FUJITSU

FUJITSU Software
Interstage Application Server

Directory Service Operator's Guide

Windows/Solaris/Linux

B1WS-1090-03ENZ0(00)
April 2014

Preface

Purpose of This Document

The purpose of this document is to explain the setup and operation of Interstage Directory Service.

Intended Readers

This document is intended for the users of Interstage Directory Service.

It is assumed that readers have a basic understanding of the following:

- The relevant operating system
- The Internet
- SSL
- LDAP and X.500
- C
- Java
- Java application development using JNDI
- Relational database
- Symfoware Server
- Oracle Database

Structure of This Document

This Operator's Guide is document is organized as follows.

Chapter 1 Overview

This chapter explains concepts such as Interstage Directory Service system configuration, and the basics of the directory service. It also provides a functional overview.

Chapter 2 Environment Setup

This chapter explains the environment setup for Interstage Directory Service.

Chapter 3 Creating Databases

This chapter explains the database environment setup if an RDB is used as the repository database.

Chapter 4 Setting up an Environment for SSL Communication

This chapter explains the SSL communication environment setup if SSL communication is used for Interstage Directory Service communications.

Chapter 5 Creating a Repository

This chapter explains procedure involved from creation of the Interstage Directory Service repository to creation/registration of data.

Chapter 6 Creating a Load Distribution Environment

This chapter explains the procedure for creating an environment for database sharing.

Chapter 7 Entry Management

This chapter explains how to manage entries in Interstage Directory Service.

Chapter 8 Creating an Application (JNDI)

This chapter describes how to create a JNDI application using Interstage Directory Service.

Chapter 9 Creating an Application (C API)

This chapter describes how to create applications in C using Interstage Directory Service APIs.

Chapter 10 Operating and Maintaining Repositories

This chapter explains how to operate the Interstage Directory Service repository, and provides information on its maintenance.

Appendix A Interstage Directory Service Object Classes

This appendix describes object classes that can be used by Interstage Directory Service.

Appendix B Interstage Directory Service Attributes

This appendix describes attributes that can be used by Interstage Directory Service.

Appendix C Creating a Load Distribution Environment (Replication Mode)

This appendix explains how to create the replication mode operation environment, for the Standard Database, Symfoware/RDB or an Oracle database.

Appendix D Estimating Resources for Symfoware/RDB

This chapter describes the formulae for estimating resources required by Symfoware/RDB when running Interstage Directory Service applications.

Appendix E Estimating Resources for Oracle Databases

This chapter describes the formulae for estimating resources required by Oracle databases when running Interstage Directory Service applications.

Conventions

Representation of Platform-specific Information

In the manuals of this product, there are parts containing content that relates to all products that run on the supported platform. In this case, an icon indicating the product platform has been added to these parts if the content varies according to the product. For this reason, refer only to the information that applies to your situation.

Windows32	Indicates that this product (32-bit) is running on Windows.
Windows64	Indicates that this product (64-bit) is running on Windows.
Windows32/64	Indicates that this product (32/64-bit) is running on Windows.
Solaris32	Indicates that this product (32-bit) is running on Solaris.
Solaris64	Indicates that this product (64-bit) is running on Solaris.
Solaris32/64	Indicates that this product (32/64-bit) is running on Solaris.
Linux32	Indicates that this product (32-bit) is running on Linux.
Linux64	Indicates that this product (64-bit) is running on Linux.
Linux32/64	Indicates that this product (32/64-bit) is running on Linux.

Abbreviations

Read occurrences of the following Components as their corresponding Service.

Service	Component
CORBA Service	ObjectDirector
Component Transaction Service	TransactionDirector

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 Overview

This chapter provides an overview of Interstage Directory Service and its functions.

1.1 Interstage Directory Service

To deal with rapidly changing market environments, corporate users are integrating their information systems with Web services based on Internet technologies. To realize this goal, two elements are required: high-level security to authenticate and manage users, and reduced development and operation costs.

Interstage Directory Service provides a directory service based on the Lightweight Directory Access Protocol (LDAP) that reduces operation, management and development costs by enabling centralized control of resources instead of conventional distributed control.

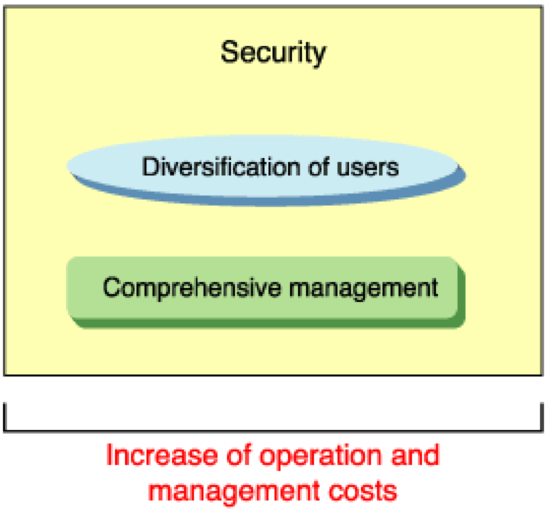
1.1.1 Considerations for Integrating Web Services

It is natural, when building a corporate information system, to want to utilize existing resources (including systems and data) to reduce development costs and time. An integrated Web service based on Internet technologies is indispensable for corporate information systems as it lends itself to utilizing these resources.

However, the following issues must be considered before integrating a Web service:

- Integrated management, including the integration of departmental systems.
- Support for diversified users.
- Security.
- Increased operation and management costs.

Figure 1.1 Problems of a Conventional System



Integrated Management, including the Integration of Departmental Systems

Under a Web service, numerous departmental systems are also integrated. However, various systems (for example, the personnel information system or business management system) are used by different people, all with differing levels of system access depending on their departments and positions.

Furthermore, in response to the rapidly changing market, the number of required information systems will increase, with users increasing accordingly.

System integration is ineffectual if users continue to be managed system by system.

Support for Diversified Users

The business environment of a company is drastically changing. This is evident in the shift from the traditional department-and-section system to a project team system, and the diversification of employment types to include loaned staff, part-time, contract, and temporary employees.

Additionally, companies increasingly disclose information to their customers via the Internet.

New information systems differ from traditional ones in that the types and levels of system users are fragmented. Managing fragmented users is, therefore, a major challenge of implementing a new information system.

Security

Security of information, including in-house and customer information is a high business priority. Businesses cannot over-emphasize the importance of providing adequate security for all of their data.

However, ensuring security for diversified users with varying access levels has become almost impossible through conventional solutions.

Increase of Operation and Management Costs

Offering convenience to an increasing number of diversified users, while also ensuring their security entails high development costs. Operation and management have also become major concerns in terms of both human resources and costs.

1.1.2 Advantages of Introducing Interstage Directory Service

A directory service can help solve the problems mentioned above. Directory services provide the location and information for resources (such as Web servers, Web services, and user information) that are distributed over a system.

This type of integrated resource management will free individual systems from performing their own resource management.

Interstage Directory Service provides a directory service based on the Lightweight Directory Access Protocol (LDAP), which is becoming increasingly recognized as a global standard.

Interstage Directory Service offers features including operations on the Interstage Management Console; simplified entry administration; high reliability through replication, backup/restore, and access logs; automatic encoding of passwords; and security through SSL communications.

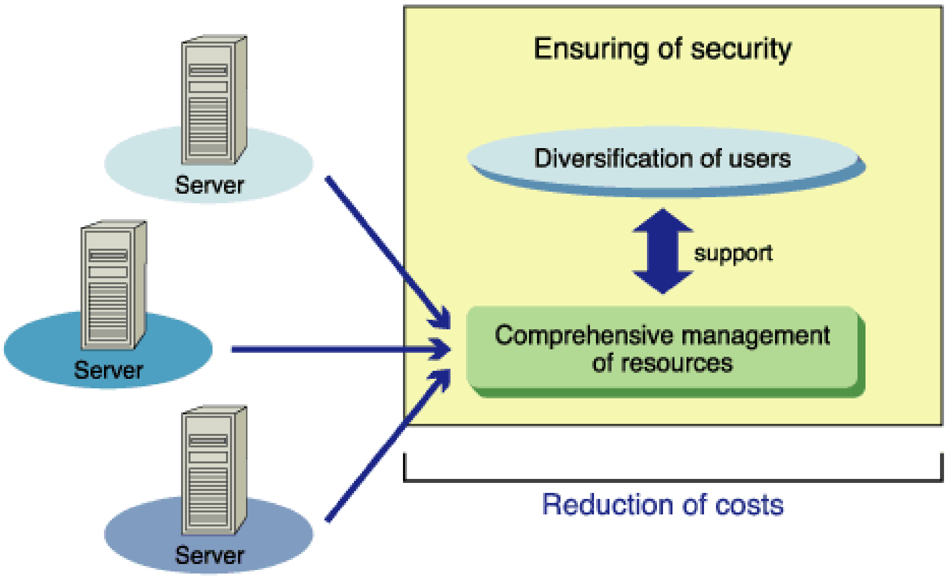
Using these features, Interstage Directory Service can centrally control the resources of all integrated systems and customize settings for diversified users. User access permissions can therefore be carefully managed.

Automatic encoding of passwords provides thorough security.

When used in combination with the Interstage Single Sign-on, Interstage Directory Service allows users to access Web servers and Web services to which they have permission using only one User ID and password. This maintains security and offers convenience.

These features will significantly reduce the system development and operation management costs.

Figure 1.2 Benefits of Integrated Resource Management with Directory Services



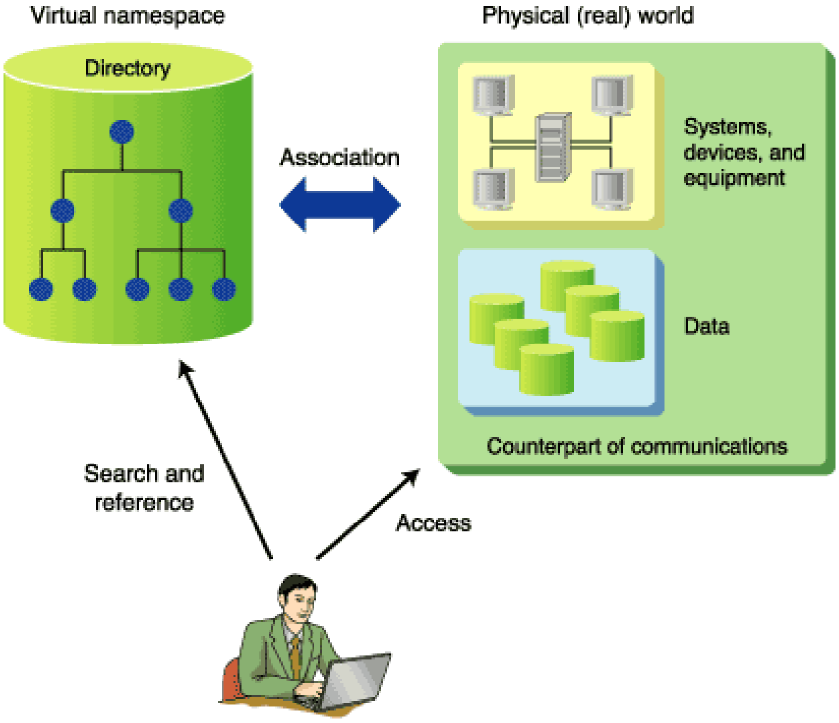
1.2 Basic Knowledge of Directory Services and LDAP

This section provides basic information on the directory services required to use Interstage Directory Service.

1.2.1 Directory Services

A directory service is used to efficiently navigate and manage access to information. Directory services associate physical (real) resources including systems, devices, and equipment with virtual namespaces managed by the directory service. This allows users to search for and reference necessary information and access systems, devices, and equipment using the location information provided.

Figure 1.3 Directory Services



In Interstage Directory Service, each system that manages the directory service information is called a 'repository.'

1.2.2 LDAP

A directory service was standardized and defined by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) in the 'X.500' specification.

Although X.500 is a highly versatile protocol, software developed based upon it tends to be large-scaled and thus has a higher development cost. The Lightweight Directory Access Protocol (LDAP) is a subset of essential X.500 functions that can be easily used in Internet technologies.

LDAP is an Internet-standard directory access protocol that runs on TCP/IP, which allows an LDAP client such as a browser to directly search for and reference data using a directory service.

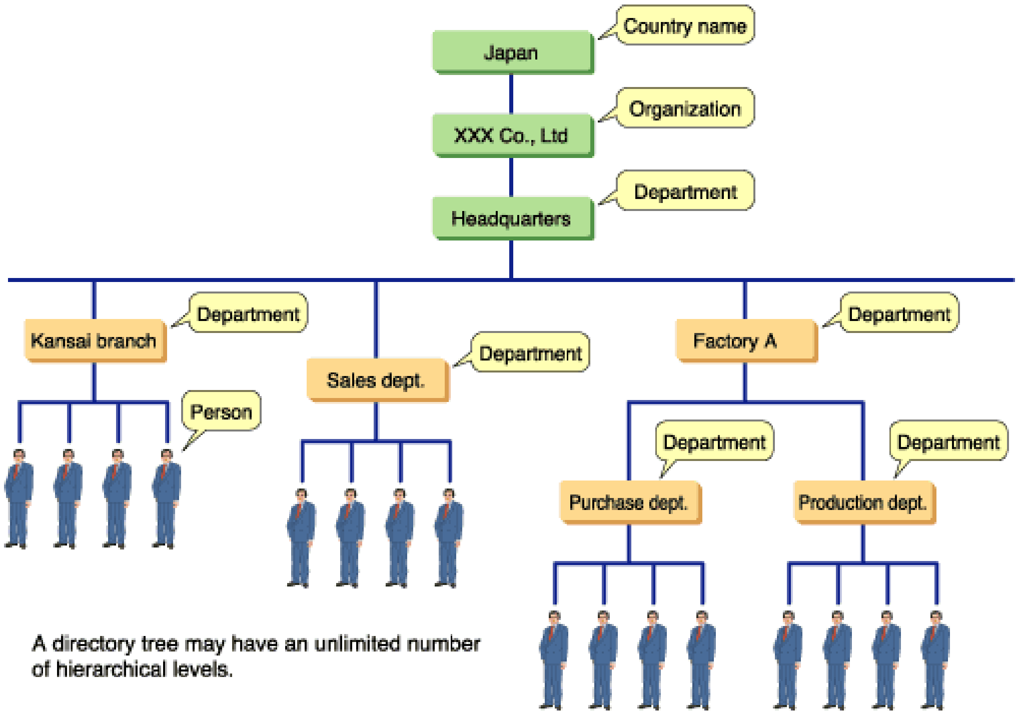
Directory Data Model

For ease of understanding, Directory may be thought of as a hierarchical database.

In Directory, a unit of information such as a person or organization is called an entry.

Entries are managed in a hierarchical fashion (in a tree).

Figure 1.4 Hierarchical Directory Tree



The hierarchical structure of entries is called a 'Directory Information Tree (DIT).' A database storing a DIT is called a 'Directory Information Base (DIB).'

Entries are classified into the following types depending on their position in a DIT:

Top entry

An entry located at the top (root) of a DIT. A top entry, unique to a directory server, is a special entry with a different attribute value for each directory server.

Upper entry

An entry located above a particular entry.

Lower entry

An entry located below a particular entry.

Leaf entry

An entry without a lower entry.

Sub tree

A part of a DIT consisting of a particular entry and its lower entries.

Object and Object Class

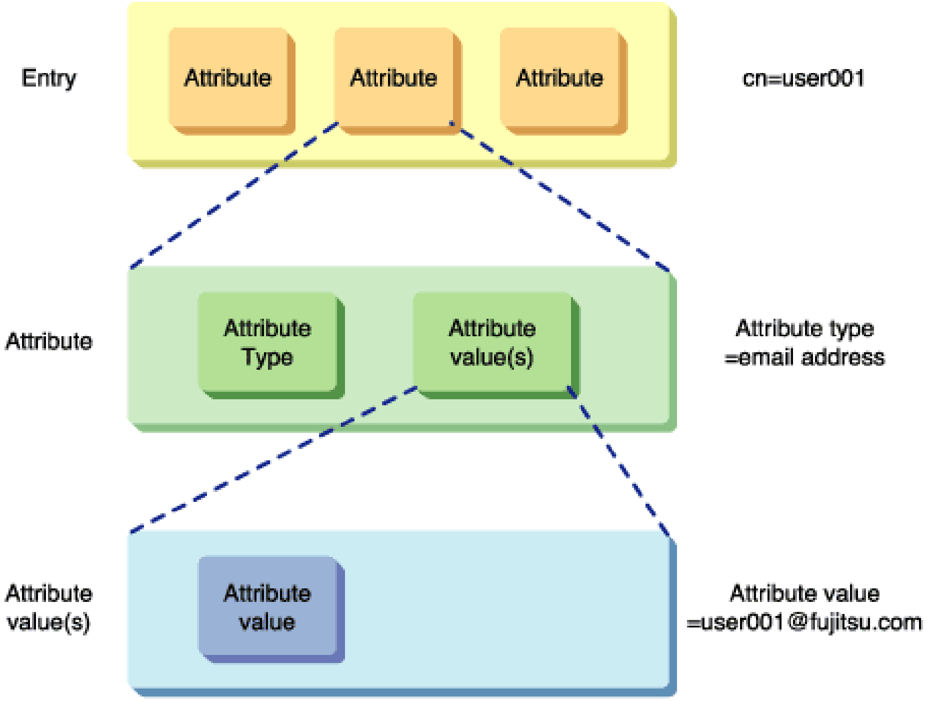
In an entry, an 'object' is characterized by an 'object class' indicating an attribute of the information.

Entries are classified according to object classes. The following describes an object and an object class.

Attribute Type and Attribute Value

An object has an 'attribute type' representing its detailed item name and an 'attribute value' representing the actual value (content) of the item.

Figure 1.5 Attribute Types and Values



Distinguished Names of Entries

Entries have distinguished names, which consist of RDNs and DNs.

RDN (Relative distinguished name)

A name used to identify an entry's immediately lower entry. An RDN must be unique in its sibling relationship.

```
Example: "o=fujitsu"
```

DN (Distinguished name)

A name defined as a string of RDNs of the entry and its upper entries, representing an object. A DN must be unique in a DIT.

```
Example: "cn=user001,o=fujitsu,c=jp"
```

Interstage Directory Service also has a special DN called an Administrator DN, which is used to manage a repository.

Schema

A set of definitions of data types (DIT structure, object class, and attribute) to be stored in a directory is called a 'schema'.

1.2.3 Basic Services of LDAP

Interstage Directory Service supports LDAP V3 as an access protocol for use between a server and a client. LDAP V3 allows a user or a client to reference and modify the information in a directory.

The following lists the services provided by the directory. For more information, refer to the "Creating an Application (JNDI)" chapter.

- Bind

  To access a directory, you need to enter your DN and password information for authentication. However, no particular authentication is required to access a directory as anonymous (an anonymous user). In this case, the directory server will see you as an anonymous user.

- Unbind

  To close the connection to the directory server, you need to perform the unbind operation.

- Search

  To view information stored on the directory server, you can use the search operation.

- Compare

  The server will compare a password or other item with the information stored on it to check whether it is correct. Unlike search, no actual information will be displayed. This function can also distinguish entries that do not have a specified attribute value or attribute type.

- Add

  The add operation adds information to the directory server.

- Delete

  The delete operation deletes information stored on the directory server.

- Modify

  The modify operation modifies information stored on the directory server.

- ModifyDN and ModifyRDN

  When modifying a distinguished name, specify whether you want to delete the attribute values of the DN, new RDN, and old RDN of the entry being modified. To move an entry (and a sub tree), specify the DN of a new immediately upper entry.

- Abandon

  To stop searching for information on the directory server, perform the abandon operation.

1.3 Features and Configuration of Interstage Directory Service

This section describes the features and configuration of Interstage Directory Service.

1.3.1 Features of Interstage Directory Service

Interstage Directory Service has the following features:

- Interstage Directory Service is based on the LDAP V3 Internet standard.

- Interstage Directory Service allows the use of relational databases (RDB). (*1)

  If more than 10,000 entries (user information and policy information) are to be managed, use a relational database.

- Interstage Directory Service can be used with large-scale configurations.

  Interstage Directory Service can manage more than 100,000 entries (user information and policy information).

- Interstage Directory Service can achieve stable responses even in large-scale configurations.

  Interstage Directory Service uses an RDB as the database for storing directory entries (*1), and uses the RDB high-performance search function to provide stable response times even for large numbers of accesses.

- Interstage Directory Service can be easily operated using familiar tools, thereby helping to reduce the TCO.

  Different types of database systems can be integrated into a single RDB, which means that Interstage Directory Service can be administered with utilities and tools that have been used with existing RDB operations, thereby reducing costs.

- Interstage Directory Service guarantees data integrity.

  The RDB product's powerful backup and recovery, data consistency maintenance, and security functions can be used (*1), so that even if an error does occur, the integrity of the data can still be guaranteed.

- When Interstage Directory Service is accessed using the API (for Java), the information needed by an application on the Application Server is easily stored in or searched from Interstage Directory Service.

- The commands *irepmodifyent*, *irepaddrole*, *ldapmodify*, *ldapsearch*, and *ldapdelete* and the Entry Administration Tool are provided to facilitate search, add, delete, and modify operations in Interstage Directory Service.

- The Interstage Management Console facilitates the construction of a repository.

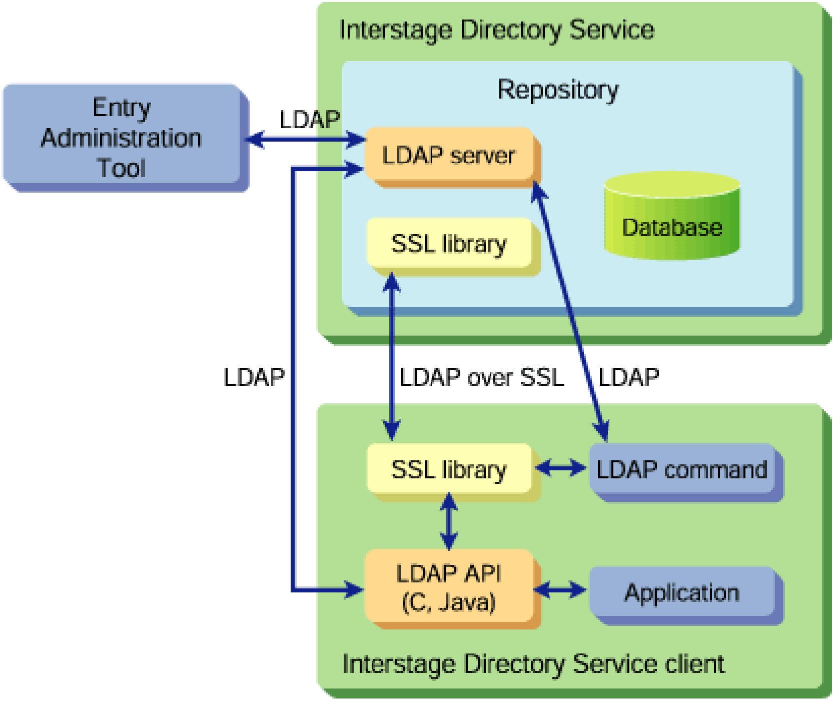
*1 The RDB can only be used with the Enterprise Edition of Interstage Application Server.

1.3.2 Configuration of Interstage Directory Service

This section describes the component configuration of Interstage Directory Service.

Configuration that Uses the Standard Database

Figure 1.6 Interstage Directory Service Component Configuration



- Interstage Directory Service

  An Interstage Directory Service consists of the LDAP server and the Interstage data store.

  - LDAP server

    A program that searches and stores information when it receives a request from an application through the LDAP API.

  - Interstage data store

    A database that stores information. Interstage data store is used.

- Interstage Directory Service Client

  An Interstage Directory Service client consists of the LDAP-API and LDAP commands.

  - LDAP API (C, Java)

    A library running on the Application Server to allow an LDAP application to access the Interstage Directory Service. The LDAP API is available for C and Java. The APIs for the C language can only be used with the Interstage Application Server Enterprise Edition.

  - LDAP commands

    Commands that facilitate operations involving information on the Interstage Directory Service (search, add, delete, and modify).

- Entry Administration Tool

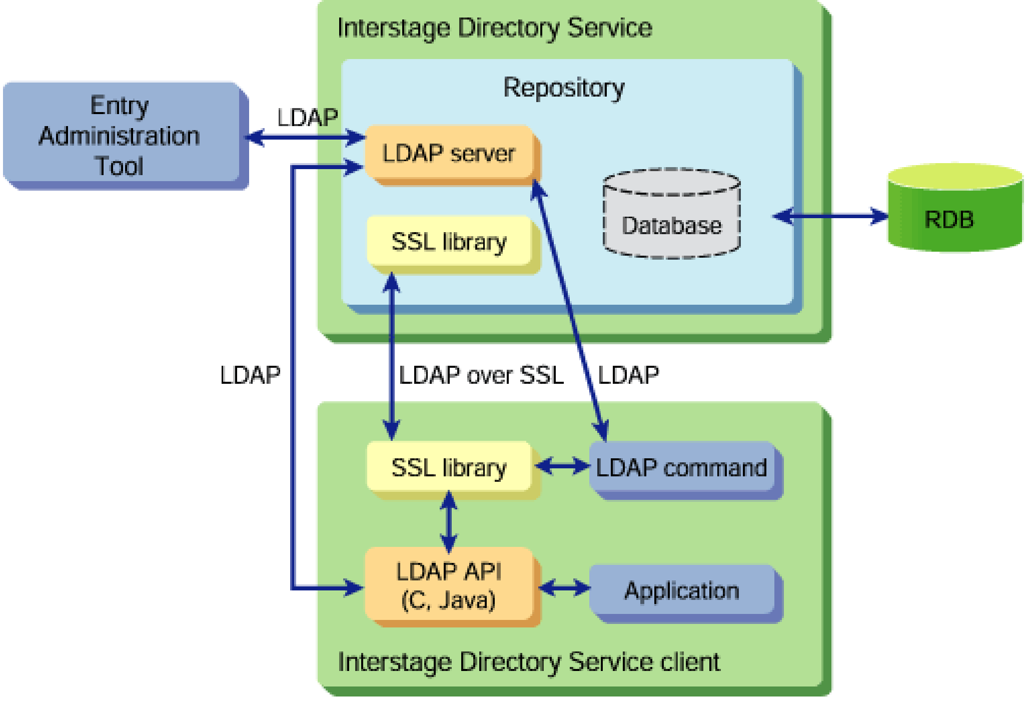
  A GUI-based tool that facilitates operations involving information on the Interstage Directory Service (search, add, delete, and modify).

Configuration using the RDB (*1)

An RDB (Symfoware Server and Oracle Database) can be used as the database for storing information instead of the standard database.

If the number of entries to be managed is no more than 10 000, use a standard database. If the number exceeds 10 000, use a relational database.

Figure 1.7 Interstage Directory Service Component Configuration (using the RDB)



*1 The RDB can only be used with the Interstage Application Server Enterprise Edition. For Linux 64 (bit) and Windows (64 bit), the standard database cannot be used, so use the RDB.

1.3.3 Operating Modes

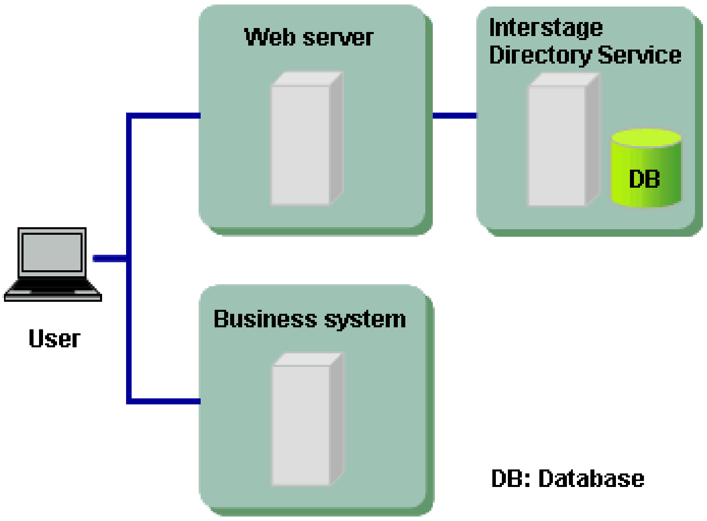
Interstage Directory Service uses a Web server to link to the Interstage single sign-on authentication function and the Interstage HTTP Server online collation function. Interstage Directory Service offers the following operation modes, depending on the particular objectives and considerations of your system (such as the system scale and the ensuring of high reliability).

Furthermore, each server can be operated in 1:1 Fixed standby mode depending on the cluster.

Operations where information is managed on one Interstage Directory Service Server (standalone operations)

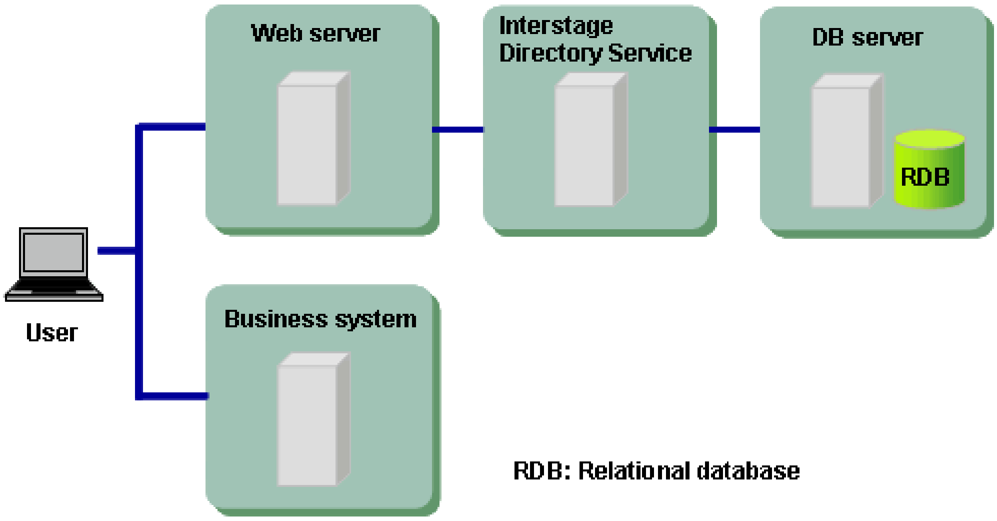
In this scenario, information is managed on one server. This kind of operation is appropriate in situations where the business system only has a small number of users, or where the number of simultaneous accesses is low.

Figure 1.8 Interstage Directory Service Standalone Mode (Standard DB)



When this is the case, the RDB can be used as the database for storing Interstage Directory Service information. (The RDB can only be used with the Interstage Application Server Enterprise Edition).

Figure 1.9 Interstage Directory Service Standalone Mode (RDB)



Operations in which information is managed using a single database server and multiple Interstage Directory Service servers

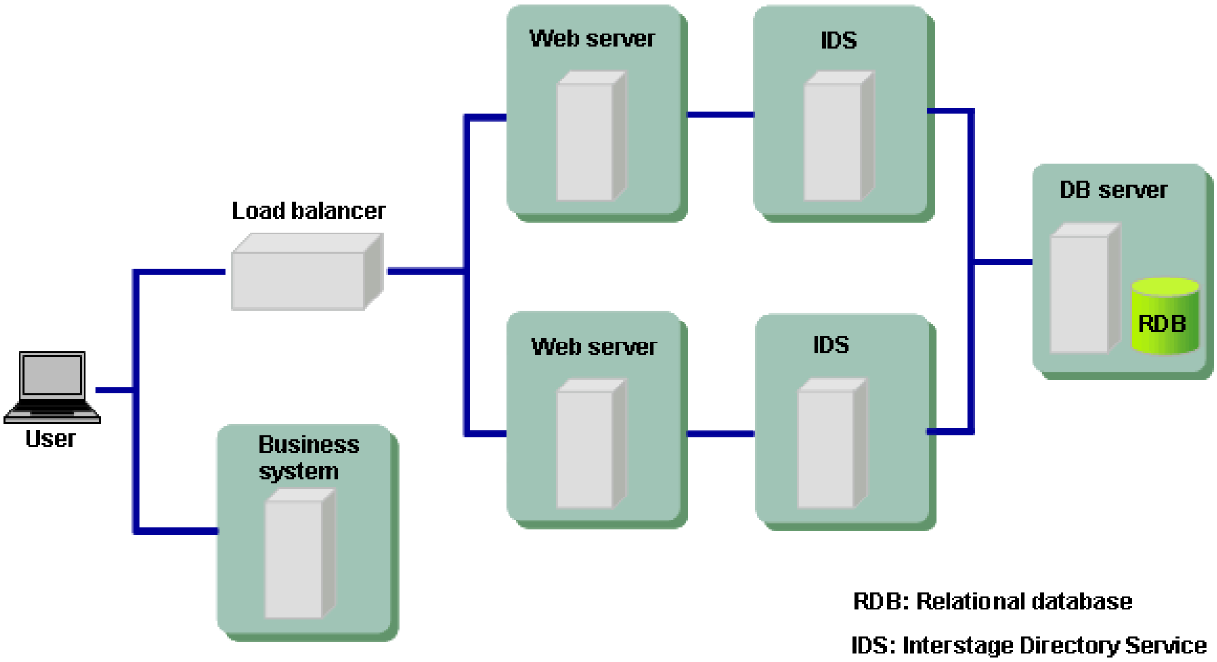
Note

This operation mode can only be used when an RDB is used as the database.

In this operation mode, more than one Interstage Directory Service server is installed so that the load is distributed over the servers, and information is managed by a single database server.

This mode is suitable when the number of users of a business system or the number of concurrent accesses is large and it is desirable to prevent the load being concentrated on any one server. Because information is managed using a single database server, it is easier to build, operate and manage the environment than when replication is used.

Figure 1.10 Interstage Directory Service Database Sharing

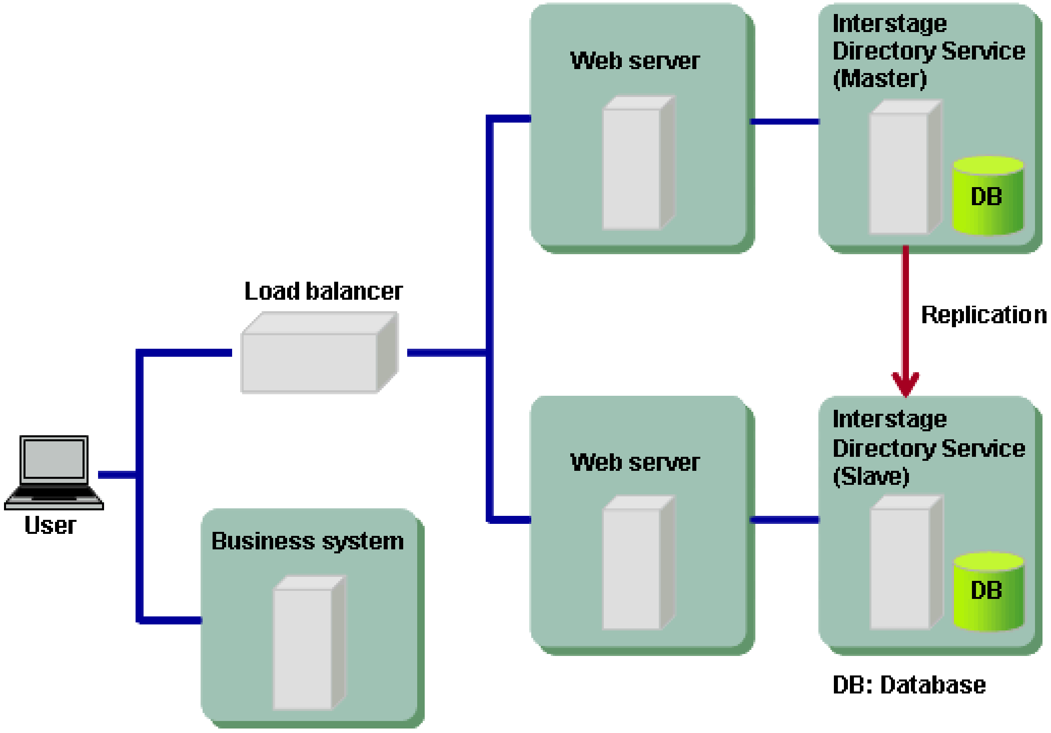


Operations where one master server is used and its copies are managed by more than one slave server (replication operations)

This configuration does not only distribute the load imposed on one server, but it also creates a high-reliability system.

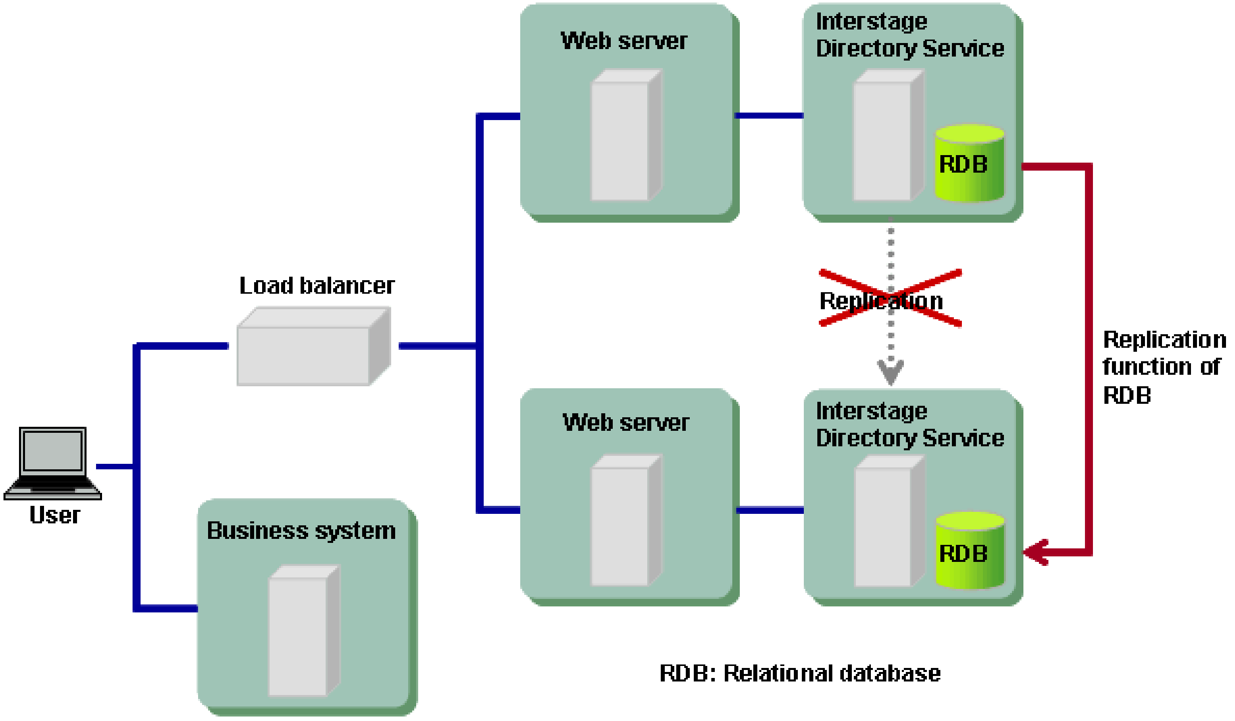
This mode is suitable when the number of users of a business system or the number of concurrent accesses is large and it is desirable to prevent load becoming concentrated on any one server; and when it is also desirable to have the load replicated over several databases.

Figure 1.11 Interstage Directory Service Replication Mode (Standard DB)



An RDB can also be used in replication mode. In such cases, replication is accomplished using the RDBs function instead of the Interstage Directory Service function.

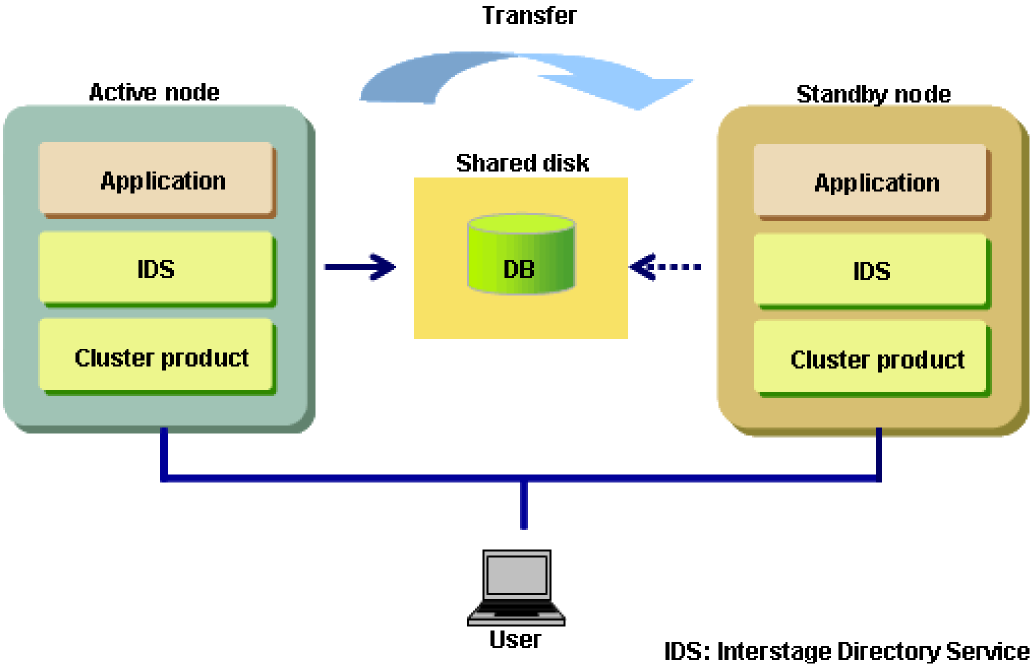
Figure 1.12 Interstage Directory Service Replication Mode (RDB)



1:1 Fixed Standby Mode

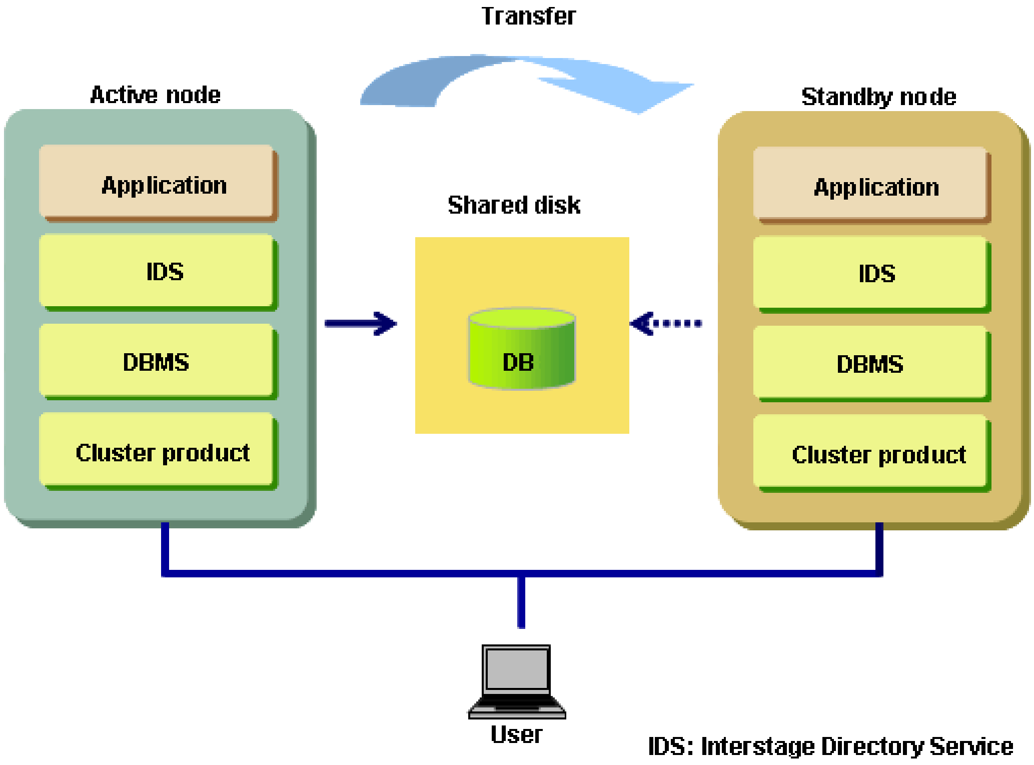
Here, there is one server machine operating (the 'active server') and another server on standby in case something goes wrong (the 'standby server'). A disk is shared between the active server and the standby server. Data is placed on the disk that is shared between the active server and the standby server, and if the active server fails because of a hardware fault, the standby server takes over jobs and the disk is accessed from the standby server. This operation pattern using the cluster server function enables operations to continue without stopping all jobs.

Figure 1.13 Interstage Directory Service 1:1 Fixed Standby Mode



An RDB can also be used.

Figure 1.14 Interstage Directory Service 1:1 Fixed Standby Mode



1.4 Major Functions of Interstage Directory Service

Interstage Directory Service provides the following functions:

- 1.4.1 User Authentication
- 1.4.2 Password Protection
- 1.4.3 SSL Communication
- 1.4.4 Entry Administration
- 1.4.5 Load Balancing (Replication)
- 1.4.6 Schema Extension
- 1.4.7 Access Control
- 1.4.8 Operation Monitoring

1.4.1 User Authentication

The Authentication function checks that only authorized users access Interstage Directory Service. It therefore protects resources stored in Interstage Directory Service from unauthorized access.

Before gaining access, users are required to enter their user entry information (user DN and password) stored in the database of Interstage Directory Service.

Although the stored user passwords have been encrypted using the user password encryption method, users specify a plain text password for authentication.

1.4.2 Password Protection

Interstage Directory Service can store user authentication information for various applications. At this time, the password (userPassword attribute) can be encrypted as the entry information of the user. To export passwords using unencrypted text, use the *irepadmin* command.

Refer to the "Interstage Directory Service Operation Commands" chapter in the Reference Manual (Command Edition) for information on the *irepadmin* command. The password encryption method can only be changed after the new repository is created using the Interstage Management Console and before the repository is started for the first time.

Note

- Exporting passwords using unencrypted text is a security risk.
- A function for referencing the password encryption method settings is not offered because of the possibility of the threat to security. The user must take care that the settings are managed securely.

1.4.3 SSL Communication

Data transmitted over a network may be stolen by a third party. SSL can be used to encrypt data before it is transmitted over a network to prevent eavesdropping and ensure safe communications.

SSL communications use the server authentication method in which a client that is about to communicate with Interstage Directory Service will first check whether Interstage Directory Service has a correct identity and then encrypt data before transmitting it.

Target of SSL Communications

The following table shows the communication paths used by Interstage Directory Service for SSL communications.

Table 1.1 Communication Paths

Communication path	Target of SSL communications
Communications with a command	Encrypted communications may be performed between one of the following commands and a repository: - ldapsearch command - ldapmodify command - ldapdelete command
Communications with an application	Encrypted communications may be performed between a client application and a repository.
Communications in replication mode	Encrypted communications may be performed between a repository (master) and another repository (slave) in replication mode.

Note

When you use the Entry Administration Tool or an entry administration command (*irepmodifyent*), SSL communications cannot be performed on the communication path. Therefore, run the Entry Administration Tool or entry administration command in a sufficiently secure environment; for example, on the same computer as the repository.

For security measures, refer to the "Security Measures" chapter in the Security System Guide.

1.4.4 Entry Administration

In Interstage Directory Service, the following features are available to add an entry to the database or modify an existing entry.

- Commands
- Entry Administration Tool
- SDK

Note

When an entry is modified, Interstage Directory Service does not check the schema.

Therefore, incorrectly modifying an entry (for example deleting a required attribute in the entry, or incorrectly adding an attribute to an object class) causes conflict between items of information in the repository. Be careful when modifying an entry.

Operating an Entry

Commands

Manipulate the entry information of the repository using commands.

You can specify Japanese characters (Shift JIS and EUC) for these commands. You can also manipulate binary data (such as jpegPhotos) in an entry.

The following four commands are available:

- irepmodifyent
- ldapmodify
- ldapsearch
- ldapdelete

Of the above commands, *ldapmodify*, *ldapsearch*, and *ldapdelete* support the use of the SSL function, which secures communications.

For information on using the commands, refer to the "Interstage Directory Service Operation Commands" chapter in the Reference Manual (Command Edition).

Command Functions

The following describes the use of the commands:

Table 1.2 Command Descriptions

Command function	Description
Adding entry information	Add entry information to the repository using the *irepmodifyent* or *ldapmodify* command.
Modifying entry information	Modify entry information in the repository using the *irepmodifyent* or *ldapmodify* command.
Deleting entry information	Delete entries from the repository using the *ldapdelete*, *irepmodifyent*, or *ldapmodify* command.
Searching for entry information	Search for entries in the repository using the *ldapsearch* command.

For more information on the command functions, refer to "Using Commands to Manage Entries" in the "Entry Management" chapter.

Entry Administration Tool

The Entry Administration Tool is a GUI used to manage entries registered in the repository.

The Entry Administration Tool allows you to manipulate entries as described in the following table:

Table 1.3 Entry Administration Tool

Manipulation of entries	Description
Adding an entry	To add an entry, bring up the window for adding an entry. Enter values to register an entry in the connected repository.
Modifying an entry	To modify an entry, bring up the window for modifying an entry. Enter values to modify an entry in the connected repository.
Deleting an entry	Select the entry that you want to delete and thus delete an entry from the connected repository.

Manipulation of entries	Description
Search	Search for an entry in the connected repository. Enter the required search conditions and start searching from the specified search start position. Entries extracted in the search will then be displayed. You can also modify, delete, or rename the extracted entries.
Rename	Select an entry in the connected repository and rename the entry.
Move	Move an entry in the connected repository.
Copy	Copy an entry in the connected repository.
Display mode	Change the mode in which data is displayed in the list view.
Display options	Set options of the display of the administration tool.

SDK

The SDK allows you to develop an LDAP application that accesses an Interstage Directory Service server on an Application Server. The application may be developed in C or Java. The C language can only be used with the Interstage Application Server Enterprise Edition. For more information, refer to the "Creating an Application (C API)" or "Creating an Application (JNDI)" chapter.

1.4.5 Load Balancing (Replication)

If information in the Interstage Directory Service database is managed on one computer, database performance may deteriorate when it becomes large-scaled and the number of accesses increases.

The database sharing function and the replication function enable load balancing in large-scale configurations. These functions can distribute load that is concentrated on a single Interstage Directory Service server or database server.

The database sharing function stores and manages information (entries) from multiple repositories in a single database. It enables information to be managed using a single database server and load on individual servers to be distributed when multiple Interstage Directory Service servers are installed. And, because information is managed using a single database, the environment can be built, operated and managed more easily that when replication is used.

This function can only be used when an RDB is used as the database.

For information on building a database sharing environment, refer to "Database Sharing" in the "Creating a Load Distribution Environment" chapter.

The replication function provides load balancing in a large-scale configuration. This function allows the database of a server to be duplicated to another server.

Using the replication function, any entry modification made in Interstage Directory Service (master), including adding, modifying, and deleting entries, will be reflected in another Interstage Directory Service (slave). Because repository information is managed using more than one database, the load on the database server is more effectively distributed than when the database sharing function is used.

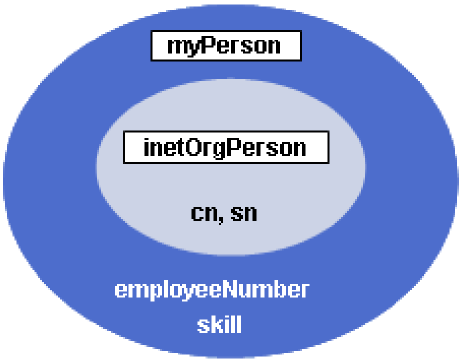
For information on how to build a replication environment, refer to the "Creating a Load Distribution Environment (Replication Mode)" chapter.

1.4.6 Schema Extension

A schema definition defines how information about people, organizations, devices, etc., is stored in a repository. A schema definition can be an object class definition or an attribute definition.

Schema extension refers to adding or inheriting these object class definitions and attribute definitions. Take an object class called "inetOrgPerson" for example. "inetOrgPerson" represents the Internet users of an organization and is usually used for company employee information. To add the technical skills of employees, it is possible to define an attribute named "skill" and then a new object class called "myPerson" that extends inetOrgPerson to include the "skill" attribute.

Figure 1.15 Schema extension



To extend a schema, a definition statement is specified in the schema definition file. The extended schema is referred to as a "user-defined schema" and the file that specified the user-defined schema is referred to as a "user-defined schema file". Note that this function is only available with the Interstage Application Server Enterprise Edition when an RDB is used as the database.

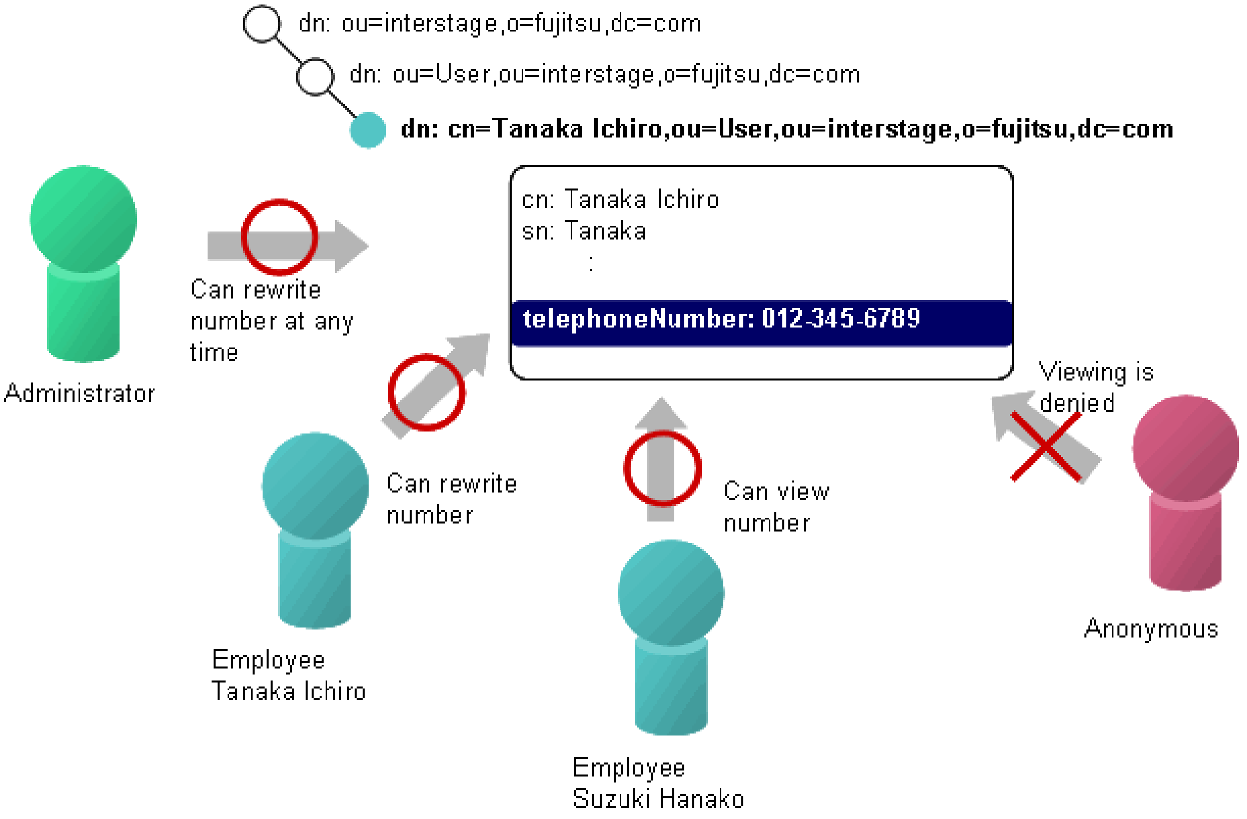
For details on how to extend schemas, refer to "Extending Schemas" in the "Creating a Repository" chapter.

1.4.7 Access Control

Access control is a security enhancement feature that allows viewing and updating rights to be set with respect to attributes and entries in a repository on a per-user basis. Access control is effective for all users (DN) and anonymous users specified when a client accesses a repository.

For example, in the case of the telephone number attribute "telephoneNumber", access control can specify that the user who owns that telephone number has permission to write to it, while anonymous users are forbidden to access it and all other users can only read it.

Figure 1.16 Access control


dn: ou=interstage,o=fujitsu,dc=com
dn: ou=User,ou=interstage,o=fujitsu,dc=com
dn: cn=Tanaka Ichiro,ou=User,ou=interstage,o=fujitsu,dc=com
cn: Tanaka Ichiro
sn: Tanaka
:
telephoneNumber: 012-345-6789
Administrator
Can rewrite number at any time
Can rewrite number
Employee Tanaka Ichiro
Can view number
Employee Suzuki Hanako
Viewing is denied
Anonymous

The access control definition is part of the repository environment definition. The section that defines access control is referred to as the access control list. The access directive (setup parameter) is used to enter definition statements in the access control list definition file. Note that this function is only available with the Interstage Application Server Enterprise Edition when an RDB is used as the database.

For more information on the access control list, refer to "Registering Access Control Lists" in the "Creating a Repository" chapter of this Manual and "Access Control for the Interstage Directory Service" chapter of the Security System Guide.

1.4.8 Operation Monitoring

The access log function collects Interstage Directory Service. This function allows you to check whether any unauthorized access has occurred.

For more information, refer to "Monitoring Repository Operation" in the "Operating and Maintaining Repositories" chapter.

1.5 Compatible Databases

The Interstage Directory Service allows the following databases to be selected for storing information. Refer to "Directory Service" in the "Supported Software" chapter of the Product Notes manual for information on database versions that can be used.

- Standard Database

  This is the standard database that is bundled with Interstage Application Server. It is suitable for use when the number of Interstage Directory Service users or concurrent accesses is small.

- Relational database (RDB)

  This database is suitable for use when 10,000 or more data entries are to be stored, and when the number of Interstage Directory Service users or concurrent accesses is large. The following two types of databases can be selected for use:

  - Symfoware Server

  - Oracle Database

  Note that these databases are not bundled with Interstage Application Server and must be purchased separately.

Chapter 2 Environment Setup

This chapter explains the environment setup required to use Interstage Directory Service.

The environment for Interstage Directory Service is set up using the Interstage Management Console.

Environment definitions such as the following can be set:

- General settings of the repository (such as public directory and Administrator DN)
- Detailed settings of the repository (such as connection settings, access log settings, and replication settings)

To operate the Interstage Management Console, use the following window after starting the Interstage Management Console and logging in.

- To create a repository or define a replication environment:

  Select the [Create a New Repository] tab on the [Repository: View Status] window on the [System] > [Service] > [Repository]

- To reference or modify the simple or detailed settings of the repository:

  Select the Repository option on the Service menu, and then choose the repository name from the list in the [Repository: View Status] window on the [System] > [Service] > [Repository].

To operate the Interstage Management Console on Admin Server, use the following window.

- To create a repository or define a replication environment:

  Select the [Create a New Repository] tab on the [Repository: View Status] window on the [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]

- To reference or modify the simple or detailed settings of the repository:

  Select the Repository option on the Service menu, and then choose the repository name from the list in the [Repository: View Status] window on the [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository].

For information on the startup of the Interstage Management Console, see "Configuring the Interstage Management Console" in the Operator's Guide. For information on window operations of the Interstage Management Console, see "Services" in the Operator's Guide.

2.1 Designing a Repository

Design a repository before installing Interstage Directory Service.

- Choose the operation mode:

  Choose the operation mode of the Interstage Directory Service. The Interstage Directory Service can operate in the following modes:

  - Standalone mode

    In this mode, information is managed using a single Interstage Directory Service server, or a single Interstage Directory Service server and a database server.

  - Database sharing mode

    In this mode, multiple Interstage Directory Service servers are installed and information is managed by a single database server. This mode can only be used when an RDB is used as the database.

  - Replication (master/slave) mode

    In this mode, an Interstage Directory Service server is designated as the master server (update system) and multiple slave servers (reference system) are used to manage copies of the master server.

  Also decide if SSL communication is to be used.

- Design the data

  The following information is stored in the repository:

  - user information such as the user name, password, and E-mail address
  - information on the organization to which the user belongs.

Decide which data is to be stored.

After deciding the data (entries) to be stored in the repository, define the hierarchical structure between entries and entry names.

- Design the data structure (schema)

  Entries stored in the repository must conform to a schema. Decide which schema components are to be associated with the data to be stored in the repository that was determined by the data design. If necessary, also consider the use of schema extensions.

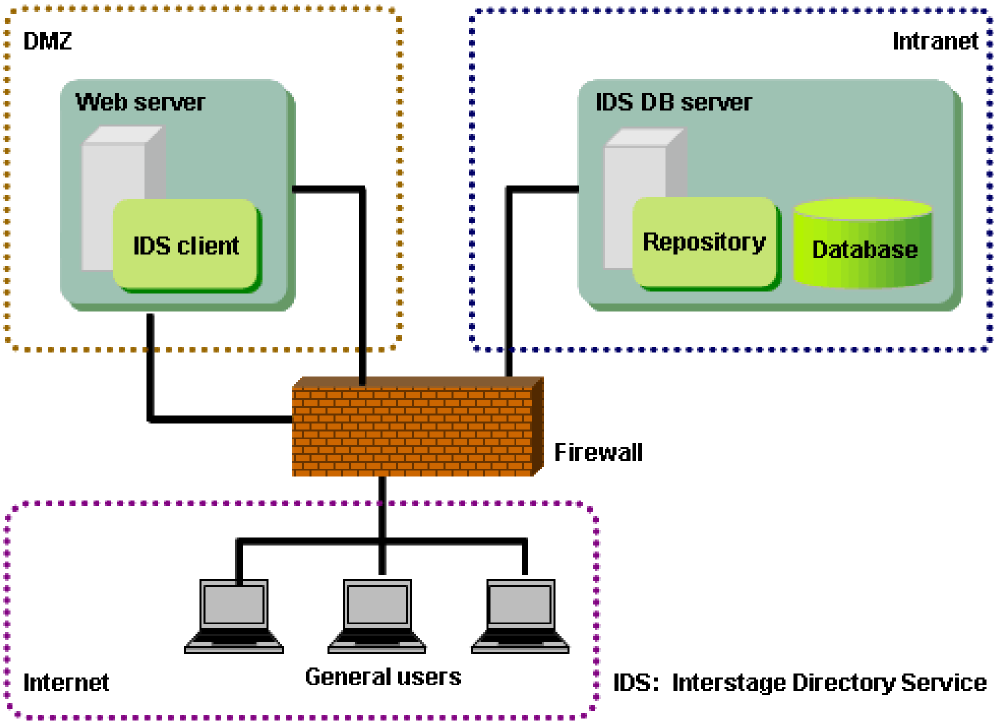
2.1.1 Choosing the Operating Mode

Determining the system configuration and operation mode

Standalone mode

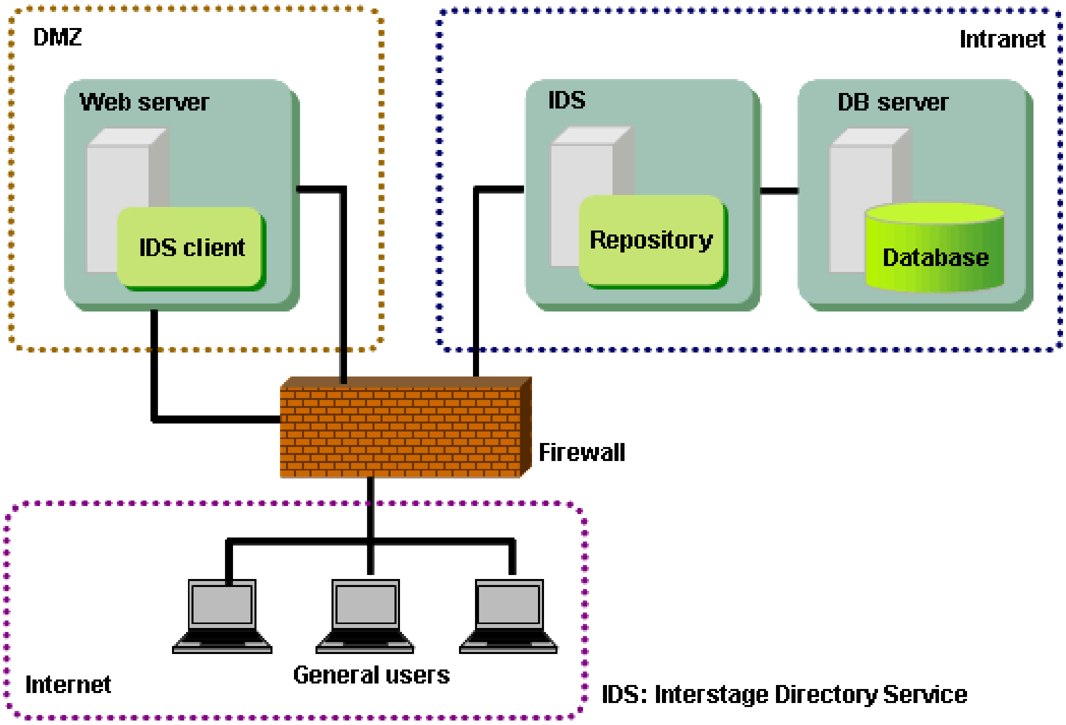
The operating mode in which one server is used to manage information in the Interstage Directory Service is called the standalone mode.

Figure 2.1 Standalone mode



When an RDB database is used, it is also possible to connect to the database on a server that is separate from the Interstage Directory Service. In such cases, the RDB should be installed within the intranet.

Figure 2.2 Standalone mode (Installing the database on a separate server)

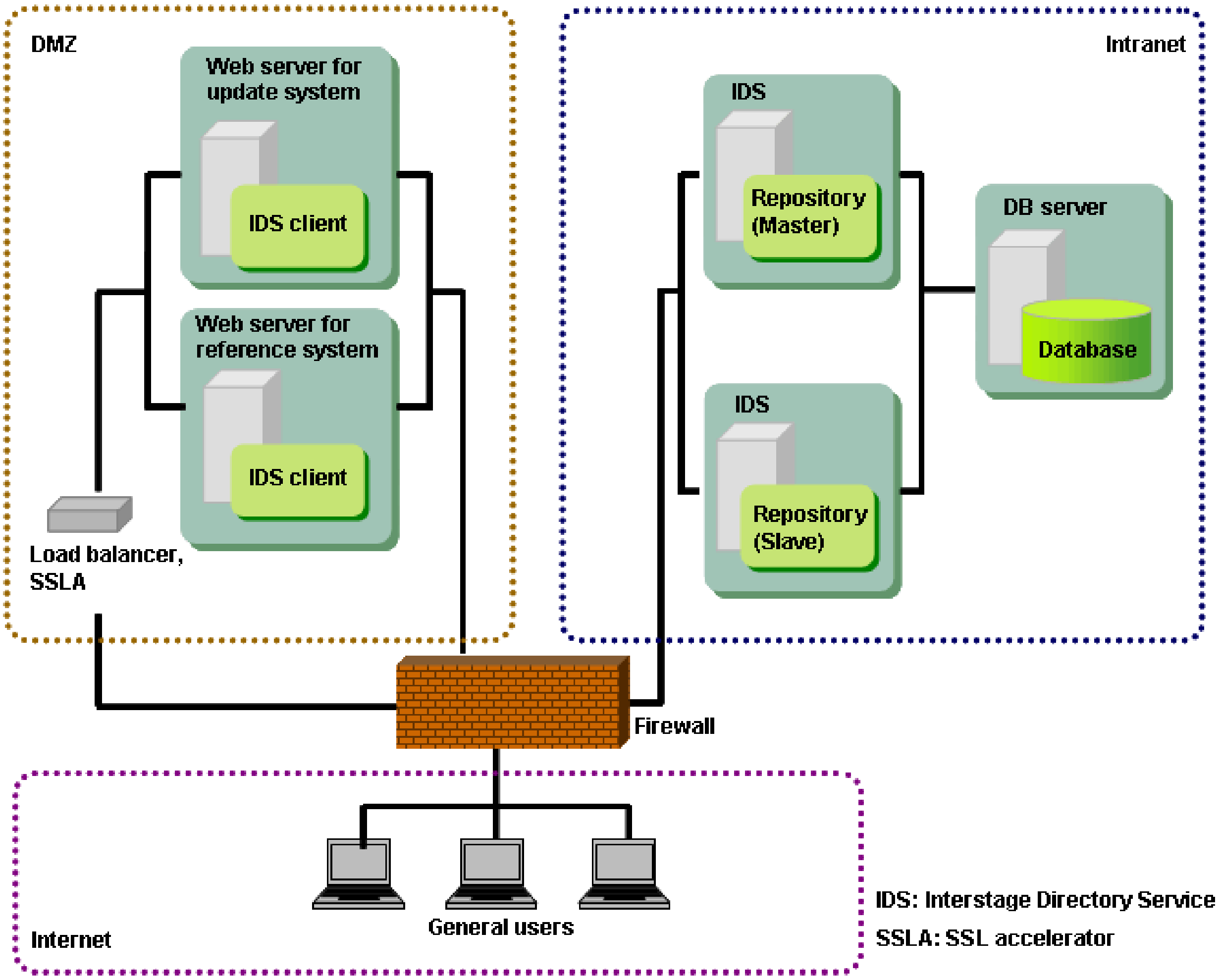


Database sharing mode

In this operation mode, information is managed using a single database server and multiple Interstage Directory Service servers. These are installed so the load is distributed across all servers. This operation mode is suitable when a business system has a large number of users or many concurrent accesses, and it is desirable to distribute load so that it is not concentrated on a single server. And, because information is managed by a single database, this operation mode is easier to build, operate and manage than the replication mode.

This operation mode can only be used when an RDB is used as the database.

Figure 2.3 Database sharing mode

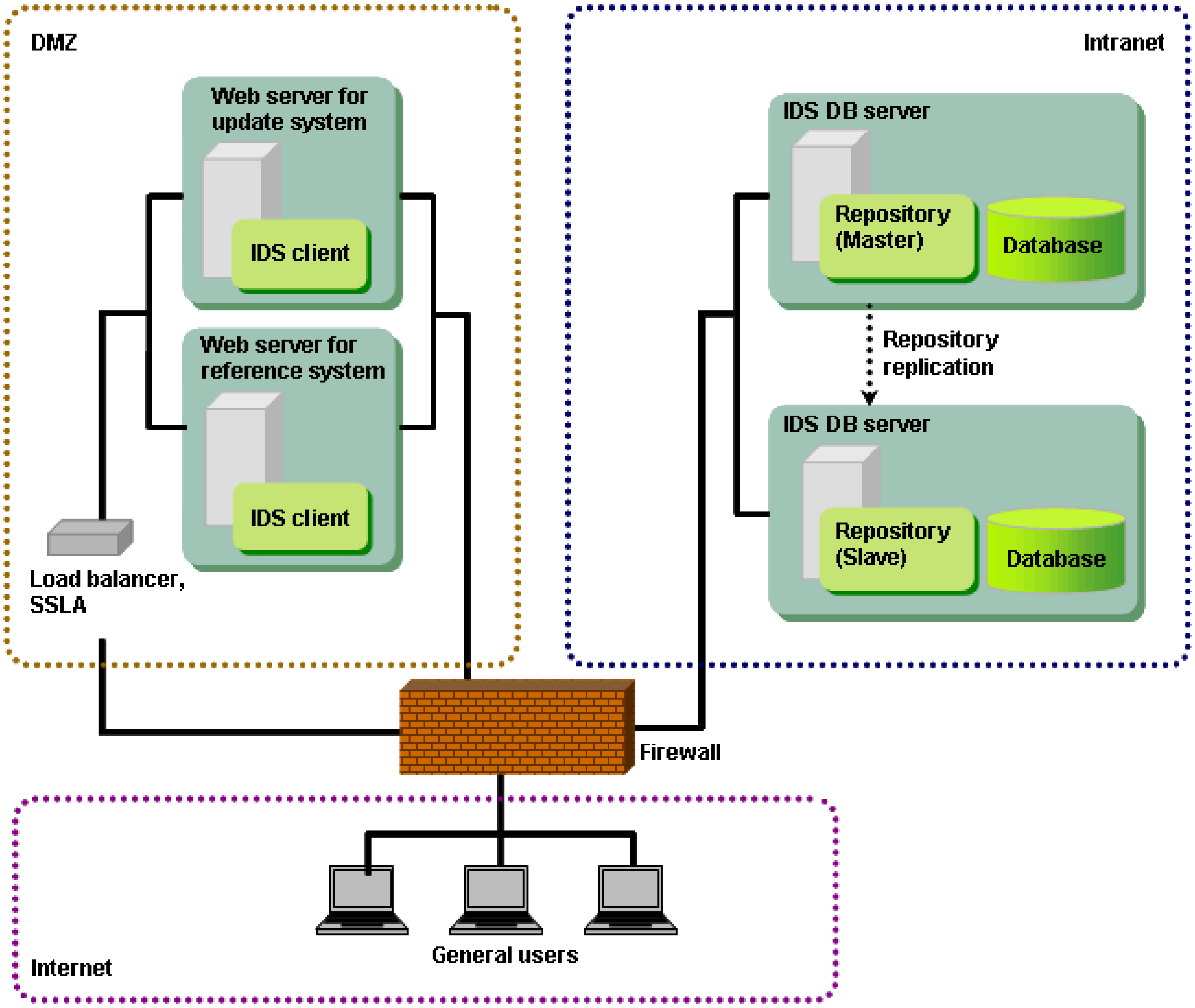


Replication mode

In the standalone and database sharing modes, as the system grows so does the number of system accesses. As a result of this, performance may suffer. The replication function is provided to balance the load in large-scale configurations. Using replication, copies of the server database are created on separate servers with client requests divided between them.

Replication mode not only distributes load to prevent it becoming concentrated on a single server, it can also be used to construct high-reliability systems. Select this mode when the number of business system users or concurrent accesses is large and it is desirable to distribute both load concentrations on individual servers and load concentrations on the database.

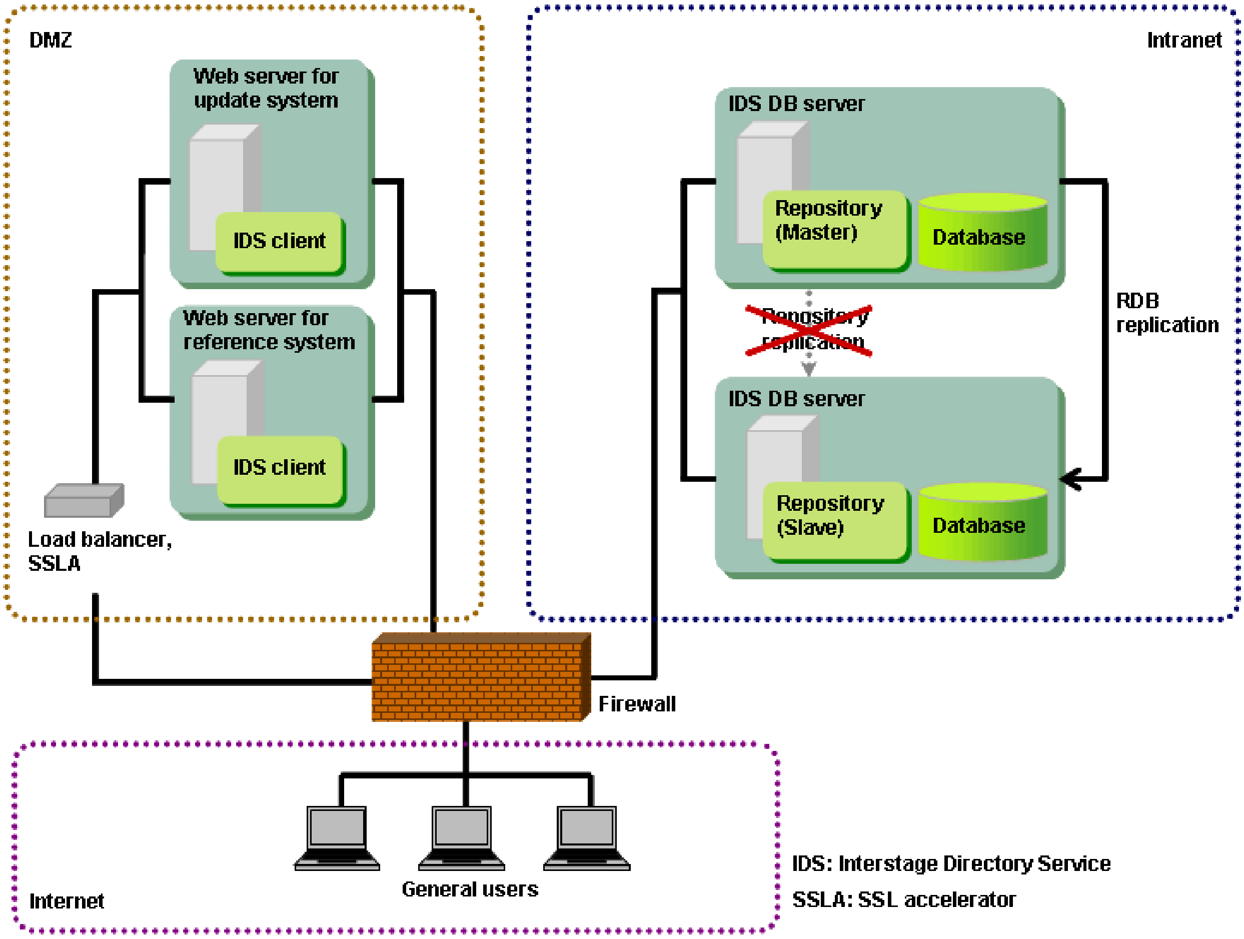
Figure 2.4 Replication mode (using the Standard Database)



The replication function of the Interstage Directory Service cannot be used when an RDB (Symfoware or other) is used. In such cases, the replication function of the RDB itself must be used.

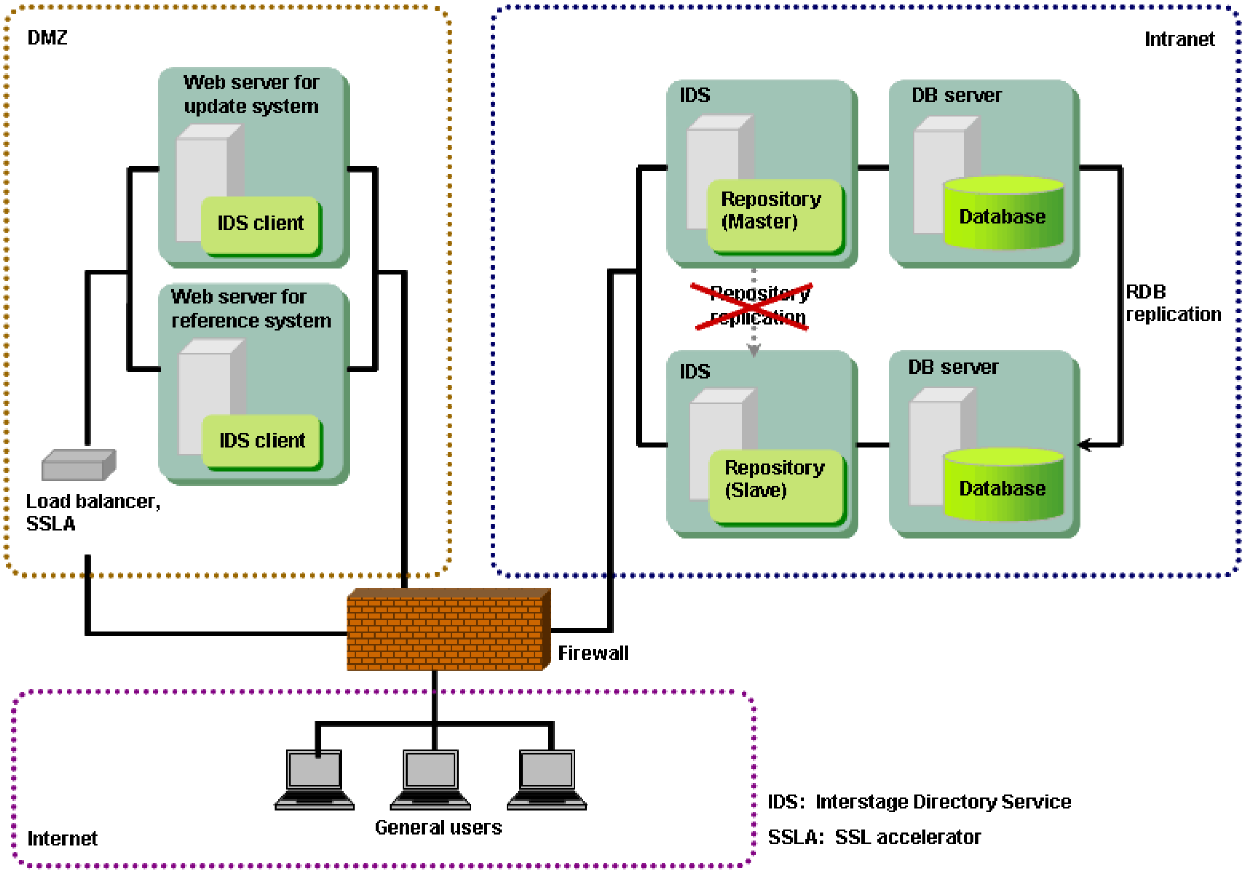
To install the replication mode, it is necessary to set up both the master server that can perform updates of information (such as addition, modification, and deletion) and slave servers that maintain copies.

Figure 2.5 Replication mode (when RDB is Used)



Even in replication mode, it is possible to connect to and use a database on a server other than an Interstage Directory Service server.

Figure 2.6 Replication mode (using an RDB installed on a separate server))



Each operation mode of the Interstage Directory Service can also be used in clustered environments.

For more information on the environment construction procedure for using the Interstage Directory Service in a cluster environment, refer to "Environment Setup Procedure for Cluster Service" in the High Availability Systems Operation Guide.

Decision Whether to Use SSL Communication

Under the initial setup, when clients request processing from Interstage Directory Service, the distinguished name (DN), password, and other communication data are used without encryption. This also applies to communication between the master server and slave servers when replication is used.

SSL communication is used to encrypt data sent in the transmission lines. SSL encryption protects data from the threats of decryption and eavesdropping, even if the communication lines are monitored.

If client authentication is used, access to the SSL server is permitted only to those SSL clients who present a certificate issued by a specific CA, preventing access of clients who disguise themselves.

If the number of clients is large and access to Interstage Directory Service is frequent, it is recommended to reduce the server load by using the SSL accelerator to ensure response performance.

An SSL communication environment needs to be set up before creating a repository.

2.1.2 Designing the Data

This section explains how to design the data (entries) to be stored in a repository, and how to design the directory information trees that determine the hierarchical structure between entries.

2.1.2.1 Designing Data

Decide on the data to be stored in the repository.

The repository is generally used for information searching (similar to a telephone directory) and management of users of the Web server.

Since the repository is suitable for reference (information search), do not store the following types of data in the repository:

- Data that is frequently modified (overwritten)
- Large data, such as image and audio data
- Data with a large number of attributes per unit of data (entry)

By considering not only the current data needs, but also the data that may be needed in the future, the required database capacity and future expansion requirements can be estimated more easily.

2.1.2.2 Designing a Tree

Decide the structure of the directory information tree such as the hierarchical structure between entries and entry names.

Consider the following three points:

- Entry name

  Each entry name in the repository must be unique. Use one or more attribute values for the entry name. The cn attribute (name), for example, is generally employed as the user entry, but if there are two or more users with the same name, it will not be unique. In that case, use the uid (user ID) attribute or employeeNumber (employee number) attribute.

  Note

  A DN identical to the "Administrator DN" cannot be used as an entry name.

- Tree root (public directory)

  Entry at the top (root) of a tree. This entry is specific to the repository and all other entries are stored under this entry. Any attribute can be used as the root entry name, but it is recommended to use the domain name (dc(domainComponent)), organization (o(organization)), and country (c(country)).

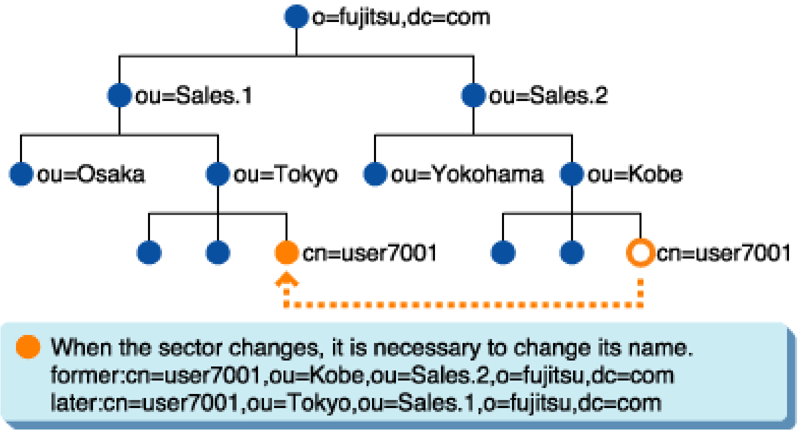
- Relationship between entries

  Make the hierarchical structure of a tree as shallow and flat as possible. This is because any name change should be avoided. Do not use an organization name or department name of a company at a branch point, because organization names may be changed. Name changes can be avoided if entries are divided into "user information," "service," and so on.

