

z/OS



Managed System Infrastructure for Setup Installation

Version 1 Release 4

z/OS



Managed System Infrastructure for Setup Installation

Version 1 Release 4

Note!

Before using this information and the product it supports, be sure to read the general information under "Notices" on page 61.

First Edition (September 2002)

This edition applies to Version 1 Release 4 of z/OS™ (product number 5694-A01), and Version 1 Release 4 of z/OS.e (product number 5655-G52), and to all subsequent releases and modifications until otherwise indicated in new editions.

Order publications through your IBM® representative or the IBM branch office serving your locality. Publications are not stocked at the address given below.

A form for readers' comments appears at the back of this publication. If the form has been removed, address your comments to:

IBM Deutschland Entwicklung GmbH
Department 3248
Schoenaicher Strasse 220
D-71032 Boeblingen
Federal Republic of Germany

Internet e-mail: s390id@de.ibm.com
z/OS Web site: <http://www.ibm.com/servers/eserver/zseries/zos/>

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© Copyright International Business Machines Corporation 2002. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About this document	v
Who should read this document.	v
How to use this document.	v

Part 1. Planning for installing msys for Setup. 1

Chapter 1. Which parts make up msys for Setup?. 3

The host code	3
The workplace.	3
The management directory	4

Chapter 2. Setup environments. 7

Communications	7
Connections	7
Secure socket layer	8
Firewalls.	8
Example of a simplified environment	8
System integrity	9
Maintaining multiple subtrees	9

Chapter 3. System requirements. 11

z/OS system requirements	11
Security	12
LDAP server requirements	12
msys for Setup workplace requirements	13

Part 2. Installing msys for Setup . . 15

Chapter 4. Installing the z/OS system 17

Coexistence with pre-V1R4 z/OS system	17
Restrictions for z/OS systems	18
Minimum configuration	18
Parmlib restrictions.	18

Chapter 5. Setting up an LDAP server 21

Adapting the LDAP profile files	21
Processing the profile files	22
Steps for processing the profile files	22
Modifying the schema entry for the TDBM backend 23	
Steps for modifying the schema entry for the TDBM backend	24
What is different without RACF?	25
Password encryption	26

Chapter 6. Preparing the z/OS system for msys for Setup 27

Authorizing the Java DLLs	27
Steps for restricting access to the authorized DLLs	27
Steps for authorizing the Java DLLs	28

Setting up z/OS UNIX System Services for msys for Setup users	29
Choosing a JES job class	29
Verifying the communications	29
Assuring that the MIGLIB is authorized and accessible	29
Authorizing the msys for Setup users.	30

Chapter 7. Setting up the msys for Setup workplace 33

Ensuring that the workstation is defined to TCP/IP 33	
Steps for assigning a host name to a Windows NT workstation	33
Steps for assigning a host name to a Windows 2000 workstation	34
Verifying the TCP/IP connection to the LDAP server 34	
Downloading the workplace.	34
Steps for downloading the workplace code with FTP	35
Steps for downloading the workplace code with your Web browser	35
Installing the workplace on your workstation . . . 36	
Starting the workplace.	36

Chapter 8. Creating a new management directory subtree 39

What you need to know about the management directory	39
What is a suffix and what can it contain? . . . 39	
Where can an msys for Setup management directory subtree be located	40
Recommendations	42
Creating the subtree	42
Overview of the panel flow for creating the subtree	42
Steps for creating the subtree	43

Part 3. Maintenance 45

Chapter 9. Migrating from a prior msys for Setup release 47

Migrating the management directory to V1R4 . . . 47	
LDAP server requirements	47
Guidelines and restrictions for migrating your management directory structure	47
Migrating the management directory	48
Migration actions for your z/OS systems	49
Reinstalling the workplace	49

Chapter 10. Applying service to msys for Setup. 51

What to service	51
How to prepare for service?.	51

Where to get service	51
Servicing the workplace	51
Steps for accessing the management directory after deinstalling a PTF	52
Keeping the LDAP schema up to date	52

Part 4. Appendixes. 53

**Appendix A. LDAP connection
worksheet 55**

**Appendix B. Worksheet for editing the
LDAP profile files 57**

**Appendix C. Worksheet for product set
installation data 59**

Notices	61
Trademarks	62

Where to find more information 63

Managed System Infrastructure for Setup publications	63
Related z/OS publications	63
Accessing Books on the Internet	63
Accessing z/OS licensed documents on the Internet	64
Using LookAt to look up message explanations . .	64

Index 67

About this document

This document provides information you need to install Managed System Infrastructure for Setup (msys for Setup). In previous z/OS releases, this information had been included in *z/OS Managed System Infrastructure for Setup User's Guide*.

After reading this document, you will understand:

- How to plan for msys for Setup
- How to install msys for Setup
- How to service msys for Setup

For a general introduction to msys for Setup refer to *z/OS Managed System Infrastructure for Setup User's Guide*.

This document assumes that you are familiar with, or have access to a person who is familiar with:

- z/OS
- z/OS Security Server RACF®
- DB2®
- eNetwork Communication Server for z/OS/IP (TCP/IP) and its FTP Server
- CustomPac¹
- Windows NT® or Windows® 2000 Professional

This document further assumes that you have some conceptual knowledge of the Lightweight Directory Access Protocol (LDAP) although you do not need to be an expert.

Note: References to z/OS apply to all available versions and releases of z/OS and z/OS.e, unless the reference states a specific version or release.

Who should read this document

This document is intended for all persons involved in installing and customizing Managed System Infrastructure for Setup and its prerequisite and co-requisite products.

This includes:

- z/OS system programmers
- Database administrators, in particular LDAP and DB2 administrators
- Security administrators

For convenience, this document refers to all these persons as *administrators*.

How to use this document

Use this document to plan for, install, and prepare msys for Setup for use.

1. CustomPac is a generic term that comprises ServerPac, SystemPac®, ProductPac®, and FunctionPac®

Part 1, “Planning for installing msys for Setup” on page 1 provides information that helps you to plan for msys for Setup.

Part 2, “Installing msys for Setup” on page 15 gives guidance and detailed instructions for installing and customizing msys for Setup.

Part 3, “Maintenance” on page 45 tells you what you need to know to apply service to msys for Setup and what to do when you install a new version of z/OS.

Before you start working with this document you should familiarize yourself with the introduction to msys for Setup that is provided in *z/OS Managed System Infrastructure for Setup User’s Guide*. The user’s guide provides information on:

- What you can do with msys for Setup
- How to customize other products with msys for Setup
- Definitions of msys for Setup specific terms

Part 1. Planning for installing msys for Setup

This part provides an overview of the parts of msys for Setup that you have to install and of the systems they run on. It also provides information that helps you to plan for the required communications and for security.

Chapter 1. Which parts make up msys for Setup?

You must set up the three main components of msys for Setup:

- The msys for Setup host code
- The msys for Setup workplace
- An LDAP server to accommodate the management directory

The host code

The msys for Setup host code provides a framework that invokes product specific plug-ins (supporting services). The plug-ins are provided by msys for Setup enabled products. The host framework provides, for example:

- Communication with the msys for Setup workplace
- Communication with the management directory
- Control and coordination of the host plug-ins

The host plug-ins provide functions to update configuration resources according to the configuration data that msys for Setup users enter on the workplace. The framework provides the host plug-ins with the required data, for example, where the configuration resource resides and which configuration data to use.

Where to install it?

The msys for Setup host code runs on each z/OS system that is to be customized with the help of msys for Setup.

It resides in the z/OS UNIX System Services hierarchical file system (HFS) at /usr/lpp/cim. After installing the CustomPac it is already in the HFS at the required location. z/OS systems that share the HFS also share the host code.

Where to get it?

msys for Setup is a base element of z/OS. You do not need to order it separately. It is included in your z/OS CustomPac order (see Chapter 4, "Installing the z/OS system" on page 17).

The workplace

The msys for Setup workplace is the interface through which administrators work with z/OS systems. Administrators can customize products through the workplace without directly logging on to the z/OS system where the product is installed. The workplace also provides a framework that is used by msys for Setup enabled products. The workplace provides, for example:

- A platform for running the customization dialogs that are provided by msys for Setup enabled products
- Communication with the z/OS systems
- Communication with the management directory

Where to install it?

The msys for Setup workplace code runs on a Windows NT or Windows 200 workstation. You can have multiple workstations with the workplace code. The workplace code must be at least at the same level as the host code it communicates with.

Where to get it?

The msys for Setup workplace code is provided as a self-extracting file that is included in the host code. The file is called cimsetup.exe and resides in HFS directory /usr/lpp/cim.

See “Downloading the workplace” on page 34 for details.

The management directory

The management directory is msys for Setup’s central data repository for data on all z/OS systems to be customized. It is based on the Lightweight Directory Access Protocol (LDAP) support available as part of z/OS or OS/390®.

LDAP is an access method that provides a tree view of the accessed data. It does not physically hold the data but relies on backends that implement access to a persistent storage mechanism. msys for Setup can use two backends that connect LDAP to databases. Only one LDAP server system with one IP address is required for both backends.

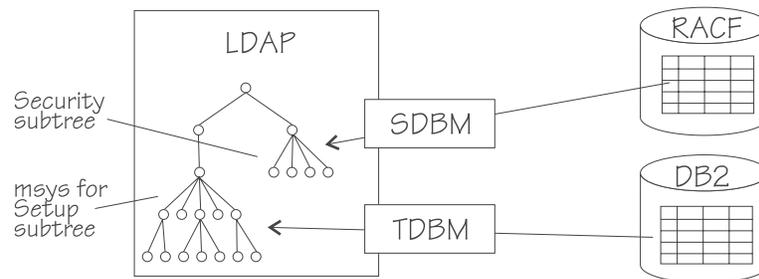


Figure 1. LDAP with backends

TDBM is required. It implements access to a DB2 database. The data for the msys for Setup management directory subtree resides in the DB2 database and is accessed through TDBM. The entire msys for Setup subtree must reside on one DB2 database.

SDBM is optionally available if you are using RACF for security. It implements access to a RACF database. You can use RACF for authenticating msys for Setup users.

For information on the structure of the management directory see “What you need to know about the management directory” on page 39.

Where to install it?

The LDAP server that provides access to the management directory can run on any z/OS or OS/390 R10 system to which both the workstation and the host have TCP/IP connectivity.. This can be one of the z/OS systems to be customized with msys for Setup. The DB2 subsystem that holds the management directory data and the RACF database must reside on this system.

Where to get it?

The required level of LDAP is included in z/OS or OS/390 R10.

The LDAP server is packaged as part of the Security Server Optional Feature. However, it is licensed with OS/390 and z/OS. The LDAP server can be used without enabling the Security Server Optional Feature.

You can use an existing DB2 subsystem. If you do not have the DB2 product installed, you must order one separately (see also “LDAP server requirements” on page 12). Setting up DB2 is beyond the scope of this document. Refer to *DB2 Installation Guide* if you need to set up DB2.

