refer to "config" in the "CORBA Service Environment Definition" appendix of the Tuning Guide.
- When using the SSL linkage function, execute the *odsetSSL* command corresponding to the import destination SSL environment.

Windows32/64

- After importing the CORBA service resources, the startup type of the following services may be registered with "automatic" being set as the type.
  - InterfaceRep_Cache Service
  - InterfaceRep_Cache_e Service
  - Naming Service
  - NS LoadBalancingOption

  Change the startup type, if required, using the following procedure when the setting such as the automatic activation of Interstage was set in the backup environment.

  1. Log in using the Administrator's authority.
  2. Click [Control Panel] > [Management Tools] > [Service] to activate.
  3. Check the startup type for each service.
  4. If "Automatic" is registered for the startup type, change it to "Manual" in [Property] after selecting a service.

12.2.3.6 Importing Event Service Resource

The importing procedure of the Event Service resource is the same as the restore procedure on the same machine. Refer to "12.1.6.6 Restoring Event Service Resource".

In systems that have more than one IP address, if the event channel is created using the *esmkchnl* command with the -host and -port options, the event channel resources cannot be exported to another server.

In this case, after the import procedure is complete, delete the event channel using the *esrmchnl* command and then re-create it using the *esmkchnl* command. If the event channel is not re-created, the event channel will not start and the es10026 or es10027 error message will display. For details on these commands, refer to the Reference Manual (Command Edition).

12.2.3.7 Importing Interstage Single Sign-on Resources

The procedure for importing the Interstage Single Sign-on resources is the same as the restore procedure on the same machine. Refer to "12.1.6.10 Restoring Interstage Single Sign-on Resources".

If the machine is replaced, however, note the following points when relocating the machine:

- The Repository server, Authentication server, and Business server constituting the Interstage Single Sign-on system establish communication between machines. If host names differ between the export source and import destination, no communication can be executed between servers.
- When importing an environment to another machine due to machine relocation, make sure the host names (IP addresses) are the same between the export source and import destination, to enable communication using the host name (IP address) of the export source.

12.2.3.8 Importing Interstage HTTP Server Resource

This section explains how to import Interstage HTTP Server resources.

Import Command

The following command is used for importing Interstage HTTP Server resources.

Windows32/64

```
C:\Interstage\bin\ihsrestore.exe
```

Solaris32/64 Linux32/64

```
/opt/FJSVihs/bin/ihsrestore
```

All web servers must be stopped before the *ihsrestore* command can be used.

Import Procedure

Windows32/64

In the following example the backup destination path is X:\Backup\F3Fmihs.

Specify the backup directory with the *ihsrestore* command, and import the Interstage HTTP Server resources (*1).

```
ihsrestore  -d  X:\Backup  -t all  -h c:\Interstage\F3FMihs\etc\conf\host_table
```

Solaris32/64 Linux32/64

In the following example the backup destination path is /backup/FJSVihs.

Specify the backup directory with the *ihsrestore* command, and import the Interstage HTTP Server resources (*1).

```
ihsrestore  -d  /backup  -t all  -h /etc/opt/FJSVihs/etc/host_table
```

- *1 The -t all option of the *ihsrestore* command is specified for the environment definition file and is also specified, when necessary, for the password file and public root directory (the directory specified in the DocumentRoot directive of the environment definition file (httpd.conf). If the -t all option of the *ihsrestore* command is specified, the -t all option of the *ihsbackup* command must also be specified.

  Specify the -h option of the *ihsrestore* command to convert the host name/IP address. Make the following entries in the host_table file:

```
(IP address before conversion) > (IP address after conversion)
(Host name before conversion) > (Host name after conversion)
```

  - Start each comment line with a hash sign (#).
  - Half-width spaces and tabs are ignored.

Example

Convert the host name and IP address as shown below:

- Before conversion: IP address "192.168.0.1", After conversion: IP address "192.168.0.3"
- Before conversion: IP address "192.168.0.2", After conversion: IP address "192.168.0.4"
- Before conversion: host name www.fujitsu.com, After conversion: host name www.interstage.com
- Before conversion: host name "host1.fujitsu.com", After conversion: host name "host2.fujitsu.com"

```
### Host IP conversion table ###

# IP address conversion definition
  192.168.0.1 > 192.168.0.3
  192.168.0.2 > 192.168.0.4

# Host name conversion definition
  www.fujitsu.com > www.interstage.com
  host1.fujitsu.com > host2.fujitsu.com
```

Note

- If the import destinations contain files, they will be overwritten.
- The system where the files will be imported must have the same disk configuration as the system where the export was performed.
- The host name and IP address converted with the -h option are specified in the directives below.
  - Listen
  - ServerName
  - VirtualHost
  - NameVirtualHost
- If the port numbers set for the export original and the import destination in the Interstage HTTP Server environment definition file (httpd.conf) are different, set the port number for the import destination in the directive for setting the port number.

- When the content and the file used in setting the environment (other than httpd.conf) and the password file were backed up, restore the corresponding files.
- When using the SSL of the Interstage certificate environment (configured with the Interstage Management Console), it is necessary to restore the Interstage certificate environment resources backup. Refer to "12.1.6.16 Restoring Interstage Certificate Environment Resources" for more information on restoring the backed up resources.
- When using the SSL of certificate/key management environment (configured with the SMEE command), restore the following backed up resources to the path specified in the corresponding directive of httpd.conf file:
  - Slot information directory (directory specified in SSLSlotDir directive of httd.conf file)
  - Operation control directory (directory specified in SSLEnvDir directive of httd.conf file)
  - User PIN control file (file specified in SSLUserPINFile directive of httd.conf file)
- To import V9 or later, export target resources (Apache HTTP Server 2.0-based), execute the command applicable to the import destination server type under the following conditions:
  - For Standalone Server
    - The number of web servers and the web server names match those of the environment that was exported.
    - All web servers have been deleted.
    - There is just one "FJapache" web server, and the Interstage Single Sign-on business server, authentication server, and repository server environment have not been set up in the "FJapache" web server
  - For Admin Server Windows32/64 Solaris32 Linux32/64
    - The number of web servers and the web server names match those of the environment that was exported.
    - All web servers have been deleted.
    - There is just one "FJapache" web server.
  - For Managed Server Windows32/64 Solaris32 Linux32/64
    - There is only one "FJapache" web server, and one "FJapache" web server in the operating environment that was exported.
- If V8/V7 export target resources (Apache HTTP Server 1.3-based) are imported, the web server name is "FJapache". If the "FJapache" web server does not exist, create it. Settings for existing "FJapache" web servers are overwritten.
- Export target resources (Apache HTTP Server 1.3-based) in V6 and before cannot be imported using the *ihsrestore* command.

12.2.3.9 Importing J2EE Common Resource File

The procedure for importing the J2EE common resource file is the same as the restore procedure on the same machine. Refer to "12.1.6.12 Restoring J2EE Common Resource File".

12.2.3.10 Importing IJServer Resource File

The procedure for importing the IJServer resource file is the same as the restore procedure on the same machine. Refer to "12.1.6.13 Restoring IJServer Resource File".

However, in the following cases, it is necessary to convert the IP address:

- The server is a standalone server; and
- The IJServer and the web server operate separately; and
- The IP addresses of the Servlet container and web server at the import source and the import destination are different.

Perform one of the following tasks to match the IP address with that in the import target environment:

- Convert the IP address by specifying the "-h host_table" argument when executing the *ijsrestore* command.

- After the restore, change the following items from Interstage Management Console:
  - [WorkUnit] > "WorkUnit name" > [Environment Settings] > [Web Server Connector (Connector) Settings] > [IP Address of Web Server Accepting Request]
  - [WorkUnit] > "WorkUnit name" > [Environment Settings] > [Servlet Container Settings] > [Servlet Container IP Address]
  - 'Servlet Container IP address: port number' in the web server connector environment settings.

Note

- For the -h host_table argument of the *ijsrestore* command, specify the full path to the file describing the IP addresses before and after the change. This allows the IP address to be automatically converted during import. For details, refer to the Reference Manual (Command Edition).
- To change the virtual host IP address or Hostname when Interstage HTTP Server is imported, first import the IJServer resource files and then use the Interstage Management Console or the *isj2eeadmin* command to reset the virtual host used by IJServer.

  If the virtual host is not reset, it might cause an inconsistency to occur in the definition between Interstage HTTP Server and the IJServer so that it does not run normally. The above operation must be performed to use the virtual host in the IJServer.

  There is no need to perform above operation if the virtual host is not used in the IJServer.

12.2.3.11 Importing Interstage JMS Resource

The procedure for importing the Interstage JMS resource is the same as the restore procedure on the same machine. Refer to "12.1.6.14 Restoring Interstage JMS Resource".

However, if another host is specified in the Destination definition IP address (host name)/port number, it may be necessary to change the host name/port number after the Interstage JMS resources are imported.

The following steps illustrate how to convert the host name/port number.

1. Check that the IP address (host name)/port number has been specified in the Destination definition.

   If the host specified in the Destination definition is the target of the migration, the host name/port number must be changed at this point.

   ```
   jmsinfodst
   ```

2. Export the Destination definition information.

   ```
   isj2eeadmin resource -e -all -k jmsdst -f filename
   ```

3. Change the host name/port number of the Destination definition information that was exported.
4. Import the Destination definition information.

   Specify the file name that was created in step 3.

   ```
   isj2eeadmin resource -o -f filename
   ```

   The *isj2eeadmin* command must be executed when Interstage JMX Service is running. For details on the *isj2eeadmin* command, refer to the Reference Manual (Command Edition).

12.2.3.12 Importing Interstage Certificate Environment Resources

The ability to import Interstage Certificate Environment resources depends on the policy of the Certification Authority that issues site certificates.

In some cases, the Certification Authority does not allow different servers to use an identical site certificate. In other cases, such usage is conditionally allowed. Verify with Certification Authorities that their site certificates are usable for your planned operation before importing Interstage Certificate Environment resources.

If Certification Authorities do not allow different servers to use identical site certificates, use such site certificates separately on each server (build an Interstage Certificate Environment separately on each server). Alternately, obtain site certificates only from certification authorities that allow use of their site certificates for the planned operation.

Resource files in Interstage Certificate Environment are classified into the following two types:

- Certificate environment file
- SSL configuration files.

  SSL configuration files can be imported regardless of Certification Authority policy.

Import Procedure

When Certification Authorities permit import of their site certificates to other servers, or no site certificates have been registered, the steps for importing Interstage Certificate Environment resources are the same as those for restoring Interstage Certificate Environment resources on a single machine. Refer to "12.1.6.16 Restoring Interstage Certificate Environment Resources".

Otherwise, it is necessary to build an Interstage Certificate Environment on each server. SSL configuration files can be imported. Refer to the description below for details on how to import an SSL configuration file.

Windows32/64

In the following example the backup destination path is X:\Backup\scs.

```
xcopy  /E /I X:\Backup\scs\sslconf  C:\Interstage\etc\security\sslconf
```

Copy the SSL configuration file in the backup directory to the original directory using the *xcopy* command (or Explorer).

Solaris32/64 Linux32/64

In the following example the backup destination path is /backup/scs.

```
cp -rp /backup/scs/security/sslconf /etc/opt/FJSVisscs/security
```

Copy the SSL configuration file from the backup directory to the original directory using the *cp* command.

Note

- Solaris32/64 Linux32/64

  The Interstage Certificate Environment resources can be accessed from the group specified during environment configuration. For this reason, match the system information on user accounts and groups with that on the import source machine. Alternatively, create a group for accessing the Interstage Certificate Environment and redefine it using the *scsmakeenv* command.

Resetting the SSL configuration

After importing Interstage certificate environment resources, it may be necessary to reset the SSL configuration. The required operations are described below.

Running the import destination server as a standalone server

When the import destination server as a standalone server and only the SSL configuration file is imported (an Interstage certificate environment has been set up for each server), execute the operation shown below for the imported SSL configuration:

1. From the Interstage Management Console, expand the navigation tree to System > Security > SSL. In the View SSL Configurations tab, click the appropriate SSL Configuration Name. In the SSL Settings tab, select the Site Certificate Nickname to be used by the server.
2. Click Detailed Settings **[Show]** link and change the CA certificate settings if necessary.
3. Repeat steps 1 and 2 for all the imported SSL configurations.

Running the import destination server as a Managed Server Windows32/64 Solaris32 Linux32/64

The operations for using the multiserver management function to run the import destination server as a Managed Server, refer to "12.1.6.16 Restoring Interstage Certificate Environment Resources".

12.2.3.13 Importing Interstage Directory Service Resources

The import procedure for Interstage Directory Service resources is the same as the restore procedure on the same machine. Refer to "12.1.6.15 Restoring Interstage Directory Service".

Note the following points when using the RDB for the repository database:

Using Symfoware Server

To use the Symfoware Server for the repository database, the host name that can be resolved in the repositories of both the export source and the import destination must have been specified as the "database connection host name" specified when the repository was created in the export source. If the host name that cannot be resolved at both the export source and import destination is specified, the repository must be recreated.

To create the repository on the machine that is the export source, specify, when creating the repository, the host name that can be resolved in the repositories of both the export source and the import destination as the "database connection host name".

Using Oracle database

To use the Oracle database as the repository database, the host name specified as that of the database being specified as the connection destination in the Net service setting made during the database creation procedure on the machine on which the Interstage directory service has been installed must be a host name that can be resolved in the repositories of both the export source and the import destination.

To make the Net service setting on the machine that is the export source, the host name that can be resolved in the repositories of both the export source and the import source must be specified at the time of Net service setting.

12.2.3.14 Starting Up Services

Windows32/64

Log in with Administrator authority. Use the *isstart* command to start up the services that were stopped in '(1) Stopping Services'.

Solaris32/64 Linux32/64

Log in as a superuser. Use the *isstart* command to start services that were stopped previously.

```
isstart
```

Note

- Services that cannot be started using the *isstart* command must be started by a separate startup operation.
- If startup of the service fails after importing the resource, check if there is a shortage of the imported resources or an error in the importing procedure before taking the action described in the output message.

12.3 Collective Maintenance

A sample batch file (Windows®) and Shell script (Solaris and Linux) for 12.1 Backing Up and Restoring Resources and 12.2 Moving Resources to Another Server collectively are provided. Users can operate collectively when specifying the procedures suitable for batch files (Windows®) and Shell scripts (Solaris and Linux) respectively.

Adapt the sample batch file (Windows®) and the Shell script (Solaris and Linux) if necessary.

In some cases, additional operations may be required in each service after collective maintenance. For details, refer to "12.1 Backing Up and Restoring Resources" and "12.2 Moving Resources to Another Server".

12.3.1 Resource Backup/Export

The sample collective procedures for Interstage resource backup and export are provided.

Windows32/64

```
C:\Interstage\sample\backup_restore\isbackup.bat
```

Solaris32/64 Linux32/64

```
/opt/FJSVisas/sample/backup_restore/isbackup
```

isbackup describes the procedures of Interstage backup and export as an instruction.

Each process has a comment in the format shown below according to the processing content.

```
#=====================================================
#   Number    Explanation of alphanumeric characters
#=====================================================
```

12.3.2 Process Outline

Explanation of each process outline

Windows32/64 Linux32/64

Table 12.1 Process Outline for Windows and Linux

Comment	Process content
:DEFINITION_PART	Backup target definition
:PROCEDURE_PART	Main process

Solaris32/64

Table 12.2 Process Outline for Solaris

Comment	Process content
0. Environment Check	Authorization check.
1. check the input parameter	Command parameter check.
2-1. set the restore CO	Command name variable definition.
2-2. set the section name list	Backup target variable definition.
2-3. get the file line and set line = 0	Syntax analysis of backup target resource files6.

Comment	Process content
2-4. check the def file format	
2-5. check sub-routines	
3. MAIN	Main process
4. Sub-Routines	Backup process of backup target resources

12.3.3 Backup/Export Process of Backup Target Resources

Backup/export process is delimited using the format shown below at each backup target resource:

```
## Service name  START
     :
   (Backup process description)
## Service name  END
```

Service names (changeable) correspond to the backup resources as listed below.