  Note that if it there are plans to output entries to an LDIF file to perform maintenance tasks, the design should allow the hierarchical structure of the tree to be divided up so that the number of entries in a single tree is between approximately 10,000 and 100,000 and the output can be split between multiple LDIF files.

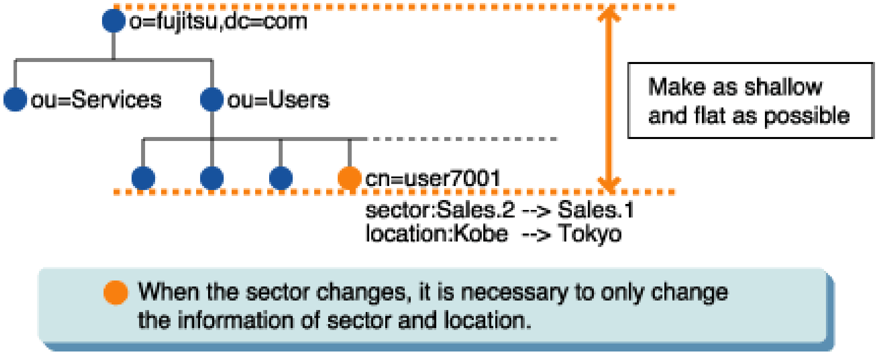
  The following figure below illustrates the complications of changing names within complex hierarchies.

Figure 2.7 Change Sector Details in a Complex Tree


o=fujitsu,dc=com
ou=Sales.1
ou=Sales.2
ou=Osaka
ou=Tokyo
ou=Yokohama
ou=Kobe
cn=user7001
cn=user7001
When the sector changes, it is necessary to change its name.
former:cn=user7001,ou=Kobe,ou=Sales.2,o=fujitsu,dc=com
later:cn=user7001,ou=Tokyo,ou=Sales.1,o=fujitsu,dc=com

In the following figure, since the tree is of a flat structure, changing the sector details does not involve a complex name change.

Figure 2.8 Change Sector Details in a Flat Tree


o=fujitsu,dc=com
ou=Services
ou=Users
cn=user7001
sector:Sales.2 --> Sales.1
location:Kobe --> Tokyo
Make as shallow and flat as possible
When the sector changes, it is necessary to only change the information of sector and location.

2.1.3 Design the Data Structure (schema)

This section outlines data structures (schemas) that can be used.

Information about entries that need to be added or modified in a repository must comply with a schema. If an add/modify request does not obey the schema, an error is returned from the repository.

The following table shows the elements of the LDAP schema.

In Interstage Directory Service, 'Object class definition,' 'Attribute type definition,' 'Attribute syntax definition,' and 'Matching rule definition' can be used.

Table 2.1 Elements of the LDAP Schema

Element	Explanation
Object class definition	Defines the class type, base class, and attributes that an entry can hold.
Attribute type definition	Defines the type of data that an attribute can hold. The attribute type is defined by element, such as the name, attribute syntax, and matching rule.
Attribute syntax definition (syntax)	Defines the characters that can be used for an attribute value and attribute value type.
Matching rule definition (matching rule)	Defines the attribute matching rules that are used to compare and search.
Name format definition	Defines the attributes that can be used for RDN. This element cannot be used by Interstage Directory Service.
DIT structure rule definition	Defines the entry placement restrictions. This element cannot be used by Interstage Directory Service.
DIT content rule definition	Defines the combination of object classes. This element cannot be used by Interstage Directory Service.

The following explains the object class definition and attribute type definition. Details about the attribute syntax definition and matching rule definition is explained in 'Attribute type definition.'

Note

In Interstage Directory Service, the standard schema defined by RFC is used. Schemas can be extended by adding new schemas not included in the standard one, and by inheriting and extending existing schemas.

For information about the schema definitions that can be used in Interstage Directory Service, see Appendix C - List of Object Classes and Appendix D - List of Attributes. Refer to "Extending Schemas" for information on how to extend schemas.

2.1.3.1 Object Class Definition

An object class definition consists of the following elements:

- Object class OID

- Object class name
- Base class
- Object class type
- Required attributes
- Optional attributes.

Object Class OID

Object identifier, OID (Object IDentifier), to identify each object class.

OID is assigned not only to each object class, but also to each element in LDAP. This is an ISO standard.

Object Class Name

Name of the object class to be defined.

Base Class

This is a definition of an object class on which another object class is based. If defining some object class, it may be defined based on the definition of another object class. The object class on which a new definition is based is called the base class.

A derived class inherits the required attributes and optional attributes from the base class.

Object Class Type

An object class can be divided into one of the following categories, abstract type (ABSTRACT), structural type (STRUCTURAL), or auxiliary type (AUXILIARY). These categories are explained in the following table.

Table 2.2 Object Class Types

Type	Explanation
Abstract type (ABSTRACT)	An object class provided to define other object classes. Top is a typical example of this type of object class. An entry that belongs to an abstract object class only cannot exist.
Structural type (STRUCTURAL)	An object class from which an entry can be created. An entry must always belong to one of the structural object classes.
Auxiliary type (AUXILIARY)	An object class that cannot create an entry alone and can create one only in combination with another structural object class. An entry that belongs to an auxiliary object class only cannot exist.

Required Attributes

Attributes of an object class that must be registered when using the class.

Optional Attributes

Attributes (not required) of an object class that are used as additional information when using this class.

For information about the object class definition that can be used in Interstage Directory Service, see 'List of Object Classes.'

2.1.3.2 Attribute Type Definition

An attribute type definition consists of the following elements:

- Attribute type OID
- Attribute type name
- Base attribute type

- Matching rules
  - Matching rules of equality
  - Matching rules of ordering
  - Matching rules of substring matching
- Attribute syntax
- Single flag

Attribute Type OID

OID to identify the attribute type.

Attribute Type Name

Name of the defined attribute.

Base Attribute Type

Attribute on which another attribute is based. The attribute syntax and matching rules are inherited from the base attribute type. However, in contrast to the object classes, there are also some cases where an attribute type does not inherit from another attribute type.

Matching Rules

Matching rules describe the conditions checked when comparing attributes. If the matching rules are not specified, comparisons between attributes cannot be made to match them.

- Matching Rules of Equality

  Matching rules based on values being equal are applied for searches and other operations.

Table 2.3 Matching Rules of Equality

Name	Explanation
objectIdentifierMatch	OID
distinguishedNameMatch	DN
caseIgnoreMatch	Case-insensitive, space ignored
caseExactMatch	Case-sensitive, space ignored
numericStringMatch	Numeric string
booleanMatch	True/false
octetStringMatch	Optional octet string
telephoneNumberMatch	Case-insensitive, space and '-' ignored
caseExactIA5Match	Case-sensitive, space ignored
caseIgnoreIA5Match	Case-insensitive, space ignored
caseIgnoreListMatch	Case-insensitive, space ignored
integerMatch	Numeric string
generalizedTimeMatch	Character string that can be used in local time or international standard time

- Matching Rules of Ordering

  Matching rules based on inequality are applied for searches and other operations.

Table 2.4 Matching Rules of Ordering

Name	Explanation
caseIgnoreOrderingingMatch	Case-insensitive, space ignored
caseExactOrderingingMatch	Case-sensitive, space ignored
generalizedTimeOrderingMatch	Character string that can be used in local time or international standard time

- Matching Rules of Substring Matching

  Matching rules are applied for searches or comparisons with a partial string.

Table 2.5 Substring Matching

Name	Explanation
caseIgnoreIA5SubstringsMatch	Case-insensitive, leading and trailing spaces ignored, consecutive spaces treated as single spaces
caseIgnoreListSubstringsMatch	Case-insensitive, space ignored
caseIgnoreSubstringsMatch	Case-insensitive, space ignored
caseExactSubstringsMatch	Case-sensitive, space ignored
numericStringSubstringsMatch	Numeric string

Attribute Syntax

Format of the attribute values:

Table 2.6 Attribute Values Syntax

Syntax	Allowable Value
Audio	Sound data can be used. (Binary type)
Binary	Binary data can be used. (Binary type)
Certificate	Certificate data can be used. (Binary type)
Certificate List	Certificate list data can be used. (Binary type)
Certificate Pair	Certificate pair data can be used. (Binary type)
Directory String	Usable within the range handled by UTF-8. In terms of characters, this corresponds to being within the Unicode range. (String type)
DN	DN can be used. (String type) Example: cn=User001,o=fujitsu,dc=com
Facsimile Telephone Number	Strings similar to those of Printable String can be used. (String type)
Generalized Time	The local time (using the YYYYMMDDhhmmss.p or "YYYYMMDDhhmmss.p(+|-HHMM)" format) or the international standard time (YYYYMMDDhhmmss.pZ format) can be used. (String type)
IA5 String	The CCITT International Alphabet No.5 (equivalent to ASCII) can be used. (String type)
INTEGER	Numeric characters can be used. (Numeric type) Example: 1321
JPEG	JPEG data can be used. (Binary type)
Name And Optional UID	Character string of the format "<DN>#<bit string>". The "#<bit string>" component is optional. (String type)
Numeric String	Numeric characters (0 to 9) and space can be used. (String type) Example: 1997

Syntax	Allowable Value
Octet String	Byte strings (Each byte is any value between 0x00 and 0xFF) can be used. (String type)
OID	OID can be used. (String type) Example: 1.2.3.4
Other Mailbox	Electronic mailbox data other than X.400 and RFC822 can be used. (String type) The format is as follows: mailbox-type '$' mailbox mailbox-type is the type of mail and mailbox is a mail address Example: user001@interstage.fujitsu.com

Postal Address	Usable within the range (Unicode) handled by Directory String. (String type)
	*1: Using alphanumeric characters only results in the following format. Up to six dstring can be combined.
	postal-address = dstring *('$' dstring)
	dstring = 30 alphanumeric characters

Printable String	Alphanumeric characters and the following symbols can be used: (String type) - Space - ''' (Single quotation mark) - '(' (left bracket) - ')' (right bracket) - '+' (plus sign) - ',' (comma) - '-' (Minus sign) - '.' (period) - '/' (slash) - ':' (colon) - '=' (equals sign) - '?' (question mark)
Supported Algorithm	Syntax of the supportAlgorithm attribute. (Binary type)
Telephone Number	Characters similar to those of Printable String can be used. (String type) *1: Using '-' (Minus sign) and space results in the following examples: If searched with telephoneNumber=0123* 012-345-6789 0123456789 Both hit.
Telex Number	The Teletex numbers can be used. The format is as follows: (String type) actual-number '$' country '$' answerback actual-number syntactically represents the number part of the Teletex number that is to be encrypted. Country is the country code of Teletex and answerback is the return code for the Teletex terminal.

Single Flag

The single flag indicates whether one or multiple attribute values can be set.

For example, the telephone number may use multiple attributes, but using multiple attributes for an employee number could cause problems. In such a case, set the single flag to True.

For the attribute type definition, attribute syntax definition, and matching rule definition that can be used in Interstage Directory Service, see 'List of Attributes.'

2.2 Flow of the Environment Setup

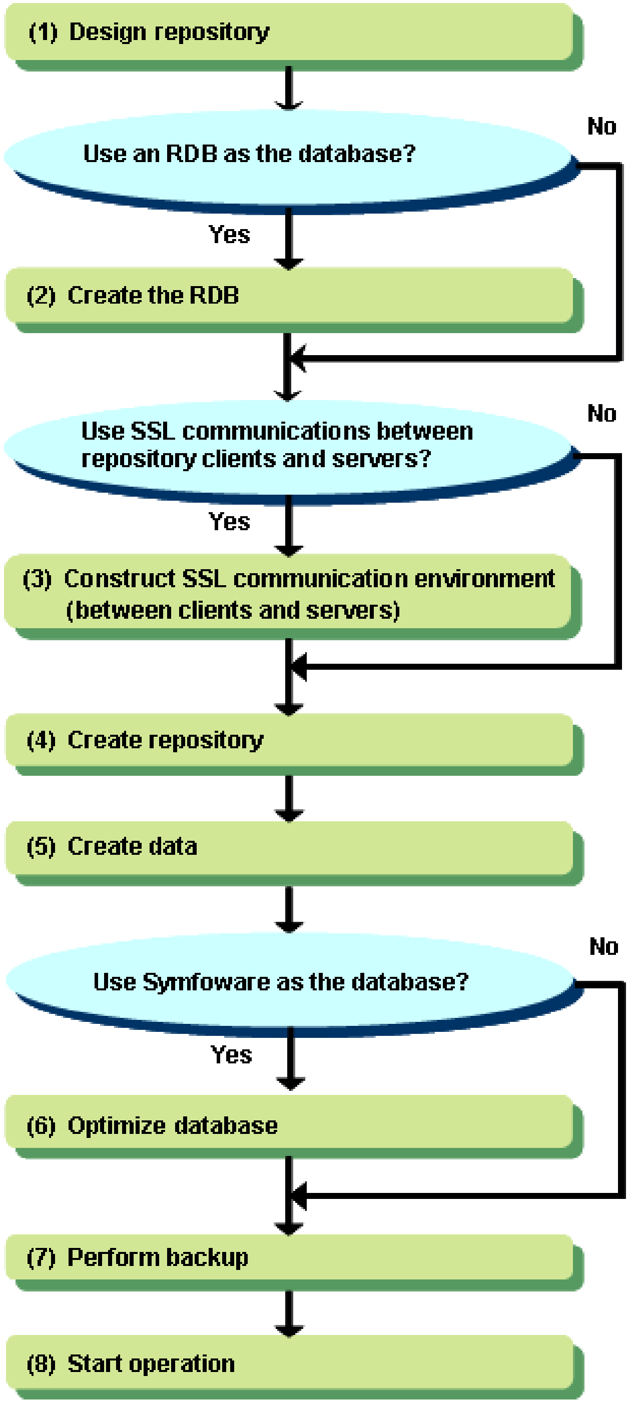
The environment setup for Interstage Directory Service can roughly be divided into the following five parts (although these steps vary depending on the configuration being setup):

- Repository design (data and tree design and operating mode decision)
- Database creation
- SSL communication environment setup (required only if SSL communication is used)
- Repository creation
- Registration of user information

Application development is common to standalone mode, database sharing mode and replication mode. When database sharing mode is used, it is necessary to create the repositories that will share the database; when replication mode is used, it is necessary to create the slave server environment.

When creating more than one repository, an RDB must be created for each one.

Figure 2.9 Environment Setup Flow


(1) Design repository
Use an RDB as the database?
No
Yes
(2) Create the RDB
Use SSL communications between repository clients and servers?
No
Yes
(3) Construct SSL communication environment (between clients and servers)
(4) Create repository
(5) Create data
Use Symfoware as the database?
No
Yes
(6) Optimize database
(7) Perform backup
(8) Start operation

Operations using standalone mode

For operations using the standalone pattern, create an environment using the following procedure:

1. Designing a Repository
2. Creating a database

   Perform this operation when using an RDB as the database.
3. Setting up an Environment for SSL Communication

   Perform this operation if SSL communication is to be used.

4. Creating a Repository
5. Creating data

Operations using database sharing mode

For operations using database sharing mode, create an environment using the following procedure: For operations that use the database sharing pattern, create an environment using the following procedure:

1. Designing a Repository
2. Creating a database
3. Setting Up an Environment for SSL Communication

   Perform this operation if SSL communication is to be used.
4. Creating a Repository
5. Creating data

Operations using replication mode

For operations using replication mode, create an environment using the following procedure.

Note that when an RDB is used for the database, the replication function of the Interstage Directory Service cannot be used for replication mode. In such cases, the replication function of the RDB itself must be used instead.

1. Designing a Repository
2. Creating a Database
3. Setting up an Environment for SSL Communication

   Perform this operation if SSL communication is to be used.
4. Creating a Repository
5. Setting Up an Environment for Replication Mode
6. Creating Data

Perform "Setting up an Environment for SSL Communication" in step 3 of each operation mode when encrypted communication based on SSL is to be used between Interstage Directory Service clients and servers. SSL is recommended for communications in the Interstage Directory Service.

Chapter 3 Creating Databases

3.1 Using the Symfoware/RDB

If Symfoware/RDB is used for the repository database, create an environment for Symfoware/RDB before creating the repository.

Additionally, if Symfoware/RDB is installed on a different machine to the Interstage Directory Service, the Symfoware Server client function must be installed on the machine where the Interstage Directory Service is installed. Ensure that the Symfoware Server client function is installed before creating the tables for storing repository data. Refer to the Symfoware Server Installation Guide (Client Edition) for information about installing the Symfoware Server client function.

3.1.1 Estimating the Resources used by Symfoware/RDB

Estimate the following resources used by Symfoware/RDB:

- The capacity of the RDB dictionary
- The RDB directory file
- The log capacity
- Log group management files
- Log management files
- Temporary log files
- Archive log files
- In-doubt log files
- Work area
- Audit log
- RDB system disk space
- RDB system memory

As an estimate for the disk space used in the RDB system, approximately 10GB of database space is required to register 100,000 entries in the repository, and approximately 100GB of database space is required to register 1,000,000 entries in the repository.

For details about the resource estimation formula, refer to the "Estimating Resources for Symfoware/RDB" chapter.

3.1.2 Creating a Raw Device

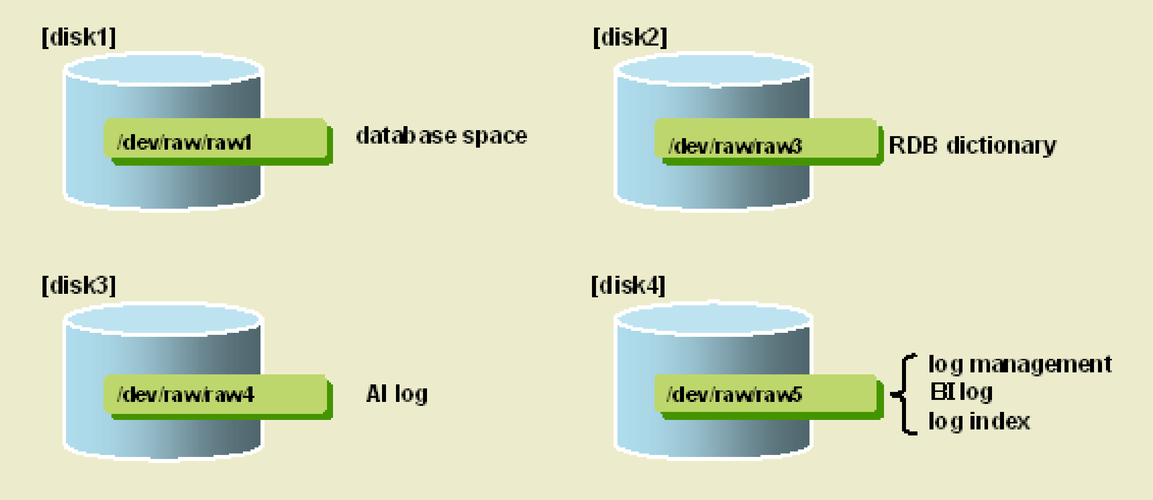
Reserve the raw device required for Symfoware/RDB operations. It is recommended that the database resources used by Interstage Directory Service be placed on the raw device. (These database resources can also be placed on the file system.)

Windows32/64

If Symfoware/RDB uses a SynfinityCluster cluster configuration, database resources can be placed on the raw device.

The following example shows the creation of the raw devices.

Figure 3.1 Creation of Raw Devices



Refer to "Preparations before setup" in the Symfoware Server Setup Guide for more information on creating a raw device.

3.1.3 Tuning the Kernel Resources

Solaris32/64 Linux32/64

To run Symfoware/RDB, kernel resources for the Symfoware/RDB operating environment definition must be secured.

The kernel resources required to run Symfoware/RDB are as follows:

- Shared memory resources
- Semaphore resources
- Message queue resources

For details about the kernel resources required to run Interstage Directory Service using Symfoware/RDB in the repository database, refer to "System Resources of the Interstage Directory Service" in the "System Tuning" chapter of the Tuning Guide.

For details about the Symfoware/RDB kernel resources, refer to "Preparation before setup" - "Preparation" in the Symfoware Server Setup Guide.

3.1.4 Setting up Symfoware/RDB

The procedure for setting up Symfoware/RDB is shown below. It is recommended that these operations be performed using the Symfoware Server WebAdmin or commands.

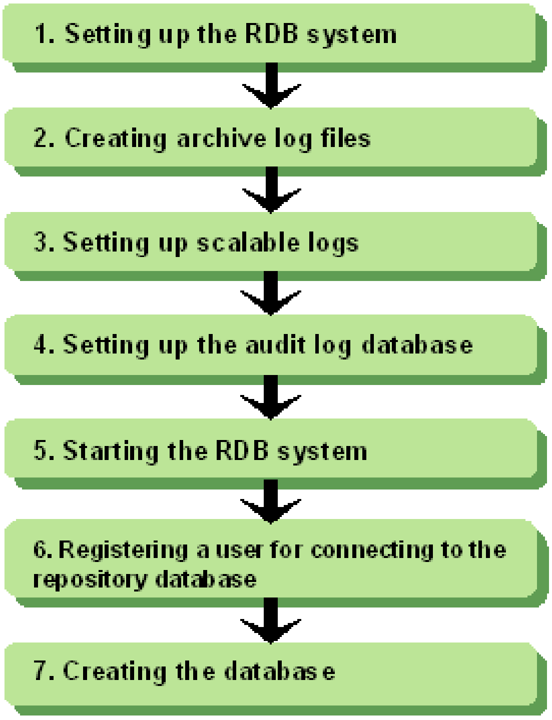
- Creating more than one repository

  If more than one repository is created, repeat steps 6 and 7 below for each repository. If the same connection user runs the repository database in more than one repository, step 6 is unnecessary. In this case, repeat step 7.

- Creating an environment for database sharing configurations

  Perform the following procedure only once, in order to share the database. Refer to "Database Sharing" in the "Creating a Load Distribution Environment" chapter for more information.

Figure 3.2 Symfoware/RDB Setup Flow


1. Setting up the RDB system
2. Creating archive log files
3. Setting up scalable logs
4. Setting up the audit log database
5. Starting the RDB system
6. Registering a user for connecting to the repository database
7. Creating the database

3.1.4.1 Setting up the RDB System

Set up the RDB system used by Interstage Directory Service. Create the RDB system so that it meets the following conditions:

- The RDB system must be specified.

  Characters that can be used for the RDB system name are alphanumeric, the start character of which must be a letter. Specify a maximum of 8 characters.

- Register the port number for remote connections (e.g., 2050)

- The number of local connections ((the maximum number of connections from the repository to the RDB + 1) * the number of repositories).

  Specify this to connect to a local Symfoware/RDB.

- The number of remote connections ((the maximum number of connections from the repository to the RDB + 1) * the number of repositories).

  Specify this to connect to a remote Symfoware/RDB. (Seen from the Symfoware/RDB, Interstage Directory Service is the database client used for remote connections.)

- If database resources are placed on a raw device, place the RDB directory file on the raw device as well.

Refer to "Setting up Symfoware/RDB using WebAdmin" or "Setting up Symfoware /RDB using commands" in the Symfoware Server Setup Guide for more information on creating an RDB system.

The maximum number of connections from the repository to the RDB is set when the repository is created. For details, refer to "Using the Symfoware/RDB" in the "Creating a Repository" chapter.

3.1.4.2 Creating Archive Log Files

To perform recovery by applying archive logs, create at least two archive log files.

1. Initialize the archive log files

   Use the *rdblog* command -G and -a options to initialize the archive log files.

   Refer to "3.1.1 Estimating the Resources used by Symfoware/RDB" and specify the calculated archive log file capacity.

2. Add the archive log files

   Use the *rdblog* command -U and -a options to add the archive log files. The size of the added archive log files cannot be specified at this time. The initialized value is used regardless of the size of the specified raw device.

Refer to "Setting up Symfoware/RDB using commands" in the Symfoware Server Setup Guide for more information.

3.1.4.3 Setting up Scalable Logs

In scalable log applications, set up the scalable log according to the following procedure:

1. Edit the RDB configuration parameter files

   The log group management files required for scalable log applications must be created. Specify the log group management file directory in RDBLOGGROUPMANAGE of the RDB configuration parameter file.

   For details about the RDB configuration parameter files, refer to "Symfoware/RDB application parameter definitions" in the "Symfoware Server Setup Guide".

2. Create the log group management files

   Use the *rdblog* command -M option to create the log group management files.

   The log group management files are created in the raw device or directory specified in RDBLOGGROUPMANAGE in the RDB configuration parameter file.

3. Create the user log group log management files

   Use the *rdblog* command -I and -g options to create the user log group log management files.

   The user log group log management files are created in the raw device or directory specified in the command. This command can only be executed for the number of log groups that exist.

4. Create the user log group temporary log files

   Create the user log group temporary log files. Use the *rdblog* command -G, -t, and -g options to create the temporary log files.

5. Create the user log group archive log files

   To recover user log group resources by applying the archive log, 2 or more archive log files must be created.

   a. Initialize the archive log files

      Use the *rdblog* command -G and -a options to initialize the archive log files.

      Refer to "3.1.1 Estimating the Resources used by Symfoware/RDB" and specify the calculated archive log file capacity.

   b. Add the archive log files

      Use the *rdblog* command -U and -a options to add the archive log files. The size of the added archive log files cannot be specified at this time. The initialized value is used regardless of the size of the specified raw device.

6. Create the user log group RDB directory files

   Use the *rdbscldir* command -G option to create the user log group RDB directory files.

For scalable log operations, set up scalable logs. Refer to "Setting up Symfoware/RDB using commands" in the Symfoware Server Setup Guide for more information.

3.1.4.4 Setting up the Audit Log Database

In audit log applications, set up the audit log according to the following procedure:

Set up the audit log database according to the following procedure:

1. Create the log group management files

   Create the audit log database log group for the audit log application. If there is already a scalable log application, this task is unnecessary. If there is no scalable log application, perform the following tasks and create the log group management files.

   If Symfoware/RDB is running, stop it.

   Specify the path of the log group management file raw device or directory in RDBLOGGROUPMANAGE of the RDB configuration parameter file.

   For details about the RDB configuration parameter files, refer to "Symfoware/RDB application parameter definitions" in the "Symfoware Server Setup Guide".

   After RDBLOGGROUPMANAGE is specified, use the *rdblog* command -M option to create the log group management files.

2. Create the audit log database log management files

   Create the audit log database log management files. Use the *rdblog* command -I and -g options to create the log management files. Specify "#RDBII_ADTLOG#" in the log group name.

3. Create the audit log database temporary log files

   Use the *rdblog* command -G, -t, and -g options to create the audit log database temporary log files. Specify "#RDBII_ADTLOG#" in the log group name.

4. Create the audit log database

   Create the audit log database for obtaining the audit log.

   a. Create the audit log database

      Use the *rdbaudit* command -c, -n, -s, and -r (or -f) options to create the audit log database.

      Start Symfoware/RDB, and then execute the *rdbaudit* command.

      Note

      - If the audit log database is created on one disk, the audit log application cannot continue if disk input/output errors occur in the audit log database. For this reason, it is recommended that audit log elements are distributed to more than one disk before they are added.

   b. Add the audit log elements

      Use the *rdbaudit* command -a, -n, and -r options to add the audit log elements.

5. Select the audit log get range

   Tune the audit log get range and the action to take when the audit log database is full in the SET SYSTEM PARAMETER statement.

   - AUDIT_SESSION_SUCCESS

     Specify whether or not to get the audit log for executing the application when the connection is successful.

   - AUDIT_SESSION_FAIL

     Specify whether or not to get the audit log for executing the application when the connection fails.

   - AUDIT_ACCESS_SUCCESS

     Specify whether or not to get the audit log for successful access to tables and procedural routine resources.

   - AUDIT_ACCESS_FAIL

     Specify whether or not to get the audit log for unsuccessful access to tables and procedural routine resources.

   - AUDIT_MANAGE

     Specify whether or not to get the audit log for administrator execution.

   - AUDIT_ERROR

     Specify whether or not to get the audit log for major errors and other problems that occur in the system.

- AUDIT_LOG_FULL

  Specify the action to take when the audit log database is full.

For details, refer to "Setting up Symfoware/RDB using commands" in the Symfoware Server Setup Guide.

3.1.4.5 Starting the RDB System

Start the RDB system created in "3.1.4.1 Setting up the RDB System" using the *rdbstart* command. Refer to "Starting and stopping Symfoware Server" in the Symfoware Server Setup Guide for more information on starting the RDB system.

3.1.4.6 Registering a User for Connecting to the Repository Database

In Interstage Directory Service, the user that accesses Symfoware/RDB is called the "repository database connection user".

The user account of the repository database connection user must be registered in the OS for the repository database connection user to be able to access the database. A maximum of 30 characters in the range 'A' to 'Z', and 0 to 9 can be used in the database connection user name (schema name) for the repository. The first character must be a letter.

For details about how to register the user account, refer to the OS documentation.

3.1.4.7 Creating the Database

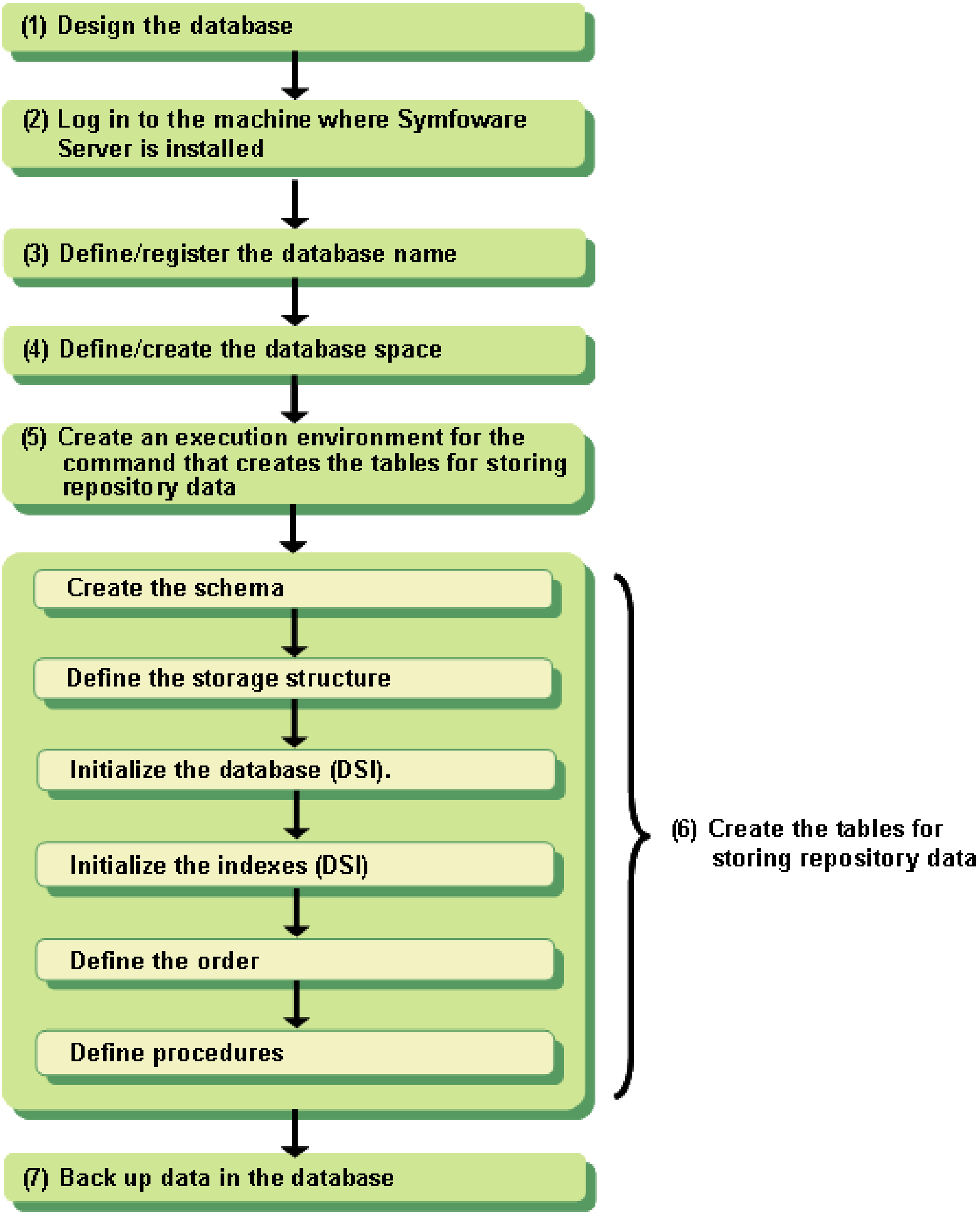
Create the database.

If Interstage Directory Service and Symfoware Server have been installed on different machines, perform these operations on the machine where Symfoware Server has been installed.

The database can be created with or without using Symfoware Server WebDBtools.

If WebDBtools is used, refer to the Symfoware Server WebDBtools User's Guide, otherwise refer to the Symfoware Server RDB Operator's Guide (Database Definitions).

Figure 3.3 Procedure for Creating the Database


(1) Design the database
(2) Log in to the machine where Symfoware Server is installed
(3) Define/register the database name
(4) Define/create the database space
(5) Create an execution environment for the command that creates the tables for storing repository data
Create the schema
Define the storage structure
Initialize the database (DSI).
Initialize the indexes (DSI)
Define the order
Define procedures
(6) Create the tables for storing repository data
(7) Back up data in the database

1. Design the database

   Database design involves table design, attribute design and storage structure design. The tables, attributes and storage structure have been designed to be appropriate for repositories, and are defined and set up using the repository data storage table creation command described later in this procedure.

   If table or attribute design meets the following conditions, detailed settings for tables must be made:

   - Multiple database spaces are used
   - The maximum length of attribute values is changed

     The initial value for the maximum length is 942 bytes for string-type attributes and 32 kilobytes for binary-type attributes)
   - There are more than 20 attributes (including the "objectClass" attribute) per entry on average
   - The total size of the binary attributes per entry is greater than 2 kilobytes
   - The average size of string-type attributes registered in the repository is longer than 200 bytes

Create a detailed definition file in advance, by referring to '3.2.4.1 Detailed Settings for Tables'. Specify this detailed definition file when creating tables.

Example: The total size of the binary attributes per entry is greater than 2 kilobytes

Windows32/64

```
# First entry
dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
cn: User001
sn: Fujitsu
jpegPhoto:< file:///C:\data\photo1.jpg                  <- 2.5 KB binary file
jpegPhoto:< file:///C:\data\photo2.jpg                  <- 2.0 KB binary file

# Second entry
dn: cn=User002,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: User002
sn: Fujitsu CREATE DATABASE SRDB
```

Solaris32/64 Linux32/64

```
# First entry
dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
cn: User001
sn: Fujitsu
jpegPhoto:< file:///data/photo1.jpg                  <- 2.5 KB binary file
jpegPhoto:< file:///data/photo2.jpg                  <- 2.0 KB binary file

# Second entry
dn: cn=User002,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: User002
sn: Fujitsu CREATE DATABASE SRDB
```

a. Total size of the binary-type attribute for the first entry = 2.5K + 2.0K

= 4.5 KB

a. Total size of the binary-type attribute for the second entry = 0 bytes

b. Number of entries = 2

c. ((a) + (b)) / (c) = 2.25 KB

In this example, detailed settings for tables must be made because the total size of binary attributes per entry is more than 2 kilobytes.

Example: The average size of string-type attributes registered in the repository is longer than 200 bytes

Windows32/64

```
# First entry
dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
# First entry
```

```
dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com   <- 49 bytes
objectclass: top                                        <- 3 bytes
objectclass: person                                     <- 6 bytes
objectclass: organizationalPerson                       <- 20 bytes
cn: User001                                             <- 7 bytes
sn: Fujitsu                                             <- 7 bytes
description:< file:///C:\data\sentence1.txt             <- 1,500 bytes of text

# Second entry
dn: cn=User002,ou=User,ou=interstage,o=fujitsu,dc=com   <- 49 bytes
objectclass: top                                        <- 3 bytes
objectclass: person                                     <- 6 bytes
objectclass: organizationalPerson                       <- 20 bytes
cn: User002                                             <- 7 bytes
sn: Fujitsu                                             <- 7 bytes
description:< file:///C:\data\sentence2.txt             <- 1,200 bytes of text
```

Solaris32/64 Linux32/64

```
# First entry
dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
# First entry
dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com   <- 49 bytes
objectclass: top                                        <- 3 bytes
objectclass: person                                     <- 6 bytes
objectclass: organizationalPerson                       <- 20 bytes
cn: User001                                             <- 7 bytes
sn: Fujitsu                                             <- 7 bytes
description:< file:///data/sentence1.txt                <- 1,500 bytes of text

# Second entry
dn: cn=User002,ou=User,ou=interstage,o=fujitsu,dc=com   <- 49 bytes
objectclass: top                                        <- 3 bytes
objectclass: person                                     <- 6 bytes
objectclass: organizationalPerson                       <- 20 bytes
cn: User002                                             <- 7 bytes
sn: Fujitsu                                             <- 7 bytes
description:< file:///data/sentence2.txt                <- 1,200 bytes of text
```

a. Total size of the string-type attributes for the first entry = 49 + 3 + 6 + 20 + 7 + 7 + 1,500

= 1,592 bytes

a. Total size of the string-type attributes for the second entry = 49 + 3 + 6 + 20 + 7 + 7 + 1,200

= 1,292 bytes

a. Total number of string-type attributes for the first entry = 7

b. Total number of string-type attributes for the second entry = 7

c. ((a) + (b)) / ((c) + (d)) = 206 bytes

In this example, detailed settings for tables must be made because the average size of the string-type attributes registered in the repository is longer than 200 bytes.

The design for the storage structure must include an estimate for the amount of database space required. The amount of database space required depends on the amount of data to be stored in the repository, so estimate this value by referring to the Appendix 'Estimating Database Spaces'.

2. Log in to the machine where Symfoware Server has been installed

   Windows32/64

   Log in to the console of the machine on which Symfoware Server is installed or to a remote desktop that is connected to the console session.

Log in using the 'Administrator' (Windows(R)) or 'root' (Solaris/Linux) authority for a user/command, or the operating system account that was registered in "3.1.4.6 Registering a User for Connecting to the Repository Database".

3. Define and register the database name

   Use the command or WebDBtools to execute the following SQL.

   Example: Defining the database name as "DSDB"

```
CREATE DATABASE DSDB
```

   When defining and registering the database name, specify an arbitrary name using up to eight alphanumeric characters, the start character of which must be a letter. Make a note of the database name and save it so that it can be backed up and restored following an error.

4. Define and create the database space

   Use the command or WebDBtools to execute the following SQL.

   Windows32/64

   Example: When the "DSDBSPACE" database space is defined for a raw device with the "SHD_RAW_DIR" logic drive name

```
CREATE DBSPACE DSDBSPACE ALLOCATE RAWDEVICE \\.\SHD_RAW_DIR
```

   Solaris32/64 Linux32/64

   Example: Defining the database space name as "DSDBSPACE" in raw device /dev/raw/raw4

```
CREATE DBSPACE DSDBSPACE ALLOCATE RAWDEVICE /dev/raw/raw4
```

   If detailed settings are not made when the tables for storing repository data are created, specify "DSDBSPACE" as the database space name when defining and registering the database space name. Make a note of the database space name ("DSDBSPACE") and save it so that it can be backed up and restored following an error.

5. Create an environment for the command for creating the tables for storing repository data.

   If Interstage Directory Service and Symfoware Server have been installed on different machines, the executable environment for the table creation command must be created. This environment must also be created if a table is created by a repository database connection user that is not the system administrator, even if Interstage Directory Service and Symfoware Server are installed on the same server.

   On the server used to install Interstage Directory Service, the directory shown below contains files with compressed command environments. For this reason, copy the archive files to the server used to install Interstage Directory Service.

- Windows32/64 When Interstage Directory Service is installed on a Windows® system:

Machine used to install Symfoware Server	Location of compressed files for the command runtime environment
Windows®	C:\Interstage\IREP\bin\RDB\archive\DBCRT_Win.exe
Solaris	C:\Interstage\IREP\bin\RDB\archive\DBCRT_Sol.tar.gz
Linux(RHEL5(x86)/(Intel64))	C:\Interstage\IREP\bin\RDB\archive\DBCRT_RHEL5.tar.gz

- Solaris32/64 Linux32/64 When Interstage Directory Service is installed on a Solaris or Linux system:

Machine used to install Symfoware Server	Location of compressed files for the command runtime environment
Solaris	/opt/FJSVirep/bin/RDB/archive/DBCRT_Sol.tar.gz
Linux(RHEL5(x86)/(Intel64))	/opt/FJSVirep/bin/RDB/archive/DBCRT_RHEL5.tar.gz
Windows®	/opt/FJSVirep/bin/RDB/archive/DBCRT_Win.exe

Copy the command environment according to the following procedure.

Creating tables with administrator authority

a. Forward the following archive files to the server used to install Interstage Directory Service

Machine used to install Symfoware Server	Compressed files for the command runtime environment
Windows®	DBCRT_Win.exe (self-extracting)
Solaris	DBCRT_Sol.tar.gz
Linux(RHEL5(x86)/(Intel64))	DBCRT_RHEL5.tar.gz

b. Expand the archive file to an arbitrary directory.

c. After the archive files are extracted, they must be deleted.

Creating tables as a repository database connection user without administrator authority

a. Copy the archive files.

   Ask the system administrator to extract or copy the platform archive files to any location. If Symfoware Server is installed on a different server, forward the archive files to that server.

b. Extract the copied archive files.

   The system administrator extracts the copied archive files.

c. After the archive files are extracted, change the directory owner.

   After the archive files are extracted, change the directory owner so that the repository database connection user can execute this command.

   Example: Changing the repository database connection user ID to DSADMIN, the repository database connection user group to DSGRP, and the directory name to DBCRT

```
chown -R DSADMIN:DSGRP DBCRT
```

d. Delete the copied archive files

   If the archive files were copied or forwarded, they must be deleted.

Note

If the execution environment for the table creation command is copied to a Windows® machine other than the one where the Interstage Directory Service has already been installed, the Microsoft Visual C++ 2005 Redistributable Package (x86) must be installed before the command can be used. If this package has not been installed yet, download it from the Microsoft website and install it.

1. Creating Tables for Storing Repository Data

   Create tables by executing the "*irepgendb*" table creation command.

   Note

   To execute the table creation command on a Solaris machine, verify that the following Solaris patches have been applied.

   - Solaris 10:

     118367-04

   The method for executing the command is explained below.

   a. Move to the directory where the command is stored.

      Windows32/64

```
C:\Interstage\IREP\bin\RDB
```

      Solaris32/64 Linux32/64

```
/opt/FJSVirep/bin/RDB
```

If Interstage Directory Service and Symfoware Server are installed on separate servers, or tables are created as a repository database connection user without administrator authority, change the command executable environment in step 5 (b) to the extracted directory.

b. Delete the command execution result output directory files

The user account logged in step 2 requires Write authority for the command execution result output directory files. Previously, if the table creation command was executed by a different user account, write authority for the user account logged in step 2 disappeared.

The command execution result is output in the files shown below. If required, change the file name with administrator authority and delete the files.

- Interstage Directory Service and Symfoware Server are installed on the same server, or the system administrator performs the execution

Windows32/64

```
C:\Interstage\IREP\bin\RDB\log\ds_gen.log
```

Solaris32/64 Linux32/64

```
/opt/FJSVirep/bin/RDB/log/ds_gen.log
```

- Interstage Directory Service and Symfoware Server are installed on separate servers, or tables are created by a repository database connection user without system administrator authority

If, when the executable environment was created for the table creation command (refer to step 5), the command environment was extracted in the server used to install Symfoware Server, the execution result is output in the following location:

```
Directory used to extract the command executable environment/log/ds_gen.log
```

Permission to write to the user account from step 2 above is also required for the command execution result file.

If another user account was used to execute the table creation command, there are no permissions to write to the execution result file using the user account from step 2. For this reason, delete the execution result file. However if the file is required change its name using system administrator permissions and then back it up.

a. Execute the *irepgendb* command.

```
irepgendb
```

Refer to the "Interstage Directory Service Operation Commands" chapter in the Reference Manual (Command Edition) for more information about the table creation command.

Windows32/64

If this command is executed using Terminal Services, the message below may be output.

To execute the command from the console of the machine where Symfoware Server is installed or from a remote desktop that is connected to the console session, type y and then press <RETURN> to continue.

To execute the command from a different environment, type n and then press <RETURN> to stop the command from executing, and then log back in to the console on the machine where Symfoware Server is installed or to a remote desktop that is connected to the console session.

```
Care must be taken when executing commands in the terminal service.
To execute this command, log in to the console of the machine on which the command is to be
executed or to a remote desktop that is connected to the console session.
Continue? [y,n]: y or n <RETURN>
```

a. Select the database to be used.

Select the type of database to be used with the repository. Specify 1.

```
Select the database to be used [1:Symfoware,2:Oracle]: 1 <RETURN>
```

b. A message will be displayed prompting for the RDB system name to be input.

Enter RDB System name<RETURN>. Applications must have an RDB system name. This name must be entered.

The following characters can be used in the RDB system name: Alphanumerics, the start character of which must be a letter. Specify the name using up to 8 characters.

```
Enter the RDB system name : dsdbsys <RETURN>
```

c. A message will be displayed prompting for the RDB name to be input.

Enter RDB-name<RETURN>. The following characters can be used in the RDB system name: Alphanumerics, the start character of which must be a letter. Specify the name using up to 8 characters.

```
Enter the database name : DSDB <RETURN>
```

d. A message will be displayed prompting for the RDB schema name to be input.

Enter RDB Schema<RETURN>. Enter the name that was used for the specified OS account when the database was created for the schema name. A maximum of 30 characters in the range 'A' to 'Z', and 0 to 9. can be used in the database schema name: The first character must be a letter.

```
Enter the database schema name : DSADMIN <RETURN>
```

e. Specify whether to make detailed settings for tables.

To make detailed settings for tables, type y, otherwise type n.

Refer to "3.2.4.1 Detailed Settings for Tables" for more information about detailed settings for tables and detailed definition files.

```
Do you want to make the detailed settings for the table ? [y,n]: y or n <RETURN>
```

- If y (make detailed settings for tables) has been specified

Specify a detailed definition file where the size of each resource in the tables is specified.

```
Specify the definition file for the table for storing the repository : file name <RETURN>
```

- If n (do not make detailed settings for tables) has been specified

Specify a value (no more than 10,000,000) for the maximum number of entries that can be registered in the repository.

Check that there is sufficient disk space for storing the specified number of entries. For details about estimating the required size, refer to "3.1.1 Estimating the Resources used by Symfoware/RDB".

```
Enter the maximum number of entries to be registered in the table for storing the repository :
100000<RETURN>
```

a. Table creation information will be displayed.

To create tables using the information displayed, type y and then press <RETURN>. To change these settings, type n and then press <RETURN>. To cancel processing, type q and then press <RETURN>.

```
Information for creating the Interstage Directory Service table for storing the repository
data
  Database used                            :  Symfoware
  RDB system name                          :  DSDBSYS
  Database name                            :  DSDB
  Database schema name                     :  DSADMIN
  Maximum number of entries registered     :  100000
=============================================================
= It will take some time to create the table for storing    =
= the repository data.                                      =
= Do not stop the command forcibly until the table is       =
= created.                                                  =
= If the command is stopped forcibly, the table will not be =
=  complete.                                                =
============================================================
Start table creation ? [y,n,q]:y or n or q <RETURN>
```

The command execution result is output in the files shown in step 6 (b), using the character code applicable when Symfoware Server was installed. If execution fails, look up the Symfoware Server message list and eliminate the cause of the error. After correcting the error, create the database again.

2. Back up the data in the database

   Back up the data in the database in case an error occurs. For details, refer to "Maintenance (Backing up resources)" - "Backing up and restoring resources" in the "Interstage Application Server Application Guide".

If the executable environment for the table creation command is extracted, delete the directory after the database is created.

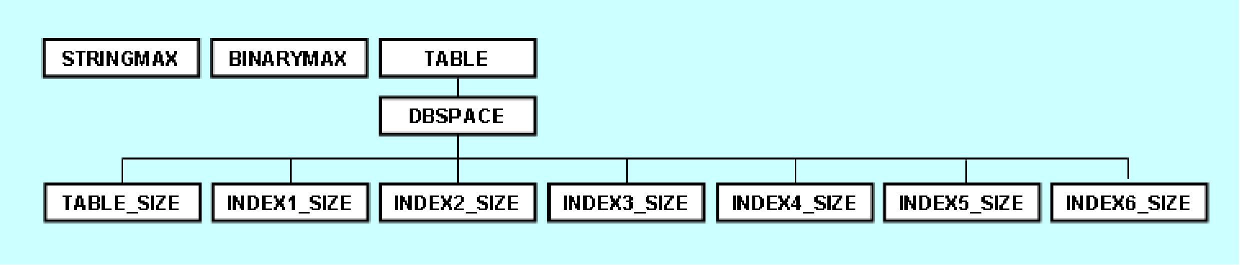
3.1.4.8 Detailed Settings for Tables

Selecting "y" (make detailed definitions for tables) when creating the tables for storing repository data allows you to configure detailed settings, such as the allocation size and allocation space for each table in the database, and extensions such as the maximum length of string and binary type attributes.

Detailed settings for tables can be made only when new tables are created, using the procedures in '3.1.4.7 Creating the Database' if Symfoware/RDB is used, or '3.2.4 Creating the Database' if an Oracle database is used.

Note also that the database's index function cannot be used if detailed table settings are made, which results in reduced operation performance for the repository.

Figure 3.4 Overview of Detailed Definitions



To configure detailed settings for tables, a detailed definition file (as shown below) with the kind of hierarchical structure shown in the figure above must be prepared in advance. Use this file to define things like the allocation size and allocation space for each table in the database, and extensions such as the maximum length of string- and binary-type attributes.

For information about the values to set in the detailed definition file, refer to "Estimating the Database Space" if Symfoware/RDB is being used and "Estimating Table Spaces (TABLESPACE)" if an Oracle database is being used.

Detailed definition file

The detailed definition file is edited using a text editor. Samples of describing new detailed definition files are provided in the Interstage Directory Service. These files are edited using a text editor.

The location of the sample files is as follows:

Windows32/64

```
C:\ Interstage\IREP\bin\RDB\sample\irepdb.conf
```

Solaris32/64 Linux32/64

```
/opt/FJSVirep/bin/RDB/sample/irepdb.conf
```

File Format

This section explains the format for the detailed definition file.

Note

- An error will occur if tag values are not specified.

- Tag names are not case-sensitive.
- The order in which tags appear does not matter as long as the hierarchical position of the tags is correct. An error will occur if tags are entered in the wrong hierarchical position.
- An error will occur if tags other than the tags that need to be entered in the definition file (the tags explained below) are entered.
- There is no need to specify the LOB table contents in the detailed definition file when using an Oracle database.

STRINGMAX

[Description]

Specify the maximum length of strings that can be registered for string-type attributes.

[Number of times that this tag can be specified]

Once. This tag cannot be omitted.

BINARYMAX

[Description]

Specify the maximum length of binary data that can be registered for binary-type attributes.

Do not specify this tag if an Oracle database is used.

[Number of times that this tag can be specified]

Once. This tag cannot be omitted.

TABLE

[Description]

Specify the name of the table.

[Number of times that this tag can be specified]

Cannot be omitted. Specify DS_SCOPE, DS_FILTER and DS_ENTRY once each.

[Subordinate element]

DBSPACE

DBSPACE

[Description]

Specify the name of the space allocated to the table.

If Symfoware/RDB is being used , specify the name of the database space.

If an Oracle database is being used, specify the name of the table space (TABLESPACE).

[Number of times that this tag can be specified]

Cannot be omitted.

- When using Symfoware/RDB

  This can be specified a maximum number of 10 times in one TABLE tag.

- When using an Oracle database

  The number of times this can be specified is the same as the number of times that tags (except for the DBSPACE tag) can be specified in each table.

For details, refer to the table below.

Table 3.1 Number of tags that can be specified in each table

Table Name	Extend STRINGMAX?	
	Yes	No
DS_SCOPE	4	6
DS_FILTER	5	7
DS_ENTRY	3	3

The same table/index cannot be specified for more than one DBSPACE.

[Superior element]

TABLE

[Subordinate element]

TABLE_SIZE, INDEX1_SIZE, INDEX2_SIZE, INDEX3_SIZE, INDEX4_SIZE, INDEX5_SIZE, INDEX6_SIZE

TABLE_SIZE

[Description]

Specify the total size of the table.

[Number of times that this tag can be specified]

Cannot be omitted.

- When using Symfoware/RDB

  This tag can be specified one or more times for each TABLE tag.

  However, only one TABLE_SIZE tag can be specified for each DBSPACE tag.

- When using an Oracle database

  This tag can be specified only once for each TABLE tag.

[Superior element]

DBSPACE

INDEX1_SIZE

[Description]

Specify the size of an index for the table.

[Number of times that this tag can be specified]

- When using Symfoware/RDB

  This tag can be specified one or more times for each TABLE tag.

  However, only one this tag can be specified for each DBSPACE tag.

- When using an Oracle database

  This tag can be specified only once for each TABLE tag.

[Superior element]

DBSPACE

INDEX2_SIZE

This is the same as for INDEX1_SIZE.

INDEX3_SIZE

This is the same as for INDEX1_SIZE.

INDEX4_SIZE

This is the same as for INDEX1_SIZE.

INDEX5_SIZE

This is the same as for INDEX1_SIZE.

INDEX6_SIZE

This is the same as for INDEX1_SIZE.

The following table shows the maximum length of each data type.

Table 3.2 Maximum Length of Each Data Type

Item	Using Symfoware	Using Oracle	Remarks
The maximum length of string types STRINGMAX	942 to 10000 bytes	942 to 4000 bytes	942 bytes if detailed settings for tables are not made.
The maximum length of binary types BINARYMAX	32 K to 16 M	-	32K if detailed settings for tables are not made.
TABLE_SIZE	64 K to 999999 M	64 K to 999999M	If detailed settings for tables are not configured, this value depends on the value specified as the maximum number of entries that can be registered in the table when the table was created.
INDEX1_SIZE INDEX2_SIZE INDEX3_SIZE INDEX4_SIZE INDEX5_SIZE INDEX6_SIZE	64 K to 999999 M	64 K to 999999 M	If detailed settings for tables are not configured, this value depends on the value specified as the maximum number of entries that can be registered in the table that was specified when the table was created.

Except for the STRINGMAX tag, the size of each item can be specified by appending K (kilobytes) or M (megabytes) to the value for each item. 1 kilobyte (KB) is 1,024 bytes and 1 megabyte (MB) is 1024 kilobytes.

The following table shows which tags can be specified for each table.

Table 3.3 Valid Tags for Each Table

Tag Name	Value specified for the TABLE tag		
	DS_SCOPE	DS_FILTER	DS_ENTRY
TABLE_SIZE	R	R	R
INDEX1_SIZE	R	R	R
INDEX2_SIZE	R	R	R
INDEX3_SIZE	C	C	O
INDEX4_SIZE	C	R	O
INDEX5_SIZE	R	C	O
INDEX6_SIZE	O	R	O

R: Required

C: Conditional, cannot be specified if STRINGMAX is extended

O: Optional

The following example shows the definitions in the detailed definition file if Symfoware/RDB is used.

Example definitions for a detailed definition file with the following conditions:

- The maximum length of attribute values is not changed

- Only the DSDBSPACE database space is used
- The number of entries to be registered in a single repository is 10,000
- The average number of attributes per entry (including the "objectClass" attribute) is 30
- The total size of binary-type attributes per entry is 2 kilobytes
- The average size of sting-type attributes registered in the repository is 200 bytes

```
<STRINGMAX> 942 </STRINGMAX>
<BINARYMAX> 32K </BINARYMAX>
<TABLE> DS_SCOPE
    <DBSPACE> DSDBSPACE
        <TABLE_SIZE> 6400K </TABLE_SIZE>
        <INDEX1_SIZE> 800K </INDEX1_SIZE>
        <INDEX2_SIZE> 1200K </INDEX2_SIZE>
        <INDEX3_SIZE> 5600K </INDEX3_SIZE>
        <INDEX4_SIZE> 5600K </INDEX4_SIZE>
        <INDEX5_SIZE> 800K </INDEX5_SIZE>
    </DBSPACE>
</TABLE>
<TABLE> DS_FILTER
    <DBSPACE> DSDBSPACE
        <TABLE_SIZE> 120M </TABLE_SIZE>
        <INDEX1_SIZE> 21M </INDEX1_SIZE>
        <INDEX2_SIZE> 53M </INDEX2_SIZE>
        <INDEX3_SIZE> 170M </INDEX3_SIZE>
        <INDEX4_SIZE> 39M </INDEX4_SIZE>
        <INDEX5_SIZE> 170M </INDEX5_SIZE>
        <INDEX6_SIZE> 39M </INDEX6_SIZE>
    </DBSPACE>
</TABLE>
<TABLE> DS_ENTRY
    <DBSPACE> DSDBSPACE
        <TABLE_SIZE> 147M </TABLE_SIZE>
        <INDEX1_SIZE> 22M </INDEX1_SIZE>
        <INDEX2_SIZE> 36M </INDEX2_SIZE>
    </DBSPACE>
</TABLE>
```

Specify the table allocation size and index allocation sizes for each table as shown in this example.

Example: In the following example, DBSPACE is specified more than once. This example is based on the above example.

- Dividing DBSPACE for each table

```
<TABLE> DS_SCOPE
    <DBSPACE> DSDBSPACE_1
        <TABLE_SIZE> 6400K </TABLE_SIZE>
        <INDEX1_SIZE> 800K </INDEX1_SIZE>
        <INDEX2_SIZE> 1200K </INDEX2_SIZE>
        <INDEX3_SIZE> 5600K </INDEX3_SIZE>
        <INDEX4_SIZE> 5600K </INDEX4_SIZE>
        <INDEX5_SIZE> 800K </INDEX5_SIZE>
    </DBSPACE>
</TABLE>
<TABLE> DS_FILTER
    <DBSPACE> DSDBSPACE_2
        <TABLE_SIZE> 120M </TABLE_SIZE>
        <INDEX1_SIZE> 21M </INDEX1_SIZE>
        <INDEX2_SIZE> 53M </INDEX2_SIZE>
        <INDEX3_SIZE> 170M </INDEX3_SIZE>
        <INDEX4_SIZE> 39M </INDEX4_SIZE>
        <INDEX5_SIZE> 170M </INDEX5_SIZE>
        <INDEX6_SIZE> 39M </INDEX6_SIZE>
    </DBSPACE>
</TABLE>
<TABLE> DS_ENTRY
    <DBSPACE> DSDBSPACE_3
        <TABLE_SIZE> 147M </TABLE_SIZE>
        <INDEX1_SIZE> 22M </INDEX1_SIZE>
        <INDEX2_SIZE> 36M </INDEX2_SIZE>
    </DBSPACE>
</TABLE>
```

- Creating the table and index in a different DBSPACE

```
<TABLE> DS_SCOPE
    <DBSPACE> DSDBSPACE_TBL
        <TABLE_SIZE>  6400K </TABLE_SIZE>
    </DBSPACE>
    <DBSPACE> DSDBSPACE_IDX
        <INDEX1_SIZE>  800K </INDEX1_SIZE>
        <INDEX2_SIZE> 1200K </INDEX2_SIZE>
        <INDEX3_SIZE> 5600K </INDEX3_SIZE>
        <INDEX4_SIZE> 5600K </INDEX4_SIZE>
        <INDEX5_SIZE>  800K </INDEX5_SIZE>
    </DBSPACE>
</TABLE>
```

- Creating the table and index in DBSPACE that are all different

```
<TABLE> DS_FILTER
    <DBSPACE> DSDBSPACE_TBL
        <TABLE_SIZE>  120M </TABLE_SIZE>
    </DBSPACE>
    <DBSPACE> DSDBSPACE_IDX1
        <INDEX1_SIZE>  21M </INDEX1_SIZE>
    </DBSPACE>
    <DBSPACE> DSDBSPACE_IDX2
        <INDEX2_SIZE> 53M </INDEX2_SIZE>
    </DBSPACE>
    <DBSPACE> DSDBSPACE_IDX3
        <INDEX3_SIZE> 170M </INDEX3_SIZE>
    </DBSPACE>
    <DBSPACE> DSDBSPACE_IDX4
        <INDEX4_SIZE> 39M </INDEX4_SIZE>
    </DBSPACE>
    <DBSPACE> DSDBSPACE_IDX5
        <INDEX5_SIZE>  170M </INDEX5_SIZE>
    </DBSPACE>
    <DBSPACE> DSDBSPACE_IDX6
        <INDEX6_SIZE> 39M </INDEX6_SIZE>
    </DBSPACE>
</TABLE>
```

- Creating the table in more than one DBSPACE (this can only be specified if the database is Symfoware/RDB)

```
<TABLE> DS_ENTRY
    <DBSPACE> DSDBSPACE_TBL1
        <TABLE_SIZE>  100M </TABLE_SIZE>
    </DBSPACE>
    <DBSPACE> DSDBSPACE_TBL2
        <TABLE_SIZE>  47M </TABLE_SIZE>
    </DBSPACE>
    <DBSPACE> DSDBSPACE_IDX
        <INDEX1_SIZE>  22M </INDEX1_SIZE>
        <INDEX2_SIZE>  36M </INDEX2_SIZE>
    </DBSPACE>
</TABLE>
```

3.1.4.9 Deleting the Database

If an error occurs during the creation of the tables, or if the database space needs to be changed, delete the database using the Symfoware/RDB function. The deletion method is explained below. Refer to the Symfoware Server RDB Operator's Guide (Database Definition) for more information about deleting the database.

- Delete all resources under the schema

  Execute the following SQL using a command or WebDBtools:

  ```
  DROP SCHEMA DSADMIN CASCADE
  ```

  The underlined part is the schema name that was specified when the database was created.

- Delete the database space

  Execute the following SQL using a command or WebDBtools:

  ```
  DROP DBSPACE DSDBSPACE
  ```

  The underlined part is the database space name that was specified when the database was created.

- Delete the database name

  Execute the following SQL using a command or WebDBtools:

  ```
  DROP DATABASE DSDB
  ```

  The underlined part is the database name that was specified when the database was created.

3.2 Using the Oracle Database

If an Oracle database is used for the repository database, create an environment for the Oracle database before creating the repository.

Additionally, if the Oracle database is installed on a different machine from the Interstage Directory Service, Oracle client software (including Oracle Net software) must be installed on the machine where the Interstage Directory Service is installed. Ensure that the Oracle client software is installed before creating the tables for storing repository data. Refer to the Oracle database manual for information on how to install Oracle client software.

Note

The Oracle client software's "Instant Client" function cannot be used with the Interstage Directory Service.

3.2.1 Estimating the Resources Used by the Oracle Database

Estimate the following resources used by the Oracle database.

- Table spaces
- Data files
- Control files
- Temporary log files
- REDO log files
- Password files and other important files such as PFILE
- Listener control files

As an estimate for the disk space used in the Oracle database, approximately 10GB of table space is required to register 100,000 entries in the repository, and approximately 100GB of table space is required to register 1,000,000 entries in the repository.

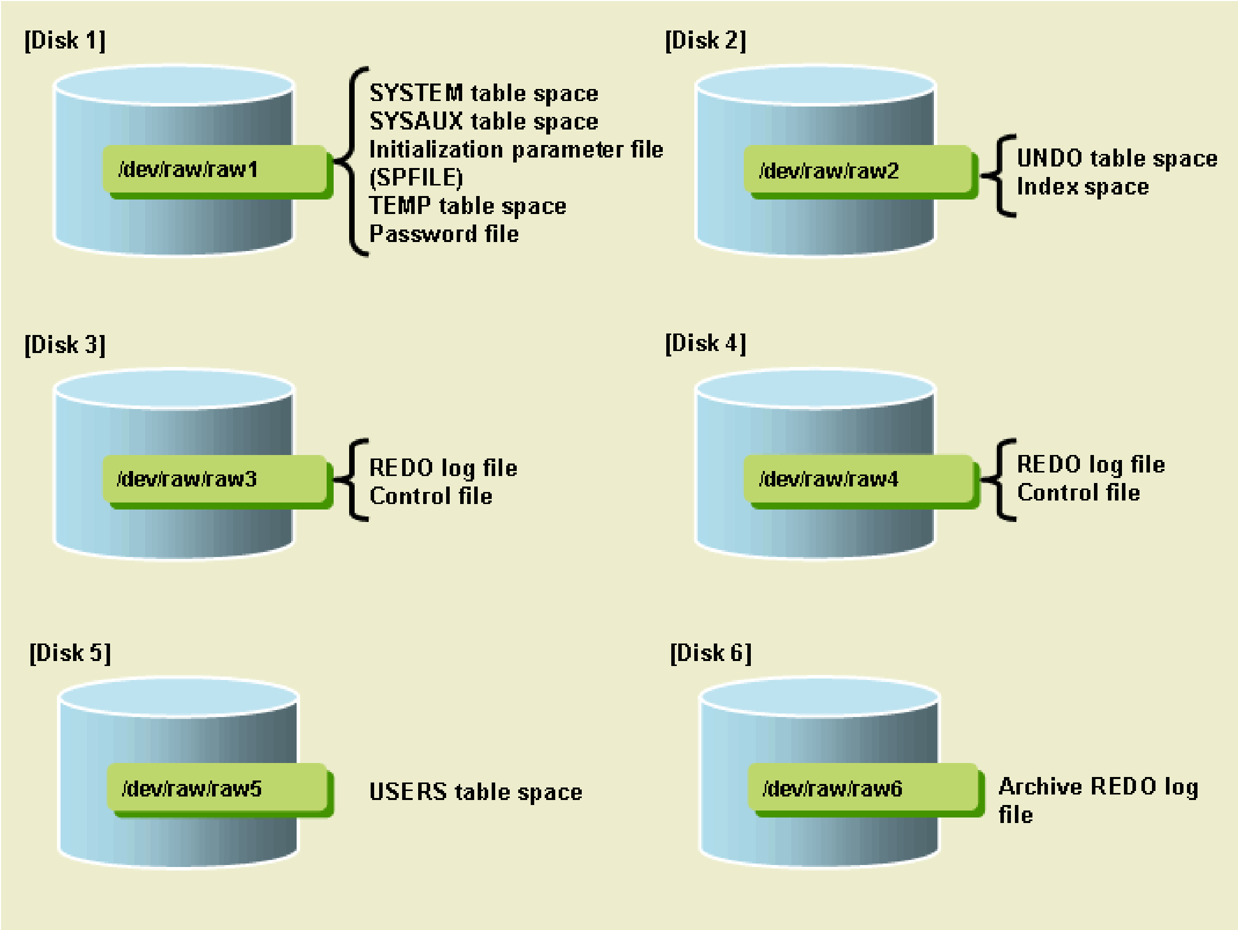
Refer to the the "Estimating Resources for Oracle Databases" chapter for information on how to estimate table spaces. Refer to the Oracle database manual for information on how to estimate other resources.

3.2.2 Creating a Raw Device

Reserve the raw device required for Oracle database operations. It is recommended that the database resources used by Interstage Directory Service be placed on the file system.

The following example shows the creation of the raw devices using Oracle 10g.

Figure 3.5 Creation of Raw Devices



Refer to the Oracle database manual for more information on how to create raw devices.

3.2.3 Tuning the Kernel Resources

Solaris32/64 Linux32/64

To run the Oracle database, kernel resources for the Oracle database operating environment definition must be reserved.

The kernel resources that must be set up to run the Oracle database are as follows:

- Shared memory resources
- Semaphore resources
- File system resources (Linux only)
- Network resources (Linux only)

For details about the kernel resources required to run Interstage Directory Service using an Oracle database as the repository database, refer to "System Resources of Interstage Directory Service" in the "System Tuning" chapter of the Tuning Guide.

For details about the Oracle database kernel resources, refer to the Oracle database manual.

3.2.4 Creating the Database

The procedure for creating the database is shown below. Create the database either using SQL statements or using the DBCA (Database Configuration Assistant) GUI tool.

Notes

- Creating more than one repository

  Repeat the following procedure for each repository.

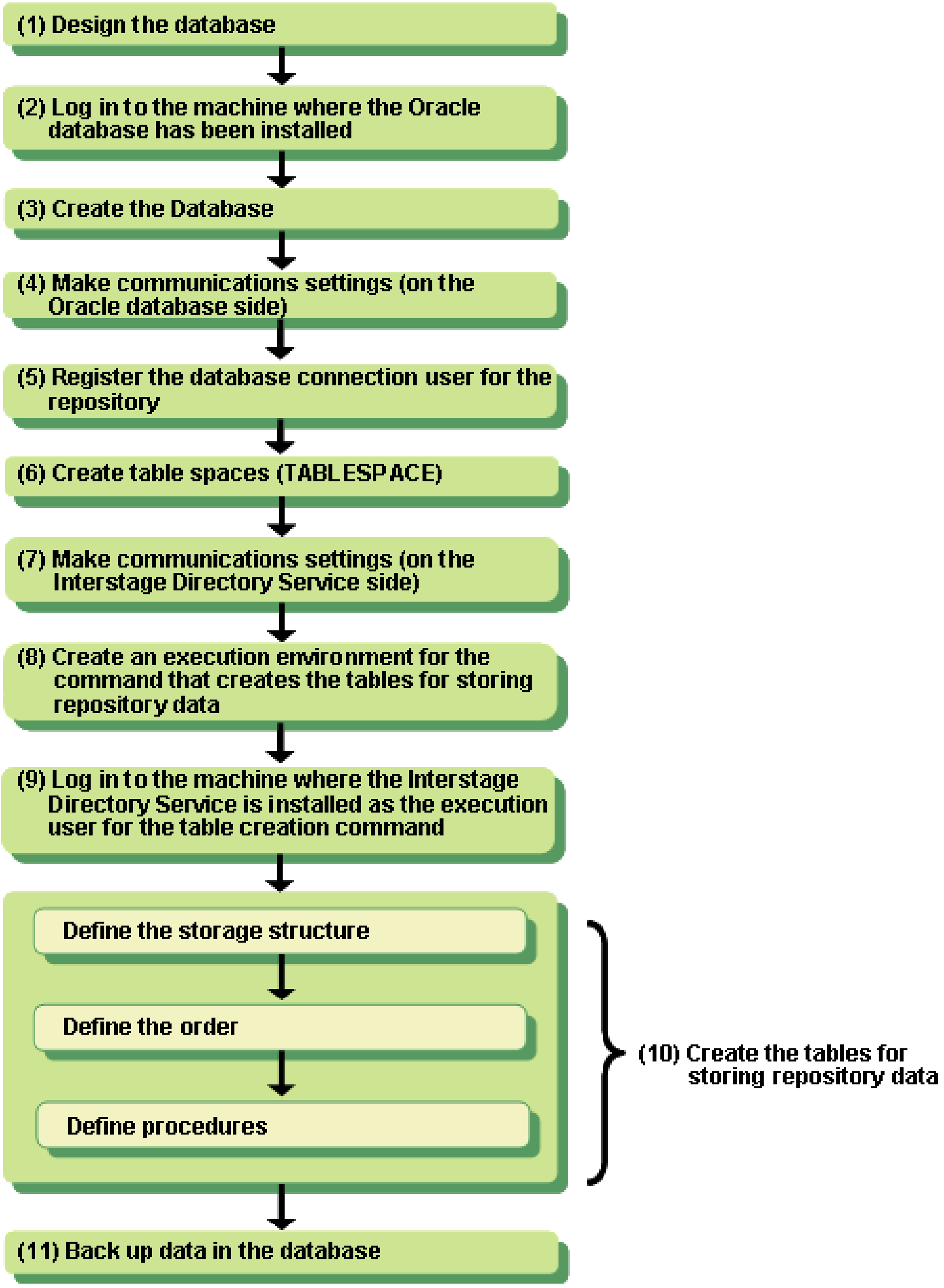
- Creating an environment for database sharing configurations

  Perform the following procedure only once. Refer to "Database Sharing" in the "Creating a Load Distribution Environment" chapter for more information.

- Do not use the initial database

  An initial database can be created when the Oracle database is installed, but there are restrictions on some functions of the initial database. Fujitsu recommends using a newly created database for repository databases, without using the initial database. Refer to the Oracle database manual for information about the restrictions on the initial database.

Figure 3.6 Procedure for Creating the Database


(1) Design the database
(2) Log in to the machine where the Oracle database has been installed
(3) Create the Database
(4) Make communications settings (on the Oracle database side)
(5) Register the database connection user for the repository
(6) Create table spaces (TABLESPACE)
(7) Make communications settings (on the Interstage Directory Service side)
(8) Create an execution environment for the command that creates the tables for storing repository data
(9) Log in to the machine where the Interstage Directory Service is installed as the execution user for the table creation command
Define the storage structure
Define the order
Define procedures
(10) Create the tables for storing repository data
(11) Back up data in the database

1. **Design the database**

   Database design involves designing tables, attributes, and a storage structure. The tables, attributes, and storage structure have been designed to be appropriate for repositories, and are defined and set up using the repository data storage table creation command described later in this procedure.

   If table or attribute design meets the following conditions, detailed settings for tables must be made. Create a detailed definition file in advance, by referring to "3.2.4.1 Detailed Settings for Tables". Specify this detailed definition file when creating tables.

   - Multiple table spaces (TABLESPACE) are used

- The maximum length of attribute values is changed

  The initial value for the maximum length is 942 bytes for string-type attributes and 32 kilobytes for binary-type attributes)

- There are more than 20 attributes (including the "objectClass" attribute) per entry on average

- The total size of the binary attributes per entry is greater than 2 kilobytes

- The average size of string-type attributes registered in the repository is longer than 200 bytes

Example: The total size of the binary attributes per entry is greater than 2 kilobytes

Windows32/64

```
# First entry
dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
cn: User001
sn: Fujitsu
jpegPhoto:< file:///C:\data\photo1.jpg                  <- 2.5 KB binary file
jpegPhoto:< file:///C:\data\photo2.jpg                  <- 2.0 KB binary file

# Second entry
dn: cn=User002,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: User002
sn: Fujitsu CREATE DATABASE SRDB
```

Solaris32/64 Linux32/64

```
# First entry
dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
cn: User001
sn: Fujitsu
jpegPhoto:< file:///data/photo1.jpg                  <- 2.5 KB binary file
jpegPhoto:< file:///data/photo2.jpg                  <- 2.0 KB binary file

# Second entry
dn: cn=User002,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: User002
sn: Fujitsu CREATE DATABASE SRDB
```

a. Total size of the binary-type attribute for the first entry = 2.5K + 2.0K

= 4.5 KB

a. Total size of the binary-type attribute for the second entry = 0 bytes

b. Number of entries = 2

c. ((a) + (b)) / (c) = 2.25 KB

In this example, detailed settings for tables must be made because the total size of binary attributes per entry is more than 2 kilobytes.

Example: The average size of string-type attributes registered in the repository is longer than 200 bytes

Windows32/64

```
# First entry
dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
# First entry
dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com   <- 49 bytes
objectclass: top                                        <- 3 bytes
objectclass: person                                     <- 6 bytes
objectclass: organizationalPerson                       <- 20 bytes
cn: User001                                             <- 7 bytes
sn: Fujitsu                                             <- 7 bytes
description:< file:///C:\data\sentence1.txt             <- 1,500 bytes of text
# Second entry
dn: cn=User002,ou=User,ou=interstage,o=fujitsu,dc=com   <- 49 bytes
objectclass: top                                        <- 3 bytes
objectclass: person                                     <- 6 bytes
objectclass: organizationalPerson                       <- 20 bytes
cn: User002                                             <- 7 bytes
sn: Fujitsu                                             <- 7 bytes
description:< file:///C:\data\sentence2.txt             <- 1,200 bytes of text
```

Solaris32/64 Linux32/64

```
# First entry
dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
# First entry
dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com   <- 49 bytes
objectclass: top                                        <- 3 bytes
objectclass: person                                     <- 6 bytes
objectclass: organizationalPerson                       <- 20 bytes
cn: User001                                             <- 7 bytes
sn: Fujitsu                                             <- 7 bytes
description:< file:///data/sentence1.txt                <- 1,500 bytes of text
# Second entry
dn: cn=User002,ou=User,ou=interstage,o=fujitsu,dc=com   <- 49 bytes
objectclass: top                                        <- 3 bytes
objectclass: person                                     <- 6 bytes
objectclass: organizationalPerson                       <- 20 bytes
cn: User002                                             <- 7 bytes
sn: Fujitsu                                             <- 7 bytes
description:< file:///data/sentence2.txt                <- 1,200 bytes of text
```

a. Total size of the string-type attributes for the first entry = 49 + 3 + 6 + 20 + 7 + 7 + 1,500

= 1,592 bytes

a. Total size of the string-type attributes for the second entry = 49 + 3 + 6 + 20 + 7 + 7 + 1,200

= 1,292 bytes

a. Total number of string-type attributes for the first entry = 7

b. Total number of string-type attributes for the second entry = 7

c. ((a) + (b)) / ((c) + (d)) = 206 bytes

In this example, detailed settings for tables must be made because the average size of the string-type attributes registered in the repository is longer than 200 bytes.

The design for the storage structure must include an estimate for the amount of required table space. The amount of table space required depends on the amount of data to be stored in the repository, so make this estimate by referring to 'Estimating Table Spaces (TABLESPACE)'.

2. Log in to the machine where the Oracle database has been installed

   Log on as an Oracle software owner (Oracle user).

   Windows32/64

   Log in either from the console on the machine where the Oracle database is installed or from a remote desktop connected to a console session.

3. Configure communications (on the Oracle database side)

   Listener information must be set up on the machine where the Oracle database has been installed in order to allow the Interstage Directory Service to connect to the Oracle database.

   Use either the Oracle Net Configuration Assistant or the Oracle Net Manager to configure listener information settings.

   Refer to the Oracle database manual for more information on how to configure these settings.

   When Listener information has been set, start the Listener.

4. Create the database

   There are two ways of creating the database: either using SQL statements or using the DBCA (Database Configuration Assistant).

   To create the database using the DBCA, set up the following items:

   - The template for creating the database (*)
   - The name of the global database (*)
   - SID (*)
   - The database management method (*)
   - The password for the user account for the database (*)
   - The memory area mechanism (file system or raw device) used by the database (*)
   - The location where the database file is to be created

     Select "Use a common location for all database files"

     However, the database can be created in any location (*)

   - The recovery option for the database (*) (**)
   - Whether to install sample schemas and script (*)
   - Initialization parameters (*)

     Before setting "PROCESSES" or "SESSIONS" and "TRANSACTIONS", consider the number of connections required to use the Interstage Directory Service that is calculated according to the formula shown below:

     (Maximum number of connections from the repository to the RDB + 1) * Number of repositories

   - The storage locations for the control files, data files and REDO log files that make up the database (*)

   (*) These setting values are not determined by Interstage Directory Service operations.

   Set appropriate values according to the environment being used.

   (**) Oracle9i does not have this configuration item.

   Refer to the manuals for the Oracle database for information on how to use DBCA, detailed information about these settings, and information on how to create databases using SQL statements.

   The maximum number of connections from the repository to the RDB is set when the repository is created. For details, refer to "Using the Oracle Database" in the "Creating a Repository" chapter.

5. Register the database connection user for the repository

   The user that the Interstage Directory Service uses to access the Oracle database is called the repository database connection user.

There are two ways of registering the repository database connection user with the repository database: either using SQL statements or using the Oracle Enterprise Manager. Characters that can be used in the database connection user name (schema name) for the repository: A maximum of 30 characters in the range 'A' to 'Z', and 0 to 9, and underscores (_).The first character must be a letter.

Execute the following kind of SQL statements using either a command or a tool such as SQL *Plus.

Note also that the following two roles must be set up for the repository database connection user to be registered.

- "CONNECT"
- "RESOURCE"

Example: If the user name is "DSADMIN" and the password is "DSPASSWD" (for Oracle 10g)

```
CREATE USER DSADMIN PROFILE DEFAULT IDENTIFIED BY DSPASSWD ACCOUNT UNLOCK;
GRANT CONNECT,RESOURCE TO DSADMIN;
```

Reflect to the Oracle manuals for more information about how to register users.

6. Create table spaces (TABLESPACE)

   Create the table space (TABLESPACE) for storing repository data.

   Table spaces can be created either using SQL statements or using the Oracle Enterprise Manager, as is the case with registering repository database connection users.

   If detailed settings are not made when the tables for storing repository data are created, specify "DSDBSPACE" for the name of the table space when the table space is created.

   Execute the following kind of SQL statements using either a command or a tool such as SQL *Plus.

   Windows32/64

   Example: Defining the table space "DSDBSPACE" on the location "C:\ORADB" (in the case of Oracle 10g)

   ```
   CREATE SMALLFILE TABLESPACE DSDBSPACE DATAFILE 'C:\ORADB\DSDBSPACE' SIZE
   100M LOGGING EXTENT MANAGEMENT LOCAL SEGMENT SPACE MANAGEMENT AUTO;
   ```

   Solaris32/64 Linux32/64

   Example: Defining the table space "DSDBSPACE" on the location "/home/oracle/ORADB" (in the case of Oracle 10g)

   ```
   CREATE SMALLFILE TABLESPACE DSDBSPACE DATAFILE '/home/oracle/ORADB/DSDBSPACE' SIZE 100M LOGGING
   EXTENT MANAGEMENT LOCAL
   SEGMENT SPACE MANAGEMENT AUTO;
   ```

   Make a note of the name of the table space ("DSDBSPACE"), and keep the note so that the table space can be backed up and restored in case an error occurs.

   Refer to the Oracle database manual for more information about how to create table spaces.

7. Configure communications (on the Interstage Directory Service side)

   The Net Service must be set up on the machine where the Interstage Directory Service is installed so that the Interstage Directory Service can connect to the Oracle database.

   Use either the Oracle Net Configuration Assistant or the Oracle Net Manager to make Net Service settings. Characters that can be used in the Naming Service are alphanumeric, dollar signs ($), hash marks (#), and underscores (_). Specify a maximum of 128 characters.

   Refer to the Oracle database manual for more information on how to configure these settings.

   Notes

   - If the Interstage Directory Service and the Oracle database are installed on different machines, Oracle client software (including Oracle Net software) must be installed in advance. The "Instant Client" function cannot be used with the Interstage Directory Service.
   - The Interstage Directory Service cannot connect to the Oracle database correctly if the storage location of the TNS file (tnsnames.ora) is specified in an environment variable such as TNS_ADMIN and this location is a directory other than the Oracle home directory. Ensure that you set up the TNS file so that it is stored in the Oracle home directory.

- Windows32/64 If using Interstage Directory Service with Windows Server(R) x64 Editions, install a 32-bit(x86) Oracle Database Client on the machine where Interstage Directory Service is to be installed.

- Windows32/64 If using Interstage Directory Service with Windows Server(R) x64 Editions, store the TNS file in the Oracle home directory of the 32-bit(x86) Oracle Database Client.

8. Create an execution environment for the command that creates the tables for storing repository data

   An execution environment for the table creation command must be created if the table creation command is executed by an Oracle software owner (oracle user). This step is not required if the table creation command is executed by the system administrator, in which case skip to step 10.

   The following directory is located on the machine where the Interstage Directory Service has been installed and contains an archive file that with a compressed version of the environment for the table creation command. Copy and extract this file to an arbitrary location.

Machine used to install Interstage Directory Service	Location of compressed files for the command runtime environment
Windows®	C:\Interstage\IREP\bin\RDB\archive\DBCRT_Win.exe
Solaris	/opt/FJSVirep/bin/RDB/archive/DBCRT_Sol.tar.gz
Linux(RHEL5(x86)/(Intel64))	/opt/FJSVirep/bin/RDB/archive/DBCRT_RHEL5.tar.gz

   Copy the command environment according to the following procedure.

   a. Copy the archive file.

      Ask the system administrator to extract or copy the archive file for the platform being used to an arbitrary location.

   b. Extract the copied archive file.

      Extract the archive file that has been copied by the system administrator.

   c. Solaris32/64 Linux32/64 Change the owner for the directory that has been extracted.

      Change the owner for the directory that has been extracted to ensure that the appropriate user will be able to execute the table creation command.

      Example: When the ID for the user account that executes the table creation command is "oracle", the user account group is "oinstall", and the directory name is "DBCRT"

```
chown -R oracle:oinstall DBCRT
```

   d. Delete the copy of the archive file.

      If the archive file has been copied, be sure to delete the copy.

9. Log in to the machine where the Interstage Directory Service is installed as the execution user for the table creation command

   If the table creation command is executed by an Oracle software user (oracle user), the Oracle software user (oracle user) should log in to the machine where the Interstage Directory Service is installed.

   Windows32/64

   Log in either from the console on the machine or from a remote desktop connected to a console session.

10. Create the tables for storing repository data

    Create tables by executing the *irepgendb* table creation command.

    Note

    To execute the table creation command on a Solaris machine, verify that the following Solaris patches have been applied.

    - Solaris 10:

      118367-04

    Solaris32/64 Linux32/64

To execute the table creation command, the "ORACLE_HOME" environment variable must be set. Specify in the "ORACLE_HOME" environment variable the Oracle home directory that was set up when the Oracle database was installed.