Chapter 2. Setup environments

This section explains what a basic msys for Setup system environment consists of and which variations are possible.

- “Communications” shows on a simplified example how you must connect the basic components.
- “Example of a simplified environment” on page 8 shows a more realistic example for a small installation.
- “Maintaining multiple subtrees” on page 9 explains what you must observe if you maintain multiple management directory subtrees.

Communications

The simplest possible msys for Setup system environment includes:

- A z/OS system with the host code
- A workstation with the msys for Setup workplace
- An LDAP server with a management directory

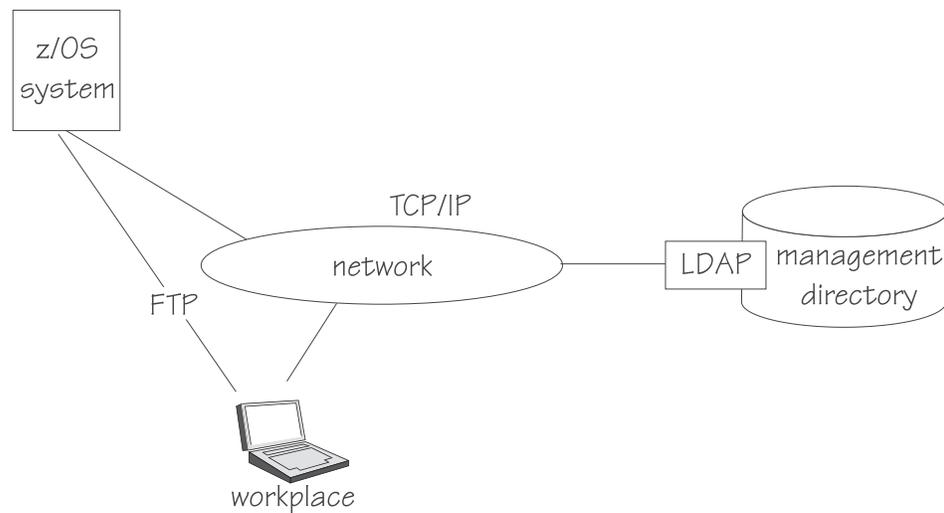


Figure 2. Basic msys for Setup system environment

Connections

You need a TCP/IP connection from the workplace to the LDAP server.

You need an FTP connection from the workplace to the z/OS system to be customized. On the z/OS system the FTPD server must be running and configured for remote job submission.

The z/OS system to be customized must have a TCP/IP connection to the LDAP server.

Secure socket layer

Secure socket layer (SSL)-encrypted communication is not supported in the current release of msys for Setup. msys for Setup uses non-secure socket layer (non-SSL) LDAP as well as FTP protocols that send passwords unencrypted using the TCP/IP protocol.

Recommendation: Use msys for Setup only in a secure intranet environment.

Firewalls

Firewalls can prevent messages from being transmitted from a z/OS system to the workplace. As a consequence, the workplace user cannot receive any job notifications.

For workstation firewalls, ensure that you allow the host to connect via a TCP socket connection to port 1999.

Example of a simplified environment

One of the benefits of msys for Setup is that it simplifies setting up a sysplex. Therefore, a typical environment includes multiple, often a large number, of z/OS systems.

You can also have multiple workplaces so that different workplace users can perform different tasks simultaneously, for example, work with different z/OS systems in the environment, or customize different products for the same system.

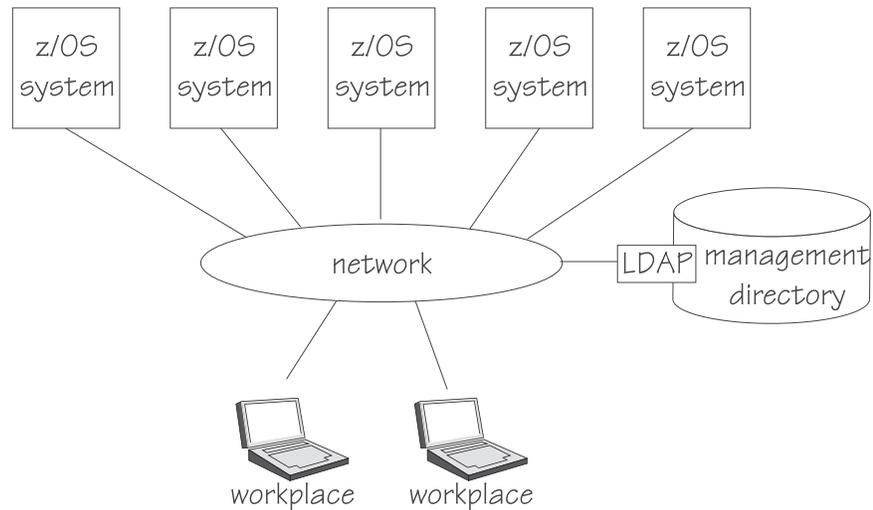


Figure 3. Simple msys for Setup system environment

In this environment:

- Each workplace has a TCP/IP connection to the LDAP server.
- Each workplace has an FTP connection to each z/OS system.
- Each z/OS system has a TCP/IP connection to the LDAP server that provides access to the management directory.

System integrity

In an environment with multiple workplaces different workplaces can work with the same z/OS system at the same time. The logic of the host framework ensures that the jobs that different workplaces start on the same z/OS system do not interfere with each other.

A locking mechanism in the management directory prevents multiple workstations from updating the same data simultaneously.

Maintaining multiple subtrees

The resources that you can work with in a workplace session are defined by the data that is stored in a single management directory, more precisely, in a single sysplex for Setup subtree of the management directory data tree.

You will have to decide how many management directory subtrees you want to maintain for the systems in your enterprise. Multiple management directory subtrees can mean better performance. In addition, user rights are assigned at the granularity of a subtree.

On the other hand, multiple subtrees can mean more administrative overhead. You also cannot share any data across subtrees.

Multiple subtrees can but need not be accessed through the same LDAP server.

Recommendation: Keep sysplexes that share data or are otherwise closely associated in a single subtree. Keep sysplexes that operate independent of one another in separate subtrees.

Rule: You must keep data for systems that belong to a sysplex in one environment. You cannot include a system from one management directory subtree in a sysplex that is described in another management directory subtree.

Important

Each system must only be represented in one management directory subtree.

Representing a system in more than one management directory subtree can lead to interferences between the subtrees and data inconsistency.

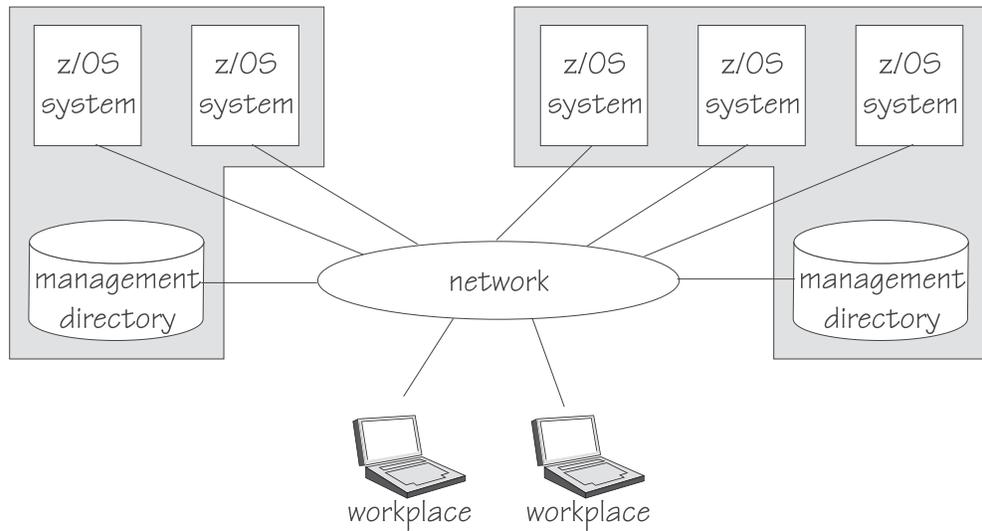


Figure 4. Scope of multiple management directory subtrees

An msys for Setup workplace is not permanently associated with a particular management directory subtree. Each workplace can connect to any management directory subtree for which the required connections are in place and that has a compatible level of code. A workplace cannot connect to a management directory subtree that contains systems where the msys for Setup host code is later than the workplace code.

Chapter 3. System requirements

This section describes the hardware and software requirements for the systems described in Chapter 2, “Setup environments” on page 7.

- z/OS system requirements
- LDAP server requirements
- msys for Setup workplace requirements

Where applicable, the sections also discuss the security of the respective system. For security considerations with regard to communications see “Communications” on page 7.

z/OS system requirements

This section describes the requirements for the z/OS systems to be customized with msys for Setup.

Hardware Requirements

The z/OS system hardware must fulfill the hardware requirements for z/OS.

In addition, allow about 1.5 GB of space for the msys for Setup job report files. If you are prepared to clear up obsolete files at frequent intervals you can use less space.

Software requirements

The z/OS systems require this software:

Program	Release/Version	Program number
z/OS	V1R1 or higher	5694-A01
Required non-z/OS software:		
Developer kit for OS/390, Java™ 2 Technology Edition (corresponds to JDK level 1.3)	Java 1.3 or higher Refer to the PSP bucket on RETAIN® for PTF and APAR requirements	5655-D35
DFSORT™ or an equivalent sort program	Release 14 or higher	5740-SM1

See Chapter 10, “Applying service to msys for Setup” on page 51 for information about installing PTFs.

To establish if any plug-ins you are using have further requirements refer to the respective service information files. You can access a service information file from the respective service’s context menu on the workplace (see *z/OS Managed System Infrastructure for Setup User’s Guide*).

Communications

The z/OS system requires a TCP/IP connection to the LDAP server and an FTP connection to the msys for Setup workplace (see Figure 2 on page 7). The FTPD server must be running and configured for remote job submission.

Security

If you use RACF, you must define it as a subsystem in an IEFSSNxx parmlib member and the subsystem must be started. msys for Setup uses the z/OS subsystem interface to pass commands to RACF.

You need a security system for z/OS UNIX. See *z/OS UNIX System Services Planning*, GA22-7800 for information on how to do this.

LDAP server requirements

This section describes the requirements for the host system that runs the LDAP server.

The LDAP server can be installed on one of the z/OS systems to be customized, or on a separate V2R10 OS/390 or z/OS system. The LDAP server must run on the same system where DB2 is installed.

Hardware requirements

The system that runs the LDAP server must fulfill the hardware requirements for z/OS or OS/390.

In addition, the LDAP server requires approximately 300 MB of DB2 backend storage for the management directory.