Table 12.3 Service Names with Corresponding Backup Resources

Service name	Backup target resources
ISCOM	Backup of Interstage setup resources
GUI	Backup of Interstage Management Console resources
JMX	Backup of Interstage JMX Service resources
OD	Backup of CORBA service resources
ES	Backup of Event service resources
PORB	Backup of Portable-ORB resources
TD	Backup of Component Transaction service resources
Windows32/64 Solaris32 Linux32/64 OTS	Backup of Database Linkage Service resources
IJServer	Backup of IJServer resources
SSOsv (*1)(*2)	Interstage Single Sign-on resource (Repository server)
SSOac	Interstage Single Sign-on resource (Authentication server)
SSOaz	Interstage Single Sign-on resource (Business server)
JMS	Backup of Interstage JMS resources
J2EE	Backup of J2EE common resources
IHS	Backup of Interstage HTTP Server resources
AHS	Backup of Interstage HTTP Server 2.2 resources
WSC	Backup of Web Server Connector (for Interstage HTTP Server 2.2) resources
ISSCS	Backup of Interstage Certificate Environment resources
IREP	Backup of Interstage Directory Service resources
JavaEE	Backup of IJServer cluster resources
JavaEE6	Backup of Java EE 6 resources

*1 This is not valid for Standard-J Edition on Linux (64 bit).

*2 This is not valid for Standard-J Edition on Windows (64 bit).

12.3.4 Operation Procedures

Procedures of resource backup/export using the *isbackup* command are described below.

12.3.4.1 Stopping the Service

Windows32/64

Log in with Administrator authority, and use the *isstop* command to stop all the Interstage services and server applications.

Solaris32/64 Linux32/64

Use the *isstop* command to stop all the Interstage services and server applications:

```
isstop -f
```

Note

- Services that are not stopped by the *isstop* command must be stopped separately. For more information on how to stop Interstage services, refer to "12.1.5.1 Stopping Interstage Services".

12.3.4.1.1 Stopping the Interstage Directory Service

Application Management

Interstage Management Console > Site > Security > Repository	View Status

Standalone

Interstage > Interstage Application Server > System > Services > Repository	View Status

To stop the service:

1. Check the checkbox to the left of repositories to be stopped.
2. Click the **Stop** button.

Note

- Alternately, stop the service as follows:
  - Windows32/64

    Stop the 'Interstage Directory Service (%s1),' Windows® service,

    where %s1 is the repository name.
  - Solaris32/64 Linux32/64

    Use the *irepstop* command to stop the service. The -R option specifies the repository name to stop.

    Example

    /opt/FJSVirep/bin/irepstop -R rep001

    For details on the *irepstop* command, refer to the Reference Manual (Command Edition).

12.3.4.2 Backup/Export Target Resource Definition

Windows32/64 Linux32/64

Define Interstage backup target resources in the batch file.

Use the following syntaxes to define the target resources:

Solaris32/64

Define Interstage backup target resources in the backup target definition file.

The backup target definition file can be created with an arbitrary name according to the following syntaxes:

For details, refer to "12.1.5 Backup Procedure (for Systems Other than the Admin Server)" and "12.2.2 Resource Exporting Procedure".

The sample of the backup target resource definition file is provided below.

Windows32/64

Define Interstage backup target resources in the batch file:

Solaris32/64

```
/opt/FJSVisas/sample/backup_restore/sample.def
```

Linux32/64

Define Interstage backup target resources in Shell.

12.3.4.2.1 Description Format

Windows32/64

Write one definition on a single line in the batch file:

```
rem [Section name]
set definition name = Definition value
```

Solaris32/64

Write one definition on a single line in the definition file:

```
[Section name]
definition name = Definition value
```

Linux32/64

Write one definition on a single line in the shell:

```
# [Section name]
set definition name = Definition value
```

Note

- Write "[", "]", and "=" in en-size characters.

- Solaris32/64

  When writing a comment, write # after the definition value. Do not specify # at the top of a line.

12.3.4.2.2 Definition Item List

Backup target items are listed below.

- Section names or definition names cannot be omitted.
- Definition values are indicated as below.
- y: required; -: can be omitted; x: cannot be specified

Windows32/64 Linux32/64

Table 12.4 Backup Target items for Windows and Linux

Section name	Explanation of section name	Definition name	Definition value	Explanation	Remarks
Common	Specifies basic information in operation.	INST_DIR	Directory y	Interstage installation directory.	Change according to the installation environment.
		COMMON_PATH	Directory y	Specifies a directory that stores the backup/export resources.	
ISCOM	Species Interstage setup resource related items.	ISCOM_TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
GUI	Specifies Interstage Management Console related items.	GUI_TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
JMX	Specifies Interstage JMX Service related items.	JMX_TARGET	on or off y	Specifies whether the Interstage JMX Service resources will be operation targets. on: They will be operation targets off: They will not be operation targets	
		JMX_IPADDRESS		If it will be necessary to convert the IP address used in the Interstage JMX Service when the resources are imported, specify the IP address. (*6) Specify this IP address in the cases shown below. If this item is not specified, the IP address will not be changed.	

Section name	Explanation of section name	Definition name	Definition value	Explanation	Remarks
				- When the IP address is specified in isjmx.xml of the server in which the resources are backed up - When the resources are restored in a server that has multiple IP addresses, and another IP address is specified for the admin LAN IP address and business LAN IP address	
		JMX_USERREP	on or off	Specify whether the Interstage JMX Service user repository definition will be a restore target. (*6) on: The resources are restored (default) off: The resources are not restored	
		JMX_SITEINFO	on or off y	To migrate the site, specify "on". Normally, specify "off".	
OD	Specifies CORBA service related items.	OD_TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
ES	Specifies event service related items.	ES_TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
PORB	Specifies Portable-ORB related items.	PORB_TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
TD	Specifies component transaction service related items.	TD_TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
OTS	Specifies database linkage service related items.	OTS_TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
IJServer	Specifies IJServer related items.	IJSERVER_TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
		IJSERVER_HOST_TABLE		When importing as follows, specify the name of a file (full path) that has a description of	

Section name	Explanation of section name	Definition name	Definition value	Explanation	Remarks
				IP addresses before and after the change. (*1) - When the server is a standalone server - When the operation is by separating the IJServer and the web server, and - IP addresses for the Servlet container and web server are different at the import source and the export destination	
JMS	Specifies Interstage JMS related items.	JMS_TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
J2EE	Specifies J2EE shared resource related items.	J2EE_TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
IHS	Specifies Interstage HTTP Server related items. (*4)	IHS_TARGET	on or off	An operation target when specifying "on". Not an operation target when specifying "off".	
		IHS_OPTION_FROM_V6	on or off	To restore/import V5.1/V6.0 resources backed up/exported using maintenance batch execution batch file (Windows®) or shell script (Linux) to an 8.0 environment, specify "on".	
		IHS_OPTION	1, 2 or 3	Specifies the operation target resources from below: 1. Environment definition information. 2. Environment definition information and password file. 3. Environment definition information, and directory specified in the DocumentRoot directive. 3 is enabled when IHS_OPTION_FROM_V6 is off.	
		IHS_HOST_TABLE		If it is necessary to change the host name/IP address at the time of import, specify the file name containing the host	

Section name	Explanation of section name	Definition name	Definition value	Explanation	Remarks
				name/IP address before and after conversion. This can be omitted for restores. This is enabled when IHS_OPTION_FROM_V6 is off. (*5)	
		IHS_PASSWD_SOURCE		Specifies the file name for the password file that was specified to restore and import V5.1/V6.0 resources when V5.1/V6.0 resources were backed up/imported. This is enabled when IHS_OPTION_FROM_V6 is on, and IHS_OPTION is 2.	
		IHS_PASSWD_TARGET		Specifies the restore/import target directory for the password file for restoring and importing resources in V5.1/V6.0. This is enabled when IHS_OPTION_FROM_V6 is on, and IHS_OPTION is 2.	
AHS	Specifies Interstage HTTP Server 2.2 related items. (*4)	AHS_TARGET	on or off	An operation target when specifying "on". Not an operation target when specifying "off".	
		AHS_OPTION	1, 2 or 3	Specifies the operation target resources from below: 1. Environment definition information. 2. Environment definition information and password file. 3. Environment definition information, password file, and contents.	
		AHS_HOST_TABLE		If it is necessary to change the host name/IP address at the time of import, specify the file name containing the host name/IP address before and after conversion. This can be omitted for restores. (*5)	
WSC	Specifies Web Server	WSC_TARGET	on or off	An operation target when specifying "on". Not an	

Section name	Explanation of section name	Definition name	Definition value	Explanation	Remarks
	Connector (for Interstage HTTP Server 2.2) related items.		y	operation target when specifying "off".	
		WSC_HOST_TABLE		When importing as follows, specify the name of a file (full path) that has a description of IP addresses before and after the change.(*1) - When the server is a standalone server - When operating the web server and the IJServer cluster on different machines, and - IP addresses for the web container and web server are different at the import source and the export destination	
ISSCS(*8)	Specifies Interstage Certificate Environment related items.	ISSCS_TARGET	on or off	An operation target when specifying "on". Not an operation target when specifying "off".	
		ISSCS_OPTION	1 or 2	This is invalid when specified for backup.	
IREP(*7)	Specifies Interstage Directory Service related items.	IREP_TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
SSOsv(*7)	Specifies Interstage Single Sign-on resource (Repository server) related items.	SSOSV_TARGET	on or off	An operation target when specifying "on". Not an operation target when specifying "off".	
SSOac	Specifies Interstage Single Sign-on resource (Authentication server) related items.	SSOAC_TARGET	on or off	An operation target when specifying "on". Not an operation target when specifying "off".	
SSOaz	Specifies Interstage Single Sign-on resource (Business server) related items.	SSOAZ_TARGET	on or off	An operation target when specifying "on". Not an operation target when specifying "off".	
JavaEE (*7)	Specifies Java EE related items.	JAVAEE_TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	

Section name	Explanation of section name	Definition name	Definition value	Explanation	Remarks
		IP_HOST_FILE		Contains the path name for the IP address/host name settings file when resources are imported.	
JavaEE6	Specifies Java EE 6 related items.	JAVAEE6_TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
		JAVAEE6_IP_HOST_FILE		Contains the path name for the IP address/host name settings file when resources are imported.	

Solaris32/64

Table 12.5 Backup Target Items for Solaris

Section name	Explanation of section name	Definition name	Definition value	Explanation	Remarks
Common	Specifies basic information in operation.	host	Host name x	Specifies only in restore or import.	
		path	Directory y	Specifies a directory that stores the backup/export resources.	
		target_server	x	Specifies only in restore or import.	
ISCOM	Species Interstage setup resource related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
		source	File path x	Specifies only in restore or import.	
GUI	Specifies Interstage Management Console items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
JMX	Specifies Interstage JMX Service related items.	target	on or off y	Specifies whether the Interstage JMX Service resources will be operation targets. on: They will be operation targets off: They will not be operation targets	
		ipaddress		If it will be necessary to convert the IP address used in the Interstage JMX Service when the resources are imported, specify the IP address. (*6)	

Section name	Explanation of section name	Definition name	Definition value	Explanation	Remarks
				Specify this IP address in the cases shown below. If this item is not specified, the IP address will not be changed. - When the IP address is specified in isjmx.xml of the server in which the resources are backed up - When the resources are restored in a server that has multiple IP addresses, and another IP address is specified for the admin LAN IP address and business LAN IP address	
		jmx_userrep	on or off	Specifies whether the Interstage JMX Service user repository definition will be a restore target. (*6) on: The resources are restored (default) off: The resources are not restored	
		siteinfo	on or off y	To migrate the site, specify "on". Normally, specify "off".	
OD	Specifies CORBA service related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
		port	Port number x	Specifies only in restore or import.	
		db_path	Directory x	Specifies only in restore or import.	
ES	Specifies event service related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
PORB	Specifies Portable-ORB related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
TD	Specifies component transaction service related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
Solaris32 OTS	Specifies database linkage service related items.	target	on or off y	An operation target when specifying "on". Not an	

Section name	Explanation of section name	Definition name	Definition value	Explanation	Remarks
				operation target when specifying "off".	
IJServer	Specifies IJServer related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
		ijserver_host_table		When importing as follows, specify the name of a file (full path) that has a description of IP addresses before and after the change. (*1) - When the server is a standalone server - When the operation is by separating the IJServer and the web server, and - IP addresses for the Servlet container and web server are different at the import source and the export destination	
JMS	Specifies Interstage JMS related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	(*2)
J2EE	Specifies J2EE shared resource related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	(*3)
IHS	Specifies Interstage HTTP Server related items. (*4)	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
		from_v6	on or off	To restore/import V5.1/V6.0 resources backed up/exported using maintenance batch execution shell script to an 8.0 environment, specify "on".	
		option	1, 2 or 3	Specifies the operation target resources from below. 1. Environment definition information. 2. Environment definition information and password file. 3. Environment definition information, and directory specified in	

Section name	Explanation of section name	Definition name	Definition value	Explanation	Remarks
				the DocumentRoot directive. 3 is enabled when from_v6 is off.	
		ihs_host_table		If it is necessary to change the host name/IP address at the time of import, specify the file name containing the host name/IP address before and after conversion. This can be omitted for restores. This is enabled when from_v6 is off. (*5)	
		passwd_source		Specifies the file name for the password file that was specified to restore and import V5.1/V6.0 resources when V5.1/V6.0 resources were backed up/imported. This is enabled when from_v6 is on, and option is 2.	
		passwd_target		Specifies the restore/import target directory for the password file for restoring and importing resources in V5.1/V6.0. This is enabled when from_v6 is on, and option is 2.	
AHS	Specifies Interstage HTTP Server 2.2 related items. (*4)	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
		option	1, 2 or 3	Specifies the operation target resources from below. 1. Environment definition information. 2. Environment definition information and password file. 3. Environment definition information, password file, and contents.	
		ahs_host_table		If it is necessary to change the host name/IP address at the time of import, specify the file name containing the host name/IP address before and after conversion.	

Section name	Explanation of section name	Definition name	Definition value	Explanation	Remarks
				This can be omitted for restores. (*5)	
WSC	Specifies Web Server Connector (for Interstage HTTP Server 2.2) related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
		wsc_host_table		When importing as follows, specify the name of a file (full path) that has a description of IP addresses before and after the change.(*1) - When the server is a standalone server - When the operation is by separating the IJServer cluster and the web server, and - IP addresses for the web container and web server are different at the import source and the export destination	
ISSCS(*8)	Specifies Interstage Certificate Environment related items.	target	on or off	An operation target when specifying "on". Not an operation target when specifying "off".	
		option	1 or 2	This is invalid when specified for backup.	
IREP(*7)	Interstage Directory Service related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
SSOsv(*7)	Specifies Interstage Single Sign-on resource (Repository server) related items.	target	on or off	An operation target when specifying "on". Not an operation target when specifying "off".	
SSOac	Specifies Interstage Single Sign-on resource (Authentication server) related items.	target	on or off	An operation target when specifying "on". Not an operation target when specifying "off".	
SSOaz	Specifies Interstage Single Sign-on resource (Business server) related items.	target	on or off	An operation target when specifying "on". Not an operation target when specifying "off".	

Section name	Explanation of section name	Definition name	Definition value	Explanation	Remarks
JavaEE(*7)	Specifies Java EE related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
		ip_host_file		When importing resources, specify the name of a file (full path) that has a description of IP addresses before and after the change.	
JavaEE6	Specifies Java EE 6 related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
		javaee6_ip_host_file		When importing resources, specify the name of a file (full path) that has a description of IP addresses before and after the change.	

The following notes relate to Table 12.4 Backup Target items for Windows and Linux and Table 12.5 Backup Target Items for Solaris.

- *1 The name of the file (full path) with a description of the IP addresses before and after changing the IJSERVER_HOST_TABLE or WSC_HOST_TABLE must be specified in the section [IJServer] or [WSC] when importing under the following circumstances:
  - When the server is a standalone server,
  - When the operation is by separating the IJServer/IJServer cluster and the web server, and
  - The IP addresses of the Servlet container/web container and the web server are different at the import source and the import destination.