The following section explains how to execute the command.

a. Move to the directory where the command is stored.

   Windows32/64

   ```
   C:\Interstage\IREP\bin\RDB
   ```

   Solaris32/64 Linux32/64

   ```
   /opt/FJSVirep/bin/RDB
   ```

   To create the tables using a repository database connection user other than the system administrator, move to the directory from where the command execution environment was extracted in step 8 b) (i.e., where the command execution environment was copied).

b. Delete the execution result output file for the command

   The user account that was used to log on in either step 2 or step 9 must have write authority to the execution result output file for the command. If the table creation command has been previously executed using another user account, the user account that logged on in step 2 or step 9 will have lost write permission to the execution result output file.

   The execution results for the command are output to the following file. If necessary, delete this file by using administrator privileges to rename it.

   - If tables were created by the system administrator

     Windows32/64

     ```
     C:\Interstage\IREP\bin\RDB\log\ds_gen.log
     ```

     Solaris32/64 Linux32/64

     ```
     /opt/FJSVirep/bin/RDB/log/ds_gen.log
     ```

   - If tables were created by a repository database connection user other than the system administrator

     Windows32/64

     ```
     Directory used to extract the command executable environment\log\ds_gen.log
     ```

     Solaris32/64 Linux32/64

     ```
     Directory used to extract the command executable environment/log/ds_gen.log
     ```

     Permissions to write to the user account from steps 2 and 9. above are also required for the command execution result file. If another user account was used to execute the table creation command, there are no permissions to write to the execution result file using the user account from steps 2 and 9. For this reason, delete the execution result file. However if the file is required change its name and then back it up.

c. Execute the *irepgendb* command.

   ```
   irepgendb
   ```

   Refer to the "Interstage Directory Service Operation Commands" chapter of the Reference Manual (Command Edition*)* for more information about the table creation command.

d. Windows32/64 If this command is executed using Terminal Services, the message below may be output.

   On the console of the machine where Symfoware Server is installed or from a remote desktop that is connected to the console session, type y and then press <RETURN> to continue.

   To execute the command from a different environment, type n and then press <RETURN> to stop the command from executing, and then log back in to the console on the machine where Symfoware Server is installed or to a remote desktop that is connected to the console session.

```
Care must be taken when executing commands in the terminal service.
To execute this command, log in to the console of the machine on which
the command is to be executed or to a remote desktop that is connected to
the console session.
Continue? [y,n]: y or n <RETURN>
```

e. Select the database to be used.

   Select the type of database to be used with the repository. Specify 2.

```
Select the database to be used [1:Symfoware,2:Oracle]: 2 <RETURN>
```

f. A message will display prompting for the net service name of the database to be entered.

   Enter the net service name for connecting to the Oracle database remotely, and then enter the net service name and press <RETURN>. Be sure to enter this information.

   The following characters can be used with net service names: alphanumeric characters, dollar signs ($), hash signs (#) and underscores (_).Specify the name using up to 128 characters.

```
Enter the Net service name : DSDB <RETURN>
```

g. A message will display prompting for the name of the schema used for connecting to the database.

   Enter the name of the repository database connection user (schema) that has been registered with the Oracle database, and press <RETURN>.

   Characters that can be used in the schema name: A maximum of 30 characters in the range 'A' to 'Z', and 0 to 9, and underscores (_).The first character must be a letter.

```
Enter the database schema name : DSADMIN <RETURN>
```

h. A message will prompt for the password to the schema used for connecting to the database.

   Enter the password for the repository database connection user (schema) that has been registered with the Oracle database, and press <RETURN>.

   The password that is entered will not be echoed back on the screen. Specify the password using up to 30 characters.

```
Enter the schema password : <RETURN>
```

i. Specify whether to configure detailed settings for tables.

   To make detailed settings for tables, specify y, otherwise specify n.

   Refer to "3.2.4.1 Detailed Settings for Tables" for more information about detailed settings and definition files.

```
Do you want to make the detailed settings for the table ? [y,n]: y or n <RETURN>
```

   - If y (make detailed settings for tables) has been specified

     Specify a detailed definition file where the size of each resource in the tables is specified.

```
Specify the definition file for the table for storing the repository : file name <RETURN>
```

   - If n (do not make detailed settings for tables) has been specified

     Specify a value (of no more than 10,000,000) for the maximum number of entries that can be registered in the repository.

     Ensure that enough disk space has been reserved to store the specified number of entries. Refer to "Estimating Resources for Oracle Databases" chapter for information about how to estimate the amount of space required.

```
Enter the maximum number of entries to be registered in the table for storing the
repository : 100000<RETURN>
```

j. Table creation information will be displayed.

   To create tables using the information displayed, type y and press <RETURN>. To change these settings, type n and press <RETURN>. To cancel processing, type q and press <RETURN>.

```
Information for creating the Interstage Directory Service table for storing the repository
data
  Database used                          :  Oracle
  Net service name                       :  DSDB
  Database schema name                   :  DSADMIN
  Maximum number of entries registered   :  100000
=============================================================
= It will take some time to create the table for storing    =
= the repository data.                                      =
= Do not stop the command forcibly until the table is       =
= created.                                                  =
= If the command is stopped forcibly, the table will not be =
=  complete.                                                =
============================================================
Start table creation ? [y,n,q]:y or n or q <RETURN>
```

The execution results for the command will be output to the file shown in step 10 b), in English. If execution fails, refer to the Oracle database manual, resolve the error, and create the database again.

11. Back up data in the database

    Back up the data in the database in case an error occurs. Refer to "Backing Up and Restoring Resources" in the "Maintenance (Resource Backup)" chapter of the Operator's Guide for more information.

If the execution environment for the table creation command has been extracted, delete the extracted directory after the database has been created.

3.2.4.1 Detailed Settings for Tables

The method for configuring detailed settings for the tables where repository data is stored is the same as for when Symfoware/RDB is used for the database. Refer to "3.1.4.8 Detailed Settings for Tables".

3.2.4.2 Deleting Databases

If an error occurs while the database is being created, or if the table space (TABLESPACE) is to be changed, delete the database using the Oracle database functions. The deletion method is explained below. Refer to the Oracle database manual for more information about how to delete the database.

- Delete all resources under the schema

  Use the Oracle Enterprise Manager to delete the schema with the "cascade" option. Alternatively, delete the schema by executing the following SQL statement with SQL *Plus:

```
DROP USER DSADMIN CASCADE;
```

  The underlined section is the name of the schema that was specified when the database was created.

- Delete the table space (TABLESPACE)

  Use Oracle Enterprise Manager to delete the table space. Alternatively, delete the table space by executing the following SQL statement with SQL *Plus:

```
DROP TABLESPACE DSDBSPACE INCLUDING CONTENTS AND DATAFILES;
```

  The underlined section is the name of the table space that was specified when the database was created.

- Delete the database

  Use the Database Configuration Assistant to delete the database.

Chapter 4 Setting up an Environment for SSL Communication

An SSL communication environment needs to be set up to enable encrypted communication between the client and server.

Note

Install the Application Server as the management target server for construction of the SSL communication environment in the Admin Server. For details of the Admin Server and Managed Server, refer to "Site" in the Operator's Guide. For details about installing the Application Server, refer to "Installation Information".

Setup of an SSL Communication Environment (Between Client and Server)

Interstage Directory Service is intended to allow SSL communication for the following clients:

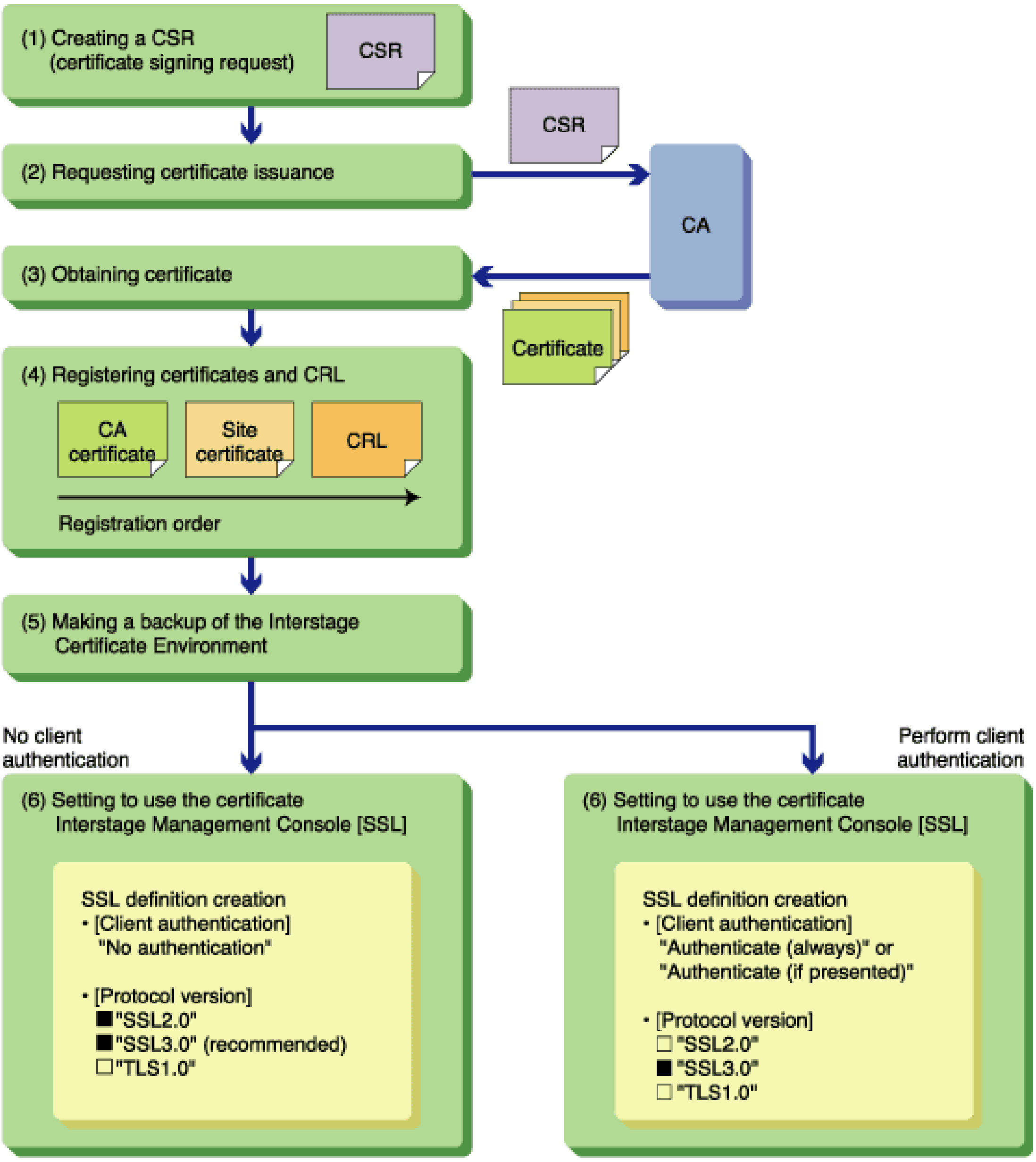
- Interstage Directory Service LDAP command (ldapsearch, ldapmodify, and ldapdelete commands)
- User applications that access the Interstage Directory Service

Set up an SSL communication environment according to the following procedure:

- Server
    1. Setup of an Interstage certificate environment ((1) to (5) in the following figure)
    2. Implementation settings to use the certificate ((6) in the following figure)

The following flow diagram illustrates how to set up an SSL communication environment for the server.

Figure 4.1 Server Communication Environment Setup

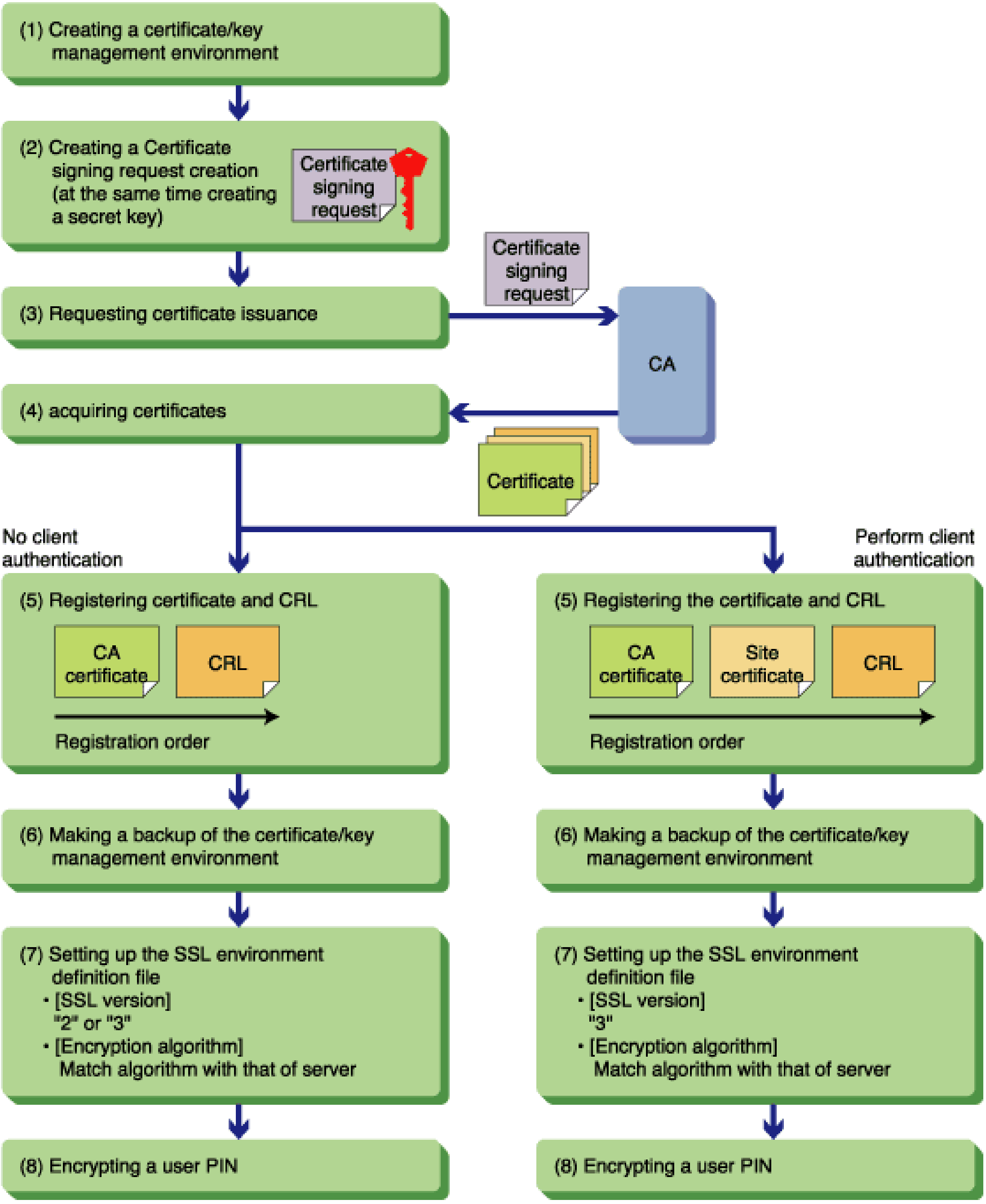

(1) Creating a CSR
(certificate signing request)
CSR
CSR
(2) Requesting certificate issuance
CA
(3) Obtaining certificate
Certificate
(4) Registering certificates and CRL
CA certificate
Site certificate
CRL
Registration order
(5) Making a backup of the Interstage Certificate Environment
No client authentication
Perform client authentication
(6) Setting to use the certificate
Interstage Management Console [SSL]
SSL definition creation
• [Client authentication]
"No authentication"
• [Protocol version]
■"SSL2.0"
■"SSL3.0" (recommended)
□"TLS1.0"
(6) Setting to use the certificate
Interstage Management Console [SSL]
SSL definition creation
• [Client authentication]
"Authenticate (always)" or
"Authenticate (if presented)"
• [Protocol version]
□"SSL2.0"
■"SSL3.0"
□"TLS1.0"

- Client

    1. Creation of a certificate/key management environment ((1) in the following figure)
    2. Creation of a private key and acquisition of a certificate ((2) to (4) in the following figure)
    3. Registration of the certificate and CRL ((5) to (6) in the following figure)
    4. Setting of the SSL environment definition file ((7) in the following figure)
    5. Encryption of the user PIN ((8) in the following figure)

The following figure illustrates the set up of an SSL communication environment for the client.

Figure 4.2 Client Communication Environment Setup


(1) Creating a certificate/key management environment
(2) Creating a Certificate signing request creation (at the same time creating a secret key)
Certificate signing request
Certificate signing request
(3) Requesting certificate issuance
CA
(4) acquiring certificates
Certificate
No client authentication
Perform client authentication
(5) Registering certificate and CRL
CA certificate
CRL
Registration order
(5) Registering the certificate and CRL
CA certificate
Site certificate
CRL
Registration order
(6) Making a backup of the certificate/key management environment
(6) Making a backup of the certificate/key management environment
(7) Setting up the SSL environment definition file
・[SSL version] "2" or "3"
・[Encryption algorithm] Match algorithm with that of server
(7) Setting up the SSL environment definition file
・[SSL version] "3"
・[Encryption algorithm] Match algorithm with that of server
(8) Encrypting a user PIN
(8) Encrypting a user PIN

The following explains the case where the CA of certificates used by the client and server are the same. For an explanation of the case in which the client and server use different CA certificates, and for further details on encrypted communication using SSL, see the "Security System Guide."

4.1 Creating the Environment on the Server

This section explains how to create the Interstage Directory Service environment on the server.

4.1.1 Setting up an Interstage Certificate Environment (Server)

Set up an Interstage certificate environment on a server of Interstage Directory Service.

The following explains how to set up an Interstage certificate environment using CSR (certificate signing request).

Setting up an Interstage certificate environment entails the following steps:

1. Setup of an Interstage certificate environment and creation of CSR (certificate signing request)
2. Request to issue a certificate
3. Registration of the certificate and CRL (certificate revocation list)

After setting up an Interstage certificate environment, configure the environment to use the certificate. For more details, see 4.1.1.1 Setting to Use the Certificates (Server).

For details of each command to be used in the following procedure, see the Reference Manual (Command Edition).

Note

Windows32/64

Execute the commands as a user with the Administrator authority.

Solaris32/64 Linux32/64

Execute the commands as a superuser.

Set the installation path of JDK or JRE to the environment variable JAVA_HOME for command execution.

Setup of an Interstage Certificate Environment and Creation of CSR (Certificate Signing Request)

To perform signing and encryption such as SSL, a certificate is necessary. For this purpose, create a CSR (certificate signing request), which is data used to request a certificate from CA (VeriSign Inc., Cybertrust, Inc. or another Certification Authority).

If no Interstage certificate environment exists at this point, an Interstage certificate environment is created at the same time. If an Interstage certificate environment exists, that environment is used.

Note

No test certificate can be used in the following cases. Create a CSR instead of a test certificate.

- Interstage Directory Service in standalone mode or in database sharing mode.
- Slave server in replication mode. (when the standard database is used)
- Master server when performing client authentication in replication mode (when the Standard Database is used)

An example of creating a CSR is shown below:

Windows32/64

Nickname of the site certificate: SiteCert

Request output destination file name: C:\sslenv\my_csr.txt

Name: repository.fujitsu.com

Organization unit name: Interstage

Organization name: Fujitsu Ltd.

City name: Yokohama

Prefectural name: Kanagawa

Country code: jp

```
scsmakeenv -n SiteCert -f C:\sslenv\my_csr.txt -c
New Password:   (*1)
Retype:   (*1)

Input X.500 distinguished names.
What is your first and last name?
[Unknown]:repository.fujitsu.com   (*2)
What is the name of your organizational unit?
[Unknown]:Interstage   (*2)
```

```
What is the name of your organization?
[Unknown]:Fujitsu Ltd.   (*2)
What is the name of your City or Locality?
[Unknown]:Yokohama   (*2)
What is the name of your State or Province?
[Unknown]:Kanagawa   (*2)
What is the two-letter country code for this unit?
[Un]:jp   (*2)
Is <CN=repository.fujitsu.com, OU=Interstage, O=Fujitsu Ltd., L=Yokohama,
ST=Kanagawa, C=jp> correct?
[no]:yes   (*3)
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
SCS: INFO: scs0101: CSR was issued <C:\sslenv\my_csr.txt>
```

Solaris32/64 Linux32/64

Nickname of the site certificate: SiteCert

Request output destination file name: /sslenv/my_csr.txt

Name: repository.fujitsu.com

Organization unit name: Interstage

Organization name: Fujitsu Ltd.

City name: Yokohama

Prefectural name: Kanagawa

Country code: jp

```
# scsmakeenv -n SiteCert -c -f /sslenv/my_csr.txt
New Password:   (*1)
Retype:   (*1)

Input X.500 distinguished names.
What is your first and last name?
[Unknown]:repository.fujitsu.com   (*2)
What is the name of your organizational unit?
[Unknown]:Interstage   (*2)
What is the name of your organization?
[Unknown]:Fujitsu Ltd.   (*2)
What is the name of your City or Locality?
[Unknown]:Yokohama   (*2)
What is the name of your State or Province?
[Unknown]:Kanagawa   (*2)
What is the two-letter country code for this unit?
[Un]:jp   (*2)
Is <CN=repository.fujitsu.com, OU=Interstage, O=Fujitsu Ltd., L=Yokohama,
ST=Kanagawa, C=jp> correct?
[no]:yes   (*3)
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
Certificate was added to keystore
UX: SCS: INFO: scs0101: CSR was issued </sslenv/my_csr.txt>
```

*1 Enter the password. The entered string will not be echoed back. If Re-type is displayed, re-enter (re-type) the password for confirmation.

*2 For the content to be entered, see the "Reference Manual (Command Edition)."

*3 If the displayed content is correct, enter "yes." To retry the input, enter "no."

Note

- Specify the nickname specified in the -n option when registering a site certificate. Do not forget it.
- If CSR is created, a private key is created in the Interstage certificate environment. To protect the private key, back up the Interstage certificate environment until a certificate is obtained. For details of the backup method, see the Operator's Guide.

  If the Interstage certificate environment is damaged and no backup is available, make another request for an Interstage certificate environment (CSR creation) and the issue of a certificate.

Request to Issue a Certificate

Make a request to issue a certificate to the CA and obtain it.

If the scsmakeenv command is executed normally, a request is output to the file that stores the CSR (certificate signing request). This file is specified in the "-f" option of the scsmakeenv command. Send the file to the CA to request the issue of a certificate. Follow the request creation procedure of each CA.

Registration of a Certificate and CRL (Certificate Revocation List)

Register the certificates and CRL obtained from the CA in the Interstage certificate environment.

Register the certificates starting with the certificate of the CA.

Registration of a Certificate of CA

Register the obtained certificate of CA.

The following shows some examples of registration:

Windows32/64

CA certificate: C:\sslenv\CA.der

Nickname of the CA certificate: CA

```
scsenter -n CA -f C:\sslenv\CA.der
Password:   (*1)
Certificate was added to keystore
SCS: INFO: scs0104: Certificate was imported
```

Solaris32/64 Linux32/64

CA certificate: /sslenv/CA.der

Nickname of the CA certificate: CA

```
# scsenter -n CA -f /sslenv/CA.der
Password:   (*1)
```

```
certificate was added to keystore
UX: SCS: INFO: scs0104: Certificate was imported
```

*1 Enter the password. The entered string will not be echoed back.

Registration of an intermediate CA certificate

Depending on the CA, in addition to the CA certificate and the site certificate there may also be an intermediate CA certificate. In this case, register the intermediate CA certificate that is distributed by the CA before registering the site certificate.

The registration method is the same as for CA certificates. For details, refer to "Registration of a CA Certificate".

Reference:

The spec of Secure Server ID, issued by Verisign Japan Limited, changed in March 2007. As a result, the intermediate CA certificate is now also provided. In this product version, the intermediate CA certificate is also included in the integrated certificate list file. For this reason, if the [-c] option is specified in the scsmakeenv command when the Interstage certificate environment is set up, the intermediate CA certificate is registered with the CA certificate in the Interstage certificate environment.

Registration of a Site Certificate

Register the issued certificate as a site certificate.

The following shows some examples of registration:

Windows32/64

Site certificate: C:\sslenv\SiteCert.der

Nickname of the site certificate: SiteCert

```
scsenter -n SiteCert -f C:\sslenv\SiteCert.der -o
Password:   (*1)
Certificate reply was installed in keystore
SCS: INFO: scs0104: Certificate was imported
```

Solaris32/64 Linux32/64

Site certificate: /sslenv/SiteCert.der

Nickname of the site certificate: SiteCert

```
# scsenter -n SiteCert -f /sslenv/SiteCert.der -o
Password:   (*1)
Certificate reply was installed in keystore
UX: SCS: INFO: scs0104: Certificate was imported
```

*1 Enter the password. The entered string will not be echoed back.

Registration of CRL

Register the obtained CRL.

The following shows some examples of registration:

Windows32/64

CRL C:\sslenv\CRL.der

```
scsenter -c -f C:\sslenv\CRL.der
Password:   (*1)
SCS: INFO: scs0105: CRL was imported
```

Solaris32/64 Linux32/64

CRL /sslenv/CRL.der

```
# scsenter -c -f /sslenv/CRL.der
Password:   (*1)
UX: SCS: INFO: scs0105: CRL was imported
```

*1 Enter the password. The entered string will not be echoed back.

Backup of an Interstage Certificate Environment

After registering the obtained certificates and CRL, be sure to back up the Interstage certificate environment. For the backup method, see the Operator's Guide.

If the Interstage certificate environment is damaged and no backup is available, make another request for an Interstage certificate environment (CSR creation) and the issue of a certificate.

The following shows some examples of registration:

Windows32/64

```
mkdir X:\Backup\scs
xcopy /E C:\Interstage\etc\security X:\Backup\scs   (*1)
```

Solaris32/64 Linux32/64

```
# mkdir /backup/scs
# cp -rp /etc/opt/FJSVisscs/security /backup/scs   (*1)
```

*1 It is recommended to save to removable media.

4.1.1.1 Setting to Use the Certificates (Server)

Make the setting on a server of Interstage Directory Service.

After setting up an Interstage certificate environment, some set up is required to enable use of the certificates. The required setup procedure is described in the following sections.

Setting to Use the Certificates

Certificates that have been registered in the Interstage certificate environment can be displayed in the following Interstage Management Console windows:

- [System] > [Security] > [Certificates] > [CA Certificate] window, or
- [System] > [Security] > [Certificates] > [Site certificate] window

For the management server, certificates can be displayed in the following windows:

- [Application Management] > [Interstage Management Console] > [Interstage Application Server] > [Security] > [Certificates] > [CA Certificate] window, or
- [Application Management] > [Interstage Management Console] > [Interstage Application Server] > [Security] > [Certificates] > [Site certificate] window

Check whether the content of the obtained certificate is correct.

To communicate via SSL, SSL definitions must be created. Create SSL definitions using the following windows of the Interstage Management Console:

- [System] > [Security] > [SSL] > [New] tab (For the management server, [Application Management] > [Interstage Management Console] > [Interstage Application Server] > [Security] > [SSL] > [New] tab)

Select a site certificate rather than a test certificate.

When no client authentication needs to be performed, select "Do not authenticate" in [Client authentication]. In [Protocol version], select "SSL 2.0", "SSL 3.0", or "TLS 1.0". It is recommended that you select either "SSL 3.0" or "TLS 1.0".

To perform client authentication, select "Authenticate (Always authenticate a client certificate)" or "Authenticate (Authenticate if a client certificate is presented)" in [Client authentication]. In [Protocol version], select either "SSL 3.0." or "TLS 1.0".

4.2 Creating the Environment on the Client

This section explains how to create the Interstage Directory Service environment on the client.

4.2.1 Creating a Certificate and Key Management Environment (Client)

Implement the required settings on a client of Interstage Directory Service.

Create a certificate and key management environment, which is an operation environment for SSL.

Perform the following procedures as a user who executes the Interstage Directory Service client.

Use the SMEE command to build the Certificate/Key management environment of the Interstage Directory Service client. For details about each of the commands shown on this page, refer to "SSL Environment Setting Commands" in the "Reference Manual -Command Edition".

Windows32/64

SMEE commands are stored in the following directories.

- Create/Setup command of SMEE3 private key management environment (makeslot, maketoken)
    - Windows (64bit)

      %ProgramFiles%\SecurecryptoLibraryR64\PROGRAM\bin
    - Other than Windows (64bit)

      %ProgramFiles%\SecurecryptoLibraryR\PROGRAM\bin
- Excluding the above.

  %CommonProgramFiles%\Fujitsu Shared\F3FSSMEE

Creation of a Management Directory

Create the directories needed to manage the certificates and private keys.

The following shows some examples of creating directories:

Windows32/64

```
mkdir D:\sslenv\slot   (*1)
mkdir D:\sslenv\sslcert   (*2)
mkdir D:\sslenv\sslcert\cert   (*3)
mkdir D:\sslenv\sslcert\crl   (*4)
```

Solaris32/64 Linux32/64

```
$ mkdir /sslenv/slot   (*1)
$ mkdir /sslenv/sslcert   (*2)
$ mkdir /sslenv/sslcert/cert   (*3)
$ mkdir /sslenv/sslcert/crl   (*4)
```

*1 Slot information directory

*2 Operation control directory

*3 Certificate management directory

*4 CRL management directory

Creation and Setting of a Private Key Management Environment

Create and set a private key management environment required to manage the private keys.

The following shows some examples of creating a private key management environment:

Windows32/64

```
makeslot -d D:\sslenv\slot
New Slot-password:   (*1)
Retype:   (*1)
makeslot: Succeeded. New Slot-ID is 1.   (*2)
maketoken -d D:\sslenv\slot -s 1 -t Token01   (*2)
Slot-password:   (*1)
New SO-PIN for Token01:   (*3)
Retype:   (*3)
New User-PIN for Token01:   (*4)
Retype:   (*4)
```

Solaris32/64 Linux32/64

```
$ makeslot -d /sslenv/slot
New Slot-password:   (*1)
Retype:   (*1)
makeslot: Succeeded. New Slot-ID is 1.   (*2)
$ maketoken -d /sslenv/slot -s 1 -t Token01   (*2)
Slot-password:   (*1)
New SO-PIN for Token01:   (*3)
Retype:   (*3)
New User-PIN for Token01:   (*4)
Retype:   (*4)
```

*1 Enter the slot password. The entered string will not be echoed back. If Re-type is displayed, re-enter (re-type) the password for confirmation.

*2 As a result of executing the makeslot command, the slot ID of the generated slot is returned. Specify this value in the -s option of the maketoken command.

*3 Enter SO-PIN. The entered string will not be echoed back. If Re-type is displayed, re-enter (re-type) the password for confirmation.

*4 Enter user PIN. The entered string will not be echoed back. If Re-type is displayed, re-enter (re-type) the password for confirmation.

Creation of a Certificate and CRL Management Environment

Create and set a certificate and CRL management environment to manage the certificates and CRL.

To use a certificate of VeriSign Inc. Cybertrust, Inc. or another Certification Authority, register the CA Certificate of the root CA of VeriSign Inc. Cybertrust, Inc. or another Certification Authority.

The following shows an example of creating a certificate and CRL management environment using a Certificate (Integration Certificate List File "contractcertlist"):

Windows32/64

```
cmmkenv D:\sslenv\sslcert -todir
D:\sslenv\sslcert\cert,D:\sslenv\sslcert\crl
cmsetenv D:\sslenv\sslcert -sd D:\sslenv\slot -jc 1 -rc
C:\Interstage\IS_cert\contractcertlist
```

Solaris32/64 Linux32/64

```
# cmmkenv /sslenv/sslcert -todir /sslenv/sslcert/cert,/ sslenv/sslcert/crl
# cmsetenv /sslenv/sslcert -sd /sslenv/slot -jc 1 -rc /etc/opt/FJSVisas/contractcertlist
```

4.2.1.1 Creating a Private Key and Acquiring a Certificate (Client)

Create a private key and acquire a certificate on a client of Interstage Directory Service.

Make a request to issue a certificate to CA (certification authority) and obtain it.

Creation of a Certificate Signing Request (Concurrent Creation of a Private Key)

Create a certificate signing request to make a request to CA to issue a certificate.

If the following command is executed, a private key is created at the same time.

The following shows some examples of creating a certificate signing request:

Windows32/64

```
cmmakecsr -ed D:\sslenv\sslcert -sd D:\sslenv\slot -f TEXT -c jp -cn
"repository.fujitsu.com" -o "Fujitsu Ltd." -ou "Interstage" -l "Yokohama" -s
"Kanagawa" -kt RSA -kb 1024 -tl Token01 -of D:\sslenv\myCertRequest
ENTER TOKEN PASSWORD=>   (*1)
```

In this case, the certificate acquisition request is created in the following location:

```
D:\sslenv\myCertRequest
```

Solaris32/64 Linux32/64

```
$ cmmakecsr -ed /sslenv/sslcert -sd /sslenv/slot -f TEXT -c jp -cn
"repository.fujitsu.com" -o "Fujitsu Ltd." -ou "Interstage" -l "Yokohama" -s
"Kanagawa" -kt RSA -kb 1024 -tl Token01 -of /sslenv/myCertRequest
ENTER TOKEN PASSWORD=>   (*1)
```

In this case, the certificate acquisition request is created in the following location:

```
/sslenv/myCertRequest
```

*1 Enter the user PIN. The entered characters will not be echoed back.

Request to Issue a Certificate

Send a certificate signing request to the CA to make a request for a site certificate.

Follow the procedure of each CA for making a request.

Acquisition of a Certificate

Obtain a certificate signed by the CA.

Follow the procedure of each CA for obtaining a signed certificate.

4.2.1.2 Registering a Certificate and CRL (Client)

Register a certificate and CRL with a client of Interstage Directory Service.

Register a certificate and CRL in a certificate and CRL management environment.

Registration of a CA Certificate

Register the obtained CA certificates in the certificate and CRL management environment.

Register the certificates starting with the CA certificate of the root CA.

Note

Certificates of the same CA must be registered with the Interstage Directory Service and Interstage Directory Service client that use SSL.

The following shows some examples of registration:

CA Certificate: CA.der

Windows32/64

```
cmentcert D:\sslenv\CA.der -ed D:\sslenv\sslcert -ca -nn CA
normal end certid = IG6GwPx4gjZEZ2NptohObuWHU9A=   (*1)
```

Solaris32/64 Linux32/64

```
$ cmentcert /sslenv/CA.der -ed /sslenv/sslcert -ca -nn CA
normal end certid = qpD2dla7zA5xUEeDoLNgtb4c5WE=   (*1)
```

*1 The value of certid may be different each time the command is executed.

Note

- The client verifies the site certificate registered with the client. Register the CA certificates used by the client to verify the site certificates with the client.
- All CA certificates registered with the client become the reliable CA certificates when conducting SSL communication between client and server. Since the site certificates are specified in the SSL configuration used by the server repository, register the CA certificates needed to verify a specified site certificate with the client.

Registration of an intermediate CA certificate

Depending on the CA, in addition to the CA certificate and the site certificate there may also be an intermediate CA certificate. In this case, register the intermediate CA certificate that is distributed by the CA before registering the site certificate.

The registration method is the same as for CA certificates. For details, refer to "Registration of a CA Certificate".

Reference:

The spec of Secure Server ID, issued by Verisign Japan Limited, changed in March 2007. As a result, the intermediate CA certificate is now also provided. In this product version, the intermediate CA certificate is also included in the integrated certificate list file. For this reason, if the [-rc] option is specified in the cmsetenv command when the certificate/key management environment is set up, the intermediate CA certificate is registered with the CA certificate in the certificate/key management environment.

Registration of a Site Certificate

Register a site certificate in a certificate and CRL management environment.

Perform the registration only if client authentication is required.

If no client authentication is needed, there is no need to register a site certificate.

Note

No certificate for testing can be used.

The following shows some examples of registration:

Site certificate: user-cert.der

Windows32/64

```
cmentcert D:\sslenv\user-cert.der -ed D:\sslenv\sslcert -own -nn user-cert
normal end certid = 4aCjpxEud6++drEiLbyx4XPCQ2U=   (*1)
```

Solaris32/64 Linux32/64

```
$ cmentcert /sslenv/user-cert.der -ed /sslenv/sslcert -own -nn user-cert
normal end certid = HhMYCOMdh+gzxHToSyoOyEogdac=   (*1)
```

*1 The value of certid may be different each time the command is executed.

Registration of CRL

Register the obtained CRL in a certificate and CRL management environment.

The following shows some examples of registration:

Windows32/64

```
cmentcrl D:\sslenv\CRL.der -ed D:\sslenv\sslcert
normal end CrlID = bAAqy9Qgh8bw2CUG18m3IuEc2mM=   (*1)
```

Solaris32/64 Linux32/64

```
# cmentcrl /sslenv/CRL.der -ed /sslenv/sslcert
normal end CrlID = WLw6q/bNZ7qsQ+8hRjVOJzinmJY=   (*1)
```

*1 The value of CrlID may be different each time the command is executed.

Backup of the Certificate/CRL/Private Key Management Environment

Back up the certificate/CRL/private key management environment.

The following shows some examples:

Windows32/64

```
mkdir X:\Backup\irepcli
xcopy /E D:\sslenv\slot X:\Backup\irepcli   (*1)
xcopy /E D:\sslenv\sslcert X:\Backup\irepcli   (*1)
```

Solaris32/64 Linux32/64

```
$ mkdir /backup/irepcli
$ cp -rp /sslenv/slot /backup/irepcli   (*1)
$ cp -rp /sslenv/sslcert /backup/irepcli   (*1)
```

*1 It is recommended to save to removable media.

4.2.1.3 Setting an SSL Environment Definition File (Client)

Store information about the SSL environment on the Interstage Directory Service client.

For user applications using JNDI or the Interstage Directory Service LDAP command (ldapsearch, ldapmodify, and ldapdelete commands), store the information in the SSL environment definition file.

For the Interstage Directory Service LDAP command, specify the SSL environment definition file using the -Z option.

Interstage Directory Service provides some samples of the SSL environment definition file. Copy the file and then customize it for the environment.

Windows32/64

```
C:\Interstage\IREPSDK\sample\conf\sslconfig.cfg
```

Solaris32/64 Linux32/64

```
/opt/FJSVirepc/sample/conf/sslconfig.cfg
```

Description Format

In the file, describe the definition of each item in a separate line.

The description format is shown below.

```
Definition name = Value
```

Do not enter blanks before or after '='.

Value refers to the characters enclosed by '=' and the new line character. Blank characters and the tab are also valid for Value.

A line starting with '#' is considered a comment.

Note Windows32/64

If a blank character is contained in a directory name or file name, specify the name in the 8.3 format (i.e. "file name.extension" in which the file name consists of up to eight characters and the extension can be up to three characters).

A file name in the 8.3 format can be checked by adding the "/X" option to the DIR command.

List of Definition Items

The following table lists the items in the SSL environment definition file.

Table 4.1 SSL Environment Definition Items

Definition item	Definition name	Required or Optional setting
SSL version	ssl_version	
Encryption algorithm	crypt	Optional
Slot information directory	slot_path	Required
Token label	tkn_lbl	Required
User PIN	tkn_pwd	Required
Operation control directory	cert_path	Required
User certificate nickname	user_cert_name	*1 (see below)
Certificate verification method	ssl_verify	Required
Timer value	ssl_timer	Optional

*1 If omitted, a user certificate (site certificate) registered in the certificate management environment is assumed.

SSL Version (ssl_version)

Explanation

Describe the version of the SSL protocol to be used:

Setup value	Explanation
2	Use the SSL version 2.0 only.
3	Use the SSL version 3.0 only.
31	Use the TLS version 1.0 only.

Abbreviation Value

3

Example

```
ssl_version=3
```

Encryption Algorithm (crypt)

Explanation

Specify the encryption method to be used with SSL by selecting from the following. If multiple encryption methods are selected, it describes them separated by ':' in order of priority.

Configure the same settings as those of the SSL configuration used by the Interstage Directory Service, which is the communication party.

If '2' is specified as the SSL version (ssl_version), the following values can be used:

Setup value	Explanation
DES-CBC3-MD5	168bit triple DES encryption, MD5 MAC
RC4-MD5	128bit RC4 encryption, MD5 MAC
RC2-MD5	128bit RC2 encryption, MD5 MAC
DES-CBC-MD5	56bit DES encryption, MD5 MAC
EXP-RC4-MD5	40bit RC4 encryption, MD5 MAC
EXP-RC2-MD5	40bit RC encryption, MD5 MAC

If either '3' or '31' is specified as the SSL version (ssl_version), the following values can be used:

Setup value	Explanation
RSA-SC2000-256-SHA	256 bit SC2000 encryption, SHA-1 MAC
RSA-AES-256-SHA	256 bit AES encoding, SHA-1 MAC
RSA-SC2000-128-SHA	128 bit SC2000 encryption, SHA-1 MAC
RSA-AES-128-SHA	128 bit AES encoding, SHA-1 MAC
RSA-3DES-SHA	168bit triple DES encryption, SHA-1 MAC
RSA-RC4-MD5	128bit RC4 encryption, MD5 MAC
RSA-RC4-SHA	128bit RC4 encryption, SHA-1 MAC
RSA-DES-SHA	56bit DES encryption, SHA-1 MAC
RSA-EXPORT-RC4-MD5	40bit RC4 encryption, MD5 MAC
RSA-EXPORT-RC2-MD5	40bit RC2 encryption, MD5 MAC
RSA-NULL-SHA	No encryption, SHA-1 MAC
RSA-NULL-MD5	No encryption, MD5 MAC

The encryption methods supported by Interstage Application Server are as follows:

- Public key encryption method: RSA
- Private key encryption method: SC2000, AES, DES, 3DES (triple DES), RC4, RC2 (NULL indicates no encryption)
- Private key processing mode: CBC (the number is the block length)
- Hash key: SHA, MD5

MAC is a message authentication code.

Abbreviation Value

Specifying a SSL version (ssl_version), will cause the following values to be specified. In the following explanation, each encryption method is on a new line.

- If the SSL version(ssl_version) '2' is specified:

  DES-CBC3-MD5:

  DES-CBC-MD5:

  RC4-MD5:

  RC2-MD5:

  EXP-RC4-MD5:

  EXP-RC2-MD5

- If either '3' or '31' is specified for the SSL version(ssl_version):

  RSA-SC2000-256-SHA:

RSA-AES-256-SHA:

RSA-SC2000-128-SHA:

RSA-AES-128-SHA

RSA-3DES-SHA:

RSA-RC4-MD5:

RSA-RC4-SHA:

RSA-DES-SHA:

RSA-EXPORT-RC4-MD5:

- RSA-EXPORT-RC2-MD5:

Example

```
crypt=RSA-3DES-SHA:RSA-RC4-MD5:RSA-RC4-SHA:RSA-DES-SHA:RSA-EXPORT-RC4-MD5:RSA-EXPORT-RC2-MD5
```

Slot Information Directory (slot_path)

Explanation

Describe the slot information directory created in "Creating a Certificate and Key Management Environment (Client)" using the full specification.

Abbreviation Value

This definition item cannot be abbreviated.

Example

Windows32/64

```
slot_path=D:\sslenv\slot
```

Solaris32/64 Linux32/64

```
slot_path=/sslenv/slot
```

Token Label (tkn_lbl)

Explanation

Specify the token label specified in "Creation and Setting of a Private Key Management Environment."

Abbreviation Value

This definition item cannot be abbreviated.

Example

```
tkn_lbl=Token01
```

User PIN (tkn_pwd)

Explanation

Enter the user PIN specified in "Creation and Setting of a Private Key Management Environment."

After entering the user PIN, the irepencupin command needs to be used for encryption.

For details on encryption of the user PIN, refer to 4.2.1.4 Encrypting the User PIN (Client). For information about how to use the irepencupin command, see "Interstage Directory Service operation command" in the Reference Manual (Command Edition)."

Abbreviation Value

This definition item cannot be abbreviated.

Example

```
tkn_pwd=Token111
```

Operation Control Directory (cert_path)

Explanation

Describe the operation control directory created in "Creating a Certificate and Key Management Environment (Client)" using the full pathname.

Abbreviation Value

This definition item cannot be abbreviated.

Example

Windows32/64

```
cert_path=D:\sslenv\sslcert
```

Solaris32/64 Linux32/64

```
cert_path=/sslenv/sslcert
```

User Certificate Nickname (user_cert_name)

Explanation

Specify the nickname of the user certificate (site certificate) specified in "Registering a Certificate and CRL (Client) ".

Abbreviation Value

All nicknames of the user certificate (site certificate) registered in the certificate management environment are assumed.

Example

```
user_cert_name=user-cert
```

Certificate Verification Method (ssl_verify)

Explanation

Specify the verification method of certificates. The following verification methods can be specified:

Setup value	Certificate verification method
0	No verification
1	Verify certificates used by the Interstage Directory Service client.
2	Verify certificates used by the Interstage Directory Service client and those sent by the Interstage Directory Service server.

Abbreviation Value

This definition item cannot be abbreviated.

Example

```
ssl_verify=2
```

Timer Value (ssl_timer)

Explanation

Specify the wait time for connecting the server and client or sending/receiving data in seconds. Specify a value equal to or greater than 1.

Abbreviation Value

3600

Example

```
ssl_timer=300
```

Examples of SSL Definition File Settings

Windows32/64

```
#
# ==== SSL environment file ====
#
# ----------------------------
# SSL protocol version
#  ssl_version=2 | 3 | 31
# ----------------------------
ssl_version=3


# ----------------------------
# Slot directory
#  slot_path=directory path
# ----------------------------
slot_path=D:\sslenv\slot


# ----------------------------
# Token label
#  tkn_lbl=token label
# ----------------------------
tkn_lbl=Token01


# ----------------------------
# User PIN
#  tkn_pwd=user pin
# ----------------------------
tkn_pwd=xxxxxxxx   (*1)


# ----------------------------
# Certificate directory
#  cert_path=directory path
# ----------------------------
cert_path=D:\sslenv\sslcert


# ----------------------------
# User certificate nickname
#  user_cert_name=nickname
# ----------------------------
#user_cert_name=user-cert   (*2)


# ----------------------------
# Verify mode
#  ssl_verify=0 | 1 | 2
# -----------------------------
ssl_verify=2


# -----------------------------
# Timer
#  ssl_timer=time(sec)
# -----------------------------
#ssl_timer=300
```

*1 Specify the user PIN specified in "Creation and setting of a private key management environment."

*2 To enable all site certificates registered in the certificate and key management environment, place "#" at the start of the lines.

Solaris32/64 Linux32/64

```
#
# ==== SSL environment file ====
#
# -----------------------------
# SSL protocol version
#  ssl_version=2 | 3 | 31
# -----------------------------
ssl_version=3


# -----------------------------
# Slot directory
#  slot_path=directory path
# -----------------------------
slot_path=/sslenv/slot


# -----------------------------
# Token label
#  tkn_lbl=token label
# -----------------------------
tkn_lbl=Token01


# -----------------------------
# User PIN
#  tkn_pwd=user pin
# -----------------------------
tkn_pwd=xxxxxxxx   (*1)


# -----------------------------
# Certificate directory
#  cert_path=directory path
# -----------------------------
cert_path=/sslenv/sslcert


# -----------------------------
# User certificate nickname
#  user_cert_name=nickname
# -----------------------------
#user_cert_name=user-cert   (*2)


# -----------------------------
# Verify mode
#  ssl_verify=0 | 1 | 2
# ----------------------------
ssl_verify=2


# ----------------------------
# Timer
#  ssl_timer=time(sec)
# ----------------------------
#ssl_timer=300
```

*1 Specify the user PIN specified in "Creation and setting of a private key management environment."

*2 To enable all site certificates registered in the certificate and key management environment, place "#" at the start of the lines.

4.2.1.4 Encrypting the User PIN (Client)

The user PIN described in the SSL environment definition file needs to be encrypted.

By specifying the SSL environment definition file in the irepencupin command, the user PIN described in the file will be encrypted. For information about how to use the irepencupin command, see "Interstage Directory Service operation command" in the Reference Manual (Command Edition)."

The following shows some execution examples:

Windows32/64

```
irepencupin -f D:\conf\sslconfig.cfg
```

Solaris32/64 Linux32/64

```
# irepencupin -f /conf/sslconfig.cfg
```

Note

Solaris32/64

If the command is executed successfully, a backup file (SSL environment definition file name.backup) will be created in the same directory. If no backup file will be needed, delete it.

4.3 Communication between the Repository and the Database

If an RDB is used for the repository database, data communication between the repository and the RDB is sent and received without encryption.

To encrypt data communication during transmission, use SSL communication. Using SSL communication means that even if communication is intercepted the risks of decryption and eavesdropping are countered by the SSL encryption.

To use SSL encrypted communication between the repository and the RDB, use the functionality of the RDB. Refer to the RDB manual for more information.

If there are a large number of clients and a high frequency of accesses to the Interstage Directory Service, Fujitsu recommends reducing the load on the server by using an SSL accelerator in order to ensure response performance.

Chapter 5 Creating a Repository

This chapter explains the procedures for creating repositories, and for creating and registering data.

5.1 Using the Standard Database

This section explains how to create a repository that uses the standard database.

The Interstage Management Console of the machine that sets up the server is used to create a repository. For information on how to operate the Interstage Management Console, refer to the "Services" chapter of the Operator's Guide.

1. Select [System] > [Service] > [Repository] > [Create a New Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository] > [Create a New Repository]).

2. Click the [Create] button after specifying the following details for each item:

   [Simple Settings]

   - Repository name

     Specify the repository name that identifies each repository. This item can be specified only when creating a new repository. Once the repository has been created, the name cannot be changed.

   - Administrator DN

     Specify the DN (distinguished name) for the administrator who will manage the created repository in the DN format. This item can be specified only when creating a new repository. Once the repository has been created, the value cannot be changed.

   - Administrator DN password

     Specify the password of the administrator who will manage the created repository.

   - Administrator DN password (re-entry)

     Re-enter the password of the administrator who will manage the created repository.

   - Public Directory

     Specify the top entry to make the repository public in the DN (distinguished name) format. The public directory can be specified only when creating a new repository. Once the repository is created, the value cannot be changed.

   - Repository database

     Select "Standard DB".

   - Database storage directory

     Specify the database directory using its full path. Be sure to specify this item if the standard database is used as the repository database. This item can only be specified when a new repository is created. This value cannot be changed once the repository has been created.

   [Detailed Settings] Connection Settings

   - Port number

     Specify the port number to use for non-SSL communication. This item can be specified only during creation of a new repository. Once the repository is created, the value cannot be changed.

   - Enable SSL encryption?

     Specify whether to conduct SSL communication. This item can be specified only during creation of a new repository. Once the repository is created, the value cannot be changed.

   - SSL Port number

     Specify the port number to use for SSL communication. This item can be specified only during creation of a new repository. Once the repository is created, the value cannot be changed.

- SSL configuration

  Decide on the SSL configuration to be used for SSL communication.

For other items, there is normally no need to change the initial values. Change them if required.

For character definitions, including the number of characters and the range that can be specified for each item, refer to "5.2 Setting Items of the Interstage Management Console".

Once the repository has been created, it is added to the [Repository: View Status] window (open this window by selecting [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository])).

Windows32/64

The created repository will also be added to the Windows(R) service under the following name:

```
Interstage Directory Service (repository name)
```

When the repository is created, the initial tree is created under the top entry specified in "Public Directory". This initial tree structure can be shared by all services.

The initial tree structure can be used by the following services:

- The repository server for single sign-on
- The online access management function for HTTP Server
- The security function for J2EE applications
- User management for Interstage Portalworks LDAP servers

If "ou=interstage,o=fujitsu,dc=com" is specified as the initial value for the public directory, the initial tree that is created will be as follows. If the "Public Directory" is changed from the default value, the "ou=interstage,o=fujitsu,dc=com" part will changed to the specified directory.

Tree created (DN format)	Usage
ou=User,ou=interstage,o=fujitsu,dc=com	Tree for storing user information for each service
ou=SSO ACI,ou=interstage,o=fujitsu,dc=com	Tree for storing access control information for single sign-on
ou=Resource,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com	Tree for storing protected resources for single-sign on
ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com	Tree for storing role definitions for single sign-on

Note

Several minutes are needed to create a repository. This includes the time needed to create database information used inside the repository. The total time required varies a little depending on the machine performance.

3. Use the *irepadmin* command to change the password encryption method before starting the repository.

   The password encryption method cannot be changed after the application has started. For details, refer to the "Interstage Directory Service Operation Commands" chapter of the Reference Manual (Command Edition).

4. Start the created repository from the [Repository: View Status] window.

As soon as the repository is created, it is set to start automatically when the operating system starts. Refer to "Automatic Start" in the "Operating and Maintaining Repositories" chapter for information on changing automatic startup.

When using a replication configuration, for the repository on the slave server, back up the repository that has been created on the master server, and then restore this repository on the slave server. For information about this procedure, refer to the "Using the Standard Database" in the "Creating a Load Distribution Environment (Replication Mode)" appendix.

For the master server in a replication configuration, use the Interstage Management Console for the machine where the master server is to be constructed Refer to the help for the Interstage Management Console for more information on how to use it.

5.1.1 Using the Symfoware/RDB

This section explains how to create a repository that uses Symfoware/RDB.

The Interstage Management Console of the machine that sets up the server is used to create a repository. For information on how to operate the Interstage Management Console, refer to the "Services" chapter of the Operator's Guide.

1. Select [System] > [Service] > [Repository] > [Create a New Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository] > [Create a New Repository]).

2. Click the [Create] button after specifying the following details for each item:

   [Simple Settings]

   - Repository name

     Specify the repository name that identifies each repository. This item can be specified only when creating a new repository. Once the repository has been created, the name cannot be changed.

   - Administrator DN

     Specify the DN (distinguished name) for the administrator who will manage the created repository in the DN format. This item can be specified only when creating a new repository. Once the repository has been created, the value cannot be changed.

   - Administrator DN password

     Specify the password of the administrator who will manage the created repository.

   - Administrator DN password (re-entry)

     Re-enter the password of the administrator who will manage the created repository.

   - Public Directory

     Specify the top entry to make the repository public in the DN (distinguished name) format. The public directory can be specified only when creating a new repository. Once the repository is created, the value cannot be changed.

   - Repository database

     Select "Symfoware". An RDB environment must already have been created. This option can be specified only when a new repository is created. Its value cannot be changed after the repository has been created.

   - The database connection host name

     Specify the host name for the database.

     This option can be specified only when a new repository is created. Its value cannot be changed after the repository has been created.

     To share the database, specify a host name that can be resolved by all repositories sharing the database.

   - Database connection port number

     Specify the port number for the database.

     This option can be specified only when a new repository is created. Its value cannot be changed after the repository has been created.

   - Database name

     Specify the name of the database.

     Databases that are being used by other repositories cannot be used. Similarly, databases that have been used by a deleted repository cannot be used even if they are currently not used.

     This option can be specified only when a new repository is created. Its value cannot be changed after the repository has been created.

   - Database connection user ID

     Specify the database connection user for the repository. Specify the user account that was registered with the operating system as the database connection user when the database was created.

This option can be specified only when a new repository is created. Its value cannot be changed after the repository has been created.

- Database connection password

  Specify the password for the database connection user for the repository. The password information managed by the operating system will not be overwritten by the value of this item.

[Detailed Settings] Connection Settings

- Port number

  Specify the port number to use for non-SSL communication. This item can be specified only during creation of a new repository. Once the repository is created, the value cannot be changed.

- Enable SSL encryption?

  Specify whether to conduct SSL communication. This item can be specified only during creation of a new repository. Once the repository is created, the value cannot be changed.

- SSL Port number

  Specify the port number to use for SSL communication. This item can be specified only during creation of a new repository. Once the repository is created, the value cannot be changed.

- SSL configuration

  Decide on the SSL configuration to be used for SSL communication.

For other items, there is normally no need to change the initial values. Change them if required.

For character definitions, including the number of characters and the range that can be specified for each item, refer to "5.2 Setting Items of the Interstage Management Console".

Once the repository has been created, it is added to the [Repository: View Status] window (open this window by selecting [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository])).

Windows32/64

The created repository will also be added to the Windows(R) service under the following name:

```
Interstage Directory Service (repository name)
```

When the repository is created, the initial tree is created under the top entry specified in "Public Directory". This initial tree structure can be shared by all services.

The initial tree structure can be used by the following services:

- The repository server for single sign-on
- The online access management function for HTTP Server
- The security function for J2EE applications
- User management for Interstage Portalworks LDAP servers

If "ou=interstage,o=fujitsu,dc=com" is specified as the initial value for the public directory, the initial tree that is created will be as follows. If the "Public Directory" is changed from the default value, the "ou=interstage,o=fujitsu,dc=com" part will changed to the specified directory.

Tree created (DN format)	Usage
ou=User,ou=interstage,o=fujitsu,dc=com	Tree for storing user information for each service
ou=SSO ACI,ou=interstage,o=fujitsu,dc=com	Tree for storing access control information for single sign-on
ou=Resource,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com	Tree for storing protected resources for single-sign on

Tree created (DN format)	Usage
ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com	Tree for storing role definitions for single sign-on

Note

Several minutes are needed to create a repository. This includes the time needed to create database information used inside the repository. The total time required varies a little depending on the machine performance.

3. Use the *irepadmin* command to change the password encryption method before starting the repository.

   The password encryption method cannot be changed after the application has started. For details, refer to the "Interstage Directory Service Operation Commands" chapter of the Reference Manual (Command Edition).

4. Depending on the specification of the server that was used to install Symfoware/RDB, the multikey search functionality can be improved by setting an appropriate value for the number of connections from the repository to the RDB.

   The maximum number of connections from the repository to the RDB is set using the *irepadmin* command. The initial value is [16]. It is recommended that you set the following value:

   CPU of the server that was used to install Symfoware/RDB * 4

   For details about this configuration, refer to the "Interstage Directory Service Operation Commands" chapter of the Reference Manual (Command Edition).

   Depending on the specified maximum number of connections, it may also be necessary to configure/change the settings for the maximum number of connections on the database-side.

   This value is specified using the following operating environment file parameters that are used by the system. Specify/add the number of connections required to use the Interstage Directory Service (the maximum number of connections from the repository to the RDB + 1).

   - MAX_CONNECT_SYS (if the database is on the same server as the repository)
   - MAX_CONNECT_TCP (if the database is on a different server to the repository)

5. Start the created repository from the [Repository: View Status] window.

The repository will be configured to automatically start when the operating system starts, immediately after it has been created. However Symfoware/RDB must start before the repository in order for the repository to start correctly. Refer to "Automatic Start" in the "Operating and Maintaining Repositories" chapter for information about the automatic startup settings for repositories and Symfoware/RDB.

5.1.2 Using the Oracle Database

This section explains how to create a repository that uses an Oracle database.

The Interstage Management Console of the machine that sets up the server is used to create a repository. For information on how to operate the Interstage Management Console, refer to the "Services" chapter of the Operator's Guide.

1. Select [System] > [Service] > [Repository] > [Create a New Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository] > [Create a New Repository]).

2. Click the [Create] button after specifying the following details for each item:

   [Simple Settings]

   - Repository name

     Specify the repository name that identifies each repository. This item can be specified only when creating a new repository. Once the repository has been created, the name cannot be changed.

   - Administrator DN

     Specify the DN (distinguished name) for the administrator who will manage the created repository in the DN format. This item can be specified only when creating a new repository. Once the repository has been created, the value cannot be changed.

   - Administrator DN password

     Specify the password of the administrator who will manage the created repository.

- Administrator DN password (re-entry)

  Re-enter the password of the administrator who will manage the created repository.

- Public Directory

  Specify the top entry to make the repository public in the DN (distinguished name) format. The public directory can be specified only when creating a new repository. Once the repository is created, the value cannot be changed.

- Repository database

  Select "Oracle". An RDB environment must already have been created. This option can be specified only when a new repository is created. Its value cannot be changed after the repository has been created.

- Net service name

  Specify the net service name for connecting to the database. This option can be specified only when a new repository is created. Its value cannot be changed after the repository has been created.

- Oracle home directory

  Specify the Oracle home directory that was set up when the Oracle database was installed.

  Windows32/64

  To use Interstage Directory Service with Windows Server(R) x64 Editions (32-bit compatible), install 32-bit(x86) Oracle Database Client on the machine used to run Interstage Directory Service.

  For the Oracle home directory, specify the 32-bit(x86) Oracle Database Client Oracle home directory.

- Database connection user ID

  Specify the database connection user for the repository. Specify the user account that was registered with the Oracle database as the database connection user when the database was created.

  This option can be specified only when a new repository is created. Its value cannot be changed after the repository has been created.

- Database connection password

  Specify the password for the database connection user for the repository. Specify the password for the user account that has been registered with the Oracle database. The password information registered with the Oracle database will not be overwritten by the value of this item.

[Detailed Settings] Connection Settings

- Port number

  Specify the port number to use for non-SSL communication. This item can be specified only during creation of a new repository. Once the repository is created, the value cannot be changed.

- Enable SSL encryption?

  Specify whether to conduct SSL communication. This item can be specified only during creation of a new repository. Once the repository is created, the value cannot be changed.

- SSL Port number

  Specify the port number to use for SSL communication. This item can be specified only during creation of a new repository. Once the repository is created, the value cannot be changed.

- SSL configuration

  Decide on the SSL configuration to be used for SSL communication.

For other items, there is normally no need to change the initial values. Change them if required.

For character definitions, including the number of characters and the range that can be specified for each item, refer to "5.2 Setting Items of the Interstage Management Console".

Once the repository has been created, it is added to the [Repository: View Status] window (open this window by selecting [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository])).

Windows32/64

The created repository will also be added to the Windows(R) service under the following name:

```
Interstage Directory Service (repository name)
```

When the repository is created, the initial tree is created under the top entry specified in "Public Directory". This initial tree structure can be shared by all services.

The initial tree structure can be used by the following services:

- The repository server for single sign-on
- The online access management function for HTTP Server
- The security function for J2EE applications
- User management for Interstage Portalworks LDAP servers

If "ou=interstage,o=fujitsu,dc=com" is specified as the initial value for the public directory, the initial tree that is created will be as follows. If the "Public Directory" is changed from the default value, the "ou=interstage,o=fujitsu,dc=com" part will changed to the specified directory.

Tree created (DN format)	Usage
ou=User,ou=interstage,o=fujitsu,dc=com	Tree for storing user information for each service
ou=SSO ACI,ou=interstage,o=fujitsu,dc=com	Tree for storing access control information for single sign-on
ou=Resource,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com	Tree for storing protected resources for single-sign on
ou=Role,ou=SSO ACI,ou=interstage,o=fujitsu,dc=com	Tree for storing role definitions for single sign-on

Note

Several minutes are needed to create a repository. This includes the time needed to create database information used inside the repository. The total time required varies a little depending on the machine performance.

3. Use the *irepadmin* command to change the password encryption method before starting the repository.

   The password encryption method cannot be changed after the application has started. For details, refer to the "Interstage Directory Service Operation Commands" chapter of the Reference Manual (Command Edition).

4. Depending on the specification of the server that was used to install the Oracle database, the multikey search functionality can be improved by configuring an appropriate number of connections from the repository to the RDB.

   The maximum number of connections from the repository to the RDB is set using the *irepadmin* command. The initial value is [16]. It is recommended that you set the following value:

   (CPU number of the server that was used to install the Oracle database) * 4

   For details about this configuration, refer to the "Interstage Directory Service Operation Commands" chapter of the Reference Manual (Command Edition).

   Depending on the specified maximum number of connections from the repository to the RDB, it may also be necessary to configure/change the settings for the maximum number of connections on the database-side.

   This value is specified using the following database initialization parameters that are used by the system. When selecting a value, consider the number of connections required to use the Interstage Directory Service (the maximum number of connections from the repository to the RDB + 1) and also refer to the Oracle database manual before calculating the value.

   - PROCESSES

   or

   - SESSIONS

    - TRANSACTIONS

5. Start the created repository from the [Repository: View Status] window.

The repository will be configured to automatically start when the operating system starts, immediately after it has been created. However, the Oracle database must start before the repository in order for the repository to start correctly. Refer to "Automatic Start" in the "Operating and Maintaining Repositories" chapter for more information about the automatic startup settings for repositories and Oracle databases.

5.2 Setting Items of the Interstage Management Console

This section describes the items to be set for the Interstage Management Console.

General Settings

- Repository Name
- Administrator DN
- Administrator DN password
- Public Directory
- Repository database
- Database Storage Directory
- Cache Size
- Database connection host name
- Database connection port number
- Database name
- Net service name
- Oracle home directory
- Database connection user ID
- Database connection password

Connection Settings

- Port number
- Enable SSL encryption?
- SSL port number
- SSL configuration
- Connection idle timeout

Search Settings

- Maximum number of searchable entries
- Search Timeout

Access Log Settings

- Output Access Log?
- Output level
- Access log storage directory
- Rotation type
- Size
- Number of access log files

Replication Settings

- Operation mode

Slave Operation Settings

- Master host name

Master Operation Definition (Replication Connection Settings)

- Host name
- Port number
- Enable SSL encryption?
- Present client certificate?
- SSL configuration
- DN for connection
- Password for the connection.

Note

Do not directly edit the files created when setting up an environment for Interstage Directory Service. If files are directly edited, operational problems may occur.

General Settings

- Repository Name

  Specify the repository name that identifies each repository, using a string of up to eight characters.

  Allowable characters include alphanumeric characters and the underline (_). The first character must always be an alphabetical character. If an alphabetical upper-case character is specified, it will be converted into an alphabetical lower-case character. The initial value is "repnnn" (nnn are numeric characters 001, 002, 003 ...).

  The repository name can be specified only during repository setup.

  To enable replication, the [Repository name] value for the master and slave must be identical.

  Note

  Interstage Directory Service uses a database to store repository data. Either Interstage data store or a relational database (RDB) can be used as the database. Note the following points if Interstage data store is used (that is, if "Do not use" was selected for "Use relational database as the repository database").

  The following products of Interstage use Interstage data store.

  - Interstage Studio
  - Interstage Contentbiz
  - Interstage Portalworks

  If any of these products and Interstage Directory Service are both installed on the same server, the data store name and the repository name of Interstage data store used in these products must be different.

  Windows32/64

  The DOS device name cannot be the same as the repository name.

- Administrator DN

  Specify the DN (distinguished name) for the administrator who will manage the repository created in the DN format. The DN is a string of up to 512 bytes. The string specified in [Public Directory] will be added to the specified Administrator DN.

  "cn", "ou", "o", "c", "l", and "dc" can be specified as an attribute of RDN (relative distinguished name) which constitutes the DN (distinguished name) format.

  Alphanumeric characters, the minus sign (-), the period (.), and the underline (_) can be specified as an attribute value of RDN (relative distinguished name) which constitutes the DN (distinguished name) format.

Insert the equal sign (=) between the specified attribute name and attribute value of the RDN (relative distinguished name) which constitutes DN (distinguished name) format.

If multiple RDN (relative distinguished name) are specified, separate them with a comma (,). For example, "cn=manager" and "cn=manager, ou=managergroup" can be specified. The initial value is "cn=manager", it can only be modified when the repository is first created.

Note

It is not possible to specify multiple attributes for the RDN (relative distinguished name) of the Administrator DN (Multi-AVA cannot be used). For example, multiple attributes cannot be specified using the plus sign (+) for example, "cn=User001+sn=fujitsu".

- Administrator DN Password

  Use a string of up to 128 bytes to specify the password for the administrator to manage the created repository. . Allowable characters include alphanumeric characters, the comma (,), the plus sign (+), the equals sign (=), the minus sign (-), the period (.), and the underline (_). No initial value is provided.

- Public Directory

  Use a string of up to 512 bytes to specify the top entry that makes the repository public in the DN (distinguished name) format.

  "cn", "ou", "o", "c", "l", and "dc" can be specified as an attribute of the RDN (relative distinguished name), which constitutes DN (distinguished name) format.

  Alphanumeric characters, the minus sign (-), the period (.), and the underline (_) can also be specified as an attribute value of the RDN (relative distinguished name) which composes DN (distinguished name) format.

  Specify equal sign (=) between the attribute name and the attribute value of RDN (relative distinguished name) which composes DN (distinguished name) format is specified.

  If multiple RDN (relative distinguished name) are specified, separate them with a comma (,). For example,"ou=interstage,o=fujitsu,dc=com" and "c=jp" can be specified. The initial values are "ou=interstage,o=fujitsu,dc=com."

  The public directory can only be modified when the repository is first created.

  To enable replication, the value in [Public directory] must be the same for both master and slave.

  Note

  It is not possible to specify multiple attributes for the RDN (relative distinguished name) of the public directory (Multi-AVA cannot be used). For example, multiple attributes cannot be specified by using plus sign (+) like "ou=fujitsu+st=tokyo".

- Repository Database

  Select the database used by the repository. If a relational database (RDB) is used, more than 10,000 entries can be managed. The default value is "Standard database". This option can be specified only when a new repository is created.

  - Standard database

    The repository will use the standard database (Interstage data store) for the Interstage Directory Service.

  - Symfoware

    The repository will use Symfoware/RDB. An RDB environment must already have been created.

  - Oracle

    The repository will use an Oracle database. An RDB environment must already have been created.

  The display of database information items differs depending on the selected database:

  - Standard database

    - Database Storage Directory

    - Cache Size

  - Symfoware

    - Database connection host name

    - Database connection port number

        - Database name
        - Database connection user ID
        - Database connection password
    - Oracle
        - Net service name
        - Oracle home directory
        - Database connection user ID
        - Database connection password
- Database Storage Directory

  Enter the storage directory of the database using the full specification. Be sure to specify this item if the standard database is used as the repository database.

  The actual storage directory of the database is defined by appending "/repository_name/data" (or for Windows(R) "\repository_name \data") to the specified storage directory.

Table 5.1 Valid Directory Lengths and Characters

	Windows32/64	Solaris32/64	Linux32/64
Length	Up to 192 bytes	Up to 242 bytes	Up to 242 bytes
Valid characters	En-size alphanumeric character Dollar sign ($) Ampersand (&) Single quotation mark (') Plus sign (+) Minus sign (-) Period (.) Equals sign (=) at sign (@) Underline (_) Back quotation mark (`) Tilde (~) Square bracket ([]) Brace ({}) Space ( ) Colon (:) Slash (/) Backslash (\)	En-size alphanumeric character Slash (/) Minus sign (-) Underline (_) Tilde (~)	En-size alphanumeric character Slash (/) Minus sign (-) Underline (_) Tilde (~)

The multi-byte code system cannot be used. In Windows®, the colon (:) can be used only when specifying a drive character and the backslash (\) can be used only to separate directories. When specifying a drive, include "\" for example, "C:\"

The initial values are as follows:

Windows32/64

```
"C:\Interstage\Enabler\EnablerDStores\IREP" (default installation path)
```

Solaris32/64

```
"/var/opt/FJSVena/EnablerDStores/FJSVirep"
```

Linux32/64

```
"/var/opt/FJSVena/DStores/FJSVirep"
```

Always specify this item. This item can be specified only for new creation.

To enable replication, [Database storage directory] for the master and the slave must by identical.

Note

- Set the database storage directory after ensuring that sufficient disk space is available.
- Note the Permissions settings when any database storage directory other than the initial value is set.

Windows32/64

When specifying a database storage directory other than the default, give the "Administrators" group full control access to all directories within the directory.

Solaris32/64 Linux32/64

When specifying a database storage directory other than the default, set the owner of all directories within the storage directory to "oms" and permit "read," "write," and "execute" to the owner.

The following shows an example of setting permissions on the storage directory (the database storage directory is assumed to be "/data/user"):

1. If no storage directory is created, create a database storage directory. By specifying the -p argument, a non-existent parent directory can also be created.

   ```
   mkdir -p /data/user
   ```

2. Set the permissions of "read," "write," and "execute" to the directory. By specifying the -R argument, the permissions can be set recursively through the sub-directories.

   ```
   chmod -R 700 /data
   ```

3. Set "oms" to the directory as its owner. By specifying the -R argument, the owner can be set recursively through the sub-directories.

   ```
   chown -R oms /data
   ```

- Cache Size

  Specify the cache size when performing a search. Values can be between 100 and 65535 pages. One page corresponds to 4KB. The initial size is "1000" pages. Be sure to specify this item if the standard database is used as the repository database.

- Database Connection Host Name

  Specify the host name for the database using a string of no more than 106 bytes. Ensure that you specify a host name with an IP address that can be resolved. The following characters can be used: alphanumeric characters, minus sign (-), period (.) and underscore (_).There is no default value.

  Ensure that you specify this item. It can be specified only when a new database is created.

- Database Connection Port Number

  Specify the port number for the database. A value between 1 and 65535 can be specified. The default value is "2050".

  Ensure that you specify this item. It can be specified only when a new database is created.

- Database Name

  Specify the name of the database using a string of no more than 8 bytes. The following characters can be used: alphanumeric characters. There is no default value.

  Ensure that you specify this item. It can be specified only when a new database is created.

- Net Service Name

  Specify the net service name used to configure communication for the Oracle database using a string of no more than 128 bytes. The following characters can be used: alphanumeric characters, underscore (_), hash sign (#) and dollar sign ($).There is no default value.

  Ensure that you specify this item. It can be specified only when a new database is created.

- Oracle Home Directory

  Specify the Oracle home directory that was set up when the Oracle database was installed.

  The following table shows the maximum length of each string, and the characters that can be used.

Table 5.2 Valid Directory Lengths and Characters

	Windows32/64	Solaris32/64	Linux32/64
Length	Up to 256 bytes	Up to 256 bytes	Up to 256 bytes
Valid characters	En-size alphanumeric character Dollar sign ($) Ampersand (&) Single quotation mark (') Plus sign (+) Minus sign (-) Period (.) Equals sign (=) at sign (@) Underline (_) Back quotation mark (`) Tilde (~) Square bracket ([]) Brace ({}) Space ( ) Colon (:) Slash (/) Backslash (\)	En-size alphanumeric character Slash (/) Minus sign (-) Period (.) Underline (_) Tilde (~)	En-size alphanumeric character Slash (/) Minus sign (-) Period (.) Underline (_) Tilde (~)

  The multi-byte code system cannot be used. In Windows®, the colon (:) can be used only when specifying a drive character and the backslash (\) can be used only to separate directories. When specifying a drive, include "\" for example, "C:\"

The initial values are as follows:

- Database Connection User ID

  Specify the user account that will connect to the database.

  When Symfoware/RDB is used as the repository database, the operating system's authentication mechanism is used to connect to it. Specify the user account that was registered with the operating system as the database connection user when the database was created. There is no default value.

  If an Oracle database is used as the repository database, a user account that has been registered with the Oracle database is used to connect to it. Specify the user account that was registered with the Oracle database as the database connection user when the database was created. There is no default value.

  Ensure that you specify this item. It can be specified only when a new database is created.

- Database Connection Password

  Specify the password for the user account that connects to the database.

  When Symfoware/RDB is used as the repository database, the operating system's authentication mechanism is used to connect to the database. Specify the password for the user account that was registered with the operating system as the database connection user when the database was created. The password information managed by the operating system will not be overwritten by the value of this item. There is no default value.

  If an Oracle database is used as the repository database, a user account that has been registered with the Oracle database is used to connect to the database. Specify the password for the user account that was registered with the Oracle database as the database connection user when the database was created. The password information registered with the Oracle database will not be overwritten by the value of this item. There is no default value.

  Ensure that you specify this item.

Connection Settings

- Port Number

  Specify the port number (between 1 and 65535) used for non-SSL communication. The initial value is 389.

  It is a good idea to specify the port number after designing the port numbers to be used by each service on the server.

  The port number can be specified only during repository setup.

  Note

  There is a higher risk of services attempting to use the same ports if a port number other than the initial value is used. This is particularly relevant for port numbers between 1 and 1023 which are commonly-used.

- Enable SSL Encryption?

  Specify whether to use SSL communication. If it is specified, the client-server authentication and encrypted communication of SSL will be used as the communication protocol between each service connected to the repository. This makes it possible to protect information and avoid threats such as tapping, falsification, and impersonation.

  - Yes

    SSL communication is performed. The port number specified in [SSL port number] and the SSL configuration specified in [SSL configuration] will be used for communication.

  - No (Default setting)

    SSL communication is not performed.

  Only the [SSL Port number] and [SSL configuration] need to be specified if SSL communication is used.

  Enable SSL encryption? can be defined only during repository setup.

  Note

  Since the normal (non-SSL) port will be set up even if "Yes" is specified in [Enable SSL encryption?], protection by the firewall will be needed.

- SSL Port Number

  Specify the port number (between 1 and 65535) used for SSL communication.

  Specify the port number after designing the port numbers used by each service on the server. The initial value is "636."

  Specify this item only if SSL communication is being used. The SSL port number can be specified only when creating a new repository.

  Note

  There is a higher risk of services attempting to use the same ports if a port number other than the initial value is used. This is particularly relevant for port numbers between 1 and 1023 which are commonly-used.

- SSL Configuration

  To conduct SSL communication, specify the SSL definition that has been created.

If no SSL definitions have been created, "None" will be displayed, so create the definitions and then configure the settings again. If SSL definitions have been created, the first SSL definition name (in ascending order) will be selected. If necessary, select an appropriate SSL definition.c file.

- Connection Idle Time

  Specify the period after which connection to the non-communicating client is disconnected. Values can be between 0 and 3600 seconds. The initial time is "900" seconds.

  Specify "0" to set an unlimited connection idle time.

Search Settings

- Maximum Number of Searchable Entries

  Specify the maximum number of entries to be returned after performing a search (between 0 and 10000). The maximum number is unlimited if a search is performed by an Administrator DN. The initial value is "500"

  Specify "0" to set an unlimited maximum number of entries to be retrieved.

- Search Timeout

  Specify the timeout period when performing a search (between 0 and 3600 seconds). The timeout period is unlimited if the search is performed by an Administrator DN. The initial time is "3600" seconds.

  Specify "0" to set an unlimited retrieval processing timeout.

  Point

  Operation when the maximum number of searchable entries and search timeout are specified.

  The maximum number of searchable entries and the search timeout can be defined on the Interstage Directory Service server and the client respectively.

  The client refers to the *ldapsearch* command, Entry Administration Tool, and user applications that access the Interstage Directory Service server.

  The following table shows the relationship between the Interstage Directory Service server and client designations.

Table 5.3 Interstage Directory Service Server and Client Designations

DN accessed from the client (bound DN)	Client specified value	Relationship between server specified value and client specified value	Operation
Administrator DN	Present	Client < Server	Client specified value is valid
	Present	Client >= Server	Client specified value is valid
	None	-	Unlimited
	0	-	Unlimited
Others	Present	Client < Server	Client specified value is valid
	Present	Client >= Server	Server specified value is valid
	None	-	Server specified value is valid
	0	-	Server specified value is valid

The following shows how to specify the maximum number of searchable entries and search timeout on the client:

- *ldapsearch* command

  -l option (search time limit) and -z option (search size limit) of "ldapsearch" in Reference Manual (Command Edition).

- Entry Administration Tool

  "Entry Administration Tool" > "Operate Entry" > "Search Entry/Attribute" > "Specify search option" in the Entry Administration Tool Help

- User applications (C APIs)

  LDAP_OPT_SIZELIMIT and LDAP_OPT_TIMELIMIT in "Interface for Session Handle Option Settings/Reference" in the "C Interface" chapter of the Reference Manual (API Edition).

Access Log Settings

- Output Access Log?

  Specify whether to output the access log. The default value is "Yes".

  - Yes

    Outputs the access log.

  - No

    The access log will not be output.

  If the access log is unnecessary, there is no need to set values for [Output types], [Access log storage directory], [Rotation type], [Size], and [Number of access log files to maintain].

- Output Type

  Specify the output content of the access log. If output the access log has been selected, at least one output level must be specified. "Client requests" and "Server errors" are set in the state of the initial stage.

  - Client requests

    Outputs request information from the client.

  - Server errors

    Outputs error responses of the server.

  - Normal Server responses

    Outputs normal responses of the server.

  - Server search result of DN

    Outputs search result responses of the server.

- Access Log Storage Directory

  Enter the access log storage directory of the access log using the full specification. Be sure to specify this item if access logs are to be output.

  The actual access log storage directory of the access log is a directory defined by appending "/repository_name/log" (for Windows(R), "\repository_name\log") to the specified access log storage directory.

Table 5.4 Valid Access Log Storage Directory Characters

	Windows32/64	Solaris32/64	Linux32/64
Length	Up to 192 bytes	Up to 960 bytes	Up to 960 bytes
Valid character	En-size alphanumeric character Dollar sign ($) Ampersand (&) Single quotation mark (') Plus sign (+) Minus sign (-) Period (.) Equals sign (=) at sign (@)	En-size alphanumeric character Slash (/) Minus sign (-) Underline (_) Tilde (~)	En-size alphanumeric character Slash (/) Minus sign (-) Underline (_) Tilde (~)

	Underline (_) Back quotation mark (`) Tilde (~) Square bracket ([]) Brace ({}) Space ( ) Colon (:) Slash (/) Backslash (\)		

The multi-byte code system cannot be used. In Windows®, the colon (:) can be used only when specifying a drive character and the backslash (\) can be used only to separate directories. When specifying a drive, include "\" for example, "C:\"

The initial values are as follows:

Windows32/64

```
"C:\Interstage\IREP\var" (default installation path)
```

Solaris32/64 Linux32/64

```
"/var/opt/FJSVirep"
```

Always specify this item.

Note

- Set the access log storage directory after ensuring that sufficient disk space is available.
- Note the Permissions settings when any access log storage directory other than the initial value is set.

Windows32/64

When specifying an access log storage directory other than the default value, give the "Administrators" group full control access to all directories within the access log storage directory.

- Rotation Type

  Specify how to split the access log. If the log reaches the maximum size, the number of files set in [Number of access log files to maintain] will be saved. The default value is "Size".

  - Size

    Rotation in file size

  - Daily

    Rotation in days

  - Monthly

    Rotation in months

- Size

  Specify the maximum size of the access log between 1 and 1024 MB. Be sure to specify this item if access logs are to be output. If the log reaches this size, the number of files set in [Number of access log files to maintain] will be saved. The initial value is "5" MB.

- Number of Access Log Files to Maintain

  Specify the number of access log files between 1 and 99. Be sure to specify this item if access logs are to be output. If this number is exceeded, the access logs will be deleted in order of date. The initial value is "2."

Replication Settings

- Operation Mode

  Specify the operating mode with regards to replication. The operating mode must be specified for each host. The default value is "Stand-alone".

  - Stand-alone

    Operated on a stand-alone basis. No replication operation is performed.

  - Slave

    Operated as a slave.

  - Master

    Operated as the master.

  Note

  Once the operating mode is set to "Slave" or "Master," it cannot be changed to another mode.

Slave Operation Settings

- Master Host Name

  Specify the host name of the master using a string of up to 106 bytes. Only host names that can be address-resolved are valid. Allowable characters include en-size alphanumeric characters, the minus sign (-), the period (.), and the underline (_). No initial value is provided.

  When performing a cluster operation, specify the host names of the operation and standby nodes separated by a comma (,) in a string of up to 106 bytes. For example, "cluster01, cluster02." The same host name cannot be specified as both the operation node and standby node.

  This item can be specified only when "Slave" is specified in [Operation mode].

  For details of restarting the Interstage Management Console, refer to the "Configuring the Interstage Management Console" chapter of the Operator's Guide.

Master Operation Definition (Replication Connection Settings)

- Host Name

  Specify the host name of the slave specified in advance using a string of up to 106 bytes. Only host names that can be address-resolved are valid. Characters that can be used include en-size alphanumeric characters, the minus sign (-), the period (.), and the underline (_). No initial value is provided.

  When performing a cluster operation of the slave, specify the logical host name in the cluster environment.

  The host name can be specified only when adding [Replication connection settings].

  For details of restarting the Interstage Management Console, refer to the "Configuring the Interstage Management Console" chapter of the Operator's Guide.

- Port Number

  Specify the port number for replication of the slave between 1 and 65535. The initial value is "389."

  The port number can be specified only when adding [Replication Connection Settings].

- Enable SSL Encryption?

  Specify whether SSL will be used with the port number specified for replication of the slave. "No" is set by default.

  Enable SSL encryption? can be specified only when adding [Replication Connection Settings].

  - Yes

    SSL communication performed. Specify whether to present the client certificate in [Present client certificate?].

  - No

    SSL communication is not performed.

  If SSL communication is not going to be used, there is no need to specify [SSL configuration] and [Present client certificate?].

  To use SSL communication with the port number specified in for replication of the slave, "Yes" must always be specified.

- Present Client Certificate?

  When using the SSL communication with the port number specified for replication of the slave, select to present the client certificate?. "No" is set by default.

  - Yes

    A client certificate needs to be presented when conducting SSL communication. Specify the client certificate to be presented in [SSL configuration].

  - No

    No client certificate needs to be presented when conducting SSL communication.

  If "No" is selected, the contents of [SSL configuration] will be invalidated.

  If "Authenticate (Always authenticate a client certificate)" is specified in [Client authentication] of the environment settings of the SSL configuration specified for the slave, "Yes" must always be specified.

  This setting must be specified if "Yes" is selected in [Enable SSL encryption?] when adding [Replication Connection Settings].