Software requirements

The LDAP server requires this software:

Program	Release/Version	Program number
Either :	V1R1 or higher	5694-A01
z/OS		
OR :	V2R10	5647-A01
OS/390		
Required non-z/OS software:		
Either :	V5	5655-DB2
DB2 Server for OS/390		
OR :	V6	5645-DB2
DB2 Universal Database® Server for OS/390		
OR :	V7	5675-DB2
DB2 Universal Database Server for OS/390 and z/OS		

Refer to the IBM Database 2™ Program Directory shipped with DB2 for keyword specifications for Preventive Service Planning (PSP). Use Information/Access or the ServiceLink facility of IBMLink™ to check the most current information about DB2 and other products. Contact the IBM Support Center if you do not have access to IBMLink.

If using OS/390 R10 as the LDAP server, refer to section 5 of z/OS V1R4 PSP Bucket, SUBSET MSYS, for information regarding LDAP Server PTFs that need to be installed.

Communications

The msys for Setup workplace and all z/OS systems to be customized require a TCP/IP connection to the LDAP server (see Figure 2 on page 7).

msys for Setup workplace requirements

This section contains information on the requirements for the workstation on which the msys for Setup workplace is installed.

Hardware requirements

The following table lists the minimum requirements for the workstation on which the msys for Setup workplace runs:

Processor	Pentium® or equivalent
Speed	400 MHz
Memory	256 MB
Available disk capacity	100 MB
Screen resolution	1024x768

Software requirements

The workplace requires this software:

Operating system	<ul style="list-style-type: none">• Either Windows NT 4.0 with fixpack 4 or higher, or• Windows 2000 Professional
------------------	--

Communications

The msys for Setup workplace requires a TCP/IP connection to the LDAP server and an FTP connection to the all z/OS systems to be customized (see Figure 2 on page 7).

Part 2. Installing msys for Setup

This section describes the installation tasks you must perform before you can use msys for Setup. Depending on the assignment of responsibilities, installing msys for Setup can require the cooperation of several persons. The following table provides an overview of the main tasks and who typically performs them:

Task	Administrator
Chapter 4, "Installing the z/OS system" on page 17	z/OS system programmer
Chapter 5, "Setting up an LDAP server" on page 21	LDAP administrator
Chapter 6, "Preparing the z/OS system for msys for Setup" on page 27	z/OS system programmer
Chapter 7, "Setting up the msys for Setup workplace" on page 33	LDAP administrator / msys for Setup administrator
Chapter 8, "Creating a new management directory subtree" on page 39	LDAP administrator

Chapter 4. Installing the z/OS system

The only special msys for Setup requirement for installing your z/OS system is that it is a CustomPac installation. CustomPac is a generic term that comprises ServerPac, SystemPac, ProductPac, and FunctionPac.

Your z/OS system can be:

- A z/OS V1R4 system
- A z/OS V1R3, z/OS V1R2, or z/OS V1R1 system (see “Coexistence with pre-V1R4 z/OS system”)
- A CustomPac installed OS/390 V2R10 system that has been upgraded to z/OS V1R1 with the z/OS V1R1 Upgrade Package for OS/390 V2R10
- A system that has been cloned from an existing CustomPac installed z/OS system.

Guiding you through the CustomPac install is beyond the scope of this document. For installing your CustomPac use *ServerPac: Installing Your Order* an order specific documentation that is included in your order.

During the installation you will generate several jobs, including job XMLGNR8. Follow the instructions in *ServerPac: Installing Your Order* for running this job. It creates an XML document (product definition XML) that describes the products in your order to msys for Setup.

The data set to which the XML document is written is specified for SCPPXML DD in XMLGNR8. Make a note of this data set and, if it is not cataloged, the volser it resides on. The person who makes the products in your CustomPac known to msys for Setup will need this information.

Tip: Fill in Appendix C, “Worksheet for product set installation data” on page 59.

Coexistence with pre-V1R4 z/OS system

Before you read this: This information applies to you if you want to use or are already using msys for Setup for z/OS V1R1, z/OS V1R2, and z/OS V1R3 systems.

With z/OS V1R4, msys for Setup introduces enhancements that include a different data structure in the management directory. You can use these enhancements on z/OS V1R1, z/OS V1R2, and z/OS V1R3 systems if you install FMID JMSI743 on them.

All systems that are described in a particular management directory subtree must use the same data structure. This means that if one system is V1R4 or has FMID JMSI743 installed, all other systems in that management directory subtree must either be V1R4 or FMID JMSI743 must be installed on them.

Recommendation: You are advised to install FMID JMSI743 on all z/OS V1R1, z/OS V1R2, and z/OS V1R3 systems for which you are using or want to use msys for Setup.

If you have never used msys for Setup, you set up your environment as described in Part 2, “Installing msys for Setup” on page 15. Otherwise refer to Chapter 9, “Migrating from a prior msys for Setup release” on page 47 for additional information.

Restrictions for z/OS systems

The following sections describe restrictions that apply to z/OS systems for which you want to use msys for Setup.

Minimum configuration

The msys for Setup host code runs on the z/OS system to be configured. The system must, therefore, be IPLed before msys for Setup can be used to set up products.

In addition, the z/OS systems must fulfil the requirements as stated in “z/OS system requirements” on page 11.

Parmlib restrictions

Observe the following restrictions for the parmlib of the z/OS systems:

- msys for Setup relies on the parmlib concatenation as specified in LOADxx. msys for Setup neither parses MSTJCLxx parmlib members nor MSTJCLxx modules in linklib. If you have not specified the parmlib concatenation in LOADxx, then msys for Setup will not be able to find the concatenation. If you create your own master scheduler JCL and specify information that overrides information in the parmlib, take extreme care!
- Symbols must not be used in parmlib members for any keywords or syntactically relevant delimiters. Also, the list indicator, L, as used in suffix lists must not be coded in symbols. If it is, it will be ignored.
Symbols can only be resolved if they are correctly defined for the target system profile in an IEASYM member.
- msys for Setup does not issue any error message if it encounters OPI=YES. However, OPI=YES in combination with operator input may lead to incorrect results from parsing. Therefore msys for Setup recommends the use of OPI=NO.
- Filters in IEASYM must be specified directly following a SYMDEF keyword. If they are not, then msys for Setup will process them as if they were specified immediately following the preceding SYMDEF. See “Filter restrictions in IEASYM” for details.

Filter restrictions in IEASYM

Filters in IEASYM must be specified directly following a SYSDEF keyword. The first of the following code samples shows a specification that msys for Setup cannot work. The second sample shows how the specification can be rewritten to comply with the requirements of msys for Setup.

Do not specify:

```
SYSDEF
  HWNAME(hwname)
  SYSNAME(sname1)
  SYMDEF(sybo11)
  SYMDEF(sybo12)
  SYMDEF(sybo13)
  SYMDEF(sybo14)
  SYMDEF(sybo15)
  SYMDEF(sybo16)
```

```
LPARNAME(1name)
SYSNAME(sname2)
SYMDEF(sybo17)
SYMDEF(sybo18)
```

Specify instead:

```
SYSDEF
  HNAME(hwname)
  SYSNAME(sname1)
  SYMDEF(sybo11)
  SYMDEF(sybo12)
  SYMDEF(sybo13)
  SYMDEF(sybo14)
  SYMDEF(sybo15)
  SYMDEF(sybo16)
```

```
SYSDEF
  HNAME(hwname)
  LPARNAME(1name)
  SYSNAME(sname2)
  SYMDEF(sybo17)
  SYMDEF(sybo18)
```

Chapter 5. Setting up an LDAP server

Recommendation: Set up a new LDAP server to be used exclusively by msys for Setup.

Reference

- *z/OS Security Server LDAP Server Administration and Use*, SC24-5923
- *Understanding LDAP*, SG24-4986

This redbook is available at <http://www.redbooks.ibm.com>

Use the `ldapcnf` utility that is provided by z/OS to set up your LDAP server. When using the utility you provide your customization input by editing four profile files. `ldapcnf` uses these profiles to generate all the necessary jobs, input data sets, and `parmlib` members.

If you are using an OS/390 R10 system for your LDAP server, you can obtain the `ldapcnf` utility from a PTF. The PTF number can be found in the msys for Setup PSP bucket.

This section describes the subtasks for setting up a new LDAP server for use with msys for Setup. Perform the subtasks in this order:

1. “Adapting the LDAP profile files”
2. “Processing the profile files” on page 22
3. “Modifying the schema entry for the TDBM backend” on page 23

Perform these tasks on the system where you want to establish your LDAP server.

Note: The descriptions in this section assumes that you are using RACF to protect your management directory. If you are not using RACF, refer to “What is different without RACF?” on page 25 for what you must do different when setting up the LDAP server.

Result: After completing these tasks, the LDAP server can be accessed by the workplace. Perform all remaining initialization tasks for the LDAP server from a workplace.

Adapting the LDAP profile files

The files you need to adapt to your environment are located in the HFS at `/usr/lpp/ldap/etc`.

Copy the files to a directory where you have write access. Then access the files with your favorite editor for the z/OS UNIX environment, for example `vi`. The files contain instructions on which values you must supply and which values are msys for Setup defaults that you can modify.

Before you begin: The information you will have to provide is summarized in Appendix B, “Worksheet for editing the LDAP profile files” on page 57.

Tip: Accept the provided defaults if they are compatible with your environment. This minimizes the effort for setting up the workplace. Note down any changes you make to the defaults in Appendix A, “LDAP connection worksheet” on page 55. You will need this information when you create the management directory subtree (see Chapter 8, “Creating a new management directory subtree” on page 39) or to connect to the LDAP server for the first time from a particular workplace.

Adapt these files:

ldap.msyp.profile

This is the main profile file for the LDAP server. The information in this file includes parameters for the ldapcnf utility, the TDBM and SDBM suffixes, and specifications for the LDAP administrator.

Examine all items that are listed in Appendix B, “Worksheet for editing the LDAP profile files” on page 57. Although there are defaults for some items, expect to have to adapt the values to your environment.

Note: If you are not using RACF to protect your management directory, see “What is different without RACF?” on page 25 for special instructions.

ldap.msyp.db2.profile

This file contains information on the DB2 database that serves as a persistent storage mechanism for the TDBM backend.

The file is complete with defaults. View the file and verify that the defaults are compatible with your environment. Only edit the file if you need to overwrite the defaults.

ldap.msyp.slapped.profile

This file contains additional LDAP settings.

The file is complete with defaults. View the file and verify that the defaults are compatible with your environment. In particular, verify that port number 3389 is available and not used, for example, by an existing LDAP server. Only edit the file if you need to overwrite the defaults.

ldap.msyp.racf.profile

This file contains security information, for example, on who is authorized to start the LDAP server.

The file is complete with defaults. View the file and verify that the defaults are compatible with your environment. Only edit the file if you need to overwrite the defaults.

Processing the profile files

This section describes how to process the LDAP profile files with the ldapcnf utility and how to use the output to set up an LDAP server.

Before you start: You must have adapted the files to your environment (see “Adapting the LDAP profile files” on page 21).