  [IJServer]

  The IP addresses subject to conversion are the following items on the Interstage Management Console.

  - [WorkUnit] > "WorkUnit name" > [Environment Settings] > [Detailed Settings] > [Web Server Connector (Connector) Settings] > [IP Address of Web Server Accepting Request]
  - [WorkUnit] > "WorkUnit name" > [Environment Settings] > [Detailed Settings] > [Servlet Container Settings] > [Servlet Container IP Address]
  - [Web Server] > "Web server name" > [Web Server Connector] > "WorkUnit name" > [Environment Settings] > [Servlet Container IP Address: Port Number]
  - [WorkUnit] > "WorkUnit name" > [Environment Settings] > [Detailed Settings] > [Servlet Container Settings] > [Access Permission IP Address]

  [WSC]

  - IP Address:port number defined by wscadmin command add-instance-ref subcommand.

  Update the values as required because, when the session recovery function is in use, the following items on the Interstage management console are not subject to the IP address conversion.

  - [WorkUnit] > "WorkUnit name" > [Environment Settings] > [Detailed Settings] > [Session Recovery Settings] > [Session Registry Server Address in the Session Backup Destination: Port]

  Example

  Windows32/64

```
..
:DEFINITION_PART
    ...
rem [IJServer]
set IJSERVER_TARGET=on
set IJSERVER_HOST_TABLE=C:\Work\host_table.txt
..
```

Solaris32/64 Linux32/64

```
..
:DEFINITION_PART
    ...
#[IJServer]
set IJSERVER_TARGET=on
set IJSERVER_HOST_TABLE=/usr/work/host_table.txt
```

Enter the following descriptions in host_table.

- To comment out a line, enter a hash sign (#) at the start of the line.
- Spaces and tabs are ignored.

```
(IP address before conversion) > (IP address after conversion)[(IJServer workunit name)]
```

IP addresses before conversion: Specify the IP addresses of the Servlet container and the web server in the import source environment.

IP address after conversion: Specify the IP addresses of the Servlet container and the web server in the environment after the import.

IJServer workunit name: Specify the target IJServer workunit name when the IP address for a specific IJServer only is converted. When omitted, IP addresses will be converted for all the IJServers.

Example: Converting the IP address as follows:

- Pre-conversion: IP address "192.168.0.1" Post-conversion: IP address "192.168.0.3"
- Pre-conversion: IP address "192.168.0.2" Post-conversion: IP address "192.168.0.4" Conversion target IJServer: "IJServer01"

```
192.168.0.1 > 192.168.0.3
192.168.0.2 > 192.168.0.4 IJServer01
```

- *2 For [JMS] section, the following path to CLASSPATH must be specified for backup.

```
CLASSPATH=/opt/FJSVj2ee/lib/isj2ee.jar:/opt/FJSVjms/lib/fjmsprovider.jar
```

- *3 For [J2EE] section, the directory that stores *jar* command must be included in the environment variable PATH because *jar* command is used in the internal process.
- *4 For Interstage HTTP Server, when the SSL definition is set with Interstage Management Console, it must be backed up in the [ISSCS] section.
- *5 If it is necessary to change the host name/IP address of the [IHS]/[AHS] section during import, specify the file name containing the host name/IP address before and after the change in IHS_HOST_TABLE/AHS_HOST_TABLE.

Example

For [IHS] section

Windows32/64

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
:DEFINITION_PART
  ...
rem [IHS]
set IHS_TARGET=on
set IHS_OPTION_FROM_V6=off
rem 1: set DEF only, 2: set DEF and password file 3: set DEF and
password and DocumentRoot
set IHS_OPTION=2
set IHS_HOST_TABLE=C:\Work\host_table.txt
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Solaris32/64

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
  [IHS]
  target = on
  from_v6 = off
  option = 1
  ihs_host_table = /usr/work/host_table.txt
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Linux32/64

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
DEFINITION_PART:
...
#[IHS]
set IHS_TARGET=on
set IHS_OPTION_FROM_V6=off
# 1: set DEF only, 2: set DEF and password file 3: set DEF and password
and DocumentRoot
set IHS_OPTION=2
set IHS_HOST_TABLE=/usr/work/host_table.txt
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

For [AHS] section

Windows32/64

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
:DEFINITION_PART
  ...
rem [AHS]
set AHS_TARGET=on
set AHS_OPTION=2
set AHS_HOST_TABLE=C:\Work\host_table.txt
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Solaris32/64

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
  [AHS]
  target = on
  option = 1
```

```
  ahs_host_table = /usr/work/host_table.txt
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Linux32/64

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
DEFINITION_PART:
```

```
  ...
```

```
#[AHS]
```

```
set AHS_TARGET=on
```

```
set AHS_OPTION=2
```

```
set AHS_HOST_TABLE=/usr/work/host_table.txt
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Enter the following descriptions in host_table.txt.

```
(IP address before conversion) > (IP address after conversion)
(Host name before conversion) > (Host name after conversion)
```

- To comment out a line, enter a hash sign (#) at the start of the line.
- Half-width spaces and tabs are ignored.

Example

Convert the host name and IP address as shown below:

- Before conversion: IP address "192.168.0.1", After conversion: IP address "192.168.0.3"
- Before conversion: IP address "192.168.0.2", After conversion: IP address "192.168.0.4"
- Before conversion: host name "www.fujitsu.com", After conversion: host name www.interstage.com
- Before conversion: host name "host1.fujitsu.com", After conversion: host name "host2.fujitsu.com"

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
### Host IP conversion table ###
..
# IP address conversion definition
  192.168.0.1 > 192.168.0.3
  192.168.0.2 > 192.168.0.4
..
# Host name conversion definition
  www.fujitsu.com > www.interstage.com
  host1.fujitsu.com > host2.fujitsu.com
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

- *6 In section [JMX], it if is necessary to change the Interstage JMX Service IP address when the resources are imported, specify the new IP address for JMX_IPADDRESS/ipaddress.

Examples

Windows32/64

The following is an example of the JMX_IPADDRESS definition.

```
:DEFINITION_PART
...
rem [JMX]
set JMX_TARGET=on
    rem ============================================================================
    rem Please specify the following definitions only when you edit
    rem IP address used by the Interstage JMX service.
    rem ============================================================================
set JMX_IPADDRESS=192.168.0.1
```

The following is an example of a description in the JMX_USERREP definition.

```
rem [JMX]
set JMX_USERREP = off
```

Linux32/64

The following is an example of the JMX_IPADDRESS definition.

```
DEFINITION_PART:
...
#[JMX]
set JMX_TARGET=on
    #============================================================================
    # Please specify the following definitions only when you edit
    # IP address used by the Interstage JMX service.
    #============================================================================
set JMX_IPADDRESS=192.168.0.1
```

The following is an example of a description in the JMX_USERREP definition.

```
#[JMX]
set JMX_USERREP = off
```

Solaris32/64

The following is an example of the ipaddress definition.

```
[JMX]
target = on
ipaddress = 192.168.0.1    # Host IP address
```

The following is an example of a description in the jmx_userrep definition.

```
[JMX]
JMX_USERREP = off
```

- *7 In Interstage Application Server Enterprise Edition cluster environments, restore the backup data collected on one node to both nodes.

- *8 In Interstage Application Server Enterprise Edition cluster environments:
  - If the primary node (FQDN for the failover IP address) certificate has been registered in the Interstage certificate environment, restore the backup data collected on one node to both nodes.
  - If certificates for each node have been registered in the Interstage certificate environment, collect backup data from both nodes and then restore it to each node.

12.3.4.3 Interstage Resource Backup/Export

Perform collective backup/export of Interstage resources.

The sample of backup target resource definition file with the name of backupdef.txt is shown below.

Windows32/64

```
isbackup
```

Solaris32/64

```
isbackup  backupdef.txt
```

Note

- Be sure that the disk for creating a directory for storing backup resource has enough free space. The disk space required for storing backup resource is the total sum of the amounts of backup target resources shown in 12.1.1 Outline.
- Back up the SSL resource when the CORBA Service resource is the backup target, and SSL is used by the CORBA Service. Refer "Note" in "12.1.5.5 Backing Up Interstage JMX Service Resource".
- For environment variable PORB_HOME, the installation directory "/opt/FJSVporb" of Portable-ORB must be specified (Solaris only). The operation targets are under the installation directory of Portable-ORB only. The resources for downloading operation of Portable-ORB or SSL operation are not the operation targets. For these non-target resources, refer to "12.1.5.8 Backing Up Portable-ORB Resource".
- The encryption information (service ID) file must be backed up from the shared disk if the Interstage Single Sign-on repository server is running in the following environments:
  - An environment that uses a cluster system.
  - An environment that uses session management.

  For details, refer to "Backing up Interstage Single Sign-on Resources" - "Backup Procedure (Repository Server Resources)".
- For Interstage HTTP Server, to back up the content (except for that in the directory specified in the DocumentRoot directive), and when a file used in setting the environment other than httpd.conf and the password file exists, save the corresponding file to the backup directory.

  When using SSL of certificate/key management environment (configured with the SMEE command), restore the following backed up resources to the path specified in the corresponding directive of the SSL environment definition file:
  - Slot information directory (directory specified in SSLSlotDir directive of httd.conf file)
  - Operation control directory (directory specified in SSLEnvDir directive of httd.conf file)
  - User PIN control file (directory specified in SSLUserPINFile directive of httd.conf file)

- For Interstage HTTP Server 2.2, to back up the content or CGI file (except for that in the directory specified in the DocumentRoot/Alias/ScriptAlias directive), and when a file used in setting the environment other than httpd.conf and the password file exists, save the corresponding file to the backup directory.

  When using SSL of certificate/key management environment (configured with the SMEE command), restore the following backed up resources to the path specified in the corresponding directive of the SSL environment definition file:

  - Slot information directory (directory specified in SSLSlotDir directive of httd.conf file)
  - Operation control directory (directory specified in SSLEnvDir directive of httd.conf file)
  - User PIN control file (directory specified in SSLUserPINFile directive of httd.conf file)

- If isbackup has an error, an error message is output at the erroneous point. If the command described in *isbackup* has an error, respond according to the output message of the command.
- *isbackup* uses the following commands:
  - *iscbackupsys*
  - *isguibackup*
  - *odbackupsys*
  - *esbackupsys*
  - *tdbackupsys*
  - *otsbackupsys* Windows32/64 Solaris32 Linux32/64
  - *jsbackup*
  - *jar*
  - *jmsbackup*
  - *j2eebackup*
  - *ijsbackup*
  - *ijbackup*
  - *ij6backup*
  - *ihsbackup*
  - *ahsbackup*
  - *wscbackup*
  - *ssobackup*
  - *irepbacksys*

    If an error occurs with their usage, check the command output message, and verify that it was used correctly using the command.
- If an error occurs in *isbackup*, delete the backup destination directory, and execute *isbackup* again.

Solaris32/64 Linux32/64

- When specifying the Interstage Directory Service resource as the backup or export target, if a backup file with same name exists, an overwrite message is output. Set the IREP_BACKUP_MODE environment variable to "SILENT" to disable output of this message and overwrite the existing file, then execute the *isbackup* command. Messages from the *irepbacksys* command are output to the system log (event log on Windows®).

12.3.5 Resource Restore/Import

The sample procedures of the collective Interstage resource restore and import are shown below.

Windows32/64

Restore

```
C:\Interstage\sample\backup_restore\isrestore.bat
```

Import

```
C:\Interstage\sample\backup_restore\isimport.bat
```

Solaris32/64

```
/opt/FJSVisas/sample/backup_restore/isrestore
```

The procedures of Interstage restore and import are described as an instruction in isrestore and isimport.

Each process has a comment in the format shown below according to the processing content.

```
#=====================================================
#   Number    Explanation of alphanumeric characters
#=====================================================
```

12.3.6 Process Outline

Explanation of each process outline

Windows32/64 Linux32/64

Table 12.6 Process Outline for Windows and Linux

Comment	Process content
:DEFINITION_PART	Restore target definition
:PROCEDURE_PART	Main process

Solaris32/64

Table 12.7 Process Outline for Solaris

Comment	Process content
0. Environment Check	Authorization check.
1. check the input parameter	Command parameter check.
2-1. set the restore CO	Command name variable definition.
2-2. set the section name list	Restore target variable definition.
2-3. get the file line and set line = 0	Syntax analysis of restore target resource files6.
2-4. check the def file format	
2-5. check sub-routines	
3. MAIN	Main process
4. Sub-Routines	Restore process of backup target resources

12.3.7 Restore/Import Process of Restore Target Resources

Restore/import process is delimited using the format shown below at each backup target resource.

```
## Service name  START
     :
   (Restore process description)
## Service name  END
```

Service names (changeable) correspond to the restore resources as listed below.

Table 12.8 Service Names with Corresponding Restore Resources

Servicename	Restore target resources
ISCOM	Restore of Interstage setup resources
GUI	Restore of Interstage Management Console resources
JMX	Restore of Interstage JMX Service resources
OD	Restore of CORBA service resources
ES	Restore of Event service resources
PORB	Restore of Portable-ORB resources
TD	Restore of Component Transaction service resources
Windows32/64 Solaris32 Linux32/64 OTS	Restore of Database Linkage Service resources
IJServer	Restore of IJServer resources
JMS	Restore of Interstage JMS resources
J2EE	Restore of J2EE common resources
IHS	Restore of Interstage HTTP Server resources
AHS	Restore of Interstage HTTP Server 2.2 resources
WSC	Restore of Web Server Connector (for Interstage HTTP Server 2.2) resources
ISSCS	Restore of Interstage Certificate Environment resources
IREP	Restore of Interstage Directory Service resources
SSOsv	Restore of Interstage Single Sign-on resource (Repository server)
SSOac	Restore of Interstage Single Sign-on resource (Authentication server)
SSOaz	Restore of Interstage Single Sign-on resource (Business server)
JavaEE	Restore of IJServer cluster resources
JavaEE6	Restore of Java EE 6 resources

12.3.8 Operation Procedures

Procedures of resource backup/export using the *isrestore* command are described below.

12.3.8.1 Stopping the Service

Windows32/64

Log in with Administrator authority, and use the *isstop* command to stop all the Interstage services and server applications.

Solaris32/64 Linux32/64

Use the *isstop* command to stop all the Interstage services and server applications.

```
isstop -f
```

Note

- Services that are not stopped by the *isstop* command must be stopped separately. For more information on how to stop Interstage services, refer to "12.1.5.1 Stopping Interstage Services".

12.3.8.2 Restore/Import Target Resource Definition

Windows32/64 Linux32/64

Define Interstage restore target resources in the batch file.

Use the following syntaxes to define the target resources:

Solaris32/64

Define Interstage restore target resources in the backup target definition file.

The restore target definition file can be created with an arbitrary name according to the following syntaxes:

For details, refer to "12.1 Backing Up and Restoring Resources" and "12.2.3 Resource Importing Procedure".

The sample of the restore target resource definition file is provided below.

Windows32/64

Define Interstage restore target resources in the batch file.

Solaris32/64

```
/opt/FJSVisas/sample/backup_restore/sample.def
```

Linux32/64

Define Interstage backup target resources in Shell.

12.3.8.2.1 Description Format

Windows32/64

Write one definition on a single line in the batch file

```
rem [Section name]
set definition name = Definition value
```

Solaris32/64

Write one definition on a single line in the definition file.

```
[Section name]
definition name = Definition value
```

Linux32/64

Write one definition on a single line in the shell.

```
# [Section name]
set definition name = Definition value
```

Note

- Write "[", "]", and "=" in en-size characters.
- Solaris32/64

  When writing a comment, write # after the definition value. Do not specify # at the top of a line.

12.3.8.2.2 Definition Item List

Restore target items are listed below.

