z/OS

DCE Configuring and Getting Started

SC24-5910-00

z/OS

DCE Configuring and Getting Started

SC24-5910-00

Note

Before using this information and the product it supports, be sure to read the general information under Appendix E, “Notices” on page 123.

First Edition (March 2001)

This edition, SC24-5910-00, applies to Version 1 Release 1 of z/OS DCE Base Services, z/OS DCE user Data Privacy (DES and CDMF), z/OS DCE User Data Privacy (CDMF) (program number 5694-A01), 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.

IBM welcomes your comments. A form for reader's comments may be provided at the back of this publication, or you may address your comments to the following address:

International Business Machines Corporation
Information Development, Dept. G60
1701 North Street
Endicott, NY 13760-5553
United States of America

FAX (United States & Canada): 1+607+752-2327
FAX (Other Countries):
Your International Access Code +1+607+752-2327

IBMLink™ (United States customers only): GDLVME(PUBRCF)
Internet e-mail: pubrcf@vnet.ibm.com
World Wide Web: http://www.ibm.com/servers/eserver/zseries/zos/

If you would like a reply, be sure to include your name, address, telephone number, or FAX number.

Make sure to include the following in your comment or note:

- Title and order number of this book
- Page number or topic related to your comment

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

The following statements are provided by the Open Software Foundation.

Contents

Figures

Tables

About This Book

This book will help system and network administrators configure z/OS DCE. This book is used after the successful installation of the z/OS DCE. Installation is described in the *z/OS Program Directory*.

Who Should Use This Book

This book is intended for system administrators who understand the basic concepts of the Distributed Computing Environment (DCE). A knowledge of TCP/IP communications will also help administrators to use this book more effectively. Administrators who have little or no experience with Distributed Computing Environment (DCE) are advised to read *z/OS DCE Introduction*, GC24-5911, before using this book.

How to Use This Book

This book provides overview information on configuring z/OS DCE, and takes you through the steps you will perform to prepare for configuration and to configure DCE. You can use the DCECONF configuration program to configure DCE by using interactive ISPF panels or from the TSO command line or batch. Appendix A, "Files and Namespace Entries Created at Configuration" on page 79 provides information on files that the DCECONF program creates. This book also provides information on setting up the registry in the security service, and information on RACF® interoperability. (RACF is a component of the SecureWay® Security Server for z/OS.)

In this book the term "DCE Security Server" (or simply "Security Server") refers to the z/OS SecureWay Security Server DCE or to a DCE Security Server provided on another host in the DCE cell. The z/OS SecureWay Security Server DCE is a component of the SecureWay Security Server for z/OS.

Any reference to DCE in this book is understood to specifically mean DCE for the IBM z/OS operating system, unless otherwise noted.

Product Names

The product name **z/OS DCE** refers to the DCE services on z/OS.

Conventions Used in This Book

This book uses the following typographic conventions:

Bold	**Bold** words or characters represent system elements that you must enter into the system literally, such as commands, options, or path names.
Italic	*Italic* words or characters represent values for variables.
`Example font`	Examples and information displayed by the system appear in `constant width type style`.
[ ]	Brackets enclose optional items in format and syntax descriptions.
{ }	Braces enclose a list from which you must choose an item in format and syntax descriptions.
|	A vertical bar separates items in a list of choices.

< >	Angle brackets enclose the name of a key on the keyboard.
...	Horizontal ellipsis points indicate that you can repeat the preceding item one or more times.
\	A backslash is used as a continuation character when entering commands from the shell that exceed one line (255 characters). If the command exceeds one line, use the backslash character **** as the last non-blank character on the line to be continued, and continue the command on the next line.

This book uses the following keying conventions:

<**Alt-***c*>	The notation <**Alt-***c*> followed by the name of a key indicates a control character sequence.
<**Return**>	The notation <**Return**> refers to the key on your keyboard that is labeled with the word Return or Enter, or with a left arrow.
Entering commands	When instructed to enter a command, type the command name and then press <**Return**>.

Where to Find More Information

Where necessary, this book references information in other books using shortened versions of the book title. For complete titles and order numbers of the books for all products that are part of z/OS, see the *z/OS Information Roadmap*, SA22-7500. For complete titles and order numbers of the books for z/OS DCE, refer to the publications listed in the “Bibliography” on page 135.

For information about installing z/OS DCE components, see the *z/OS Program Directory*.

To understand most of the topics that are covered in this book, refer to the *z/OS DCE Administration Guide*.

For information about planning for DCE components, refer to *z/OS DCE Planning*. For information about administrative commands and syntax, refer to the *z/OS DCE Command Reference*.

Information about DCE configuration on other IBM systems can be found in the configuration guide for those systems.

Softcopy Publications

The z/OS DCE library is available on a CD-ROM, *z/OS Collection*, SK3T-4269. The CD-ROM online library collection is a set of unlicensed books for z/OS and related products that includes the IBM Library Reader.™ This is a program that enables you to view the BookManager® files. This CD-ROM also contains the Portable Document Format (PDF) files. You can view or print these files with the Adobe Acrobat reader.

Internet Sources

The Softcopy z/OS publications are also available for web-browsing and for viewing or printing PDFs using the following URL:

`http://www.ibm.com/servers/eserver/zseries/zos/bkserv/`

You can also provide comments about this book and any other z/OS documentation by visiting that URL. Your feedback is important in helping to provide the most accurate and high-quality information.

Using LookAt to Look up Message Explanations

LookAt is an online facility that allows you to look up explanations for z/OS messages. You can also use LookAt to look up explanations of system abends.

Using LookAt to find information is faster than a conventional search because LookAt goes directly to the explanation.

LookAt can be accessed from the Internet or from a TSO command line.

You can use LookAt on the Internet at:

`http://www.ibm.com/servers/eserver/zseries/zos/bkserv/lookat/lookat.html`

To use LookAt as a TSO command, LookAt must be installed on your host system. You can obtain the LookAt code for TSO from the LookAt Web site by clicking on the **News and Help** link or from the *z/OS Collection*, SK3T-4269.

To find a message explanation from a TSO command line, simply enter: **lookat** *message-id* as in the following:

```
lookat iec192i
```

This results in direct access to the message explanation for message IEC192I.

To find a message explanation from the LookAt Web site, simply enter the message ID and select the release with which you are working.

Note: Some messages have information in more than one book. For example, IEC192I has routing and descriptor codes listed in *z/OS MVS Routing and Descriptor Codes*, SA22-7624. For such messages, LookAt prompts you to choose which book to open.

Accessing Licensed Books on the Web

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

`http://www.ibm.com/servers/resourcelink`

Licensed books are available only to customers with a z/OS license. Access to these books requires an IBM Resource Link user ID, password, and z/OS licensed book key code. The z/OS order that you received provides a memo that includes your key code.

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

`http://www.ibm.com/servers/resourcelink`

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

1. Logon to Resource Link using your Resource Link user ID and password.
2. Select **User Profiles** located on the left-hand navigation bar.
3. Select **Access Profile**.
4. Select **Request Access to Licensed books**.
5. Supply your key code where requested and select the **Submit** button.

If you supplied the correct key code you will receive confirmation that your request is being processed.

After your request is processed you will receive an e-mail confirmation.

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

To access the licensed books:

1. Logon to Resource Link using your Resource Link user ID and password.
2. Select **Library**.
3. Select **zSeries**.
4. Select **Software**.
5. Select **z/OS**.
6. Access the licensed book by selecting the appropriate element.

Chapter 1. Overview of the z/OS DCE Configuration

This chapter is an overview of the configuration of DCE on a z/OS host. It briefly describes the DCE concepts that are relevant to configuration. The **DCE Kernel** (**DCEKERN**) address space is described to show you how the DCE daemons are implemented in z/OS DCE. The **DCECONF** program configures the z/OS host. "Configuration Log File" on page 7 discusses the log file that DCECONF creates. You can use the **DCECONF** program to configure the z/OS host using interactive ISPF panels (see Chapter 3, "Using the DCECONF Configuration Panels" on page 21 for details) or from the TSO command line or batch (see Chapter 4, "Using DCECONF from the TSO Command Line or Batch" on page 45 for details).

What Is z/OS DCE?

The OSF Distributed Computing Environment (DCE) is a set of services that make up a high-level, coherent environment for developing and running distributed applications. It is based on a **client/server** model, where a client requests a service from a server. DCE provides a set of services that make this interaction possible. The four core services in DCE are Remote Procedure Call, Directory Service, Security Service, and Distributed Time Service. The elements of these services run as long-running processes or **daemons**.

z/OS DCE offers the DCE services that enable a z/OS host to operate as a member of a DCE cell. z/OS DCE includes the following daemons:

- DCE daemon
- Security server daemon
- CDS Advertiser daemon
- CDS Clerk daemon
- CDS daemon
- DTS Null Time Provider daemon
- DTS daemon (can be configured either as a server or a clerk)
- Audit daemon
- Password Management daemon
- GDA daemon.

DCE Cell

The basic unit of DCE operation is the **cell**, which is a logical grouping of users, computers, data, and other resources that share either a common purpose or a common level of trust. The cell provides security, administrative, and naming boundaries for users and resources within that cell. The DCE services are managed within the context of a cell. Figure 1 on page 2 illustrates a DCE cell.

Cell Name

Each DCE cell must have a unique name. DCE cell names may be expressed as X.500 names, such as **/.../C=US/O=MNO/L=Chicago**. They can also be Domain Name System (DNS) names, such as **/.../xyz.com**.

The name of the cell is specified during the **initial configuration of the cell**, that is, when the first Security and CDS servers are configured.

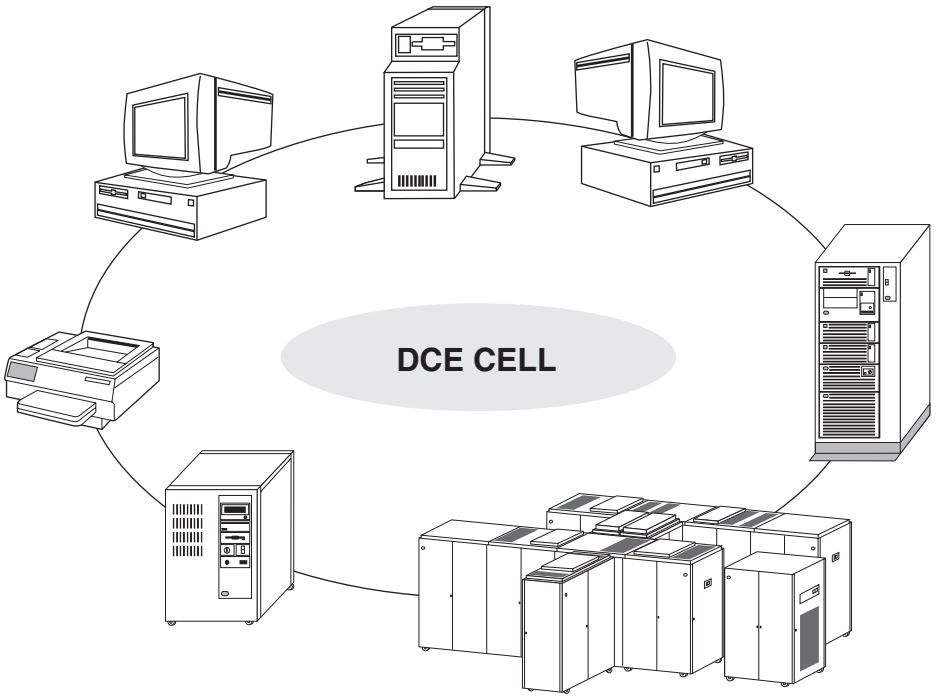

Figure 1. DCE Cell

Important

It is recommended that cells be assigned fully qualified X.500 or DNS names, for example, **/.../C=US/O=IBM/OU=Sales** (X.500) or **/.../foo.ibm.com** (DNS). The cell name is assigned during the initial configuration of the Security server.

For more information on naming cells, refer to *z/OS DCE Administration Guide*. The z/OS DCE configuration program requires as one of its inputs, the name of the DCE cell. The cell name should be entered without the leading **/.../**.

TCP/IP Host Addresses and Names

The Transmission Control Protocol/Internet Protocol (TCP/IP) is the underlying transport mechanism for reliable communication in DCE. TCP/IP addresses are used to locate DCE server and client host systems.

Each TCP/IP host has a unique address, a 32-bit integer expressed in the form *nnn.nnn.nnn.nnn*. The *nnn* represents the decimal value of each of the 4 bytes of the 32-bit address. This address is called the **Internet address**. The Internet address of the z/OS host is assigned during TCP/IP installation.

An alternative TCP/IP addressing scheme uses user-friendly names to identify host systems in the network. These are called TCP/IP names. They use a high-level naming method called the **Domain Naming System**, which uses meaningful, symbolic names to identify host machines. These names consist of a sequence of parts separated by periods, for example, **cello.finance.xyz.com**.

TCP/IP names use a hierarchical naming methodology which reflects the delegation of authority in administering these names. In our previous example, **cello.finance.xyz.com** is the **fully-qualified name** for the machine **cello** in the domain **finance.xyz.com**. The **simple name** of the host system is **cello**.

The configuration program displays panels that prompt for the TCP/IP names of the Security server host, CDS server host, and the z/OS host system that is being configured.

For more information on TCP/IP names, see *z/OS Communications Server: IP Configuration Reference*, SC31-8776.

The z/OS DCE configuration program uses the TCP/IP host names for two purposes:

- To look up the Internet addresses of the host systems from the TCP/IP tables. TCP/IP address tables resolve the mapping between Internet addresses and TCP/IP names. These tables may reside on the local host system, or can be searched from name servers in the TCP/IP network.
- As a basis for creating name entries for the host in the CDS and Security namespaces.

TCP/IP host names are case sensitive when used in the z/OS DCE configuration program. TCP/IP names must be entered in exactly the same way they were entered during TCP/IP installation.

Note: A DCE Cell is often a TCP/IP subnet (but not necessarily). When putting a z/OS host system in a cell, ensure that the z/OS TCP/IP subnet mask matches the subnet mask of the subnet to which it belongs.
Also, if the z/OS TCP/IP connection is through a point-to-point link, then z/OS TCP/IP and RPC cannot perform broadcasts.

Daemon Requirements in a DCE Cell

At the minimum, a DCE cell requires at least one Security server, one CDS server, and one DTS server. In this book, the host system that runs the Security server is called the Security server host, and the host system that runs the CDS server is called the CDS server host. The Security server host and the CDS server host can be running on two different machines or on the same machine within the cell. The typical daemon configuration in a cell is shown in Figure 2.

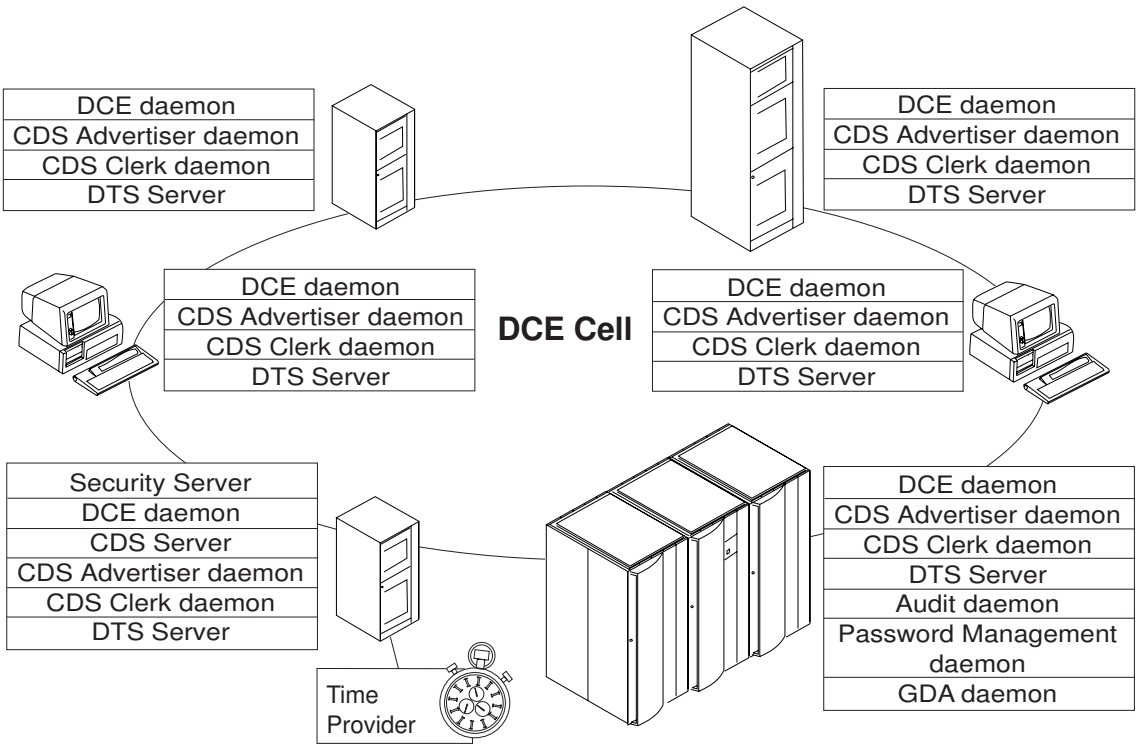

Figure 2. DCE Daemons in the Cell

The DCE client daemons that interact with the Security and CDS servers must run on every DCE host system. All daemons, their functions, and where they should be running are listed in Table 1.

Table 1 (Page 1 of 2). Functions and Locations of DCE Daemons

Daemon	Function	Where It Should Run
DCE daemon	Provides the **endpoint map** service for the system, and ensures that the credentials of the machine's principal are up-to-date, so that other DCE servers can act on behalf of the machine.	Every DCE host system must run the DCE daemon.
Security server daemon [1]	Provides support for authentication and controlled access to resources.	At least one Security server must be running in the cell.
CDS Advertiser daemon	Sends and receives advertisements on the availability of CDS servers.	Each DCE host system must run the CDS Advertiser daemon.
CDS Clerk daemon	Acts as the intermediary between the CDS client run time and the CDS server.	Each DCE host system must run the CDS Clerk daemon. In OSF DCE, the CDS Clerk daemon is a forked process that is created for each client that requests service from CDS. Thus, on hosts running OSF DCE, multiple CDS Clerk daemons can be running at any one time. In z/OS DCE, the CDS Clerk is a long-running process that serves all CDS clients. Only one CDS Clerk daemon runs on the z/OS DCE host system at any time.
Cell Directory Service daemon [1]	Provides directory services to DCE applications in the cell.	At least one CDS server must be running within the cell.
DTS Null Time Provider daemon	Obtains the time from the clock of the host system and gives it to the DTS daemon, if it runs as a server.	If configured, the DTS Null Time Provider daemon must run on the same machine as the DTS server.
DTS daemon	Ensures that the time on the host is synchronized with other machines in the cell.	At least one DTS daemon must be running in the cell. The DTS daemon can be configured either as a DTS server or DTS clerk. All DCE host systems must run the DTS daemon, configured either as a server or a clerk.
Audit daemon	Maintains a database of audit events. The type of events that are audited for various servers is controlled by a set of administrative commands.	The Audit daemon may be run on any host system in the DCE cell.
Password Management daemon	Enforce password management policies for DCE principals.	The Password Management daemon may be run on any host system in the DCE cell.

[1] The terms **Security server daemon** and **CDS daemon** are used in OSF DCE to refer to processes that provide security and directory services, respectively, in the cell as defined in OSF DCE. Other DCE platforms may use different terms to describe these services. Refer to the documentation provided by the platforms that offer these services.

Table 1 (Page 2 of 2). Functions and Locations of DCE Daemons

Daemon	Function	Where It Should Run
GDA daemon	Locates foreign cells in a multi-cell environment.	The GDA daemon may be run on any host system in the DCE cell.

Initial Cell Configuration

Configuring the initial Security and CDS servers is known as **Initial Cell Configuration**. The cell resulting from this configuration is called the **initial cell**. When the Security and CDS servers are configured, the DCE cell is initialized in the following manner:

- The Security registry database is created, and the principals, groups, organizations, and accounts that will be used by the DCE services, DCE host systems, and administrators are added to the Security registry.
- The CDS namespace is created, and the initial namespace entries, including RPC profile entries that will be used by DCE services, DCE host systems, and administrators, are added.

Important

If the z/OS system is configured as a DCE client machine and either the Security server host or the CDS server host is reconfigured for DCE, all entries for the z/OS host system in the Security registry and CDS namespace will be lost. You must reconfigure z/OS DCE on the z/OS host system.

DCE Kernel Address Space

All the z/OS DCE daemons are controlled by the Control Task running in the **DCE Kernel** (referred to as **DCEKERN**) address space. Figure 3 on page 6 illustrates the default structure of the DCEKERN address space. The dashed lines indicate daemons that run in their own address spaces but are controlled by the Control Task in the DCEKERN address space. All requests to start or stop the DCE daemons, either collectively or individually, are made through the Control Task.

The **dced**, **cdsadv**, **cdsclerk**, and **dtsd** daemons run as child processes of the Control Task within the DCEKERN address space. Each of the other daemons (**secd**, **cdsd**, **dtstp**, **auditd**, **pwdmgmt**, and **gdad**) can run, either as a child process of the Control Task in the DCEKERN address space, or as a process in its own address space. By default, **cdsd** and **secd** run in their own address spaces, while the others run as child processes of the Control Task. To override this default, use the **_EUV_DAEMONS_IN_AS** environment variable in DCEKERN's **envar** file.

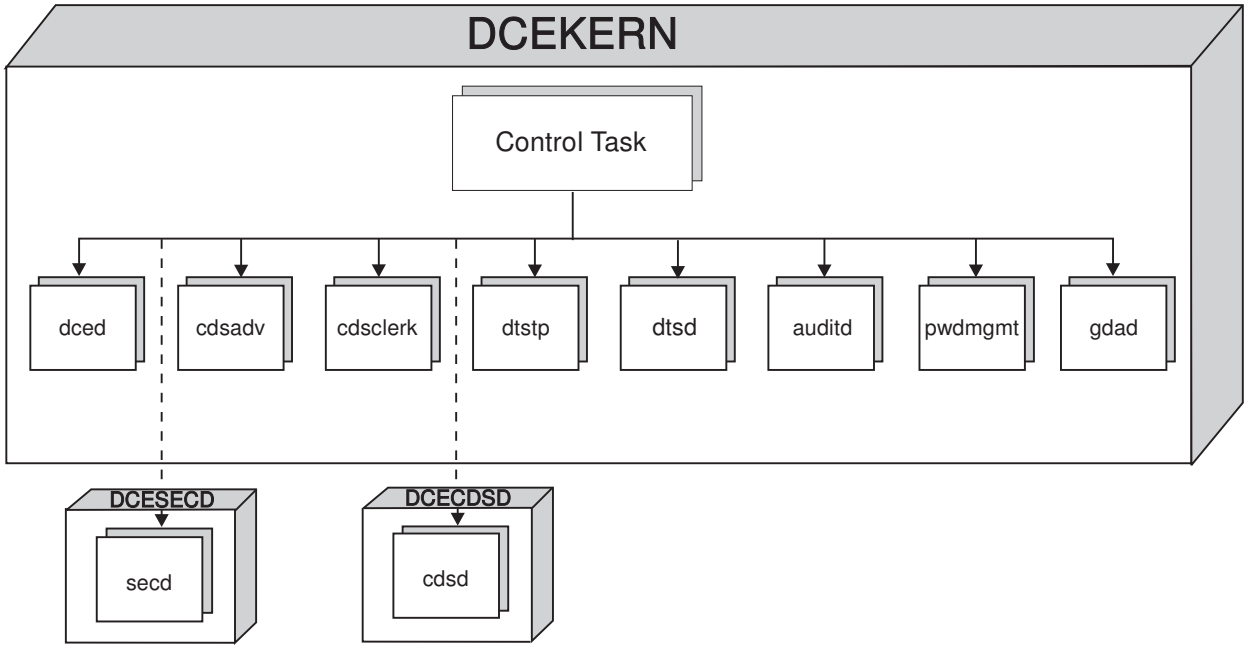

Figure 3. DCEKERN Address Space

Important

Before you can configure the z/OS DCE daemons, you must start the DCEKERN address space.

Variant Characters in Client Applications

If the DCE client applications will use variant characters, these clients must run in the same code page as the CDS Clerk daemon (cdsclerk). You can either set the locale when running the individual client processes or change the code page of DCEKERN.

To change the code page of DCEKERN, you must set the LANG environment variable for each of the z/OS DCE daemons. Each z/OS DCE daemon has an environment variable file in its home directory. The location of the daemons' environment variable files are listed in “Environment Variable Files for DCE Daemons” on page 7. You can set the environment variables for each daemon in the daemon's environment variable file. Setting environment variables is described in *z/OS DCE Administration Guide*.

For more information on variant characters in client applications, see *z/OS DCE Application Development Guide: Core Components*. For more information on the environment variable for setting code pages, see the description of LANG in the section on setting environment variables in the *z/OS DCE Administration Guide*.

RPC Server Group

In z/OS DCE, access to the Endpoint Map is controlled through Access Control Lists (ACLs). To facilitate the administration of authorized application servers that can access the Endpoint Map, a default Security group, referred in this book as the **RPC Server Group**, is created during z/OS DCE configuration. The name of this group is **subsys/dce/rpc-server-group**. For an application server to have the appropriate permissions to the Endpoint Map, it must be made a member of this group. For more information on the RPC server group, refer to *z/OS DCE Administration Guide*.

Configuration Log File

DCECONF creates a log file that details the steps that it performs in configuring or deconfiguring z/OS DCE on the host system. The log file is created in the home directory of the administrator who performed the configuration, with the file name **dceconf.log**. This path name can be modified using the **_EUV_CFG_LOG_FILE** environment variable. Setting DCECONF environment variables is discussed in "DCECONF Environment Variables" on page 14.

The configuration log file is a valuable tool in troubleshooting problems in z/OS DCE configuration. For examples of configuration log files, see Appendix B, "Example DCECONF Log Files" on page 85.

Environment Variable Files for DCE Daemons

Each DCE daemon has its own home directory. Each home directory contains the **environment variable file** (**envar**), where the environment variables are set for each of the daemons.

The envar files of the DCE daemons are:

- /opt/dcelocal/home/auditd/envar
- /opt/dcelocal/home/cdsadv/envar
- /opt/dcelocal/home/cdsclerk/envar
- /opt/dcelocal/home/cdsd/envar
- /opt/dcelocal/home/dced/envar
- /opt/dcelocal/home/dts_null_provider/envar
- /opt/dcelocal/home/dtsd/envar
- /opt/dcelocal/home/gdad/envar
- /opt/dcelocal/home/pwdmgmt/envar
- /opt/dcelocal/home/secd/envar

In addition, the DCEKERN Control Task has its own home directory and environment variable file: /opt/dcelocal/home/dcekern/envar.

Environment variable **_EUV_DAEMONS_IN_AS** can be added to this file to specify daemons that are to run in their own address space, rather than that of DCEKERN, in order to reduce contention for resources in DCEKERN's address space. The list can contain from none to all of the following:

- **auditd**
- **cdsd**
- **dtstp**
- **gdad**
- **pwdmgmt**
- **secd**

For example,

```
_EUV_DAEMONS_IN_AS=auditd cdsd secd
```

will cause only those 3 daemons to start in their own address spaces. You can modify the variable value at any time, stop DCEKERN if it is running, and then restart DCEKERN to change where a daemon is started.

If the **_EUV_DAEMONS_IN_AS** variable is not specified, the default is to run only **cdsd** and **secd** in their own address spaces. To override the default and run all daemons within DCEKERN's address space, specify:

```
_EUV_DAEMONS_IN_AS=N
```

Note that there are several daemons (**dced**, **cdsadv**, **cdsclerk**, and **dtsd**) that *only* run within the DCEKERN address space; these are ignored if specified in the variable.

Changing Environment Variable Files for DCE Daemons

Note: In z/OS DCE, use code page IBM-1047 when updating envar files.

Do not make changes to the default envar files in **/usr/lpp/dce/home/**, or you will lose your changes when you upgrade to the next release of z/OS DCE. For each release of z/OS DCE, all of the default envar files are shipped in **/usr/lpp/dce/home/**. Symbolic links (or *symlinks*) in **/etc/dce/home/** point to these envar files. In addition, on z/OS DCE, **/opt/dcelocal/home** is a link to **/etc/dce/home**.

To change the envar files:

1. Rename the envar symlink.
2. Copy the default file from **/usr/lpp/dce/home/***xxx***/envar** to **/etc/dce/home/***xxx***/envar** (*xxx* is a specific daemon). For example:

   ```
   >>cd/etc/dce/home/dced
   /etc/dce/home/dced>> mv envar envarold
   /etc/dce/home/dced>> cp envarold envar
   ```

3. Make your updates to the file just created in /etc/.

Chapter 2. Preparing for Configuration

This chapter describes the prerequisites for a successful z/OS DCE configuration and the steps you follow to prepare a z/OS host system for configuration. A worksheet is provided on page 13 to help you with this task.

Prerequisites for Configuring the DCE Daemons

Before configuring the DCE daemons, make sure that the following prerequisites are satisfied:

- z/OS DCE and all its software prerequisites were installed on the host system. All the installation procedures described in *z/OS Program Directory* were performed.
- If the Security server is not going to be configured on the z/OS host, the Security Server daemon (**secd**) was configured and is running on another machine in the DCE cell. In addition, at least one DTS daemon is configured as a server and running on another machine in the DCE cell.
- If **secd** is going to be configured on the z/OS host, and the CDS server daemon (**cdsd**) is not, **secd** must be configured on this host before **cdsd** is configured on the other machine.
- If neither **secd** nor **cdsd** is going to be configured on the z/OS host, they must be configured on another machine before other daemons are configured.
- If **gdad** is going to be configured on the z/OS host, **dced** must be configured on this host first.
- The z/OS UNIX and TCP/IP parameters were configured as indicated in the *z/OS Program Directory*.
- The z/OS UNIX kernel address space was started on the host system.
- The TCP/IP address space was started on the host system and has successfully connected to the z/OS UNIX kernel address space.
- The **/opt/dcelocal/etc/rpc_interfaces** control file was created if DCE is not supposed to use all of the available network interfaces.
- The DCEKERN address space was started.

Parameters for z/OS DCE and TCP/IP

The *z/OS Program Directory* provides the details of the z/OS DCE and TCP/IP parameters that must be reset from the default values for z/OS DCE.

DCE requires the use of TCP/IP port 135. Be sure that the data set **hlq.PROFILE.TCPIP** does not reserve port 135 for another application. See *z/OS Communications Server: IP Configuration Guide*, SC31-8775, for information about the PORT statement in the profile.

Both the **MAXTHREADTASKS** and **MAXTHREADS** parameters of z/OS DCE are recommended to be set to 500. You may need more if you have a large number of z/OS clients. If you notice **pthread_create()** failures while running DCEKERN, you may have to increase this number. In doing so, however, you should consider the increased storage demands of DCE servers running on your system (because of the increase in the number of initial threads created). Refer to the *z/OS DCE Application Development Guide: Core Components* for this information.

Also, DCE does not run properly if you run out of TCP/IP envelopes. Make sure that you have a sufficient number of envelopes to handle DCE traffic.

How to Prepare for Configuration

Following is a step-by-step description of how you can prepare the z/OS host system for z/OS DCE configuration.

1. Know Your Cell Configuration Plans

Be aware of your cell configuration plans. Plans for your cell configuration include information on the size and boundaries of your cell, where to run the DCE and application servers, and time provider considerations. How to plan your DCE configuration is discussed in *z/OS DCE Planning*.

2. Obtain DCE and Host Information

The z/OS DCE configuration program prompts you for certain DCE and network-related information. You must have the following information ready:

- If the Security server is not going to be configured on the z/OS host, the cell name, and the **Cell Admin ID** and **Password** of the administrator. Because DCE configuration involves accessing sensitive DCE databases and resources, configuration must be performed by privileged users only. The Cell Admin ID is a special principal. It has all the required access privileges to perform DCE configuration tasks. The default Cell Admin ID is **cell_admin**.

  Note: If the Security server is going to be configured on the z/OS host, you will be asked to select the cell name, and the Cell Admin ID and Password.
- The TCP/IP name of the z/OS host to be configured. (TCP/IP names are briefly described in "TCP/IP Host Addresses and Names" on page 2.)
- The DCE name of the z/OS host to be configured. The default DCE name is the TCP/IP name of the z/OS host; however, the two names do not have to be the same.
- If the Security server is not going to be configured on the z/OS host, the name of the cell that the z/OS host is about to be configured into.

  Note: If the Security server is going to be configured on the z/OS host, you will be asked to select the name for your DCE cell.
- If the Security server is not going to be configured on the z/OS host, the TCP/IP name or address of the host where the Security server is running in the DCE cell.
- If the CDS server is not going to be configured on the z/OS host, the TCP/IP name or address of the host where the CDS server is running in the cell.

3. Set the Correct Time Zone

During the installation of the z/OS DCE product, the time zone is set to **GMT0**.

You must set the **TZ** environment variable to the appropriate time zone in the environment variable file (**envar**) of DCEKERN and each individual daemon. The envar file is in the home directory of DCEKERN and the daemons. The home directories of DCEKERN and the daemons are in **/opt/dcelocal/home**. If you do not set TZ in these envar files, the messages sent to stdout (but not the console log) will be time stamped relative to Greenwich Mean Time (GMT), not local time, or, in some cases, DCE may not even start. By default, only DCEKERN messages with severities of **svc_c_sev_warning** and **svc_c_sev_notice_verbose** are directed to stdout.

4. Adjust Any Time Difference with the Security Server Host

If the z/OS host is not going to be configured as the Security Server of the DCE cell, ensure that the z/OS host software clock (TOD clock) is within five minutes of the clock on the host where the Security server is running. These time values must be the GMT relative times between the z/OS host system and the Security server host. If the difference between these two clocks is more than five minutes, authentication errors may result and configuration will not succeed.

You can either change the clock of the Security server host, in which case you will have to reconfigure the DCE cell, or change the clock on the local z/OS host. The DCE software clock on the z/OS host can be changed using the MODIFY DCEKERN CLOCK operator command.

Note: If you want the z/OS host to be the source of reliable time in the cell (that is, if you want to propagate the z/OS host time to other hosts in the cell), you must change the clock of the Security Server host, not the software clock of the z/OS host.

MODIFY DCEKERN CLOCK Command: Use the SET option of this command to change the software clock as follows:

MODIFY DCEKERN, CLOCK SET *time-value*

where *time-value* is the new time in UT C format, for example:

MODIFY DCEKERN, CLOCK SET 1994-11-21-13:30:25

You can also use the **relative time** using the **SETREL** option of this command.

The UTC time formats are described in *z/OS DCE Administration Guide*. For a more detailed description of the MODIFY DCEKERN CLOCK command, see *z/OS DCE Command Reference*.

5. Determine If You Have Access to a Reliable Time Source

If you configure the DTS daemon as a server entity, you will be prompted if you want to configure and start the Null Time Provider daemon. If your host system is already a recipient of reliable time, such as in a sysplex environment with ETR, you may want to configure and start the Null Time Provider daemon, which takes this already-reliable time and gives it to the DTS daemon.

Note: You can also choose to use your own time provider program (instead of the Null Time Provider daemon). In this case, you will have to manually edit the **Daemon Configuration File**, **/opt/dcelocal/etc/euvpdcf**, and enter the load module name of the time provider program in the load module field of the file. If you use your own time provider, you are recommended to run the **dtstp** daemon within the DCEKERN address space; to do this, ensure that **dtstp** is *not* specified in the **_EUV_DAEMONS_IN_AS** variable in the /opt/dcelocal/home/dcekern/envar file.

The Daemon Configuration File is discussed in “Daemon Configuration File” on page 18.

6. Set Up the DCECONF Administrator TSO User ID

You must set up a TSO user ID that has authority to run **DCECONF**, the z/OS DCE configuration program.

Following are the specifics of the TSO user ID that has authority to run DCECONF, the DCECONF administrator:

- The DCECONF administrator must be defined to the Security subsystem as a z/OS UNIX user. You can use the ADDUSER or ALTUSER commands to create or modify z/OS UNIX user accounts. With

this command, you can specify z/OS UNIX-specific information for the user such as the home directory and the z/OS UNIX user identifier.

- The DCECONF administrator must have a superuser ID. In z/OS UNIX, the superuser or root has a user identifier (UID) of zero (0). A user can be accorded superuser privileges by specifying zero in the UID parameter of the ADDUSER or ALTUSER commands.
- Add the SEUVPNL data set to the ISPPLIB concatenation.
- Add the SEUVMSG data set to the ISPMLIB concatenation.
- Add the SEUVEXEC library to the SYSEXEC or SYSPROC concatenation.