  Note

  If any client certificate is installed in the Interstage certificate environment, the client certificate will be presented even if "No" is selected.

- SSL Configuration

  To conduct SSL communication that presents the client certificate, create an SSL configuration in which the client certificate is specified and then specify the created SSL configuration.

  If "Authenticate (Always authenticate a client certificate)" is specified in [Client authentication] of the environment settings of the SSL configuration specified for the slave, the SSL configuration must always be specified.

  This setting must be specified if "Yes" is specified in [Enable SSL encryption?] when adding [Replication Connection Settings] and "Yes" is specified in [Present client certificate].

- DN for the Connection

  Specify, in a string of up to 512 bytes, the "Administrator DN (distinguished name)" for connecting to the slave. The public directory will be added to the specified DN (distinguished name) for connection.

  "cn", "ou", "o", "c", "l", and "dc" can be specified as an attribute of the RDN (relative distinguished name), which uses DN (distinguished name) format.

  Alphanumeric characters, the minus sign (-), the period (.), and the underline (_) can also be specified for an attribute value of the RDN (relative distinguished name) which comprises the DN (distinguished name) format.

  Insert the equal sign (=) between the specified attribute name and attribute value of the RDN (relative distinguished name), which composes DN (distinguished name) format.

  If multiple RDN (relative distinguished name) are specified, separate them with a comma (,). For example, "cn=manager" and "cn=manager, ou=managergroup". The initial value is "cn=manager",

  [DN for the connection] can be specified only when adding "Replication Connection Settings".

  Note

  It is not possible to specify multiple attributes for the RDN (relative distinguished name) of the DN for connection (Multi-AVA cannot be used). For example, multiple attributes cannot be specified by using the plus sign (+) like "cn=User001+sn=fujitsu".

- Password for the Connection

  Specify (using a string of up to 128 bytes) the password of the "DN (distinguished name) for manager" for the slave as a password for connecting to the slave. Valid characters include alphanumeric characters, the comma (,), the plus sign (+), the equals sign (=), the minus sign (-), the period (.), and the underline (_). No initial value is provided.

5.3 Extending Schemas

Schema definitions can be extended using the following procedure:

1. 5.3.1 Design the Schema Definitions
2. 5.3.2 Define User-defined Schemas
3. 5.3.3 Register User-defined Schemas

An attribute or object class that is extended in a user-defined schema can be specified in LDIF or CSV file format and used, in the same way as attributes and object classes already defined in standard schemas. For details about using LDIF files, refer to "5.5.1.1 LDIF Standard Format" or "5.5.1.2 LDIF Modification Format". For details about using CSV files, refer to "5.5.2.1 CSV and Rule Files",

5.3.1 Design the Schema Definitions

When new schemas are defined, Fujitsu recommends inheriting (deriving) the existing schema definitions provided by the Interstage Directory Service and using auxiliary classes (explained below).

Refer to "Object Class Types (Optional)" for information on auxiliary classes.

5.3.1.1 Acquiring Object Identifiers (OIDs)

Object identifiers (OIDs) are unique numbers in a one-to-one relationship with each object class or attribute. OIDs must be acquired when new schemas are defined, they cannot be made up. Each schema element is identified by a globally unique OID.

OIDs are issued by an issuing organization such as the International Organization for Standardization (ISO).

OIDs can be subdivided hierarchically if necessary, so if an OID has already been allocated to the enterprise or organization to which the user belongs, it can be subdivided within the organization. Check whether an OID has been allocated to the user's organization. OID allocation can be checked on the Internet Assigned Numbers Authority (IANA) Web site (http://www.iana.org/cgi-bin/enterprise.pl). If an OID has not been allocated to the user's organization, apply for an OID through the registration system provided by a private company managed by IANA. OIDs can be registered free of charge.

Obtain an enterprise/organization code in this way, and then allocate OIDs using the following format.))

Format: a.b.c.d.e.f.g.h.i

<OID Regulations>

a: 1 (Fixed. Represents the ISO)

b: 2 (Fixed. Represents the member-body)

c: 392 (Fixed. Represents Japan. (The US is 840))

d: Represents the enterprise code.

e: 65 (Fixed. Represents "Directory Service")

f: 0 (Arbitrary, but the fixed value "0" is used)

g: 0 (Arbitrary, but the fixed value "0" is used)

h: 1 or 2 ("1 for object class or "2" for attribute))

i: Serial number for each object class or attribute

5.3.1.2 Selecting Name Prefixes

As well as allocating unique OIDs to each individual schema element, each element must be given at least one name. This name must not be the same as any other schema element. In particular, take care not to duplicate any names that are currently standardized or that may be standardized in the future.

To reduce the likelihood of names being duplicated, adopt a convention, such as the use of a prefix for names to indicate changes local to the organization. Fujitsu recommends using a prefix such as "comFujitsu" (for elements relating to the organization where the domain is "fujitsu.com".)

5.3.2 Define User-defined Schemas

Edit the user-defined schema file using a text editor. The Interstage Directory Service provides a sample file so that new schema definitions can be entered. The sample file can be found at the following location:

Windows32/64

```
C:\Interstage\IREP\sample\schema\schema.txt
```

Solaris32/64 Linux32/64

```
/opt/FJSVirep/sample/schema/schema.txt
```

5.3.2.1 File Format

The format for user-defined schema files is shown below. User-defined schema files are made up of attribute types (attributetype) and object classes (objectclass).

```
# attribute

attributetype ( 1.1.2.1.1
                NAME 'skill'
                DESC 'skill'
                EQUALITY caseIgnoreMatch
                SUBSTR caseIgnoreSubstringsMatch
                SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

# objectclass

objectclass ( 1.1.2.2.2
                NAME 'myPerson'
                DESC 'my person'
                SUP inetOrgPerson
                MUST ( employeeNumber )
                MAY skill )
```

- Comment lines

  Lines that start with a hash sign (#) are treated as comments.

- Definition statements

  Separate each item with a space. Lines that start with a space are treated as continuing from the preceding line. Do not put a space at the start of line 1. Make line 1 a comment line or a definition statement.

- Blank lines

  Blank lines separate definition information. (The sections before and after blank lines are regarded as separate definitions.)

- Multi-byte characters

  Comment lines and definition statements cannot include multi-byte characters such as Japanese.

- Comment lines and definition statements cannot be longer than 1,024 bytes per line, regardless of whether they are continued lines.

5.3.2.2 Attribute Type Definitions

Use the following format to define new attribute types.

```
attributetype (
    OID for attribute type
    NAME 'name of attribute type'
    [DESC 'description']
    [SUP superior attribute type]
    [EQUALITY matching rules for equality]
    [ORDERING matching rules for ordering]
    [SUBSTR matching rule for substring matches]
    [SYNTAX attribute syntax]
    [SINGLE-VALUE] )
```

Separate each item with a blank character.

A single definition can be split over multiple lines. If a line starts with whitespace followed by a continuation of the definition, the line will be regarded as a continuation of the previous line.

Blank lines are regarded as definition separators.

Example: The definition below is for the ssoRoleName attribute. (There is already a definition for this attribute, so it cannot be added.)

```
attributetype (
    1.2.392.200001.65.1.8.4.0
    NAME 'ssoRoleName'
    EQUALITY caseIgnoreMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{32} )
```

OID for Attribute Type (Required)

This is the OID for the attribute type. Ensure that you specify this item.

NAME 'name of attribute type' (Required)

Specify the name of the attribute type, enclosed in single quotes. Ensure that you specify this item using alphanumeric characters with a total maximum of up to 32 bytes. Multi-byte characters cannot be used. Multiple names can be specified, however, separate each name with spaces and enclose them in parentheses. When the repository returns results, the first name in the definition will be returned.

DESC 'description' (Optional)

Enter a simple description for the attribute type, enclosed in single quotes. The description can be no longer than 1,024 bytes.

SUP Superior Attribute Type (Optional)

This attribute is the base for the definition of the attribute being defined (i.e., this attribute is the higher-order attribute from which the attribute being defined is derived). The attribute being defined inherits the attribute syntax and matching rules from its superior attribute type.

Use this attribute to define a new attribute type by extending the definition of an existing attribute.

If this attribute is not specified, the attribute type being defined will not have a superior attribute, and therefore must have an attribute syntax. If this attribute is omitted, the attribute syntax must be specified.

EQUALITY Matching Rules for Equality (Option)

The following matching rules specify the situations in which values will be regarded as equal, and are used when checking for equality in searches.

Name	Explanation	Attribute syntax that can be applied
objectIdentifierMatch	This rule compares equality for attribute values that meet the "OID" syntax. For name strings, this rule does not distinguish case for alphabetic characters, and values are regarded as equal if the targets that they refer to are equivalent.	OID
distinguishedNameMatch	This rule parses the attribute value according to the rule for the "DN" syntax, ignoring any whitespace on either side of commas (,), plus signs (+) or equals signs (=), and then compares the attribute type section using the "objectIdentifierMatch" rule and the attribute value part using the matching rule for equality that has been defined for the attribute type.	DN
caseIgnoreMatch	This rule makes comparisons by ignoring case for alphabetic characters, ignoring leading and trailing whitespace, and treating continuous whitespace as a single space.	Directory String

Name	Explanation	Attribute syntax that can be applied
caseExactMatch	This rule makes comparisons by distinguishing case for alphabetic characters, ignoring leading and trailing whitespace, and treating continuous whitespace as a single space.	Directory String
numericStringMatch	This rule makes comparisons for "Numeric String" syntax (comprising the numbers 0 to 9 and spaces), ignoring whitespace.	Numeric String
octetStringMatch	Arbitrary octet strings are regarded as equal if they have the same length and all octets match.	Octet String
telephoneNumberMatch	This rule compares equality for attribute values that meet the "Telephone Number" syntax. This matching rule is the same as "caseIgnoreMatch" except that minus signs (-) and all whitespace is ignored.	Telephone Number
caseExactIA5Match	This rule makes comparisons by distinguishing case for alphabetic characters, ignoring leading and trailing whitespace, and treating continuous whitespace as a single space.	IA5 String
caseIgnoreIA5Match	This rule makes comparisons by ignoring case for alphabetic characters, ignoring leading and trailing whitespace, and treating continuous whitespace as a single space.	IA5 String
caseIgnoreListMatch	This rule compares equality for attribute values that meet the "Postal Address" syntax. This rule compares element strings separated by "$" using "caseIgnoreMatch", and regards values as equal if all elements match.	Postal Address
integerMatch	This rule compares equality for attribute values that meet the "INTEGER" syntax.	INTEGER
generalizedTimeMatch	This rule compares equality for attribute values that meet the "Generalized Time" syntax.	Generalized Time

ORDERING Matching Rules for Ordering (Optional)

The following matching rules are applied when greater than/less than relationships are checked during searches and so on.

Name	Explanation	Attribute syntax that can be applied
caseIgnoreOrderingMatch	This rule makes size comparisons using dictionary order by converting lower-case alphabetic characters to upper-case, ignoring leading and trailing whitespace and treating continuous whitespace as a single space.	Directory String
caseExactOrderingMatch	This rule makes size comparisons using dictionary order by distinguishing upper- and lower-case alphabetic characters, ignoring leading and trailing whitespace and treating continuous whitespace as a single space.	Directory String
generalizedTimeOrderingMatch	This rule compares ordering for attribute values that meet the "Generalized Time" syntax.	Generalized Time

SUBSTR Matching Rules for Substring Matches (Optional)

The following matching rules specify the situations in which strings will be regarded as including substrings, and are applied when checking for substring matches during searches.

Name	Explanation	Attribute syntax that can be applied
caseIgnoreSubstringsMatch	This rule checks whether the value presented is a substring of the attribute value, ignoring case for alphabetic characters, ignoring leading and trailing whitespace and treating continuous whitespace as a single space.	Directory String
caseExactSubstringsMatch	This rule checks whether the value presented is a substring of the attribute value, distinguishing case for alphabetic characters, ignoring leading and trailing whitespace and treating continuous whitespace as a single space.	Directory String
caseIgnoreIA5SubstringsMatch	This rule checks whether the value presented is a substring of the attribute value, ignoring case for alphabetic characters, ignoring leading and trailing whitespace and treating continuous whitespace as a single space.	IA5 String
numericStringSubstringsMatch	This rule is the same as "caseIgnoreSubstringMatch" except that all whitespace is ignored.	Numeric String
caseIgnoreListSubstringsMatch	This rule checks substrings against attribute values that meet the "Postal Address" syntax. This rule checks whether the presented value is a substring of the string that contains all of the element strings in the attribute value that are separated by "$".	Postal Address

If matching rules are omitted, only the matching rules for the superior attribute type will be applied. Matching rules are needed in order to perform searches. If they are omitted, ensure that you specify a superior attribute type and define at least one matching rule.

More than one kind of matching rule (for equality, ordering, or substring matches) can be specified for the same attribute, but all of the matching rules must handle case in the same way. For example, "caseIgnore...Match" and "caseExact...Match" cannot be specified at the same time. Note that "caseIgnoreMatch" and "caseIgnoreSubstringMatch" can be specified at the same time, but "caseIgnoreMatch" and "caseExactSubstringMatch" cannot be specified at the same time.

If "caseIgnore...Match" is defined, the case of alphabetic characters will be ignored when values are compared. For example, the "cn" attribute has been defined using the "caseIgnoreMatch" rule. The following search filters will all match.

Example: If there is an entry with "cn: Fujitsu Taro", the following search filters will all match.

```
(cn=Fujitsu Taro)
(cn=FUJITSU TARO)
(cn=fujitsu taro)
(cn=fuJItsU TARo)
```

If "caseIgnore...Match" is defined, the attribute cannot have multiple values that differ only by case. For example, the "cn" attribute has been defined using the "caseIgnoreMatch" rule. Combinations of the following kinds of values cannot be specified together.

Example: cn: Fujitsu Taro

```
cn: FUJITSU TARO
cn: fujitsu taro
```

SYNTAX Attribute Syntax (Optional)

Specify the numerical value for the OID that indicates the format for the attribute value.

If this specification is omitted, the attribute will inherit the attribute syntax for the superior attribute type. In this case, the attribute type must have an attribute syntax. If this option is omitted, be sure to specify the superior attribute type.

OID	Attribute syntax	Explanation
1.3.6.1.4.1.1466.115.121.1.4	Audio	Sound data can be used. (binary type)
1.3.6.1.4.1.1466.115.121.1.5	Binary	Binary data can be used. (binary type)
1.3.6.1.4.1.1466.115.121.1.8	Certificate	Certificate data can be used. (binary type)
1.3.6.1.4.1.1466.115.121.1.9	Certificate List	Certificate list data can be used. (binary type)
1.3.6.1.4.1.1466.115.121.1.10	Certificate Pair	Cross-authentication certificate data can be used. (binary type)
1.3.6.1.4.1.1466.115.121.1.15	Directory String	The range of characters that can be handled by UTF-8 can be used. The characters that can be used are the Unicode range (ISO10646). (string type)
1.3.6.1.4.1.1466.115.121.1.12	DN	DNs can be used. (string type) (Example))cn=User001,o=fujitsu,dc=com Use the following format: "<RDN>,<RDN>,...<RDN>". For each <RDN>, list at least one "<*attribute type*>=<*attribute value*>" pair, separating pairs by "+".Make the specification in one of the ways shown below if an <*attribute value*> includes any of the following characters: = , + < > # ; \ " Escape the character by placing a backslash "\" in front of it. Use the hexadecimal character code following a backslash "\", as in "\34". Enclose the entire attribute value in double quotes (""). (Either escape double quotes and backslashes, or use hexadecimal notation.)
1.3.6.1.4.1.1466.115.121.1.22	Facsimile Telephone Number	Enter numbers in "Telephone Number" format, followed by one of these options. Use a dollar sign ($) to separate the number from the option. (string type) twoDimensional fineResolution unlimitedLength b4Length a3Width b4Width uncompressed
1.3.6.1.4.1.1466.115.121.1.24	Generalized Time	Either local time (either YYYYMMDDhhmmss.p format or YYYYMMDDhhmmss.p(+|-HHMM) format) or international standard time (YYYYMMDDhhmmss.pZ format) can be used. (string type)
1.3.6.1.4.1.1466.115.121.1.26	IA5 String	The CCITT International Alphabet No.5 (equivalent to ASCII characters) can be used. (string type)
1.3.6.1.4.1.1466.115.121.1.27	INTEGER	Decimal notation for integers. (numeric type) (Example)))) 1321
1.3.6.1.4.1.1466.115.121.1.28	JPEG	JPEG data can be used. (binary type)
1.3.6.1.4.1.1466.115.121.1.34	Name And Optional UID	"<*DN*>#<*bit string*>" format string. The "#<*bit string*>" part is optional. (string type)

OID	Attribute syntax	Explanation
1.3.6.1.4.1.1466.115.121.1.36	Numeric String	Numbers (from 0 to 9) and spaces can be used. (string type) (Example) 1997
1.3.6.1.4.1.1466.115.121.1.40	Octet String	Byte strings can be used. (Each byte can be an arbitrary value between 0x00 and 0xFF) (string type)
1.3.6.1.4.1.1466.115.121.1.38	OID	OID expressed using integers separated by a dot (.), or name string. For name strings, this must be a string that starts with a letter, and consists of letters, numbers, hyphens or semicolons. (string type) (Example) 1.2.3.4
1.3.6.1.4.1.1466.115.121.1.39	Other Mailbox	Electronic mailbox data other than X.400 and RFC822 can be used. The format is as follows. (string type) mailbox-type "$" mailbox In this example, "mailbox-type" indicates the type of mail, and "mailbox" indicates the mail address (e.g., user001@interstage.fujitsu.com)
1.3.6.1.4.1.1466.115.121.1.41	Postal Address	The range of characters (Unicode) that can be handled by "Directory String" can be used. (string type) (Note) If only alphanumeric characters are used, the format is as follows. Also, up to six "dstring" can be combined. postal-address = dstring *("$" dstring) " dstring = 30 alphanumeric characters Example) 1234 Main St.$Anytown, CA 12345$USA \241,000,000 Sweepstakes$PO Box 1000000$Anytwon, CA 12345$USA"
1.3.6.1.4.1.1466.115.121.1.44	Printable String	Alphanumeric characters and the following symbols can be used. (string type) Space ( ) Single quotation mark (') Left parenthesis (( ) Right parenthesis ( )) Plus sign (+) Comma (,) Minus sign (-) Period (.) Slash (/) Colon (:) Equals sign (=) Question mark (?)
1.3.6.1.4.1.1466.115.121.1.49	Supported Algorithm	Syntax for the "supportAlgorithm" attribute (binary type)
1.3.6.1.4.1.1466.115.121.1.50	Telephone Number	The characters that can be used are the same as for "Printable String" (string type)

OID	Attribute syntax	Explanation
		Note: If spaces or minus signs (-) are used, searches will work as shown in the following example. If "telephoneNumber=0123456789" is used in a search: 012-345-6789 123456789 Both telephone numbers will match the search conditions.
1.3.6.1.4.1.1466.115.121.1.52	Telex Number	Telex numbers can be used. The format is as follows. (string type) actual-number "$" country "$" answerback In this example, "actual-number" expresses the number part of an encrypted telex number syntactically, "country" indicates the country code for the telex, and "answerback" indicates the return code for the telex terminal.

The maximum number of characters for string-based attribute syntax values (such as "Directory String"), or the maximum number of bytes of other attribute syntax values can be specified within braces after the OID. The upper limit for the specified values depends on whether detailed settings are made when the table for storing repository data is created, as shown in the following table.

Refer to "Detailed Settings for Tables" for more information about making detailed settings for tables.

Detailed Settings

Type of attribute value	Detailed settings for the table	
	Not made	Made
String type	942 bytes	The value specified in the detailed settings
Numeric type	4 bytes (signed)	Detailed settings cannot be made.
Binary type	32,768 bytes	The value specified in the detailed settings (*1)

*1 Specify the maximum length in bytes, without adding K or M (which can be specified when detailed settings are made). 1 Kbyte is 1024 bytes and 1 Mbyte is 1024 Kbytes.

Example: Specifying a maximum length of 32 bytes

```
1.3.6.1.4.1.1466.115.121.1.15{32}
```

SINGLE-VALUE (Optional)

Specify this option to define attributes that cannot have more than one attribute value.

If this specification is omitted, the attribute will be defined as being able to have multiple attribute values.

5.3.2.3 Defining Object Classes

Use the following format to define new object classes.

```
objectclass (
    Object class OID
    NAME 'object class name'
    [DESC 'description']
    SUP superior object class
    [Object class type (ABSTRACT/STRUCTURAL/AUXILIARY)]
    [MUST mandatory attribute]
    [MAY optional attribute] )
```

Separate each item with a blank character.

A single definition can be split over multiple lines. If a line starts with whitespace followed by a continuation of the definition, the line will be regarded as a continuation of the previous line.

Blank lines are regarded as definition separators.

Example: This definition example is for ssoUser. (This object class has already been defined, and so cannot be added.)

```
objectclass (
    1.2.392.200001.65.1.8.6.0
    NAME 'ssoUser'
    SUP top
    AUXILIARY
    MAY ( ssoRoleName $ ssoAuthType $ ssoCredentialTTL $
          ssoUserStatus $ ssoNotBefore $ ssoNotAfter $
          ssoFailureCount $ ssoLockTimeStamp $ dnQualifier ) )
```

Object Class OID (Required)

This is the OID for the object class. Ensure that you specify this item.

'NAME 'object class name' (Required)

Specify the name of the object class, enclosed in single quotes. Ensure that you specify this item. Specify the name using up to 32 bytes' worth of alphanumeric characters. Multi-byte characters cannot be used.

DESC 'description' (Option)

Specify a simple description for the object class, enclosed in single quotes. The description can be no longer than 1,024 bytes.

SUP Superior Object Class (Required)

This is the object class that is the base of the definition for the object class being defined (i.e., this object class is the higher-order object class from which the object class being defined is derived). The object class being defined inherits the mandatory and optional attributes from its superior object class.

Object Class Types (Optional)

Object classes can be classified as ABSTRACT, STRUCTURAL, or AUXILIARY.

If this specification is omitted, the object class will be defined as STRUCTURAL.

- ABSTRACT

  This object class is prepared to define other object classes."top" is a typical example of this type of object class.

  Entries cannot belong to ABSTRACT object classes only.

- STRUCTURAL

  This object class can be used to create entries. Entries must belong to a STRUCTURAL object class.

- AUXILIARY

  This object class cannot be used to create entries by itself, but can be used together with other STRUCTURAL object classes to create entries. Entries cannot belong to AUXILIARY object classes only.

MUST Mandatory Attribute (Optional)

Specify the names of any attributes that must be registered when this object class is used.

If this specification is omitted, the only mandatory attributes will be the mandatory attributes of the superior object classes.

MAY Optional Attribute (Optional)

Specify the names of any optional attributes that are used for additional information when this object class is used.

If this specification is omitted, the only optional attributes will be the optional attributes of the superior object class.

Multiple attributes can be specified as mandatory attributes or optional attributes. If multiple attributes are specified, separate them with a dollar sign, and enclose them in parentheses.

5.3.3 Register User-defined Schemas

Use the following procedure to reflect user-defined schemas.

1. Stop the repository by selecting [System] > [Service] > [Repository] from the Interstage Management Console.

   In the Interstage Management Console of the Admin Server, click [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository], and stop the repository in the [Repository > View Status] window.

2. Register the user-defined schema file using the command for registering, deleting, and displaying user-defined schema files (irepschema).

3. Start the repository by selecting [System] > [Service] > [Repository] from the Interstage Management Console.

   In the Interstage Management Console of the Admin Server, click [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository], and start the repository in the [Repository > View Status] window.

Refer to "*irepschema*" in the "Interstage Directory Service Operation Commands" chapter of the Reference Manual (Command Edition) for more information on the command for registering, deleting, and displaying user-defined schemas.

5.4 Registering Access Control Lists

The procedure for registering access control lists is shown below.

Refer to the "Access Control for the Interstage Directory Service" chapter of the Security System Guide for more information about how to design access control lists and define access control list definition files.

1. Stop the repository by selecting [System] > [Service] > [Repository] from the Interstage Management Console.

   In the Interstage Management Console of the Admin Server, click [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository], and stop the repository in the [Repository > View Status] window.

2. Register an access control list definition file using the command for registering and displaying access control list definition files (irepacl).

3. Start the repository by selecting [System] > [Service] > [Repository] from the Interstage Management Console.

   In the Interstage Management Console of the Admin Server, click [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository], and start the repository in the [Repository > View Status] window.

Refer to "*irepacl*" in the "Interstage Directory Service Operation Commands" chapter of the Reference Manual (Command Edition) for more information about the command for registering and displaying access control list definition files.

5.5 Creating Data

To register entry data (user information) in the repository that has been created, either of the two data formats below can be selected, depending on the type of operation and the amount of user information to be registered.

- LDAP Data Interchange Format (LDIF)

  LDIF is a standard format for entering directory entries in text format, and is defined by RFC2849. A file is created using LDIF (an LDIF file) and entries are registered in the repository as a batch.

- CSV file

  This method is suitable when user information is controlled in one place (for example, in a personnel database).

  Large amounts of user information are added to the repository using a CSV file, which is extracted from the source of the information (in this example, the personnel database). When information needs to be updated, for example to accommodate personnel changes and new recruits, a CSV file extracting only the new information is used to update the repository.

5.5.1 Using the LDAP Data Interchange Format (LDIF)

The following types of LDIF are available:

1. Standard format to describe entry information.

   Use this format to save time if a large number of entries needs to be added to the repository

2. Modification format to describe modification information of entries.

   Use this format to change entry information in the repository.

The sample LDIF file provided by the Interstage Directory Service is stored in the following location. LDIF files can be created easily by adapting this sample LDIF file and adding entries and changing information.

Windows32/64

```
C:\Interstage\IREP\sample\ldif\
```

Solaris32/64 Linux32/64

```
/opt/FJSVirep/sample/ldif/
```

- LDIF file sample to add an entry: addldif.txt
- LDIF file sample to delete an entry: delldif.txt
- LDIF file sample to modify an entry: modldif.txt
- LDIF file sample to change the entry name: nameldif.txt

5.5.1.1 LDIF Standard Format

The following explains the standard format to describe entry information.

For the object classes and attributes described in the examples, refer to "List of Objects" in the "Interstage Directory Service Object Classes" appendix and "List of Attributes" in the "Interstage Directory Service Attributes" appendix respectively.

Example: Standard format of described two entries

```
version: 1
# First entry

dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: User001
sn: Fujitsu

# Second entry

dn: cn=User002,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: User002
sn: Fujitsu
```

- version line

  In the first line of the LDIF file, specify the version of LDIF. If it is omitted, Version 1 is used by default. Specify Version 1 to use for the repository.

  1: Function specified by RFC2849

  0: LDIF function used by ldap-3.3 of the Michigan University

- Comment line

  A line starting with '#' is ignored as a comment line.

- Entry information

  Entry information consists of one or more entries. Each entry is separated by inserting one blank line. Each entry consists of DN (distinguished name), one or more object classes, and one or more attribute definitions . Describe entry information as shown below:

  ```
  dn: Entry DN
  objectclass: Object class
  objectclass: Object class
  Attribute type: Attribute value
  Attribute type: Attribute value
  ```

  Use the colon ':' to separate dn, objectclass, or the attribute type, and the value in each line. Blanks before and after ':' are ignored. If a binary value is set as an attribute value, no blank may be specified after ':' because it is not a delimiter between the attribute and the attribute value.

- Blank line

  Separates entry information.

  Note

  - If the first line is blank, all lines in the LDIF file are ignored.
  - If blank lines continue, subsequent lines are ignored.

When a Line is Long

If DN or an attribute value is too long, it can be described in multiple lines. In that case, leave the space of one character blank in the head of the next line and start to the sequence of attribute values thereafter to indicate that the new line is continued from the preceding one. If a line starts with a blank character, it is considered to be a continuation line from the preceding line.

Example: When a long attribute value is wrapped around

```
dn: cn=User002,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: User002
sn: Fujitsu
description: She is good at English, German, and French.
 She has experience in overseas assignment.
```

Referencing an Attribute Value from an External File

To specify an external file as an attribute value, describe the command in the following format.

```
Attribute name:< file name   *1
```

*1 Do not insert any blank character between the ':' (colon) and '<' (less than). If there is a blank character between ':' and '<', a string described after ':' will be registered as an attribute value.

The DN cannot read from a file. Only local files can be specified. The file name is not stored in the repository.

The syntax for the path to the file depends on the character encoding. The following example explains how this works when a text file is specified for the "description" attribute.

Convert the character encoding of the file to UTF-8, and specify the path to the file using URL format.

Windows32/64

```
description:< file:///C:\data\utf8.txt
```

Solaris32/64 Linux32/64

```
description:< file:///data/utf8.txt
```

Binary Notations

To specify a binary value as an attribute value, describe it in the following format. To enter values encoded in base 64 directly, use the format described below in the example "Describing Base64-encoded values directly (Part 1)" for attributes listed as "";binary" does not need to be appended' in "Appendix B Interstage Directory Service Attributes". Use the format described below in the example "Describing Base64-encoded values directly (Part 2)" for values listed as "';binary" must be appended' in "Appendix B Interstage Directory Service Attributes".

- Describing Base64-encoded values directly (Part 1)

```
Attribute name:: attribute value (Base64-encoded)
```

- Describing Base64-encoded values directly (Part 2)

```
Attribute name;binary:: attribute value (Base64-encoded)
```

- Specifying external file content

```
Attribute name:< file:///full pathname
```

If external file content is specified as the value of a binary attribute, only the external file content is stored in the repository in the Base64-encoded format. The file name is not stored.

Example: Describing the Base64-encoded values directly

```
dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
cn: User001
sn: Fujitsu
jpegPhoto:: /9j/4AAQSkZJRgABAQEAYABgAAD/2wBDAP////////////////////////
 ////////////////////////////////////////////////////////////wAAL
 CAAIAAgBAREA/8QAHwAAAQUBAQEBAQEAAAAAAAAAAAECAwQFBgcICQoL/8QAt
 RAAAgEDAwIEAwUFBAQAAAF9AQIDAAQRBRIhMUEGE1FhByJxFDKBkaEII0Kxw
 RVS0fAkM2JyggkKFhcYGRolJicoKSo0NTY3ODk6Q0RFRkdISUpTVFVWV1hZW
 mNkZWZnaGlqc3R1dnd4eXqDhIWGh4iJipKTlJWWl5iZmqKjpKWmp6ipqrKzt
 LW2t7i5usLDxMXGx8jJytLT1NXW19jZ2uHi4+Tl5ufo6erx8vP09fb3+Pn6/
 9oACAEBAAA/ADnA6ds9ucjr15Hf65xxX//Z
```

Using Attributes and Object Classes Defined by User-defined Schemas

When attributes and object classes defined by user-defined schemas are used, they can be specified using the same format as attributes and object classes that have already been defined in the standard schema.

Example: Specifying the "myPerson" object class that has been defined by a user-defined schema

```
#myPerson
dn: cn=User1001,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: myPerson
cn: User1001
sn: Fujitsu
employeeNumber: 991001
skill: Interstage Certified Professional
```

5.5.1.2 LDIF Modification Format

The following explains the modification format to describe the change information of entries. In addition to the format described in 'LDIF standard format,' describe the target, type, and content of change.

1. DN of the entry to be changed
2. Change type (changetype line)

   Specify one of the following four types as the change type:

   - add

     Add the entry specified in the dn line to the repository.

   - delete

     Delete the entry specified in the dn line from the repository.

   - modify

     Modify the entry specified in the dn line.

   - modrdn

     Change RDN (relative distinguished name) of the entry specified in the dn line.

   If the changetype line is omitted, the change type is interpreted to mean the following:

   - If the -a option is specified in the ldapmodify command: add
   - If the -a option is not specified in the ldapmodify command: modify

3. Change content

Adding Entries

Specify 'add' in the changetype line and then describe the attribute definition in the subsequent lines.

Example: Adding entries

```
dn: cn=User002,ou=User,ou=interstage,o=fujitsu,dc=com
changetype: add
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: User002
sn: Fujitsu
```

For the object classes and attributes described in the example, refer to "List of Objects" in the "Interstage Directory Service Object Classes" appendix and "List of Attributes" in the "Interstage Directory Service Attributes" appendix respectively.

Deleting Entries

Specify 'delete' in the changetype line

Example: Deleting entries

```
version: 1
dn: cn=User003,ou=User,ou=interstage,o=fujitsu,dc=com
changetype: delete
```

For the object classes and attributes described in the example, refer to "List of Objects" in the "Interstage Directory Service Object Classes" appendix and "List of Attributes" in the "Interstage Directory Service Attributes" appendix respectively.

Modifying Entries

To perform addition, deletion, or replacement on an attribute or attribute value of an entry, specify 'modify' in the changetype line. Specify the change method in the next line.

- add: attribute name

  Add the attribute to the entry specified in the dn line. If the attribute type is already in the entry, the attribute value is added.

- delete: attribute name

  Delete the attribute from the entry specified in the dn line. If there are multiple attribute values to the attribute type, all attribute values are deleted. To delete only one attribute value among the multiple attribute values, describe the attribute name and attribute value in the line following the delete line.

- replace: attribute name

  Replace the attribute of the entry specified in the dn line with the specified value. If the specified entry does not have the specified attribute, the attribute will be created.

If the attribute change type is omitted, the following assumption is made:

- If the -r option is specified in the ldapmodify command: replace
- If the -r option is not specified in the ldapmodify command: add

In the line following the attribute change type line, specify the attribute content to be changed. If duplicate changes are described consecutively, separate them by '-.'

Describe the changes in the following format:

```
dn: Entry DN
changetype: modify
Attribute change type (add|delete|replace): attribute type
Attribute type: attribute value
```

Adding Attribute Values

Specify 'add: attribute-name' in the line directly after 'changetype: modify'.

Example: Adding the mail attribute

```
dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
changetype: modify
add: mail
mail: user001@interstage.fujitsu.com
```

Example: Adding two telephonenumber attributes and one jpegPhoto attribute

Windows32/64

```
dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
changetype: modify
add: telephonenumber
telephonenumber: 7777-1234
telephonenumber: 7777-5678
-
add: jpegPhoto
jpegPhoto:< file:///C:\data\photo\photo.jpg
```

Solaris32/64 Linux32/64

```
dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
changetype: modify
add: telephonenumber
telephonenumber: 7777-1234
telephonenumber: 7777-5678
-
add:jpegPhoto
jpegPhoto:< file:///data/photo/photo.jpg
```

Deleting Attribute Values

Specify 'delete: attribute-name' in the line directly after 'changetype: modify'.

Example: Deleting the description attribute

```
dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
changetype: modify
delete: description
```

Deleting a Specific Attribute Value from Multiple Attribute Values

Specify 'delete' as the attribute change type.

The entry information of User001 looks like the following.

```
dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: User001
sn: Fujitsu
telephonenumber: 7777-1234
telephonenumber: 7777-5678
```

Example: Deleting the telephone number 7777-1234

```
dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
changetype: modify
delete: telephonenumber
telephonenumber: 7777-1234
```

As a result, the entry information of User001 looks like the following.

```
dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: User001
sn: Fujitsu
telephonenumber: 7777-5678
```

Replacing Attribute Values

Specify 'replace' as the attribute change type.

Example: Replacing the mail address user001@fujitsu.com with user001_fujitsu@fujitsu.com

```
dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
changetype: modify
replace: mail
mail: user001_Fujitsu@interstage.fujitsu.com
```

Replacing a Specific Attribute Value Among the Multiple Attribute Values

Delete the target attribute value and then add a new value.

The entry information of User001 looks like the following.

```
dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: User001
sn: Fujitsu
```

```
telephonenumber: 7777-1234
telephonenumber: 7777-5678
```

Example: Replacing the telephone number 7777-1234 with 7777-9001

```
dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
changetype: modify
delete: telephonenumber
telephonenumber: 7777-1234
-
add: telephonenumber
telephonenumber: 7777-9001
```

As a result, the entry information of User001 looks like the following.

```
dn: cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: User001
sn: Fujitsu
telephonenumber: 7777-5678
telephonenumber: 7777-9001
```

For the object classes and attributes described in the example, refer to "List of Objects" in the "Interstage Directory Service Object Classes" appendix and "List of Attributes" in the "Interstage Directory Service Attributes" appendix respectively.

Changing the Identifier of an Entry

Specify 'modrdn' in the changetype line. In the following line, specify the detailed method of changing the entry identifier.

The following two detailed methods of changing the entry identifier are available. Specify them in the following order:

1. newrdn: new RDN
2. deleteoldrdn: (1|0)

To delete an older RDN after changing to a new RDN, specify. '1.' To retain it as an attribute value, specify '0.'

'deleteoldrdn' can be omitted. If it is omitted, older RDN will be deleted.

Describe the identifier change in the following format.

```
dn: Entry DN
changetype: modrdn
newrdn: New RDN
deleteoldrdn: (1|0)
```

Example: Changing RDN of the User002 entry to U002. Fujitsu

```
dn: cn=User002,ou=User,ou=interstage,o=fujitsu,dc=com
changetype: modrdn
newrdn: cn=U002
deleteoldrdn: 1
```

For the object classes and attributes described in the examples, refer to "List of Objects" in the "Interstage Directory Service Object Classes" appendix and "List of Attributes" in the "Interstage Directory Service Attributes" appendix respectively.

Unsupported LDIF Description

The following functions defined in 'RFC2849' (June. 2000) are not supported by Interstage Directory Service:

- Operation on attributes without value

  No attribute without an attribute value can be registered.

- Display format of attribute values that end with a blank character

  Attribute values that end with a blank character are not output in the Base64 format.

- Designation of control

  The control function from LDIF cannot be specified.

- Designation OID

  Attributes specified by OID from LDIF cannot be specified.

- charaset syntax

  The languages used for attribute values cannot be specified.

The following shows some description examples.

Example

```
dn:: b3U95Za25qWt6YOoLG89QWlyaXVz
# dn:: ou=<JapaneseOU>
objectclass: top
objectclass: organizationalUnit
ou:: 5Za25qWt6Yoo
# ou:: <JapaneseOU>
ou;lang-ja:: 5Za25qWt6YOo
# ou;lang-ja:: <JapaneseOU>
ou;lang-ja;phonetic:: 44GI44GE44GO44KH44GG44G2
# ou;lang-ja:: <JapaneseOU_in_phonetic_representation>
ou;lang-en: User
description: Japanese office
```

5.5.1.3 Registering Entry Data Using an LDIF File

The following example shows how to register entry data using the ldapmodify command and an LDIF file.

For the administrator DN and password, specify the administrator DN and password that were set when the repository was created by selecting the [System] > [Service] > [Repository] > [Create a New Repository] tab on the Interstage Management Console. On the Admin Server, select the [Batch Operation] > [Interstage Management Console] > [Interstage Application Server] > [Security] > [Repository] > [Create a New Repository] tab.

Example:

Administrator DN "cn=manager,ou=interstage,o=fujitsu,dc=com"

Administrator DN password admin

Repository host name hostname

Port number 389

Windows32/64 LDIF file C:\Interstage\IREP\sample\ldif\addldif.txt

```
ldapmodify -H ldap://hostname:389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -w admin -a -f C:\Interstage\IREP\sample\ldif\addldif.txt
```

Solaris32/64 Linux32/64 LDIF file /opt/FJSVirep/sample/ldif/addldif.txt

```
/opt/FJSVirepc/bin/ldapmodify -H ldap://hostname:389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -w admin -a -f /opt/FJSVirep/sample/ldif/addldif.txt
```

Refer to the "Interstage Directory Service Operation Commands" chapter of the Reference Manual (Command Edition) for more information about the *ldapmodify* command.

5.5.2 Using CSV Files Extracted from the Database

Once information has been fetched from source data managed in an external database and saved in a CSV file, the data in the CSV file can be used to perform addition, modification and deletion of entries to the database of Interstage Directory Service.

In the CSV file, information required to add, delete, or modify one entry is described in one line. A comma is used as the delimiter for each record (item). Double quotation marks (") should enclose values that include commas.

It is necessary to define the meaning of each item in the CSV file and operations on entries in an XML rule file. To import user information using the CSV file, the rule file must also be specified in the irepmodifyent command.

Some sample files are placed in the following locations.

Windows32/64

```
C:\Interstage\IREP\sample\csv\EN
```

Solaris32/64 Linux32/64

```
/opt/FJSVirep/sample/csv/EN
```

- CSV file sample to add an entry: add.csv
- CSV file sample to delete an entry: del.csv
- CSV file sample to modify an entry: mod.csv
- Rule file sample: rule.xml

The repository setting used by the sample files is as follows:

Repository host name	hostname
Administrator DN password	admin
Others	Use the initial value.

Some LDIF file samples or file samples that can perform the same operations as those of the above CSV file samples are placed in the following locations. Use these files to check processing results.

Windows32/64

```
C:\Interstage\IREP\sample\ldif\
```

Solaris32/64 Linux32/64

```
/opt/FJSVirep/sample/ldif/
```

- LDIF file sample to add an entry: addldif.txt
- LDIF file sample to delete an entry: delldif.txt
- LDIF file sample to modify an entry: modldif.txt

5.5.2.1 CSV and Rule Files

The following section explains the formats that are used for the CSV and rule files.

CSV File

Entry information to be imported is defined as follows only for the 0th item (The item count starts with '0'). Operations on the repository can be specified.

If any value other than the specified values (including the case in which nothing is described) is described for the 0th item, the line is considered to be a comment line.

Contents of the first and subsequent items can be freely defined by specifying a rule file.

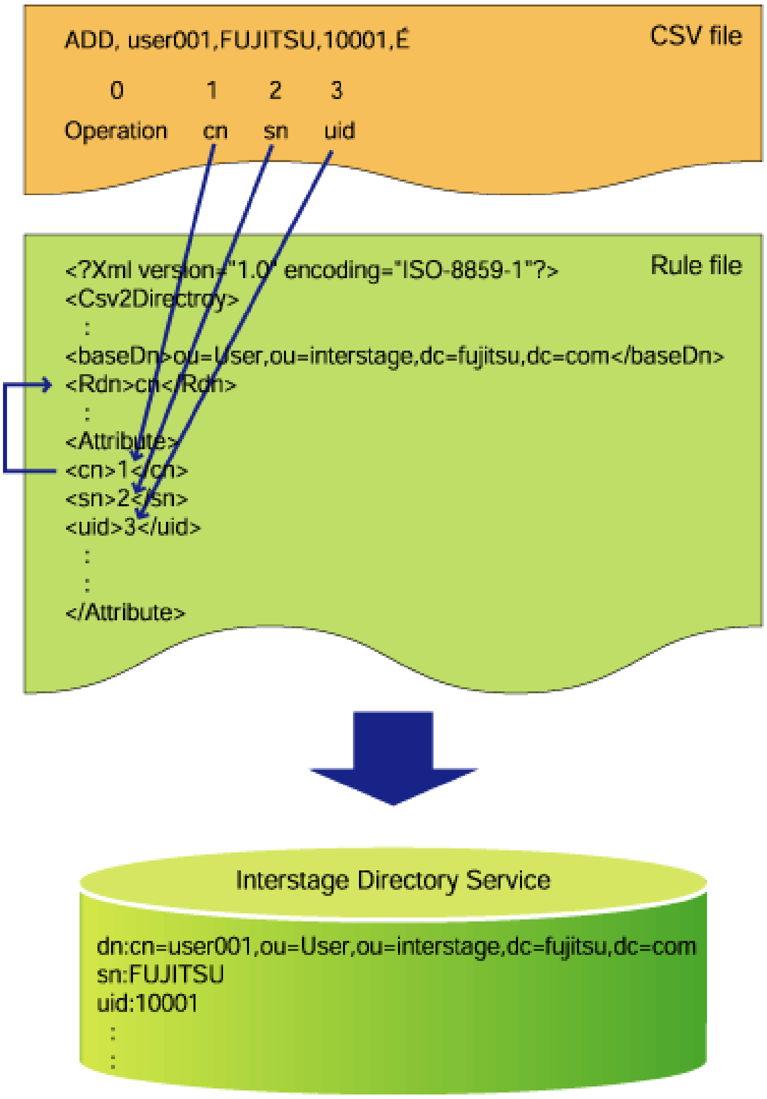
Specified value	Meaning
ADD	Adds an entry.
DEL	Deletes an entry.
MOD	Modifies an entry.

If 'MOD' is specified on an entry that does not exist in the repository, the 'ADD' operation is performed.

Rule File

The rule file is a file that defines the conversion rules used to register (modify and delete) CSV file information in the Interstage Directory Service database. The following figure shows the relationship between the CSV file and rule file.

Figure 5.1 Relationship between CSV and Rule File


CSV file
ADD, user001,FUJITSU,10001,É
0 1 2 3
Operation cn sn uid
Rule file
<?Xml version="1.0" encoding="ISO-8859-1"?>
<Csv2Directroy>
:
<baseDn>ou=User,ou=interstage,dc=fujitsu,dc=com</baseDn>
<Rdn>cn</Rdn>
:
<Attribute>
<cn>1</cn>
<sn>2</sn>
<uid>3</uid>
:
:
</Attribute>
Interstage Directory Service
dn:cn=user001,ou=User,ou=interstage,dc=fujitsu,dc=com
sn:FUJITSU
uid:10001
:
:

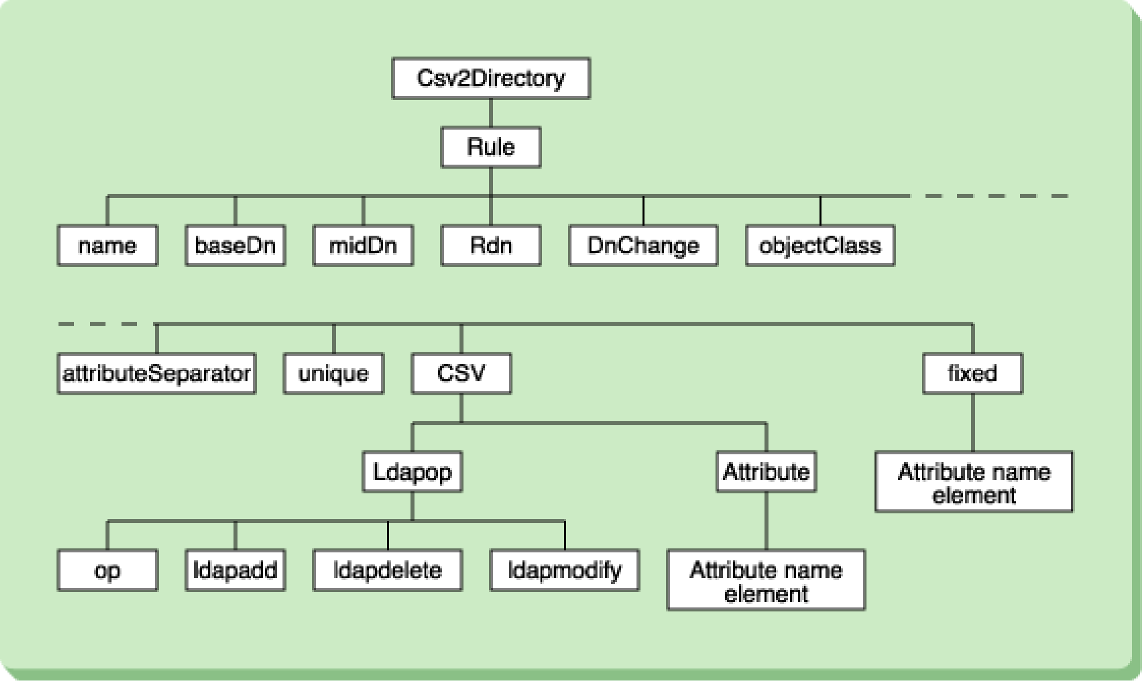
This section explains the rule file format.

Since the following tags describe the XML declaration and DTD (document type definition), they must be included at the beginning of a rule file. It is recommended that tags are used by copying them from the sample file.

```
<?xml version="1.0" encoding="EUC-JP" ?>
<!DOCTYPE Csv2Directory [
<!ELEMENT Rule (name, baseDn, midDn?, Rdn+, DnChange?, objectClass+, attributeSeparator?, unique*,
CSV, fixed?)>
<!ELEMENT CSV (ldapop?, Attribute)>
<!ELEMENT ldapop (op?, ldapadd?, ldapdelete?, ldapmodify?)>
<!ELEMENT name (#PCDATA)>
<!ELEMENT baseDn (#PCDATA)>
<!ELEMENT Rdn (#PCDATA)>
<!ELEMENT objectClass (#PCDATA)>
<!ELEMENT attributeSeparator (#PCDATA)>
<!ELEMENT op (#PCDATA)>
<!ELEMENT ldapadd (#PCDATA)>
<!ELEMENT ldapdelete (#PCDATA)>
!ELEMENT ldapmodify (#PCDATA)>
]>
```

The following explains the elements that constitute a rule file. The following is a configuration diagram of elements.

Figure 5.2 Configuration Diagram of Elements



Note

The following lists the general notes related to the description of a rule file:

- If no value of a tag is specified, the tag can be handled as no tag description.
- The tag name is case-sensitive. However, the attribute name tag, which is an attribute or fixed element, is case-insensitive.
- If the hierarchical position of a tag is correct, the order of occurrence of the tag does not matter. Conversely, if the description of the hierarchical position of a tag is incorrect, the tag will be ignored.
- If any tag other than those tags needed (element and attribute name tags explained above) for the description of a rule file is described, the tag will be ignored.
- The tags and values in the ldapop tag hierarchy and below are fixed. Do not change them. Do not move or copy them to other locations. If any of them is changed, no guarantee of operation can be provided.
- If two tags with the same name are described at different locations and they are in the same hierarchical position, they will be processed together.

The following explains each element.

Csv2Directory

Settings

No setting

Required or Optional

Required

This element can be set only once.

Lower Element

Rule

Rule

Settings

No setting

Required or Optional

Required

Upper Element

Csv2Directory

Lower Element

name, baseDn, midDn, Rdn, DnChange, objectClass, attributeSeparator, unique, CSV, fixed

name

Settings

This value does not affect command execution. Use the sample description as is.

Initial Value

None

Required or Optional

Required

This element can be set only once.

Upper Element

Rule

baseDn

Settings

Enter the base DN during entry operation in the DN format.

Initial Value

None

Required or Optional

Required

This element can be set only once.

Upper Element

Rule

midDn

Settings

If the target entry is not immediately below the base DN, specify an intermediate RDN for remedy in the DN format.

Initial Value

None

Required or Optional

Optional

This element can be set only once.

Upper Element

Rule

Rdn

Settings

Specify the attribute name to be the RDN of an entry. Depending on the Attribute element description, RDN may not be uniquely identified by the attribute name. In such a case, specify the item number of the CSV file. Item numbers cannot be concatenated using '+.'

It is invalid to specify duplicate values.

Initial Value

None

Required or Optional

Required

This element can be set more than once.

Upper Element

Rule

DnChange

Settings

Specify 1 if a DN change is considered to be a move. In this case, older (original) entries will be deleted when a DN is changed. If any value other than 1 is entered, only new entries will be created and older (original) entries will not be deleted.

Initial Value

1

Required or Optional

Optional

This element can be set only once.

Upper Element

Rule

objectClass

Settings

Specify objectClass to be specified for an entry. It is invalid to specify duplicate values.

Initial Value

None

Required or Optional

Required

This element can be set more than once.

Upper Element

Rule

attributeSeparator

Settings

Enter the separator character to be used for concatenating items when mapping from the CSV file. Optional strings may be specified. If multiple separators are entered, the separator specified first is adopted.

Initial Value

None

Required or Optional

Optional

Upper Element

Rule

unique

Settings

Specify the attribute to be checked for uniqueness under the base DN. Depending on the Attribute element description, the attribute may not be unique. In such a case, specify the item number of the CSV file. Item numbers cannot be concatenated using '+.'

Initial Value

None

Required or Optional

Optional

This element can be set less than twice.

Upper Element

Rule

CSV

Settings

No setting

Initial Value

None

Required or Optional

Required

Upper Element

Rule

Lower Element

Ldapop, Attribute

Ldapop

Settings

No setting. This tag is fixed. Do not change its hierarchical position.

Initial Value

None

Required or Optional

Optional

Upper Element

CSV

Lower Element

op, ldapadd, ldapdelete, ldapmodify

op

Settings

This is the item position of the CSV file that determines the operation type of entries. The first line is counted as the 0th line. This tag is fixed. Do not change its hierarchical position and value.

Initial Value

0

Required or Optional

Optional

This element can be set only once.

Upper Element

Ldapop

ldapadd

Settings

Specify a string to instruct entry addition. This tag is fixed. Do not change its hierarchical position.

Example: ADD

If, in this case, 'ADD' is described in the item position of the CSV file specified by the op element, entry addition is performed with information in the line.

A duplicate value must not be specified to the ldapadd, ldapdelete, and ldapmodify elements.

Initial Value

ADD

Required or Optional

Optional

This element can be set only once.

Upper Element

Ldapop

ldapdelete

Settings

Specify a string to instruct entry deletion. This tag is fixed. Do not change its hierarchical position.

Example: DEL

If 'DEL' is included in the item position of the CSV file specified by the op element, entries specified in the line after the word DEL are deleted.

A duplicate value must not be specified to the ldapadd, ldapdelete, and ldapmodify elements.

Initial Value

DEL

Specifiable Count

Required or Optional

Optional

This element can be set only once.

Upper Element

Ldapop

ldapmodify

Settings

Specify a string to instruct entry modification. This tag is fixed. Do not change its hierarchical position.

Example: MOD

In this case, 'MOD' is described in the item position of the CSV file specified by the op element, entries specified in the line followed by the word MOD are modified.

A duplicate value must not be specified to the ldapadd, ldapdelete, and ldapmodify elements.

Initial Value

MOD

Required or Optional

Optional

This element can be set only once.

Upper Element

Ldapop

Attribute

Settings

An attribute and the item position of the CSV file are associated by any element. Specify the attribute name to be set as a string of tags. For example, <cn>1</cn>.

Specify, as a lower element of this element, the attribute name element to be added to an entry or to be modified. The attribute name to be set must be variable. Specify, as a lower element, the item position of the target item in the CSV file by starting to count the item with 0. It is also possible to specify multiple items by concatenating them by '+.' Example: <description>8+1</description>

If the CSV file has more items than the maximum value of the item position set by the Attribute tag, the CSV file items exceeding the maximum number will be ignored.

If the CSV file has less items than the maximum value of the item position set by the Attribute tag, the lacking items are considered to have no corresponding values.

Initial Value

None

Required or Optional

Required

Upper Element

CSV

Lower Element

The name of an attribute to be added to an entry or to be modified is defined as a lower element name. Specify a lower element name whose attribute value is variable.

Example: <cn>1</cn>

fixed

Settings

A fixed value can be set for an attribute by any element. Specify the attribute name as a string of the tag.

As a lower element of this element, the attribute name element to be added to an entry or to be modified. The attribute name must be a fixed value.

Initial value

None

Required or Optional

Optional

This element can be set only once.

Upper element

Rule

Lower Element

The name of an attribute to be added to an entry or to be modified is defined as a lower element name. Specify a lower element name whose attribute value is fixed.

Example: <o>fujitsu</o>

If the same attribute name as that of a lower element of the Attribute tag is specified, precedence is given to the name of the lower element of the fixed tag.

5.5.2.2 Adding, Deleting, and Modifying Entries Using the CSV file

Example of Adding Entries

The following section gives examples of adding user information entries.

For the object classes and attributes described in the example, refer to "List of Objects" in the "Interstage Directory Service Object Classes" appendix and "List of Attributes" in the "Interstage Directory Service Attributes" appendix respectively.

Adding User Information Entries

The following examples illustrate how user information entries are added to the repository by associating the CSV file data with the user entry attributes listed below.

Table 5.5 CSV File Data

Item position	Item name	Attribute name
1	common name	Cn
2	Family name	Sn
3	Given name	givenName
4	User ID	Uid
5	Password	userPassword
6	Employee number	employeeNumber
7	E-mail address	Mail

CSV File

Specify 'ADD' in the 0th item position. In the subsequent item positions, according to the table above, describe the information to be added.

Example: CSV file for adding user information entries

```
ADD,User001,Fujitsu,user001,user001,u5zMEqXX,10001,user001@interstage.fujitsu.com
ADD,User002,Fujitsu,user002,user002,iyaBWF09,10002,user002@interstage.fujitsu.com
ADD,User003,Fujitsu,user003,user003,YNY62GCO,10003,user003@interstage.fujitsu.com
ADD,User004,Fujitsu,user004,user004,mfQShkEK,10004,user004@interstage.fujitsu.com
ADD,User005,Fujitsu,user005,user005,9pcurysl,10005,user005@interstage.fujitsu.com
ADD,User006,Fujitsu,user006,user006,JqzLhqI6,10006,user006@interstage.fujitsu.com
*1
```

*1 Each entry is describe in one line.

Rule File

Describe the Attribute tag in the ordering of each item in the CSV file.

If all entries to be added have the same attribute type and attribute value, the description in the CSV file can be reduced by adding the fixed tag.

Example: Rule file for adding user information entries

```
<?xml version="1.0" encoding="EUC-JP" ?>
<!-- Prohibit corrections -->

<!DOCTYPE Csv2Directory [
<!ELEMENT Rule (name, baseDn, midDn?, Rdn+, DnChange?, objectClass+,
attributeSeparator?, unique*, CSV, fixed?)>
<!ELEMENT CSV (ldapop?, Attribute)>
<!ELEMENT ldapop (op?, ldapadd?, ldapdelete?, ldapmodify?)>
<!ELEMENT name (#PCDATA)>
<!ELEMENT baseDn (#PCDATA)>
<!ELEMENT Rdn (#PCDATA)>
<!ELEMENT objectClass (#PCDATA)>
<!ELEMENT attributeSeparator (#PCDATA)>
<!ELEMENT op (#PCDATA)>
<!ELEMENT ldapadd (#PCDATA)>
<!ELEMENT ldapdelete (#PCDATA)>
<!ELEMENT ldapmodify (#PCDATA)>
]>
<!-- Prohibit corrections -->

<Csv2Directory>
    <Rule>
        <name>rule</name>

<!-- Define baseDn (required)-->

        <baseDn>ou=User,ou=interstage,o=fujitsu,dc=com</baseDn>

<!-- Define RDN (required/multiple RDN allowed/duplicate RDN not allowed) -->
<!-- Enter either a unique number or attribute name -->

        <Rdn>cn</Rdn>

<!-- Whether a DN change is considered to be a move (optional)-->
<!-- Specify 1 if considered so -->

        <DnChange>1</DnChange>
        <objectClass>top</objectClass>
        <objectClass>person</objectClass>
        <objectClass>inetOrgPerson</objectClass>

<!-- Delimiter when an attribute value consists of multiple CSV items (optional) -->
<!-- One blank character if not to be specified -->
<!-- The blank character cannot be specified -->

        <attributeSeparator>-</attributeSeparator>

<!-- Specify attributes that are not allowed duplication under baseDn -->
<!-- Enter either unique numbers or attribute names -->
<!-(optional/multiple attributes allowed/duplicate attributes not allowed) -->

        <unique>uid</unique>

        <CSV>
<!-- Operation (add/delete/change) on the repository and CSV position (optional) -->
```

```
<!-- If the operation method is described in the 0th position -->

            <ldapop>
                <op>0</op>
                <ldapadd>ADD</ldapadd>
                <ldapdelete>DEL</ldapdelete>
                <ldapmodify>MOD</ldapmodify>
            </ldapop>

<!-- Associate items of CSV and entry attributes (optional)-->

            <Attribute>
                <cn>1</cn>
                <sn>2</sn>
                <givenName>3</givenName>
                <uid>4</uid>
                <userPassword>5</userPassword>
                <employeeNumber>6</employeeNumber>
                <mail>7</mail>
            </Attribute>
        </CSV>

<!-- Define items that can be set as fixed values (optional)-->

        <fixed>
            <postalCode>105-7123</postalCode>
            <postalAddress>1-5-2 Higashi-Shimbashi Minato-ku</postalAddress>
            <st>Tokyo</st>
            <o>fujitsu</o>
        </fixed>
    </Rule>
</Csv2Directory>
```

Example of Using the irepmodifyent Command

```
irepmodifyent -h hostname -p 389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -r rule.xml -i add.csv   *1
```

*1 Make an entry in one line without starting a new line.

Example of Deleting Entries

The following example shows how to delete user information entries.

For the object classes and attributes described in the example, refer to "List of Objects" in the "Interstage Directory Service Object Classes" appendix and "List of Attributes" in the "Interstage Directory Service Attributes" appendix respectively.

The association of the CSV file data and user entry attributes is the same as that shown in the table in 'Adding user information entries.'

The following shows the description examples of the CSV file and rule file used to delete the following two user information entries:

```
dn:  cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
dn:  cn=User006,ou=User,ou=interstage,o=fujitsu,dc=com
```

CSV File

Specify 'DEL' in the 0th item position and then, in the subsequent item positions, describe the entries to be deleted.

Example: CSV file for deleting user information entries

```
DEL,User001,Fujitsu,user001,100001,u5zMEqXX,10001,user001@interstage.fujitsu.com
DEL,User006,Fujitsu,user006,100006,JqzLhqI6,10006,user006@interstage.fujitsu.com   *1
```

*1 Make one entry in one line.

Rule File

Describe the Attribute tag in the ordering of each item in the CSV file. Use the rule file shown above in 'Adding user information entries.'

Example of how to use the irepmodifyent command:

```
irepmodifyent -h hostname -p 389 -D "cn=manager,
ou=interstage,o=fujitsu,dc=com" -r rule.xml -i del.csv   *1
```

*1 Make an entry in one line without starting a new line.

Example of Modifying Entries

The following shows an example of modifying user information entries.

For the object classes and attributes described in the example, refer to "List of Objects" in the "Interstage Directory Service Object Classes" appendix and "List of Attributes" in the "Interstage Directory Service Attributes" appendix respectively.

Note

If no user information entry to be modified exists, add the target entry.

Adding Attribute Values

The following explains how to describe the CSV file and rule file using a scenario in which the telephone number is added to the following entry:

```
dn:  cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
```

In the association between the CSV file data and user entry attributes (see table) the telephone number is the 8th item.

Item position	Item name	Attribute name
8	Telephone number	Telephonenumber

CSV File

Specify 'MOD' in the 0th item position and then, in the subsequent item positions, describe entry information of attribute values to be added. Describe the telephone number (telephonenumber) in the 8th item position.

Example: CSV file for adding the telephone number

```
MOD,User001,Fujitsu,user001,100001,u5zMEqXX,10001,user001@interstage.fujitsu.com,5555-0123   *1
```

*1 Describe one entry in one line.

Rule File

Describe the Attribute tag in the ordering of each item in the CSV file. Use the rule file shown above in 'Adding user information entries.'

Add the telephonenumber description to the Attribute tag.

Example: Rule file for adding the telephone number (Only the content inside the Attribute tag is shown)

```
<Attribute>
    <cn>1</cn>
    <sn>2</sn>
    <givenName>3</givenName>
    <uid>4</uid>
    <userPassword>5</userPassword>
    <employeeNumber>6</employeeNumber>
    <mail>7</mail>
    <telephonenumber>8</telephonenumber>
</Attribute>
```

Deleting Attribute Values

The following shows the description examples of the CSV file and rule file to delete the telephone number added in the example in 'Adding attribute values.'

CSV File

Specify 'MOD' in the 0th item position and then, in the subsequent item positions, describe entry information of attribute values to be deleted. If a telephone number (telephonenumber) is entered in the 8th item, delete the value from the line. Take care not to delete the comma after the 7th item.

Example: CSV file for deleting the telephone number

```
MOD,User001,Fujitsu,user001,100001,u5zMEqXX,10001,user001@interstage.fujitsu.com,   *1
```

*1Describe one entry in one line.

Rule File

Describe the Attribute tag in the ordering of each item in the CSV file. For the CSV file (in the example of deleting the telephone number), use the same rule file as that shown above in the example in 'Adding attribute values'.

Deleting a Specific Attribute Value from Multiple Attribute Values

The following shows the description examples of the CSV file and rule file to delete the telephone number 5555-0123 from the following user information entries.

```
dn:  cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
cn:  User001
sn:  Fujitsu
givenName:  user001
uid:  100001
userPassword:  u5zMEqXX
employeeNumber:  10001
mail:  user001@interstage.fujitsu.com
telephonenumber:  5555-0123
telephonenumber:  5555-6789
```

CSV File

Specify 'MOD' in the 0th item position and then, in the subsequent item positions, describe entry information of attribute values to be deleted. If telephone numbers (telephonenumber) are entered in the 8th and9th items, and the telephone number to be deleted is in the 8th item position, delete the value. Pay attention that the comma before and after the 8th item should not be deleted.

Example: CSV file for deleting one telephone number

```
MOD,User001,Fujitsu,user001,100001,u5zMEqXX,10001,user001@interstage.fujitsu.com,,5555-6789   *1
```

*1 Describe one entry in one line.

Rule File

Describe the Attribute tag in the ordering of each item in the CSV file.

Example: Rule file for deleting one telephone number (Only the content inside the Attribute tag is shown)

```
<Attribute>
    <cn>1</cn>
    <sn>2</sn>
    <givenName>3</givenName>
    <uid>4</uid>
    <userPassword>5</userPassword>
    <employeeNumber>6</employeeNumber>
    <mail>7</mail>
    <telephonenumber>8</telephonenumber>
    <telephonenumber>9</telephonenumber>
</Attribute>
```

Replacing Attribute Values

The following shows the description examples of the CSV file and rule file to replace the telephone number 5555-6789 in the following user information entries with 5555-9001.

```
dn:  cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com
cn:  User001
sn:  Fujitsu
givenName:  user001
uid:  100001
userPassword:  u5zMEqXX
employeeNumber:  10001
mail:  user001@interstage.fujitsu.com
telephonenumber:  5555-6789
```

CSV File

Specify 'MOD' in the 0th item position and then, in the subsequent item positions, describe entry information of attribute values to be replaced. If a telephone number (telephonenumber) is entered in the 8th item, delete the old one and enter the new one in its place in the file.

Example: CSV file for replacing the telephone number

```
MOD,User001,Fujitsu,user001,100001,u5zMEqXX,10001,user001@interstage.fujitsu.com,5555-9001   *1
```

*1 Describe one entry in one line.

Rule File

Describe the Attribute tag according to the order of each item in the CSV file. For the CSV file in the example of replacing the telephone number above, use the same rule file as that used in 'Adding attribute values' described above.

Example of Using the irepmodifyent Command

```
irepmodifyent -h hostname -p 389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -r rule.xml -i mod.csv
```

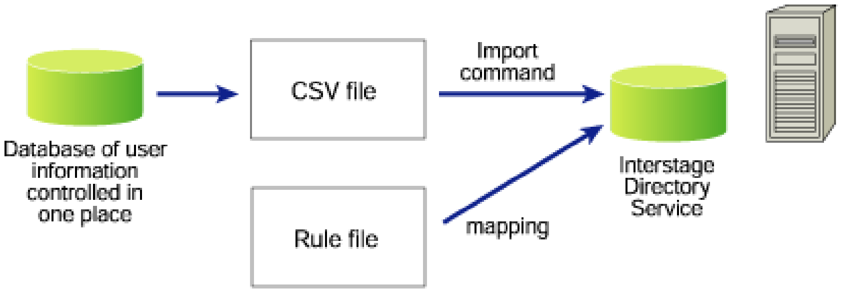
*1 Make an entry in one line without starting a new line.

5.5.2.3 Importing User Information Using the CSV File

The following diagram shows the procedure for adding entries using the CSV file:

1. Extract CSV format data from the database of user information.
2. Set the mapping rules (conversion rules).
3. Execute the import command.

Figure 5.3 Add Entries using the CSV File


Database of user information controlled in one place
CSV file
Import command
Rule file
mapping
Interstage Directory Service

Extracting CSV Format Data from the Database of User Information Controlled in One Place

Use the database functions to extract data in the CSV format from the database of user information. If data on the database is binary, such as certificates, convert it into text (Base64) format.

Setting the Mapping Rules (Conversion Rules)

Set up the rule file for making associations between CSV-format data and information in the repository.

Executing the Import Command

Execute the irepmodifyent command. Entry data will then be added according to the mapping rules.

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

5.6 Optimizing the Database

If Symfoware/RDB is used as the repository database, optimize the database after data has been created.

Refer to "Repository Optimization when Symfoware/RDB is Used" in the "Chapter 10 Operating and Maintaining Repositories" chapter for information about how to optimize the database.

Chapter 6 Creating a Load Distribution Environment

This chapter explains the procedure for creating an environment for database sharing.

Refer to the "Creating a Load Distribution Environment (Replication Mode)" chapter for information on how to create environments for replication configurations.

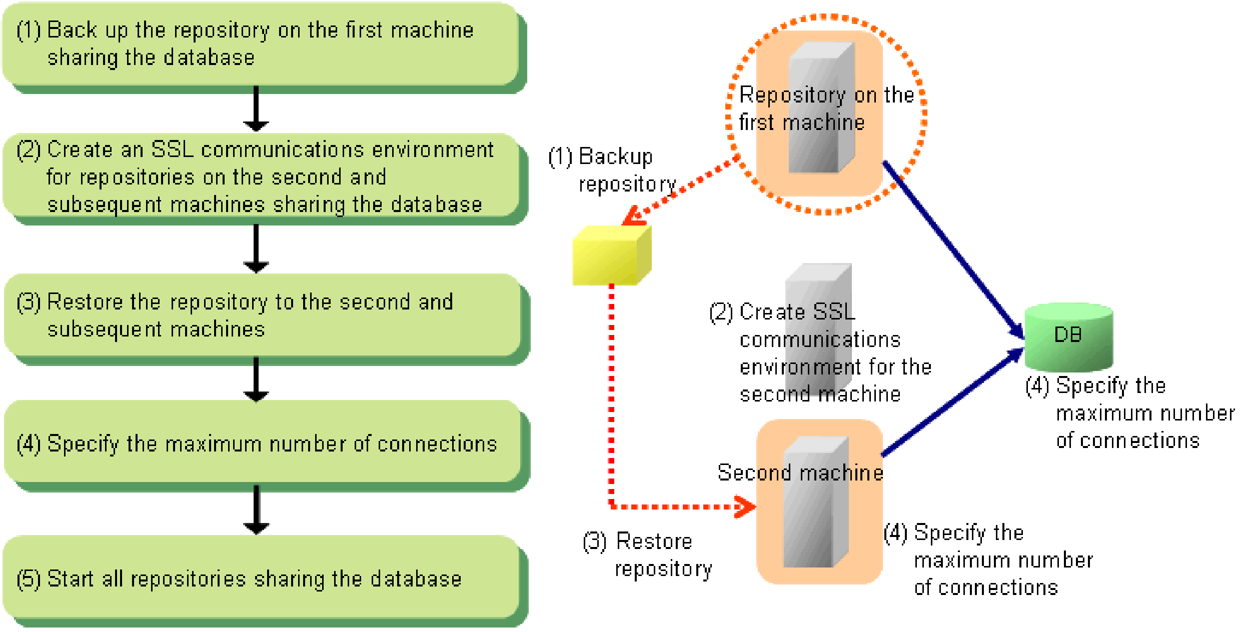
6.1 Database Sharing

This section explains how to create an environment for database sharing. Note that the database sharing function can be used only if an RDB is used for the repository database.

It is assumed that the database has already been created, and that the repository has already been created on the first machine (of those to share the database) To do either of the above, refer to 'Operations using database sharing mode' under the 'Flow of the Environment Setup' in the 'Environment Setup' chapter.

Repositories on the second and subsequent machines sharing the database are created using the backup/restore function. These repositories cannot be created from the Interstage Management Console.

Figure 6.1 Procedure for Creating an Environment for Database Sharing


(1) Back up the repository on the first machine sharing the database
(2) Create an SSL communications environment for repositories on the second and subsequent machines sharing the database
(3) Restore the repository to the second and subsequent machines
(4) Specify the maximum number of connections
(5) Start all repositories sharing the database
Repository on the first machine
(1) Backup repository
(2) Create SSL communications environment for the second machine
DB
(4) Specify the maximum number of connections
Second machine
(3) Restore repository
(4) Specify the maximum number of connections

Notes

- The number of repositories that can be allocated to a single database (RDB) depends on the load per repository and the machine specifications for the database environment.
- If Symfoware Server is used for the database, take care with the host names for machines where Symfoware Server is installed. The host names for all machines with repositories that share the database must be names that can be resolved.
- If the password for an account managed by the operating system or the database management system is changed, set up the database connection password for all repositories sharing the database again.
- Use the same operating system for all platforms for repositories that share the database.
- Install Interstage in the same location on all machines that share the database.
- Use the same version of Interstage on all machines that share the database.
- A database cannot be shared between multiple repositories on the same machine.

To use database sharing in a cluster environment, refer to "Standalone Mode (Using an RDB)" under "Using Interstage Directory Service" in the 'Environment Setup Procedure for Cluster Service' chapter of the High Availability System Guide.

6.1.1 Backing Up the Repository for Database Sharing

To create the repository for the second and subsequent machines that share the database, first back up the repository on the first machine, and then restore this repository on the second and subsequent machines.

This section explains how to back up the repository environment on the first machine. Note that there is no need to back up repository data because the database will be shared.

1. Start the Interstage Management Console on the first machine

   Use the Interstage Management Console on the first machine to select [System] > [Service] > [Repository]

   If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository].

2. Stop the repository

   Select the checkbox corresponding to the repository used for database sharing in the [Repository: Status] window, and then stop the repository by clicking the [Stop] button.

3. Back up the repository environment

   Back up the repository environment by executing the *irepbacksys* command on the first machine. Administrator privilege is required to execute the *irepbacksys* command with.

   Refer to the "Backup Commands" chapter in the Reference Manual (Command Edition) for more information on the *irepbacksys* command.

   Example

   Windows32/64

   Backup destination directory: X:\Backup\irep\rep001_back

   Repository name: rep001

   ```
   irepbacksys -d X:\Backup\irep\rep001_back -R rep001
   IREP: INFO: irep11000:Backup has completed. X:\Backup\irep\rep001_back [rep001]
   ```

   Solaris32/64 Linux32/64

   Backup file name (excluding file extension): /backup/irep/rep001_back

   Repository name: rep001

   For the backup file name, specify the name of the file where repository data will be backed up. Specify the file name without the file extension. After the irepbacksys command has been executed, the following file will be created:

   - /backup/irep/rep001_back.tar.gz.

   ```
   # irepbacksys -f /backup/irep/rep001_back -R rep001
   UX:IREP: INFO: irep11000: Backup has completed. /backup/irep/rep001_back.tar.gz [rep001]
   ```

6.1.2 Creating SSL Communication Environments for Repositories Sharing the Database

If the repository on the first machine uses SSL-encrypted communication, the same SSL environment as that for the repository on the first machine must be created for repositories on the second and subsequent machines sharing the database.

Use the following procedure to create SSL communication environments:

1. Create an Interstage certificate environment

2. Make settings for using certificates

When creating SSL definitions in step 2, use the same name as the SSL definitions used by the repository on the first machine.

For detailed procedure, refer to "Setup of an SSL Communication Environment (Between Client and Server)" in the "Setting up an Environment for SSL Communication" chapter.

6.1.3 Restoring the Repository to Second and Subsequent Machines

Restore the backup of the repository environment for the first machine to the second and subsequent machines sharing the database.

1. Transfer the backup of the repository environment for the first machine to the second and subsequent machines.

   Transfer the backup directory (or backup file for Solaris and Linux) created in "6.1.1 Backing Up the Repository for Database Sharing" to the second and subsequent machines sharing the database.

   Ensure this transfer is not intercepted by third parties. Also, delete these files after they have been used.

2. Restore the repository environment on the second and subsequent machines

   Restore the data in the backup directory (or backup file for Solaris and Linux) by executing the *ireprestsys* command on the second and subsequent machines sharing the database. Specify the same name as the backed up repository for the repository name specified with this command.

   Refer to the "Backup Commands" chapter in the Reference Manual (Command Edition) for more information about the *ireprestsys* command.

   Example

   Windows32/64

   Backup destination directory: X:\Backup\irep\rep001_back

   Repository name: rep001

```
ireprestsys -d X:\Backup\irep\rep001_back -R rep001
IREP: INFO: irep11001: Restore has completed. X:\Backup\irep\rep001_back [rep001]
```

   Solaris32/64 Linux32/64

   Backup file name: /backup/irep/rep001_back.tar.gz

   Repository name: rep001

```
# ireprestsys -f /backup/irep/rep001_back.tar.gz -R rep001
UX:IREP: INFO: irep11001: Restore has completed. /backup/irep/rep001_back.tar.gz [rep001]
```

Notes

- If a Symfoware Server is being used for the database

  - If the Interstage Directory Service and Symfoware Server are installed on separate machines, the Symfoware Server client function must be installed on the second and subsequent machines. Refer to the Symfoware Server Start Guide: Client for more information on installing the client function.

- If an Oracle database is being used for the database

  - If the Interstage Directory Service and the Oracle database are installed on separate machines, Oracle client software (including Oracle Net software) must be installed on the second and subsequent machines. Note also that the "Instant Client" function cannot be used with the Interstage Directory Service. Refer to the Oracle database manual for more information on installing this software.

  - Net Service settings must be made so that the Interstage Directory Service can connect to the Oracle database. When making Net Service settings, use the same Net Service name that was set up when the database was created on the first machine. Refer to the Oracle database manual for more information on how to make these settings.

  - Check that the "Oracle home directory" settings for each restored repository match the Oracle home directory that was set up when the Oracle database or Oracle client software was installed on the machines where the repository has been restored.

    If these settings do not match, change the "Oracle home directory" settings for the repository to match the Oracle home directory settings for the machines where the repository has been restored.

  - If the TNS file (tnsnames.ora) has been stored in a location other than the Oracle home directory (by specifying the TNS_ADMN environment variable, etc.), the Interstage Directory Service will not be able to connect to the Oracle database correctly. Ensure settings are made so that the TNS file is stored in the Oracle home directory.

6.1.4 Specifying the Maximum Number of Connections

If an RDB is used for the database, concurrent search performance can be improved by setting an appropriate value for the maximum number of connections from repositories to the RDB.

Specify the maximum number of connections to the database for all of repositories sharing the database.

The default value is "16". Fujitsu recommend setting the following value:

4 x the number of CPUs on the server where the database is located

Use the *irepadmin* command to set up the maximum number of connections from repositories to the RDB. Refer to "irepadmin" in the "Interstage Directory Service Operation Commands" chapter of the Reference Manual (Command Edition) for more information on how to make these settings.

The maximum number of connections must be set or changed on the database side according to the settings for the maximum number of connections from repositories to the RDB. The number of connections required to use the Interstage Directory Service is calculated according to the following formula:

```
(Maximum number of connections from the repository to the RDB + 1) * (number of repositories)
```

- For Symfoware Server

  Make this specification using parameters from the system environment file. For the value that is specified for the parameters, specify/add the value that that is calculated for the number of connections required to use the Interstage Directory Service shown above.

  - MAX_CONNECT_SYS (if the database is on the same machine as the repository)

  - MAX_CONNECT_TCP (if the database and the repository are on different machines)

- For Oracle database

  Make this specification using database initialization parameters. For the value that is specified for the parameters, consider the value that that is calculated for the number of connections required to use the Interstage Directory Service shown above and refer to the Oracle database manual before calculating the value.

  - PROCESSES

  or

  - SESSIONS

  - TRANSACTIONS

6.1.5 Starting the Repositories Sharing the Database

Start the repository that has been restored in "6.1.3 Restoring the Repository to Second and Subsequent Machines" and all repositories sharing the database.

1. Start the Interstage Management Console on machines sharing the database

   Use the Interstage Management Console on the machines sharing the database to select [System] > [Service] > [Repository]

   If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository].

2. Start the repositories

   Select the checkboxes for the repositories sharing the database in the [Repository: Status] window, and then start the repositories by clicking the [Start] button.

Chapter 7 Entry Management

This chapter explains how to manage entries. The following three methods can be used:

- Use commands
- Use the Entry Administration Tool
- Use the SDK (C language only can be used with Interstage Application Server Enterprise Edition.)

This chapter explains how to manage entries using commands or the Entry Administration Tool. For information on how to manage entries using the SDK, refer to the 'Creating an Application (JNDI)' and 'Creating an Application (CAPI)' chapters.

The following table lists access restrictions to entries that are set in Interstage Directory Service. 'Administrator DN' access is not restricted. More detailed settings can be made by changing access control settings. For more information on changing access control settings, refer to the "Access Control for the Interstage Directory Service" chapter of the Security System Guide.

Table 7.1 Interstage Directory Service Access Restrictions

Attributes, entries	Access type	Authenticated user	Anonymous user
Personal userPassword attribute	Modify	Y	-
	Reference	Y	-
	Search	Y	-
	Compare	Y	-
Others' userPassword attribute	Modify	N	N
	Reference	N	N
	Search	N	N
	Compare	Y	N
Personal entries	Modify	Y	-
	Reference	Y	-
	Search	Y	-
	Compare	Y	-
Other attributes and entries	Modify	N	N
	Reference	Y	Y
	Search	Y	Y
	Compare	Y	Y

Y: Available

N: Not available

-: Not applicable

The userPassword Attribute

Encrypted text passwords must be used for passwords specified in authentication (BIND) request parameters.

If a userPassword attribute value is specified in the search conditions, searches can be performed only if this value is not encrypted.

Specifying a Special Character in a DN

To specify a special character in a command, SDK, or DN, it is necessary to either include a backslash (\) before the special character as an escape character or enclose the special character in double quotes (").

When special characters are specified in the command, enclose them in single or double quotation marks depending on the command line used.

The following lists the special characters for which an escape character is needed.

- "," (Comma)
- "+" (Plus)
- """ (Double quote)
- "<" (Less than)
- ">" (Greater than)
- ";" (Semicolon)
- "#" (Hash) (only when it is specified as the first character of the DN)
- "/" (Slash) (only for JNDI)

Example

Examples of a DN containing special characters that require the escape treatment:

```
cn=a\b,o=Fujitsu, Inc.,c=jp
```

For a Command

For a command, it is necessary to apply the escape treatment to special characters, and enclose the attribute values that include the special characters with double quotes (").

```
cn="a\\b",o="Fujitsu\, Inc.",c=jp
```

For the SDK (C API)

The backslash (\) operates as a special character in LDAP and the C language.

For the SDK (JNDI)

Care needs to be taken for JNDI.

The backslash (\) functions as a special character in LDAP, JNDI, and the Java language.

```
String name = "cn=a\\\\\\\\b,o=Fujitsu\\\\, Inc.,c=jp";
```

Refer to 'Application Development Notes' in 'Creating an Application (C API)' or 'Application Development Notes' in 'Creating an Application (JNDI)' for more information about escape methods with SDKs.

Note

- No schema check is performed when entries are modified in Interstage Directory Service.

  This means that if inappropriate entry modifications (such as deleting a required attribute in an entry or adding an attribute to the Object Class that must not be added) are performed, information in the repository will be contradictory. Sufficient care must therefore be taken when modifying entries.

- Entries of the repository in slave operation cannot be added, modified, or deleted.

7.1 Using Commands to Manage Entries

This section explains how to manage entries using commands.

Entry information can be fetched into a file from the database in Interstage Directory Service. This operation is called exporting. At this point, the file is stored in the LDIF.

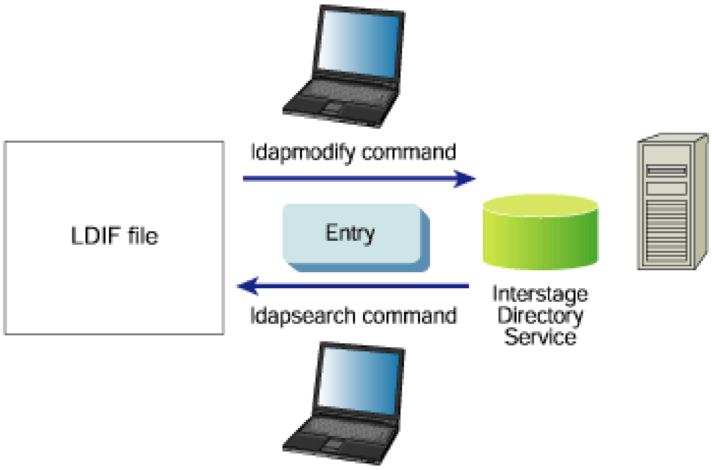
It is also possible to register a large amount of entries in the database in Interstage Directory Service using the CSV or LDIF files. This operation is called importing.

When the LDIF file is used, the ldapmodify command is used for importing and the ldapsearch command is used for exporting.

When the CSV file is used, the irepmodifyent command is used for importing.