- Section names or definition names cannot be omitted.
- Definition values are indicated as below.

  y: required; -: can be omitted; x: cannot be specified

Windows32/64 Linux32/64

Table 12.9 Restore Target Items for Windows and Linux

Section name	Explanation of section name	Definition name	Definition value	Explanation	Remarks
Common	Specifies basic information in operation.	HOST	Host name y	Specifies the import destination host name.	Effective at import only
		INST_DIR	Directory y	Interstage installation directory	Change according to the installation environment.
		COMMON_PATH	Directory y	Specifies a directory that stores the backup/export resources.	
ISCOM	Species Interstage setup resource related items.	ISCOM_TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
GUI	Specifies Interstage Management Console related items.	GUI_TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
JMX	Specifies Interstage JMX Service related items.	JMX_TARGET	on or off y	Specifies whether the Interstage JMX Service resources will be operation targets. on: They will be operation targets off: They will not be operation targets	

Section name	Explanation of section name	Definition name	Definition value	Explanation	Remarks
		JMX_IPADDRESS		If it will be necessary to convert the IP address used in the Interstage JMX Service when the resources are imported, specify the IP address. (*6) Specify this IP address in the cases shown below. If this item is not specified, the IP address will not be changed. - When the IP address is specified in isjmx.xml of the server in which the resources are backed up - When the resources are restored in a server that has multiple IP addresses, and another IP address is specified for the admin LAN IP address and business LAN IP address	
		JMX_USERREP	on or off	Specifies whether the Interstage JMX Service user repository definition will be a restore target. (*6) on: The resources are restored (default) off: The resources are not restored	
		JMX_SITEINFO	on or off y	To migrate the site, specify "on". Normally, specify "off".	
OD	Specifies CORBA service related items.	OD_TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
		OD_PORT	Port number y	Specifies the port number used for CORBA communication.	Effective at import only
		OD_DBPATH	Directory y	Specifies when changing the database directory used in the interface repository during importing.	Effective at import only
ES	Specifies event service related items.	ES_TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	

Section name	Explanation of section name	Definition name	Definition value	Explanation	Remarks
PORB	Specifies Portable-ORB related items.	PORB_ TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
TD	Specifies component transaction service related items.	TD_TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
OTS	Specifies database linkage service related items.	OTS_ TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
IJServer	Specifies IJServer related items.	IJSERVER_ TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
JMS	Specifies Interstage JMS related items.	JMS_ TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
J2EE	Specifies J2EE shared resource related items.	J2EE_ TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	(*2)
IHS	Specifies Interstage HTTP Server related items. (*3)	IHS_TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
		IHS_OPTION_FROM_V6	on or off	To restore/import V5.1/V6.0 resources backed up/exported using maintenance batch execution batch file (Windows®) or shell script (Linux) to an 8.0 environment, specify "on".	
		IHS_OPTION	1, 2 or 3	Specifies the operation target resources from below: 1. Environment definition information. 2. Environment definition information and password file. 3. Environment definition information, and directory specified in the DocumentRoot directive. 3 is enabled when IHS_OPTION_FROM_V6 is off.	

Section name	Explanation of section name	Definition name	Definition value	Explanation	Remarks
		IHS_HOST_ TABLE		If it is necessary to change the host name/IP address at the time of import, specify the file name containing the host name/IP address before and after conversion. This is enabled when IHS_OPTION_FROM_V6 is off. (*4)	
		IHS_PASSWD_SOURCE		Specifies the file name for the password file that was specified to restore and import V5.1/V6.0 resources when V5.1/V6.0 resources were backed up/imported. This is enabled when IHS_OPTION_FROM_V6 is on, and IHS_OPTION is 2.	
		IHS_PASSWD_TARGET		Specifies the restore/import target directory for the password file for restoring and importing resources in V5.1/V6.0. This is enabled when IHS_OPTION_FROM_V6 is on, and IHS_OPTION is 2.	
AHS	Specifies Interstage HTTP Server 2.2 related items. (*3)	AHS_TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
		AHS_OPTION	1, 2 or 3	Specifies the operation target resources from below: 1. Environment definition information. 2. Environment definition information and password file. 3. Environment definition information, password file, and contents.	
		AHS_HOST_ TABLE		If it is necessary to change the host name/IP address at the time of import, specify the file name containing the host name/IP address before and after conversion. (*4)	
WSC	Specifies Web Server Connector (for Interstage	WSC_TARGET	on or off y	An operation target when specifying "on". Not an	

Section name	Explanation of section name	Definition name	Definition value	Explanation	Remarks
	HTTP Server 2.2) related items.			operation target when specifying "off".	
		WSC_HOST_TABLE		When importing as follows, specify the name of a file (full path) that has a description of IP addresses before and after the change.(*1) - When the server is a standalone server - When the operation is by separating the IJServer cluster and the web server, and - IP addresses for the web container and web server are different at the import source and the export destination	
ISSCS(*8)	Specifies Interstage Certificate Environment related items.	ISSCS_ TARGET	on or off	An operation target when specifying "on". Not an operation target when specifying "off".	
		ISSCS_ OPTION	1 or 2	Specify the following resources: 1. SSL configuration file 2. Interstage certificate environment resources (SSL configuration file, certificate environment file) (Note) These are valid for import. Before selecting these resources, refer to "12.2.3.12 Importing Interstage Certificate Environment Resources".	
IREP(*7)	Specifies Interstage Directory Service related items.	IREP_ TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
SSOsv(*7)	Specifies Interstage Single Sign-on resource (Repository server) related items.	SSOSV_ TARGET	on or off	An operation target when specifying "on". Not an operation target when specifying "off".	
SSOac	Specifies Interstage Single Sign-on resource (Authentication	SSOAC_ TARGET	on or off	An operation target when specifying "on". Not an operation target when specifying "off".	

Section name	Explanation of section name	Definition name	Definition value	Explanation	Remarks
	server) related items.				
SSOaz	Specifies Interstage Single Sign-on resource (Business server) related items.	SSOAZ_ TARGET	on or off	An operation target when specifying "on". Not an operation target when specifying "off".	
JavaEE(*7)	Specifies Java EE related items.	JAVAEE_ TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying	
		IP_HOST_FILE		Contains the path name for the IP address/host name settings file when resources are imported.	
JavaEE6	Specifies Java EE 6 related items.	JAVAEE6_TARGET	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
		JAVAEE6_IP_HOST_FILE		Contains the path name for the IP address/host name settings file when resources are imported.	

Solaris32/64

Table 12.10 Restore Target Items for Solaris

Section name	Explanation of section name	Definition name	Definition value	Explanation	Remarks
Common	Specifies basic information in operation.	host	Host name Restore: - Import: y	Specifies the import destination host name.	
		path	Directory y	Specifies a directory that stores the backup/export resources.	
		target_server	current or others y	Specifies "current" for restores. Specifies "others" for export operation.	
ISCOM	Species Interstage setup resource related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
GUI	Specifies Interstage Management Console items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
JMX	Specifies Interstage JMX	target	on or off	Specifies whether the Interstage JMX Service	

Section name	Explanation of section name	Definition name	Definition value	Explanation	Remarks
	Service related items.		y	resources will be operation targets. on: They will be operation targets off: They will not be operation targets	
		ipaddress		If it will be necessary to convert the IP address used in the Interstage JMX Service when the resources are imported, specify the IP address. (*6) Specify this IP address in the cases shown below. If this item is not specified, the IP address will not be changed. - When the IP address is specified in isjmx.xml of the server in which the resources are backed up - When the resources are restored in a server that has multiple IP addresses, and another IP address is specified for the admin LAN IP address and business LAN IP address	
		jmx_userrep	on or off	Specifies whether the Interstage JMX Service user repository definition will be a restore target. (*6) on: The resources are restored (default) off: The resources are not restored	
		siteinfo	on or off y	To migrate the site, specify "on". Normally, specify "off".	
OD	Specifies CORBA service related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
		port	Port number Restore: - Import: x	Specifies only in restore or import.	
		db_path	Directory	Specifies only in restore or import.	

Section name	Explanation of section name	Definition name	Definition value	Explanation	Remarks
			Restore: - Import: x		
ES	Specifies event service related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
PORB	Specifies Portable-ORB related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
TD	Specifies component transaction service related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
Solaris32 OTS	Specifies database linkage service related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
IJServer	Specifies IJServer related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
JMS	Specifies Interstage JMS related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	(*1)
J2EE	Specifies J2EE shared resource related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	(*2)
IHS	Specifies Interstage HTTP Server related items. (*3)	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
		from_v6	on or off	To restore/import V5.1/ V6.0 resources backed up/ exported using maintenance batch execution shell script to an 8.0 environment, specify "on".	
		option	1, 2 or 3	Specifies the operation target resources from below. 1. Environment definition information. 2. Environment definition information and password file.	

Section name	Explanation of section name	Definition name	Definition value	Explanation	Remarks
				3. Environment definition information, and directory specified in the DocumentRoot directive. 3 is enabled when from_v6 is off.	
		ihs_host_ table		If it is necessary to change the host name/IP address at the time of import, specify the file name (full path) containing the host name/IP address before and after conversion. This is enabled when from_v6 is off (*4)	
		passwd_ source		Specifies the file name for the password file that was specified to restore and import V5.1/V6.0 resources when V5.1/V6.0 resources were backed up/imported. This is enabled when from_v6 is on, and option is 2.	
		passwd_ target		Specifies the restore/import target directory for the password file for restoring and importing resources in V5.1/V6.0. This is enabled when from_v6 is on, and option is 2.	
AHS	Specifies Interstage HTTP Server 2.2 related items. (*3)	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
		option	1, 2 or 3	Specifies the operation target resources from below: 1. Environment definition information. 2. Environment definition information and password file. 3. Environment definition information,	

Section name	Explanation of section name	Definition name	Definition value	Explanation	Remarks
				password file, and contents.	
		ahs_host_ table		If it is necessary to change the host name/IP address at the time of import, specify the file name (full path) containing the host name/IP address before and after conversion. (*4)	
WSC	Specifies Web Server Connector (for Interstage HTTP Server 2.2) related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
		wsc_host_table		When importing as follows, specify the name of a file (full path) that has a description of IP addresses before and after the change. - When the server is a standalone server - When the operation is by separating the IJServer cluster and the web server, and IP addresses for the web container and web server are different at the import source and the export destination.	
ISSCS(*8)	Specifies Interstage Certificate Environment related items.	target	on or off	An operation target when specifying "on". Not an operation target when specifying "off".	
		option	1 or 2	Specify the following resources: 1. SSL configuration file. 2. Interstage certificate environment resources (SSL configuration file, certificate environment file). (Note) These are valid for import. Before selecting these resources, refer to "12.2.3.12 Importing	

Section name	Explanation of section name	Definition name	Definition value	Explanation	Remarks
				Interstage Certificate Environment Resources".	
IREP	Specifies Interstage Directory Service related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
SSOsv(*7)	Specifies Interstage Single Sign-on resource (Repository server) related items.	target	on or off	An operation target when specifying "on". Not an operation target when specifying "off".	
SSOac	Specifies Interstage Single Sign-on resource (Authentication server) related items.	target	on or off	An operation target when specifying "on". Not an operation target when specifying "off".	
SSOaz	Specifies Interstage Single Sign-on resource (Business server) related items.	target	on or off	An operation target when specifying "on". Not an operation target when specifying "off".	
JavaEE(*7)	Specifies Java EE related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
		ip_host_file		Contains the path name for the IP address/host name settings file when resources are imported.	
JavaEE6	Specifies Java EE 6 related items.	target	on or off y	An operation target when specifying "on". Not an operation target when specifying "off".	
		javaee6_ip_host_file		When importing resources, specify the name of a file (full path) that has a description of IP addresses before and after the change.	

The following notes relate to Table 12.9 Restore Target Items for Windows and Linux and Table 12.10 Restore Target Items for Solaris.

- ***1** For [JMS] section, the following path to CLASSPATH must be specified for restore.

  Solaris32/64

```
CLASSPATH=/opt/FJSVj2ee/lib/isj2ee.jar:/opt/FJSVjms/lib/fjmsprovider.jar
```

- *2 For [J2EE] section, the directory that stores *jar* command must be included in the environment variable PATH because *jar* command is used in the internal process.

- *3 For the Interstage HTTP Server, when the SSL definition is set with Interstage Management Console, it must be restored in the [ISSCS] section.
- *4 If it is necessary to change the host name/IP address of the [IHS]/[AHS] section during import, specify the file name containing the host name/IP address before and after the change in IHS_HOST_TABLE/AHS_HOST_TABLE.

Example

For [IHS] section

Windows32/64

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
:DEFINITION_PART
...
rem [IHS]
set IHS_TARGET=on
set IHS_OPTION_FROM_V6=off
rem 1: set DEF only, 2: set DEF and password file 3: set DEF and password
and DocumentRoot
set IHS_OPTION=2
set IHS_HOST_TABLE=C:\Work\host_table.txt
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Solaris32/64

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
  [IHS]
  target = on
  from_v6 = off
  option = 1
  ihs_host_table = /usr/work/host_table.txt
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Linux32/64

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
DEFINITION_PART:
...
#[IHS]
set IHS_TARGET=on
set IHS_OPTION_FROM_V6=off
# 1: set DEF only, 2: set DEF and password file 3: set DEF and password
and DocumentRoot
set IHS_OPTION=2
set IHS_HOST_TABLE=/usr/work/host_table.txt
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

For [AHS] section

Windows32/64

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
:DEFINITION_PART
  ...
rem [AHS]
set AHS_TARGET=on
set AHS_OPTION=2
set AHS_HOST_TABLE=C:\Work\host_table.txt
```

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Solaris32/64

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
  [AHS]
  target = on
  option = 1
  ahs_host_table = /usr/work/host_table.txt
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Linux32/64

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
DEFINITION_PART:
```

```
  ...
```

```
#[AHS]
```

```
set AHS_TARGET=on
```

```
set AHS_OPTION=2
```

```
set AHS_HOST_TABLE=/usr/work/host_table.txt
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Enter the following descriptions in host_table.txt.

```
(IP address before conversion) > (IP address after conversion)
(Host name before conversion) > (Host name after conversion)
```

- To comment out a line, enter a hash sign (#) at the start of the line.
- Half-width spaces and tabs are ignored.

Example

Convert the host name and IP address as shown below:

- Before conversion: IP address "192.168.0.1", After conversion: IP address "192.168.0.3"
- Before conversion: IP address "192.168.0.2", After conversion: IP address "192.168.0.4"
- Before conversion: host name "www.fujitsu.com", After conversion: host name www.interstage.com
- Before conversion: host name "host1.fujitsu.com", After conversion: host name "host2.fujitsu.com"

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
### Host IP conversion table ###

# IP address conversion definition
  192.168.0.1 > 192.168.0.3
  192.168.0.2 > 192.168.0.4

# Host name conversion definition
  www.fujitsu.com > www.interstage.com
  host1.fujitsu.com > host2.fujitsu.com
```

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

- *6 Windows32/64 In section [JMX], it if is necessary to change the Interstage JMX Service IP address when the resources are imported, specify the new IP address for JMX_IPADDRESS/ipaddress.

  Examples

  Windows32/64

  The following is an example of the JMX_IPADDRESS definition.

```
:DEFINITION_PART
...
rem [JMX]
set JMX_TARGET=on
    rem ========================================================================
    rem Please specify the following definitions only when you edit
    rem IP address used by the Interstage JMX service.
    rem ========================================================================
set JMX_IPADDRESS=192.168.0.1
```

  The following is an example of a description in the JMX_USERREP definition.

```
rem [JMX]
set JMX_USERREP = off
```

  Linux32/64

  The following is an example of the JMX_IPADDRESS definition.

```
DEFINITION_PART:
...
#[JMX]
set JMX_TARGET=on
    #========================================================================
    # Please specify the following definitions only when you edit
    # IP address used by the Interstage JMX service.
    #========================================================================
set JMX_IPADDRESS=192.168.0.1
```

  The following is an example of a description in the JMX_USERREP definition.

```
#[JMX]
set JMX_USERREP = off
```

  Solaris32/64

  The following is an example of the ipaddress definition.

```
[JMX]
target = on
ipaddress = 192.168.0.1    # Host IP address
```

  The following is an example of a description in the jmx_userrep definition.

```
[JMX]
JMX_USERREP = off
```

- *7 In Interstage Application Server Enterprise Edition cluster environments, restore the backup data collected on one node to both nodes.
- *8 In Interstage Application Server Enterprise Edition cluster environments:
  - If the primary node (FQDN for the failover IP address) certificate has been registered in the Interstage certificate environment, restore the backup data collected on one node to both nodes.
  - If certificates for each node have been registered in the Interstage certificate environment, collect backup data from both nodes and then restore it to each node.