Steps for processing the profile files

Perform these steps to process the profile files:

1. Run the ldapcnf utility for each file.

For example, if you have copied the files to a directory `/u/msys/` issue commands like this from a z/OS UNIX command prompt:

```
ldapcnf -i /u/msys/ldap.msys.profile
ldapcnf -i /u/msys/ldap.msys.db2.profile
ldapcnf -i /u/msys/ldap.msys.slapd.profile
ldapcnf -i /u/msys/ldap.msys.racf.profile
```

See *z/OS Security Server LDAP Server Administration and Use* for details on the `ldapcnf` utility.

Result: The utility creates an output data set with members that are generated according to the information in the profile files. The members include a `proclib` member, a `parmlib` member, several jobs, and a SPUFI input file. The name of the output data set is the value for `OUTPUT_DATASET` in `ldap.msys.profile`.

-
2. Copy the LDAP server started task procedure from the output data set to the system's `proclib`. The name of the member corresponds to the value you specified for `LDAPUSRID` in `ldap.msys.profile`; the default is "MSYSLDAP".

 3. Copy the `PROGxx` member from the output data set to the z/OS system's `parmlib`. `xx` corresponds to the value for `PROG_SUFFIX` in `ldap.msys.profile`.

 4. Submit the jobs that were generated from TSO. Submit the jobs in this order:
 - a. RACF
 - b. APF
 - c. DBCLI

Note: DB2 must be up and running before you submit this job.

 - d. PRGMCTRL

Note: You need to submit this job only if Program Control is active on your LDAP server system.

 5. Submit the `DBSPUFI` member with the DB2 SPUFI interactive tool.
-

Modifying the schema entry for the TDBM backend

`msys` for Setup is shipped with schema files that define the structure of the management directory data tree. This section explains how to load these files into your LDAP server.

Before you begin:

- You must have set up the TDBM backend (see "Processing the profile files" on page 22).
- The LDAP server must be running. If you have accepted the default for `LDAPUSRID` in `ldap.msys.profile`, for example, enter:

```
/s MSYSLDAP
```

in SDSF, or enter
s MSYSLDAP

on the operator console to start it.

Steps for modifying the schema entry for the TDBM backend

Perform these steps to modify the schema entry for the TDBM backend:

1. Copy the required ldif-files from /usr/lpp/ldap/etc into a local directory.

If you are setting up your LDAP server on a	Then copy these ldif-files
---	----------------------------

z/OS R1 or OS/390 R10 system and you have *not* installed the PDFs for APAR OW47594

- schema.user.ldif
- schema.IBM.ldif
- ManagedSystemInfrastructure.ldif

z/OS R2 or later system

- schema.user.ldif
- schema.IBM.ldif

or

z/OS R1 or OS/390 R10 system with APAR OW47594

On z/OS R1 and OS/390 R10 with APAR OW47594, and on z/OS R2 or later systems the definitions of ManagedSystemInfrastructure.ldif are included in schema.IBM.ldif

-
2. Edit schema.user.ldif.

Find this line near the top of the file:

```
dn:cn=schema,<suffix>
```

Replace <suffix> with the TDBM suffix that you have specified in file ldap.msys.profile.

Example: if you have accepted the default, "ou=msys,o=ibm,c=us", edit the line to read:

```
dn:cn=schema,ou=msys,o=ibm,c=us
```

3. Depending on your system, load the schema files in this order:

If you are setting up your LDAP server on a	Then load these ldif-files
---	----------------------------

z/OS R1 or OS/390 R10 system and you have *not* installed the PDFs for APAR OW47594

- a. schema.user.ldif
- b. schema.IBM.ldif
- c. ManagedSystemInfrastructure.ldif

z/OS R2 or later system

- a. schema.user.ldif
- b. schema.IBM.ldif

or

z/OS R1 or OS/390 R10 system with APAR OW47594

Note: Do not load ManagedSystemInfrastructure.ldif if you have a z/OS R2 or later system or a z/OS R1 or OS/390 R10 system with APAR OW47594.

To load a file issue a command like this from a z/OS UNIX command prompt, for example from telnet or OMVS:

```
ldapmodify -h <ldaphost>
            -p <port>
            -D "racfid=<ADMIN>,profiletype=user,sysplex=msysplex"
            -w <passwd>
            -f <file>
```

where:

- <ldaphost> is the name of the host system where the LDAP server is running.
- <port> is the port at which the LDAP server is listening
- <ADMIN> is the LDAP administrator user ID
- <passwd> is the password of the LDAP administrator user ID
- <file> is the schema file

Example:

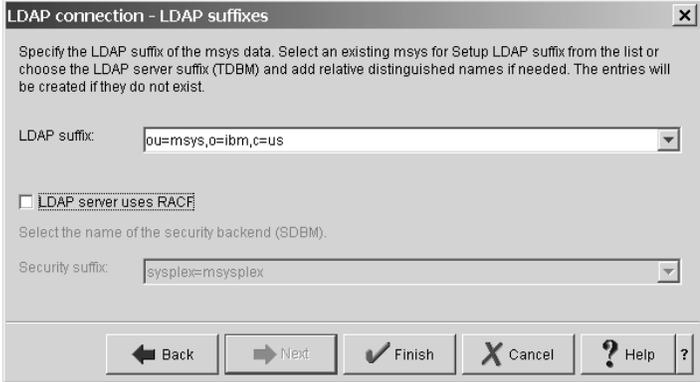
```
ldapmodify -h dbsys
            -p 1234
            -D "racfid=bill,profiletype=user,sysplex=msysplex"
            -w secret
            -f schema.user.ldif
```

Tip: If you have used the worksheet in Appendix B, “Worksheet for editing the LDAP profile files” on page 57, you have a record of these parameters.

What is different without RACF?

This section summarizes what you must do different if your management directory is not RACF-protected. Skip this section if you use RACF for protection.

Stage	Description
Before you install the LDAP server: “Adapting the LDAP profile files” on page 21 Note: If the LDAP server is already installed, make these changes in the LDAP server configuration file and restart the server.	Make the following changes in ldap.msyp.profile: <ul style="list-style-type: none">• Change the name of the LDAP administrator to “cn=ADMIN,sysplex=msysplex”• Accept “ADMIN” as the administrator user ID or change it to the ID you want to use instead.• Remove the hash sign (#) in front of the ADMINPW parameter to activate the administrator password• Accept the default “secret” or overwrite it with the password you want to use. Note: Be sure that access to the configuration file is restricted. The password is in clear text and can be read by anyone who can open the configuration file.• Make the SDBM backend inactive by setting SDBM_SUFFIX=""

Stage	Description
Connecting to the management directory: "Creating the subtree" on page 42	Clear the LDAP server uses RACF check box in the "LDAP suffixes" panel of the "LDAP connection" wizard: 
Logging on to the management directory: "Creating the subtree" on page 42	Log on with the user ID and password that you defined in ldap.msys.profile. If you have accepted the defaults: <ul style="list-style-type: none"> • The user ID is "ADMIN" • The password is "secret"

Password encryption

Password encryption should be present on the LDAP server. Otherwise the passwords are written to the management directory in clear text.

Chapter 6. Preparing the z/OS system for msys for Setup

This section describes the following tasks that you must perform on all z/OS systems that are to be customized with msys for Setup:

- “Authorizing the Java DLLs”
- “Setting up z/OS UNIX System Services for msys for Setup users” on page 29
- “Choosing a JES job class” on page 29
- “Verifying the communications” on page 29
- “Assuring that the MIGLIB is authorized and accessible” on page 29
- “Authorizing the msys for Setup users” on page 30

Authorizing the Java DLLs

msys for Setup runs functions that require APF-authorization. Therefore, it must be able to start a Java Virtual Machine in an authorized mode. To make this possible, use the EXTATTR command to turn on the APF extended attribute in the HFS for each Java dynamic link library (DLL).

msys for Setup provides a sample job, CIMAPFJ, that can do this for you.

Before you begin:

- The Java runtime environment must be installed and configured.
- The HFS that contains Java must be mounted in read/write mode.
- You must have READ access to BPX.FILEATTR.PROGCTL.

Recommendation: To prevent unauthorized users from manually using the authorized DLLs you are advised to restrict access to /usr/lpp/cim/bin/IBM/CIMJAVA to msys for Setup users.

Steps for restricting access to the authorized DLLs

You can perform these steps restrict access to /usr/lpp/cim/bin/IBM/CIMJAVA if you are using RACF for security. If you are using another security product do the equivalent in that product:

1. Ensure that “List of group access checking” is enabled. From TSO issue:

```
SETOPTS GRPLIST
```

-
2. Ensure that /usr/lpp/cim/bin/IBM is mounted in read/write mode.

-
3. Define an msys for Setup group. From TSO, issue commands like this:

```
ADD GROUP MSYS  
DATA('MSYS USERS')  
NOTERMUACC  
SUPGROUP(xx)  
OMVS(GID(yy))  
OWNER(zz)
```

Choose values for xx, yy, and zz according to your needs.

-
4. Connect at least one msys for Setup user to this group:

```
CONNECT <userid> GROUP(MSYS) AUTH(USE)
```

where <userid> is the user's ID

Tip: to connect multiple user IDs, u1, u2, ..., un, with a single command you specify all IDs with a space as separator:

```
CONNECT u1 u2 ... un GROUP(MSYS) AUTH(USE)
```

-
5. Define group MSYS as the owner of CIMJAVA. Change to /usr/lpp/cim/bin/IBM/CIMJAVA. From a z/OS UNIX command prompt issue:

```
chgrp MSYS /usr/lpp/cim/bin/IBM/CIMJAVA
```

-
6. Restrict the access rights for /usr/lpp/cim/bin/IBM/CIMJAVA to the owning group MSYS:

```
chmod 750 /usr/lpp/cim/bin/IBM/CIMJAVA
```

Result: Only users ID that have been added to group MSYS can run CIMJAVA manually.

Steps for authorizing the Java DLLs

Perform these steps to APF-authorize the Java Virtual Machine:

1. Check the Java version by using the command: `java -fullversion` at the z/OS UNIX System Services command prompt. You require Java 1.3 or higher.

2. Find sample job CIMAPFJ in SYS1.SAMPLIB and make a copy of it for your use.

3. Edit your copy of CIMAPFJ according to your environment. You will find instructions on what you have to adapt in CIMAPFJ.

4. Submit the edited job.

You know that you have successfully authorized the DLLs if you get RC=0.

Result: msys for Setup can start the Java virtual machine in authorized mode and run jobs that require APF. The authorization does not extend to Java programs that are started through the Java command.

Note: You must repeat this task each time you apply a Java PTF.

Setting up z/OS UNIX System Services for msys for Setup users

Some msys for Setup functions have high storage requirements in the UNIX[®] environment (256 MB). To satisfy these requirements set the maximum address space size in z/OS UNIX System Services.