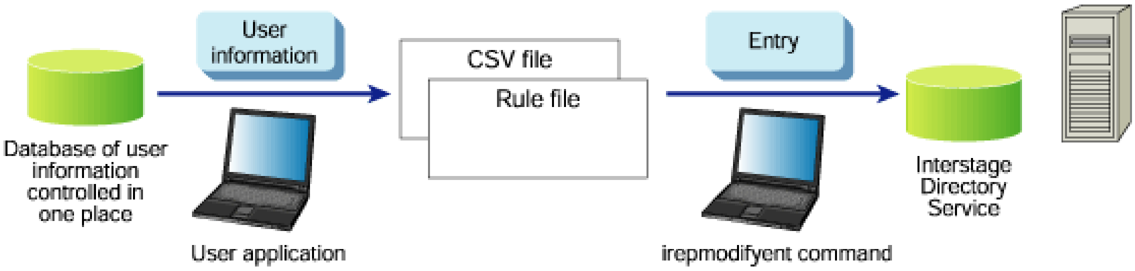
Importing and Exporting from LDIF Files

Figure 7.1 Import and Export using the LDIF file



Importing from CSV Files

Figure 7.2 Import Flow using CSV File


User information
Database of user information controlled in one place
User application
CSV file
Rule file
Entry
irepmodifyent command
Interstage Directory Service

7.1.1 Searching for Entries

Entry search is performed as follows:

1. Narrow down information by specifying a search range.
2. For the attribute value of each entry in the search range, specify filtering criteria to extract the items that match the criteria.

Refer to 7.1.2 Search Filters for more information on search filters.

Search ranges are described below.

Search Range

Three levels of search are provided:

Search Range	Description
Base object search	Searches specified entry itself.
One level search	Searches the layer one level under that of specified entry.
Sub tree search	Searches the specified entry and all the layers under its layer.

Repository entries can be searched by using the ldapsearch command. It is also possible to use a search filter to extract specific information.

For the method of using this command, refer to 'Interstage Directory Service operation command' in the Reference Manual (Command Edition).

Example

Windows32/64

- Searching for entries whose attribute cn is 'user1' to extract information about the attribute sn

```
C:\Interstage\bin\ldapsearch -H ldap://hostname:389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -W -b
"ou=interstage,o=fujitsu,dc=com" "cn=user1" sn   *1
```

*1 Make an entry in one line without starting a new line.

- Output all entries to a file (ldif.txt)

```
C:\Interstage\bin\ldapsearch -H ldap://hostname:389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -W -b
"ou=interstage,o=fujitsu,dc=com" "objectclass=*" > ldif.txt   *1
```

*1 Make an entry in one line without starting a new line.

Solaris32/64 Linux32/64

- Searching for entries whose attribute cn is 'user1' to extract information about the attribute sn

```
/opt/FJSVirepc/bin/ldapsearch -H ldap://hostname:389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -W -b
"ou=interstage,o=fujitsu,dc=com" "cn=user1" sn   *1
```

*1 Make an entry in one line without starting a new line.

- Output all entries to a file (ldif.txt)

```
/opt/FJSVirepc/bin/ldapsearch -H ldap://hostname:389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -W -b
"ou=interstage,o=fujitsu,dc=com" "objectclass=*" > ldif.txt   *1
```

*1 Make an entry in one line without starting a new line.

7.1.2 Search Filters

This section details the (RFC1558-compliant) search filters that can be used with Interstage Directory Service clients. It also provides examples of their use.

Search Filters that Can be Used

The following five filters can be specified:

Filter	Description
Equal	Extracts items with an attribute value equal to the specified value.
Substring	Extracts items when the attribute value contains the specified substring. Forward matching, backward matching, arbitrary part matching, or any combination of these can be used in the substring.
Greater	Extracts items with an attribute value greater than the specified value.
Less	Extracts items with an attribute value less than the specified value.
Present	Extracts items with an attribute value.

In addition, by combining some of the above filters, more detailed filtering criteria can be specified. The following table contains the logical operations that are used to combine filters:

Logical Operation	Description
AND	Combine multiple filters with the logical product (AND) operation. Valid if all the criteria are true.
OR	Combine multiple filters with the logical add (OR) operation. Valid if any of the criteria is true.
NOT	Evaluates to true if the specified operand is false. Only one operand can be specified. Example: (!(cn=Fujitsu)) Statements such as (!(cn=Fujitsu)(uid=0123)) are not valid.

Search Filter Syntax

The syntax of the search filter is described in the following RFC documents:

- RFC1960 "A String Representation of LDAP Search Filters"
- RFC2254 "The String Representation of LDAP Search Filters"

Example

- Equal (=)

  Search for entries whose cn is User001.

```
(cn=User001)
```

- Greater (>=), less (<=)

  Search for entries whose dnQualifier is greater than 0.

```
(dnQualifier>=abc)
```

- Present (=*)

  Search for all entries that contain cn.

```
(cn=*)
```

- Substring (string*)

  Search for entries whose cn begins with Fujitsu.

```
(cn=Fujitsu*)
```

- AND (&)

  Search for entries whose cn is User001 and whose sn is Fujitsu.

```
(&(cn=User001)(sn=Fujitsu))
```

- OR (|)

  Search for entries whose givenName is User001 or User002.

```
(|(givenName=User001)(givenName=User002))
```

- Negation (!) (only valid if the RDB is used)

  Search for entries where cn does not start with Fujitsu.

```
(!(cn=Fujitsu*))
```

Note

- When specifying a search filter, enclose it in double quotation marks. When special characters are specified in the *ldapsearch* command, put them in single or double quotation marks depending on the command line used.
- When the standard database is used, up to two search conditions can be specified using OR.

  A search filter such as the one specified below is invalid.

```
(|(givenName=User001)(givenName=User002)(mail=*))
```

  If three or more search conditions are specified in combination when an RDB is used, express the search condition as combinations of pairs of conditions, as follows:

```
(&(&(cn=User001)(sn=Fujitsu))(givenName=User001))
```

Specifying Special Characters

If any of the special characters listed below are specified as search filter values, they must be escaped using "\" (backslash).

In the ldapsearch command, the character must be specified as a hexadecimal number after the escape character "\" (backslash).

In C API, the character must be specified as a hexadecimal number after the two escape characters "\\" (backslash).

In JNDI, there is no need to specify these characters in hexadecimal. They are specified as follows:

Special character	ldapsearch command	C API	JNDI
*	\2a	\\2a	*
(	\28	\\28	\\(
)	\29	\\29	\\)
\	\5c	\\5c	\\\\

Note

To set "AB(C)" to the value of search filter, specify as follows:

- ldapsearch command

```
(o=AB\28C\29)
```

- C API

```
(o=AB\\28C\\29)
```

- JNDI

```
(o=AB\\(C\\))
```

7.1.3 Adding Entries using Commands

Entries can be added to the repository by using the *ldapmodify* or *irepmodifyent* command.

If entry information is specified from the standard input or an LDIF file, use the *ldapmodify* command. For information on LDIF, refer to 'Using the LDAP Data Interchange Format (LDIF)' under 'Creating Data' in 'Creating a Repository'.

If entry information is specified in a CSV file, use the *irepmodifyent* command. For information on CSV, refer to 'Using CSV Files Extracted from the Database' under 'Creating Data' in 'Creating a Repository'.

For the method of using each command, refer to 'Interstage Directory Service operation command' in the Reference Manual (Command Edition).

Examples

- Using the LDIF file in the ldapmodify command

Windows32/64

```
C:\Interstage\bin\ldapmodify -H ldap://hostname:389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -W -f ldif.txt   *1
```

*1 Make an entry in one line without starting a new line.

Solaris32/64 Linux32/64

```
/opt/FJSVirepc/bin/ldapmodify -H ldap://hostname:389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -W -f ldif.txt   *1
```

*1 Make an entry in one line without starting a new line.

- Using the CSV file in the ldapmodify command

```
irepmodifyent -H ldap://hostname:389 -D "cn=manager,ou=interstage,o=fujitsu,dc=com" -r rule.xml -
i add.csv
```

*1 Make an entry in one line without starting a new line.

7.1.4 Deleting Entries using Commands

Entries can be deleted from the repository using the ldapdelete command. The ldapmodify and irepmodifyent commands can also be used to delete entries.

The ldapdelete command can be used to delete entries by specifying the DN names to be deleted or a file containing the DN names. Note that, instead of the LDIF format, only DN names are specified for the ldapdelete command.

If entry information is specified in the standard input or a file, use the ldapmodify command.

If entry information is specified in a CSV file, use the *irepmodifyent* command. For information on the use of CSV files, refer to 'Using CSV Files Extracted from the Database' under 'Creating Data' in 'Creating a repository'.

For details on how to use each command, refer to 'Interstage Directory Service operation command' in the Reference Manual (Command Edition).

Examples

- Using a file in the ldapdelete command

Windows32/64

```
C:\Interstage\bin\ldapdelete -H ldap://hostname:389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -W -f delete_input.txt   *1
```

*1 Make an entry in one line without starting a new line.

Solaris32/64 Linux32/64

```
/opt/FJSVirepc/bin/ldapdelete -H ldap://hostname:389 -D
"cn=manager,ou=interstage,o=fujitsu,dc=com" -W -f delete_input.txt   *1
```

*1 Make an entry in one line without starting a new line.

- Using the CSV file in the irepmodifyent command

```
irepmodifyent -H ldap://hostname:389 -D "cn=manager,ou=interstage,o=fujitsu,dc=com" -r rule.xml -
i del.csv   *1
```

*1 Make an entry in one line without starting a new line.

7.1.5 Modifying Entries using Commands

Entries in the repository can be modified using the *ldapmodify* or *irepmodifyent* command.

If entry information is specified in the standard input or LDIF file, use the ldapmodify command. For information about LDIF files, refer to 'Using the LDAP Data Interchange Format (LDIF)' under 'Creating Data' in 'Creating a Repository'.

If entry information is specified in the CSV file, use the irepmodifyent command. For information about the use of CSV files, refer to 'Using CSV Files Extracted from the Database' under 'Creating Data' in 'Cleaning a Repository'.

For the method of using each command, refer to 'Interstage Directory Service operation command' in the Reference Manual (Command Edition).

Examples

- Using the LDIF file in the ldapmodify command

  Windows32/64

  ```
  C:\Interstage\bin\ldapmodify -H ldap://hostname:389 -D
  "cn=manager,ou=interstage,o=fujitsu,dc=com" -W -f ldif.txt   *1
  ```

  *1 Make an entry in one line without starting a new line.

  Solaris32/64 Linux32/64

  ```
  /opt/FJSVirepc/bin/ldapmodify -H ldap://hostname:389 -D
  "cn=manager,ou=interstage,o=fujitsu,dc=com" -W -f ldif.txt   *1
  ```

  *1 Make an entry in one line without starting a new line.

- Using the CSV file in the irepmodifyent command

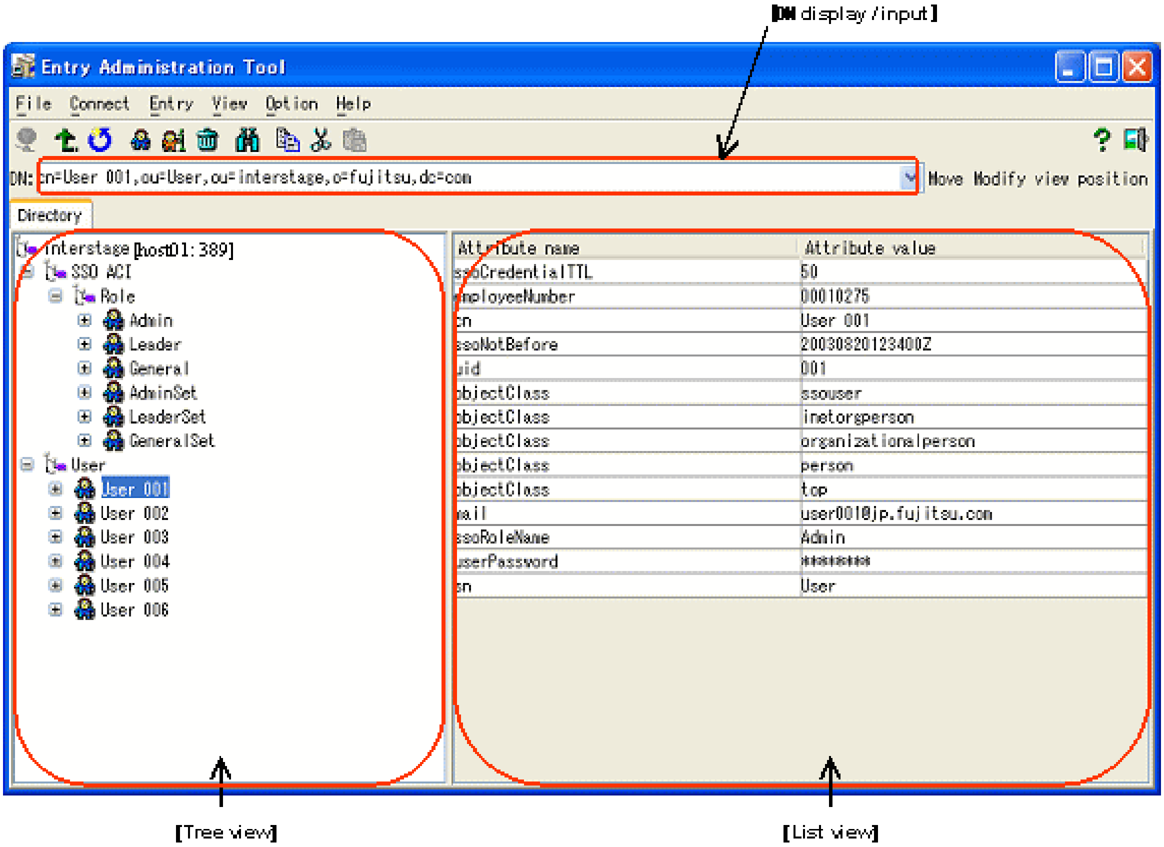
  ```
  irepmodifyent -H ldap://hostname:389 -D "cn=manager,ou=interstage,o=fujitsu,dc=com" -r rule.xml -
  i mod.csv   *1
  ```

  *1 Make an entry in one line without starting a new line.

7.2 Using the Entry Administration Tool

The Entry Administration Tool is a tool to manage entries. Using the Entry Administration Tool, operations such as addition, modification, deletion, and searching of entries registered with the repository can be performed through a GUI.

Figure 7.3 Entry Administration Tool window


[DN display/input]
Entry Administration Tool
File Connect Entry View Option Help
Move Modify view position
Directory
[Tree view]
[List view]

DN: cn=User 001,ou=User,ou=interstage,o=fujitsu,dc=com

```
interstage [host01:389]
  SSO ACI
    Role
      Admin
      Leader
      General
      AdminSet
      LeaderSet
      GeneralSet
  User
    User 001
    User 002
    User 003
    User 004
    User 005
    User 006
```

Attribute name	Attribute value
ssoCredentialTTL	50
employeeNumber	00010275
cn	User 001
ssoNotBefore	20030820123400Z
uid	001
objectClass	ssouser
objectClass	inetorgperson
objectClass	organizationalperson
objectClass	person
objectClass	top
mail	user001@jp.fujitsu.com
ssoRoleName	Admin
userPassword	********
sn	User

1. DN display/input
2. Tree view
3. List view

DN Display/Input

Displays DN of the selected entry. DN can be entered or selected from the drop-down list.

Tree View

Displays entry information registered with the repository in the hierarchical configuration. Nodes in the tree can be opened and closed by the mouse or from the keyboard.

List View

Displays entries selected in [Tree view]. Two display modes are available: one mode displays attribute information about one entry, the second mode lists entries at the same level in the hierarchy.

Note

If an external file is specified as a binary attribute value, only the content of the external file is stored; the file name is not stored. Thus, if an entry containing a binary attribute is selected, only the data size of the binary file stored in the repository is displayed in the attribute value field of the binary attribute.

Operation Method

Start and operate the Entry Administration Tool using the following procedure:

1. Bitmap display is required

   On the machine that uses the Entry Administration Tool, configure a display and driver that can be specified with over 256 colors on the monitor.

   Solaris32/64 Linux32/64

A bitmap display is needed.

2. Start the Entry Administration Tool

   Windows32/64

   Select [Programs] > [Interstage Application Server] > [Interstage Directory Service] > [Entry Administration Tool] from the [Start] menu.

   Solaris32/64 Linux32/64

```
irepeditent
```

3. Login

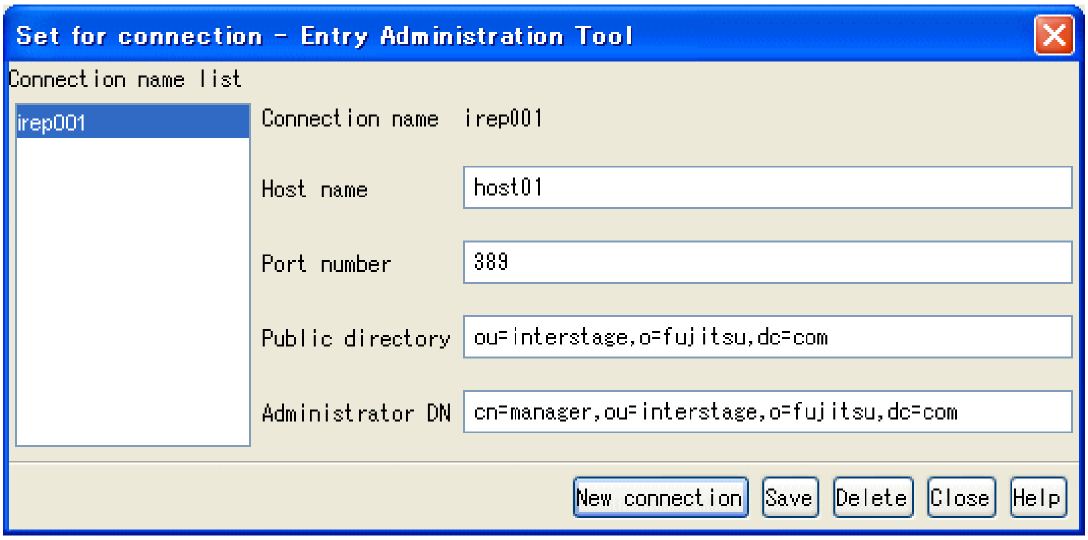
   Use either of the following methods to display the [Login] window:

   - Click [Login] from the [Connect] menu.
   - Click [Login] button on the tool bar.

     1. Select the connection destination from the [Connection destination]
     2. Enter the Administration DN password in the [Password]
     3. Click [Login]

   If it is the first login after installation of the product, or connection destination information is being added or changed, the connection information needs to be set. For details about connection, refer to the Entry Administration Tool Help.

Figure 7.4 Entry Administration Tool - Set for connection dialog



Set for connection - Entry Administration Tool

Connection name list

irep001

Connection name irep001

Host name host01

Port number 389

Public directory ou=interstage,o=fujitsu,dc=com

Administrator DN cn=manager,ou=interstage,o=fujitsu,dc=com

4. Initial display

   When connecting to the repository which operates entries after login, the Entry Administration Tool is initially displayed (the directory information tree of the connected repository is displayed in the left column 'Tree view').

   For details of adding, modifying and searching operation methods, refer to the explanation on the next pages and the Entry Administration Tool help.

Note

- If an external file is specified as a binary attribute value, only the content of the external file is stored; the file name is not stored. Thus, if an entry containing a binary attribute is selected, only the data size of the binary file stored in the repository is displayed in the attribute value field of the binary attribute.
- The Entry Administration Tool is mainly used for development and testing when setting up a directory by the system administrator. Create a dedicated application for entry management in user operation. For information about application development, refer to 'Creating an Application (C API)' or 'Creating an Application (JNDI)'.

7.2.1 Adding Entries using the Entry Administration Tool

The Add an Entry and Import windows are provided to add entries. By opening these windows and entering settings and values, entries can be registered with the connected repository.

Adding Entries One by One

1. Select the upper entry of the entry to be added from [Tree view].
2. Select [Add...Ctrl+N] from the [Entry (E)] menu or right-click and select [Add... Ctrl+N] from the pop-up menu.
3. The Add an Entry window is displayed. Enter the attributes required for entries to be added to add entries.

For more details, refer to the Entry Administration Tool Help.

Adding Entries Using the LDIF File

1. Select [Import...F3] from the [Options (O)] menu.
2. The import window is displayed. In the field [LDIF file], specify the LDIF file containing information about the entry to be added. Specify the file by either of the following methods::
    - Clicking [Browse...] and browsing to the file.
    - Entering the path of the LDIF file.
3. Select the character set of the specified LDIF file from [Character set].
4. Select [Add] of the specified type.
5. Click [OK] to add the entry specified in the LDIF file.

For more details, refer to the Entry Administration Tool Help.

7.2.2 Deleting Entries using the Entry Administration Tool

Entries can be deleted one by one or using the LDIF file.

Deleting Entries One by One

1. Select the entry to be deleted from [Tree view].
2. Select [Delete...Delete] from the [Entry (E)] menu or right-click and select [Delete...Delete] from the pop-up menu.

For more details, refer to the Entry Administration Tool Help.

Deleting Entries using the LDIF File

1. Select [Import...F3] from the [Options (O)] menu.
2. The import window is displayed. In the field [LDIF file], specify the LDIF file containing information about the entry to be added. Specify the file by either of the following methods::
    - Clicking [Browse...] and browsing to the file.
    - Enter the path of the LDIF file.
3. Select the character set of the specified LDIF file from [Character set].
4. Select [Modify] of the specified type.
5. Click [OK] to delete the entry specified in the LDIF file.

For more details, refer to the Entry Administration Tool Help.

7.2.3 Modifying Entries using the Entry Administration Tool

The entry modification window and import window are provided to modify entries. By opening these windows and entering settings and values, entries can be modified with the connected repository.

Modifying Entries One by One

1. Select the entry to be modified from [Tree view].
2. Select [Modify... Ctrl+M] from the [Entry (E)] menu or right-click and select [Modify... Ctrl+M] from the pop-up menu.

For more details, refer to the Entry Administration Tool Help.

Modifying Entries using the LDIF File

1. Select [Import...F3] from the [Options (O)] menu.
2. The import window is displayed. In the field [LDIF file], specify the LDIF file containing information about the entry to be added. Specify the file by either of the following methods:
   - Clicking [Browse...] and browsing to the file.
   - Enter the path of the LDIF file.
3. Select the character set of the specified LDIF file from [Character set].
4. Select [Modify] of the specified type.
5. Click [OK] to modify the entry specified in the LDIF file.

For more details, refer to the Entry Administration Tool Help.

7.2.4 Searching Entries using the Entry Administration Tool

1. Select the entry to be searched for from [Tree view].
2. Select [Search...Ctrl+S] from the [View] menu.
3. The search window is displayed. Create a search filter on the search window to search for the entry.

For more details, refer to the Entry Administration Tool Help.

7.2.5 Changing the Entry Identifier using the Entry Administration Tool

1. Select the entry whose identifier should be changed from [Tree view].
2. Select [Rename...F2] from the [Entry (E)] menu or right-click and select [Rename...F2] from the pop-up menu.

For more details, refer to the Entry Administration Tool Help.

Chapter 8 Creating an Application (JNDI)

This chapter describes the method of creating an application using Interstage Directory Service with JNDI.

8.1 Application Development Environment

Java applications can access the Interstage Directory Service server using JNDI.

To create a JNDI application, a Java program compilation environment is required. Ensure that JDK has been installed. Download and refer to the following documents from the Oracle website for JNDI usage and interface details:

- The JNDI Tutorial
- Java 2 Platform API Specification (javadoc)

8.2 Creating the Source Program

8.2.1 Specifying Symbols

Symbols can be specified in DN and in the attribute value. This section explains how to describe a symbol with JNDI.

Specifying DN including symbols

The following symbols are regarded as special characters when specifying the symbols.

- "," (Comma)
- "+" (Plus)
- """ (Double quote)
- "<" (Less than)
- ">" (Greater than)
- ";" (Semicolon)
- "#" (Hash) (only when it is specified as the first character of the DN)
- "/" (Slash)

To specify special characters, place a "\"(backslash) before the character.

Example

A DN containing special characters that must be preceded by the backslash:

```
cn=a\b,o=Fujitsu, Inc.,c=jp
```

The backslash (\) functions as a special character in LDAP, JNDI, and the Java language:

```
String name = "cn=a\\\\\\\\b,o=Fujitsu\\\\, Inc.,c=jp";
```

Specifying the Search Filter Including Symbols

When symbols are specified in the search filter, some symbols are treated as special characters. These characters must be preceded by a "\\" (double backslash).

Symbols that require the escape treatment are indicated below:

- "*" (asterisk)
- "(" (open bracket)
- ")" (close bracket)
- "\" (backslash)

Example

To set "AB(C)" as the value of search filter, specify as follows:

```
(o=AB\\(C\\))
```

8.2.2 Flow of Basic Operations

To access an Interstage Directory Service server in JNDI, it is necessary to perform the following steps.

1. Pre-treatment

   Performs session opening, initial settings and user authentication (simple authentication by password)

2. Access to the Interstage directory service

   This explains the flow of operation for processes that can be requested via the Interstage directory service.

   - Entry search
   - Changing entry attribute value
   - Adding entry
   - Deleting entry
   - Changing entry name
   - Comparing entry attribute value

3. Post-processing

   Closing the session

8.2.3 Opening a Session, Initial Settings and User Authentication

To access Interstage directory service using JNDI, perform session opening, initial settings and use authentication.

Opening a Session

To open the session, create the initial context using the following classes.

```
javax.naming.InitialContext
```

Initial Settings and User Authentication

When creating the initial context, set the following information using the environment property:

- LDAP service provider
- Connection destination repository (host name, port number)
- Method of authentication
- User DN when bind to repository
- User DN password when bind to repository

LDAP service provider

Specify the following in the environment property

javax.naming.Context.INITIAL_CONTEXT_FACTORY "com.sun.jndi.ldap.LdapCtxFactory"

Repository for connection destination (host name, port number)

Specify the URL information with the format below in the environment property javax.naming.Context.PROVIDER_URL.

"ldap://host name: post number"

When specifying IPv6 address, use "[]"(square brackets).

"ldap://[IPv6 address]:port number"

Method of authentication

Specify the method of authentication which is used when a repository is bound in the environment property javax.naming.Context.SECURITY_AUTHENTICATION. Specify "none"or "simple" for the value.

- "none": anonymous(anonymous user) authentication
- "simple": simple authentication

User DN that binds to a repository

Specify the user DN that binds to the repository in the environment property. The default value is anonymous (anonymous user).

User DN password that binds to a repository

Specify the user DN password that binds to a repository in the environment property javax.naming.Context.SECURITY_CREDENTIALS. The default value has no password.

This explains how to create the initial context with examples.

```
Hashtable<String, Object> env = new Hashtable<String, Object>();
env.put(Context.INITIAL_CONTEXT_FACTORY, "com.sun.jndi.ldap.LdapCtxFactory");
env.put(Context.PROVIDER_URL, "ldap://localhost:389");
env.put(Context.SECURITY_AUTHENTICATION, "simple");
env.put(Context.SECURITY_PRINCIPAL, "cn=User001, ou=interstage, o=fujitsu,dc=com");
env.put(Context.SECURITY_CREDENTIALS, "mypassword");
DirContext ctx = new InitialDirContext(env);
```

The session must be closed after ending access to the Interstage directory service.

Using SSL Communication

An ldaps scheme is used for the URL information for the connection destination repository. This is different from the situation where ldap scheme is used when SSL communication is not used.

Connection destination repository (host name, port number)

Specify the URL information with the format below in the environment property javax.naming.Context.PROVIDER_URL. Specify the port number used for SSL communication.

"ldaps://host name:port number"

When using SSL communication, specify the following environment property and system property in addition to the environment property of "initial settings, user authentication"

Security protocol

Specify the security protocol in the environment property javax.naming.Context.SECURITY_PROTOCOL

Socket factory

Specify the socket factory class name in the environment property java.naming.ldap.factory.socket. If the environment property is omitted, SSL cannot be used. Specify the following value.

"com.fujitsu.ssl.FjSSLSocketFactory"

SSL environment definition file

Specify the full path for the SSL environment definition file in the system property user.sslenvfile. For information on how to create this file, refer to "Setting an SSL Environment Definition File (Client)" in the "Setting up an Environment for SSL Communication" chapter.

SSL log file output destination

Specify the destination directory for the SSL log file in the system property user.ssllogdir. The log file produced by the SSL library will be stored in this directory during SSL communication.

The following example shows how to create the initial context when using SSL communication.

```
Hashtable<String, Object> env = new Hashtable<String, Object>();
env.put(Context.INITIAL_CONTEXT_FACTORY, "com.sun.jndi.ldap.LdapCtxFactory");
```

```
  env.put(Context.PROVIDER_URL, "ldaps://localhost:636");
  env.put(Context.SECURITY_AUTHENTICATION, "simple");
  env.put(Context.SECURITY_PRINCIPAL, "cn=User001, ou=interstage, o=fujitsu,dc=com");
  env.put(Context.SECURITY_CREDENTIALS, "mypassowrd");
  /* The environment property settings for SSL */
  env.put("java.naming.ldap.factory.socket", "com.fujitsu.ssl.FjSSLSocketFactory");
  env.put(Context.SECURITY_PROTOCOL, "ssl" );

  /* Acquisiton of system property */
  Properties prop = System.getProperties();

  prop.put("user.sslenvfile", sslenvfile);
  prop.put("user.ssllogdir", ssllogdir );
  DirContext ctx = new InitialDirContext(env);
```

Acquiring an SSL Error

This section describes how to acquire an error on SSL.

From a message output by SSL, an error type and an error code can be acquired.

1. From an output message, extract error information using 'FjSSLSocket' as a key.
2. From error information, extract an error type using 'errtype=' as a key.
3. From error information, extract an SSL error code using 'SSLLerrorcode=' as a key.

Sample message:

```
com.fujitsu.ssl.SSLException: FjSSLSocket:SSL_Init error, errtype=10
SSLLerrorcode=10004c
```

An error type and an SSL error code can be acquired in the following way:

```
catch(NamingException ne){
        Throwable msg       = ne.getRootCause();
        String    msgStr    = null;
        int       ssl_error = -1;
        if ( msg != null ){
            /* Get an error message */
            msgStr = msg.toString();
            /* Acquire error information using "FjSSLSocket" as a key. (1)
*/
            ssl_error = msgStr.indexOf("FjSSLSocket");
        }
        /* When SSL is used */
        if ( ssl_error != -1 ){
            int index1 = msgStr.indexOf("errtype=");
            int index2 = msgStr.indexOf("SSLLerrorcode=");
            if ( index1 != -1 ){
                /* Acquire an error type using "errtype=" as a key. (2) */
                String error = msgStr.substring(index1 + "errtype=".length(), index1 +
"errtype=".length() + 2);
                /* Print an error type */
                System.out.println("SSL Error type : " + error);
            }
            if ( index2 != -1 ){
                /* Acquire an SSL error code using "SSLLerrorcode=" as a key.
(3) */
                String error = msgStr.substring(index2 + "SSLLerrorcode=".length());
                /* Print a SSL error code */
                System.out.println("SSL Error code : " + error);
            }
        }
}
```

Refer to "SSLException Error Types" and "SSL Error Codes" in the "Error Codes to be Reported from Interstage Directory Service" chapter of the Messages manual for information about SSLException error types and code values, and how to resolve them.

Note

Cases in which Multiple Sessions are Needed

The javax.naming.directory.InitialDirContext class performs initial setup and user authentication as soon as a session is opened. To modify user authentication information during processing, users must open a new session.

In this case, only close the sessions that have been started. In addition, use the javax.naming.ldap.InitialLdapContext class to modify the user authentication settings, etc. while the sessions are open. For information about the specification method, refer to the following example:

```
Hashtable env = new Hashtable(5, 0.75f);
env.put(Context.INITIAL_CONTEXT_FACTORY,
"com.sun.jndi.ldap.LdapCtxFactory");
env.put(Context.PROVIDER_URL, "ldap://host:389");

// Open a session by getting authentication as anonymous (anonymous user).
env.put(Context.SECURITY_AUTHENTICATION, "simple");
env.put(Context.SECURITY_PRINCIPAL, "");
env.put(Context.SECURITY_CREDENTIALS, "");
InitialLdapContext ctx = new InitialLdapContext(env,null);


// Getting authentication again as administrator.
ctx.addToEnvironment(Context.SECURITY_AUTHENTICATION, "simple");
ctx.addToEnvironment(Context.SECURITY_PRINCIPAL,
"cn=admin,ou=interstage,o=fujitsu,dc=com");
ctx.addToEnvironment(Context.SECURITY_CREDENTIALS, "admin");
ctx.reconnect(null);


// Close the session.
ctx.close();
```

Maximum Number of Sessions

The maximum number of sessions which can be maintained in one process is 1024. If an attempt is made to open a session when after the maximum has been exceeded, an SSLException will be thrown.

SSLException error type value (int): 99, SSL error code: 200002

Take the following actions on the application side:

- Coding to close the unnecessary session(s).
- If the session is reusable, decrease the number of sessions. For details on how to decrease the number, refer to "Cases in which Multiple Sessions are Needed", above.
- Increasing the number of processes and then dividing the sessions among them is a way to limit the number of sessions in one process from the application side.

8.2.4 Entry Search

If requesting an Interstage Directory Service entry search, the entry information that matches the search condition will be sent. For an entry search, use the following method:

```
javax.naming.DirContext.search()
```

For a basic search, specify the search base and the search filter. For the search filter, specify the search condition format. For instance, when searching something that has an sn attribute value of Fujitsu and a mail attribute value of .fujitsu.com, use the following format,

```
  (&(sn=Fujitsu)(mail=*.fujitsu.com))
```

Examples of search

```
String filter = "(&(sn=Fujitsu)(mail=*.fujitsu.com))";
NamingEnumeration results = ctx.search("ou=User,ou=interstage,o=fujitsu,dc=com", filter, null);
```

For details of search filter format, refer to "Search Filters" in the "Entry Management" chapter.

The search target can be narrowed down and the search result waiting period can be specified. These options are explained in the next section.

8.2.4.1 Search Option

Set the search option for the session using the following class:

```
javax.naming.directory.SearchControls
```

Search object scope

Use the setSearchScope() method to specify the search object scope using the following values. The initial value is ONELEVEL_SCOPE.

- OBJECT_SCOPE: Search the hierarchy specified in the search base.
- ONELEVEL_SCOPE: Search the "singlelevel" entry under the hierarchy specified in the search base.
- SUBTREE_SCOPE: Search the "wholesubtree" entries under the hierarchy specified in the search base.

  The examples below relate to a search under the hierarchy specified in the search base.

  ```
  SearchControls constraints = new SearchControls();
  constraints.setSearchScope(SearchControls.SUBTREE_SCOPE);
  ```

Attributes to obtain search result

For the basic search, all attribute information that can be read will be returned. Depending on the application process, only required attributes can be returned, and the setReturningAttributes() method is used. The attribute name that retrieves the search result is specified with the string. The initial value is null, and this returns all attributes. Use a blank string if no attributes are to be returned.

Examples of retrieving mail and telephonenumber attributes.

```
String[] attrs = {"mail", "telephonenumber"};
SearchControls constraints = new SearchControls();
constraints.setReturningAttributes(attrs);
```

Maximum number of searches

Use the setCountLimit() method to limit the maximum number of search entry results. The initial value is 0 (Unlimited).

Example of limiting to 10 cases

```
SearchControls constraints = new SearchControls();
constraints.setCountLimit(10);
```

Maximum timeout time

Use the setTimeLimit() method to specify the maximum timeout time for searches in milli-seconds. The initial value is 0 (Unlimited).

Example of limiting to one second

```
SearchControls constraints = new SearchControls();
constraints.setTimeLimit(1000);
```

Note

The values set for the maximum number of searches on the server side and the maximum timeout time may not take effect, depending on the access DN (Bind DN) from the client. For details, refer to "Setting Items of the Interstage Management Console" in the "Creating a Repository" chapter.

8.2.4.2 Obtaining a Search Result

The javax.naming.DirContext.search() method recover value is the SearchResult list with NamingEnumeration. The following example shows how to display the search result.

```
NamingEnumeration results = ctx.search("ou=User,ou=interstage,o=fujitsu,dc=com",
    filter, constraints);
while (results != null && results.hasMore()) {
    SearchResult si = (SearchResult)results.next();
    System.out.println("name: " + si.getName());
    Attributes attrs = si.getAttributes();
    if (attrs == null) {
        System.out.println("No attributes");
    } else {
        /* print each attribute */
        for (NamingEnumeration ae = attrs.getAll();
            ae.hasMoreElements(); ) {
            Attribute attr = (Attribute)ae.next();
            String id = attr.getID();

            /* print each value */
            for (Enumeration vals = attr.getAll();
                vals.hasMoreElements();
                System.out.println(id + ": " + vals.nextElement()));
        }
    }
}
```

Obtaining a Binary Attribute Value

The Binary attribute value is received by byte[]. In default, the following attributes will be returned as the binary value.

- audio
- jpegPhoto
- javaSerializedData
- userPassword
- userCertificate
- cACertificate
- authorityRevocationList
- certificateRevocationList
- crossCertificatePair

The following is an example of how to show the binary attribute value.

```
NamingEnumeration results = ctx.search("ou=User,ou=interstage,o=fujitsu,dc=com",
    filter, constraints);
while (results != null && results.hasMore()) {
    SearchResult si = (SearchResult)results.next();
    Attributes attrs = si.getAttributes();
    if (attrs == null) {
        System.out.println("No attributes");
    } else {
        /* print each attribute */
        for (NamingEnumeration ae = attrs.getAll();
            ae.hasMoreElements(); ) {
            Attribute attr = (Attribute)ae.next();
            String id = attr.getID();

            /* print each value */
            for (Enumeration vals = attr.getAll();
                vals.hasMoreElements(); ) {
                System.out.print( id + ": " );
                Object val = vals.nextElement();
                if (val instanceof String) {
                    System.out.println( val );
                } else {
                    byte[] buf = (byte[])val;
                    for (int i = 0; i < buf.length; i++) {
                        System.out.print(Integer.toHexString(buf[i]) + " ");
                    }
                }
                System.out.println();
            }
        }
    }
}
```

When the schema is extended and the attribute structure, which is not a character string, is specified, use the environment property java.naming.ldap.attributes.binary to be returned as the binary value.

```
env.put("java.naming.ldap.attributes.binary","mpegVideo myspecialkey");
```

Obtaining the Search Result and Accumulating the Connection

The UNBIND command will not be sent straight away if all search results are not extracted or destroyed, even if the session is closed. Connections are accumulated between the client and server until the next time they are closed as follows:

- when the Java VM invokes finalize() upon exit from an application.
- when the Java VM performs garbage collection when the reference to variables in the search results becomes invalid.

If a servlet is run in JNDI or if a program repeatedly opens and closes a connection, problems connecting to the Interstage Directory Service may occur.

To avoid accumulating connections, clear the search result using one of the following methods so that UNBIND is definitely sent out.

- Extracting all the search results:

```
DirContext ctx = new InitialDirContext(env);
NamingEnumeration results = ctx.search("dc=com", "cn=User001",
constraints);
while (results != null && results.hasMore()){
    SearchResult sr = (SearchResult)results.next();
}
```

- Discarding the search results:

```
DirContext ctx = new InitialDirContext(env);
NamingEnumeration results = ctx.search("dc=com", "cn=User001",
constraints);
results.close();
```

8.2.5 Modifying Entries

To modify an entry, a specified attribute can be added / deleted / replaced. An attribute that has not already been specified cannot be modified.

When modifying an entry, use the following method:

```
javax.naming.DirContext.modifyAttributes()
```

Create an attribute list of operation objects using the javax.naming.directory.ModificationItem class. ModificationItem consists of a numeric constant indicating the type of modification to make and the operation object attribute describing the actual modification to make. Specify one of the following as the modification types:

- DirContext.ADD_ATTRIBUTE: addition of attribute value
- DirContext.REMOVE_ATTRIBUTE: deletion of attribute value
- DirContext.REPLACE_ATTRIBUTE: replacement of attribute value.

Three attribute values are changed in the following examples.

- Replace the telephoneNumber attribute value with a new value of 123-456-7890.
- Add the value user001@interstage.fujitsu.com into the mail attribute.
- Delete the title attribute

```
  ModificationItem[] mods = new ModificationItem[3];

  Attribute mod0 = new BasicAttribute("telephoneNumber", "123-456-7890");
  mods[0] = new ModificationItem(DirContext.REPLACE_ATTRIBUTE, mod0);

  Attribute mod1 = new BasicAttribute("mail","user001@interstage.fujitsu.com");
  mods[1] = new ModificationItem(DirContext.ADD_ATTRIBUTE, mod1);

  Attribute mod2 = new BasicAttribute("title");
  mods[2] = new ModificationItem(DirContext.REMOVE_ATTRIBUTE, mod2);
```

This attribute list is specified using the modifyAttributes() method

```
  ctx.modifyAttributes(mod_dn, mods);
```

8.2.6 Adding Entries

To add an entry, use the following method:

```
javax.naming.DirContext.createSubcontext()
```

Specify the DN and the attribute set. The attribute set uses the javax.naming.directory.Attributes and javax.naming.directory.Attribute interfaces.

Examples of adding entries

```
  Attribute objClasses = new BasicAttribute("objectclass");
  objClasses.add("top");
  objClasses.add("person");
  objClasses.add("organizationalPerson");
  objClasses.add("inetOrgPerson");

  Attribute cn    = new BasicAttribute("cn",    "User001"   );
  Attribute sn    = new BasicAttribute("sn",    "Fujitsu"   );
  Attributes orig = new BasicAttributes();
  orig.put(objClasses);
  orig.put(cn);
  orig.put(sn);

  ctx.createSubcontext("cn=User001,ou=User", orig);
```

8.2.7 Deleting Entries

To delete an entry, use the following method:

```
javax.naming.directory.Context.destroySubcontext()
```

Specify the DN of the entry to be deleted.

```
  ctx.destroySubcontext("cn=User001,ou=User");
```

8.2.8 Replacing Names

To replace the DN or RDN, use the following method:

```
javax.naming.directory.Context.rename()
```

Specify the current DN and a new DN. To indicate whether or not the old RDN value is to be deleted from the entry, specify the environment property "javax.naming.ldap.deleteRDN". The initial vale is "true".

- true: delete the old RDN value.
- false: do not delete the old RDN value.

Examples of keeping RDN

```
  env.put("java.naming.ldap.deleteRDN", "false")
  DirContext ctx = new InitialDirContext(env);
  ctx.rename("cn=oldName", "cn=newName");
```

8.2.9 Comparing Attribute Values

Based on attribute value comparison, the value can be determined without reading the attribute value. When comparing attribute values, use the following method:

```
DirContext.search()
```

Although DirContext.search() is used for compare (as well as searching), the following restrictions apply when using to compare:

- In the search filter, specify using "(attribute name = attribute value)" syntax.

  Wildcards cannot be used when using the function for a compare operation.
- In the search object scope, specify OBJECT_SCOPE.
- In the option "Attribute to acquire the search result", specify nothing to notify.

Examples of comparing the attribute values

```
  SearchControls constraints = new SearchControls();
  constraints.setSearchScope(SearchControls.OBJECT_SCOPE);
  constraints.setReturningAttributes(new String[0]);

  NamingEnumeration results = ctx.search("cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com",
                              "mail=user001@sample.fujitsu.com", constraints);
```

8.2.10 Closing a Session

After you have completed processing on an Interstage Directory Service, close a session.

Example:

```
ctx.close();   *
```

Note

ctx is an instance variable acquired as described in 'Opening a session and performing initial setup and user authentication.'

8.2.11 Compile Link

Set the environment variables required for running the compile and application.

Windows32/64

If using SSL, set up the following Java Archive (jar) files in CLASSPATH.

- C:\Interstage\lib\irepssl.jar

In JAVA_HOME, the following value has been automatically set during installation.

- For JDK 6

  C:\Interstage\JDK6

In PATH, set the following directory:

- C:\Interstage\lib

Solaris32/64 Linux32/64

If using SSL, set up the following Java Archive (jar) files in CLASSPATH.

- /opt/FJSVirepc/lib/irepssl.jar

In JAVA_HOME, set either of the following directories:

- For JDK 6

  /opt/FJSVawjbk/jdk6

In LD_LIBRARY_PATH, set the following directory:

- /opt/FJSVirepc/lib

When executing the created .class file, set up the storage path of the created .class file in CLASSPATH.

8.3 Sample Programs

Windows32/64

JNDI sample programs are stored in 'C:\Interstage\IREPSDK\sample\JAVA.'

Solaris32/64 Linux32/64

JNDI sample programs are stored in '/opt/FJSVirepc/sample/JAVA.'

8.3.1 List of Sample Program Files

The following is a list of source documents for JNDI sample programs:

Source name	Overview of processing
SampleBase.java	Session opening, initial settings and user authentication
SampleSearch.java	Entry search
SampleSearchScope.java	Search that uses the search scope
SampleSearchRetAttrs.java	Search that uses the attribute to acquire the result
SampleSearchSizeLimit.java	Search that uses a maximum number of entry of result
SampleSearchTimeLimit.java	Search that uses a maximum waiting period for result
SamplePrintResult.java	Displaying the search result
SampleModAttrs.java	Changing the attribute value (add/change/delete)
SampleAdd.java	Adding entry
SampleAddByte.java	Adding entry that includes the binary attribute value
SampleDelete.java	Deleting entry
SampleModrdn.java	Changing name
SampleCompare.java	Comparing the attribute value

8.3.2 Execution Procedure of a Sample Program

This section explains the procedures from compilation to execution of a sample program.

1. Copy all the files in the sample program storage directory to a work directory.
2. Change the "Write" authority settings for the work directory and the directory owner.

   chmod -R +w example

   chown -R owner:group example

3. Modify the parameter values in the sample source according to the environment of the Interstage Directory Service to be connected. For the applicable parameters, refer to comments in the sample source.
4. Compile the sample program based on the following compilation example. After compilation is executed, check that a class file has been created.

   Example

   The following shows a compilation example.

   To use JDK 6, enter:

   Windows32/64

   ```
   C:\Interstage\JDK6\bin\javac SampleSearch.java
   ```

   Solaris32/64 Linux32/64

   ```
   /opt/FJSVawjbk/jdk6/bin/javac SampleSearch.java
   ```

   After compilation, a 'SampleSearch.class' file will be created.

5. Set up the storage path for the created .class file in CLASSPATH and execute the sample program as shown in the following execution example:

   Example

   The following text provides an example of execution.

   To use JDK 6, enter:

   Windows32/64

   ```
   C:\Interstage\JDK6\bin\java SampleSearch
   ```

   Solaris32/64 Linux32/64

   ```
   /opt/FJSVawjbk/jdk6/bin/java SampleSearch
   ```

Chapter 9 Creating an Application (C API)

This chapter explains how to create applications in C using Interstage Directory Service APIs.

9.1 Application Development Environment

Refer to "Software Products Required for Application Development" in the "Supported Software" chapter of the Product Notes.

9.2 Before Creating an Application

The following should be noted when creating an application in C using Interstage Directory Service API's.

DN Containing Special Characters

If symbols are contained in the DN, they are treated as special characters. If special characters are used, a backslash ("\") escape character must be placed before the special character, or the special character must be enclosed in double quotation marks (""").

Special characters are as follows:

- Comma (,)
- Plus sign (+)
- Double quotation marks (")
- Less than sign (<)
- Greater than sign (>)
- Semicolon (;)
- Hash (#) Note: These can only be used as the DN start character.

The example DN below is one that contains a backslash (\) character in the cn attribute, and this backslash is not being used as an escape character, it is part of the cn value:

```
cn=a\b,o=Fujitsu, Inc.,c=jp
```

In LDAP and C, the backslash (\) is also treated as a special character. Some examples are shown below.

As shown above the DN, the cn attribute value contains a backslash (\) character:

```
a\b
```

The backslash (\) escape character must be added because of the LDAP rule:

```
cn=a\\b
```

In addition to the LDAP rule, there is the C rule; therefore each backslash must be preceded with another backslash as its escape character.

```
char *name1 = "cn=a\\\\b";
```

In C therefore, the DN shown above is specified as follows:

```
char *name = "cn=a\\\\b,o=Fujitsu\\, Inc.,c=jp";
```

Commas (,) and double quotation marks (") are specified as follows:

```
char *name2 = "cn=a\\,b";
char *name3 = "cn=a\\\"b";
```

Specifying the Search Filter Using Symbols

Some symbols that can be used as values in search filters are treated as special characters. These special characters must be specified with the hexadecimal number next to the (\\) yen mark (backslash) .

Special characters are as follows:

- Asterisk (*)
- Open Bracket (( )
- Close Bracket ( ))
- Backslash (\ )

Example

The search for "o=Fujitsu(C)" is expressed in C as follows,

```
"o=Fujitsu\\28C\\29"
```

For details of search filters refer to "Search Filters" in the "Entry Management" chapter.

Using C APIs in Multithread Environment

The LDAP APIs support multithreading with the exception of ldapssl_init(). However, multiple threads cannot share one session. If multiple threads communicate with the Interstage Directory Service, each thread must open its own session.

9.3 Creation of Source Program

9.3.1 Procedure for Application Processing

The client must be processed in the following order to access the Interstage Directory Service.

1. Pre-processing

   Open sessions, initial settings and user authentication (simple authentication by password)

2. Access to Interstage Directory Service

   The following requests can be made to Interstage Directory Services:

   - Searching for entries
   - Changing entry attribute values
   - Adding entries
   - Deleting entries
   - Changing the DN (or RDN) of an entry
   - Comparing entry attribute values

3. Post-processing

   Closing sessions

9.3.2 Session Open and Initial Settings

Before starting communications with the Interstage Directory Service, the session initialization and session handle option settings must be implemented for the client.

Opening the Session

Open the client session using the following functions.

For details on how to use this function, refer to "Interface for Opening and Closing Sessions" in the "C Interface" chapter of the Reference Manual (API Edition).

- LDAP *ldap_init(const char *hostname, int portno):

  This function opens a session initializing it without SSL communication.

- LDAP *ldapssl_init(const char *hostname, int portno, SSLENV *sslenv):

  This function opens a session initializing it using SSL communication.

These functions return the session handle for identification. An opened session cannot be shared by multiple threads, therefore if using multiple threads open one session for each thread.

- **SSL communication is not used**

  The session is opened with ldap_init()

  Example

```
LDAP    *ld;

/* Opening sessions */
ld = ldap_init( "hostname", 389 );
if ( ld == NULL ) {
    /* Process when an error occurred */
    return -1;
}
```

- **Using SSL communication**

  In a client API library, secure communications can be performed with an Interstage Directory Service using SSL. When using the SSL protocol, sessions are opened with ldapssl_init() instead of ldap_init(). Use ldapssl_error() to access error codes from the SSL library. Only the Fujitsu SSL library can be used in this version.

  When building the SSL environment on a client, SSL settings must be configured to match those of the server which is performing these communications. For details on setting up this environment, refer to "Setup of an SSL Communication Environment (Between Client and Server)" in the "Setting up an Environment for SSL Communication" chapter.

  Example

```
LDAP    *ld;
SSLENV  sslenv

memset( sslenv, 0x00, sizeof(SSLENV) );
sslenv->ssl_version = 3;
sslenv->crypt       = "RSA-3DES-SHA:RSA-DES-SHA";
sslenv->tkn_lbl     = "Token01";
sslenv->tkn_pwd     = "userpin";
sslenv->slot_path   = "/sslenv/slot";
sslenv->cert_path   = (unsigned char *)"/sslenv/sslcert";

/* Opening sessions using SSL */
ld = ldapssl_init( "hostname", 636, &sslenv );
if ( ld == NULL ) {
    /* Process when an error occurred */
    return -1;
}
```

  SSLENV is the structure address used to define the SSL environment for the client, and information is specified in sslenv.

  When an error occurs in the ldapssl_init() SSL library, an error code is set in ssl_err, and ssl_err_detail member. ldapssl_error() is used to refer to the SSL library error code that occurred in the function after ldapssl_init().

Session initial settings

The client can set up or refer to the operation environment per applicable session for the session handle option.

The client uses the following functions to execute session handle option settings/reference:

- ldap_set_option(LDAP *ld, int option, const void *optdata):

  This function sets the session handle option.

- ldap_get_option(LDAP *ld, int option, const void *optdata):

  This function references the session handle option value.

The following items can be set up and referred to

- Maximum number of entry for search result
- Maximum waiting period for search result
- Operation at interruption
- LDAP protocol version
- Repository host name and a port number for the default connection
- Latest LDAP error number
- Latest LDAP error message
- Maximum waiting period for a connection response
- Initialization and process completion for Windows Sockets DLL Windows32/64

- **Specifying the LDAP version**

  If the LDAP protocol version is not specified, the LDAP V2 protocol is used. The LDAP V2 protocol is not supported in the Interstage Directory Service, so specify the LDAP V3 protocol in the session handle option.

  ```
  /* Option settings ( LDAP_VERSION3 ) */
  optdata = LDAP_VERSION3;
  rtn = ldap_set_option( ld, LDAP_OPT_PROTOCOL_VERSION, (void *)(&optdata) );
  ```

  For details on how to use this function, refer to "Interface for Session Handle Option Settings/Reference" in the "C Interface" chapter of the Reference Manual (API Edition).

9.3.3 User Authentication

After the opening of the session/default settings is completed, user authentication must be performed before the Interstage Directory Service can be accessed. The following functions are used in user authentication:

- ldap_simple_bind(LDAP *ld, const char *dn, const char *passwd):

  Used for asynchronous type simple authentication

- ldap_simple_bind_s(LDAP *ld, const char *dn, const char *passwd):

  Used for synchronous type simple authentication

Example

```
/* Simple authentication */
char    *dn = "cn=manager,ou=interstage,o=fujitsu,dc=com";
char    *passwd = "secret";
rtn = ldap_simple_bind_s( ld, dn, passwd );
if ( rtn != LDAP_SUCCESS ) {
    /* Process when an error occurred */
    ldap_unbind_s( ld );
    return -1;
}
```

Administrator DN or user entry DN is specified in dn (Binding DN).

If the LDAP V3 protocol is used, user authentication can be omitted. If user authentication is omitted, access to the Interstage Directory Service is processed as anonymous.

9.3.4 Searching for Entries

If a request to search for entries is made to the Interstage Directory Service, the entry information that matched with the search conditions will be sent.

The following functions are used to search for entries:

- ldap_search(LDAP *ld, const char *base, int scope, const char *filter, char **attrs, int attrsonly):

  Asynchronous type search

- ldap_search_s(LDAP *ld, const char *base, int scope, const char *filter, char **attrs, int attrsonly, LDAPMessage **res):

  Synchronous type search

Basic Search Method

The search base (search start position), search ranges, and search filter will be specified for basic search.

The search ranges can be narrowed down by combining the following parameters:

- **Search base**

  Specify the DN of the search base entry. This cannot be omitted.

- **Search execution range**

  Specify one of the following search ranges:

  - Search the level specified in the search base

  - Search one level under the specified search base

  - Search all levels of the specified search base

- **Search filter**

  The search condition format is "cn=User001". When NULL is specified, all of the usable searched entries are returned.

  The following is an example of a synchronous type search:

```
  /* Entry search */
  rtn = ldap_search_s( ld, "ou=interstage,o=fujitsu,dc=com", LDAP_SCOPE_SUBTREE, "cn=User001",
NULL, 0, &result );
  if ( rtn != LDAP_SUCCESS ) {
      /* Process when an error occurred */
      return -1;
  }
```

Advanced Search Method

In addition to the basic search method, advanced features such as limiting the number of targets, setting a maximum number of results to display, and setting a timeout value can be used.

These methods are explained below.

1. Limit the search to a specific attribute

   A specific attribute can be specified for the search.

```
  char  *attrs[] = { "cn", "telephonenumber","mail", NULL };
  ......
  rtn = ldap_search_s( ld, "ou=interstage,o=fujitsu,dc=com", LDAP_SCOPE_SUBTREE, "cn=User001",
attrs, 0, &result );
```

   When NULL is included, all attributes that match the search conditions will be sent.

2. Search only for the DN

   Only the DN can be returned in the search result

```
  char  *attrs[] = { LDAP_NO_ATTRS, NULL };
  ......
  rtn = ldap_search_s( ld, "ou=interstage,o=fujitsu,dc=com", LDAP_SCOPE_SUBTREE, "cn=User001",
attrs, 0, &result );
```

3. Set a limit for the number of entries for the search result

   Set a maximum number of entries for the search result using the session handle option LDAP_OPT_SIZELIMIT.

```
  int sizelimit = 3;
  rtn = ldap_set_option( ld, LDAP_OPT_SIZELIMIT, (void *)(&sizelimit) );
```

   A maximum entry number can be limited using the function without the session handle.

   - ldap_search_ext(LDAP *ld, const char *base, int scope, const char *filter, char **attrs, int attrsonly, LDAPControl **serverctrls, LDAPControls clientctrls, struct timeval *timeout, int sizelimit, int *msgidp)

     Search an asynchronous type

   - ldap_search_ext_s(LDAP *ld, const char *base, int scope, const char *filter, char **attrs, int attrsonly, LDAPControl **serverctrls, LDAPControls clientctrls, struct timeval *timeout, int sizelimit, LDAPMessage **res)

     A n example of a synchronous type search:

```
  int sizelimit = 3;
  rtn = ldap_search_ext_s( ld, "ou=interstage,o=fujitsu,dc=com", LDAP_SCOPE_SUBTREE,
"cn=User001", NULL, 0, NULL, NULL, NULL, sizelimit, &result );
```

4. Set a maximum waiting period for the search result

   A maximum waiting period for the search result can be set in seconds, using the session handle option LDAP_OPT_TIMELIMIT.

```
  int timelimit = 5;
  rtn = ldap_set_option( ld, LDAP_OPT_TIMELIMIT, (void *)(&timelimit) );
```

   The following functions can also be used.

   - ldap_search_st(LDAP *ld, const char *base, int scope, const char *filter, char **attrs, int attrsonly, struct timeval *timeout, LDAPMessage **res)

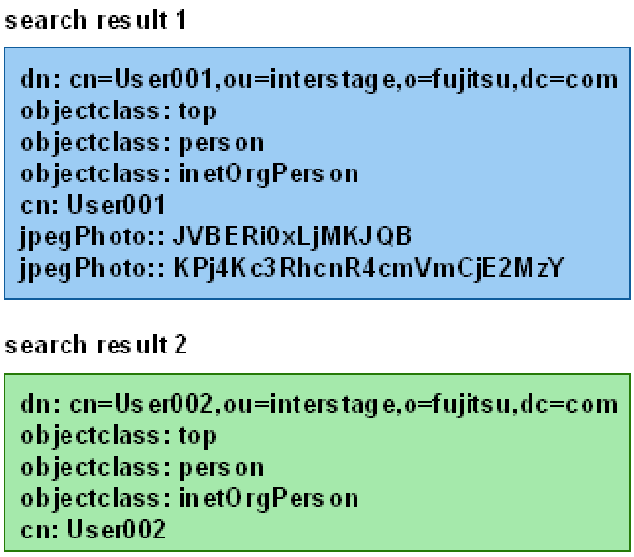
     An example of a synchronous type search with a time limit set:

```
  timeout.tv_sec  = 5L; /* unit per second */
  timeout.tv_usec = 0L; /* unit per micro second */
  rtn = ldap_search_st( ld, "ou=interstage,o=fujitsu,dc=com", LDAP_SCOPE_SUBTREE,
"cn=User001", NULL, 0, &timeout, &result );
```

     A maximum waiting period can also be specified using ldap_search_ext(),ldap_search_ext_s().

9.3.5 Analyzing the Search Result

An example of the search result is displayed in the LDIF image below; it demonstrates how to analyze the search result.



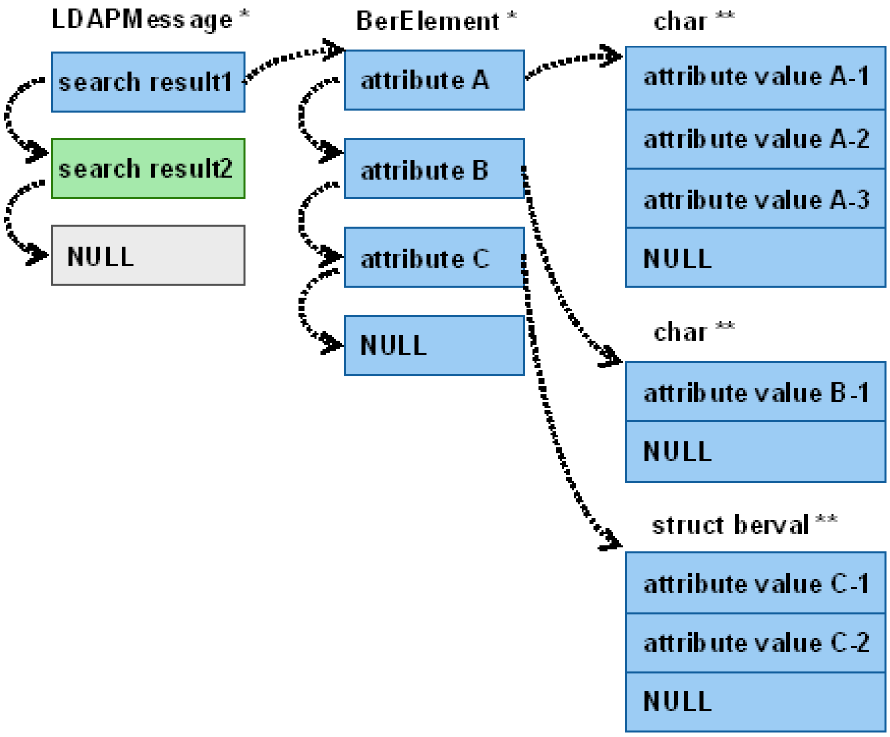
search result 1

```
dn: cn=User001,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: inetOrgPerson
cn: User001
jpegPhoto:: JVBERi0xLjMKJQB
jpegPhoto:: KPj4Kc3RhcnR4cmVmCjE2MzY
```

search result 2

```
dn: cn=User002,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: inetOrgPerson
cn: User002
```

The search result will be returned with the following structure



Search results can be analyzed by "Analyzing Entries", "Referencing Attributes", "Reading Attribute Values" and "Reading and Analyzing the DN".

Analyzing Entries

The entries contained in the search result can be referenced using the following functions.

- ldap_first_entry(LDAP *ld, LDAPMessage *res):

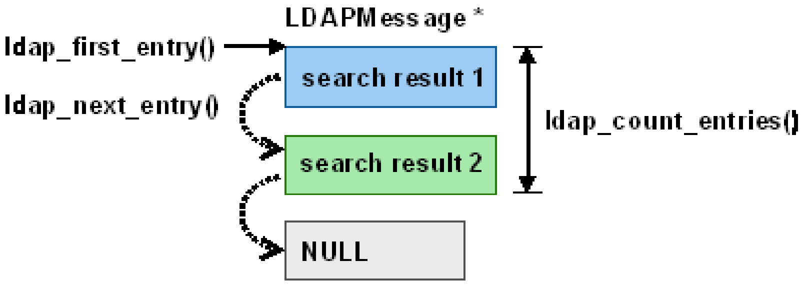
  Requests the address of the start entry

- ldap_next_entry(LDAP *ld, LDAPMessage *entry):

  Requests the address of the next entry

- ldap_count_entries(LDAP *ld, LDAPMessage *res):

  Requests the entry number



Example code for analyzing entries:

```
int  finished;
int  num_entry;
LDAPMessage *entry;
:
/* Perform asynchronous type search */
msgid = ldap_search( ld, basedn, LDAP_SCOPE_SUBTREE, filter, NULL, 0 );

/* Receive the search result */
finished = 0;
while ( finished == 0 ) {
  rtn = ldap_result( ld, msgid, LDAP_MSG_ALL, &timeout, &result );
  switch( rtn ) {
case 0: /* timeout */
      break;
case -1: /* error occurred */
      return 1:
default: /* success */
      finished = 1;
      break;
  }
}

/* Check the number of entries in the search result  */
num_entry = ldap_count_entries(ld, result);
if( num_entry == 0){
    fprintf( stderr, "Not matched.\n" );
    return 0;
}

/* Read the search result  */
entry = ldap_first_entry( ld, result );
for ( ; entry != NULL; entry = ldap_next_entry( ld, entry ) ) {
    Referencing Attributes
}
```

Referencing Attributes

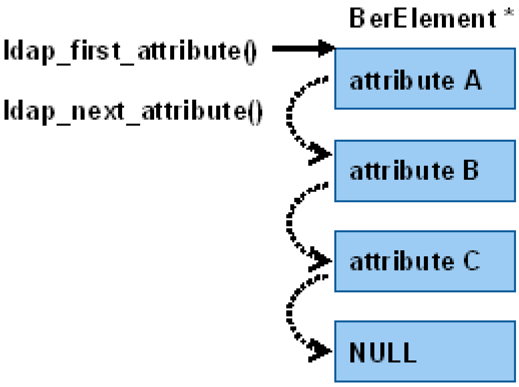
The following functions can be used to obtain the attribute name within the entry:

- ldap_first_attribute(LDAP *ld, LDAPMessage *entry, BerElement **ptr):

  Requests the first attribute in the entry

- ldap_next_attribute(LDAP *ld, LDAPMessage *entry, BerElement **ber):

  Requests the next attribute in the entry



Example code to obtain the attribute name:

```
char *attr;
BerElememt *ber;
  :
entry = ldap_first_entry( ld, result );
attr = ldap_first_attribute( ld, entry, &ber );
for ( ; attr != NULL; attr = ldap_next_attribute( ld, entry, ber ) ) {
  Reading Attribute Values
  ldap_memfree(attr);
}
```

Reading Attribute Values

Attributes in the entry can be referenced using the following functions:

- ldap_get_values(LDAP *ld, LDAPMessage *entry, const char *attr):

  Reads the specified attribute value, and notifies it as string data

- ldap_get_values_len(LDAP *ld, LDAPMessage *entry, const char *attr):

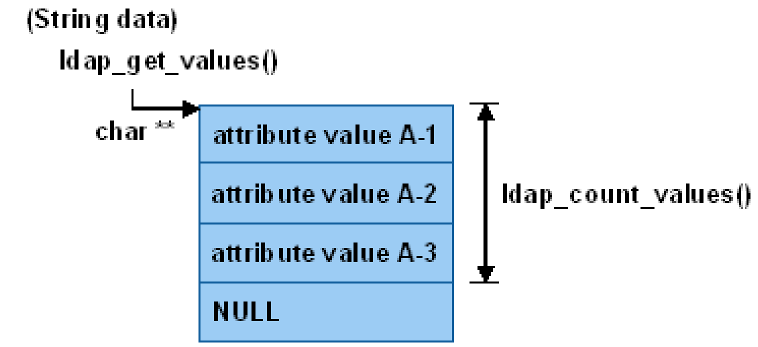
  Reads the specified attribute value, and notifies it as binary format data

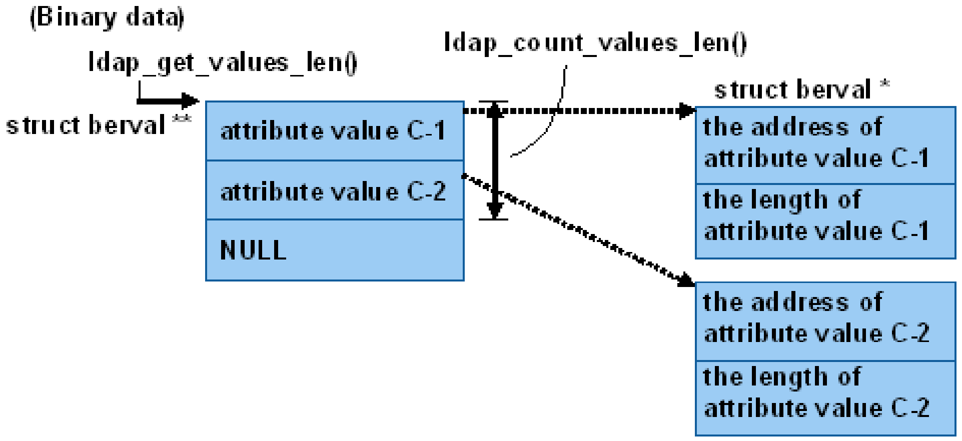
- ldap_count_values(char **vals):

  Reads the attribute value number that is returned in ldap_get_values()

- ldap_count_values_len(struct berval **vals):

  Reads the attribute value number that is returned in ldap_get_values_len()




(Binary data)
ldap_get_values_len()
ldap_count_values_len()
struct berval **
attribute value C-1
attribute value C-2
NULL
struct berval *
the address of attribute value C-1
the length of attribute value C-1
the address of attribute value C-2
the length of attribute value C-2

The ldap_get_values() and ldap_count_values() functions are used when the attribute value is treated as string data. For this reason, they cannot be used for attributes for which binary data is set.

The ldap_get_values_len() and ldap_count_values_len() functions are used when the attribute value is treated as binary data.

For details of the format for the returned attribute value, refer to "Interface for Reading Attribute Values" in the "C Interface" chapter of the Reference Manual (API Edition).

Example code to obtain the attribute value

```
LDAPMessage   *entry;
char          *attr;
char          **vals;
int           i;
struct berval  **bervals;
int           count;

vals = ldap_get_values( ld, entry, attr );
if( vals == NULL ){
    return -1;
}
count = ldap_count_values( vals );
for ( i=0; i<count; i++ ) {
    printf( "%s: %s\n", attr, vals[i] );
}
```

Reading and Analyzing the DN

Use ldap_get_dn() to reference the entry DN.

- ldap_get_dn(LDAP *ld, LDAPMessage *entry)

  Read the DN of the specified entry

To explode the DN in each configuration element and request an RDN, use ldap_explode_dn().

- ldap_explode_dn(const char *dn, int notypes)

  The specified DN is broken down into each structure element

At this time, the "notypes" parameter can be specified to extract from the RDN in a format without attributes.

To explode the RDN in a configuration element, use ldap_explode_rdn().

- ldap_explode_rdn(const char *rdn, int notypes)

  The specified RDN is broken down into each structure element

For details of the functions used for reading and analyzing the DN, refer to "Interface for Reading/Analyzing the DN" in the "C Interface" chapter of the Reference Manual (API Edition).

9.3.6 Changing Entries

When an entry is changed, the specified attribute can be added/deleted/replaced. Attributes that are not specified are not changed.

The following functions are used for changing entries:

- ldap_modify(LDAP *ld, const char *dn, LDAPMod **mods):

  Update the entry asynchronously

- ldap_modify_s(LDAP *ld, const char *dn, LDAPMod **mods):

  Update the entry synchronously

Specify the following parameters in the client to change an entry:

- Entry DN

  Specify the DN of the entry to be changed.

- Operation attributes

  Specify the following parameters for each operation attribute:

  - Change Attribute

    Specify the operation attribute.

  - Change Operation Type

    Specify add, delete, or replace.

  - Attribute Value Type

    Specify string data or binary data.

  - Attribute Value (more than one value can be specified)

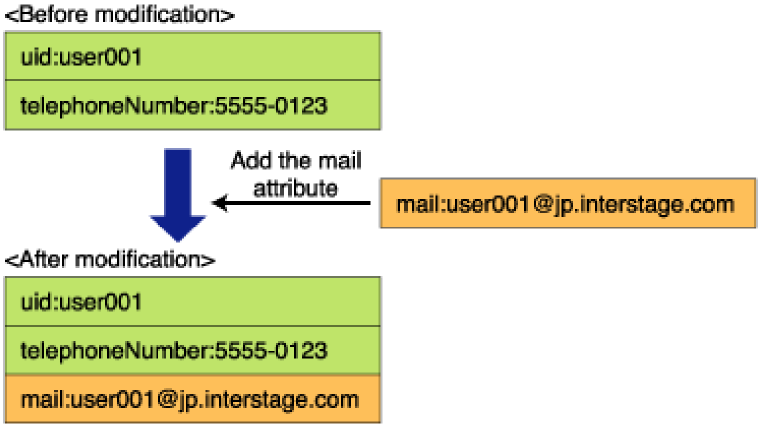
    Specify the attribute value.

The Interstage Directory Service processes according to the specified Change Operation Type, as shown below.

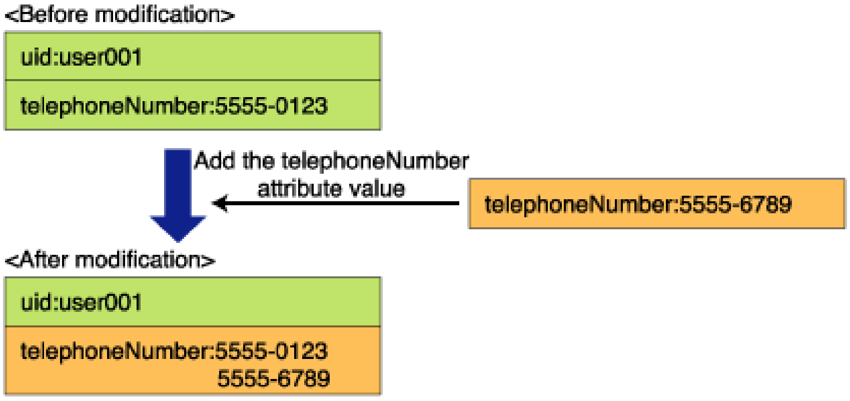
9.3.6.1 Adding Attribute Values

Add the specified attribute and attribute value to the entry.

The following figure shows how an attribute value is added.


<Before modification>
uid:user001
telephoneNumber:5555-0123
Add the mail attribute
mail:user001@jp.interstage.com
<After modification>
uid:user001
telephoneNumber:5555-0123
mail:user001@jp.interstage.com

If an existing attribute is specified, the attribute value is added to the specified attribute.


<Before modification>
uid:user001
telephoneNumber:5555-0123
Add the telephoneNumber attribute value
telephoneNumber:5555-6789
<After modification>
uid:user001
telephoneNumber:5555-0123
5555-6789

Specifying binary data in the attribute value

The Berval structure is used to specify binary data in attribute values. To indicate that binary data is registered, specify LDAP_MOD_BVALUES in LDAPMod structure mod_op member using an OR operation. Then, specify a berval structure in the mod_bvalues member.

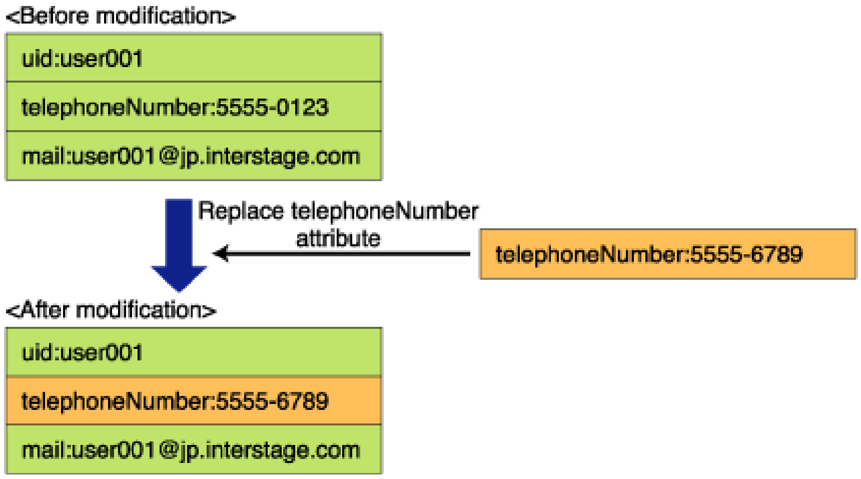
Example code to specify binary data in the attribute value

```
LDAPMod   **mods[];
struct berval  berval;
struct berval  *ber_array[2];

readBinary( filename, &berval);
ber_array[0] =berval;
ber_array[1] =NULL;

mods[0]->mod_op   = LDAP_MOD_ADD | LDAP_MOD_BVALUES;
mods[0]->mod_type = "jpegPhoto";
mods[0]->mod_bvalues = ber_array;

rtn = ldap_modify_s( ld, mod_dn, mods );
```

9.3.6.2 Replacing Attribute Values

The specified attribute value replaces the value specified in the client.

The following figure shows how a value is replaced.


<Before modification>
uid:user001
telephoneNumber:5555-0123
mail:user001@jp.interstage.com
Replace telephoneNumber attribute
telephoneNumber:5555-6789
<After modification>
uid:user001
telephoneNumber:5555-6789
mail:user001@jp.interstage.com

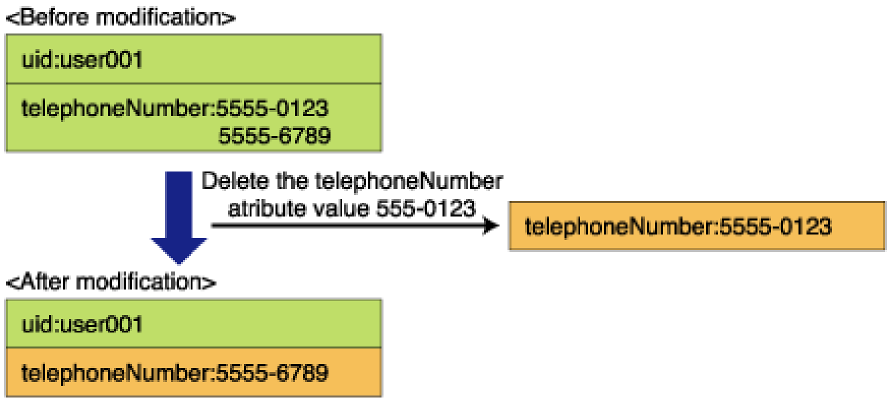
Example of code to replace attribute values

```
LDAPMod **mod;
char    *vals[] = {"5555-0123", "5555-6789", NULL};

mod[0]->mod_op    = LDAP_MOD_REPLACE;
mod[0]->mod_type = "telephoneNumber";
mod[0]->mod_values = vals;

rtn = ldap_modify_s( ld, mod_dn, mod );
```

9.3.6.3 Deleting Attribute Values

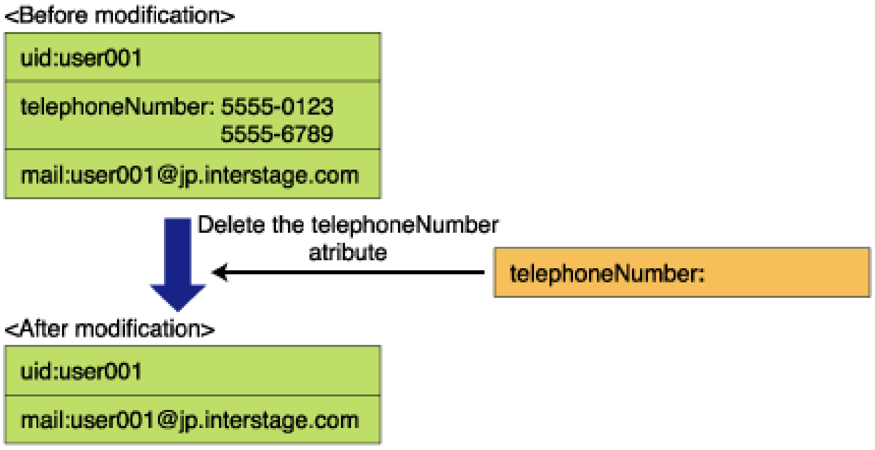
Clients can delete the value of specified attributes. If there is one entry attribute value, it is deleted at this time.

The following figure shows how an attribute value is deleted.


<Before modification>
uid:user001
telephoneNumber:5555-0123
5555-6789
Delete the telephoneNumber atribute value 555-0123
telephoneNumber:5555-0123
<After modification>
uid:user001
telephoneNumber:5555-6789

```
Example of code to delete an attribute value

  LDAPMod mod1;
  char    *vals1[ 2 ];
  vals1[0] = "5555-0123";
  vals1[1] = NULL;
  mod1.mod_op    = LDAP_MOD_DELETE;
  mod1.mod_type = "telephoneNumber";
  mod1.mod_values = vals1;

  rtn = ldap_modify_s( ld, mod_dn, mod1 );
```

If the attribute is specified and the value is not, the attribute will be deleted.


<Before modification>
uid:user001
telephoneNumber: 5555-0123
5555-6789
mail:user001@jp.interstage.com
Delete the telephoneNumber
atribute
telephoneNumber:
<After modification>
uid:user001
mail:user001@jp.interstage.com

9.3.7 Adding Entries

The following functions are used to add entries:

- ldap_add(LDAP *ld, const char *dn, LDAPMod **attrs):

  Add entry asynchronously.

- ldap_add_s(LDAP *ld, const char *dn, LDAPMod **attrs):

  Add entry synchronously.

To add an entry to the directory tree, specify the following parameters in the client:

- Entry DN

  Specify the DN to be created.

- Collect entry attribute

  Specify the attribute and the collected attribute values for the entry to be created. Specify the following in each attribute specified here:

  - Attribute

    Specify the name of the attribute.

  - Attribute Value Type

    Specify string data or binary data.

  - Attribute Value

    Specify the attribute value that is set in this attribute. More than one value can be specified.

Example of code to add an entry

```
  LDAPMod    **mods;
  char        *objectclass_values[] = { "top", "person", "organizationalPerson", "inetOrgPerson",
NULL};
  char        *userpassword_values[]    = { "pass001", NULL };
  char        *telephonenumber_values[] = { "001-9999-5555", NULL };
  char        *title_values[]           = { "chief engineer", NULL };
  char        *sn_values[]              = { "Fujitsu", NULL };
  char        *cn_values[]              = { "User001", NULL };
  char        *dn;

  mods[0]->mod_op     = 0;
  mods[0]->mod_type   = "objectclass";
  mods[0]->mod_values = objectclass_values;

  mods[1]->mod_op     = 0;
```

```
mods[1]->mod_type   = "userpassword";
mods[1]->mod_values = userpassword_values;

mods[2]->mod_op     = 0;
mods[2]->mod_type   = "telephonenumber";
mods[2]->mod_values = telephonenumber_values;

mods[3]->mod_op     = 0;
mods[3]->mod_type   = "title";
mods[3]->mod_values = title_values;

mods[4]->mod_op     = 0;
mods[4]->mod_type   = "sn";
mods[4]->mod_values = sn_values;

mods[5]->mod_op     = 0;
mods[5]->mod_type   = "cn";
mods[5]->mod_values = cn_values;

mods[6] = NULL;

dn = "cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com";

rtn = ldap_add_s( ld, dn, mods );
if ( rtn != LDAP_SUCCESS ) {
    /* Process when an error occurred */
    return -1;
}
```

9.3.8 Deleting Entries

The following functions are used to delete entries:

- ldap_delete(LDAP *ld, const char *dn):

  Delete entry asynchronously.

- ldap_delete_s(LDAP *ld, const char *dn):

  Delete entry synchronously.

To delete an entry, specify the DN of the entry as a parameter in the client.

Example of code to delete an entry

```
char *dn;
dn = "cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com";
rtn = ldap_delete_s( ld, dn );
if ( rtn != LDAP_SUCCESS ) {
    /* Process when an error occurred */
    return -1;
}
```

9.3.9 Changing Names

The following functions are used to change the DN or RDN:

- ldap_rename(): Asynchronous type renaming

- ldap_rename_s(): Synchronous type renaming

For details of the specifications for each function, refer to "Interface for Changing Entry Names" in the "C Interface" chapter of the Reference Manual (API Edition). To change the DN or RDN of an entry, specify the following parameters in the client:

- Current DN

  Specify the DN of the entry to be changed.

- New RDN

  Specify the new RDN of the entry to be changed.

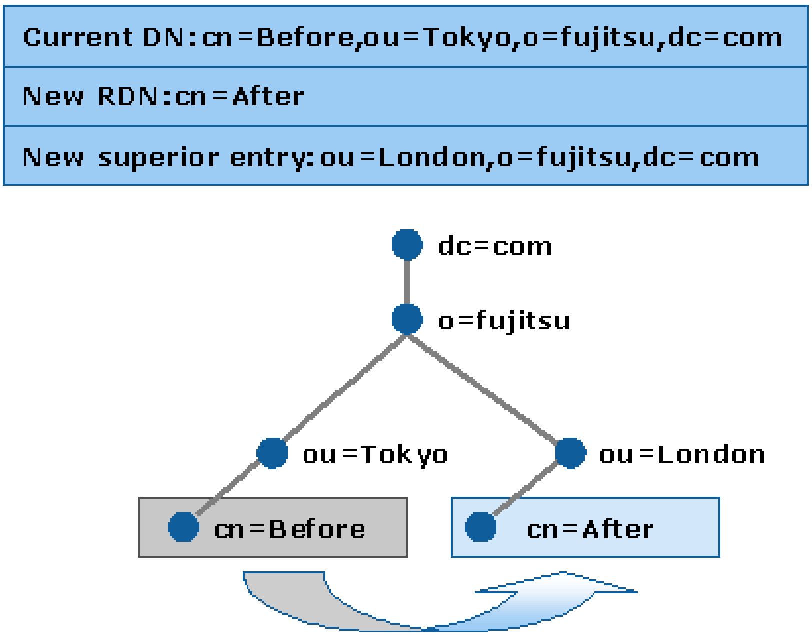
- New superior entry

  Specify the entry to which the new entry is to be allocated.

- Process the original RDN

  Specify whether or not to delete the attribute value that corresponds to the original RDN from the entry:

  - Delete the attribute value that corresponds to the original RDN (Values other than 0 can be specified)
  - Do not delete the attribute value that corresponds to the original RDN (0 is used in this case)


Current DN:cn=Before,ou=Tokyo,o=fujitsu,dc=com
New RDN:cn=After
New superior entry:ou=London,o=fujitsu,dc=com
dc=com
o=fujitsu
ou=Tokyo
ou=London
cn=Before
cn=After

Example of code to change names

```
char   *dn;
char   *newrdn;
char   *newparent;

dn        = "cn=Before,ou=Tokyo,o=fujitsu,dc=com";
newrdn    = "After";
newparnt  = "ou=London,o=fujitsu,dc=com";
rtn = ldap_rename_s( ld, dn, new_rdn, newparent, 0, NULL, NULL );
if ( rtn != LDAP_SUCCESS ) {
    /* Process when an error occurred */
    return -1;
}
```

9.3.10 Comparing Attribute Values

Compare the attribute values to determine a value without reading the attribute value. The following functions are used to search for attribute values to be compared:

- ldap_compare(LDAP *ld, const char *dn, const char *attr, const char *value):

  Compare value asynchronously.