  Note: Avoid mixing RECFM=VB and RECFM=FB data sets in the SYSEXEC or SYSPROC concatenation. Follow the instructions in the *z/OS Program Directory*.
- Allocate a **CEEDUMP** data set. For example, in the DCECONF administrator's logon CLIST:

  ```
  "ALLOC   FI(CEEDUMP) DS(MYFILE) SHR"
  ```

  The suggested parameters for a 3390 DASD volume are:

  – Record format = FB

  – Record length = 133

  – Block size = 0

  – Size = 1 CYL
- Give the DCECONF administrator update authority to the **DCEKERN.START.REQUEST** Security facility. This facility is created during the installation of z/OS DCE. It is described in *z/OS Program Directory*. It determines if a TSO user has the necessary permissions to start or stop the z/OS DCE daemons in the DCEKERN address space.

  If you want to use a facility name other than **DCEKERN.START.REQUEST**, you must set the **_EUV_RACF_FACILITY_NAME** environment variable to the facility name. You must set this variable in the **envar** file of DCEKERN before starting DCEKERN. The path name of this envar file is **/opt/dcelocal/home/dcekern/envar**.

  DCECONF uses the data set that defines TCP/IP system parameters that client programs need. You can define this data set in one of the following ways:

  – By setting the environment variable RESOLVER_CONFIG to the data set name:

    ```
    RESOLVER_CONFIG=hlq.TCPIP.DATA
    ```

    The *hlq* is the high-level qualifier, and TCPIP.DATA is a sample data set name.

  – By specifying a DDNAME of SYSTCPD.

    Your system-wide TSO user or batch job profiles can define SYSTCPD. If they do not, you can specify it:

    - From the TSO command line:

      ```
      ALLOC FILE(SYSTCPD) DA('hlq.TCPIP.DATA') SHR
      ```

    - In a batch job:

      ```
      //SYSTCPD DD DSN=hlq.TCPIP.DATA, DISP=SHR
      ```

  The DCE administrator needs access to DCE resources. To access the DCE resources required by **DCECONF**, you must be a member of the **subsys/dce/cds-admin**, **subsys/dce/sec-admin**, and **acct-admin** Security groups. This requirement is satisfied if you enter the correct Cell Admin ID and Password in the fields provided by the DCE Configuration Menu.

- Set the DCECONF environment variables. This is optional. You can set environment variables to pass the host information described in "2. Obtain DCE and Host Information" on page 10 to the z/OS DCE configuration program, as well as to influence the behavior of the configuration program. See "DCECONF Environment Variables" on page 14 for more information.

z/OS DCE Configuration Worksheet

This section contains a worksheet you can use when preparing for z/OS DCE configuration.

Table 2 (Page 1 of 2). DCE Configuration Worksheet (Required)	
Required Information: (Enter Information in Column 2)	
Cell Admin ID	
Cell Admin Password	
Cell Name	
TCP/IP Name of z/OS Host	
DCE Name of z/OS Host	
TCP/IP Name of Security Server Host, or Internet Address of Security Server Host	
TCP/IP Name of CDS Server Host, or Internet Address of CDS Server Host	
Time Zone to Use for z/OS Host	
Connected to Reliable Time Source? (Y/N)	
Prerequisites: (Checklist)	
Perform all installation procedures documented in the *z/OS Program Directory*.	
The z/OS UNIX kernel address space was started.	
The TCP/IP address space was started and connected to the z/OS UNIX kernel address space.	
If the Security server is not going to be configured on the z/OS host, the Security server is running in the cell.	
If the Cell Directory server is not going to be configured on the z/OS host, the CDS server is running in the cell.	
DCEKERN address space is running on z/OS host.	
Preparatory Activities: (Checklist)	
Know your DCE cell configuration plans. Read *z/OS DCE Planning*, GC24-5913.	
Set the correct time zone.	
If the Security server is not going to be configured on the z/OS host, the difference between the clocks of z/OS host and Security Server host must be less than 5 minutes. Know the locale to be configured in and set up the daemon envar files.	
Set up DCECONF Administrator User ID: (Checklist)	
Define DCECONF Admin as z/OS UNIX user.	

Table 2 (Page 2 of 2). DCE Configuration Worksheet (Required)	
DCECONF Admin must have root UID.	
Add SEUVPNL data set to ISPPLIB concatenation.	
Add SEUVMSG data set to ISPMLIB concatenation.	
Add SEUVEXEC library to SYSPROC concatenation.	
Allocate CEEDUMP data set.	
DCECONF Admin must have update authority to DCEKERN.START.REQUEST Security facility.	
Set DCECONF environment variables (optional)	

DCECONF Environment Variables

You can enter the **DCECONF** command with no options (to call an interactive ISPF panel interface) or with options (to configure DCE from the TSO command line or batch). If you are configuring DCE from the TSO command line or batch, it is **recommended** that you use environment variables rather than entering options on the command line because MVS has a 100-character limit on the length of parameter lists. If you set any environment variables before running DCECONF and you are using the interactive ISPF panels, the values are displayed in the configuration panels when you run the z/OS DCE configuration program. The values you specify in environment variables are used instead of the default values. You can override these values by typing over them in the configuration panels or by explicitly specifying options when entering the **dceconf** command. (For a list of command line options and corresponding environment variables, see page 50.)

The z/OS DCE configuration program can use the following panel input environment variables to set default values for host information.

Table 3 (Page 1 of 4). Environment Variables Table	
Variable	**Description**
_EUV_CCACHE_TYPE	Specifies the Kerberos credentials cache type. Valid values are: **FILE** The credentials cache is stored in a file located in the **/opt/dcelocal/var/security/creds** directory. This is the default. **XMEM** The credentials cache is stored in a data space that the DCE security server manages. The DCE security server must be running on each system using XMEM credentials caches. Only DCE applications can use XMEM credentials caches. (They are not available to Kerberos applications.)
_EUV_CFG_AUDIT_FILE_NAME	Specifies the file name of the audit trail file. The file name must be 50 or fewer characters. It is truncated if you specify more than 50 characters. Only the auditd component uses this environment variable.
_EUV_CFG_AUDIT_FILE_PATH	Specifies the full path name of the directory where you want the audit trail file to reside. The path name must be 50 or fewer characters. It is truncated if you specify more than 50 characters. Only the auditd component uses this environment variable.

Table 3 (Page 2 of 4). Environment Variables Table

Variable	Description
_EUV_CFG_AUDIT_FILE_WRAP	Specifies whether the audit daemon should wrap. Valid values are Y (yes) and N (no). N causes the audit daemon to open a new audit trail file when the current audit trail file reaches the maximum size. The current audit trail file is renamed and the new file is opened with the original name. The default is N. Only the auditd component uses this environment variable.
_EUV_CFG_AUDIT_OWN_EVENTS	Specifies whether the audit daemon should audit its own events. Valid values are Y (yes) and N (no). The default is N. Only the auditd component uses this environment variable.
_EUV_CFG_CDSD_MACHINE_ADDR	Specifies the Internet address of the CDS server host. There is no default for this variable.
_EUV_CFG_CDSD_MACHINE_NAME	Specifies the TCP/IP name of the CDS server host. There is no default for this variable.
_EUV_CFG_CELL_ID	Specifies the DCE principal name of the administrator who is performing the z/OS DCE configuration. The default value is **cell_admin**.
_EUV_CFG_CELL_NAME	Specifies the name of the DCE cell, without the leading "***/.../***". If a machine is already configured into a cell, that cell name overrides this value in the configuration panels. There is no default for this variable.
_EUV_CFG_CELL_PW	Specifies the cell administrator's password. **Important Note** Putting this password in a plain-text file can compromise the security of your cell. This environment variable must be set if you are configuring DCE with the **mkdce** operand (see "Using mkdce for Configuration" on page 46) instead of using interactive ISPF panels. DCECONF uses its value for the cell administrator's password without prompting you. This feature can be useful when automating configuration tasks. To limit the security risk, the cell administrator's password should be changed after the tasks are completed and the value of the EUV_CFG_CELL_PW environment variable is unset. This environment variable is not used if you are configuring or deconfiguring DCE using interactive ISPF panels (see Chapter 3, "Using the DCECONF Configuration Panels" on page 21).
_EUV_CFG_CLEARINGHOUSE	Specifies the clearinghouse name for an additional **cdsd**. The default value is *hostname*_ch.
_EUV_CFG_DCE_MACHINE_NAME	Specifies the identifying name within the cell of the machine being configured. This can be the same as the TCP/IP host name, but it does not have to be. The default is the long TCP/IP host name (hostname.domain) of the local machine.
_EUV_CFG_DIRLIST	Specifies the list of directories to be replicated at configuration time by an additional CDS server (cds_second).

Table 3 (Page 3 of 4). Environment Variables Table	
Variable	**Description**
_EUV_CFG_GDAD_BIND	Specifies whether to configure the bind conduit of the Global Directory Agent (GDAD). Valid values are **Y** (yes) and **N** (no). The default is **Y**. **Note:** Specifying the **-B** command line option is equivalent to **Y**; not specifying **-B** is equivalent to **N**. If you specify **Y**, then you must also specify RESOLVER_CONFIG, either in the user's envar file, the GDAD daemon's envar file, or on the GDAD configuration menu. (See *z/OS DCE Administration Guide* for information about RESOLVER_CONFIG.)
_EUV_CFG_GDAD_LDAP	Specifies whether to configure the LDAP conduit of the Global Directory Agent (GDAD). Valid values are **Y** (yes) and **N** (no). The default is **Y**. **Note:** Specifying the **-L** command line option is equivalent to **Y**; not specifying **-L** is equivalent to **N**. If you specify **Y**, then you must also specify LDAP_SERVER, LDAP_AUTH_DN, and LDAP_AUTH_DN_PW, either in the user's envar file, the GDAD daemon's envar file, or on the GDAD configuration menu.
_EUV_CFG_KEYSEED	Specifies the keyseed for the initial security database master key. There is no default.
_EUV_CFG_LDAP_ADDCELL_DELETE	Specifies whether LDAP global cell registration should delete any existing data. Valid values are **Y** (yes) and **N** (no). The default is **N**.
_EUV_CFG_MAX_AUDIT_TRAIL	Specifies the maximum size of the audit trail file in bytes. The range is 1 to 429467294. The default is 2,000,000. Only the auditd component uses this environment variable.
_EUV_CFG_MAX_ID	Specifies the maximum value the Security server may automatically generate for a principal or group UNIX ID. The default value is **32767**.
_EUV_CFG_MIN_PW_LTH	Specifies the minimum length of a principal's password. Specify 0 to indicate no minimum length. The maximum password length is 512 characters. Only the pwd component uses this environment variable.
_EUV_CFG_PW_ONLY_ALPHANUM	Specifies whether passwords should be limited to alphanumeric characters. Valid values are Y (yes) and N (no). The default is N. Only the pwd component uses this environment variable.
_EUV_CFG_PW_SPACE_OK	Specifies whether passwords can contain all spaces. Valid values are Y (yes) and N (no). The default is N. Only the pwd component uses this environment variable.
_EUV_CFG_RGY_DB_TYPE	Specifies the type of registry database for the Security server. This is only used for component sec_srv. Valid values are HFS and RDB.
_EUV_CFG_RGY_INTERVAL	Specifies the checkpoint interval for the registry database. Only the sec_srv component uses this environment variable.
_EUV_CFG_SECD_DCE_MACHINE_NAME	Specifies the DCE host name of the Security server host. There is no default for this value. It is needed if you are configuring the initial CDS server on the z/OS host and the initial Security server on another machine in the DCE cell.

Table 3 (Page 4 of 4). Environment Variables Table	
Variable	**Description**
_EUV_CFG_REPLICANAME	Specifies the replica security server's name. The default value is **cell_replica**.
_EUV_CFG_SECD_MACHINE_ADDR	Specifies the Internet address of the Security server host. There is no default for this variable.
_EUV_CFG_SECD_MACHINE_NAME	Specifies the TCP/IP name of the Security server host. There is no default for this variable.
_EUV_CFG_START_GID	Specifies the value at which the Security server starts assigning automatically-generated group UNIX IDs. The default value is **100**.
_EUV_CFG_START_OID	Specifies the value at which the Security server starts assigning automatically-generated organization UNIX IDs. The default value is **100**.
_EUV_CFG_START_UID	Specifies the value at which the Security server starts assigning automatically-generated principal UNIX IDs. The default value is **100**.

If these environment variables are not set, DCECONF prompts for the respective host information.

The DCE configuration program also uses the following environment variables that affect execution behavior:

Table 4. Environment Variables Affecting Execution Behavior	
Variable	**Description**
EUV_CFG_INFORM_LEVEL	Specifies the level of information that is displayed on the screen during the configuration of the host system. The valid values are: 0 Only messages regarding the progress of configuration are written. 1 Progress messages and the commands used by the configuration program are written. This is the default value. 2 Progress messages, commands, and the output from most commands are written.
_EUV_CFG_LOG_FILE	Specifies the name of the configuration log file. The default value is **dceconf.log** in the administrator's home directory.
NLSPATH	NLSPATH determines the language in which DCE messages are displayed. If DCE messages are not in English, DCECONF cannot configure or deconfigure properly. If you are using code page IBM-939, you must set NLSPATH to En_US.IBM-1047. See the description of the NLSPATH environment variable in *z/OS DCE Administration Guide* for more information.

Setting DCECONF Environment Variables

The DCECONF environment variables are declared in the **envar** file in the home directory of the administrator performing the z/OS DCE configuration. Environment variables are set using the following syntax:

VARIABLE_NAME=*value*

Figure 4 is an example of the entries in the **envar** file for the z/OS DCE configuration program:

```
_EUV_CFG_CELL_ID=cell_admin
_EUV_CFG_CELL_NAME=baritonecell.ibm.com
_EUV_CFG_SECD_MACHINE_NAME=baritone
_EUV_CFG_CDSD_MACHINE_NAME=baritone
_EUV_CFG_INFORM_LEVEL=2
_EUV_CFG_LOG_FILE=dceconf.log
```

Figure 4. Example DCECONF Environment Variables

Note: If you plan to configure the z/OS DCE host as the security server or a Replica Security server, the **HOME** and **PATH** environment variables **must** be set prior to running configuration, or you will see message EUVA08639E in the **dceconf.log**.

Daemon Configuration File

During configuration, DCECONF uses a file called the **Daemon Configuration File** to determine how the z/OS DCE daemons are to be started. DCECONF does this through the Control Task of the DCEKERN address space. The path name to this file is **/opt/dcelocal/etc/euvpdcf**. Each line in this file contains configuration information on the individual z/OS DCE daemons.

The Daemon Configuration File contains the following fields:

1. Name of the z/OS DCE daemon. For example, in Figure 5 on page 19, DCED.
2. Whether the daemon is locally configured or not. For example, CONFIGURED=N.
3. Name of the load module to run when starting the daemon. For example, LMD=EUVDCED.
4. Arguments (or parameters) that are passed to the load module when starting the daemon. For example:

   ARG="ENVAR('_EUV_HOME=/opt/dcelocal/home/dced')/ >DD:DCEDOUT"
5. Minimum time interval in seconds between restart attempts for the daemon. For example, RESTART=300.
6. Maximum time in seconds for the daemon to complete its initialization. For example, TIMEOUT=300.

The Daemon Configuration File is created during the installation of z/OS DCE. Figure 5 on page 19 shows the typical contents of the Daemon Configuration file.

```
DCED     CONFIGURED=N LMD=EUVDCED  ARG="ENVAR('_EUV_HOME=/opt/dcelocal/home/dced')/              >DD:DCEDOUT"  RESTART=300 TIMEOUT=300
SECD     CONFIGURED=N LMD=EUVSSECD ARG="ENVAR('_EUV_HOME=/opt/dcelocal/home/secd')/-dcekern      >DD:SECDOUT"  RESTART=300 TIMEOUT=300
CDSD     CONFIGURED=N LMD=EUVCCDSD ARG="ENVAR('_EUV_HOME=/opt/dcelocal/home/cdsd')/"             >DD:CDSDOUT"  RESTART=300 TIMEOUT=300
CDSADV   CONFIGURED=N LMD=EUVCADV  ARG="ENVAR('_EUV_HOME=/opt/dcelocal/home/cdsadv')/           >DD:ADVOUT"   RESTART=300 TIMEOUT=300
CDSCLERK CONFIGURED=N LMD=EUVCCLRK ARG="ENVAR('_EUV_HOME=/opt/dcelocal/home/cdsclerk')/         >DD:CLRKOUT"  RESTART=300 TIMEOUT=300
DTSD     CONFIGURED=N LMD=EUVTDTSD ARG="ENVAR('_EUV_HOME=/opt/dcelocal/home/dtsd')/-r            >DD:DTSDOUT"  RESTART=300 TIMEOUT=300
DTSTP    CONFIGURED=N LMD=EUVTNP   ARG="ENVAR('_EUV_HOME=/opt/dcelocal/home/dts_null_provider')/ >DD:TNPOUT"   RESTART=300 TIMEOUT=300
AUDITD   CONFIGURED=N LMD=EUVSAUDD ARG="ENVAR('_EUV_HOME=/opt/dcelocal/home/auditd')/           >DD:AUDOUT"   RESTART=300 TIMEOUT=300
PWDMGMT  CONFIGURED=N LMD=EUVSPWD  ARG="ENVAR('_EUV_HOME=/opt/dcelocal/home/pwdmgmt')/-dcekern  >DD:PWDOUT"   RESTART=300 TIMEOUT=300
GDAD     CONFIGURED=N LMD=EUVCGDAD ARG="ENVAR('_EUV_HOME=/opt/dcelocal/home/gdad)/              >DD:GDADOUT"  RESTART=300 TIMEOUT=300
```

Figure 5. Daemon Configuration File

Initially, the **CONFIGURED** field is set to **N** (for NO). After finishing the configuration of the host, DCECONF changes the value of this field to **Y** (for Yes) for all configured z/OS DCE daemons. For subsequent restarts of DCEKERN, only the configured daemons (with **Y** on the CONFIGURED field) will be automatically started.

For more information on the DCE Configuration File, see *z/OS DCE Administration Guide*. For information on migrating **euvpdcf** from earlier releases of OS/390® DCE, see *z/OS DCE Planning*.

Chapter 3. Using the DCECONF Configuration Panels

Use DCECONF to configure the z/OS DCE daemons. If you call the DCECONF configuration program with no options, it provides interactive panels that prompt and guide you through the details of configuring the z/OS DCE daemons. You can also call DCECONF with the **-c** option to configure the z/OS DCE daemons from the TSO command line or from batch. See Chapter 4, “Using DCECONF from the TSO Command Line or Batch” on page 45 for details.

DCECONF uses the DCE administrative facilities to enter configuration information in the Security Registry and the CDS namespace. These facilities are the Registry Editor, ACL Editor, RPC Control Program, CDS Control Program, and the DCE Control Program. The DTS Control Program is used to enable the DTS daemon.

In the DCECONF panels, you are either prompted to select from a list of options or to enter a value, such as the name of your cell. To select from a list of options, enter the number corresponding to the desired function in the selection field. For panels that require values, enter the appropriate response in the input field.

Details on using these panels are described in this chapter. The terms **z/OS DCE configuration program** and **DCECONF** are used interchangeably in this book.

Starting and Stopping DCECONF

You can start the DCE configuration program from TSO by entering the **DCECONF** command. If you plan to use the ISPF interactive panels, enter:

```
dceconf
```

For information about using **DCECONF** to configure DCE from the TSO command line or from batch see Chapter 4, “Using DCECONF from the TSO Command Line or Batch” on page 45.

To exit from DCECONF, enter:

```
end
```

on the command line in the DCE Configuration Main Menu, or press F3. If you are in a subpanel of the DCE Configuration Main Menu, entering **END** at the command line brings you back to the calling configuration panel.

DCE Login Panel

To configure z/OS DCE on the z/OS host, you must be duly authenticated and authorized by the DCE Security Service. If you attempt to perform any of the functions provided by **DCECONF** that require DCE authentication, **DCECONF** automatically displays the DCE LOGIN panel. You must then enter the correct Cell Admin ID and password. This ensures that you are logged in to DCE as the administrator who has all the necessary permissions to configure z/OS DCE.

Further authorizations may be needed if your security server resides on z/OS, using DATABASE 2™ (DB2®) for registry database. The DB2 administrator must issue the following SQL statements to grant access to your userid for the SRGYDATA database and plan:

1. GRANT DBADM ON DATABASE SRGYDATA TO your-userid;
2. GRANT BIND,EXECUTE ON PLAN SRGYDATA TO your-userid;

3. SET CURRENT SQLID='DCEKERN';
4. GRANT BINDAGENT TO your-userid;

The Cell Admin ID and Cell Admin Password are usually the same as those used during the initial configuration of the cell. However, these may have been changed.

This panel is not displayed if you configure a new cell with the Security Server on MVS. In this case, you enter the **cell_admin** user ID and password on the Security Server definition panel. In all other cases, you see the panel once unless there is a problem with login, in which case, it is displayed again. You can use **F4** or the END command to exit from the panel. Figure 6 shows the DCE LOGIN panel.

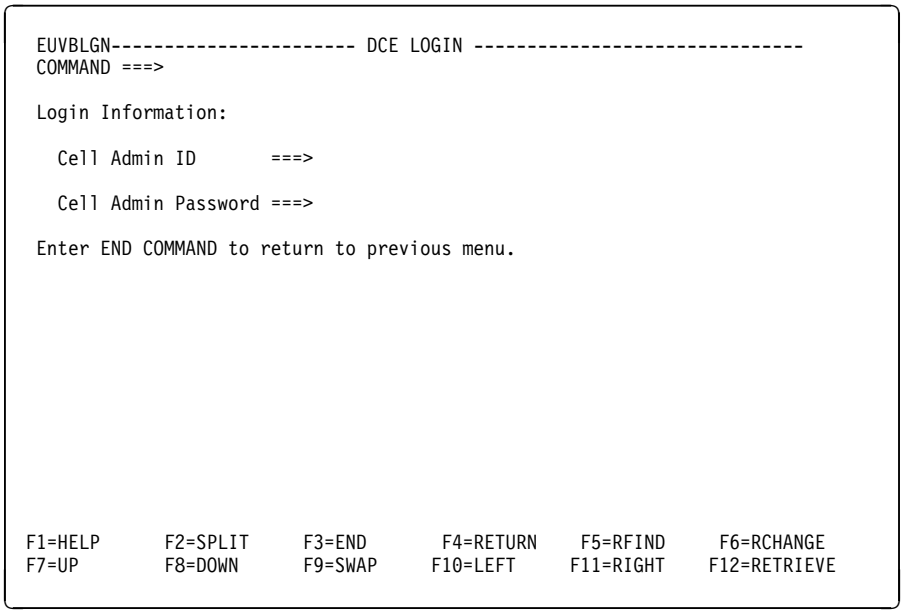

Figure 6. DCE Login Panel

If you have previously set the **_EUV_CFG_CELL_ID** environment variable, its value is displayed in the **Cell Admin ID** field of the panel. You can either accept it or overwrite it with a new value.

DCE Configuration Main Menu

After you enter the DCECONF command from TSO, the DCECONF Main Menu displays. The DCECONF Main Menu is shown in Figure 7 on page 23.

```
EUVBMAIN---------------------- DCECONF MAIN MENU ------------------------
SELECT OPTION ===>

                     1. Configure Server Machines
                     2. Deconfigure Server Machines
                     3. Configure DCE Client Machine
                     4. Deconfigure DCE Client Machine
                     5. Reconfigure Local DTS Entity
                     6. Register Cell Globally

Enter END COMMAND to terminate.

      ********************************************************************
      *    Licensed Materials - Property of IBM                          *
      *    5647-A01                                                      *
      *    (C) Copyright IBM Corp. 1995, 1997      All Rights Reserved   *
      ********************************************************************



 F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE
 F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

Figure 7. DCECONF Main Menu

The menu items are:

Menu Item	Description
Configure Server Machines	Lists all DCE Servers that may be configured and started on DCE.
Deconfigure Server Machines	Lists all DCE Servers that may be individually stopped and deconfigured on DCE.
Configure DCE Client Machine	Configures and starts the z/OS DCE daemons necessary for the z/OS host to become a DCE client machine.
Deconfigure DCE Client Machine	Deletes configuration files and DCE database entries created by previous z/OS DCE configuration requests.
Reconfigure Local DTS Entity	Configures the DTS daemon as a local server, global server or clerk, and optionally configures the Null Time Provider.
Register Cell Globally	Register with an external name service.

Configuring Server Machines

Selecting “Configure Server Machines” from the DCECONF Main Menu displays the panel shown in Figure 8 on page 24.

```
EUVBSERV----------------- SERVER CONFIGURATION MENU ---------------------------
SELECT OPTION ===>

                      1. Configure Security server
                      2. Configure Replica Security server
                      3. Configure Audit server
                      4. Configure Password Management server
                      5. Configure Initial Cell Directory server
                      6. Configure Additional Cell Directory server
                      7. Configure Global Directory Agent

Enter END COMMAND to return to main menu.









 F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE
 F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

Figure 8. Configuring Server Machines Panel

The menu items are:

Menu Item	Description
Configure Security server	Configures the DCE host as the Security server for a DCE cell during initial cell configuration.
Configure Replica Security server	Configures and starts a replica Security server on the DCE host.
Configure Audit server	Configures and starts the Audit daemon on the DCE host.
Configure Password Management server	Configures and starts the Password Management daemon on the DCE host.
Configure Initial Cell Directory server	Configures the initial Cell Directory server daemon for the cell.
Configure Additional Cell Directory server	Configures and starts an additional Cell Directory server daemon.
Configure Global Directory Agent	Configures and starts the Global Directory Agent daemon on the DCE host.

Configuring a z/OS Host as a Security Server for a DCE Cell

Selecting “Configure Security server” from the DCECONF Server Configuration Menu displays the panel shown in Figure 9 on page 25.

Important

You can only configure a master Security server during initial cell configuration. If you want to configure your z/OS host as the master Security server of a preexisting DCE cell, you must configure it as a Replica Security server and then use the **sec_admin** command to swap the identity of the master and Replica Security servers.

```
EUVBSECD------------------SECURITY SERVER CONFIGURATION-----------------------
COMMAND ===>

Cell Name            ===> dcecell21.endicott.ibm.com
Host Machine Name    ===> DCEDRBLD

Security Server Replica Name  ===> master

Keyseed for initial database master key   ===>
Starting UID         ===> 100
Starting GID         ===> 100
Starting OID         ===> 100

Principal name for the Cell Administrator   ===> cell_admin
Password for the Cell Administrator         ===>
Re-enter Cell Administrator password        ===>

Options:
  Checkpoint interval for the master registry (seconds)  ===> 7200
  Type of registry database (HFS or RDB)                 ===> HFS

Enter END COMMAND to return to main menu.

F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE
F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

Figure 9. Configuring Security Server Panel

The Security Server configuration panel prompts for the information necessary to configure the DCE host as the Security server during initial cell configuration. The fields are:

Field	Explanation
Cell Name	The name you want the DCE cell to be known as. Enter the name without the leading /.../. This value may already be supplied if you have set the environment variable, _EUV_CFG_CELL_NAME. That cell name will appear, overriding the variable. If a value is supplied you can overtype it. **Important** The cell name must be unique. If you attempt to configure a new cell using the name of a cell that already exists and is running, you will probably be unable to configure your initial CDS server. This is because the CDS advertiser and clerk will communicate with the CDS server in the existing cell.
Host Machine Name	The simple name of the z/OS host. The default value is the TCP/IP name of the z/OS host.
SECD Internet Address	The Internet address of the DCE host. **Note:** You can **either** enter this address, **or** leave it blank and enter the TCP/IP name of the DCE host in the SECD Machine Name field.
SECD Machine Name	TCP/IP name of the DCE host.
Keyseed	A character string you enter for the random key generator to use in creating a master key for the master database. The master database and the slave database each has its own master key and, therefore, its own keyseed. The Security server configuration uses the keyseed.

Starting UID	The value at which the Security server starts assigning automatically generated principal UNIX IDs.
Starting GID	The value at which the Security server starts assigning automatically generated group UNIX IDs.
Starting OID	The value at which the Security server starts assigning automatically generated organization UNIX IDs.
Principal for Cell Administrator	The user ID you want to be used for the cell administrator.
Password for Cell Administrator	The initial password you want to be used for the cell administrator.
Checkpoint interval	The checkpoint interval used by the Security server.
Type of registry database	The type (HFS or RDB) of database to be used for the registry. The default is HFS.

If you use the DCE Configuration Panel (see “Configuring a DCE Host as a DCE Client Machine” on page 34) to set the DCECONF environment variables (see “DCECONF Environment Variables” on page 14) before you run the configuration program, the values of the environment variables corresponding to each field are automatically displayed. You can either accept these values or overwrite them with new ones.

Note: There are two environment variables, **HOME** and **PATH**, that **must** be set prior to running configuration, or you will see message EUVA08639E in the **dceconf.log**.

Fill in the required fields with the appropriate values and then press the Enter key.

Configuring a z/OS Host as a Replica Security Server

Selecting “Configure Replica Security server” from the DCECONF Server Configuration Menu displays the panel shown in Figure 10 on page 27.

Important Note

Before configuring a Replica Security server, you must configure the DCE image as a DCE Client Machine as described in “Configuring a DCE Host as a DCE Client Machine” on page 34.

```
EUVBREP---------------REPLICA SECURITY SERVER CONFIGURATION--------------------
COMMAND ===>

Cell Name            ===> dcecell21.endicott.ibm.com

Replica Security Server
Name                 ===> rep_plat

Keyseed for initial database
master key           ===>

Options:
  Checkpoint interval for the master registry (seconds)  ===> 7200
  Type of registry database (HFS or RDB)                 ===> HFS




Enter END COMMAND to return to main menu.

F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE
F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

Figure 10. Configuring Replica Security Server Panel

The Replica Security Server configuration panel prompts you for the information necessary to configure the DCE host as a replica security server. The fields are:

Field	Explanation
Replica Security Server Name	The name you want the Replica Security server to be known as.
Keyseed	A character string you enter for the random key generator to use in creating a master key for the replica database. The master database and the replica database each has its own master key and, therefore, its own keyseed. The Security server configuration uses the keyseed.
Checkpoint interval	The checkpoint interval used by the Replica Security server.
Type of registry database	The type (HFS or RDB) of database to be used for the registry. The default is HFS.

If you set the DCECONF environment variables (see “DCECONF Environment Variables” on page 14) before you run the configuration program, the values you set are automatically displayed. You can accept these values or overwrite them with new ones.

The exception to this is the **PATH** and **HOME** environment variables, which **must** be set prior to running configuration, or you will see error EUVA08639E in the **dceconf.log** file.

Fill in the required fields with the appropriate values and then press the Enter key. When the Replica Security server initializes, you are returned to the DCECONF Main Menu.

Configuring a z/OS Host as an Audit Server

Selecting “Configure Audit Server” from the DCECONF Server Configuration Menu displays the panel shown in Figure 11.

Important Note

Before configuring an Audit server, you must configure the DCE image as a DCE Client Machine as described in “Configuring a DCE Host as a DCE Client Machine” on page 34.

```
EUVBAUDD---------------------AUDIT SERVER CUSTOMIZATION--------------------
COMMAND ===>

Maximum size of the audit trail
file in bytes (1-4294967294).         ===> 2000000

Should the Audit daemon audit its
own events (Y or N)?                  ===> N

Should the audit trail file wrap
(Y or N)?                             ===> N

Pathname of the directory where the
audit trail file resides (truncated
if over 50 chars).
   ===> /opt/dcelocal/var/audit/adm

Filename of the audit trail file
(truncated if over 50 chars).
   ===> central_trail

Enter END COMMAND to return to main menu.

F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE
F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

Figure 11. Configuring a DCE Host As an Audit Server Machines Panel

The Audit Server configuration panel prompts for the information necessary to configure the DCE host as an Audit server. The fields are:

Field	Explanation
Maximum size of the audit trail file	The maximum size of the audit trail file in bytes. Enter a value in the range from 1 to 4294967294.
Should the Audit daemon audit its own events?	Answering yes (Y) tells the audit daemon to audit its own events.
Should the audit trail file wrap?	Answering yes (Y) causes the audit trail file to wrap. Answering no (N) causes the audit daemon to open a new audit trail file when the current audit trail file reaches the maximum size. The current audit trail file is renamed and the new file is opened with the original name.
Pathname of audit trail file	The full path name of the directory where you want the audit trail file to reside. The path name must be 50 characters or less; it is truncated if more than 50 characters are entered.

File name of audit trail file	The file name of the audit trail file. The file name must be 50 characters or less; it is truncated if more than 50 characters are entered.

Fill in the required fields with the appropriate values, and then press the Enter key. When the Audit server initializes, you are returned to the DCECONF Main Menu.

Configuring a Host as a Password Management Server

Selecting “Configure Password Management Server” from the DCECONF Server Configuration Menu displays the panel shown in Figure 12.

Important Note

Before configuring a Password Management server, you must configure the DCE image as a DCE Client Machine as described in “Configuring a DCE Host as a DCE Client Machine” on page 34.

```
EUVBPWDM--------------PASSWORD MANAGEMENT SERVER CUSTOMIZATION-------------
COMMAND ===>

Minimum Password Length               ===>

Allow Passwords to contain Spaces     ===> N

Allow Only Alphanumerics in Password  ===> N

Enter END COMMAND to return to main menu.









F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE
F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

Figure 12. Configuring Password Management Server

The Password Management Server configuration panel prompts for the information necessary to configure the DCE host as a Password Management server. The fields are:

Field	Explanation
Minimum Password Length	Specify the minimum length for a principal's password. Specify 0 to indicate no minimum length. **Note:** The maximum password length is 512 characters.
Allow Passwords to contain Spaces	Answering yes (Y) tells the Password Management server to allow passwords that contain all spaces. Answering no (N) disallows passwords that are all spaces.

Allow Only Alphanumerics in Password	Answering yes (Y) tells the Password Management server to allow passwords that contain only alphanumeric characters. Answering no (N) disallows passwords that contain only alphanumeric characters.

Fill in the required fields with the appropriate values, and then press the Enter key. When the Password Management server initializes, you are returned to the DCECONF Main Menu.

Configuring the Cell Directory Server

There are two paths you can take to configure the CDS server depending on whether you have just configured the Security Server on this machine.

After You Have Configured the Security Server: If you have configured the Security server, the panel in Figure 13 is automatically displayed.

```
EUVBWCDS------------------- INITIAL CDSD LOCATION -----------------------------
SELECT OPTION ===>

     Initial Cell Directory Server configuration:

           1. Configure CDS server on this machine
           2. Configure and start CDS server on another
              machine in this cell

Enter END COMMAND to return to main menu.

 F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE
 F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

Figure 13. Initial Cell Directory Server Location Panel

If you choose option 1, the CDS server and the CDS client are configured. Then, the DTS Configuration Panel (Figure 20 on page 36) is displayed.

If you choose option 2, the panel in Figure 14 on page 31 is displayed.

```
EUVBRCDS-------------------REQUEST START OF CDS SERVER-------------------------
COMMAND ===>

Please start the CDS Server on another machine in this cell.
Enter Y (for Yes) when CDS has completed initialization.
                    ===>

Enter END COMMAND to return to main menu.

 F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE
 F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

Figure 14. Request Start of CDS Server

The “Request Start of CDS Server” configuration panel prompts you to enter Y (for Yes) when you complete the configuration of the CDS Server on another machine in the DCE cell.

When you enter the appropriate value on this screen, you are returned to the DCECONF Main Menu.

Configuring CDS from the Server Configuration Menu: If you have configured the Security server on another machine in the DCE cell, then you can select “Configure Initial Cell Directory server” from the DCECONF Server Configuration Menu. The panel in Figure 15 is displayed.

```
EUVBICDS---------------- Initial CDSD Configuration -------------------------
COMMAND ===>

Cell Name           ===> dcefvt1.endicott.ibm.com

Host Machine Name   ===> DCEFVT1

Security Server Information:

SECD Information:

  Internet Address     ===>
    OR
  TCP/IP Machine Name  ===>

  DCE Machine Name     ===>


Enter END COMMAND to return to main menu.


 F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE
 F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

Figure 15. Initial Cell Directory Server Configuration Panel

The fields in this panel are:

Field	Explanation
Cell Name	The name of the DCE cell to which the DCE host system belongs. Enter the name without the leading /.../. This value may already be supplied if you have set the environment variable, _EUV_CFG_CELL_NAME. That cell name appears, overriding the variable. If a value is supplied, and **secd** is on another host, you can overtype the value. If **secd** is on this host, you cannot change the cell name or the host name.
Host Machine Name	The simple name of the z/OS host. The default value is the TCP/IP name of the z/OS host.
SECD Internet Address	The Internet address of the host that runs the Security server. **Note:** You can **either** enter this address, **or** leave it blank and enter the TCP/IP name of the Security server host in the SECD Machine Name field.
SECD TCP/IP Machine Name	TCP/IP name of the host that runs the Security server.
DCE Machine Name	The DCE host name for the machine where the Security Server is located.

After you have entered the appropriate values on the panel, you are returned to the DCECONF Main Menu.

Only one **cdsd** is permitted on a host. If you want to have another **cdsd** in the cell, configure the client here, then go to the “Additional CDSD Configuration” panel (see Figure 16).

Configuring an Additional Cell Directory Server: Selecting “Configure Additional Cell Directory server” from the DCECONF Server Configuration Menu displays Figure 16.