12.3.8.3 Interstage Resource Restore/Import

Perform collective backup/export of Interstage resources.

The sample of backup target resource definition file with the name of backupdef.txt is shown below.

Windows32/64

Restore

```
isrestore.bat
```

Import

```
isimport.bat
```

Solaris32/64

```
isrestore  backupdef.txt
```

Note

- Restore the SSL resource when the CORBA Service resource is the restore target, and the SSL resource is backed up. Refer to "Note" in "12.1.6.5 Restoring CORBA Service Resource" for details.
- For environment variable PORB_HOME, the installation directory "/opt/FJSVporb" of Portable-ORB must be specified (Solaris only). The operation targets are under the installation directory of Portable-ORB only. The resources for downloading the operation of Portable-ORB or SSL operation are not the operation targets. For these non-target resources, refer to "12.1.5.8 Backing Up Portable-ORB Resource" to restore/import.
- If the Interstage Single Sign-on repository server resources were backed up from the shared disk, refer to "Restoring Interstage Single Sign-on Resources" - "Restore Procedure (Repository Server Resources)", and then restore the encryption information (service ID) file.
- For Interstage HTTP Server, to back up the content (except for that in the directory specified in the DocumentRoot directive), and the file used in setting the environment (other than httpd.conf) and the password file were backed up, restore the corresponding files.

  When using the SSL of certificate/key management environment (configured with the SMEE command), restore the following backed up resources to the path specified in the corresponding directive of httpd.conf file:

  - Slot information directory (directory specified in SSLSlotDir directive of httd.conf file)

  - Operation control directory (directory specified in SSLEnvDir directive of httd.conf file)
  - User PIN control file (file specified in SSLUserPINFile directive of httd.conf file)

- For Interstage HTTP Server 2.2, to back up the content or CGI file (except for that in the directory specified in the DocumentRoot/Alias/ScriptAlias directive), and the file used in setting the environment (other than httpd.conf) and the password file were backed up, restore the corresponding files.

  When using the SSL of certificate/key management environment (configured with the SMEE command), restore the following backed up resources to the path specified in the corresponding directive of httpd.conf file:

  - Slot information directory (directory specified in SSLSlotDir directive of httd.conf file)
  - Operation control directory (directory specified in SSLEnvDir directive of httd.conf file)
  - User PIN control file (file specified in SSLUserPINFile directive of httd.conf file)

- If *isrestore* detects an error, an error message is output at the erroneous point. If the commands described in *isrestore* have an error, respond according to the output message of the command.

- *isrestore* uses the following commands:

  - *iscrestoresys*
  - *isguirestore*
  - *odrestoresys*
  - *esrestoresys*
  - *tdrestoresys*
  - *otsrestoresys* Windows32/64 Solaris32 Linux32/64
  - *jsrestore*
  - *jar*
  - *jmsrestore*
  - *j2eerestore*
  - *ijsrestore*
  - *ijrestore*
  - *ij6restore*
  - *ihsbackup*
  - *ahsbackup*
  - *wscrestore*
  - *ssorestore*
  - *ireprestsys*

  If an error occurs with their usage, check the command output message, and verify that it was used correctly using the command.

Linux32/64

- There is no execution authority for the sample shell script. To use the sample shell script, execution authority is necessary.

Chapter 13 Performance Monitoring

13.1 Introduction

The Performance Monitoring Tool includes the functionality to obtain performance information for:

- EJB application (for an old version compatible environment) operating on the business server
- Light EJB container (for an old version compatible environment)
- IJServer EJB container
- Transaction applications
- Wrapper objects (only Windows® and Solaris)
- CORBA applications.

Note: Old version refers to the operation execution environment of Application Server V5 and older.

The Performance Monitoring Tool provides the following two functionalities:

1. 13.2.1.1 Output of Log Information to the Performance Log File

   This function collects the performance information of specified objects in the performance log file. The accumulated performance information can be output in CSV format using the report output command.

2. 13.2.1.2 Realtime Monitoring of Performance Information by a Network Control Manager (Monitoring by MIB)

   By using the Management Information Base (MIB) (*1) monitoring function of a Network Control Manager such as Systemwalker CentricMGR (*2), the performance information of the specified object can be displayed and monitored in real time.

   Displaying and monitoring performance information using a Network Control Manager is called 'real-time monitoring'.

The Performance Monitoring Tool consists of the Performance Monitoring Logger that collects performance information, and various commands.

This chapter describes how to issue commands on the application server, and display performance information when using Systemwalker CentricMGR as a Network Control Manager.

*1 MIB is a management information area that has been defined for managing the system and TCP/IP information.

*2 Network Control Manager is a software program for displaying and monitoring performance information on the monitor server.

Note

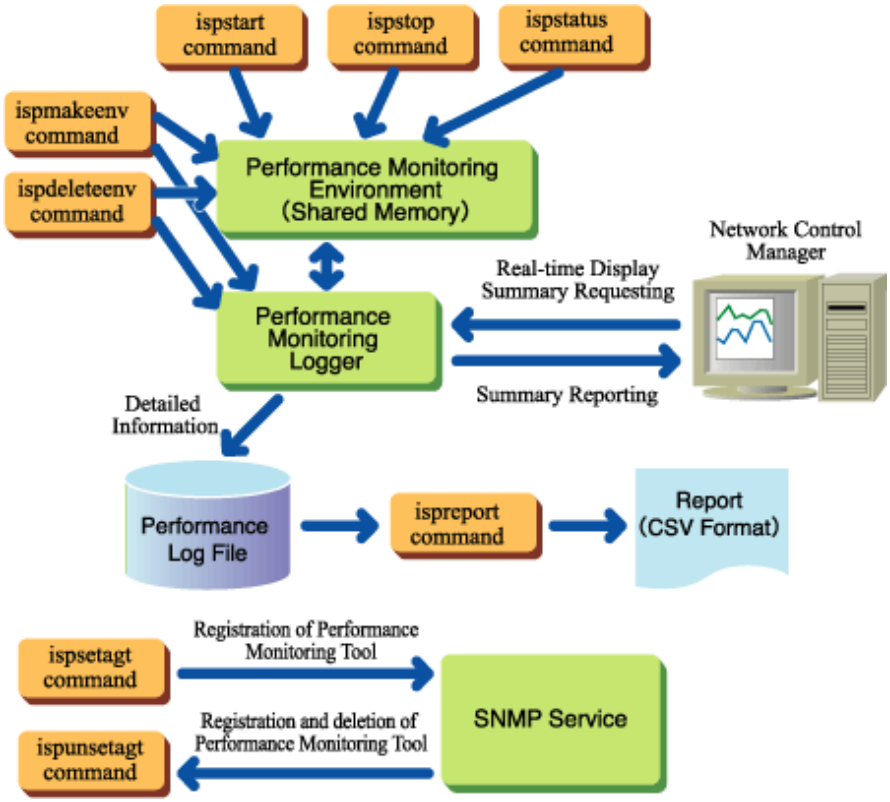
- Performance information on IJServers of type IJServer (Web + EJB [same VM]) and IJServer (Web Only) cannot be obtained.

13.2 The Performance Monitoring Tool

The Performance Monitoring Tool provides the commands shown in the following figures.

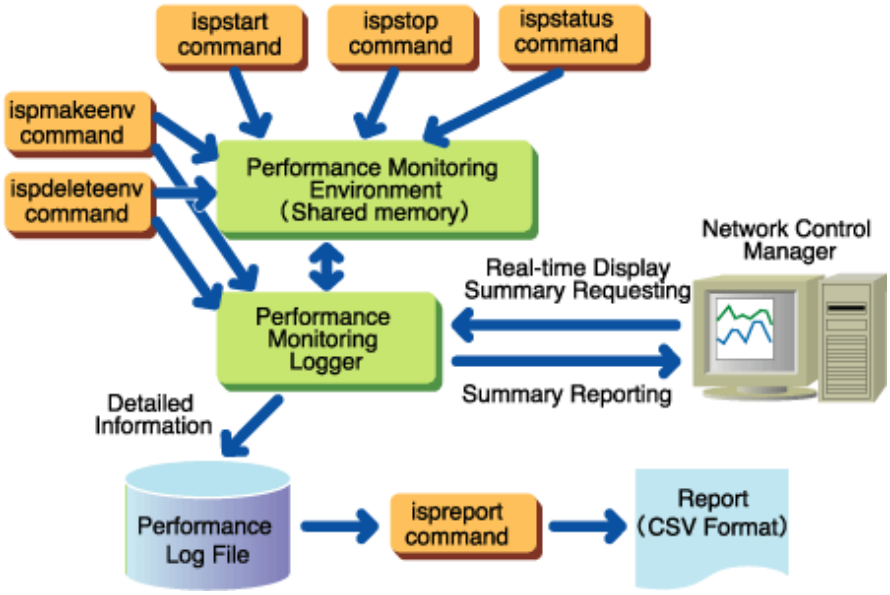
Windows32/64

Figure 13.1 Performance Monitoring Tool Commands



Solaris32/64

Figure 13.2 Performance Monitoring Tool Commands



Windows32/64 Solaris32/64

ispmakeenv command: Creates the performance monitoring environment and starts the performance monitoring logger

ispdeleteenv command: Deletes the performance monitoring environment and stops the performance monitoring logger

ispstart command: Starts monitoring performance

ispstop command: Stops monitoring performance

ispstatus command: Displays performance monitoring status information.

ispreport command: Outputs the performance log file report

Windows32/64

ispsetagt command: Registers the Performance Monitoring Tool with the SNMP service.

ispunsetagt command: Unregisters the Performance Monitoring Tool with the SNMP service.

13.2.1 Functions Provided by the Performance Monitoring Tool

This section describes the Performance Monitoring Tool functions.

13.2.1.1 Output of Log Information to the Performance Log File

This function collects performance information of specified objects of the transaction applications and the wrapper. The performance information is placed in the performance log file. The performance information is collected at the interval specified when the performance monitoring environment is created.

The accumulated performance information can be output in CSV format by executing the report output command. This is useful for performance information analysis and the accumulation of statistical information. These data items enable detailed performance analysis.

The information below can be collected using the log information output function.

Collection Start Date

Date performance information measurement for the record was started.

Data Collection Start Time

Time performance information measurement for the record was started.

Data Collection End Date

Date the performance information measurement for the record was finished.

Data Collection End Time

Time the performance information measurement for the record was finished.

EJB Application Name (EJB applications)

EJB application name (max 256 bytes).

Light EJB Container Name (Light EJB containers)

Light EJB container name/EJB application name (max 288 bytes).

IJServer Name/EJB application name (IJServer EJB containers)

IJServer name/EJB application name (Max 288 bytes).

Method Name + Signature

Name of the method to be monitored and signature (type of method argument and return value).

Process ID

Server application process ID.

Thread ID

ID of the thread in which the method to be monitored operates.

Request Processing Time (maximum/average/minimum)

Time (in milliseconds) required for executing the method in 'Method name' in this thread. This value is used for evaluating a method/signature pair.

Request Processing Wait Time (maximum/average/minimum)

Time (in milliseconds) from receiving a request from a client until method execution start. This value is used for evaluating each EJB application, Light EJB container or EJB container of IJServer.

This value is not collected if the EJB application, Light EJB container or EJB container of IJServer is a message-driven bean.

Number of Times the Operation has been Executed

Maximum number of requests that await processing by an EJB application, Light EJB container or EJB container of IJServer.

This value is used for evaluating each EJB application, Light EJB container or EJB container of IJServer.

This value is not collected if the EJB application, Light EJB container or EJB container of IJServer is a message-driven bean.

Number of Processes

Number of method operations in the 'Thread ID' thread. This value is used for evaluating a method/signature pair.

Number of Requests Received

Accumulated number of the EJB application, Light EJB container or EJB container of IJServer operations from when performance monitoring was started. This value is used for evaluating each EJB application, Light EJB container or EJB container of IJServer.

Number of EJB Object (Session)

This is the number of current EJB objects. The number of EJB objects is the difference between the number of executed create methods and executed remove methods. The output value is the maximum value within the interval time. This value is used for evaluating each EJB application, Light EJB container or EJB container of IJServer.

This value is not collected if the EJB application, Light EJB container or EJB container of IJServer is a message-driven bean.

Passivate Number for Entity (maximum)

Number of instance pooling in the EJB application, Light EJB container (process) or EJB container of IJServer. The output value is the maximum value in the time interval. This value is used for evaluating each EJB application, Light EJB container or EJB container of IJServer.

Size of Memory Area used in VM (maximum/average)

Memory (in kilobytes) used by the VM of the EJB application, Light EJB container or EJB container of IJServer. This value is used for evaluating each EJB application, Light EJB container or EJB container of IJServer.

13.2.1.2 Realtime Monitoring of Performance Information by a Network Control Manager (Monitoring by MIB)

The real time monitoring function reports the performance information of the specified objects of the transaction applications and the wrapper as MIB information (*1).

This function can only use the Windows® version and the Solaris version.

In Solaris 10 or later, real-time monitoring functions that use System Manager Agent (SMA) cannot be used. Instead, use Solstice Enterprise Agents (SEA) software. For details on how to make environment settings to use SEA without using SMA, refer to "13.2.1.2.1 Setting the Solaris 10 or later Environment to use SEA instead of SMA for Real-time Monitoring Functions".

Network Control Managers such as Systemwalker CentricMGR support the MIB monitoring function. Using the Network Control Manager function, the operations below can be performed.

- Output Statistical Information Report

  The performance information can be displayed in graph or CSV format. This is useful in the collection of statistical information.

- Monitor Performance Abnormality

  By setting the threshold value for performance information such as 'Number of requests awaiting processing' and monitoring it, abnormalities in performance information can be detected in advance. This function enables prompt response to abnormal events.

See

*1 The MIB is the defined management information domain in order to manage system information and TCP/IP information.

When this function is used, the information can be output to the performance log file at the same time. For a more detailed performance analysis such as information in units of operations, the information collected in the performance log file can be analyzed.

For the monitoring method using MIB information, refer to the manual of the Network Control Manager.

The information below can be collected using the realtime monitoring function.

EJB Application Name (EJB applications)

The name of the target EJB application.

Light EJB Container/EJB Application Name (Light EJB container)

Light EJB container/EJB application name.

IJServer name/EJB Application Name (IJServer EJB container)

IJServer name/EJB application name (Max 288 bytes).

Request Processing Time (maximum/average/minimum)

Processing time of the target EJB application, Light EJB container or EJB container of IJServer.

Request Processing Wait Time (maximum/average/minimum)

The time between acceptance of a request from a client application and processing start.

Number of Requests Awaiting Processing

The maximum number of requests placed in the EJB application.

Number of Requests Received

The accumulation value of the number of times by which the EJB application concerned or the Light EJB container was processed from when performance monitoring started.

13.2.1.2.1 Setting the Solaris 10 or later Environment to use SEA instead of SMA for Real-time Monitoring Functions

In Solaris 10 or later, real-time monitoring functions that use System Manager Agent (SMA) cannot be used. The following procedure shows an example of how to define environment settings to use SEA instead of SMA:

1. Stop SMA.

```
# /etc/init.d/init.sma stop
```

2. Configure the settings so that SMA and related services do not start automatically when the OS is booted.

   Configure the settings so that the following services do not start automatically when the OS is booted:

- svc:/application/management/sma
- svc:/application/management/seaport

```
# svcadm disable svc:/application/management/sma
# svcadm disable svc:/application/management/seaport
```

Since "svc:/application/management/snmpdx" has a dependency relationship with "svc:/application/management/seaport", "svc:/application/management/snmpdx" does not start when "svc:/application/management/seaport" is disabled. Remove the dependency relationship.

For details about settings, for example for the service dependency relationship, refer to the OS manual.