Do not update the MAXASSIZE in BPXPRMxx to accomplish this. Instead, use the ASSIZEMAX parameter in the OMVS profile of each user ID that is required to log on to the z/OS system when using msys for Setup.

Tip: if you are using RACF you can use this RACF command:

```
ALTUSER xxxx OMVS(ASSIZEMAX(268435456))
```

msys for Setup submits jobs with REGION=256M. Be sure not to overwrite the extended region for these jobs using IEALIMIT or IEFUSI.

Also set the following parameter values in BPXPRMxx:

- MAXFILEPROC 200
- MAXPROCSYS 1000
- MAXPROCUSER 50
- MAXCPU TIME 2147483647 (which means unlimited)

Choosing a JES job class

To prevent msys for Setup jobs from timing out a JES job class must be available that fulfills the requirements of all msys for Setup jobs. Some jobs:

- Take several hours to complete and require a job class that has a long maximum CPU time, for example TIME=1440
- Start nested jobs during processing and require a job class for which there are multiple initiators

Ensure that an according job class is available. Define one if necessary. Make a note of this job class. The msys for Setup sysplex and systems administrator requires this information when describing the z/OS system to msys for Setup.

Verifying the communications

Ensure that the FTP server is running and configured for remote job submission.

Ensure that TCP/IP is configured and active. Ensure that the required connections are established:

- To the LDAP server
- To the workstation where you are going to install the workplace

Use, for example, a ping command.

Assuring that the MIGLIB is authorized and accessible

SYS1.MIGLIB must be APF-authorized. If applicable add SYS1.MIGLIB to the APF list.

Authorizing the msys for Setup users

msys for Setup users must be sufficiently authorized to run the host processes on the z/OS systems they work with. There are basic authorizations that all msys for Setup users require. In addition, there are service specific authorizations. These correspond to the authorizations required by administrator roles as they are practised at many installations.

Examples:

- The authorizations for service RACFSecurity correspond to the authorizations for the security administrator
- The authorizations for service TCP/IP correspond to the authorizations for the network administrator

The following table tells you what is required for all msys for Setup users. It also tells you what is required in addition for users that work with two services that are central to msys for Setup, RACFSecurity and Parallel Sysplex®. For the required authorizations for all other services refer to the respective service information file. You can access a service information file from the respective service's context menu on the workplace (see *z/OS Managed System Infrastructure for Setup User's Guide*).

Note: The table provides examples for commands you can use if you are using RACF for security. Perform equivalent actions, if you are using a different security product.

Table 1. Authorizations required by msys for Setup users

User ID	Authorization
All msys for Setup users	<p>All msys for Setup users must have authority to create data sets "<user ID>.*" to allow msys for Setup to create temporary data sets; and the user ID must have read/write access rights to such data sets.</p> <p>To satisfy high storage requirements in the UNIX environment set the ASSIZEMAX parameter in the user's OMVS profile: ALTUSER <user-ID> OMVS(ASSIZEMAX(268435456))</p> <p>See also "Setting up z/OS UNIX System Services for msys for Setup users" on page 29.</p> <p>Tip: You can establish a user group for the msys for Setup users and assign these authorities to the group. See also "Steps for restricting access to the authorized DLLs" on page 27.</p>
For service RACFSecurity	<p>To perform the 'Update system configuration' task, the user ID needs the RACF SPECIAL attribute: ALTUSER <user-ID> SPECIAL</p> <p>If you do not want to grant this authority, consider selecting the No update of the RACF database check box in the authorization policy (Category RACFSecurity). See <i>z/OS Managed System Infrastructure for Setup User's Guide</i> for further details.</p>

Table 1. Authorizations required by msys for Setup users (continued)

User ID	Authorization
For service Parallel Sysplex	<p>The msys for Setup host code uses the REXX ADDRESS CONSOLE environment to issue D XCF commands during Refresh and Update. If your installation does not have the ADDRESS CONSOLE environment enabled, you will have to verify the following:</p> <ul style="list-style-type: none"> • The CONSPROF command is defined authorized in TSO <ul style="list-style-type: none"> – SYS1.CMDLIB must be APF-authorized – CONSPROF must be added to the AUTHCMD section of IKJTSOxx • The user ID is allowed to use the CONSOLE command in TSO PERMIT CONSOLE CLASS(TSOAUTH) ID(<user-ID>) ACCESS UPDATE • The user ID is authorized to issue 'DISPLAY XCF' Console commands. Actual RACF commands needed depend on the usage of the OPERCMDS class at your installation. <p>If Couple data sets exist, for instance in an existing Sysplex that is planned to be maintained by msys for Setup, then the following RACF resource profiles will be present on the system. To work with Parallel Sysplex the user ID needs to have READ access to these resources.</p> <ul style="list-style-type: none"> • MVSADMIN.XCF.SFM • MVSADMIN.XCF.CFRM • MVSADMIN.XCF.ARM • MVSADMIN.WLM.POLICY • MVSADMIN.LOGR (additionally, the user ID that will be used to submit commit jobs, must have "ALTER" authority). Use : PERMIT <resource> CLASS(FACILITY) ID(<user-ID>) ACCESS(ALTER) <p>For the current level of the code, the user ID requires these authorities even if you do not use Couple data sets in your installation. To assign the authorities we recommend that you issue the following RACF command: PERMIT <resource> CLASS(FACILITY) ID(<user-ID>) ACCESS(READ)</p> <p>Notes:</p> <ol style="list-style-type: none"> 1. Depending on how you have organized the couple resource profiles in RACF, the resource is either a generic entry MVSADMIN.** or the command has to be issued for each of the above listed resources. 2. The Parallel Sysplex plug-in will allow further refinement of the authorities.

Chapter 7. Setting up the msys for Setup workplace

This section describes the tasks for setting up the msys for Setup workplace on your workstation. Perform the subtasks in this order:

1. "Ensuring that the workstation is defined to TCP/IP"
2. "Verifying the TCP/IP connection to the LDAP server" on page 34
3. "Downloading the workplace" on page 34
4. "Installing the workplace on your workstation" on page 36
5. "Starting the workplace" on page 36

Ensuring that the workstation is defined to TCP/IP

The workstation you use for running the workplace needs a host name in addition to an IP address.

To display your workstations host name type
hostname

at a command prompt and press Enter. If the command returns a host name you are done. If not, follow the instructions in this section to assign one.

Before you begin:

- You must have administrator rights on the workstation you are using to make the necessary changes to the system settings.
- Consult your network administrator about which host name and domain you should use.

Steps for assigning a host name to a Windows NT workstation

Perform these steps to assign a host name to a Windows NT workstation:

1. On the desktop, click **Start** → **Settings** → **Control Panel**.

-
2. Double click **Network**.

-
3. In the Network property pages, click the **Protocols** tab.

-
4. Select TCP/IP from network protocols, then click **Properties**.

-
5. Click the **DNS** tab.

-
6. On the DNS panel, type a host name into the **Host Name** field.

-
7. Ensure that the domain name is correct.

-
8. Click **OK** → **OK**.

Steps for assigning a host name to a Windows 2000 workstation

Perform these steps to assign a host name to a Windows NT workstation:

1. On the desktop, click **Start** → **Settings** → **Control Panel**.
2. Double click **System**.
3. In the System Properties, select the **Network Identification** tab.
4. Click **Properties** to display the “Identification Changes” panel.
5. Type the host name into the **Computer name** entry field.
6. Click **More** to display the “DNS Suffix and NetBIOS Computer name” panel.
7. Ensure that the domain name is correct. If you have made changes on this panel, close it with **OK**; if you have not made any changes, close it with **Cancel**.
8. Click **OK** → **OK**.

Verifying the TCP/IP connection to the LDAP server

At a command prompt on the workstation, enter:

```
ping hostname
```

where *hostname* is the host name or IP address of the system where the LDAP server runs.

You can use either of these means to verify that the LDAP server is running:

- Access the LDAP server with an LDAP client, for example an LDAP browser (not delivered with msys for Setup).
- Check the LDAP server log file
- Use the `ldapsearch` facility. Refer to *z/OS Security Server LDAP Server Administration and Use* for details.

Downloading the workplace

The workplace installation program `cimsetup.exe` resides in the hierarchical file system (HFS), in directory `/usr/lpp/cim` on the CustomPac installed z/OS system volumes.

Download `cimsetup.exe` to a temporary directory on the workstation where you want to install the workplace. You can use:

- FTP
- A Web browser

The following sections provide detailed steps for downloading the file.

Before you begin: You require an ID on the z/OS system with at least read access to the HFS.

Steps for downloading the workplace code with FTP

Perform these steps to download the workplace code with FTP:

1. Open a command prompt on your workstation.

-
2. Create a temporary directory, for example:

```
c:  
md cimsetup  
cd cimsetup
```

-
3. Open an FTP session with a z/OS system.

```
ftp hostname
```

where *hostname* is the host name or the IP address of the z/OS system.

-
4. Enter your user ID and password for the z/OS system when prompted. Your user ID must have read access to /usr/lpp/cim.

-
5. Change to the HFS directory where the workstation code resides:

```
cd /usr/lpp/cim
```

-
6. Change to binary mode, get the file, and exit FTP:

```
binary  
get cimsetup.exe  
quit
```

Steps for downloading the workplace code with your Web browser

Before you begin: Using a Web browser might require some preparation on the z/OS system from where you want to download the code. If either:

- Your network setup uses a proxy
- You use Microsoft Internet Explorer 5.0 (with or without proxy)

you might need to configure your FTP-server to go to the HFS by default. To do this, set STARTDIR HFS in FTPSDATA (see *z/OS Communications Server: IP Configuration Guide* for details).

Perform these steps to download the workplace code with a web browser:

1. Direct your browser at this URL:

ftp://<your userID>@<hostname>/usr/lpp/cim/cimsetup.exe

where:

<hostname>

is the host name or the IP address of the z/OS system.

<your userID>

is your ID on the z/OS system.

2. Enter your password when prompted.
-

3. Save the file to your workstation.

Example: If you are using Netscape Communicator, select **File** → **Save as...**

Installing the workplace on your workstation

Before you begin: You must have administrator rights on the workstation.

The workplace installation is performed with the workplace installation program. To install the workplace run cimsetup.exe and follow the instructions on the screen.

If you are installing the workplace for the first time on your workstation, you will be prompted to specify an install directory. Subsequent installations of newer levels of workstation code will automatically install over and replace the previous installation. Settings like, for example, the LDAP connection are preserved.

If you have installed a new version of the workplace over a prior one, check that the installation resulted in the correct version. To do this, start the workplace, log on, and click **Help** → **Product information...** on the menu. If the information shows that you still have the old version of the workplace, use the Windows control panel to deinstall the old version and then rerun the installation program.

Tip: Delete cimsetup.exe when you have completed the installation. This releases about 30 MB of storage on your workstation

Starting the workplace

Start the workplace to confirm that you have installed it successfully.