```
EUVBACDS--------------- Additional CDSD Configuration -------------------------
COMMAND ===>

Cell Name           ===> dcecell21.endicott.ibm.com

Host Machine Name   ===> DCEDRBLD

Location of Cached CDS Server:
  Internet Address  ===>
    OR
  Machine Name      ===> dcecell21.endicott.ibm.com

Clearinghouse and replica information:

  Clearinghouse Name  ===> DCEDRBLD



Enter END COMMAND to return to main menu.




 F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE
 F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

Figure 16. Additional Cell Directory Server Configuration Panel

The fields in this panel are:

Field	Explanation
Location of Cached CDS Server	The Internet address *or* machine (TCP/IP) name of the CDS cache. The CDS cache is the collection of information on servers, clearinghouses, and other CDS resources that the CDS clerk establishes on the local system.
Clearinghouse Name	The name of the database on the CDS server that is used to store CDS entries. If this is left blank it defaults to *machinename*_ch.

Fill in the fields on the Additional CDSD Configuration panel and the Additional CDSD Directory Replication panel (Figure 17) is displayed.

```
EUVBDCDS----------  Additional CDSD Directory Replication  -------------------


    Enter the names of directories to replicate separated by spaces,
    up to a maximum of 255 characters.

    Press ENTER to process, or
    press END to return to main menu

  Directories to replicate  ===>




Enter END COMMAND to return to main menu.




 F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE
 F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

Figure 17. Additional Cell Directory Replication Panel

The input to this panel is the list of directories that you want to replicate. This panel is displayed again until you press the END key so that you may enter all desired directories. You are limited to 255 characters each time.

You may press the END key (F3, usually) the first time you see this panel.

Note: If you are configuring an additional Cell Directory server and receive either of the following status codes:

Ox141290if Decryption integrity check fails.

or

Ox10d0a3ec CDS cannot communicate with CDS server.

follow the procedure the *z/OS DCE Administration Guide* describes.

Configuring the Global Directory Agent

Selecting “Configure Global Directory Agent” from the DCECONF Server Configuration Menu displays Figure 18.

```
EUVBGDCF---------------------- GDAD CONFIGURATION -----------------------------
COMMAND ===>

Cell Name         ===> dcefvt1.endicott.ibm.com

Host Machine Name ===> DCEFVT1

Use BIND conduit:  ===> Y

  RESOLVER_CONFIG:  ===>

Use LDAP conduit:  ===> Y

  LDAP_SERVER:      ===>
  LDAP_AUTH_DN_PW:  ===>
  LDAP_AUTH_DN:     ===>



Enter END COMMAND to return to main menu.


 F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE
 F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

Figure 18. Global Directory Agent Configuration Panel

On this panel, if you answer “Y” (for Yes) to “Use BIND conduit:,” then fill in “RESOLVER_CONFIG:” with the name of the configuration file. Otherwise, leave it blank. If you answer “Y” to “Use LDAP conduit:,” then fill in the “LDAP:” information; otherwise, leave it blank. The field items are:

Field	Explanation
LDAP_SERVER	This is the IP address or TCP/IP hostname of the LDAP server.
LDAP_AUTH_DN_PW	This is the password information stored at the distinguished name specified in LDAP_AUTH_DN.
LDAP_AUTH_DN	This is the distinguished name in the LDAP namespace at which authentication information is stored.

For more information about the environment variables LDAP_SERVER, LDAP_AUTH_DN_PW, and LDAP_AUTH_DN, see *z/OS DCE Administration Guide*.

Now you must configure the DCE image as a DCE Client Machine as described in “Configuring a DCE Host as a DCE Client Machine.”

Configuring a DCE Host as a DCE Client Machine

Important Note

If your host system was previously configured for DCE, you must **deconfigure** it before you can successfully configure the z/OS DCE daemons. See “Deconfiguring a DCE Host Configured as a DCE Client Machine” on page 40 for more information on deconfiguring DCE from the host.

Selecting “Configure DCE Client Machine” from the DCECONF Main Menu displays the panel shown in Figure 19 on page 35.

```
EUVBCFG----------------------- DCE CONFIGURATION -----------------------------
COMMAND ===>

Cell Name           ===> dcecell21.endicott.ibm.com

Host Machine Name   ===> DCEDRBLD

SECD Information:
  Internet Address  ===>
    OR
  Machine Name      ===> dcecell21.endicott.ibm.com

CDSD Information:
  Internet Address  ===>
    OR
  Machine Name      ===> dcecell21.endicott.ibm.com

Enter END COMMAND to return to main menu.




F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE
F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

Figure 19. DCE Configuration Panel

This DCE Configuration Panel prompts for information necessary for configuring the z/OS host as a DCE client machine. The fields are:

Field	Explanation
Cell Name	Name of the DCE cell to which the z/OS host system belongs. Enter the name without the leading **/.../**. This value may already be supplied if you have set the environment variable, _EUV_CFG_CELL_NAME. That cell name will appear, overriding the variable. If a value is supplied you can overtype it.
Host Machine Name	The simple name of the z/OS host. The default value is the TCP/IP name of the z/OS host.
SECD Internet Address	The Internet address of the host that runs the Security server. **Note:** You can **either** enter this address, **or** leave it blank and enter the TCP/IP name of the Security server host in the SECD Machine Name field.
SECD Machine Name	TCP/IP name of the host that runs the Security server.
CDSD Internet Address	The Internet address of the host (non-z/OS) that runs the CDS server. **Note:** You can **either** enter this address, **or** leave it blank and enter the TCP/IP name of the CDS server host in the CDSD Machine Name field.
CDSD Machine Name	TCP/IP name of the host that runs the CDS server.

If you set the DCECONF environment variables (see “DCECONF Environment Variables” on page 14) before you run the configuration program, the values of the environment variables corresponding to each

field in this panel are automatically displayed. You can either accept these values or overwrite them with new ones.

When you have filled the required fields with the appropriate values, press the Enter key. After all non-DTS configuration is complete, the **DTS Configuration Menu**, shown in Figure 20 is displayed.

```
EUVBDTS---------------------- DTS CONFIGURATION ----------------------
SELECT OPTION ===>

                    1. Configure DTS Entity as a Clerk
                    2. Configure DTS Entity as a Local Server
                    3. Configure DTS Entity as a Global Server

                    Configure DTS Null Time Provider? N

Enter END COMMAND to return to main menu.









F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE
F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

Figure 20. DTS Configuration Menu

After the required fields are completed (see the description of your choices in "DTS Servers and Clerks," "Creating DTS Servers and Clerks," and "Configuring the DTS Null Time Provider" on page 37), DTS configuration processing initiates. When processing is complete, you are returned to the DCECONF Main Menu.

DTS Servers and Clerks

The DTS daemon can be configured as a local server, a global server, or a clerk. A DTS local server is available only to servers and clerks within the same LAN. A DTS global server interacts across LANs within a cell. A DTS clerk acts as the intermediary between DCE clients and DTS servers.

A DTS server can act as a **courier**. In this case, it can request a time value from a global server at every synchronization. If the DTS server host is connected to a time provider, the DTS server is a **noncourier**, meaning that it can request the time only from the time provider.

Creating DTS Servers and Clerks

To create a local noncourier server, select Configure DTS Entity as a Local Server from the DTS Configuration Menu.

To create a global noncourier server, select Configure DTS Entity as a Global Server from the DTS Configuration Menu.

To creates a DTS Clerk, select Configure DTS Entity as a Clerk from the DTS Configuration Menu.

Configuring the DTS Null Time Provider

In z/OS DCE, a Null Time Provider daemon is provided that acts as a time provider to DTS. The Null Time Provider daemon takes the time from the z/OS host system's TOD clock and gives it to the DTS server. This is useful for z/OS host systems that already have a reliable external time source, such as in sysplex environments.

At the Configure DTS Null Time Provider? prompt, enter **Y** if you already have a reliable external time source that you want to use, or **N** if you do not want to configure the DTS Null Time Provider daemon.

Note: You can only enter **Y** at this prompt if you are configuring the DTS daemon as a local or global server.

For more details on the Null Time Provider daemon, see *z/OS DCE Administration Guide*.

Reconfiguring the DTS Entity

You can reconfigure the DTS entity as a DTS server or as a DTS Clerk using the DTS Configuration Menu.

When you select Reconfigure Local DTS Entity from the DCECONF Main Menu, the panel shown in Figure 20 on page 36 displays. You can select any of the three choices provided in this menu. Remember that to enter **Y** at the Configure DTS Null Time Provider? prompt, the DTS daemon must be configured as a server.

When you reconfigure the DTS entity, the z/OS DCE daemons are unavailable for a brief period of time.

Note: You must use only DCECONF to reconfigure the DTS daemon either from server to clerk, or clerk to server. Do not use the DTS control program to perform this task.

After the required fields are filled in and you press the Enter key, DTS reconfiguration processing starts. When processing is complete, you are returned to the DCECONF Main Menu.

Registering a Cell Globally

Selecting “Register Cell Globally” from the DCECONF Main Menu displays Figure 21 on page 38.

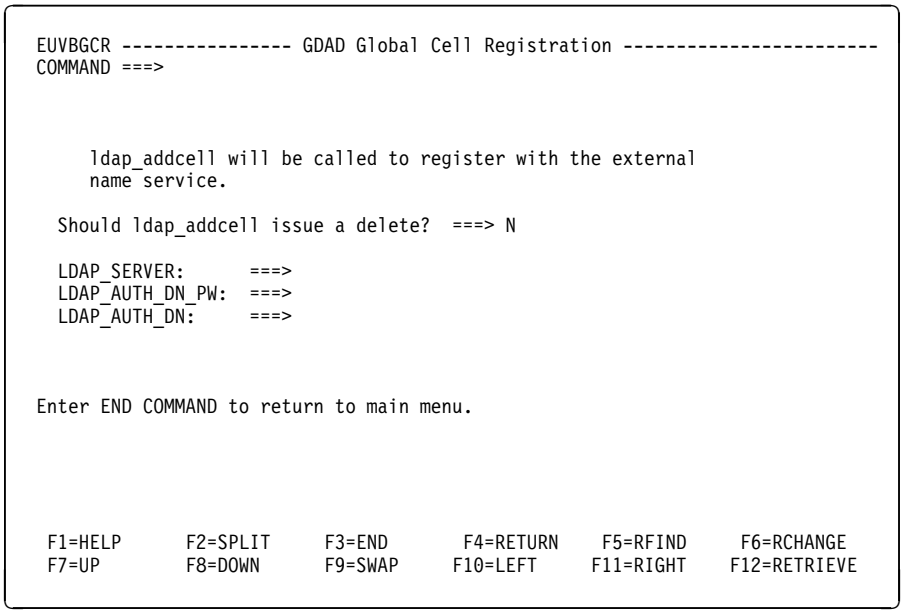

Figure 21. Global Directory Agent Configuration Panel

If you respond "Y" (for Yes) to "Should ldap_addcell issue a delete," the **ldap_addcell** command is run with the **-d** option. The field items are:

Field	Explanation
LDAP_SERVER	This is the IP address or TCP/IP host name of the LDAP server.
LDAP_AUTH_DN_PW	This is the password stored at the Distinguished Name specified in LDAP_AUTH_DN.
LDAP_AUTH_DN	This is the Distinguished Name in the LDAP namespace where authentication information is stored.

For more information about the environment variables LDAP_SERVER, LDAP_AUTH_DN_PW, and LDAP_AUTH_DN, see *z/OS DCE Administration Guide*.

Note: This panel should be used only for registering CDS cell information in an LDAP server, as the procedure is only for cells with typed (X.500) cell names. For untyped (DNS-style) cell names, run **mkdceregister** from the z/OS shell environment. See the *z/OS DCE Command Reference* for more information on running **mkdceregister**.

Deconfiguring Server Machines

Selecting "Deconfigure Server Machines" from the DCECONF Main Menu displays the panel shown in Figure 22 on page 39.

When Should You Deconfigure?

You need to deconfigure the z/OS host if:

- The name of the cell was changed (for example, if you are moving to a different cell).
- The TCP/IP name of the z/OS host system was changed.
- The Security server in the cell was moved to a different host or was reconfigured for any other reason.
- The CDS server in the cell was moved to a different host or was reconfigured for any other reason.
- The z/OS DCE configuration failed on the host system.
- You are changing the code page on the host system.

In general, you should deconfigure any servers you have running before deconfiguring the client. The exceptions are the primary cell directory server and security servers.

Using the Server Deconfiguration Menu

```
EUVBDCS----------------- SERVER DECONFIGURATION MENU --------------------------
SELECT OPTION ===>

                      1. Deconfigure Replica Security server
                      2. Deconfigure Audit server
                      3. Deconfigure Password Management server
                      4. Deconfigure Cell Directory server
                      5. Deconfigure Global Directory Agent

Enter END COMMAND to return to main menu.









 F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE
 F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

Figure 22. Deconfiguring Server Machines Panel

The menu items are:

Menu Item	Description
Deconfigure Replica Security server	Deconfigures the Replica Security server from the DCE host.
Deconfigure Audit server	Deconfigures the Audit server from the DCE host.
Deconfigure Password Management server	Deconfigures the Password Management server from the DCE host.
Deconfigure Cell Directory server	Deconfigures the Cell Directory server from the DCE host.
Deconfigure Global Directory Agent	Deconfigures the Global Directory Agent from the DCE host.

Selecting one of the above Menu Items initiates the deconfiguration process for the specified daemon. When processing is complete you are returned to the DCECONF Main Menu panel.

Deconfiguring a DCE Host Configured as a DCE Client Machine

If you need to reconfigure the z/OS DCE daemons on the z/OS host system, you may have to first **deconfigure** the host from its existing configuration.

Important

Selecting “Deconfigure DCE Client Machine” from the DCECONF Main Menu deconfigures all DCE client daemons and server daemons that were previously configured with the DCECONF program.

When Should You Deconfigure?

You need to deconfigure the z/OS host if:

- The name of the cell was changed (for example, if you are moving to a different cell).
- The TCP/IP name of the z/OS host system was changed.
- The Security server in the cell was moved to a different host or was reconfigured for any other reason.
- The CDS server in the cell was moved to a different host or was reconfigured for any other reason.
- The z/OS DCE configuration failed on the host system.
- You are changing the code page on the host system.

Using the DCE Deconfiguration Menu

Selecting “Deconfigure DCE Client Machine” from the DCECONF Main Menu displays the panel shown in Figure 23.

```
EUVBDCFG---------------------- DCE DECONFIGURATION -----------------------------
COMMAND ===>

Cell Name         ===> dcecell21.endicott.ibm.com

Host Machine Name ===> DCEDRBLD

Options:
  Remove Local Files?       ===> Y
  Remove Security Objects?  ===> Y
  Remove Directory Objects? ===> Y

Enter END COMMAND to return to main menu.









 F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE
 F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

Figure 23. DCE Deconfiguration Panel

Important

If your site is running the Distributed File System (DFS), you must deconfigure DFS before deconfiguring DCE. See *z/OS Distributed File Service Customization*, SC24-5916, for how to do this.

In addition, if you have any other DCE servers or applications running, they should also be stopped and possibly deconfigured. See the documentation for the applications you are running to determine how to do this.

The DCE Deconfiguration panel prompts you for the information necessary to deconfigure the z/OS host as a DCE client machine. The fields are:

Field	Explanation
Cell Name	Name of the DCE cell to which the z/OS host system belongs. Enter the name without the leading **/.../**. If a value is supplied you can overtype it.
Host Machine Name	The simple name of the z/OS host. The default value is the TCP/IP name of the z/OS host.
Remove Local Files?	You must enter **Y** in this field. All local configuration files (HFS files) are removed. You do not have to log in to DCE to remove the local DCE configuration files.
Remove Security Objects?	If you enter **Y** in this field, all entries that were created by DCECONF in the DCE Security registry are removed. To be able to remove entries in the DCE Security registry: • You must have the proper authorization to remove these entries. • The Security server daemon must be running on the Security server host.
Remove Directory Objects?	If you enter **Y** in this field, all entries that were created by DCECONF in the CDS namespace are removed. If you enter **Y** in this field, you must enter **Y** in the Remove Security Objects? field. To be able to remove entries in the CDS namespace: • You must have the proper authorization to remove these entries. • The Security server daemon must be running on the Security server host. • The CDS Advertiser and Clerk daemons must be running on the z/OS host that is being deconfigured. • The CDS server daemon must be running on the CDS server host. **Note:** Only the Security objects and the credential files (in **/opt/dcelocal/var/security/creds**) must be deleted to ensure that reconfiguration is successful.

After the required fields are completed (see the following paragraphs), deconfiguration processing initiates. When processing is complete, the user is returned to the DCECONF Main Menu.

Guidelines for Specifying Deconfiguration Options

If the host is being reconfigured because of a previous configuration error, specifying the deconfiguration options depends on the step at which the error occurred. To determine the step where configuration failed, compare your configuration log file to the files in Appendix B, “Example DCECONF Log Files” on page 85.

The following guidelines should be followed when specifying the deconfiguration options:

- If no daemons were started successfully, enter:
  - **Y** for Remove Local Files
  - **N** for Remove Security Objects
  - **N** for Remove Directory Objects.

  Note: If you are deconfiguring after the CDS or Security server configuration was already changed, stop the DCEKERN address space and then restart it using the **start** (**/s**) operator command with the **-nodce** option:

  ```
  /s dcekern,parms='-nodce'
  ```

  This restarts DCEKERN without starting the z/OS DCE daemons.
- If the DCE host daemon was started successfully, enter:
  - **Y** for Remove Local Files
  - **Y** for Remove Security Objects
  - **N** for Remove Directory Objects
- If the CDS advertiser and clerk daemons started successfully, enter **Y** for all three options.

If you enter a combination other than the 3 combinations above, the message "Invalid value" is displayed.

Reconfiguring after Changes in Security or CDS Servers

If the host that runs the primary CDS server or Security server is deconfigured, you must reconfigure the z/OS host. It is recommended that the z/OS host be deconfigured before the primary CDS or Security server configuration is changed. You can deconfigure the host using the DCECONF program. On the deconfiguration panel, you should enter:

- **Y** to Remove Local files
- **Y** to Remove Security Objects (if the Security server was not changed)
- for Remove Directory Objects:
  - **Y** to Remove Directory Objects if the CDS server was not changed and the DCEKERN address space was not restarted with the **-nodce** option.
  - **N** to Remove Directory Objects if the CDS server was changed and the DCEKERN address space was restarted with the **-nodce** option.

Manually Deleting the Configuration Object Entries

You can also manually remove the Security and CDS objects by deleting these objects using the Registry Editor, the CDS control program, the RPC control program, and the DCE control program. Look at your configuration log file to determine the objects that were successfully created. Using the Registry Editor, CDS control program, the RPC control program, and the DCE control program is described in *z/OS DCE Administration Guide*.

Deconfiguring the Entire Cell

There may be times when it is necessary to deconfigure an entire cell when the primary **cdsd** or the master Security server is on the z/OS host.

Attention:

The entire cell must be reconfigured if you do this.

To deconfigure the cell, do these steps:

1. Stop DCEKERN
2. Start DCEKERN with the **-nodce** option:

   ```
   /s dcekern,parms='-nodce'
   ```

3. Deconfigure, specifying:
   - **Y** for Remove Local Files
   - **N** for Remove Security Objects
   - **N** for Remove Directory Objects

Chapter 4. Using DCECONF from the TSO Command Line or Batch

You can use DCECONF to configure the z/OS DCE daemons with or without using the interactive ISPF panels. For information about configuring with the panels, see Chapter 3, “Using the DCECONF Configuration Panels” on page 21.

If you choose not to use the interactive panels, you can configure DCE from the TSO command line or from batch. You can also use this method from the z/OS UNIX System Services shell. Configuring DCE without requiring an interactive session lets you automate configuration tasks. It also allows third parties to configure z/OS DCE from a remote system, facilitating centralized management of the DCE cell or z/OS system.

DCECONF uses the DCE administrative facilities to enter configuration information in the Security Registry and the CDS namespace. These facilities are:

- Registry Editor
- ACL Editor
- RPC Control Program
- CDS Control Program
- DCE Control Program.

The DTS Control Program is used to enable the DTS daemon.

Starting DCECONF

To configure z/OS DCE on the z/OS host, you must be duly authenticated and authorized by the DCE Security Service. If you attempt to perform any of the functions provided by **DCECONF** that require DCE authentication and have not specified the Cell Administrator's password in the **_EUV_CFG_CELL_PW** environment variable in your **envar** file, you receive an error message. This ensures that you are logged in to DCE as the administrator who has all the necessary permissions to configure z/OS DCE.

Note: You can specify the cell administrator's ID in the _EUV_CFG_CELL_ID environment variable or with the **-a** *cell_admin* option.

If you enter the **DCECONF** command with no options, it calls up the ISPF panel interface; see “Starting and Stopping DCECONF” on page 21. To configure (or deconfigure) DCE from the TSO command line, you use the **DCECONF** command with the **-c** option. To configure DCE, use the **mkdce** operand:

dceconf -c mkdce *options components*

The **-c** indicates that this is a command line call and not to use interactive mode (ISPF). The **mkdce** means configure. See “Using mkdce for Configuration” on page 46 for details about options. See page 59 for examples of the parameters to use when configuring from batch rather than from the TSO command line.

To deconfigure DCE, use the **rmdce** operand:

dceconf -c rmdce *options components*

The **-c** indicates that this is a command line call and not to use interactive mode (ISPF). The **rmdce** means deconfigure (or unconfigure, in UNIX parlance). See “Using rmdce for Deconfiguration” on page 60 for details about options. See page 63 and page 64 for examples of the parameters to use when configuring from batch rather than from the TSO command line.

Using mkdce for Configuration

You can use the **dceconf** command with the **-c** option and the **mkdce** operand to configure DCE from the TSO command line. (You can also use the **-c** option and **mkdce** operand from batch. See page 59 for examples.) You can:

- Configure a server machine as follows:
  - Security server (Configure the DCE host as the Security server for a DCE cell during initial cell configuration)
  - Replica Security server (Configure and start a replica Security server on the DCE host)
  - Audit server (Configure and start the Audit daemon on the DCE host)
  - Password Management Server (Configure and start the Password Management daemon on the DCE host)
  - Initial Cell Directory server (Configure the initial Cell Directory server daemon for the cell)
  - Additional Cell Directory server (Configure and start an additional Cell Directory server daemon)
  - Global Directory Agent (Configure and start the Global Directory Agent daemon on the DCE host)
- Configure a DCE client machine
- Reconfigure a local DTS entity.

Format

```
dceconf [-c mkdce [-a cell_admin] [-A] [-B] [-c cds_server] [-C clearinghouse_name]
        [-d directory_list] [-D secd_dce_host_name] [-G min_group_id]
        [-h dce_hostname] [-I registry_interval] [-K keyseed] [-L] [-M max_UNIX_id]
        [-n cell_name] [-o full] [-O min_org_id] [-P min_principal_id]
        [-Q min_password_length] [-r sec_rep_name] [-R] [-S sec_rgy_db_type]
        [-s security_server] [-T pw_may_have_spaces] [-U pw_only_alphanumerics]
        [-V max_audit_trail_size] [-W audit_own_events] [-X audit_file_wrap]
        [-Y audit_file_path] [-Z audit_file_name] component...
]
```

Parameters

-a *cell_admin*
Specifies the name of the cell administrator's account. When you are configuring the Master Security Server (the sec_srv component), the **mkdce** operand gives this account privileges throughout the cell. Otherwise, the account named must have sufficient privilege to perform configuration tasks within the cell. The value for cell_admin is used for all components. The default is cell_admin.

-A Specifies running ldap_addcell with the delete option. Global cell registration (gdad_register) uses this option.

-B Specifies configuring GDAD with a bind conduit. When GDAD is configured, you must specify at least one of **-B** and **-L** or their respective environment variables.

-c *cds_server*
Specifies the TCP/IP host name or TCP/IP address of a CDS server, if none is located on the same LAN as the current machine. You should use these options for all components except rpc, the initial sec_srv, and the initial cds_srv. If you do not specify the **-c** option and a router or gateway that does not pass broadcast packets separates the local machine from all CDS servers, CDS cannot be configured correctly.

-C *clearinghouse_name*
Specifies the initial clearinghouse name for this CDS server. The default is *host_name* with the string `_ch` appended at the end. Only cds_second uses this option.

-d *directory_list*
Specifies the list of directories for an additional CDS server (cds_second) to replicate at configuration time. If you are specifying multiple entries, separate them with spaces and enclose the entire string in double quotation marks. For example:

```
dceconf -c mkdce -d "subsys subsys/dce subsys/dce/sec" cds_second
```

-D *secd_dce_host_name*
Specifies the DCE host name of the Security Server. This option is only used when configuring the Initial CDS server for the cell on this host (**cds_srv**).

-G *min_group_id*
Specifies the starting point (minimum UNIX ID) for UNIX IDs automatically generated by the Security Service when groups are added with the **rgy_edit** command. The default is 100. This option is used only when configuring sec_srv as the Master Security Server.

-h *dce_hostname*
Specifies the identifying name within the cell of the machine being configured. This can be the same as the TCP/IP host name, but does not have to be. The default is the long TCP/IP host name (hostname.domain) of the local machine.

-I *registry_interval*
Specifies the checkpoint interval for the registry database. Only component sec_srv uses this option.

-K *keyseed*
Specifies the keyseed to use for the Security Server database. Only component sec_srv uses this option.

-L Specifies that GDAD should be configured with an LDAP conduit. When GDAD is configured, you must specify at least one of **-B** and **-L** or their respective environment variables.

-M *max_UNIX_id*
Specifies the highest UNIX ID that the Security Service can assign to principals, groups, or organizations. The default is 32767. This option is used only when configuring sec_srv as the Master Security Server.

-n *cell_name*
Specifies the name of the DCE cell into which the machine should be configured. If you specify no *-n* option, the **mkdce** operand uses the cell name in the file **/opt/dcelocal/dce_cf.db**. All components require a value for cell_name. This value can either be in the form of */.../cellname* or *cellname*. This option is required if the machine is being configured into a DCE cell. If the machine is already configured into a DCE cell, this option is ignored and the value in /opt/dcelocal/dce_cf.db is used.

-o *full*
indicates full configuration. (Local and administrative configuration are not supported.) For full configuration, the DCE cell administrator must have root authority on the local machine to be configured into the cell (UID(0)).

-O *min_org_id*
Specifies the starting point for UNIX IDs that the Security Service automatically generates when organizations are added with the **rgy_edit** command. The default is 100. This option is used only when configuring sec_srv as the Master Security Server.

-P *min_principal_id*
Specifies the starting point (minimum UNIX ID) for UNIX IDs that Security Service automatically generates when principals are added with the **rgy_edit** command. The default is 100. This option is used only when configuring sec_srv as the Master Security Server.

-Q *min_password_length*
Specifies the minimum length of a principal's password. Specify 0 to indicate no minimum length. Note: the maximum password length is 512 characters. Only component pwd uses this option.

-r *sec_rep_name*
Specifies the name to be given to the Security Replica. The default name, `cell_replica`, is used if a Security Replica is configured without specifying a name in the **-r** option. Each Security Replica must have a unique name within the cell. Using the default name helps ensure this uniqueness.

-R Configures the secd security daemon as a Security Replica and not as a Master Security Server. You must specify the sec_srv component when you use the **-R** option to locate the Master Security Server. You also need to use the **-s** option when you use the **-R** option to locate the Master Security Server.

-s *security_server*
Specifies the host name of the Master Security Server. You can use the TCP/IP host name or the TCP/IP address of the Security Server. If you do not specify the **-s** option, the **mkdce** operand uses the Security server in the file **/opt/dcelocal/etc/security/pe_site**. A value for security_server is required for all components except master sec_srv.

-S *sec_rgy_db_type*
Specifies the database type for the Security Server. Valid values are HFS and RDB. The default is HFS.

-T *pw_may_have_spaces*
Specifies whether passwords can contain all spaces. Valid values are **Y** (yes) and **N** (no). The default is **N**. Only the component pwd uses this option.

-U *pw_only_alphanumerics*
Specifies whether passwords should be limited to alphanumeric characters. Valid values are **Y** (yes) and **N** (no). The default is **N**. Only the component pwd uses this option.

-V *max_audit_trail_size*
Specifies the maximum size of the Audit trail file, in bytes. The default is 2000000. Only the component auditd uses this option.

-W *audit_own_events*
Specifies whether the audit daemon should audit its own events. Valid values are **Y** (yes) and **N** (no). The default is **N**. Only the component auditd uses this option.

-X *audit_file_wrap*
Specifies whether the audit trail file should wrap. Valid values are **Y** (yes) and **N** (no). Specifying **Y** causes the audit trail file to wrap. Specifying **N** causes the audit daemon to open a new audit trail file when the current audit trail file reaches the maximum size. The current audit trail file is renamed and the new file is opened with the original name. Only the component auditd uses this option.

-Y *audit_file_path*
Specifies the full path name of the directory where you want the audit trail file to reside. The default path is: **/opt/dcelocal/var/audit/adm**. The path name must be 50 or fewer characters. Only the component auditd uses this option.

-Z *audit_file_name*
Specifies the name of the audit trail file. The default name is “central_trail”. The file name must be 50 or fewer characters. Only the component auditd uses this option.

component
The components are:

all_cl All clients (CDS clerk, CDS advertiser, dced). DTS is started but not configured.

auditd	Audit Daemon.
cds_second	Secondary CDS server. This component and **cds_srv** are mutually exclusive.
cds_srv	Initial CDS server for the cell. This component and **cds_second** are mutually exclusive. For **rmdce**, this is equivalent to **cds_second**.
dts_cl	DTS clerk. This component and **dts_local** and **dts_global** are mutually exclusive.
dts_global	DTS global server. This component and **dts_local** and **dts_cl** are mutually exclusive.
dts_local	DTS local server. This component and **dts_global** and **dts_cl** are mutually exclusive.
dts_tp	DTS null time provider.
gdad	Global Directory Agent. See “Configuring the Global Directory Agent” on page 56 for information GDAD configuration requires.
gdad_register	Register Cell Globally. Runs ldap_addcell. See “Registering a Cell Globally” on page 58 for information about global registration.
pwd	Password Management Server.
sec_srv	Security Server. This component can be the Master Security Server for the cell or a Security replica. To configure a replica, use the **-R** option with this component.

Notes:

1. **dceconf** with the **-c** option does not bring up the ISPF panel interface. If needed data is missing, you receive an error message and the DCECONF program exits.
2. If you are configuring DCE without using the ISPF panels, you must specify the cell administrator's password in the _EUV_CFG_CELL_PW environment variable. (Otherwise you receive an error message.) You can specify all other needed data in the options in the parameter list or in their corresponding environment variables. See Table 5 on page 50.
3. Values that you specify on the command line take precedence over values in the **envar** file.

Relationship between Options and Environment Variables

Table 5. Options and Their Corresponding Environment Variables

Option	Environment Variable
-a	_EUV_CFG_CELL_ID
-A	_EUV_CFG_LDAP_ADDCELL_DELETE
-B	_EUV_CFG_GDAD_BIND
-c	_EUV_CFG_CDSD_MACHINE_NAME or _EUV_CFG_CDSD_MACHINE_ADDR
-C	_EUV_CFG_CLEARINGHOUSE
-d	_EUV_CFG_DIRLIST
-D	_EUV_CFG_SECD_DCE_MACHINE_NAME
-G	_EUV_CFG_START_GID
-h	_EUV_CFG_DCE_MACHINE_NAME
-I	_EUV_CFG_RGY_INTERVAL
-K	_EUV_CFG_KEYSEED
-L	_EUV_CFG_GDAD_LDAP
-M	_EUV_CFG_MAX_ID
-n	_EUV_CFG_CELL_NAME
-o	N/A
-O	_EUV_CFG_START_OID
-P	_EUV_CFG_START_UID
-Q	_EUV_CFG_MIN_PW_LTH
-r	_EUV_CFG_REPLICANAME
-R	N/A
-s	_EUV_CFG_SECD_MACHINE_ADDR or _EUV_CFG_SECD_MACHINE_NAME
-S	_EUV_CFG_RGY_DB_TYPE
-T	_EUV_CFG_PW_SPACE_OK
-U	_EUV_CFG_PW_ONLY_ALPHANUM
-V	_EUV_CFG_MAX_AUDIT_TRAIL
-W	_EUV_CFG_AUDIT_OWN_EVENTS
-X	_EUV_CFG_AUDIT_FILE_WRAP
-Y	_EUV_CFG_AUDIT_FILE_PATH
-Z	_EUV_CFG_AUDIT_FILE_NAME

Notes:

1. It is **recommended** that you specify information for these options in the environment variables rather than as options on the **dceconf** command because MVS has a 100-character limit on the length of parameter lists.
2. You cannot specify your password as an option when using the TSO command line or batch. You **must** specify your password in the environment variable _ENV_CFG_CELL_PW.

3. There are no options to match the following environment variables that DCECONF uses:
   - RESOLVER_CONFIG
   - LDAP_SERVER
   - LDAP_AUTH_DN
   - LDAP_AUTH_DN_PW

Configuring a z/OS Host as a Security Server for a DCE Cell

Important

You can configure a master Security server only during initial cell configuration. If you want to configure your z/OS host as the master Security server of a preexisting DCE cell, you must configure it as a Replica Security server and then use the **sec_admin** command to swap the identity of the master and Replica Security servers.

The information you need to provide to configure a z/OS host as a Security Server for a DCE cell is:

Information	Explanation and Where to Specify It
Cell Name	The name you want to use for the DCE cell. Specify the name without the leading /.../. You can specify this in the _EUV_CFG_CELL_NAME environment variable or as *cell_name* in the **-n** option. **Important** The cell name must be unique. If you try to configure a new cell using the name of a cell that already exists and is running, you will probably be unable to configure your initial CDS server. This is because the CDS advertiser and clerk will communicate with the CDS server in the existing cell.
Host Machine Name	The simple name of the z/OS host. You can specify this in the _EUV_CFG_DCE_MACHINE_NAME environment variable or as *dce_hostname* in the **-h** option. The default value is the TCP/IP name of the z/OS host. You can specify the TCP/IP name in the _EUV_CFG_CDSD_MACHINE_NAME environment variable or as *cds_server* in the **-c** option.
SECD Internet Address	The Internet address of the DCE host. You can specify this in the _EUV_CFG_SECD_MACHINE_ADDR environment variable or as *security_server* in the **-s** option **or** you can specify the TCP/IP name of the DCE host for the SECD Machine Name (next item).
SECD Machine Name	TCP/IP name of the DCE host. You can specify this in the _EUV_CFG_SECD_MACHINE_NAME environment variable or as *security_server* in the **-s** option
Keyseed	A character string for the random key generator to use in creating a master key for the master database. The master database and the slave database each has its own master key and, therefore, its own keyseed. The Security server configuration uses the keyseed. You can specify this in the _EUV_CFG_KEYSEED environment variable or as *keyseed* in the **-K** option.

Starting UID	The value at which the Security server starts assigning automatically generated principal UNIX IDs. You can specify this in the _EUV_CFG_START_UID environment variable or as *min_principal_id* option of the **-P** option.
Starting GID	The value at which the Security server starts assigning automatically generated group UNIX IDs. You can specify this in the _EUV_CFG_START_GID environment variable or as *min_group_id* in the **-G** option.
Starting OID	The value at which the Security server starts assigning automatically generated organization UNIX IDs. You can specify this in the _EUV_CFG_START_OID environment variable or as *min_org_id* in the **-O** option.
Principal for cell administrator	The user ID you want to use for the cell administrator. You can specify this in the _EUV_CFG_CELL_ID environment variable or as *cell_admin* in the **-a** option.
Password for cell administrator	The initial password to use for the cell administrator. You specify this in the _EUV_CFG_CELL_PW environment variable. No matching command line option exists for this password.
Checkpoint interval	The checkpoint interval the Security server uses. You can specify this in the _EUV_CFG_RGY_INTERVAL environment variable or as *registry_interval* in the **-I** option.
Type of registry database	The type (HFS or RDB) of database to use for the registry. The default is HFS. You can specify this in the _EUV_CFG_RGY_DB_TYPE environment variable or as *sec_rgy_db_type* in the **-S** option.