3. Change the port number used by SEA to '161'.

   Change the 'port' entry in the '/etc/snmp/conf/snmpdx.reg' file from '16161' to '161'

4. Create the SEA settings files.

```
# cp /etc/snmp/conf/mibiisa.rsrc- /etc/snmp/conf/mibiisa.rsrc
# cp /etc/snmp/conf/snmpdx.acl /etc/snmp/conf/mibiisa.acl
```

5. Restart SEA.

```
# /etc/init.d/init.snmpdx stop
# /etc/init.d/init.shmpdx start
```

Note

- The port number used by Solstice Enterprise Agents (SEA) software is not 161, (the default SNMP port number). To use '161' as the port number, change the 'port' line in the following file as demonstrated in step 4 above:

```
/etc/snmp/conf/snmpdx.reg
```

13.2.2 Performance Monitoring Procedure

13.2.2.1 Performance Monitoring Procedure for Windows Version

To monitor and analyze the performance of Interstage job applications using the Performance Monitoring Tool:

1. Register with the SNMP service
2. Start the Performance Monitoring Tool
3. Monitor
4. Stop the Performance Monitoring Tool
5. Delete the Performance Monitoring Tool from the SNMP service.

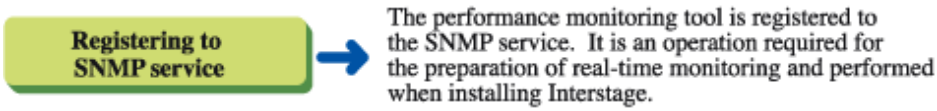
Each step is explained in below.

13.2.2.1.1 Registering with the SNMP Service

Register the Performance Monitoring Tool with the SNMP service.

Register Interstage with the SNMP service.

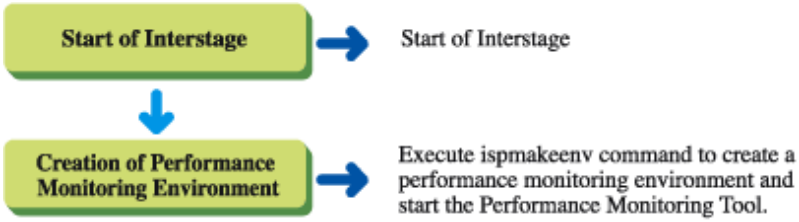
Figure 13.3 Registering with the SNMP Service



13.2.2.1.2 Starting the Performance Monitoring Tool

Start the Performance Monitoring Tool as shown in the following figure.

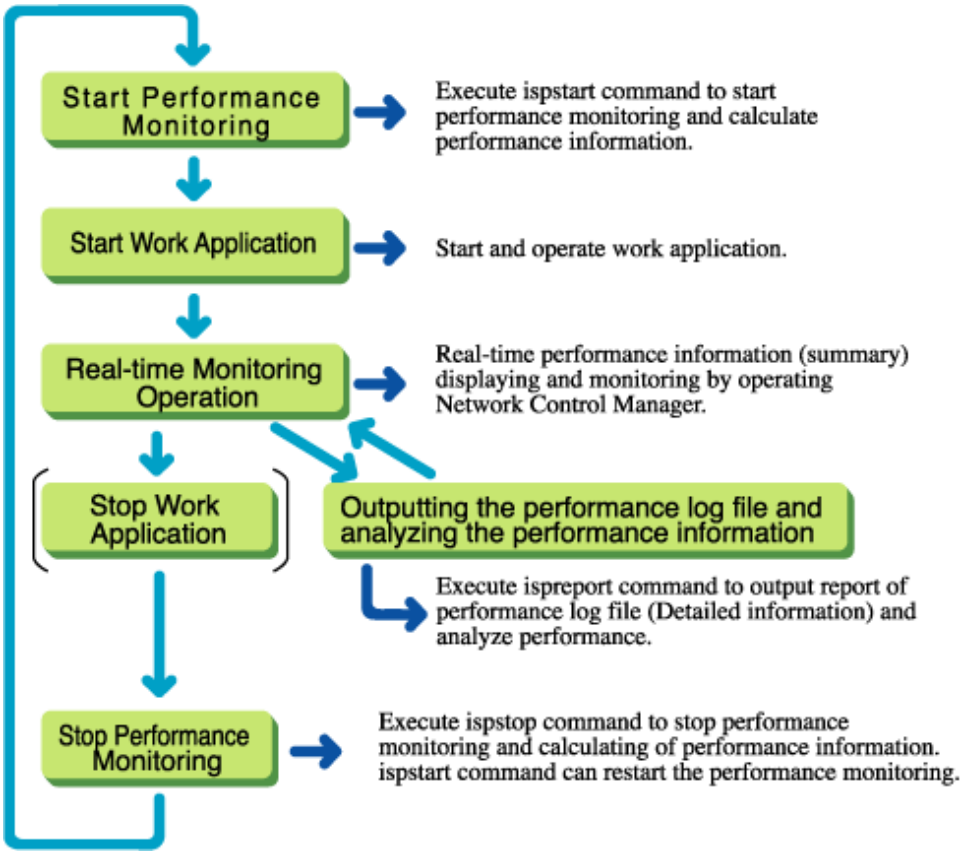
Figure 13.4 Starting the Performance Monitoring Tool



13.2.2.1.3 Monitoring

Follow the procedure in the following diagram to measure, monitor and analyze performance information.

Figure 13.5 Monitoring



Note

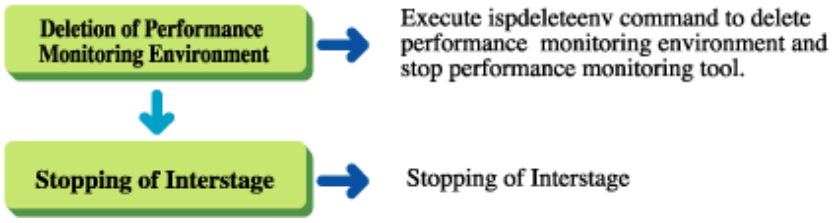
- Performance monitoring can be stopped by executing the *ispstop* command instead of stopping the application. However, performance information will not be measured after execution of the *ispstop* command. To restart measuring performance information, execute the *ispstart* command.

- After the *ispmakeenv* command is executed, start the business application (WorkUnit) that measures the performance. Performance of business applications started before execution of the *ispmakeenv* command is not measured.
- When a Network Control Manager such as Systemwalker CentricMGR is used to display performance information in real time, do not start or stop performance monitoring while performance information is being displayed. Ensure that the performance information display screen is closed before starting performance monitoring, and perform real-time monitoring operation and display performance information after performance monitoring is started.

13.2.2.1.4 Stopping the Performance Monitoring Tool

Follow the procedure in the following diagram to stop the Performance Monitoring Tool.

Figure 13.6 Stopping the Performance Monitoring Tool



Note

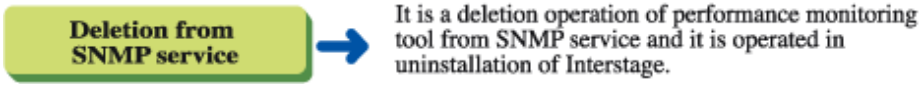
- Restart Interstage before creating the performance monitoring environment again.

13.2.2.1.5 Deleting the Performance Monitoring Tool from the SNMP Service

Follow the procedure in the following diagram to uninstall Interstage.

Delete the Performance Monitoring Tool registered in the SNMP service.

Figure 13.7 Deleting the Performance Monitoring Tool



13.2.2.2 Performance Monitoring Procedure for Solaris Version

To monitor and analyze the performance of Interstage job applications using the Performance Monitoring Tool:

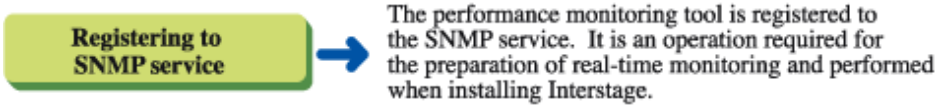
1. Register with the SNMP Service
2. Start the Performance Monitoring Tool
3. Monitor
4. Stop the Performance Monitoring Tool.

Each step is explained in below.

13.2.2.2.1 Registering with the SNMP Service

Register the Performance Monitoring Tool in the SNMP service during Interstage installation.

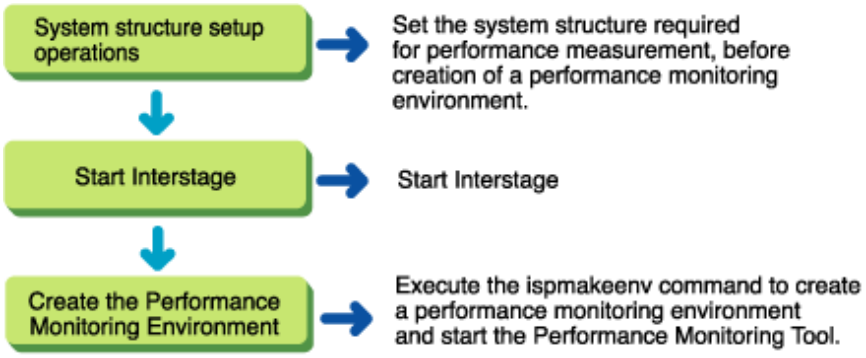
Figure 13.8 Installing



13.2.2.2.2 Starting the Performance Monitoring Tool

Follow the procedure in the following diagram to start the Performance Monitoring Tool.

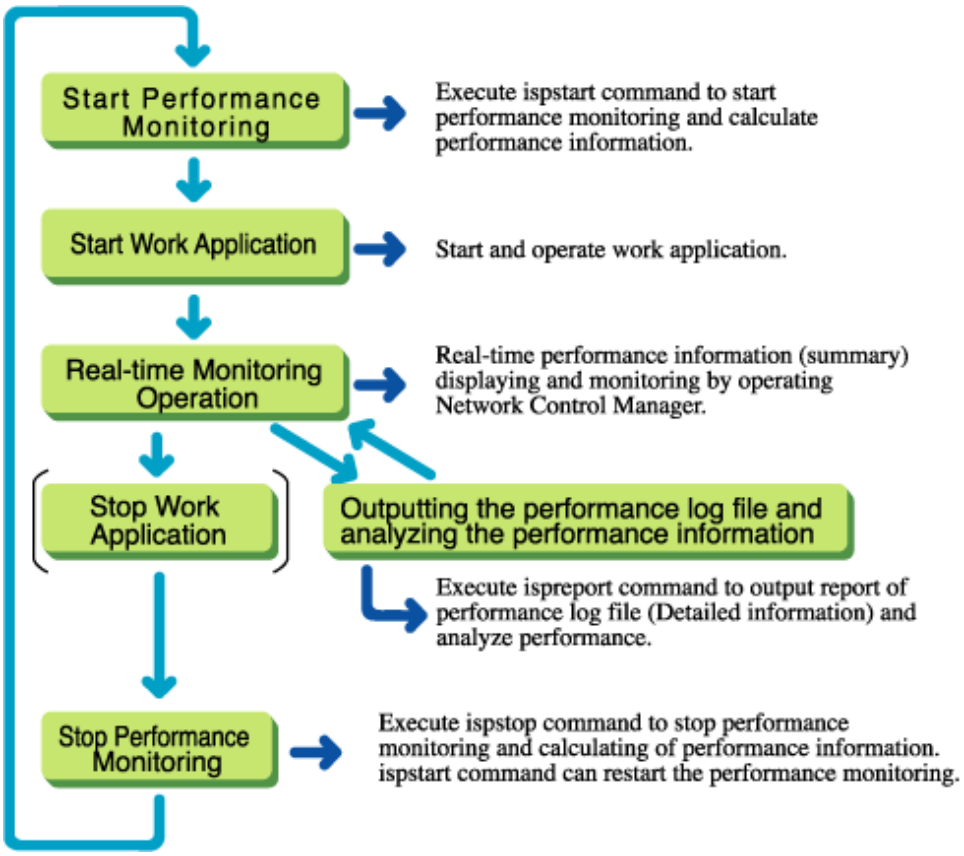
Figure 13.9 Starting the Performance Monitoring Tool



13.2.2.2.3 Monitoring

Follow the procedure in the following diagram to measure, monitor, and analyze performance information.

Figure 13.10 Monitoring Operation



Note

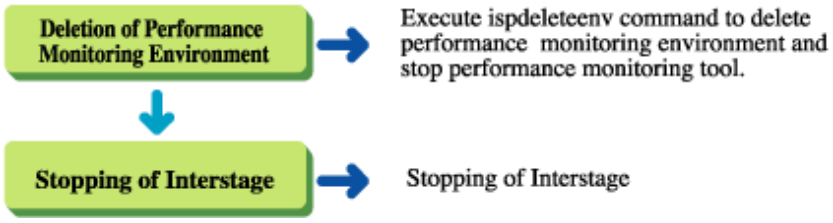
- Performance monitoring can be stopped by executing the *ispstop* command instead of stopping the application. However, performance information will not be measured after the *ispstop* command is executed. To restart measuring performance information, execute the *ispstart* command.
- After the *ispmakeenv* command is executed, start the business application (WorkUnit) that measures the performance. The performance of the business applications that are started before the execution of the *ispmakeenv* command is not measured.

- When a Network Control Manager such as Systemwalker CentricMGR is used to display performance information in real time, do not start or stop performance monitoring while performance information is being displayed. Ensure that the performance information display screen is closed before starting performance monitoring, and perform real-time monitoring operation and display performance information after performance monitoring is started.

13.2.2.2.4 Stopping the Performance Monitoring Tool

Follow the procedure in the following diagram to stop the Performance Monitoring Tool.

Figure 13.11 Stopping the Performance Monitoring Tool



Note

- Restart Interstage before creating the performance monitoring environment again.

13.2.2.3 Registering with the SNMP Service

After Interstage installation, the following operation is required to allow real-time performance monitoring with a Network Control Manager such as Systemwalker CentricMGR.

Note

- If real-time monitoring is not required, the following operation can be omitted.

Windows32/64

Execute the *ispsetagt* command to register the Performance Monitoring Tool in the SNMP service. After executing the *ispsetagt* command, re-start the SNMP service from the 'Service' dialog in Windows. The Performance Monitoring Tool can be registered in the SNMP service only when the SNMP service has been installed. Before executing the *ispsetagt* command, install the SNMP service.

Windows Server® 2003

To install the SNMP service in Windows Server® 2003:

1. Insert the Windows Server® 2003 CD-ROM into the CD drive.
2. Select "Install optional Windows components". The Windows Components Wizard will be displayed.
3. Select "Management and Monitoring Tools".
4. Click the Details button.
5. Select "Simple Network Management Protocol" (SNMP).
6. Click the OK button.
7. Click the Next button.
8. Click the Finish button.

Windows Server® 2008 or later

To install the SNMP service in Windows Server® 2008 or later:

1. Run Server Manager
2. Click "Features"
3. Click "Add Features"
4. Select and install "SNMP Service".

13.2.2.3.1 Copying the Performance Monitoring Tool Solaris32/64

Copy the Performance Monitoring Tool files shown in the following tables to the indicated directories to enable the Network Control Manager to display performance information. Copy these files during Interstage installation. Reboot the machine when the files have been copied.

Table 13.1 Performance Monitoring Tool Files

Filename	Copy source directory	Copy destination directory
ispsubad8	TD_HOME/isp/lib	/usr/lib/snmp
ispsuba8.acl	/etc/opt/FSUNtd/snmp/conf	/etc/snmp/conf
ispsuba8.reg	/etc/opt/FSUNtd/snmp/conf	/etc/snmp/conf
ispsuba8.rsrc	/etc/opt/FSUNtd/snmp/conf	/etc/snmp/conf

TD_HOME: Component Transaction Service installation directory

Note

- When using the real-time monitoring function of the performance monitoring tool, the mandatory software must be installed and the mandatory patch must be applied.

13.2.2.3.2 Reading the MIB Definition File

To collect performance information from the Network Control Manager, the MIB definition file for performance information must be read using the Network Control Manager. Use the following method to enable the Network Control Manager to read the MIB definition file from the machine on which Interstage has been installed:

- When the Network Control Manager operates under Windows®

  Read TD_HOME\isp\mib\ispmibNT.my

- When the Network Control Manager operates under Solaris

  Read TD_HOME\isp\mib\ispmibSol.my.