During installation the InstallShield creates a program group with a start entry for the msys for setup workplace. Use the start menu to start the workplace.

If you have accepted the InstallShield defaults for the group and entry name, select: **Start** → **Programs** → **IBM msys for Setup** → **IBM msys for Setup Workplace**

Result: For a first time installation on a workstation the workplace comes up with the "LDAP connection" wizard.

If this is the first workplace that has been installed for a particular msys for Setup environment, proceed with Chapter 8, “Creating a new management directory subtree” on page 39 to create a management directory subtree. If you want to use the workplace with an existing management directory subtree complete the wizard to connect to that subtree.

Chapter 8. Creating a new management directory subtree

The workplace presents the data that is stored in an msys for Setup management directory subtree. If you have set up a new LDAP server, you must use the workplace to create the subtree.

This section contains:

- General information on the management directory in “What you need to know about the management directory”.
- The steps you must preform in “Creating the subtree” on page 42

Before you begin: Familiarize yourself with the information in “What you need to know about the management directory”.

To create an msys for Setup management directory subtree you need LDAP administrator rights and this information:

Host name or IP address of the LDAP server

Port for communicating with the LDAP server

TDBM suffix for the management directory subtree

Security suffix
for the SDBM (RACF) backend

Tip: If you have filled it in when setting up the LDAP server, use the values you entered into the worksheet (Appendix A, “LDAP connection worksheet” on page 55).

What you need to know about the management directory

This topic describes the LDAP management directory in relation to msys for Setup. For general information on LDAP, see the following Web sites:

- <http://www.umich.edu/~dirsvcs/ldap/doc/>
- <http://www.openldap.org>

After reading this section you should know:

- What an LDAP suffix is
- What the TDBM suffix is
- Which suffixes you can use for the msys for Setup management directory subtree
- What msys for Setup recommends about msys for Setup management directory subtrees

What is a suffix and what can it contain?

msys for Setup stores all data on an msys for Setup environment in a management directory subtree. The management directory organizes data as data objects in a tree like structure. The objects and their place in the tree hierarchy are based on the Common Information Model (CIM) data schema.

According to the schema, the first four levels in the tree are:

- c** country
- l** location
- o** organization
- ou** organization unit

Not all levels need to be used. The following example omits l:

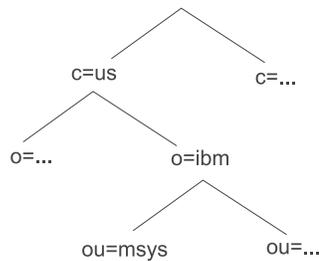


Figure 5. Example directory tree

An entry in the data tree is a collection of attributes and is identified by its distinguished name. A distinguished name is a succession of type=value pairs. Similar to a path specification, these pairs represent all levels of the hierarchy from the root to the entry. The first pair is the relative distinguished name (RDN) of the entry, then follows the RDN of the entry above it in the tree and the last the RDN of the topmost entry in the tree. Adjacent RDNs are separated by commas.

For example, with reference to Figure 5, the DN “ou=msys,o=ibm,c=us” uniquely identifies the entry “ou=msys”.

Where can an msys for Setup management directory subtree be located

The msys for Setup management directory subtree begins with an “ibm-msysdiscipline=setup” entry that is always located below an **ou**. For example, the subtree could begin below “ou=msys” of Figure 5.

Figure 6 on page 41 shows what you get when you accept the default for the first levels of the data tree when setting up the LDAP server (see “Adapting the LDAP profile files” on page 21), and later when creating the msys for Setup subtree with the workplace (see “Creating the subtree” on page 42).

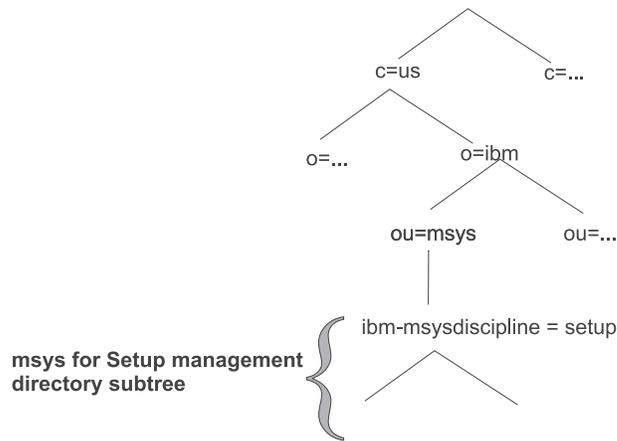


Figure 6. Management directory example with msys for Setup subtree, default suffix

Because RDN of entries below “ou=msys” all end with “ou=msys,o=ibm,c=us” the latter is also called a suffix for the data tree below “ou=msys”.

All management objects created by msys for Setup are located under the “ibm-msysdiscipline=setup” entry. User access rights are given for “ibm-msysdiscipline=setup”.

If you want to allow for multiple msys for Setup subtrees or want a suffix that includes more information, for example on the organizational unit it corresponds to, you can use additional, **c**, **l**, **o**, or **ou** specifications. The following suffix uses an additional **ou** specifications: “ou=yourunit,ou=msys,o=yourcompany,c=us”.

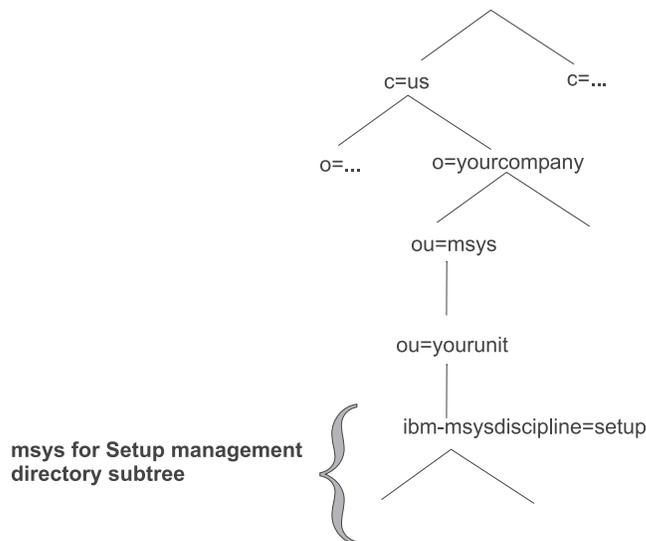


Figure 7. Management directory example with msys for Setup subtree, user defined suffix

The TDBM suffix that you specify in the ldap.msys.profile — file (see “Adapting the LDAP profile files” on page 21) when you set up the new LDAP server is a common suffix for all objects that are accessed through the TDBM backend on that server. Therefore:

Rules:

- Your subtree suffix must contain the TDBM suffix. At a minimum it can be equal to the TDBM suffix.
- The entire msys for Setup namespace (ibm-msysDiscipline=setup name tree) must reside within one LDAP server instance.

Recommendations

msys for Setup recommends that:

- You create only one msys for Setup subtree in a management directory, even if you have sysplexes in different countries.

The **c** for country, is only a conceptual representation, and is not meant in a strict geographical sense. If you have defined a subtree at **c=us**, and you have a sysplex in **c=de**, you do not have to create a second subtree at **c=de**.

- You define a single subtree for your entire enterprise
- Use lower case only for the attribute values.

According to this recommendation the terms management directory and msys for Setup management directory subtree become interchangeable.

You might want to divert from that recommendation, for example, if your enterprise includes independent units that you want to keep strictly separated.

Creating the subtree

Perform this task once for each new management directory subtree, that is, for each new msys for Setup system environment.

Note: If you are not using RACF to protect your management directory, see “What is different without RACF?” on page 25 for special instructions.

Overview of the panel flow for creating the subtree

You enter the information for creating the subtree in the “LDAP connection” wizard. Then you are prompted to log on with your LDAP administrator ID and password. After a successful logon, msys for Setup creates the management directory subtree and prompts you to define the first msys for Setup user administrator.

Figure 8 on page 43 gives an overview of the panel flow that guides you through the task.

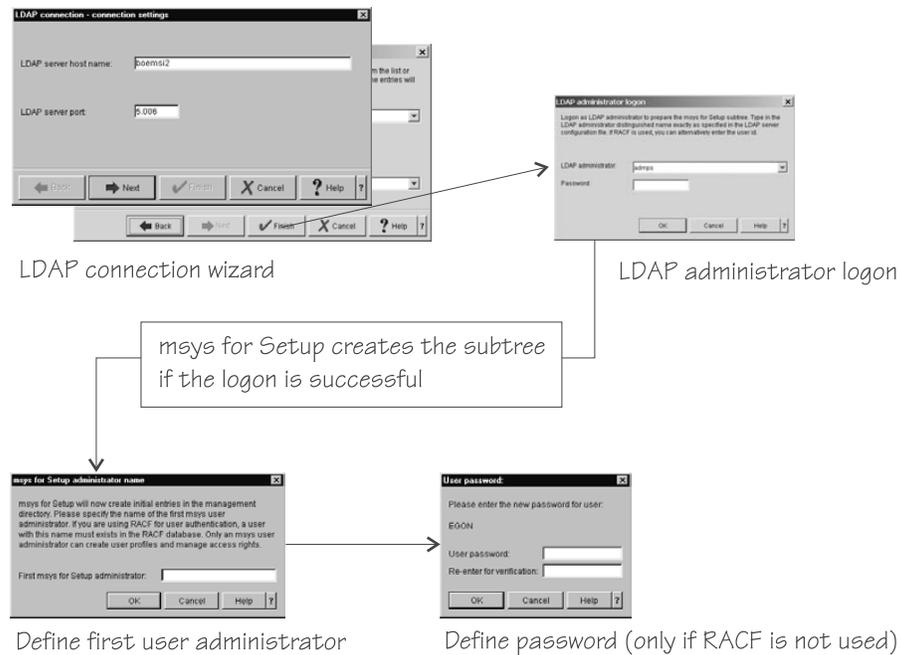


Figure 8. Panel flow for creating a management directory subtree

When you start a newly installed workplace for the first time the “LDAP connection” wizard is launched automatically (see also “Starting the workplace” on page 36).

You can launch the wizard manually by clicking **Set up LDAP connection...** on the “Log on to Setup” panel.

Steps for creating the subtree

Perform these steps to create the subtree:

1. Follow the instructions in the “LDAP connection” wizard to specify where the new subtree resides and how it is protected.

2. When you have completed the wizard, a message tells you that you need to log on as an LDAP administrator for the LDAP server you have specified. Respond with **OK** to display the logon panel.



Figure 9. LDAP administrator logon panel

-
3. Type your administrator ID and password and click **OK**.
If the logon is successful, msys for Setup creates the management directory subtree. Then the “msys for Setup administrator name” panel is displayed.