Configuring a z/OS Host as a Replica Security Server

Important Note

Before configuring a Replica Security server, you must configure the DCE image as a DCE Client Machine as described in “Configuring a DCE Host as a DCE Client Machine” on page 56.

If you are configuring a DCE host as a Replica Security server, you need to provide the following information:

Information	Explanation and Where to Specify It
Replica Security Server Name	The name you want to use for the Replica Security server. You can specify this in the _EUV_CFG_REPLICANAME environment variable or as *sec_rep_name* in the **-r** option.
SECD Internet Address	The Internet address of the host that runs the Security server. **Note:** You can specify this in the _EUV_CFG_SECD_MACHINE_ADDR environment variable or as *security_server* in the **-s** option **or** you can specify the TCP/IP name of the DCE host for the SECD Machine Name (next item).
SECD Machine Name	TCP/IP name of the host that runs the Security server. You can specify this in the _EUV_CFG_SECD_MACHINE_NAME environment variable or as *security_server* in the **-s** option.

Keyseed	A character string you enter for the random key generator to use in creating a master key for the replica database. The master database and the replica database each has its own master key and, therefore, its own keyseed. The Security server configuration uses the keyseed. You can specify this in the _EUV_CFG_KEYSEED environment variable or as *keyseed* in the **-K** option.
Checkpoint interval	The checkpoint interval that the Replica Security server uses. You can specify this in the _EUV_CFG_RGY_INTERVAL environment variable or as *registry_interval* in the **-I** option.
Type of registry database	The type (HFS or RDB) of database to use for the registry. The default is HFS. You can specify this in the _EUV_CFG_RGY_DB_TYPE environment variable or as *sec_rgy_db_type* in the **-S** option.

You must set the **PATH** and **HOME** environment variables before running configuration, or you will see error EUVA08639E in the **dceconf.log** file.

Configuring a z/OS Host as an Audit Server

Important Note

Before configuring an Audit server, you must configure the DCE image as a DCE Client Machine as described in "Configuring a DCE Host as a DCE Client Machine" on page 56.

To configure a host as an Audit server, you need the following information:

Information	Explanation and Where to Specify It
Maximum size of the audit trail file	The maximum size of the audit trail file in bytes. This value must be in the range from 1 to 4294967294. You can specify this in the _EUV_CFG_MAX_AUDIT_TRAIL environment variable or as *max_audit_trail_size* in the **-V** option.
Should the Audit daemon audit its own events?	You can specify **Y** (yes) or **N** (no) in the _EUV_CFG_AUDIT_OWN_EVENTS environment variable or as *audit_own_events* in the **-W** option.
Should the audit trail file wrap?	You can specify **Y** (yes) or **N** (no) in the _EUV_CFG_AUDIT_FILE_WRAP environment variable or as *audit_file_wrap* in the **-X** option. Specifying **N** causes the audit daemon to open a new audit trail file when the current audit trail file reaches the maximum size. The current audit trail file is renamed and the new file is opened with the original name.
Pathname of audit trail file	The full path name of the directory where you want the audit trail file to reside. The path name must be 50 characters or fewer. It is truncated if you specify more than 50 characters. You can specify this in the _EUV_CFG_AUDIT_FILE_PATH environment variable or as *audit_file_path* in the **-Y** option.
File name of the audit trail file	The file name of the audit trail file. The file name must be 50 characters or fewer. It is truncated if you specify more than 50 characters. You can specify this

in the _EUV_CFG_AUDIT_FILE_NAME environment variable or as *audit_file_name* in the **-Z** option.

Configuring a Host as a Password Management Server

Important Note

Before configuring a Password Management server, you must configure the DCE image as a DCE Client Machine as described in "Configuring a DCE Host as a DCE Client Machine" on page 56.

To configure a host as a Password Management server, you need to specify the following information:

Information	Explanation and Where to Specify It
Minimum Password Length	The minimum length for a principal's password. Specify 0 to indicate no minimum length. **Note:** The maximum password length is 512 characters. You can specify this in the _EUV_CFG_MIN_PW_LTH environment variable or as *min_password_length* of the **-Q** option.
Allow Passwords to contain spaces	Specifying **Y** (yes) tells the Password Management server to allow passwords that contain all spaces. Specifying **N** (no) disallows passwords that are all spaces. You can specify this in the _EUV_CFG_PW_SPACE_OK environment variable or as *pw_may_have_spaces_* of the **-T** option.
Allow Only Alphanumerics in Password	Specifying **Y** (yes) tells the Password Management server to allow passwords that contain only alphanumeric characters. Specifying **N** (no) disallows passwords that contain only alphanumeric characters. You can specify this in the _EUV_CFG_PW_ONLY_ALPHANUM environment variable or as *pw_only_alphanumerics* of the **-U** option.

Configuring an Initial Cell Directory Server

To configure the initial Cell Directory server in the DCE cell, you need to supply the following information:

Information	Explanation and Where to Specify It
Cell Name	The name of the DCE cell to which the DCE host system belongs. Specify the name without the leading /.../. You can specify this in the _EUV_CFG_CELL_NAME environment variable or as *cell_name* in the **-n** option.
Host Machine Name	The simple name of the z/OS host. You can specify this in the _EUV_CFG_DCE_MACHINE_NAME environment variable or as *dce_hostname* in the **-h** option. The default value is the TCP/IP name of the z/OS host. You can specify the TCP/IP name in the _EUV_CFG_CDSD_MACHINE_NAME environment variable or as *cds_server* in the **-c** option.
SECD Internet Address	The Internet address of the host that runs the Security server. You can specify this in the _EUV_CFG_SECD_MACHINE_ADDR environment variable or as *security_server* in the **-s** option **or** you can specify the TCP/IP name of the Security server host (next item).

SECD TCP/IP Machine Name	TCP/IP name of the host that runs the Security server. You can specify this in the _EUV_CFG_SECD_MACHINE_NAME environment variable or as *security_server* in the **-s** option.
DCE Machine Name	The DCE host name for the machine where the Security Server is located. You can specify this in the _EUV_CFG_SECD_DCE_MACHINE_NAME environment variable or as *secd_dce_host_name* in the **-D** option.

Only one **cdsd** is permitted on a host. If you want to have another **cdsd** in the cell, configure the client as described here; then see "Configuring an Additional Cell Directory Server."

Configuring an Additional Cell Directory Server: To configure an additional Cell Directory server, you need to specify the following information:

Information	Explanation and Where to Specify It
Location of Cached CDS Server	The Internet address *or* machine (TCP/IP) name of the CDS cache. The CDS cache is the collection of information on servers, clearinghouses, and other CDS resources that the CDS clerk establishes on the local system. You can specify this in the _EUV_CFG_CDSD_MACHINE_NAME environment variable or as *cds_server* in the **-c** option.
Clearinghouse Name	The name of the database on the CDS server that is used to store CDS entries. You can specify this in the _EUV_CFG_CLEARINGHOUSE environment variable or as *clearinghouse_name* in the **-C** option. The default value is *hostname*_ch.

You can also specify the following optional information:

Information	Explanation and Where to Specify It
list of directories	These are the directories that you want to replicate. You can specify this list in the _EUV_CFG_DIRLIST environment variable or as *directory_list* in the **-d** option.

Note: If you are configuring an additional Cell Directory server and receive either of the following status codes:

```
0x141290if Decryption integrity check fails.
```

or

```
0x10d0a3ec CDS cannot communicate with CDS server.
```

follow the procedure the *z/OS DCE Administration Guide* describes.

Configuring the Global Directory Agent

To configure a global directory agent, you need to specify the following information:

Information	Explanation and Where to Specify It
Use BIND conduit	Specifies whether to configure the bind conduit of the Global Directory Agent (GDAD). You can specify **Y** (yes) or **N** (no) in the _EUV_CFG_GDAD_BIND environment variable. (The default is **Y**.) Or you can specify the **-B** option (is equivalent to **Y**) or omit this option (is equivalent to **N**). If you specify **Y** or the **-B** option, then you must also specify RESOLVER_CONFIG, the name of the configuration file, in the user's **envar** file or in the GDAD daemon's **envar** file. (See *z/OS DCE Administration Guide* for information about RESOLVER_CONFIG.)
Use LDAP conduit	Specifies whether to configure the LDAP conduit of the Global Directory Agent (GDAD). You can specify **Y** (yes) or **N** (no) in the _EUV_CFG_GDAD_LDAP environment variable. (The default is **Y**.) Or you can specify the **-L** option (is equivalent to **Y**) or omit this option (is equivalent to **N**). If you specify **Y** or the **-L** option, you must also specify the following information, in the user's **envar** file or in the GDAD daemon's **envar** file. **LDAP_SERVER** — This is the IP address or TCP/IP hostname of the LDAP server. **LDAP_AUTH_DN_PW** — This is the password information stored at the distinguished name specified in LDAP_AUTH_DN. **LDAP_AUTH_DN** — This is the distinguished name in the LDAP namespace at which authentication information is stored.

For more information about the environment variables LDAP_SERVER, LDAP_AUTH_DN_PW, and LDAP_AUTH_DN, see *z/OS DCE Administration Guide*.

You must configure the DCE image as a DCE Client Machine as described in “Configuring a DCE Host as a DCE Client Machine.”

Configuring a DCE Host as a DCE Client Machine

Important Note

If your host system was previously configured for DCE, you must **deconfigure** it before you can successfully configure the z/OS DCE daemons. See “Deconfiguring a DCE Host Configured as a DCE Client Machine” on page 62 for more information on deconfiguring DCE from the host.

To configure a DCE host as a DCE client machine, you need to specify the following information:

Information	Explanation and Where to Specify It
Cell Name	Name of the DCE cell to which the z/OS host system belongs. Specify the name without the leading **/.../**. You can specify this in the _EUV_CFG_CELL_NAME environment variable or as *cell_name* in the **-n** option.
Host Machine Name	The simple name of the z/OS host. You can specify this in the _EUV_CFG_DCE_MACHINE_NAME environment variable or as *dce_hostname* in the **-h** option. The default value is the TCP/IP name of the z/OS host. You can specify the TCP/IP name in the _EUV_CFG_CDSD_MACHINE_NAME environment variable or as *cds_server* in the **-c** option.
SECD Internet Address	The Internet address of the host that runs the Security server. You can specify this in the _EUV_CFG_SECD_MACHINE_ADDR environment variable or as *security_server* in the **-s** option **or** you can specify the TCP/IP name of the Security server host in the SECD Machine Name field (next item).
SECD Machine Name	TCP/IP name of the host that runs the Security server. You can specify this in the _EUV_CFG_SECD_MACHINE_NAME environment variable or as *security_server* in the **-s** option.
CDSD Internet Address	The Internet address of the (non-z/OS) host that runs the CDS server. You can specify this in the _EUV_CFG_CDSD_MACHINE_ADDR environment variable or as *cds_server* in the **-c** option **or** you can specify the TCP/IP name of the CDS server host in the CDSD Machine Name (next item).
CDSD Machine Name	TCP/IP name of the host that runs the CDS server. You can specify this in the _EUV_CFG_CDSD_MACHINE_NAME environment variable or as *cds_server* in the **-c** option.

To continue this task, see “DTS Servers and Clerks,” “Creating DTS Servers and Clerks,” or “Configuring the DTS Null Time Provider” on page 58

DTS Servers and Clerks

The DTS daemon can be configured as a local server, a global server, or a clerk. A DTS local server is available only to servers and clerks within the same LAN. A DTS global server interacts across LANs within a cell. A DTS clerk acts as the intermediary between DCE clients and DTS servers.

A DTS server can act as a **courier**. In this case, it can request a time value from a global server at every synchronization. If the DTS server host is connected to a time provider, the DTS server is a **noncourier**, meaning that it can request the time only from the time provider.

Creating DTS Servers and Clerks

To create a local noncourier server, specify the DTS local server component (dts_local).

To create a global noncourier server, specify the DTS global server component (dts_global).

To create a DTS clerk, specify the DTS clerk component (dts_cl).

Configuring the DTS Null Time Provider

In z/OS DCE, a Null Time Provider daemon is provided that acts as a time provider to DTS. The Null Time Provider daemon takes the time from the z/OS host system's TOD clock and gives it to the DTS server. This is useful for z/OS host systems that already have a reliable external time source, such as in sysplex environments.

To configure the DTS Null Time Provider, specify the DTS null time provider component (dts_tp).

You can configure dts_tp only if you are configuring DTS as a local or global server.

For more details on the Null Time Provider daemon, see *z/OS DCE Administration Guide*.

Reconfiguring the DTS Entity

You can reconfigure the DTS entity as a DTS server or as a DTS Clerk.

Remember that if you are specifying configuring a DTS Null Time Provider, the DTS daemon must be configured as a server.

When you reconfigure the DTS entity, the z/OS DCE daemons are unavailable for a brief period of time.

Note: You must use only DCECONF to reconfigure the DTS daemon either from server to clerk or from clerk to server. Do not use the DTS control program to perform this task.

Registering a Cell Globally

To register a cell globally, you need to specify the following information:

Information	Explanation and Where to Specify It
Should ldap_addcell issue a delete	This specifies whether the **ldap_addcell** command runs with the **-d** option, deleting any existing data. You can specify **Y** (yes) or **N** (no) in the _EUV_CFG_LDAP_ADDCELL_DELETE environment variable. (The default is **N**.) Or you can specify the **-A** option (is equivalent to **Y**) or omit this option (is equivalent to **N**). If you specify **Y**, you must also specify the following information in the user's envar file or in the GDAD daemon's envar file. **LDAP_SERVER** This is the IP address or TCP/IP host name of the LDAP server. **LDAP_AUTH_DN_PW** This is the password stored at the Distinguished Name specified in LDAP_AUTH_DN. **LDAP_AUTH_DN** This is the Distinguished Name in the LDAP namespace where authentication information is stored.

For more information about the environment variables LDAP_SERVER, LDAP_AUTH_DN_PW, and LDAP_AUTH_DN, see *z/OS DCE Administration Guide*.

Note: This procedure is only for cells with typed (X.500) cell names. For untyped (DNS-style) cell names, run **mkdceregister** from the z/OS shell environment. See the *z/OS DCE Command Reference* for more information on running **mkdceregister**.

Configuration Examples

To configure a new DCE cell with a Security Server, Cell Directory server, and DTS local server on this host, taking all defaults, issue:

```
dceconf -c mkdce -n my_cell_name sec_srv cds_srv dts_local
```

To configure this host as a DCE Client, issue:

```
dceconf -c mkdce -n my_cell_name -c cds.machine.name -s security.machine.name all_cl
```

To configure a DCE client, you can use the following on the TSO command line:

```
dceconf -c mkdce -n cell21 -c dcecell21 -s dcecell21 all_cl
```

To perform the same configuration of a DCE client from batch, you need:

1. An **envar** file
2. A JCL file.

The JCL in Figure 25 and several other JCL examples in this chapter all use the following environment variables file:

```
_EUV_CFG_CELL_NAME=drbld_cell
_EUV_CFG_CDSD_MACHINE_NAME=DCEDRBLD
_EUV_CFG_SECD_MACHINE_NAME=DCEDRBLD
_EUV_CFG_DCE_MACHINE_NAME=dce_drbld
_EUV_CFG_INFORM_LEVEL=1
_EUV_CFG_CELL_PW=cell_admin_password
_EUV_CFG_CLEARINGHOUSE=junk_ch
_EUV_CFG_START_GID=250
_EUV_CFG_START_UID=250
_EUV_CFG_MAX_ID=32000
_EUV_CFG_KEYSEED=abcdefg
_EUV_CFG_MIN_PW_LTH=6
_EUV_CFG_REPLICANAME=dcedrbld_replica
```

Figure 24. Environment Variables File Used with JCL Examples

The following JCL configures a DCE client from batch.

```
//DCECONF  JOB (),'SYSPROG',CLASS=A,
//             MSGCLASS=H,MSGLEVEL=(1,1),NOTIFY=&SYSUID
/*
//*******************************************************************
//* THIS JOB RUNS DCE CONFIG
//*******************************************************************
//* ----------------------------------------------------------------
//CONFIG   EXEC PGM=EUVBCONF,
//         PARM='-c mkdce -n cell21 -c dcecell21 -s dcecell21 all_cl'
```

Figure 25. Sample JCL for Configuring a DCE Client from Batch

To configure a machine as a new cell with a Security Server and Initial Cell Directory Server, you can use the following on the TSO command line:

```
dceconf -c mkdce sec_srv cds_serv dts_cl
```

Or you can do the same configuration from batch, using the following JCL file. (See Figure 24 for the environment variable file to use in conjunction with this JCL.)

```
//DCECONF  JOB (),'SYSPROG',CLASS=A,
//             MSGCLASS=H,MSGLEVEL=(1,1),NOTIFY=&SYSUID
/*
//*******************************************************************
//* THIS JOB RUNS DCE CONFIG
//*******************************************************************
//* ----------------------------------------------------------------
//CONFIG   EXEC PGM=EUVBCONF,
//         PARM='-c mkdce sec_srv cds_srv dts_cl'
```

Figure 26. Configuring with a Security Server and Initial Cell Directory Server

Using rmdce for Deconfiguration

You need to deconfigure the z/OS host if:

- The name of the cell was changed (for example, if you are moving to a different cell).
- The TCP/IP name of the z/OS host system was changed.
- The Security server in the cell was moved to a different host or was reconfigured for any other reason.
- The CDS server in the cell was moved to a different host or was reconfigured for any other reason.
- The z/OS DCE configuration failed on the host system.
- You are changing the code page on the host system.

In general, you should deconfigure any servers you have running before deconfiguring the client. The exceptions are the primary cell directory server and security servers.

You can use the **dceconf** command with the **-c** option and the **rmdce** operand to deconfigure DCE from the TSO command line. (You can also perform the deconfiguration from batch. See page 63 and 64 for examples.)

You can deconfigure:

- Server machines from the DCE host:
  - Replica Security server
  - Audit server
  - Password Management server
  - Cell Directory server
  - Global Directory Agent
- A DCE host configured as a DCE client machine
- The entire cell.

Note: You can deconfigure only a Replica Security server. Trying to deconfigure a Master Security server fails.

Format

dceconf [-c rmdce [**-a** *cell_admin*] [**-F**] [**-g**] [**-l**] [**-o** full] [**-o** local] [**-o** security] *component*...]

Parameters

-a *cell_admin*
Specifies the name of the cell administrator's account. The default is cell_admin.

-F Forces deconfigure of components named on the command line, even if other components depend on their presence.

-g Deconfigures dependent components. This specifies also configuring any components that depend on those listed on the command line.

The components are:

all	All DCE components. It specifies deconfiguring all configured components.
all_cl	All DCE components. It specifies deconfiguring all configured components.
auditd	Audit Daemon.
cds_second	Secondary CDS server. This component and **cds_srv** are mutually exclusive.
gdad	Global Directory Agent. See “Configuring the Global Directory Agent” on page 56 more information about GDAD configuration.
sec_srv	Security Server. This component can be the Master Security Server for the cell or a Security replica. To configure a replica, use the **-R** option with this component. Attempts to deconfigure the Master Security Server fail.
pwd	Password Management Server.

-l Same as **-o local**. **This removes all traces of DCE configuration from this host**.

-o full
Full deconfiguration of the requested components. Root authority and cell administrator privileges are required.

-o local
Deconfigure only local portions. This stops all daemons and removes local files. No dce_login is done so the cell administrator ID and password are not needed. This option is available only for components all and all_cl. It is equivalent to using the ISPF "Deconfigure Client" screen and choosing only to remove local files. **This removes all traces of DCE configuration from this host**. If there is a problem with stopping daemons when running this option, you should stop DCEKERN and restart it with the **-nodce** option, and then try the deconfiguration again.

-o security
Deconfigure only Security objects and local files. This does not deconfigure directory objects. You should use this only when configuration of a DCE Client failed because of problems with CDS. This option is available only for components all and all_cl. Root authority and cell administrator privileges are required.

Usage Notes

Notes:

1. **dceconf** with the **-c** option does not bring up the ISPF panel interface. If needed data is missing, you receive an error message and the DCECONF program exits.
2. You can specify all needed data (except the cell administrator's password, which must be in an environment variable), in a command line option or in its corresponding environment variable. For a list of command line options and corresponding environment variables, see page 50.
3. Values that you specify on the command line take precedence over values in the **envar** file.

Deconfiguring Server Machines

To deconfigure a server machine, use:

dceconf -c rmdce *component*

The *component* is the component name for the server.

Deconfiguring a DCE Host Configured as a DCE Client Machine

If you need to reconfigure the z/OS DCE daemons on the z/OS host system, you may have to first **deconfigure** the host from its existing configuration.

Use:

```
dceconf -c rmdce all_cl
```

or

```
dceconf -c rmdce all
```

Guidelines for Specifying Deconfiguration Options

If the host is being reconfigured because of a previous configuration error, specifying the deconfiguration options depends on the step at which the error occurred. To determine the step where configuration failed, compare your configuration log file to the files in Appendix B, “Example DCECONF Log Files” on page 85.

If you do not specify an **-o** option (**-o full**, **-o local**, or **-o security**) when deconfiguring, the default value is **-o full**.

The following guidelines should be followed when specifying the deconfiguration options:

- If no daemons were started successfully, specify **-o local**.

  Note: If you are deconfiguring after the CDS or Security server configuration was already changed, stop the DCEKERN address space and then restart it using the **start** (**/s**) operator command with the **-nodce** option:

  ```
  /s dcekern,parms='-nodce'
  ```

  This restarts DCEKERN without starting the z/OS DCE daemons.
- If the DCE host daemon was started successfully, specify **-o security**.
- If the CDS advertiser and clerk daemons started successfully, specify **-o full**.

Deconfiguration Example

To deconfigure a DCE client, you can use the following on the TSO command line:

```
dceconf -c rmdce all_cl
```

You can perform the same deconfiguration from batch using the following JCL. (See Figure 24 on page 59 for the environment variable file to use in conjunction with this JCL.)

```
//DCECONF  JOB (),'SYSPROG',CLASS=A,
//             MSGCLASS=H,MSGLEVEL=(1,1),NOTIFY=&SYSUID
/*
//*********************************************************************
//* THIS JOB RUNS DCE CONFIG
//*********************************************************************
//* -------------------------------------------------------------------
//CONFIG   EXEC PGM=EUVBCONF,
//         PARM='-c rmdce all_cl'
```

Figure 27. Deconfiguring a DCE Client from Batch

Reconfiguring after Changes in Security or CDS Servers

If the host that runs the primary CDS server or Security server is deconfigured, you must reconfigure the z/OS host. It is recommended that the z/OS host be deconfigured before the primary CDS or Security server configuration is changed.

Security Server change?	CDS change?	Option
yes	yes	**-o local**
yes	no	**-o local**
no	yes	**-o security**
no	no	**-o full**

Manually Deleting the Configuration Object Entries

You can also manually remove the Security and CDS objects by deleting these objects using the Registry Editor, the CDS control program, the RPC control program, and the DCE control program. Look at your configuration log file to determine the objects that were successfully created. Using the Registry Editor, CDS control program, the RPC control program, and the DCE control program is described in the *z/OS DCE Administration Guide*.

Deconfiguring the Entire Cell

There may be times when it is necessary to deconfigure an entire cell when the primary **cdsd** or the master Security server is on the z/OS host.

Attention

The entire cell must be reconfigured if you do this.

Deconfiguring a single cell does not require **dce_login**.

To deconfigure the cell, do these steps:

1. Stop DCEKERN
2. Start DCEKERN with the **-nodce** option:

   /s dcekern,parms='-nodce'

3. Use **dceconf** to deconfigure the cell.

   You can use the following on the TSO command line:

   dceconf -c rmdce -Fgl all

   Or you can perform the same deconfiguration from batch by using the JCL in Figure 28. (See Figure 24 on page 59 for the environment variable file to use in conjunction with this JCL.)

```
//DCECONF  JOB (),'SYSPROG',CLASS=A,
//             MSGCLASS=H,MSGLEVEL=(1,1),NOTIFY=&SYSUID
/*
//*********************************************************************
//* THIS JOB RUNS DCE CONFIG
//*********************************************************************
//* -------------------------------------------------------------------
//DECONFIG EXEC PGM=EUVBCONF,
//         PARM='-c rmdce -Fgl all'
```

Figure 28. Deconfiguring a Cell from Batch

Chapter 5. Setting Up the Registry

This chapter describes the steps to set up the registry in the Security service on MVS. The DCECONF command during DCE configuration automatically handles some of these steps. You perform others, using DCE utilities and control programs. This chapter includes descriptions of setting up the master registry database and slave replica databases on MVS. You can have one security server on each host in your cell. One security server is the master and the rest are slaves. You can use DCECONF to create the master or slave on MVS. To create master or slave databases on another system, use the tool appropriate to that system.

The steps for setting up the registry follow. If you want the master registry database to be on this system and the slave to be on another system, follow the instructions outlined by steps 1, 2, 3, and 4, and create the slave using the appropriate tool on the other system. If you want the slave database to be on MVS and the master to be on another system, follow the instructions in step 1, create the master database using the appropriate tool on the other system, and then follow the instructions outlined in step 5.

1. Plan where the Security Service components are to be located in your network.
2. Create the master registry database (performed by the DCECONF command during system configuration if DCE is configured on MVS).
3. Start the master security server (performed by the DCECONF command during system configuration).
4. Populate the registry database (performed by using the **dcecp** or **rgy_edit** command).
    a. Set policies and properties.
    b. Add names and accounts.
5. Create a slave database and start the slave replica (performed by the DCECONF command during system configuration if DCE is configured on MVS).

Because the registry uses the Cell Directory Service to obtain information about network resources, this chapter assumes that your network is configured properly for Cell Directory Service operation.

Planning Sites for Security Service Components

The first thing that you do to configure the Security Service in your network is choose the sites for the master replica and any slave replicas of the registry. These sites will run **secd**, the Security server. Machines running **secd** must be up and available at all times. It is especially important that the machine where the master replica runs be available throughout the network.

The machine size required to run **secd** depends on the platform and operating system. As a very general rule, choose machines large enough to accommodate future growth of the registry database. The machines must have enough disk space for the registry database and enough backing store so that processes do not thrash.

When you run the DCECONF command, it configures the master replica site to run the DCE Host daemon (**dced**), which provides the Endpoint Mapper Service for the local host, and any required Cell Directory Service servers.

Creating the Master Registry Database

When you initially configure your cell's Security server, the DCECONF command starts the *dcelocal***/bin/sec_create_db** command to create the master replica. When **sec_create_db** creates a new master replica, it initializes its database with names and accounts.

Note: Only the DCECONF command should run the **sec_create_db** command.

The **sec_create_db** command also creates a registry configuration file, which is named **opt/***dcelocal***/etc/security /pe_site**, that contains the cell name and network address of the master replica. This file supplies the binding address of the **secd** server to clients running on that machine, if the Cell Directory Service is unavailable.

The Results of sec_create_db

The master registry database that is created by **sec_create_db** contains the principals, groups, and organizations listed in Table 6.

Table 6. Initial Persons, Groups, and Organizations

Principal	Group	Organization
bin	bin	none
daemon	daemon	-
dce-ptgt	kmem	-
dce-rgy	mail	-
krbtgt/*local_cell_name*	nogroup	-
hosts/*local_host*/self	none	-
mail	system	-
nobody	tcb	-
root	tty	-
sys	uucp	-
tcb	-	-
uucp	-	-
who	-	-

The accounts that are created by the **sec_create_db** command are as follows:

- **bin bin none**
- **daemon daemon none**
- **dce-ptgt none none**
- **dce-rgy none none**
- **hosts/***local_host***/self none none**
- **krbtgt/***cell_name* **none none**
- **nobody nogroup none**
- **root system none**
- **uucp uucp none**

Some of the objects that were initially created by **sec_create_db** are reserved and cannot be deleted. These are as follows:

- The reserved principals are as follows:

  - **dce-ptgt**
  - **krbtgt/***cell_name*
  - **dce-rgy**.
- The reserved group is **none**.
- The reserved organization is **none**
- The reserved accounts are as follows:
  - **dce-ptgt none none**
  - **krbtgt/***cell_name* **none none**
  - **dce-rgy none none**.

With one exception, all of the accounts created by the **sec_create_db** command are assigned randomly generated passwords and are marked as incorrect. Before these principals can log into these accounts, you must change the account passwords and mark the accounts as valid. You can do this by using the **dcecp account modify** command or **rgy_edit change** command. The *z/OS DCE Administration Guide* provides instructions for using the **dcecp account modify** command to change all of the attributes for a principal's account in the registry, including the principal's password. Also, both commands have options to randomly generate new passwords.

However, the exception is that the account created for the registry creator is valid and is assigned the DCE default password (**-dce-**). Change the default password to ensure the security of the registry creator account.

In addition to the group memberships implied by the accounts that are created by **sec_create_db**, the principals are also made members of the groups listed in Table 7.

Table 7. Group Memberships Created by sec_create_db

The principal:	Is a member of the group:
who	bin
root	system kmem tty
sys	kmem
mail	mail
tcb	tcb

Starting the Master Replica

After the DCECONF command creates the master replica, it starts the master replica. To start the master replica (**secd**) explicitly, use the following steps:

1. Obtain a console where MVS operator commands can be issued.
2. Use the **modify dcekern,query dced** command to ensure that a **dced** is running on the machine. If one is not running, start one by typing:

   ```
   modify dcekern,start dced
   ```

3. Start the master replica by typing:

   ```
   modify dcekern,start secd
   ```

Populating the New Registry Database

Once the master replica is created and started, you must populate the database by setting policies and procedures and adding accounts.

Setting Policies and Properties

Use the **dcecp registry show** and **dcecp registry modify** commands to view policies and properties and to change them as desired. The **rgy_edit properties**, **policy**, and **authpolicy** commands perform the same functions.

Adding Accounts

After a new registry database is created, it contains only the principals, groups, organizations, and accounts that were added as initial information by **sec_create_db**. Use the **dcecp account create** command or **rgy_edit add** command to add any other names and accounts that your site requires. You can do this now or at any time later. See the *z/OS DCE Administration Guide* for information about adding accounts by using **dcecp**.

If you plan to cross link existing RACF users with the new DCE principals to obtain RACF-DCE interoperability and single sign-on, it may be easier to create the DCE principals and then perform the cross linking by using the z/OS DCE utilities, **mvsimpt** and **mvsexpt**. For more information, see the chapter on RACF interoperability in the *z/OS DCE Administration Guide*.

Creating Slave Replicas

After the master replica database is created and started and its database is populated, run the DCECONF command at the slave sites to create the slave replicas and start them. To create and start a slave replica, the DCECONF command first ensures that the sites are running **dced** and the appropriate CDS servers. It then processes the following **sec_create_db** command:

```
$ /bin/sec_create_db -slave -myname my_server_name
```

First, the command creates a database for the new slave replica. The database consists of only stub files. The command then locates the master replica and adds the new slave to the master's replica list. The master marks the new replica for initialization. Finally, the DCECONF command starts **secd** and ensures that it starts automatically each time DCEKERN is started.

You must run the DCECONF command to configure a slave replica at each machine where you want to run a slave replica.

Verifying That the Replicas are Running

After the master and slave replicas are in place and started, perform the following steps to ensure that they are running:

1. Start **sec_admin**, as follows:

```
$ /bin/sec_admin
Default replica:/.../giverny.com/subsys/dce/sec/art_server_master
Default cell:/.../giverny.com
sec_admin>
```

2. Issue the **lrep** command with the **-state** option to display all Security servers and their status, as follows:

```
sec_admin> lrep -state

Default cell:/.../giverny.com
Default replica:/.../giverny.com/subsys/dce/sec/art_server_master

subsys/dce/sec/art_server_master (master)
          State:              in service - master
          Last update time: Tue Feb  8 14:39:57 1996
subsys/dce/sec/mk
          State:              in service - slave
          Last update time: Tue Feb  8 14:39:57 1996
```

Migrating to or from a DB2 Registry

If you are already using the Hierarchical File System (HFS) to store your registry, you can migrate the registry to DB2 without losing your data.

Note: You must be a z/OS UNIX **root** user to do these steps. In addition, if security registry is in DB2, your TSO userid must have DBADMIN authority. The DB2 administrator must issue the following SQL statements to grant access to your userid for the SRGYDATA database and plan:

1. GRANT DBADM ON DATABASE SRGYDATA TO your-userid;
2. GRANT BIND,EXECUTE ON PLAN SRGYDATA TO your-userid;
3. SET CURRENT SQLID='DCEKERN';
4. GRANT BINDAGENT TO your-userid;

Follow these steps to migrate:

1. Be sure that the SRGYDATA database has been created in DB2, and that the SRGYDATA application has been bound. These steps are described in the *z/OS Program Directory*.
2. Set the **SECD_DB2_SUBSYSTEM** environment variable to the DB2 subsystem name (the default is DSN). This environment variable must be set in the **secd** envar file (**opt/dcelocal/home/secd/envar**) and in the envar file of the DCE administrator who runs the DCECONF command. It must also be set in the envar file of anyone who runs the **sec_create_db**, **sec_export_db**, or **sec_import_db** commands. For more information about changing envar files, see “Changing Environment Variable Files for DCE Daemons” on page 8.
3. Disable the registry for updates, so that nothing is changed while you export the registry data to a file.

   dcecp -c registry disable
4. Run the **sec_export_db** command to export the master registry to a file. For example:

   sec_export_db rgydata.out -verbose
5. Stop the DCE kernel:

   stop dcekern
6. Start the DCE kernel without starting all the daemons, so that you can create a new registry with DB2:

   start dcekern,parms='-nodce'
7. Run the **sec_create_db** command with the **-rdb** and **-force** options to create a new skeleton registry in DB2. Specify the same replica name and creator that was used by DCECONF. (The replica name is usually **subsys/dce/sec/master** and the creator name is usually **cell_admin**.)

   sec_create_db -master -my subsys/dce/sec/master -rdb -k
   keyseed **-cr cell_admin -pa** *password* **-force**

8. Run the **sec_import_db** command with the **-replace** option to import the master registry. For example:

   ```
   sec_import_db rgydata.out -rep -v
   ```

9. Restart all the DCE daemons:

   ```
   modify dcekern,start all
   ```

Whenever service is applied to the Security Server, the bind job must be run again, because the DB2 resource definitions will have changed. (There are timestamps in the **secd** load module, the DB2 resource module, and the DB2 catalog which must be synchronized or **secd** will not be able to open the database.) The bind step is the only step that you must run when service is applied.

If you have the registry in DB2, you also need to run the migration job EUVMGDB2.SQL. This job needs to be run to define an additional column for some existing tables. It also defines a new table.

If, for some reason, you must migrate the Registry back to HFS, repeat the steps above, specifying **-hfs** on the **sec_create_db** command to create the registry as an HFS file.

Cross-Memory Credentials Support

Cross-Memory Credentials Support allows the Kerberos credentials cache to be stored in a data space that the DCE Security Server manages. This eliminates the need for HFS credentials cache file I/O and allows the credentials cache to be shared within the same sysplex. (Only the owning system can modify or delete the credentials cache.) This support is available only through DCE interfaces and requires the DCE Security Server to be running on each system in the sysplex.

The credentials cache is volatile and does not persist across a restart of the DCE Security Server that owns the credentials cache. The maximum size of all credentials stored in a single credentials cache is 60000 bytes. Expired credentials are removed from a credentials cache each time a new credential is added to the cache.

The default is to use the normal Kerberos credentials cache file support (FILE cache type). To use a cross-memory credentials cache, set the _EUV_CCACHE_TYPE environment variable to XMEM. A cache type of XMEM is available only to DCE applications. It is not available to native Kerberos applications.

Client applications do not generally derive benefits from a cross-memory credentials cache. This is because the DCE version of Kerberos is designed so that credential lookup operations do not repeatedly access the physical cache file. Applications that will benefit from this support are server applications that use delegation or impersonation to make outbound requests on behalf of a client.

DCE Security Server Support

Communication between the DCE client application and the DCE security server is through the Program Call (PC) instruction. The RACF identity associated with the current thread or process is used for authentication and authorization checking. To access an existing XMEM credentials cache, the user must have created the credentials cache or must have uid 0. The XMEM credentials caches are stored in the EUVSCRED data space. This is the same data space that is used for the context tokens that the sec_login_create_context_token() function creates. A periodic cleanup routine deletes all expired data space entries. (The DCE identity expiration time is used because DCE does not grant any tickets with an end time greater than the identity expiration time). This cleanup routine is driven from the registry database checkpoint timer. In addition, individual expired credentials are purged whenever a new credential is stored in the credentials cache. This keeps a credentials cache from growing without bounds for long-running servers that renew their network credentials.

The SECD_CREDS_SIZE environment variable specifies the maximum size of the EUVSCRED data space in kilobytes. An attempt to specify a size less than 1024K (1MB) or greater than 2097148K (2GB) results in the maximum size being set to the default of 20480K (20MB). The initial data space size is 1024K (1MB) and is increased in increments of 1MB as needed to store credentials and context tokens.