- ldap_compare_s(LDAP *ld, const char *dn, const char *attr, const char *value):

  Compare value synchronously.

Specify the following parameters in the client to compare the attribute values:

- Entry DN

  Specify the DN of the entry to be compared.

- Attribute to be compared

  Specify the attribute to be compared.

- Value to be compared

  Specify the value to be compared. Specify string data.

The Interstage Directory Service determines whether or not the attribute value of the specified entry matches the value specified in the client.

Example of code to determine whether the "mail" attribute has a value of "user001@sample.fujitsu.com"

```
attr = "mail";
value = "user001@sample.fujitsu.com";
rtn = ldap_compare_s( ld, dn, attr, value );
switch ( rtn ) {
case LDAP_COMPARE_TRUE:
    printf( "Matched.\n" );
    break;
case LDAP_COMPARE_FALSE:
    printf( "Not matched.\n" );
    break;
default:
    /* Process when an error occurred */
    return -1;
}
```

9.3.11 Closing the Session

Upon completion of processing the Interstage Directory Service session can be closed using the following functions:

- ldap_unbind(LDAP *ld):

  Synchronous type UNBIND processing

- ldap_unbind_s(LDAP *ld):

  Synchronous type UNBIND processing

When UNBIND processing is complete, all connections with resources used in the session are released. ldap_unbind() and ldap_unbind_s() differ in name only.

9.3.12 Asynchronous Operation

It is possible to receive processing results in a specified time after an asynchronous request is sent to Interstage Directory Service from an application when using an asynchronous operation.

9.3.12.1 Execution of Asynchronous Operation

The following are the functions of major asynchronous operations.

- ldap_simple_bind(LDAP *ld, const char *dn, const char *passwd)

  Request an asynchronous type simple authentication for the repository server.

- ldap_search(LDAP *ld, const char *base, int scope, const char *filter, char **attrs, int attrsonly)

  Perform asynchronous search.

ldap_modify(LDAP *ld, const char *dn, LDAPMod **mods)

Change entry asynchronously.

- ldap_add(LDAP *ld, const char *dn, LDAPMod **attrs)

  Add entry asynchronously.

- ldap_delete(LDAP *ld, const char *dn)

  Delete entry asynchronously.

- ldap_rename(LDAP *ld, const char *dn, const char *newrdn, const char *newparent, int deleteoldrdn, LDAPControl **serverctrls, LDAPControl **clientctrls, int *msgidp)

  Change the name of the entry asynchronously.

- ldap_compare(LDAP *ld, const char *dn, const char *attr, const char *value)

  Compare the attribute value asynchronously.

9.3.12.2 Operating Result Information

Receiving "result" Information

ldap_result () must be called to receive the "result" information (processing result) that is sent from the Interstage Directory Service.

- ldap_result(LDAP *ld, int msgid, int all, struct timeval *timeout, LDAPMessage **resp)

  Receives the process result or search result of asynchronous functions

When ldap_result() is called, it waits until the "result" information is received from the Interstage Directory Service, then returns the information to the call source. The following parameters are specified in ldap_result():

- Message ID

  Specify the value that is returned when the asynchronous type function is issued.

  Specify the message ID of the function to wait for specific asynchronous type function "result" information. If you do not require a specific asynchronous type function for waiting, specify LDAP_RES_ANY.

- Receive process type

  Specify the process type for receiving the processing result:

  - Receive All (receive up until receipt of the last item and then return)

  - Receive in Sequence (receive one item and then return)

  - Notify received messages (read the received messages)

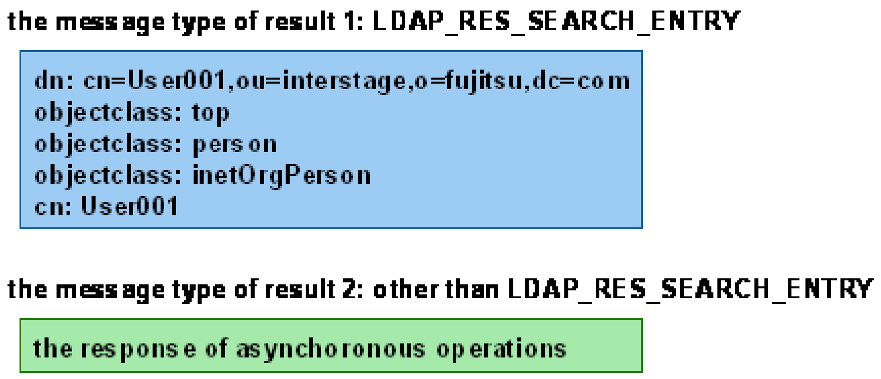
  If Receive All is specified, the information is returned to the call source after the last message is received. If Receive in Sequence is specified, when a message is received it is returned to the call source at once.

- Wait Timer

  If a message is not received within the time specified here, LDAP_TIMEOUT is returned to the call source.

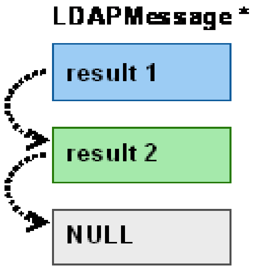
ldap_result() returns the received "result" information type as the function return value. This can be used to determine the asynchronous processing to which the "result" information applies. For details of ldap_result(), refer to "Interface for Receiving/Analyzing Processing Results" in the "C Interface" chapter of the Reference Manual (API Edition).

The example below describes how to analyze the process result.


the message type of result 1: LDAP_RES_SEARCH_ENTRY
the message type of result 2: other than LDAP_RES_SEARCH_ENTRY
the response of asynchoronous operations

```
dn: cn=User001,ou=interstage,o=fujitsu,dc=com
objectclass: top
objectclass: person
objectclass: inetOrgPerson
cn: User001
```

The asynchronous operation result will be returned within the structure shown below.



Reading the Result Information and Obtaining the Message Type

The result information will be returned within the message list. The following functions will be used to analyze the message list.

- ldap_first_message(LDAP *ld, LDAPMessage *res)

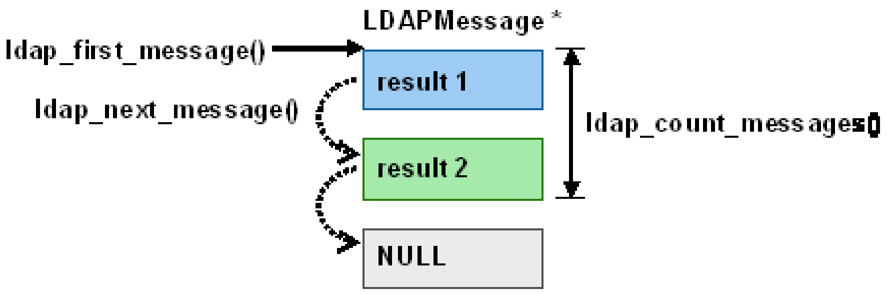
  Send the message address at the beginning

- ldap_next_message(LDAP *ld, LDAPMessage *res)

  Send the next message address

- ldap_count_messages(LDAP *ld, LDAPMessage *res)

  Send the number of a message list



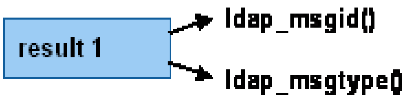
The "result" information message ID and type can be determined using the following functions:

- ldap_msgid(LDAPMessage *lm):

  References the message ID

- ldap_msgtype(LDAPMessage *lm):

  References the message type



The following values will be sent as a message type

Message type	Explanation
LDAP_RES_BIND	Result information for user authentication
LDAP_RES_SEARCH_ENTRY	The entry that matched the search condition.
LDAP_RES_SEARCH_RESULT	Show the notice of the entry search result
LDAP_RES_MODIFY	Result information for changed entry
LDAP_RES_ADD	Result information for additional entry
LDAP_RES_DELETE	Result information for deleted entry
LDAP_RES_MODDN	Result information for the changed entry name
LDAP_RES_COMPARE	Result information for comparison of attribute value

Analyzing the "result" Information

The result received from the asynchronous operation can be analyzed in different ways depending on the message type obtained with ldap_msgtype().

- LDAP_RES_SEARCH_ENTRY

  The search result for the Entry is stored here, refer to "9.3.5 Analyzing the Search Result" for information on analyzing the result information.

- Other than LDAP_RES_SEARCH_ENTRY

  Asynchronous operation response is stored. The value sent to the result information is obtained using the following functions.

  - ldap_parse_result()

    The information contained in "result" is read and then stored in the variable specified in the parameter.

    The following information is returned:

  - LDAP error code

  - Detailed error message string

  - Appropriate DN range

Example code for obtaining the entry search result.

```
msgid = ldap_search( ld, basedn, LDAP_SCOPE_SUBTREE, filter, NULL, 0 );
  if ( msgid == -1 ) {
      /* Process when an error occurred */
      return -1;
  }

  timeout.tv_sec  = 10L;    /* 10sec */
  timeout.tv_usec = 0L;
  finished = 0;
  while ( finished == 0 ) {
      doOtherWork();

      rtn = ldap_result( ld, msgid, LDAP_MSG_ALL, &timeout, &result );
      switch( rtn ) {
      case 0:
          /* Timeout */
          sleep(1);
          break;
      case -1:
          /* Process when an error occurred */
          return -1;
      default:
          /* success */
          finished = 1;
          break;
      } /* switch */
  } /* while */

  message = ldap_first_message( ld, result );
  printf( "ldap_count_messages()=%d\n", ldap_count_messages( ld, message ) );

  for ( ; message != NULL; message = ldap_next_message( ld, message ) ) {
      msgtype = ldap_msgtype( message );
      if ( msgtype == LDAP_RES_SEARCH_ENTRY ) {
          printf( "dn: %s\n", ldap_get_dn( ld, message ) );
      } else {
          int     errcode  = 0;
          char    *matched = NULL;
          char    *errmsg  = NULL;

          ldap_parse_result( ld, message, &errcode, &matched, &errmsg, 0, 0, 0 );
          printf( "ldap_parse_result errcode=%s(%d)\n",
                  ldap_err2string(errcode), errcode );
          ldap_msgfree( result );
          ldap_memfree( matched );
          ldap_memfree( errmsg );
          return -1;
      }
  }
```

9.3.12.3 Canceling Asynchronous Operations

If the asynchronous type function is used to send a request to the Interstage Directory Service, the request can be canceled using the following functions:

- ldap_abandon(LDAP *ld, int msgid):

  Stop the asynchronous type LDAP operation

To cancel an asynchronous request, specify the message ID of the request concerned. The message ID is returned when the asynchronous request is issued.

When ldap_abandon() is issued, and the "result" information of the asynchronous request to be cancelled has already been received, the "result" information is destroyed.

```
msgid = ldap_search( ld, basedn, LDAP_SCOPE_SUBTREE, filter, NULL, 0 );

rtn = ldap_abandon( ld, msgid );
if( rtn == -1 ) {
    /* Process when an error occurred */
    return -1;
}
```

9.3.13 Analyzing Errors

When errors occur in communications with directory services, the cause can be investigated using the following functions:

- The error message character string

  ldap_err2string(int err)

  Returns an error message string for the LDAP error code.

- The error code

  ldap_get_option(LDAP *ld, int option, void *optdata)

  Use LDAP_OPT_RESULT_CODE in the session handle to return the LDAP error code.

- An SSL library error code

  ldapssl_error(LDAP *ld, int ssl_err, int ssl_err_detail)

  Codes for errors detected by the SSL library while using the SSL session

9.3.14 Compile and Link Options

9.3.14.1 Windows (32 bit)

Library

The path for the directory in which the SDK library (F3FMirepldap2.dll) is stored is set in PATH.

Compile and Link Options

To use the LDAP client API function, the following options must be specified for compiling and linking.

Microsoft(R) Visual C++(R) .NET Standard

Compiling (essential)

- Include directory

  1. Select a project in the Solution Explorer.
  2. Open the property page by selecting [View] and then [Property page].
  3. Set the folder "C:\Interstage\IREPSDK\include" in which the idldap.h is installed with "Additional include directory" in [C/C++] - [General].

- Precompiled header

  1. Select a project in the Solution Explorer.
  2. Open the property page by selecting [View] and then [Property page].
  3. Set "Create/use precompiled headers" in [C/C++] - [Precompiled header] to "Create automatically (YX)".

- Runtime library

  1. Select a project in the Solution Explorer.
  2. Open the property page by selecting [View] and then [Property page].
  3. Set "Runtime library" in [C/C++] - [Create codes] to "Multithread DLL (/MD)".

Link Options

- LDAP-API Library

  1. Select a project in the Solution Explorer.
  2. Open the property page by selecting [View] and then [Property page].
  3. Add "F3FMirepldap2.lib" in "Add dependency file" in [Linker] - [Input].

- Library Directory

  1. Select a project in the Solution Explorer.
  2. Open the property page by selecting [View] and then [Property page].
  3. Set the folder ("C:\Interstage\IREPSDK\lib") in which the LDAP-API library is installed in "Additional library directory" in [Linker] - [General].
  4. Set "Validate the incremental link" to "/INCREMENTAL", if it is set as "INCREMENTAL:NO" in [Linker] - [General].

Microsoft(R) Visual C++(R) .NET Standard 2003

Compiling (essential)

- Include directory
  1. Select a project in the Solution Explorer.
  2. Open the property page by selecting [View] and then [Property page].
  3. Set the folder ("C:\Interstage\IREPSDK\include") in which the idldap.h is installed with "Additional include directory" in [C/C++] - [General]..
- Precompiled header
  1. Select a project in the Solution Explorer.
  2. Open the property page by selecting [View] and then [Property page].
  3. Set "Create/use precompiled headers" in [C/C++] - [Precompiled header] to "Create automatically (YX)".
- Runtime library
  1. Select a project in the Solution Explorer.
  2. Open the property page by selecting [View] and then [Property page].
  3. Set "Runtime library" in [C/C++] - [Create codes] to "Multithread DLL (/MD)".

Link Options

- LDAP-API Library
  1. Select a project in the Solution Explorer.
  2. Open the property page by selecting [View] and then [Property page].
  3. Add "F3FMirepldap2.lib" in "Add dependency file" in [Linker] - [Input]
- Library Directory
  1. Select a project in the Solution Explorer.
  2. Open the property page by selecting [View] and then [Property page].
  3. Add the folder "C:\Interstage\IREPSDK\lib" in which the LDAP-API library is installed in "Additional library directory" in [Linker] - [General].
  4. Set "Validate the incremental link" to "/INCREMENTAL", if it is set as "INCREMENTAL:NO" in [Linker] - [General].

Microsoft(R) Visual Studio(R) 2005, or Microsoft(R) Visual Studio(R) 2008

Compiling (essential)

- Include directory
  1. Select a project in the Solution Explorer.
  2. Open the property page by selecting [View] and then [Property page].
  3. Set the folder ("C:\Interstage\IREPSDK\include") in which the idldap.h is installed with "Additional include directory" in [C/C++] - [General].
- Precompiled header
  1. Select a project in the Solution Explorer.
  2. Open the property page by selecting [View] and then [Property page].
  3. Set "Create/use precompiled headers" in [C/C++] - [Precompiled headers] to "Do not use."
- Runtime library
  1. Select a project in the Solution Explorer.
  2. Open the property page by selecting [View] and then [Property page].
  3. Set "Runtime library" in [C/C++] - [Create codes] to "Multithread DLL (/MD)".

Link Options

- LDAP-API Library

    1. Select a project in the Solution Explorer.
    2. Open the property page by selecting [View] and then [Property page].
    3. Add "F3FMirepldap2.lib" in "Add dependency file" in [Linker] - [Input].

- Library Directory

    1. Select a project in the Solution Explorer.
    2. Open the property page by selecting [View] and then [Property page].
    3. Set the folder "C:\Interstage\IREPSDK\lib" in which the LDAP-API library is installed in "Additional library directory" in [Linker] - [General].
    4. Set "Validate the incremental link" to "/INCREMENTAL", if it is set as "INCREMENTAL:NO" in [Linker] - [General].

9.3.14.2 Windows (64 bit)

Microsoft(R) Visual Studio(R) 2005 or Microsoft(R) Visual Studio(R) 2008

1. Copy the following files/folders to any folder on the machine that Microsoft(R) Visual Studio(R) 2005 or Microsoft(R) Visual Studio(R) 2008 is installed on.

    - Include files

      "C:\Interstage\IREPSDK\include\idldap.h"

    - Library

      "C:\Interstage\IREPSDK\lib\F3FMirepldap2.lib"

2. Configure the following settings:

Compile Options

- Include directory

    1. Select a project in the Solution Explorer.
    2. Open the property page by selecting [View] and then [Property page].
    3. Set "Additional include directory" in [C/C++] - [General] to the folder with the files that were copied in step 1 above.

- Precompiled header

    1. Select a project in the Solution Explorer.
    2. Open the property page by selecting [View] and then [Property page].
    3. Set "Create/use precompiled headers" in [C/C++] - [Precompiled headers] to "Do not use."

- Runtime library

    1. Select a project in the Solution Explorer.
    2. Open the property page by selecting [View] and then [Property page].
    3. Set "Runtime library" in [C/C++] - [Create codes] to "Multithread DLL (/MD)".

Link Options

- LDAP API Library

    1. Select a project in the Solution Explorer.
    2. Open the property page by selecting [View] and then [Property page].
    3. Add "F3FMirepldap2.lib" to "Add dependency file" in [Linker] - [Input].

- Library Directory

    1. Select a project in the Solution Explorer.
    2. Open the property page by selecting [View] and then [Property page].
    3. Specify the folder in which the LDAP-API library is installed with procedure 1 in "Additional library directory" in [Linker] - [General].
    4. Set "Validate the incremental link" to "/INCREMENTAL", if it is set as "INCREMENTAL:NO" in [Linker] - [General].

Microsoft(R) Platform SDK or Microsoft Windows(R) SDK that supports an IA64 platform

Compile Options

- Include directory

  Set the following paths:

  C:\Interstage\IREPSDK\include

  Example:

  set INCLUDE=%INCLUDE%;C:\Interstage\IREPSDK\include

- Runtime library

  Specify "/MD" as the runtime library.

Link Options

- LDAP-API Library

  Specify "F3FMirepldap2.lib".

- Library Directory

  Set the following paths:

  C:\Interstage\IREPSDK\lib

  Example:

  set LIB=%LIB%;C:\Interstage\IREPSDK\lib

9.3.14.3 Solaris/Linux System

This explains how to compile and link with Solaris and Linux.

Library

The SDK library (libirepldap2.so) is stored at "/opt/FJSVirepc/lib".

Compile and Link Options

The "include" file is stored in the following directory:

"/opt/FJSVirepc/include"

Libraries are suitable for multi-thread environments. Specify the following:

Solaris32/64

```
"-mt"
```

Linux32/64

```
"-fPIC -D_REENTRANT"
```

9.4 Sample Programs

Sample programs in C which show how to use the API function are located in the following folders:

Windows32/64

```
"C:\Interstage\IREPSDK\sample\C".
```

Solaris32/64 Linux32/64

```
"/opt/FJSVirepc/sample/C".
```

9.4.1 Sample Program File List

Sample source

Category	File name	Overview
Entry search	SampleSearch.c	entry search (English characters)
	SampleSearchRetAttrs.c	Search narrowed down to attribute
	SampleSearchSizeLimit.c	Search with size limit set
	SampleSearchTimeLimit.c	Search with time limit set
Comparing attribute values	SampleCompare.c	Comparing attribute values
Changing entries	SampleModAttrs.c	Changing entries
	SampleModAttrsBinary.c	Changing entries (binary data)
Renaming entries	SampleModrdn.c	Renaming entries
Adding entries	SampleAdd.c	Adding entries
	SampleAddBinary.c	Adding entries (binary data)
Deleting entries	SampleDelete.c	Deleting entries
Asynchronous process	SampleSearchResult.c	Asynchronous type entry search
	SampleAbandon.c	Stopping asynchronous operations
Common process	SampleBase.c	Common process (session initialization)
	SampleCommon.c	Common process (Connection)
	SamplePrintEntry.c	Display of the search result
	SampleBase.h	Common functions declaration
	SampleDef.h	Common definition of a sample program

Other

Windows32/64

build folder	Sample project file for compile
make_jp.bat	Sample program batch file for compile (Windows (64 bit) Japanese samples)
make_en.bat	Sample program batch file for compile (Windows (64 bit) English samples)

Solaris32/64 Linux32/64

Makefile	Sample program makefile for compile

List of parameters

Defined value	Explanation
SAMPLE_HOST	The host name or IP address of the repository server to which connection is to be made
SAMPLE_PORT	The port number of the repository server
SAMPLE_BINDDN	Specify administrator DN
SAMPLE_PASSWORD	Specify administrator DN password
SAMPLE_BASEDN	Search base DN
SAMPLE_CONV_CODE	Specify the code system for multi-byte characters. The following values are set in the initial value Windows32/64 SJIS Solaris32/64 Linux32/64 EUC
SAMPLE_SSL_USE	Activate this definition when using SSL.
SAMPLE_SSL_VERSION	Specify SSL version
SAMPLE_SSL_CRYPT	Specify encrypted algorism
SAMPLE_SSL_TOKEN	Specify the token label
SAMPLE_SSL_PASSWORD	Specify the user PIN
SAMPLE_SSL_SLOT	Specify the slot information directory
SAMPLE_SSL_CERT	Specify the operation management directory

9.4.2 Compiling Sample Programs

This section explains the procedure from compilation to execution of the sample program.

9.4.2.1 Windows (32 bit)

1. Copy all files in the C language sample program storage folder to the work folder.

   The sample program location is as follows:

   "C:\Interstage\IREPSDK\sample\C"

2. Open the build\EN\build.sln file in the work folder using a development tool such as Microsoft(R) Visual C++(R) .NET Standard, Microsoft(R) Visual C++(R) .NET Standard 2003, Microsoft(R) Visual Studio(R) 2005 or Microsoft(R) Visual Studio(R) 2008.

   Note

   All files in the 'build' folder are solution files and a project file for Microsoft(R) Visual C++(R) .NET Standard. If Microsoft(R) Visual C++(R) .NET Standard 2003 Microsoft(R) Visual Studio(R) 2005 or Microsoft(R) Visual Studio(R) 2008 is used, a confirmation screen is displayed, asking the user if they would like to upgrade the project or solution file being opened to the current version. Change the format according to the directions on the screen.

3. Set the compile options and link options. Refer to "Compile and Link Options".

4. Change the parameter values in the sample source according to the environment of the repository server to which connection is to be made. For details of the corresponding parameters, refer to "List of parameters". For general parameter details, refer to the explanation of each function parameter in "Interstage Directory Service Interface" in the "C Interface" chapter of the Reference Manual (API Edition).

5. Build the sample program using Microsoft(R) Visual C++(R) .NET Standard, Microsoft(R) Visual C++(R) .NET Standard 2003, or Microsoft(R) Visual Studio(R) 2005. When the build is finished, a "Release" folder or a folder with the same name as the project file is created in the "build\EN" folder is created, and the execute file is stored.

9.4.2.2 Windows (64 bit)

Using Microsoft(R) Visual Studio(R) 2005 or Microsoft(R) Visual Studio(R) 2008

1. Copy the following files/folders to a work folder on the machine that Visual Studio(R) 2005 or Microsoft(R) Visual Studio(R) 2008 is installed on.

   - Samples

     Everything under the "C:\Interstage\IREPSDK\sample\C" folder

2. Open the build\JA\build.sln file under the work folder in Microsoft(R) Visual Studio(R) 2005 or Microsoft(R) Visual Studio(R) 2008.

3. Set the compile options. For details about the settings, refer to "9.3.14 Compile and Link Options", "9.3.14.2 Windows (64 bit)".

4. Change the parameter values in the sample source according to the environment of the repository server to which connection is to be made. For details of the corresponding parameters, refer to "List of parameters". For general parameter details, refer to the explanation of each function parameter in "Interstage Directory Service Interface" in the "C Interface" chapter of the Reference Manual (API Edition).

5. Build the project for the samples compiled in Microsoft(R) Visual Studio(R) 2005 or Microsoft(R) Visual Studio(R) 2008. When the build is finished, the "Itanium\Release" folder and executable files with the same name as the project files are stored under the "build\JA" folder.

6. Copy the generated executable files to Windows (64 bit) and then execute them.

For details on using Microsoft(R) Visual Studio(R) 2005 or Microsoft(R) Visual Studio(R) 2008, refer to the Help files attached to each product.

Using Microsoft(R) Platform SDK or Microsoft(R) Windows(R) SDK that supports an IA64 Platform

1. Copy all the files/folders under the "C:\Interstage\IREPSDK\sample\C" folder to a work folder.

2. Open the Microsoft(R) Platform SDK or Microsoft(R) Windows(R) SDK command prompt.

3. Set the compile options. For details about the settings, refer to "9.3.14 Compile and Link Options", "9.3.14.2 Windows (64 bit)".

4. Change the parameter values in the sample source according to the environment of the repository server to which connection is to be made. For details of the corresponding parameters, refer to "List of parameters". For general parameter details, refer to the explanation of each function parameter in "Interstage Directory Service Interface" in the "C Interface" chapter of the Reference Manual (API Edition).

5. Execute the make_jp.bat work folder. When the build is finished, the executable files are stored under the current folder.

9.4.2.3 Solaris/Linux System

1. Copy all files in the C language sample program storage directory to the work directory.

   The sample program location is as follows:

   "/opt/FJSVirepc/sample/C"

2. Change the "Write" authority settings for the work directory and the directory owner.

   Example

   chmod -R +w example

   chown -R owner:group example

3. Change the parameter values in the sample source according to the environment of the repository server to which connection is to be made. For details of the corresponding parameters, refer to "List of parameters". For general parameter details, refer to the explanation of each function parameter in "Interstage Directory Service Interface" in the "C Interface" chapter of the Reference Manual (API Edition).

4. Compile the sample program using the "*make*" command. When the "*make*" command is executed, check that the "Makefile" file exists. Check that the executable file for the source files for each LDAP operation in "9.4.1 Sample Program File List" is created.

9.4.3 Execution Procedure

The following execution modules will be created when a sample program is compiled:

Execution module

Execution module	Process details
SampleSearch	Search the entry under the base DN with the filter conditions "(cn=User00*)"
SampleSearchRetAttrs	Search the entry under the base DN with filter conditions "cn=User00*"and acquire attribute value cn, telephonenumber, and mail.
SampleSearchSizeLimit	Search the entry under the base DN with filter conditions "(cn=User00*)". Set 2 for a size limit.
SampleSearchTimeLimit	Search all entries under base DN, and set a time limit of one second.
SampleCompare	Compare whether "mail" attribute for entry "cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com" matches "user001@sample.fujitsu.com".
SampleModAttrs	Change the attribute values for the entry "cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com", as follows; replace the "telephoneNumber" attribute, add a "mail" attribute and delete "title" attribute.
SampleModAttrsBinary	Add "jpegPhoto" attribute to the entry "cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com". For binary data, a file name is specified with the argument.
SampleModrdn	Change the name of the entry "cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com" to "cn=User901,ou=User,ou=interstage,o=fujitsu,dc=com".
SampleAdd	Add the entry "cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com"
SampleAddBinary	Add the entry "cn=User002,ou=User,ou=interstage,o=fujitsu,dc=com" that includes binary data. For binary data, a file name is specified with the argument.
SampleDelete	Delete the entry "cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com"
SampleSearchResult	Search the entry under the base DN with the filter conditions "cn=User00*" using asynchronous type functions.
SampleAbandon	Perform an asynchronous search and cancel the process.

How to execute a sample program

Example of executing the program "SampleAdd" that adds an entry:

```
SampleAdd is start
ldap_init( "localhost", 389 )
ldap_set_option( LDAP_OPT_PROTOCOL_VERSION, 3 )
ldap_simple_bind_s( "cn=manager,ou=interstage,o=fujitsu,dc=com", "******" )
ldap_add_s( "cn=User001,ou=User,ou=interstage,o=fujitsu,dc=com" )
ldap_add_s(): Already exists
already exists, no need to add.
ldap_unbind_s()
```

In this example, the entry already exists so that "Already exists" is returned.

For details of messages output in the sample program, refer to "LDAP Error Codes" in the "Error Codes to be Reported from Interstage Directory Service" chapter of the Messages manual.

Chapter 10 Operating and Maintaining Repositories

This chapter explains the environment setup required to use Interstage Directory Service.

10.1 Starting/Stopping a Repository

This section explains how to start and stop a repository of Interstage Directory Service.

10.1.1 Standalone Operation

Starting a Repository

If an RDB is used as the repository database, first start the database that was created in the "Creating Databases" chapter. If Symfoware Server is being used, refer to "Starting and stopping Symfoware Server" in the Symfoware Setup Guide for more information on starting the database. If an Oracle database is being used, refer to the Oracle database manual.

The Interstage Management Console is used to start a repository within Interstage Directory Service.

Log in after starting the Interstage Management Console.

To perform the startup operation, select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]).

For information on startup of the Interstage Management Console, see 'Configuring the Interstage Management Console' in the Operator's Guide. For information on the screen operations, see 'Services' in the Operator's Guide.

Note

- Startup time for each repository make take from several seconds to several minutes. The startup time will vary depending on the number of registered entries, operation mode, and machine performance.

10.1.2 Automatic Start

10.1.2.1 Standard Database

The automatic start settings for the repository when the OS starts up can be changed according to the following method:

Windows32/64

Click [Contol Panel] > [Administrative Tools] > [Services], and change the Interstage Directory Service (Interstage Directory Service (Repository name)) startup type.

Solaris32/64 Linux32/64

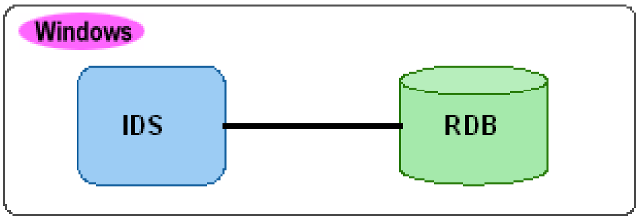
The automatic start settings for the repository can be changed using the "-startup" option of the *irepadmin* command. Immediately after the repository is created, it is set up to start automatically when the operating system starts. For details, refer to the "Interstage Directory Service Operation Commands" chapter of the "Reference Manual (Command Edition)".

10.1.2.2 RDB

Windows32/64

In Windows(R), the setup method differs depending on whether the Interstage Directory Service and RDB will run on the same machine, or on separate machines.

When the Interstage Directory Service and RDB run on the same machine



IDS : Interstage Directory Service

1. Check that the setup type for the Interstage Directory Service is [Automatic].

   Once the repository is created, it is set to start automatically when the OS starts up. If the setup type is [Manual], change it to [Automatic].

2. Use the "-setsvc" option of the *irepadmin* command to set the dependency for the Interstage Directory Service and the RDB service. There is no need to set the RDB service.

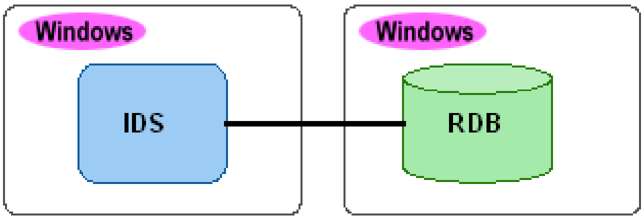
   Immediately after the repository is created, the dependency is not set up. For details on the *irepadmin* command, refer to the "Interstage Directory Service Operation Commands" chapter of the "Reference Manual (Command Edition)".

- **When the Interstage Directory Service and RDB are run on separate machines**

  It is essential that the RDB service is started up before Interstage Directory Service.

  Startup of the RDB service cannot be made to wait.

- **When the RDB is run in Windows(R)**



IDS : Interstage Directory Service

1. Check that setup type for the Interstage Directory Service is [Automatic].

   Once the repository is created, it is set to start automatically when the OS starts up. If the setup type is [Manual], change it to [Automatic].

2. Configure the settings so that the RDB service starts automatically.

   The Symfoware/RDB service name is as follows:

```
SymfoWARE RDB RDB system
```

   The Oracle Database service name is as follows:

   - Listener service name

     When using a default listener

```
Oracle<Oracle home name>TNSListener
```

   - When using a non-default listener

```
Oracle<Oracle home name >TNSListener< Listener name>
```

- Oracle database service name

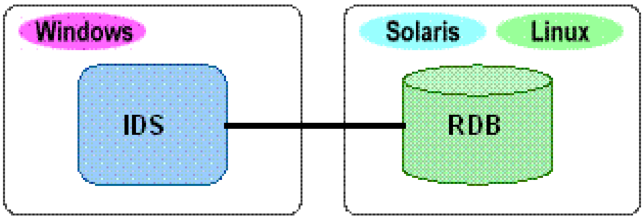
```
OracleService<Oracle instance identity name(Oracle SID)>
```

If the setup type is [Manual], change it to [Automatic].

Note

When Interstage Directory Service and RDB are run on separate servers, dependency cannot be set for the Interstage Directory Service's service and the RDB service.

- **When RDB is run on Solaris or Linux**



IDS : Interstage Directory Service

In the RDB, during OS setup, automatic startup functionality is not always supported.

- If an Oracle database is being used

  Refer to the Oracle manual, and set up a startup script so that the RDB system starts automatically.

- If a Symfoware Server is being used

  If the Symfoware Server does not provide an RDB system startup script, modify the sample RDB system startup script (see below) provided with the Interstage Directory Service, and place it in the following directory:

  Solaris32/64

  ```
  /etc/rc2.d/S90FJSVireprdb2b
  /etc/rc3.d/S90FJSVireprdb2b
  ```

  Linux32/64

  ```
  /etc/rc.d/rc0.d/K20FJSVireprdb2b
  /etc/rc.d/rc1.d/K20FJSVireprdb2b
  /etc/rc.d/rc2.d/S81FJSVireprdb2b
  /etc/rc.d/rc3.d/S81FJSVireprdb2b
  /etc/rc.d/rc4.d/S81FJSVireprdb2b
  /etc/rc.d/rc5.d/S81FJSVireprdb2b
  /etc/rc.d/rc6.d/S81FJSVireprdb2b
  ```

Sample Startup Scripts

The RDB system start script samples are contained in the following directory:

```
C:\Interstage\IREP\sample\RDB\SYM\PROCEDURE
```

Specify the RDB system created in the "Creating Databases" chapter for RDBNAME in the start script. Correct all the start scripts before saving them.

```
#!/bin/sh
# ---
# All Rights Reserved, Copyright (c) FUJITSU LIMITED 2006
# ---
```

```
RDBNAME=dsdbsys
LC_ALL=C
export RDBNAME
export LC_ALL
SYS=`uname`
if ( test "$SYS" = "SunOS" ) then
    RDBPATH=/opt/FSUNrdb2b
    LD_LIBRARY_PATH=$RDBPATH/lib:/etc/opt/FSUNiconv/lib
    LD_LIBRARY_PATH_64=$RDBPATH/lib
elif ( test "$SYS" = "Linux" ) then
    RDBPATH=/opt/FJSVrdb2b
    LD_LIBRARY_PATH=$RDBPATH/lib
fi
case "$1" in
start)
    if ( test -f $RDBPATH/bin/rdbstart ) then
        $RDBPATH/bin/rdbstart
    fi
    ;;

There is no need to correct the following part, so it has been omitted.
```

Solaris32/64 Linux32/64

In Solaris/Linux, configure the following settings regardless of whether or not Interstage Directory Service and RDB are run on the same server.

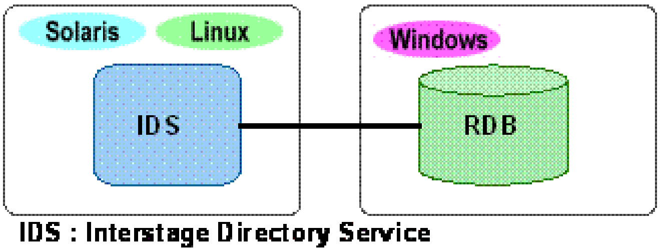
1. Use the irepadmin command to check that the repository has been set to start automatically ("-startup" option is "Auto").

   Once the repository is created, it is set to start automatically when the OS starts up.

   If the repository has been set to start manually ("-startup" option is "Manual"), use the irepadmin command to change the settings so that the repository starts automatically. For details, refer to the "Interstage Directory Service Operation Commands" chapter of the "Reference Manual (Command Edition)".

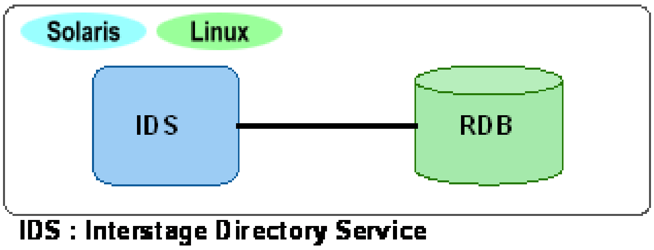
2. Perform setup so that when the OS starts up, the RDB service automatically starts up

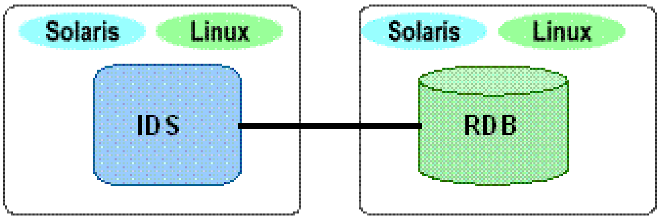
   - **When the RDB is run in Windows(R)**

   Set up with reference to step 2 of "When the RDB is run in Windows(R)".

   - **When the RDB is run in Solaris or Linux**



IDS : Interstage Directory Service

In the RDB, during OS setup, automatic database startup functionality is not always supported.

- **If an Oracle database is being used**

  Refer to the Oracle manual, and set up a startup script so that the RDB system starts automatically.

- **If a Symfoware Server is being used**

  If the Symfoware Server does not provide an RDB system startup script, modify the sample RDB system startup script (see below) provided with the Interstage Directory Service, and place it in the following directory:

  Solaris32/64

  ```
  /etc/rc2.d/S90FJSVireprdb2b
  /etc/rc3.d/S90FJSVireprdb2b
  ```

  Linux32/64

  ```
  /etc/rc.d/rc0.d/K20FJSVireprdb2b
  /etc/rc.d/rc1.d/K20FJSVireprdb2b
  /etc/rc.d/rc2.d/S81FJSVireprdb2b
  /etc/rc.d/rc3.d/S81FJSVireprdb2b
  /etc/rc.d/rc4.d/S81FJSVireprdb2b
  /etc/rc.d/rc5.d/S81FJSVireprdb2b
  /etc/rc.d/rc6.d/S81FJSVireprdb2b
  ```

  The RDB system start script samples are contained in the following directory:

  ```
  /opt/FJSVirep/sample/RDB/SYM/PROCEDURE
  ```

Specify the RDB system created in the "Creating Databases" chapter for RDBNAME in the start script. Correct all the start scripts before saving them.

For details on the contents of the startup script samples, refer to "Sample Startup Scripts".

3. If the repository has been configured to start automatically when the system starts up (i.e. "Auto" has been specified for the "-startup" option), then the repository can be set up to wait for the RDB service to start. Use the "-rdbwait" option of the *irepadmin* command to configure the repository to wait for the RDB service to start.

   If, after the repository is created, the "-rdbwait" option has not been set, the repository does not wait for the RDB service to start. In this case, automatic startup of the repository will fail and return an error.

   Refer to the "Interstage Directory Service Operation Commands" chapter of the Reference Manual (Command Edition) for more information.

   Note

   RDB must be started before Interstage Directory Service.

10.1.2.3 Stopping a Repository

The Interstage Management Console is used to stop a repository within Interstage Directory Service.

Log in after starting the Interstage Management Console.

To perform the stop operation, select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]).

For information on the stopping of the Interstage Management Console, refer to 'Configuring the Interstage Management Console' in the Operator's Guide. For information on the screen operations, refer to 'Services' in the Operator's Guide.

10.1.3 Load Balancing Operations

Starting a Repository

If the Repository is being Operated in Database Sharing Mode

The procedure for starting the repository and the RDB system is the same as for "10.1.1 Standalone Operation".

If the Repository is being Operated in Replication Mode

Refer to the "Creating a Load Distribution Environment (Replication Mode)" chapter for information on how to start the repository and the RDB system.

10.2 Stopping a Repository

If the Repository is being Operated in Database Sharing Mode

The procedure for stopping the repository and the RDB system is the same as for "10.1.1 Standalone Operation".

If the Repository is being Operated in Replication Mode

Refer to the "Creating a Load Distribution Environment (Replication Mode)" chapter for information on how to stop the repository and the RDB system.

10.3 Notes about OS shutdowns and restarting

Note the following points about shutting down and restarting the OS.

Standard Databases

- For details on the repository automatic startup settings for when the OS is restarted, refer to "10.1.2 Automatic Start".
- Windows32/64

  Stop all repositories before shutting down or restarting the OS.

RDB

Depending on the system configuration, it is possible to start the repository automatically after making it wait for the startup of the RDB when the OS restarts. For details, refer to "10.1.2 Automatic Start".

IDS	RDB			
	Windows(R)		Solaris/Linux	
	Same as IDS	Different to IDS	Same as IDS	Different to IDS
Windows(R)	Waits	Doesn't wait (*1)	-	Doesn't wait (*1)
Solaris/Linux	-	Waits	Waits	Waits

IDS: Interstage Directory Service

*1 Although it is possible to configure the settings so that Interstage Directory Service is started automatically, it cannot be made to wait for the startup of the RDB.

10.4 Changing Passwords

This section explains the procedure for changing passwords during repository operations.

10.4.1 Changing the Password for the Repository Administrator DN

Standalone Operation

Change the password for the administrator DN using the following procedure:

1. Stop the repository using an Interstage Management Console connected to the machine where the repository has been created.
2. Click the repository that has been stopped to display the [Settings] window.
3. In the dialog box displayed, under [Change Password], select "Change", and then click the [OK] button.
4. In the dialog box displayed, set up the same new password in the [New Administrator DN password] and [New Administrator DN password (re-enter)] fields, and then click the [Apply] button.
5. Use the Interstage Management Console to start the repository for which the new password has been set up in step 4.

Load Balancing Operations

If Load Balancing is being Performed in Database Sharing Mode

The procedure for changing the password for the administrator DN is the same as for "Standalone Operation".

If Load Balancing is being Performed in Replication Mode

Refer to the "Creating a Load Distribution Environment (Replication Mode)" chapter for information on how to change the password for the administrator DN.

10.4.2 Changing the Password for Connecting to the Database

Standalone Operation

Use the following procedure to change the password for connecting to the database:

Note

- To change the password used for connecting to the database when Symfoware/RDB is being used for the repository database, change the password for the database connection user in the operating system for the machine where the database is installed, and then perform the change operations below.
- To change the password for connecting to the database when an Oracle database is being used for the repository database, change the password for the user account registered with the Oracle database for the machine where the database has been installed, and then perform the change operations below.

1. Stop the repository using an Interstage Management Console connected to the machine where the repository has been created.
2. Click the repository that has been stopped to display the [Settings] window.
3. In the dialog box displayed, under [Change the password for connecting to the database], select "Change", and then click the [OK] button.
4. Set up the new password in the [New password for connecting to the database] fields displayed, and then click the [Apply] button.
5. Use the Interstage Management Console to start the repository for which the new password has been set up in step 4.

Load Balancing Operations

If Load Balancing is being Performed in Database Sharing Mode

The procedure for changing the password for connecting to the database is the same as for "Standalone Operation".

Note

To change the password for connecting to the database for repositories that use database sharing, the password for connecting to the database must be changed for all repositories sharing the database.

If Load Balancing is being Performed in Replication Mode

Refer to the "Creating a Load Distribution Environment (Replication Mode)" chapter for information on how to change the password for connecting to the database.

10.5 Monitoring Repository Operation

Interstage Directory Service outputs the following logs:

- Access history to Interstage Directory Service
- Maintenance information of Interstage Directory Service

10.5.1 Access History to Repository

Interstage Directory Service features an access log which stores access history. The following information is recorded in the log:

- Access date/time
- IP address
- Events
- Detailed information about events

Using the Interstage Management Console, it is possible to change the following settings:

- Output types of the access log
- Access log storage directory of the access log
- Rotation type of the access log

10.5.2 Setting the Access Log

The following procedure explains how to set the access log.

- **Setting the Access Log When Creating a New Repository**
  1. Start the Interstage Management Console.
  2. Select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]) and create a repository.
  3. Click [View Status] to display detailed settings.
  4. Specify [Output types], [Access log storage directory], and [Rotation Type] in [Access log settings]. Also specify [Size] and [Number of access log files to maintain] as required.
- **Changing the Access Log Settings of an Active Repository Server**
  1. Start the Interstage Management Console.
  2. Stop the repository.
  3. Change the repository setting.
  4. Click [View] to display detailed settings.
  5. Specify [Output types], [Access log storage directory], and [Rotation Type] in [Access log settings] and also specify [Size] and [Number of access log files to maintain] as required.
  6. Start the repository from the [Repository : View Status] window.

  Refer to 'Services' in the Operator's Guide for further operating details.

Output Level of the Access Log

When all access history from the client is output to the access log, it can take a large amount of hard disk space. To manage this situation, events to be output to the access log can be changed in [Output types].

- A combination of the following can be specified in [Output types].
- Client requests
- Server errors
- Normal server response
- Server search result of DN

Access Log Storage Destination

The access log is created under the following directory by default:

Windows32/64

```
C:\Interstage\IREP\var\<repository-name>\log
```

Solaris32/64 Linux32/64

```
/var/opt/FJSVirep/<repository-name>/log
```

The rules for generating the file name of the access log are as follows:

access_YYYYMMDD_XXXXX

YYYY: Year of the access log output

MM: Month of the access log output

DD: Day of the access log output

XXXXX: Interstage Directory Service administration name (Both the content and number of digits can be changed)

Output example:

If the access log was output on April 1, 2003

```
access_20030401_81600
```

Note

- If the storage directory is changed, delete the old storage directory before the change and log information as required.

Rotation of the Access Log

The access log can be divided in accordance with the rotation.

The following types can be selected as [Rotation Type].

Rotation type	Meaning
Size	A new file is created after the specified size is reached.
Monthly	A new file is created each month. However, when the maximum size of one file is reached; a new file is automatically created.
Daily	A new file is created each day. However, when the maximum size of one file is reached; a new file is automatically created.

In addition to [Rotation Type]; [Size] and [Number of access log files to maintain] can also be specified.

In [Size], specify the size of one access log file in Mbytes.

In [Number of access log files to maintain], specify the number of generations of files to maintain.

Note

- If Interstage Directory Service is restarted, the file is divided regardless of [Rotation Type].

10.5.3 How to Read Access Logs

The format of access logs and the procedure for analyzing them are given below.

Output Form

- One record is output in one line.
- Items in one record are divided by the tab (0x09).
- If the content of 'DETAIL' (shown in the format below) is divided into multiple items, they will be divided by blanks.
- The access log is output in the 'UTF-8 format.'
- If any multi-byte character is contained in the access log, use an editor that supports the 'UTF-8 format' to reference it. If the 'UTF-8 format' cannot be handled, convert the code system of the access log from the 'UTF-8 format' to a code system that works with the editor.

Format

The following shows the format of the access log:

```
MM/DD  hh:mm:ss.nnnnnn  THREAD  CONN  OP  FD  REQ/RES  EVENT  DETAIL
```

Format Details

The following table lists the details of the access log format.

Table 10.1 Access Log Format Details

MM/DD hh:mm:ss.nnnnnn	Shows the date and time of the access log output MM: month DD: day hh: hour (24 hours) mm: minute ss: second nnnnnn: microsecond
THREAD	Shows the thread ID (hexadecimal) in Interstage Directory Service that executed the request (for maintenance).
CONN	Shows the management number (connection ID) by which Interstage Directory Service accepted the connection (for maintenance).
OP	Shows the management number (operation ID) by which Interstage Directory Service accepted the request within one connection (for maintenance).
FD	Shows the file descriptor (fd) of the connection socket.
REQ/RES	Indicates whether a request or a response. --->: Request from a variety of clients to Interstage Directory Service <---: Response from Interstage Directory Service to a variety of clients
EVENT	Shows information about requests to Interstage Directory Service and results of such requests. For more details, see the EVENT table.
DETAIL	Shows detailed information about EVENT. For more details, see the EVENT table.

Details of EVENT and DETAIL of the Access Log

The following table lists the details of EVENT and DETAIL of the access log.

Table 10.2 EVENT and DETAIL Access Log Table

EVENT	DETAIL	Meaning	Output level [X: Output]			
			Output request information of the client	Output error response of the server	Output normal response of the server	Output search result response of the server
CONNECT	IP address: port number (host name)	Connection request from the client	X			
CONNECTION REJECTED	IP address: port number (host name)	Error response from the server (connection failure)		X		
DISCONNECT	IP address: port number (host name)	Normal response from the server (successful disconnection)			X	
TIMEOUT	IP address: port number (host name)	Error response from the server (timeout)		X		
BIND	Bind DN, protocol version	Authentication request bind DN from the client: Bind DN used for connecting to Interstage Directory Service Protocol version: Protocol version of LDAP used for connecting to Interstage Directory Service	X			
SEARCH	Search base, Search scope, Alias reference rule, Size limit, Time limit, Attribute acquisition method, Search filter	Search request from the client Search base: Entry to the search start position. "?" indicates that the search base is not specified. Search scope: 0: Searches the entries specified by the search base. 1: Searches the subordinator entries of the entries specified by the search base. 2: Searches the entries specified by the search	X			

EVENT	DETAIL	Meaning	Output level [X: Output]			
			Output request information of the client	Output error response of the server	Output normal response of the server	Output search result response of the server
		base and entire entries below them. Alias reference rule: 0: No alias reference 1: Reference the alias only during searching. 2: Reference the alias only when searching the search base. 3: Reference the alias. Size limit: Maximum number of entries to be searched Time limit: Timeout period for searching Attribute acquisition method: 0: Searches for the attribute name and attribute value. Otherwise: Searches for the attribute name. Search filter: Search filter. 'empty' indicates that the search filter is not specified. "*","\","(", and ")" will export the code that was escaped by [\].				
COMPARE	DN to be compared	Comparison request from the client	X			
MODIFY	DN to be modified	Modification request from the client	X			
MODRDN	DN to be modified, New RDN, Old DN deletion flag	Identifier change request from the client DN to be modified: DN (old DN) before modification New RDN: New RDN	X			

EVENT	DETAIL	Meaning	Output level [X: Output]			
			Output request information of the client	Output error response of the server	Output normal response of the server	Output search result response of the server
		Old DN deletion flag 0: Does not delete the old DN. Otherwise: Deletes the old DN.				
ADD	DN to be added	Addition request from the client	X			
DELETE	DN to be deleted	Deletion request from the client	X			
BIND OK	None	Normal response from the server (successful authentication)			X	
COMPARE OK	None	Normal response from the server (successful comparison)			X	
MODIFY OK	None	Normal response from the server (successful change)			X	
MODRDN OK	None	Normal response from the server (successful identifier change)			X	
ADD OK	None	Normal response from the server (successful addition)			X	
DELETE OK	None	Normal response from the server (successful deletion)			X	
BIND NG	Error code	Error response from the server (authentication failure)		X		
COMPARE NG	Error code	Error response from the server (comparison failure)		X		
MODIFY NG	Error code	Error response from the server (change failure)		X		
MODRDN NG	Error code	Error response from the server (identifier change failure)		X		
ADD NG	Error code	Error response from the server (addition failure)		X		
DELETE NG	Error code	Error response from the server (deletion failure)		X		
SEARCH OK	Number of found entries	Normal response from the server (successful search)			X	

EVENT	DETAIL	Meaning	Output level [X: Output]			
			Output request information of the client	Output error response of the server	Output normal response of the server	Output search result response of the server
SEARCH NG	Error code	Error response from the server (search failure)		X		
SEARCH ENT	Entry DN of the search result	Search result response from the server				X
UNBIND	None	Release request from the client	X			

The LDAP error code is output to the error code of DETAIL. For details of the LDAP error code, see 'LDAP error codes' in the Messages.

Analyzing the Access Log

The following explains how to analyze the access log by example:

```
08/01 13:40:22.436320    0020    0    0    6    --->    CONNECT
IP=127.0.0.1:40199(localhost)     (line 1)
08/01 13:40:22.440007    0004    0    0    6    --->    BIND
"cn=manager,ou=interstage,o=fujitsu,dc=com" 3     (line 2)
08/01 13:40:22.443245    0005    0    1    6    --->    ADD
"ou=interstage,o=fujitsu,dc=com"     (line 3)
08/01 13:40:37.837376    0006    0    2    6    --->    ADD
"cn=ssoUser1,o=Fujitsu Limited,c=jp"     (line 4)
08/01 13:40:37.838490    0007    0    2    6    <---    ADD     NG    53
(line 5)
08/01 13:41:22.493324    0008    0    3    6    --->    UNBIND     (line 6)
```

line 1

A request processed at 13:40:22.436320 on August 1.

This indicates that Interstage Directory Service received a connection request (CONNECT) from an application whose IP address is '127.0.0.1(localhost)' and port number is '40199.'

line 2

A request processed at 13:40:22.440007 on August 1.

This indicates that an authentication request (BIND) was received. Since the value of CONN (connection ID) is '0', which is the same as that in line 1, the request can be assumed to have come from the same application as line 1.

line 3

A request processed at 13:40:22.443245 on August 1.

An addition request (ADD) to the entry tree 'ou=interstage,o=fujitsu,dc=com' was received.

line 4

A request processed at 13:40:37.837376 on August 1.

An addition request (ADD) to the entry tree 'cn=ssoUser1,o=Fujitsu,c=jp' was received.

line 5

A request processed at 13:40:37.838490 on August 1.

An addition request (ADD) failed (NG) and the error code '53' was returned. The error code '53' is an error code of LDAP (For the meaning of the error code, see 'LDAP error codes' in the Messages).

Since CONN (connection ID) is '0' and OP (operation ID) is '2,' the investigation of the access log (with the same CONN and OP) shows that this is a response to the request of line 4.

line 6

A request processed at 13:41:22.493324 on August 1.

A release request (UNBIND) was received.

10.5.4 Maintenance Information of Repository

Interstage Directory Service outputs maintenance information to assist troubleshooting. Maintenance information is output to the following directory. When a problem occurs, save the information in the following directory:

Windows32/64

```
C:\Interstage\IREP\var\_system
C:\Interstage\IREP\var\<repository name>\tmp
```

Solaris32/64 Linux32/64

```
/var/opt/FJSVirep/_system
/var/opt/FJSVirep/<repository name>/tmp
```

Maintenance information collects the following types of information. However, not all details are released due to their nature.

Maintenance information	Description
Message log	Message information output by Interstage Directory Service is collected.
Trace log	When some failure or error occurs in Interstage Directory Service, its contents are collected
Process information	Process ID and parameters during execution are collected.
IPC information Solaris32/64 Linux32/64	Information about acquired IPC resources is collected.

10.6 Search Tuning

This section explains the environment setting tuning method for improving the search performance or reducing the server load.

10.6.1 Limiting the Time of Exclusive Use of the Repository per Search Request

An exclusive search request on a repository with a large amount of registered entry data will result in the slow response of Interstage Directory Service. This time delay can be prevented by changing environment settings to limit the exclusive use of the repository for search requests.

To limit the duration of exclusive use of a repository by a search request, use the Interstage Management Console to change the environment settings, as follows:

1. Start the Interstage Management Console.
2. Select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]).

   The [Repository : View Status] window will be displayed. If the repository is active, stop it.
3. Select the repository to change from the [Repository : View Status] window.
4. Click [Detailed settings] to display the detailed settings.
5. Specify the search time per search request in [Search Timeout].
6. Start the repository from the [Repository : View Status] window.

Refer to 'Services' in the Operator's Guide for the time range that can be specified in [Search Timeout].

10.6.2 Limiting the Number of Entries to be Searched per Search Request

An exclusive search request on a repository with a large amount of registered entry data will result in the slow response of Interstage Directory Service. This delay can be prevented by changing environment settings to limit the number of entries to be searched per search request.

To limit the number of entries searched, per request, change the environment settings as follows:

1. Start the Interstage Management Console.
2. Select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]).
    - The [Repository: View Status] window will be displayed. If the repository is active, stop it.
3. From the [Repository: View Status] window, select the repository to change.
4. Click [Detailed settings] to display the detailed settings.
5. Specify the maximum number of entries to be searched per search request, in [Maximum number of searchable entries].
6. Start the repository from the [Repository: View Status] window.

Refer to 'Services' in the Operator's Guide for the range of allowable values for [Maximum number of searchable entries].

10.6.3 Changing the Connection Cutoff Time in Non-communication State

The connection cutoff time determines when the connection to the client program is interrupted in a non-communication state. The cutoff time can be customized for the environment.

To change the connection cutoff time in a non-communication state, use the Interstage Management Console to change the environment settings according to the following procedure:

1. Start the Interstage Management Console.
2. Select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]).
    - The [Repository: View Status] window will be displayed. If the repository is active, stop it.
3. Select the repository to change from the [Repository: View Status] window.
4. Specify the connection cutoff time in a non-communication state in [Connection Idle Timeout].
5. Start the repository from the [Repository: View Status] window.

Refer to 'Services' in the Operator's Guide for the range of allowable [Connection Idle Timeout] values.

10.6.4 Setting the Maximum Number of Connections from the Repository to the RDB

If an RDB is used for the database and the Interstage Directory Service and the databases are placed on different servers, concurrent search performance can be improved by setting an appropriate value for the maximum number of connections from the repository to the RDB, according machine specifications for the database server.

The maximum number of connections from the repository to the RDB is set using the *irepadmin* command. Refer to "irepadmin" in the "Interstage Directory Service Operation Commands" chapter of the Reference Manual (Command Edition) for more information on how to make this setting.

To change the settings for the maximum number of connections from the repository to the RDB, check that an appropriate value has been set for the maximum number of connections on the database side, and change if necessary.

- **For Symfoware Server**

  Specify either MAX_CONNECT_SYS (if the database and the repository are on the same machine) or MAX_CONNECT_TCP (if the database and the repository are on different machines) in the system environment file.

- **For Oracle databases**

  Specify PROCESSES (SESSIONS and TRANSACTIONS) in the database initialization parameters.

Refer to the database manual for more information on settings for the maximum number of connections on the database side.

10.7 Adding and Deleting User-Defined Schemas

The procedure for adding user-defined schemas is the same as the procedure for extending new schemas. Refer to "Extending Schemas" in the "Creating a Repository" chapter for more information.

User-defined schemas are deleted using the command for registering, deleting and displaying user-defined schemas. Refer to "irepschema" in the "Interstage Directory Service Operation Commands" chapter of the Reference Manual (Command Edition) for more information on how to delete user-defined schemas.

Note

When deleting user-defined schemas, first delete all entries or entry attributes that use the object classes or attributes to be deleted from the entry data in the repository. If entry data that uses these object classes or attributes is left in the repository when the schema definition is deleted, it will not be possible to access these entries.

10.8 Changing Access Control

The procedure for changing access control definitions is the same as the procedure for registering access control definitions. Refer to the "Access Control for the Interstage Directory Service" chapter in the Security System Guide for more information.

10.9 Managing the SSL Communication Environment

To ensure continual SSL communication, the Interstage certificate environment needs to be managed. The Certificates required to use SSL communication have a limited life, so new certificates must be obtained and registered in the Interstage certificate environment and the certificate/key management environment using the SMEE commands, before the current one expires. Additionally, the new CRL (certificate revocation list), if obtained, needs to be registered.

For information on management of the Interstage certificate environment, refer to the 'Setting and Use of the Interstage Certificate Environment' chapter of the Security System Guide. For information on management of the certificate/key management environment using the SMEE commands, refer to the 'Setting and Use of the Certificate/Key Management Environment Using the SMEE Command' chapter of the Security System Guide.

10.10 Backing up and Restoring Interstage Directory Service

Interstage Directory Service repositories, can be backed up using the irepbacksys command. For information on the backup operation, see 'Maintenance (Resource Backup)' in Operator's Guide.

10.11 Optimizing the Repository

10.11.1 Repository Optimization when the Standard Database is Used

If the standard database is used as the repository database, frequent read/write operations to the database storage directory (of the repository) result in fragmentation of the hard disk drive. This causes slow read/write operations and a loss of useable space. Both space and performance can be improved by optimizing the hard disk drive through defragmentation. Periodically defragment the hard disk drive if entries are modified frequently. However, since defragmentation cannot reclaim all free space, the area that cannot be used may grow gradually, leading to insufficient disk space. In such a case, expand the hard disk area.

Note

If an accident, such as a system power failure, occurs during optimization of the repository, data may be damaged. Thus, be sure to back up the repository before optimizing it.

For information on backing up the repository, refer to "Maintenance (Resource Backup)" in the Operator's Guide.

Optimize the repository as follows:

1. Use the Interstage Management Console to stop the repository to be optimized.

2. Solaris32/64 Linux32/64

   Specify "C" in the LANG environment variable.

3. Execute the following optimization command in the following order:

   Example

   When the repository name is "rep001"

   Windows32/64

```
C:\Interstage\Enabler\server\bin\omsreorg.exe rep001 -f
C:\Interstage\Enabler\server\bin\omsreorg.exe rep001 -s
C:\Interstage\Enabler\server\bin\omsreorg.exe rep001 -k
C:\Interstage\Enabler\server\bin\omsreorg.exe rep001 -i
C:\Interstage\Enabler\server\bin\omsreorg.exe rep001 -r
```

   Solaris32/64

```
/opt/FJSVena/server/bin/omsreorg rep001 -f
/opt/FJSVena/server/bin/omsreorg rep001 -s
/opt/FJSVena/server/bin/omsreorg rep001 -k
/opt/FJSVena/server/bin/omsreorg rep001 -i
/opt/FJSVena/server/bin/omsreorg rep001 -r
```

   Linux32/64

```
/opt/FJSVena/Enabler/server/bin/omsreorg rep001 -f
/opt/FJSVena/Enabler/server/bin/omsreorg rep001 -s
/opt/FJSVena/Enabler/server/bin/omsreorg rep001 -k
/opt/FJSVena/Enabler/server/bin/omsreorg rep001 -i
/opt/FJSVena/Enabler/server/bin/omsreorg rep001 -r
```

   Note

   These command options cannot be specified at the same time. Always execute the command options in this order.

4. If optimization terminates normally, the following message will be displayed.

   Example

   When the repository name is "rep001"

```
Datastore rep001 reorganized
```

   If an error message is displayed when the optimization command is executing, take the action shown in the following table:

Message	Actions
Datastore not stopped.	Wait until the repository has stopped, and then re-execute the optimization command. Repository stopping time is dependant on hardware performance and the number of registered entries in the repository. A repository with approximately ten thousand entries (operated continually over an hour) will require an approximate time period of 10 minutes to stop.
Files of datastore were not closed properly. Datastore is inconsistent.	The repository was stopped because of a flawed write. Restart the repository.

Message	Actions
	Re-stop the repository, after starting the target repository, by using the Interstage Management Console. Wait until the repository has stopped, and then re-execute the optimization command.
Administration function currently active on datastore.	The optimization command is already operating. Wait until it has finished.

5. Use the Interstage Management Console to start the optimized repository.

10.11.2 Repository Optimization when Symfoware/RDB is Used

10.11.2.1 Optimization Information Setup

Symfoware/RDB checks the tables associated with the SQL statement instructions to determine processing procedures that correspond to search conditions. This process is referred to as "optimization processing" (or "optimizer"), and is achieved using optimization information based on information about the amount of data and the storage status. This means that optimization information must be collected and set up in advance.

Fujitsu recommend making optimization information settings periodically when the repository is stopped, such as when repository resources are backed up. If optimization information settings are made when repository resources are backed up, Fujitsu recommend making optimization information settings before backup so that resources that have already been restored can be optimized.

Interstage Directory Service provides a sample batch file (for Windows®) and shell script (for Solaris and Linux) for setting up optimization information for Symfoware/RDB with repositories that use Symfoware Server. Users can easily set up database optimization information by entering procedures appropriate to each of these environments in the sample batch file or shell script.

Sample files are provided both for databases where the tables for storing repository data have been created using the *irepgendb* command and databases where the tables for storing repository data have been created using the *irepcrttbl* command.

Sample Files

A sample file for setting up optimization information for Symfoware/RDB can be found at the following location:

Windows32/64

If the tables for storing repository data were created using the *irepgendb* command

- If Symfoware Server has been installed on a Windows ® machine

```
C:\Interstage\IREP\sample\RDB\SYM\ANALYZE\windows\irepanalyze.bat
```

- If Symfoware Server has been installed on a Solaris or Linux machine

```
C:\Interstage\IREP\sample\RDB\SYM\ANALYZE\unix\irepanalyze.sh
```

If the tables for storing repository data were created using the *irepcrttbl* command

- If Symfoware Server has been installed on a Windows ® machine

```
C:\Interstage\IREP\sample\RDB\SYM\ANALYZE\windows\compatible\irepanalyze_80.bat
```

- If Symfoware Server has been installed on a Solaris or Linux machine

```
C:\Interstage\IREP\sample\RDB\SYM\ANALYZE\unix\compatible\irepanalyze_80.sh
```

Solaris32/64 Linux32/64

If the tables for storing repository data were created using the *irepgendb* command

- If Symfoware Server has been installed on a Windows ® machine

```
/opt/FJSVirep/sample/RDB/SYM/ANALYZE/windows/irepanalyze.bat
```

- If Symfoware Server has been installed on a Solaris or Linux machine

```
/opt/FJSVirep/sample/RDB/SYM/ANALYZE/unix/irepanalyze.sh
```

If the tables for storing repository data were created using the *irepcrttbl* command

- If Symfoware Server has been installed on a Windows ® machine

```
/opt/FJSVirep/sample/RDB/SYM/ANALYZE/windows/compatible/irepanalyze_80.bat
```

- If Symfoware Server has been installed on a Solaris or Linux machine

```
/opt/FJSVirep/sample/RDB/SYM/ANALYZE/unix/compatible/irepanalyze_80.sh
```

The following section explains how to define a batch file (for Windows ®) or shell script (for Solaris or Linux) for setting up optimization information.

List of Definition Items

To set up optimization information, change the definition items shown below in the sample batch file or shell script. Ensure that a value is specified for all definition items.

For each definition item, specify the RDB system name, database or database schema name that was specified when the Symfoware/RDB was set up in "Setting up Symfoware/RDB" in the Creating Databases chapter.

Definition item name	Explanation of definition value
RDBNAME	Specify the name of the RDB system. The following characters can be used in RDB system names: A maximum of 8 characters in the range 'A' to 'Z', 'a' to 'z', and 0 to 9. The first character must be a letter.
DBNAME	Specify the name of the database. The following characters can be used in database names: A maximum of 8 characters in the range 'A' to 'Z', 'a' to 'z', and 0 to 9. The first character must be a letter.
SCHEMA	Specify the name of the schema for the database. Specify the same schema name that was specified for the operating system account specified when the database was created. The following characters can be used in database schema names: A maximum of 30 characters in the range 'A' to 'Z', and 0 to 9. The first character must be a letter.

There is no need to change any definition items other than the items above in order to use the sample file.

Syntax

Use the following format for the definition items in the "List of Definition Items" specified in the sample batch file or shell script.

```
set definition item name = definition value
```

- Enter one definition item per line.
- Definition item names cannot be omitted.

Example

The following example shows how to specify "DSDBSYS" for the RDB system name, "DSDB" for the database name and "DSADMIN" for the database schema name.

```
set RDBNAME=DSDBSYS
set DBNAME=DSDB
set SCHEMA=DSADMIN
```

Execution Method

1. Stop the repository for the Interstage Directory Service

   Refer to "10.1 Starting/Stopping a Repository" for information on how to stop the repository.

2. Log on to the machine where Symfoware Server is installed

   Log in using either the operating system account that was registered in "Registering a User for Connecting to the Repository Database" (refer to the Creating Databases chapter) or the administrator account ("Administrator" for Windows ® systems; "root" for Solaris or Linux systems; not a user account with administrator privileges).

3. Modify the batch file or shell script

   The sample batch file (for Windows ®) or shell script (for Solaris or Linux) is copied to the working directory.

   Modify the sample batch file or shell script by referring to "List of Definition Items" and "Syntax".

   EXIT is also described in the Windows(R) batch file sample, so that the batch ends normally. Correct this appropriately for the application.

4. Security measures

   It is possible that a security gap will occur in the batch file or the shell script. It is important to ensure that execution can only be done by either the system administrator account (if using Windows(R), this is "the Administrator", if using Solaris or Linux, this is the "root"), or the OS account that was registered as the "repository database connection user". We recommend changing the execution permissions of the batch file or the shell script.

5. Execute the batch file or shell script

   Execute the batch file or shell script that was modified in step 3.

   Examples are shown below.

Example

Windows32/64

```
C:\Interstage\IREP\sample\RDB\SYM\ANALYZE\windows\irepanalyze.bat
```

Solaris32/64 Linux32/64

```
/opt/FJSVirep/sample/RDB/SYM/ANALYZE/unix/irepanalyze.sh
```

Defragmentation

In Symfoware/RDB, the mapping of storage data in the allocated database space is automatically tuned or adjusted. However, if data is repeatedly added, updated or deleted, the automatic tuning range can be exceeded. This can cause fragmentation of data, resulting in a loss of efficient processing.

Check the fragmentation status periodically.

If a fragmentation status check reveals that the average usage rate of the table or the index is 80% or less, defragmentation is recommended.

In the Interstate Directory Service, samples for checking fragmentation status and for defragmentation are provided in a batch file (Windows (R)) or a shell script (Solaris or Linux). The administrator can easily check the fragmentation status or perform defragmentation. Simply follow the procedures outlined in the batch file or the shell script as appropriate for that environment.

This is a sample that is provided for repository data storage tables created using the irepgendb command.

Checking Fragmentation Status

Samples

Samples for checking the fragmentation status of Symfoware/RDB are contained in the following directory:

Windows32/64

When Symfoware Server is installed on Windows(R)

```
C:\Interstage\IREP\sample\RDB\SYM\GARBAGE\windows\irepgcstat.bat
```

When Symfoware Server is installed on Solaris or Linux

```
C:\Interstage\IREP\sample\RDB\SYM\GARBAGE\unix\irepgcstat.sh
```

Solaris32/64 Linux32/64

If Symfoware Server was installed in Windows(R)

```
/opt/FJSVirep/sample/RDB/SYM/GARBAGE/windows/irepgcstat.bat
```

If Symfoware Server was installed in Solaris or Linux

```
/opt/FJSVirep/sample/RDB/SYM/GARBAGE/unix/irepgcstat.sh
```

Below is an explanation of the definition method for batch files (Windows(R)) or shell script (Solaris or Linux), in order to check the fragmentation status.

List of Definition Items

To check fragmentation, update the definition items shown below in the sample batch file or shell script. Ensure that a value is specified for all definition items.

For each definition item, specify the RDB system name and database name that were specified in "Symfoware/RDB Set up" at the time of Symfoware/RDB set up.

Definition item name	Explanation of definition value
RDBNAME	Specify the name of the RDB system. The following characters can be used in RDB system names: A maximum of 8 characters in the range 'A' to 'Z', 'a' to 'z', and 0 to 9. The first character must be a letter.
DBNAME	Specify the name of the database. The following characters can be used in database names: A maximum of 8 characters in the range 'A' to 'Z', 'a' to 'z', and 0 to 9. The first character must be a letter.

If using a sample, it is not necessary to update any definition items other than those mentioned above.

Description Format

The definition items in "List of Definition Items", specified in the batch file and shell script samples, are described in the format below.

```
set definition item name = definition value
```

- 1 definition item is stated per line.

- Definition item names cannot be omitted.

Example

In this example, "DSDBSYS" is specified for the RDB system name, and "DSDB" is specified for the database name in the Windows(R) batch file. If using Solaris or Linux, specify the same in the shell script.

```
rem------------------------------------
set RDBNAME=DSDBSYS
set DBNAME=DSDB
rem------------------------------------
```

Method of execution

1. Log in to the machine on which Symfoware Server is installed

   Either log in to the system administrator account (in Windows(R), this is "Administrator"; in Solaris/Linux, it is "root"), or log in using the OS account that was registered as the "repository database connection user".

2. Correct the samples

   Copy the batch file (Windows(R)) or shell script (Solaris/Linux) samples to the work directory.

   Refer to "Description Format" and "List of Definition Items", and correct the batch file (Windows (R)) or shell script (Solaris/Linux) samples.

3. Security measures

   It is possible that a security gap will occur in the batch file or the shell script. It is important to ensure that execution can only be done by either the system administrator account (if using Windows(R), "the Administrator", if using Solaris or Linux, the "root"), or the OS account that was registered as the "repository database connection user". We recommend changing the execution permissions of the batch file or the shell script.

4. Set the LANG environment variable

   Set the Symfoware/RDB locale (the OS default locale) in the LANG environment variable.

5. Delete the execution result output destination file

   The batch file or shell script execution result is output as follows:

   ```
   Directory in which the batch file or shell script was executed/log/irepgcstat.log
   ```

   Write permissions for the user account that was logged into in step 1 are required for the batch file or shell script execution result output destination file.

   If the file has previously been executed using a different user account, the write permissions for the user account that was logged into in step 1 are not part of the access permissions for the execution result output destination file. For this reason, delete the execution result output destination file. If this file is required, back it up by changing the file name using system administrator permissions.

6. Execute the batch file or shell script

   Execute the batch file or shell script that was corrected.

   An example is shown below.

   Windows32/64

   ```
   C:\work\irepgcstat.bat
   ```

   Solaris32/64 Linux32/64

   ```
   /work/irepgcstat.sh
   ```

7.The execution result is displayed.

```
==================================================
  DSI Defragmentation
        Table : 85%
```

```
        Index : 75%
==================================================
```

Name of displayed item	Explanation of displayed item
Table	This is the average table usage rate (the rate at which data is stored for DSI pages that are in use). If this is 80% or less, defragmentation is recommended.
Index	This is the average index usage rate (the rate at which data is stored for DSI pages that are in use). If this is 80% or less, defragmentation is recommended.

The batch file or shell script execution result is output to the file shown in step 5. The character code type of the file is the character code type when Symfoware Server was installed.

Defragmentation

Samples

Symfoware/RDB defragmentation samples are contained in the following directory:

Windows32/64

When Symfoware Server is installed on Windows(R)

```
C:\Interstage\IREP\sample\RDB\SYM\GARBAGE\windows\irepgarbage.bat
```

When Symfoware Server is installed on Solaris or Linux

```
C:\Interstage\IREP\sample\RDB\SYM\GARBAGE\unix\irepgarbage.sh
```

Solaris32/64 Linux32/64

When Symfoware Server is installed on Windows(R)

```
/opt/FJSVirep/sample/RDB/SYM/GARBAGE/windows/irepgarbage.bat
```

When Symfoware Server is installed on Solaris or Linux

```
/opt/FJSVirep/sample/RDB/SYM/GARBAGE/unix/irepgarbage.sh
```

The method to define the batch file (Windows(R)) or shell script (Solaris/Linux) for defragmentation is explained in this section.

List of Definition Items

The definition items in the batch file or shell script samples, shown in the table below, are modified for defragmentation. Ensure that a value is specified for all definition items.

For each definition item, specify the RDB system name and database name that were specified in "Symfoware/RDB Set up" at the time of Symfoware/RDB set up.

Definition item name	Explanation of definition value
RDBNAME	Specify the name of the RDB system. The following characters can be used in RDB system names: A maximum of 8 characters in the range 'A' to 'Z', 'a' to 'z', and 0 to 9. The first character must be a letter.
DBNAME	Specify the name of the database.

Definition item name	Explanation of definition value
	The following characters can be used in database names: A maximum of 8 characters in the range 'A' to 'Z', 'a' to 'z', and 0 to 9. The first character must be a letter.
W_DIR	Specify the path name of the directory for storing reconfiguration command work files. Use the full path. The formula for calculating the required capacity for the work area (in kilobytes) is shown below. When detailed settings are not configured using the table creation command (14 * number of entries + 48) * r When detailed settings are configured using the table creation command Maximum size of the indexes specified in the detail definition file * r r: Safety margin (1.5 or greater)
U_DIR	Specify the path name of the directory for storing reconfiguration command interim backup files. Use the full path. The formula for calculating the required capacity for the interim backup area (in kilobytes) is shown below. When detailed settings are not configured using the table creation command 13.6 * number of entries + 160 When detailed settings are configured using the table creation command Maximum size of the tables specified in the detail definition file
TARGET	Either of the following can be specified as the reconfiguration target DSI: FULL Both the table and the index are targets INDEX Only the index is a target

If using a sample, it is not necessary to update any definition items other than those mentioned above.

Description Format

The definition items in "List of Definition Items", specified in the batch file and shell script samples, are described in the format below.

```
set definition item name = definition value
```

- 1 definition item is stated per line.
- Definition item names cannot be omitted.

Example

In this example, "DSDBSYS" is specified for the RDB system name, and "DSDB" is specified for the database name in the Windows(R) batch file. If using Solaris or Linux, specify the same in the shell script.

Windows32/64

```
rem----------------------------------
set RDBNAME=DSDBSYS
set DBNAME=DSDB
set W_DIR=C:\work
```

```
  set U_DIR=C:\back
  set TARGET=INDEX  rem-----------------------------------
```

Method of execution

1. Stop the Interstage directory service repository

   For details on stopping the repository, refer to "Starting/Stopping a Repository".

2. Log in to the machine on which Symfoware Server is installed

   Either log in to the system administrator account (in Windows(R), this is "Administrator"; in Solaris/Linux, it is "root"), or log in using the OS account that was registered as the "repository database connection user".

3. Correct the samples

   Copy the batch file (Windows(R)) or shell script (Solaris/Linux) samples to the work directory.

   Refer to "Description Format" and "List of Definition Items", and correct the batch file (Windows (R)) or shell script (Solaris/Linux) samples.

4. Security measures

   It is possible that a security gap will occur in the batch file or the shell script. It is important to ensure that execution can only be done by either the system administrator account (if using Windows(R), "the Administrator", if using Solaris or Linux, the "root"), or the OS account that was registered as the "repository database connection user". We recommend changing the execution permissions of the batch file or the shell script.

5. Set the LANG environment variable

   Set the Symfoware/RDB locale (the OS default locale) in the LANG environment variable.

6. Delete the execution result output destination file

   The batch file or shell script execution result is output as follows:

   ```
   Directory in which the batch file or shell script was executed/log/irepgarbage.log
   ```

   Write permissions for the user account that was logged into in step 1 are required for the batch file or shell script execution result output destination file.

   If the file has previously been executed using a different user account, the write permissions for the user account that was logged into in step 1 are not part of the access permissions for the execution result output destination file. For this reason, delete the execution result output destination file. If this file is required, back it up by changing the file name using system administrator permissions.

7. Execute the batch file or shell script

   Execute the batch file or shell script that was corrected.

   An example is shown below.

   Windows32/64

   ```
   C:\work\irepgarbage.bat
   ```

   Solaris32/64 Linux32/64

   ```
   /work/irepgarbage.sh
   ```

8. A confirmation window is displayed.

   ```
     ================== WARNING ========================
     = Fragmentation takes a short period to clear.  =
     = Do not stop this process once it has started, =
     = as this may cause corruption of the database.  =
     =================================================
   Garbage start? [y, q]: y or q <RETURN>
   ```

The batch file or shell script execution result is output to the file shown in step 6. The character code type of the file is the character code type when Symfoware Server was installed.

If the execution fails, refer to Symfoware Server "Messages" to establish the cause of the error. Take action, and then re-execute.

9. Optimization settings

   Set the optimization information for the Symfoware/RDB that is defragmented.

10.12 Recovering Repositories

10.12.1 Standalone Operation

This section explains the repository recovery procedure for stand-alone mode.

Environment Has been Destroyed

If the environment is damaged, recreate a repository in stand-alone mode. The repository can be restored by using the backup directory (for Solaris/Linux, it is backup file). If there is no backup directory (for Solaris/Linux, it is backup file), the repository needs to be recreated.

The following describes the procedure used to restore the repository from the backup directory (for Solaris/Linux, it is backup file) for a stand-alone operation,

1. Stop the repository using Interstage Management Console.
2. Delete the repository stopped in step 1.
3. Use the ireprestsys command to restore the repository from the backup directory (for Solaris/Linux, it is backup file).

   Example

   Windows32/64

   Backup directory name: X:\Backup\irep\rep001_back

   Repository name: rep001

```
ireprestsys -d X:\Backup\irep\rep001_back -R rep001
IREP: INFO: irep11001: Restore has completed.  X:\Backup\irep\rep001_back [rep001]
```

   Solaris32/64 Linux32/64

   Backup file name: /backup/irep/rep001_back.tar.gz

   Repository name: rep001

```
ireprestsys -f /backup/irep/rep001_back.tar.gz -R rep001
UX:IREP: INFO: irep11001: Restore has completed.  /backup/irep/rep001_back.tar.Z [rep001]
```

4. Use the Interstage Management Console to start the recreated repository.

   Data in Database Has been Destroyed

   If the Standard Database is Used

   When data in database has been destroyed, only restore the data in database.

   Data in database can be restored to the status when it has been backed up by using the backup directory (for Solaris/Linux, it is backup file). If there is no backup directory (for Solaris/Linux, it is backup file), the data needs to be recreated.

   The following procedure details how to restore data in the database of the repository in stand-alone mode:

5. Stop the repository using Interstage Management Console.
6. Delete the repository stopped in step 1.
7. Using the Interstage Management Console set the following items with same value of the repository deleted in step 2, and then create a new repository.

   - [Repository name]

- [Public directory]
- [Create default tree?]
- [User password encryption method]
- [Database storage directory]

8. Select [System] > [Service] > [Repository] > [Create a New Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository] > [Create a New Repository]). Click the [Create] button.

9. Use the ireprestsys command (with the -dataonly option) to restore the repository from the latest backup directory (for Solaris/Linux, it is backup file). Specify the same repository name as the backup repository.

10. A message displays, requesting confirmation to replace the database. To replace the database and continue restoring the repository, enter 'y' or 'Y'. To stop restoring the repository, enter 'n' or 'N'. If any other key is typed, the confirmation message is displayed again.

    Example

    Windows32/64

    Backup directory name: X:\Backup\irep\rep001_back

    Repository name: rep001

    ```
    ireprestsys -d X:\Backup\irep\rep001_back -R rep001 -dataonly
    Data already exists in database store.  (C:\Interstage\Enabler\EnablerDStores\IREP\rep001\data)
    Are you sure of deleting data in database store? (y/n):y
    IREP: INFO: irep11001: Restore has completed.  X:\Backup\irep\rep001_back [rep001]
    ```

    Solaris32/64

    Backup file name: /backup/irep/rep001_back.tar.gz

    Repository name: rep001

    ```
    #ireprestsys -f /backup/irep/rep001_back.tar.gz -R rep001 -dataonly
    Data already exists in database store.  (/var/opt/FJSVena/EnablerDStores/FJSVirep/rep001/data)
    Are you sure of deleting data in database store? (y/n):y
    UX:IREP: INFO: irep11001: Restore has completed.  /backup/irep/rep001_back.tar.Z [rep001]
    ```

    Linux32/64

    Backup file name: /backup/irep/rep001_back.tar.gz

    Repository name: rep001

    ```
    ireprestsys -f /backup/irep/rep001_back.tar.gz -R rep001 -dataonly
    Data already exists in database store.  (/var/opt/FJSVena/DStores/FJSVirep/rep001/data)
    Are you sure of deleting data in database store? (y/n):y
    UX:IREP: INFO: irep11001: Restore has completed.  /backup/irep/rep001_back.tar.Z [rep001]
    ```

11. Use the Interstage Management Console to start repository.

For details of the ireprestsys commands, see 'Backup commands' in the Reference Manual (Command Edition).

- **If an RDB is Used**

  If an RDB is used and data in the database becomes damaged, restore the data. The backup, restore, and recovery functions of the RDB product can be used to restore the data in the database to the state when the last backup was taken. If there is no backup, the data must be created again from scratch.

  The data restoration procedure is described below.

  - If a Backup Exists

    1. Use the Interstage Management Console to stop the repository to be restored.

2. Use the RDB function to restore the backed up data.

   For details about how to restore backed up data, refer to "Maintenance (Backing up resources)" - "Backing up and restoring resources" - "Restoration procedure (Managed Server and Stand-alone Server)" - "Restoring Interstage Directory Service resources" in the "Interstage Application Server Operator's Guide".

3. Use the Interstage Management Console to start the restored repository.

- There is no Backup

  1. Use the Interstage Management Console to stop the repository to be restored.

  2. Delete the repository stopped in step 1.

  3. Delete the database that was connected to the repository stopped in step 1.

     If Symfoware/RDB is being used, delete the database by referring to "Deleting the Database" under "Using Symfoware/RDB" in the "Creating Databases" chapter.