 4. Specify an ID. If your subtree is RACF-protected, this ID must also exist in the RACF database.

 5. Click **OK**. If your subtree is RACF-protected, you have completed the task, otherwise the “User password” panel is displayed.
If applicable, enter a password and click **OK** to complete.
-

Result: You have created a new subtree and its user administrator. There are no further tasks you as LDAP administrator can perform on the workplace. The workplace logs you off and prompts the user administrator to log on.

Remember to inform the user administrator of the ID and, if applicable, the password.

For a description of the user administrator tasks see *z/OS Managed System Infrastructure for Setup User's Guide*.

Part 3. Maintenance

This part provides information on applying service to msys for Setup, going to a new level of code of msys for Setup, and extending the scope of msys for Setup by installing new product sets.

Chapter 9. Migrating from a prior msys for Setup release

Who should read this: This section only applies to you if you have been using msys for Setup prior to V1R4.

Introducing the first:

- z/OS V1R4 system or
- FMID JMSI743 for a z/OS V1R1, z/OS V1R2, or z/OS V1R3 system

to an existing management directory subtree necessitates changes to all major components of an msys for Setup environment.

- Management directory
- z/OS systems
- Workplace

Before you begin: If updates have been performed, they should also be committed. Be sure that the current configuration on all systems is a good configuration. The system configuration at migration time is used as the new initial configuration beyond which you cannot undo configuration changes. Where necessary, perform “Undo all updates” before starting the migration.

Migrating the management directory to V1R4

This section describes the requirements and options you have with respect to the management directory.

Before you begin: To perform the LDAP migration you require LDAP administrator rights.

LDAP server requirements

The msys for Setup code that is delivered with z/OS V1R4 or FMID JMSI743 requires a management directory that resides on an OS/390 V2R10 or z/OS LDAP server. If you have been using OS/390 V2R8 or V2R9 to host the LDAP server you must now migrate, preferably to z/OS.

See *z/OS Security Server LDAP Server Administration and Use*, SC24-5923 for details.

Guidelines and restrictions for migrating your management directory structure

Regardless of the platform for your LDAP server, you must use the enhanced V1R4 data structure. You have two options:

- Use the new workplace to create a new management directory subtree and reenter your data
- Migrate your existing subtree

Guideline: Unless you have entered a significant amount of customization data that you want to reuse, you are advised to create a new subtree. The new level of code provides you with wizards that help you to quickly describe your product

sets², sysplexes, and systems in the new subtree. This approach also allows you to assign independent sysplexes to separate management directories subtrees (see “Maintaining multiple subtrees” on page 9).

If you decide to migrate your existing subtree, be aware of the following restrictions.

Restrictions:

- All data for product homes that were created based on OS/390 V2R8 or OS/390 V2R9 product homes cannot be migrated to a V1R4 product set.
- The system that was used as focal point system in msys for Setup becomes the sysplex driving system during migration. This is the system where the tasks for sysplex-wide services run. Be sure that the system that you want to be the sysplex driving system is the focal point system at the time of migration. For the new level of code there are temporary restrictions for changing the sysplex driving system to a different system.

To change the focal point:

1. Change the focal point to the system profile that corresponds to the system you want as sysplex driving system.
2. Refresh the management directory.
3. Open the Parallel Sysplex customization dialog and click **Save**.

Note:

The focal point system concept was introduced in PTF UW90716 for z/OS V1R1. If you are migrating from a z/OS V1R1 system on which the PTF was not installed, a focal point system does not exist. In this case, the system that corresponds to the first system profile to which a product set was added becomes the sysplex driving system during migration.

- Only one system profile can be associated with a sysplex driving system.
- After migrating the management directory you must upgrade all product sets that were created from existing product homes. You do this from the workplace. The upgrade is mostly automatic but might require additional customization for some services. For details, refer to the migration appendix of *z/OS Managed System Infrastructure for Setup User’s Guide*.

Migrating the management directory

When you first use a V1R4 workplace to log on to a management directory with the pre-V1R4 structure you are asked if you want to perform the migration. If you agree, the migration is performed automatically for you. If you decline, you cannot work with the management directory from the new workplace.

The migration may take several hours. If it cannot be completed (for example, because the computer is shut down at the end of the day), the migration will start again from the beginning at the next logon.

Before V1R4, the resource tree did not show systems but system profiles. Which system a system profile corresponded to was implied by the data that defined a system profile but not stated explicitly. In V1R4 all existing system profiles are assigned to the new system objects in the resource trees.

2. Depending on the context product sets are either packages or product homes, in the prior level of code.

Some system profiles included the information that is required for job submission, others did not include this information. In V1R4 all systems must include the information required for job submission.

As part of the management directory migration you are prompted to assign the existing system profiles to systems and to complete the system data if necessary.

You cannot continue to work with the services on systems and system profiles for which the information has not been completed.

You are also prompted to define an msys user administrator. This msys user administrator can later define other msys users, including other msys user administrators.

A copy of the old tree is saved as a backup. This enables you to revert to an earlier version of msys for Setup if necessary. As soon as it is decided that the migrated tree is to be used, an LDAP administrator can log on to the msys for Setup workplace and delete the backup copy of the old resource tree.

Migration actions for your z/OS systems

When adding the first z/OS V1R4 or later system to your management directory subtree you must install FMID JMSI743 on all z/OS systems that remain as z/OS V1R1, z/OS V1R2, or z/OS V1R3. The FMID enables these systems to coexist with z/OS V1R4 in the same management directory subtree. You cannot work with systems from the new subtree until you have installed FMID JMSI743.

You can obtain FMID JMSI743 as a Web deliverable at <http://www.ibm.com/servers/eserver/zseries/zos/downloads/>.

The V1R4 host code and the host code delivered with the FMID JMSI743 requires Java 1.3. Be sure that all z/OS systems run Java at this level.

Reinstalling the workplace

To support a V1R4 z/OS system in your environment you must replace all workplaces with the new level of code. With a backlevel workplace, you will not be able to log on to a management directory subtree that has been migrated to V1R4.

See Chapter 7, “Setting up the msys for Setup workplace” on page 33 for information on how to install a new workplace.

Chapter 10. Applying service to msys for Setup

This section provides information on how to service the msys for Setup framework, FMID HMSI707 or FMID JMSI743, and its prerequisite software.

For information on service for the plug-ins that are provided by msys for Setup enabled products refer to the documentation of the respective service.

Recommendation: FMID JMSI743 makes the V1R4 enhancements for msys for Setup available on V1R1, V1R2, and V1R3 systems. Install FMID JMSI743 on all systems of these levels that you are using or intending to use msys for Setup. Be aware of the information in Chapter 9, “Migrating from a prior msys for Setup release” on page 47 before you begin.

What to service

Apart from msys for Setup framework PTFs, ensure that the requisite PTFs for the following are applied:

- LDAP server
- Java
- XCF MIGLIB
- DFSMS
- TCP/IP
- z/OS UNIX

How to prepare for service?

msys for Setup PTFs may be large. Your z/OS system programmer must ensure that you have at least 100 MB space in the SMP/E PTF Temporary Storage (PTS).

Before applying PTFs, refer to the z/OS PSP Bucket for SUBSET MSYS for the z/OS release of the respective system.

Where to get service

Because msys for Setup is a base element of z/OS, PTFs can be ordered and obtained through the usual channels for z/OS PTFs.

Servicing the workplace

Whenever a new PTF for the msys for Setup framework is applied, the workplace code must be refreshed after the successful application of the PTF.

Every time a job is submitted from a workplace, the compatibility of the msys for Setup workplace and the z/OS system where the host code runs is verified. If the workplace is backlevel, msys for Setup issues an error message. To proceed further the workplace user must download and install the latest version of msys for Setup workplace (see “Downloading the workplace” on page 34). Inform all users after applying a PTF.

All workplaces that work with the same management directory subtree must be at the same level of code.

If you have to deinstall a PTF with SMP/E after a workplace has been updated, the new workplace no longer matches the version of the host code. You must then restore the older level of the workplace by reinstalling it from the host code after deinstalling the PTF. Because the management directory keeps a record of the latest level of workplace that it has accessed it and always requires the latest level, you have to inform it that an older level had to be restored.

Steps for accessing the management directory after deinstalling a PTF

Perform these steps to access the management directory with a workplace that has been restored to an earlier level because a PTF had to be deinstalled:

1. With the workplace closed, go to the directory where you have installed the workplace.

2. Locate file Workplace.properties and open it with your favorite text editor.

3. Locate the following line:
`VersionCheck=ENABLED`

and change it to:
`VersionCheck=DISABLE`

4. Save your changes and close the file.

Result: When you next log on to the management directory the logon is permitted and the record of the latest level of the workplace that has logged on to the management directory is reset to the current level of the workplace.

Keeping the LDAP schema up to date

A PTF for msys for Setup or a new release of z/OS might require an update of the LDAP schema. If this is the case, msys for Setup asks the first user who attempts to log on to Setup whether an automatic update of the management directory to the new schema should be initiated.

The user can only access the management directory after the schema update has been performed.

Updating the schema requires LDAP administrator rights. The update needs to be done once only for an LDAP server, from any workplace.

Part 4. Appendixes

Appendix A. LDAP connection worksheet

The first part of this worksheet summarizes the information that is required by any msys for Setup user who wants to connect to an LDAP server from a particular workplace for the first time. The second part is for the LDAP administrator who wants to log on to an LDAP server from the workplace, for example to create a management directory subtree (see Chapter 8, “Creating a new management directory subtree” on page 39).

Fill in this worksheet when you edit the LDAP server profile files (see “Adapting the LDAP profile files” on page 21). Complement the information for the msys for Setup user administrator after creating the management directory subtree.

Connecting to the LDAP server		
LDAP server host name or IP address		
LDAP server port		Source: ldap.msys.slapd.profile Default: 3389
LDAP suffix (TDBM suffix)		Source: ldap.msys.profile Default: "ou=msys,o=ibm,c=us"
Security suffix (SDBM suffix)		Only applicable if the LDAP server is protected by RACF Source: ldap.msys.profile Default: "sysplex=msysplex"
msys for Setup user administrator ID		Defined during the Chapter 8, “Creating a new management directory subtree” on page 39 task
msys for Setup user administrator password	Memorize this password	Only applicable if the LDAP server is <i>not</i> protected by RACF Defined during the Chapter 8, “Creating a new management directory subtree” on page 39 task
LDAP Administrator information		
LDAP administrator user ID		Source: ldap.msys.profile
LDAP administrator password	Memorize this password	Only applicable if the LDAP server is <i>not</i> protected by RACF Source: ldap.msys.profile

Appendix B. Worksheet for editing the LDAP profile files

This worksheet is for the administrator setting up the LDAP server for msys for Setup. Compile the information for this worksheet before you start to edit your configuration files (see "Adapting the LDAP profile files" on page 21).

Consult your database administrator to determine if the values are suitable for your DB2 installation.