DCE Client Support

Any application that uses DCE security functions can use a cross-memory credentials cache. Cross-memory credentials cache support is not available to applications that use Kerberos functions. A new credentials cache type of XMEM has been defined to support cross-memory credentials. The dce_login, kinit, klist, and kdestroy commands have been enhanced to support XMEM as well as FILE for the credentials cache type. The various sec_login and gssapi API functions have also been enhanced to support the XMEM credentials cache type.

Chapter 6. RACF Interoperability and Single Sign-on

z/OS DCE provides interoperability between z/OS DCE and Resource Access Control Facility (RACF) on z/OS. This security interoperability allows a DCE client to access a DCE-enabled server on a z/OS system and allows the DCE-enabled server to acquire corresponding local security credentials for the DCE client to access z/OS resources. The interoperability function allows:

- Appropriately authorized DCE servers to acquire corresponding z/OS security credentials for the DCE client and to use the DCE client's corresponding z/OS user ID for access to RACF-authorized resources.
- A z/OS user to be transparently logged in to DCE when necessary, without prompting for a DCE user ID or password. This ability is called single sign-on. With this feature, a z/OS user authenticates to z/OS and can start a DCE program without reauthenticating to DCE.

z/OS DCE also provides utilities to incorporate into RACF the information that associates a z/OS RACF user ID with a DCE principal's identifying information and the DCE principal's UUID with the corresponding z/OS RACF user ID. This is called cross-linking information and is what allows interoperability and single sign-on to work.

The cross-linking information must be set up before interoperability functions can be used. To do this, DCE provides two utilities, **mvsimpt** and **mvsexpt**, for creating the initial cross-linking between the two registries. This cross-linking can be done from either the RACF database or the DCE registry, but **mvsimpt** and **mvsexpt** must be started from the z/OS system where the RACF database resides whose users are to be cross linked.

If single sign-on is enabled for a z/OS user, the user must have saved their DCE password in their DCE segment using the z/OS DCE command **storepw** before a DCE application is started. For subsequent password changes, the **-r** flag on the **storepw** command can change the password in both the DCE registry and RACF at the same time. Users must use the **storepw** command *before* invoking a DCE application, and the user's principal must be in the security manager (such as RACF) before **storepw** can update the user's DCE registry. The **storepw** command is described in the *z/OS DCE Command Reference*.

Notes:

1. Although the discussion in this chapter focuses on RACF, any MVS external security manager (ESM) that has equivalent support can be used instead of RACF. However, z/OS DCE provides utilities for cross linking information only between DCE and RACF. If you are not using RACF as your ESM, see the publications that come with your ESM product to determine if similar utilities are provided with the product.
2. Before you start any DCE server, be sure that the z/OS user ID under which it will be started has either of the following:
   - No DCE segment created for that user in RACF
   - The AUTOLOGIN variable in the DCE segment set to NO

   This is necessary whether the server is started by batch job or by a procedure. Configuring this user ID differently could produce unpredictable results when the server is started.

Overview of RACF Interoperability

To have interoperability, the RACF database must contain information that associates a z/OS RACF user ID with a DCE principal and the DCE principal's UUID with the corresponding z/OS RACF user ID. This interoperability information is contained in a new RACF DCE segment and in the RACF general resource class, DCEUUIDS.

When this DCE segment is created for a user by a RACF administrator, either by using RACF commands or by using the z/OS DCE **mvsexpt** utility, the RACF profile for a given z/OS user ID was enhanced to contain a DCE segment. In this segment, you find DCE information for that z/OS user including principal name, cell name, principal UUID, cell UUID, and **AUTOLOGIN** setting. The segment also contains the DCE principal's password. (For more information about this, see "Single Sign-on for z/OS and DCE.")

The information placed in both the RACF DCE segment and the RACF general resource class, DCEUUIDS, is called cross-linking information.

Before the cross-linking process can begin, there is some setup required in the RACF database for proper encryption of DCE passwords, authorization to some Security Authorization Facility (SAF) application programming interfaces (APIs), and so forth. For more information, see *z/OS SecureWay Security Server RACF Security Administrator's Guide*, SA22-7683.

This cross-linking information must be set up before interoperability functions can be used. To do this, DCE provides two utilities, **mvsimpt** and **mvsexpt**, for creating the initial cross-linking between the two registries. The initial cross-linking can be done from either the RACF database or the DCE registry, but **mvsimpt** and **mvsexpt** must be started from the z/OS system where the RACF database resides.

For complete instructions on how to run the **mvsimpt** and **mvsexpt** utilities, see the *z/OS DCE Administration Guide*.

Single Sign-on for z/OS and DCE

In conjunction with RACF interoperability, DCE provides users the ability to effectively sign on (log in) to both z/OS and DCE in one operation. z/OS DCE single sign-on allows a z/OS user who is already authenticated to RACF to be logged in to DCE. DCE does this automatically when a DCE application is started in an address space and the user is not already logged in to DCE.

Note: Single sign-on is not supported for servers that must log in to DCE. Servers must log in to DCE using DCE interfaces.

Preparing for DCE Single Sign-on

Before z/OS DCE single sign-on can be started for a z/OS user, the administrator must enroll the user for single sign-on support. To enroll a user, do these steps:

1. Be sure necessary RACF setup and authorizations were done.
2. Create a DCE segment for the z/OS user, supplying necessary information. Use of the **mvsimpt** and **mvsexpt** utilities to create the segment is recommended.
3. Be sure that the **AUTOLOGIN** flag in the z/OS user's DCE segment is set to YES. Since the default setting is NO (single sign-on is *not* enabled), **AUTOLOGIN=YES** must be explicit.
4. Have the z/OS user store their current DCE password in the RACF database using the **storepw** command. The **storepw** command is described in the *z/OS DCE Command Reference* and *z/OS*

DCE User's Guide. For subsequent password changes, the **-r** flag on the **storepw** command can change the password in both the DCE registry and RACF at the same time.

Automatic DCE Single Sign-on Invocation

After all users requiring single sign-on are enrolled, and each has started the z/OS DCE command **storepw** to save their password in the DCE segment (and, optionally, in the DCE registry), they can authenticate themselves to RACF and start DCE applications. DCE single sign-on is started when a DCE application is run and the user is not already logged in to DCE.

User Control of Automatic DCE Single Sign-on

DCE allows individual users the ability to control whether they have z/OS DCE single sign-on, after the administrator sets **AUTOLOGIN** to YES in the DCE segment for each user. If the administrator sets **AUTOLOGIN** to NO or if there is no setting for **AUTOLOGIN** in a user's DCE segment, then that user does *not* have control over automatic single sign-on. In other words, a user may override the **AUTOLOGIN** setting in the DCE segment only if it is set to YES.

The mechanism for overriding the **AUTOLOGIN=YES** setting is an environment variable entry in the user's ENVAR file that is called **_EUV_AUTOLOG**. The only value that a user can specify for this variable is NO. (Any other variable is ignored.) This environment variable must be set by the user, but if there is no **_EUV_AUTOLOG** environment variable (or it is set to something other than NO), the **AUTOLOGIN** value in the user's DCE segment is used.

For more on DCE environment variables, see the *z/OS DCE Administration Guide* and *z/OS DCE User's Guide*.

Chapter 7. Hardware Cryptography in DCE

z/OS DCE can take advantage of the encryption and decryption function in System/390® and **z**Series 900 processors. DCE uses several of these functions itself for internal system encryption and decryption and for user data privacy features. This support is provided by the combination of the Integrated Cryptographic Feature (ICRF) on the processor and the Integrated Cryptographic Service Facility (ICSF) software product.

If ICSF is installed on your system, you must permit the user IDs of users running DCE access to the RACF-controlled ICSF cryptographic keys and services. This can be done on a user ID or group basis. See the section on controlling who can use cryptographic keys and services in the *z/OS ICSF Administrator's Guide*, SA22-7521, for more information.

Appendix A. Files and Namespace Entries Created at Configuration

This appendix briefly describes most of the files that are created when the DCE configuration program is run. It also lists most entries that are created in the CDS Namespace and the Security Registry for the z/OS host machine and the DCE daemons. For a more complete list of files and entries created during configuration, refer to your configuration log file.

If you are having problems deconfiguring the z/OS host machine using the DCECONF deconfiguration panels, you should remove these files and entries manually. The files and entries that you should remove depend on which DCE daemon you are trying to deconfigure. For example, if you are trying to deconfigure the Password Management server, remove the files and entries created by its configuration.

Configuration Files

This section lists most of the files created for various configurations of the z/OS host.

For z/OS Host Configured as a DCE Client

The following list briefly describes most files created when a z/OS host is configured as a DCE client machine.

File	Description

/opt/dcelocal/dce_cf.db	Contains the cellname and the DCE name of the z/OS host. The file has the following format:
	`cellname /.../cellname`
	`hostname hosts/hostname`
	where *cellname* and *hostname* are the values entered in the DCE Configuration panel.

/opt/dcelocal/etc/security/pe_site	Used by the DCE client daemon to locate the Security server in the cell. This file contains the following information: • Name of the DCE cell. • Object UUID of the Security server in the cell. • The protocol sequence that identifies the network protocol used by DCE. • Internet address of the host that runs the Security server in the cell. This file has the following format: *cellname object-uuid@protocol:IP-address*[]
/krb5/krb.conf	Contains the cellname and the DCE name of the z/OS host. This file has the following format: *cellname* *cellname hostname*
/krb5/krb5.conf	This is the default Kerberos configuration file, although **/krb5/krb.conf** is still supported. Entries in **/krb5/krb5.conf** override those in **/krb5/krb.conf**. The DCE configuration program creates and

	maintains **/krb5/krb.conf**, but you must create and maintain **/krb5/krb5.conf** yourself if you wish to use it. See Appendix D, "Kerberos Configuration Files" on page 117 for more information on this file.
/krb5/v5srvtab	Contains the passwords of the z/OS DCE daemons. This is also known as the **keytab** file of the z/OS DCE daemons.
/opt/dcelocal/etc/cds.conf	File used to configure the CDS client daemons. It contains the following information: • DCE principal name of the z/OS host system • The name of the Security group to which the CDS server belongs • The name of the Security group that has the privileges to administer CDS • The principal that the GDA daemon runs under

For z/OS Host Configured as a Master or Replica Security Server

No files are created when a z/OS host is configured as a master or replica Security server.

For z/OS Host Configured as an Audit Server

The following list briefly describes most files created when a z/OS host is configured as an Audit server.

File	Description
/opt/dcelocal/var/audit/adm/acl	The access control list for the Audit daemon.

For z/OS Host Configured as a Password Management Server

The following list briefly describes most files created when a z/OS host is configured as a Password Management Server.

File	Description
/krb5/pwd_strength_tab	Contains the password for the Password Management server.

For z/OS Host Configured as a Global Directory Agent Server

The following list briefly describes most files created or modified when a z/OS host is configured as a Global Directory Agent server.

File	Description
/opt/dcelocal/etc/cds.conf	The principal name that the GDA daemon runs under is added to this file. Updated by DCECONF during configuration of the GDA daemon.
/krb5/v5srvtab	This file is updated by DCECONF to add keytab entries.
/opt/dcelocal/etc/gda_id	Contains the UUID of the clearinghouse replica that CDS attribute information (gdaAttribute) is added to.

/opt/dcelocal/var/directory/cds/gda_mgmt_acl_v1.dat Contains security information used by the GDA daemon.

For z/OS Host Configured as the Master Cell Directory Server

The following list briefly describes most files created when a z/OS host is configured as the master CDS. For the files listed in the following table, specify the path **/opt/dcelocal/var/directory/cds/**.

File	Description
cellname#*clearinghouse_name*.**checkpoint000000000***n*	File used by a CDS clearinghouse. One for each clearinghouse.
cellname#*clearinghouse_name*.**tlog000000000***n*	File used by a CDS clearinghouse. One for each clearinghouse.
cellname#*clearinghouse_name*.**version**	File used by a CDS clearinghouse. One for each clearinghouse.
cds_files	The list of clearinghouses for this host.
server_mgmgt_acl_v1.dat	Contains security information used by the CDS daemon.

For z/OS Host Configured as a Secondary Cell Directory Server

The following list briefly describes most files created when a z/OS host is configured as a secondary CDS. For the files listed in the following table, specify the path **/opt/dcelocal/var/directory/cds/**.

File	Description
cellname#*clearinghouse_name*.**checkpoint000000000***n*	File used by a CDS clearinghouse. One for each clearinghouse.
cellname#*clearinghouse_name*.**tlog000000000***n*	File used by a CDS clearinghouse. One for each clearinghouse.
cellname#*clearinghouse_name*.**version**	File used by a CDS clearinghouse. One for each clearinghouse.
cds_files	The list of clearinghouses for this host.
server_mgmgt_acl_v1.dat	Contains security information used by the CDS daemon.

CDS Namespace Entries

This section lists most of the CDS namespace entries for various configurations of the z/OS host.

For z/OS Host Configured as a DCE Client

The following list briefly describes most CDS namespace entries created when a z/OS host is configured as a DCE client machine.

Entry	Description
/.:/hosts/*hostname*	Directory into which RPC server entries, groups, and profiles associated with the z/OS host system are stored.

/.:/hosts/*hostname***/self**	Object entry for the z/OS host system. It contains the binding to the DCE daemon.
/.:/hosts/*hostname***/cds-clerk**	Object entry for the CDS Clerk and Advertiser. It contains the binding to the CDS Advertiser.
/.:/hosts/*hostname***/profile**	The default profile for the z/OS host system. It must contain a default that points (possibly indirectly) at **/.:/cell-profile**.
/.:/hosts/*hostname***/dts-entity**	Object entry for the DTS entity. It contains the binding to the DTS entity. This is created by the DTS daemon, not DCECONF. DCECONF adds the DTS entity to the LAN profile (**/.:/lan-profile**) and the Cell profile (**.:/cell-profile**).

For z/OS Host Configured as a Master or Replica Security Server

This section lists CDS namespace entries created when a z/OS host is configured as a master or replica Security server.

Entry	Description
/.:/subsys/dce/sec/*servername*	Directory entry for the local Security server. One is created for each Security server in the cell.

For z/OS Host Configured as an Audit Server

The following list briefly describes most CDS namespace entries created when a z/OS host is configured as an Audit server.

Entry	Description
/.:/hosts/*hostname***/audit-server**	Object entry for the Audit server.

For z/OS Host Configured as a Password Management Server

The following list briefly describes most CDS namespace entries created when a z/OS host is configured as a Password Management server.

Entry	Description
/.:/subsys/dce/pwd_mgmt	Directory in which information is stored pertaining to the Password Management server.
/.:/subsys/dce/pwd_mgmt/pwd_strength	Object entry for the Password Management server.

For z/OS Host Configured as a Global Directory Agent Server

The following list briefly describes most CDS namespace entries created when a z/OS host is configured as a Global Directory Agent server.

Entry	Description
/.:/hosts/*hostname***/cds-gda**	Object entry for the GDA daemon; created by DCECONF. Contains binding information to GDA daemons in the cell.

For z/OS Host Configured as the Master Cell Directory Server

The following list briefly describes most CDS namespace entries created when a z/OS host is configured as the master CDS.

Entry	Description
/.:/*clearinghouse_name*	Clearinghouse entry
/.:/cell-profile CDS_Class RPC_Profile CDS_ClassVersion 1.0	Object entry
/.:/lan-profile CDS_Class RPC_Profile CDS_ClassVersion 1.0	Object entry
/.:/subsys	Directory entry
/.:/subsys/dce	Directory entry
/.:/subsys/dce/sec	Directory entry
/.:/subsys/dce/dfs	Directory entry
/.:/hosts	Directory entry
/.:/hosts/*hostname*	Directory entry
/.:/hosts/*hostname***/profile CDS_Class RPC_Profile CDS_ClassVersion 1.0**	Object entry
/.:/hosts/*hostname***/self CDS_Class RPC_Entry CDS_ClassVersion 1.0**	Object entry
/.:/sec CDS_Class RPC_Group CDS_ClassVersion 1.0	Object entry
/.:/sec-v1 CDS_Class RPC_Group CDS_ClassVersion 1.0	Object entry
/.:/hosts/*hostname***/cds-server**	Object entry for the CDS server
/.:/fs	Distributed File System junction

For z/OS Host Configured as a Secondary Cell Directory Server

The following list briefly describes most CDS namespace entries created when a z/OS host is configured as a secondary CDS.

Entry	Description
/.:/*clearinghouse_name*	Clearinghouse entry for the CDS server
/.:/hosts/*hostname***/cds-server**	Object entry for the CDS server

Security Registry Entries

This section lists most of the Registry entries for various configurations of the z/OS host.

For z/OS Host Configured as a DCE Client

The following list briefly describes most Registry entries created when a z/OS host is configured as a DCE client machine.

Entry	Description
hosts/*hostname***/self**	Principal and account for the z/OS host system.

subsys/dce/rpc-server-group Server group that has the appropriate permissions to the Endpoint map. Application servers on the host that need to register their endpoints in the endpoint map must be made members of this group.

For z/OS Host Configured as a Master or Replica Security Server

No Registry entries are created when a z/OS host is configured as a master or replica Security server.

For z/OS Host Configured as an Audit Server

No Registry entries are created when a z/OS host is configured as an Audit server.

For z/OS Host Configured as a Password Management Server

The following list briefly describes most Registry entries created when a z/OS host is configured as a Password Management server.

Entry	Description
pwd_strength	Principal and account for the Password Management server.

For z/OS Host Configured as a Global Directory Agent Server

The following list briefly describes most Registry entries created when a z/OS host is configured as a Global Directory Agent server.

Entry	Description
hosts/*hostname***/gda**	Principal and account for the Global Directory Agent server. This account is a member of the Registry group **subsys/dce/cds-server** and is created by DCECONF.

For z/OS Host Configured as the Master Cell Directory Server

The following list briefly describes most Registry entries created when a z/OS host is configured as the master Cell Directory server.

Entry	Description
subsys/dce/rpc-server-group	This is the group name for the master Cell Directory server.
hosts/*hostname***/cds-server**	Principal and account for the master Cell Directory server.

For z/OS Host Configured as a Secondary Cell Directory Server

The following list briefly describes most Registry entries created when a z/OS host is configured as a secondary Cell Directory server.

Entry	Description
hosts/*hostname***/cds-server**	Principal and account for the secondary Cell Directory server.

Appendix B. Example DCECONF Log Files

This appendix shows the contents of the log file after:

- Configuration of a Security server on a z/OS host
- Configuration of a Security Replica server on a z/OS host
- Configuration of the Audit server on a z/OS host
- Deconfiguration of the Audit server from a z/OS host
- Configuration of the Password Management server on a z/OS host
- Deconfiguration of the Password Management server from a z/OS host
- Configuration of a z/OS host system as a DCE client machine
- Deconfiguration of a z/OS host system configured as a client machine
- Configuration of a new cell with secd and cdsd
- Deconfiguration of a new cell with secd and cdsd
- Configuration of a new cell with secd and cdsd on different hosts
- Deconfiguration of a new cell with secd and cdsd on different hosts
- Configuration of an additional cdsd on a z/OS host
- Reconfiguring the DTS daemon as a DTS clerk
- Configuration of a Global Directory Agent on a z/OS host
- Deconfiguration of a Global Directory Agent on a z/OS host

Note: z/OS DCE does not erase the log files. To conserve space, you can edit or erase the log files.

The messages that are written in your log file may differ slightly from the messages shown in these examples.

After Configuring a Security Server

The following is an example DCECONF log file after successfully configuring a Security server on a z/OS host.

```
Notice:  DCECONF started at Mon Jan 15 21:15:09 1996.

Notice:  Option EUVBMAIN.1 selected.

Notice:  Option EUVBSERV.1 selected.
Configuring the Security daemon

(/opt/dcelocal/dce_cf.db)
cellname /.../testcell
hostname hosts/DCEDRBLD
rm /home/sudrbld/.rgy_editrc
rm /opt/dcelocal/etc/security/pe_site
rm /opt/dcelocal/var/security/lrgy
rm /opt/dcelocal/var/security/sec_clientd
rm /opt/dcelocal/var/security/.mkey
rm /krb5/v5srvtab
rm /opt/dcelocal/var/rcache/krb5kdc_rcache

(/krb5/krb.conf)
testcell
testcell DCEDRBLD
```

```
EUVB00015I Starting DCE daemon.
EUVS14046I Creating master registry database for cell /.../testcell.
EUVS13706I Checkpointing registry database.
EUVS13712I Saving file rgy.
EUVS13713I Saving relation acct.
EUVS13713I Saving relation person.
EUVS13713I Saving relation group.
EUVS13713I Saving relation org.
EUVS13713I Saving relation replicas.
EUVS13713I Saving relation acl.
EUVS13713I Saving relation attributes.
EUVS13713I Saving relation attr_schema.
EUVS13713I Saving relation login_activity.
EUVS13713I Saving relation journal_file.
EUVS13707I Successfully checkpointed registry database.
EUVS14045I Registry database created.
EUVS14058I pe_site file created.

EUVB00015I Starting DCE daemon.
EUVB00015I Starting Security daemon.
EUVB00017I Login for cell_admin at Mon Jan 15 21:18:46 1996.
dce_login cell_admin
EUVS24588I Warning - change current password.
EUVS24577I Login successful.


rgy_edit -up
Current site is: registry server at /.../testcell/subsys/dce/sec/master.
domain group
Domain changed to: group
add acct-admin
add subsys/dce/sec-admin
add subsys/dce/cds-admin
add subsys/dce/dfs-admin
add subsys/dce/dts-admin
add subsys/dce/dskl-admin
add subsys/dce/audit-admin
add subsys/dce/cds-server
add subsys/dce/dts-servers
add subsys/dce/dfs-fs-servers
add subsys/dce/dfs-bak-servers
member acct-admin -a cell_admin
member subsys/dce/sec-admin -a cell_admin
member subsys/dce/cds-admin -a cell_admin
member subsys/dce/audit-admin -a cell_admin
member subsys/dce/dts-admin -a cell_admin
member subsys/dce/dfs-admin -a cell_admin
member subsys/dce/dskl-admin -a cell_admin

EUVB00906I Security Server configuration is successful.
```

After Configuring a Replica Security Server

The following is an example DCECONF log file after successfully configuring a Security Replica server on a z/OS host.

```
Notice:  Option EUVBMAIN.1 selected.

Notice:  Option EUVBSERV.2 selected.
Configuring the Replica Server
acl_edit /.:/sec/replist  -m user:hosts/DCEDRBLD/self:imI

acl_edit /.:/sec/replist -m group:acct-admin:cidmA

acl_edit /.:/subsys/dce/sec -m user:hosts/DCEDRBLD/self:rwdtcia

acl_edit /.:/subsys/dce/sec -io -m user:hosts/DCEDRBLD/self:rwdtc

acl_edit /.:/subsys/dce/sec -ic -m user:hosts/DCEDRBLD/self:rwdtci
```

```
acl_edit  -e /.:/sec -m user:hosts/DCEDRBLD/self:rwdtc

acl_edit /.:  -m user:dce-rgy:rti

acl_edit -e /.:/cell-profile  -m user:dce-rgy:rwt

EUVS14047I Creating replica registry database for cell /.../testcell.
EUVS13706I Checkpointing registry database.
EUVS13712I Saving file rgy.
EUVS13713I Saving relation acct.
EUVS13713I Saving relation person.
EUVS13713I Saving relation group.
EUVS13713I Saving relation org.
EUVS13713I Saving relation replicas.
EUVS13713I Saving relation acl.
EUVS13713I Saving relation attributes.
EUVS13713I Saving relation attr_schema.
EUVS13713I Saving relation login_activity.
EUVS13713I Saving relation journal_file.
EUVS13707I Successfully checkpointed registry database.
EUVS14045I Registry database created.
EUVS13203I Exporting 0d7c1e50-113a-11ca-b71f-08001e01dc6c,1.0 to /.../testcell/subsys/dce/sec/mvs-security-replica.
EUVS14060I RPC string bindings appended to pe_site file.

EUVB00015I Starting Security Replica.
EUVB00907I Replica Security Server configuration is successful.
```

After Configuring the Audit Server

The following is an example DCECONF log file after successfully configuring the Audit server on a z/OS host.

```
Notice:  Option EUVBMAIN.1 selected.

Notice:  Option EUVBSERV.3 selected.
Configuring the Audit daemon
EUVB00015I Starting Audit daemon.
dcecp -c audfilter create world -at {dce_sec_modify success log}

dcecp -c audfilter create world -at {dce_sec_modify {failure denial} all}

dcecp -c audfilter create world -at {dce_sec_server success log}

dcecp -c audfilter create world -at {dce_sec_server {failure denial} all}

dcecp -c audfilter create world -at {dce_sec_authent {failure denial} all}

dcecp -c audfilter create world -at {dce_sec_query denial all}

dcecp -c audfilter create world -at {dce_dts_mgt_modify success all}

dcecp -c audfilter create world -at {dce_dts_mgt_modify {failure denial} all}

dcecp -c audfilter create world -at {dce_dts_mgt_query {failure denial} all}

dcecp -c audfilter create world -at {dce_audit_admin_modify success all}

dcecp -c audfilter create world -at {dce_audit_admin_modify {failure denial} all}

dcecp -c audfilter create world -at {dce_audit_filter_modify success log}

dcecp -c audfilter create world -at {dce_audit_filter_modify {failure denial} all}

dcecp -c audfilter create world -at {dce_audit_admin_query {failure denial} all}

dcecp -c audfilter create world -at {dce_audit_filter_query {failure denial} all}

EUVB00908I Audit Server configuration is successful.
```

After Deconfiguring the Audit Server

The following is an example DCECONF log file after successfully deconfiguring the Audit server from a z/OS host.

```
Notice:  Option EUVBMAIN.2 selected.

Notice:  Option EUVBDCS .2 selected.
EUVB00083I Deconfiguration of the Audit daemon has started.
EUVB00016I Stopping Audit daemon.
cdscp delete obj /.:/hosts/DCEDRBLD/audit-server

rm /opt/dcelocal/var/audit/adm/acl
EUVB00903I This machine has been successfully deconfigured.
```

After Configuring the Password Management Server

The following is an example DCECONF log file after successfully configuring the Password Management server on a z/OS host.

```
Notice:  Option EUVBMAIN.1 selected.

Notice:  Option EUVBSERV.4 selected.
Configuring the Password Management Server
 pwd_min_len: 8
                          all_spaces : 0
                          alpha_num  : 0

rgy_edit -up

rgy_edit -up

rgy_edit -up

cdscp

rpccp

rgy_edit -up
Current site is: registry server at /.../testcell/subsys/dce/sec/master.
domain principal
Domain changed to: principal
add pwd_strength

domain account
add pwd_strength -g acct-admin -o none -pw XXXXXXXX -mp XXXXXXXX
rgy_edit -up

ktadd -p pwd_strength -pw XXXXXXXX -f /krb5/pwd_strength_tab
ktadd -p pwd_strength -a -r -f /krb5/pwd_strength_tab
rgy_edit -up

cdscp
create dir /.:/subsys/dce/pwd_mgmt


rpccp
export /.:/subsys/dce/pwd_mgmt/pwd_strength -i bababf24-dd2d-11cc-8dfb-080009353559,1.0 -b ncacn_ip_tcp:DCEDRBLD
-b ncadg_ip_udp:DCEDRBLD
EUVR12391I Binding information exported.


acl_edit /.:/subsys/dce/pwd_mgmt -m user:cell_admin:rwidtca

acl_edit -e /.:/subsys/dce/pwd_mgmt/pwd_strength -m user:cell_admin:rwdtc user:pwd_strength:rwt user:dce-rgy:rt

acl_edit -e /.:/hosts/DCEDRBLD/config/epmap -m user:pwd_strength:clidsxt
```

```
EUVB00015I Starting Password Management daemon.
EUVB00909I Password Management Server configuration is successful.
```

After Deconfiguring the Password Management Server

The following is an example DCECONF log file after successfully deconfiguring the Password Management server from a z/OS host.

```
Notice:  Option EUVBMAIN.2 selected.

Notice:  Option EUVBDCS .3 selected.
EUVB00016I Stopping Password Management daemon.

EUVB00080I Deleting Password Management objects
cdscp delete obj /.:/subsys/dce/pwd_mgmt/pwd_strength

cdscp delete dir /.:/subsys/dce/pwd_mgmt

rgy_edit -up
Current site is: registry server at /.../testcell/subsys/dce/sec/master.
domain principal
Domain changed to: principal
del pwd_strength

rm /krb5/pwd_strength_tab
EUVB00903I This machine has been successfully deconfigured.
```

After Configuring as a DCE Client Machine

The following is an example DCECONF log file after successfully configuring the z/OS host as a DCE client machine. In this example, the DTS daemon was configured as a local server.

```
Notice:  DCECONF started at Thu Jan 11 16:29:33 1996.

Notice:  Option EUVBMAIN.3 selected.
EUVB00001I Client configuration initiated at Thu Jan 11 16:30:17 1996.

Notice: Panel Data:
        <cellname>    = !testcell!
        <secd ipname> = !dcecell21!
        <secd ipaddr> = !9.130.79.118!
        <cdsd ipname> = !dcecell21!
        <cdsd ipaddr> = !9.130.79.118!
        <hostname>    = !DCEDRBLD!


EUVB00008I Step 1: Creating bootstrap login environment.


(/opt/dcelocal/dce_cf.db)
cellname /.../testcell
hostname hosts/DCEDRBLD
rpccp show mapping ncadg_ip_udp:9.130.79.118 -i4c878280-5000-0000-0d00-028714000000,1.0


Notice: SECD Binding Data:
  <object>         84acebcc-4c2b-11cf-8313-10005ab169d0
  <interface id>   4c878280-5000-0000-0d00-028714000000,1.0
  <string binding> ncacn_ip_tcp:9.130.79.118[3232]
  <annotation>     DCE user registry rs_misc_v1_0_s_ifspec


(/opt/dcelocal/etc/security/pe_site)
/.../testcell 84acebcc-4c2b-11cf-8313-10005ab169d0@ncacn_ip_tcp:9.130.79.118[]

Notice: SECD Binding Data:
```

```
  <object>         84acebcc-4c2b-11cf-8313-10005ab169d0
  <interface id>   4c878280-5000-0000-0d00-028714000000,1.0
  <string binding> ncadg_ip_udp:9.130.79.118[3076]
  <annotation>     DCE user registry rs_misc_v1_0_s_ifspec

/.../testcell 84acebcc-4c2b-11cf-8313-10005ab169d0@ncadg_ip_udp:9.130.79.118[]
EUVB00017I Login for cell_admin at Thu Jan 11 16:30:30 1996.
dce_login cell_admin
EUVS24588I Warning - change current password.
EUVS24577I Login successful.


EUVB00009I Step 2: DCE Host daemon (security) configuration is in progress.


(/krb5/krb.conf)
testcell
testcell DCEDRBLD
domain principal
add hosts/DCEDRBLD/self
domain account
add hosts/DCEDRBLD/self -g none -o none -pw XXXXXXXX -mp XXXXXXXX
ktadd -p hosts/DCEDRBLD/self -pw XXXXXXXX
ktadd -p hosts/DCEDRBLD/self -a -r
rgy_edit -up


EUVB00010I Step 3: DCE Host daemon (endpoint map) configuration is in progress.

rgy_edit -up
Current site is: registry server at /.../testcell/subsys/dce/sec/master.
domain group
Domain changed to: group
add subsys/dce/rpc-server-group

EUVB00015I Starting DCE daemon.

EUVB00011I Step 4: CDS configuration is in progress.


(/opt/dcelocal/etc/cds.conf)
cds.*.security.host_princ_name: hosts/DCEDRBLD/self
cds.*.security.server_group_name: subsys/dce/cds-server
cds.*.security.admin_group_name: subsys/dce/cds-admin
EUVB00015I Starting CDS advertiser.
EUVB00015I Starting CDS clerk.

EUVB00013I Step 5: Creating objects in name space.

cdscp define cached server dcecell21 tower ncadg_ip_udp:9.130.79.118

cdscp show obj /.:/hosts/DCEDRBLD/config

cdscp create dir /.:/hosts/DCEDRBLD

cdscp create obj /.:/hosts/DCEDRBLD/self

cdscp create obj /.:/hosts/DCEDRBLD/cds-clerk CDS_Class RPC_Entry CDS_ClassVersion 1.0

cdscp create obj /.:/hosts/DCEDRBLD/dts-entity CDS_Class RPC_Entry CDS_ClassVersion 1.0

cdscp create obj /.:/hosts/DCEDRBLD/profile CDS_Class RPC_Entry CDS_ClassVersion 1.0

rpccp export -i 4ea31de8-9a94-11c9-bb60-08002b0f79aa,0003.0000 -b ncadg_ip_udp: -o dc8c6fc0-6143-11ca-b4b9-08002b1bb4f5 -s dce
/.:/hosts/DCEDRBLD/cds-clerk

rpccp add element /.:/hosts/DCEDRBLD/profile -m /.:/cell-profile -d -p 0

acl_edit /.:/hosts/DCEDRBLD -m user:hosts/DCEDRBLD/self:rwdtcia

acl_edit -e /.:/hosts/DCEDRBLD/self -m user:hosts/DCEDRBLD/self:rwdtc
```

```
acl_edit -e /.:/hosts/DCEDRBLD/cds-clerk -m user:hosts/DCEDRBLD/self:rwt

acl_edit -e /.:/hosts/DCEDRBLD/dts-entity -m user:hosts/DCEDRBLD/self:rwt

acl_edit -e /.:/hosts/DCEDRBLD/profile -m user:hosts/DCEDRBLD/self:rwt

acl_edit /.:/hosts/DCEDRBLD/config/epmap -m user:hosts/DCEDRBLD/self:clidsxt

acl_edit /.:/hosts/DCEDRBLD/config/epmap -m user:cell_admin:clidsxt

acl_edit /.:/hosts/DCEDRBLD/config/epmap -m group:subsys/dce/rpc-server-group:lst

acl_edit /.:/hosts/DCEDRBLD/config/epmap -m any_other:lt

acl_edit /.:/hosts/DCEDRBLD/config/epmap -m unauthenticated:lt

acl_edit /.:/hosts/DCEDRBLD/config -m user:hosts/DCEDRBLD/self:crws

acl_edit /.:/hosts/DCEDRBLD/config -m user:cell_admin:crws

acl_edit /.:/hosts/DCEDRBLD/config -m any_other:r

acl_edit /.:/hosts/DCEDRBLD/config -m unauthenticated:r

acl_edit /.:/hosts/DCEDRBLD/config/hostdata -m user:hosts/DCEDRBLD/self:criI

acl_edit /.:/hosts/DCEDRBLD/config/hostdata -m user:cell_admin:criI

acl_edit /.:/hosts/DCEDRBLD/config/hostdata -m any_other:r

acl_edit /.:/hosts/DCEDRBLD/config/hostdata -m unauthenticated:r

acl_edit /.:/hosts/DCEDRBLD/config/hostdata -m user:hosts/DCEDRBLD/self:cdprw -io

acl_edit /.:/hosts/DCEDRBLD/config/hostdata -m user:cell_admin:cdprw -io

acl_edit /.:/hosts/DCEDRBLD/config/hostdata -m any_other:- -io

acl_edit /.:/hosts/DCEDRBLD/config/hostdata -m unauthenticated:- -io

acl_edit /.:/hosts/DCEDRBLD/config/keytab -m user:hosts/DCEDRBLD/self:criI

acl_edit /.:/hosts/DCEDRBLD/config/keytab -m user:cell_admin:criI

acl_edit /.:/hosts/DCEDRBLD/config/keytab -m any_other:r

acl_edit /.:/hosts/DCEDRBLD/config/keytab -m unauthenticated:r

acl_edit /.:/hosts/DCEDRBLD/config/keytab -m user:hosts/DCEDRBLD/self:acdepr -io

acl_edit /.:/hosts/DCEDRBLD/config/keytab -m user:cell_admin:acdepr -io

acl_edit /.:/hosts/DCEDRBLD/config/keytab -m any_other:- -io

acl_edit /.:/hosts/DCEDRBLD/config/keytab -m unauthenticated:- -io

acl_edit /.:/hosts/DCEDRBLD/config/srvrconf -m user:hosts/DCEDRBLD/self:criI

acl_edit /.:/hosts/DCEDRBLD/config/srvrconf -m user:cell_admin:criI

acl_edit /.:/hosts/DCEDRBLD/config/srvrconf -m any_other:r

acl_edit /.:/hosts/DCEDRBLD/config/srvrconf -m unauthenticated:r

acl_edit /.:/hosts/DCEDRBLD/config/srvrconf -m user:hosts/DCEDRBLD/self:cdfrwx -io

acl_edit /.:/hosts/DCEDRBLD/config/srvrconf -m user:cell_admin:cdfrwx -io

acl_edit /.:/hosts/DCEDRBLD/config/srvrconf -m any_other:- -io

acl_edit /.:/hosts/DCEDRBLD/config/srvrconf -m unauthenticated:- -io
```

```
acl_edit /.:/hosts/DCEDRBLD/config/srvrexec -m user:hosts/DCEDRBLD/self:criI

acl_edit /.:/hosts/DCEDRBLD/config/srvrexec -m user:cell_admin:criI

acl_edit /.:/hosts/DCEDRBLD/config/srvrexec -m any_other:r

acl_edit /.:/hosts/DCEDRBLD/config/srvrexec -m unauthenticated:r

acl_edit /.:/hosts/DCEDRBLD/config/srvrexec -m user:hosts/DCEDRBLD/self:crws -io

acl_edit /.:/hosts/DCEDRBLD/config/srvrexec -m user:cell_admin:crws -io

acl_edit /.:/hosts/DCEDRBLD/config/srvrexec -m any_other:- -io

acl_edit /.:/hosts/DCEDRBLD/config/srvrexec -m unauthenticated:- -io

acl_edit /.:/hosts/DCEDRBLD/config/xattrschema -m user:hosts/DCEDRBLD/self:criI

acl_edit /.:/hosts/DCEDRBLD/config/xattrschema -m user:cell_admin:criI

acl_edit /.:/hosts/DCEDRBLD/config/xattrschema -m any_other:r

acl_edit /.:/hosts/DCEDRBLD/config/xattrschema -m unauthenticated:r

acl_edit /.:/hosts/DCEDRBLD/config/xattrschema -m user:hosts/DCEDRBLD/self:crwd -io

acl_edit /.:/hosts/DCEDRBLD/config/xattrschema -m user:cell_admin:crwd -io

acl_edit /.:/hosts/DCEDRBLD/config/xattrschema -m any_other:- -io

acl_edit /.:/hosts/DCEDRBLD/config/xattrschema -m unauthenticated:- -io

acl_edit /.:/hosts/DCEDRBLD/config/secval -m user:hosts/DCEDRBLD/self:csux

acl_edit /.:/hosts/DCEDRBLD/config/secval -m user:cell_admin:csux

acl_edit /.:/hosts/DCEDRBLD/config/secval -m any_other:-

acl_edit /.:/hosts/DCEDRBLD/config/secval -m unauthenticated:-


EUVB00085I Step 6: Starting DTS daemon.

EUVB00015I Starting DTS daemon.

EUVB00014I Step 7: Configuring DTS daemon as local server.


Notice:  Option EUVBDTS .2 selected.
EUVB00003I DTS configuration initiated at Thu Jan 11 17:54:10 1996.

rgy_edit -up
Current site is: registry server at /.../testcell/subsys/dce/sec/master.
domain group
Domain changed to: group
member subsys/dce/dts-servers -a hosts/DCEDRBLD/self

EUVB00016I Stopping DCE daemon.
rm /opt/dcelocal/var/security/creds/dcecred_ffffffff
rm /opt/dcelocal/var/security/creds/dcecred_ffffffff.data
EUVB00015I Starting DCE daemon.

dtscp create type server

dtscp set courier role noncourier

dtscp enable

EUVB00901I This machine is successfully configured as a DCE client.
```