     If an Oracle database is being used, delete the database by referring to "Deleting Databases" under "Using the Oracle Database" in the "Creating Databases" chapter.

  4. Create a new stand-alone system.

  Refer to "Environment setup" - "Environment setup procedure" and create the stand-alone system.

10.12.2 Load Balancing Operations

This section explains how to recover the repository if problems occur during load balancing operations and the repository needs to be recovered.

If Load Balancing is being Performed in Database Sharing Mode

The procedure for recovering the repository and the database is the same as for "10.12.1 Standalone Operation".

If Load Balancing is being Performed in Replication Mode

Refer to "the "Creating a Load Distribution Environment (Replication Mode)" chapter for information on how to recover the repository and the database.

10.13 Deleting the Repository

Delete Interstage Directory Service repositories using the Interstage Management Console.

To delete repositories, start the Interstage Management Console, log in, and then open the [System] > [Services] > [Repository] > [Repository: Status] window. For the management server, open the [Application Management] > [Interstage Management Console] > [Interstage Application Server] > [Security] > [Repository] > [Repository:Status] window.

Refer to "Starting and stopping the Interstage Management Console" in the Interstage Application Server Operator's Guide for information on stopping the Interstage Management Console. Refer to the Interstage Management Console help for information on Interstage Management Console operations.

If RDB is used, in addition to deleting the Interstage Directory Service repository use the RDB function to delete the database.

For information on how to delete the database, refer to "Deleting the Database" under "Using Symfoware/RDB" in the "Creating Databases" chapter if Symfoware/RDB is being used; refer to "Deleting Databases" under "Using the Oracle Database" in the "Creating Databases" chapter if an Oracle database is being used.

Appendix A Interstage Directory Service Object Classes

This appendix describes the object classes that can be used in Interstage Directory Service. Note that object classes not listed in this appendix cannot be used.

[A]

- account
- applicationEntity
- applicationProcess

[C]

- certificationAuthority
- certificationAuthority-V2
- corbaContainer
- corbaObject
- corbaObjectReference
- country
- cRLDistributionPoint

[D]

- dcObject
- deltaCRL
- device
- dmd
- dNSDomain
- document
- documentSeries
- domain
- domainRelatedObject

[F]

- friendlyCountry

[G]

- groupOfNames
- groupOfUniqueNames

[I]

- inetOrgPerson

[J]

- javaContainer
- javaMarshalledObject
- javaNamingReference
- javaObject
- javaSerializedObject

A.1 List of Objects

A.1.1 [A]

account

Definition

Define computer account information. This object class is defined in RFC1274.

OID

0.9.2342.19200300.100.4.5

Base Class

top

Type

STRUCTURAL

Required Attributes

uid(userid)	The user ID of an account.

Optional Attributes

description	A description for this entry.
seeAlso	The DN information related to this entry.
l (localityName)	A related country, city, or other geographical area.
o (organizationName)	An organization name.
ou (organizationalUnitName)	An organization unit name.
host	The host name of a computer.

applicationEntity

Definition

Define an application entity. This object class is defined in RFC2256.

OID

2.5.6.12

Base Class

top

Type

STRUCTURAL

Required Attributes

presentationAddress	The OSI display address of the entry.
cn (commonName)	A common name or full name.

Optional Attributes

supportedApplicationContext	A description of the entry.
seeAlso	The DN information related to this entry.
ou (organizationalUnitName)	An organization unit name.
o (organizationName)	An organization name.
l (localityName)	A related country, city, or other geographical area.
description	DN information related to an account.

applicationProcess

Definition

Define an application process. This object class is defined in RFC2256.

OID

2.5.6.11

Base Class

top

Type

STRUCTURAL

Required Attributes

cn (commonName)	A common name or full name.

Optional Attributes

seeAlso	The DN information related to this entry.
ou (organizationalUnitName)	An organization unit name.
l (localityName)	A related country, city, or other geographical area.
description	DN information related to an account.

A.1.2 [C]

certificationAuthority

Definition

Define the information related to the certificate issuing authority (Certificate Authorities CAs) of a directory. This object class is defined in RFC2256.

OID

2.5.6.16

Base Class

top

Type

AUXILIARY

Required Attributes

authorityRevocationList	A list of revoked certificate authorities.
certificateRevocationList	A list of revoked user certificates.
cACertificate	A CA certificate.

Optional Attributes

crossCertificatePair	A cross certificate.

certificationAuthority-V2

Definition

Define the information related to the certificate issuing authority (Certificate Authorities, CAs) of a directory.

OID

2.5.6.16.2

Base Class

certificationAuthority

Type

AUXILIARY

Optional Attributes

deltaRevocationList	A list of revoked deltas

corbaContainer

Definition

Define the container of a CORBA object.

OID

1.3.6.1.4.1.42.2.27.4.2.10

Base Class

top

Type

STRUCTURAL

Required Attributes

cn (commonName)	A common name or full name.

corbaObject

Definition

Define a CORBA object.

OID

1.3.6.1.4.1.42.2.27.4.2.9

Base Class

top

Type

ABSTRACT

Optional Attributes

corbaRepositoryId	A Repository ID implemented by a CORBA object.
description	DN information related to an account.

corbaObjectReference

Definition

Define a CORBA object reference.

OID

1.3.6.1.4.1.42.2.27.4.2.11

Base Class

corbaObject

Type

AUXILIARY

Required Attributes

corbaIor	A character string representation of IOR of a CORBA object

country

Definition

Define a country. This object class is defined in RFC2256.

OID

2.5.6.2

Base Class

top

Type

STRUCTURAL

Required Attributes

c (countryName)	A two-character code defined by ISO to indicate a country name in the directory.

Optional Attributes

description	DN information related to an account.

cRLDistributionPoint

Definition

Define the way in which CRL information can be obtained.

OID

2.5.6.19

Base Class

top

Type

STRUCTURAL

Required Attributes

Cn (commonName)	A common name or full name.

Optional Attributes

certificateRevocationList	A list of revoked user certificates.
authorityRevocationList	A list of revoked certificate authorities.
deltaRevocationList	A list of revoked deltas.

A.1.3 [D]

dcObject

Definition

Define the domain component of the entry. This object class is defined in RFC2247.

OID

1.3.6.1.4.1.1466.344

Base Class

top

Type

AUXILIARY

Required attributes

dc (domainComponent)	A DNS domain.

deltaCRL

Definition

Define a list of revoked deltas. This object class is defined in RFC2587.

OID

2.5.6.23

Base Class

top

Type

AUXILIARY

Optional attributes

deltaRevocationList	A list of revoked deltas.

device

Definition

Define information on network devices such as printers.

OID

2.5.6.14

Base Class

top

Type

STRUCTURAL

Required Attributes

Cn (commonName)	A common name or full name.

Optional Attributes

serialNumber	A serial number.
seeAlso	The DN information related to this entry.
Owner	The distinguished name of the responsible person.
ou (organizationalUnitName)	An organization unit name.
o (organizationName)	An organization name.
l (localityName)	A related country, city, or other geographical area.
description	DN information related to an account.

dmd

Definition

Define directory management domain information.

OID

2.5.6.20

Base Class

top

Type

STRUCTURAL

Required Attributes

dmdName	The administration permission required to operate a directory management domain (DMD) and a directory server.

Optional Attributes

userPassword	A user password.
seeAlso	The DN information related to this entry.
businessCategory	The type of business in which the entry is engaged.
x121Address	The x121 address of the user.
registeredAddress	A registered emergency contact address.
destinationIndicator	The address information required to provide the telegram service.
telexNumber	A telex number.
telephoneNumber	A telephone number.
internationaliSDNNumber	An international ISDN number.
facsimileTelephoneNumber (fax)	A FAX number.
street (streetAddress)	The building name and street number of the entry.
postOfficeBox	A post-office box.
postalCode	A postal code.
postalAddress	A postal address.
physicalDeliveryOfficeName	The name of the city, town, or village in which the office is located.
st (stateOrProvinceName)	The name of the state or province in which the entry is located.
l (localityName)	A related country, city, or other geographical area.
description	DN information related to an account.

dNSDomain

Definition

Define a DNS resource record.

OID

0.9.2342.19200300.100.4.15

Base Class

domain

Type

STRUCTURAL

Optional Attributes

aRecord	An Address DNS resource.

mDRecord	The equivalent of an MD record in DNS.
mXRecord	A Mail Exchange DNS resource.
nSRecord	A Name Server DNS resource.
sOARecord	A Start of Authority DNS resource.
cNAMERecord	The proper name of a DNS resource.

document

Definition

The document object class is used to define entries which represent documents.

OID

0.9.2342.19200300.100.4.6

Base Class

top

Type

STRUCTURAL

Required Attributes

documentIdentifier	The unique identifier of a document.

Optional Attributes

cn (commonName)	A common name or full name.
description	DN information related to an account.
seeAlso	The DN information related to this entry.
l (localityName)	A related country, city, or other geographical area.
o (organizationName)	An organization name.
ou (organizationalUnitName)	An organization unit name.
documentTitle	The title of the document.
documentVersion	The version of the document.
documentAuthor	The distinguished name of the document author.
documentLocation	The location of the original copy of the document.
documentPublisher	A user or organization that published the document.

documentSeries

Definition

Define a document series.

OID

0.9.2342.19200300.100.4.9

Base Class

top

Type

STRUCTURAL

Required Attributes

cn (commonName)	A common name or full name.

Optional attributes

description	DN information related to an account.
seeAlso	The DN information related to this entry.
telephonenumber	A telephone number.
l (localityName)	A related country, city, or other geographical area.
o (organizationName)	An organization name.
ou (organizationalUnitName)	An organization unit name.

domain

Definition

Define a DNS domain.

OID

0.9.2342.19200300.100.4.13

Base Class

top

Type

STRUCTURAL

Required Attributes

dc (domainComponent)	DNS domain.

Optional (Attributes

associatedName	An entry in the organizational DIT entry related to a DNS domain.
o (organizationName)	An organization name.
description	DN information related to an account.
businessCategory	The type of business in which the entry is engaged.
seeAlso	The DN information related to this entry.
userPassword	A user password.
l (localityName)	A related country, city, or other geographical area.
st (stateOrProvinceName)	The name of the state or province in which the entry is located.
street (streetAddress)	The building name and street number of the entry.
physicalDeliveryOfficeName	The name of the city, town, or village in which the office is located.
postalAddress	A postal address.
postalCode	A postal code.
postOfficeBox	A post-office box.
facsimileTelephoneNumber (fax)	A FAX number.
internationaliSDNNumber	An international ISDN number.
telephoneNumber	A telephone number.
telexNumber	A telex number.
destinationIndicator	The address information required to provide the telegram service.

registeredAddress	A registered emergency contact address.
x121Address	The x121 address of the user.

domainRelatedObject

Definition

Define an entry that is the DNS domain equivalent of the X.500 domain representing an organization or organization unit. This object class is defined in RFC1274.

OID

0.9.2342.19200300.100.4.17

Base Class

top

Type

AUXILIARY

Required Attributes

associatedDomain	An entry in the organizational DIT entry related to the DNS domain.

A.1.4 [F]

friendlyCountry

Definition

Define a friendly country. This object class is defined in RFC2256.

OID

0.9.2342.19200300.100.4.18

Base Class

country

Type

STRUCTURAL

Required Attributes

co (friendlyCountryName)	A country name.

A.1.5 [G]

groupOfNames

Definition

Define a group name. This object class is defined in RFC2256.

OID

2.5.6.9

Base Class

top

Type

STRUCTURAL

Required Attributes

member	The distinguished name of a group name member.
cn (commonName)	A common name or full name.

Optional Attributes

businessCategory	The type of business in which the entry is engaged.
seeAlso	The DN information related to this entry.
owner	The distinguished name of a responsible person.
ou (organizationalUnitName)	An organization unit name.
O (organizationName)	An organization name.
description	The description of the entry.

groupOfUniqueNames

Definition

Define a group of unique names. This object class is defined in RFC2256.

OID

2.5.6.17

Base Class

top

Type

STRUCTURAL

Required Attributes

uniqueMember	A group of names associated with an entry where each name was given a uniqueIdentifier to distinguish it.
cn (commonName)	A common name or full name.

Optional Attributes

businessCategory	The type of business in which the entry is engaged.
seeAlso	The DN information related to this entry.
owner	The distinguished name of a responsible person.
ou (organizationalUnitName)	An organization unit name.
o (organizationName)	An organization name.
description	A description of the entry.

A.1.6 [I]

inetOrgPerson

Definition

Define an entry of an Internet user of an organization. This object class is defined in RFC2789.

OID

2.16.840.1.113730.3.2.2

Base Class

organizationalPerson

Type

STRUCTURAL

Optional Attributes

Audio	A sound file.
businessCategory	The type of business in which the entry is engaged.
carLicense	An automobile license plate number.
departmentNumber	A department number.
displayName	The display name of the entry.
employeeNumber	An employee number.
employeeType	An employment type.
givenName (gn)	The generation information of the name.
homePhone (homeTelephoneNumber)	A home telephone number.
homePostalAddress	A home address.
initials	Initials.
jpegPhoto	A JPEG photo.
labeledURI	A Uniform Resource Identifier (URI).
mail (rfc822Mailbox)	An email address.
manager	The distinguished name of a manager.
mobile (mobileTelephoneNumber)	A mobile telephone number.
o (organizationName)	An organization name.
pager (pagerTelephoneNumber)	A pager number.
roomNumber	The room number of an object.
secretary	A secretary or assistant.
uid (userid)	A user ID.
userCertificate	A user certificate.
preferredLanguage	The preferred language.
userSMIMECertificate	An S/MINE certificate.
userPKCS12	User PKCS#12.

A.1.7 [J]

javaContainer

Definition

Define the container for a JAVA object.

OID

1.3.6.1.4.1.42.2.27.4.2.1

Base Class

top

Type

STRUCTURAL

Required Attributes

cn (commonName)	A common name or full name.

javaMarshalledObject

Definition

Define a JAVA Marshaled object.

OID

1.3.6.1.4.1.42.2.27.4.2.8

Base Class

javaObject

Type

AUXILIARY

Required Attributes

javaSerializedData	Java serialized data.

javaNamingReference

Definition

Define a JNDI reference.

OID

1.3.6.1.4.1.42.2.27.4.2.7

Base Class

javaObject

Type

AUXILIARY

Optional Attributes

javaReferenceAddress	The address of a JNDI reference.
javaFactory	The location from which to load an object factory identified with the javaFactory attribute.

javaObject

Definition

Define a JAVA object.

OID

1.3.6.1.4.1.42.2.27.4.2.4

Base Class

top

Type

ABSTRACT

Required Attributes

javaClassName	A Java class name or interface name.

Optional Attributes

javaClassNames	The class name of an object factory that can be used to create an instance of an object identified by the attribute javaClassName.
javaCodebase	The URL of a class definition.
javaDoc	The JAVA document of a class.
description	A description of the entry.

javaSerializedObject

Definition

Define a JAVA serialized object.

OID

1.3.6.1.4.1.42.2.27.4.2.5

Base Class

javaObject

Type

AUXILIARY

Required Attributes

javaSerializedData	Java serialized data.

A.1.8 [L]

labeledURIObject

Definition

Define URL value information and an existing directory object. This object class is defined in RFC2079.

OID

1.3.6.1.4.1.250.3.15

Base Class

top

Type

AUXILIARY

Optional Attributes

labeledURI	A Uniform Resource Identifier (URI). Example: labeledURI: http://www.fujitsu.com

locality

Definition

Define a locality or geographical area. This object class is defined in RFC2256.

OID

2.5.6.3

Base Class

top

Type

STRUCTURAL

Optional Attributes

street (streetAddress)	The building name and street number of the entry.
seeAlso	The DN information related to this entry.
st (stateOrProvinceName)	The name of the state or province in which the entry is located.
l (localityName)	A related country, city, or other geographical area.
description	The description of the entry.

A.1.9 [O]

organization

Definition

Define an organization. This object class is defined in RFC2256.

OID

2.5.6.4

Base Class

top

Type

STRUCTURAL

Required Attributes

o (organizationName)	An organization name.

Optional Attributes

userPassword	A user password.
seeAlso	The DN information related to this entry.
businessCategory	The type of business in which the entry is engaged.
x121Address	The x121 address of the user.
registeredAddress	A registered emergency contact address.
destinationIndicator	The address information required to provide the telegram service.
telexNumber	A telex number.
telephoneNumber	A telephone number.
internationaliSDNNumber	A related country, city, or other geographical area.
facsimileTelephoneNumber (fax)	A FAX number.
street (streetAddress)	The building name and street number of the entry.
postOfficeBox	A post-office box.
postalCode	A postal code.
postalAddress	A postal address.
physicalDeliveryOfficeName	The name of the city, town, or village in which the office is located.
st (stateOrProvinceName)	The name of the state or province in which the entry is located.
l (localityName)	A related country, city, or other geographical area.

description	The description of the entry.

organizationalPerson

Definition

Define a user who is an employee or a relevant person in an organization. This object class is defined in RFC2256.

OID

2.5.6.7

Base Class

person

Type

STRUCTURAL

Optional Attributes

Title	A title.
x121Address	The x121 address of the user.
registeredAddress	A registered emergency contact address.
destinationIndicator	The address information required to provide the telegram service.
telexNumber	A telex number.
telephoneNumber	A telephone number.
internationaliSDNNumber	A related country, city, or other geographical area.
facsimileTelephoneNumber (fax)	A FAX number.
street (streetAddress)	The building name and street number of the entry.
postOfficeBox	A post-office box.
postalCode	A postal code.
postalAddress	A postal address.
physicalDeliveryOfficeName	The name of the city, town, or village in which the office is located.
ou (organizationalUnitName)	An organization unit name.
st (stateOrProvinceName)	The name of the state or province in which the entry is located.
l (localityName)	A related country, city, or other geographical area.

organizationalRole

Definition

Define the role of an organization. This object class is defined in RFC2256.

OID

2.5.6.8

Base Class

top

Type

STRUCTURAL

Required Attributes

cn (commonName)	A common name or full name.

Optional Attributes

x121Address	The x121 address of the user.
registeredAddress	A registered emergency contact address.
destinationIndicator	The address information required to provide the telegram service.
telexNumber	A telex number.
telephoneNumber	A telephone number.
internationaliSDNNumber	A related country, city, or other geographical area.
facsimileTelephoneNumber (fax)	A FAX number.
seeAlso	The DN information related to this entry.
roleOccupant	The distinguished name of the user acting in the role defined in the organizationalRole entry.
street (streetAddress)	The building name and street number of the entry.
postOfficeBox	A post-office box.
postalCode	A postal code.
postalAddress	A postal address.
physicalDeliveryOfficeName	The name of the city, town, or village in which the office is located.
ou (organizationalUnitName)	An organization unit name.
st (stateOrProvinceName)	The name of the state or province in which the entry is located.
l (localityName)	A related country, city, or other geographical area.
description	The description of the entry.

organizationalUnit

Definition

Define an organization unit. This object class is defined in RFC2256.

OID

2.5.6.5

Base Class

top

Type

STRUCTURAL

Required Attributes

ou (organizationalUnitName)	An organization unit name.

Optional Attributes

userPassword	A user password.
seeAlso	The DN information related to this entry.
businessCategory	The type of business in which the entry is engaged.
x121Address	The x121 address of the user.
registeredAddress	A registered emergency contact address.
destinationIndicator	The address information required to provide the telegram service.
telexNumber	A telex number.

telephoneNumber	A telephone number.
internationaliSDNNumber	A related country, city, or other geographical area.
facsimileTelephoneNumber (fax)	A FAX number.
street (streetAddress)	The building name and street number of the entry.
postOfficeBox	A post office box.
postalCode	A postal code.
postalAddress	A postal address.
physicalDeliveryOfficeName	The name of the city, town, or village in which the office is located.
st (stateOrProvinceName)	The name of the state or province in which the entry is located.
l (localityName)	A related country, city, or other geographical area.
description	The description of the entry.

A.1.10 [P]

person

Definition

Define a person. This object class is defined in RFC2256.

OID

2.5.6.6

Base Class

top

Type

STRUCTURAL

Required Attributes

cn (commonName)	A common name or full name.
sn (surname)	A family name or last name.

Optional Attributes

userPassword	A user password.
telephoneNumber	A telephone number.
seeAlso	The DN information related to this entry.
description	The description of the entry.

pilotOrganization

Definition

Define a pilot Organization.

OID

0.9.2342.19200300.100.4.20

Base Class

organization organizationalUnit

Type

STRUCTURAL

Optional Attributes

buildingName	The name of a building.

pilotPerson (newPilotPerson)

Definition

Define a pilot Person.

OID

0.9.2342.19200300.100.4.4

Base Class

person

Type

STRUCTURAL

Optional Attributes

uid (userid)	A user ID.
textEncodedORAddress	A text-encoded originator/recipient (X.400) address.
mail (rfc822Mailbox)	An email address.
drink (favouriteDrink)	A favorite drink.
roomNumber	The room number of the object.
userClass	The category of computer user.
homePhone (homeTelephoneNumber)	A home telephone number.
homePostalAddress	A home address.
secretary	A secretary or assistant.
personalTitle	A personal title.
businessCategory	The type of business in which the entry is engaged.
janetMailbox	An email address that can be used by a U.K. user
otherMailbox	The value of an email box type other than X.400 and RFC822.
mobile (mobileTelephoneNumber)	A mobile telephone number.
pager (pagerTelephoneNumber)	A pager number.
organizationalStatus	A category by which the user is often referred to in an organization.
mailPreferenceOption	Environment information indicating whether the user name should be included on a mailing list.

pkiCA

Definition

Define PKICA information. This object class is defined in RFC2587.

OID

2.5.6.22

Base Class

top

Type

AUXILIARY

Optional Attributes

authorityRevocationList	A list of revoked certificate authorities.
certificateRevocationList	A list of revoked user certificates.
cACertificate	A CA certificate.
crossCertificatePair	A cross certificate.

pkiUser

Definition

Define PKI user information. This object class is defined in RFC2587.

OID

2.5.6.21

Base Class

top

Type

AUXILIARY

Optional Attributes

userCertificate	A user certificate.

A.1.11 [R]

residentialPerson

Definition

Define a person's residential information. This object class is defined in RFC2256.

OID

2.5.6.10

Base Class

person

Type

STRUCTURAL

Required Attributes

l (localityName)	A related country, city, or other geographical area.

Optional Attributes

businessCategory	The type of business in which the entry is engaged.
x121Address	The x121 address of the user.
registeredAddress	A registered emergency contact address.
destinationIndicator	The address information required to provide the telegram service.
telexNumber	A telex number.
telephoneNumber	A telephone number.

internationaliSDNNumber	A related country, city, or other geographical area.
facsimileTelephoneNumber (fax)	A FAX number.
street (streetAddress)	The building name and street number of the entry.
postOfficeBox	A post-office box.
postalCode	A postal code.
postalAddress	A postal address.
physicalDeliveryOfficeName	The name of the city, town, or village in which the office is located.
st (stateOrProvinceName)	The name of the state or province in which the entry is located.

RFC822localPart

Definition

Define an entry that specifies the local part of an RFC822 email address. This object class is defined in RFC2256.

OID

0.9.2342.19200300.100.4.14

Base Class

domain

Type

STRUCTURAL

Optional Attributes

cn (commonName)	A common name or full name.
sn (surname)	A family name or last name.
description	The description of the entry.
seeAlso	The DN information related to this entry.
physicalDeliveryOfficeName	The name of the city, town, or village in which the office is located.
postalAddress	A postal address.
postalCode	A postal code.
postOfficeBox	A post-office box.
street (streetAddress)	The building name and street number of the entry.
facsimileTelephoneNumber (fax)	A FAX number.
telephoneNumber	A telephone number.
internationaliSDNNumber	A related country, city, or other geographical area.
telexNumber	A telex number.
destinationIndicator	The address information required to provide the telegram service.
registeredAddress	A registered emergency contact address.
x121Address	The x121 address of the user.

room

Definition

Define a room.

OID

0.9.2342.19200300.100.4.7

Base Class

top

Type

STRUCTURAL

Required Attributes

cn (commonName)	A common name or full name.

Optional Attributes

roomNumber	The room number of the object.
description	The description of the entry.
seeAlso	The DN information related to this entry.
telephoneNumber	A telephone number.

A.1.12 [S]

simpleSecurityObject

Definition

Define simple security. This is used if the main object class does not have the attribute 'userPassword'. This object class is defined in RFC2256.

OID

0.9.2342.19200300.100.4.19

Base Class

top

Type

AUXILIARY

Required Attributes

userPassword	A related country, city, or other geographical area.

ssoResource

Definition

Define the resource information for SSO.

OID

1.2.392.200001.65.1.8.6.4

Base Class

top

Type

STRUCTURAL

Required Attributes

cn (commonName)	A common name or full name.

Optional Attributes

ssoRoleName	The role to which the user belongs or a role that can access a resource, etc.

ssoSessionInfo	Internal information required for managing sessions.
ssoUserAttribute	An attribute name to be notified to a Web application.

ssoRole

Definition

Define role information for SSO.

OID

1.2.392.200001.65.1.8.6.1

Base Class

top

Type

STRUCTURAL

Required Attributes

cn (commonName)	A common name or full name.

Optional Attributes

ssoAuthType	An authentication type necessary to give the user or the role.
ssoSessionInfo	Internal information required for managing sessions.

ssoRoleSet

Definition

Define a set of roles for SSO.

OID

1.2.392.200001.65.1.8.6.2

Base Class

top

Type

STRUCTURAL

Required Attributes

cn (commonName)	A common name or full name.

Optional Attributes

ssoRoleName	The role to which the user belongs or a role that can access a resource, etc.
ssoSessionInfo	Internal information required for managing sessions.

ssoSite

Definition

Define the site information for SSO.

OID

1.2.392.200001.65.1.8.6.3

Base Class

top

Type

AUXILIARY

Optional Attributes

ssoPortNumber	A port number.
ssoSessionInfo	Internal information required for managing sessions.

ssoUser

Definition

Define the user information for SSO.

OID

1.2.392.200001.65.1.8.6.0

Base Class

top

Type

AUXILIARY

Optional Attributes

ssoRoleName	The role to which the user belongs or a role that can access a resource, etc.
ssoAuthType	An authentication type necessary to give the user or the role.
ssoCredentialTTL	The validity period of a credential.
ssoUserStatus	Used to manage the user's lock status.
ssoNotBefore	The date and time at which the user becomes valid.
ssoNotAfter	The date and time at which the user becomes invalid.
ssoFailureCount	The maximum number of password authentication retries before the system is locked.
ssoLockTimeStamp	The time at which the system locks because the password authentication failed consecutively more than the specified number of times.
ssoSessionInfo	Internal information required for managing sessions.
dnQualifier	A DN prefix.

strongAuthenticationUser

Definition

Define a strong authentication user. This object class is defined in RFC2256.

OID

2.5.6.15

Base Class

top

Type

AUXILIARY

Required Attributes

userCertificate	A user certificate.

A.1.13 [T]

top

Definition

Used as a base class for all the objects.

OID

2.5.6.0

Type

ABSTRACT

Optional Attributes

objectClass	An object.

A.1.14 [U]

uidObject

Definition

Define a UID object. This object class is defined in RFC2377.

OID

1.3.6.1.1.3.1

Base Class

top

Type

AUXILIARY

Required Attributes

uid (userid)	A user ID.

userSecurityInformation

Definition

Define user security information. This object class is defined in RFC2256.

OID

2.5.6.18

Base Class

top

Type

AUXILIARY

Optional Attributes

supportedAlgorithms	The name of a supported algorithm.

Appendix B Interstage Directory Service Attributes

This appendix describes the attributes that can be used in Interstage Directory Service.

The names in brackets are attribute aliases, and when the repository returns a result, it returns the attribute name, not the alias. If more than one name has been defined for the attribute name in schema extension, it returns the name that was defined first.

For the meanings of matching rules and attribute syntax, refer to "Matching Rules" and "Attribute Syntax" in "Attribute Definitions" under "Design the Data Structure (schema)" of the 'Environment Setup' chapter.

The matching rule is used for search and comparison. Comparison and search can only be carried out on attributes for which matching rules are described.

[A]

aRecord

associatedDomain

associatedName

audio

authorityRevocationList

[B]

buildingName

businessCategory

[C]

c (countryName)

cACertificate

carLicense

certificateRevocationList

cn (commonName)

cNAMERecord

co (friendlyCountryName)

corbaIor

corbaRepositoryId

crossCertificatePair

[D]

dc (domainComponent)

deltaRevocationList

departmentNumber

description

destinationIndicator

displayName

distinguishedName

dmdName

dnQualifier

documentAuthor

documentIdentifier

B.1 List of Attributes

B.1.1 [A]

aRecord

Definition

Set an Address DNS resource.

OID

0.9.2342.19200300.100.1.26

Matching Rules

Equality: caseIgnoreIA5Match

Attribute Syntax

IA5 String

associatedDomain

Definition

Set a DNS domain related to a DIT object. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.37

Matching Rules

Equality: caseIgnoreIA5Match

Substr: caseIgnoreIA5SubstringsMatch

Attribute Syntax

IA5 String

associatedName

Definition

Set an entry in the organizational DIT entry related to a DNS domain. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.38

Matching Rules

Equality: distinguishedNameMatch

Attribute Syntax

DN

audio

If this attribute is registered, ";binary" does not need to be added.

Definition

Set a sound file.

OID

0.9.2342.19200300.100.1.55

Attribute Syntax

Audio,binary

Maximum Length

250000

authorityRevocationList

If this attribute is registered, ";binary" needs to be added.

Definition

Set a list of revoked certificate authorities. This attribute is defined in RFC2256.

OID

2.5.4.38

Attribute Syntax

Certificate List

B.1.2 [B]

buildingName

Definition

Set the name of a building. This attribute is defined in RFC3112.

OID

0.9.2342.19200300.100.1.48

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

businessCategory

Definition

Set the type of business in which the entry is engaged. This attribute is defined in RFC2256.

OID

2.5.4.15

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

128

B.1.3 [C]

c (countryName)

Definition

Set a two-character code defined by ISO to indicate a country name in the directory. This attribute is defined in RFC2256.

For example, set the two-character code for Japan as follows:

countryName: jp or c: jp

OID

2.5.4.6

Attribute Syntax

single-valued

Base Attribute

name

cACertificate

If this attribute is registered, ";binary" needs to be added.

Definition

Set a CA certificate. This attribute is defined in RFC2256.

OID

2.5.4.37

Attribute Syntax

Certificate, binary

carLicense

Definition

Set an automobile license plate number. This attribute is defined in RFC2798.

OID

2.16.840.1.113730.3.1.1

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

certificateRevocationList

If this attribute is registered, ";binary" needs to be added.

Definition

Set a list of revoked user certificates. This attribute is defined in RFC2256.

OID

2.5.4.39

Attribute Syntax

Certificate List, binary

cn (commonName)

Definition

Set a common name or full name. This attribute is defined in RFC2256.

OID

2.5.4.3

Base Attribute

name

cNAMERecord

Definition

Set the proper name of a DNS resource. This attribute is defined in RFC2256.

OID

0.9.2342.19200300.100.1.31

Matching Rules

Equality: caseIgnoreIA5Match

Attribute Syntax

IA5 String

co (friendlyCountryName)

Definition

The country attribute is used to show the two-character country code and "friendlyCountryName" attribute.

OID

0.9.2342.19200300.100.1.43

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

corbaIor

Definition

Set a character string representation for an IOR of a CORBA object.

OID

1.3.6.1.4.1.42.2.27.4.1.14

Matching Rules

Equality: caseIgnoreIA5Match

Attribute Syntax

IA5 String, single-valued

corbaRepositoryId

Definition

Set a repository ID implemented by a CORBA object.

OID

1.3.6.1.4.1.42.2.27.4.1.15

Matching Rules

Equality: caseExactMatch

Attribute Syntax

Directory String

crossCertificatePair

If this attribute is registered, ";binary" needs to be added.

Definition

Set a cross certificate. This attribute is defined in RFC2256.

OID

2.5.4.40

Attribute Syntax

Certificate Pair

B.1.4 [D]

dc (domainComponent)

Definition

Set a DNS domain. This attribute is defined in RFC1274/2247.

OID

0.9.2342.19200300.100.1.25

Matching Rules

Equality: caseIgnoreIA5Match

Substr: caseIgnoreIA5SubstringsMatch

Attribute Syntax

IA5 String, single-valued

deltaRevocationList

If this attribute is registered, ";binary" needs to be added.

Definition

Set a list of revoked deltas. This attribute is defined in RFC2256.

OID

2.5.4.53

Attribute Syntax

Certificate List, binary

departmentNumber

Definition

Set a department number. This attribute is defined in RFC2798.

OID

2.16.840.1.113730.3.1.2

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

description

Definition

Set the description of the entry. This attribute is defined in RFC2256.

OID

2.5.4.13

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

1024

destinationIndicator

Definition

Set the address information required for the telegram service. This attribute is defined in RFC2256.

OID

2.5.4.27

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Printable String

Maximum Length

128

displayName

Definition

Set the display name of the entry. This attribute is defined in RFC2798.

OID

2.16.840.1.113730.3.1.241

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String, single-valued

distinguishedName

Definition

Sets the DN (distinguished name identifier) for the entry.

An example is shown below.

Example:dn: cn=User001,o=User,ou=interstage,o=fujitsu,dc=com

OID

1.3.6.1.4.1.1466.115.121.1.12

Matching Rules

Equality: distinguishedNameMatch

Attribute Syntax

DN

dmdName

Definition

Set the administration permission required to operate a directory management domain (DMD) and a directory server. This attribute is defined in RFC2256.

OID

2.5.4.54

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Base Attribute

name

dnQualifier

Definition

Set a DN prefix. This attribute is defined in RFC2256.

OID

2.5.4.46

Matching Rules

Equality: caseIgnoreMatch

Ordering: caseIgnoreOrderingMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Printable String

documentAuthor

Definition

Set the DN (distinguished name) of the document author. This attribute is defined in RFC1274.

As the attribute value, set the DN of the document author. The following is an example.

Example: documentAuthor: cn=Taro Fujitsu, o=User,ou=interstage,o=fujitsu,dc=com

OID

0.9.2342.19200300.100.1.14

Matching Rules

Equality: distinguishedNameMatch

Attribute Syntax

DN

documentIdentifier

Definition

Set the unique identifier of a document. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.11

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

documentLocation

Definition

Set the location of the original copy of a document. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.15

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

documentPublisher

Definition

Set the user or organization that published the document. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.56

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

documentTitle

Definition

Set the title of the document. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.12

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

documentVersion

Definition

Set the version of the document. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.13

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

drink (favouriteDrink)

Definition

Set a favorite drink. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.5

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

B.1.5 [E]

employeeNumber

Definition

Set an employee number. This attribute is defined in RFC2798.

OID

2.16.840.1.113730.3.1.3

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String, single-valued

Maximum Length

256

employeeType

Definition

Set an employment type. This attribute is defined in RFC2798.

OID

2.16.840.1.113730.3.1.4

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

B.1.6 [F]

facsimileTelephoneNumber(fax)

Definition

Set a FAX number. This attribute is defined in RFC2256.

OID

2.5.4.23

Attribute Syntax

Facsimile Telephone Number

B.1.7 [G]

givenName(gn)

Definition

Set a given name or first name. This attribute is defined in RFC2256.

OID

2.5.4.42

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Base Attribute

name

B.1.8 [H]

homePhone(homeTelephoneNumber)

Definition

Set a home telephone number. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.20

Matching Rules

Equality: telephoneNumberMatch

Substr: telephoneNumberSubstringsMatch

Attribute Syntax

Telephone Number

homePostalAddress

Definition

Set a home address. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.39

Matching Rules

Equality: caseIgnoreListMatch

Substr: caseIgnoreListSubstringsMatch

Attribute Syntax

Postal Address

host

Definition

Set the host name of the computer. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.9

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

B.1.9 [I]

initials

Definition

Set initials. This attribute is defined in RFC2256.

OID

2.5.4.43

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Base Attribute

name

internationaliSDNNumber

Definition

Set an international ISDN number. This attribute is defined in RFC2256.

OID

2.5.4.25

Matching Rules

Equality: numericStringMatch

Substr: numericStringSubstringsMatch

Attribute Syntax

Numeric String

Maximum Length

36

B.1.10 [J]

janetMailbox

Definition

Set an email address that can be used by a U.K. user. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.46

Matching Rules

Equality: caseIgnoreIA5Match

Substr: caseIgnoreIA5SubstringsMatch

Attribute Syntax

IA5 String

Maximum Length

256

javaClassName

Definition

Set a Java class name or interface name.

OID

1.3.6.1.4.1.42.2.27.4.1.6

Matching Rules

Equality: caseExactMatch

Attribute Syntax

Directory String, single-valued

javaClassNames

Definition

Set the class name of an object factory that can be used to create an instance of an object identified using the JavaClassName attribute.

OID

1.3.6.1.4.1.42.2.27.4.1.13

Matching Rules

Equality: caseExactMatch

Attribute Syntax

Directory String

javaCodebase

Definition

Set the URL specifying the location of a class definition.

OID

1.3.6.1.4.1.42.2.27.4.1.7

Matching Rules

Equality: caseExactIA5Match

Attribute Syntax

IA5 String

javaDoc

Definition

Specify the JAVA document of a class.

OID

1.3.6.1.4.1.42.2.27.4.1.12

Matching Rules

Equality: caseExactIA5Match

Attribute Syntax

Directory String

javaFactory

Definition

Set the location used to load an object factory identified using the javaFactory attribute.

OID

1.3.6.1.4.1.42.2.27.4.1.10

Matching Rules

Equality: caseExactMatch

Attribute Syntax

Directory String, single-valued

javaReferenceAddress

Definition

Set the sequence of a JNDI reference address.

OID

1.3.6.1.4.1.42.2.27.4.1.11

Matching Rules

Equality: caseExactMatch

Attribute Syntax

Directory String

javaSerializedData

Definition

Set Java serialized data.

OID

1.3.6.1.4.1.42.2.27.4.1.8

Attribute Syntax

Octet String, single-valued

jpegPhoto

If this attribute is registered, ";binary" does not need to be added.

Definition

Set a JPEG photo. This attribute is defined in RFC2798.

OID

0.9.2342.19200300.100.1.60

Attribute Syntax

JPEG

B.1.11 [K]

knowledgeInformation

Definition

Set knowledge information. This attribute is defined in RFC2256.

OID

2.5.4.2

Matching Rules

Equality: caseIgnoreMatch

Attribute Syntax

Directory String

Maximum Length

32768

B.1.12 [L]

l (localityName)

Definition

Set a related country, city, or other geographical area. This attribute is defined in RFC2256.

OID

2.5.4.7

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Base Attribute

name

labeledURI

Definition

Set a Uniform Resource Identifier (URI). This attribute is defined in RFC2079.

OID

1.3.6.1.4.1.250.1.57

Matching Rules

Equality: caseExactMatch

Attribute Syntax

Directory String

B.1.13 [M]

mail (rfc822Mailbox)

Definition

Set an email address. This attribute is defined in RFC2252.

OID

0.9.2342.19200300.100.1.3

Matching Rules

Equality: caseIgnoreIA5Match

Substr: caseIgnoreIA5SubstringsMatch

Attribute Syntax

IA5 String

Maximum Length

256

mailPreferenceOption

Definition

Set environment information indicating whether the user should be included on a mailing list. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.47

Attribute Syntax

INTEGER

manager

Definition

Set the distinguished name (DN) of a manager. This attribute is defined in RFC1274.

As the attribute value, set the DN of a manager. The following is an example.

Example: manager: cn=user001, o=User,ou=interstage,o=fujitsu,dc=com

OID

0.9.2342.19200300.100.1.10

Matching Rules

Equality: distinguishedNameMatch

Attribute Syntax

DN

mDRecord

Definition

Set the MD record. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.27

Matching Rules

Equality: caseIgnoreIA5Match

Attribute Syntax

IA5 String

member

Definition

Set the DN (distinguished name) of each member of a group. This attribute is defined in RFC2256.

As the attribute value, set the DN of a member to be included in a group. The following is an example.

Example: To include as a group member cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com, enter:

member: cn=user001,ou=User,ou=interstage,o=fujitsu,dc=com

OID

2.5.4.31

Matching Rules

Equality: caseIgnoreMatch

Base Attribute

distinguishedName

mobile(mobileTelephoneNumber)

Definition

Set a mobile telephone number. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.41

Matching Rules

Equality: telephoneNumberMatch

Substr: telephoneNumberSubstringsMatch

Attribute Syntax

Telephone Number

mXRecord

Definition

Set a Mail Exchange DNS resource.

OID

0.9.2342.19200300.100.1.28

Matching Rules

Equality: caseIgnoreIA5Match

Attribute Syntax

IA5 String

B.1.14 [N]

name

Definition

This attribute is used as a supertype for attributes used for naming. The attribute itself cannot be used as a value in an entry.

OID

2.5.4.41

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

32768

nSRecord

Definition

Set a Name Server DNS resource.

OID

0.9.2342.19200300.100.1.29

Matching Rules

Equality: caseIgnoreIA5Match

Attribute Syntax

IA5 String

B.1.15 [O]

o(organizationName)

Definition

Set an organization name. This attribute is defined in RFC2256.

OID

2.5.4.10

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Base Attribute

name

objectClass

Definition

Set an object class. This attribute is defined in RFC2256.

OID

2.5.4.0

Matching Rules

Equality: objectIdentifierMatch

Maximum Length

256

organizationalStatus

Definition

Set the category by which the user is typically referred to in an organization. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.45

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

otherMailbox

Definition

Set the value of an email box type other than X.400 and rfc822. This attribute is defined in RFC1274.

As the attribute value, set the value of an email box type. The following is an example.

Example: otherMailbox: internet $ user001@interstage.fujitsu.com

OID

0.9.2342.19200300.100.1.22

Attribute Syntax

Other Mailbox

ou(organizationalUnitName)

Definition

Set an organization unit name. This attribute is defined in RFC2256.

OID

2.5.4.11

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Base Attribute

name

owner

Definition

Set the DN (distinguished name) of a responsible person. This attribute is defined in RFC2256.

As the attribute value, set the distinguished name of a responsible person. The following is an example.

Example: owner: cn=user001, o=User,ou=interstage,o=fujitsu,dc=com

OID

2.5.4.32

Matching Rules

Equality: caseIgnoreMatch

Base Attribute

distinguishedName

B.1.16 [P]

pager(pagerTelephoneNumber)

Definition

Set a pager number. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.42

Matching Rules

Equality: telephoneNumberMatch

Substr: telephoneNumberSubstringsMatch

Attribute Syntax

Telephone Number

personalTitle

Definition

Set a personal title. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.40

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

physicalDeliveryOfficeName

Definition

Set the name of the city, town, or village in which the office is located. This attribute is defined in RFC2256.

OID

2.5.4.19

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

128

postalAddress

Definition

Set a postal address. This attribute is defined in RFC2256.

OID

2.5.4.16

Matching Rules

Equality: caseIgnoreListMatch

Substr: caseIgnoreListSubstringsMatch

Attribute Syntax

Postal Address

postalCode

Definition

Set a postal code. This attribute is defined in RFC2256.

OID

2.5.4.17

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

40

postOfficeBox

Definition

Set a post-office box. This attribute is defined in RFC2256.

OID

2.5.4.18

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

40

preferredLanguage

Definition

Set a desired language. This attribute is defined in RFC2798.

OID

2.16.840.1.113730.3.1.39

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String, single-valued

B.1.17 [R]

registeredAddress

Definition

Set a registered emergency contact address. This attribute is defined in RFC2256.

OID

2.5.4.26

Matching Rules

Equality: caseIgnoreListMatch

Substr: caseIgnoreListSubstringsMatch

Attribute Syntax

Postal Address

Base Attribute

postalAddress

roleOccupant

Definition

Set the DN (distinguished name) of the user acting in the role defined in the organizationalRole entry. This attribute is defined in RFC2256.

As the attribute value, set the DN of a user. The following is an example.

Example: roleOccupant: cn=user001, o=User,ou=interstage,o=fujitsu,dc=com

OID

2.5.4.33

Matching Rules

Equality: caseIgnoreMatch

Base Attribute

distinguishedName

roomNumber

Definition

Set the room number of an object. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.6

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

B.1.18 [S]

secretary

Definition

Set the DN (distinguished name) of a secretary or assistant. This attribute is defined in RFC1274.

As the attribute value, set the DN of a secretary or assistant. The following is an example.

Example: secretary: cn=user001, o=User,ou=interstage,o=fujitsu,dc=com

OID

0.9.2342.19200300.100.1.21

Matching Rules

Equality: distinguishedNameMatch

Attribute Syntax

DN

seeAlso

Definition

Set the DN information related to this entry. This attribute is defined in RFC2256.

As the attribute value, set the DN information. The following is an example.

Example: seeAlso: cn=user001, o=User,ou=interstage,o=fujitsu,dc=com

OID

2.5.4.34

Matching Rules

Equality: caseIgnoreMatch

Base Attribute

distinguishedName

serialNumber

Definition

Set a serial number. This attribute is defined in RFC2256.

OID

2.5.4.5

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Printable String

Maximum Length

64

sn(surname)

Definition

Set a family name or last name. This attribute is defined in RFC2256.

OID

2.5.4.4

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Base Attribute

name

sOARecord

Definition

Specifies a type SOA (Start of Authority) DNS resource record.

OID

0.9.2342.19200300.100.1.30

Matching Rules

Equality: caseIgnoreIA5Match

Attribute Syntax

IA5 String

ssoAuthType

Definition

It specifies an authentication type required for the user or the role.

OID

1.2.392.200001.65.1.8.4.1

Matching Rules

Equality: caseIgnoreIA5Match

Attribute Syntax

IA5 String, single-valued

Maximum Length

256

ssoCredentialTTL

Definition

Set the validity period of a credential.

OID

1.2.392.200001.65.1.8.4.2

Matching Rules

Equality: integerMatch

Attribute Syntax

INTEGER, single-valued

Maximum Length

8

ssoFailureCount

Definition

Set a number of times the password authentication can fail.

OID

1.2.392.200001.65.1.8.4.8

Matching Rules

Equality: integerMatch

Attribute Syntax

INTEGER, single-valued

Maximum Length

8

ssoLockTimeStamp

Definition

Set the time at which the system locks because the password authentication failed successively more than the permitted number of times.

OID

1.2.392.200001.65.1.8.4.9

Matching Rules

Equality: generalizedTimeMatch

Ordering: generalizedTimeOrderingMatch

Attribute Syntax

Generalized Time, single-valued

Maximum Length

64

ssoNotAfter

Definition

Set the date and time at which the user becomes invalid.

OID

1.2.392.200001.65.1.8.4.5

Matching Rules

Equality: generalizedTimeMatch

Ordering: generalizedTimeOrderingMatch

Attribute Syntax

Generalized Time, single-valued

Maximum Length

64

ssoNotBefore

Definition

Set the date and time at which the user becomes valid.

OID

1.2.392.200001.65.1.8.4.4

Matching Rules

Equality: generalizedTimeMatch

Ordering: generalizedTimeOrderingMatch

Attribute Syntax

Generalized Time, single-valued

Maximum Length

64

ssoPortNumber

Definition

Set a port number.

OID

1.2.392.200001.65.1.8.4.6

Matching Rules

Equality: integerMatch

Attribute Syntax

INTEGER, single-valued

Maximum Length

8

ssoRoleName

Definition

Set a role to which the user belongs or a role that can access a resource, etc.

OID

1.2.392.200001.65.1.8.4.0

Matching Rules

Equality: caseIgnoreMatch

Attribute Syntax

Directory String

Maximum Length

32

ssoSessionInfo

Definition

The Interstage Single Sign-on Repository server sets this value.

OID

1.2.392.200001.65.1.8.4.10

Matching Rules

(Equivalence) caseIgnoreMatch

Attribute Syntax

Directory String

Maximum Length

1024

ssoUserAttribute

Definition

Set an attribute name to be notified to a Web application.

OID

1.2.392.200001.65.1.8.4.7

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

ssoUserStatus

Definition

Set the user's lock status. The Interstage Single Sign-on Repository server sets this value.

OID

1.2.392.200001.65.1.8.4.3

Matching Rules

Equality: caseIgnoreIA5Match

Attribute Syntax

IA5 String, single-valued

Maximum Length

256

st(stateOrProvinceName)

Definition

Set the name of the state or province in which the entry is located. This attribute is defined in RFC2256.

OID

2.5.4.8

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Base Attribute

name

street(streetAddress)

Definition

Set the building name and block number of the entry. This attribute is defined in RFC2256.

OID

2.5.4.9

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

128

supportedAlgorithms

If this attribute is registered, ";binary" needs to be added.

Definition

Set the name of a supported algorithm. This attribute is defined in RFC2256.

OID

2.5.4.52

Attribute Syntax

Supported Algorithm

B.1.19 [T]

telephoneNumber

Definition

Set a telephone number. This attribute is defined in RFC2256.

OID

2.5.4.20

Matching Rules

Equality: telephoneNumberMatch

Substr: telephoneNumberSubstringsMatch

Attribute Syntax

Telephone Number

Maximum Length

32

telexNumber

Definition

Set a telex number. The telex number can be in the following format:

actual-number "$" country "$" answerback
In the above format, "actual-number" is the syntactic representation of the number portion of the telex number to be encoded, "country" the telex country code, and "answerback" is the answerback code of the telex terminal. This attribute is defined in RFC2256.

OID

2.5.4.21

Attribute Syntax

Telex Number

textEncodedORAddress

Definition

Set a text-encoded originator/recipient (X.400) address.

OID

0.9.2342.19200300.100.1.2

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

title

Definition

Set a title. This attribute is defined in RFC2256.

OID

2.5.4.12

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Base Attribute

name

B.1.20 [U]

uid (userid)

Definition

Set a user ID. This attribute is defined in RFC1274.

OID

0.9.2342.19200300.100.1.1

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

uniqueMember

Definition

Set a group of names related to an entry where each name was given a uniqueIdentifier to ensure its uniqueness. This attribute is defined in RFC2256.

OID

2.5.4.50

Matching Rules

Equality: uniqueMemberMatch

Attribute Syntax

Name and Optional UID

userCertificate

If this attribute is registered, ";binary" needs to be added.

Definition

Set a user certificate. This attribute is defined in RFC2256.

OID

2.5.4.36

Attribute Syntax

Certificate, binary

userClass

Definition

Set the computer user category. This attribute is defined in RFC1274.

OID

2.5.4.36

Matching Rules

Equality: caseIgnoreMatch

Substr: caseIgnoreSubstringsMatch

Attribute Syntax

Directory String

Maximum Length

256

userPassword

Definition

Set a user password. This attribute is defined in RFC2256/2307.

OID

2.5.4.35

Matching Rules

Equality: octetStringMatch

Attribute Syntax

Octet String

Maximum Length

128

userPKCS12

If this attribute is registered, ";binary" does not need to be added.

Definition

Set user PKCS#12. This attribute is defined in RFC2798.

OID

2.16.840.1.113730.3.1.216

Attribute Syntax

Binary

userSMIMECertificate

If this attribute is registered, ";binary" does not need to be added.

Definition

Set an S/MINE certificate. This attribute is defined in RFC2798.

OID

2.16.840.1.113730.3.1.40

Attribute Syntax

Binary

B.1.21 [X]

x121Address

Definition

Set a user X.121 address. This attribute is defined in RFC2256.

OID

2.5.4.24

Matching Rules

Equality: numericStringMatch

Substr: numericStringSubstringsMatch

Attribute Syntax

Numeric String

Maximum Length

15

Appendix C Creating a Load Distribution Environment (Replication Mode)

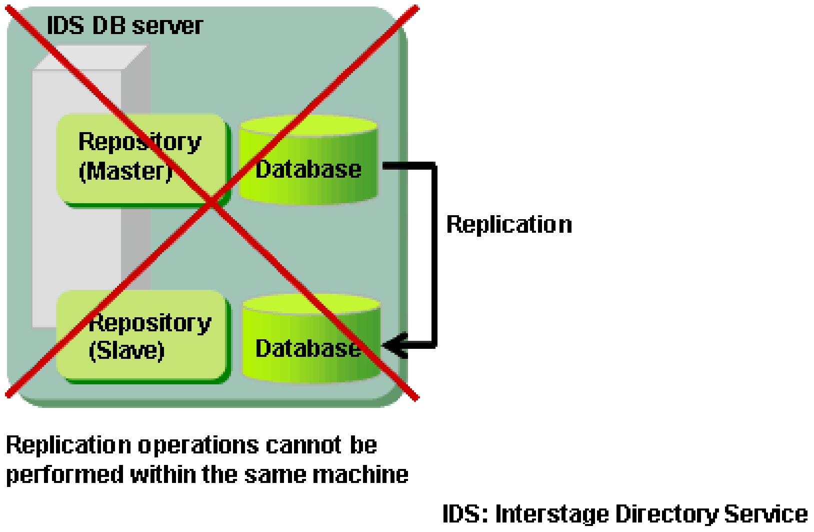
This appendix explains how to create an operation environment for replication mode, depending on which database is used for the repository.

Note the following points that are common to all database types when creating an operation environment for replication mode.

Note

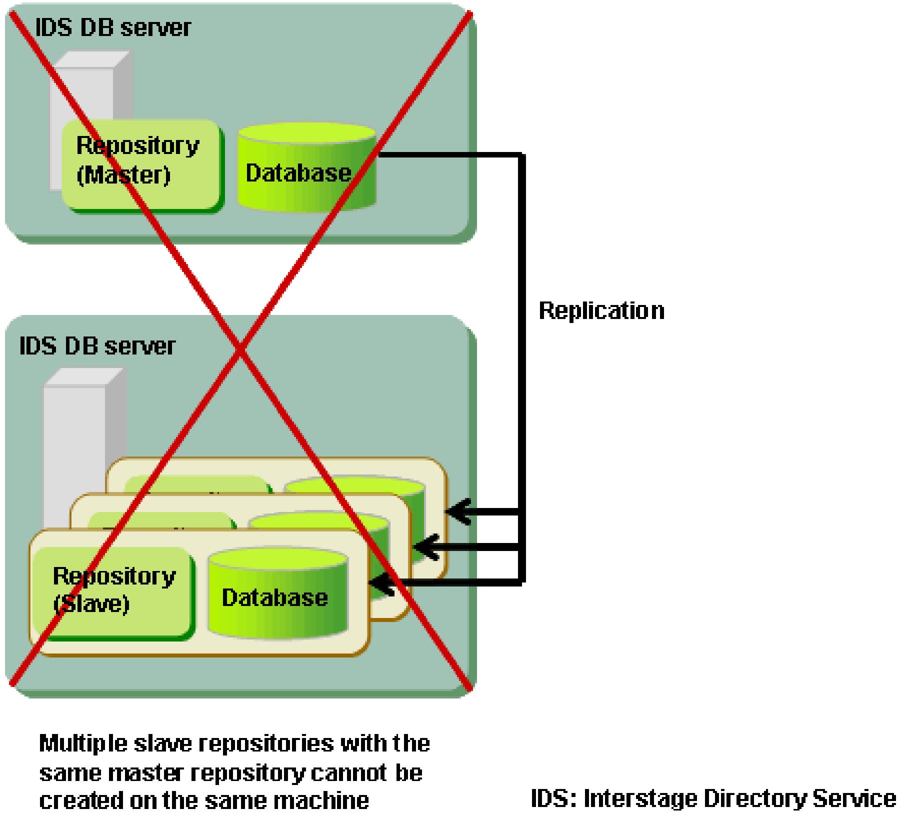
- Replication mode cannot be set up using multiple repositories on the same machine.

Figure C.1 Replication Operations within the Same Machine


IDS DB server
Repository (Master)
Database
Replication
Repository (Slave)
Database
Replication operations cannot be performed within the same machine
IDS: Interstage Directory Service

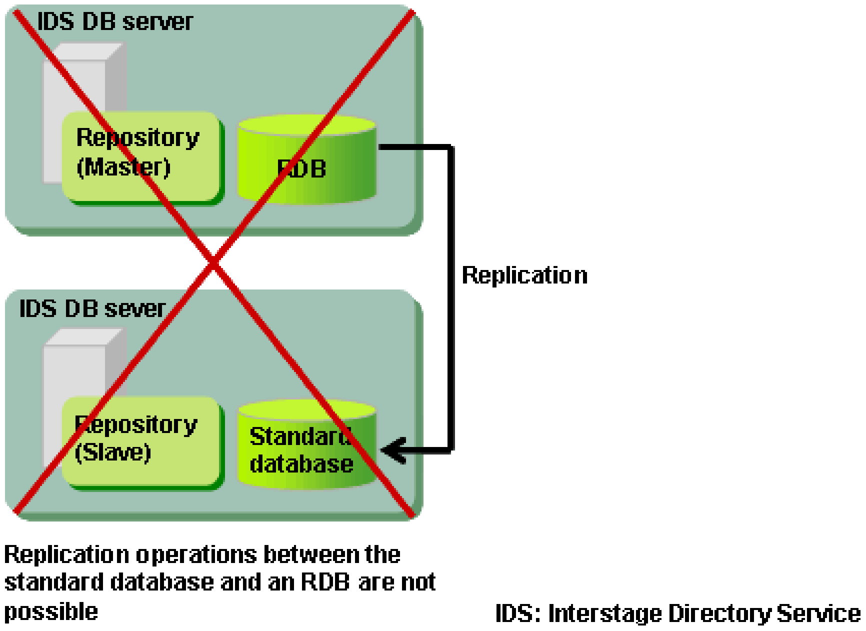
- Set up multiple slave repositories with the same master repository on the same machine is unsupported.

Figure C.2 Creating Multiple Slave Repositories with the Same Master Repository on the Same Machine


IDS DB server
Repository (Master)
Database
Replication
IDS DB server
Repository (Slave)
Database
Multiple slave repositories with the same master repository cannot be created on the same machine
IDS: Interstage Directory Service

- The replication pattern cannot be created if one repository uses the standard database and another repository uses the RDB.

Figure C.3 Replication Operations between the Standard Database and an RDB


IDS DB server
Repository (Master)
RDB
Replication
IDS DB sever
Repository (Slave)
Standard database
Replication operations between the standard database and an RDB are not possible
IDS: Interstage Directory Service

- Configure the master machine and the slave machine with same platform.
- Build master machine and slave machine using the same version.

C.1 Using the Standard Database

This section explains the procedure for creating an operation environment for replication mode where the standard database is used as the database for the repository.

Using a sheet to prevent setting errors while creating a replication environment

A Interstage Directory Service environment setup sheet (Excel file) is available to assist the configuration of the Interstage Management Console during the replication operation setup. This file is stored in "ApplicationServer\tuning" in Manual package. Use this sheet if the standard database is used as the repository database.

If Microsoft(R) Excel 2000 or a later version has been installed, design a replication operation using the file "DS_repli.xls." For details on how to use it, refer to the explanation within that file.

Conditions for Using the Interstage Directory Service Environment Setup Sheet

The Interstage Directory Service environment setup sheet is a file that can be used if Microsoft(R) Excel 2000 or later has been installed.

Since the setup sheet uses macros, before using it, enable the macros by setting the security level of Microsoft(R) Excel. For details on how to set the security level, refer to the Microsoft(R) Excel Help. Consult the security Administrator before changing the security level.

The following procedure describes how to set the security level to use the sheet in Microsoft(R) Excel 2002.

1. Start Microsoft(R) Excel 2002 and select [Macros] and then [Security] from the Tools menu.
2. The Security window will display. Select the radio button [Medium] on the [Security level] tab.
3. Click the [OK] button.
4. Shut down Microsoft(R) Excel and then restart it.
5. Select [Open] from the File menu, browse to the Interstage Directory Service environment setup sheet, and select it.
6. If the Enable Macros dialog box displays, click the [Enable macros] button to enable the macros.
7. Restore the macro security level to its original level as required.

Procedure for Creating Replication Mode

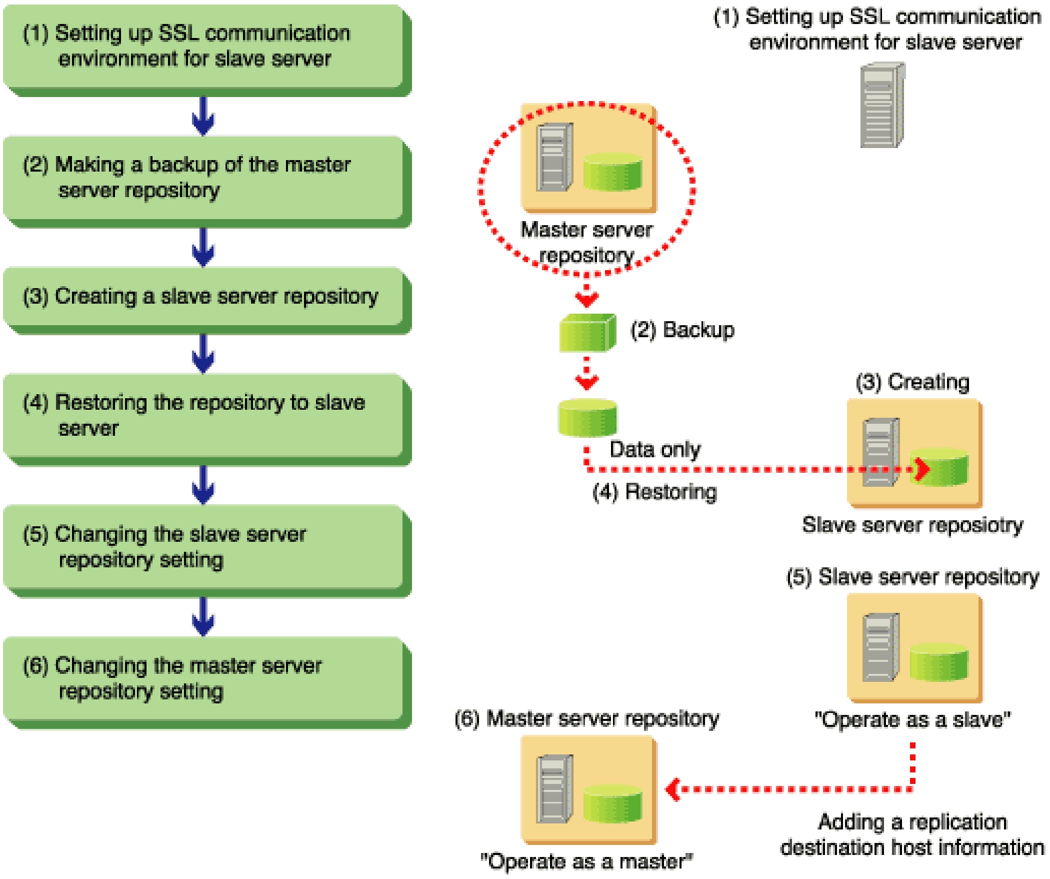
To set up a new system in replication mode, or to change from standalone mode to replication mode, configure a new environment according to the following procedure.

- Changing from standalone operations to replication operations
- Adding a slave server with the replication pattern

If SSL communications are performed between the master server and slave servers during replication mode operations, you will need to create an SSL environment on the master server and set up SSL information for the slave servers that perform SSL communication. In replication mode, SSL communications can be used for either communications between clients and servers or for communications between the master server and slave servers or both.

The following flow diagram illustrates the procedure for setting up a new system in replication mode.

Figure C.4 Creating Replication Mode


(1) Setting up SSL communication environment for slave server
(2) Making a backup of the master server repository
(3) Creating a slave server repository
(4) Restoring the repository to slave server
(5) Changing the slave server repository setting
(6) Changing the master server repository setting
(1) Setting up SSL communication environment for slave server
Master server repository
(2) Backup
Data only
(4) Restoring
(3) Creating
Slave server reposiotry
(5) Slave server repository
"Operate as a slave"
(6) Master server repository
"Operate as a master"
Adding a replication destination host information

The Master server repository is the repository created in the chapter "Environment Setup". If the repository for the master server is not created, create it by referring to the details in the "Environment Setup" chapter.

Note

- Data is reflected in the slave server only after replication connection settings are added to the master server.
- During replication installation, do not add, modify, or delete entries not related to the installation.
- If SSL communications are used for communications between the master server and slave servers, do not change the SSL definitions or their content during replication operations. Continued operation cannot be guaranteed if SSL definitions are changed during replication.

When using a cluster environment for replication operation, refer to the "Environment Setup Procedure for Cluster Service" chapter of the High Availability System Guide.

C.1.1 Setting up an SSL Communication Environment for the Slave Server

To conduct encrypted communication using SSL in replication mode, set up an SSL environment for the master server and configure SSL information on the slave servers that will be communicating with SSL.

Note

Do not specify test certificates in the SSL definitions used by the repository on the slave server.

Configuring an SSL communication environment for the slave servers entails the following steps:

1. Interstage certificate environment setup

2. Implementing settings to use the certificates

For the detailed procedure, refer to the 'Server' procedure described in 'Setting up an SSL Communication Environment'.

C.1.2 Setting up an SSL Communication Environment for the Master Server

If SSL-encrypted communications are used with replication, an SSL environment must be created on the master server and corresponding SSL information must be set up on slave servers that perform SSL communications.

The procedure for creating an SSL communication environment on the master server is shown below.

Performing No Client Authentication

Note

- It is necessary to use the same CA certificate and CRL as those obtained when setting up an SSL communication environment for the slave server.

Set up an SSL communication environment for the master server according to the following procedure:

1. Setup of an Interstage certificate environment ((1) and (2) in the following figure)
    - Create a site certificate for testing.
    - Nickname of the site certificate for testing: testCert
    - Name: repository.fujitsu.com
    - Organization unit name: Interstage
    - Organization name: Fujitsu Ltd.
    - City name: Yokohama
    - Prefectural name: Kanagawa
    - Country code: jp

```
scsmakeenv -n testCert
Password:   (*1)

Input X.500 distinguished names.
What is your first and last name?
[Unknown]:repository.fujitsu.com   (*2)
What is the name of your organizational unit?
[Unknown]:Interstage   (*2)
What is the name of your organization?
[Unknown]:Fujitsu Ltd.   (*2)
What is the name of your City or Locality?
[Unknown]:Yokohama   (*2)
What is the name of your State or Province?
[Unknown]:Kanagawa   (*2)
What is the two-letter country code for this unit?
[Un]:jp   (*2)
Is <CN=SiteName.domain, OU=Interstage, O=Fujitsu Ltd., L=Yokohama,
ST=Kanagawa, C=jp> correct?
[no]:yes   (*3)
SCS: INFO: scs0102: Self-sign certificate was issued
```

*1 Enter the password. The entered string will not be echoed back. If Re-type is displayed, re-enter (re-type) the password for confirmation.

*2 For the content to be entered, refer to the "Reference Manual (Command Edition)."

*3 If the displayed content is correct, enter "yes." To re-try the input, enter "no."

2. Setting to use the certificates ((3) in the following figure)

   Certificates that have been registered in the Interstage certificate environment can be displayed in the following Interstage Management Console windows:

   - [System] > [Security] > [Certificates] > [CA Certificate] window, or
   - [System] > [Security] > [Certificates] > [Site certificate] window

   For the management server, certificates can be displayed in the following windows:

   - [Application Management] > [Interstage Management Console] > [Interstage Application Server] > [Security] > [Certificates] > [CA Certificate] window, or
   - [Application Management] > [Interstage Management Console] > [Interstage Application Server] > [Security] > [Certificates] > [Site certificate] window

   Check whether the content of the acquired certificate is correct.

   To communicate via SSL, SSL definitions must be created. Create SSL definitions using the following windows of the Interstage Management Console:

   - [System] > [Security] > [SSL] > [New] tab

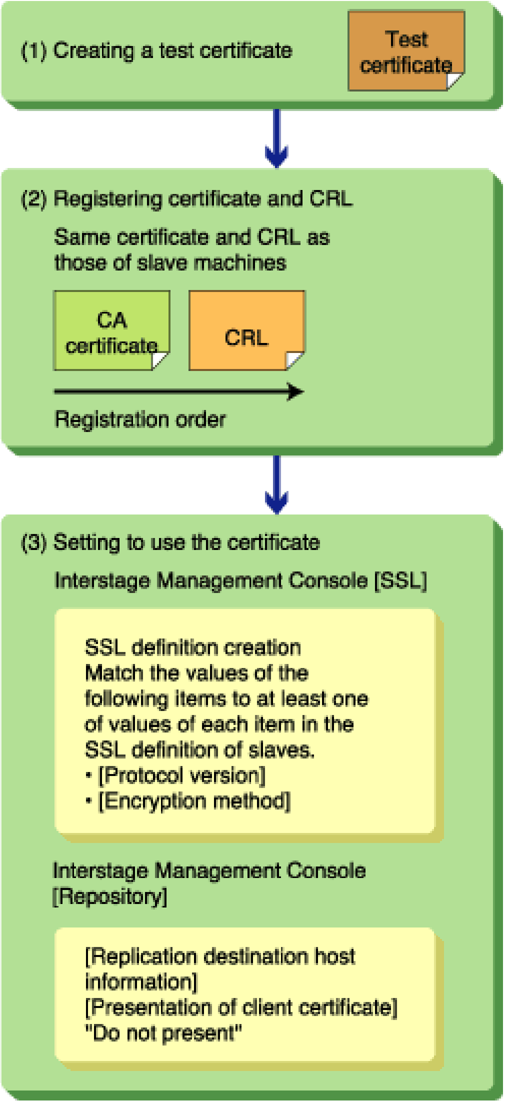
   For the management server, create SSL definitions using the following windows:

   - [Application Management] > [Interstage Management Console] > [Interstage Application Server] > [Security] > [SSL] > [New] tab

   It is necessary for [Protocol version] and [Encryption method] to match at least one definition in the SSL configuration used by the repository of the slave server respectively.

The following flow diagram illustrates the procedure for setting up an SSL communication environment when no client authentication is performed.

Figure C.5 SSL: Communication Environment without Authentication


(1) Creating a test certificate
Test certificate
(2) Registering certificate and CRL
Same certificate and CRL as those of slave machines
CA certificate
CRL
Registration order
(3) Setting to use the certificate
Interstage Management Console [SSL]
SSL definition creation
Match the values of the following items to at least one of values of each item in the SSL definition of slaves.
• [Protocol version]
• [Encryption method]
Interstage Management Console [Repository]
[Replication destination host information]
[Presentation of client certificate] "Do not present"

Performing Client Authentication

Note

- It is necessary to use the same CA certificate and CRL as those obtained when setting up an SSL communication environment for the slave server.
- If the setting of [Client authentication] of [Environment settings] in the SSL configuration used by the repository of the slave server is "Authenticate (Always authenticate a client certificate)," do not specify a certificate for testing in the SSL configuration used for replication.

Set up an SSL communication environment for the master server according to the following procedure:

1. Setup of an Interstage certificate environment ((1) to (5) in the following figure)

   The detailed procedure up to this point is the same as the Server procedure described in "Setting up an SSL Communication Environment".

2. Setting to use the certificate ((6) in the following figure)

   Certificates that have been registered in the Interstage certificate environment can be displayed in the following Interstage Management Console windows:

   - [System] > [Security] > [Certificates] > [CA Certificate] window, or
   - [System] > [Security] > [Certificates] > [Site certificate] window

   For the management server, certificates can be displayed in the following windows:

   - [Application Management] > [Interstage Management Console] > [Interstage Application Server] > [Security] > [Certificates] > [CA Certificate] window, or
   - [Application Management] > [Interstage Management Console] > [Interstage Application Server] > [Security] > [Certificates] > [Site certificate] window

   Check whether the content of the acquired certificate is correct.

   To communicate via SSL, SSL definitions must be created. Create SSL definitions using the following windows of the Interstage Management Console:

   - [System] > [Security] > [SSL] > [New] tab

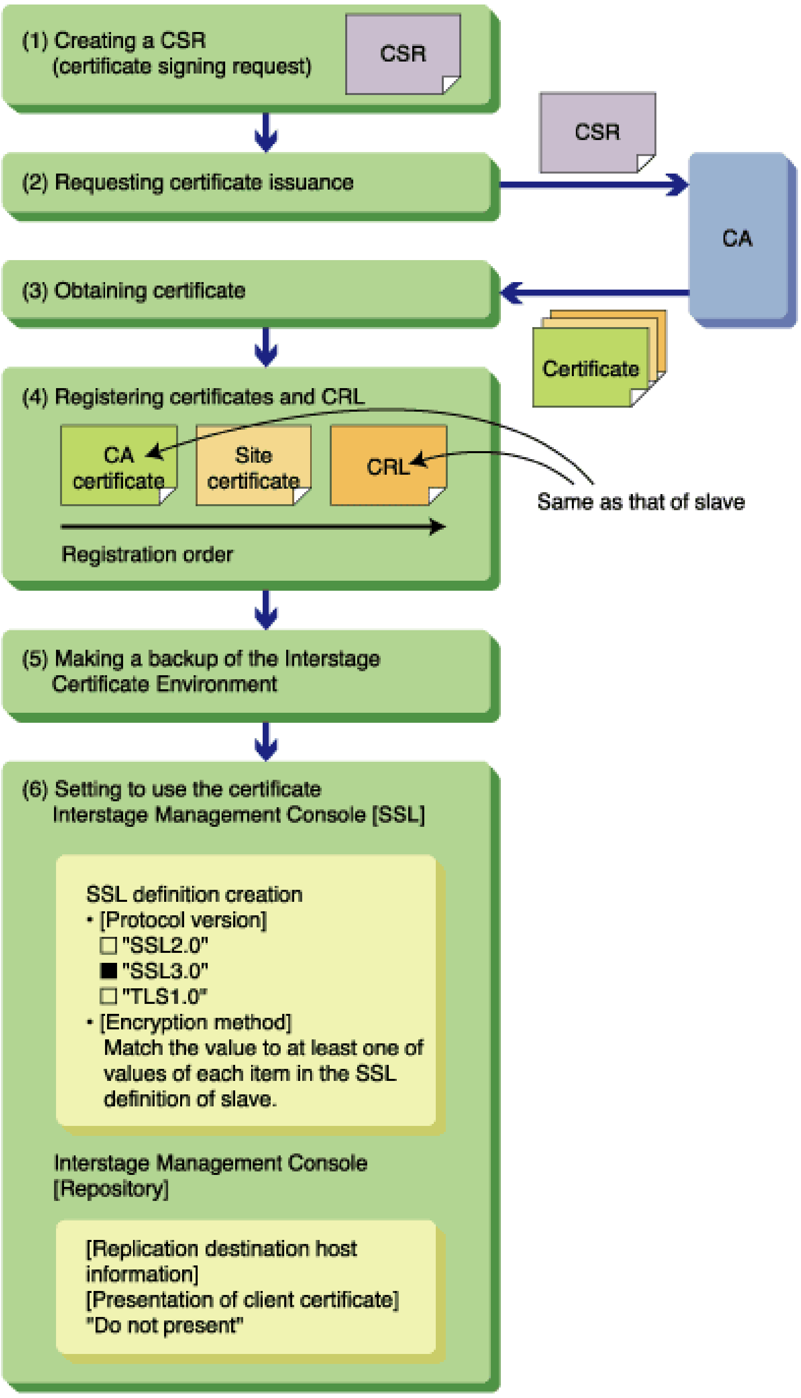
   For the management server, create SSL definitions using the following windows:

   - [Application Management] > [Interstage Management Console] > [Interstage Application Server] > [Security] > [SSL] > [New] tab

   Select both or one of, "SSL3.0" and "TLS 1.0" for [Protocol version]. It is necessary for [Encryption] to match at least one definition in the SSL configuration used by the repository of the slave server.

The following flow diagram illustrates the procedure for setting up an SSL communication environment when client authentication is performed.

Figure C.6 SSL Communication with Client Authentication


(1) Creating a CSR
(certificate signing request)
CSR
CSR
(2) Requesting certificate issuance
CA
(3) Obtaining certificate
Certificate
(4) Registering certificates and CRL
CA certificate
Site certificate
CRL
Same as that of slave
Registration order
(5) Making a backup of the Interstage Certificate Environment
(6) Setting to use the certificate
Interstage Management Console [SSL]
SSL definition creation
• [Protocol version]
□ "SSL2.0"
■ "SSL3.0"
□ "TLS1.0"
• [Encryption method]
Match the value to at least one of values of each item in the SSL definition of slave.
Interstage Management Console [Repository]
[Replication destination host information]
[Presentation of client certificate] "Do not present"

C.1.3 Backing up the Master Server Repository

To create a repository of the slave server, it is necessary to back up repository data of the master server and restore it on the slave server machine.

The following explains how to back up repository data of the master server.

1. Select [Repository] from the [System] > [Service] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]) on the Interstage Management Console of the master server machine.

2. Select the check box of the repository intended for master operation on the [Repository: View Status] window and then click the [Stop] button to stop the repository.

3. On the master server, execute the irepbacksys command with the -dataonly option. This will back up the repository data of the master server to a file. The command should be executed with Administrator authority.

   For details of the irepbacksys command, refer to 'Backup Commands' in the 'Reference Manual (Command Edition)'.

   Windows32/64

   Backup destination directory: X:\Backup\irep\rep001_back

   Repository name: rep001

   ```
   irepbacksys -d X:\Backup\irep\rep001_back -R rep001 -dataonly
   IREP: INFO: irep11000: Backup has completed. X:\Backup\irep\rep001_back
   [rep001]
   ```

   Solaris32/64 Linux32/64

   Backup file name (excluding the extension): /backup/irep/rep001_back

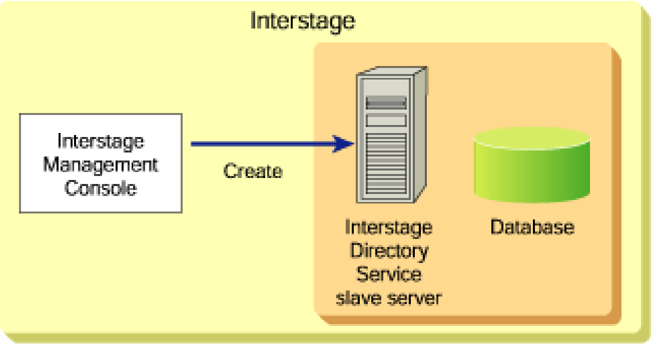
   Repository name: rep001

   For the backup file name, specify the name of the file (excluding the extension) in which repository data is backed up.

   ```
   # irepbacksys -f /backup/irep/rep001_back -R rep001 -dataonly
   UX:IREP: INFO: irep11000: Backup has completed.
   /backup/irep/rep001_back.tar.gz [rep001]
   ```

C.1.4 Creating a Repository for the Slave Server

Figure C.7 Use Interstage Management Console to Create a Repository


Interstage
Interstage Management Console
Create
Interstage Directory Service slave server
Database

The following procedure describes how to create a repository on the slave server using the Interstage Management Console.

Note

Several minutes are needed to create a repository. This includes the time needed to create database information used inside the repository. The total time required varies a little depending on the machine performance.

1. Select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]). Then select the [Create a New Repository] tab.

2. Click the [Create] button after completing the details for each item shown below. Details shown in bold must be configured in the same way as the repository of the master server.

   - [General Settings]

     - Repository Name

       Specify the same repository name as that of the master server. This must be configured during repository setup. After the repository is created, the name cannot be changed.

    - Administrator DN

      Specify the DN (distinguished name) for the administrator who will manage the created repository in the DN format. This must be configured during repository setup. After creating a repository, the value cannot be changed.

      Administrator DN password Specify the password of the administrator who will manage the repository.

    - Administrator DN password (re-entry)

      Re-enter the password of the administrator who will manage the created repository.

    - Public Directory

      Configure with the same value as the master server. This must be configured during repository setup. After the repository is created, the value cannot be changed.

    - Database Storage Directory

      Specify the same storage directory as that of the master server. This must be configured during repository setup. After the repository is created, the value cannot be changed.

- [Detailed Settings] Connection Settings

    - Port number

      Specify the port number to use for non-SSL communication. This must be configured during repository setup. After the repository is created, the value cannot be changed.

    - Enable SSL encryption?

      Specify whether SSL communication will be used. This must be configured during repository setup. After the repository is created, the value cannot be changed.

    - SSL port number

      Specify the port number to use for SSL communication. This must be configured during repository setup. After the repository is created, the value cannot be changed.

    - SSL configuration

      Define the SSL configuration to be used for SSL communication.

For other items, there is normally no need to change the initial values; however, change them if it is required.

For character definitions, such as the number of characters and the range that can be specified for each item, refer to 'Setting Items of the Interstage Management Console'.

After the repository has been created, it will be added to the [Repository: Status] window. Open the window by selecting [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]).

Windows32/64

The created repository will also be added to the Windows(R) service under the following name:

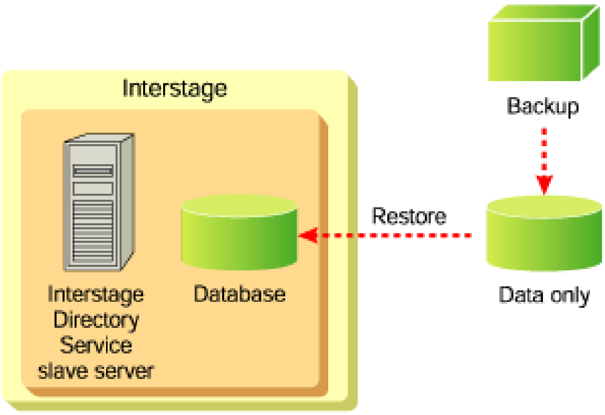
```
Interstage Directory Service (repository name)
```

To check the master server settings, use the Interstage Management Console on the master server. Select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]) and then select the repository created for the master server from the [Repository: View Status] window. Select [General Settings] or [Detailed Settings (display)] to view them.

3. Start the created repository from the [Repository: View Status] window.

C.1.5 Restoring the Repository to the Slave Server

Figure C.8 Restore Data to the Slave Server Repository



The backups of the master server repository data can be restored to the machine of the slave server.

The following procedure describes how to restore repository data.

1. Transfer the backup directory (backup file, if on Solaris or Linux) (created in the procedure above, "Backing up the Master Server Repository") to the machine of the slave server. Ensure that, during transfer, the data is not intercepted by unauthorized parties. After copying the file, make sure that it is deleted.
2. Select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]) in the Interstage Management Console on the slave server.
3. Check the status of the slave repository from the [Repository: View Status] window. If it does not display as stopped, check its check box and then click the [Stop] button to stop the repository.
4. On the slave server machine, execute the ireprestsys command with the -dataonly option. This will restore the backup directory (backup file, if on Solaris or Linux) data. Specify the backed-up repository name in the command.

   A confirmation message displays, requesting to overwrite the database. To replace it and continue restoring the data, enter 'y' or 'Y'. To stop the data restoration, enter 'n' or 'N'. If any other key is typed, the following message will display, awaiting user input: "Data already exists in database store. (C:\Interstage\Enabler\EnablerDStores\IREP\rep001\data)

   Are you sure of deleting data in database store? (y/n):"

   For details of the ireprestsys command, refer to the 'Reference Manual (Command Edition)'.

   Windows32/64

   Backup destination directory: X:\Backup\irep\rep001_back

   Repository name: rep001

   Database storage directory: C:\Interstage\Enabler\EnablerDStores\IREP\rep001\data

   ```
   ireprestsys -d X:\Backup\irep\rep001_back -R rep001 -dataonly
   Data already exists in database store. (C:\Interstage\Enabler\EnablerDStores\IREP\rep001\data)
   Are you sure of deleting data in database store? (y/n):y
   IREP: INFO: irep11001: Restore has completed. X:\Backup\irep\rep001_back
   [rep001]
   ```

   Solaris32/64

   Backup destination directory: /backup/irep/rep001_back.tar.gz

   Repository name: rep001

Database storage directory: /var/opt/FJSVena/EnablerDStores/FJSVirep/rep001/data

```
#ireprestsys -f /backup/irep/rep001_back.tar.gz -R rep001 -dataonly
Data already exists in database store.
(/var/opt/FJSVena/EnablerDStores/FJSVirep/rep001/data)
Are you sure of deleting data in database store? (y/n):y
UX:IREP: INFO: irep11001: Restore has completed.
/backup/irep/rep001_back.tar.gz[rep001]
```

Linux32/64

Backup destination directory: /backup/irep/rep001_back.tar.gz

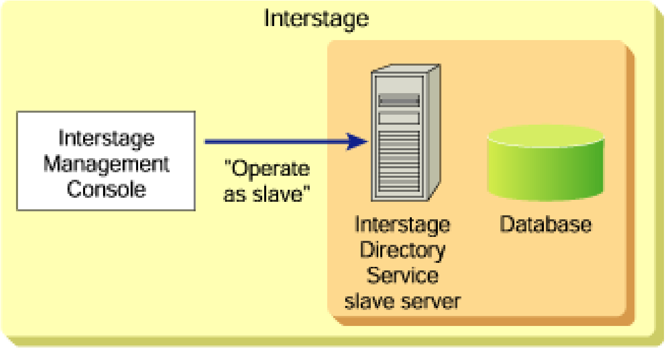
Repository name: rep001

Database storage directory: /var/opt/FJSVena/DStores/FJSVirep/rep001/data

```
#ireprestsys -f /backup/irep/rep001_back.tar.gz -R rep001 -dataonly
Data already exists in database store.
(/var/opt/FJSVena/DStores/FJSVirep/rep001/data)
Are you sure of deleting data in database store? (y/n):y
UX:IREP: INFO: irep11001: Restore has completed.
/backup/irep/rep001_back.tar.gz[rep001]
```

C.1.6 Changing the Repository Settings of the Slave Server

Figure C.9 Change Repository Settings of the Slave Server


Interstage
Interstage Management Console
"Operate as slave"
Interstage Directory Service slave server
Database

Change the repository settings of the slave server to have it operate in replication mode. The following procedure describes how to change the settings using the Interstage Management Console on the slave server.