When using the Windows® version of Systemwalker CentricMGR (operation management server), read the MIB definition file as follows:

1. Use FTP or a similar application to copy the MIB definition file from the machine on which Interstage is installed to the machine on which Systemwalker CentricMGR is installed.
2. Activate Systemwalker CentricMGR System Monitor.
3. Choose **Tools**, and then Extend MIB from the System Monitor screen to display the Extend MIB screen.
4. Click the add button on the MIB Extension Operation screen to display the Select of Extend MIB File Selection screen.
5. Select the MIB file from the Extension MIB File Selection screen, and click the Open button. Then, click the Close button on the MIB Extension Operation screen.

When using the Solaris version of Systemwalker CentricMGR, read the MIB definition file as follows:

1. Use FTP to copy the MIB definition file from the machine on which Interstage is installed to the job management client on which Systemwalker CentricMGR is installed.
2. Activate Systemwalker CentricMGR (Job Monitor).
3. Choose **Tools**, and then Extend MIB from the Job Monitor screen to display the MIB Extension Operation screen.

4. Click the add button on the MIB Extension Operation screen to display the Extend MIB File Selection screen.
5. Select the MIB file from the Extend MIB File Selection screen, and then click the Open button. Then, click the Close button on the MIB Extension Operation screen.
6. Choose Policy, then Distribute policy from the Job Monitor screen to display the Policy Distribution screen.
7. Set the required items in the Policy Distribution screen, and then click the OK button.

13.2.2.3.3 Setting the Port Number Solaris32/64

The Performance Monitoring Tool uses a communications port to post performance information to the Network Control Manager. The default port number is 7042. If this port number is used by other programs, change the Performance Monitoring Tool port number during Interstage installation. Then, reboot the system.

To change the port number:

1. Use an editor to open the environment settings file.

   /etc/snmp/conf/ispsuba8.reg.

   The file contains the following information:

```
agents =
  {
    {
      name = "ispsubad8"
          subtrees = { isPerformanceInf }
      timeout = 40000000
      watch-dog-time = 2000000
      port = 7042
    }
  }
```

2. Replace the '7042' part of 'port = 7042' with an unused port number.
3. Save the file and close the editor.
4. Restart the system.

13.2.2.4 Setting System Configuration Information

Solaris32/64

The system configuration information shown below must be modified in the system configuration information file before the performance monitoring environment is created and the Performance Monitoring Tool started. Following modification, reboot the system.

```
Semsys:seminfo_semmnu
```

Always estimate the values to be set in the above system configuration information before starting the Performance Monitoring Tool. If the estimation suggests that the settings do not need to be changed, the system configuration information need not be set again.

Refer to the Environment information in the Tuning Guide for details of how to estimate the values to be set.

13.2.3 Creating a Performance Monitoring Environment

13.2.3.1 Starting the Performance Monitoring Tool Operation

To construct the environment for using the performance monitoring tool:

1. Start Interstage

2. Create the Performance Monitoring Environment.

Each step is explained in below.

13.2.3.1.1 Starting Interstage

Execute the *isstart* command to start Interstage.

13.2.3.1.2 Creating the Performance Monitoring Environment

Use the *ispmakeenv* command to create a performance monitoring environment and activate the Performance Monitoring Tool.

In this case, the following two interval times are specified:

- Interval time for performance log file

  The interval at which the performance information is output to the performance log file. The interval can be 5, 10, 20, or 30 minutes or 1, 2, 3, or 4 hours. The default is one hour.

- Interval time for real time monitoring

  The interval for collecting the performance information to be notified to the Network Control Manager. Specify the interval time when performance monitoring is executed from the Network Control Manager. The interval can be specified between 1 and 60 minutes. The default is 5 minutes.

After the *ispmakeenv* command has executed, start the business application (WorkUnit) that measures the performance. Performance is not measured for business applications that are started up before the *ispmakeenv* command is executed.

13.2.4 Monitoring Operations

This section describes monitoring using the performance monitoring tool.

13.2.4.1 Starting Performance Monitoring

Use the *ispstart* command to start performance monitoring of the specific object. From this point onwards, the performance information is output to the performance log file at the interval specified in the performance monitoring tool automatic start definition file (Windows® Enterprise Edition or Standard Edition only) or *ispmakeenv* command.

Performance information is collected until it is stopped by the *ispstop* command.

These commands are shown in the following figure.

Figure 13.12 Starting and Terminating Performance Monitoring

13.2.4.2 Starting a Business Application

Execute the *isstartwu* command to start the WorkUnit.

13.2.4.2.1 Real-time Monitoring

This section describes how to display and monitor performance information using a Network Control Manager such as Systemwalker CentricMGR. Use the following procedure to display performance information on the Network Control Manager screen.

This procedure is an overview of real-time monitoring operation when the Windows version of Systemwalker CentricMGR operation management server is used. When using a Network Control Manager other than Systemwalker CentricMGR, refer to the user's guide for the Network Control Manager that needs to be used.

Windows32/64

1. Activate Systemwalker CentricMGR System Monitor.
2. Select the Application Server to be Monitored.

   Click the application server name to be monitored on the System Monitor screen.
3. Display the Get MIB Data screen.

   Choose **Tools | Specific System | Get/Set MIB Data | Get MIB Data** on the System Monitor screen menu to display the Get MIB Data screen.
4. Display the List of Object Names and check the **Instance Number of the Object to be Monitored**.

   Make the following settings on the Get MIB Data screen and click the Retrieve button.

   - Choose **Not check Polling Interval**.
   - Specify **DUMP** as the Request Type.
   - Specify "ispSumObjectName" in the MIB (performance information measurement item) to be displayed.

     Specify the MIB according to the following procedure:

     Click the Browse button to display the MIB Tree screen.

     On the MIB Tree screen, expand the tree structure by double-clicking the options internet, private, enterprises, fujitsu, application, aplNetWork, aplNetFunction, aplInterstage, isPerformanceinf, ispSummaryTable, and ispSummaryTableEntry in that order. The performance information items that can be displayed in real-time monitoring will appear on the display. Click ispSumObjectName.

     Click the Add button on the Get MIB Data screen.
5. Set the Reference Value

   - On the System Monitoring screen, choose **Policy | Setting Policy | Node | MIB State change** to display the MIB State Change screen.
   - Click the Add button on the MIB State Change screen to display the Threshold Details screen.
   - Specify the MIB name (the display item name of the performance information to be monitored), instance number, and threshold value (reference value) on the Threshold Details screen. Refer to step 4 above for further information about how to specify the MIB name.
   - Choose On on the MIB Monitoring screen.
6. Display the Real-time Display Screen (Performance Information)

   Make the following settings and click the Retrieve button.

   - Set the polling time to 5 minutes or more.
   - Specify GET as the Request Type.
   - Specify the instance number of the object to be monitored.

     When the list of object names is displayed, the following number appears. Specify this number as the instance number.

     "ispSumObjectName : "ispSumObjectName. *number*: *object-name*"
   - Specify the display item name of the performance information to be displayed in the MIB Name field. Refer to step 4 above for further information about how to specify the MIB name.

Solaris32/64

1. Activate Systemwalker CentricMGR (Job Monitor).
2. Select the Application Server to be Monitored.

   Choose Monitor for Select function on the Job Monitor screen, and choose Node list for Select tree.

   A job server list will be displayed. Click the name of the job server to be monitored.

3. Display the Get MIB Data screen.

   Choose **Tools | Specific Object | Get/Set MIB Data | Get MIB Data** on the Job Monitor screen menu to display the Get MIB Data screen.

4. Display the List of Object Names and check the Instance Number of the Object to be Monitored.

   Configure the following settings on the Get MIB Data screen and click the Retrieve button.

   - Choose **Not check Polling Interval**.
   - Specify **DUMP** as the Request Type.
   - Specify "ispSumObjectName" in the MIB (performance information measurement item) to be displayed.

     Specify the MIB according to the following procedure:

     Click the Browse button to display the MIB Tree screen.

     On the MIB Tree screen, expand the tree structure by double-clicking the options shown below in this order; internet, private, enterprises, fujitsu, application, aplNetWork, aplNetFunction, aplInterstage, isPerformanceinf, ispSummaryTable, and ispSummaryTableEntry.

     The performance information items that can be viewed in real-time monitoring will appear on the display. Click ispSumObjectName.

     Click the Add button on the Get MIB Data screen.

5. Set the Reference Value.

   - On the Job Monitor screen, choose **Policy | Setting Policy | Node | MIB State change** to display the MIB State Change screen.
   - Click the Add button on the MIB State Change screen to display the Threshold Details screen.
   - Specify the MIB name (the display item name of the performance information to be monitored), instance number, and threshold value (reference value) on the Threshold Details screen. Refer to step 4 above for further information about how to specify the MIB name.
   - Choose On on the MIB Monitoring screen.

6. Display the Real-time Display Screen (Performance Information).

   Make the following settings and click the Retrieve button.

   - Set the polling time to 5 minutes or more.
   - Specify GET as the Request Type.
   - Specify the instance number of the object to be monitored.

     When the list of object names is displayed, the following number appears. Specify this number as the instance number.

     "ispSumObjectName : "ispSumObjectName. *number*: *object-name*"

   - Specify the display item name of the performance information to be displayed in the MIB Name field. Refer to step 4 above for further information about how to specify the MIB name.

The following table shows the performance information items that can be displayed in real-time monitoring. The display item name in this table means the item name of the performance information displayed by the Network Control Manager.

Table 13.2 Performance Information Items

Performance Information Item Name	Unit	Display Item Name	Meaning
Object name	-	IspSumObjectName	Object name of the application for which performance information is measured
Maximum request processing time	ms	IspSumExecTimeMax	Maximum processing time (within a polling time) required for processing the object
Minimum request processing time	ms	IspSumExecTimeMin	Minimum processing time (within a polling time) required for processing the object

Performance Information Item Name	Unit	Display Item Name	Meaning
Averaged request processing time	ms	IspSumExecTimeAve	Averaged processing time (within a polling time) required for processing the object
Maximum request processing wait time	ms	IspSumWaitTimeMax	Maximum time (within a polling time) from the time of a client request to the initiation of a server application
Minimum request processing wait time	ms	IspSumWaitTimeMin	Minimum time (within a polling time) from the time of a client request to the initiation of a server application
Averaged request processing wait time	ms	IspSumWaitTimeAve	Averaged time (within a polling time) from the time of a client request to the initiation of a server application
Number of requests received	Number	IspSumRequestNum	Accumulated number of processes from the time of starting the performance monitoring up to the timing of this object.
Number of requests awaiting processing	Number	IspSumWaitReqNum	Maximum number of requests waiting for processing of this object, within the polling time.

Note

1. Unless the list of object names is to be displayed, always specify "GET" as the acquisition method when displaying performance information. If DUMP is specified for real-time display, an enormous amount of communications may be required between Systemwalker CentricMGR and the Performance Monitoring Tool, resulting in a heavy load on the network as well as on the application server.
2. When there is no object for which performance information can be displayed, "NONE" will be displayed as the object name.

13.2.4.3 Outputting the Performance Log File and Analyzing the Performance Information

Windows32/64 Solaris32/64

When the threshold value is exceeded during real-time monitoring and there is a possibility of performance abnormality analyze the detailed information saved as the performance log file.

Use the *ispreport* command to output a performance log file report. This command converts the performance information saved as the performance log file into CSV format and outputs it to the standard output. If the performance log file is to be converted into CSV format and output as a file, specify the output destination file name when executing the *ispreport* command as follows.

```
"ispreport option > output-destination-file-name"
```

When the *ispreport* command is executed, performance information in the performance log file will be converted one record at a time and output to the standard output in the following format.

- Line format

  "D1,D2,D3, D4,D5,D6, D7,D8,D9, D10,D11,D12,D13, D14,D15,D16,D17,D18,D19,D20,D21"

- Output items in each line

  The following table shows a list of output items, where items D1 to D21 in the 'Item No.' column correspond to those shown in Line format above.

  EJB Application

Table 13.3 Output Items

Item No.	Performance Information Item Name	Unit	Meaning
D1	Data collection start date	-	Date the performance information measurement for the record was started
D2	Data collection start time	-	Time the performance information measurement for the record was started
D3	Data collection end date	-	Date the performance information measurement for the record was finished
D4	Data collection end time	-	Time the performance information measurement for the record was finished
D5	For an EJB application: EJB application name For Light EJB container: Light EJB container name/EJB application name	-	EJB application name, or Light EJB container name / EJB application name by which performance information is measured.
D6	Method name + signature	-	Name of method to be monitored and signature (type of method argument and return value).
D7	Process ID	-	Process ID of the EJB application for which performance information is being measured.
D8	Thread ID	-	ID of a thread in which the method to be monitored operates.
D9	Maximum request processing time	ms	Maximum processing time of the method to be monitored in the thread within the interval time
D10	Minimum request processing time	ms	Minimum processing time of the method to be monitored in the thread within the interval time
D11	Averaged request processing time	ms	Averaged processing time of the method to be monitored in the thread within the interval time
D12	Maximum request processing wait time	ms	Maximum wait time for processing from receiving a request from a client application to starting the method processing within the interval time 0 is always output if the EJB application or Light EJB container is a message-driven Bean.
D13	Minimum request processing wait time	ms	Minimum wait time for processing from receiving a request from a client application to starting the method processing within the interval time. 0 is always output if the EJB application or Light EJB container is a message-driven Bean.
D14	Averaged request processing wait time	ms	Averaged wait time for processing from receiving a request from a client application to starting the method processing within the interval time. 0 is always output if the EJB application or Light EJB container is a message-driven Bean.
D15	Number of processes	Number	Number of operations of the method to be monitored in the thread within the interval time
D16	Number of requests received	Number	Accumulated number of operations of the EJB application or Light EJB container within the interval time.

Item No.	Performance Information Item Name	Unit	Meaning
D17	Number of requests awaiting processing	Number	Accumulated number of operations of the EJB application or Light EJB container within the interval time 0 is always output if the EJB application or Light EJB container is a message-driven Bean.
D18	Number of EJB object (Session)	Number	Number of the current EJB objects (difference between the executed create methods and executed remove methods)
D19	Maximum Passivate number for Entity	-	Maximum number of instance pooling in the EJB application or Light EJB container (process) within the interval time
D20	Maximum size of memory area used in VM	K byte	Maximum size of memory area used in VM for the EJB application or Light EJB container. Becomes 0 if the method is not processed within the interval time.
D21	Averaged size of memory area used in VM	K byte	Averaged size of memory area used in VM for the EJB application or Light EJB container. Becomes 0 if the method is not processed within the interval time.

13.2.4.4 Stopping the Application

Execute the *isstopwu* command to start the WorkUnit.

13.2.4.5 Stopping the Performance Monitor

The Performance Monitor is stopped with the *ispstop* command. When this command is executed, performance information is extracted and output on a performance log file stop.

13.2.4.6 Deleting the Performance Monitoring Environment

Use the *ispdeleteenv* command to stop the Performance Monitoring Tool and delete the performance monitoring environment. Delete the performance monitoring environment after performance monitoring has stopped. Otherwise, performance information will not be collected after the performance monitoring environment is deleted.

To restart performance monitoring, create a new performance monitoring environment after restarting Interstage.

13.2.4.7 Stopping Interstage

Execute the *isstop* command to stop Interstage.

13.2.4.8 Deleting the Performance Monitoring Tool from the SNMP Service

Windows32/64

Execute the *ispunsetagt* command to delete the Performance Monitoring Tool from the SNMP service. After executing the *ispunsetagt* command, use the Services dialog to restart the SNMP service. This operation is required only when the Performance Monitoring Tool has been registered in the SNMP service by using the *ispsetagt* command.

- Windows®

  Click [SNMP Service] for "Administrative Tools" "Services" and then execute [Stop] and [Start].

13.2.5 Analyzing the Performance Information and Taking Action

This section describes the method used to analyze the performance information collected from the performance log file and during real-time monitoring. The action that should be taken for each scenario is also described.

Real-time monitoring is only available in the Windows® version and the Solaris version.

13.2.5.1 Function of Outputting Log Information to the Performance Log File

This section describes the performance information that can be collected using the function of outputting log information to the performance log file, the evaluation method, and the method for taking action.