After Deconfiguring the DCE Client Machine

The following is an example DCECONF log file after successfully deconfiguring a z/OS host that was configured as a DCE client machine.

```
Notice:  Option EUVBMAIN.4 selected.
EUVB00002I Client deconfiguration initiated at Thu Jan 11 18:19:10 1996.

Notice: Panel Data:
        local files: 1
        sec objects: 1
        dir objects: 1


EUVB00007I Step 1: Deleting RPC profiles.
 Any message reference to a profile that does not exist is a normal condition.
rpccp remove element /.:/lan-profile -m /.../testcell/hosts/DCEDRBLD/dts-entity -i 019ee420-682d-11c9-a607-08002b0dea7a,1.0
EUVR12290A RPC control program cannot perform requested subcommand.
           DCE status code: 0x16c9a0aa - Profile element is not found.
EUVB00033I Error occurs while running rpccp command.

rpccp remove element /.:/cell-profile -m /.../testcell/hosts/DCEDRBLD/dts-entity -i 17579714-82c9-11c9-8a59-08002b0dc035,1.0
EUVR12290A RPC control program cannot perform requested subcommand.
           DCE status code: 0x16c9a0aa - Profile element is not found.
EUVB00033I Error occurs while running rpccp command.


EUVB00006I Step 2: Deleting directory objects.

cdscp delete obj /.:/hosts/DCEDRBLD/profile

cdscp delete obj /.:/hosts/DCEDRBLD/self

cdscp delete obj /.:/hosts/DCEDRBLD/cds-clerk

cdscp delete obj /.:/hosts/DCEDRBLD/dts-entity

cdscp delete obj /.:/hosts/DCEDRBLD/config

cdscp delete dir /.:/hosts/DCEDRBLD


EUVB00005I Step 3: Deleting security objects.


rgy_edit -nq
Current site is: registry server at /.../testcell/subsys/dce/sec/master.
domain principal
Domain changed to: principal
del hosts/DCEDRBLD/self

EUVB00016I Stopping all daemons.

EUVB00004I Step 4: Deleting configuration and daemon files.

rm /opt/dcelocal/dce_cf.db
rm /opt/dcelocal/etc/security/pe_site
rm /krb5/v5srvtab
rm /opt/dcelocal/etc/cds.conf
rm /opt/dcelocal/etc/cds_config
rm /opt/dcelocal/etc/cdscache.shmid
rm /opt/dcelocal/var/adm/time/mgt_acl
rm /opt/dcelocal/var/adm/time/dtsconfg
rm /opt/dcelocal/var/adm/time/dts_shared_memory_id
rm /opt/dcelocal/var/security/rcache/krb5kdc_rcache
rm /.rgy_editrc
rm /home/sudrbld/.rgy_editrc
rm /krb5/krb.conf
rm /opt/dcelocal/var/dced/Acl.db
rm /opt/dcelocal/var/dced/Ep.db
rm /opt/dcelocal/var/dced/Hostdata.db
```

```
rm /opt/dcelocal/var/dced/Keytab.db
rm /opt/dcelocal/var/dced/Srvrconf.db
rm /opt/dcelocal/var/dced/Srvrexec.db
rm /opt/dcelocal/var/dced/Xattrschema.db
rm /opt/dcelocal/var/security/sec_clientd.binding
rm /opt/dcelocal/var/security/.mkey
rm /opt/dcelocal/var/security/pwd_strengthd.log
rm /opt/dcelocal/var/security/lrgy
rm /opt/dcelocal/var/adm/time/dts-inacc.log
rm /opt/dcelocal/var/audit/adm/acl
rm /opt/dcelocal/var/adm/time/dtsd.acl
rm /krb5/pwd_strength_tab
rm /opt/dcelocal/var/security/creds
rm /opt/dcelocal/var/security/preauth
rm /opt/dcelocal/var/security/creds/dcecred_ffffffff
rm /opt/dcelocal/var/security/creds/dcecred_ffffffff.data
rm /opt/dcelocal/var/security/creds/dcecred_ffffffff.nc
rm /opt/dcelocal/var/security/creds/dummy.file
rm /opt/dcelocal/var/security/creds/SUDRBLD.CACHE.DT960111.TM163035
rm /opt/dcelocal/var/security/creds/SUDRBLD.CACHE.DT960111.TM163035.data
rm /opt/dcelocal/var/security/creds/SUDRBLD.CACHE.DT960111.TM163035.nc
rm /opt/dcelocal/var/adm/directory/cds/cds_cache.version
rm /opt/dcelocal/var/adm/directory/cds/cds_cache.wan
rm /opt/dcelocal/var/adm/directory/cds/cds_cache.0000000001
rm /opt/dcelocal/var/adm/directory/cds/cds_clerk
rm /opt/dcelocal/var/adm/directory/cds/cdsAdver
rm /opt/dcelocal/var/adm/directory/cds/clerk_mgmt_acl_v1.dat

EUVB00903I This machine has been successfully deconfigured.
```

After Configuring a New Cell with secd and cdsd

The following is an example DCECONF log file after successfully configuring a new cell with **secd** and **cdsd** on a z/OS host.

```
Notice:  DCECONF started at Tue May  6 11:15:58 1997.

Notice:  Option EUVBMAIN.1 selected.

Notice:  Option EUVBSERV.1 selected.
Configuring the Security daemon

(/opt/dcelocal/dce_cf.db)
cellname /.../drbld_cell
hostname hosts/dcedrbld
rm /.rgy_editrc
rm /opt/dcelocal/etc/security/pe_site
rm /opt/dcelocal/var/security/lrgy
rm /opt/dcelocal/var/security/sec_clientd
rm /opt/dcelocal/var/security/.mkey
rm /krb5/v5srvtab
rm /opt/dcelocal/var/rcache/krb5kdc_rcache

(/krb5/krb.conf)
drbld_cell
drbld_cell dcedrbld
EUVB00015I Starting DCE daemon.
sec_create_db=>
-my subsys/dce/sec/master -keyseed -creator cell_admin -password -pe 100 -g 100 -o 100 -ma 32767 -hfs
EUVS14046I Creating master registry database for cell /.../drbld_cell.

Tue May  6 11:16:50 1997 VERBOSE SED/RS_CREATE_DB create_db.c:396
EUVS13712I Saving file rgy.

Tue May  6 11:16:53 1997 VERBOSE SED/RS_RSDB rsdb.c:470
EUVS13713I Saving relation acct.

Tue May  6 11:16:53 1997 VERBOSE SED/RS_RSDB rsdb_hfs.c:266
EUVS13713I Saving relation person.
```

```
Tue May  6 11:16:53 1997 VERBOSE SED/RS_RSDB rsdb_hfs.c:266
EUVS13713I Saving relation group.

Tue May  6 11:16:54 1997 VERBOSE SED/RS_RSDB rsdb_hfs.c:266
EUVS13713I Saving relation org.

Tue May  6 11:16:54 1997 VERBOSE SED/RS_RSDB rsdb_hfs.c:266
EUVS13713I Saving relation replicas.

Tue May  6 11:16:54 1997 VERBOSE SED/RS_RSDB rsdb_hfs.c:266
EUVS13713I Saving relation acl.

Tue May  6 11:16:55 1997 VERBOSE SED/RS_RSDB rsdb_hfs.c:266
EUVS13713I Saving relation attributes.

Tue May  6 11:16:55 1997 VERBOSE SED/RS_RSDB rsdb_hfs.c:266
EUVS13713I Saving relation attr_schema.

Tue May  6 11:16:56 1997 VERBOSE SED/RS_RSDB rsdb_hfs.c:266
EUVS13713I Saving relation login_activity.

Tue May  6 11:16:56 1997 VERBOSE SED/RS_RSDB rsdb_hfs.c:266
EUVS13713I Saving relation journal_file.

Tue May  6 11:16:57 1997 VERBOSE SED/RS_RSDB rsdb_hfs.c:266
EUVS14058I pe_site file created.

EUVS14045I Registry database created.


EUVB00015I Starting DCE daemon.
EUVB00015I Starting Security daemon.
EUVS24588I Attention - change current password.

EUVS24577I Login successful.


rgy_edit -up
Current site is: registry server at /.../drbld_cell.
domain group
Domain changed to: group
add acct-admin
add subsys/dce/sec-admin
add subsys/dce/cds-admin
add subsys/dce/dfs-admin
add subsys/dce/dts-admin
add subsys/dce/dskl-admin
add subsys/dce/audit-admin
add subsys/dce/cds-server
add subsys/dce/dts-servers
add subsys/dce/dfs-fs-servers
add subsys/dce/dfs-bak-servers
member acct-admin -a cell_admin
member subsys/dce/sec-admin -a cell_admin
member subsys/dce/cds-admin -a cell_admin
member subsys/dce/audit-admin -a cell_admin
member subsys/dce/dts-admin -a cell_admin
member subsys/dce/dfs-admin -a cell_admin
member subsys/dce/dskl-admin -a cell_admin


Notice:  Option EUVBWCDS.1 selected.
EUVS24588I Attention - change current password.

EUVS24577I Login successful.


EUVB00093I Initial CDSD configuration started at Tue May  6 11:19:12 1997.

EUVB00009I Step 2: DCE Host daemon (security) configuration is in progress.
```

```
rgy_edit -up
Current site is: registry server at /.../drbld_cell.
domain principal
Domain changed to: principal
view hosts/dcedrbld/self
hosts/dcedrbld/self                          102


EUVB00010I Step 3: DCE Host daemon (endpoint map) configuration is in progress.

rgy_edit -up
Current site is: registry server at /.../drbld_cell.
domain group
Domain changed to: group
add subsys/dce/rpc-server-group

domain principal
add hosts/dcedrbld/cds-server
domain account
add hosts/dcedrbld/cds-server -g subsys/dce/cds-server -o none -pw XXXXXXXXXX -mp XXXXXXXXXX
ktadd -p hosts/dcedrbld/cds-server -pw XXXXXXXXXX
ktadd -p hosts/dcedrbld/cds-server -a -r
rgy_edit -up


EUVB00011I Step 4: CDS configuration is in progress.


(/opt/dcelocal/etc/cds.conf)
cds.cdsd.security.server_princ_name: /.../drbld_cell/hosts/dcedrbld/cds-server
cds.*.security.host_princ_name: hosts/dcedrbld/self
cds.*.security.server_group_name: subsys/dce/cds-server
cds.*.security.admin_group_name: subsys/dce/cds-admin
EUVB00015I Starting CDS advertiser.
EUVB00015I Starting CDS clerk.
EUVB00015I Starting CDS daemon.
EUVB00098I Initializing the CDS name space.

acl_edit /.: -ic -s unauthenticated:rt group:subsys/dce/cds-admin:rwcidta group:subsys/dce/cds-server:rwcidta
any_other:rt

acl_edit /.: -io -s unauthenticated:rt group:subsys/dce/cds-admin:rwcdt group:subsys/dce/cds-server:rwcdt
any_other:rt

acl_edit /.: -s unauthenticated:rt group:subsys/dce/cds-admin:rwcidta group:subsys/dce/cds-server:rwcidta
any_other:rt

cdscp
create obj /.:/cell-profile CDS_Class RPC_Profile CDS_ClassVersion 1.0

create obj /.:/lan-profile CDS_Class RPC_Profile CDS_ClassVersion 1.0

create dir /.:/subsys

create dir /.:/subsys/dce

create dir /.:/subsys/dce/sec

create dir /.:/subsys/dce/dfs

create dir /.:/hosts

create dir /.:/hosts/dcedrbld

create obj /.:/hosts/dcedrbld/profile CDS_Class RPC_Profile CDS_ClassVersion 1.0

create obj /.:/hosts/dcedrbld/self CDS_Class RPC_Entry CDS_ClassVersion 1.0

create obj /.:/sec CDS_Class RPC_Group CDS_ClassVersion 1.0

create obj /.:/sec-v1 CDS_Class RPC_Group CDS_ClassVersion 1.0
```

```
rpccp
add element -i d46113d0-a848-11cb-b863-08001e046aa5,2.0 -a rs_bind -m /.:/sec /.:/cell-profile
EUVR12386I Profile element added.


add element -i 0d7c1e50-113a-11ca-b71f-08001e01dc6c,1.0 -a secidmap -m /.:/sec-v1 /.:/cell-profile
EUVR12386I Profile element added.


add element -i 8f73de50-768c-11ca-bffc-08001e039431,1.0 -a krb5rpc  -m /.:/sec /.:/cell-profile
EUVR12386I Profile element added.


add element -i b1e338f8-9533-11c9-a34a-08001e019c1e,1.0 -a rpriv -m /.:/sec /.:/cell-profile
EUVR12386I Profile element added.


add element -i b1e338f8-9533-11c9-a34a-08001e019c1e,1.1 -a rpriv -m /.:/sec /.:/cell-profile
EUVR12386I Profile element added.


add_element /.:/cell-profile -i 6f264242-b9f8-11c9-ad31-08002b0dc035,0001.0000 -m /.:/lan-profile -a LAN -p 0
EUVR12386I Profile element added.


add_element /.:/hosts/dcedrbld/profile -m /.:/cell-profile -d -p 0
EUVR12385I Default profile element added.


add_element /.:/hosts/dcedrbld/profile -i 6f264242-b9f8-11c9-ad31-08002b0dc035,0001.0000 -m /.:/lan-profile -a LAN -p 0
EUVR12386I Profile element added.



rpccp export -i 000cf72e-0688-1acb-97ad-08002b12b8f8,0001.0000 -b ncadg_ip_udp: -o faf2e540-58b8-11ca-a04a-08002b12a70d
-s dce /.:/hosts/dcedrbld/cds-server

rpccp export -i 000cf72e-0688-1acb-97ad-08002b12b8f8,0001.0000 -b ncadg_ip_udp: -o dc8c6fc0-6143-11ca-b4b9-08002b1bb4f5
-s dce /.:/hosts/dcedrbld/cds-clerk

uuidgen

uuidgen

rpccp
add entry /.:/fs
EUVR12372I RPC control program adds entry to name service database.

export -o 974d9208-5547-1e9e-ba11-001234567890 /.:/fs
EUVR12390I Objects exported.


export -o de7c5000-5547-1e9e-9d1d-001234567890 /.:/subsys/dce/dfs/bak
EUVR12390I Objects exported.


add element -i 4d37f2dded43.02.c0.37.cf.2e.00.00.01,4.0 -a fs -m /.:/fs /.:/cell-profile
EUVR12386I Profile element added.


add element -i eb814e2a-0099-11ca-8678-02608c2ea96e,4.0 -a bak -m /:/subsys/dce/dfs/bak /.:/cell-profile
EUVR12386I Profile element added.



rpccp export-i e1af8308-5d1f-11c9-91a4-08002b14a0fa,3.0 -b ncadg_ip_udp:9.130.79.52[135] /.:/hosts/dcedrbld/self

acl_edit /.:/subsys/dce/sec -ic -m user:dce-rgy:rwcidt -m group:subsys/dce/sec-admin:rwcidta

acl_edit /.:/subsys/dce/sec -io -m user:dce-rgy:rwdt -m group:subsys/dce/sec-admin:rwcdt
```

```
acl_edit /.:/subsys/dce/sec -m user:dce-rgy:rwcidt -m group:subsys/dce/sec-admin:rwcidta

acl_edit -e /.:/cell-profile -m group:subsys/dce/dts-admin:rwt -m group:subsys/dce/dts-servers:rwt
-m user:dce-rgy:rwt

acl_edit -e /.:/lan-profile -m group:subsys/dce/dts-admin:rwcdt -m group:subsys/dce/dts-servers:rwcdt

acl_edit -e /.:/dcedrbld_ch -s unauthenticated:rt group:subsys/dce/cds-admin:rwcdt group:subsys/dce/cds-server:rwcdt
any_other:rt

acl_edit /.:/dcedrbld_ch -s unauthenticated:rt group:subsys/dce/cds-admin:rwcdt group:subsys/dce/cds-server:rwcdt
any_other:rt

acl_edit /.:/hosts -m user:hosts/dcedrbld/self:rwdtcia

acl_edit /.:/hosts/dcedrbld -m user:hosts/dcedrbld/self:rwdtcia

acl_edit -e /.:/sec -m group:subsys/dce/sec-admin:rwcdt -m user:dce-rgy:rwcdt

acl_edit -e /.:/sec-v1 -m group:subsys/dce/sec-admin:rwcdt -m user:dce-rgy:rwcdt

acl_edit -e /.:/hosts/dcedrbld/self -m user:hosts/dcedrbld/self:rwdtc

acl_edit -e /.:/hosts/dcedrbld/cds-clerk -m user:hosts/dcedrbld/self:rwt

acl_edit -e /.:/hosts/dcedrbld/cds-server -m user:hosts/dcedrbld/self:rwt

acl_edit -e /.:/hosts/dcedrbld/profile -m user:hosts/dcedrbld/self:rwt

acl_edit -e /.:/fs -m group:subsys/dce/dfs-admin:rwcdt -m group:subsys/dce/dfs-fs-servers:rwcdt

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal -io  -m unauthenticated:rg
-m user_obj:rfug -m group:acct-admin:rcDnfmaug -m other_obj:rg

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal -ic -m group:acct-admin:rcidDn

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal -m group:acct-admin:rcidDn

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal/krbtgt -ic -m group:acct-admin:
rcidDn

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal/krbtgt -io -m group:acct-admin:
rcDnfmaug

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal/krbtgt -m group:acct-admin:rciDdn

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal/krbtgt/drbld_cell -m unauthenticated:rg
-m group:acct-admin:rcDnfmaug

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal/hosts -m group:acct-admin:rcidDn

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal/hosts -io -m group:acct-admin:
rcDnfmaug

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal/hosts -ic -m group:acct-admin:
rcidDn

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal/hosts/dcedrbld
-m group:acct-admin:rcidDn

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal/hosts/dcedrbld -io
-m unauthenticated:rg -m group:acct-admin:rcDnfmaug

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal/hosts/dcedrbld -ic
-m group:acct-admin:rcidDn

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal/hosts/dcedrbld/self
-m group:acct-admin:rcDnfmag

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal/hosts/dcedrbld/cds-server
-m group:acct-admin:rcDnfmag -m group:subsys/dce/cds-admin:rcDnfmag
```

```
acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group -ic -m group:acct-admin:rcidDn
-m any_other:r

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group -io -m group:acct-admin:rctDnfmM
-m any_other:r

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group -m group:acct-admin:rcidDn
-m any_other:r

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group/acct-admin
-m group_obj:rctDnfmM

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group/subsys -m group:acct-admin:rcidDn

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group/subsys -io
-m group:acct-admin:rctDnfmM

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group/subsys -ic -m group:acct-admin:rcidDn

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group/subsys/dce -m group:acct-admin:rcidDn

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group/subsys/dce -io
-m group:acct-admin:rctDnfmM

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group/subsys/dce -ic
-m group:acct-admin:rcidDn

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group/subsys/dce/sec-admin
-m group:acct-admin:rctDnfmM

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group/subsys/dce/dts-admin
-m group:acct-admin:rctDnfmM

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group/subsys/dce/dts-servers
-m group:acct-admin:rctDnfmM -m group:subsys/dce/dts-admin:rctDnfmM

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group/subsys/dce/dfs-admin
-m group:acct-admin:rctDnfmM -m any_other:rt

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group/subsys/dce/dfs-fs-servers
-m group:acct-admin:rctDnfmM -m group:subsys/dce/dfs-admin:rctDnfmM -m any_other:rt

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group/subsys/dce/dfs-bak-servers
-m group:acct-admin:rctDnfmM -m group:subsys/dce/dfs-admin:rctDnfmM -m any_other:rt

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group/subsys/dce/cds-admin
-m group:acct-admin:rctDnfmM

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group/subsys/dce/cds-server
-m group:acct-admin:rctDnfmM -m group:subsys/dce/cds-admin:rctDnfmM -m group:subsys/dce/cds-server:rctDnfmM

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 org -m group:acct-admin:rcidDn

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 org -io -m group:acct-admin:rctDnfmM

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 org -ic -m group:acct-admin:rcidDn

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 policy
-m group:acct-admin:rcma

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal/nobody -m group:acct-admin:rcDnfmaug

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal/root -m group:acct-admin:rcDnfmaug

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal/daemon -m group:acct-admin:rcDnfmaug

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal/sys -m group:acct-admin:rcDnfmaug

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal/bin -m group:acct-admin:rcDnfmaug

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal/uucp -m group:acct-admin:rcDnfmaug
```

```
acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal/who -m group:acct-admin:rcDnfmaug

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal/mail -m group:acct-admin:rcDnfmaug

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal/tcb -m group:acct-admin:rcDnfmaug

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal/dce-ptgt -m group:acct-admin:rcDnfmaug

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 principal/dce-rgy -m group:acct-admin:rcDnfmaug

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group/none -m group:acct-admin:rctDnfmM

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group/system -m group:acct-admin:rctDnfmM

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group/daemon -m group:acct-admin:rctDnfmM

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group/uucp -m group:acct-admin:rctDnfmM

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group/bin -m group:acct-admin:rctDnfmM

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group/kmem -m group:acct-admin:rctDnfmM

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group/mail -m group:acct-admin:rctDnfmM

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group/tty -m group:acct-admin:rctDnfmM

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 group/tcb -m group:acct-admin:rctDnfmM

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 org/none -m group:acct-admin:rctDnfmM

acl_edit -addr 43b97e06-540c-1e9e-81e7-001234567890@ncacn_ip_tcp:9.130.79.52 replist -m user:hosts/dcedrbld/self:imI

acl_edit /.:/subsys/dce/sec -m user:hosts/dcedrbld/self:rwdtcia

acl_edit /.:/subsys/dce/sec -io -m user:hosts/dcedrbld/self:rwdtc

acl_edit /.:/subsys/dce/sec -ic -m user:hosts/dcedrbld/self:rwdtci

acl_edit -e /.:/sec -m user:hosts/dcedrbld/self:rwdtc

acl_edit -e /.:/hosts/dcedrbld/config/epmap -m user:hosts/dcedrbld/cds-server:clidsxt


EUVB00085I Step 6: Starting DTS daemon.

EUVB00015I Starting DTS daemon.

EUVB00014I Step 7: Configuring DTS daemon as local server.


Notice:  Option EUVBDTS .2 selected.
EUVB00003I DTS configuration initiated at Tue May  6 11:31:39 1997.

rgy_edit -up
Current site is: registry server at /.../drbld_cell.
domain group
Domain changed to: group
member subsys/dce/dts-servers -a hosts/dcedrbld/self

EUVB00016I Stopping DCE daemon.
rm /opt/dcelocal/var/security/creds/dcecred_ffffffff
rm /opt/dcelocal/var/security/creds/dcecred_ffffffff.data
EUVB00015I Starting DCE daemon.

dtscp create type server

dtscp set courier role noncourier

dtscp enable

EUVB00906I Security Server configuration is successful.
```

```
Notice:  DCECONF ended at Tue May  6 11:33:10 1997.
-------------------------------------------------------------------------------------------------------------------------
Notice:  DCECONF started at Tue May  6 11:33:21 1997.

Notice:  DCECONF ended at Tue May  6 11:33:25 1997.
-------------------------------------------------------------------------------------------------------------------------
```

After Deconfiguring a New Cell with secd and cdsd

The following is an example DCECONF log file after you have successfully deconfigured a new cell (one that had **secd** and **cdsd** on it) by stopping **dcekern** and starting it again using:

/s dcekern,parms='-nodce'

```
Notice:  DCECONF started at Tue May  6 12:33:24 1997.

Notice:  Option EUVBMAIN.4 selected.
EUVB00002I Client deconfiguration initiated at Tue May  6 12:33:33 1997.

Notice: Panel Data:
        local files: 1
        sec objects: 0
        dir objects: 0

EUVB00016I Stopping all daemons.


EUVB00004I Step 4: Deleting configuration and daemon files.

rm /opt/dcelocal/dce_cf.db
rm /opt/dcelocal/etc/security/pe_site
rm /krb5/v5srvtab
rm /opt/dcelocal/etc/cds.conf
rm /opt/dcelocal/etc/cds_config
rm /opt/dcelocal/etc/cdscache.shmid
rm /opt/dcelocal/var/adm/time/mgt_acl
rm /opt/dcelocal/var/adm/time/dtsconfg
rm /opt/dcelocal/var/adm/time/dts_shared_memory_id
rm /opt/dcelocal/var/security/rcache/krb5kdc_rcache
rm /.rgy_editrc
rm /.rgy_editrc
rm /krb5/krb.conf
rm /opt/dcelocal/var/dced/Acl.db
rm /opt/dcelocal/var/dced/Ep.db
rm /opt/dcelocal/var/dced/Hostdata.db
rm /opt/dcelocal/var/dced/Keytab.db
rm /opt/dcelocal/var/dced/Srvrconf.db
rm /opt/dcelocal/var/dced/Srvrexec.db
rm /opt/dcelocal/var/dced/Xattrschema.db
rm /opt/dcelocal/var/security/sec_clientd.binding
rm /opt/dcelocal/var/security/.mkey
rm /opt/dcelocal/var/security/pwd_strengthd.log
rm /opt/dcelocal/var/security/lrgy
rm /opt/dcelocal/var/adm/time/dts-inacc.log
rm /opt/dcelocal/var/audit/adm/acl
rm /opt/dcelocal/var/adm/time/dtsd.acl
rm /krb5/pwd_strength_tab
rm /opt/dcelocal/var/security/creds/dcecred_ffffffff
rm /opt/dcelocal/var/security/creds/dcecred_ffffffff.data
rm /opt/dcelocal/var/security/creds/dcecred_ffffffff.nc
rm /opt/dcelocal/var/security/creds/dcecred_36f4bed0
rm /opt/dcelocal/var/security/creds/dcecred_36f4bed0.data
rm /opt/dcelocal/var/security/creds/dcecred_36f4bed0.nc
rm /opt/dcelocal/var/security/creds/dcecred_36f4c3a0
rm /opt/dcelocal/var/security/creds/dcecred_36f4c3a0.data
rm /opt/dcelocal/var/security/creds/dcecred_36f4c3a0.nc
rm /opt/dcelocal/var/security/creds/dummy.file
rm /opt/dcelocal/var/security/preauth/pl3KS9tpteC
rm /opt/dcelocal/var/security/preauth/rqm9u0Qy_aO
rm /opt/dcelocal/var/security/preauth/JL0hhjbw59u
```

```
rm /opt/dcelocal/var/adm/directory/cds/cds_cache.version
rm /opt/dcelocal/var/adm/directory/cds/cds_cache.wan
rm /opt/dcelocal/var/adm/directory/cds/cds_cache.0000000001
rm /opt/dcelocal/var/adm/directory/cds/cds_clerk
rm /opt/dcelocal/var/adm/directory/cds/cdsclerk
rm /opt/dcelocal/var/adm/directory/cds/cdsAdver
rm /opt/dcelocal/var/adm/directory/cds/clerk_mgmt_acl_v1.dat
rm /opt/dcelocal/var/security/rgy_data/acct
rm /opt/dcelocal/var/security/rgy_data/acl
rm /opt/dcelocal/var/security/rgy_data/attr_schema
rm /opt/dcelocal/var/security/rgy_data/attributes
rm /opt/dcelocal/var/security/rgy_data/group
rm /opt/dcelocal/var/security/rgy_data/journal_file
rm /opt/dcelocal/var/security/rgy_data/login_activity
rm /opt/dcelocal/var/security/rgy_data/master_info
rm /opt/dcelocal/var/security/rgy_data/org
rm /opt/dcelocal/var/security/rgy_data/person
rm /opt/dcelocal/var/security/rgy_data/replicas
rm /opt/dcelocal/var/security/rgy_data/rgy
rm /opt/dcelocal/var/security/rgy_data/rgy_state
rm /opt/dcelocal/var/security/rgy_data/update_log
rm /opt/dcelocal/var/directory/cds/adm
rm /opt/dcelocal/var/directory/cds/cds_files
rm /opt/dcelocal/var/directory/cds/drbld_cell#dcedrbld_ch.checkpoint0000000003
rm /opt/dcelocal/var/directory/cds/drbld_cell#dcedrbld_ch.tlog0000000003
rm /opt/dcelocal/var/directory/cds/drbld_cell#dcedrbld_ch.version
rm /opt/dcelocal/var/directory/cds/server_mgmt_acl_v1.dat

EUVB00903I This machine has been successfully deconfigured.

Notice:  DCECONF ended at Tue May  6 12:33:46 1997.
```