1. Click [System] > [Service] > [Repository] (If on the Admin Server, click [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]) and then select the slave repository in the [Repository: View Status] window.

2. Click [Detailed Settings (View)] and then under [Replication Settings], select "Slave" as the [Operation mode].

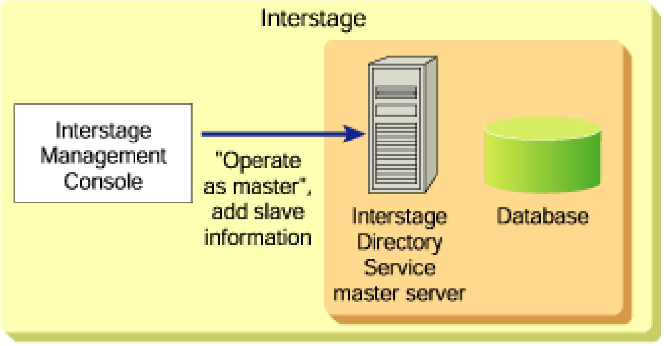
3. Select the host name of the master server machine in the newly-displayed [Slave operation settings].

4. Click the [Apply] button.

5. Check the check box of the changed repository, and then click the [Start] button to start the repository.

C.1.7 Changing the Repository Settings of the Master Server

Figure C.10 Configure the Master Server with Slave Information


Interstage
Interstage Management Console
"Operate as master", add slave information
Interstage Directory Service master server
Database

Configure the master server repository with information about the newly-added slave server repository. The following procedure describes how to configure the master server using the Interstage Management Console on the master server machine.

1. Click [System] > [Service] > [Repository] (If on the Admin Server, click [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]) and then select the master repository in the [Repository: View Status] window.
2. Click [Detailed Settings (View)]. If the [Operation mode] under [Replication Settings] is "Master," proceed to Step 3. If the setting is not "Master," select this option. [List of replication destination hosts will then display.
3. Click the [Add] button, and configure the information about the slave server machine for each item in [Replication destination host list]. Click the [Apply] button. If using SSL communication for replication operation, select "Yes" for [Present client certificate?], and the value of [SSL configuration] defined in the master server's SSL communication environment setup].

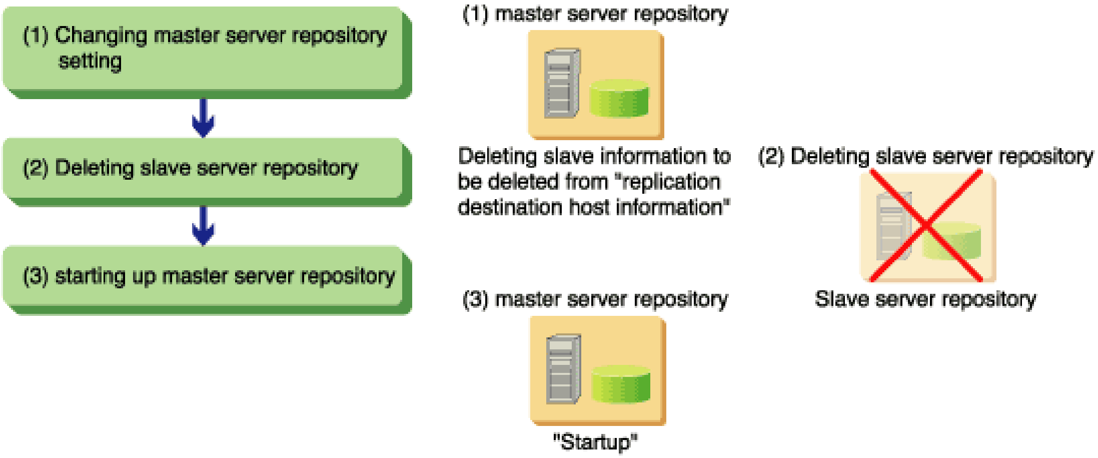
   Note

   - If "No" is selected in [Present client certificate?] while site certificates are registered, no SSL configuration will be needed. However, all site certificates will automatically be sent from the master server to the slave server. For security, it is recommended that select "Yes".
   - Several seconds to several minutes are needed to change the repository settings. This includes the time needed to confirm the connection to the replication destination. The total time varies a little depending on the use of SSL, network environment, and machine performance.
4. Check the check box of the changed repository and then click the [Start] button to start the repository.

C.1.8 Procedure for Deleting a Slave Server during Replication Operation

The following figure illustrates the procedure for deleting a slave server during replication operation.

Figure C.11 Delete a Slave Server in Replication Mode


(1) Changing master server repository setting
(2) Deleting slave server repository
(3) starting up master server repository
(1) master server repository
Deleting slave information to be deleted from "replication destination host information"
(2) Deleting slave server repository
Slave server repository
(3) master server repository
"Startup"

Changing the Repository Settings of the Master Server

This procedure involves deleting information about the slave server repository from the master server repository.

1. Stop the repository during the master operation. This is performed by using the Interstage Management Console connected to the machine of the master server.
2. Click [Detailed Settings [display]] on the [Environment settings] window of the stopped repository.
3. Select the slave repository to be deleted from [Replication destination host list]
4. Click the [Delete] button.

Deleting the Repository of the Slave Server

The repository of the slave server will be deleted.

1. Stop the repository in slave operation using the Interstage Management Console connected to the machine of the slave server.
2. Delete the stopped repository in slave operation.

Starting up the Repository of the Master Server

Use the instruction shown below to start the repository of the master server.

Start the repository in master operation using the Interstage Management Console connected to the machine of the master server.

C.1.9 Basic Operations for Replication Operations (Using the Standard Database)

This section explains the operating procedures for each system to perform replication.

These operations are performed on the copy-source system (the master server for the repository) and the copy-destination system (the slave server for the repository).

Starting Replication Operations

Use the following procedure to start replication operations:

1. Start the repository on the slave server

   Start the repository for slave operations using an Interstage Management Console connected to the machine that is the slave for replication.

2. Start the repository on the master server

   Start the repository for master operations using an Interstage Management Console connected to the machine that is the master for replication.

Finishing Replication Operations

Use the following procedure to finish replication operations:

1. Stop the repository on the master server

   Stop the repository for master operations using an Interstage Management Console connected to the machine that is the master for replication.

2. Stop the repository on the slave server

   Stop the repository for slave operations using an Interstage Management Console connected to the machine that is the slave for replication.

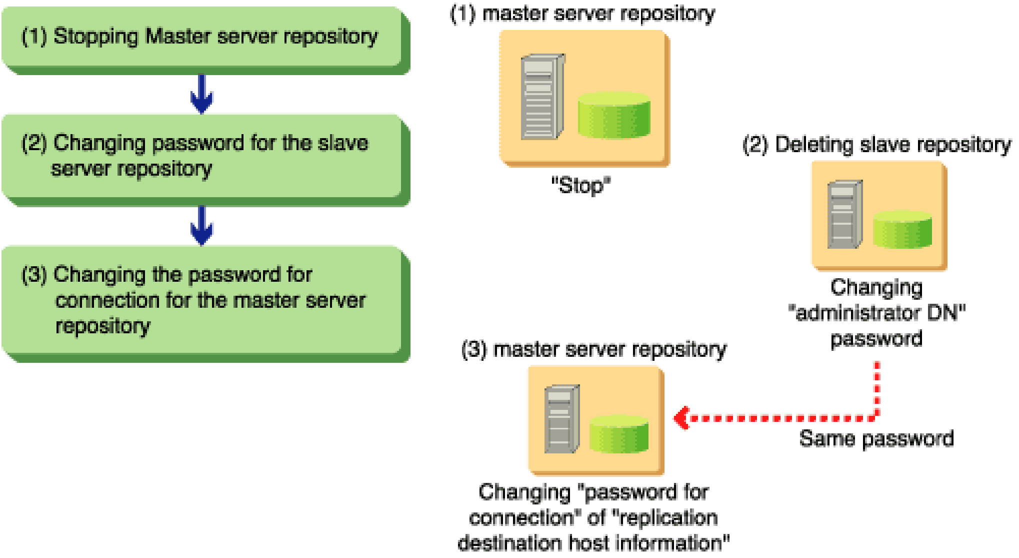
C.1.10 Procedure for Changing the Password

This section explains the procedure for changing the slave password during a replication operation.

If the administrator DN password of a repository (in slave operation) is changed, a new password must set by selecting [Password for the connection] and then [Replication Connection Settings] for the repository in master operation.

The following shows a flow diagram of the procedure for changing the password of the slave during replication operation.

Figure C.12 Change a Password of the Slave.


(1) Stopping Master server repository
(2) Changing password for the slave server repository
(3) Changing the password for connection for the master server repository
(1) master server repository
"Stop"
(2) Deleting slave repository
Changing "administrator DN" password
(3) master server repository
Same password
Changing "password for connection" of "replication destination host information"

Stopping a Repository of the Master Server

Use the Interstage Management Console to stop a repository of the master server. The procedure for doing this is as follows:

Stop the repository during master operation. This is performed using the Interstage Management Console connected to the master server machine.

Changing the Password of a Repository of the Slave Server

Change the password of a slave server repository as follows:

1. Stop the repository during slave operation. This is performed using the Interstage Management Console connected to the slave server machine.
2. Click the stopped repository in slave operation to display the [Settings] window.
3. Select 'Change' in [Change password?] and then, after a dialog box is displayed, click the [OK] button.
4. After [New Administrator DN password] and [New Administrator DN password (re-entry)] are displayed, set the same new password and then click the [Apply] button.
5. Start the repository using the Interstage Management Console.

Changing the Password of the Repository Used to Connect to the Slave Server

Change the password of the master server repository as follows:

1. Using the Interstage Management Console that connected to a master server, select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]).

   The [Repository : View Status] window is displayed.
2. Click the stopped repository (Described on 'Stopping a Repository of the Master Server') to display the [Settings] window, and then click the [show] to display detailed settings.
3. Select the name of the host where the slave operation repository's Administrator DN password has been changed on [Replication destination host list], and then click [Edit].
4. In the displayed [Password for the connection] of [Replication Connection Settings], set the password with a same value that has been set on slave server, and then click the [Update] button.

5. Start the repository using the Interstage Management Console.

C.2 Using the Oracle Database

This section explains the procedure for creating an operation environment for replication mode where an Oracle database is used as the database for the repository.

1. Physically design the database for the master and the slave (estimate disk and memory capacities)
2. Create raw devices for the master and the slave (recommended for Solaris and Linux)
3. Create the master database (script)
4. Create the master repository
5. Register data with the master repository
6. Create the slave database (script)
7. Create the slave repository
8. Configure settings for replication operations between the master database and the slave database

When creating repositories, make definitions using "standalone operations" (do not make definitions for "master operations" and "slave operations").

Two or more repositories for standalone operations can be created, but you must specify the same value (DN) for the "Public Directory" for each repository.

Refer to the Oracle database manual for more information about how to create an environment for replication mode.

C.3 Operation Monitoring in Replication Mode and Recovering Repositories

This section explains messages output, when problems occur during operation in replication mode, and the recovery procedure for restoring the repository.

C.3.1 Monitoring of Operation in Replication Mode

If the standard database is used

Solaris32/64 Linux32/64

If a problem occurs in replication mode, messages beginning with irep15XXX are output to the system log of the master server.

Windows32/64

If a problem occurs in replication mode, messages beginning with irep15XXX are output to the event log.

By monitoring the log files, replication errors can be detected quickly.

Refer to 'Messages beginning with irep15XXX' in 'Messages' for error messages and the associated [User action].

If an RDB is used

To perform operation monitoring for replication when an Oracle database is used, refer to the Oracle database manual.

C.3.2 Restoring the Slave Repository in Replication Mode

The following procedure describes how to restore the slave repository in replication mode.

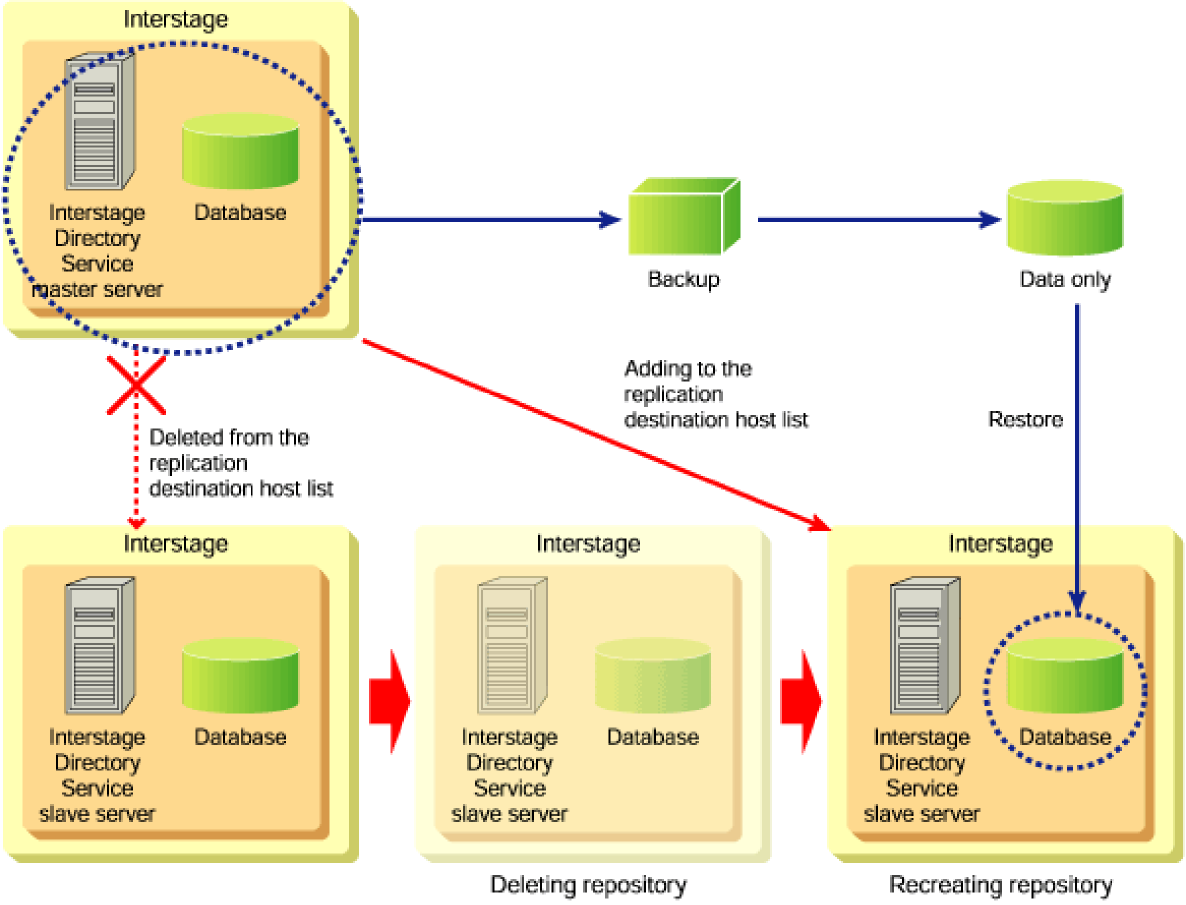
If the environment is damaged, the repository is restored by recreating a slave repository.

If data inside the database is damaged, only data in the slave repository is restored.

Environment Has been Destroyed

- **If the standard database is used**

Figure C.13 Environment has been Destroyed


Interstage
Interstage Directory Service master server
Database
Backup
Data only
Adding to the replication destination host list
Restore
Deleted from the replication destination host list
Interstage
Interstage Directory Service slave server
Database
Interstage
Interstage Directory Service slave server
Database
Interstage
Interstage Directory Service slave server
Database
Deleting repository
Recreating repository

Operation on the Master Server

1. Stop the repository that has the same name as the restoring repository for the slave server. This step is performed using the Interstage Management Console
2. Use the ireprestsys command to backup the repository that has same name as the restoring repository for the slave server.
3. Transfer the backup directory (for Solaris/Linux, it is backup file) created in step 2 to the slave server.
4. Click [Detailed setting [show]] on the [Settings] window of the repository stopped in step 1.
5. Select and delete the host name of the slave server where the repository to be restored exists from [Replication destination host list].

Operation on the Slave Server

1. Stop the restoring repository using the Interstage Management Console
2. Delete the repository stopped in step 6.
3. Use the Interstage Management Console to ensure the following items have the same settings as the master repository by using [Create a New Repository] tab (after selecting [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository])) and then click the [Create] button.
    - [Repository name]
    - [Public directory]

- [Database storage directory]

4. Use the ireprestsys command with the specified -dataonly option to restore the repository from the backup directory (for Solaris/ Linux, it is backup file) in step 3.

5. Specify the same repository name as that of the backed up repository.

6. A message displays, requesting confirmation to replace the database. To replace the database and continue restoring the repository, enter 'y' or 'Y'. To stop restoring the repository, enter 'n' or 'N'. If any other key is typed, the confirmation message is displayed again.

   Example

   Windows32/64

   Backup directory name: X:\Backup\irep\rep001_back

   Repository name: rep001

   ```
   ireprestsys -d X:\Backup\irep\rep001_back -R rep001 -dataonly
   Data already exists in database store. (C:\Interstage\Enabler\EnablerDStores\IREP
   \rep001\data)
   Are you sure of deleting data in database store? (y/n):y
   IREP: INFO: irep11001: Restore has completed. X:\Backup\irep\rep001_back [rep001]
   ```

   Solaris32/64

   Backup file name: /backup/irep/rep001_back.tar.gz

   Repository name: rep001

   ```
   ireprestsys -f /backup/irep/rep001_back.tar.gz -R rep001 -dataonly
   Data already exists in database store. (/var/opt/FJSVena/EnablerDStores/FJSVirep/rep001/data)
   Are you sure of deleting data in database store? (y/n):y
   UX:IREP: INFO: irep11001: Restore has completed. /backup/irep/rep001_back.tar.Z [rep001]
   ```

   Linux32/64

   Backup file name: /backup/irep/rep001_back.tar.gz

   Repository name: rep001

   ```
   ireprestsys -f /backup/irep/rep001_back.tar.gz -R rep001 -dataonly
   Data already exists in database store. (/var/opt/FJSVena/DStores/FJSVirep/rep001/data)
   Are you sure of deleting data in database store? (y/n):y
   UX:IREP: INFO: irep11001: Restore has completed. /backup/irep/rep001_back.tar.Z [rep001]
   ```

7. Using the Interstage Management Console, select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]). Click the restored repository displayed on the [Repository : View Status] window.

8. Click [Detailed settings [View]] on the [Settings] window and then select 'Slave' from [Replication settings].

9. Set the host name of the master server in [Slave operation settings] and then click the [Apply] button.

10. Start the restored repository using the Interstage Management Console.

Operation on the Master Server

1. In the Interstage Management Console, select [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository]). Open the [Repository : View Status] window. Click the repository with the same name as the restored slave repository displayed in the window.

2. Click [Detailed settings [View]] on the [Settings] window.

3. Click the [Add] button in [Replication destination host list].

4. Enter information about the restored slave repository to each item in [Replication Connection Settings] and then click the [Apply] button.

5. Start the restored master repository from the [Repository : View Status] window (found by selecting [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository])).

For details of the irepbacksys and ireprestsys commands, refer to 'Backup commands' in the 'Reference Manual (Command Edition)'.

- **If the RDB is used**

  Operation on the Master Server

  1. Use the Interstage Management Console to stop the repository with the same name as the slave-side repository to be recovered.

  Operation on the Slave Server

  1. Stop the repository to be recovered.
  2. Delete the repository that was stopped in step 2.
  3. Restore the resources for the slave-side repository that was backed up when the environment was created. Restore the resources using the ireprestsys command with the "-confonly" option.
  4. Use the Interstage Management Console to start the recovered repository.

  Operation on the Master Server

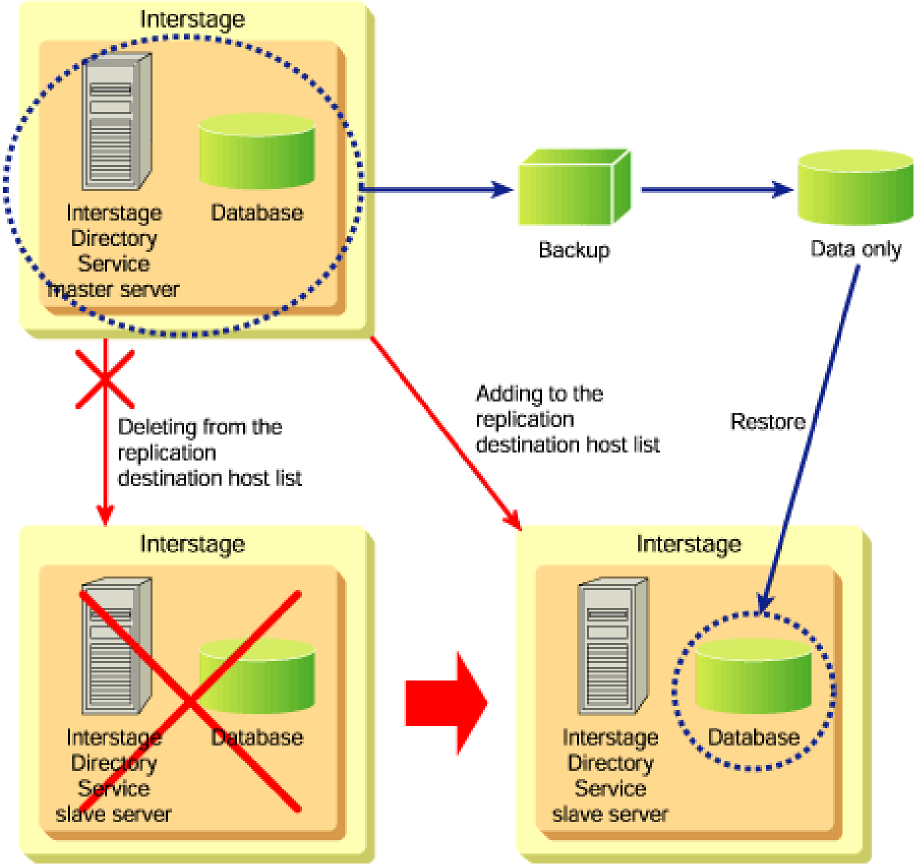
  1. Use the Interstage Management Console to start the master-side repository that was stopped in step 1.

Refer to "Backup Commands" in the Reference Manual (Command Edition) for more information about the *ireprestsys* command.

Data in Database Has been Destroyed

- **If the standard database is used**

Figure C.14 Data in Database has been Destroyed


Interstage
Interstage Directory Service master server
Database
Backup
Data only
Deleting from the replication destination host list
Adding to the replication destination host list
Restore
Interstage
Interstage Directory Service slave server
Database
Interstage
Interstage Directory Service slave server
Database

Operation on the Master Server

1. Stop the repository using the Interstage Management Console. If multiple repositories are defined, select the repository with the same name as that of the slave repository to be restored.
2. Use the irepbacksys command to back up the repository stopped in step 1.
3. Transfer the backup file created in step 2 to the slave server on which the repository to be restored exists.
4. Click [Detailed settings [show]] on the [Settings] window of the repository stopped in step 1.
5. From [Replication destination host list], select and delete the host name of the slave server on which the repository to be restored exists.

Operation on the Slave Server

1. In the Interstage Management Console, stop the repository to be restored.
2. Use the ireprestsys command with the specified -dataonly option to restore only data inside the database from the backed up directory (In Solaris/Linux case, it is backed up file) transferred in step 3. Specify the same repository name as that of the backup repository.
3. A message displays, requesting confirmation to replace the database. To replace the database and continue restoring the repository, enter 'y' or 'Y'. To stop restoring the repository, enter 'n' or 'N'. If any other key is typed, the confirmation message is displayed again.

Example)

Windows32/64

Backup directory name: X:\Backup\irep\rep001_back

Repository name: rep001

```
ireprestsys -d X:\Backup\irep\rep001_back -R rep001 -dataonly
Data already exists in database store. (C:\Interstage\Enabler\EnablerDStores\IREP
\rep001\data)
Are you sure of deleting data in database store? (y/n):y
IREP: INFO: irep11001: Restore has completed. X:\Backup\irep\rep001_back [rep001]
```

Solaris32/64

Backup file name: /backup/irep/rep001_back.tar.gz

Repository name: rep001

```
ireprestsys -f /backup/irep/rep001_back.tar.gz -R rep001 -dataonly
Data already exists in database store. (/var/opt/FJSVena/EnablerDStores/FJSVirep/rep001/data)
Are you sure of deleting data in database store? (y/n):y
UX:IREP: INFO: irep11001: Restore has completed. /backup/irep/rep001_back.tar.Z [rep001]
```

Linux32/64

Backup file name: /backup/irep/rep001_back.tar.gz

Repository name: rep001

```
ireprestsys -f /backup/irep/rep001_back.tar.gz -R rep001 -dataonly
Data already exists in database store. (/var/opt/FJSVena/DStores/FJSVirep/rep001/data)
Are you sure of deleting data in database store? (y/n):y
UX:IREP: INFO: irep11001: Restore has completed. /backup/irep/rep001_back.tar.Z [rep001]
```

4. In the Interstage Management Console, start the restored repository.

Operation on the Master Server

1. In the Interstage Management Console, click the repository stopped in step 1 displayed in the [Repository: View Status] window (found by selecting [System] > [Service] > [Repository] (If on the Admin Server, select [Application Management] > [Interstage] > [Interstage Application Server] > [Security] > [Repository])).
2. Click [Detailed settings [View]] on the [Settings] window.
3. Click the [Add] button in [Replication destination host list].
4. Enter information about the restored slave repository to each item in [Replication Connection Settings] and then click the [Apply] button.
5. Use the Interstage Management Console to start the restored master repository.

For details of the irepbacksys and ireprestsys commands, refer to 'Backup commands' in the 'Reference Manual (Command Edition)'.

- **If the RDB is used**

  If an RDB is being used and data in the database is damaged, recover the data in the database. The backup/restore/recovery function of the RDB product can be used to recover data in the database to the state when the last backup was taken. If no backup has been taken, the data will need to be created again.

  Operation on the Master Server

  1. Use the Interstage Management Console to stop the repository with the same name as the slave-side repository to be recovered.

  Operation on the Slave Server

  1. Use the Interstage Management Console to stop the repository to be recovered.
  2. Recover the data using the backup/restore/recovery function of the RDB product.

3. Use the Interstage Management Console to start the recovered repository.

Operation on the Master Server

1. Use the Interstage Management Console to start the master-side repository that was stopped in step 1.

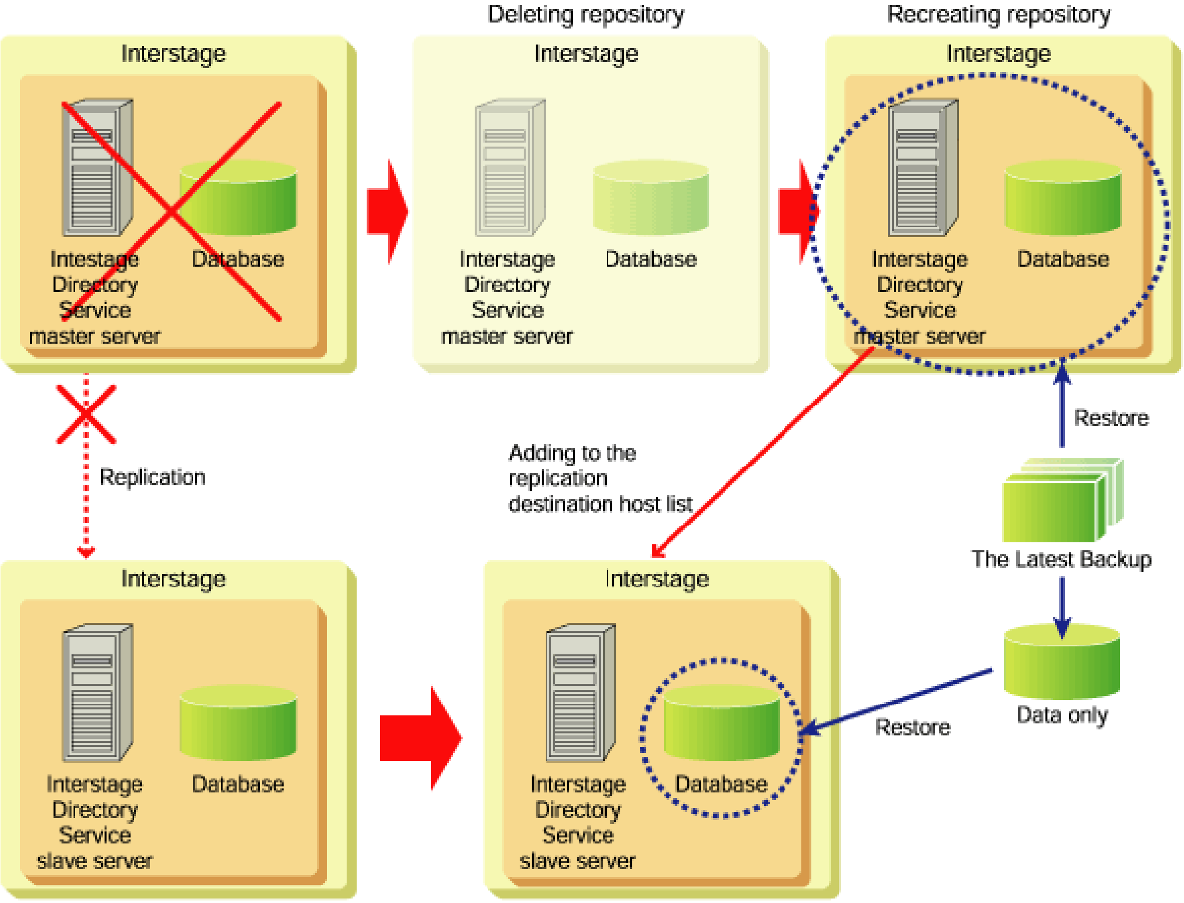
C.3.3 Restoring the Master Repository in Replication Mode

Using the master repository backed up directory (In Solaris/Linux case, it is backed up file), the master repository can be restored in replication mode. If there is no backed up directory (In the case of Solaris/Linux, it is a backed up file), the replication mode needs to be recreated.

Backed up Directories (or Files)

- **If the standard database is used**

Figure C.15 Backed up Directories (or Files)


Deleting repository
Recreating repository
Interstage
Intestage Directory Service master server
Database
Interstage
Interstage Directory Service master server
Database
Interstage
Interstage Directory Service master server
Database
Replication
Adding to the replication destination host list
Restore
The Latest Backup
Interstage
Interstage Directory Service slave server
Database
Interstage
Interstage Directory Service slave server
Database
Restore
Data only

Operation on the Master Server

1. Stop the repository to be restored using the Interstage Management Console.
2. Delete the repository stopped in step 1.

Operation on the Slave Server

1. Using the Interstage Management Console, stop the repository with same process in step 1. If multiple repositories are defined, stop the repository with the same name as the master repository to be restored.
2. Use the ireprestsys command (with the specified -dataonly option) to restore the data from the backed up directory (In Solaris/Linux case, it is backed up file) of the master repository.

3. Use the Interstage Management Console to start the restored repository.

Operation on the Master Server

1. Use the ireprestsys command (with the -S option) to restore the master repository backup directory (for Solaris/Linux, it is backup file)
2. Select the restored repository as displayed in the [Repository : View Status] window.
3. Click [Detailed settings [show]] on the [Settings] window and then select 'Master' from [Replication Settings].
4. Click the [Add] button in [Replication destination host list].
5. Set information about the restored slave repository for each item in [Replication Connection Settings] and then click the [Apply] button.
6. Use the Interstage Management Console to start the restored master repository.

For details of the irepbacksys and ireprestsys commands, refer to 'Backup commands' in 'Reference Manual (Command Edition)'.

- **If the RDB is used**

  The backup/restore/recovery function of the RDB product can be used to recover data in the database to the state when the last backup was taken.

  Operation on the Master Server

  1. Use the Interstage management console to stop the repository that is to be recovered.
  2. Delete the repository that was stopped in step 1.

  Operation on the Slave Server

  1. Use the Interstage Management Console to stop the repository to be recovered.
  2. Recover the data using the backup/restore/recovery function of the RDB product.
  3. Use the Interstage Management Console to start the recovered repository.

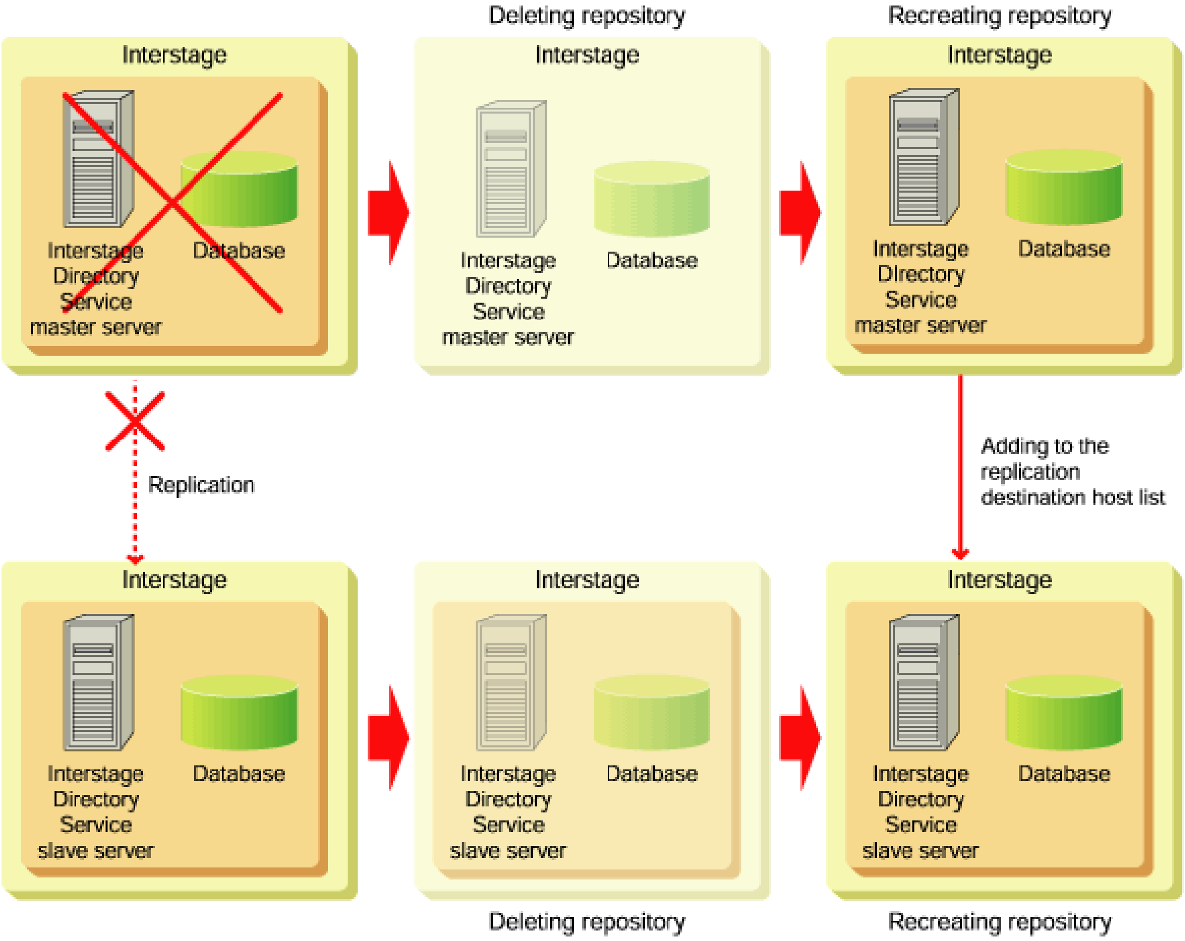
  Operation on the Master Server

  1. Restore the resources for the master-side repository that was backed up when the environment was created. Restore the resources using the ireprestsys command with the "-confonly" option.
  2. Recover the data using the backup/restore/recovery function of the RDB product.
  3. Use the Interstage Management Console to start the master-side repository that was stopped in step 1.

Refer to "Backup Commands" in the Reference Manual (Command Edition) for more information about the *ireprestsys* command.

No Backed up Directories (or Files) Exist

Figure C.16 No Backed Up Directories (or Files) Exist


Deleting repository
Recreating repository
Interstage
Interstage Directory Service master server
Database
Replication
Adding to the replication destination host list
Interstage Directory Service slave server
Deleting repository
Recreating repository

Operation on the Master Server

1. Stop the repository to be restored using the Interstage Management Console.

Operation on the Slave Server

1. Use the Interstage Management Console to stop the repository, with the same name, as the master repository to be restored.
2. Delete the repository stopped in step 2.

Operation on the Master Server

1. Delete the repository stopped in step 1.
2. Create the replication mode. For details of the environment setup in replication mode, refer to "Creating a Load Distribution Environment (Replication Mode)".

Appendix D Estimating Resources for Symfoware/RDB

This section describes the formula for estimating resources required by Symfoware/RDB when running Interstage Directory Service applications.

For details about estimating the required options, refer to the "Setup Guide" in the Symfoware Server manual.

D.1 Estimating Disk Space

This section explains the disk space that is required for the repository database, as part of the disk space required by the RDB system.

D.1.1 Estimating the Database Space

If Detailed Settings are not Made for Tables

If detailed settings are not made for tables when the tables for storing repository data are created, the database space required by the repository is calculated using the following estimation formula:

```
Database space(K bytes) = ( 82.5 x number of registered entries + 1,200 ) x r
  r : Safety factor (1.2 or more)

(*1)(*2)
```

1K byte is 1,024 bytes.

*1 Correct the calculated database space so that it is a multiple of 32K bytes.

*2 Round up the value calculated for N to the nearest whole number.

Note

- The database space required by the repository is 100 MB if no more than 1,000 entries are to be registered in the repository. In this case there is no need to make any calculations using the estimation formula.

If Detailed Settings are Made for Tables

If detailed settings are made for tables when the tables for storing repository data are created, the database space required by the repository is calculated using the following estimation formula:

```
Database space (K bytes) = (T + I) x r
  T : Amount of database space for table DSIs (K bytes)
  I : Amount of database space for index DSIs (K bytes)
  r : Safety factor (1.2 or more)

(*1)(*2)
```

1K byte is 1,024 bytes.

*1 Correct the calculated database space so that it is a multiple of 32K bytes.

*2 Round up the result of the calculation to the nearest whole number.

1. **Amount of Database Space for Table DSIs**

```
(Amount of space for DS_SCOPE(bytes) + Amount of space for DS_FILTER(bytes) + Amount of space
for DS_ENTRY(bytes) )/1,024
```

Calculate the amount of space for each table that is to be specified when detailed settings are made.

Use the variable information in the following table to calculate the amount of space for each table by referring to 'SEQUENTIAL Structure' under 'Estimating the Required Amount of Database Space' in the 'RDB User's Guide: Database Definition' Symfoware Server manual.

Table D.1 Table Space Calculation

Table name	Sum of lengths of fixed-length columns (bytes)	Number of variable-length columns	Sum of lengths of variable-length columns (bytes)	Number of columns without a NOT NULL specification for the target base table	Page length (bytes)	Total number of records
DS_SCOPE	16	3	S x 2 + 30	1	32,768	Number of entries
DS_FILTER	21	3	S + 55	2	32,768	Number of entries x Average number of attributes per entry
DS_ENTRY	16	4	S + B + 50	2	32,768	Number of entries x (Average number of attributes per entry + 1)

where:

- S: Average length of text data

  Total length of string-type attribute values for all entries (bytes) / Total number of string-type attributes for all entries

  Round the result up to the nearest whole number.

- B: Average length of binary data

  Total size of binary-type attribute values for all entries (bytes) / Total number of attributes for all entries

  Round up the result up to the nearest whole number.

2. **Amount of database space for index DSIs**

```
(Total amount of space for the index part and the data part of the indexes for DS_SCOPE(bytes)
+ Total amount of space for the index part and the data part for
DS_FILTER(bytes)
+ Total amount of space for the index part and the data part for
DS_ENTRY(bytes) )/1,024
```

Calculate the amount of space for each index of each table that is to be specified when detailed settings are made.

For each table, calculate the amount of space for the index part and the data part for each index using the variable information in the following table by referring to 'BTREE structure data part' and 'BTREE structure index part' under 'Estimating the Required Amount of Database Space' in the 'RDB User's Guide: Database Definition 'Symfoware Server manual.

Table D.2 Index Memory Requirements Calculation

Table name	Index	Total length of index key configuration columns (bytes)	Page length of the data part (bytes)	Page length of the index part (bytes)	Number of records in the table
DS_SCOPE	Index 1	8	4,096	4,096	Number of entries
	Index 2	30	4,096	4,096	
	Index 3	S + 8	4,096	4,096	
	Index 4	S + 8	4,096	4,096	
	Index 5	8	4,096	4,096	
DS_FILTER	Index 1	8	4,096	4,096	Number of entries x Average number of attributes per entry
	Index 2	63	4,096	4,096	
	Index 3	S + 33	4,096	4,096	

Table name	Index	Total length of index key configuration columns (bytes)	Page length of the data part (bytes)	Page length of the index part (bytes)	Number of records in the table
	Index 4	38	4,096	4,096	
	Index 5	S + 33	4,096	4,096	
	Index 6	38	4,096	4,096	
DS_ENTRY	Index 1	8	4,096	4,096	Number of entries x (Average number of attributes per entry + 1)
	Index 2	33	4,096	4,096	

3. **S: Average length of text data**

   Total length of string-type attribute values for all entries (bytes) / Total number of string-type attributes for all entries

   Round the result up to the nearest whole number.

D.1.2 Estimating the RDB Dictionary Capacity

The RDB dictionary capacity estimation is shown below.

The initial value is the capacity immediately after the RDB dictionary is created.

The basic value is the capacity required for each database that is added.

Specify 20M bytes or more for the RDB dictionary capacity.

If there is insufficient capacity, calculate the capacity according to the basic value and then extend the capacity.

1K byte is 1,024 bytes, and 1M byte is 1,024K bytes.

Initial value

550K bytes

Basic value

100K bytes

D.1.3 Estimation Formula for RDB Directory Files

This section describes the estimation formula for RDB directory files.

Estimation Formula for RDB Directory Files

The estimation formula for RDB directory files is shown below.

- User database RDB directory files
- RDB dictionary RDB directory files

This section describes the estimation formula for each file. The result of the division is rounded up to the nearest whole number.

1K byte is 1,024 bytes, and 1M byte is 1,024K bytes.

- **User Database RDB Directory Files**

```
User database RDB directory files = ((4 + 2.1 x B + 1.1 x S + 1.5 x D + P) / 256) x r (M bytes)

  B: RDB system database number
  S: RDB system database space number
```

```
 D: RDB system DSI number                    (*1)
 P: Page management area
 r: Safety margin (1.3 or more)              (*2)
```

*1 If an RDB system is created for the Interstage Directory Service, a total of 16 DSIs will be created.

*2 1.3 is recommended.

Page management area = DSI page number total / 8,704

DSI page number total

DSI space allocation amount total (K bytes) / 4

DSI space allocation amount total

- If detailed settings are not made for tables

  82.5 x Number of entries + 1,200

- If detailed settings are made for tables

  Sum of sizes defined in detailed definition file

- **RDB Dictionary RDB Directory Files**

```
RDB dictionary RDB directory files = 1M bytes
```

Estimation Formula for RDB Directory Files for Each Application

The estimation formula for RDB directory files is shown below.

- Audit log applications
- Failover applications
- Load share applications

The result of the division is rounded up to the nearest whole number. 1K byte is 1,024 bytes.

- **Audit Log Applications**

  The estimation formula for audit log applications is shown below.

  - **RDB Directory File**

```
RDB directory file = A + B + C + 1 (M bytes)

  A: Value estimated for user database RDB directory files
  B: Value estimated for RDB dictionary RDB directory files
  C: Audit log management information
```

For details about the value estimated for user database RDB directory files and RDB dictionary RDB directory files, refer to "D. 1.3 Estimation Formula for RDB Directory Files".

  - **Audit Log Management Information**

```
Audit log management information = ((1.1 x E + 1.5 x F + G) / 512) x r(M bytes)

  E: Raw device number for deploying the audit log database
  F: Audit log database element number
  G: Audit log page management area
  r: Safety margin (1.3 or more) (Note 1)
```

Note 1: 1.3 is recommended.

Audit log page management area = (41.6 x audit log element size x F) / 5,632

For details about the audit log element size, refer to "D.1.11 Estimation Formula for Audit Logs". If the result of the page management area calculation is less than F (element number), round up to F.

- **Failover Applications**

  The estimation formula for failover applications is shown below.

  - RDB Directory File

```
RDB directory file = A + B + 1 (M bytes)

  A: Value estimated for user database RDB directory files
  B: Value estimated for RDB dictionary RDB directory files
```

For details about the value estimated for user database RDB directory files and RDB dictionary RDB directory files, refer to "Estimation Formula for RDB Directory Files".

- **Load Share Applications**

  The estimation formula for load share applications is shown below.

  - RDB Directory File

    Capital

    For details, refer to "Failover applications", "RDB directory file".

    Satellite

```
RDB directory file = A + 2 (M bytes)
A: Value estimated for user database RDB directory files
```

For details on the value estimated for user database RDB directory files, refer to "Estimation Formula for RDB Directory Files".

D.1.4 Estimation Formula for Log Capacity

The estimation formula for log capacity is shown below.

The log capacity estimated here is output according to the database update performed by the application. The log capacity is a basic value for estimating temporary log files (BI log capacity, AI log capacity), archive log files, and in doubt log files.

BI Log Capacity

The BI log capacity for each transaction unit is estimated according to the formula shown below.

It is recommended that the safety margin (1.3) is multiplied by the BI log capacity for the calculated transaction.

```
Transaction BI log capacity = (
42,837 x Number of attributes included in entry that will be updated + 8,255) x safety margin (1.3)
```

AI Log Capacity

The AI log capacity for each transaction unit is estimated according to the formula shown below.

It is recommended that the safety margin (1.3) is multiplied by the AI log capacity for the calculated transaction.

```
Transaction AI log capacity = (
42,837 x Number of attributes included in entry that will be updated + 8,255 ) x safety margin (1.3)
```

Archive Log Capacity

The archive log capacity for each transaction unit is the same as the AI log capacity.

- In doubt Log Capacity

  The in doubt log file is only required for running load share applications. The in doubt log is collected in the in doubt log file. The in doubt log capacity for each transaction unit is the same as the BI log capacity.

D.1.5 Estimating Log Group Management Files

The log group management file is 256K bytes.

1K byte is 1,024 bytes.

D.1.6 Log Management File

The log management file is 100K bytes.

1K byte is 1,024 bytes.

D.1.7 Estimation Formula for Temporary Log Files

This section describes the formula for estimating the temporary log files.

1. Estimate the values below for the application number simultaneously executed and the update BI log capacity:
   - Transaction entry number
   - Transaction update data amount and concurrency
   - BI log area
2. Next, estimate the values below for the BI log area and the database recovery processing time (crash recovery time) target value:
   - Crash recovery time
   - AI log area
   - Recovery log capacity

Transaction Entry Number

The estimation formula for the transaction entry number is shown below.

If flush treatment recovery application is performed in a load share application, double the estimated value.

```
Transaction entry number = (Maximum thread number + 1) x Number of repositories x 4
```

The temporary log index area is determined by the transaction entry number. Calculate the size of the log index part size using the formula shown below.

- **Symfoware Server Enterprise Extended Edition**

```
Temporary log index area = Block length + 2 x BLOCK(248 x T + 304) (in bytes)

  T: Transaction entry number
  Block length: This is the temporary log area block length.
              This is the value specified using the io
              option when the temporary log file is created.
              If this is not specified, this is 512 bytes.
  BLOCK( ): The formula in brackets is rounded up using block boundary.
```

- **Symfoware Server Enterprise Edition, and Symfoware Server Standard Edition**

```
Temporary log index area = Block length + 2 x BLOCK(240 x T + 304) (in bytes)

  T: Transaction entry number
  Block length: This is the temporary log area block length.
              This is the value specified using the io
              option when the temporary log file is created.
              If this is not specified, this is 512 bytes.
  BLOCK( ): The formula in brackets is rounded up using block boundary.
```

Example

The Symfoware Server Enterprise Extended Edition block length is 512 (in bytes), and the transaction entry number is 256

```
Temporary log index area = 512 + 2 x BLOCK(248 x 256 + 304)
                             = 512 + 2 x 64,000
                             = 128,512 (in bytes)
```

Transaction Update Data Amount and Concurrency

For details about the transaction update data amount, refer to "D.1.4 Estimation Formula for Log Capacity" and then estimate the amount.

Estimate the transaction concurrency according to the maximum number of transactions executed simultaneously.

Create a temporary log file using less than 16G bytes.

If there is a large fluctuation between transactions collected in the log, the incidental error in this estimation formula will increase. For this reason, change the temporary log file if necessary.

If it is necessary to change the temporary log file capacity while the application is running, it can be changed using the rdblog command.

BI Log Area

Estimate the BI log area from the viewpoint of the transaction concurrency and the BI log capacity output by the transaction. If there is a large fluctuation between transactions collected in the log, the incidental error in this estimation formula will increase. For this reason, change the temporary log file if necessary.

If flush treatment recovery application is performed in a load share application, double the value for the estimation formula.

```
BI log area = Lb x Transaction entry number

  Lb: Maximum value for the transaction update log capacity (number of bytes)
```

Crash Recovery Time

This is the database recovery processing time used to restart Symfoware/RDB or for changeover extensions if there is a system crash while the database is running.

The target value for the restart time following a system crash (this may be a customer request, for example) until the crash recovery time must be investigated.

AI Log Area

As a general rule, the AI log area is decided based on the recovery log capacity. As a guide, the AI log area total size is approximately double the recovery log capacity.

If the AI total size is too small even when the recovery time is reduced, however, there is a danger that depletion will occur while the transaction is running. For this reason, the total size must not be equal to or less than the BI size capacity.

If flush treatment recovery application is performed in a load share application, double the value for the estimation formula.

```
X = Recovery log capacity x 2
Y = BI log area

AI log area = MAX(X,Y) (Select whichever of X or Y is greater)
```

If Advanced Backup Controller is used, the log capacity for the backup obtaining period is increased. Add the value calculated according to the estimation formula shown below to the AI log area.

If the calculated result is negative, there is no need to consider this log capacity.

```
AI log increment = O x P x n - R

  O: Number of writings in one database space per second (Note)
  P: Page length (Unit: Bytes)
  n: Database space number
  R: Recovery log capacity (Unit: Bytes)
```

Note: It is recommended that O is calculated using the sar command from the actual measurement data statistically. As a guide, the estimation stages are shown below.

Example

An example of the calculation is shown below.

```
O: Number of writings in one database space per second = 300 x 1 = 300
K: Update page number per transaction = 1
T: Average transaction amount per second = 300
P: Page length = 32,768 (32K bytes)
n: Database space number = 3
R: Recovery log capacity = 10,485,760 (10M bytes)

AI log increment = 300 x 32,768 x 3 - 10,485,760
          = 19,005,400 (approximately 19M bytes)
```

Recovery Log Capacity

Recovery log capacity affects the stationary performance and crash recovery time. The RDB system performs the writing from the database buffer to the disk at fixed intervals to maintain a fixed recovery log capacity.

If the recovery log capacity is low, the frequency of writing from the database buffer increases. For this reason, there is a possibility that the stationary performance will be adversely affected.

If the recovery log capacity is great, more crash recovery time will be needed.

Accordingly, if the emphasis is on stationary performance, make the crash recovery time increase the recovery log capacity until there is no problem in the application.

The calculation method for the crash recovery time is different if flush treatment recovery is used, however. This section describes scenarios in which flush treatment recovery is used, and is not used.

For details about flush treatment recovery, refer to the "Cluster Introduction Application Guide" in the Symfoware Server manual.

- Using Flush Treatment Recovery

  Estimate the crash recovery time using flush treatment recovery according to the formula shown below.

  Synchronized flush treatment recovery applications

  Estimate according to the formula shown below.

  ```
  Crash recovery time = Approximately every 5 seconds for recovery log capacity of 10M bytes
  ```

  Non Synchronized flush treatment recovery applications

  Estimate according to the formula shown below.

  ```
  Crash recovery time = Approximately every 3 seconds for recovery log capacity of 10M bytes
  ```

  The crash recovery time for the above non synchronized flush treatment recovery applications is the time for block processing for in-progress data. If cluster applications changeover and recovery executed in Non Synchronized is not completed, there is a possibility that access to the database will result in an error.

Estimate the time at which all data can be accessed according to the formula shown below.

- Flush Treatment Recovery is Used

  If recovery log capacity is not specified, the default is 512K bytes if the AI log capacity is 1.25M bytes or more, and 40% of the AI log area if the AI log capacity is 1.25M bytes or less. In this case, the crash recovery time is approximately 1 to 2 seconds.

  The initial settings for the crash recovery time assume from 5 to 15 seconds for each 10M bytes of recovery log capacity. The recovery log capacity and crash recovery time relationship, however, is greatly affected by disk performance and buffer size.

  Accordingly, to ensure accurate recovery log capacity reset the recovery log capacity using the -U, -t, and -c options of the rdblog command according to the actual measurement for the crash recovery time in the environment of the actual application.

D.1.8 Estimating Archive Log Files

The methods for estimating archive log files are shown below.

- Applications in which archive logs are backed up

- Applications in which archive logs are not backed up

The archive log file capacity depends on the application form, database update amount, and resource backup cycle. The resources required for backup are as follows:

- Database (backed up using the rdbdmp command)

- RDB dictionary (backed up using the rdbdmpdic command)

The update log must be retained in the archive log file from the point when the backup for the above resources is obtained until the next backup is obtained.

Estimate the archive log file capacity according to the result calculated for the archive log capacity per hour shown below to meet the requirements of the application.

```
Archive log capacity per hour = Archive log capacity for each transaction unit x Update entry number
per hour
```

For details about the archive log capacity for each transaction unit, refer to "D.1.4 Estimation Formula for Log Capacity".

Applications in which Archive Logs are Backed Up

There must be sufficient capacity for saving update data from the point when the backup for the archive log file is obtained until the next archive log file backup is obtained.

The archive log file backup is the same as the database difference backup.

For example, if the archive log file backup is performed on a daily basis, the archive log file capacity must be sufficient for saving at least one day's worth of update data. The database must be backed up regularly, even in this application.

If old archive logs are not destroyed even when the database is backed up regularly, there is a possibility that the archive log for recovering the database is enlarged and the database recovery time is prolonged.

Applications in which Archive Logs are not Backed Up

There must be sufficient capacity for saving update data from the point when the backup for the database is obtained until the next backup is obtained.

For example, if database backup is performed once weekly, there must be sufficient capacity for saving update data at least once weekly.

D.1.9 Estimation Formula for in Doubt Log Files

The estimation formula for in doubt log files is shown below.

```
in doubt log files = Lb x (Maximum thread number + 1) x 4 (in bytes)

Lb: Maximum value for the transaction update data amount (number of bytes)
```

For details about the maximum value for the transaction update data amount, refer to "D.1.4 Estimation Formula for Log Capacity".

D.1.10 Estimating the Work Area

A work disk is required for database application and operation in the following cases:

- Input file and output file for RDB commands and applications
- Work area used for RDB commands and internal processing of SQL statements

The required work area (disk capacity) for database application and operation is given below. RDB commands executed simultaneously, input files, output files used in the applications, and work areas used in internal processing of SQL statements are all totals.

```
Work area = (RDB command and application input file total
              + RDB command and application output file total
              + Total work area used for RDB commands and internal processing of SQL statements) x r

  r: Safety margin (1.5 or more)
```

Input File and Output File for RDB Commands and Applications

Estimate the size of the input and output files shown below.

- Data files for database creation (load file)
- Data files extracted from the database (unload file)
- DSI backup files for media recovery
- Archive log files for recovery
- Core files when Symfoware/RDB crashes
- RDB report files for Symfoware/RDB message output
- Files used by applications

Input/output file	Estimation Contents
Load file	Estimate this using the table DSI capacity. The work area depends on the load file retained and processed on the disk.
Unload file	Estimate this using the table DSI capacity. The work area depends on the unload file retained on the disk.
Backup file	Estimate this using the table DSI capacity. If all the backup data is retained on the disk, total DSI capacity is used. If the backup data is backed up using a tape mechanism, the size for the temporarily retained backup data file is used.
Archive log file	The archive log file must be retained on all disks before media recovery is performed. Accordingly, if the archive log file is backed up and run using a tape mechanism, the disk capacity for the archive log file size is required.
Core file	This is the core file for investigation output when an abnormality occurs in Symfoware/RDB causing it to crash. This can be estimated using the memory capacity used by Symfoware/RDB and the commands. The maximum amount is the total for the memory capacity and swap area implemented on the server.
RDB report file	This is the file for error and information messages output in Symfoware/RDB. The amount is double that used for the size specified for RDBREPORTSIZE in the RDB configuration parameter file.
Application input/output file	Estimate the input/output file size for each application.

Work Area Used for RDB Commands and Internal Processing of SQL Statements

In for RDB command and SQL statement processing, the work area used internally changes according to the processed data amount. If the work area is small, only the memory is used and processed. If the work area is large, however, the disk is used automatically. Estimate the work area used as shown below.

Symfoware/RDB processing	Estimation Contents
Database creation-type commands - rdbsloader - rdbsaloader	This is the work area required to sort the index DSI. Estimate this using the index DSI capacity. If this is executed for concurrency, add it to each work area.
Database update-type commands - rdbsuloader	Estimate this using the table DSI capacity. If this is executed for concurrency, add it to each work area.
Database reconfiguration commands - rdbgcdsi	Estimate this using the table DSI capacity. If this is executed for concurrency, add it to each work area.
RDB dictionary reconfiguration commands rdbgcdic	Estimate this using the RDB dictionary capacity.
Database media recovery - rdbadjrcv - rdbmrrcv - rdbrcv - rdbrcvdic	Estimate this using the larger of the AI log area capacity or index DSI capacity. For rdbadjrcv, calculate an amount double that used for the AI log area capacity. If this is executed for concurrency, add it to each work area.
Optimization information settings - rdbups	This is the work area required to sort the index DSI. Estimate this using the index DSI capacity. If this is executed for concurrency, add it to each work area.
Execution of SQL statements - rdbunlsql	To execute SQL statements, a work area is required for retaining processing data and for sort processing temporarily. Although it is difficult to estimate the work area used for executing SQL statements, estimate this based on the SQL statement search result. Work area = SQL statement search result x 2 x Concurrency

For details about the estimation formula for the AI log area, refer to "D.1.7 Estimation Formula for Temporary Log Files".

D.1.11 Estimation Formula for Audit Logs

Estimating for Each Element

The information obtained in the audit log database is as follows:

- Information for executing user applications
- Information for accessing user resources
- Information for maintaining and running systems as the administrator
- Information for abnormal events detected in the system

The estimation formula for this information is shown below.

- **Estimating information for executing user applications**

  The total of connection occurrences and closures per hour is assumed. The amount in Interstage Directory Service is shown below.

```
A: Information for executing user applications = 340 x (Maximum thread number + 1) x Number of
repositories (in bytes)
```

- **Estimating information for accessing user resources**

  The number of all SQL statements executed per hour is assumed. This is calculated according to the estimation formula shown below.

```
B: Information for accessing user resources = 5,635 x Entry update number per hour + 805 Entry
search number per hour (in bytes)
```

- **Estimating information for maintaining and running systems as the administrator**

  The number of RDB command and SQL statements executed by the administrator per hour is assumed. This is calculated according to the estimation formula shown below.

```
C: Information for maintaining and running systems as the administrator = 9,548 x Entry update
number per hour + 1,346 x Entry search number per hour (in bytes)
```

- **Estimating information for abnormal events detected in the system**

  This is specified according to the error events that occur per hour. The minimum value is 10,000 bytes.

```
D: Information for abnormal events detected in the system = 10,000 (in bytes)
```

Audit Log Element Size

The value multiplied by the escape interval required for the audit log element capacity per hour is the audit log element size specified using the rdbaudit command.

If the escape interval is H (time), the audit log element size that is provided is as follows:

```
Audit log element size = (A + B + C + D + 10,000) x H (in bytes)
```

D.2 Estimating Memory Requirements

This section explains the memory required for the repository database, as part of the memory required by the RDB system.

The rough estimate is given by the following formula:

```
RDB system memory capacity    (Note 1)
      = Initial amount
       + Fluctuating memory capacity specified in the RDB configuration parameter file
       + Fluctuating memory capacity in the RDB system configuration
       + Shared memory size
       + Shared buffer size
       + Default buffer size
       + Application memory capacity
       + Database access memory capacity
       + Load share application memory capacity    (Note 2)
       + Audit log application memory capacity
```

Notes

1. In fail-over applications, the amount of memory estimated for nodes used to deploy standby-type cluster applications is the same as the total estimated for nodes used to deploy application-type cluster applications.

2. This only needs to be estimated for load share applications.

3. If "K bytes" and "M bytes" is not specified, then the unit is "bytes".

D.2.1 Initial Amount

```
Initial amount
      = 2,150K bytes + 200K bytes x Loading CPU
        + 1K bytes x audit log log group number
```

Loading CPU

This is the logic CPU loaded in the processing mechanism.

Audit Log Log Group Number

If audit log control is not used, the audit log log group number is [0]. If it is used, the audit log log group number is [1].

D.2.2 Fluctuating Memory Capacity Specified in the RDB Configuration Parameter File

The rough estimate for the fluctuating memory capacity specified in the RDB configuration parameter file is given by the following formula:

```
Fluctuating memory capacity specified in the RDB configuration parameter file
      = Log buffer memory capacity
        + Database space I/O formula memory capacity
        + RDB dictionary memory residence memory capacity

    Log buffer memory capacity
          = (2,048K bytes + log buffer size) x log group number

        Log buffer size
              =(BI log buffer number + AI log buffer number) x block length

        Log group number
              = 1 + audit log log group number

    Database space I/O formula memory capacity
          = N x Loading CPU x 200K bytes
          + (1 - N) x database space reader/writer number x 500K bytes

    RDB dictionary memory residence memory capacity
          = 12K bytes + 4.5K bytes x RDB dictionary page number

        RDB dictionary page number = RDB dictionary capacity / 4,096
```

BI Log Buffer Number, AI Log Buffer Number

These are the temporary log files log buffer numbers specified in the RDB configuration parameter file RDBLOG.

Block Length

This is the block length specified when temporary log files are created.

The block length is specified using the -io option of the rdblog command. If the -io option is omitted, it defaults to [512].

For details on how to specify the rdblog command, refer to "Command References" in the Symfoware Server manual.

Audit Log Log Group Number

If audit log control is not used, the audit log log group number is [0]. If it is used, the audit log log group number is [1].

Database Space I/O Formula Memory Capacity

If YES is specified for RDBASYNCIO in the RDB configuration parameter file, N is [1].

If NO is specified for RDBASYNCIO in the RDB configuration parameter file, N is [0]. In this case, the database space reader/writer number is the reader/writer number specified for RDBDBSNUM of the RDB configuration parameter file.

RDB Dictionary Memory Residence Memory Capacity

If YES is specified for RDBDICONBUFFER in the RDB configuration parameter file, then the RDB dictionary resides in the memory. In this case, estimate the amount of memory required by the RDB dictionary. Although the RDB directory file also resides in the memory, there is no need to estimate the amount of memory required by it.

If NO is specified for RDBDICONBUFFER in the RDB configuration parameter file, then the RDB dictionary does not reside in the memory. In this case, the amount of memory allocated for the RDB dictionary memory is [0] bytes.

If nothing is specified for RDBDICONBUFFER, it is assumed that NO was specified.

RDB Dictionary Capacity

This is the allocation amount (in bytes) specified when the RDB dictionary is created.

It is not the size of the raw device for deploying the RDB dictionary, but is the allocation amount specified using the -a option of the rdbcrdic command.

For details on how to specify the rdbcrdic command, refer to "Command References" in the Symfoware Server manual.

D.2.3 Fluctuating Memory Capacity in the RDB System Configuration

This is the fluctuating memory capacity in the RDB system configuration (log environment, database definition number, database capacity).

The rough estimate for the fluctuating memory capacity in the RDB system configuration is given by the following formula:

```
Fluctuating memory capacity in the RDB system configuration
      = 10,251K bytes
        + Fluctuating memory capacity in the database configuration

    Fluctuating memory capacity in the database configuration
          = RDB dictionary object information memory capacity (A)
```

(A) RDB dictionary object information memory capacity

This is the memory capacity used in the RDB dictionary object information.

The rough estimate for the RDB dictionary object information memory capacity is as follows:

```
RDB dictionary object information memory capacity
      = 20,276K bytes
```

D.2.4 Shared Memory Size

This is the shared memory size used by RDB processes for information exchange outside the process.

"Obtained in batch formula" is used as the formula for obtaining shared memory.

The "Obtained in batch formula" shared memory size is as follows:

```
"Obtained in batch formula" shared memory size = 3,520K bytes
```

D.2.5 Shared Buffer Size

This is the size of the shared buffer created using the rdbcrbf command.

For details on how to specify the rdbcrbf command, refer to "Command References" in the Symfoware Server manual.

The shared buffer size required for Interstage Directory Service applications is as follows:

```
Shared buffer size = 14.6M bytes
```

D.2.6 Default Buffer Size

This is the default shared buffer size.

Information for the default buffer is defined in the rdbbuf text file under the directory specified in RDBSYSBUF in the RDB configuration parameter file.

The default buffer is used for the following DSI access:

- RDB dictionary (system table DSI)
- Audit log database (database required for audit log control)
- DSI for which dependency with the shared buffer has not been registered using the rdbconbf command

The default buffer size is estimated by the following formula:

```
Default buffer size = 3,135K bytes + 3K bytes x audit log log group number
```

Audit log log group number

If audit log control is not used, the audit log log group number is [0]. If it is used, the log group number is [1].

D.2.7 Application Memory Capacity

This is the memory capacity obtained in the RDB process for executing requests from applications.

The rough estimate for the application memory capacity is as follows:

```
Application memory capacity = 3,407K bytes
```

D.2.8 Database Access Memory Capacity

This is the memory capacity obtained in the RDB process in accordance with database access from applications.

The database access memory capacity estimation target includes the DSI located in the RDB system. This DSI is shown in the DSI configured in the access target table (table and index DSI). (Table DSI and index DSI targets are defined under the RDB system)

The rough estimate for the database access memory capacity is given by the following formula:

```
Database access memory capacity
      = Exclusion information memory capacity (A)
        + index update information memory capacity (B)
```

(A) Exclusion Information Memory Capacity

This is the memory capacity used for database exclusion control.

The rough estimate for the exclusion information memory capacity is given by the following formula:

```
Exclusion information memory capacity
      = Total memory capacity used for each transaction unit that uses exclusion for each DSI unit
        + Total memory capacity used for each transaction unit that uses exclusion for each page unit
        + Total memory capacity used for each transaction unit that uses exclusion for each line unit

    Memory capacity used for each transaction unit that uses exclusion for each DSI unit
          = Access target DSI number x 128

    Memory capacity used for each transaction unit that uses exclusion for each page unit
          = Access target page number x 256

    Memory capacity used for each transaction unit that uses exclusion for each line unit
          = Access target record number x 256
            + key exclusion information memory capacity

        Key exclusion information memory capacity
```

```
              = Total key exclusion information memory capacity for each index DSI unit

            Key exclusion information memory capacity for each index DSI unit
                  = 2,068 + update key value number x 2,128

                Update key value number
                      = INSERT key value number
                        + UPDATE key value number
```

Total memory capacity used for each transaction unit that uses exclusion for each DSI unit

This is the aggregate memory capacity used for each transaction unit that uses exclusion for each DSI unit.

It provides the amount of memory used for each transaction unit that uses exclusion for each DSI unit, and calculates the total.

Total memory capacity used for each transaction unit that uses exclusion for each page unit

This is the aggregate memory capacity used for each transaction unit that uses exclusion for each page unit.

It provides the amount of memory used for each transaction unit that uses exclusion for each page unit, and calculates the total.

Total memory capacity used for each transaction unit that uses exclusion for each line unit

This is the aggregate memory capacity used for each transaction unit that uses exclusion for each line unit.

It provides the amount of memory used for each transaction unit that uses exclusion for each line unit, and calculates the total.

Access target DSI number

This is the DSI number accessed in the transaction. (The table and index DSI number total)

Access target page number

This is the page number accessed in the transaction. (The table and index page number total)

It is difficult to estimate the page number accessed. It is, therefore, recommended that you estimate memory as an exclusion for each line unit, even if there is a page unit exclusion. It can be expected that the estimate for the line unit exclusion will be greater than for the page unit exclusion, but it is safer to estimate a greater amount.

Access target record number

This is the record (line) number accessed in the transaction. (The table record (line) number)

Total key exclusion information memory capacity for each index DSI unit

This is the aggregate key exclusion information memory capacity for each index DSI unit.

It provides the amount of key exclusion information memory used for each index DSI unit updated in the transaction that uses the line unit exclusion, and calculates the total.

Update key value number

This is the index DSI update key value number.

It is the total of the INSERT key value number and UPDATE key value number.

The DELETE key value number is not included in the update key value number in the key exclusion information.

(B) Index Update Information Memory Capacity

This is the memory capacity used when the index key value is updated and line unit exclusion is used.

The rough estimate for the index update information memory capacity is given by the following formula:

If using an XML structure index, for "BTREE structure data part page length" read "XML structure data part page length".

For details on estimating both the update work index part page number and update work data part page number, refer to "RDB Application Guide (XML Adapter Edition)" - "Estimating XML data index capacity" in the Symfoware Server manual.

```
Index update information memory capacity
      = Total index update information memory capacity for each transaction unit

    Index update information memory capacity for each transaction unit
          = Total index update information memory capacity for each index DSI unit
```

```
        Index update information memory capacity for each index DSI unit
              = update work index part page number
                x (150 + BTREE structure data part page length)
                + update work data part page number
                x (150 + BTREE structure data part page length)
```

Total index update information memory capacity for each transaction unit

This is the aggregate index update information memory capacity for each transaction unit.

It provides the amount of index update information memory used for each transaction unit that uses exclusion for each line unit, and calculates the total.

Total index update information memory capacity for each index DSI unit

This is the aggregate index update information memory capacity for each index DSI unit.

It provides the amount of index update information memory used for each transaction unit that uses exclusion for each index DSI unit, and calculates the total.

Update work index part page number

This is the update work index part page buffer number.

Refer to "Estimating the database space" - "BTREE structure index part" in the "RDB Application Guide (Database Definition Edition)" of the Symfoware Server manual, and then estimate the update work index part page number.

Calculate "data part page number" using "update work data part page number", and the "index part page length" using "BTREE structure data part page length".

```
Update key value number
     = INSERT key value number + UPDATE key value number x 2
      + DELETE key value number
```

BTREE structure data part page length

This is the index DSI (BTREE structure) data part page length (in bytes).

The update work index part page length and update work data part page length together form the index DSI (BTREE structure) data part page length.

Update key value number

This is the index DSI update key value number.

It is the result of adding the INSERT key value number, UPDATE key value number x 2, and DELETE key value number.

D.2.9 Load Share Application Memory Capacity

This is the amount of memory obtained in the RDB process used to run load share applications.

The rough estimate for the load share application memory capacity is given by the following formula:

```
Load share application memory capacity
      = 200K bytes
        + flush treatment recovery memory capacity  ..(A)
        + Remote access memory capacity                 ..(B)
        + Database access memory capacity             ..(C)
```

(A) Flush Treatment Recovery Memory Capacity

This is the amount of memory obtained in the RDB process if flush treatment recovery is used. The RDB system running in the application node can immediately be inherited to a standby node if a changeover event (such as a node crash) occurs.

The rough estimate for the flush treatment recovery memory capacity is given by the following formula:

```
Flush treatment recovery memory capacity
      = Total memory capacity for flush treatment recovery for each log group unit
```

```
    Flush treatment recovery memory capacity for each log group unit
          = BI log area + MIN (AI log area, recovery log capacity x 2)
```

Total memory capacity for flush treatment recovery for each log group unit

This is the aggregate flush treatment recovery memory capacity for each log group unit.

It provides the amount of flush treatment recovery memory for each log group unit, and calculates the total.

Log groups are as follows:

- System log group (one log group in the RDB system)
- User log group (log group defined additionally for running scalable log applications)

- **BI log area**

  This is the BI log area specified when a temporary log file is created for the log group.

- **AI log area**

  This is the AI log area specified when a temporary log file is created for the log group.

- **Recovery log capacity**

  This is the recovery log capacity specified when a temporary log file is created for the log group.

- **MIN (AI log area, recovery log capacity x 2)**

  "AI log area" and "recovery log capacity x 2" are compared, and the smaller value is used for the estimate.

(B) Remote Access Memory Capacity

This is the amount of memory obtained in the RDB process for making requests from applications connected to other RDB systems.

The rough estimate for the remote access memory capacity is given by the following formula:

```
Remote access memory capacity
      = Total memory capacity for each remote access unit

    Memory capacity for each remote access unit
          = 0.7M bytes
           + Total memory capacity for each access target table unit
           + Memory capacity for table access including BLOB type columns
           + Processing procedure storage buffer size
           + Work area
           + Sort area

        Memory capacity for each access target table unit
              = 10K bytes
                + (table DSO number + index DSO number) x 9K bytes
                + table DSI number located in the RDB system x 250
                + division number x 704
                + DSI number located in the RDB system x 2,400

            table DSO number = 1

        Memory capacity for table access including BLOB type columns
              = Total memory capacity for each table unit containing BLOB type columns

            Memory capacity for each table unit containing BLOB type columns
                  = Average data length for the BLOB type column
```

Total memory capacity for each remote access unit

This is the aggregate memory capacity for each remote access unit.

It provides the amount of memory for each remote access unit and calculates the remote access memory capacity total that occurs simultaneously in the RDB system.

Total memory capacity for each access target table unit

This is the aggregate memory capacity for each access target table unit.

It provides the amount of memory for each access target table unit, and calculates the total.

Index DSO number

This is the index DSO number defined in the table.

Table DSI number located in the RDB system

This is the table DSI number of the DSI configured in the table in the RDB system. (Table DSI targets are defined under the RDB system)

Division number

This is the table division number (DSI division number).

DSI number located in the RDB system

This is the DSI number for the DSI (table and index DSI) configured in the table in the RDB system. (Table DSI and index DSI targets are defined under the RDB system)

Memory capacity for table access including BLOB type columns

If there is no access to tables including BLOB type columns, the memory capacity for table access including BLOB type columns is [0] bytes.

If there is access to tables including BLOB type columns, estimate the amount of memory required for table access, including BLOB type columns.

Total memory capacity for each table unit containing BLOB type columns

This is the aggregate memory capacity for each table unit containing BLOB type columns.

It provides the amount of memory for each table unit containing BLOB type columns, and calculates the total.

Average data length for the BLOB type column

This is the average data length (in bytes) for the BLOB type column in the table.

It provides the average data length for each column unit if more than one BLOB type column is defined for the table, and also calculates the total.

Buffer size for storage of the processing procedure (default= 256K bytes)

This is the buffer size for storing the SQL processing procedure.

The buffer size is specified in OPL_BUFFER_SIZE in the client or server operating environment file.

The value specified in the remote access source operating environment file is inherited.

For details about estimating the buffer size for storage of the processing procedure, refer to "D.2.7 Application Memory Capacity", "Buffer size for storage of the processing procedure".

Work area (default= 64K bytes)

This is the memory used as the work area (work table). It is specified in WORK_MEM_SIZE in the client or server operating environment file.

The value specified in the remote access source operating environment file is inherited.

For example, it is used to move the cursor in the direction specified for SCROLL of the cursor declaration, or to use sub-queries. It can also be used for other work area purposes.

Sort area (default= 2,112K bytes)

This is the memory used as the work area for sort processing. It is specified in SORT_MEM_SIZE in the client or server operating environment file.

The value specified in the remote access source operating environment file is inherited, and is used to issue SQL statements that require the sort area.

This includes the following SQL:

- ORDER BY
- GROUP BY
- UNION
- JOIN

(C) Database access memory capacity

For details, refer to "D.2.8 Database Access Memory Capacity".

D.2.10 Audit Log Application Memory Capacity

This is the amount of Symfoware/memory obtained in the RDB process for running audit log applications.

The rough estimate for the audit log application memory capacity is given by the following formula:.

```
Audit log application memory capacity
      = Memory capacity for audit log control

    Memory capacity for audit log control
          = 4M bytes + Memory capacity for audit log database management information

        Memory capacity for audit log database management information (M bytes)
             = (raw device number for deploying the audit log database x 3.1
               + audit log element number x 7.5
               + audit log database page assignment information x 2.1)/ 512
            audit log database page assignment information
                 = audit log database page number / 5,632
                audit log database page number
                      = 41.6 x audit log element number
                        x audit log element size (M bytes)
```

Memory capacity for audit log control

If audit log control is not used, the memory capacity for audit log control is [0] bytes. If it is used, estimate the amount of memory required for audit log control.

Memory capacity for audit log database management information (M bytes)

The result of the division is rounded up so that the numbers after the decimal point are lost.

Raw device number for deploying the audit log database

This is the raw device number for deploying the audit log database.

Audit log element number

This is the defined audit log element number.

Audit log database page assignment information

The result of the calculation (division) of the audit log database page assignment information is rounded up so that the numbers after the decimal point are lost.

The result of the calculation (division) of the audit log database page assignment information is also rounded up to the audit log element number if it is less than the audit log element number.

Audit log database page number

The result of the calculation of the audit log database page number is rounded up so that the numbers after the decimal point are lost.

Audit log element size (M bytes)

This is the defined audit log element size (M bytes). It is not the size of the raw device for deploying the audit log database, but. is the element size specified using the -s option of the rdbaudit command.

Appendix E Estimating Resources for Oracle Databases

This appendix explains how to estimate the various resources used by the Oracle database that are required to operate the Interstage Directory Service.

Refer to the Oracle database manual for more information on the items that need to be estimated, and for information about resource estimation methods that are not described in this manual.

E.1 Estimating Disk Space

This section explains the disk space required for the repository database, as part of the disk space required by the Oracle database.

E.1.1 Estimating Table Spaces (TABLESPACE)

If detailed settings are not made for tables

If detailed settings are not made for tables when the tables for storing repository data are created, the table space (TABLESPACE) required by the repository is calculated using the estimation formula shown below.

Note also that the table space required by the repository is 100 MB if no more than 1,000 entries are to be registered in the repository. In this case there is no need to make calculations using the estimation formula.

```
Table space(K bytes) = ( 82.5 x number of registered entries + 1,200 ) x r
  r : Safety factor (1.2 or more)
  (*1)(*2)
```

1K byte is 1,024 bytes.

*1 Correct the calculated database space so that it is a multiple of 32K bytes.

*2 Round the result of the calculation up to the nearest whole number.

If detailed settings are made for tables

If detailed settings are made for tables when the tables for storing repository data are created, the table space required by the repository is calculated using the estimation formula shown below.

```
Table space(K bytes) = ( T + I ) x r
  T : Table size(K bytes)
  I : Index size(K bytes)
  r : Safety factor (1.2 or more)
  (*1)(*2)
```

1K byte is 1,024 bytes.

*1 Correct the calculated database space so that it is a multiple of 32K bytes.

*2 Round the result of the calculation up to the nearest whole number.

Table Size

```
(Table size for DS_SCOPE(K bytes) + Table size for DS_FILTER(K bytes) + Table size for DS_ENTRY(K
bytes) + Size of the LOB table(K bytes) )
```

Table Size for DS_SCOPE, DS_FILTER and DS_ENTRY

Use the following formula to calculate the table space for each table that is to be specified when detailed settings are made for tables.

```
Table size(K bytes) = ( Bn x Bs ) / 1,024
  Bn : Assumed number of blocks
  Bs : Block size(bytes)
  (*1)
```

*1 Round the result of the calculation up to the nearest whole number.

Assumed Number of Blocks

If the average record length is smaller than the size of the data storage part for blocks:

```
Assumed number of records / Number of records that will fit in one block
```

Round the result up to the nearest whole number.

If the average record length is larger than the size of the data storage part for blocks:

```
(Average record length(bytes) / Size of the data storage part for blocks(bytes) ) x Assumed
number of records
```

Round the result up to the nearest whole number.

Assumed Number of Records

Assumed number of records for DS_SCOPE:

```
Number of registered entries
```

Assumed number of records for DS_FILTER:

```
Number of registered entries x Average number of attributes per entry
```

Assumed number of records for DS_ENTRY:

```
Number of registered entries x (Average number of attributes per entry + 1)
```

Assumed number of records for the LOB table:

```
Total number of binary-type attributes for all entries
```

Average Record Length

Average record length for DS_SCOPE:

```
Average length of text data(bytes) x 2 + 62
```

Average record length for DS_FILTER:

```
Average length of text data(bytes) + 92
```

Average record length for DS_ENTRY:

```
Average length of text data(bytes) + 100
```

Average Length of Text Data

```
Total length of string-type attribute values for all entries(bytes) / Total number of string-
type attributes for all entries
```

Round the result up to the nearest whole number.

Average Length for Binary Data (LOB)

```
Total size of binary-type attribute values for all entries(bytes) / Total number of binary-type
attributes for all entries
```

Round the result up to the nearest whole number.

Block Size

```
The block size (for the table space) that is specified when the database is created.
```

The default value used when databases are created is 8,192 bytes.

Number of Records that will Fit in One Block/ Size of the Data Storage Part for Blocks

Calculate "the number of records that will fit in one block", and "the size of the data storage part for blocks" for each table (DS_SCOPE, DS_FILTER and DS_ENTRY). To do so, use the variable information above and the fixed information below, and refer to information on the physical design for Oracle databases, table design or estimating table size.

INITRANS	1
PCTFREE	10%

Size of the LOB Table

Calculate "the number of records that will fit in one block", "the size of the data storage part for blocks" and "the size of the LOB table". To do so, use the variable information above and the fixed information below, and refer to information on the physical design for Oracle databases, table design or estimating table size.

Binary storage method	DISABLE IN LOW
CHUNK	Size of each block
RETENTION(PCTVERSION) area	About 20% of the LOB storage area

Note that the "Size of the LOB table" does not need to be defined in the detailed definition file when detailed settings are made for tables.

Index Size

```
( Size of each index for DS_SCOPE(K bytes) + Size of each index for DS_FILTER(K bytes) + Size of
each index for DS_ENTRY(K bytes) )
```

Index Size for DS_SCOPE, DS_FILTER and DS_ENTRY

Use the following formula to calculate the size of each index for each table that is specified when detailed settings are made.

```
Index size(K bytes) = (Bn x Bs) / 1,024
  Bn : Assumed number of blocks
  Bs : Block size(bytes)
  (*1)
```

*1 Round the result of the calculation up to the nearest whole number.

Assumed Number of Blocks

If the average record length is smaller than the size of the data storage part for blocks:

```
( Assumed number of records x 1.05 ) / Number of records that will fit in one block
```

Round the result up to the nearest whole number.

If the average record length is larger than the size of the data storage part for blocks:

```
(Average record length(bytes) / Size of the data storage part for blocks(bytes) ) x ( Assumed
number of records x 1.05 )
```

Round the result up to the nearest whole number.

Assumed Number of Records

Assumed number of records for DS_SCOPE:

```
Number of registered entries
```

Assumed number of records for DS_FILTER:

```
Number of registered entries x Average number of attributes per entry
```

Assumed number of records for DS_ENTRY:

```
Number of registered entries x (Average number of attributes per entry + 1 )
```

Average Record Length

Use the following formula to calculate the average record length for each index of each table.

Table E.1 Formulae to calculate average record length of index

Table name	Index	Average record length(bytes)
DS_SCOPE	Index 1	25
	Index 2	45
	Index 3	Average length of text data + 30
	Index 4	Average length of text data + 30
	Index 5	25
DS_FILTER	Index 1	25
	Index 2	84
	Index 3	Average length of text data + 58
	Index 4	61
	Index 5	Average length of text data + 58
	Index 6	61
DS_ENTRY	Index 1	25
	Index 2	53

Average Length of Text Data

```
Total length of string-type attribute values for all entries(bytes) / Total number of string-
type attributes for all entries
```

Round the result up to the nearest whole number.

Block Size

```
The block size (for the table space) that is specified when the database is created.
```

The default value used when databases are created is 8,192 bytes.

Number of Records that will Fit in One Block/ Size of the Data Storage Part for Blocks

Calculate "the number of records that will fit in one block" and "the size of the data storage part for blocks" for each index of each table (DS_SCOPE, DS_FILTER and DS_ENTRY). To do so, use the variable information above and the fixed information below, and refer to information on the physical design for Oracle databases, index design or estimating size of indexes.

INITRANS	2
PCTFREE	10%