13.2.5.1.1 EJB Application (for an Old Version Compatible Environment), Light EJB Container (for an Old Version Compatible Environment), or IJServer EJB Container

13.2.5.1.2 Collectable Performance Information

The function of outputting log information to the performance log file allows the accumulated information to be output in CSV format. Use the *ispreport* command to execute this function..

The performance information is described below.

- Line format

  "D1,D2,D3, D4,D5,D6, D7,D8,D9, D10,D11,D12,D13, D14,D15,D16.D17,D18,D19,D20,D21"

- Output items in each line

  The following table shows a list of output items. Items D1 to D21 in the 'Item No.' column correspond to those shown in Line format above).

  For outputting the EJB application performance information, add the "-k EJBAPL" option to the *ispreport* command.

Table 13.4 Output Items

Item No.	Performance Information Item Name	Unit	Meaning
D1	Data collection start date	-	Date the performance information measurement for the record was started
D2	Data collection start time	-	Time the performance information measurement for the record was started
D3	Data collection end date	-	Date the performance information measurement for the record was finished
D4	Data collection end time	-	Time the performance information measurement for the record was finished
D5	For EJB application(for an old version compatible environment): EJB application name For Light EJB container(for an old version compatible environment): Light EJB container name/EJB application name For EJB container of IJServer: IJServer name/EJB application name	-	EJB application name, Light EJB container name/EJB application name or IJServer name/EJB application name by which performance information is measured.
D6	Method name + signature	-	Name of method to be monitored and signature (type of method argument and return value)

Item No.	Performance Information Item Name	Unit	Meaning
D7	Process ID	-	Process ID of the EJB application for which performance information is being measured
D8	Thread ID	-	ID of a thread in which the method to be monitored operates
D9	Maximum request processing time	ms	Maximum processing time of the method to be monitored in the thread within the interval time
D10	Minimum request processing time	ms	Minimum processing time of the method to be monitored in the thread within the interval time
D11	Averaged request processing time	ms	Averaged processing time of the method to be monitored in the thread within the interval time
D12	Maximum request processing wait time	ms	Maximum wait time for processing from receiving a request from a client application to starting the method processing within the interval time 0 is always output if the EJB application, Light EJB container or EJB container of IJServer is a message-driven Bean.
D13	Minimum request processing wait time	ms	Minimum wait time for processing from receiving a request from a client application to starting the method processing within the interval time 0 is always output if the EJB application, Light EJB container or EJB container of IJServer is a message-driven Bean.
D14	Averaged request processing wait time	ms	Averaged wait time for processing from receiving a request from a client application to starting the method processing within the interval time 0 is always output if the EJB application or Light EJB container is a message-driven Bean.
D15	Number of processes	Number	Number of operations of the method to be monitored in the thread within the interval time
D16	Number of requests received	Number	Accumulated number of operations of the EJB application or Light EJB container within the interval time
D17	Number of requests awaiting processing	Number	Accumulated number of operations of the EJB application or Light EJB container within the interval time 0 is always output if the EJB application, Light EJB container or EJB container of IJServer is a message-driven Bean.
D18	Number of EJB object (Session)	Number	Number of the current EJB objects (difference between the executed create methods and executed remove methods)
D19	Maximum Passivate number for Entity	-	Maximum number of instance pooling in the EJB application or Light EJB container (process) within the interval time
D20	Maximum size of memory area used in VM	K byte	Maximum size of memory area used in VM for the EJB application, Light EJB container or EJB container of IJServer.

Item No.	Performance Information Item Name	Unit	Meaning
			Becomes 0 if the method is not processed within the interval time.
D21	Averaged size of memory area used in VM	K byte	Average size of memory area used in VM for the EJB application, Light EJB container or EJB container of IJServer. Becomes 0 if the method is not processed within the interval time.

The *ispreport* command outputs the interval time information in units of operations for each process. The output information consists of information for each process in units of operations and in units of objects.

13.2.5.1.3 Evaluation and Action

Reference each item in the following:

- Evaluation by operation (D8-D10, D14)

  D8-D10 and D14 indicate the request processing time for the operation (indicated in D6 for the process indicated in D7) and the number of times the operation has been executed. With this information, a process can be evaluated for each operation.

- Evaluation by object (D11-D13, D15, D16)

  D15 and D16 indicate the number of requests received, and the number of requests awaiting processing, for the object indicated in D5. With this information each object can be evaluated.

The methods of evaluating performance information and the actions to be taken are listed in the following table.

If a performance abnormality was detected, take appropriate action using the following table as a reference.

Table 13.5 Performance Items Details

Item No.	Performance Information Details	Action
1	In all the time slots when performance monitoring was performed, the maximum request processing time is long and the averaged request processing time is close to the maximum request processing time.	If the request processing time is longer than the target value, one or both of the following causes can be assumed: - The server application has a performance problem. - System workload is too high. Review the server application and system from the above viewpoints.
2	In a particular time slot, the maximum, minimum, and averaged request processing times are long.	In a particular time slot, system workload is high. Check the workload status by measuring performance information of other server applications.
	In a particular time slot, the maximum, minimum, and average request processing wait times are long.	
3	Although the maximum request processing time is long, the averaged request processing time is short and close to the minimum request processing time.	One or both of the following causes can be assumed: - System work load have temporarily become high. - Under a particular condition, the server application has a performance problem. Review the server application and system from the above viewpoints.
	Although the maximum request processing wait time is long, the averaged request processing wait time is short and close to the minimum request processing wait time.	
4	In all the time slots when performance monitoring was performed, the maximum request processing wait time and average request processing wait time are long.	Processing capacity of the server application is insufficient for the number of requests from the client. Take action to increase the processing capacity, such as increasing the process multiplicity in the WorkUnit definition.

Item No.	Performance Information Details	Action
5	In a particular time slot, the number of processes and the number of requests waiting to be processed are high.	In a particular time slot, the number of requests to the server application has increased. If the processing capacity of the server application is insufficient for the number of requests from the client, take action to increase the processing capacity such as increasing the process multiplicity in the WorkUnit definition.
6	In all the time zones that carried out performance surveillance, the maximum demand processing waiting time and average demand processing waiting time are long.	The throughput of server application is insufficient to the number of demands from a client. Please carry out management which improves the throughput of server application, such as raising the degree of process multiplex by WorkUnit definition.
7	In the specific time zone, the number of processes and the number of the waiting demands for processing have increased.	The number of demands to the server application is increasing in the specific time zone. When the throughput of server application is insufficient to the number of demands from a client, please perform management which improves the throughput of server application, such as raising the degree of process multiplex by WorkUnit definition.
8	Number of EJB objects is larger than the number of client connections.	The number of EJB objects has increased. The remove method may not be executed for a create method. Reexamine the client application.
9	Number of Passivate is too large.	The Entity initial instance counts are insufficient. Increase the Entity initial instance counts in accordance with the increased number of Passivate.
10	Size of memory area used in VM is too large.	Memory leakage may have occurred. Re-examine the server application considering whether objects should be deleted or other actions should be taken.
11	Number of requests waiting to be processed is large, but average wait time for request processing is short.	Use the *isinfobj* command periodically to check the status of waiting queues and loading state within the interval time.

13.2.5.2 Performance Information Collected by the Network Control Manager with the Real Time Monitoring Function

This section describes the performance information that can be collected by the real time monitoring function, the method of evaluating it, and the various actions available.

13.2.5.2.1 Collectable Performance Information

The types of information that can be collected by using the real-time monitoring function are summarized below.

Table 13.6 Output Items

Performance Information Item Name	Unit	Meaning
Object name	-	Object name of the application for which performance information is measured
Maximum request processing time	ms	Maximum processing time within the time required for processing the object
Minimum request processing time	ms	Minimum processing time within the time required for processing the object

Performance Information Item Name	Unit	Meaning
Averaged request processing time	ms	Average processing time within the time required for processing the object
Maximum request processing wait time	ms	Maximum time within a poling time from the time of request by the client to the initiation of the server application
Minimum request processing wait time	ms	Minimum time from the time of request from by the client to the initiation of the server application
Averaged request processing wait time	ms	Average time from the time of request by the client to the initiation of the server application
Number of requests received	Number	Accumulated number of processes, from the time of starting the performance monitoring to the timing of this object.
Number of requests awaiting processing	Number	Maximum number of requests waiting for processing of this object, within the polling time.

13.2.5.2.2 Evaluation and Action

The method used to evaluate the performance information collected with the real time monitoring function, and the method used to take action, are listed in the following table.

If a performance abnormality was detected, take appropriate action using the following table as reference. Also, use the performance information output to the performance log file as a guide for evaluation.

Table 13.7 Performance Item Details

Item No.	Performance Information Details	Action
1	In each of the time slots when performance monitoring is performed, the maximum request processing time is long. The average request processing time is close to the maximum request processing time.	If the request processing time is longer than the target value, one or both of the following causes can be assumed: - There is a performance problem in the server application - System workload is too high Review the server application and system from the above viewpoints.
2	In a particular time slot, the maximum, minimum, and average request processing times are long.	In a particular time slot, the system workload is high. Check the workload status by measuring performance information of other server applications.
	In a particular time slot, the maximum, minimum, and average request processing wait times are long	
3	Although the maximum request processing time is long, the average request processing time is short and close to the minimum request processing time.	One or both of the following causes can be assumed: - System workload has temporarily become high - Under a particular condition, there is a performance problem in the server application Review the server application and system from the above viewpoints.
	Although the maximum request processing wait time is long, the averaged request processing wait time is short and close to the minimum request processing wait time.	
4	In all the time slots when performance monitoring was performed, the maximum request processing wait time and average request processing wait time are too long.	Processing capacity of the server application is insufficient for the number of requests from the client. Take action to increase the processing capacity, such as increasing the process multiplicity in the WorkUnit definition.

Item No.	Performance Information Details	Action
5	In a particular time slot, the number of processes and requests waiting to be processed are high.	In a particular time slot, the number of requests to the server application has increased. If the processing capacity of the server application is insufficient for the number of requests from the client, take action to increase the processing capacity such as increasing the process multiplicity in the WorkUnit definition.

13.2.5.3 Warnings on Evaluation of Performance Information

The following caveat applies to evaluating performance information:

- If the server application is terminated abnormally during processing, its request is not reflected in the performance information.

13.2.6 Managing the Performance Log Files

Ensure there is enough disk space to create performance log files before starting the Performance Monitoring Tool. Use the following formula to estimate the required disk space.

```
Disk space required =
 shared-memory-size-specified-when-starting-performance-monitoring-tool
 x (time-from-when-performance-monitoring-tool-is-started-until-stopped
 / time-interval-specified-when-starting-performance-monitoring-tool)
```

Back up the performance log files and delete unnecessary files at regular intervals. Otherwise, the disk may be getting full. If the backed up and deleted files are to be output as a report, store these files in a folder and output a report with these files specified.

Performance log files will be created in the following folders:

- The folder specified in the *ispmakeenv* command parameter
- The folder specified in the ISP_LOG environment variable

Performance log files will be created in the folder specified in either the *ispmakeenv* command or the ISP_LOG environment variable according to the naming convention shown below. If both are specified, the folder name specified in the *ispmakeenv* command will take priority. If neither of them is specified, the folder name 'TD_HOME\isp\log' will be used as the default folder name. 'TD_HOME' is the interstage-installation-folder\td.

```
Performance log file name: ispYYYYMMDD.log
 YYYYMMDD is a file creation date.
  YYYY: Year
  MM: Month (01 to 12)
  DD: Day (01 to 31)
```

The Performance Monitoring Tool creates a performance log file for the date when it is activated. If the Performance Monitoring Tool has been operated over several days, performance log files for these days will be created on the daily basis.

- After executing the *ispmakeenv* command, do not delete performance log files that are being created by the Performance Monitoring Tool. Otherwise, performance information may not be stored correctly. Use the *ispdeleteenv* command to delete performance log files.

13.2.7 Performance Monitoring Tool Definition Files

The definition files used by the Performance Monitoring Tool are explained below.

13.2.7.1 Performance Monitoring Target Specification File (ispstart Command)

Performance monitoring targets used by the Performance Monitoring Tool are specified in this file. These targets are specified as *ispstart* command parameters. For further information about using the *ispstart* command, refer to "ispstart" in the " Performance Analysis Monitoring Commands" chapter of the Reference Manual (Command Edition).

A maximum of 1000 performance monitoring targets can be specified.

Format

```
[Section name]
Performance monitoring target application
:

[Section name]
Performance monitoring target application
:
```

Items Specified

The section names that can be specified, and the performance monitoring target application in each section, are shown below.

Section name	Performance monitoring target application
TD-OBJECT	Specify the following: Transaction applications Windows32/64 Solaris32/64 Wrapper objects
EJBCONT	Specify IJServer (Note)
CORBA-IMPLID	Specify the CORBA application implementation repository ID

Note

Performance information for the IJServer (Web + EJB [1VM]) and IJServer (Web only) IJServer types cannot be collected.

In the case of IJServer (Web + EJB [separate VMs]), only the information for the Java VM that the EJB application runs on can be collected.

Definition Examples

Examples of definition file entries are shown below.

Note that the section name is surrounded by square brackets, [ ].

```
[TD-OBJECT]
TD1/INTF1
WRAP2/INTF2

[EJBCONT]
myserver
IJServer_Split
IJServer_EJB

[CORBA-IMPLID]
IMPLID
```

13.2.7.2 Performance Monitoring Tool Automatic Startup Definition File (ispsetautostart Command)

Windows32/64

The environments that will be used for performance measurement, and performance monitoring target applications, are specified in this file when automatic operations are performed using the Performance Monitoring Tool. These targets are specified as *ispsetautostart* command parameters. For further information about using the *ispsetautostart* command, refer to "ispsetautostart" in the "Performance Analysis Monitoring Commands" chapter of the Reference Manual (Command Edition).

A maximum of 1000 performance monitoring targets can be specified.

Format

```
[Section name]
Defined item
:

[Section name]
Defined item
```

Items Specified

The section names that can be specified, and the defined items that can be specified in each section, are explained below.

Section name	Defined item	Meaning
Control	Shmsize	Specify the shared memory size in MB. The default value is 1. The minimum value that can be specified is 1. The maximum value that can be specified is the lesser value of the maximum amount of shared memory defined in the system (MB) and 2046. In the Performance Monitoring Tool, the shared memory is used in the collection of performance information. Calculate the volume from the amount of performance information that will be collected and then specify this volume. For details on how to estimate the performance information amount, refer to the Tuning Guide.
	Log_path	Specify the performance log file output destination. The default value is "C:\Interstage\td\isp\log".
	Auto_start	Specify whether performance monitoring for the performance monitoring target application specified in the definition file will start automatically when Interstage starts. The default value is NO. YES: Performance monitoring for the performance monitoring target application specified in the definition file will start automatically when Interstage starts. If a performance monitoring target application has not been specified, performance monitoring will not start. NO: Performance monitoring will not start when Interstage starts.
Interval	local_interval	Specify the time interval that will be used for performance log file collection. The default value is 1. The ranges that can be specified are as follows: Hours: 1, 2, 3, 4 Minutes: 1m, 5m, 10m, 20m, 30m
	real_interval	Specify the time interval (in minutes) that will be used for real-time monitoring. The default value is 5. A range between 1 and 60 can be specified.
TD-OBJECT		Specify transaction applications and wrapper objects.
EJBCONT		Specify IJServer.

Section name	Defined item	Meaning
CORBA-IMPLID		Specify the CORBA application implementation repository ID.

Note

If the setting is "Auto_start=YES", but the performance monitoring target application name is invalid, only the Performance Monitoring Tool will be started. Performance monitoring will not start. Specify a valid application name in the performance monitoring target specification file, then start the performance monitoring using the *ispsetautostart* command.

Definition Examples

Examples of definition file entries are shown below.

Note that the section name is surrounded by square brackets, [ ].

```
[Control]
Shmsize = 10
Auto_Start = NO
Log_Path = c:\log

[Interval]
local_interval = 5m
real_interval = 1

[TD-OBJECT]
TD1/INTF1
WRAP2/INTF2

[EJBCONT]
myserver
IJServer_Split
IJServer_EJB

[CORBA-IMPLID]
IMPLID
```