After Configuring a New Cell with secd and cdsd on Different Hosts

The following is an example DCECONF log file after successfully configuring a new cell with **secd** on a machine other than the z/OS host and **cdsd** on the z/OS host.

```
Notice:  DCECONF started at Tue May  6 15:30:06 1997.

Notice:  Option EUVBMAIN.1 selected.

Notice:  Option EUVBSERV.5 selected.
EUVB00093I Initial CDSD configuration started at Tue May  6 16:03:51 1997.

Notice: Panel Data:
       <cellname>     = !dcecell21.endicott.ibm.com!
       <hostname>     = !DCEDRBLD!
       <secd ipname>  = !dcecell21.endicott.ibm.com!
       <secd ipaddr>  = !!
       <secd dcename> = !dcecell21!


(/opt/dcelocal/dce_cf.db)
cellname /.../dcecell21.endicott.ibm.com
hostname hosts/DCEDRBLD
rpccp show mapping ncadg_ip_udp:9.130.79.118 -i4c878280-5000-0000-0d00-028714000000,1.0


Notice: SECD Binding Data:
  <object>         cedd0ffc-c64a-11d0-b387-10005ab169d0
  <interface id>   4c878280-5000-0000-0d00-028714000000,1.0
  <string binding> ncacn_ip_tcp:9.130.79.118[1341]
  <annotation>     DCE user registry rs_misc_v1_0_s_ifspec


(/opt/dcelocal/etc/security/pe_site)
/.../dcecell21.endicott.ibm.com cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118[]

Notice: SECD Binding Data:
```

```
  <object>         cedd0ffc-c64a-11d0-b387-10005ab169d0
  <interface id>   4c878280-5000-0000-0d00-028714000000,1.0
  <string binding> ncadg_ip_udp:9.130.79.118[1291]
  <annotation>     DCE user registry rs_misc_v1_0_s_ifspec

/.../dcecell21.endicott.ibm.com cedd0ffc-c64a-11d0-b387-10005ab169d0@ncadg_ip_udp:9.130.79.118[]

EUVB00008I Step 1: Creating bootstrap login environment.

EUVB00017I Login for cell_admin at Tue May  6 16:04:02 1997.
dce_login cell_admin
EUVS24588I Attention - change current password.

EUVS24577I Login successful.


EUVB00093I Initial CDSD configuration started at Tue May  6 16:04:09 1997.

EUVB00009I Step 2: DCE Host daemon (security) configuration is in progress.


(/krb5/krb.conf)
dcecell21.endicott.ibm.com
dcecell21.endicott.ibm.com DCEDRBLD
domain principal
add hosts/DCEDRBLD/self
domain account
add hosts/DCEDRBLD/self -g none -o none -pw XXXXXXXX -mp XXXXXXXX
ktadd -p hosts/DCEDRBLD/self -pw XXXXXXXX
ktadd -p hosts/DCEDRBLD/self -a -r
rgy_edit -up

rgy_edit -up
Current site is: registry server at /.../dcecell21.endicott.ibm.com.
domain principal
Domain changed to: principal
view hosts/dcecell21/self
hosts/dcecell21/self                        102


EUVB00010I Step 3: DCE Host daemon (endpoint map) configuration is in progress.

rgy_edit -up
Current site is: registry server at /.../dcecell21.endicott.ibm.com.
domain group
Domain changed to: group
add subsys/dce/rpc-server-group

EUVB00015I Starting DCE daemon.
EUVB00015I Starting DCE daemon.
domain principal
add hosts/DCEDRBLD/cds-server
domain account
add hosts/DCEDRBLD/cds-server -g subsys/dce/cds-server -o none -pw XXXXXXXX -mp XXXXXXXX
ktadd -p hosts/DCEDRBLD/cds-server -pw XXXXXXXX
ktadd -p hosts/DCEDRBLD/cds-server -a -r
rgy_edit -up


EUVB00011I Step 4: CDS configuration is in progress.


(/opt/dcelocal/etc/cds.conf)
cds.cdsd.security.server_princ_name: /.../dcecell21.endicott.ibm.com/hosts/DCEDRBLD/cds-server
cds.*.security.host_princ_name: hosts/DCEDRBLD/self
cds.*.security.server_group_name: subsys/dce/cds-server
cds.*.security.admin_group_name: subsys/dce/cds-admin
EUVB00015I Starting CDS advertiser.
EUVB00015I Starting CDS clerk.
EUVB00015I Starting CDS daemon.
EUVB00098I Initializing the CDS name space.
```

```
acl_edit /.: -ic -s unauthenticated:rt group:subsys/dce/cds-admin:rwcidta group:subsys/dce/cds-server:rwcidta
any_other:rt

acl_edit /.: -io -s unauthenticated:rt group:subsys/dce/cds-admin:rwcdt group:subsys/dce/cds-server:rwcdt
any_other:rt

acl_edit /.: -s unauthenticated:rt group:subsys/dce/cds-admin:rwcidta group:subsys/dce/cds-server:rwcidta
any_other:rt

cdscp
create obj /.:/cell-profile CDS_Class RPC_Profile CDS_ClassVersion 1.0

create obj /.:/lan-profile CDS_Class RPC_Profile CDS_ClassVersion 1.0

create dir /.:/subsys

create dir /.:/subsys/dce

create dir /.:/subsys/dce/sec

create dir /.:/subsys/dce/dfs

create dir /.:/hosts

create dir /.:/hosts/DCEDRBLD

create obj /.:/hosts/DCEDRBLD/profile CDS_Class RPC_Profile CDS_ClassVersion 1.0

create obj /.:/hosts/DCEDRBLD/self CDS_Class RPC_Entry CDS_ClassVersion 1.0

create obj /.:/sec CDS_Class RPC_Group CDS_ClassVersion 1.0

create obj /.:/sec-v1 CDS_Class RPC_Group CDS_ClassVersion 1.0


rpccp
add element -i d46113d0-a848-11cb-b863-08001e046aa5,2.0 -a rs_bind -m /.:/sec /.:/cell-profile
EUVR12386I Profile element added.


add element -i 0d7c1e50-113a-11ca-b71f-08001e01dc6c,1.0 -a secidmap -m /.:/sec-v1 /.:/cell-profile
EUVR12386I Profile element added.


add element -i 8f73de50-768c-11ca-bffc-08001e039431,1.0 -a krb5rpc  -m /.:/sec /.:/cell-profile
EUVR12386I Profile element added.


add element -i b1e338f8-9533-11c9-a34a-08001e019c1e,1.0 -a rpriv -m /.:/sec /.:/cell-profile
EUVR12386I Profile element added.


add element -i b1e338f8-9533-11c9-a34a-08001e019c1e,1.1 -a rpriv -m /.:/sec /.:/cell-profile
EUVR12386I Profile element added.


add_element /.:/cell-profile -i 6f264242-b9f8-11c9-ad31-08002b0dc035,0001.0000 -m /.:/lan-profile -a LAN -p 0
EUVR12386I Profile element added.


add_element /.:/hosts/DCEDRBLD/profile -m /.:/cell-profile -d -p 0
EUVR12385I Default profile element added.


add_element /.:/hosts/DCEDRBLD/profile -i 6f264242-b9f8-11c9-ad31-08002b0dc035,0001.0000 -m /.:/lan-profile -a LAN -p 0
EUVR12386I Profile element added.



rpccp export -i 000cf72e-0688-1acb-97ad-08002b12b8f8,0001.0000 -b ncadg_ip_udp: -o faf2e540-58b8-11ca-a04a-08002b12a70d
-s dce /.:/hosts/DCEDRBLD/cds-server
```

```
rpccp export -i 000cf72e-0688-1acb-97ad-08002b12b8f8,0001.0000 -b ncadg_ip_udp: -o dc8c6fc0-6143-11ca-b4b9-08002b1bb4f5
-s dce /.:/hosts/DCEDRBLD/cds-clerk

uuidgen

uuidgen

rpccp
add entry /.:/fs
EUVR12372I RPC control program adds entry to name service database.

export -o ad669008-9500-1e9e-bf44-001234567890 /.:/fs
EUVR12390I Objects exported.


export -o fe592409-9500-1e9e-b94e-001234567890 /.:/subsys/dce/dfs/bak
EUVR12390I Objects exported.


add element -i 4d37f2dded43.02.c0.37.cf.2e.00.00.01,4.0 -a fs -m /.:/fs /.:/cell-profile
EUVR12386I Profile element added.


add element -i eb814e2a-0099-11ca-8678-02608c2ea96e,4.0 -a bak -m /:/subsys/dce/dfs/bak /.:/cell-profile
EUVR12386I Profile element added.



rpccp export-i e1af8308-5d1f-11c9-91a4-08002b14a0fa,3.0 -b ncadg_ip_udp:9.130.79.52ff135“ /.:/hosts/DCEDRBLD/self

acl_edit /.:/subsys/dce/sec -ic -m user:dce-rgy:rwcidt -m group:subsys/dce/sec-admin:rwcidta

acl_edit /.:/subsys/dce/sec -io -m user:dce-rgy:rwdt -m group:subsys/dce/sec-admin:rwcdt

acl_edit /.:/subsys/dce/sec -m user:dce-rgy:rwcidt -m group:subsys/dce/sec-admin:rwcidta

acl_edit -e /.:/cell-profile -m group:subsys/dce/dts-admin:rwt -m group:subsys/dce/dts-servers:rwt
-m user:dce-rgy:rwt

acl_edit -e /.:/lan-profile -m group:subsys/dce/dts-admin:rwcdt -m group:subsys/dce/dts-servers:rwcdt

acl_edit -e /.:/DCEDRBLD_ch -s unauthenticated:rt group:subsys/dce/cds-admin:rwcdt
group:subsys/dce/cds-server:rwcdt any_other:rt

acl_edit /.:/DCEDRBLD_ch -s unauthenticated:rt group:subsys/dce/cds-admin:rwcdt group:subsys/dce/cds-server :rwcdt
any_other:rt

acl_edit /.:/hosts -m user:hosts/DCEDRBLD/self:rwdtcia

acl_edit /.:/hosts/DCEDRBLD -m user:hosts/DCEDRBLD/self:rwdtcia

acl_edit -e /.:/sec -m group:subsys/dce/sec-admin:rwcdt -m user:dce-rgy:rwcdt

acl_edit -e /.:/sec-v1 -m group:subsys/dce/sec-admin:rwcdt -m user:dce-rgy:rwcdt

acl_edit -e /.:/hosts/DCEDRBLD/self -m user:hosts/DCEDRBLD/self:rwdtc

acl_edit -e /.:/hosts/DCEDRBLD/cds-clerk -m user:hosts/DCEDRBLD/self:rwt

acl_edit -e /.:/hosts/DCEDRBLD/cds-server -m user:hosts/DCEDRBLD/self:rwt

acl_edit -e /.:/hosts/DCEDRBLD/profile -m user:hosts/DCEDRBLD/self:rwt

acl_edit -e /.:/fs -m group:subsys/dce/dfs-admin:rwcdt -m group:subsys/dce/dfs-fs-servers:rwcdt

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal -io  -m unauthenticated:rg
-m user _obj -m group:acct-admin:rcDnfmaug -m other_obj:rg

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal -ic -m group:acct-admin:rcidDn

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal -m group:acct-admin:rcidDn
```

```
acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal/krbtgt -ic -m group:acct-admin:rcidDn

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal/krbtgt -io
-m group:acct-admin:rcDnfmaug

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal/krbtgt -m group:acct-admin:rciDdn

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal/krbtgt/dcecell21.endicott.ibm.com
-m unauthenticated:rg -m group:acct-admin:rcDnfmaug

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal/hosts -m group:acct-admin:rcidDn

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal/hosts -io
-m group:acct-admin:rcDnfmaug

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal/hosts -ic -m group:acct-admin
:rcidDn

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal/hosts/DCEDRBLD
-m group:acct-admin:rcidDn

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal/hosts/DCEDRBLD -io -m unauthenticated:rg
-m group:acct-admin:rcDnfmaug

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal/hosts/DCEDRBLD -ic
-m group:acct-admin:rcidDn

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal/hosts/DCEDRBLD/self
-m group:acct-admin:rcDnfmag

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal/hosts/DCEDRBLD/cds-server
-m group:acct-admin:rcDnfmag -m group:subsys/dce/cds-admin:rcDnfmag

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group -ic
-m group:acct-admin:rcidDn -m any_other:r

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group -io -m group:acct-admin:rctDnfmM
-m any_other:r

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group -m group:acct-admin:rcidDn
-m any_other:r

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group/acct-admin -m group_obj:rctDnfmM

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group/subsys -m group:acct-admin:rcidDn

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group/subsys -io
-m group:acct-admin:rctDnfmM

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group/subsys -ic -m group:acct-admin:rcidDn

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group/subsys/dce -m group:acct-admin:rcidDn

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group/subsys/dce -io
-m group:acct-admin:rctDnfmM

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group/subsys/dce -ic
-m group:acct-admin:rcidDn

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group/subsys/dce/sec-admin
-m group:acct-admin:rctDnfmM

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group/subsys/dce/dts-admin
-m group:acct-admin:rctDnfmM

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group/subsys/dce/dts-servers
-m group:acct-admin:rctDnfmM -m group:subsys/dce/dts-admin:rctDnfmM

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group/subsys/dce/dfs-admin
-m group:acct-admin:rctDnfmM -m any_other:rt
```

```
acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group/subsys/dce/dfs-fs-servers
-m group:acct-admin:rctDnfmM -m group:subsys/dce/dfs-admin:rctDnfmM -m any_other:rt

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group/subsys/dce/dfs-bak-servers
-m group:acct-admin:rctDnfmM -m group:subsys/dce/dfs-admin:rctDnfmM -m any_other:rt

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group/subsys/dce/cds-admin
-m group:acct-admin:rctDnfmM

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group/subsys/dce/cds-server
-m group:acct-admin:rctDnfmM -m group:subsys/dce/cds-admin:rctDnfmM
-m group:subsys/dce/cds-server:rctDnfmM

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 org -m group:acct-admin:rcidDn

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 org -io -m group:acct-admin:rctDnfmM

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 org -ic -m group:acct-admin:rcidDn

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 policy -m group:acct-admin:rcma

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal/nobody
-m group:acct-admin:rcDnfmaug

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal/root
-m group:acct-admin:rcDnfmaug

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal/daemon
-m group:acct-admin:rcDnfmaug

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal/sys -m group:acct-admin:rcDnfmaug

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal/bin -m group:acct-admin:rcDnfmaug

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal/uucp
-m group:acct-admin:rcDnfmaug

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal/who -m group:acct-admin:rcDnfmaug

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal/mail
-m group:acct-admin:rcDnfmaug

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal/tcb -m group:acct-admin:rcDnfmaug

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal/dce-ptgt
-m group:acct-admin:rcDnfmaug

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 principal/dce-rgy
-m group:acct-admin:rcDnfmaug

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group/none -m group:acct-admin:rctDnfmM

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group/system -m group:acct-admin:rctDnfmM

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group/daemon -m group:acct-admin:rctDnfmM

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group/uucp -m group:acct-admin:rctDnfmM

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group/bin -m group:acct-admin:rctDnfmM

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group/kmem -m group:acct-admin:rctDnfmM

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group/mail -m group:acct-admin:rctDnfmM

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group/tty -m group:acct-admin:rctDnfmM

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 group/tcb -m group:acct-admin:rctDnfmM

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 org/none -m group:acct-admin:rctDnfmM

acl_edit -addr cedd0ffc-c64a-11d0-b387-10005ab169d0@ncacn_ip_tcp:9.130.79.118 replist -m user:hosts/dcecell21/self:imI
```

```
acl_edit /.:/subsys/dce/sec -m user:hosts/dcecell21/self:rwdtcia

acl_edit /.:/subsys/dce/sec -io -m user:hosts/dcecell21/self:rwdtc

acl_edit /.:/subsys/dce/sec -ic -m user:hosts/dcecell21/self:rwdtci

acl_edit -e /.:/sec -m user:hosts/dcecell21/self:rwdtc

acl_edit -e /.:/hosts/DCEDRBLD/config/epmap -m user:hosts/DCEDRBLD/cds-server:clidsxt


EUVB00085I Step 6: Starting DTS daemon.

EUVB00015I Starting DTS daemon.

EUVB00014I Step 7: Configuring DTS daemon as local server.


Notice:  Option EUVBDTS .2 selected.
EUVB00003I DTS configuration initiated at Tue May  6 16:18:38 1997.

rgy_edit -up
Current site is: registry server at /.../dcecell21.endicott.ibm.com.
domain group
Domain changed to: group
member subsys/dce/dts-servers -a hosts/DCEDRBLD/self

EUVB00016I Stopping DCE daemon.
rm /opt/dcelocal/var/security/creds/dcecred_ffffffff
rm /opt/dcelocal/var/security/creds/dcecred_ffffffff.data
EUVB00015I Starting DCE daemon.

dtscp create type server

dtscp set courier role noncourier

dtscp enable

EUVB00910I Initial Cell Directory Server configuration is successful.

Notice:  DCECONF ended at Tue May  6 16:20:20 1997.
```

After Deconfiguring a New Cell with secd and cdsd on Different Hosts

For an example DCECONF log file after successfully deconfiguring a new cell with **secd** on a machine other than the z/OS host and **cdsd** on the z/OS host, see “After Deconfiguring a New Cell with secd and cdsd” on page 101.

After Configuring an Additional cdsd on a z/OS Host

The following is an example DCECONF log file after successfully configuring an additional **cdsd** on the z/OS host after configuring the host as a DCE client.

```
Notice:  DCECONF started at Tue May  6 14:00:09 1997.

Notice:  Option EUVBMAIN.1 selected.

Notice:  Option EUVBSERV.6 selected.
EUVB00094I Additional CDSD configuration initiated at Tue May  6 14:00:31 1997.

Notice: Panel Data:
        <cellname>      = !dcecell21.endicott.ibm.com!
      <hostname>      = !DCEDRBLD!
      <cdsd ipname>   = !dcecell21.endicott.ibm.com!
      <cdsd ipaddr>   = !!
```

```
      <clearinghouse> = !DCEDRBLD_ch!
      <dirlist>       = !!

EUVB00017I Login for cell_admin at Tue May  6 14:00:36 1997.
dce_login cell_admin
EUVS24588I Attention - change current password.

EUVS24577I Login successful.


domain principal
add hosts/DCEDRBLD/cds-server
domain account
add hosts/DCEDRBLD/cds-server -g subsys/dce/cds-server -o none -pw XXXXXXXX -mp XXXXXXXX
ktadd -p hosts/DCEDRBLD/cds-server -pw XXXXXXXX
ktadd -p hosts/DCEDRBLD/cds-server -a -r
rgy_edit -up

cdscp dump clerk cache

rpccp export -i 4ea31de8-9a94-11c9-bb60-08002b0f79aa,0003.0000 -b ncadg_ip_udp: -o faf2e540-58b8-11ca-a04a-08002b12a70d
-s dce /.:/hosts/DCEDRBLD/cds-server

acl_edit -e /.:/hosts/DCEDRBLD/cds-server -m user:hosts/DCEDRBLD/self:rwt

acl_edit -e /.:/hosts/DCEDRBLD/config/epmap -m user:hosts/DCEDRBLD/cds-server:clidsxt

EUVB00015I Starting CDS daemon.
cdscp create clearinghouse /.:/DCEDRBLD_ch

cdscp set dir /.: to skulk

acl_edit -e /.:/DCEDRBLD_ch -s unauthenticated:rt group:subsys/dce/cds-admin:rwcdt group:subsys/dce/cds-server:rwcdt
any_other:rt

acl_edit /.:/DCEDRBLD_ch -s unauthenticated:rt group:subsys/dce/cds-admin:rwcdt group:subsys/dce/cds-server:rwcdt
any_other:rt

EUVB00911I Additional Cell Directory Server configuration is successful.

Notice:  DCECONF ended at Tue May  6 14:04:02 1997.
-------------------------------------------------------------------------------------------------------------------------
```

After Deconfiguring an Additional cdsd on a z/OS Host

The following is an example DCECONF log file after successfully deconfiguring an additional **cdsd** on the z/OS host. The host was first configured as a DCE client.

```
Notice:  DCECONF started at Tue May  6 14:04:08 1997.

Notice:  Option EUVBMAIN.2 selected.

Notice:  Option EUVBDCS .4 selected.
EUVB00017I Login for cell_admin at Tue May  6 14:05:04 1997.
dce_login cell_admin
EUVS24588I Attention - change current password.

EUVS24577I Login successful.


EUVB00100I Deconfiguration of CDSD has started.
cdscp set dir /.: to skulk

cdscp show object /.:/*

cdscp
set cdscp confidence high

delete clearinghouse /.../dcecell21.endicott.ibm.com/DCEDRBLD_ch
```

```
cdscp set dir /.: to skulk

EUVB00016I Stopping CDS daemon.
cdscp delete obj /.:/hosts/DCEDRBLD/cds-server

rgy_edit -v -up -p hosts/DCEDRBLD/cds-server

rgy_edit -up

rgy_edit -p -up
Current site is: registry server at /.../dcecell21.endicott.ibm.com.
ktdelete -p hosts/DCEDRBLD/cds-server -v 1
ktdelete -p hosts/DCEDRBLD/cds-server -v 2
delete hosts/DCEDRBLD/cds-server
quit
Exiting rgy_edit.

rm /opt/dcelocal/var/directory/cds/adm
rm /opt/dcelocal/var/directory/cds/cds_files
rm /opt/dcelocal/var/directory/cds/server_mgmt_acl_v1.dat
EUVB00903I This machine has been successfully deconfigured.

Notice:  DCECONF ended at Tue May  6 14:08:22 1997.
```

After Reconfiguring the DTS Daemon

The following is an example DCECONF log file after successfully reconfiguring the DTS daemon as a DTS clerk on a z/OS host.

```
Notice:  Option EUVBMAIN.5 selected.

Notice:  Option EUVBDTS .1 selected.
EUVB00003I DTS configuration initiated at Thu Jan 11 18:14:33 1996.

EUVB00016I Stopping DTS daemon.

rm /opt/dcelocal/var/adm/time/mgt_acl
rm /opt/dcelocal/var/adm/time/dtsconfg

rgy_edit -up
Current site is: registry server at /.../testcell/subsys/dce/sec/master.
domain group
Domain changed to: group
member subsys/dce/dts-servers -r hosts/DCEDRBLD/self

EUVB00015I Starting DTS daemon.

dtscp create type clerk

dtscp enable

EUVB00902I DTS daemon is successfully reconfigured.
```

After Configuring the Global Directory Agent

The following is an example DCECONF log file after successfully configuring the GDA daemon on a z/OS host.

```
Notice:  DCECONF started at Fri Jun  6 14:58:54 1997.

Notice:  Option EUVBMAIN.1 selected.

Notice:  Option EUVBSERV.7 selected.
EUVB00095I GDAD configuration initiated at Fri Jun  6 14:59:06 1997.

Notice: Panel Data:
        <cellname>         = !dcecell14.endicott.ibm.com!
        <hostname>         = !DCECDS3!
        <bind conduit>     = !Y!
        <ldap conduit>     = !Y!

Notice: Panel Data:
        <RESOLVER_CONFIG>   = !//'SHR.TCPIP32.DATA'!
        <LDAP_SERVER>       = !dcecell26!
        <LDAP_AUTH_DN>      = !cn=smithj,o=IBM,c=US!

EUVB00017I Login for cell_admin at Fri Jun  6 14:59:12 1997.
dce_login cell_admin
EUVS24588I Attention - change current password.
EUVS24577I Login successful.

domain principal
add hosts/DCECDS3/gda
domain account
add hosts/DCECDS3/gda -g subsys/dce/cds-server -o none -pw XXXXXXXX -mp XXXXXXXX
rgy_edit -up

dcecp -c registry verify

ktadd -p hosts/DCECDS3/gda -pw XXXXXXXX
ktadd -p hosts/DCECDS3/gda -a -r
rgy_edit -up

acl_edit -addr 9d914f2a-b5fc-11d0-9a68-08005a191a6c@ncacn_ip_tcp:9.130.44.50 principal/hosts/DCECDS3/gda
-m group:acct-admin:rcDnfmaug
-m group:subsys/dce/cds-admin:rcDnfmaug

rpccp export -i 000cf72e-0688-1acb-97ad-08002b12b8f8,0001.0000 -b ncadg_ip_udp:
-o fa620458-924f-11cc-840e-08002b1c8a62 -s dce /.:/hosts/DCECDS3/cds-gda

acl_edit -e /.:/hosts/DCECDS3/cds-gda -m user:hosts/DCECDS3/self:rwt

EUVB00015I Starting GDA daemon.
EUVB00912I Global Directory Agent configuration is successful.

Notice:  DCECONF ended at Fri Jun  6 15:07:24 1997.
```

After Deconfiguring the Global Directory Agent

The following is an example DCECONF log file after successfully deconfiguring the GDA daemon on a z/OS host.

```
Notice:  DCECONF started at Fri Jun  6 14:57:34 1997.

Notice:  Option EUVBMAIN.2 selected.

Notice:  Option EUVBDCS .5 selected.
EUVB00101I Deconfiguration of GDAD has started.
EUVB00017I Login for cell_admin at Fri Jun  6 14:57:45 1997.
dce_login cell_admin
EUVS24588I Attention - change current password.
EUVS24577I Login successful.

EUVB00016I Stopping GDA daemon.
EUVB00034E Error occurs while issuing kernel request. DCE kernel return code: 302.
rpccp unexport -i 000cf72e-0688-1acb-97ad-08002b12b8f8,0001.0000 -o fa620458-924f-11cc-840e-08002b1c8a62 -s
dce /.:/hosts/DCECDS3/cds-gda

cdscp delete obj /.:/hosts/DCECDS3/cds-gda

rgy_edit -v -up -p hosts/DCECDS3/gda

rgy_edit -up

rgy_edit -p -up
Current site is: registry server at /.../dcecell14.endicott.ibm.com/subsys/dce/sec/master.
ktdelete -p hosts/DCECDS3/gda -v 1
ktdelete -p hosts/DCECDS3/gda -v 2
delete hosts/DCECDS3/gda
quit
Exiting rgy_edit.

rm /opt/dcelocal/var/directory/cds/gda_mgmt_acl_v1.dat
rm /opt/dcelocal/etc/gda_id
EUVB00903I This machine has been successfully deconfigured.

Notice:  DCECONF ended at Fri Jun  6 14:58:50 1997.
--------------------------------------------------------------------------------------------------------------------------
```

Appendix C. z/OS DCE Directories and Files

This appendix lists the important z/OS DCE files and subdirectories in the **/opt/dcelocal** and the **/usr/lpp/dce** directories. The tables indicate whether the file (or directory) was created by the installation procedure, by the configuration program (DCECONF), or by the z/OS DCE daemons.

Directories and Files in /opt/dcelocal

Table 8 lists the directories in **/opt/dcelocal** and a brief description of each. Table 9 on page 114 lists the files in **/opt/dcelocal**. The pathnames are relative to **/opt/dcelocal**.

Table 8 (Page 1 of 2). z/OS DCE Directories in /opt/dcelocal

Name	Created by	Description
bin	Installation	Contains link to /bin script files
dcecp	Installation	Contains links to dcecp script files
etc/audit	Installation	Contains audit-related working files
etc/security	Installation	Contains security-related working files
etc/zoneinfo	Installation	Contains links to the time zone files
home	Installation	Contains the home directories of the z/OS DCE daemons (see next entries)
home/auditd	Installation	Home directory of the Audit daemon
home/cdsadv	Installation	Home directory of the CDS Advertiser
home/cdsclerk	Installation	Home directory of the CDS Clerk
home/cdsd	Installation	Home directory of the CDS daemon
home/dced	Installation	Home directory of the DCE daemon
home/dcekern	Installation	Home directory of DCEKERN
home/dts_null_provider	Installation	Home directory of the Null Time Provider
home/dtsd	Installation	Home directory of the DTS daemon
home/gdad	Installation	Home directory of the GDA daemon
home/pwdmgmt	Installation	Home directory of the Password Management daemon
home/secd	Installation	Home directory of the Security daemon
security	Installation	Contains security files
svc	Installation	Serviceability subdirectory of DCE
tcl	Installation	Contains links to Tcl script files
var/security/creds	Installation	Contains the credentials cache files of users
var/adm/rpc	Installation	Contains working files
var/adm/time	Installation	Contains working files
var/audit/admin	Installation	Contains working files
var/audit/client	Installation	Contains working files
var/directory/cds	Installation	Contains CDS database files
var/directory/cds/adm	Installation	Contains working files
var/directory/cds/adm/gdad	Installation	Contains working files

Table 8 (Page 2 of 2). z/OS DCE Directories in /opt/dcelocal

Name	Created by	Description
var/security/preauth	Installation	Contains working files

Table 9 (Page 1 of 2). z/OS DCE Files in /opt/dcelocal

File or Directory	Created by
dce_cf.db	DCECONF
etc/cds.conf	DCECONF
etc/cds_attributes	Installation
etc/cds_globalnames	Installation
etc/cdscache.shmid	Daemon
etc/cdscp.bpt	Installation
etc/dtscp.bpt	Installation
etc/ether_addr	Installation
etc/euvpdcf	Installation
etc/EXPTVAR	Installation
etc/gda_id	Daemon
etc/IMPTVAR	Installation
etc/rpc_interfaces	DCE administrator
etc/security/pe_site	DCECONF
etc/xoischema	Installation
var/adm/directory/cds/cds_cache.version	Daemon
var/adm/directory/cds/cds_cache.0000000001	Daemon
var/adm/directory/cds/cds_clerk	Daemon
var/adm/directory/cds/cdsAdver	Daemon
var/adm/directory/cds/clerk_mgmt_acl_v1.dat	Daemon
var/adm/time/dts_shared_memory_id	Daemon
var/adm/time/dtsconfg	Daemon
var/adm/time/dtsd.acl	Daemon
var/adm/time/dtsd.binding	Daemon
var/dced/cell_aliases	Daemon
var/dced/cell_name	Daemon
var/dced/host_name	Daemon
var/dced/objectuuid.txt	Daemon
var/dced/post_processors	Daemon
var/dced/Acl.db	Daemon
var/dced/Ep.db	Daemon
var/dced/Hostdata.db	Daemon
var/dced/Keytab.db	Daemon
var/dced/Srvrconf.db	Daemon
var/dced/Srvrexec.db	Daemon

Table 9 (Page 2 of 2). z/OS DCE Files in /opt/dcelocal

File or Directory	Created by
var/dced/Xattrschema.db	Daemon
var/directory/cds/cellname#machinename_ch.checkpoint0000000001	Daemon
var/directory/cds/cellname#machinename_ch.tlog0000000001	Daemon
var/directory/cds/cellname#machinename_ch.version0000000001	Daemon
var/directory/cds/cds_files	Daemon
var/directory/cds/gda_mgmt_acl_v1.dat	Daemon
var/directory/cds/server_mgmt_acl_v1.dat	Daemon
var/security/sec_clientd.binding	Daemon
var/security/creds/dcecred_ffffffff	Daemon
var/security/creds/dcecred_ffffffff.data	Daemon
var/security/creds/dcecred_ffffffff.nc	Daemon

Note: Installation files are links to corresponding files on **/usr/lpp/dce**.

Files and Directories in /usr/lpp/dce

Table 10 lists the directories and the file lib/libdce.a in the /usr/lpp/dce directory. It also gives a short description of the directories. The pathnames are relative to /usr/lpp/dce.

Table 10. z/OS DCE Files and Directories in /usr/lpp/dce

File or Directory	Created by	Description
bin	Installation	Contains the administration and user commands.
examples	Installation	Contains the example envar file and applications.
lib/libdce.a	Installation	DCE library file
lib/nls/msg/En_US.IBM-1047	Installation	Contains DCE catalog files.
share/include	Installation	Contains the DCE header files.
dcecp	Installation	Contains **dcecp** script files.

Appendix D. Kerberos Configuration Files

The default Kerberos configuration file is **krb5/krb5.conf**. For compatibility with DCE, the Kerberos runtime also supports the **krb5/krb.conf** configuration file. Entries in **krb5/krb5.conf** override entries in **krb5/krb.conf**. The DCE configuration program creates and maintains the **krb5/krb.conf** file. The user is responsible for creating and maintaining the **krb5/krb5.conf** file if it is needed.

The krb5/krb.conf File

The **krb5/krb.conf** configuration file consists of two or more lines. The first line contains a single token which specifies the name of the local Kerberos realm. All lines after the first line contain two tokens: a realm name and the name of the host containing the Key Distribution Center (KDC) for the realm.

For example, suppose we have two realms: **dceprod.endicott.ibm.com** and **ends390.endicott.ibm.com**. Then the **krb5/krb.conf** file for realm **dceprod.endicott.ibm.com** might look like the following:

```
dceprod.endicott.ibm.com
dceprod.endicott.ibm.com gandalf.endicott.ibm.com
ends390.endicott.ibm.com allanon.endicott.ibm.com
```

This says that the KDC for realm **dceprod.endicott.ibm.com** is located on **gandalf.endicott.ibm.com** while the KDC for realm **ends390.endicott.ibm.com** is located on **allanon.endicott.ibm.com**.

The krb5/krb5.conf File

The **krb5/krb5.conf** configuration file is much more powerful than the **krb5/krb.conf** configuration file. This file is divided into sections. Each section contains one or more name-value pairs with one pair per line. The name and value are separated by an equal sign. The value may be either a character string or a group of name-value pairs. If a character string is specified, it consists of all characters starting with the first non-blank character following the equal sign and continuing until the last non-blank character on the line. The maximum length of a single line in the configuration file is 2046 bytes. Comment lines are denoted by a semi-colon in the first position of the line and blank lines are ignored.

A section name is enclosed in brackets and must appear on a line by itself. Group values are enclosed in braces with one group per line. The opening brace for a group may follow the equal sign or may be on a line by itself. The closing brace must be on a line by itself so that it won't be treated as part of the value string.

The default configuration file is **krb5/krb5.conf**. This can be changed by defining the KRB5_CONFIG environment variable. Multiple configuration files can be specified for the KRB5_CONFIG variable by separating the names with colons. If a named entry can have just one value, then the first occurrence of the name is used. Otherwise, all of the entries for the same name are grouped together in the order they are encountered.

The configuration file must be in code page 1047. To support other code pages, the following trigraphs can be used:

- ??(= left bracket
- ??) = right bracket
- ??< = left brace
- ??> = right brace

The following sections are supported:

- **[libdefaults]**

  This section provides defaults for the Kerberos runtime routines.

- **[realms]**

  This section defines each of the realms which can be reached from the local realm. For each realm, one or more KDC hosts must be defined. If this section is not defined, the realm information is obtained from the **/krb5/krb.conf** configuration file.

- **[domain_realm]**

  This section defines the mapping between DNS names and Kerberos realm names.

- **[capath]**

  This section defines connection paths between realms. This section is not required if the Kerberos realms are arranged in a hierarchical configuration. Even in a hierarchical configuration, this section should be defined if there are direct connections between realms.

Here are the details of the sections:

- **[libdefaults]**

  clockskew — Specifies the maximum clock difference in seconds. The default is 300 (5 minutes). A Kerberos request is rejected if the difference between the server time and the request timestamp exceeds the clock skew value.

  kdc_req_checksum_type — Specifies the default checksum type for a KDC request as follows:

  - crc32
  - rsa-md4.
  - rsa-md4-des
  - descbc
  - rsa-md5
  - rsa-md5-des

  The checksum type must be rsa-md4 to interoperate with earlier levels of the DCE security server. The default is rsa-md5.

  ap_req_checksum_type — Specifies the default checksum type for an application request. The checksum type must be rsa-md4 to interoperate with earlier levels of the DCE security server. The default is rsa-md5.

  safe_checksum_type — Specifies the default checksum type for a safe request. The default is rsa-md5-des.

  kdc_default_options — Specifies the default options used when requesting an initial ticket from the KDC as follows:

  - 0x00000010 = KDC_OPT_RENEWABLE_OK (DCE default)
  - 0x10000000 = KDC_OPT_PROXIABLE
  - 0x40000000 = KDC_OPT_FORWARDABLE

  Multiple options may be specified by ORing the values together. The default is 0x00000010.

  kdc_timesync — Specifies whether or not the local time is to be synchronized with the KDC time. Specify 1 to synchronize the time and 0 to not synchronize the time. Do not specify 1 if the local system is running a time daemon

which synchronizes the clock (for example, the dtsd daemon provided with DCE). The default is 0.

ccache_type
: Specifies the format of the credentials cache file as an integer value between 1 and 4. Specify type 2 to share credentials cache files with DCE. The default is 2.

default_tkt_enctypes
: Specifies one or more initial ticket encryption types separated by commas. The first encryption type specified is used when generating random keys, so it must be an encryption type supported by all KDC servers that might be accessed by applications on the local system. The following encryption types are supported:

  – des-cbc-crc
  – des-cbc-md5
  – des-cbc-raw

  The first encryption type must be des-cbc-crc to interoperate with earlier levels of the DCE security server. The default is des-cbc-crc,des-cbc-md5.

default_tgs_enctypes
: Specifies one or more ticket-granting ticket encryption types separated by commas. The first encryption type specified is used when generating random keys, so it must be an encryption type supported by all KDC servers that might be accessed by applications on the local system. The first encryption type must be des-cbc-crc to interoperate with earlier levels of the DCE security server. The default is des-cbc-crc,des-cbc-md5.

rsa-md4-des-compat
: Specifies whether to generate MD4 DES checksums in compatibility mode (1) or in strict mode (0). You must specify compatibility mode to interoperate with earlier levels of Kerberos V5.

rsa-md5-des-compat
: Specifies whether to generate MD5 DES checksums in compatibility mode (1) or in strict mode (0). You must specify compatibility mode to interoperate with earlier levels of Kerberos V5.

default_keytab_name
: Specifies the default key table name. The default is **/krb5/v5srvtab**.

default_realm
: Specifies the default realm. If not specified, the default realm name is obtained from the **/krb5/krb.conf** file.

- **[realms]**

  [realm]
  : The realm value is a Kerberos realm name. The value is a group definition which defines the KDC servers for the realm. Each realm that can be contacted by applications on the local system must have an entry in the [realms] section of the configuration file. The group entry consists of one or more occurrences of the **kdc** name. The value for each **kdc** name entry is the host name and the port, separated by a colon. If the port is omitted, it defaults to 88.

- **[domain_realm]**

  hostname
  : The hostname value is a DNS host name. The value is the name of the Kerberos realm which contains the specified host system.

  .suffix
  : The .suffix value is the domain portion of a DNS host name. The value is the name of the Kerberos realm which contains host systems in the specified domain. A specific host name definition takes precedence over the domain specification.

- **[capath]**

  [realm] Each realm value is a Kerberos realm name and represents the starting point for a request. If the configuration file is not shared between systems, then the only realm that needs to be specified is the local realm. Otherwise, there needs to be a realm definition for each system sharing the configuration file. The value is a group definition which defines the target realms. If multiple hops are required to reach the target realm, there are multiple entries defining each of the hops from the local realm to the target realm. If there is a direct connection between the local realm and the target realm, specify the hop as a period.

Sample krb5/krb5.conf Configuration File

```
; Numeric values can be specified as follows:
;   ddddddd = decimal number
;   0ddddddd = octal number
;   0xddddd = hexadecimal number

; Checksum types
;   crc32
;   rsa-md4 (required for DCE interoperability)
;   rsa-md4-des
;   descbc
;   rsa-md5 (Kerberos V5 default)
;   rsa-md5-des

; Encryption types
;   des-cbc-crc (required for DCE interoperability)
;   des-cbc-md5 (Kerberos V5 default)
;   des-cbc-raw

; KDC option codes
;   0x00000010 = KDC_OPT_RENEWABLE_OK (DCE default)
;   0x10000000 = KDC_OPT_PROXIABLE
;   0x40000000 = KDC_OPT_FORWARDABLE

[libdefaults]

; Maximum clock skew in seconds
;   DCE always uses 5 minutes for the clock skew
clockskew = 300

; Checksum used for KDC requests
kdc_req_checksum_type = rsa-md4

; Checksum used for application requests
ap_req_checksum_type = rsa-md4

; Checksum used for safe requests
safe_checksum_type = rsa-md5-des

; Kerberos V5 Beta 1 through Beta 5 computed the checksum
; incorrectly for rsa-md4-des and rsa-md5-des.  Setting the
; compatibility mode to 1 will cause the old algorithm to be used
```

```
; when generating a checksum.  Set the compatibility mode to 0
; to use the new algorithm.
rsa_md4_des_compat = 1
rsa_md5_des_compat = 1

; Default KDC options
kdc_default_options = 0x00000010

; Synchronize Kerberos library time with KDC server
kdc_timesync = 0

; Credentials cache file version
;     Specify ccache_type=2 to share credentials cache files
;     with older levels of DCE
ccache_type = 2

; Ticket encryption types (listed in priority order)
;     Must include des-cbc-crc for interoperability with DCE
default_tkt_enctypes = des-cbc-crc,des-cbc-md5
default_tgs_enctypes = des-cbc-crc,des-cbc-md5

;  The default_realm value will be obtained from the /krb5/krb.conf
;  file if it is not specified here.
default_realm = dcesec4.endicott.ibm.com

;  The default key table name.  The KRB5_KTNAME environment variable
;  will override this specification.
default_keytab_name = FILE:/krb5/v5srvtab

[realms]
;  Realm definitions are not used in the DCE environment but are
;  required in the stand-alone Kerberos environment.  The KDC relation
;  is repeated for each KDC in the realm.  The realm definitions will
;  be obtained from the /krb5/krb.conf file if they are not specified
;  here.
dcesec4.endicott.ibm.com = {
    kdc = dcesec4.endicott.ibm.com:88
    kdc = dcecell5.endicott.ibm.com:88
}

ends390.endicott.ibm.com = {
    kdc = allanon.endicott.ibm.com:88
}

[domain_realm]
;  Convert host names to realm names.  Individual host names may be
;  specified.  Domain suffixes may be specified with a leading period
;  and will apply to all host names ending in that suffix.
dcesec4.endicott.ibm.com = dcesec4.endicott.ibm.com
dcecell5.endicott.ibm.com = dcesec4.endicott.ibm.com
dcetape.endicott.ibm.com = dceprod.endicott.ibm.com
dcedfs.endicott.ibm.com = dceprod.endicott.ibm.com
.endicott.ibm.com = ends390.endicott.ibm.com

[capaths]
;  Configurable authentication paths which define the trust relationships
;  between client and servers.  Each entry represents a client realm
;  and consists of the trust relationships for each server which can
```

```
;  be accessed from that realm.  A server may be listed multiple times
;  if there are multiple trust relationships involved.  Specify '.' for
;  a direct connection.
;
;  In this example, we have the following trust connections:
;      dcesec4 is connected to ends390
;      dceprod is connected to ends390
;      pokgate is connected to ends390
;      pokfvt is connected to pokgate
dcesec4.endicott.ibm.com = {
    dceprod.endicott.ibm.com = ends390.endicott.ibm.com
    pokgate.pok.ibm.com = ends390.endicott.ibm.com
    pokfvt.pok.ibm.com = ends390.endicott.ibm.com
    pokfvt.pok.ibm.com = pokgate.pok.ibm.com
    ends390.endicott.ibm.com = .
}
```

Appendix E. 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.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

Any references in this information to non-IBM 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 Corporation
Mail Station P300
522 South Road
Poughkeepsie, NY 12601-5400
U.S.A

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

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

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

This product contains code licensed from RSA Data Security Incorporated.