Table 2. Worksheet for setting up LDAP server for msys for Setup

Information required for ldap.msys.profile		
Keyword="default"	Description	What to enter
OUTPUT_DATASET= "GLD.CNFOUT"	Name of data set where all configuration utility output will be placed. Check if you have write access to a data set with this name. ldapcnf will allocate it during runtime.	
GLDHLQ= "GLD"	High-level qualifier of the LDAP server data sets.	
DSN_SDSNEXITHLQ= "DSN610"	High-level qualifier of the DB2 SDSNEXIT data sets.	
DSN_SDSNLOADHLQ= "DSN610"	High-level qualifier of the DB2 SDSNLOAD data sets.	
DSN_SDSNDBRMHLQ= "DSN610"	High-level qualifier of the DB2 SDSNDBRM data sets.	
DSN_SSID="DSN6"	DB2 subsystem name.	
CEEHLQ="CEE"	High-level qualifier of Language Environment® data sets.	
CBCHLQ="CBC"	High-level qualifier of C++ Library data sets.	
ADMINDN= "racfid= ADMIN, profiletype=user,sysplex= msysplex"	The Distinguished Name (DN) of the LDAP administrator. You have to substitute the user name of the LDAP administrator for ADMIN . This user ID must already exist in the RACF subsystem the LDAP server uses. It will not be created through ldapcnf.	

Table 2. Worksheet for setting up LDAP server for msys for Setup (continued)

Information required for ldap.msys.profile		
PROG_SUFFIX=""	Suffix of the PROG member to be created in the output data set. The PROG member contains the APF authorization statements required for an LDAP server. After ldapcnf completes successfully, the PROG member should be copied to the target system's PARMLIB prior to submitting the APF JCL job.	
APF_JOBCARD_1="" PRGCTRL_JOBCARD_1="" DB2_JOBCARD_1="" RACF_JOBCARD_1=""	These are job cards for the output JCL jobs that will be produced. Enter a valid job card that conforms to the policies of your shop, e.g. "//MSYSAPF JOB MSGCLASS=H,MSGLEVEL=(1,1)"	

Table 3. ldap.msys.db2.profile

Information required for ldap.msys.db2.profile		
Item	Description	What to enter
TDBM_DB2_LOCATION=" LOC1"	DB2 server location (or data source).	
TDBM_DB2_ENTRYBUFFERPOOL="BP0"	Name of LDAP entry tablespace buffer pool. You do not have to change these lines unless you want DB2 to use a different buffer pool, for example, for performance reasons. Check with your database administrator if the values are suitable for your DB2 installation.	
There are similar lines for all other tables spaces.	You do not have to change these lines unless you want DB2 to use a different buffer pool, for example, for performance reasons.	

Appendix C. Worksheet for product set installation data

This worksheet is for the product set administrator who makes installed products or sets of products known to msys for Setup.

Fill in this worksheet as you are:

- Installing a CustomPac order
- Installing a product or product set with SMP/E
- Installing a product or product set that includes an XML document with a description, using any install mechanism
- Cloning a product set

Table 4. Worksheet for providing install information to the product set administrator

Description of the installed product set	
System on which the product set has been installed or systems that share the installation (SYSNAME)	
If an up-to-date product definition XML document with a product set description exists	
Data set or member that contains the XML document	
Volser where the data set with the XML document resides (only if not cataloged or catalogs are not shared)	
For SMP/E installed product sets for which there is no product definition XML	
Global CSI data set	
Target zones	
HLQs for <ul style="list-style-type: none"> • SMP/E product • ISPF product • Order dialog data sets • Master dialog data sets 	
For cloned product sets	

Table 4. Worksheet for providing install information to the product set administrator (continued)

Mapping of source to target volumes	
Mapping of source to target HLQs	
Path information changes	

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Deutschland
Informationssysteme GmbH
Department 3982

Pascalstrasse 100
70569 Stuttgart
Germany

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement or any equivalent agreement between us.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

Database 2	IBMLink	RACF
DB2	Language Environment	Resource Link
DB2 Universal Database	MVS	RETAIN
DFSORT	OS/390	SystemPac
FunctionPac	Parallel Sysplex	VM/ESA
IBM	ProductPac	z/OS

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Where to find more information

This section lists books that can be of help to you. For the most recent information on msys for Setup, see the msys for Setup home page:

<http://www.ibm.com/servers/eserver/zseries/msys>

Other useful homepages include:

- <http://www.ibm.com/servers/eserver/zseries/zos> - z/OS home page
- <http://www.ibm.com/s390/products/psa/> - Parallel Sysplex home page

Managed System Infrastructure for Setup publications

Title	Order Number
<i>z/OS Managed System Infrastructure for Setup User's Guide</i>	SC33-7985
<i>z/OS Managed System Infrastructure for Setup Installation</i>	SC33-7997
<i>z/OS Managed System Infrastructure for Setup Messages</i>	SC33-7996

Related z/OS publications

This section lists books that can be useful when planning for installation and after installation.

Table 5. Books for installation

Title	Order Number
<i>z/OS UNIX System Services Planning</i>	GA22-7800
<i>z/OS MVS Initialization and Tuning Reference</i>	SA22-7592
<i>z/OS MVS Migration</i>	GA22-7580

Table 6. LDAP books

<i>z/OS Security Server LDAP Server Administration and Use</i>	SC24-5923
<i>Understanding LDAP</i>	SG24-4986
<i>LDAP Implementation Cookbook</i>	SG24-5110

Table 7. DB2 books

<i>DB2 Installation Guide</i>	GC26-9936
<i>DB2 Administration Guide</i>	SC26-9931

Accessing Books on the Internet

In addition to making softcopy books available on CD-ROM and tape, IBM provides access to z/OS softcopy books on the Internet.

Refer to the z/OS home page

(<http://www.ibm.com/servers/eserver/zseries/zos/>) from which softcopy books

can be accessed. The library pages include PDF (Portable Document Format) versions of the current books which you can download.

IBM Systems Center publications (redbooks) are available in softcopy at this website: <http://www.redbooks.ibm.com/>.

Accessing z/OS licensed documents on the Internet

z/OS licensed documentation is available on the Internet in PDF format at the IBM Resource Link™ Web site at:

<http://www.ibm.com/servers/resourceLink>

Licensed documents are available only to customers with a z/OS license. Access to these documents requires an IBM Resource Link user ID and password, and a key code. With your z/OS order you received a Memo to Licensees, (GI10-0671), that includes this key code.³

To obtain your IBM Resource Link user ID and password, log on to:

<http://www.ibm.com/servers/resourceLink>

To register for access to the z/OS licensed documents:

1. Sign in to Resource Link using your Resource Link user ID and password.
2. Select **User Profiles** located on the left-hand navigation bar.

Note: You cannot access the z/OS licensed documents unless you have registered for access to them and received an e-mail confirmation informing you that your request has been processed.

Printed licensed documents are not available from IBM.

You can use the PDF format on either **z/OS Licensed Product Library CD-ROM** or IBM Resource Link to print licensed documents.

Using LookAt to look up message explanations

LookAt is an online facility that allows you to look up explanations for most messages you encounter, as well as for some system abends and codes. Using LookAt to find information is faster than a conventional search because in most cases LookAt goes directly to the message explanation.

You can access LookAt from the Internet at:

<http://www.ibm.com/eserver/zseries/zos/bkserv/lookat/>

or from anywhere in z/OS where you can access a TSO/E command line (for example, TSO/E prompt, ISPF, z/OS UNIX System Services running OMVS). You can also download code from the *z/OS Collection* (SK3T-4269) and the LookAt Web site that will allow you to access LookAt from a handheld computer (Palm Pilot VIIx suggested).

To use LookAt as a TSO/E command, you must have LookAt installed on your host system. You can obtain the LookAt code for TSO/E from a disk on your *z/OS Collection* (SK3T-4269) or from the **News** section on the LookAt Web site.

3. z/OS.e™ customers received a Memo to Licensees, (GI10-0684) that includes this key code.

Some messages have information in more than one document. For those messages, LookAt displays a list of documents in which the message appears.

Index

A

APF, Java DLL 27
ASSIZEMAX 29
authorizations, for msys for Setup users 30

C

CIMAPFJ 27
cimsetup.exe 34
class
 choose for JES job 29
cloned systems 17
communications 7
connections 7
CustomPac 17

D

DB2 4
documents, licensed 64

F

firewalls 8
FTPD server on the z/OS system 7
FunctionPac 17

H

hardware requirements
 workplace 13
host name
 TCP/IP 33

I

Installing msys for Setup 15

J

Java DLL, authorizing 27
JES job class
 choosing 29
job class
 JES, choosing 29

L

LDAP connection 42
 setting up 39
 worksheet 55
LDAP server
 ldapcnf 21
 setting up a new 21
 system requirements 12
ldap worksheet 57

ldapcnf
 editing profile files 21
 running 22
licensed documents 64
LookAt message retrieval tool 64

M

management directory
 initialize 39
MAXCPUPTIME 29
MAXFILEPROC 29
MAXPROCSYS 29
MAXPROCUSER 29
message retrieval tool, LookAt 64
msys for Setup users
 set up UNIX System Services 29

P

Parallel Sysplex authorizations 30
product installation worksheet 59
ProductPac 17

R

RACF authorizations 30
requirements 11
restrictions
 z/OS system 18

S

Secure socket layer 8
security
 communications 8
 z/OS system 12
ServerPac 17
software requirements
 workplace 13
SSL 8
subtree in management directory
 msys for Setup 39
system requirements 11
 for z/OS system running LDAP server 12
SystemPac 17

T

TCP/IP
 ensuring that the workstation is defined 33
 verifying the connection to the LDAP server 34
TCP/IP connections 7
TDBM 4
trademarks 62

U

UNIX System Services
 msys for Setup users 29
User authorizations on z/OS systems 30
user ID
 setup UNIX System Services for msys 29

W

workplace
 downloading the code 34
 installing 36
 installing and initializing 33
 requirements 13
worksheet
 LDAP connection 55
 product installation 59
workstation
 requirements 13

Z

z/OS system 11
restrictions 18
user authorizations 30

Readers' Comments — We'd Like to Hear from You

z/OS
Managed System Infrastructure for Setup
Installation
Version 1 Release 4

Publication No. SC33-7997-00

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	<input type="checkbox"/>				

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	<input type="checkbox"/>				
Complete	<input type="checkbox"/>				
Easy to find	<input type="checkbox"/>				
Easy to understand	<input type="checkbox"/>				
Well organized	<input type="checkbox"/>				
Applicable to your tasks	<input type="checkbox"/>				

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? Yes No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name

Address

Company or Organization

Phone No.



Fold and Tape

Please do not staple

Fold and Tape

PLACE
POSTAGE
STAMP
HERE

IBM Deutschland Entwicklung GmbH
Information Development
Department 3248
Schoenaicher Strasse 220
71032 Boeblingen
Germany

Fold and Tape

Please do not staple

Fold and Tape



Program Number: 5694-A01, 5655-G52

SC33-7997-00