Trademarks

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

BookManager	CICS	CICS/ESA
DATABASE 2	DB2	IBM
IBMLink	IMS	IMS/ESA
Library Reader	OS/390	RACF
Resource Link	SecureWay	System/390
VTAM	z/OS	zSeries

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.

Glossary

This glossary defines technical terms and abbreviations used in z/OS DCE documentation. If you do not find the term you are looking for, refer to the index of the appropriate z/OS DCE manual or view the *IBM Glossary of Computing Terms*, located at:

http://www.ibm.com/ibm/terminology

This glossary includes terms and definitions from:

- *IBM Dictionary of Computing*, SC20-1699.
- *Information Technology—Portable Operating System Interface (POSIX),* from the POSIX series of standards for applications and user interfaces to open systems, copyrighted by the Institute of Electrical and Electronics Engineers (IEEE).
- *American National Standard Dictionary for Information Systems,* ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies may be purchased from the American National Standards Institute, 11 West 42nd Street, New York, New York 10036. Definitions are identified by the symbol (A) after the definition.
- *Information Technology Vocabulary,* developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1.SC1).
- *CCITT Sixth Plenary Assembly Orange Book, Terms and Definitions* and working documents published by the International Telecommunication Union, Geneva, 1978.
- Open Software Foundation (OSF).

The following abbreviations indicate terms that are related to a particular DCE service:

CDS	Cell Directory Service
CICS/ESA®	Customer Information Control System/ESA
DTS	Distributed Time Service
GDS	Global Directory Service
IMS/ESA®	Information Management System/ESA
RPC	Remote Procedure Call
Security	Security Service
Threads	Threads Service
XDS	X/Open Directory Services
XOM	X/Open OSI-Abstract-Data Manipulation

A

absolute time. A point on a time scale.

access control list (ACL). (1) GDS: Specifies the users with their access rights to an object. (2) Security: Data that controls access to a protected object. An ACL specifies the privilege attributes needed to access the object and the permissions that may be granted, to the protected object, to principals that possess such privilege attributes.

account. Data in the Registry database that allows a principal to log in. An account is a registry object that relates to a principal.

ACL. Access control list.

adapter. Synonym for *attachment facility*.

address. An unambiguous name, label, or number that identifies the location of a particular entity or service. See *presentation address*.

attachment facility. Application Support Server: Refers to the CICS® adapter and the IMS® adapter. Synonymous with *adapter*.

attribute. (1) RPC: An Interface Definition Language (IDL) or attribute configuration file (ACF) that conveys information about an interface, type, field, parameter, or operation. (2) DTS: A qualifier used with DTS commands. DTS has four attribute categories: characteristics, counters, identifiers, and status. (3) XDS: Information of a particular type concerning an object and appearing in an entry that describes the object in the directory information base (DIB). It denotes the attribute's type and a sequence of one or more attribute values, each accompanied by an integer denoting the value's syntax.

attribute syntax. GDS: A definition of the set of values that an attribute may assume. Attribute syntax includes the data type, in ASN.1, and usually one or more matching rules by which values may be compared.

attribute type. (1) XDS: The component of an attribute that indicates the type of information given by that attribute. Because it is an object identifier, it is unique among other attribute types. (2) XOM: Any of various categories into which the client dynamically groups values on the basis of their semantics. It is an integer unique only within the package.

attribute value. XDS, XOM: A particular instance of the type of information indicated by an attribute type.

authentication. In computer security, a method used to verify the identity of a principal.

authorization. (1) The determination of a principal's permissions with respect to a protected object. (2) The approval of a permission sought by a principal with respect to a protected object.

B

binding. RPC: A relationship between a client and a server involved in a remote procedure call.

binding handle. RPC: A reference to a binding. See *binding information*.

binding information. RPC: Information about one or more potential bindings, including an RPC protocol sequence, a network address, an endpoint, at least one transfer syntax, and an RPC protocol version number. See *binding*. See also *endpoint*, *network address*, *RPC protocol*, *RPC protocol sequence*, and *transfer syntax*.

broadcast. A notification sent to all members within an arbitrary grouping such as nodes in a network or threads in a process. See also *signal*.

C

cache. (1) CDS: The information that a CDS clerk stores locally to optimize name lookups. The cache contains attribute values resulting from previous lookups, as well as information about other clearinghouses and namespaces. (2) Security: Contains the credentials of a principal after the DCE login. (3) GDS: See *DUA cache*.

CDS. Cell Directory Service.

CDS clerk. The software that provides an interface between client applications and CDS servers.

CDS control program (CDSCP). A command interface that CDS administrators use to control CDS servers and clerks and manage the name space and its contents. See also *manager*.

CDSCP. CDS control program.

cell. The basic unit of operation in the distributed computing environment. A cell is a group of users, systems, and resources that are grouped around a common purpose and that share common DCE services.

Cell Directory Service (CDS). A DCE component. A distributed replicated database service that stores names and attributes of resources located in a cell. CDS manages a database of information about the resources in a group of machines called a DCE cell.

CICS. Customer Information Control System.

class. A category into which objects are placed on the basis of their purpose and internal structure.

clerk. (1) DTS: A software component that synchronizes the clock for its client system by requesting time values from servers, calculating a new time from the values, and supplying the computed time to client applications. (2) CDS: A software component that receives CDS requests from a client application, ascertains an appropriate CDS server to process the requests, and returns the results of the requests to the client application.

client. A computer or process that accesses the data, services, or resources of another computer or process on the network. Contrast with *server*.

client context. RPC: The state within an RPC server generated by a set of remote procedures and maintained across a series of calls for a particular client. See *context handle*. See also *manager*.

client stub. RPC: The surrogate code for an RPC interface that is linked with and called by the client application code. In addition to general operations such as marshalling data, a client stub calls the RPC runtime to perform remote procedure calls and, optionally, to manage bindings. See *server stub*.

client/server model. A form of computing where one system, the client, requests something, and another system, the server, responds.

clock. The combined hardware interrupt timer and software register that maintains the system time.

clock adjustment. DTS: The DTS process of changing the system clock time by changing the incremental value that is added to the clock's software register for a specified duration.

code page. (1) A table showing codes assigned to character sets. (2) An assignment of graphic characters and control function meanings to all code points. (3) Arrays of code points representing characters that establish numeric order of characters. [OSF] (4) A particular assignment of hexadecimal identifiers to graphic elements. (5) Synonymous with code set. (6) See also *code point, extended character*.

context handle. RPC: A reference to state (client context) maintained across remote procedure calls by a server on behalf of a client. See *client context*.

control task. The parent process of the DCE daemons in the DCEKERN address space. All requests to start or stop DCE daemons are handled by the Control Task.

copy. GDS, XDS: Either a copy of an entry stored in other DSAs through bilateral agreement or a locally and dynamically stored copy of an entry resulting from a request (a cache copy).

courier. DTS: A local server that requests a time value from a randomly selected global server. The time value returned is used for synchronization.

credentials. Security: A general term for privilege attribute data that has been certified by a trusted privilege certification authority.

cross-linking information. In order for z/OS DCE to provide RACF-DCE interoperability and single sign-on to DCE, DCE provides utilities (see **mvsexpt** and **mvsimpt**) to incorporate into RACF the information that associates a z/OS-RACF user ID with a DCE principal's identifying information and the DCE principal's UUID with the corresponding z/OS-RACF user ID. The information is placed in a RACF DCE segment and the RACF general resource class, DCEUUIDS. This is called **cross-linking information** and is what allows interoperability and single sign-on to work. See also *interoperability* and *single sign-on*.

Customer Information Control System (CICS). An IBM licensed program that enables transactions entered at remote terminals to be processed concurrently by user-written application programs. It includes facilities for building, using, and maintaining databases.

D

daemon. (1) A long-lived process that runs unattended to perform continuous or periodic system-wide functions such as network control. Some daemons are triggered automatically to perform their task; others operate periodically. An example is the **cron** daemon, which periodically performs the tasks listed in the **crontab** file. Many standard dictionaries accept the spelling *demon*. (2) A DCE server process.

daemon configuration file. A file containing information on which daemons are configured on the host, which environment variables to set, the parameters to pass to the process, minimum restart interval, and the time-out period.

DCE. Distributed Computing Environment.

DCECONF. program used to configure and start the DCE daemons.

DCEKERN. The address space that contains the DCE daemons.

default element. RPC: An optional profile element that contains a nil interface identifier and object UUID and that specifies a default profile. Each profile can contain only one default element. See *default profile*, *profile*, and *profile element*.

default profile. RPC: A backup profile referred to by the default element in another profile. The NSI import and lookup operations use the default profile, if present, whenever a search based on the current profile fails to find any useful binding information. See *default element* and *profile*.

DFS. Distributed File Service.

directory. (1) A logical unit for storing entries under one name (the directory name) in a CDS namespace. Each physical instance of a directory is called a replica. (2) A collection of open systems that cooperates to hold a logical database of information about a set of objects in the real world.

directory schema. GDS: The set of rules and constraints concerning directory information tree (DIT) structure, object class definitions, attribute types, and syntaxes that characterize the directory information base (DIB).

Directory Service. A DCE component. The Directory Service is a central repository for information about resources in a distributed system. See *Cell Directory Service* and *Global Directory Service*.

distributed computing. A type of computing that allows computers with different hardware and software to be combined on a network, to function as a single computer, and to share the task of processing application programs.

Distributed Computing Environment (DCE). A comprehensive, integrated set of services that supports the development, use, and maintenance of distributed applications. DCE is independent of the operating system and network; it provides interoperability and portability across heterogeneous platforms.

Distributed File Service (DFS). A DCE component. DFS joins the local file systems of several file server machines making the files equally available to all DFS client machines. DFS allows users to access and share files stored on a file server anywhere in the network, without having to consider the physical location of the file. Files are part of a single, global name space, so that a user can be found anywhere in the network by means of the same name.

Distributed Time Service (DTS). A DCE component. It provides a way to synchronize the times on different hosts in a distributed system.

DNS. Domain Name System.

Domain Name System (DNS). A hierarchical scheme for giving meaningful names to hosts in a TCP/IP network.

domain name. A unique network name that is associated with a network's unique address.

drift. DTS: The change in a clock's error rate over a specified period of time.

DTS. Distributed Time Service.

DTS entity. DTS: The server or clerk software on a system.

DUA cache. GDS: The part of the DUA that stores information to optimize name lookups. Each cache contains copies of recently accessed object entries as well as information about DSAs in the directory.

E

element. RPC: Any of the bits of a bit string, the octets of an octet string, or the octets by means of which the characters of a character string are represented.

encrypt. To systematically encode data so that it cannot be read without knowing the coding key.

endpoint. RPC: An address of a specific server instance on a host.

endpoint map. RPC: A database local to a node where local RPC servers register binding information associated with their interface identifiers and object identifiers. The endpoint map is maintained by the endpoint map service of the DCE daemon.

endpoint map service. RPC: A service that maintains a system's endpoint map for local RPC servers. When an RPC client makes a remote procedure call using a partially bound binding handle, the endpoint map service looks up the endpoint of a compatible local server. See *endpoint map*.

entity. (1) CDS: Any manageable element through the CDS namespace. Manageable elements include directories, object entries, servers, replicas, and clerks. The CDS control program (CDSCP) commands are based on directives targeted for specific entities. (2) DTS: See *DTS entity*.

entry. GDS, XDS: The part of the DIB that contains information relating to a single directory object. Each entry consists of directory attributes.

environment variable (ENV). A variable included in the current software environment that is available to any called program that requests it.

exception. (1) An abnormal condition such as an I/O error encountered in processing a data set or a file. (2) One of five types of errors that can occur during a floating-point exception. These are valid operation, overflow, underflow, division by zero, and inexact results. [OSF] (3) Contrast with *interrupt, signal*.

export. (1) RPC: To place the server binding information associated with an RPC interface or a list of object UUIDs or both into an entry in a name service database. (2) To provide access information for an RPC interface. Contrast with *unexport*.

F

filter. An assertion about the presence or value of certain attributes of an entry to limit the scope of a search.

foreign cell. A cell other than the one to which the local machine belongs. A foreign cell and its binding information are stored in either GDS or the Domain Name System (DNS). The act of contacting a foreign cell is called intercell. Contrast with *local cell*.

fully bound binding handle. RPC: A server binding handle that contains a complete server address including an endpoint. Contrast with *partially bound binding handle*.

G

GDS. Global Directory Service.

Global Directory Service (GDS). A DCE component. A distributed replicated directory service that provides a global namespace that connects the local DCE cells into one worldwide hierarchy. DCE users can look up a name outside a local cell with GDS.

global server. DTS: A server that provides its clock value to courier servers on other cells, or to DTS entities that have failed to obtain the specified number of servers locally.

group. (1) RPC: A name service entry that corresponds to one or more RPC servers that offer common RPC interfaces, RPC objects, or both. A group contains the names of the server entries, other groups, or both that are members of the group. See *NSI group attribute*. (2) Security: Data that associates

a named set of principals that can be granted common access rights. See *subject identifier*.

group member. (1) RPC: A name service entry whose name occurs in the group. (2) Security: A principal whose name appears in a security group. See *group*.

H

handle. RPC: An opaque reference to information. See *binding handle*, *context handle*, *interface handle*, *name service handle*, and *thread handle*.

home cell. Synonym for *local cell*.

host ID. Synonym for *network address*.

I

IMS. Information Management System.

inaccuracy. DTS: The bounded uncertainty of a clock value as compared to a standard reference.

Information Management System (IMS). A database and data communication system capable of managing complex databases and networks in virtual storage.

interoperability. The capability to communicate, execute programs, or transfer data among various functional units in a way that requires the user to have little or no knowledge of the unique characteristics of those units.

instance. XOM: An object in the category represented by a class.

interface. RPC: A shared boundary between two or more functional units, defined by functional characteristics, signal characteristics, or other characteristics, as appropriate. The concept includes the specification of the connection of two devices having different functions. See *RPC interface*.

interface definition. RPC: A description of an RPC interface written in the DCE Interface Definition Language (IDL). See *RPC interface*.

interface handle. RPC: A reference in code to an interface specification. See *binding handle* and *interface specification*.

interface identifier. RPC: A string containing the interface Universal Unique Identifier (UUID) and major and minor version numbers of a given RPC interface. See *RPC interface*.

interface specification. RPC: An opaque data structure that is generated by the DCE IDL compiler from an interface definition. It contains identifying and descriptive information about an RPC interface. See *interface definition*, *interface handle*, and *RPC interface*.

interface UUID. RPC: The Universal Unique Identifier (UUID) generated for an RPC interface definition using the UUID generator. See *interface definition* and *RPC interface*.

Internet address. The 32-bit address assigned to hosts in a TCP/IP network.

Internet Protocol (IP). In TCP/IP, a protocol that routes data from its source to its destination in an Internet environment. IP provides the interface from the higher level host-to-host protocols to the local network protocols. Addressing at this level is usually from host to host.

interval. DTS: The combination of a time value and the inaccuracy associated with it; the range of values represented by a combined time and inaccuracy notation. As an example, the interval 08:00.00I00:05:00 (eight o'clock, plus or minus five minutes) contains the time 07:57.00.

IP. Internet Protocol

K

Kerberos. The authentication protocol used to carry out DCE private key authentication. Kerberos was developed at the Massachusetts Institute of Technology.

key. A value used to encrypt and decrypt data.

L

LAN. Local area network.

local. (1) Pertaining to a device directly connected to a system without the use of a communication line. (2) Pertaining to devices that have a direct, physical connection. Contrast with *remote*.

local area network (LAN). A network in which communication is limited to a moderate-sized geographical area (1 to 10 km) such as a single office building, warehouse, or campus, and which does not generally extend across public rights-of-way. A local network depends on a communication medium capable of moderate to high data rate (greater than 1Mbps), and normally operates with a consistently low error rate.

local cell. The cell to which the local machine belongs. Synonymous with *home cell*. Contrast with *foreign cell*.

local server. DTS: A server that synchronizes with its peers and provides its clock value to other servers and clerks in the same network.

M

manager. RPC: A set of remote procedures that implement the operations of an RPC interface and that can be dedicated to a given type of object. See also *object* and *RPC interface*.

mask. (1) A pattern of characters used to control the retention or deletion of portions of another pattern of characters (2) Security: Used to establish maximum permissions that can then be applied to individual ACL entries. (3) GDS: The administration screen interface menus.

master replica. CDS: The first instance of a specific directory in the namespace. After copies of the directory have been made, a different replica can be designated as the master, but only one master replica of a directory can exist at a time. CDS can create, update, and delete object entries and soft links in a master replica.

MODIFY DCEKERN. MODIFY command used to start, stop, and display the status of DCE daemons.

mvsexpt. One of two (the other is **mvsimpt**) utilities used to automate much of the administrator's work in creating the cross-linking information for DCE-RACF interoperability. The **mvsexpt** utility creates the cross-linking information in the RACF database from information in the DCE registry. See also *cross-linking information*, *interoperability*, and *single sign-on*.

mvsimpt. One of two (the other is **mvsexpt**) utilities used to automate much of the administrator's work in creating the cross-linking information for DCE-RACF interoperability. The **mvsimpt** utility creates DCE principals from information obtained from the RACF database. See also *cross-linking information*, *interoperability*, and *single sign-on*.

N

name. GDS, CDS: A construct that singles out a particular (directory) object from all other objects. A name must be unambiguous (denote only one object); however, it need not be unique (be the only name that unambiguously denotes the object).

name service. A central repository of named resources in a distributed system. In DCE, this is the same as Directory Service.

name service handle. RPC: An opaque reference to the context used by the series of next operations called during a specific name service interface (NSI) search or inquiry.

namespace. CDS: A complete set of CDS names that one or more CDS servers look up, manage, and share. These names can include directories, object entries, and soft links.

network. A collection of data processing products connected by communications lines for exchanging information between stations.

network address. An address that identifies a specific host on a network. Synonymous with *host ID*.

Network Data Representation (NDR). RPC: The transfer syntax defined by the Network Computing Architecture. See *transfer syntax*.

network protocol. A communications protocol from the Network Layer of the Open Systems Interconnection (OSI) network architecture, such as the Internet Protocol (IP).

null time provider. The daemon that fetches the time from the hardware clock of the DCE host for DTS.

NSI binding attribute. RPC: An RPC-defined attribute (NSI attribute) of a name service entry; the binding attribute stores binding information for one or more interface identifiers offered by an RPC server and identifies the entry as an RPC server entry. See *binding information* and *NSI object attribute*. See also *server entry*.

NSI group attribute. RPC: An RPC-defined attribute (NSI attribute) of a name service entry that stores the entry names of the members of an RPC group and identifies the entry as an RPC group. See *group*.

NSI object attribute. RPC: An RPC-defined attribute (NSI attribute) of a name service entry that stores the object UUIDs of a set of RPC objects. See *object*.

NSI profile attribute. RPC: An RPC-defined attribute (NSI attribute) of a name service entry that stores a collection of RPC profile elements and identifies the entry as an RPC profile. See *profile*.

NULL. In the C language, a pointer that does not point to a data object.

O

object. (1) A data structure that implements some feature and has an associated set of operations. (2) RPC: For RPC applications, anything that an RPC server defines and identifies to its clients using an object Universal Unique Identifier (UUID). An RPC object is often a physical computing resource such as a

database, directory, device, or processor. Alternatively, an RPC object can be an abstraction that is meaningful to an application, such as a service or the location of a server. See *object UUID*. (3) XDS: Anything in the world of telecommunications and information processing that can be named and for which the directory information base (DIB) contains information. (4) XOM: Any of the complex information objects created, examined, changed, or destroyed by means of the interface.

object entry. CDS: The name of a resource (such as a node, disk, or application) and its associated attributes, as stored by CDS. CDS administrators, client application users, or the client applications themselves can give a resource an object name. CDS supplies some attribute information (such as a creation timestamp) to become part of the object, and the client application may supply more information for CDS to store as other attributes. See *entry*.

object UUID. RPC: The Universal Unique Identifier (UUID) that identifies a particular RPC object. A server specifies a distinct object UUID for each of its RPC objects. To access a particular RPC object, a client uses the object UUID to find the server that offers the object. See *object*.

Open Software Foundation (OSF). A nonprofit research and development organization set up to encourage the development of solutions that allow computers from different vendors to work together in a true open-system computing environment.

operation. (1) GDS: Processing performed within the directory to provide a service, such as a read operation. (2) RPC: The task performed by a routine or procedure that is requested by a remote procedure call.

organization. (1) The third field of a subject identifier. (2) Security: Data that associates a named set of users who can be granted common access rights that are usually associated with administrative policy.

OSF. Open Software Foundation.

P

partially bound binding handle. RPC: A server binding handle that contains an incomplete server address lacking an endpoint. Contrast with *fully bound binding handle*.

password. A secret string of characters shared between a computer system and a user. The user must specify the character string to gain access to the system.

person. See *principal*.

platform. The operating system environment in which a program runs.

presentation address. An unambiguous name that is used to identify a set of presentation service access points. Loosely, it is the network address of an open systems interconnection (OSI) service.

principal. Security: An entity that can communicate securely with another entity. In the DCE, principals are represented as entries in the Registry database and include users, servers, computers, and authentication surrogates.

privacy. RPC: A protection level that encrypts RPC argument values. in secure RPC communications.

profile. RPC: An entry in a name service database that contains a collection of elements from which name service interface (NSI) search operations construct search paths for the database. Each search path is composed of one or more elements that refer to name service entries corresponding to a given RPC interface and, optionally, to an object. See *NSI profile attribute* and *profile element*.

profile element. RPC: A record in an RPC profile that maps an RPC interface identifier to a profile member (a server entry, group, or profile in a name service database). See *profile*. See also *group*, *interface identifier* and *server entry*.

programming interface. The supported method through which customer programs request software services. The programming interface consists of a set of callable services provided with the product.

protocol. A set of semantic and syntactic rules that determines the behavior of functional units in achieving communication.

protocol sequence. Synonym for *RPC protocol sequence*.

R

RACF. Resource Access Control Facility.

read-only replica. (1) CDS: A copy of a CDS directory in which applications cannot make changes. Although applications can look up information (read) from it, they cannot create, change, or delete entries in a read-only replica. Read-only replicas become consistent with other, changeable replicas of the same directory during skulks and routine propagation of updates. (2) Security: A replicated Registry server.

register. (1) RPC: To list an RPC interface with the RPC runtime. (2) To place server-addressing information into the local endpoint map. (3) To insert

authorization and authentication information into binding information. See *endpoint map* and *RPC interface*.

Registry database. Security: A database of security information about principals, groups, organizations, accounts, and security policies.

relative time. A discrete time interval that is usually added to or subtracted from an absolute time. See *absolute time*.

remote. Pertaining to a device, file or system that is accessed by your system through a communications line. Contrast with *local*.

remote procedure. RPC: An application procedure located in a separate address space from calling code. See *remote procedure call*.

remote procedure call. RPC: A client request to a service provider located anywhere in the network.

Remote Procedure Call (RPC). A DCE component. It allows requests from a client program to access a procedure located anywhere in the network.

replica. CDS: A directory in the CDS namespace. The first instance of a directory in the name space is the master replica. See *master replica* and *read-only replica*.

replication. The making of a shadow of a database to be used by another node. Replication can improve availability and load-sharing.

request. A command sent to a server over a connection.

resource. Items such as printers, plotters, data storage, or computer services. Each has a unique identifier associated with it for naming purposes.

Resource Access Control Facility (RACF). An IBM licensed program, that provides for access control by identifying and verifying the users to the system, authorizing access to protected resources, and logging the detected unauthorized access to protected resources.

ROM. Read-only memory.

RPC. Remote Procedure Call.

RPC control program (RPCCP). An interactive administrative facility for managing name service entries and endpoint maps for RPC applications.

RPCCP. RPC control program

RPC interface. A logical group of operations, data types, and constant declarations that serves as a network contract for a client to request a procedure in a server. See also *interface definition* and *operation*.

RPC protocol. An RPC-specific communications protocol that supports the semantics of the DCE RPC API and runs over either connectionless or connection-oriented communications protocols.

RPC protocol sequence. A valid combination of communications protocols represented by a character string. Each RPC protocol sequence typically includes three protocols: a network protocol, a transport protocol, and an RPC protocol that works with the network and transport protocols. See *network protocol*, *RPC protocol*, and *transfer protocol*. Synonymous with *protocol sequence*.

S

schema. See *directory schema*.

Security Service. A DCE component that provides trustworthy identification of users, secure communications, and controlled access to resources in a distributed system.

segment. One or more contiguous elements of a string.

server. (1) On a network, the computer that contains programs, data, or provides the facilities that other computers on the network can access. (2) The party that receives remote procedure calls. Contrast with *client*.

server entry. RPC: A name service entry that stores the binding information associated with the RPC interfaces of a particular RPC server and object Universal Unique Identifiers (UUIDs) for any objects offered by the server. See also *binding information*, *NSI binding attribute*, *NSI object attribute*, *object* and *RPC interface*.

server stub. RPC: The surrogate calling code for an RPC interface that is linked with server application code containing one or more sets of remote procedures (managers) that implement the interface. See *client stub*. See also *manager*.

service. In network architecture, the capabilities that the layers closer to the physical media provide to the layers closer to the end user.

signal. Threads: To wake only one thread waiting on a condition variable. See *broadcast*.

sign-on. (1) A procedure to be followed at a terminal or workstation to establish a link to a computer. (2) To begin a session at a workstation. (3) Same as log on or log in.

simple name. CDS: One element in a CDS full name. Simple names are separated by slashes in the full name.

single sign-on. In z/OS DCE, single sign-on to DCE allows a z/OS user who has already been authenticated to an MVS external security manager, such as RACF, to be logged in to DCE. DCE does this automatically when a DCE application is started, if the user is not already logged in to DCE.

specific. XOM: The attribute types that can appear in an instance of a given class, but not in an instance of its superclasses.

standard. A model that is established and widely used.

string. An ordered sequence of bits, octets, or characters, accompanied by the string's length.

stub. RPC: A code module specific to an RPC interface that is generated by the Interface Definition Language (IDL) compiler to support remote procedure calls for the interface. RPC stubs are linked with client and server applications and hide the intricacies of remote procedure calls from the application code. See *client stub* and *server stub*.

subject identifier (SID). A string that identifies a user or set of users. Each SID consists of three fields in the form person.group.organization. In an account, each field must have a specific value; in an access control list (ACL) entry, one or more fields may use a wildcard.

synchronization. DTS: The process by which a Distributed Time Service entity requests clock values from other systems, computes a new time from the values, and adjusts its system clock to the new time.

syntax. (1) XOM: An object management (OM) syntax is any of the various categories into which the OM specification statically groups values on the basis of their form. These categories are additional to the OM type of the value. (2) A category into which an attribute value is placed on the basis of its form. See *attribute syntax*.

sysplex. Systems complex. Multiple MVS systems connected together to perform the processing for an installation.

T

TCP. Transmission Control Protocol

TCP/IP. Transmission Control Protocol/Internet Protocol

thread handle. RPC: A data item that enables threads to share a storage management environment.

time provider (TP). DTS: A process that queries universal time coordinated (UTC) from a hardware device and provides it to the server.

time provider program. DTS: An application that functions as a time provider.

tower. CDS: A set of physical address and protocol information for a particular server. CDS uses this information to locate the system on which a server resides and to determine which protocols are available at the server. Tower values are contained in the **CDS_Towers** attribute associated with the object entry that represents the server in the cell namespace.

transfer syntax. RPC: A set of encoding rules used for transmitting data over a network and for converting application data to and from different local data representations. See also *Network Data Representation*.

Transmission Control Protocol (TCP). A communications protocol used in Internet and any other network following the U.S. Department of Defense standards for inter-network protocol. TCP provides a reliable host-to-host protocol in packet-switched communication networks and in an interconnected system of such networks. It assumes that the Internet Protocol is the underlying protocol. The protocol that provides a reliable, full-duplex, connection-oriented service for applications.

Transmission Control Protocol/Internet Protocol (TCP/IP). A set of non-proprietary communications protocols that support peer-to-peer connectivity functions for both local and wide area networks.

type. XOM: A category into which attribute values are placed on the basis of their purpose. See *attribute type*.

type UUID. RPC: The Universal Unique Identifier (UUID) that identifies a particular type of object and an associated manager. See also *manager* and *object*.

U

UDP. User Datagram Protocol.

unexport. RPC: To remove binding information from a server entry in a name service database. Contrast with *export*.

Universal Time Coordinated (UTC). The basis of standard time throughout the world. Synonymous with Greenwich mean time (GMT).

Universal Unique Identifier (UUID). RPC: An identifier that is immutable and unique across time and space. A UUID can uniquely identify an entity such as an object or an RPC interface. See *interface UUID*, *object UUID*, and *type UUID*.

user. A person who requires the services of a computing system.

User Datagram Protocol (UDP). In TCP/IP, a packet-level protocol built directly on the Internet protocol layer. UDP is used for application-to-application programs between TCP/IP host systems.

UTC. Universal Time Coordinated

UUID. Universal unique identifier

V

value. XOM: An arbitrary and complex information item that can be viewed as a characteristic or property of an object. See *attribute value*.

Virtual Telecommunications Access Method (VTAM®). An IBM licensed program that controls communication and the flow of data in an SNA network. It provides single-domain, multiple-domain, and interconnected network capability.

VTAM. Virtual Telecommunications Access Method.

W

WAN. Wide area network.

wide area network (WAN). A network that provides communication services to a geographic area larger than that served by a local area network (LAN).

X

X.500. The CCITT/ISO standard for the open systems interconnection (OSI) application-layer directory. It allows users to register, store, search, and retrieve information about any objects or resources in a network or distributed system.

Bibliography

This bibliography is a list of publications for z/OS DCE and other products. The complete title, order number, and a brief description is given for each publication.

z/OS DCE Publications

This section lists and provides a brief description of each publication in the z/OS DCE library.

Overview

- *z/OS DCE Introduction*, GC24-5911

  This book introduces z/OS DCE. Whether you are a system manager, technical planner, z/OS system programmer, or application programmer, it will help you understand DCE and evaluate the uses and benefits of including z/OS DCE as part of your information processing environment.

Planning

- *z/OS DCE Planning*, GC24-5913

  This book helps you plan for the organization and installation of z/OS DCE. It discusses the benefits of distributed computing in general and describes how to develop plans for a distributed system in a z/OS environment.

Administration

- *z/OS DCE Configuring and Getting Started*, SC24-5910

  This book helps system and network administrators configure z/OS DCE.

- *z/OS DCE Administration Guide*, SC24-5904

  This book helps system and network administrators understand z/OS DCE and tells how to administer it from the batch, TSO, and shell environments.

- *z/OS DCE Command Reference*, SC24-5909

  This book provides reference information for the commands that system and network administrators use to work with z/OS DCE.

- *z/OS DCE User's Guide*, SC24-5914

  This book describes how to use z/OS DCE to work with your user account, use the directory service, work with namespaces, and change access to objects that you own.

Application Development

- *z/OS DCE Application Development Guide: Introduction and Style*, SC24-5907

  This book assists you in designing, writing, compiling, linking, and running distributed applications in z/OS DCE.

- *z/OS DCE Application Development Guide: Core Components*, SC24-5905

  This book assists programmers in developing applications using application facilities, threads, remote procedure calls, distributed time service, and security service.

- *z/OS DCE Application Development Guide: Directory Services*, SC24-5906

  This book describes the z/OS DCE directory service and assists programmers in developing applications for the cell directory service and the global directory service.

- *z/OS DCE Application Development Reference*, SC24-5908

  This book explains the DCE Application Program Interfaces (APIs) that you can use to write distributed applications on z/OS DCE.

Reference

- *z/OS DCE Messages and Codes*, SC24-5912

  This book provides detailed explanations and recovery actions for the messages, status codes, and exception codes issued by z/OS DCE.

z/OS SecureWay® Security Server Publications

This section lists and provides a brief description of books in the z/OS SecureWay Security Server library that may be needed for z/OS SecureWay Security Server DCE and for RACF® interoperability.

- *z/OS SecureWay Security Server DCE Overview*, GC24-5921

  This book describes the z/OS SecureWay Security Server DCE and provides z/OS SecureWay Security Server DCE information about the z/OS DCE library.

- *z/OS SecureWay Security Server LDAP Client Programming*, SC24-5924

  This book describes the Lightweight Directory Access Protocol (LDAP) client APIs that you can use to write distributed applications on z/OS DCE and gives you information on how to develop LDAP applications.

- *z/OS SecureWay Security Server RACF Security Administrator's Guide*, SA22-7683.

  This book explains RACF concepts and describes how to plan for and implement RACF.

- *z/OS SecureWay Security Server LDAP Server Administration and Use*, SC24-5923

  This book describes how to install, configure, and run the LDAP server. It is intended for administrators who will maintain the server and database.

- *z/OS SecureWay Security Server Firewall Technologies*, SC24-5922

  This book provides the configuration, commands, messages, examples and problem determination for the z/OS Firewall Technologies. It is intended for network or system security administrators who install, administer and use the z/OS Firewall Technologies.

Tool Control Language Publication

- *Tcl and the Tk Toolkit*, John K. Osterhout, (c)1994, Addison—Wesley Publishing Company.

  This non-IBM book on the Tool Control Language is useful for application developers, DCECP script writers, and end users.

IBM C/C++ Language Publication

- *z/OS C/C++ Programming Guide*, SC09-4765

  This book describes how to develop applications in the C/C++ language in z/OS.

z/OS DCE Application Support Publications

This section lists and provides a brief description of each publication in the z/OS DCE Application Support library.

- *z/OS DCE Application Support Configuration and Administration Guide*, SC24-5903

  This book helps system and network administrators understand and administer Application Support.

- *z/OS DCE Application Support Programming Guide*, SC24-5902

  This book provides information on using Application Support to develop applications that can access CICS® and IMS™ transactions.

Encina Publications

- *z/OS Encina Toolkit Executive Guide and Reference*, SC24-5919

  This book discusses writing Encina applications for z/OS.

- *z/OS Encina Transactional RPC Support for IMS*, SC24-5920

  This book is to help software designers and programmers extend their IMS transaction applications to participate in a distributed, transactional client/server application.

Index

Special Characters

A

B

C

D

E

G

I

K

L

Readers' Comments

z/OS
DCE Configuring and Getting Started
Publication No. SC24-5910-00

You may use this form to report errors, to suggest improvements, or to express your opinion on the appearance, organization, or completeness of this book.

Date: _____

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

Note

Report system problems to your IBM representative or the IBM branch office serving you.
U.S. customers can order publications by calling the IBM Software Manufacturing Solutions at **1-800-879-2755**.

In addition to using this postage-paid form, you may send your comments by:

FAX	1-607-752-2327	Internet	pubrcf@vnet.ibm.com
IBMLink	GDLVME(PUBRCF)		

Would you like a reply? ___**YES** ___ **NO** If yes, please tell us the type of response you prefer.

___ Electronic address: _____

___ FAX number: _____

___ Mail: (Please fill in your name and address below.)

Name _____ Address _____

Company or Organization _____

Phone No. _____

Readers' Comments
SC24-5910-00

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

Department G60
International Business Machines Corporation
Information Development
1701 North Street
ENDICOTT NY 13760-5553

Fold and Tape **Please do not staple** Fold and Tape

SC24-5910-00

Cut or Fold
Along Line

Program Number: 5694-A01

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

SC24-5910-00

Spine information:

z/OS DCE Configuring and Getting Started